Citrix NetScaler Command Reference Guide

Citrix® NetScaler® 9.1

Copyright and Trademark Notice

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler Request Switch™ 9000 Series equipment. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

Last Updated: June 2009

Contents

Preface

Before you begin to use the Citrix NetScaler 9.1 release, take a few minutes to review this chapter and learn about related documentation, other support options, and ways to send us feedback.

In This Preface

About This Guide

This guide provides a detailed description of all the commands. The contents of this guide are identical to the man pages. The chapters in this guide reflect the command groups.

Audience

This guide is intended for system and network administrators who configure and maintain Citrix NetScaler appliances.

Related Documentation

A complete set of documentation is available on the Documentation tab of your NetScaler and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/.)

To view the documentation

1. From a Web browser, log on to the NetScaler appliance.

2. Click the **Documentation** tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

Getting Service and Support

Citrix provides technical support primarily through the Citrix Solutions Network (CSN). Our CSN partners are trained and authorized to provide a high level of support to our customers. Contact your supplier for first-line support, or check for your nearest CSN partner at http://support.citrix.com/.

You can also get support from Citrix Customer Service at http://citrix.com/. On the **Support** menu, click **Customer Service**.

In addition to the CSN program and Citrix Customer Service, Citrix offers the following support options for Citrix NetScaler.

Knowledge Center

The Knowledge Center offers a variety of self-service, Web-based technical support tools at http://support.citrix.com/.

Knowledge Center features include:

- A knowledge base containing thousands of technical solutions to support your Citrix environment
- An online product documentation library
- Interactive support forums for every Citrix product
- Access to the latest hotfixes and service packs
- Knowledge Center Alerts that notify you when a topic is updated

---

Note: To set up an alert, sign in at http://support.citrix.com/ and, under **Products**, select a specific product. In the upper-right section of the screen, under **Tools**, click **Add to your Hotfix Alerts**. To remove an alert, go to the Knowledge Center product and, under **Tools**, click **Remove from your Hotfix Alerts**.

- Security bulletins
- Online problem reporting and tracking (for organizations with valid support contracts)

Silver and Gold Maintenance

In addition to the standard support options, Silver and Gold maintenance options are available. If you purchase either of these options, you receive documentation with special Citrix Technical Support numbers you can call.

Silver Maintenance Option

The Silver maintenance option provides unlimited system support for one year. This option provides basic coverage hours, one assigned support account manager for nontechnical relations management, four named contacts, and advanced replacement for materials.

Technical support is available at the following times:

- North America, Latin America, and the Caribbean: 8 A.M. to 9 P.M. U.S. Eastern Time, Monday through Friday
- Asia (excluding Japan): 8 A.M. to 6 P.M. Hong Kong Time, Monday through Friday
- Australia and New Zealand: 8 A.M. to 6 P.M. Australian Eastern Standard Time (AEST), Monday through Friday
- Europe, Middle East, and Africa: 8 A.M. to 6 P.M. Coordinated Universal Time (Greenwich Mean Time), Monday through Friday

Gold Maintenance Option

The Gold maintenance option provides unlimited system support for one year. Support is available 24 hours a day, 7 days a week. There is one assigned support account manager for nontechnical relations management, and there are six named contacts.

Subscription Advantage

Your product includes a one-year membership in the Subscription Advantage program. The Citrix Subscription Advantage program gives you an easy way to stay current with the latest software version and information for your Citrix products. Not only do you get automatic access to download the latest feature releases, software upgrades, and enhancements that become available during the term of your membership, you also get priority access to important Citrix technology information.

You can find more information on the Citrix Web site at http://www.citrix.com/ (on the **Support** menu, click **Subscription Advantage**).

You can also contact your sales representative, Citrix Customer Care, or a member of the Citrix Solutions Advisors program for more information.

Education and Training

Citrix offers a variety of instructor-led and Web-based training solutions. Instructor-led courses are offered through Citrix Authorized Learning Centers (CALCs). CALCs provide high-quality classroom learning using professional courseware developed by Citrix. Many of these courses lead to certification.

Web-based training courses are available through CALCs, resellers, and from the Citrix Web site.

Information about programs and courseware for Citrix training and certification is available at http://www.citrixtraining.com.

Documentation Feedback

You are encouraged to provide feedback and suggestions so that we can enhance the documentation. You can send email to the following alias or aliases, as appropriate. In the subject line, specify "Documentation Feedback." Be sure to include the document name, page number, and product release version.

- For NetScaler documentation, send email to nsdocs_feedback@citrix.com.
- For Command Center documentation, send email to ccdocs_feedback@citrix.com.
- For Access Gateway documentation, send email to agdocs_feedback@citrix.com.

You can also provide feedback from the Knowledge Center at http://support.citrix.com/.

To provide feedback from the Knowledge Center home page

1. Go to the Knowledge Center home page at http://support.citrix.com/.
2. On the Knowledge Center home page, under **Products**, expand **NetScaler Application Delivery**, and then click **NetScaler Application Delivery Software 9.1**.>
3. On the **Documentation** tab, click the guide name, and then click **Article Feedback**.
4. On the **Documentation Feedback** page, complete the form, and then click **Submit**.

Introduction - Classic CLI

Welcome to the Command Reference Guide. This reference covers all aspects of using the Command Line Interface in the configuration and operation of the system. For information on accessing your system's Command Line Interface, please refer to the installation chapter in the Installation and Configuration Guide before continuing on from this point.

How to use This Reference

This command reference consists of three chapters:

- Chapter 1: The Command Line Overview which explains how to use the Command Line Interface.
- Chapter 2: The Command Line Overview which explains how to use the Contextual Command Line Interface (CCLI).
- Chapter 3: Alphabetically ordered descriptions of all of the commands.

If you are unfamiliar with using the system, you should start with the CLI usage chapter to familiarize yourself with the interface after reviewing the following section on document conventions. Otherwise, this document serves as the primary source of information on the commands available in the NSCLI and may be accessed at any arbitrary point as your needs dictate.

Command Conventions

These conventions are used to describe the commands in this guide.

Convention	**Alerts You To**
command	Command and argument names can be entered in any combination of upper and lower case characters. In this document command and argument names are sometimes displayed in upper and lower case. This is for readability and does not reflect the way in which the commands must be entered.
command argument	This typeface represents a command argument.
screen text	Text with this typeface represents information on a screen, as well as the names of directories, files, and commands.
<key name>+<key name>	Keyboard key names appear within angle brackets. A plus sign appears between keys you must press simultaneously.

text in italics	Italic type emphasizes text or indicates new terms.
Square Brackets ([ ])	Arguments that are contained within square brackets are optional. Arguments that are not contained within brackets are required
Angle Brackets (< >)	Arguments within angle brackets are variable place holders. Replace these with values appropriate for your configuration.
Vertical Bars (|)	When arguments are separated by vertical bars, either argument can be specified.

Note: When entering the argument, neither the brackets nor the vertical bars are included.

Command Line Overview

This section discusses the usage of the Command Line Interface. The discussion is broken up in to two sections, basic and advanced CLI usage. The basic section covers all of the rudimentary aspects of the CLI which provides the information necessary for basic CLI usage. The advanced usage section expands on the remaining features of the Command Line Interface which allow you to further control and enhance your sessions but are not required for day to day operation.

Basic Command Line Usage

This section discusses the essential instruction necessary for basic command line usage with the system. Start with this section if you are unfamiliar with the CLI.

Understanding the Command Structure

Most commands adhere to the general format shown here.

```
action groupname entity <entityname> [-parameter]
```

An action is the task that the command is performing such as an add or set action. The groupname is the functional area or feature where the action is being taken such as dns or lb. An entity is the specific type of object such as a vserver that the command is being issued against. The entityname is the name given to an entity instance that the command is being issued upon. If an entity instance is being created with the issued command, such as with the add action, the entityname will be a name of your choosing. Lastly, the parameters applicable to the command are listed. The actual number and type of available parameters will vary by command.

Getting Help in the CLI

The help command offers a quick way to get more information on commands. The command can return help on specific commands, groups of commands, or the entire set of nscli commands.

By typing help alone on the command line, the system will print a brief general help message as shown here.

```
> help

  nscli - command-line interface to NetScaler

  Try :
    help <commandName> for full usage of a specific command
```

```
   help <groupName>   for brief usage of a group of commands
   help -all          for brief usage of all nscli commands


 The command groups are:
       basic                  aaa                    authentication
       authorization          cache                  cli
       cmp                    cr                     cs
       dns                    dos                    filter
       gslb                   lb                     ns
       policy                 pq                     router
       snmp                   sc                     ssl
       system                 tunnel                 vpn
 Done
>
```

And by entering help help, you will see the following output which shows the syntax for the help command.

```
> help help
Usage:  help  [(commandName) | (<groupName> | [-all]) |]
 Done
>
```

If you need help on using a specific command or command group, utilize the syntax shown above substituting that command or group name you need help for.By specifying the command name, the CLI feedback will provide you with a full listing of the command's syntax along with an expansion on those parameters with limited sets of options.If you enter a group name, the CLI will print a full list of the commands that belong to that group. The output below shows an example of using this help method for the add vserver command.

```
> help add vserver


Usage:  add vserver <vServerName>@ <serviceType> [<IPAddress> @
           <port> -range <positive_integer>] [-cacheType <cacheType>]
        [-backupVServerName <string>] [-redirectURL <URL>]
        [-cacheable ( YES | NO )] [-cltTimeout <secs>]
        [-soMethod ( CONNECTION | NONE )]
        [-soPersistence ( ENABLED | DISABLED )]
        [-soPersistenceTimeOut <positive_integer>]
        [-soThreshold <positive_integer>] [-state (
        ENABLED | DISABLED )]


 where:
    <serviceType> = ( HTTP | FTP | TCP | UDP | SSL | SSL_BRIDGE |
    SSL_TCP | NNTP | DNS | DHCPRA | ANY )
    <cacheType> = ( TRANSPARENT | REVERSE | FORWARD )
```

```
 Done
>
```

The question mark **<?>** can also be used to get help in the CLI. By typing a question mark alone, the system will print out a listing of all the actions available from the top level command structure.

Getting Help with Man Pages

The command line interface has it's own set of man pages similar to those traditionally found in UNIX and UNIX like operating systems. This system returns the same command reference information as is found in this guide. To use this help feature, issue the man command using the name of the command you wish to view information on as the argument.

Once the first screen is displayed, you may scroll through the page either a screen at a time or line by line. To advance line by line, press the **<Enter>** key. To advance to the next screen use the space bar.

When viewing commands with man, to exit the page before reaching the end of it, press the **<Q>** key.

Using Command Completion

When working on the command line, you can use both the **<Tab>** key or the **<?>** key for command completion and assistance. For example, typing show e followed by entering the **<Tab>** key will complete the command as show expression. If, after typing **<Tab>** once and no completion is displayed, then hit **<Tab>** once more and the system will offer you a set of possible completions.After the output is displayed, you are returned to the prompt with the portion of the command that was previously entered so that you may continue where you left off at.

Using the question mark key offers a slightly different completion options.You may enter a question mark at any point on the command line and the system will provide you with a list of all possible completions that are recognized from that point forward. The following example illustrates this usage with the enable command.

```
> enable <?>
acl           fipsSIMsource mode          service
alarm         fipsSIMtarget monitor       snmp ...
arp           interface     ns ...        ssl ...
feature       ip           server       vserver
> enable
```

Once the possible completions are printed, you are again returned to the command line with your previous entry still at the prompt for you to work with. Note that the question mark you type is not echoed at the CLI prompt.

Any entries in the output that are followed by the ellipsis, such as the ssl command shown in the previous example's output, have further command completion levels beyond this point in the hierarchy.

Utilizing Command Abbreviations and Shortcuts

Another way to shorten command line input is to use command abbreviations. The CLI command abbreviation feature allows you to enter partial commands. To use this feature, you need only enter enough of the command's key words such that each of them is uniquely identifiable by the CLI. For example, to shorten the command add lb vserver, you may enter as little as ad lb vs and the CLI will correctly interpret your command.

Note however, that for command group names you may not abbreviate them. In many cases you may leave them out entirely though. This is possible wherever command usage makes the group implicit, such as with the snmp and system group names when the entity type being acted upon is unique to the group. For example, there are no other entities of the community type outside of the snmp command group so issuing the add community command, rather than add snmp community, implicitly places this command in the snmp command group.

This behavior is also illustrated with the system group and its entities. The user entity type exists in the system command group as well as the aaa command group therefore the user entity is not unique to the system group. So if you are issuing an action against a system user, such as an add command, you must specify the system group type so that the CLI will interpret your command as being directed at a system user, not an aaa user. The CLI will alert you in those cases where the group type is omitted incorrectly with an "ERROR: No such command" message.

More examples of using these shortcuts are shown in Table 1.1

Table 1: Sample Command Abbreviations

Abbreviated Command	CLI Interpreted Command
cl r	clear ns rnat
sh ve	show ns version
se vpn p	set vpn parameters
f f	force ns failover
rm mx	rm dns mxRec
ad lb vs	add lb vserver
ad pol exp a e	add policy expression

Navigating Command Output

Often times, you will find that the screen output from the NSCLI will span multiple screens. When an output stream pauses at the first screen’s worth of output with --More-- displayed, you can navigate the remaining output with keystrokes.

- To cancel viewing the remaining output, press the <Q> key or use <Ctrl>+<C> to abort the command.
- To stream the remaining output without pauses, press the <C> key.
- To advance through the output one screen at a time press any other key.

Understanding Error Feedback

When a CLI command is entered with invalid arguments, an error message is displayed, possibly preceded by an indication of the location of the error within the command line. After most errors, a short version of the command usage is also displayed.

For example, typing the following command at the prompt:

```
> add vserver vs 1 htto 10.101.4.99 80
```

Returns the following error messages:

```
add vserver vs1 htto 10.101.4.99 80
                ^^^^
```

ERROR: invalid argument value [serviceType, htto]

The carats ("^^^^"), if present, indicate the location of the error in the command line.

Note: The CLI will alert you if you try to configure a disabled or unlicensed feature. If you attempt to configure disabled features, your configurations will be applied, however they will have no effect on the runtime behavior of the system until the feature is enabled. If you attempt to configure an unlicensed feature, the system will return an error.

Accessing the Command History

The command line maintains a per user command entry history across sessions. This history maintains the last 100 user entered commands. Note that the history does not record sequentially duplicated commands. You may loop through the history on the command line by using the up and down arrow keys on your keyboard. You can recall the entire history log using the history command. A sample of the history log output is shown here.

```
> history
     1  21:31   sh version
     2  21:31   man save ns config
     3  21:31   builtins
     4  21:32   help authentication
     5  21:44   help
     6  21:52   history
     7  21:53   exit
     8  21:53   history
>
```

You can also recall specific entries from within the history using the exclamation mark, or bang character (!). Use the ! in combination with either the desired history event number or an offset from the current event number to recall a specific history entry.

Advanced Command Line Usage

This section illustrates the remaining advanced features of the Command Line Interface.

Understanding NSCLI Built-ins

The Command Line Interface has several tools, or builtins, at your disposal for use within CLI sessions. To view these builtins use the builtins command. In addition to the previously mentioned history builtin tool, the use of other builtins can be used as discussed in the following sections.

Compounding CLI Commands

The nscli supports using the semicolon (;) character to enter multiple commands. To use this function, simply enter a semicolon between commands on the command line. The commands will be executed in order of entry.

Using grep, more, and the Pipe Operator

To help in managing and navigating command output the nscli supports the standard UNIX grep and more commands as well as the pipe operator (|). For the grep and more commands refer to the man pages in the nscli for complete usage details.

The pipe operator is used in the nscli as it is on standard UNIX shells to redirect command output into another command, commonly with the grep and more commands.

Applying Formatting Options

In the nscli, most show commands have an implicit –format argument. This argument formats the command's output in one of three ways.

Normally the show server command outputs to the screen as shown here.

```
> show server
        2 servers:
1)      Name:  s1               IPAddress:  10.10.10.11
        State:  ENABLED
2)      Name:  s2               IPAddress:  10.10.10.12
        State:  ENABLED
 Done
>
```

With the -format input option, the show server command prints in the command form that it would be input to the CLI, as shown here.

```
> show server -format input
        2 servers:
add server s1 10.10.10.11
add server s2 10.10.10.12
 Done
>
```

The second formatting option, -format hierarchical, prints in a Cisco-like hierarchical format.

```
> show server -format hierarchical
        2 servers:
server s1
        IPAddress: 10.10.10.11
server s2
        IPAddress: 10.10.10.12
 Done
>
```

And the third type of formatting option, -format xhierarchical, prints the output in a Juniper-like hierarchical format

```
> show server -format xhierarchical
        2 servers:
server s1 {
        IPAddress 10.10.10.11;
}
server s2 {
        IPAddress 10.10.10.12;
}
```

```
 Done
>
```

Creating and Using Aliases

In order to allow you to customize your own command shortcuts, the system supports using aliases. To create a command alias you will need to use the alias command followed by the desired alias name and the command you wish to alias. For example, to create an alias for the show system users command you would enter the command as shown below.

```
> alias users show system users
```

To use the new alias, specify it as you would any other command.

```
> users
        1 Configured system user:
1)      User name: nsroot
 Done
>
```

And to view the established aliases, use the alias command alone on the command line.

```
> alias
users   (show system users)
>
```

To delete an alias, use the unalias command.

```
> unalias users
>
```

Customizing the CLI Prompt

By default for all users, the CLI prompt is marked by the > character. You may customize the prompt to display differently using the set cli prompt command. The possible settings and parameters are listed in the following table followed by an example use of the command.

Table 2: Prompt Settings

Parameter	Prompt Displays
%!	Current history event number
%u	User name
%h, %m	Configured hostname
%t	Current system time
%T	Current system time in 24 hour format
%d	Current date

Example:

```
> set cli prompt "%[T] %u@%h"
 Done
[22:23] nsroot@localhost>
```

Notice that you need to enclose the parameter in double quotes. You may chain multiple parameters together in addition to arbitrary strings and spaces to further customize the prompt. To do this, just include the desired string and parameters within a single double quoted string, as shown in the above example. If you would like to reset the prompt back to the system default, use the clear cli prompt command.

To ensure that your prompt setting is retained across sessions, save your configuration once your desired prompt is set. This command prompt setting will apply only to the current system user.

Using the @ Range Operator

Many CLI commands allow for the creation and manipulation of a range of entities. Any command that has the **@** symbol in its parameter listing is one of these commands. The presence of the range operator means that the argument it follows may be used with a range specification in order to act on a consecutive array of entities. To use these arguments with a range, you simply specify the argument normally and follow it with a bracketed range.

For example, the command for creating a range of five load balancing vservers would use the following syntax:

```
> add lb vserver httpvserve[1-5] http 192.168.1.1[1-5] 80
```

Notice that the IP address argument also specifies an address range. When adding a range of entities as shown here, dependant arguments must have a matching range specified as well. The command will return an error if the ranges differ. When you use an add command with the range option as shown here, the system will create 5 vservers with IP addresses ranging from 192.168.1.11 to 192.168.1.15.

When alternately deleting a range of entities, the same methodology applies. To remove the range of vservers created in this example, you would issue the following command:

```
> rm vserver httpvserve[1-5]
 Done
>
```

Note: If a range of entities created with the range operation is somehow broken, such as via the manual removal of one or more of the entities, using the corresponding rm or set commands with a range operation against the range will not complete successfully.

Executing Looped Commands

The nscli allows for the use of UNIX shell style loops for repeated execution of commands. The example here uses this functionality to create ten http vservers with IP addresses 1.1.1.25 to 1.1.1.34.

```
> @ n = 10
> @ x = 25
> while ($n)
add vserver test$n http 1.1.1.$x 80
@ n--
@ x++
end
 Done
 Done
 Done
 Done
```

```
 Done
 Done
 Done
 Done
 Done
 Done
>
```

The primary keywords available in the nscli for using this feature are while, end, and the @ operator. More details on these keywords are available in the respective man pages for each of them as well as their Command Reference descriptions in this reference.

Introduction - Contextual CLI

Welcome to the Command Reference Guide. This reference covers all aspects of using the Command Line Interface in the configuration and operation of the system. For information on accessing your system's Command Line Interface, please refer to the Installation chapter in the Installation and Configuration Guide before continuing on from this point.

How to use This Reference

This command reference consists of three chapters:

- Chapter 1: The Command Line Overview which explains how to use the Command Line Interface.
- Chapter 2: The Command Line Overview which explains how to use the Contextual Command Line Interface (CCLI).
- Chapter 3: Alphabetically ordered descriptions of all of the commands.

If you are unfamiliar with using the system, you should start with the CLI usage chapter to familiarize yourself with the interface after reviewing the following section on document conventions. Otherwise, this document serves as the primary source of information on the commands available both in the NSCLI and CCLI and may be accessed at any arbitrary point as your needs dictate.

Command Conventions

These conventions are used to describe the commands in this guide.

Convention	Alerts You To
command	Command and argument names can be entered in any combination of upper and lower case characters. In this document command and argument names are sometimes displayed in upper and lower case. This is for readability and does not reflect the way in which the commands must be entered.
command argument	This typeface represents a command argument.
screen text	Text with this typeface represents information on a screen, as well as the names of directories, files, and commands.
<key name>+<key name>	Keyboard key names appear within angle brackets. A plus sign appears between keys you must press simultaneously.

text in italics	Italic type emphasizes text or indicates new terms.
Square Brackets ([ ])	Arguments that are contained within square brackets are optional. Arguments that are not contained within brackets are required
Angle Brackets (< >)	Arguments within angle brackets are variable place holders. Replace these with values appropriate for your configuration.
Vertical Bars (|)	When arguments are separated by vertical bars, either argument can be specified.

Note: When entering the argument, neither the brackets nor the vertical bars are included.

Command Line Overview

This section discusses the usage of the Contextual Command Line Interface. The discussion is broken up in to two sections, basic and advanced CLI usage. The basic section covers all of the rudimentary aspects of the CLI which provides the information necessary for basic CCLI usage. The advanced usage section expands on the remaining features of CCLI, which allow you to further control and enhance your sessions, but are not required for day to day operation.

Basic Command Line Usage

This section discusses the essential instruction necessary for basic command line usage with the system. Start with this section if you are unfamiliar with the CLI.

Understanding the Contextual CLI

To use CCLI, execute the config command at the command prompt. This is the top-level context from where the user can access the other contexts.

```
> config
 Done
config>
```

To configure system entities, you must enter a child context from the config context. To view all the child contexts, type ? at the command prompt. This command works at all contexts.

```
config>
        aaa ...
        audit ...
        authentication ...
        authorization ...
        cache ...
        cli ...
        cmp ...
        cr ...
        cs ...
        dns ...
        dos ...
```

```
        filter ...
        gslb ...
        lb ...
        ns ...
        policy ...
        pq ...
        protocol ...
        rewrite ...
        router ...
        snmp ...
        sc ...
        ssl ...
        system ...
        tunnel ...
        vpn ...
        server
        service
        serviceGroup
        monitor
        vlan
        interface
        channel
        lacp
        location
        locationParameter
        locationFile
```

To create an entity, you need to specify all the required arguments at the 'config' prompt.

```
config> lb vserver vlb1 http
```

This creates a load balancing vserver named vlb1.

Note: The name need not always be the only key argument for an entity. For commands corresponding to SNMP traps, the 'trapclass' and 'trapdestination' are the key arguments for uniquely identifying the entity.

Notice that the prompt changes to display the context and the system entity being accessed. Once you reach the context corresponding to a system entity, you can execute commands to view and modify the parameters of the entity. In the following example, the persistence on the vserver is set to SOURCEIP.

```
config lb vserver vlb1> persistenceType SOURCEIP
 Done
config lb vserver vlb1> sh
lb vserver vlb1 HTTP 80 -range 1
        IPAddress 10.102.29.52
```

```
        persistenceType SOURCEIP
        persistenceBackup NONE
        lbMethod LEASTCONNECTION
        persistMask 255.255.255.255
        pq OFF
        sc OFF
        m IP
        dataLength 0
        dataOffset 0
        sessionless DISABLED
        timeout 2
        connfailover DISABLED
        cacheable NO
        soMethod NONE
        soPersistence DISABLED
        soPersistenceTimeOut 2
        redirectPortRewrite DISABLED
        sendRespVsvrDown DISABLED
!


 Done
```

When you type the name of an entity at the command prompt, the system transfers you to the entity specific-context if the entity exists. For example, when you type lb vserver vlb1, the prompt changes to config lb vserver vlb1. This is because the vserver vlb1 already exists.

```
config> lb vserver vlb1
config lb vserver vlb1>
```

However, if the entity does not exist, an error message is displayed. This is illustrated in the following example. Here, the vserver vlb2 does not exist.

```
config> lb vserver vlb2
ERROR: No such resource [vserver, vlb2]
```

It is usually necessary to enter additional parameters to create a new entity:

```
config> lb vserver vlb2 http 10.101.20.20 80
config lb vserver vlb2>
```

Some commands which are not strictly part of the current context can be executed in context, and are implicitly applied to the entity. Here the show command is executed at the entity-specific context corresponding to the vserver, vlb1.

```
config lb vserver vlb1> show
lb vserver vlb1 HTTP 80 -range 1
        IPAddress 10.102.29.52
        persistenceType SOURCEIP
        persistenceBackup NONE
        lbMethod LEASTCONNECTION
```

```
        persistMask 255.255.255.255
        pq OFF
        sc OFF
        m IP
        dataLength 0
        dataOffset 0
        sessionless DISABLED
        timeout 2
        connfailover DISABLED
        cacheable NO
        soMethod NONE
        soPersistence DISABLED
        soPersistenceTimeOut 2
        redirectPortRewrite DISABLED
        sendRespVsvrDown DISABLED
!

 Done
```

To modify another entity, you must return to the config context and enter the context of the other entity.

```
config lb vserver vlb1> persistenceType SRCIPDESTIP
 Done
config lb vserver vlb1> exit
 Done
config> lb vserver vlb2
config lb vserver vlb2> persistenceType SRCIPDESTIP
 Done
```

To delete an entity or disable an attribute, use the ‘no’ command. This is illustrated by the following examples.

```
config> no lb vserver vlb1
Done
```

Getting Help in the CLI

The help command offers a quick way to get more information on commands. The command can return help on specific commands, groups of commands, or the entire set of nscli commands.

By typing help alone on the command line, the system will print a brief general help message as shown here.

```
config> help

   NetScaler command-line interface

   Try :
```

```
    'help <commandName>' for full usage of a specific command
    'help <groupName>'   for brief usage of a group of commands
    'help -all'          for brief usage of all nscli commands
    'man <commandName>'  for a complete command description

    '?' will show possible completions in the current context

The command groups are:
      basic                 aaa                   audit
      authentication        authorization         cache
      cli                   cmp                   cr
      cs                    dns                   dos
      filter                gslb                  lb
      ns                    policy                pq
      protocol              rewrite               router
      snmp                  sc                    ssl
      system                tunnel                vpn
Done
```

If you need help on using a specific command or command group, utilize the syntax shown above substituting that command or group name you need help for. By specifying the command name, the CLI feedback will provide you with a full listing of the command's syntax along with an expansion on those parameters with limited sets of options.If you enter a group name, the CLI will print a full list of the commands that belong to that group. The question mark <**?**> can also be used to get help in the CLI. By typing a question mark alone, the system will print out a listing of all the actions available from the top level command structure.

Getting Help with Man Pages

The command line interface has it’s own set of man pages similar to those traditionally found in UNIX and UNIX like operating systems. This system returns the same command reference information as is found in this guide. To use this help feature, issue the man command using the name of the command you wish to view information on as the argument.

Once the first screen is displayed, you may scroll through the page either a screen at a time or line by line. To advance line by line, press the <**Enter**> key. To advance to the next screen use the space bar.

When viewing commands with man, to exit the page before reaching the end of it, press the <**Q**> key.

Using Command Completion

When working on the command line, you can use both the <**Tab**> key or the <**?**> key for command completion and assistance. For example, typing show e followed by entering the <**Tab**> key will complete the command as show expression. If, after typing <**Tab**> once and no completion is displayed, then hit <**Tab**> once more and the system will offer you a set of possible completions.After the output is displayed, you are returned to the prompt with the portion of the command that was previously entered so that you may continue where you left off at.

Using the question mark key offers a slightly different completion options.You may enter a question mark at any point on the command line and the system will provide you with a list of all possible completions that are recognized from that point forward. The following example illustrates this usage with the enable command.

```
> enable <?>
acl           fipsSIMsource mode          service
alarm         fipsSIMtarget monitor       snmp ...
arp           interface     ns ...        ssl ...
feature       ip           server       vserver
> enable
```

Once the possible completions are printed, you are again returned to the command line with your previous entry still at the prompt for you to work with. Note that the question mark you type is not echoed at the CLI prompt.

Any entries in the output that are followed by the ellipsis, such as the ssl command shown in the previous example's output, have further command completion levels beyond this point in the hierarchy.

Utilizing Command Abbreviations and Shortcuts

Another way to shorten command line input is to use command abbreviations. The CLI command abbreviation feature allows you to enter partial commands. To use this feature, you need only enter enough of the command's key words such that each of them is uniquely identifiable by the CLI. For example, to shorten the command add lb vserver, you may enter as little as ad lb vs and the CLI will correctly interpret your command.

Note however, that for command group names you may not abbreviate them. In many cases you may leave them out entirely though. This is possible wherever command usage makes the group implicit, such as with the snmp and system group names when the entity type being acted upon is unique to the group. For example, there are no other entities of the community type outside of the snmp command group so issuing the add community command, rather than add snmp community, implicitly places this command in the snmp command group.

This behavior is also illustrated with the system group and its entities. The user entity type exists in the system command group as well as the aaa command group therefore the user entity is not unique to the system group. So if you are issuing an action against a system user, such as an add command, you must specify the system group type so that the CLI will interpret your command as being directed at a system user, not an aaa user. The CLI will alert you in those cases where the group type is omitted incorrectly with an "ERROR: No such command" message.

More examples of using these shortcuts are shown in Table 1.1

Table 3: Sample Command Abbreviations

Abbreviated Command	CLI Interpreted Command
cl r	clear ns rnat
sh ve	show ns version
se vpn p	set vpn parameters
f f	force ns failover
rm mx	rm dns mxRec
ad lb vs	add lb vserver

Abbreviated Command	CLI Interpreted Command
ad pol exp	add policy expression
a e	

Navigating Command Output

Often times, you will find that the screen output from the NSCLI will span multiple screens. When an output stream pauses at the first screen's worth of output with --More-- displayed, you can navigate the remaining output with keystrokes.

- To cancel viewing the remaining output, press the <Q> key or use <Ctrl>+<C> to abort the command.
- To stream the remaining output without pauses, press the <C> key.
- To advance through the output one screen at a time press any other key.

Understanding Error Feedback

When a CLI command is entered with invalid arguments, an error message is displayed, possibly preceded by an indication of the location of the error within the command line. After most errors, a short version of the command usage is also displayed.

For example, typing the following command at the prompt:

```
> add vserver vs 1 htto 10.101.4.99 80
```

Returns the following error messages:

```
add vserver vs1 htto 10.101.4.99 80
                ^^^^
```

ERROR: invalid argument value [serviceType, htto]

The carats ("^^^^"), if present, indicate the location of the error in the command line.

Note: The CLI will alert you if you try to configure a disabled or unlicensed feature. If you attempt to configure disabled features, your configurations will be applied, however they will have no effect on the runtime behavior of the system until the feature is enabled. If you attempt to configure an unlicensed feature, the system will return an error.

Accessing the Command History

The command line maintains a per user command entry history across sessions. This history maintains the last 100 user entered commands. Note that the history does not record sequentially duplicated commands. You may loop through the history on the command line by using the up and down arrow keys on your keyboard. You can recall the entire history log using the history command. A sample of the history log output is shown here.

```
> history
     1  21:31   sh version
     2  21:31   man save ns config
     3  21:31   builtins
     4  21:32   help authentication
     5  21:44   help
```

```
     6  21:52   history
     7  21:53   exit
     8  21:53   history
>
```

You can also recall specific entries from within the history using the exclamation mark, or bang character (!). Use the ! in combination with either the desired history event number or an offset from the current event number to recall a specific history entry.

Advanced Command Line Usage

This section illustrates the remaining advanced features of the Command Line Interface.

Compounding CLI Commands

The nscli supports using the semicolon (;) character to enter multiple commands. To use this function, simply enter a semicolon between commands on the command line. The commands will be executed in order of entry. This is illustrated by the following example.

```
> add service SVC10 10.102.11.11 HTTP 80 ; add service SVC20 10.102.11.12 HTTP 80
```

Using grep, more, and the pipe Operator

To help in managing and navigating command output the CLI supports the standard UNIX grep and more commands as well as the pipe operator (|). For the grep and more commands, refer to the man pages for complete usage details.

The pipe operator is used as it is on standard UNIX shells to redirect command output into another command, commonly with the grep and more commands.

Applying Formatting Options

In the nscli, most show commands have an implicit –format argument. This argument formats the command's output in one of three ways.

Normally the show server command outputs to the screen as shown here.

```
> show server
        2 servers:
1)      Name:  s1               IPAddress:  10.10.10.11
        State:  ENABLED
2)      Name:  s2               IPAddress:  10.10.10.12
        State:  ENABLED
 Done
>
```

In addition, CCLI supports the following output formats:

- INPUT - When this format is specified, the output is displayed in the contextual format. This is illustrated as follows.

```
config> sh lb vserver -format INPUT
lb vserver vlb1 HTTP 80
        IPAddress 10.102.29.52
!
```

```
lb vserver vdns DNS 53
        IPAddress 10.102.29.53
        persistenceType NONE
```

- OLD - When this format is specified, the output is displayed in the Classic CLI format. This is illustrated as follows.

```
config> sh lb vserver -format OLD
add lb vserver vlb1 HTTP 10.102.29.52 80
add lb vserver vdns DNS 10.102.29.53 53 -persistenceType NONE
```

- TEXT - When this format is specified, the output is displayed with all the details of the entity. This is illustrated as follows.

```
config> sh lb vserver -format TEXT
1)      Name:  vlb1             Value:
        IPAddress:  10.102.29.52 Port:  80
        Range:  1               ServiceType:  HTTP
        Type:  ADDRESS          State:  UP
        EffectiveState:  UP     Status:  3
        CacheType:  SERVER      Redirect:
        Precedence:             RedirectURL:
        Authentication:  OFF    HomePage:  ""
        DnsVserverName:  ""     Domain:  a.com
        Rule:  ""               PolicyName:  ""
        ServiceName:  ""        Weight:  0
        CacheVserver:  ""       BackupVServer:  ""
        Priority:  0            CltTimeout:  180
        SoMethod:  NONE         SoPersistence:  DISABLED
        SoPersistenceTimeOut:  2 SoThreshold:  0
        SoDynamicThreshold:  0  LbMethod:  LEASTCONNECTION
        HashLength:  0          DataOffset:  0
        DataLength:  0          Netmask:  0.0.0.0
        Rule:  ""               GroupName:  dqfw
        M:  IP                  PersistenceType:  COOKIEINSERT
        CookieDomain:  a.com    PersistMask:  255.255.255.255
        PersistenceBackup:  NONE Timeout:  2
        Cacheable:  NO          Pq:  OFF
        Sc:  OFF                Sessionless:  DISABLED
        Map:  OFF               Connfailover:  DISABLED
        RedirectPortRewrite:  DISABLED SendRespVsvrDown:  DISABLED
2)      Name:  vdns             Value:
        IPAddress:  10.102.29.53 Port:  53
        Range:  1               ServiceType:  DNS
        Type:  ADDRESS          State:  UP
```

```
        EffectiveState:  UP      Status:  3
        CacheType:  SERVER       Redirect:
        Precedence:              RedirectURL:
        Authentication:  OFF     HomePage:  ""
        DnsVserverName:  ""      Domain:  ""
        Rule:  ""                PolicyName:  ""
        ServiceName:  ""         Weight:  0
        CacheVserver:  ""        BackupVServer:  ""
        Priority:  0             CltTimeout:  120
        SoMethod:  NONE          SoPersistence:  DISABLED
        SoPersistenceTimeOut:  2 SoThreshold:  0
        SoDynamicThreshold:  0   LbMethod:  LEASTCONNECTION
        HashLength:  0           DataOffset:  0
        DataLength:  0           Netmask:  0.0.0.0
        Rule:  ""                GroupName:  ""
        M:  IP                   PersistenceType:  NONE
        CookieDomain:  ""        PersistMask:  255.255.255.255
        PersistenceBackup:  NONE Timeout:  2
        Cacheable:  NO           Pq:  OFF
        Sc:  OFF                 Sessionless:  DISABLED
        Map:  OFF                Connfailover:  DISABLED
        RedirectPortRewrite:  DISABLED SendRespVsvrDown:  DISABLED
```

- DECORATED - When this format is specified, the output is displayed in the contextual format with braces and semicolons. This is illustrated as follows.

```
config> sh lb vserver -format DECORATED
lb vserver vlb1 HTTP 80 {
        IPAddress 10.102.29.52;
};
lb vserver vdns DNS 53 {
        IPAddress 10.102.29.53;
        persistenceType NONE;
};
```

Creating and Using Aliases

In order to allow you to customize your own command shortcuts, the system supports using aliases. To create a command alias you will need to use the alias command followed by the desired alias name and the command you wish to alias. For example, to create an alias for the show system users command you would enter the command as shown below.

```
> alias users show system users
```

To use the new alias, specify it as you would any other command.

```
> users
        1 Configured system user:
```

```
1)      User name: nsroot
 Done
>
```

And to view the established aliases, use the alias command alone on the command line.

```
> alias
users   (show system users)
>
```

To delete an alias, use the unalias command.

```
> unalias users
>
```

Customizing the CLI Prompt

By default for all users, the CLI prompt is marked by the > character. You may customize the prompt to display differently using the set cli prompt command. The possible settings and parameters are listed in the following table followed by an example use of the command.

Table 4: Prompt Settings

Parameter	Prompt Displays
%!	Current history event number
%u	User name
%h, %m	Configured hostname
%t	Current system time
%T	Current system time in 24 hour format
%d	Current date

Example:

```
config> set cli prompt "%T %u@%h"
 Done
10:47 nsroot@localhost config>
```

Notice that you need to enclose the parameter in double quotes. You may chain multiple parameters together in addition to arbitrary strings and spaces to further customize the prompt. To do this, just include the desired string and parameters within a single double quoted string, as shown in the above example. If you would like to reset the prompt back to the system default, use the clear cli prompt command.

To ensure that your prompt setting is retained across sessions, save your configuration once your desired prompt is set. This command prompt setting will apply only to the current system user.

Using the @ Range Operator

Many CLI commands allow for the creation and manipulation of a range of entities. Any command that has the **@** symbol in its parameter listing is one of these commands. The presence of the range operator means that the argument it follows may be used with a range specification in order to act on a consecutive array of entities. To use these arguments with a range, you simply specify the argument normally and follow it with a bracketed range.

For example, the command for creating a range of five load balancing vservers would use the following syntax:

```
config> lb vserver httpvserve[1-5] http 192.168.1.1[1-5] 80
vserver "httpvserve1" added
vserver "httpvserve2" added
vserver "httpvserve3" added
vserver "httpvserve4" added
vserver "httpvserve5" added
 Done
```

Notice that the IP address argument also specifies an address range. When adding a range of entities as shown here, dependant arguments must have a matching range specified as well. The command will return an error if the ranges differ. When you use an add command with the range option as shown here, the system will create 5 vservers with IP addresses ranging from 192.168.1.11 to 192.168.1.15.

When alternately deleting a range of entities, the same methodology applies. To remove the range of vservers created in this example, you would issue the following command:

```
config> rm vserver httpvserve[1-5]
vserver "httpvserve1" removed
vserver "httpvserve2" removed
vserver "httpvserve3" removed
vserver "httpvserve4" removed
vserver "httpvserve5" removed
 Done
```

Note: If a range of entities created with the range operation is somehow broken, such as via the manual removal of one or more of the entities, using the corresponding rm or set commands with a range operation against the range will not complete successfully.

CHAPTER 3

AAA Commands

This chapter covers the aaa commands.

stat aaa

Synopsis

```
stat aaa [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display aaa statistics

Arguments

Output

Counters

Authentication successes (authsucc)
Count of authentication successes

Authentication failures (authfails)
Count of authentication failures

HTTP authorization successes (atzhtps)
Count of HTTP connections that succeeded authorization

HTTP authorization failures (atzhtpf)
Count of HTTP connections that failed authorization

Non HTTP authorization successes (atznonhtps)
Count of non HTTP connections that succeeded authorization

Non HTTP authorization failures (atznonhtpf)
Count of non HTTP connections that failed authorization

Current AAA sessions (totcursess)
Count of current AAA sessions

AAA sessions (totsess)
Count of all AAA sessions

Timed out AAA sessions (totsessto)
Count of AAA sessions that have timed out

Related Commands

show aaa stats

Synopsis

```
show aaa stats - alias for 'stat aaa'
```

Description

show aaa stats is an alias for stat aaa

Related Commands

stat aaa

show aaa session

Synopsis

```
show aaa session [-userName <string>] [-groupName
<string>] [-intranetIP <ip_addr|*>  [<netmask>]]
```

Description

Display the connections initated by the user

Arguments

userName
The user name.

groupName
The group name.

intranetIP
Intranet IP address.

Output

publicIP
Client's public IP address

publicPort
Client's public port

IPAddress
NetScaler's IP address

port
NetScaler's port

privateIP
Client's private/mapped IP address

privatePort
Client's private/mapped port

destIP
Destination IP address

destPort
Destination port

intranetIP
Specifies the Intranet IP

Example

> show aaa connection ClintIp (ClientPort) -> ServerIp(ServerPort)
---------- ---------- User Name: Joe
10.102.0.39 (2318) -> 10.102.4.245 (443) 10.102.0.39 (2320) -
> 10.102.4.245 (443) 10.102.0.39 (2340) -> 10.102.4.245 (443)
Done >

Related Commands

kill aaa session

kill aaa session

Synopsis

```
kill aaa session [-userName <string>] [-groupName
<string>] [-intranetIP <ip_addr|*>  [<netmask>]] [-all]
```

Description

Kill the user sessions

Arguments

userName

The user name. The system will terminate the session initiated by the named user.

groupName

The group name. The system will terminate the sessions of all the users within the named group.

intranetIP

The Intranet IP address. The system will terminate all sessions using the named intranet IP address

all

Terminate the sessions of all users who are currently logged in. Default value: NSAPI_SVCTYPE_CONFIGURED|NSAPI_SVCTYPE_DYNAMIC

Example

kill aaa session -user joe

Related Commands

show aaa session

add aaa user

Synopsis

```
add aaa user <userName> {-password }
```

Description

Add an AAA user.

Arguments

userName

The name of the user.

password

Enter this keyword to create or change the user's password. The entered password is not displayed. If no password is given for a new user then the system inserts the username as the default password.

Example

add expression p4port VPNPORT == 1666 add expression whizbangport VPNPORT == 7676 add expression only_finance_url URL == /finance* add expression only_finance_svc VPNIP == 10.100.3.44 add aaa user johndoe -HttpRule "only_finance_svc && only_finance_url" -ActionHttp allow -NonHttpRule "p4port || whizbangport" -ActionNonHttp allow The above example assigns the following privileges to user johndoe: HTTP: Access is restricted to: URLs with the prefix /finance and the finance application server with IP address 10.100.3.44. Non-HTTP: Access is restricted to Perforce and Whizbang applications.

Related Commands

rm aaa user

set aaa user

show aaa user

rm aaa user

Synopsis

```
rm aaa user <userName>
```

Description

Remove the AAA user.

Arguments

userName

The name of the AAA user.

Related Commands

add aaa user

set aaa user

show aaa user

set aaa user

Synopsis

```
set aaa user <userName>
```

Description

Modify the parameters for the existing AAA user.

Arguments

`userName`

The name of the user.

`password`

Enter this keyword to create or change the user's password. The entered password is not displayed. If no password is given for a new user then the system inserts the username as the default password.

Example

set aaa user johndoe password abcd The above command sets the password for johndoe to abcd

Related Commands

add aaa user

rm aaa user

show aaa user

bind aaa user

Synopsis

```
bind aaa user <userName> [-policy <string>  [-priority
<positive_integer>]] [-intranetApplication <string>]
[-urlName <string>] [-intranetIP <ip_addr>
[<netmask>]]
```

Description

Bind the resources (policy/intranetip/intranetapplication/url) to a user.

Arguments

`userName`
The user name.

`policy`
the policy to be bound to aaa user.

`intranetApplication`
The intranet vpn application.

`urlName`
The intranet url

`intranetIP`
The IP address to be bound to this user and used to access the Intranet

Example

To bind intranetip to the user joe: bind aaa user joe -intranetip 10.102.1.123

Related Commands

unbind aaa user

unbind aaa user

Synopsis

```
unbind aaa user <userName> [-policy <string>] [-
intranetApplication <string>] [-urlName <string>] [-
intranetIP <ip_addr>  [<netmask>]]
```

Description

Unbind the resource(policy/intranetip/intranetapplication/url) from an AAA user

Arguments

userName
The user name.

policy
The policy to be unbound to an aaa user.

intranetApplication
The intranet vpn application.

urlName
The intranet url

intranetIP
The Intranet IP to be unbound

Example

unbind AAA user joe -intranetip 10.102.1.123

Related Commands

bind aaa user

show aaa user

Synopsis

```
show aaa user [<userName>] [-loggedIn]
```

Description

Display the AAA user detail.

Arguments

userName
The user name.

loggedIn
The loggedin flag. When this flag is turned on, the system displays the names of all logged-in users. If a user name is included, the system displays whether the user is logged in or not. Default value: 0

summary

fullValues

format

level

Output

groupName
The group name

policy
The policy Name.

priority
The priority of the policy.

intranetApplication
The intranet vpn application.

urlName
The intranet url.

`intranetIP`
The Intranet IP bound to the user

`netmask`
The netmask for the Intranet IP

Example

Example > show aaa user joe UserName: joe IntranetIP: 10.102.1.123 Bound to groups: GroupName: engg Done >

Related Commands

add aaa user

rm aaa user

set aaa user

add aaa group

Synopsis

```
add aaa group <groupName>
```

Description

Add an AAA group. To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ...". You can also bind ranges of Intranet IP addresses to an AAA group. For example, the administrator may want to assign pools of Intranet IP addresses to groups or departments.

Arguments

groupName

The name of the group.

Example

The following adds a group called group_ad and sets the HTTP rule and action to deny HTTP access in the network 192.30.*.*: add aaa group group_ad -HttpRule exp_source -ActionHttp deny

Related Commands

rm aaa group

show aaa group

rm aaa group

Synopsis

```
rm aaa group <groupName>
```

Description

Remove an AAA group. To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ...". You can also bind ranges of Intranet IP addresses to an AAA group. For example, the administrator may want to assign pools of Intranet IP addresses to groups or departments.

Arguments

groupName

The name of the group . Note:Any user sessions belonging to the group are removed. The user must log in again.

Related Commands

add aaa group

show aaa group

bind aaa group

Synopsis

```
bind aaa group <groupName> [-userName <string>] [-
policy <string>  [-priority <positive_integer>]] [-
intranetApplication <string>] [-urlName <string>] [-
intranetIP <ip_addr>  <netmask>]
```

Description

Bind the resource(User/Intranet IP /Policy/Intranet Application) to a group. To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ...". You can also bind ranges of Intranet IP addresses to an AAA group. For example, the administrator may want to assign pools of Intranet IP addresses to groups or departments.

Arguments

`groupName`
The group name.

`userName`
The user that the group is bound to. If the user belongs to more than one group, the group expressions are evaluated at authorization to determine the appropriate action.

`policy`
The policy to be bound to an AAA group.

`intranetApplication`
The intranet vpn application.

`urlName`
The intranet url.

`intranetIP`

The ip-block or IP address to be bound with this group. This is the block or address that will be used when members of this group access Intranet resources.

Example

To bind an Intranet IP to the group engg: bind aaa group engg -intranetip 10.102.10.0 255.255.255.0

Related Commands

unbind aaa group

unbind aaa group

Synopsis

```
unbind aaa group <groupName> [-userName <string> ...]
[-policy <string>] [-intranetApplication <string>] [-
urlName <string>] [-intranetIP <ip_addr>  <netmask>]
```

Description

Unbind the resource (User/Intranet IP/Policy/Intranet Application) from a group. To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ...". You can also bind ranges of Intranet IP addresses to an AAA group. For example, the administrator may want to assign pools of Intranet IP addresses to groups or departments.

Arguments

`groupName`
The group name.

`userName`
The user to be unbound from the group.

`policy`
The policy to be unbound from the AAA group,

`intranetApplication`
The intranet vpn application.

`urlName`
The intranet url.

`intranetIP`
The Intranet IP to be unbound from the group

Example

unbind aaa group engg -intranetip 10.102.10.0 255.255.255.0

Related Commands

bind aaa group

show aaa group

Synopsis

```
show aaa group [<groupName>] [-loggedIn]
```

Description

Display details of the AAA group. To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ...". You can also bind ranges of Intranet IP addresses to an AAA group. For example, the administrator may want to assign pools of Intranet IP addresses to groups or departments.

Arguments

groupName
The group name.

loggedIn
The loggedin flag. When this flag is turned on, the system displays the names of the users in a group if at least one user in the group is logged in. When used with a group name, the system lists the users in the group who are logged in. Default value: 0

summary

fullValues

format

level

Output

userName
The user name.

policy
The policy name.

priority
The priority of the policy.

intranetApplication
The intranet vpn application.

urlName
The intranet url

intranetIP
The Intranet IP(s) bound to the group

netmask
The netmask for the Intranet IP

Example

> show aaa group engg GroupName: engg Bound AAA users: UserName: joe UserName: jane Intranetip IP: 10.102.10.0 Netmask: 255.255.255.0 Done >

Related Commands

add aaa group

rm aaa group

set aaa radiusParams

Synopsis

```
set aaa radiusParams [-serverIP <ip_addr|ipv6_addr|*>]
[-serverPort <port>] [-authTimeout <positive_integer>]
{-radKey } [-radNASip ( ENABLED | DISABLED )] [-
radNASid <string>] [-radVendorID <positive_integer>] [-
radAttributeType <positive_integer>] [-radGroupsPrefix
<string>] [-radGroupSeparator <string>] [-passEncoding
<passEncoding>] [-ipVendorID <positive_integer>] [-
ipAttributeType <positive_integer>] [-accounting ( ON |
OFF )] [-pwdVendorID <positive_integer>] [-
pwdAttributeType <positive_integer>]
```

Description

Modify the global variables for the RADIUS server. It will be used globally in SSL-VPN across all Vservers unless you create a vserver-specific configuration using authentication policies.

Arguments

serverIP

The IP address of the RADIUS server.

serverPort

The port number on which the RADIUS server is running. Default value: 1812 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the RADIUS server. Default value: 3 Minimum value: 1

radKey

The key shared between the client and the server. This information is required for the system to communicate with the RADIUS server.

radNASip
The option to send the NetScaler's IP address (NSIP) to the server as the "nasip" part of the Radius protocol. Possible values: ENABLED, DISABLED

radNASid
The nasid. If configured, this string will be sent to the RADIUS server as the "nasid" part of the Radius protocol.

radVendorID
The Vendor ID for Radius group extraction. Minimum value: 1

radAttributeType
The Attribute type for Radius group extraction. Minimum value: 1

radGroupsPrefix
The groups prefix string that precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator
The group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding
The option to encode the password in the Radius packets traveling from the NetScaler to the Radius server. Possible values: pap, chap, mschapv1, mschapv2 Default value: AAA_PAP

ipVendorID
The vendor ID of the attribute in the RADIUS response. The vendor ID denotes the intranet IP. The value of 0 denotes that the attribute is not vendor-encoded. Minimum value: 0

ipAttributeType
The attribute type of the remote IP address attribute in a RADIUS response. Minimum value: 1

accounting
The state of the RADIUS server to receive accounting messages. Possible values: ON, OFF

pwdVendorID
Vendor ID of the attribute in the RADIUS response which will be used to extract the user Password. Minimum value: 1

Example

To configure the default RADIUS parameters: set aaa radiusparams -serverip 192.30.1.2 -radkey sslvpn

Related Commands

add authentication radiusaction

set aaa ldapparams

set aaa parameter

unset aaa radiusParams

show aaa radiusParams

unset aaa radiusParams

Synopsis

```
unset aaa radiusParams [-serverIP] [-serverPort] [-
authTimeout] [-radNASip] [-radNASid] [-radVendorID] [-
radAttributeType] [-radGroupsPrefix] [-
radGroupSeparator] [-passEncoding] [-ipVendorID] [-
ipAttributeType] [-accounting] [-pwdVendorID] [-
pwdAttributeType]
```

Description

Use this command to remove aaa radiusParams settings.Refer to the set aaa radiusParams command for meanings of the arguments.

Related Commands

set aaa radiusParams

show aaa radiusParams

show aaa radiusParams

Synopsis

```
show aaa radiusParams
```

Description

Display the configured RADIUS parameters.

Arguments

format

level

Output

serverIP
The IP address of the RADIUS server.

serverPort
The port number on which the RADIUS server is running.

radKey
The key shared between the client and the server.

groupAuthName
To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ..."

authTimeout
The maximum number of seconds the system will wait for a response from the RADIUS server.

radNASip
The option to send the NetScaler's IP address (NSIP) as the "nasip" part of the Radius protocol to the server.

radNASid
The nasid. If configured, this string will be sent to the RADIUS server as the "nasid" as part of the Radius protocol.

IPAddress
IP Address.

radVendorID
The Vendor ID for Radius group extraction.

radAttributeType
The Attribute type for Radius group extraction.

radGroupsPrefix
The groups prefix string that precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator
The group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding
The option to encode the password in the Radius packets traveling from the NetScaler to the Radius server.

accounting
The state of the Radius server that will receive accounting messages.

pwdVendorID
Vendor ID of the attribute in the RADIUS response which will be used to extract the user Password.

pwdAttributeType
Attribute type of the vendor specific Password-Attribute in a RADIUS response.

Example

> show aaa radiusparams Configured RADIUS parameters Server IP: 127.0.0.2 Port: 1812 key: secret Timeout: 10 Done >

Related Commands

set aaa radiusParams

unset aaa radiusParams

set aaa ldapParams

Synopsis

```
set aaa ldapParams [-serverIP <ip_addr|ipv6_addr|*>] [-
serverPort <port>] [-authTimeout <positive_integer>] [-
ldapBase <string>] [-ldapBindDn <string>] {-
ldapBindDnPassword } [-ldapLoginName <string>] [-
searchFilter <string>] [-groupAttrName <string>] [-
subAttributeName <string>] [-secType <secType>] [-
ssoNameAttribute <string>] [-nestedGroupExtraction ( ON
| OFF )] [-maxNestingLevel <positive_integer>] [-
groupNameIdentifier <string>] [-groupSearchAttribute
<string>  [-groupSearchSubAttribute <string>]] [-
groupSearchFilter <string>]
```

Description

Set the global variables for the LDAP server. It is used globally in SSL-VPN across all Vservers unless you create a vserver-specific configuration using authentication policies.

Arguments

serverIP

The IP address of the LDAP server. The default value is localhost.

serverPort

The port number on which the LDAP server is running. Default value: 389 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the LDAP server. Default value: 3 Minimum value: 1

ldapBase

The base or node where the ldapsearch should start. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.

ldapBindDn
The full distinguished name that is used to bind to the LDAP server.

ldapBindDnPassword
The password used to bind to the LDAP server.

ldapLoginName
The name attribute used by the system to query the external LDAP server or an Active Directory.

searchFilter
The String to be combined with the default LDAP user search string to form the value. For example, vpnallowed=true with ldaploginame "samaccount" and user-supplied username "bob" would yield the LDAP search string "(&(vpnallowed=true)(samaccount=bob)".

groupAttrName
The attribute name for group extraction from the LDAP server

subAttributeName
The Sub-Attribute name for group extraction from LDAP server

secType
The type of communication between the system and the LDAP server. The values are: PLAINTEXT: No encryption required. TLS: To use the TLS protocol to communicate. SSL: To use the SSL Protocol to communicate. Possible values: PLAINTEXT, TLS, SSL Default value: AAA_LDAP_PLAINTEXT

ssoNameAttribute
The attribute used by the system to query the external LDAP server (or an Active Directory) for an alternate username to be used in Single Sign-On.

nestedGroupExtraction
Setting this option to ON enables the nested group extraction feature where the system queries the external LDAP server to determine if a group belongs to another group Possible values: ON, OFF Default value: OFF

Example

To configure authentication in the LDAP server running at 192.40.1.2: set aaa ldapparams -serverip 192.40.1.2 -ldapbase "dc=netscaler,dc=com" -

ldapBindDN "cn=Manager,dc=netscaler,dc=com" -ldapBindDnPassword secret -ldaploginname uid

Related Commands

add authentication ldapaction

set aaa radiusparams

set aaa parameter

unset aaa ldapParams

show aaa ldapParams

unset aaa ldapParams

Synopsis

```
unset aaa ldapParams [-serverIP] [-serverPort] [-
authTimeout] [-ldapBase] [-ldapBindDn] [-
ldapBindDnPassword] [-ldapLoginName] [-searchFilter]
[-groupAttrName] [-subAttributeName] [-secType] [-
ssoNameAttribute] [-nestedGroupExtraction] [-
maxNestingLevel] [-groupNameIdentifier] [-
groupSearchAttribute] [-groupSearchSubAttribute] [-
groupSearchFilter]
```

Description

Use this command to remove aaa ldapParams settings.Refer to the set aaa ldapParams command for meanings of the arguments.

Related Commands

set aaa ldapParams

show aaa ldapParams

show aaa ldapParams

Synopsis

```
show aaa ldapParams
```

Description

Display the configured LDAP parameters.

Arguments

format

level

Output

serverIP
The IP address of the LDAP server.

serverPort
The port number on which the LDAP server is running.

authTimeout
The maximum number of seconds the system will wait for a response from the LDAP server.

ldapBindDn
The full distinguished name used to bind to the LDAP server.

ldapLoginName
The name attribute used by the system to query the external LDAP server, or an Active Directory.

ldapBase
The base or node where the ldapsearch should start. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.

secType
The communication type between the system and the LDAP server.

ssoNameAttribute
The attribute used by the system to query the external LDAP server, or an Active Directory, for an alternate username to be used in Single Sign-On.

searchFilter
The String to be combined with the default LDAP user search string to form the value. For example, vpnallowed=true with ldaploginame "samaccount" and the user-supplied username "bob" would yield the LDAP search string "(&(vpnallowed=true)(samaccount=bob)".

groupAttrName
The Attribute name for group extraction from the LDAP server.

subAttributeName
The Sub-Attribute name for group extraction from LDAP server

groupAuthName
To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command "bind AAA group ... -policy ..."

nestedGroupExtraction

maxNestingLevel

groupNameIdentifier

groupSearchAttribute

groupSearchSubAttribute

groupSearchFilter

Example

> show aaa ldapparams Configured LDAP parameters Server IP: 127.0.0.1 Port: 389 Timeout: 1 BindDn: cn=Manager,dc=florazel,dc=com login: uid Base: dc=florazel,dc=com Secure Type: PLAINTEXT Done >

Related Commands

set aaa ldapParams

unset aaa ldapParams

set aaa tacacsParams

Synopsis

```
set aaa tacacsParams [-serverIP <ip_addr|ipv6_addr|*>]
[-serverPort <port>] [-authTimeout <positive_integer>]
{-tacacsSecret } [-authorization ( ON | OFF )] [-
accounting ( ON | OFF )]
```

Description

Set the global variables for the TACACS+ server. It is used globally in SSL-VPN across all Vservers unless a vserver-specific configuration is done using authentication policies.

Arguments

serverIP

The IP address of the TACACS+ server.

serverPort

The port on which the TACACS+ server is running. Default value: 49 Minimum value: 1

authTimeout

The maximum number of seconds the system will wait for a response from the TACACS+ server. Default value: 3 Minimum value: 1

tacacsSecret

The key shared between the client and the server. This information is required for the system to communicate with the TACACS+ server.

authorization

The option for streaming authorization for the TACACS+ server. Possible values: ON, OFF

accounting

The option for sending accounting messages to the TACACS+ server. Possible values: ON, OFF

Example

To configure a TACACS+ server running at 192.168.1.20 set aaa tacacsparams -serverip 192.168.1.20 -tacacssecret secret

Related Commands

add authentication tacacsaction

set aaa radiusparams

set aaa parameter

unset aaa tacacsParams

show aaa tacacsParams

unset aaa tacacsParams

Synopsis

```
unset aaa tacacsParams [-serverIP] [-serverPort] [-
authTimeout] [-tacacsSecret] [-authorization] [-
accounting]
```

Description

Use this command to remove aaa tacacsParams settings.Refer to the set aaa tacacsParams command for meanings of the arguments.

Related Commands

set aaa tacacsParams

show aaa tacacsParams

show aaa tacacsParams

Synopsis

```
show aaa tacacsParams
```

Description

Display configured AAA TACACS+ server parameters.

Arguments

format

level

Output

serverIP
The IP address of the TACACS+ server.

serverPort
The port on which the TACACS+ server is running.

authTimeout
The maximum number of seconds the system will wait for a response from the TACACS+ server.

tacacsSecret
The key shared between the client and the server.

authorization
The option for the streaming authorization for TACACS+ server.

accounting
The option to send accounting messages to TACACS+ server.

Example

> sh aaa tacacsparams Configured TACACS parameter Server IP: 192.168.1.20 Port: 49 Timeout: 1 secs Done

Related Commands

set aaa tacacsParams

unset aaa tacacsParams

set aaa nt4Params

Synopsis

```
set aaa nt4Params [-serverIP <ip_addr|ipv6_addr|*>] [-
nt4ServerName <string>] [-nt4DomainName <string>] [-
nt4AdminUser <string>] {-nt4AdminPasswd }
```

Description

Set the parameters of NT4 authentication server.

Arguments

serverIP

The IP address of the NT4 server.

nt4ServerName

The name of the NT4 server.

nt4DomainName

The domain name of the NT4 server.

nt4AdminUser

The username of an NT4 Domain Administrator.

nt4AdminPasswd

The password of the NT4 Domain Administrator.

Example

To configure an NT4 server running at 192.168.1.21 set aaa nt4params -serverip 192.168.1.21

Related Commands

unset aaa nt4Params

show aaa nt4Params

unset aaa nt4Params

Synopsis

```
unset aaa nt4Params [-serverIP] [-nt4ServerName] [-
nt4DomainName] [-nt4AdminUser] [-nt4AdminPasswd]
```

Description

Use this command to remove aaa nt4Params settings.Refer to the set aaa nt4Params command for meanings of the arguments.

Related Commands

set aaa nt4Params

show aaa nt4Params

show aaa nt4Params

Synopsis

```
show aaa nt4Params
```

Description

Display configured AAA NT4 server parameters.

Arguments

format

level

Output

serverIP
The IP address of the NT4 server.

nt4ServerName
The name of the NT4 server.

nt4DomainName
The domain name of the NT4 server.

nt4AdminUser
The username of an NT4 Domain Administrator.

nt4AdminPasswd
The password of the NT4 Domain Administrator.

Related Commands

set aaa nt4Params
unset aaa nt4Params

set aaa certParams

Synopsis

```
set aaa certParams [-userNameField <string>] [-
groupNameField <string>]
```

Description

Set the global variables for a certificate policy. It is used globally in SSL-VPN across all Vservers unless vserver-specific configuration is done using authentication policies.

Arguments

userNameField

The field in the client certificate to extract the username from. Should be of the format <field:subfield>. Allowed values for field are "Subject" and "Issuer".

groupNameField

The certificate field to extract the group from. Should be of the format <field:subfield>. Allowed values for field are "Subject" and "Issuer".

Example

To configure the default certificate parameters: set aaa certparams -userNameField "Subject:CN" -groupNameField "Subject:OU"

Related Commands

add authentication certaction

set aaa parameter

unset aaa certParams

show aaa certParams

unset aaa certParams

Synopsis

```
unset aaa certParams [-userNameField] [-groupNameField]
```

Description

Use this command to remove aaa certParams settings.Refer to the set aaa certParams command for meanings of the arguments.

Related Commands

set aaa certParams

show aaa certParams

show aaa certParams

Synopsis

```
show aaa certParams
```

Description

Display the configured CERT parameters.

Arguments

format

level

Output

twoFactor
The state of the two-factor authentication.

userNameField
The field in the certificate from which the username will be extracted.

groupNameField
The field in the certificate from which the group will be extracted.

Related Commands

set aaa certParams

unset aaa certParams

set aaa parameter

Synopsis

```
set aaa parameter [-defaultAuthType <defaultAuthType>]
[-maxAAAUsers <positive_integer>]
```

Description

Set the global AAA parameters. This will override the default authentication server setting.

Arguments

defaultAuthType

The default authentication server type. If nothing is specified, the default value is set to LDAP. Possible values: LOCAL, LDAP, RADIUS, TACACS, NT4, CERT

maxAAAUsers

The maximum number of concurrent users allowed to login in to the system at any given time. Minimum value: 1 Maximum value: 65535

Example

set aaa parameter -defaultAuthType RADIUS -maxAAAUSers 100

Related Commands

unset aaa parameter

show aaa parameter

unset aaa parameter

Synopsis

```
unset aaa parameter [-defaultAuthType] [-maxAAAUsers]
```

Description

Use this command to remove aaa parameter settings.Refer to the set aaa parameter command for meanings of the arguments.

Related Commands

set aaa parameter

show aaa parameter

show aaa parameter

Synopsis

```
show aaa parameter
```

Description

Displays the configured AAA parameters .

Arguments

format

level

Output

defaultAuthType

The default authentication server type.

maxAAAUsers

The maximum number of concurrent users allowed to log into the system at any time.

Example

> show aaa parameter Configured AAA parameters DefaultAuthType: LDAP MaxAAAUsers: 5 Done >

Related Commands

set aaa parameter

unset aaa parameter

add aaa preauthenticationaction

Synopsis

```
add aaa preauthenticationaction <name>
[<preauthenticationaction>] [-killProcess <string>] [-
deletefiles <string>]
```

Description

Add actions for end point analysis (EPA) clients before authentication.

Arguments

name
The name of the Preauthentication action.

preauthenticationaction
Deny or allow login after end point analysis results. Possible values: ALLOW, DENY

killProcess
Processes to be killed by the EPA tool.

deletefiles
Files to be deleted by EPA tool.

Related Commands

rm aaa preauthenticationaction
set aaa preauthenticationaction
unset aaa preauthenticationaction
show aaa preauthenticationaction

rm aaa preauthenticationaction

Synopsis

```
rm aaa preauthenticationaction <name>
```

Description

Remove a previously created Pre-authentication action. Note that an action cannot be removed as long as it is configured in a policy.

Arguments

name

The name of the action to be removed.

Related Commands

add aaa preauthenticationaction

set aaa preauthenticationaction

unset aaa preauthenticationaction

show aaa preauthenticationaction

set aaa preauthenticationaction

Synopsis

```
set aaa preauthenticationaction <name>
[<preauthenticationaction>] [-killProcess <string>] [-
deletefiles <string>]
```

Description

Change properties of a Pre-authentication action.

Arguments

name

The name of the Preauthentication action.

preauthenticationaction

Deny or allow login after end point analysis results. Possible values: ALLOW, DENY

killProcess

Processes to be killed by EPA tool.

deletefiles

Files to be deleted by EPA tool.

Related Commands

add aaa preauthenticationaction

rm aaa preauthenticationaction

unset aaa preauthenticationaction

show aaa preauthenticationaction

unset aaa preauthenticationaction

Synopsis

```
unset aaa preauthenticationaction <name> [-killProcess]
[-deletefiles]
```

Description

Use this command to remove aaa preauthenticationaction settings.Refer to the set aaa preauthenticationaction command for meanings of the arguments.

Related Commands

add aaa preauthenticationaction

rm aaa preauthenticationaction

set aaa preauthenticationaction

show aaa preauthenticationaction

show aaa preauthenticationaction

Synopsis

```
show aaa preauthenticationaction [<name>]
```

Description

Display details of the configured Pre-authentication action(s).

Arguments

name

The name of the RADIUS action.

summary

fullValues

format

level

Output

Related Commands

add aaa preauthenticationaction

rm aaa preauthenticationaction

set aaa preauthenticationaction

unset aaa preauthenticationaction

add aaa preauthenticationpolicy

Synopsis

```
add aaa preauthenticationpolicy <name> <rule>
[<reqAction>]
```

Description

Add a Radius authentication policy. The policy defines expressions to be evaluated by the EPA tool.

Arguments

`name`
The name to assign to the new Pre-authentication policy.

`rule`
The name of the rule or expression that the policy will use.

`reqAction`
The name of the RADIUS action the policy will use.

Related Commands

rm aaa preauthenticationpolicy

set aaa preauthenticationpolicy

show aaa preauthenticationpolicy

rm aaa preauthenticationpolicy

Synopsis

```
rm aaa preauthenticationpolicy <name>
```

Description

Remove a Pre-authentication policy.

Arguments

name

The name of the Pre-authentication policy to remove.

Related Commands

add aaa preauthenticationpolicy

set aaa preauthenticationpolicy

show aaa preauthenticationpolicy

set aaa preauthenticationpolicy

Synopsis

```
set aaa preauthenticationpolicy <name> [-rule
<expression>] [-reqAction <string>]
```

Description

Change the properties of a Pre-authentication policy.

Arguments

name

The name of the policy.

rule

The new rule to be associated with the policy.

reqAction

The new Pre-authentication action to be associated with the policy.

Related Commands

add aaa preauthenticationpolicy

rm aaa preauthenticationpolicy

show aaa preauthenticationpolicy

show aaa preauthenticationpolicy

Synopsis

```
show aaa preauthenticationpolicy [<name>]
```

Description

Display configured Pre-authentication policies.

Arguments

name

The name of the policy. If this option is not provided, all of the configured RADIUS policies will be displayed.

summary

fullValues

format

level

Output

rule

The new rule associated with the policy.

reqAction

The Pre-authentication action associated with the policy.

hits

No of hits.

boundTo

The entity name to which policy is bound

Related Commands

add aaa preauthenticationpolicy

rm aaa preauthenticationpolicy

set aaa preauthenticationpolicy

set aaa preauthenticationparameter

Synopsis

```
set aaa preauthenticationparameter [-
preauthenticationaction ( ALLOW | DENY )] [-rule
<expression>] [-killProcess <string>] [-deletefiles
<string>]
```

Description

Sets the default end point analysis (EPA) parameters before authentication.

Arguments

preauthenticationaction

Deny or allow login after end point analysis results. Possible values: ALLOW, DENY

rule

The name of the rule, or expression, to be evaluated by the EPA tool.

killProcess

Processes to be killed by the EPA tool.

deletefiles

Files to be deleted by the EPA tool.

Related Commands

unset aaa preauthenticationparameter

show aaa preauthenticationparameter

unset aaa preauthenticationparameter

Synopsis

```
unset aaa preauthenticationparameter [-rule] [-
preauthenticationaction] [-killProcess] [-deletefiles]
```

Description

Set default end point analysis(EPA) parameters before authentication. .Refer to the set aaa preauthenticationparameter command for meanings of the arguments.

Related Commands

set aaa preauthenticationparameter

show aaa preauthenticationparameter

show aaa preauthenticationparameter

Synopsis

```
show aaa preauthenticationparameter
```

Description

Display details of the configured Pre-authentication parameter(s).

Arguments

format

level

Output

preauthenticationaction
Deny or allow login after End point analysis results.

rule
The name of the rule, or expression, to be evaluated by the EPA tool.

killProcess
Processes to be killed by EPA tool.

deletefiles
Files to be deleted by EPA tool.

Related Commands

set aaa preauthenticationparameter

unset aaa preauthenticationparameter

bind aaa global

Synopsis

```
bind aaa global (-policy <string>  [-priority
<positive_integer>])
```

Description

Binds the policy globally.

Arguments

policy

The policy to be bound globally.

Example

bind aaa global -pol pol1

Related Commands

unbind aaa global

show aaa global

unbind aaa global

Synopsis

```
unbind aaa global -policy <string>
```

Description

Unbind the policy globally

Arguments

policy

The policy to be unbound to the AAA user.

Related Commands

bind aaa global

show aaa global

show aaa global

Synopsis

```
show aaa global
```

Description

Display details of the configured policies aaa global.

Arguments

summary

fullValues

format

level

Output

policy

The policy to be unbound to the AAA user.

priority

Priority of the bound policy

Related Commands

bind aaa global

unbind aaa global

CHAPTER 4

Application Firewall Commands

This chapter covers the application firewall commands.

show appfw stats

Synopsis

```
show appfw stats - alias for 'stat appfw'
```

Description

show appfw stats is an alias for stat appfw

Related Commands

stat appfw

stat appfw

Synopsis

```
stat appfw [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display Application Firewall stats.

Arguments

Output

Counters

total violations (totviols)
Number of violations seen by the application firewall

requests (reqs)
Number of requests received by the application firewall

responses (resps)
Number of responses handled by the application firewall

aborts
Number of requests aborted by the application firewall

redirects (redirect)
Number of requests redirected by the application firewall (HTTP 302)

start URL (startURL)
Number of start URL violations seen by the application firewall

deny URL (denyURL)
Number of deny URL violations seen by the application firewall

buffer overflow (bufovfl)
Number of buffer overflow violations seen by the application firewall

cookie consistency (cookie)
Number of cookie violations seen by the application firewall

HTML Cross-site scripting (xss)
Number of Cross-site scripting violations seen by the application firewall

HTML SQL injection (sql)
Number of SQL violations seen by the application firewall

field format (fieldfmt)
Number of field format violations seen by the application firewall

field consistency (fieldcon)
Number of field consistency violations seen by the application firewall

credit card (ccard)
Number of credit card violations seen by the application firewall

safe object (safeobj)
Number of safe object violations seen by the application firewall

XML Format (wfcViolations)
XML well-formedness violations

XML Denial of Service (XDoS) (xdosViolations)
XML Denial of Service violations

XML Message Validation (msgvalViolations)
XML Message Validation violations

Web Services Interoperability (wsIViolations)
XML WS-I violations

XML SQL Injection (xmlSqlViolations)
XML SQL Injection violations

XML Cross-Site Scripting (xmlXssViolations)
XML Cross-Site Scripting violations

XML Attachment (xmlAttachmentViolations)
XML Attachment violations

Related Commands

add appfw fieldType

Synopsis

add appfw fieldType <name> <regex> <priority> [-comment <string>]

Description

Add an Application Firewall field type. Field types define the type of data that can appear in a web form field. The Learning engine uses the field types list to generate appropriate field type assignments for the field formats check.

Arguments

name
The name of this field type.

regex
The regular expression that describes this field type.

priority
The priority of this field type. Minimum value: 0 Maximum value: 64000

comment
Comments associated with this field type.

Related Commands

rm appfw fieldType
set appfw fieldType
show appfw fieldType

rm appfw fieldType

Synopsis

```
rm appfw fieldType <name>
```

Description

Remove an Application Firewall field type. Field types define the type of data that can appear in a web form field. The Learning engine uses the field types list to generate appropriate field type assignments for the field formats check.

Arguments

name

The name of this field type.

Related Commands

add appfw fieldType

set appfw fieldType

show appfw fieldType

set appfw fieldType

Synopsis

```
set appfw fieldType <name> <regex> <priority> [-comment
<string>]
```

Description

Modify an Application Firewall field type. Field types define the type of data that can appear in a web form field. The Learning engine uses the field types list to generate appropriate field type assignments for the field formats check.

Arguments

`name`
The name of this field type.

`regex`
The regular expression that describes this field type.

Related Commands

add appfw fieldType
rm appfw fieldType
show appfw fieldType

show appfw fieldType

Synopsis

```
show appfw fieldType [<name>]
```

Description

Display all configured Application Firewall form field types.

Arguments

name
The name of this field type.

summary

fullValues

format

level

Output

regex
The regular expression that describes this field type.

priority
The priority of this field type.

comment
Comments associated with this field type.

Related Commands

add appfw fieldType
rm appfw fieldType
set appfw fieldType

set appfw settings

Synopsis

```
set appfw settings [-sessionTimeout <positive_integer>]
[-sessionCookieName <string>] [-clientIPLoggingHeader
<string>]
```

Description

Set the global settings for the Application Firewall module. Changes in these settings are applied to all Application Firewall profiles.

Arguments

sessionTimeout

The user session timeout (in seconds). After this many seconds of no user activity, the session is terminated and the user must establish a new session before continuing to use the protected web site. Default value: AS_ENGINESETTINGS_SESSIONTIMEOUT_DEFAULT Minimum value: 1 Maximum value: 65535

sessionCookieName

The name of the session cookie set by the Application Firewall to track the user session. Default value: NS_S_AS_DEFAULT_COOKIE_NAME

clientIPLoggingHeader

The name of the header that holds downstream IP address for logging purposes. Default value:

Related Commands

unset appfw settings

show appfw settings

unset appfw settings

Synopsis

```
unset appfw settings [-sessionTimeout] [-
sessionCookieName] [-clientIPLoggingHeader]
```

Description

Use this command to remove appfw settings settings.Refer to the set appfw settings command for meanings of the arguments.

Related Commands

set appfw settings

show appfw settings

show appfw settings

Synopsis

```
show appfw settings
```

Description

Display the global settings for the Application Firewall module.

Arguments

format

level

Output

sessionTimeout
Session timeout (in seconds).

sessionCookieName
Cookie name.

clientIPLoggingHeader
Name of header that holds downstream IP address for logging purposes.

Related Commands

set appfw settings

unset appfw settings

add appfw profile

Synopsis

```
add appfw profile <name> [-defaults ( basic | advanced )]
```

Description

Add an Application Firewall profile. A profile tells the Application Firewall how it should protect a given class of web content. Different types of content often require different protection strategies. You define these strategies in a profile. You can create profiles with basic or advanced defaults. The defaults, or predefined settings, provide solid initial protection for web content - a starting point from which you can configure additional protection for special content. Each profile is associated with a policy that tells the Application Firewall the content type of a request or response. When a request or response matches the policy, that profile is applied.

Arguments

`name`
Application Firewall profile name.

`defaults`
Default Start URLs and Deny URLs. Possible values: basic, advanced

Related Commands

rm appfw profile
set appfw profile
unset appfw profile
bind appfw profile
unbind appfw profile
show appfw profile

rm appfw profile

Synopsis

```
rm appfw profile <name>
```

Description

Remove an Application Firewall profile.

Arguments

name

Application Firewall profile name.

Related Commands

add appfw profile
set appfw profile
unset appfw profile
bind appfw profile
unbind appfw profile
show appfw profile

set appfw profile

Synopsis

```
set appfw profile <name> [-startURLAction
<startURLAction> ...] [-startURLClosure ( ON | OFF )]
[-denyURLAction <denyURLAction> ...] [-
cookieConsistencyAction <cookieConsistencyAction> ...]
[-fieldConsistencyAction <fieldConsistencyAction> ...]
[-crossSiteScriptingAction <crossSiteScriptingAction>
...] [-crossSiteScriptingTransformUnsafeHTML ( ON | OFF
)] [-crossSiteScriptingCheckCompleteURLs ( ON | OFF )]
[-SQLInjectionAction <SQLInjectionAction> ...] [-
SQLInjectionTransformSpecialChars ( ON | OFF )] [-
SQLInjectionOnlyCheckFieldsWithSQLChars ( ON | OFF )]
[-fieldFormatAction <fieldFormatAction> ...] [-
defaultFieldFormatType <string>] [-
defaultFieldFormatMinLength <positive_integer>] [-
defaultFieldFormatMaxLength <positive_integer>] [-
bufferOverflowAction <bufferOverflowAction> ...] [-
bufferOverflowMaxURLLength <positive_integer>] [-
bufferOverflowMaxHeaderLength <positive_integer>] [-
bufferOverflowMaxCookieLength <positive_integer>] [-
creditCardAction <creditCardAction> ...] [-creditCard
<creditCard> ...] [-creditCardMaxAllowed
<positive_integer>] [-creditCardXOut ( ON | OFF )] [-
XMLDoSAction <XMLDoSAction> ...] [-XMLFormatAction
<XMLFormatAction> ...] [-XMLSQLInjectionAction
<XMLSQLInjectionAction> ...] [-
XMLSQLInjectionOnlyCheckFieldsWithSQLChars ( ON | OFF
)] [-XMLSQLInjectionParseComments
<XMLSQLInjectionParseComments>] [-XMLXSSAction
<XMLXSSAction> ...] [-XMLWSIAction <XMLWSIAction> ...]
[-XMLAttachmentAction <XMLAttachmentAction> ...] [-
XMLValidationAction <XMLValidationAction> ...] [-
```

XMLErrorObject <string>] [-useHTMLErrorObject (ON | OFF)] [-errorURL <expression>] [-HTMLErrorObject <string>] [-stripComments (ON | OFF)] [-defaultCharSet <string>] [-postBodyLimit <positive_integer>] [-canonicalizeHTMLResponse (ON | OFF)] [-enableFormTagging (ON | OFF)] [-excludeFileUploadFromChecks (ON | OFF)] [-SQLInjectionParseComments <SQLInjectionParseComments>] [-type (HTML | XML) ...]

Description

Modify the settings for a given Application Firewall profile.

Arguments

name

Application Firewall profile name.

startURLAction

Start URL action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. Default value: ARRAY(0x857c258)

startURLClosure

Start URL closure. This check is applicable to Profile Type: HTML, XML. Possible values: ON, OFF Default value: OFF

denyURLAction

Deny URL action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. Default value: ARRAY(0x8585abc)

cookieConsistencyAction

Cookie consistency action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. Default value: ARRAY(0x8585ce4)

fieldConsistencyAction

Form Field Consistency action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: ARRAY(0x8585da4)

crossSiteScriptingAction
Cross-site scripting action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: ARRAY(0x8585e64)

crossSiteScriptingTransformUnsafeHTML
Transform HTML characters. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

crossSiteScriptingCheckCompleteURLs
Check complete URLs. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

SQLInjectionAction
SQL injection action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: ARRAY(0x858c018)

SQLInjectionTransformSpecialChars
Transform HTML characters. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

SQLInjectionOnlyCheckFieldsWithSQLChars
Check SQL characters. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: ON

fieldFormatAction
Field format action types. (BLOCK | LEARN | LOG | STATS | NONE) This check is applicable to Profile Type: HTML. Default value: ARRAY(0x858c1b0)

defaultFieldFormatType
Default field type. This check is applicable to Profile Type: HTML.

defaultFieldFormatMinLength
Default field type minimum length. This check is applicable to Profile Type: HTML. Default value: AS_DEFAULTFIELDFORMAT_DEFAULT_MIN_LEN Maximum value: 65535

defaultFieldFormatMaxLength
Default field type maximum length. This check is applicable to Profile Type: HTML. Default value:

AS_DEFAULTFIELDFORMAT_DEFAULT_MAX_LEN Minimum value: 1 Maximum value: 65535

bufferOverflowAction

Buffer overflow action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. Default value: ARRAY(0x858c3c0)

bufferOverflowMaxURLLength

Maximum URL length. This check is applicable to Profile Type: HTML, XML. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_URL_LEN Minimum value: 0 Maximum value: 65535

bufferOverflowMaxHeaderLength

Maximum header length. This check is applicable to Profile Type: HTML, XML. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_HDR_LEN Minimum value: 0 Maximum value: 65535

bufferOverflowMaxCookieLength

Maximum cookie length. This check is applicable to Profile Type: HTML, XML. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_COOKIE_LEN Minimum value: 0 Maximum value: 65535

creditCardAction

Credit Card action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: HTML, XML. Default value: ARRAY(0x858c5e8)

creditCard

Credit card. This check is applicable to Profile Type: HTML, XML. Default value: ARRAY(0x858c6a8)

creditCardMaxAllowed

Maximum number of times a credit card number may be seen before action is taken. This check is applicable to Profile Type: HTML, XML. Minimum value: 0 Maximum value: 255

creditCardXOut
X-out the credit card numbers. This check is applicable to Profile Type: HTML, XML. Possible values: ON, OFF Default value: OFF

XMLDoSAction
XML DOS action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: ARRAY(0x858c840)

XMLFormatAction
XML well-formed request action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: ARRAY(0x858c900)

XMLSQLInjectionAction
XML SQL injection action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: ARRAY(0x858c9c0)

XMLSQLInjectionOnlyCheckFieldsWithSQLChars
Check SQL characters. This check is applicable to Profile Type: XML. Possible values: ON, OFF Default value: ON

XMLSQLInjectionParseComments
Canonicalize SQL Comments in XML Data. This check is applicable to Profile Type: XML. Possible values: checkall, ansi, nested, ansinested Default value: AS_CHECKALL

XMLXSSAction
XML cross-site scripting action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: ARRAY(0x858cb58)

XMLWSIAction
XML WS-I action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: ARRAY(0x858cc18)

XMLAttachmentAction
XML attachment action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: ARRAY(0x858ccd8)

XMLValidationAction
XML validation action types. (BLOCK | LOG | STATS | NONE) This check is applicable to Profile Type: XML. Default value: ARRAY(0x858cd98)

XMLErrorObject
Object name for the xml error page. This check is applicable to Profile Type: XML. Default value: NS_S_AS_ERROROBJECT_DEFAULT

useHTMLErrorObject
Use HTML Error object for response instead of Redirect Error URL. Possible values: ON, OFF Default value: OFF

errorURL
Error page. This check is applicable to Profile Type: HTML. Default value: NS_S_AS_ERROR_URL_DEFAULT

HTMLErrorObject
Object name for the html error page. This check is applicable to Profile Type: HTML. Default value: NS_S_AS_ERROROBJECT_DEFAULT

stripComments
Strip HTML comments. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

defaultCharSet
Default character set. Possible values are iso-8859-1 (English US), big5 (Chinese Traditional), gb2312 (Chinese Simplified), sjis (Japanese), euc-jp (Japanese EUC-JP), utf-8 (Unicode), and euc-kr (Korean). This check is applicable to Profile Type: HTML. Default value: NS_S_AS_CHARSET_DEFAULT Maximum value: 31

postBodyLimit
Maximum allowed post body size. This check is applicable to Profile Type: HTML, XML. Default value: AS_DEFAULT_POSTBODYLIMIT Minimum value: 0 Maximum value: 1000000000

canonicalizeHTMLResponse
Entity encoding for html special characters for attributes in the response. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: ON

enableFormTagging
Enable Tagging of Forms for Field Consistency Checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: ON

excludeFileUploadFromChecks

Exclude Uploaded Files from Form checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

SQLInjectionParseComments

Canonicalize SQL Comments in form fields. This check is applicable to Profile Type: HTML. Possible values: checkall, ansi, nested, ansinested Default value: AS_DEFAULT_SQLINJECTIONPARSECOMMENTS

type

Defines the type of the Application Firewall Profile. If the profile is of type XML, then you can only set security checks that are relevent to XML. Similary, if the profile type is HTML then you can set only security checks that are relevant to HTML. Composite profile types can have HTML and XML checks. Default value: ARRAY(0x8591360)

Related Commands

add appfw profile

rm appfw profile

unset appfw profile

bind appfw profile

unbind appfw profile

show appfw profile

unset appfw profile

Synopsis

```
unset appfw profile <name> [-startURLAction] [-
startURLClosure] [-denyURLAction] [-
cookieConsistencyAction] [-fieldConsistencyAction] [-
crossSiteScriptingAction] [-
crossSiteScriptingTransformUnsafeHTML] [-
crossSiteScriptingCheckCompleteURLs] [-
SQLInjectionAction] [-
SQLInjectionTransformSpecialChars] [-
SQLInjectionOnlyCheckFieldsWithSQLChars] [-
fieldFormatAction] [-defaultFieldFormatType] [-
defaultFieldFormatMinLength] [-
defaultFieldFormatMaxLength] [-bufferOverflowAction]
[-bufferOverflowMaxURLLength] [-
bufferOverflowMaxHeaderLength] [-
bufferOverflowMaxCookieLength] [-creditCardAction] [-
creditCard] [-creditCardMaxAllowed] [-creditCardXOut]
[-XMLDoSAction] [-XMLFormatAction] [-
XMLSQLInjectionAction] [-
XMLSQLInjectionOnlyCheckFieldsWithSQLChars] [-
XMLSQLInjectionParseComments] [-XMLXSSAction] [-
XMLWSIAction] [-XMLAttachmentAction] [-
XMLValidationAction] [-XMLErrorObject] [-
useHTMLErrorObject] [-errorURL] [-HTMLErrorObject] [-
stripComments] [-defaultCharSet] [-postBodyLimit] [-
canonicalizeHTMLResponse] [-enableFormTagging] [-
excludeFileUploadFromChecks] [-
SQLInjectionParseComments] [-type]
```

Description

Use this command to remove appfw profile settings.Refer to the set appfw profile command for meanings of the arguments.

Related Commands

add appfw profile
rm appfw profile
set appfw profile
bind appfw profile
unbind appfw profile
show appfw profile

bind appfw profile

Synopsis

```
bind appfw profile <name> (-startURL <expression> | -
denyURL <expression> | (-fieldConsistency <string>
<formActionURL>  [-isRegex ( REGEX | NOTREGEX )]) | (-
cookieConsistency <string>  [-isRegex ( REGEX |
NOTREGEX )]) | (-SQLInjection <string>  <formActionURL>
[-isRegex ( REGEX | NOTREGEX )]) | (-crossSiteScripting
<string>  <formActionURL>  [-isRegex ( REGEX | NOTREGEX
)]) | (-fieldFormat <string>  <formActionURL>
<fieldType>  [-fieldFormatMinLength
<positive_integer>]  [-fieldFormatMaxLength
<positive_integer>]  [-isRegex ( REGEX | NOTREGEX )]) |
(-safeObject <string>  <expression>  <maxMatchLength>
[-action <action> ...]) | (-XMLDoSURL <expression>  [-
XMLMaxElementDepthCheck ( ON | OFF )  [-
XMLMaxElementDepth <positive_integer>]]  [-
XMLMaxElementNameLengthCheck ( ON | OFF )  [-
XMLMaxElementNameLength <positive_integer>]]  [-
XMLMaxElementsCheck ( ON | OFF )  [-XMLMaxElements
<positive_integer>]] [-XMLMaxElementChildrenCheck ( ON
| OFF )  [-XMLMaxElementChildren <positive_integer>]]
[-XMLMaxAttributesCheck ( ON | OFF )  [-
XMLMaxAttributes <positive_integer>]]  [-
XMLMaxAttributeNameLengthCheck ( ON | OFF )  [-
XMLMaxAttributeNameLength <positive_integer>]]  [-
XMLMaxAttributeValueLengthCheck ( ON | OFF )  [-
XMLMaxAttributeValueLength <positive_integer>]]  [-
XMLMaxCharDATALengthCheck ( ON | OFF )  [-
XMLMaxCharDATALength <positive_integer>]]  [-
XMLMaxFileSizeCheck ( ON | OFF )  [-XMLMaxFileSize
<positive_integer>]]  [-XMLMinFileSizeCheck ( ON | OFF
)  [-XMLMinFileSize <positive_integer>]]  [-XMLBlockPI
```

```
( ON | OFF )]  [-XMLBlockDTD ( ON | OFF )]  [-
XMLBlockExternalEntities ( ON | OFF )]) | (-XMLWSIURL
<expression>  [-XMLWSIChecks <string>]) | (-
XMLValidationURL <expression>  ((-XMLRequestSchema
<string>  [-XMLResponseSchema <string>]) | (-XMLWSDL
<string>  [-XMLAdditionalSOAPHeaders ( ON | OFF )]) | -
XMLValidateSOAPEnvelope ( ON | OFF ))    [-
XMLValidateResponse ( ON | OFF )])) [-comment <string>]
[-state ( ENABLED | DISABLED )]
```

Description

Bind a security check to the Application Firewall profile. You can bind any number of security checks to the profile. When the profile is activated (see the add appfw global command), each security check tests the data stream for the specified condition. When a test fails, the appropriate action is determined by the action configured in the profile.

Arguments

`name`
Application Firewall profile name.

`startURL`
Start URL regular expression. This binding is applicable to Profile Type: HTML, XML.

`denyURL`
Deny URL regular expression. This binding is applicable to Profile Type: HTML, XML.

`fieldConsistency`
Form field name. This binding is applicable to Profile Type: HTML.

`cookieConsistency`
Cookie name. This binding is applicable to Profile Type: HTML, XML.

`SQLInjection`
Form field name. This binding is applicable to Profile Type: HTML.

`crossSiteScripting`
Form field name. This binding is applicable to Profile Type: HTML.

fieldFormat
Field format name. This binding is applicable to Profile Type: HTML.

safeObject
Safe Object name. This binding is applicable to Profile Type: HTML, XML.

comment
Comments.

state
Enabled. Possible values: ENABLED, DISABLED Default value: ENABLED

XMLDoSURL
XML DoS URL regular expression. This binding is applicable to Profile Type: XML.

XMLWSIURL
XML WS-I URL regular expression. This binding is applicable to Profile Type: XML.

XMLValidationURL
XML Validation URL regular expression. This binding is applicable to Profile Type: XML.

Related Commands

add appfw profile
rm appfw profile
set appfw profile
unset appfw profile
unbind appfw profile
show appfw profile

unbind appfw profile

Synopsis

```
unbind appfw profile <name> (-startURL <expression> | -
denyURL <expression> | (-fieldConsistency <string>
<formActionURL>) | -cookieConsistency <string> | (-
SQLInjection <string>  <formActionURL>) | (-
crossSiteScripting <string>  <formActionURL>) | (-
fieldFormat <string>  <formActionURL>) | -safeObject
<string> | -XMLDoSURL <expression> | -XMLWSIURL
<expression> | -XMLValidationURL <expression>)
```

Description

Unbind a security check from the given Application Firewall profile.

Arguments

name
Application Firewall profile name.

startURL
Start URL regular expression.

denyURL
Deny URL regular expression.

fieldConsistency
Form field name.

cookieConsistency
Cookie name.

SQLInjection
Form field name.

crossSiteScripting
Form field name.

fieldFormat
Field format name.

safeObject
Safe Object name.

XMLDoSURL
XML DoS URL regular expression.

XMLWSIURL
XML WS-I URL regular expression.

XMLValidationURL
XML Message URL regular expression.

Related Commands

add appfw profile
rm appfw profile
set appfw profile
unset appfw profile
bind appfw profile
show appfw profile

show appfw profile

Synopsis

```
show appfw profile [<name>]
```

Description

Display all Application Firewall profiles that currently exist.

Arguments

name

The name of the Application Firewall profile.

summary

fullValues

format

level

Output

type

The profile type of of this Application Firewall profile. If the profile is of the HTML type, only checks relevant to HTML are applied. If the profile is of the XML type, only checks relevent to XML are applied. if the profile is of the Web 2.0 type, then both types of checks are applied.

useHTMLErrorObject

Use HTML Error object for response instead of Redirect Error URL.

errorURL

The error page for this profile.

HTMLErrorObject

Object name for the html error page. This check is applicable to Profile Type: HTML.

stripComments

Tells the Application Firewall to strip HTML comments from responses before sending them to the user.

defaultCharSet
The default character set. The character set that the Application Firewall uses for web pages that do not explicitly set a different character set.

postBodyLimit
The maximum body size for an HTTP POST.

canonicalizeHTMLResponse
Tells the Application Firewall to convert any non-ASCII characters into HTML entities before sending responses to the user. This is called 'canonicalization' of HTML responses.

enableFormTagging
Enables tagging of web forms for form field Consistency checks.

excludeFileUploadFromChecks
Excludes uploaded files from all web form checks.

SQLInjectionParseComments
Canonicalizes SQL Comments in form fields.

startURLAction
Start URL action types. (BLOCK | LEARN | LOG | STATS | NONE)

startURL
A literal string or regular expression that designates a URL on the Start URL list.

startURLClosure
Enable Start URL closure. When enabled, this feature allows users to start their session at a designated start URL, then navigate from that start URL to any URL on a protected web site by clicking a link on another web page on that web site. Otherwise, requests to any URL that is not explicitly allowed are blocked.

denyURLAction
Deny URL action types. (BLOCK | LOG | STATS | NONE)

denyURL
A literal string or regular expression that designates a URL on the Deny URL list.

crossSiteScriptingAction
Cross-site scripting action types. (BLOCK | LEARN | LOG | STATS | NONE)

crossSiteScriptingTransformUnsafeHTML
Enables transformation of unsafe HTML into safe HTML before forwarding a request to the web server.

crossSiteScriptingCheckCompleteURLs
Tells the Application Firewall to check complete URLs rather than just the query portion of URLs for cross-site scripting violations.

crossSiteScripting
The web form field name.

isRegex
Is the web form field name a regular expression?

formActionURL
The web form action URL.

SQLInjectionAction
SQL injection action types. (BLOCK | LEARN | LOG | STATS | NONE)

SQLInjectionTransformSpecialChars
Enables transformation of SQL special characters found in web forms into safe equivalents.

SQLInjectionOnlyCheckFieldsWithSQLChars
Tells the Application Firewall to check form fields that contain SQL special characters only, rather than all form fields, for SQL injection violations.

SQLInjection
The web form field name.

isRegex
Is the web form field name a regular expression?

formActionURL
The web form action URL.

fieldConsistencyAction
Form Field Consistency action types. (BLOCK | LEARN | LOG | STATS | NONE)

fieldConsistency
The web form field name.

isRegex
Is the web form field name a regular expression?

formActionURL
The web form action URL.

cookieConsistencyAction
Cookie consistency action types. (BLOCK | LEARN | LOG | STATS | NONE)

cookieConsistency
The name of the cookie to be checked.

isRegex
Is the cookie name a regular expression?

bufferOverflowAction
Buffer overflow action types. (BLOCK | LOG | STATS | NONE)

bufferOverflowMaxURLLength
Maximum allowed length for URLs.

bufferOverflowMaxHeaderLength
Maximum allowed length for HTTP headers.

bufferOverflowMaxCookieLength
Maximum allowed length for cookies.

fieldFormatAction
Field format action types. (BLOCK | LEARN | LOG | STATS | NONE)

defaultFieldFormatType
Name of the default field type, the field type that the Application Firewall will assign to a form field when no specific field type is assigned to that particular form field.

defaultFieldFormatMinLength
Default field type minimum length setting.

defaultFieldFormatMaxLength
Default field type maximum length setting.

`fieldFormat`
Name of the form field to which a field format will be assigned.

`isRegex`
Is the form field name a regular expression?

`formActionURL`
Action URL of the form field to which a field format will be assigned.

`fieldType`
The field type you are assigning to this form field.

`fieldFormatMinLength`
The minimum allowed length for data in this form field.

`fieldFormatMaxLength`
The maximum allowed length for data in this form field.

`creditCardAction`
Credit Card action types. (BLOCK | LOG | STATS | NONE)

`creditCard`
Credit card types. (AMEX | DINERSCLUB| DISCOVER | JBC | MASTERCARD | VISA)

`creditCardMaxAllowed`
Maximum number of times a credit card number may be seen before action is taken.

`creditCardXOut`
X-out credit card numbers.

`safeObject`
Name of the Safe Object.

`expression`
A regular expression that defines the Safe Object.

`maxMatchLength`
Maximum match length for a Safe Object expression.

`action`
Safe Object action types. (BLOCK | LOG | STATS | NONE)

XMLErrorObject
URL for the xml error page

XMLFormatAction
XML well-formed request action types. (BLOCK | LOG | STATS | NONE)

XMLDoSAction
XML DOS action types. (BLOCK | LOG | STATS | NONE)

XMLSQLInjectionAction
XML SQL Injection action types. (BLOCK | LOG | STATS | NONE)

XMLSQLInjectionOnlyCheckFieldsWithSQLChars
XML flag to check only fields with SQL characters.

XMLSQLInjectionParseComments
Canonicalize SQL Comments in XML data.

XMLXSSAction
XML cross-site scripting action types. (BLOCK | LOG | STATS | NONE)

XMLWSIAction
XML WSI action types. (BLOCK | LOG | STATS | NONE)

XMLAttachmentAction
XML attachment action types. (BLOCK | LOG | STATS | NONE)

XMLValidationAction
XML message validation action types. (BLOCK | LOG | STATS | NONE)

XMLDoSURL
XML DoS URL regular expression length.

XMLWSIURL
XML WS-I URL regular expression length.

XMLValidationURL
XML Validation URL regular expression.

state
Enabled.

XMLMaxElementDepthCheck
State if XML Max element depth check is ON or OFF.

XMLMaxElementDepth
Maximum nesting (depth) of XML elements. This check protects against documents that have excessive hierarchy depths.

XMLMaxElementNameLengthCheck
State if XML Max element name length check is ON or OFF.

XMLMaxElementNameLength
Specify the longest name of any element (including the expanded namespace) to protect against overflow attacks.

XMLMaxElementsCheck
State if XML Max elements check is ON or OFF.

XMLMaxElements
Specify the maximum number of XML elements allowed. Protects against overflow attacks.

XMLMaxElementChildrenCheck
State if XML Max element children check is ON or OFF.

XMLMaxElementChildren
Specify the maximum number of children allowed per XML element. Protects against overflow attacks.

XMLMaxNodesCheck
State if XML Max nodes check is ON or OFF.

XMLMaxNodes
Specify the maximum number of XML nodes. Protects against overflow attacks.

XMLMaxAttributesCheck
State if XML Max attributes check is ON or OFF.

XMLMaxAttributes
Specify maximum number of attributes per XML element. Protects against overflow attacks.

XMLMaxAttributeNameLengthCheck
State if XML Max attribute name length check is ON or OFF.

XMLMaxAttributeNameLength
Specify the longest name of any XML attribute. Protects against overflow attacks.

XMLMaxAttributeValueLengthCheck
State if XML Max atribute value length is ON or OFF.

XMLMaxAttributeValueLength
Specify the longest value of any XML attribute. Protects against overflow attacks.

XMLMaxCharDATALengthCheck
State if XML Max CDATA length check is ON or OFF.

XMLMaxCharDATALength
Specify the maximum size of CDATA. Protects against overflow attacks and large quantities of unparsed data within XML messages.

XMLMaxFileSizeCheck
State if XML Max file size check is ON or OFF.

XMLMaxFileSize
Specify the maximum size of XML messages. Protects against overflow attacks.

XMLMinFileSizeCheck
State if XML Min file size check is ON or OFF.

XMLMinFileSize
Enforces minimum message size.

XMLBlockPI
State if XML Block PI is ON or OFF. Protects resources from denial of service attacks as SOAP messages cannot have processing instructions (PI) in messages.

XMLBlockDTD
State if XML DTD is ON or OFF. Protects against recursive Document Type Declaration (DTD) entity expansion attacks. Also, SOAP messages cannot have DTDs in messages.

XMLBlockExternalEntities
State if XML Block External Entities Check is ON or OFF. Protects against XML External Entity (XXE) attacks that force applications to parse untrusted external entities (sources) in XML documents.

XMLWSIChecks
Specify a comma separated list of relevant WS-I rule IDs. (R1140, R1141)

XMLRequestSchema
XML Schema object for request validation .

XMLResponseSchema
XML Schema object for response validation.

XMLWSDL
WSDL object for soap request validation.

XMLAdditionalSOAPHeaders
Allow addtional soap headers.

XMLValidateSOAPEnvelope
Validate SOAP Evelope only.

XMLValidateResponse
Validate response message.

comment
Comments.

Related Commands

add appfw profile
rm appfw profile
set appfw profile
unset appfw profile
bind appfw profile
unbind appfw profile

add appfw policy

Synopsis

```
add appfw policy <name> <rule> <profileName>
```

Description

Create an Application Firewall policy.

Arguments

`name`
Application Firewall policy name.

`rule`
The rule associated with the policy.

`profileName`
Application Firewall profile name.

Related Commands

rm appfw policy
set appfw policy
show appfw policy

rm appfw policy

Synopsis

```
rm appfw policy <name>
```

Description

Remove an Application Firewall policy.

Arguments

name

Application Firewall policy name.

Related Commands

add appfw policy

set appfw policy

show appfw policy

set appfw policy

Synopsis

```
set appfw policy <name> <rule> <profileName>
```

Description

Modify an Application Firewall policy.

Arguments

`name`

Application Firewall policy name.

`rule`

The rule associated with the policy.

Related Commands

add appfw policy

rm appfw policy

show appfw policy

show appfw policy

Synopsis

```
show appfw policy [<name>]
```

Description

Display the Application Firewall policies.

Arguments

name
Application Firewall policy name.

summary

fullValues

format

level

Output

state

rule
The rule associated with the policy.

profileName
Application Firewall profile name.

hits
Number of hits.

boundTo
The entity name to which policy is bound

Related Commands

add appfw policy
rm appfw policy

set appfw policy

bind appfw global

Synopsis

```
bind appfw global <policyName> <priority> [-state (
ENABLED | DISABLED )]
```

Description

Activate an Application Firewall policy.

Arguments

policyName

Application Firewall policy name.

Related Commands

unbind appfw global

show appfw global

unbind appfw global

Synopsis

```
unbind appfw global <policyName>
```

Description

Deactivate an Application Firewall policy.

Arguments

policyName

Application Firewall policy name.

Related Commands

bind appfw global

show appfw global

show appfw global

Synopsis

```
show appfw global
```

Description

Display the active Application Firewall policies.

Arguments

summary

fullValues

format

level

Output

policyName
Application Firewall policy name.

priority
The priority of the policy.

state
The current state of the binding.

Related Commands

bind appfw global
unbind appfw global

set appfw learningsettings

Synopsis

```
set appfw learningsettings <profileName> [-
startURLMinThreshold <positive_integer>] [-
startURLPercentThreshold <positive_integer>] [-
cookieConsistencyMinThreshold <positive_integer>] [-
cookieConsistencyPercentThreshold <positive_integer>]
[-fieldConsistencyMinThreshold <positive_integer>] [-
fieldConsistencyPercentThreshold <positive_integer>]
[-crossSiteScriptingMinThreshold <positive_integer>]
[-crossSiteScriptingPercentThreshold
<positive_integer>] [-SQLInjectionMinThreshold
<positive_integer>] [-SQLInjectionPercentThreshold
<positive_integer>] [-fieldFormatMinThreshold
<positive_integer>] [-fieldFormatPercentThreshold
<positive_integer>]
```

Description

Set the Application Firewall learning settings.

Arguments

profileName

Application Firewall profile name.

startURLMinThreshold

Minimum threshold to learn Start URLs. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

startURLPercentThreshold

Minimum threshold (in percent) to learn Start URLs. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

cookieConsistencyMinThreshold
Minimum threshold to learn cookie consistency information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

cookieConsistencyPercentThreshold
Minimum threshold (in percent) to learn cookie consistency information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

fieldConsistencyMinThreshold
Minimum threshold to learn field consistency information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

fieldConsistencyPercentThreshold
Minimum threshold (in percent) to learn field consistency information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

crossSiteScriptingMinThreshold
Minimum threshold to learn cross-site scripting information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

crossSiteScriptingPercentThreshold
Minimum threshold (in percent) to learn cross-site scripting information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

SQLInjectionMinThreshold
Minimum threshold to learn SQL injection information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

SQLInjectionPercentThreshold
Minimum threshold (in percent) to learn SQL injection information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

fieldFormatMinThreshold
Minimum threshold to learn field format information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

fieldFormatPercentThreshold
Minimum threshold (in percent) to learn field format information. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

Related Commands

unset appfw learningsettings

show appfw learningsettings

unset appfw learningsettings

Synopsis

```
unset appfw learningsettings <profileName> [-
startURLMinThreshold] [-startURLPercentThreshold] [-
cookieConsistencyMinThreshold] [-
cookieConsistencyPercentThreshold] [-
fieldConsistencyMinThreshold] [-
fieldConsistencyPercentThreshold] [-
crossSiteScriptingMinThreshold] [-
crossSiteScriptingPercentThreshold] [-
SQLInjectionMinThreshold] [-
SQLInjectionPercentThreshold] [-
fieldFormatMinThreshold] [-
fieldFormatPercentThreshold]
```

Description

Use this command to remove appfw learningsettings settings.Refer to the set appfw learningsettings command for meanings of the arguments.

Related Commands

set appfw learningsettings

show appfw learningsettings

show appfw learningsettings

Synopsis

```
show appfw learningsettings [<profileName>]
```

Description

Display the Application Firewall learning settings.

Arguments

profileName
Application Firewall profile name.

summary

fullValues

format

level

Output

startURLMinThreshold
Minimum threshold to learn Start URLs.

startURLPercentThreshold
Minimum threshold (in percent) to learn Start URLs.

cookieConsistencyMinThreshold
Minimum threshold to learn cookie consistency information.

cookieConsistencyPercentThreshold
Minimum threshold (in percent) to learn cookie consistency information.

fieldConsistencyMinThreshold
Minimum threshold to learn field consistency information.

fieldConsistencyPercentThreshold
Minimum threshold (in percent) to learn field consistency information.

crossSiteScriptingMinThreshold
Minimum threshold to learn cross-site scripting information.

crossSiteScriptingPercentThreshold
Minimum threshold (in percent) to learn cross-site scripting information.

SQLInjectionMinThreshold
Minimum threshold to learn SQL injection information.

SQLInjectionPercentThreshold
Minimum threshold (in percent) to learn SQL injection information.

fieldFormatMinThreshold
Minimum threshold to learn field format information.

fieldFormatPercentThreshold
Minimum threshold (in percent) to learn field format information.

Related Commands

set appfw learningsettings
unset appfw learningsettings

rm appfw learningdata

Synopsis

```
rm appfw learningdata <profileName> (-startURL
<expression> | -cookieConsistency <string> | (-
fieldConsistency <string>  <formActionURL>) | (-
crossSiteScripting <string>  <formActionURL>) | (-
SQLInjection <string>  <formActionURL>) | (-fieldFormat
<string>  <formActionURL>))
```

Description

Remove some raw Application Firewall learning data.

Arguments

profileName
Application Firewall profile name.

startURL
Start URL configuration.

cookieConsistency
Cookie Name.

fieldConsistency
Form field name.

crossSiteScripting
Cross-site scripting.

SQLInjection
Form field name.

fieldFormat
Field format name.

Related Commands

show appfw learningdata

show appfw learningdata

Synopsis

```
show appfw learningdata <profileName> <securityCheck>
```

Description

Display the raw Application Firewall learning data.

Arguments

profileName
Application Firewall profile name.

securityCheck
Security check. Possible values: startURL, cookieConsistency, fieldConsistency, crossSiteScripting, SQLInjection, fieldFormat

summary

fullValues

Output

data
Learned data.

Related Commands

rm appfw learningdata

add appfw confidField

Synopsis

```
add appfw confidField <fieldName> <url> [-isRegex (
REGEX | NOTREGEX )] [-comment <string>] [-state (
ENABLED | DISABLED )]
```

Description

Define a form field (identified by the action URL and the field name) as confidential. These fields will have their values X'ed out in the audit logs.

Arguments

fieldName
Form field name.

url
Form action URL.

isRegex
Is field name a regular expression? Possible values: REGEX, NOTREGEX Default value: NS_NOTREGEX

comment
Comments associated with this confidential form field.

state
Enabled. Possible values: ENABLED, DISABLED Default value: ENABLED

Related Commands

rm appfw confidField

set appfw confidField

unset appfw confidField

show appfw confidField

rm appfw confidField

Synopsis

```
rm appfw confidField <fieldName> <url>
```

Description

Remove a confidential field. The field values will be logged as-is in the audit logs.

Arguments

fieldName
Form field name.

url
Form action URL.

Related Commands

add appfw confidField
set appfw confidField
unset appfw confidField
show appfw confidField

set appfw confidField

Synopsis

```
set appfw confidField <fieldName> <url> [-comment
<string>] [-state ( ENABLED | DISABLED )]
```

Description

Modify a confidential field setting. Confidential fields have their values X'ed out in the audit logs

Arguments

`fieldName`
Form field name.

`url`
Form action URL.

`comment`
Comments associated with this confidential form field.

`state`
Enabled. Possible values: ENABLED, DISABLED Default value: ENABLED

Related Commands

add appfw confidField
rm appfw confidField
unset appfw confidField
show appfw confidField

unset appfw confidField

Synopsis

```
unset appfw confidField <fieldName> <url> [-comment] [-state]
```

Description

Use this command to remove appfw confidField settings.Refer to the set appfw confidField command for meanings of the arguments.

Related Commands

add appfw confidField

rm appfw confidField

set appfw confidField

show appfw confidField

show appfw confidField

Synopsis

```
show appfw confidField [<fieldName>  <url>]
```

Description

Display all configured confidential form fields.

Arguments

fieldName
Form field name.

url
Form action URL.

summary

fullValues

format

level

Output

isRegex
Is field name a regular expression?

comment
Comments associated with this confidential form field.

state
Enabled.

Related Commands

add appfw confidField
rm appfw confidField
set appfw confidField
unset appfw confidField

rm appfw wsdl

Synopsis

```
rm appfw wsdl <name>
```

Description

Removes the object imported by import wsdl.

Arguments

name

Indicates name of the imported wsdl to be removed. Maximum value: 31

Example

rm wsdl <name>

Related Commands

show appfw wsdl

import appfw wsdl

rm appfw xmlschema

Synopsis

```
rm appfw xmlschema <name>
```

Description

Removes the object imported by import xmlschema.

Arguments

name

Indicates name of the imported xmlschema to be removed. Maximum value: 31

Example

rm xmlschema <name>

Related Commands

show appfw xmlschema

import appfw xmlschema

rm appfw xmlerrorpage

Synopsis

```
rm appfw xmlerrorpage <name>
```

Description

Removes the object imported by import xmlerrorpage.

Arguments

name

Indicates name of the imported xml error page to be removed. Maximum value: 31

Example

rm xmlerrorpage <name>

Related Commands

show appfw xmlerrorpage

import appfw xmlerrorpage

rm appfw htmlerrorpage

Synopsis

```
rm appfw htmlerrorpage <name>
```

Description

Removes the object imported by import htmlerrorpage.

Arguments

name

Indicates name of the imported html error page to be removed. Maximum value: 31

Example

rm htmlerrorpage <name>

Related Commands

show appfw htmlerrorpage

import appfw htmlerrorpage

show appfw wsdl

Synopsis

```
show appfw wsdl
```

Description

Displays the object imported by import wsdl.

Arguments

Output

Example

show appfw wsdl

Related Commands

rm appfw wsdl

import appfw wsdl

show appfw xmlschema

Synopsis

```
show appfw xmlschema
```

Description

Displays the object imported by import xmlschema.

Arguments

Output

Example

show appfw xmlschema

Related Commands

rm appfw xmlschema

import appfw xmlschema

show appfw xmlerrorpage

Synopsis

```
show appfw xmlerrorpage
```

Description

Displays the object imported by import xmlerrorpage.

Arguments

Output

Example

show appfw xmlerrorpage

Related Commands

rm appfw xmlerrorpage

import appfw xmlerrorpage

show appfw htmlerrorpage

Synopsis

```
show appfw htmlerrorpage
```

Description

Displays the object imported by import htmlerrorpage.

Arguments

Output

Example

show appfw htmlerrorpage

Related Commands

rm appfw htmlerrorpage

import appfw htmlerrorpage

import appfw wsdl

Synopsis

```
import appfw wsdl <src> <name>
```

Description

Compiles the input WSDL file into NetScaler native format.

Arguments

src

Indicates source from where to get the wsdl. Maximum value: 2047

name

Indicates name of the wsdl to import. Maximum value: 31

Example

import wsdl <src> <name>

Related Commands

rm appfw wsdl

show appfw wsdl

import appfw xmlschema

Synopsis

```
import appfw xmlschema <src> <name>
```

Description

Compiles the input XML Schema file into NetScaler native format.

Arguments

src

Indicates source from where to get the xmlschema. Maximum value: 2047

name

Indicates name of the xmlschema to import. Maximum value: 31

Example

import xmlschema <src> <name>

Related Commands

rm appfw xmlschema

show appfw xmlschema

import appfw xmlerrorpage

Synopsis

```
import appfw xmlerrorpage <src> <name>
```

Description

Downloads the input XML Error Page to NetScaler Box with the given object name

Arguments

src

Indicates source from where to get the xml error page. Maximum value: 2047

name

Indicates name of the xml error page to import. Maximum value: 31

Example

import xmlerrorpage <src> <name>

Related Commands

rm appfw xmlerrorpage

show appfw xmlerrorpage

import appfw htmlerrorpage

Synopsis

```
import appfw htmlerrorpage <src> <name>
```

Description

Downloads the input HTML Error Page to NetScaler Box with the given object name

Arguments

src

Indicates source from where to get the html error page. Maximum value: 2047

name

Indicates name of the html error page to import. Maximum value: 31

Example

import htmlerrorpage <src> <name>

Related Commands

rm appfw htmlerrorpage

show appfw htmlerrorpage

CHAPTER 5

Auditing Commands

This chapter covers the auditing commands.

stat audit

Synopsis

```
stat audit [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display the audit statistics

Arguments

Output

Counters

Audit logs sent to syslog server(s) (LogSnd)
Syslog messages sent to the syslog server(s).

Audit log messages generated (LogGen)
Syslog messages about to be sent to the syslog server.

NAT allocation failed (Ernatpcb)
NAT allocation failed

Nsb allocation failed (Ernsb)
Nsb allocation failed

Memory allocation failed (Ermem)
Failures in allocation of Access Gateway context structure. When an Access Gateway session is established, the NetScaler creates an internal context structure , which identifies the user and the IP address from which the user has logged in.

Port allocation failed (Erport)
Number of times the NetScaler failed to allocate a port when sending a syslog message to the syslog server(s).

NAT lookup failed (Hshmiss)
NAT lookup failed.

Context not found (Ctxntfnd)
Failures in finding the context structure for an Access Gateway session during attempts to send session-specific audit messages. During an Access Gateway session, audit messages related to the session are queued up in the auditlog buffer for transmission to the audit log server(s). If the session is killed before the messages are sent, the context structure allocated at session creation is removed. This structure is needed for sending the queued auditlog messages. If it is not found, this counter is incremented.

Nsb chain allocation failed (Ernsbchn)
Nsb Chain allocaiton failed.

Client connect failed (Erclconn)
Failures in establishment of a connection between the NetScaler and the auditserver tool (the Netscaler's custom logging tool).

MP buffer flush command count (flcmdcnt)
Auditlog buffer flushes. In a multiprocessor NetScaler, both the main processor and the co-processor can generate auditlog messages and fill up the auditlog buffers. But only the primary processor can free up the buffers by sending auditlog messages to the auditlog server(s). The number of auditlog buffers is fixed. If the co-processor detects that all the auditlog buffers are full, it issues a flush command to the main processor.

Related Commands

show audit stats

Synopsis

```
show audit stats - alias for 'stat audit'
```

Description

show audit stats is an alias for stat audit

Related Commands

stat audit

show audit messages

Synopsis

```
show audit messages [-logLevel <logLevel> ...] [-
numOfMesgs <positive_integer>]
```

Description

display the most recent audit log messages

Arguments

logLevel

The log level filter.

numOfMesgs

The number of log messages to be printed.Maximum value can be 256 Default value: 20 Minimum value: 1

summary

fullValues

Output

value

The Audit message

Related Commands

add audit syslogAction

Synopsis

```
add audit syslogAction <name> <serverIP> [-serverPort
<port>] -logLevel <logLevel> ... [-dateFormat (
MMDDYYYY | DDMMYYYY )] [-logFacility <logFacility>] [-
tcp ( NONE | ALL )] [-acl ( ENABLED | DISABLED )] [-
timeZone ( GMT_TIME | LOCAL_TIME )]
```

Description

Add an syslog action

Arguments

name
The name of the syslog action.

serverIP
The IP address of the syslog server.

serverPort
The port on which the syslog server is running. Default value: DEFAULT_SYSLOGPORT Minimum value: 1

logLevel
The audit log level.

dateFormat
The date format. Possible values: MMDDYYYY, DDMMYYYY Default value: NS_MMDDYYYY

logFacility
The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 Default value: SYSLOG_FACILITY_0

tcp
Log the tcp messages Possible values: NONE, ALL Default value: NS_LOG_DEFAULT

acl
Log the acl messages Possible values: ENABLED, DISABLED Default value: NS_LOG_DEFAULT

timeZone
Specifies the timezone in which the timestmps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME Default value: NS_GMT_TIME

Related Commands

rm audit syslogAction

set audit syslogAction

unset audit syslogAction

show audit syslogAction

rm audit syslogAction

Synopsis

```
rm audit syslogAction <name>
```

Description

Remove a previously configured syslog action. Note that the syslog action cannot be removed if it is bound to a syslog policy.

Arguments

name

The name of the action .

Related Commands

add audit syslogAction

set audit syslogAction

unset audit syslogAction

show audit syslogAction

set audit syslogAction

Synopsis

```
set audit syslogAction <name> [-serverIP
<ip_addr|ipv6_addr|*>] [-serverPort <port>] [-logLevel
<logLevel> ...] [-dateFormat ( MMDDYYYY | DDMMYYYY )]
[-logFacility <logFacility>] [-tcp ( NONE | ALL )] [-
acl ( ENABLED | DISABLED )] [-timeZone ( GMT_TIME |
LOCAL_TIME )]
```

Description

Modify an existing syslog action.

Arguments

name

The name for the syslog action.

serverIP

The IP address of the syslog server.

serverPort

The port on which the syslog server is running. Default value: DEFAULT_SYSLOGPORT Minimum value: 1

logLevel

The audit log level.

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY Default value: NS_MMDDYYYY

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 Default value: SYSLOG_FACILITY_0

tcp
Log the tcp messages Possible values: NONE, ALL Default value: NS_LOG_DEFAULT

acl
Log the acl messages Possible values: ENABLED, DISABLED Default value: NS_LOG_DEFAULT

timeZone
Specifies the timezone in which the timestmps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME Default value: NS_GMT_TIME

Related Commands

add audit syslogAction
rm audit syslogAction
unset audit syslogAction
show audit syslogAction

unset audit syslogAction

Synopsis

```
unset audit syslogAction <name> [-serverPort] [-
logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-
timeZone] [-serverIP]
```

Description

Reset an existing syslog action..Refer to the set audit syslogAction command for meanings of the arguments.

Related Commands

add audit syslogAction

rm audit syslogAction

set audit syslogAction

show audit syslogAction

show audit syslogAction

Synopsis

```
show audit syslogAction [<name>]
```

Description

Display details of the configured syslog action(s).

Arguments

name

The name of the syslog action. If no syslog action name is provided, all the configured syslog actions will be displayed.

summary

fullValues

format

level

Output

Related Commands

add audit syslogAction

rm audit syslogAction

set audit syslogAction

unset audit syslogAction

add audit syslogPolicy

Synopsis

```
add audit syslogPolicy <name> <rule> <action>
```

Description

Add a syslog policy. The policy defines the conditions under which the specified syslog server will be used for logging.

Arguments

`name`

The name of syslog policy.

`rule`

The name of the rule or expression that the policy will use. Currently supports only the rule "ns_true".

`action`

The name of the syslog action to be bound to the the policy.

Related Commands

rm audit syslogPolicy

set audit syslogPolicy

unset audit syslogPolicy

show audit syslogPolicy

rm audit syslogPolicy

Synopsis

```
rm audit syslogPolicy <name>
```

Description

Remove an audit syslog policy.

Arguments

name

The name of the syslog policy.

Related Commands

add audit syslogPolicy
set audit syslogPolicy
unset audit syslogPolicy
show audit syslogPolicy

set audit syslogPolicy

Synopsis

```
set audit syslogPolicy <name> [-rule <expression>] [-
action <string>]
```

Description

Modify the properties of a syslog policy.

Arguments

`name`

The name of syslog policy.

`rule`

The name of the rule or expression that the policy will use. Currently supports only the rule "ns_true".

`action`

The name of the syslog action to be bound to the the policy.

Related Commands

add audit syslogPolicy

rm audit syslogPolicy

unset audit syslogPolicy

show audit syslogPolicy

unset audit syslogPolicy

Synopsis

```
unset audit syslogPolicy <name> [-rule] [-action]
```

Description

Use this command to remove audit syslogPolicy settings.Refer to the set audit syslogPolicy command for meanings of the arguments.

Related Commands

add audit syslogPolicy

rm audit syslogPolicy

set audit syslogPolicy

show audit syslogPolicy

show audit syslogPolicy

Synopsis

```
show audit syslogPolicy [<name>]
```

Description

Display the configured syslog policies.

Arguments

name

The name of the policy to be displayed. If the policy name is not provided, all the configured syslog policies will be displayed.

summary

fullValues

format

level

Output

rule

action

boundTo

The entity name to which policy is bound

Related Commands

add audit syslogPolicy

rm audit syslogPolicy

set audit syslogPolicy

unset audit syslogPolicy

set audit syslogParams

Synopsis

```
set audit syslogParams [-serverIP
<ip_addr|ipv6_addr|*>] [-serverPort <port>] [-
dateFormat ( MMDDYYYY | DDMMYYYY )] [-logLevel
<logLevel> ...] [-logFacility <logFacility>] [-tcp (
NONE | ALL )] [-acl ( ENABLED | DISABLED )] [-timeZone
( GMT_TIME | LOCAL_TIME )]
```

Description

Modify the syslog parameters.

Arguments

serverIP

The IP address of the syslog server.

serverPort

The port on which the syslog server is running. Default value: DEFAULT_SYSLOGPORT Minimum value: 1

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY Default value: NS_MMDDYYYY

logLevel

The audit log level for which messages should be logged.

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 Default value: SYSLOG_FACILITY_0

tcp

Log the tcp messages Possible values: NONE, ALL Default value: NS_LOG_DEFAULT

acl
Log the acl messages Possible values: ENABLED, DISABLED Default value: NS_LOG_DEFAULT

timeZone
Specifies the timezone in which the timestmps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME Default value: NS_GMT_TIME

Related Commands

unset audit syslogParams

show audit syslogParams

unset audit syslogParams

Synopsis

```
unset audit syslogParams [-serverIP] [-serverPort] [-
logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-
timeZone]
```

Description

Unset syslog parameters.Refer to the set audit syslogParams command for meanings of the arguments.

Related Commands

set audit syslogParams

show audit syslogParams

show audit syslogParams

Synopsis

```
show audit syslogParams
```

Description

Display configured syslog params.

Arguments

format

level

Output

name
Name.

serverPort

Related Commands

set audit syslogParams
unset audit syslogParams

add audit nslogAction

Synopsis

```
add audit nslogAction <name> <serverIP> [-serverPort
<port>] -logLevel <logLevel> ... [-dateFormat (
MMDDYYYY | DDMMYYYY )] [-logFacility <logFacility>] [-
tcp ( NONE | ALL )] [-acl ( ENABLED | DISABLED )] [-
timeZone ( GMT_TIME | LOCAL_TIME )]
```

Description

Add an nslog action

Arguments

name

The name of the nslog action.

serverIP

The IP address of the nslog server.

serverPort

The port on which the nslog server is running. Default value: DEFAULT_NSLOGPORT Minimum value: 1

logLevel

The audit log level.

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY Default value: NS_MMDDYYYY

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 Default value: SYSLOG_FACILITY_0

tcp

Log the tcp messages Possible values: NONE, ALL Default value: NS_LOG_DEFAULT

acl
Log the acl messages Possible values: ENABLED, DISABLED Default value: NS_LOG_DEFAULT

timeZone
Specifies the timezone in which the timestmps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME Default value: NS_GMT_TIME

Related Commands

rm audit nslogAction

set audit nslogAction

unset audit nslogAction

show audit nslogAction

rm audit nslogAction

Synopsis

```
rm audit nslogAction <name>
```

Description

Remove a previously configured nslog action. Note that the nslog action cannot be removed if it is bound to an nslog policy.

Arguments

name

The name of the nslog action.

Related Commands

add audit nslogAction

set audit nslogAction

unset audit nslogAction

show audit nslogAction

set audit nslogAction

Synopsis

```
set audit nslogAction <name> [-serverIP
<ip_addr|ipv6_addr|*>] [-serverPort <port>] [-logLevel
<logLevel> ...] [-dateFormat ( MMDDYYYY | DDMMYYYY )]
[-logFacility <logFacility>] [-tcp ( NONE | ALL )] [-
acl ( ENABLED | DISABLED )] [-timeZone ( GMT_TIME |
LOCAL_TIME )]
```

Description

Modify an existing nslog action.

Arguments

name

The name for the nslog action.

serverIP

The IP address of the nslog server.

serverPort

The port on which the nslog server is running. Default value: DEFAULT_NSLOGPORT Minimum value: 1

logLevel

The audit log level.

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY Default value: NS_MMDDYYYY

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 Default value: SYSLOG_FACILITY_0

tcp
Log the tcp messages Possible values: NONE, ALL Default value: NS_LOG_DEFAULT

acl
Log the acl messages Possible values: ENABLED, DISABLED Default value: NS_LOG_DEFAULT

timeZone
Specifies the timezone in which the timestmps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME Default value: NS_GMT_TIME

Related Commands

add audit nslogAction

rm audit nslogAction

unset audit nslogAction

show audit nslogAction

unset audit nslogAction

Synopsis

```
unset audit nslogAction <name> [-serverPort] [-
logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-
timeZone]
```

Description

Unsets an existing nslog action..Refer to the set audit nslogAction command for meanings of the arguments.

Related Commands

add audit nslogAction

rm audit nslogAction

set audit nslogAction

show audit nslogAction

show audit nslogAction

Synopsis

```
show audit nslogAction [<name>]
```

Description

Display details of the configured nslog action(s).

Arguments

name

The name of the nslog action. If the nslog action name is not provided, all of the configured nslog actions will be displayed.

summary

fullValues

format

level

Output

Related Commands

add audit nslogAction

rm audit nslogAction

set audit nslogAction

unset audit nslogAction

add audit nslogPolicy

Synopsis

```
add audit nslogPolicy <name> <rule> <action>
```

Description

Add an nslog policy. The policy defines the conditions under which the specified nslog server will be used for logging.

Arguments

`name`

The name of nslog policy.

`rule`

The name of the rule or expression that the policy will use. Currently supports only the rule "ns_true". Default value: DEFAULT_RULE

`action`

The name of the nslog action to be bound to the nslog policy.

Related Commands

rm audit nslogPolicy

set audit nslogPolicy

unset audit nslogPolicy

show audit nslogPolicy

rm audit nslogPolicy

Synopsis

```
rm audit nslogPolicy <name>
```

Description

Remove an nslog policy.

Arguments

name

The name of the nslog policy.

Related Commands

add audit nslogPolicy

set audit nslogPolicy

unset audit nslogPolicy

show audit nslogPolicy

set audit nslogPolicy

Synopsis

```
set audit nslogPolicy <name> [-rule <expression>] [-
action <string>]
```

Description

Modify properties of a nslog policy.

Arguments

`name`

The name of the nslog policy to be modified.

`rule`

The new rule to be associated with the policy. Default value: DEFAULT_RULE

`action`

The new nslog action to be associated with the policy.

Related Commands

add audit nslogPolicy

rm audit nslogPolicy

unset audit nslogPolicy

show audit nslogPolicy

unset audit nslogPolicy

Synopsis

```
unset audit nslogPolicy <name> [-rule] [-action]
```

Description

Use this command to remove audit nslogPolicy settings.Refer to the set audit nslogPolicy command for meanings of the arguments.

Related Commands

add audit nslogPolicy

rm audit nslogPolicy

set audit nslogPolicy

show audit nslogPolicy

show audit nslogPolicy

Synopsis

```
show audit nslogPolicy [<name>]
```

Description

Display configured nslog policies.

Arguments

name

The name of the nslog policy. If an nslog policy name is not provided, all of the configured nslog policies will be displayed.

summary

fullValues

format

level

Output

rule

action

boundTo

The entity name to which policy is bound

Related Commands

add audit nslogPolicy

rm audit nslogPolicy

set audit nslogPolicy

unset audit nslogPolicy

set audit nslogParams

Synopsis

```
set audit nslogParams [-serverIP <ip_addr|ipv6_addr|*>]
[-serverPort <port>] [-dateFormat ( MMDDYYYY | DDMMYYYY
)] [-logLevel <logLevel> ...] [-logFacility
<logFacility>] [-tcp ( NONE | ALL )] [-acl ( ENABLED |
DISABLED )] [-timeZone ( GMT_TIME | LOCAL_TIME )]
```

Description

Modify the nslog parameters

Arguments

serverIP

The IP address of the nslog server.

serverPort

The port on which the nslog server is running. Default value: DEFAULT_NSLOGPORT Minimum value: 1

dateFormat

The date format. Possible values: MMDDYYYY, DDMMYYYY Default value: NS_MMDDYYYY

logLevel

The audit log level for which messages should be logged.

logFacility

The log facility (RFC 3164). Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 Default value: SYSLOG_FACILITY_0

tcp

Log the tcp messages Possible values: NONE, ALL Default value: NS_LOG_DEFAULT

acl

Log the acl messages Possible values: ENABLED, DISABLED Default value: NS_LOG_DEFAULT

timeZone

Specifies the timezone in which the timestamps in the log messages will be generated Possible values: GMT_TIME, LOCAL_TIME Default value: NS_GMT_TIME

Related Commands

unset audit nslogParams

show audit nslogParams

unset audit nslogParams

Synopsis

```
unset audit nslogParams [-serverIP] [-serverPort] [-
logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-
timeZone]
```

Description

Unset nslog parameters.Refer to the set audit nslogParams command for meanings of the arguments.

Related Commands

set audit nslogParams

show audit nslogParams

show audit nslogParams

Synopsis

```
show audit nslogParams
```

Description

Display configured nslog params.

Arguments

format

level

Output

name
Name of the nslog param.

serverIP

serverPort

dateFormat

logLevel
The audit log level.

logFacility

Related Commands

set audit nslogParams
unset audit nslogParams

CHAPTER 6

Authentication Commands

This chapter covers the authentication commands.

add authentication radiusAction

Synopsis

```
add authentication radiusAction <name> {-serverIP
<ip_addr|ipv6_addr|*>} [-serverPort <port>] [-
authTimeout <positive_integer>] {-radKey } [-radNASip (
ENABLED | DISABLED )] [-radNASid <string>] [-
radVendorID <positive_integer>] [-radAttributeType
<positive_integer>] [-radGroupsPrefix <string>] [-
radGroupSeparator <string>] [-passEncoding
<passEncoding>] [-ipVendorID <positive_integer>] [-
ipAttributeType <positive_integer>] [-accounting ( ON |
OFF )] [-pwdVendorID <positive_integer>  [-
pwdAttributeType <positive_integer>]]
```

Description

Add a profile for a RADIUS server. The profile contains all the configuration data necessary to communicate with a RADIUS server.

Arguments

`name`
The name of the RADIUS action.

`serverIP`
The IP address of the RADIUS server.

`serverPort`
The port on which the RADIUS Server is running. Default value: 1812 Minimum value: 1

`authTimeout`
The maximum number of seconds the system will wait for a response from the RADIUS server. Default value: 3 Minimum value: 1

`radKey`
The key shared between the client and the server. This information is required for the system to communicate with the RADIUS server.

radNASip
If enabled, the system's IP address (NSIP) is sent to the server as the "nasip" in accordance with the RADIUS protocol. Possible values: ENABLED, DISABLED

radNASid
If configured, this string is sent to the RADIUS server as the "nasid" in accordance with the RADIUS protocol.

radVendorID
The vendor ID for using RADIUS group extraction. Minimum value: 1

radAttributeType
The Attribute type for using RADIUS group extraction. Minimum value: 1

radGroupsPrefix
The groups prefix string that precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator
The group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding
This option specifies how passwords should be encoded in the radius packets traveling from the system to the RADIUS server. Possible values: pap, chap, mschapv1, mschapv2 Default value: AAA_PAP

ipVendorID
The vendor ID of the attribute in the RADIUS response which denotes the intranet IP. The value of 0 denotes that the attribute is not vendor encoded. Minimum value: 0

ipAttributeType
The attribute type of the remote IP address attribute in a RADIUS response. Minimum value: 1

accounting
The state of the RADIUS server that will receive accounting messages. Possible values: ON, OFF

pwdVendorID
Vendor ID of the attribute in the RADIUS response which will be used to extract the user Password. Minimum value: 1

pwdAttributeType
Attribute type of the vendor specific Password-Attribute in a RADIUS response. Minimum value: 1

Related Commands

rm authentication radiusAction

set authentication radiusAction

unset authentication radiusAction

show authentication radiusAction

rm authentication radiusAction

Synopsis

```
rm authentication radiusAction <name>
```

Description

Remove a previously created RADIUS action. Note that an action cannot be removed as long as it is configured in a policy.

Arguments

name

The name of the action to be removed.

Related Commands

add authentication radiusAction

set authentication radiusAction

unset authentication radiusAction

show authentication radiusAction

set authentication radiusAction

Synopsis

```
set authentication radiusAction <name> {-serverIP
<ip_addr|ipv6_addr|*>} [-serverPort <port>] [-
authTimeout <positive_integer>] {-radKey } [-radNASip (
ENABLED | DISABLED )] [-radNASid <string>] [-
radVendorID <positive_integer>] [-radAttributeType
<positive_integer>] [-radGroupsPrefix <string>] [-
radGroupSeparator <string>] [-passEncoding
<passEncoding>] [-ipVendorID <positive_integer>] [-
ipAttributeType <positive_integer>] [-accounting ( ON |
OFF )] [-pwdVendorID <positive_integer>] [-
pwdAttributeType <positive_integer>]
```

Description

Change the profile for a RADIUS server. The profile contains all the configuration data needed to communicate with a RADIUS server.

Arguments

`name`
The name of the RADIUS action.

`serverIP`
The IP address of the RADIUS server.

`serverPort`
The port on which RADIUS Server is running. Default value: 1812 Minimum value: 1

`authTimeout`
The maximum number of seconds the system will wait for a response from the RADIUS server. Default value: 3 Minimum value: 1

`radKey`
The key shared between the client and the server. This information is required for the system to communicate with the RADIUS server.

radNASip
If enabled, the system's IP address (NSIP) is sent to the server as the "nasip" in accordance with the RADIUS protocol. Possible values: ENABLED, DISABLED

radNASid
If configured, this string is sent to the RADIUS server as the "nasid" in accordance with the RADIUS protocol.

radVendorID
The Vendor ID for using RADIUS group extraction. Minimum value: 1

radAttributeType
The Attribute type for using RADIUS group extraction. Minimum value: 1

radGroupsPrefix
The groups prefix string that precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator
The group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding
This option specifies how passwords should be encoded in RADIUS packets traveling from the system to the RADIUS server. Possible values: pap, chap, mschapv1, mschapv2 Default value: AAA_PAP

ipVendorID
The vendor ID of the attribute in the RADIUS response which denotes the intranet IP. The value of 0 denotes that the attribute is not vendor encoded. Minimum value: 0

ipAttributeType
The attribute type of the remote IP address attribute in a RADIUS response. Minimum value: 1

accounting
The state of the RADIUS server that will receive accounting messages. Possible values: ON, OFF

pwdVendorID
Vendor ID of the attribute in the RADIUS response which will be used to extract the user Password. Minimum value: 1

Related Commands

add authentication radiusAction
rm authentication radiusAction
unset authentication radiusAction
show authentication radiusAction

unset authentication radiusAction

Synopsis

```
unset authentication radiusAction <name> [-serverPort]
[-authTimeout] [-radNASip] [-radNASid] [-radVendorID]
[-radAttributeType] [-radGroupsPrefix] [-
radGroupSeparator] [-passEncoding] [-ipVendorID] [-
ipAttributeType] [-accounting] [-pwdVendorID] [-
pwdAttributeType]
```

Description

Use this command to remove authentication radiusAction settings.Refer to the set authentication radiusAction command for meanings of the arguments.

Related Commands

add authentication radiusAction

rm authentication radiusAction

set authentication radiusAction

show authentication radiusAction

show authentication radiusAction

Synopsis

```
show authentication radiusAction [<name>]
```

Description

Display details of the configured RADIUS action(s).

Arguments

`name`
The name of the RADIUS action.

`summary`

`fullValues`

`format`

`level`

Output

`IPAddress`
IP address.

`radGroupsPrefix`
The groups prefix string that precedes the group names within a RADIUS attribute for RADIUS group extraction.

`radGroupSeparator`
The group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction.

`accounting`
The state of the RADIUS server that will receive accounting messages.

`pwdVendorID`
Vendor ID of the attribute in the RADIUS response which will be used to extract the user Password.

pwdAttributeType
Attribute type of the vendor specific Password-Attribute in a RADIUS response.

Related Commands

add authentication radiusAction
rm authentication radiusAction
set authentication radiusAction
unset authentication radiusAction

add authentication ldapAction

Synopsis

```
add authentication ldapAction <name> [-serverIP
<ip_addr|ipv6_addr|*>] [-serverPort <port>] [-
authTimeout <positive_integer>] [-ldapBase <string>] [-
ldapBindDn <string>] {-ldapBindDnPassword } [-
ldapLoginName <string>] [-searchFilter <string>] [-
groupAttrName <string>] [-subAttributeName <string>] [-
secType <secType>] [-ssoNameAttribute <string>] [-
authentication ( ENABLED | DISABLED )] [-requireUser (
YES | NO )] [-nestedGroupExtraction ( ON | OFF )  [-
maxNestingLevel <positive_integer>]  [-
groupSearchSubAttribute <string>]  [-groupSearchFilter
<string>]] [-groupNameIdentifier <string>] [-
groupSearchAttribute <string>]
```

Description

Add a profile for an LDAP server. This profile contains all the configuration data needed to communicate with the LDAP server..

Arguments

`name`
The name for the new LDAP action.

`serverIP`
The IP address of the LDAP server.

`serverPort`
The port number on which the LDAP server is running. Default value: 389 Minimum value: 1

`authTimeout`
The maximum number of seconds the system will wait for a response from the LDAP server. Default value: 3 Minimum value: 1

ldapBase
The base, or node where the ldapsearch should start. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.

ldapBindDn
The full distinguished name that is used to bind to the LDAP server. The default value of the bindDN is cn=Manager,dc=netscaler,dc=com.

ldapBindDnPassword
The password that is used to bind to the LDAP server.

ldapLoginName
The name attribute used by the system to query the external LDAP server or an Active Directory.

searchFilter
The string to be combined with the default LDAP user search string to form the value. For example, vpnallowed=true with ldaploginame "samaccount" and the user-supplied username "bob" would yield the LDAP search string "(&(vpnallowed=true)(samaccount=bob)".

groupAttrName
The Attribute name for group extraction from the LDAP server.

subAttributeName
The Sub-Attribute name for group extraction from the LDAP server.

secType
This option indicates whether communication between the system and the authentication server should be encrypted. The following values are allowed: PLAINTEXT: No encryption required. TLS: Communicate using TLS protocol. SSL: Communicate using SSL Protocol. Possible values: PLAINTEXT, TLS, SSL Default value: AAA_LDAP_PLAINTEXT

ssoNameAttribute
The attribute used by the system to query the external LDAP server, or an Active Directory, for an alternate username to be used in Single Sign-On.

authentication
Disable authentication. If disabled this LDAP action will return authentication success if the user is found. This should only be used for authorization group extraction and in conjuction with other authentication methods. The other authentication methods should be bound to a primary list

or flagged as secondary. Possible values: ENABLED, DISABLED Default value: ENABLED

requireUser
Setting this option to NO allows failed user searches to be considered authentication successes. If you set require user to NO, you may only configure it with authentication DISABLED Possible values: YES, NO Default value: YES

nestedGroupExtraction
Setting this option to ON enables the nested group extraction feature where the system queries the external LDAP server to determine if a group belongs to another group Possible values: ON, OFF Default value: OFF

maxNestingLevel
If NESTED GROUP EXTRACTION is set to ON, this option specifies the level upto which ancestors of a group/subgroup will be determined Default value: 2 Minimum value: 2

groupNameIdentifier
The group-attribute used by the system to uniquely identify a group in LDAP/AD

groupSearchAttribute
This option specifies the attribute that will be used to determine group-membership of a 'group'

groupSearchSubAttribute
This option specifies the sub-attribute that will be used to determine group-membership of a 'group'

groupSearchFilter
The string to be combined with the default LDAP group search string to form the value. For example, vpnallowed=true with groupIdentifier "samaccount" and the groupname "g1" would yield the LDAP search string "(&(vpnallowed=true)(samaccount=g1)".

Related Commands

rm authentication ldapAction

set authentication ldapAction

unset authentication ldapAction

show authentication ldapAction

rm authentication ldapAction

Synopsis

```
rm authentication ldapAction <name>
```

Description

Remove an LDAP action. Note that an action cannot be removed as long as it is configured in a policy.

Arguments

name

The name of the LDAP action to be removed.

Related Commands

add authentication ldapAction

set authentication ldapAction

unset authentication ldapAction

show authentication ldapAction

set authentication ldapAction

Synopsis

```
set authentication ldapAction <name> [-serverIP
<ip_addr|ipv6_addr|*>] [-serverPort <port>] [-
authTimeout <positive_integer>] [-ldapBase <string>] [-
ldapBindDn <string>] {-ldapBindDnPassword } [-
ldapLoginName <string>] [-searchFilter <string>] [-
groupAttrName <string>] [-subAttributeName <string>] [-
secType <secType>] [-ssoNameAttribute <string>] [-
authentication ( ENABLED | DISABLED )] [-requireUser (
YES | NO )] [-nestedGroupExtraction ( ON | OFF )] [-
maxNestingLevel <positive_integer>] [-
groupNameIdentifier <string>] [-groupSearchAttribute
<string>  [-groupSearchSubAttribute <string>]] [-
groupSearchFilter <string>]
```

Description

Changes the profile of an LDAP server. The profile contains all of the configuration data needed to communicate with the LDAP server.

Arguments

`name`
The name for the new LDAP action.

`serverIP`
The IP address of the LDAP server.

`serverPort`
The port number on which the LDAP server is running. Default value: 389 Minimum value: 1

`authTimeout`
The maximum number of seconds for the system will wait for a response from the LDAP server. Default value: 3 Minimum value: 1

ldapBase
The base, or node, where the ldapsearch should start. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.

ldapBindDn
The full distinguished name that is used to bind to the LDAP server. The default value of the bindDN is cn=Manager,dc=netscaler,dc=com.

ldapBindDnPassword
The password that is used to bind to the LDAP server.

ldapLoginName
The name attribute used by the system to query the external LDAP server or an Active Directory.

searchFilter
The string to be combined with the default LDAP user search string to form the value.For example, vpnallowed=true with ldaploginame "samaccount" and the user-supplied username "bob" would yield the LDAP search string "(&(vpnallowed=true)(samaccount=bob)".

groupAttrName
The Attribute name for group extraction from the LDAP server.

subAttributeName
The Sub-Attribute name for group extraction from the LDAP server.

secType
This option indicates whether communication between the system and the authentication server should be encrypted. The following values are allowed: PLAINTEXT: No encryption required. TLS: Communicate using TLS protocol. SSL: Communicate using SSL protocol. Possible values: PLAINTEXT, TLS, SSL Default value: AAA_LDAP_PLAINTEXT

ssoNameAttribute
The attribute used by the system to query the external LDAP server, or an Active Directory, for an alternate username to be used in Single Sign-On.

authentication
Disable authentication. If disabled this LDAP action will return authentication success if the user is found. This should only be used for authorization group extraction and in conjuction with other authentication methods. The other authentication methods should be bound to a primary list

or flagged as secondary. Possible values: ENABLED, DISABLED Default value: ENABLED

`requireUser`

This option allows failed searches to be considered authentication successes. If you set require user to NO, you may only configure it with authentication DISABLED Possible values: YES, NO Default value: YES

`nestedGroupExtraction`

Setting this option to ON enables the nested group extraction feature where the system queries the external LDAP server to determine if a group belongs to another group Possible values: ON, OFF Default value: OFF

Related Commands

add authentication ldapAction

rm authentication ldapAction

unset authentication ldapAction

show authentication ldapAction

unset authentication ldapAction

Synopsis

```
unset authentication ldapAction <name> [-serverIP] [-
serverPort] [-authTimeout] [-ldapBase] [-ldapBindDn] [-
ldapBindDnPassword] [-ldapLoginName] [-searchFilter]
[-groupAttrName] [-subAttributeName] [-secType] [-
ssoNameAttribute] [-authentication] [-requireUser] [-
nestedGroupExtraction] [-maxNestingLevel] [-
groupNameIdentifier] [-groupSearchAttribute] [-
groupSearchSubAttribute] [-groupSearchFilter]
```

Description

Use this command to remove authentication ldapAction settings.Refer to the set authentication ldapAction command for meanings of the arguments.

Related Commands

add authentication ldapAction

rm authentication ldapAction

set authentication ldapAction

show authentication ldapAction

show authentication ldapAction

Synopsis

```
show authentication ldapAction [<name>]
```

Description

Display details of the configured LDAP action(s).

Arguments

name

The name of the LDAP action.

summary

fullValues

format

level

Output

ldapBindDn

ldapLoginName

ldapBase

searchFilter

groupAttrName

subAttributeName

secType

ssoNameAttribute

authentication

requireUser

nestedGroupExtraction

maxNestingLevel

groupNameIdentifier

groupSearchAttribute

groupSearchSubAttribute

groupSearchFilter

Related Commands

add authentication ldapAction
rm authentication ldapAction
set authentication ldapAction
unset authentication ldapAction

add authentication tacacsAction

Synopsis

```
add authentication tacacsAction <name> [-serverIP
<ip_addr|ipv6_addr|*>] [-serverPort <port>] [-
authTimeout <positive_integer>] {-tacacsSecret } [-
authorization ( ON | OFF )] [-accounting ( ON | OFF )]
```

Description

Add a profile for a TACACS+ server. The profile contains all of the configuration data needed to communicate with the TACACS+ server.

Arguments

`name`
The name for the new TACACS+ action.

`serverIP`
The IP address of the TACACS+ server.

`serverPort`
The port on which the TACACS+ server is running. Default value: 49 Minimum value: 1

`authTimeout`
The maximum number of seconds the system will wait for a response from the TACACS+ server. Default value: 3 Minimum value: 1

`tacacsSecret`
The key shared between the client and the server. This information is required for the system to communicate with the TACACS+ server.

`authorization`
The state of the TACACS+ server that will be used for streaming authorization. Possible values: ON, OFF

`accounting`
The state of the TACACS+ server that will receive accounting messages. Possible values: ON, OFF

Related Commands

rm authentication tacacsAction
set authentication tacacsAction
unset authentication tacacsAction
show authentication tacacsAction

rm authentication tacacsAction

Synopsis

```
rm authentication tacacsAction <name>
```

Description

Remove a TACACS+ action. Note that an action cannot be removed if it is configured in a policy.

Arguments

name

The name of TACACS+ action to be removed.

Related Commands

add authentication tacacsAction

set authentication tacacsAction

unset authentication tacacsAction

show authentication tacacsAction

set authentication tacacsAction

Synopsis

```
set authentication tacacsAction <name> [-serverIP
<ip_addr|ipv6_addr|*>] [-serverPort <port>] [-
authTimeout <positive_integer>] {-tacacsSecret } [-
authorization ( ON | OFF )] [-accounting ( ON | OFF )]
```

Description

Changes the profile for a TACACS+ server. The profile contains all the configuration data needed to communicate with the TACACS+ server.

Arguments

`name`
The name for the new TACACS+ action.

`serverIP`
The IP address of the TACACS+ server.

`serverPort`
The port on which the TACACS+ server is running. Default value: 49 Minimum value: 1

`authTimeout`
The maximum number of seconds the system will wait for a response from the TACACS+ server. Default value: 3 Minimum value: 1

`tacacsSecret`
The key shared between the client and the server. This information is required for the system to communicate with the TACACS+ server.

`authorization`
The state of the TACACS+ server to be used for streaming authorization. Possible values: ON, OFF

`accounting`
The state of the TACACS+ server that will receive accounting messages. Possible values: ON, OFF

Related Commands

add authentication tacacsAction
rm authentication tacacsAction
unset authentication tacacsAction
show authentication tacacsAction

unset authentication tacacsAction

Synopsis

```
unset authentication tacacsAction <name> [-serverIP] [-
serverPort] [-authTimeout] [-tacacsSecret] [-
authorization] [-accounting]
```

Description

Use this command to remove authentication tacacsAction settings.Refer to the set authentication tacacsAction command for meanings of the arguments.

Related Commands

add authentication tacacsAction

rm authentication tacacsAction

set authentication tacacsAction

show authentication tacacsAction

show authentication tacacsAction

Synopsis

```
show authentication tacacsAction [<name>]
```

Description

Display details of the configured TACACS+ action(s).

Arguments

`name`

The name of the TACACS+ action.

`summary`

`fullValues`

`format`

`level`

Output

`tacacsSecret`

`authorization`

The state of the TACACS+ server that will be used for streaming authorization.

`accounting`

The state of the TACACS+ server that will receive accounting messages.

Related Commands

add authentication tacacsAction

rm authentication tacacsAction

set authentication tacacsAction

unset authentication tacacsAction

add authentication nt4Action

Synopsis

```
add authentication nt4Action <name> [-serverIP
<ip_addr|ipv6_addr|*>] [-nt4ServerName <string>] [-
nt4DomainName <string>] [-nt4AdminUser <string>] {-
nt4AdminPasswd }
```

Description

Add a profile for an NT4 server. The profile contains all of the configuration data needed to communicate with the NT4 server.

Arguments

name
The name for the new NT4 action.

serverIP
The IP address of the NT4 server.

nt4ServerName
The name of the NT4 server

nt4DomainName
The domain name of the NT4 server

nt4AdminUser
The username of an NT4 Domain Administrator

nt4AdminPasswd
The password of the NT4 Domain Administrator

Related Commands

rm authentication nt4Action
set authentication nt4Action
unset authentication nt4Action
show authentication nt4Action

rm authentication nt4Action

Synopsis

```
rm authentication nt4Action <name>
```

Description

Remove an NT4 action. Note that an action cannot be removed if it is configured in a policy.

Arguments

name

The name of the NT4 action to be removed.

Related Commands

add authentication nt4Action

set authentication nt4Action

unset authentication nt4Action

show authentication nt4Action

set authentication nt4Action

Synopsis

```
set authentication nt4Action <name> [-serverIP
<ip_addr|ipv6_addr|*>] [-nt4ServerName <string>] [-
nt4DomainName <string>] [-nt4AdminUser <string>] {-
nt4AdminPasswd }
```

Description

Changes the profile for an NT4 server. The profile contains all of the configuration data needed to communicate with the NT4 server.

Arguments

`name`
The name for the new NT4 action.

`serverIP`
The IP address of the NT4 server.

`nt4ServerName`
The name of the NT4 server

`nt4DomainName`
The domain name of the NT4 server

`nt4AdminUser`
The username of an NT4 Domain Administrator

`nt4AdminPasswd`
The password of the NT4 Domain Administrator

Related Commands

add authentication nt4Action
rm authentication nt4Action
unset authentication nt4Action
show authentication nt4Action

unset authentication nt4Action

Synopsis

unset authentication nt4Action <name> [-serverIP] [-nt4ServerName] [-nt4DomainName] [-nt4AdminUser] [-nt4AdminPasswd]

Description

Use this command to remove authentication nt4Action settings.Refer to the set authentication nt4Action command for meanings of the arguments.

Related Commands

add authentication nt4Action

rm authentication nt4Action

set authentication nt4Action

show authentication nt4Action

show authentication nt4Action

Synopsis

```
show authentication nt4Action [<name>]
```

Description

Display the details of the configured NT4 action(s).

Arguments

name

The name of the NT4 action.

summary

fullValues

format

level

Output

nt4ServerName

nt4DomainName

nt4AdminUser

Related Commands

add authentication nt4Action
rm authentication nt4Action
set authentication nt4Action
unset authentication nt4Action

add authentication certAction

Synopsis

add authentication certAction <name> [-twoFactor (ON | OFF)] [-userNameField <string>] [-groupNameField <string>]

Description

Add a certificate action.

Arguments

name

The name of the CERT action.

twoFactor

The state of two factor authentication. Two factor authentication means client certificate authentication followed by password authentication. Possible values: ON, OFF Default value: OFF

userNameField

The field in the client certificate from which the username will be extracted. Should be of the format <field:subfield>. Allowed values for the field are "Subject" and "Issuer".

groupNameField

The field in the certificate from which the group will be extracted. Should be of the format <field:subfield>. Allowed values for the field are "Subject" and "Issuer".

Example

add authentication certaction -twoFactor ON -userNameField "Subject:CN" -groupNameField "Subject:OU"

Related Commands

add aaa certparam

add authentication certpolicy

rm authentication certAction

set authentication certAction
unset authentication certAction
show authentication certAction

rm authentication certAction

Synopsis

```
rm authentication certAction <name>
```

Description

Remove a cert action. Note that an action cannot be removed if it is configured in a policy.

Arguments

name

The name of the NT4 action to be removed.

Related Commands

add authentication certAction

set authentication certAction

unset authentication certAction

show authentication certAction

set authentication certAction

Synopsis

```
set authentication certAction <name> [-twoFactor ( ON | OFF )] [-userNameField <string>] [-groupNameField <string>]
```

Description

Modifies the certificate action.

Arguments

name

The name of the CERT action.

twoFactor

The state of two factor authentication. Two factor authentication means client certificate authentication followed by password authentication. Possible values: ON, OFF Default value: OFF

userNameField

The field in the client certificate from which the username will be extracted. Should be of the format <field:subfield>. Allowed values for the field are "Subject" and "Issuer".

groupNameField

The field in the certificate from which the group will be extracted. Should be of the format <field:subfield>. Allowed values for the field are "Subject" and "Issuer".

Example

set authentication certaction -twoFactor ON -userNameField "Subject:CN" -groupNameField "Subject:OU"

Related Commands

add aaa certparam

add authentication certpolicy

add authentication certAction

rm authentication certAction
unset authentication certAction
show authentication certAction

unset authentication certAction

Synopsis

```
unset authentication certAction <name> [-twoFactor] [-
userNameField] [-groupNameField]
```

Description

Use this command to remove authentication certAction settings.Refer to the set authentication certAction command for meanings of the arguments.

Related Commands

add authentication certAction

rm authentication certAction

set authentication certAction

show authentication certAction

show authentication certAction

Synopsis

```
show authentication certAction [<name>]
```

Description

Display the details of configured CERT action(s).

Arguments

name

The name of the CERT action.

summary

fullValues

format

level

Output

twoFactor

The state of two factor authentication.

userNameField

The field in the certificate from which the username will be extracted.

groupNameField

The field in the certificate from which the group will be extracted.

Related Commands

add authentication certAction

rm authentication certAction

set authentication certAction

unset authentication certAction

add authentication localPolicy

Synopsis

```
add authentication localPolicy <name> <rule>
```

Description

Add an authentication LOCAL policy. The policy defines the conditions under which the kernel will authenticate the user.

Arguments

`name`

The name of the new authentication LOCAL policy.

`rule`

The name of the rule or expression the policy will use.

Related Commands

rm authentication localPolicy

set authentication localPolicy

unset authentication localPolicy

show authentication localPolicy

rm authentication localPolicy

Synopsis

```
rm authentication localPolicy <name>
```

Description

Remove an authentication LOCAL policy.

Arguments

name

The name of the LOCAL policy to remove.

Related Commands

add authentication localPolicy

set authentication localPolicy

unset authentication localPolicy

show authentication localPolicy

set authentication localPolicy

Synopsis

```
set authentication localPolicy <name> -rule
<expression>
```

Description

Change properties of a LOCAL policy.

Arguments

`name`

The name of the policy.

`rule`

The new rule to be associated with the policy.

Related Commands

add authentication localPolicy

rm authentication localPolicy

unset authentication localPolicy

show authentication localPolicy

unset authentication localPolicy

Synopsis

```
unset authentication localPolicy <name> -rule
```

Description

Use this command to remove authentication localPolicy settings.Refer to the set authentication localPolicy command for meanings of the arguments.

Related Commands

add authentication localPolicy

rm authentication localPolicy

set authentication localPolicy

show authentication localPolicy

show authentication localPolicy

Synopsis

```
show authentication localPolicy [<name>]
```

Description

Display configured LOCAL policies.

Arguments

name

The name of the policy. If a name is not provided, all the configured LOCAL policies will be displayed.

summary

fullValues

format

level

Output

rule

The new rule associated with the policy.

boundTo

The entity name to which policy is bound

Related Commands

add authentication localPolicy

rm authentication localPolicy

set authentication localPolicy

unset authentication localPolicy

add authentication radiusPolicy

Synopsis

```
add authentication radiusPolicy <name> <rule>
[<reqAction>]
```

Description

Add an authentication RADIUS policy. The policy defines the conditions under which the specified RADIUS server will be used for authentication.

Arguments

`name`

The name of the new authentication RADIUS policy.

`rule`

The name of the rule or expression the policy will use.

`reqAction`

The name of the RADIUS action the policy will use.

Related Commands

rm authentication radiusPolicy

set authentication radiusPolicy

unset authentication radiusPolicy

show authentication radiusPolicy

rm authentication radiusPolicy

Synopsis

```
rm authentication radiusPolicy <name>
```

Description

Remove an authentication RADIUS policy.

Arguments

name

The name of the RADIUS policy to remove.

Related Commands

add authentication radiusPolicy
set authentication radiusPolicy
unset authentication radiusPolicy
show authentication radiusPolicy

set authentication radiusPolicy

Synopsis

```
set authentication radiusPolicy <name> [-rule
<expression>] [-reqAction <string>]
```

Description

Change properties of a RADIUS policy.

Arguments

`name`

The name of the policy.

`rule`

The new rule to be associated with the policy.

`reqAction`

The new RADIUS action to be associated with the policy.

Related Commands

add authentication radiusPolicy

rm authentication radiusPolicy

unset authentication radiusPolicy

show authentication radiusPolicy

unset authentication radiusPolicy

Synopsis

```
unset authentication radiusPolicy <name> [-rule] [-reqAction]
```

Description

Use this command to remove authentication radiusPolicy settings.Refer to the set authentication radiusPolicy command for meanings of the arguments.

Related Commands

add authentication radiusPolicy

rm authentication radiusPolicy

set authentication radiusPolicy

show authentication radiusPolicy

show authentication radiusPolicy

Synopsis

```
show authentication radiusPolicy [<name>]
```

Description

Display configured RADIUS policies.

Arguments

name

The name of the policy. If no name is provided, all the configured RADIUS policies will be displayed.

summary

fullValues

format

level

Output

rule

The new rule associated with the policy.

reqAction

The new RADIUS action associated with the policy.

boundTo

The entity name to which policy is bound

Related Commands

add authentication radiusPolicy

rm authentication radiusPolicy

set authentication radiusPolicy

unset authentication radiusPolicy

add authentication certPolicy

Synopsis

```
add authentication certPolicy <name> <rule>
[<reqAction>]
```

Description

Add an authentication cert policy. This policy defines the conditions under which the specified cert action will be used for authentication.

Arguments

`name`
The name for the new policy.

`rule`
The name of the rule or expression the policy will use.

`reqAction`
The cert action to associate with the policy.

Related Commands

rm authentication certPolicy
set authentication certPolicy
unset authentication certPolicy
show authentication certPolicy

rm authentication certPolicy

Synopsis

```
rm authentication certPolicy <name>
```

Description

Remove a CERT authentication policy.

Arguments

name

The name of the CERT policy to be removed.

Related Commands

add authentication certPolicy

set authentication certPolicy

unset authentication certPolicy

show authentication certPolicy

set authentication certPolicy

Synopsis

```
set authentication certPolicy <name> [-rule
<expression>] [-reqAction <string>]
```

Description

Change the properties of a CERT policy.

Arguments

`name`

The name of the policy.

`rule`

The new rule to associate with the policy.

`reqAction`

The new cert action to associate to the policy.

Related Commands

add authentication certPolicy

rm authentication certPolicy

unset authentication certPolicy

show authentication certPolicy

unset authentication certPolicy

Synopsis

```
unset authentication certPolicy <name> [-rule] [-
reqAction]
```

Description

Use this command to remove authentication certPolicy settings.Refer to the set authentication certPolicy command for meanings of the arguments.

Related Commands

add authentication certPolicy

rm authentication certPolicy

set authentication certPolicy

show authentication certPolicy

show authentication certPolicy

Synopsis

```
show authentication certPolicy [<name>]
```

Description

Display configured CERT policies.

Arguments

name

The name of the policy. If a name is not provided, all of the configured policies are displayed.

summary

fullValues

format

level

Output

rule

The rule associated with the policy.

reqAction

The cert action associated with the policy.

boundTo

The entity name to which policy is bound

Related Commands

add authentication certPolicy

rm authentication certPolicy

set authentication certPolicy

unset authentication certPolicy

add authentication ldapPolicy

Synopsis

```
add authentication ldapPolicy <name> <rule>
[<reqAction>]
```

Description

Add an authentication LDAP policy. This policy defines the conditions under which the specified LDAP server will be used for authentication.

Arguments

`name`
The name for the new policy.

`rule`
The name of the rule or expression the policy will use.

`reqAction`
The LDAP action to associate with the policy.

Related Commands

rm authentication ldapPolicy
set authentication ldapPolicy
unset authentication ldapPolicy
show authentication ldapPolicy

rm authentication ldapPolicy

Synopsis

```
rm authentication ldapPolicy <name>
```

Description

Remove an LDAP authentication policy.

Arguments

name

The name of the LDAP policy to be removed.

Related Commands

add authentication ldapPolicy
set authentication ldapPolicy
unset authentication ldapPolicy
show authentication ldapPolicy

set authentication ldapPolicy

Synopsis

```
set authentication ldapPolicy <name> [-rule
<expression>] [-reqAction <string>]
```

Description

Change properties of an LDAP policy.

Arguments

`name`

The name of the policy.

`rule`

The new rule to associate with the policy.

`reqAction`

The new LDAP action to associate with the policy.

Related Commands

add authentication ldapPolicy

rm authentication ldapPolicy

unset authentication ldapPolicy

show authentication ldapPolicy

unset authentication ldapPolicy

Synopsis

```
unset authentication ldapPolicy <name> [-rule] [-
reqAction]
```

Description

Use this command to remove authentication ldapPolicy settings.Refer to the set authentication ldapPolicy command for meanings of the arguments.

Related Commands

add authentication ldapPolicy

rm authentication ldapPolicy

set authentication ldapPolicy

show authentication ldapPolicy

show authentication ldapPolicy

Synopsis

```
show authentication ldapPolicy [<name>]
```

Description

Display configured LDAP policies.

Arguments

name

The name of the policy. If a name is not provided, all of the configured policies are displayed.

summary

fullValues

format

level

Output

rule

reqAction

boundTo

The entity name to which policy is bound

Related Commands

add authentication ldapPolicy

rm authentication ldapPolicy

set authentication ldapPolicy

unset authentication ldapPolicy

add authentication tacacsPolicy

Synopsis

```
add authentication tacacsPolicy <name> <rule>
[<reqAction>]
```

Description

Add an authentication TACACS+ policy. This policy defines the conditions under which the specified TACACS+ server will be used for authentication.

Arguments

name

The name of the new TACACS+ policy.

rule

The name of the rule or expression the policy will use.

reqAction

The name of the TACACS+ action to be associated with the policy.

Related Commands

rm authentication tacacsPolicy

set authentication tacacsPolicy

unset authentication tacacsPolicy

show authentication tacacsPolicy

rm authentication tacacsPolicy

Synopsis

```
rm authentication tacacsPolicy <name>
```

Description

Remove a TACACS+ policy.

Arguments

name

The name of the TACACS+ policy to be removed.

Related Commands

add authentication tacacsPolicy
set authentication tacacsPolicy
unset authentication tacacsPolicy
show authentication tacacsPolicy

set authentication tacacsPolicy

Synopsis

```
set authentication tacacsPolicy <name> [-rule
<expression>] [-reqAction <string>]
```

Description

Change the properties of a TACACS+ policy.

Arguments

name

The name of the policy.

rule

The new rule to associate with the policy.

reqAction

The new TACACS+ action to associate to the policy.

Related Commands

add authentication tacacsPolicy

rm authentication tacacsPolicy

unset authentication tacacsPolicy

show authentication tacacsPolicy

unset authentication tacacsPolicy

Synopsis

```
unset authentication tacacsPolicy <name> [-rule] [-
reqAction]
```

Description

Use this command to remove authentication tacacsPolicy settings.Refer to the set authentication tacacsPolicy command for meanings of the arguments.

Related Commands

add authentication tacacsPolicy

rm authentication tacacsPolicy

set authentication tacacsPolicy

show authentication tacacsPolicy

show authentication tacacsPolicy

Synopsis

```
show authentication tacacsPolicy [<name>]
```

Description

Display the configured TACACS+ policies.

Arguments

name

The name of the TACACS+ policy. If no name is given, all of the configured TACACS+ policies are displayed.

summary

fullValues

format

level

Output

rule

reqAction

boundTo

The entity name to which policy is bound

Related Commands

add authentication tacacsPolicy

rm authentication tacacsPolicy

set authentication tacacsPolicy

unset authentication tacacsPolicy

add authentication nt4Policy

Synopsis

```
add authentication nt4Policy <name> <rule>
[<reqAction>]
```

Description

Add an authentication NT4 policy. The policy defines the conditions under which the specified NT4 server will be used for authentication.

Arguments

`name`
The name for the new NT4 policy.

`rule`
The name of the rule or expression the policy will use.

`reqAction`
The NT4 action the policy will use.

Related Commands

rm authentication nt4Policy
set authentication nt4Policy
unset authentication nt4Policy
show authentication nt4Policy

rm authentication nt4Policy

Synopsis

```
rm authentication nt4Policy <name>
```

Description

Remove an NT4 policy.

Arguments

name

The name of the NT4 policy to remove.

Related Commands

add authentication nt4Policy
set authentication nt4Policy
unset authentication nt4Policy
show authentication nt4Policy

set authentication nt4Policy

Synopsis

```
set authentication nt4Policy <name> [-rule
<expression>] [-reqAction <string>]
```

Description

Change the properties of an NT4 policy.

Arguments

name

The name of the NT4 policy.

rule

The name of the new rule to be associated with the policy.

reqAction

The name of the NT4 action to be associated with the policy.

Related Commands

add authentication nt4Policy

rm authentication nt4Policy

unset authentication nt4Policy

show authentication nt4Policy

unset authentication nt4Policy

Synopsis

```
unset authentication nt4Policy <name> [-rule] [-
reqAction]
```

Description

Use this command to remove authentication nt4Policy settings.Refer to the set authentication nt4Policy command for meanings of the arguments.

Related Commands

add authentication nt4Policy

rm authentication nt4Policy

set authentication nt4Policy

show authentication nt4Policy

show authentication nt4Policy

Synopsis

```
show authentication nt4Policy [<name>]
```

Description

Display NT4 policies.

Arguments

name

The name of the NT4 policy. If no name is given, all the configured NT4 policies will be displayed.

summary

fullValues

format

level

Output

rule

The name of the new rule associated with the policy.

reqAction

The name of the NT4 action associated with the policy.

boundTo

The entity name to which policy is bound

Related Commands

add authentication nt4Policy

rm authentication nt4Policy

set authentication nt4Policy

unset authentication nt4Policy

add authentication vserver

Synopsis

```
add authentication vserver <name> <serviceType>
(<IPAddress>  [-range <positive_integer>]) <port> [-
state ( ENABLED | DISABLED )] [-authentication ( ON |
OFF )] [-AuthenticationDomain <string>]
```

Description

Add an authentication virtual server.

Arguments

`name`

The name for the new authentication vserver.

`serviceType`

The authentication vserver's protocol type, e.g. SSL Possible values: SSL Default value: NSSVC_SSL

`IPAddress`

The IP address for the authentication vserver.

`port`

The TCP port on which the vserver listens. Minimum value: 1

`state`

The intital vserver server state, e.g. ENABLED or DISABLED Possible values: ENABLED, DISABLED Default value: ENABLED

`authentication`

Indicates whether or not authentication is being applied to incoming users to the vserver. Possible values: ON, OFF Default value: ON

`AuthenticationDomain`

Domain of authentication vserver FQDN Maximum value: 252

Example

The following example creates an authentication vserver named myauthenticationvip which supports SSL portocol and with AAA

functionality enabled: vserver myauthenticationvip SSL 65.219.17.34 443 -aaa ON

Related Commands

rm authentication vserver

set authentication vserver

unset authentication vserver

enable authentication vserver

disable authentication vserver

show authentication vserver

stat authentication vserver

rm authentication vserver

Synopsis

```
rm authentication vserver <name>@ ...
```

Description

Remove a virtual server.

Arguments

name

The name of the virtual server to be removed.

Example

rm vserver authn_vip

Related Commands

add authentication vserver
set authentication vserver
unset authentication vserver
enable authentication vserver
disable authentication vserver
show authentication vserver

stat authentication vserver

set authentication vserver

Synopsis

```
set authentication vserver <name> [-IPAddress
<ip_addr|ipv6_addr|*>] [-authentication ( ON | OFF )]
[-AuthenticationDomain <string>]
```

Description

Change the parameters of a authentication virtual server.

Arguments

name

The name of the vserver to be modified.

IPAddress

The new IP address of the virtual server.

authentication

Indicates whether authentication is ON/OFF on this vserver. Possible values: ON, OFF Default value: ON

AuthenticationDomain

Domain of authentication vserver FQDN Maximum value: 252

Related Commands

add authentication vserver

rm authentication vserver

unset authentication vserver

enable authentication vserver

disable authentication vserver

show authentication vserver

stat authentication vserver

unset authentication vserver

Synopsis

```
unset authentication vserver <name> [-
AuthenticationDomain] [-authentication]
```

Description

Unset the parameters of an authentication virtual server..Refer to the set authentication vserver command for meanings of the arguments.

Related Commands

add authentication vserver

rm authentication vserver

set authentication vserver

enable authentication vserver

disable authentication vserver

show authentication vserver

stat authentication vserver

bind authentication vserver

Synopsis

```
bind authentication vserver <name> [-policy <string>
[-priority <positive_integer>]  [-secondary]]
```

Description

Bind policies to a authentication vserver.

Arguments

name

The vserver to which this command shall bind parameters.

policy

The name of the policy to be bound to the vserver.

Related Commands

unbind authentication vserver

unbind authentication vserver

Synopsis

```
unbind authentication vserver <name> [-policy <string>
[-secondary]]
```

Description

Unbind policies from a authentication vserver.

Arguments

name

The name of the vserver from which an attribute is to be unbound.

policy

The name of the policy to be unbound.

Related Commands

bind authentication vserver

enable authentication vserver

Synopsis

enable authentication vserver <name>@

Description

Enable a virtual authentication server. Note:Virtual servers, when added, are enabled by default.

Arguments

name

The name of the virtual server to be enabled.

Example

enable vserver authentication1

Related Commands

add authentication vserver

rm authentication vserver

set authentication vserver

unset authentication vserver

disable authentication vserver

show authentication vserver

stat authentication vserver

disable authentication vserver

Synopsis

```
disable authentication vserver <name>@
```

Description

Disable (take out of service) a virtual server.

Arguments

name

The name of the virtual server to be disabled. Notes: 1.The system still responds to ARP and/or ping requests for the IP address of this virtual server. 2.As the virtual server is still configured in the system, you can enable the virtual server using ###enable vserver### command.

Example

disable vserver authn_vip

Related Commands

add authentication vserver

rm authentication vserver

set authentication vserver

unset authentication vserver

enable authentication vserver

show authentication vserver

stat authentication vserver

show authentication vserver

Synopsis

```
show authentication vserver [<name>] show
authentication vserver stats - alias for 'stat
authentication vserver'
```

Description

Display all of the configured Authentication virtual servers.

Arguments

`name`
The name of the authentication vserver.

`summary`

`fullValues`

`format`

`level`

Output

`IPAddress`
The Virtual IP address of the authentication vserver.

`IPAddress`
The IP address of the authentication server.

`value`
Indicates whether or not the certificate is bound or if SSL offload is disabled.

`port`
The virtual TCP port of the authentication vserver.

`range`
The range of authentication vserver IP addresses. The new range of authentication vservers will have IP addresses consecutively numbered, starting with the primary address specified with the <ipaddress> argument.

serviceType
The authentication vserver's protocol type, Currently the only possible value is SSL.

type
The type of Virtual Server, e.g. CONTENT based or ADDRESS based.

state
The current state of the Virtual server, e.g. UP, DOWN, BUSY, etc.

status
Whether or not this vserver responds to ARPs and whether or not round-robin selection is temporarily in effect.

cacheType
Virtual server's cache type. The options are: TRANSPARENT, REVERSE and FORWARD.

redirect
The cache redirect policy. The valid redirect policies are: l.CACHE - Directs all requests to the cache. 2.POLICY - Applies cache redirection policy to determine whether the request should be directed to the cache or origin. This is the default setting. 3.ORIGIN - Directs all requests to the origin server.

precedence
This argument is used only when configuring content switching on the specified virtual server. This is applicable only if both the URL and RULE-based policies have been configured on the same virtual server. It specifies the type of policy (URL or RULE) that takes precedence on the content switching virtual server. The default setting is RULE. lURL - In this case, the incoming request is matched against the URL-based policies before the rule-based policies. lRULE - In this case, the incoming request is matched against the rule-based policies before the URL-based policies. For all URL-based policies, the precedence hierarchy is: 1.Domain and exact URL 2.Domain, prefix and suffix 3.Domain and suffix 4.Domain and prefix 5.Domain only 6. Exact URL 7.Prefix and suffix 8.Suffix only 9.Prefix only 10.Default

redirectURL
The URL where traffic is redirected if the virtual server in system becomes unavailable. WARNING!Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the ###add cs policy### command. If the same domain is specified in both

arguments, the request will be continuously redirected to the same unavailable virtual server in the system. If so, the user may not get the requested content.

authentication
Indicates whether or not authentication is being applied to incoming users to the VPN.

curAAAUsers
The number of current users logged in to this vserver.

AuthenticationDomain
Domain of authentication vserver FQDN

rule
The name of the rule, or expression, if any, that policy for the authentication server is to use. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide. The default rule is ns_true.

policyName
The name of the policy, if any, bound to the authentication vserver.

serviceName
The name of the service, if any, to which the vserver policy is bound.

weight
Weight for this service, if any. This weight is used when the system performs load balancing, giving greater priority to a specific service. It is useful when the services bound to a virtual server are of different capacity.

cacheVserver
The name of the default target cache virtual server, if any, to which requests are redirected.

backupVServer
The name of the backup vpn virtual server for this vpn virtual server.

cltTimeout
The idle time, if any, in seconds after which the client connection is terminated.

soMethod
VPN client applications are allocated from a block of Intranet IP addresses. That block may be exhausted after a certain number of connections. This switch specifies the method used to determine whether or not a new connection will spillover, or exhaust, the allocated block of Intranet IP addresses for that application. Possible values are CONNECTION or DYNAMICCONNECTION. CONNECTION means that a static integer value is the hard limit for the spillover threshold. The spillover threshold is described below. DYNAMICCONNECTION means that the spillover threshold is set according to the maximum number of connections defined for the vpn vserver.

soThreshold
VPN client applications are allocated from a block of Intranet IP addresses. That block may be exhausted after a certain number of connections. The value of this option is number of client connections after which the Mapped IP address is used as the client source IP address instead of an address from the allocated block of Intranet IP addresses.

soPersistence
Whether or not cookie-based site persistance is enabled for this VPN vserver. Possible values are 'ConnectionProxy', HTTPRedirect, or NONE

soPersistenceTimeOut
The timeout, if any, for cookie-based site persistance of this VPN vserver.

priority
The priority, if any, of the vpn vserver policy.

downStateFlush
Perform delayed clean up of connections on this vserver.

disablePrimaryOnDown
Tells whether traffic will continue reaching backup vservers even after primary comes UP from DOWN state.

Example
show authentication vserver

Related Commands
add authentication vserver

rm authentication vserver

set authentication vserver
unset authentication vserver
enable authentication vserver
disable authentication vserver

stat authentication vserver

stat authentication vserver

Synopsis

```
stat authentication vserver [<name>] [-detail] [-
fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>]
```

Description

Display authentication vserver statistics.

Arguments

name

The name of the vserver for which statistics will be displayed. If not given statistics are shown for all authentication vservers.

Output

Counters

IP address (IP)

The ip address at which the service is running.

Port (port)

The port at which the service is running.

Vserver protocol (Protocol)

Protocol associated with the vserver

State

Current state of the server.

Requests (Req)

The total number of requests received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Responses (Rsp)

Number of responses received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Request bytes (Reqb)
The total number of request bytes received on this service/vserver.

Response bytes (Rspb)
Number of response bytes received on this service/vserver.

Related Commands

add authentication vserver
rm authentication vserver
set authentication vserver
unset authentication vserver
enable authentication vserver
disable authentication vserver
show authentication vserver

CHAPTER 7

Authorization Commands

This chapter covers the authorization commands.

add authorization policy

Synopsis

```
add authorization policy <name> <rule> <action>
```

Description

Add an authorization policy. Authorization policies allow AAA users and AAA groups to access resources through the SSL VPN. By default, the SSLVPN is configured to allow access to all resources. You can alter this default action by configuring authorization policies. (You can modify the default for a SSLVPN session with a vpn session policy. See "add vpn sessionpolicy"). You can selectively alter access to some resources to DENY by binding one or more authorization policies to the AAA user or AAA group. Once bound, an authorization policy acts on all incoming AAA user resource requests. If an authorization policy rule evaluates to TRUE, the specified action (ALLOW/DENY) is applied. If the rule evaluates to FALSE, the action is not applied. You can also bind multiple authorization policies to AAA users and AAA groups and give them different priorities. (See "bind aaa user/group".) Policies with different priorities are sorted in descending order. The following principles are applied when policies are evaluated: 1. DENY has the highest priority and takes effect immediately. 2. ALLOW has the next-highest priority. It waits for any other DENY policy in an authorization policy that has the same priority. 3. Implicit DENY has the third-highest priority. It waits for an explicit ALLOW/DENY of *any* priority. 4. Implicit ALLOW has the lowest priority. It waits for an explicit ALLOW/DENY with any priority and an Implict DENY with the same priority.

Arguments

`name`

The name for the new authorization policy.

`rule`

The rule or expression for conditional evaluation of the policy. This rule can be an expression specified by "add policy expression." or it may be an inline expression.

action
The action to be taken when the expression is satisfied. The allowed actions are ALLOW or DENY.

Example

Example: Consider the following authorization policy, "author-policy", add authorization policy author-policy "URL == /*.gif" DENY bind aaa user foo -policy author-policy If the user "foo" now logs in through the SSL VPN and makes any other request except "gif", the rule will be evaluated to FALSE, and the negetion of DENY, i.e. ALLOW, will be applied. So all those resource will implicitly be allowed to access. If "foo" tries to accesss "abc.gif" this access will be denied.

Related Commands

rm authorization policy

set authorization policy

unset authorization policy

show authorization policy

rm authorization policy

Synopsis

```
rm authorization policy <name>
```

Description

Remove a configured authorization policy.

Arguments

name

The name of the authorization policy to be removed.

Related Commands

add authorization policy

set authorization policy

unset authorization policy

show authorization policy

set authorization policy

Synopsis

```
set authorization policy <name> [-rule <expression>] [-
action <string>]
```

Description

Modify the rule or action value of a configured authorization policy.

Arguments

`name`

The name of the authorization policy to be modified.

`rule`

The new rule to be associated with the authorization policy.

`action`

The new action to be associated with the authorization policy.

Related Commands

add authorization policy

rm authorization policy

unset authorization policy

show authorization policy

unset authorization policy

Synopsis

```
unset authorization policy <name> [-rule] [-action]
```

Description

Use this command to remove authorization policy settings.Refer to the set authorization policy command for meanings of the arguments.

Related Commands

add authorization policy

rm authorization policy

set authorization policy

show authorization policy

show authorization policy

Synopsis

```
show authorization policy [<name>]
```

Description

Display all configured authorization policies.

Arguments

`name`
The name of the authorization policy.

`summary`

`fullValues`

`format`

`level`

Output

`rule`
Rule of the policy.

`action`
Authorization action associated with the policy. It can be either ALLOW or DENY.

`boundTo`
The entity name to which policy is bound

Related Commands

add authorization policy
rm authorization policy
set authorization policy
unset authorization policy

CHAPTER 8

Base Commands

This chapter covers the base commands.

restart dbsMonitors

Synopsis

```
restart dbsMonitors
```

Description

Use this command to clear/flush all learnt ip addresses for domain based servers

Example

restart dbsMonitors

Related Commands

clear locationData

Synopsis

```
clear locationData
```

Description

Clear all location information, including custom entries and static database entries.

Example

clear locationdata

Related Commands

stat serviceGroupMember

Synopsis

```
stat serviceGroupMember <serviceGroupName> <IP> <port>
[-detail] [-fullValues] [-ntimes <positive_integer>] [-
logFile <input_filename>]
```

Description

Display statistics of a service group member.

Arguments

serviceGroupName
The name of a service group

IP
The IP address of the member

port
The port number of the member

Output

Counters

Average server TTFB (SvrTTFB)
The average TTFB between the netscaler and the server.

IP address (IP)
The ip address at which the service is running.

Port (port)
The port at which the service is running.

Service type (Type)
The type of the service.

State
Current state of the server.

Requests (Req)
The total number of requests received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Responses (Rsp)
Number of responses received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Request bytes (Reqb)
The total number of request bytes received on this service/vserver.

Response bytes (Rspb)
Number of response bytes received on this service/vserver.

Current client connections (ClntConn)
The number of current client connections.

Requests in surge queue (SurgeQ)
The number requests in the surge queue.

Current server connections (SvrConn)
The number of current connections to the real servers behind the vserver.

Current Server Est connections (SvrEstConn)
The number of Server connections in established state.

Connections in reuse pool (ReuseP)
The number requests in the idle queue/ reuse pool.

Maximum server connections (MaxConn)
The maximum open connections allowed on this service.

Related Commands

stat service

stat serviceGroup

show configstatus

Synopsis

```
show configstatus
```

Description

Display status of packet engines.

Arguments

Output

`consistent`
State of packet engines.

`culpritCore`
Culprit core id.

`core`
Core id.

Example

show configstatus

Related Commands

add location

Synopsis

```
add location <IPfrom> <IPto> <preferredLocation>
```

Description

Add Custom Location entries in the system.

Arguments

`IPfrom`

The start of the IP address range in dotted notation.

`IPto`

The end of the IP address range in dotted notation.

`preferredLocation`

The qualifiers in dotted notation for the ipaddress range mentioned.

Example

Add location 192.168.100.1 192.168.100.100 *.us.ca.san jose

Related Commands

rm location

show location

rm location

Synopsis

```
rm location <IPfrom> <IPto>
```

Description

Remove a custom location entry configured in system

Arguments

IPfrom

The start of the IP address range in dotted notation.

IPto

The end of the IP address range in dotted notation.

Example

rm location 192.168.100.1 192.168.100.100

Related Commands

add location

show location

show location

Synopsis

```
show location [<IPfrom>]
```

Description

Display custom location entries configured in the system.

Arguments

IPfrom

The qualifiers in dotted notation for the ipaddress. If this value is not specified, all custom entries are displayed.

summary

fullValues

format

level

Output

IPto

The end of the IP address range.

preferredLocation

The qualifiers in dotted notation for the ipaddress range.

q1label

Least specific location qualifier.

q2label

Location qualifier 2.

q3label

Location qualifier 3.

q4label

Location qualifier 4.

`q5label`
Location qualifier 5.

`q6label`
Most specific location qualifier.

Example
show location

Related Commands
add location
rm location

set locationParameter

Synopsis

```
set locationParameter [-context ( geographic | custom
)] [-q1label <string>] [-q2label <string>] [-q3label
<string>] [-q4label <string>] [-q5label <string>] [-
q6label <string>]
```

Description

This command specifies the location parameters used for static proximity based load balancing.

Arguments

context

The context in which a static proximity decision has to be made. Possible values: geographic, custom

q1label

The label for the 1st qualifier. These qualifier labels specify the locations mapped with the IP addresses used to make static proximity decisions.

q2label

The label for the 2nd qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

q3label

The label for the 3rd qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

q4label

The label for the 4th qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

q5label

The label for the 5th qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

q6label

The label for the 6th qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

Example

set locationparameter -context custom

Related Commands

unset locationParameter

show locationParameter

unset locationParameter

Synopsis

```
unset locationParameter [-context] [-q1label] [-
q2label] [-q3label] [-q4label] [-q5label] [-q6label]
```

Description

Use this command to remove locationParameter settings.Refer to the set locationParameter command for meanings of the arguments.

Related Commands

set locationParameter

show locationParameter

show locationParameter

Synopsis

```
show locationParameter
```

Description

Display information about the context and qualifier labels used for static proximity based load balancing.

Arguments

`format`

`level`

Output

`context`
The context in which a static proximity decision must be made.

`q1label`
The label for the 1st qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

`q2label`
The label for the 2nd qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

`q3label`
The label for the 3rd qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

`q4label`
The label for the 4th qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

`q5label`
The label for the 5th qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

q6label
The label for the 6th qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

locationFile
Currently loaded location database file.

format

custom
Number of configured custom locations.

static
Number of configured locations in the database file (static locations).

flags
Information needed for display. This argument passes information from the kernel to the user space.

status
This argument displays when the status (success or failure) of database loading.

Example

show locationparameter

Related Commands

set locationParameter

unset locationParameter

add locationFile

Synopsis

```
add locationFile <locationFile> [-format <format>]
```

Description

load static database from the specified file into the system.

Arguments

locationFile

The name of the location file. The file name must include the full path. If the full path is not given, the default path /var/netscaler/locdb will be assumed. In high-availability mode, the static database should be stored in the same location on both systems.

format

The format of the location file. This optional argument is used to tell the system how to understand the file. The allowable values are: format = netscaler, ip-country, ip-country-isp, ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region, geoip-city, geoip-country-org, geoip-country-isp, geoip-city-isp-org . Possible values: netscaler, ip-country, ip-country-isp, ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region, geoip-city, geoip-country-org, geoip-country-isp, geoip-city-isp-org Default value: NSMAP_FORMAT_NETSCALER

Example

add locationfile /var/nsmap/locationdb -format netscaler

Related Commands

rm locationFile

show locationFile

rm locationFile

Synopsis

```
rm locationFile
```

Description

Remove the location file loaded into the system.

Example

rm locationfile

Related Commands

add locationFile

show locationFile

show locationFile

Synopsis

```
show locationFile
```

Description

Display the location file loaded in the system.

Arguments

format

level

Output

locationFile
The name of the location file.

format
The format of the location file.

Example

show locationfile

Related Commands

add locationFile
rm locationFile

add server

Synopsis

```
add server <name>@ (<IPAddress>@ | (<domain>@  [-
domainResolveRetry <integer>]  [-IPv6Address ( YES | NO
)]) | (-translationIp <ip_addr>  -translationMask
<netmask>)) [-state ( ENABLED | DISABLED )]
```

Description

Add a physical server to the system.

Arguments

name

The server's name.

IPAddress

The IP address of the server.

domain

The domain name of the server for which a service needs to be added. If an IP Address has been specified, the domain name does not need to be specified.

translationIp

The IP address used for translating dns obtained ip. Default value: 0

domainResolveRetry

The duration in seconds for which NetScaler system waits to send the next dns query to resolve the domain name, in case the last query failed. If last query succeeds, the netscaler system waits for TTL time in the response. Default value: 5 Minimum value: 5 Maximum value: 20940

state

The initial state of the service. Possible values: ENABLED, DISABLED Default value: ENABLED

IPv6Address

Defines whether server is of type ipv6 or not for DBS services Possible values: YES, NO Default value: NO

Related Commands

add service
rm server
set server
enable server
disable server
show server

rm server

Synopsis

```
rm server <name>@ ...
```

Description

Remove a server entry from the system.

Arguments

name

The name of the server.

Example

rm server web_svr

Related Commands

rm service

add server

set server

enable server

disable server

show server

set server

Synopsis

```
set server <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@ |
-domainResolveRetry <integer> | -translationIp
<ip_addr> | -translationMask <netmask> | -
domainResolveNow]
```

Description

Set server attributes.

Arguments

`name`
The name of the server.

`IPAddress`
The new IP address of the server.

`domainResolveRetry`
The duration in seconds for which NetScaler system waits to send the next dns query to resolve the domain name, in case the last query failed. If last query succeeds, the netscaler system waits for TTL time in the response. Default value: 5 Minimum value: 5 Maximum value: 20940

`translationIp`
The IP address used for translating dns obtained ip. Default value: 0

`translationMask`
The netmask of the translation ip Default value: 0

`domainResolveNow`
Restart the probe for this domain based server, immediately

Example

set server http_svr -IPAddress 10.102.1.112

Related Commands

add server

rm server
enable server
disable server
show server

enable server

Synopsis

```
enable server <name>@
```

Description

Enable all the services under the specified server. Note: A server is enabled by default when it is added to the system. When a server is disabled, all services under the server are disabled.

Arguments

name

The server name.

Related Commands

show service

enable service

add server

rm server

set server

disable server

show server

disable server

Synopsis

```
disable server <name>@ [<delay>]
```

Description

Disable all services (that have been configured in the system) for the specified server.

Arguments

name

The name of the server (created with the add server command) for which services will be disabled.

delay

The time in seconds after which all services in this server are brought down.

Example

disable server web_svr 30

Related Commands

add service

disable service

add server

rm server

set server

enable server

show server

show server

Synopsis

```
show server [<name> | -internal]
```

Description

View the attributes of a particular physical server.

Arguments

name

The name of the server. When a servername is specifed, all services under the server are displayed.

internal

Display internally created named servers. Default value: NSAPI_SERVERTYPE_INTERNAL

summary

fullValues

format

level

Output

IPAddress

The IP Address of server.

state

The State of the server.

domain

The domain name of the server.

domainResolveRetry

The duration in seconds for which NetScaler system waits to send the next dns query to resolve the domain name, in case the last query failed. If last query succeeds, the netscaler system waits for TTL time in the response.

serviceName
The services attatched to the server.

serviceGroupName
servicegroups bind to this server

translationIp
The IP address used for translating dns obtained ip.

translationMask
The netmask of the translation ip

Example

show server web_svr

Related Commands

show service
add server
rm server
set server
enable server
disable server

add service

Synopsis

```
add service <name>@ (<IP>@ | <serverName>@)
<serviceType> <port> [-clearTextPort <port>] [-
cacheType <cacheType>] [-maxClient <positive_integer>]
[-maxReq <positive_integer>] [-cacheable ( YES | NO )]
[-cip ( ENABLED | DISABLED )  [<cipHeader>]] [-usip (
YES | NO )] [-useproxyport ( YES | NO )] [-sc ( ON | OFF
)] [-sp ( ON | OFF )] [-rtspSessionidRemap ( ON | OFF
)] [-cltTimeout <secs>] [-svrTimeout <secs>] [-serverID
<positive_integer>] [-CKA ( YES | NO )] [-TCPB ( YES |
NO )] [-CMP ( YES | NO )] [-maxBandwidth
<positive_integer>] [-accessDown ( YES | NO )] [-
monThreshold <positive_integer>] [-state ( ENABLED |
DISABLED )] [-downStateFlush ( ENABLED | DISABLED )]
```

Description

Add a service to the system. Each server can have multiple services. To add multiple services, use this command for each service. Note:Each time you add a service, you must specify a unique port number for the service.

Arguments

name

The name of the service.

IP

The IP address of the server for which a service will be added.

serverName

The name of the server for which a service will be added.

serviceType

The type of service. The supported protocols are: HTTP - To load balance web servers and provide connection multiplexing, latency improvement, and other content and TCP protection benefits for HTTP traffic. FTP - To load

balance FTP servers. In FTP mode, the system provides TCP protection benefits, protection against SYN attacks, and surge protection. TCP - To host any other TCP protocols that are not HTTP, FTP, NNTP, or SSL. In TCP mode, the system provides TCP protection benefits, protection against SYN attack, and surge protection. UDP - To load balance servers with UDP-based services (other than DNS). SSL - To provide end-to-end encryption and SSL acceleration. SSL_BRIDGE - To load balance SSL servers. SSL_TCP - To offload SSL traffic for TCP applications. NNTP - To load balance NNTP servers. DNS - To load balance DNS servers. ADNS: To create an authoritative DNS service. ANY - To load balance a service type not listed above (for example, for IP traffic when load balancing firewalls). Note:The NNTP service is for cache redirection. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP

`port`
The port number to be used for the service.

`clearTextPort`
The clear text port number where clear text data is sent. Used with SSL offload service. Minimum value: 1

`cacheType`
The cache type option supported by the cache server. Possible values: TRANSPARENT, REVERSE, FORWARD

`maxClient`
The maximum number of open connections to the service. Default value: VAL_NOT_SET Maximum value: 0xFFFFFFFE

`maxReq`
The maximum number of requests that can be sent on a persistent connection to the service. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 65535

`cacheable`
The virtual server (used in load balancing or content switching) routes a request to the virtual server (used in transparent cache redirection) on the same system before sending it to the configured servers. The virtual server used for transparent cache redirection determines if the request is directed to the cache servers or configured servers. Note:This argument is disabled by

default. Do not specify this argument if a -cacheType cacheType is specified. Possible values: YES, NO Default value: NO

cip
The Client IP header insertion option for the service. Possible values: ENABLED, DISABLED Default value: VAL_NOT_SET

cipHeader
The client IP header. If client IP insertion is enabled and the client IP header is not specified, then the value set by the ###set ns config### command will be used as the Client IP header.

usip
The use of client's IP Address option to the source IP Address while connecting to this server. By default, the system uses a mapped IP address for its server connection; however, you can use this option to tell the system to use the client's IP address when it communicates with the server. Possible values: YES, NO Default value: VAL_NOT_SET

useproxyport
When USIP is enabled, based on the setting of this variable proxy port or the client port will be used as the source port for the backend connection. Possible values: YES, NO Default value: VAL_NOT_SET

sc
The state of SureConnect for the service. Note:This parameter is supported for legacy purposes only. It has no effect on this system, and its only valid value is OFF. Possible values: ON, OFF Default value: OFF

sp
The state of Surge protection for the the service. Possible values: ON, OFF Default value: VAL_NOT_SET

rtspSessionidRemap
Use this parameter to enable mapping of RTSP sessionid. Possible values: ON, OFF Default value: OFF

cltTimeout
The idle time (in seconds) after which the client connection is terminated. Default value: VAL_NOT_SET Maximum value: 31536000

svrTimeout
The idle time (in seconds) after which the server connection is terminated. Default value: VAL_NOT_SET Maximum value: 31536000

serverID
The identifier for the service. This is used when the persistency type is set to Custom Server ID. Minimum value: 0

CKA
The state of the Client Keep-Alive feature for the service. Possible values: YES, NO Default value: VAL_NOT_SET

TCPB
The state of the TCP Buffering feature for the service. Possible values: YES, NO Default value: VAL_NOT_SET

CMP
The state of the HTTP Compression feature for the service. Possible values: YES, NO Default value: VAL_NOT_SET

maxBandwidth
The maximum bandwidth in kbps allowed for the service. Maximum value: 0xFFFFFFF7

accessDown
The option to allow access to disabled or down services. If enabled, all packets to this service are bridged. If disabled, they are dropped. Possible values: YES, NO Default value: NO

monThreshold
The monitoring threshold. Default value: 0 Minimum value: 0 Maximum value: 65535

state
The state of the service after it is added. Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush
Perform delayed clean up of connections on this service. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add service http_svc 10.102.1.112 http 80

Related Commands

rm service
set service
unset service
bind service
unbind service
enable service
disable service
show service

stat service

rm service

Synopsis

```
rm service <name>@
```

Description

Remove a service from the system.

Arguments

name

The name of the service.

Example

rm service http_svc

Related Commands

add service
set service
unset service
bind service
unbind service
enable service
disable service
show service

stat service

set service

Synopsis

```
set service <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]
[-maxClient <positive_integer>] [-maxReq
<positive_integer>] [-cacheable ( YES | NO )] [-cip (
ENABLED | DISABLED )  [<cipHeader>]] [-usip ( YES | NO
)] [-useproxyport ( YES | NO )] [-sc ( ON | OFF )] [-sp
( ON | OFF )] [-rtspSessionidRemap ( ON | OFF )] [-
cltTimeout <secs>] [-svrTimeout <secs>] [-serverID
<positive_integer>] [-CKA ( YES | NO )] [-TCPB ( YES |
NO )] [-CMP ( YES | NO )] [-maxBandwidth
<positive_integer>] [-accessDown ( YES | NO )] [-
monThreshold <positive_integer>] [-weight
<positive_integer>  <monitorName>] [-downStateFlush (
ENABLED | DISABLED )]
```

Description

Use this command to modify the attributes of an existing service.

Arguments

name

The name of the service.

IPAddress

The new IP address of the service.

maxClient

The maximum number of open connections to the service. Maximum value: 0xFFFFFFFE

maxReq

The maximum number of requests that can be sent on a persistent connection to the service. Minimum value: 0 Maximum value: 65535

cacheable
The state of cache on the service. Possible values: YES, NO Default value: NO

cip
The Client IP header insertion option for the service. Possible values: ENABLED, DISABLED

usip
The usage of Client IP Address. Possible values: YES, NO

useproxyport
The usage of Client Port. Possible values: YES, NO

sc
The state of SureConnect for the service. Possible values: ON, OFF Default value: OFF

sp
The state of surge protection for the service. Possible values: ON, OFF

rtspSessionidRemap
Use this parameter to enable mapping of RTSP sessionid. Possible values: ON, OFF Default value: OFF

cltTimeout
The idle time in seconds after which the client connection is terminated. Maximum value: 31536000

svrTimeout
The idle time in seconds after which the server connection is terminated. Maximum value: 31536000

serverID
The identifier for the service. Used when the persistency type is set to Custom Server ID. Minimum value: 0

CKA
The state of the Client Keep-Alive feature for the service. Possible values: YES, NO

TCPB
The state of the TCP Buffering feature for this service. Possible values: YES, NO

CMP
The state of the HTTP Compression feature for this service. Possible values: YES, NO

maxBandwidth
The maximum bandwidth in kbps allowed for this service. Maximum value: 0xFFFFFFF7

accessDown
The option to allow access to disabled or down services. Possible values: YES, NO Default value: NO

monThreshold
The monitoring threshold. Minimum value: 0 Maximum value: 65535

weight
The weight for the specified monitor. Minimum value: 1 Maximum value: 100

downStateFlush
Perform delayed clean up of connections on this service. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set service http_svc -maxClient 100

Related Commands

add service
rm service
unset service
bind service
unbind service
enable service
disable service
show service

stat service

unset service

Synopsis

```
unset service <name>@ [-maxClient] [-maxReq] [-
cacheable] [-cip] [-usip] [-useproxyport] [-sc] [-sp]
[-rtspSessionidRemap] [-serverID] [-CKA] [-TCPB] [-CMP]
[-maxBandwidth] [-accessDown] [-monThreshold] [-
cltTimeout] [-svrTimeout] [-cipHeader] [-monitorName]
[-downStateFlush]
```

Description

Use this command to unset the attributes of an existing service..Refer to the set service command for meanings of the arguments.

Example

unset service http_svc -maxClient

Related Commands

add service
rm service
set service
bind service
unbind service
enable service
disable service
show service

stat service

bind service

Synopsis

```
bind service <name>@ -policyName <string>
```

Description

Use this command to bind a policy to a service. Notes: 1.This command does not support SureConnect policies. 2.This command only works for services that are not bound to virtual servers. If you attempt to bind a policy to a service that is already bound to a virtual server, the error message "Binding invalid policy" is displayed.

Arguments

`name`

The name of the service to which the policy will be bound.

`policyName`

The DoS protection policy name must be bound to the service. Also, for DoS protection to work on a service, an appropriate policy must be bound to the service.

Related Commands

add service

rm service

set service

unset service

unbind service

enable service

disable service

show service

stat service

unbind service

Synopsis

```
unbind service <name>@ -policyName <string>
```

Description

Unbind a policy from a service.

Arguments

name

The name of the service.

policyName

Name of the policy to be unbound.

Related Commands

add service

rm service

set service

unset service

bind service

enable service

disable service

show service

stat service

enable service

Synopsis

```
enable service <name>@
```

Description

Enable a service.

Arguments

name

The name of the service.

Example

enable service http_svc

Related Commands

enable vserver

add service

rm service

set service

unset service

bind service

unbind service

disable service

show service

stat service

disable service

Synopsis

```
disable service <name>@ [<delay>]
```

Description

Disable a service.

Arguments

name

The name of the service that needs to be disabled.

delay

The time allowed (in seconds) for a graceful shutdown. During this period, new connections and requests continue to be sent to the service for clients who already have persistent sessions on the system. Connections or requests from fresh or new clients who do not yet have a persistence sessions on the NetScaler system are not sent to the service. Instead, they are load balanced among other available services. After the delay time has passed, no new requests or connections are sent to the service.

Example

disable service http_svc 10

Related Commands

add service

rm service

set service

unset service

bind service

unbind service

enable service

show service

stat service

show service

Synopsis

show service [<name> | -all | -internal] show service bindings

Description

Display the services configured on the system. This command either lists all services or displays complete information about a particular service.

Arguments

name

The name of the service.

all

Display both configured and dynamically learned services. If you do not use this option, only the configured services are displayed. Default value: NSAPI_SVCTYPE_CONFIGURED|NSAPI_SVCTYPE_DYNAMIC|NSAPI_SVCTYPE_INTERNAL

internal

Display internally created named services. Default value: NSAPI_SVCTYPE_INTERNAL

summary

fullValues

format

level

Output

serverName

The name of the server for which a service has created.

serviceType

The type of service

serviceConfTpye
The configuration type of the serviceNOTE: This attribute is deprecated.This will no longer show the correct information. Use the serviceConfType option instead.

serviceConfType
The configuration type of the service

port
The port number to be used for the service.

value
SSL status.

clearTextPort
The clear-text port number where clear-text data is sent. Used with SSL offload service

gslb
The GSLB option for the corresponding virtual server.

cacheType
The cache type option supported by the cache server.

maxClient
The maximum number of open connections to the service.

maxReq
The maximum number of requests that can be sent on a persistent connection to the service.

cacheable

cip
The Client IP header insertion option for the service.

cipHeader
The client IP header.

usip
The use of client's IP Address option.

useproxyport
The use of client's Port.

sc
The state of SureConnect for the service.

weight
The weight of the monitor.

sp
The state of Surge protection for the the service.

rtspSessionidRemap
Use this parameter to enable mapping of RTSP sessionid.

failedprobes
Number of the current failed monitoring probes.

cltTimeout
The idle time in seconds after which the client connection is terminated.

totalprobes
The total number of probs sent.

svrTimeout
The idle time in seconds after which the server connection is terminated.

totalfailedprobes
The total number of failed probs.

publicIP
public ip

publicPort
public port

serverID
The identifier for the service. Used when the persistency type is set to Custom Server ID.

CKA
The state of the Client Keep-Alive feature for the service.

TCPB
The state of the TCP Buffering feature for the service.

CMP
The state of the HTTP Compression feature for the service.

maxBandwidth
The maximum bandwidth in kbps allowed for the service

accessDown
The option to allow access to disabled or down services. If enabled, all packets to the service are bridged; if disabled, they are dropped.

svrState
The state of the service

delay
The remaining time in seconds for the service to be disabled

IPAddress
The IP address of the server.

monitorName
The monitor Names.

monThreshold
The monitoring threshold.

monState
The configured state (enable/disable) of the monitor on this server.

monState
The running state of the monitor on this service.

monStatCode
The code indicating the monitor response.

responseTime
Response time of this monitor.

monStatParam1
First parameter for use with message code.

monStatParam2
Second parameter for use with message code.

monStatParam3
Third parameter for use with message code.

downStateFlush
Perform delayed clean up of connections on this service.

stateChangeTimeSec
Time when last state change happened. Seconds part.

stateChangeTimemSec
Time at which last state change happened. Milliseconds part.

timeSinceLastStateChange
Time in milliseconds since the last state change.NOTE: This attribute is deprecated.This will no longer show the correct information. Use the ticksSinceLastStateChange option instead.

ticksSinceLastStateChange
Time in 10 millisecond ticks since the last state change.

StateUpdateReason
Checks state update reason on the secondary node.

Example

The following is sample output of the show service -all command: 4 configured services: 1) svc1 (10.124.99.12:80) - HTTP State: UP Max Conn: 0 Max Req: 0 Use Source IP: NO Client Keepalive(CKA): NO TCP Buffering(TCPB): NO HTTP Compression(CMP): NO Idle timeout: Client: 180 sec Server: 360 sec Client IP: DISABLED 2) svc_3 (10.100.100.3:53) - DNS State: UP Max Conn: 0 Max Req: 0 Use Source IP: NO Client Keepalive(CKA): NO TCP Buffering(TCPB): NO HTTP Compression(CMP): NO Idle timeout: Client: 180 sec Server: 360 sec Client IP: DISABLED 3) tsvc1 (77.45.32.45:80) - HTTP State: UP Max Conn: 0 Max Req: 0 Use Source IP: NO Client Keepalive(CKA): NO TCP Buffering(TCPB): NO HTTP Compression(CMP): NO Idle timeout: Client: 180 sec Server: 360 sec Client IP: DISABLED 4) foosvc (10.124.99.13:7979) - HTTP State: UP Max Conn: 0 Max Req: 0 Use Source IP: NO Client Keepalive(CKA): NO TCP Buffering(TCPB): NO

HTTP Compression(CMP): NO Idle timeout: Client: 180 sec Server: 360 sec Client IP: DISABLED

Related Commands

add service
rm service
set service
unset service
bind service
unbind service
enable service
disable service

stat service

stat service

Synopsis

```
stat service [<name>] [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display statistics of a service.

Arguments

name

Name of the service

Output

Counters

Throughput (Mbps) (Throughput)

Number of bytes received/send on this service(Mbps).

Average server TTFB (SvrTTFB)

The average TTFB between the netscaler and the server.

IP address (IP)

The ip address at which the service is running.

Port (port)

The port at which the service is running.

Service type (Type)

The type of the service.

State

Current state of the server.

Requests (Req)

The total number of requests received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Responses (Rsp)
Number of responses received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Request bytes (Reqb)
The total number of request bytes received on this service/vserver.

Response bytes (Rspb)
Number of response bytes received on this service/vserver.

Current client connections (ClntConn)
The number of current client connections.

Requests in surge queue (SurgeQ)
The number requests in the surge queue.

Current server connections (SvrConn)
The number of current connections to the real servers behind the vserver.

Current Server Est connections (SvrEstConn)
The number of Server connections in established state.

Connections in reuse pool (ReuseP)
The number requests in the idle queue/ reuse pool.

Maximum server connections (MaxConn)
The maximum open connections allowed on this service.

Current load on the service (Load)
The load on the service that is calculated from bound load based monitor.

Current flags on the service (CurtFlags)
The current flags on the service for internal use in display handlers.

Service hits (Hits)
This represents the number of times that the service has been provided.

ActvTrans
The number of Active Transactions handled by this service(Includes the surgeQ count also).

Total Packets rcvd (PktRx)
The total number of packets received on this service/vserver.

Total Packets sent (PktTx)
The total number of packets sent.

Related Commands

add service
rm service
set service
unset service
bind service
unbind service
enable service
disable service
show service

stat serviceGroupMember
stat serviceGroup

add serviceGroup

Synopsis

```
add serviceGroup <serviceGroupName>@ <serviceType> [-
cacheType <cacheType>] [-maxClient <positive_integer>]
[-maxReq <positive_integer>] [-cacheable ( YES | NO )]
[-cip ( ENABLED | DISABLED )  [<cipHeader>]] [-usip (
YES | NO )] [-useproxyport ( YES | NO )] [-sc ( ON | OFF
)] [-sp ( ON | OFF )] [-rtspSessionidRemap ( ON | OFF
)] [-cltTimeout <secs>] [-svrTimeout <secs>] [-CKA (
YES | NO )] [-TCPB ( YES | NO )] [-CMP ( YES | NO )] [-
maxBandwidth <positive_integer>] [-monThreshold
<positive_integer>] [-state ( ENABLED | DISABLED )] [-
downStateFlush ( ENABLED | DISABLED )]
```

Description

Add a service group to the system.

Arguments

serviceGroupName

The name of the service group.

serviceType

The type of service group that is being added. Supported protocols are: HTTP - To load balance web servers and provide connection multiplexing, latency improvement, and other content and TCP protection benefits for HTTP traffic. FTP - To load balance FTP servers. In FTP mode, the NetScaler 9000 system provides TCP protection benefits, protection against SYN attacks, and surge protection. TCP - To host any other TCP protocols that are not HTTP, FTP, NNTP, or SSL. In TCP mode, the NetScaler 9000 system provides TCP protection benefits, protection against SYN attack, and surge protection UDP - To load balance servers with UDP-based service groups (other than DNS) SSL - To provide end-to-end encryption and SSL acceleration. SSL_BRIDGE - To load balance SSL servers. SSL_TCP - To offload SSL traffic for TCP applications. NNTP - To load balance NNTP servers. DNS - To load balance DNS servers. ANY - To load balance a service group type not listed above

(for example, for IP traffic when load balancing firewalls). Note:The NNTP service group is for cache redirection. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP

cacheType
The cache type option supported by the cache server. The options are: TRANSPARENT, REVERSE, and FORWARD. Possible values: TRANSPARENT, REVERSE, FORWARD

maxClient
The maximum number of open connections to each service in the service group. Default value: VAL_NOT_SET Maximum value: 0xFFFFFFFE

maxReq
The maximum number of requests that can be sent over a persistent connection to a service in the service group. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 65535

cacheable
Whether a virtual server (used in the NetScaler 9000 system's load balancing or content switching feature) routes a request to the virtual server (used in transparent cache redirection) on the same NetScaler 9000 system before sending it to the configured servers. The virtual server used for transparent cache redirection determines if the request is directed to the cache servers or configured servers. Note:Do not specify this argument if a cache type is specified. This argument is disabled by default. Possible values: YES, NO Default value: NO

cip
Enables or disables insertion of the Client IP header for services in the service group. Possible values: ENABLED, DISABLED Default value: VAL_NOT_SET

cipHeader
The client IP header. If client IP insertion is enabled and the client IP header is not specified, then the value set by the ###set ns config### command will be used as the Client IP header.

usip
Enables or disables use of client's IP Address as the source IP Address while connecting to the server. By default, the system uses a mapped IP address for

its server connection. However, with this option, you can tell the NetScaler 9000 system to use the client's IP address when it communicates with the server. Possible values: YES, NO Default value: VAL_NOT_SET

useproxyport
When USIP is enabled, based on the setting of this variable proxy port or the client port will be used as the source port for the backend connection. Possible values: YES, NO Default value: VAL_NOT_SET

sc
The state of SureConnect on this service group. Note:This parameter is supported for legacy purposes only; it has no effect, and the only valid value is OFF. Possible values: ON, OFF Default value: OFF

sp
Whether surge protection needs to be enabled on this service group. Possible values: ON, OFF Default value: OFF

rtspSessionidRemap
Use this parameter to enable mapping of RTSP sessionid. Possible values: ON, OFF Default value: OFF

cltTimeout
The idle time in seconds after which the client connection is terminated. Default value: VAL_NOT_SET Maximum value: 31536000

svrTimeout
The idle time in seconds after which the server connection is terminated. Default value: VAL_NOT_SET Maximum value: 31536000

CKA
The state of the Client Keep-Alive feature for the services in the service group. Possible values: YES, NO Default value: VAL_NOT_SET

TCPB
The state of the TCP Buffering feature for the services in the service group. Possible values: YES, NO Default value: VAL_NOT_SET

CMP
The state of the HTTP Compression feature for the services in the service group. Possible values: YES, NO Default value: VAL_NOT_SET

maxBandwidth
A positive integer that identifies the maximum bandwidth in kbps allowed for the services in the service group. Maximum value: 0xFFFFFFF7

monThreshold
The monitoring threshold. Default value: 0 Minimum value: 0 Maximum value: 65535

state
The state of the service group after it is added. Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush
Perform delayed clean up of connections on this service group. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add service group http_svc_group http

Related Commands

rm serviceGroup
set serviceGroup
unset serviceGroup
bind serviceGroup
unbind serviceGroup
enable serviceGroup
disable serviceGroup
show serviceGroup

stat serviceGroup

rm serviceGroup

Synopsis

```
rm serviceGroup <serviceGroupName>@
```

Description

Remove a service group.

Arguments

`serviceGroupName`

The name of the service group that will be removed.

Example

rm service group http_svc

Related Commands

add serviceGroup
set serviceGroup
unset serviceGroup
bind serviceGroup
unbind serviceGroup
enable serviceGroup
disable serviceGroup
show serviceGroup

stat serviceGroup

set serviceGroup

Synopsis

```
set serviceGroup <serviceGroupName>@ [(<serverName>@
<port>  [-weight <positive_integer>]  [-serverID
<positive_integer>]) | -maxClient <positive_integer> |
-maxReq <positive_integer> | -cacheable ( YES | NO ) |
-cip ( ENABLED | DISABLED ) | <cipHeader> | -usip ( YES
| NO ) | -sc ( ON | OFF ) | -sp ( ON | OFF ) | -
rtspSessionidRemap ( ON | OFF ) | -cltTimeout <secs> |
-svrTimeout <secs> | -CKA ( YES | NO ) | -TCPB ( YES |
NO ) | -CMP ( YES | NO ) | -maxBandwidth
<positive_integer> | -monThreshold <positive_integer> |
-downStateFlush ( ENABLED | DISABLED )] [-useproxyport
( YES | NO )]
```

Description

Modify the attributes of an existing service group.

Arguments

serviceGroupName

The name of the service group whose attributes will be changed.

serverName

The name of the server to be changed.

maxClient

The maximum number of open connections to each service in the service group. Maximum value: 0xFFFFFFFE

maxReq

The maximum number of requests that can be sent on a persistent connection to a service. Minimum value: 0 Maximum value: 65535

cacheable

The state of cache on the service group. Possible values: YES, NO Default value: NO

cip
The state of insertion of the Client IP header for a service. Possible values: ENABLED, DISABLED

usip
The usage of client's IP Address Possible values: YES, NO

useproxyport
When USIP is enabled, based on the setting of this variable proxy port or the client port will be used as the source port for the backend connection. Possible values: YES, NO

sc
Whether SureConnect will be enabled on this service. Possible values: ON, OFF Default value: OFF

sp
The state of surge protection on this service group. Possible values: ON, OFF Default value: OFF

rtspSessionidRemap
Use this parameter to enable mapping of RTSP sessionid. Possible values: ON, OFF Default value: OFF

cltTimeout
The idle time (in seconds) after which the client connection is terminated. Maximum value: 31536000

svrTimeout
The idle time in seconds after which the server connection is terminated. Maximum value: 31536000

CKA
The state of the Client Keep-Alive feature for the service. Possible values: YES, NO

TCPB
The state of the TCP Buffering feature for this service. Possible values: YES, NO

CMP
The state of the HTTP Compression feature for this service. Possible values: YES, NO

maxBandwidth
A positive integer that identifies the maximum bandwidth in kbps allowed for this service. Maximum value: 0xFFFFFFF7

monThreshold
The monitoring threshold. Minimum value: 0 Maximum value: 65535

downStateFlush
Perform delayed cleanup of connections on this service group. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set servicegroup http_svc -maxClient 100

Related Commands

add serviceGroup
rm serviceGroup
unset serviceGroup
bind serviceGroup
unbind serviceGroup
enable serviceGroup
disable serviceGroup
show serviceGroup

stat serviceGroup

unset serviceGroup

Synopsis

unset serviceGroup <serviceGroupName>@ [-serverName] [-port] [-weight] [-serverID] [-maxClient] [-maxReq] [-cacheable] [-cip] [-cipHeader] [-usip] [-useproxyport] [-sc] [-sp] [-rtspSessionidRemap] [-cltTimeout] [-svrTimeout] [-CKA] [-TCPB] [-CMP] [-maxBandwidth] [-monThreshold] [-downStateFlush]

Description

Use this command to remove serviceGroup settings.Refer to the set serviceGroup command for meanings of the arguments.

Related Commands

add serviceGroup
rm serviceGroup
set serviceGroup
bind serviceGroup
unbind serviceGroup
enable serviceGroup
disable serviceGroup
show serviceGroup

stat serviceGroup

bind serviceGroup

Synopsis

```
bind serviceGroup <serviceGroupName> (<IP>@ |
<serverName>@) <port> [-weight <positive_integer>] [-
serverID <positive_integer>] [-state ( ENABLED |
DISABLED )]
```

Description

Bind a service to a service group.

Arguments

serviceGroupName

The name of the service group to which the service will be bound.

IP

The IP address of a member to be added.

Related Commands

add serviceGroup
rm serviceGroup
set serviceGroup
unset serviceGroup
unbind serviceGroup
enable serviceGroup
disable serviceGroup
show serviceGroup

stat serviceGroup

unbind serviceGroup

Synopsis

```
unbind serviceGroup <serviceGroupName> (<IP>@ |
<serverName>@) <port>
```

Description

Unbind a service from a service group.

Arguments

serviceGroupName

The name of the service group.

IP

The IP address of a member to be removed.

Related Commands

add serviceGroup
rm serviceGroup
set serviceGroup
unset serviceGroup
bind serviceGroup
enable serviceGroup
disable serviceGroup
show serviceGroup

stat serviceGroup

enable serviceGroup

Synopsis

```
enable serviceGroup <serviceGroupName>@ [<serverName>@
<port>]
```

Description

Use this command to enable a service group.

Arguments

serviceGroupName

The name of the service group to be enabled.

serverName

The name of the server that hosts the member to be enabled from the service group.

port

The port number of the service to be enabled.

Example

enable servicegroup http_svc

Related Commands

enable service

add serviceGroup

rm serviceGroup

set serviceGroup

unset serviceGroup

bind serviceGroup

unbind serviceGroup

disable serviceGroup

show serviceGroup

stat serviceGroup

disable serviceGroup

Synopsis

```
disable serviceGroup <serviceGroupName>@
[<serverName>@  <port>] [-delay <secs>]
```

Description

Use this command to disable a service group.

Arguments

`serviceGroupName`

The name of the service group that needs to be disabled.

`serverName`

The name of the server that hosts the member to be disabled from the service group.

`port`

The port number of the service to be disabled.

`delay`

The time allowed (in seconds) for a graceful shutdown. During this period, new connections or requests will continue to be sent to this service for clients who already have a persistent session on the system. Connections or requests from fresh or new clients who do not yet have a persistence sessions on the system will not be sent to the service. Instead, they will be load balanced among other available services. After the delay time expires, no new requests or connections will be sent to the service.

Example

disable service group http_svc 10

Related Commands

add serviceGroup

rm serviceGroup

set serviceGroup

unset serviceGroup

bind serviceGroup
unbind serviceGroup
enable serviceGroup
show serviceGroup

stat serviceGroup

show serviceGroup

Synopsis

```
show serviceGroup [<serviceGroupName> | -
includeMembers]
```

Description

Display the configured service groups. This command either lists all service groups or displays complete information about a particular service group.

Arguments

serviceGroupName

The name of the service group.

includeMembers

Include a summary of the members in a group too. Default value: NSAPI_SVCTYPE_SVCGRPMEM

summary

fullValues

format

level

Output

serviceType

port

serviceConfTpye

NOTE: This attribute is deprecated.This will no longer show the correct information. Use the serviceConfType option instead.

serviceConfType

The configuration type of the service group.

value
SSL Status.

cacheType

maxClient

maxReq

cacheable
The state of cache on the service.

cip

cipHeader
CIP Header.

usip

useproxyport
The use of client's Port.

sc
Whether SureConnect is enabled on this service or not.

sp

rtspSessionidRemap
Use this parameter to enable mapping of RTSP sessionid.

cltTimeout

svrTimeout

CKA

TCPB

CMP

maxBandwidth

state
The state of the service group

svrState
The state of the service

delay
The remaining time in seconds for the service to be disabled

IPAddress
IP Address.

serverName

monitorName
Monitor name.

monThreshold

monState
Monitor state.

weight

serverID
The identifier for this IP:Port pair. Used when the persistency type is set to Custom Server ID.

monState
The running state of the monitor on this service.

monStatCode
The code indicating the monitor response.

monStatParam1
First parameter for use with message code.

monStatParam2
Second parameter for use with message code.

monStatParam3
Third parameter for use with message code.

downStateFlush
Perform delayed cleanup of connections on this vserver.

stateChangeTimeSec
Time when last state change occurred. Seconds part.

stateChangeTimemSec
Time when last state change occurred. Milliseconds part.

timeSinceLastStateChange
Time in milliseconds since the last state change.NOTE: This attribute is deprecated.This will no longer show the correct information. Use the ticksSinceLastStateChange option instead.

ticksSinceLastStateChange
Time in 10 millisecond ticks since the last state change.

StateUpdateReason
Checks state update reason on the secondary node.

groupCount
Servicegroup Count

Related Commands

add serviceGroup
rm serviceGroup
set serviceGroup
unset serviceGroup
bind serviceGroup
unbind serviceGroup

enable serviceGroup
disable serviceGroup

stat serviceGroup

stat serviceGroup

Synopsis

```
stat serviceGroup [<serviceGroupName>] [-detail] [-
fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>]
```

Description

Display statistics of service group(s).

Arguments

serviceGroupName

The name of a service group

Output

Counters

State

Current state of the server.

Service type (Type)

The type of the service.

Related Commands

add serviceGroup
rm serviceGroup
set serviceGroup
unset serviceGroup
bind serviceGroup
unbind serviceGroup
enable serviceGroup
disable serviceGroup
show serviceGroup

stat serviceGroupMember

stat service

rm vserver

Synopsis

```
rm vserver <name>@ ...
```

Description

Use this command to remove a virtual server.

Arguments

name

The name of the virtual server to be removed.

Example

rm vserver lb_vip

Related Commands

set vserver

unset vserver

enable vserver

disable vserver

show vserver

set vserver

Synopsis

```
set vserver <name>@ [-backupVServer <string>] [-
pushVserver <string>]
```

Description

Use this command to modify the parameters for an existing virtual server.

Arguments

name

The name of the virtual server for which the parameters are to be set.

backupVServer

The name of the backup virtual server for this virtual server.

redirectURL

The URL where traffic is redirected if the virtual server in the system becomes unavailable.

cacheable

Use this option to specify whether a virtual server (used for load balancing or content switching) routes requests to the cache redirection virtual server before sending it to the configured servers. Possible values: YES, NO

cltTimeout

The timeout value in seconds for idle client connection Maximum value: 31536000

soMethod

The spillover factor. The system will use this value to determine if it should send traffic to the backupvserver when the main virtual server reaches the spillover threshold. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

The state of the spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut

The spillover persistence entry timeout. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold

The spillver threshold value. Minimum value: 1 Maximum value: 0xFFFFFFFE

pushVserver

The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

Example

set vserver lb_vip -backupVServerName bkvip_lbvip

Related Commands

rm vserver

unset vserver

enable vserver

disable vserver

show vserver

unset vserver

Synopsis

Description

Use this command to unset the backup virtual server or the redirectURL that has been set on the virtual server..Refer to the set vserver command for meanings of the arguments.NOTE: This command is deprecated.

Example

unset vserver lb_vip -backupVServer

Related Commands

rm vserver

set vserver

enable vserver

disable vserver

show vserver

enable vserver

Synopsis

```
enable vserver <name>@
```

Description

Use this command to enable a virtual server. Note:Virtual servers, when added, are enabled by default.

Arguments

name

The name of the virtual server to be enabled.

Example

enable vserver lb_vip

Related Commands

rm vserver

set vserver

unset vserver

disable vserver

show vserver

disable vserver

Synopsis

```
disable vserver <name>@
```

Description

Use this command to disable (take out of service) a virtual server.

Arguments

name

The name of the virtual server to be disabled. Notes: 1.The system will continue to respond to ARP and/or ping requests for the IP address of this virtual server. 2.As the virtual server is still configured in the system, you can enable the virtual server using the ###enable vserver### command.

Example

disable vserver lb_vip

Related Commands

rm vserver

set vserver

unset vserver

enable vserver

show vserver

show vserver

Synopsis

```
show vserver [<name>]
```

Description

Use this command to display all virtual servers configured on the NetScaler system. The information displayed includes the virtual server name, IP address, port number, service type, virtual server state (enabled or disabled), and virtual server type. For virtual servers used with the system's load balancing feature, the command also displays the load balancing policy, the persistence type, the persistence timeout value, and the name of the backup virtual server. For virtual servers used in content switching, the command also displays the name of the default policy.

Arguments

name

The name of the virtual server (created with the add vserver command) for which the details will be displayed.

summary

fullValues

format

level

Output

insertVserverIPPort

The virtual IP and port header insertion option for the vserver.

vipHeader

The name of the virtual IP and port header.

IPAddress

IPAddress
The IP address of the virtual server.

port

range

IPv6Address

IPPattern
The IP pattern of the virtual server.

IPMask
The IP address mask of the virtual server.

serviceType

value

type

state

effectiveState

status

cacheType

redirect

precedence

redirectURL

authentication

homePage

dnsVserverName

domain

rule

policyName

hits

serviceName

weight

cacheVserver

backupVServer

priority

cltTimeout

soMethod

soPersistence
spill over persistence

soPersistenceTimeOut
spill over persistence timeout

soThreshold
spill over persistence threshold

lbMethod
lb method

hashLength
max hash length

dataOffset
data offset

dataLength
data length

netmask
hash netmask

groupName
group name

m
lb mode

tosId
TOS ID

persistenceType

cookieDomain
domain name

persistMask
persistence mask

persistenceBackup
backup persistence type

timeout
timeout

cacheable
cacheablity

pq
number

sc
The state of SureConnect on this vserver.

sessionless
sessionless lb

url
URL for probe

reuse
wtm

destinationVServer
destination vserver

via
via

flags
vserver flags

connfailover
connection failover

caseSensitive
persistence type

map
map

redirectPortRewrite
port rewrite for ssl

downStateFlush
Perform delayed clean up of connections on this vserver.

cookieIpPort
Encryped Ip address and port of the service that is inserted into the set-cookie http header

vserverId
Vserver Id

version
Cookie version

totalServices
Total number of services bound to the vserver.

activeServices
Total number of active services bound to the vserver.

Example

show vserver lb_vip

Related Commands

rm vserver

set vserver

unset vserver

enable vserver

disable vserver

set uiinternal

Synopsis

set uiinternal <entityType> <name> [-template <string>] [-comment <string>] [-rule <string>]

Description

set uiinternal data for the entities

Arguments

entityType

The entitiy type of UI internal data Possible values: LBVSERVER, GSLBVSERVER, CRVSERVER, VPNVSERVER, CSVSERVER, AUTHENTICATIONVSERVER, SERVER, SERVICE, SERVICEGROUP, GSLBSERVICE, EXPRESSION, VPNURL

name

The entity name

template

The application template associated with entity

comment

The application template associated with entity

rule

rules associated with entity

Example

set uiinternal lbvserver v1 -template app1

Related Commands

unset uiinternal

show uiinternal

unset uiinternal

Synopsis

```
unset uiinternal <entityType> <name> [-template] [-
comment] [-rule] [-all]
```

Description

unset uiinternal for the entities.Refer to the set uiinternal command for meanings of the arguments.

Example

unset uiinternal lbvserver v1 -template app1

Related Commands

set uiinternal

show uiinternal

show uiinternal

Synopsis

```
show uiinternal [<entityType>] [<name>]
```

Description

display all UI internal data information for the entities

Arguments

entityType

The entitiy type of UI internal data Possible values: LBVSERVER, GSLBVSERVER, CRVSERVER, VPNVSERVER, CSVSERVER, AUTHENTICATIONVSERVER, SERVER, SERVICE, SERVICEGROUP, GSLBSERVICE, EXPRESSION, VPNURL

name

The entity name

summary

fullValues

format

level

Output

template

The template associated with the entity

comment

The comment associated with the entity

uiinfo

The uiinfo associated with the entity

rule

The rule associated with the entity

Example

show uiinternal LBVSERVER v1

Related Commands

set uiinternal

unset uiinternal

CHAPTER 9

Integrated Caching Commands

This chapter covers the integrated caching commands.

show cache object

Synopsis

```
show cache object [(-url <URL>  (-host <string>  [-port
<port>]  [-groupName <string>]  [-httpMethod ( GET |
POST )])) | -locator <positive_integer> | -group
<string> | -ignoreMarkerObjects ( ON | OFF ) | -
includeNotReadyObjects ( ON | OFF )]
```

Description

Show a list of all cached objects, or the properties of a particular cache object.

Arguments

`url`
The URL of the object.

`locator`
The id of the cached object.

`host`
The hostname of the object.

`port`
The host port of the object. Default value: 80 Minimum value: 1

`groupName`
The name of the content group to be in which the cell is present

`httpMethod`
The HTTP request method that caused the object to be stored. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

`group`
The name of the content group whose objects should be listed.

`ignoreMarkerObjects`
Ignore marker objects Possible values: ON, OFF

includeNotReadyObjects
Include objects not-ready for a cache hit Possible values: ON, OFF

Output

cacheResSize
Cache response size of the object.

cacheResHdrSize
Cache response header size of the object.

httpStatus
HTTP status of the object.

cacheETag
Cache ETag of the object.

cacheResLastMod
Value of "Last-modified" header.

cacheControl
Cache-Control header of the object.

cacheResDate
Value of "Date" header

contentGroup
Name of the contentgroup in which it is stored.

destIP
Destination IP.

destPort
Destination Port.

cacheCellComplex
The state of the parameterized caching on this cell.

hitParams
Parameterized hit evaluation of an object.

hitValues
Values of hitparams for this object.

cacheCellReqTime
Required time of the cache cell object.

cacheCellResTime
Response time to the cache cell object.

cacheCurAge
Current age of the cache object.

cacheCellExpires
Expiry time of the cache cell object in seconds.

cacheCellExpiresMilliSec
Expiry time of the cache cell object in milliseconds.

flushed
Specifies whether the object is flushed.

prefetch
Specifies whether Integrated Cache should attempt to refresh an object immediately before it goes stale.

prefetchPeriod
The duration in seconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time.

prefetchPeriodMilliSec
The duration in milliseconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time.

cacheCellCurReaders
Current readers of the cache cell object.

cacheCellCurMisses
Current misses of the cache cell object.

cacheCellHits
Cache cell hits.

cacheCellMisses
Cache cell misses.

cacheCellGzipCompressed
The state of the response being gzip-compressed.NOTE: This attribute is deprecated.we display compression format using nsace_contenc_name

cacheCellDeflateCompressed
The state of the response being deflate-compressed.NOTE: This attribute is deprecated.we display compression format using nsace_contenc_name

cacheCellCompressionFormat
Compression format of this object. Identity means not compressed

cacheCellAppFWMetadataExists
AppFirewall cache object.

cacheCellHttp11
The state of the response to be HTTP/1.1.

cacheCellWeakEtag
The state of the weak HTTP Entity Tag in the cell.

cacheCellResBadSize
The marked state of the cell.

markerReason
Reason for marking the cell.

cacheCellPollEveryTime
The state to poll every time on object.

cacheCellEtagInserted
The state of the ETag to be inserted by IC for this object.

cacheCellReadyWithLastByte
The state of the complete arrived response.

cacheCellDestipVerified
The state of DNS verification.

cacheCellFwpxyObj
The state of the object to be stored on a request to a forward proxy.

cacheCellBasefile
The state of delta being used as a basefile.

cacheCellMinHitFlag
The state of the minhit feature on this cell.

cacheCellMinHit
Min hit value for the object.

policy
Policy info for the object.

policyName
Policy which created the object.

selectorName
The hit selector for the object.

rule
Selectors for this object.

selectorValue
The HTTP request method that caused the object to be stored.

cacheUrls
List of cache object URLs.

warnBucketSkip
Bucket skipped warning.

totalObjs
Total objects.

httpCalloutCell
Is it a http callout cell ?

httpCalloutName
Name of the http callout

returnType
Return type of the http callout

httpCalloutResult
First few bytes of http callout response

Related Commands

expire cache object

flush cache object

expire cache object

Synopsis

```
expire cache object (-locator <positive_integer> | (-
url <URL>  (-host <string>  [-port <port>]  [-groupName
<string>]  [-httpMethod ( GET | POST )])))
```

Description

Expire a cached object.

Arguments

locator

The id of the cached object.

url

The URL of the object to be expired.

host

The host of the object to be expired.

port

The host port of the object to be expired. Default value: 80 Minimum value: 1

groupName

The name of the content group to be in which the cell is present.

httpMethod

The HTTP request method that caused the object to be stored. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

Related Commands

show cache object

flush cache object

flush cache object

Synopsis

```
flush cache object (-locator <positive_integer> | (-url
<URL>  (-host <string>  [-port <port>]  [-groupName
<string>]  [-httpMethod ( GET | POST )])))
```

Description

Flush a cached object.

Arguments

`locator`
The ID of the cached object.

`url`
The URL of the object to be flushed.

`host`
The host of the object to be flushed.

`port`
The host port of the object to be flushed. Default value: 80 Minimum value: 1

`groupName`
The name of the content group to be in which the cell is present.

`httpMethod`
The HTTP request method that caused the object to be stored. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

Related Commands

show cache object

expire cache object

show cache stats

Synopsis

```
show cache stats - alias for 'stat cache'
```

Description

show cache stats is an alias for stat cache

Related Commands

stat cache

stat cache

Synopsis

```
stat cache [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display the Integrated Cache statistics.

Arguments

Output

Counters

Recent successful reval ratio(%) (RPSucRev)
Recently recorded percentage of times stored content was successfully revalidated by a 304 response rather than by a full response

Recent storable miss ratio(%) (RPctStMis)
Recently recorded ratio of store-able misses to all misses expressed as percentage.

Recent parameterized 304 hit ratio(%) (RPPHit)
Recently recorded ratio of parameterized 304 hits to all parameterized hits expressed as a percentage

Recent origin bandwidth saved(%) (RPOrBan)
Bytes served from cache divided by total bytes served to client. This ratio can be greater than 1 because of the assumption that all compression has been done in the NetScaler.

Recent hit ratio(%) (RPctHit)
Recently recorded cache hit ratio expressed as percentage

Recent byte hit ratio(%) (RPcByHit)
Recently recorded cache byte hit ratio expressed as percentage. Here we define byte hit ratio as ((number of bytes served from the cache)/(total number of bytes served to the client)). This is the standard definition of Byte Hit Ratio. If compression is turned ON in NS then this ratio doesn't mean

much. This might under or over estimate the origin-to-cache bandwidth saving (depending upon whether bytes served by CMP in NetScaler are more or less than compressed bytes served from the cache). If CMP is turned OFF in NS then this ratio is same as cacheRecentPercentOriginBandwidthSaved.

Recent 304 hit ratio(%) (RPct304Hit)
Recently recorded ratio of 304 hits to all hits expressed as percentage

Utilized memory(KB) (UtiMem)
Amount of memory the integrated cache is currently using.

Maximum memory(KB) (MaxMem)
Largest amount of memory the NetScaler can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the caching module continues to run.

Poll every time hit ratio(%) (PPeHit)
Percentage of cache hits in content groups that have Poll Every Time enabled, relative to all searches of content groups with Poll Every Time enabled.

Poll every time hits (PeHit)
Number of times a cache hit was found during a search of a content group that has Poll Every Time enabled.

Parameterized 304 hit ratio(%) (PP304Hit)
Percentage of parameterized 304 hits relative to all parameterized hits.

Total parameterized hits (PHit)
Parameterized requests resulting in either a 304 or non-304 hit.

Successful reval ratio(%) (PSucRev)
Percentage of times stored content was successfully revalidated by a 304 (Object Not Modifed) response rather than by a full response

Storable miss ratio(%) (PStrMiss)
Responses that were fetched from the origin, stored in the cache, and then served to the client, as a percentage of all cache misses.

Conversions to conditional req (FuToCon)
Number of user-agent requests for a cached Poll Every Time (PET) response that were sent to the origin server as conditional requests.

Successful revalidations (TSucRev)
Total number of times stored content was successfully revalidated by a 304 Not Modified response from the origin.

Revalidations (Reval)
Responses that an intervening cache revalidated with the integrated cache before serving, as determined by a Cache-Control: Max-Age header configurable in the integrated cache

Non-storable misses (NStrMiss)
Cache misses for which the fetched response is not stored in the cache. These responses match policies with a NOCACHE action or are affected by Poll Every Time.

Storable misses (StrMiss)
Cache misses for which the fetched response is stored in the cache before serving it to the client. Storable misses conform to a built-in or user-defined caching policy that contains a CACHE action.

Compressed bytes from cache (CmpBySer)
Number of compressed bytes served from the cache

Byte hit ratio(%) (PByHit)
Bytes served from the cache divided by total bytes served to the client. If compression is On in the NetScaler, this ratio may not reflect the bytes served by the compression module. If the compression is Off, this ratio is the same as cachePercentOriginBandwidthSaved.

Bytes served by cache (BySer)
Total number of bytes served from the integrated cache

Bytes served by NetScaler (RespBy)
Total number of HTTP response bytes served by NetScaler from both the origin and the cache

304 hit ratio(%) (Pct304Hit)
304 responses as a percentage of all responses that the NetScaler served.

Marker objects (NumMark)
Marker objects created when a response exceeds the maximum or minimum size for entries in its content group or has not yet received the minimum number of hits required for items in its content group.

Origin bandwidth saved(%) (POrBan)
Percentage of origin bandwidth saved, expressed as number of bytes served from the integrated cache divided by all bytes served. The assumption is that all compression is done in the NetScaler.

Hit ratio(%) (PctHit)
Cache hits as percentage of the total number of requests

Misses (TotMiss)
Intercepted HTTP requests requiring fetches from origin server.

Hits (TotHit)
Responses served from the integrated cache. These responses match a policy with a CACHE action.

Requests (CacReq)
Total cache hits plus total cache misses.

Cached objects (NumCac)
Responses currently in integrated cache. Includes responses fully downloaded, in the process of being downloaded, and expired or flushed but not yet removed.

Hits being served (CacHit)
This number should be close to the number of hits being served currently.

Misses being handled (CurMiss)
Responses fetched from the origin and served from the cache. Should approximate storable misses. Does not include non-storable misses.

Non-304 hits (Non304Hit)
Total number of full (non-304) responses served from the cache. A 304 status code indicates that a response has not been modified since the last time it was served

304 hits (304Hit)
Object not modified responses served from the cache. (Status code 304 served instead of the full response.)

Expire at last byte (ExpLa)
Instances of content expiring immediately after receiving the last body byte due to the Expire at Last Byte setting for the content group.

Flashcache misses (FlMi)
Number of requests to a content group with flash cache enabled that were cache misses. Flash cache distributes the response to all the clients in aqueue.

Flashcache hits (FlHi)
Number of requests to a content group with flash cache enabled that were cache hits. The flash cache setting queues requests that arrive simultaneously and distributes the response to all the clients in the queue.

Parameterized inval requests (PInReq)
Requests matching a policy with an invalidation (INVAL) action and a content group that uses an invalidation selector or parameters.

Full inval requests (NPInReq)
Requests that match an invalidation policy where the invalGroups parameter is configured and expires one or more content groups.

Inval requests (INStrMis)
Requests that match an invalidation policy and result in expiration of specific cached responses or entire content groups.

Parameterized requests (PReq)
Total number of requests where the content group has hit and invalidation parameters or selectors.

Parameterized non-304 hits (PN304Hit)
Parameterized requests resulting in a full response (not status code 304: Object Not Updated) served from the cache.

Parameterized 304 hits (P304Hit)
Parameterized requests resulting in an object not modified (status code 304) response.

Poll every time requests (PeReq)
Requests that triggered a search of a content group that has Poll Every Time (PET) enabled (always consult the origin server before serving cached data).

Memory allocation failures (ErrMem)
Total number of times the cache failed to allocate memory to store responses.

Largest response so far(B) (LarResp)
Size, in bytes, of largest response sent to client from the cache or the origin server.

Compressed bytes transmitted
Number of bytes the NetScaler sends to the client after compressing the response from the server.

Compressible bytes received
Number of bytes that can be compressed, which the NetScaler receives from the server. This gives the content length of the response that the NetScaler receives from server.

Response bytes received (HTRspbRx)
Bytes received as response data.

Related Commands

add cache policy

Synopsis

```
add cache policy <policyName> -rule <expression> -
action <action> [-storeInGroup <string>] [-invalGroups
<string> ...] [-invalObjects <string> ...] [-
undefAction ( NOCACHE | RESET )]
```

Description

Create Integrated Cache policies. The newly created policy is in the inactive state. To activate the policy, use the ###bind cache global### command. The type of the policy depends on whether it is a request policy or a response policy, and the type of the specified action, as follows: CACHE or MAY_CACHE action: positive cachability policy NOCACHE or MAY_NOCACHE action: negative cachability policy INVAL action: Dynamic Invalidation Policy The order in which the policies are configured is significant. For a detailed discussion of the significance of the order, see the System Installation and Configuration Guide.

Arguments

policyName

The name of the new Integrated Cache policy.

rule

The request/response rule that will trigger the given action. The only actions you can specify with a request rule are: MAY_CACHE, MAY_NOCACHE, and INVAL. You specify a rule using a single expression or a logical combination of expressions (called a compound expression). You can combine xpressions using the TWOSYM and || operators. For more information on creating expressions, refer to the add expression CLI command. Note:If a compound expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are examples of valid expressions: ns_ext_cgi||ns_ext_asp "ns_non_get TWOSYM (ns_header_cookie||ns_header_pragma)"

`action`
The integrated cache action to be applied when the system finds content that matches the rules. Possible values: CACHE, NOCACHE, MAY_CACHE, MAY_NOCACHE, INVAL

`storeInGroup`
The content group where the object will be stored when the action directive is CACHE

`invalGroups`
The content group(s) to be invalidated when the action directive is INVAL

`invalObjects`
The content group(s) where the objects will be invalidated when the action directive is INVAL

`undefAction`
A CACHE action, which is used by the policy when the rule evaluation is undefined. The undef action can be NOCACHE or RESET. Possible values: NOCACHE, RESET

Related Commands

rm cache policy

set cache policy

unset cache policy

show cache policy

rm cache policy

Synopsis

```
rm cache policy <policyName>
```

Description

Remove the specified Integrated Cache policy.

Arguments

`policyName`

The name of the cache policy to be removed.

Related Commands

add cache policy

set cache policy

unset cache policy

show cache policy

set cache policy

Synopsis

```
set cache policy <policyName> [-rule <expression>] [-
action <action>] [-storeInGroup <string>] [-invalGroups
<string> ...] [-invalObjects <string> ...] [-
undefAction ( NOCACHE | RESET )]
```

Description

Set a new rule/action/storeInGroup/invalGroups/invalObjects/undefAction for existing cache policy. The rule flow type can change only if action and undefAction(if present) are of NEUTRAL flow type

Arguments

policyName

The name of the new Integrated Cache policy.

rule

The request/response rule that will trigger the given action. The only actions you can specify with a request rule are: MAY_CACHE, MAY_NOCACHE, and INVAL. You specify a rule using a single expression or a logical combination of expressions (called a compound expression). You can combine xpressions using the TWOSYM and || operators. For more information on creating expressions, refer to the add expression CLI command. Note:If a compound expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are examples of valid expressions: ns_ext_cgi||ns_ext_asp "ns_non_get TWOSYM (ns_header_cookie||ns_header_pragma)"

action

The integrated cache action to be applied when the system finds content that matches the rules. Possible values: CACHE, NOCACHE, MAY_CACHE, MAY_NOCACHE, INVAL

storeInGroup

The content group where the object will be stored when the action directive is CACHE

invalGroups
The content group(s) to be invalidated when the action directive is INVAL

invalObjects
The content group(s) where the objects will be invalidated when the action directive is INVAL

undefAction
A CACHE action, to be used by the policy when the rule evaluation turns out to be undefined. The undef action can be NOREWRITE or RESET. Possible values: NOCACHE, RESET

Example

set cache policy pol9 -rule "Q.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

Related Commands

add cache policy
rm cache policy
unset cache policy
show cache policy

unset cache policy

Synopsis

```
unset cache policy <policyName> [-storeInGroup] [-
invalGroups] [-invalObjects] [-undefAction]
```

Description

Use this command to remove cache policy settings.Refer to the set cache policy command for meanings of the arguments.

Related Commands

add cache policy

rm cache policy

set cache policy

show cache policy

show cache policy

Synopsis

```
show cache policy [<policyName>]
```

Description

Display all configured cache policies. To display a single cache policy, specify the name of the policy. When all Integrated Cache policies are displayed, the order of the displayed policies within each group is the same as the evaluation order of the policies. There are three groups: request policies, response policies, and dynamic invalidation policies.

Arguments

`policyName`
The name of the cache policy to be displayed.

`summary`

`fullValues`

`format`

`level`

Output

`state`

`rule`
The request/response rule that will trigger the specified action.

`action`
The integrated cache action to be applied when the system sees content that matches the rules.

`storeInGroup`
The content group that will store the object when the action directive is CACHE.

invalGroups
The content group(s) to be invalidated when the action directive is INVAL.

invalObjects
The content group(s) whose objects will be invalidated when the action directive is INVAL.

priority
Priority.

hits
Hits.

undefAction
A CACHE action, to be used by the policy when the rule evaluation turns out to be undefined.

undefHits
Number of Undef hits.

flags
Flag.

precedeDefRules
Override default request/response cacheability rules.NOTE: This attribute is deprecated.Since pre-builtin, built-in and post-built-in policies are in same policy bank, this is no longer needed

activePolicy
Indicates whether policy is bound or not.

boundTo
Location where policy is bound

gotoPriorityExpression
Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType
Type of policy label invocation.

labelName
Name of the label to invoke if the current policy rule evaluates to TRUE.

Related Commands

add cache policy
rm cache policy
set cache policy
unset cache policy

add cache policylabel

Synopsis

```
add cache policylabel <labelName> -evaluates ( REQ | RES )
```

Description

Add a cache policy label.

Arguments

labelName

Name of the cache policy label.

evaluates

Gives when policies bound to this label get executed. Possible values: REQ, RES

Example

add cache policylabel cache_http_url http_req

Related Commands

rm cache policylabel

bind cache policylabel

unbind cache policylabel

show cache policylabel

rm cache policylabel

Synopsis

```
rm cache policylabel <labelName>
```

Description

Remove a cache policy label.

Arguments

labelName

Name of the cache policy label.

Example

rm cache policylabel cache_http_url

Related Commands

add cache policylabel

bind cache policylabel

unbind cache policylabel

show cache policylabel

bind cache policylabel

Synopsis

```
bind cache policylabel <labelName> -policyName <string>
-priority <positive_integer> [-gotoPriorityExpression
<expression>] [-invoke  (<labelType>  <labelName>) ]
```

Description

Bind the cache policy to one of the labels.

Arguments

labelName

Name of the cache policy label.

policyName

The cache policy name.

Example

i)bind cache policylabel cache_http_url pol_1 1 2 -invoke reqvserver CURRENT ii)bind cache policylabel cache_http_url pol_2 2

Related Commands

add cache policylabel

rm cache policylabel

unbind cache policylabel

show cache policylabel

unbind cache policylabel

Synopsis

```
unbind cache policylabel <labelName> -policyName
<string> [-priority <positive_integer>]
```

Description

Unbind entities from cache label.

Arguments

labelName

Name of the cache policy label.

policyName

The cache policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind cache policylabel cache_http_url pol_1

Related Commands

add cache policylabel

rm cache policylabel

bind cache policylabel

show cache policylabel

show cache policylabel

Synopsis

```
show cache policylabel [<labelName>]
```

Description

Display policy label or policies bound to cache policylabel.

Arguments

labelName
Name of the cache policy label.

summary

fullValues

format

level

Output

state

evaluates
Gives when policies bound to this label get executed.

numpol
Number of polices bound to label.

hits
Number of times policy label was invoked.

policyName
The cache policy name.

priority
Specifies the priority of the policy.

gotoPriorityExpression
Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType
Type of policy label invocation.

labelName
Name of the label to invoke if the current policy rule evaluates to TRUE.

flowType
Flowtype of the bound cache policy.

Example

i)show cache policylabel cache_http_url ii)show cache policylabel

Related Commands

add cache policylabel
rm cache policylabel
bind cache policylabel
unbind cache policylabel

bind cache global

Synopsis

```
bind cache global <policy> -priority <positive_integer>
[-gotoPriorityExpression <expression>] [-type <type>]
[-invoke  (<labelType>  <labelName>) ]
```

Description

Bind the cache policy to one of the two global lists of cache policies. A policy becomes active only after it is bound. All HTTP traffic will be evaluated against these two policy banks. There is a request time policy bank and a response time policy bank. The flow type of the policy implicitly determines which bank it gets bound to. Each bank of policies is an ordered list ordered by policies priority values. Policy Bank Evaluation The goal of evaluation is to traverse the ordered list of policies in the bank, find out which policies match and build a result set that will contain the actions of all the matching policies. While evaluating a policy if any PIXL expression cannot be evaluated then UNDEF processing will get triggered. There are also other scenarios during policy traversal when UNDEF processing can get triggered. If an UNDEF event occurs while processing a policy, then (i) policy bank traversal ends, (ii) the result set of actions that was built so far is wiped out (iii) the current policy's undefAction is put in the result set and the evaluation ends.

Arguments

policy

The name of the Integrated Cache policy to be bound.

Related Commands

unbind cache global

show cache global

unbind cache global

Synopsis

```
unbind cache global <policy> [-type <type>] [-priority
<positive_integer>]
```

Description

Inactivate the policy.

Arguments

policy

The name of the Integrated Cache policy to unbind

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Related Commands

bind cache global

show cache global

show cache global

Synopsis

```
show cache global [-type <type>]
```

Description

Display the cache global bindings.

Arguments

type

The bindpoint to which policy is bound. Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

summary

fullValues

format

level

Output

policyName

Name of the cache policy.

priority

Specifies the priority of the policy.

gotoPriorityExpression

Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType

Type of policy label invocation.

labelName

Name of the label to invoke if the current policy rule evaluates to TRUE.

numpol

The number of policies bound to the bindpoint.

flowType
flowtype of the bound cache policy.

rule
The request/response rule that will trigger the given action.NOTE: This attribute is deprecated.

action
The integrated cache action to be applied when the system sees content that matches the rules.NOTE: This attribute is deprecated.

storeInGroup
The content group to store the object when the action directive is CACHE.NOTE: This attribute is deprecated.

invalGroups
The content group(s) to be invalidated when the action directive is INVAL.NOTE: This attribute is deprecated.

invalObjects
The content group(s) whose objects will be invalidated when the action directive is INVAL.

hits
Hits.NOTE: This attribute is deprecated.

flags
Flags.NOTE: This attribute is deprecated.

precedeDefRules
Override the default request/response cacheability rules.NOTE: This attribute is deprecated.

Example

show cache global

Related Commands

bind cache global

unbind cache global

add cache contentGroup

Synopsis

```
add cache contentGroup <name> [-weakPosRelExpiry <secs>
| -relExpiry <secs> | -relExpiryMilliSec <msecs> | -
absExpiry <HH:MM> ... | -absExpiryGMT <HH:MM> ...] [-
heurExpiryParam <positive_integer>] [-weakNegRelExpiry
<secs>] [(-hitParams <string> ...  [-
ignoreParamValueCase ( YES | NO ) | -hitSelector
<string> | -invalSelector <string>]  [-matchCookies (
YES | NO )])] [-invalParams <string> ...  [-
invalRestrictedToHost ( YES | NO )]] [-pollEveryTime (
YES | NO )] [-ignoreReloadReq ( YES | NO )] [-
removeCookies ( YES | NO )] [-prefetch ( YES | NO )  [-
prefetchPeriod <secs> | -prefetchPeriodMilliSec
<msecs>]] [-prefetchMaxPending <positive_integer>] [-
flashCache ( YES | NO )] [-expireAtLastByte ( YES | NO
)] [-insertVia ( YES | NO )] [-insertAge ( YES | NO )]
[-insertETag ( YES | NO )] [-cacheControl <string>] [-
quickAbortSize <KBytes>] [-minResSize <KBytes>] [-
maxResSize <KBytes>] [-memLimit <MBytes>] [-
ignoreReqCachingHdrs ( YES | NO )] [-minHits <integer>]
[-alwaysEvalPolicies ( YES | NO )] [-pinned ( YES | NO
)] [-lazyDnsResolve ( YES | NO )]
```

Description

Create a new content group.

Arguments

name

The name of the content group to be created

weakPosRelExpiry
Use this parameter for responses with response codes between 200 and 399. (Similar to -relExpiry but has lesser precedence.) Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 31536000

heurExpiryParam
The heuristic expiry time, in percent of the duration since the object was last modified Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 100

relExpiry
The relative expiry time in seconds Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 31536000

relExpiryMilliSec
The relative expiry time in milliseconds. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 86400000

absExpiry
Up to 4 times a day (local time) when all objects in the content group must expire.

absExpiryGMT
Up to 4 times a day (GMT), when all objects in the content group must expire.

weakNegRelExpiry
Use this parameter for all negative responses. This value will be used only if the expiry time cannot be determiend from any other source. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 31536000

hitParams
Use these parameters for parameterized hit evaluation of an object. Up to 128 parameters can be configured.

invalParams
Use these parameters for parameterized invalidation of an object. Up to 8 parameters can be configured.

ignoreParamValueCase
Use this parameter to specify whether to ignore case when comparing parameter values during parameterized hit evaluation. (Parameter value case is always ignored during parameterized invalidation.) Possible values: YES, NO Default value: VAL_NOT_SET

matchCookies
Use this parameter to specify whether to look for parameters also in the cookie header. Possible values: YES, NO Default value: VAL_NOT_SET

invalRestrictedToHost
Use this parameter to specify whether the host header should be taken into account during parameterized invalidation. Possible values: YES, NO Default value: VAL_NOT_SET

pollEveryTime
Use this parameter to specify whether to poll every time for the objects in this content group Possible values: YES, NO Default value: NO

ignoreReloadReq
Use this parameter to specify whether a request can force the system to reload a cached object from the origin. To guard against Denial of Service attacks, you should set this flag to YES. To get RFC-compliant behavior you should set it to NO. Possible values: YES, NO Default value: YES

removeCookies
Use this parameter to specify whether to remove cookies from a response. Possible values: YES, NO Default value: YES

prefetch
Use this parameter to specify whether Integrated Cache should attempt to refresh an object immediately before it is about to go stale. Possible values: YES, NO Default value: YES

prefetchPeriod
The duration in seconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time. Default value: VAL_NOT_SET

prefetchPeriodMilliSec
The duration in seconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time. Default value: VAL_NOT_SET

prefetchMaxPending
The maximum number of outstanding prefetches on the contentgroup Default value: VAL_NOT_SET

flashCache
Use this parameter to specify whether Integrated Cache should do flash cache. Possible values: YES, NO Default value: NO

expireAtLastByte
Use this parameter to specify whether Integrated Cache should expire the content immediately after receving the last body byte. Possible values: YES, NO Default value: NO

insertVia
Use this parameter to specify whether Integrated Cache should insert a Via header. Possible values: YES, NO Default value: YES

insertAge
Use this parameter to specify whether Integrated Cache should insert an Age header. Possible values: YES, NO Default value: YES

insertETag
Use this parameter to specify whether Integrated Cache should insert an ETag header. Possible values: YES, NO Default value: YES

cacheControl
Use this parameter to specify the Cache-Control header to be inserted.

quickAbortSize
If the client aborts when the downloaded response size is less than or equal to quick-abort-size, then Integrated Cache will stop downloading the response. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 4194303

minResSize
The minimum size of the response. Default value: 0 Minimum value: 0 Maximum value: 2097151

maxResSize
The maximum size of the response Default value: 80 Minimum value: 0 Maximum value: 2097151

memLimit
The memory limit for the content group, in MB. The limit is not exact. At times, a group's memory utilization may overshoot the limit, only to stabilize later. Default value: 28665 Minimum value: 0

ignoreReqCachingHdrs
Use this parameter to specify whether to ignore the Cache-control and Pragma headers in the incoming request. Possible values: YES, NO Default value: YES

minHits
Specify the minimum number of accesses for an object to be stored in Cache. Default value: VAL_NOT_SET Minimum value: 0

alwaysEvalPolicies
Forces policy evaluation for each response arriving from origin. Possible values: YES, NO Default value: NO

pinned
Setting pinned to YES prevents IC from flushing objects from this contentgroup under memory pressure. Possible values: YES, NO Default value: NO

lazyDnsResolve
Setting this parameter to NO causes DNS resolution for every response. Setting this parameter to YES causes DNS resolution only when the destination IP in the request does not match the destination IP of the stored object. Possible values: YES, NO Default value: YES

hitSelector
The selector used for hit selection.

invalSelector
The selector used for invalidation.

Related Commands

rm cache contentGroup
set cache contentGroup
unset cache contentGroup
show cache contentGroup

expire cache contentGroup
flush cache contentGroup

rm cache contentGroup

Synopsis

```
rm cache contentGroup <name>
```

Description

Remove the specified content group.

Arguments

name

The name of the content group to be removed.

Related Commands

add cache contentGroup
set cache contentGroup
unset cache contentGroup
show cache contentGroup

expire cache contentGroup
flush cache contentGroup

set cache contentGroup

Synopsis

```
set cache contentGroup <name> [-weakPosRelExpiry <secs>
| -relExpiry <secs> | -relExpiryMilliSec <msecs> | -
absExpiry <HH:MM> ... | -absExpiryGMT <HH:MM> ...] [-
heurExpiryParam <positive_integer>] [-weakNegRelExpiry
<secs>] [-hitParams <string> ... | -hitSelector
<string> | -invalSelector <string>] [-invalParams
<string> ...] [-ignoreParamValueCase ( YES | NO )] [-
matchCookies ( YES | NO )] [-invalRestrictedToHost (
YES | NO )] [-pollEveryTime ( YES | NO )] [-
ignoreReloadReq ( YES | NO )] [-removeCookies ( YES |
NO )] [-prefetch ( YES | NO )] [-prefetchPeriod <secs>
| -prefetchPeriodMilliSec <msecs>] [-
prefetchMaxPending <positive_integer>] [-flashCache (
YES | NO )] [-expireAtLastByte ( YES | NO )] [-
insertVia ( YES | NO )] [-insertAge ( YES | NO )] [-
insertETag ( YES | NO )] [-cacheControl <string>] [-
quickAbortSize <KBytes>] [-minResSize <KBytes>] [-
maxResSize <KBytes>] [-memLimit <MBytes>] [-
ignoreReqCachingHdrs ( YES | NO )] [-minHits <integer>]
[-alwaysEvalPolicies ( YES | NO )] [-pinned ( YES | NO
)] [-lazyDnsResolve ( YES | NO )]
```

Description

Modify attributes of the content group.

Arguments

name

The name of the content group whose attibutes will be changed.

weakPosRelExpiry
Responses with response codes between 200 and 399. (Similar to -relExpiry, but has lesser precedence.) Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 31536000

heurExpiryParam
The heuristic expiry time, in percentage of the elapsed time since the object was last modified. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 100

relExpiry
The relative expiry time in seconds. Minimum value: 0 Maximum value: 31536000

relExpiryMilliSec
The relative expiry time in milliseconds. Minimum value: 0 Maximum value: 86400000

absExpiry
Expiry time for all objects in the content group(up to 4 times a day [local time]).

absExpiryGMT
Expiry time for all objects in the content group(up to 4 times a day [GMT]).

weakNegRelExpiry
All negative responses. This value is used only if the expiry time cannot be determined from any other source. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 31536000

hitParams
Parameterized hit evaluation of an object. Up to 128 parameters can be configured.

invalParams
Parameterized invalidation of an object. Up to 8 parameters can be configured.

ignoreParamValueCase
The option to ignore case while comparing parameter values during parameterized hit evaluation. The case of the parameter value is always ignored during parameterized invalidation. Possible values: YES, NO Default value: VAL_NOT_SET

matchCookies
The option to look for parameters in the cookie header. Possible values: YES, NO Default value: VAL_NOT_SET

invalRestrictedToHost
The option to consider the Host header during parameterized invalidation. Possible values: YES, NO Default value: VAL_NOT_SET

pollEveryTime
The option to poll every time for the objects in this content group. Possible values: YES, NO Default value: NO

ignoreReloadReq
For a request, the option to force the system to reload a cached object from the origin. To guard against Denial of Service attacks, you should set this flag to YES. To get RFC-compliant behavior, you should set it to NO. Possible values: YES, NO Default value: YES

removeCookies
The option to remove cookies from response. Possible values: YES, NO Default value: YES

prefetch
The option to refresh an object immediately before it goes stale. Possible values: YES, NO Default value: YES

prefetchPeriod
The duration in seconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time. Default value: VAL_NOT_SET

prefetchPeriodMilliSec
The duration in milliseconds of the period during which prefetch should be attempted, immediately before the calculated expiry time. Default value: VAL_NOT_SET

prefetchMaxPending
The maximum number of outstanding prefetches on the contentgroup. Default value: VAL_NOT_SET

flashCache
The option to do flash cache on Integrated caching. Possible values: YES, NO Default value: NO

expireAtLastByte
The option to expire the content immediately after receving the last body byte. Possible values: YES, NO Default value: NO

insertVia
The option to insert a Via header. Possible values: YES, NO Default value: YES

insertAge
The option to insert an Age header. Possible values: YES, NO Default value: YES

insertETag
The option to insert an ETag header. Possible values: YES, NO Default value: YES

cacheControl
The option to insert a Cache-Control header.

quickAbortSize
The quick abort size. If the client aborts when the downloaded response size is less than or equal to the quick-abort-size, then the Integrated Cache will stop downloading the response. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 4194303

minResSize
The minimum size of the response. Minimum value: 0 Maximum value: 2097151

maxResSize
The maximum size of the response. Default value: 80 Minimum value: 0 Maximum value: 2097151

memLimit
The memory limit in MB for the content group. The limit is not exact - a group's memory utilization may overshoot the limit, only to stabilize later. Default value: 28665 Minimum value: 0

ignoreReqCachingHdrs
The option to ignore the Cache-control and Pragma headers in the incoming request. Possible values: YES, NO Default value: YES

minHits
The minimum number of accesses for an object to be stored in Cache. Default value: VAL_NOT_SET

alwaysEvalPolicies
The option to force policy evaluation for each response arriving from the origin. Possible values: YES, NO Default value: NO

pinned
The option for IC from flushing objects from this contentgroup under memory pressure. Set YES for IC to take this state. Possible values: YES, NO Default value: NO

lazyDnsResolve
Setting this parameter to NO causes DNS resolution for every response. Setting this parameter to YES causes DNS resolution only when the destination IP in the request does not match the destination IP of the stored object. Possible values: YES, NO Default value: YES

hitSelector
The selector used for hit selection.

invalSelector
The selector used for invalidation.

Related Commands

add cache contentGroup

rm cache contentGroup

unset cache contentGroup

show cache contentGroup

expire cache contentGroup

flush cache contentGroup

unset cache contentGroup

Synopsis

```
unset cache contentGroup <name> [-weakPosRelExpiry] [-
heurExpiryParam] [-relExpiry] [-relExpiryMilliSec] [-
absExpiry] [-absExpiryGMT] [-weakNegRelExpiry] [-
hitParams] [-invalParams] [-ignoreParamValueCase] [-
matchCookies] [-invalRestrictedToHost] [-
pollEveryTime] [-ignoreReloadReq] [-removeCookies] [-
prefetch] [-prefetchPeriod] [-prefetchPeriodMilliSec]
[-prefetchMaxPending] [-flashCache] [-
expireAtLastByte] [-insertVia] [-insertAge] [-
insertETag] [-cacheControl] [-quickAbortSize] [-
minResSize] [-maxResSize] [-memLimit] [-
ignoreReqCachingHdrs] [-minHits] [-alwaysEvalPolicies]
[-pinned] [-lazyDnsResolve] [-hitSelector] [-
invalSelector]
```

Description

Use this command to remove cache contentGroup settings.Refer to the set cache contentGroup command for meanings of the arguments.

Related Commands

add cache contentGroup
rm cache contentGroup
set cache contentGroup
show cache contentGroup

expire cache contentGroup
flush cache contentGroup

show cache contentGroup

Synopsis

```
show cache contentGroup [<name>]
```

Description

Display all content groups. To display a single content group, specify the name of the content group.

Arguments

name
The name of the content group.

summary

fullValues

format

level

Output

flags
Flags.

relExpiry
The relative expiry time in seconds.

relExpiryMilliSec
The relative expiry time in milliseconds.

absExpiry
Up to 4 times a day (local time) when all objects in the content group must expire.

absExpiryGMT

heurExpiryParam

weakPosRelExpiry

weakNegRelExpiry

hitParams

invalParams

ignoreParamValueCase

matchCookies

invalRestrictedToHost

pollEveryTime

ignoreReloadReq

removeCookies

prefetch

prefetchPeriod

prefetchPeriodMilliSec

prefetchCur
Current outstanding prefetches.

prefetchMaxPending

flashCache

expireAtLastByte

insertVia

insertAge

insertETag

cacheControl

quickAbortSize

minResSize

maxResSize

memUsage
Current memory usage.

memLimit

ignoreReqCachingHdrs

cacheNon304Hits
Cache non 304 hits.

cache304Hits
Cache 304 hits.

cacheCells
Number of cells.

cacheGroupIncarnation
Cache group incarnation.

minHits

alwaysEvalPolicies

pinned

lazyDnsResolve

hitSelector

invalSelector

policyName
Active cache policies refering to this group.

cacheNumInvalPolicy
Number of active Invalidation policies refering to this group.

markerCells
Numbers of marker cells in this group.

Related Commands

add cache contentGroup
rm cache contentGroup
set cache contentGroup
unset cache contentGroup

expire cache contentGroup
flush cache contentGroup

expire cache contentGroup

Synopsis

```
expire cache contentGroup <name>
```

Description

Expire the objects in the specified content group.

Arguments

name

The name of the content group whose objects are to be expired.

Related Commands

add cache contentGroup
rm cache contentGroup
set cache contentGroup
unset cache contentGroup
show cache contentGroup

flush cache contentGroup

flush cache contentGroup

Synopsis

```
flush cache contentGroup <name> [-query <string> | -
selectorValue <string>] [-host <string>]
```

Description

Flush the objects in the specified content group.

Arguments

name

The name of the content group whose objects are to be flushed.

query

If a query string is specified, then the selected objects in this group will be flushed using parameterized invalidation. Otherwise, all objects in the group will be flushed.

host

To be set only if parameterized invalidation is being done. Objects belonging only to the specified host will be flushed. The host argument can be provided if and only if -invalRestrictedToHost is set to YES for the given group.

selectorValue

The value of the selector to be used for flushing objects in the contentgroup.

Related Commands

add cache contentGroup

rm cache contentGroup

set cache contentGroup

unset cache contentGroup

show cache contentGroup

expire cache contentGroup

add cache forwardProxy

Synopsis

```
add cache forwardProxy <IPAddress> <port>
```

Description

Add a forward proxy known to Integrated cache.

Arguments

`IPAddress`

The IP address of the forward proxy.

`port`

The port of the forward proxy. Minimum value: 1

Related Commands

rm cache forwardProxy

show cache forwardProxy

rm cache forwardProxy

Synopsis

```
rm cache forwardProxy <IPAddress> <port>
```

Description

Remove a forward proxy known to Integrated cache.

Arguments

IPAddress

The IP address of the forward proxy.

port

The port of the forward proxy. Minimum value: 1

Related Commands

add cache forwardProxy

show cache forwardProxy

show cache forwardProxy

Synopsis

```
show cache forwardProxy
```

Description

Display all forward proxies known to Integrated cache.

Arguments

summary

fullValues

format

level

Output

IPAddress

The IP address of the forward proxy.

port

Forward proxy port.

Related Commands

add cache forwardProxy

rm cache forwardProxy

add cache selector

Synopsis

```
add cache selector <selectorName> <rule> ...
```

Description

Create Integrated Cache selectors. A selector is an abstraction for a collection of PIXL expressions. After creating a selector, you can use it as either a hitSelector (for doing hit selection) or as an invalSelector (for invalidating cached objects), or both. You need to specify at least one expression when you create a selector.

Arguments

`selectorName`

The name of the Integrated Cache selector.

`rule`

The set of PIXL expressions.

Related Commands

rm cache selector

set cache selector

show cache selector

rm cache selector

Synopsis

```
rm cache selector <selectorName>
```

Description

Use this command to remove Integrated Cache selectors.

Arguments

`selectorName`

The name of the Integrated Cache selector.

Related Commands

add cache selector

set cache selector

show cache selector

set cache selector

Synopsis

```
set cache selector <selectorName> <rule> ...
```

Description

Change the set of expressions associated with Integrated Cache selectors.

Arguments

`selectorName`

The name of the Integrated Cache selector.

`rule`

The PIXL expressions.

Related Commands

add cache selector

rm cache selector

show cache selector

show cache selector

Synopsis

```
show cache selector [<selectorName>]
```

Description

Display Integrated Cache selectors.

Arguments

selectorName

The name of the Integrated Cache selector.

summary

fullValues

format

level

Output

flags

Flags.

rule

Rule.

Related Commands

add cache selector

rm cache selector

set cache selector

set cache parameter

Synopsis

```
set cache parameter [-memLimit <MBytes>] [-via
<string>] [-verifyUsing <verifyUsing>] [-maxPostLen
<positive_integer>] [-prefetchMaxPending
<positive_integer>] [-enableBypass ( YES | NO )] [-
undefAction ( NOCACHE | RESET )]
```

Description

Modify the global configuration of the Integrated Cache.

Arguments

memLimit

The memory limit for Integrated Cache. Default value: VAL_NOT_SET Minimum value: 0

via

The string to be inserted in the "Via" header. A Via header is inserted in all responses served from a content group if its insertVia flag is set.

verifyUsing

The criteria for deciding whether a cached object can be served for an incoming HTTP request. a.If the value of this attribute is set to HOSTNAME, then URL , host name and host port values in the incoming HTTP request header must match before a cached object can be served. The IP address and the TCP port of the destination host are not matched. For certain deployments the HOSTNAME setting can be a security risk. A rogue client can access a rogue server via the Integrated Cache using the following HTTP request : GET / HTTP/1.1 Host: sensitive.foo.com Integrated Cache will store the rogue page served by the rogue server. Any subsequent client trying to access the root page from sensitive.foo.com will be served the rogue page. The HOSTNAME setting should only be set if it is certain that no rogue client can access a rogue server via the Integrated Cache. The YES setting can lead to more hits if DNS-based load balancing is in use and the same content can be served by multiple backend servers. b.If the attribute is set to HOSTNAME_AND_IP, then the following items must match: URL, host

name, host port in the incoming HTTP request header, and the IP address and TCP port of the destination server. c.If the attribute is set to DNS, then the following items should match: URL, host name and host port in the incoming HTTP request, and the TCP port. The hostname is used to do a DNS lookup of the destination server's IP address, and is compared with the set of addresses returned by the DNS lookup. # <GB> # last sentence above: ok as edited? # </GB> The default value of this attribute is DNS. Possible values: HOSTNAME, HOSTNAME_AND_IP, DNS Default value: VAL_NOT_SET

`maxPostLen`

maximum number of POST body bytes to consider when evaluating parameters for a content group for which you have configured hitParams and invalParams. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 131072

`prefetchMaxPending`

The maximum number of outstanding prefetches in the IC. Default value: VAL_NOT_SET

`enableBypass`

The bypass parameter. When this value is set to NO, an incoming request will serve a hit if a matching object is found in cache storage, regardless of the cacheability policy configuration. If set to YES, the bound request cacheability policies are evaluated before attempting any hit selection in the cache storage. If the request matches a policy with a NOCACHE action, the request will bypass all cache processing. This flag does not affect processing of requests that match any invalidation policy. Possible values: YES, NO Default value: VAL_NOT_SET

`undefAction`

Set the default cache undef action. If an UNDEF event is triggered during policy evaluation and if the current policy's undefAction is not specified, then this global undefAction value is used. Can be NOCACHE or RESET. NOCACHE is the default value of default cache undef action. Possible values: NOCACHE, RESET

Related Commands

unset cache parameter

show cache parameter

unset cache parameter

Synopsis

```
unset cache parameter [-memLimit] [-via] [-verifyUsing]
[-maxPostLen] [-prefetchMaxPending] [-enableBypass] [-
undefAction]
```

Description

Use this command to remove cache parameter settings.Refer to the set cache parameter command for meanings of the arguments.

Related Commands

set cache parameter

show cache parameter

show cache parameter

Synopsis

```
show cache parameter
```

Description

Display the global configuration of the Integrated Cache.

Arguments

format

level

Output

memLimit
The memory limit for the Integrated Cache.

maxMemLimit
The maximum value of the memory limit for the Integrated Cache.

via
The string that is inserted in the "Via" header.

verifyUsing
The criteria for deciding whether a cached object can be served for an incoming HTTP request.

maxPostLen
The maximum POST body size that the IC can accumulate.

prefetchCur
Number of current outstanding prefetches in the IC.

prefetchMaxPending
The maximum number of outstanding prefetches on the content group.

enableBypass
When this value is set to NO, an incoming request will serve a hit if a matching object is found in cache storage, regardless of the cacheability

policy configuration. If set to YES, the bound request cacheability policies are evaluated before attempting any hit selection in the cache storage. If the request matches a policy with a NOCACHE action, the request will bypass all cache processing. This flag does not affect processing of requests that match any invalidation policy.

`undefAction`
Set the default cache undef action. If an UNDEF event is triggered during policy evaluation and if the current policy's undefAction is not specified, then this global undefAction value is used. Can be NOCACHE or RESET. NOCACHE is the default value of default cache undef action.

Related Commands

set cache parameter

unset cache parameter

CHAPTER 10

CLI Commands

This chapter covers the CLI commands.

show cli attribute

Synopsis

```
show cli attribute
```

Description

Display attributes of the NetScaler CLI

Arguments

Output

qquote

The construct that is used to quote strings that are to be taken as-is, without interpreting escape sequences like " ". This construct consists of: a 'q', followed by a delimiter character; the string follows immediately after the delimiter and is terminated by the first matching delimiter character. (The set of possible delimiter characters is listed below.) For example, q/a / will result in a three-character string ('a', '', 'n'); whereas "a " results in a two-character string ('a' followed by a newline).

qquoteDelimiters

The set of characters that can be used as the delimiter in a q// construct. Characters shown in pairs must be used that way, whereas characters shown singly server as thier own matching delimiter. For example, q?abc? and q{abc} are valid q// constructs, and evaluate to the string "abc"; q{abc{ is however not a valid q// construct so it will evaluate to the string "q{abc{".

Related Commands

clear cli prompt

Synopsis

```
clear cli prompt
```

Description

Use this command to return the CLI prompt to the default (a single '>').

Related Commands

set cli prompt

show cli prompt

cls

Synopsis

```
cls
```

Description

Clear the screen and reposition cursor at top right.

Related Commands

alias

Synopsis

```
alias [<pattern>  [(command)]]
```

Description

Create (short) aliases for (long) commands. Aliases are saved across NSCLI sessions. If no argument is specified, the alias command will display existing aliases.

Arguments

pattern

Alias name. (Can be a regular expression.)

Example

alias info "show ns info"

Related Commands

unalias

Synopsis

```
unalias <pattern>
```

Description

Remove an alias

Arguments

`pattern`

Name of the alias

Example

unalias info

Related Commands

batch

Synopsis

```
batch -fileName <input_filename> [-outfile
<output_filename>] [-ntimes <positive_integer>]
```

Description

Use this command to read the contents of a file and execute each line as a separate CLI command. Each command in the file must be on a separate line. Lines starting with # are considered comments.

Arguments

`fileName`

The name of the batch file.

`outfile`

The name of the file where the executed batch file will write its output. The default is standard output.

`ntimes`

The number of times the batch file will be executed. Default value: 1

Example

batch -f cmds.txt

Related Commands

source

Synopsis

```
source <fileName>
```

Description

Use this command to read the contents of a file and execute each line as a separate CLI command. Each command in the file being read must be on a separate line. Lines starting with # are considered comments.

Arguments

`fileName`

The name of the file to be sourced.

Example

source cmds.txt

Related Commands

help

Synopsis

```
help [(commandName) | <groupName> | -all]
```

Description

Use this command to display help information for a CLI command, for a group of commands, or for all CLI commands.

Arguments

commandName

The name of a command for which you want full usage information.

groupName

The name of a command group for which you want basic usage information.

all

Use this option to request basic usage information for all commands.

Example

1.To view help information for adding a virtual server, enter the following CLI command: help add vserver The following information is displayed: Usage: add vserver <vServerName> <serviceType> [<IPAddress> port>] [-type (CONTENT | ADDRESS)] [-cacheType <cacheType>] [-backupVServerName <string>] [-redirectURL <URL>] [-cacheable (ON | OFF)] [-state (ENABLED | DISABLED)] where: serviceType = (HTTP | FTP | TCP | UDP | SSL | SSL_BRIDGE | SSL_TCP | NNTP| DNS | ANY) <cacheType> = (TRANSPARENT | REVERSE | FORWARD) Done 2.To view help information for all DNS commands, enter the following command: help dns The following information is displayed: add aaaaRec <hostname> <IPv6Address> ... [-TTL <secs>] rm aaaaRec <hostname> [<IPv6Address> ...] show aaaaRec [<hostname> | -type <type>] add addRec <hostname> <IPAddress> ... [-TTL <secs>] [-private <ip_addr>] rm addRec <hostname> [<IPAddress> ...] show addRec [<hostname> | -type <type>] add cnameRec <aliasName> <canonicalName> [-TTL <secs>] rm cnameRec <aliasName> show cnameRec [<aliasName> | -type <type>] add mxRec <domain> -mx <string> -pref <positive_integer> [-TTL <secs>] rm mxRec <domain> <mx> set mxRec <domain> -mx <string> [-pref <positive_integer>] [-TTL <secs>]

show mxRec [<domain> | -type <type>] add nsRec <domain> [-p <string>] [-s <string>] [-TTL <secs>] rm nsRec <domain> [-p <string> | -s <string>] show nsRec [<domain> | -type <type>] set dns parameter [-timeout <secs>] [-retries <positive_integer>] [-minTTL <secs>] [-maxTTL <secs>] [-TTL (ENABLED | DISABLED)] [-cacheRecords (YES | NO)] show dns parameter add soaRec <domain> -contact <string> -serial <positive_integer> -refresh <secs> -retry <secs> -expire <secs> -minimum <secs>-TTL <secs> rm soaRec <domain> set soaRec <domain> [-contact <string>] [-serial <positive_integer>][-refresh <secs>] [-retry <secs>] [-expire <secs>] [-minimum <secs>][-TTL <secs>] show soaRec [<domain> | -type <type>] add dns ptrRec <reverseDomain> <domain> ... [-TTL <secs>] rm dns ptrRec <reverseDomain> [<domain> ...] show dns ptrRec [<reverseDomain> | -type <type>] add dns srvRec <domain> <target> -priority <positive_integer> -weight <positive_integer> -port <positive_integer> rm dns srvRec <domain> [<target> ...] set dns srvRec <domain> <target> [-priority <positive_integer>] [-weight <positive_integer>] [-port <positive_integer>] [-TTL <secs>] show dns srvRec [(<domain> [<target>]) | -type <type>] Done

Related Commands

history

Synopsis

```
history
```

Description

Use this command to see the history of the commands executed on CLI.

Example

history 1 add snmp trap SPECIFIC 10.102.130.228
2 save config 3 show system session 4 swhell
5 shell 6 what 7 shell 8 help
stat lbvserver ...

Related Commands

man

Synopsis

```
man [(commandName)]
```

Description

Use this command to invoke the man page for the specified command. You can specify the command in full, or partially, if it is uniquely resolvable.

Arguments

commandName

The name of the command.

Example

man add vs

Related Commands

quit

Synopsis

```
quit
```

Description

Use this command to terminate the CLI. Note: typing <Ctrl>+<d> will also terminate the CLI.

Related Commands

exit

Synopsis

```
exit
```

Description

Use this command to back out one level in config mode, or to terminate the CLI when not in config mode.);

Related Commands

whoami

Synopsis

```
whoami
```

Description

Show the current user.

Output

Related Commands

config

Synopsis

```
config
```

Description

Enter this command to enter contextual mode.

Related Commands

set cli mode

Synopsis

```
set cli mode [-page ( ON | OFF )] [-total ( ON | OFF )]
[-color ( ON | OFF )] [-disabledFeatureAction
<disabledFeatureAction>] [-timeout <secs>] [-regex ( ON
| OFF )]
```

Description

Use this command to specify how the CLI should display command output.

Arguments

page

Determines whether output that spans more than one screen is "paged". Specify ON to pause the display after each screen of ouput. The default is OFF. Possible values: ON, OFF Default value: OFF

total

Determines whether CLI "show" commands display a total count of objects before displaying the objects themselves. The default is ON. Possible values: ON, OFF Default value: OFF

color

Specifies whether output can be shown in color, if the terminal supports it. Possible values: ON, OFF Default value: OFF

disabledFeatureAction

Specifies what will happen when a configuration command is issued for a disabled feature. The following values are allowed: NONE - The action is allowed, and no warning message is issued.; ALLOW - The action is allowed, but a warning message is issued.; DENY - The action is not allowed.; HIDE - Commands that configure disabled features are hidden, and the CLI behaves as if they did not exist. Possible values: NONE, ALLOW, DENY, HIDE Default value: NS_ALLOW

timeout

CLI session inactivity timeout, in seconds Default value: 1800 Minimum value: 0 Maximum value: 100000000

regex

If ON, regular expressions can be used as argument values Possible values: ON, OFF Default value: ON

Related Commands

unset cli mode

show cli mode

unset cli mode

Synopsis

```
unset cli mode [-page] [-total] [-color] [-
disabledFeatureAction] [-timeout] [-regex]
```

Description

Use this command to remove cli mode settings.Refer to the set cli mode command for meanings of the arguments.

Related Commands

set cli mode

show cli mode

show cli mode

Synopsis

```
show cli mode
```

Description

Use this command to display the current settings of parameters that can be set with the 'set cli mode' command.

Arguments

format

level

Output

r
regular expression

argMark
mark

format
format

Related Commands

set cli mode

unset cli mode

set cli prompt

Synopsis

```
set cli prompt <promptString>
```

Description

Use this command to customize the CLI prompt.

Arguments

promptString

The prompt string. The following special values are allowed: %! - will be replaced by the history event number %u - will be replaced by the NetScaler user name %h - will be replaced by the NetScaler hostname %t - will be replaced by the current time %T - will be replaced by the current time (24 hr format) %d - will be replaced by the current date %s - will be replaced by the node state

Example

> set cli prompt "%h %T" Done lb-ns1 15:16>

Related Commands

clear cli prompt

show cli prompt

show cli prompt

Synopsis

```
show cli prompt
```

Description

Use this command to display the current CLI prompt, with special values like '%h' unexpanded.

Arguments

format

level

Output

Example

10.101.4.22 15:20> sh cli prompt CLI prompt is set to "%h %T" Done

Related Commands

clear cli prompt

set cli prompt

CHAPTER 11

Compression Commands

This chapter covers the compression commands.

stat cmp

Synopsis

```
stat cmp [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display compression statistics.

Arguments

Output

Counters

Bandwidth saving (%) (DlBndSav)
Bandwidth saving from delta compression expressed as percentage.

Delta compression ratio (DlCmpRt)
Ratio of compressible data received to compressed data transmitted (uncmp:1.0).

Decompression ratio (DTCmpRt)
Ratio of decompressed data transmitted to compressed data received (decmp:1.0).

Bandwidth saving (%) (DBndSav)
Bandwidth saving from TCP compression expressed as percentage. This is calculated using the following formula: [(Total bytes received for compression from the server ? compressed bytes transmitted to the client)/ (Total bytes received for compression from the server)] * 100

TCP compression ratio (TCmpRt)
Ratio of compressible data received to compressed data transmitted (uncmp:1.0).

TCP Bandwidth saving (%) (BndSav)
Bandwidth saving from TCP compression expressed as percentage.

Total HTTP compression ratio
Ratio of total HTTP data received to total HTTP data transmitted (uncmp:1.0).

HTTP compression ratio
Ratio of the compressible data received from the server to the compressed data sent to the client.

HTTP compression requests
Number of HTTP compression requests the NetScaler receives for which the response is successfully compressed. For example, after you enable compression and configure services, if you send requests to the NetScaler with the following header information: ?Accept-Encoding: gzip, deflate?, and NetScaler compresses the corresponding response, this counter is incremented.

Compressible bytes received
Number of bytes that can be compressed, which the NetScaler receives from the server. This gives the content length of the response that the NetScaler receives from server.

Compressed bytes transmitted
Number of bytes the NetScaler sends to the client after compressing the response from the server.

Compressible packets received
Number of HTTP packets that can be compressed, which the NetScaler receives from the server.

Compressed packets transmitted
Number of HTTP packets that the NetScaler sends to the client after compressing the response from the server.

Compressible bytes received (TCmpRxB)
Number of bytes that can be compressed, which the NetScaler receives from the server. This gives the content length of the response that the NetScaler receives from server.

Compressible packets received (TCmpRxP)
Total number of compressible packets received by NetScaler.

Compressed bytes transmitted (TCmpTxB)
Number of bytes that the NetScaler sends to the client after compressing the response from the server.

Compressed packets transmitted (TCmpTxP)
Number of TCP packets that the NetScaler sends to the client after compressing the response from the server.

Quantum compression (TCmpQuan)
Number of times the NetScaler compresses a quantum of data. NetScaler buffers the data received from the server till it reaches the quantum size and then compresses the buffered data and transmits to the client.

Push flag compression (TCmpPush)
Number of times the NetScaler compresses data on receiving a TCP PUSH flag from the server. The PUSH flag ensures that data is compressed immediately without waiting for the buffered data size to reach the quantum size.

End Of Input compression (TCmpEoi)
Number of times the NetScaler compresses data on receiving End Of Input (FIN packet). When the NetScaler receives End Of Input (FIN packet), it compresses the buffered data immediately without waiting for the buffered data size to reach the quantum size.

Timer compression (TCmpTmr)
Number of times the NetScaler compresses data on expiration of data accumulation timer. The timer expires if the server response is very slow and consequently, the NetScaler does not receive response for a certain amount of time. Under such a condition, the NetScaler compresses the buffered data immediately without waiting for the buffered data size to reach the quantum size.

Compressed bytes received (DCmpTRxB)
Total number of compressed bytes received by NetScaler.

Compressed packets received (DCmpTRxP)
Total number of compressed packets received by NetScaler.

Decompressed bytes transmitted (DCmpTTxB)
Total number of decompressed bytes transmitted by NetScaler.

Decompressed packets transmitted (DCmpTTxP)
Total number of decompressed packets transmitted by NetScaler.

Wrong data (DCmpErrD)
Number of data errors encountered while decompressing.

Less Data (DCmpErrL)
Number of times NetScaler received less data than declared by protocol.

More Data (DCmpErrM)
Number of times NetScaler received more data than declared by protocol.

Memory failures (DCmpMem)
Number of times memory failures occurred while decompressing.

Unknown (DCmpErrU)
Number of times unknown errors occurred while decompressing.

Delta compression requests (DlCmpRx)
Total number of delta compression requests received by NetScaler.

Delta compression applied (DlDone)
Total number of delta compressions done by NetScaler.

Compressible bytes received (DlCmpRxB)
Total number of delta-compressible bytes received by NetScaler.

Compressed bytes transmitted (DlCmpTxB)
Total number of delta-compressed bytes transmitted by NetScaler.

First-time access (DlCmpFAc)
Total number of delta compression first accesses.

Compressible packets received (DlCmpRxP)
Number of delta-compressible packets received.

Compressed packets transmitted (DlCmpTxP)
Total number of delta-compressed packets transmitted by NetScaler.

Basefile requests served (DlCBSrv)
Total number of basefile requests served by NetScaler.

Basefile bytes transmitted (DlCBTxB)
Number of basefile bytes transmitted by NetScaler.

Delta compression bypassed (DlCmpEBy)
Number of times delta-compression bypassed by NetScaler.

Basefile write header failed (DlCmpEBW)
Number of times basefile could not be updated in NetScaler cache.

Basefile no-store miss (DlCmpENM)
Number of times basefile was not found in NetScaler cache.

Request information too big (DlCmpERB)
Number of times basefile request URL was too large.

Request info alloc failed (DlCmpERF)
Number of times requested basefile could not be allocated.

Session allocation failed (DlCmpESF)
Number of times delta compression session could not be allocated.

Response bytes received (HTRspbRx)
Bytes received as response data.

Related Commands

show cmp stats

Synopsis

```
show cmp stats - alias for 'stat cmp'
```

Description

show cmp stats is an alias for stat cmp

Related Commands

stat cmp

add cmp action

Synopsis

```
add cmp action <name> <cmpType>
```

Description

Create a compression action. The action thus created can be associated with the compression policy. The built-in compression actions NOCOMPRESS/ COMPRESS/GZIP/DEFLATE are always present on the system. These actions are: NOCOMPRESS action - can be used to define a policy that disables compression for the matching policy.COMPRESS action - can be used to enable compression for a specific policy. This action will do GZIP or DEFLATE, based on the browser. GZIP action - can be used to enable GZIP compression for a specific policy. With this action, GZIP compression will be performed if the browser supports GZIP, other wise compression is disabled. DEFLATE action - can be used to enable DEFLATE compression for a specific policy. With this action, DEFLATE compression will be performed if the browser supports DEFLATE, otherwise compression is disabled.

Arguments

name

The name of the compression action.

cmpType

The type of compression action. Possible values: compress, gzip, deflate, nocompress

deltaType

The type of delta action (if delta type compression action is defined). Possible values: PERURL, PERPOLICY Default value: NS_ACT_CMP_DELTA_TYPE_PERURL

Example

add cmp action nocmp NOCOMPRESS

Related Commands

rm cmp action

show cmp action

rm cmp action

Synopsis

```
rm cmp action <name>
```

Description

Remove the specified compression action.

Arguments

name

The name of the compression action.

Example

rm cmp action cmp_action_name

Related Commands

add cmp action

show cmp action

show cmp action

Synopsis

```
show cmp action [<name>]
```

Description

Display the compression actions defined including the built-in actions.

Arguments

name

The name of the compression action.

summary

fullValues

format

level

Output

cmpType

The type of compression action.

deltaType

The type of delta action if compression type is delta compression.NOTE: This attribute is deprecated.Deprecating delta action in cmp policies

Example

Example 1 The following example shows output from the show cmp action command when no custom cmp actions have been defined: > show cmp action 3 Compression actions: 1) Name: GZIP Compression Type: gzip 2) Name: NOCOMPRESS Compression Type: nocompress 3) Name: DEFLATE Compression Type: deflate 4) Name: COMPRESS Compression Type: compress Done Done Example 2 The following command creates a compression action: add cmp action nocmp NOCOMPRESS The following example shows output from the show cmp action command after the previous command has been issued: > show cmp action 3 Compression actions: 1) Name: GZIP Compression Type:

gzip 2) Name: NOCOMPRESS Compression Type: nocompress 3) Name: DEFLATE Compression Type: deflate 4) Name: COMPRESS Compression Type: compress 1 Compression action: 1) Name: nocmp Compression Type: nocompress Done

Related Commands

add cmp action

rm cmp action

add cmp policy

Synopsis

```
add cmp policy <name> -rule <expression> -resAction
<string>
```

Description

Create a compression policy.

Arguments

name

The name of the new compression policy.

rule

The expression specifying the condition.

resAction

The action needs to be performed when the rule matches. The string value can be a created compression action (user defined) or one of the following built-in actions: NOCOMPRESS action - can be used to define a policy that disables compression for the matching policy.COMPRESS action - can be used to enable compression for a specific policy. This action will do GZIP or DEFLATE, based on the browser. GZIP action - can be used to enable GZIP compression for a specific policy. With this action, GZIP compression will be performed if the browser supports GZIP, other wise compression is disabled. DEFLATE action - can be used to enable DEFLATE compression for a specific policy. With this action, DEFLATE compression will be performed if the browser supports DEFLATE, otherwise compression is disabled.

Example

Example 1: add cmp policy pdf_cmp -rule "RES.HTTP.HEADER Content-Type CONTAINS application/pdf" -resAction COMPRESS After creating the above compression policy, you must activate it by binding it globally: bind cmp global pdf_cmp The NetScaler system will use the configured pdf_cmp compression policy to perform compression of pdf files. Example 2: The following command disables compression for all the access from the specific subnet. add cmp policy local_sub_nocmp -rule "SOURCEIP == 10.1.1.0 -

netmask 255.255.255.0" -rspaction NOCOMPRESS bind cmp global local_sub_nocmp

Related Commands

rm cmp policy

set cmp policy

unset cmp policy

show cmp policy

rm cmp policy

Synopsis

```
rm cmp policy <name>
```

Description

Remove a compression policy.

Arguments

name

The name of the compression policy.

Example

rm cmp policy cmp_policy_name The "show cmp policy" command shows all currently defined cmp policies.

Related Commands

add cmp policy

set cmp policy

unset cmp policy

show cmp policy

set cmp policy

Synopsis

```
set cmp policy <name> [-rule <expression>] [-resAction
<string>]
```

Description

Modify the created compression policy. Use the "show cmp policy" command to view all configured cmp policies.

Arguments

name

The name of the new compression policy.

rule

The expression specifying the condition.

resAction

The action needs to be performed when the rule matches. The string value can be a created compression action (user defined) or one of the following built-in actions: NOCOMPRESS action - can be used to define a policy that disables compression for the matching policy.COMPRESS action - can be used to enable compression for a specific policy. This action will do GZIP or DEFLATE, based on the browser. GZIP action - can be used to enable GZIP compression for a specific policy. With this action, GZIP compression will be performed if the browser supports GZIP, other wise compression is disabled. DEFLATE action - can be used to enable DEFLATE compression for a specific policy. With this action, DEFLATE compression will be performed if the browser supports DEFLATE, otherwise compression is disabled.

Example

Example 1: add cmp policy pdf_cmp -rule "RES.HTTP.HEADER Content-Type CONTAINS application/pdf" -resAction COMPRESS After creating the above compression policy, you must activate it by binding it globally: bind cmp global pdf_cmp The NetScaler system will use the configured pdf_cmp compression policy to perform compression for pdf files. To disable pdf compression for Internet Explorer, you can change the above compression policy by issuing the following command: set cmp policy pdf_cmp -rule

"RES.HTTP.HEADER Content-Type CONTAINS application/pdf && RES.HTTP.HEADER User-Agent NOTCONTAINS MSIE" To view the changed cmp policy, enter the following command: >show cmp policy pdf_cmp Name: pdf_cmp Rule: (RES.HTTP.HEADER Content-Type CONTAINS application/pdf && REQ.HTTP.HEADER User-Agent NOTCONTAINS MSIE) Response action: COMPRESS Hits: 2 Bytes In:...609284 Bytes Out:... 443998 Bandwidth saving...27.13% Ratio 1.37:1 Done

Related Commands

add cmp policy

rm cmp policy

unset cmp policy

show cmp policy

unset cmp policy

Synopsis

```
unset cmp policy <name> [-rule] [-resAction]
```

Description

Use this command to remove cmp policy settings.Refer to the set cmp policy command for meanings of the arguments.

Related Commands

add cmp policy

rm cmp policy

set cmp policy

show cmp policy

show cmp policy

Synopsis

```
show cmp policy [<name>]
```

Description

Display the created compression policies.

Arguments

name
The name of the cmp policy.

summary

fullValues

format

level

Output

rule
The expression specifying the condition.

reqAction
The compression action to be performed on requests.

resAction
The compression action to be performed on responses.

hits
Number of hits.

txbytes
Number of bytes transferred.

rxbytes
Number of bytes received.

clientTTLB
Total client TTLB value.

clientTransactions
Number of client transactions.

serverTTLB
Total server TTLB value.

serverTransactions
Number of server transactions.

boundTo
The entity name to which policy is bound

Example

> show cmp policy 4 Compression policies: 1) Name: ns_cmp_content_type Rule: ns_content_type Response action: COMPRESS Hits: 1 Bytes In:...4325 Bytes Out:... 1530 Bandwidth saving...64.62% Ratio 2.83:1 2) Name: ns_cmp_msapp Rule: (ns_msie && ns_msword || (ns_msexcel || ns_msppt)) Response action: COMPRESS Hits: 7 Bytes In:...796160 Bytes Out:... 197730 Bandwidth saving...75.16% Ratio 4.03:1 3) Name: ns_cmp_mscss Rule: (ns_msie && ns_css) Response action: COMPRESS Hits: 0 4) Name: ns_nocmp_mozilla_47 Rule: (ns_mozilla_47 && ns_css) Response action: NOCOMPRESS Hits: 0 Done You can also view an individual cmp policy by giving the cmp policy name as an argument: > show cmp policy ns_cmp_msapp Name: ns_cmp_msapp Rule: (ns_msie && ns_msword || (ns_msexcel || ns_msppt)) Response action: COMPRESS Hits: 7 Bytes In:...796160 Bytes Out:... 197730 Bandwidth saving...75.16% Ratio 4.03:1 Done

Related Commands

add cmp policy

rm cmp policy

set cmp policy

unset cmp policy

bind cmp global

Synopsis

```
bind cmp global (<policyName>  [-priority
<positive_integer>]) [-state ( ENABLED | DISABLED )]
```

Description

Activate the compression policy globally. Note that for compression feature to work, a compression license is required. To activate the compression feature, use the "enable ns feature cmp" command. When you enable the compression feature, all of the built-in compression policies are bound globally.

Arguments

policyName

The name of the compression policy.

Example

add cmp policy pdf_cmp -rule "RES.HTTP.HEADER Content-Type CONTAINS application/pdf" -resAction COMPRESS After creating the above compression policy, you must activate it by binding it globally: bind cmp global pdf_cmp After binding pdf_cmp compression policy globally, the policy gets activated and the NetScaler system will perform compression for the pdf files. To view the globally active compression policies, enter the following command: > show cmp global 5 Globally Active Compression Policies: 1) Policy Name: ns_cmp_content_type Priority: 0 2) Policy Name: ns_nocmp_mozilla_47 Priority: 0 3) Policy Name: ns_cmp_mscss Priority: 0 4) Policy Name: ns_cmp_msapp Priority: 0 5) Policy Name: pdf_cmp Priority: 0 Done

Related Commands

unbind cmp global

show cmp global

unbind cmp global

Synopsis

```
unbind cmp global <policyName>
```

Description

Deactivate an active compression policy.

Arguments

policyName

The name of the compression policy.

Example

To view the globally active compression policies, enter the following command: > show cmp global 5 Globally Active Compression Policies: 1) Policy Name: ns_cmp_content_type Priority: 0 2) Policy Name: ns_nocmp_mozilla_47 Priority: 0 3) Policy Name: ns_cmp_mscss Priority: 0 4) Policy Name: ns_cmp_msapp Priority: 0 5) Policy Name: pdf_cmp Priority: 0 Done To deactivate this globally active compression policy on the NetScaler system, enter the following command: unbind cmp global pdf_cmp

Related Commands

bind cmp global

show cmp global

show cmp global

Synopsis

```
show cmp global
```

Description

Display the globally activated compression policies.

Arguments

summary

fullValues

format

level

Output

policyName
The compression policy name.

priority
The priority of the policy.

state
The current state of the binding.

Example

> show cmp global 4 Globally Active Compression Policies: 1) Policy Name: ns_cmp_content_type Priority: 0 2) Policy Name: ns_nocmp_mozilla_47 Priority: 0 3) Policy Name: ns_cmp_mscss Priority: 0 4) Policy Name: ns_cmp_msapp Priority: 0 Done

Related Commands

bind cmp global

unbind cmp global

set cmp parameter

Synopsis

```
set cmp parameter [-cmpLevel <cmpLevel>] [-quantumSize
<positive_integer>] [-serverCmp ( ON | OFF )] [-
minResSize <positive_integer>] [-cmpBypassPct
<positive_integer>]
```

Description

Configurable parameters for compression.

Arguments

cmpLevel

Compression level. Possible values: optimal, bestspeed, bestcompression Default value: NSCMPLVL_OPTIMAL

quantumSize

Minimum amount of data to compress as one unit. Default value: 57344 Minimum value: 8 Maximum value: (62*1024)

serverCmp

Compression at back-end server. Possible values: ON, OFF Default value: ON

heurExpiry

Heuristic basefile expiry. Possible values: ON, OFF Default value: OFF

heurExpiryThres

Threshold compression ratio for heuristic basefile expiry, multiplied by 100. For example, to set the threshold ratio to 1.25, specify 125. Default value: 100 Minimum value: 1 Maximum value: 1000

heurExpiryHistWt

For heuristic basefile expiry, weightage to be given to historical delta compression ratio, specified as percentage. For example, to give 25% weightage to historical ratio (and therefore 75% weightage to the ratio for current delta compression transaction), specify 25. Default value: 50 Minimum value: 1 Maximum value: 100

minResSize

Size of the smallest HTTP response that will be compressed. Default value: 0 Minimum value: 0

cmpBypassPct

CPU usage (%) at which NetScaler should start progressively bypassing compression on HTTP requests. Default value: 100 Minimum value: 0 Maximum value: 100

Example

set cmp param -cmpLevel bestspeed -quantumSize 20480

Related Commands

unset cmp parameter

show cmp parameter

unset cmp parameter

Synopsis

```
unset cmp parameter [-cmpLevel] [-quantumSize] [-
serverCmp] [-minResSize] [-cmpBypassPct]
```

Description

Use this command to remove cmp parameter settings.Refer to the set cmp parameter command for meanings of the arguments.

Related Commands

set cmp parameter

show cmp parameter

show cmp parameter

Synopsis

```
show cmp parameter
```

Description

Display configurable parameters for compression.

Arguments

format

level

Output

cmpLevel
Compression level.

quantumSize
Minimum amount of data to compress as one unit.

serverCmp
Compression enabled/disabled at back-end server.

heurExpiry
Heuristic basefile expiry.NOTE: This attribute is deprecated.Deprecating delta action in cmp policies

heurExpiryThres
Threshold compression ratio for heuristic basefile expiry, multiplied by 100. For example, to set the threshold ratio to 1.25, specify 125.NOTE: This attribute is deprecated.Deprecating delta action in cmp policies

heurExpiryHistWt
For heuristic basefile expiry, weightage to be given to historical delta compression ratio, specified as percentage. For example, to give 25% weightage to historical ratio (and therefore 75% weightage to the ratio for current delta compression transaction), specify 25.NOTE: This attribute is deprecated.Deprecating delta action in cmp policies

minResSize
Size of the smallest HTTP response that will be compressed.

cmpBypassPct
CPU usage (%) at which NetScaler should start progressively bypassing compression on HTTP requests.

Related Commands

set cmp parameter

unset cmp parameter

CHAPTER 12

Cache Redirection Commands

This chapter covers the cache redirection commands.

add cr policy

Synopsis

```
add cr policy <policyName> -rule <expression>
```

Description

Add a cache redirection policy. To associate the policy created with a cache redirection virtual server, use the ###bind cr vserver#### command.

Arguments

policyName

The name of the cache redirection policy.

rule

A condition defined by an expression. When the condition is valid, the request is directed to the origin server. Expression logic is: expression names, separated by the logical operators || and &&, and possibly grouped using parenthesis. Note:If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are valid expressions: l ns_ext_cgi||ns_ext_asp 2ns_non_get && (ns_header_cookie||ns_header_pragma)

Related Commands

add policy map

rm policy map

show policy map

add policy expression

rm policy expression

show policy expression

add cr vserver

bind cr vserver

set cr vserver

show cr vserver

unbind cr vserver

unset cr vserver

rm cr policy
set cr policy
show cr policy

rm cr policy

Synopsis

```
rm cr policy <policyName>
```

Description

Remove a Cache Redirection policy. You can delete a user-defined cache redirection policy that is not bound to a cache redirection virtual server. If the policy is bound to a virtual server, you must first unbind the policy, and then remove it from the system.

Arguments

policyName

The name of the cache policy to be removed. You cannot remove a positive cacheability policy/content group if it has been configured as the target of a dynamic invalidation policy. In this case, to remove the policy, you must use the following procedure, which removes the dynamic invalidation policy and the action associated with the dynamic invalidation policy: a.Enter the ###show cache action### command at the system prompt. This will display all cache actions. b.Identify the action in which the contentGroupPolicy attribute matches the policy you want to remove. Enter the ###show cache policy### command at the system prompt. c.Identify the policies that the action you chose in step (b) is associated with. d.Remove the policies you identified in step (c). Enter the ###rm cache policy### command. e.Remove the action you identified in step (b). Enter the ###rm cache action### command.

Related Commands

add policy map

rm policy map

show policy map

add policy expression

rm policy expression

show policy expression

add cr vserver

bind cr vserver

set cr vserver
show cr vserver
unbind cr vserver
unset cr vserver
add cr policy
set cr policy
show cr policy

set cr policy

Synopsis

```
set cr policy <policyName> -rule <expression>
```

Description

Changes the rule for a cache redirection policy.

Arguments

`policyName`

The name of the cache redirection policy.

`rule`

The condition defined by an expression. When the condition is valid, the request is directed to the origin server. Expression logic is: expression names, separated by the logical operators || and &&, and possibly grouped using parenthesis. Note:If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are valid expressions: l ns_ext_cgi||ns_ext_asp 2ns_non_get && (ns_header_cookie||ns_header_pragma)

Related Commands

add cr policy

rm cr policy

show cr policy

show cr policy

Synopsis

```
show cr policy [<policyName>]
```

Description

Display all existing cache redirection policies.

Arguments

policyName

The name of the cache redirection policy.

summary

fullValues

format

level

Output

rule

domain

Domain name.

vstype

Virtual server type.

Related Commands

add policy map
rm policy map
show policy map
add policy expression
rm policy expression
show policy expression
add cr vserver

bind cr vserver
set cr vserver
show cr vserver
unbind cr vserver
unset cr vserver
add cr policy
rm cr policy
set cr policy

add cr vserver

Synopsis

```
add cr vserver <name> <serviceType> [<IPAddress>
<port>  [-range <positive_integer>]] [-cacheType
<cacheType>] [-redirect <redirect>] [-onPolicyMatch (
CACHE | ORIGIN )] [-cltTimeout <secs>] [-precedence (
RULE | URL )] [-arp ( ON | OFF )] [-map ( ON | OFF )] [-
format ( ON | OFF )] [-via ( ON | OFF )] [-cacheVserver
<string>] [-dnsVserverName <string>] [-
destinationVServer <string>] [-domain <string>] [-
soPersistenceTimeOut <positive_integer>] [-soThreshold
<positive_integer>] [-reuse ( ON | OFF )] [-state (
ENABLED | DISABLED )] [-downStateFlush ( ENABLED |
DISABLED )] [-backupVServer <string>]
```

Description

Add a cache redirection virtual server.

Arguments

name

Name of the cache redirection virtual server.

serviceType

The type of service handled by the virtual server. Note:Use service type HTTP to configure content switching on this virtual server. Possible values: HTTP, SSL, NNTP

IPAddress

The IP address of the cache redirection virtual server. 1.To specify a specific virtual server address, type its numeric value. 2.To specify a wildcard virtual server address, type an asterisk (*).

cacheType

The supported cache server type. Note:For this command to work, you must select one of the cache types. Possible values: TRANSPARENT, REVERSE, FORWARD Default value: CRD_TRANSPARENT

redirect
The redirect policy. The valid redirect policies are: l.CACHE - Directs all requests to the cache. 2.POLICY - Applies the cache redirection policy to determine whether the request should be directed to the cache or to the origin. This is the default setting. 3.ORIGIN - Directs all requests to the origin server. Possible values: CACHE, POLICY, ORIGIN Default value: CRD_POLICY

onPolicyMatch
Decide where to redirect the requests if the cache redirection policy is hit. The valid options are: 1.CACHE - Directs all the requests to the cache if cache redirection policy is hit. 2.ORIGIN - Directs all requests to the origing server if the cache redirection policy is hit. Note: For this option to work, you must select the cache redirection type as POLICY. Possible values: CACHE, ORIGIN Default value: CRD_ORIGIN

cltTimeout
The timeout value in seconds for idle client connection Maximum value: 31536000

precedence
You can use this argument only when configuring content switching on the specified virtual server. This argument applies only if the URL- and RULE-based policies have both been configured on the same virtual server. This argument specifies the type of policy (URL or RULE) that takes precedence on the content switching virtual server. The default setting is RULE. lURL - In this case, the incoming request is matched against the URL-based policies before it is matched against the rule-based policies. lRULE - In this case, the incoming request is matched against the rule-based policies before it is matched against the URL-based policies. For all URL-based policies, the precedence hierarchy is: 1.Domain and exact URL 2.Domain, prefix and suffix 3.Domain and suffix 4.Domain and prefix 5.Domain only 6.Exact URL 7.Prefix and suffix 8.Suffix only 9.Prefix only 10.Default Possible values: RULE, URL Default value: CS_PRIORITY_RULE

arp

ghost

map

format

via
Determines whether the system will insert a Via: header in the HTTP requests. Possible values: ON, OFF Default value: ON

cacheVserver
The name of the default target cache virtual server to which requests are redirected.

dnsVserverName
The name of the DNS virtual server used to resolve domain names arriving at the forward proxy virtual server. Note:This parameter applies only to forward proxy virtual servers, not reverse and transparent.

destinationVServer
The destination virtual server for a transparent or forward proxy cache redirection virtual server. All requests to the transparent or forward proxy cache redirection virtual server are directed to this destination virtual server.

domain
The default domain for reverse proxies. Domains are configured in the system so that they direct an incoming request from a particular configured source domain to a particular configured target domain. There may be several configured pairs of source and target domains. You can select one pair to be the default. Then, if a source domain is not present in the host header or URL of an incoming request, the request will be sent to the target domain of the selected default pair.

soPersistenceTimeOut

soThreshold

reuse
Specifies whether TCP connections to cache or origin servers will be reused across client connections. Note:You should include this argument only if the service type argument is set to HTTP. The default setting is ON. If you set this argument to OFF and: -redirect is set to CACHE: TCP connections to the

cache servers are not reused. -redirect is set to ORIGIN: TCP connections to the origin servers are not reused. -redirect is set to POLICY: TCP connections to the origin servers are not reused. If you set this argument to ON, connections are reused to both origin and cache servers. Possible values: ON, OFF Default value: ON

`state`
The initial state (enabled or disabled) of the cache redirection virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

`downStateFlush`
Perform delayed cleanup of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

`backupVServer`
The Backup Virtual Server.

Related Commands

add policy map
rm policy map
show policy map
add policy expression
rm policy expression
show policy expression
rm cr vserver
set cr vserver
unset cr vserver
enable cr vserver
disable cr vserver
show cr vserver

stat cr vserver

rm cr vserver

Synopsis

```
rm cr vserver <name>@ ...
```

Description

Remove a virtual server.

Arguments

name

The name of the virtual server to be removed.

Example

rm vserver cr_vip

Related Commands

add cr vserver

set cr vserver

unset cr vserver

enable cr vserver

disable cr vserver

show cr vserver

stat cr vserver

set cr vserver

Synopsis

```
set cr vserver <name> [-IPAddress
<ip_addr|ipv6_addr|*>] [-redirect <redirect>] [-
onPolicyMatch ( CACHE | ORIGIN )] [-precedence ( RULE |
URL )] [-arp ( ON | OFF )] [-via ( ON | OFF )] [-
cacheVserver <string>] [-dnsVserverName <string>] [-
destinationVServer <string>] [-domain <string>] [-reuse
( ON | OFF )] [-backupVServer <string>] [-redirectURL
<URL>] [-cltTimeout <secs>] [-downStateFlush ( ENABLED
| DISABLED )]
```

Description

Change the attributes of a configured cache redirection vserver.

Arguments

`name`

Name of the cache redirection virtual server.

`IPAddress`

The new IP address of the virtual server.

`redirect`

The redirect policy. Possible values: CACHE, POLICY, ORIGIN Default value: CRD_POLICY

`onPolicyMatch`

Decide where to redirect the requests if the cache redirection policy is hit. The valid options are: 1.CACHE - Directs all the requests to the cache if cache redirection policy is hit. 2.ORIGIN - Directs all requests to the origing server if the cache redirection policy is hit. Note: For this option to work, you must select the cache redirection type as POLICY. Possible values: CACHE, ORIGIN Default value: CRD_ORIGIN

precedence
The type of policy (URL or RULE) that takes precedence on the content redirection virtual server. Possible values: RULE, URL Default value: CS_PRIORITY_RULE

arp

via
The state of the system in inserting a Via: header in the HTTP requests. Possible values: ON, OFF Default value: ON

cacheVserver
The name of the default target cache virtual server to which requests are to be redirected.

dnsVserverName
The name of the DNS virtual server to be used to resolve domain names arriving at the forward proxy virtual server.

destinationVServer
The destination virtual server for the transparent or forward proxy cache redirection virtual server.

domain
The default domain for reverse proxies.

reuse
The state of reuse of TCP connections to the cache or origin servers across client connections. Possible values: ON, OFF Default value: ON

backupVServer
The Backup Virtual Server.

redirectURL
The redirect URL.

cltTimeout
The client timeout value in seconds. Maximum value: 31536000

downStateFlush
Perform delayed cleanup of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

Related Commands

add cr vserver
rm cr vserver
unset cr vserver
enable cr vserver
disable cr vserver
show cr vserver

stat cr vserver

unset cr vserver

Synopsis

```
unset cr vserver <name> [-cacheVserver] [-dnsVserver]
[-destinationVServer] [-domainName] [-backupVServer]
[-redirectURL] [-redirect] [-onPolicyMatch] [-
precedence] [-arp] [-via] [-cacheVserver] [-
dnsVserverName] [-destinationVServer] [-domain] [-
reuse] [-cltTimeout] [-downStateFlush]
```

Description

Unset the attributes of the configured cache redirection virtual server. To set the cache redirection virtual server attributes, you can use either the ###add cr vserver### or the ###set cr vserver### command..Refer to the set cr vserver command for meanings of the arguments.

Related Commands

rm policy map
show policy map
rm policy expression
show policy expression
rm cr policy
show cr policy
add cr vserver
rm cr vserver
set cr vserver
enable cr vserver
disable cr vserver
show cr vserver

stat cr vserver

bind cr vserver

Synopsis

```
bind cr vserver <name> -policyName <string>
[<targetVserver>]
```

Description

For the system's cache redirection feature, this command binds the cache redirection policy to the cache redirection virtual server.

Arguments

name

The name of the cache redirection virtual server to which the cache redirection policy will be bound.

policyName

The name of the cache redirection policy. This policy must be of the type map or cache redirection policy (created using the ###add policy map### or ###add cr policy### commands).

Related Commands

unbind cr vserver

unbind cr vserver

Synopsis

```
unbind cr vserver <name> -policyName <string>
```

Description

This command unbinds a cache redirection policy from a cache redirection virtual server.

Arguments

name

The name of the cache redirection virtual server from which to unbind the policy.

policyName

The name of the policy (previously created using the ###add cr policy### or ###add policy map### command).

Related Commands

rm policy map

show policy map

rm policy expression

show policy expression

rm cr policy

show cr policy

bind cr vserver

enable cr vserver

Synopsis

```
enable cr vserver <name>@
```

Description

Enable a virtual server. Note:Virtual servers, when added, are enabled by default.

Arguments

name

The name of the virtual server to be enabled.

Example

enable vserver cr_vip

Related Commands

add cr vserver

rm cr vserver

set cr vserver

unset cr vserver

disable cr vserver

show cr vserver

stat cr vserver

disable cr vserver

Synopsis

```
disable cr vserver <name>@
```

Description

Disables a virtual server (takes it out of service).

Arguments

name

The name of the virtual server to be disabled. Notes: 1.The system still responds to ARP and/or ping requests for the IP address of this virtual server. 2.Because the virtual server is still configured in the system, you can enable the virtual server using the ###enable vserver### command.

Example

disable vserver cr_vip

Related Commands

add cr vserver

rm cr vserver

set cr vserver

unset cr vserver

enable cr vserver

show cr vserver

stat cr vserver

show cr vserver

Synopsis

```
show cr vserver [<name>]
```

Description

Display a specified cache redirection virtual server, or all configured cache redirection virtual servers.

Arguments

name

The name of the cache redirection virtual server.

summary

fullValues

format

level

Output

IPAddress

IPAddress

The IP address of the virtual server.

state

value

The ssl card status for the transparent ssl cr vserver.

port

range

serviceType

type
Virtual server type.

state
The state of the cr vserver.

status
Status.

cacheType

redirect

onPolicyMatch

precedence

redirectURL

authentication
Authentication.

homePage
Home page.

dnsVserverName

domain

rule
Rule.

policyName
Policies bound to this vserver.

serviceName
Service name.

weight
Weight for this service.

cacheVserver

backupVServer

priority
The priority for the policy.

cltTimeout

soMethod
The spillover factor. When the main virtual server reaches this spillover threshold, it will give further traffic to the backupvserver.

soPersistence
The state of spillover persistence.

soPersistenceTimeOut
The spillover persistence entry timeout.

soThreshold
The spillover threshold value.

reuse

arp

destinationVServer

via

downStateFlush
Perform delayed clean up of connections on this vserver.

Related Commands

add policy map
rm policy map
show policy map
add policy expression
rm policy expression
show policy expression
show cs policy
add cr vserver
rm cr vserver
set cr vserver
unset cr vserver
enable cr vserver
disable cr vserver

stat cr vserver

stat cr vserver

Synopsis

```
stat cr vserver [<name>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display cache redirection vserver statistics.

Arguments

name

The name of the vserver for which statistics will be displayed. If not given statistics are shown for all cr vservers.

Output

Counters

IP address (IP)

The ip address at which the service is running.

Port (port)

The port at which the service is running.

Vserver protocol (Protocol)

Protocol associated with the vserver

State

Current state of the server.

Requests (Req)

The total number of requests received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Responses (Rsp)

Number of responses received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Request bytes (Reqb)
The total number of request bytes received on this service/vserver.

Response bytes (Rspb)
Number of response bytes received on this service/vserver.

Related Commands

add cr vserver
rm cr vserver
set cr vserver
unset cr vserver
enable cr vserver
disable cr vserver
show cr vserver

CHAPTER 13

Content Switching Commands

This chapter covers the content switching commands.

add cs policy

Synopsis

```
add cs policy <policyName> [-url <string> | -rule
<expression>] [-domain <string>]
```

Description

Add a content switching policy. The policy created can be associated with a content switching virtual server using the bind cs vserver CLI command

Arguments

policyName

The name of the new content switching policy.

url

The URL, with wildcards. Specify the string value in this format: // [[prefix] [*]] [.suffix]

rule

The condition for applying this policy. Expression logic is as follows: - Expression names separated by the logical operators || and &&. - Expression names may be grouped using parenthesis. - If the expression contains blanks (e.g., between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following example shows valid expression logic: ns_ext_cgi||ns_ext_asp "ns_non_get && (ns_header_cookie||ns_header_pragma)"

domain

The domain name. The string value can range to 63 characters.

Example

To match the requests that have URL "/", you would enter the following command: add cs policy <policyName> -url / To match with all URLs that start with "/sports/", you would enter the following command: add cs policy <policyName> -url /sports/* To match requests with URLs that start with "/sports", you would enter the following command: add cs policy <policyName> -url /sports* To match requests with the URL "/sports/tennis/index.html", you would enter the following command: add cs policy

<policyName> -url /sports/tennis/index.html To match requests that have URLs with the extension "jsp", you would enter the following command: add cs policy <policyName> -url /*.jsp To match requests with URLs that start with "/sports/" and the file extension "jsp", you would enter the following command: add cs policy <policyName> -url /sports/*.jsp To match requests with URLs that contain "sports", you would enter the following commands: add pol expression sports_url "URL contains sports" add cs policy <policyName> -rule sports_url To match requests with URL queries that contain "gold" or cookie headers that contain "gold", you would enter the following commands: add pol expression gold_query "URLQUERY contains gold" add pol expression gold_cookie "Header COOKIE contains gold" add cs policy <policyName> -rule "(gold_query ||gold_cookie)" To match requests with the domain name www.domainxyz.com, you enter the following command: add cs policy <policyName> -domain "www.domainxyz.com" To match requests with the domain name www.domainxyz.com and URLs with the extension "jsp", you would enter the following command: add cs policy <policyName> -url /*.jsp -domain "www.domainxyz.com" To match requests with the domain name www.domainxyz.com and URLs that contain "sports", you would enter the following commands: add pol expression sports_url "URL contains sports" add cs policy <policyName> -rule sports_url -domain "www.domainxyz.com"

Related Commands

rm cs policy

set cs policy

unset cs policy

show cs policy

rm cs policy

Synopsis

```
rm cs policy <policyName>
```

Description

Remove the specified content switching policy. Note:The policy must be unbound from the content switching virtual server before it is removed.

Arguments

policyName

The name of the content switching policy to be removed.

Related Commands

add cs policy

set cs policy

unset cs policy

show cs policy

set cs policy

Synopsis

```
set cs policy <policyName> [-url <string> | -rule
<expression>] [-domain <string>]
```

Description

Change a previously configured content switching policy.

Arguments

policyName
Name of the policy.

url
The URL, with wildcards.

rule
The condition for applying this policy.

domain
The domain name.

Related Commands

add cs policy
rm cs policy
unset cs policy
show cs policy

unset cs policy

Synopsis

```
unset cs policy <policyName> [-url] [-rule] [-domain]
```

Description

Use this command to remove cs policy settings.Refer to the set cs policy command for meanings of the arguments.

Related Commands

add cs policy

rm cs policy

set cs policy

show cs policy

show cs policy

Synopsis

```
show cs policy [<policyName>]
```

Description

Display all of the content switching policies.

Arguments

policyName

The name of the policy to be displayed. if no name is given then all policies will be displayed.

summary

fullValues

format

level

Output

url

The URL with wildcards.

rule

The condition for applying this policy.

domain

The domain name.

vstype

Virtual server type.

hits

Total number of hits.

piHits

Total number of hits.

bindHits
Total number of hits.

labelName
Name of the label invoked.

labelType
The invocation type.

target
Target flag

priority
priority of bound policy

Related Commands

show cs vserver
add cs policy
rm cs policy
set cs policy
unset cs policy

add cs policylabel

Synopsis

```
add cs policylabel <labelName> <cspolicylabeltype>
```

Description

Add a content switching policy label.

Arguments

labelName

Name of the content switching policy label.

cspolicylabeltype

The type of the policy label. Possible values: HTTP, TCP, RTSP, SSL, SSL_TCP

Example

add cs policylabel trans_http_url HTTP

Related Commands

rm cs policylabel

bind cs policylabel

unbind cs policylabel

show cs policylabel

rm cs policylabel

Synopsis

```
rm cs policylabel <labelName>
```

Description

Remove a content switching policy label.

Arguments

labelName

Name of the content switching policy label.

Example

rm cs policylabel trans_http_url

Related Commands

add cs policylabel

bind cs policylabel

unbind cs policylabel

show cs policylabel

bind cs policylabel

Synopsis

```
bind cs policylabel <labelName> <policyName> <priority>
[-targetVserver <string> | -gotoPriorityExpression
<expression>] [-invoke  (<labelType>  <labelName>) ]
```

Description

Bind the content switching policy to one of the labels.

Arguments

labelName

Name of the content switching policy label.

policyName

Name of the policy to be bound to content switching policy label.

priority

Priority with which the policy is to be bound. Minimum value: 1 Maximum value: 2147483647

targetVserver

The virtual server name (created with the add lb vserver command) to which content will be switched.

gotoPriorityExpression

Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. o If gotoPriorityExpression is not present or if it is equal to END then the policy bank evaluation ends here o Else if the gotoPriorityExpression is equal to NEXT then the next policy in the priority order is evaluated. t o Else gotoPriorityExpression is evaluated. The result of gotoPriorityExpression (which has to be a number) is processed as follows: - An UNDEF event is triggered if . gotoPriorityExpression cannot be evaluated . gotoPriorityExpression evaluates to number which is smaller than the maximum priority in the policy bank but is not same as any policy's priority . gotoPriorityExpression evaluates to a priority that is smaller than the current policy's priority - If the gotoPriorityExpression evaluates to the priority of the current policy then

the next policy in the priority order is evaluated. - If the gotoPriorityExpression evaluates to the priority of a policy further ahead in the list then that policy will be evaluated next.

`invoke`

Invoke flag. Default value: NSAPI_PICON_INVOKE

Example

i) bind cs policylabel cs_lab lbvs_1 pol_cs 1 2

Related Commands

add cs policylabel

rm cs policylabel

unbind cs policylabel

show cs policylabel

unbind cs policylabel

Synopsis

```
unbind cs policylabel <labelName> <policyName>
```

Description

Unbind entities from content switching label.

Arguments

labelName

Name of the content switching policy label.

policyName

The name of the policy to be unbound.

Example

unbind cs policylabel cs_lab pol_cs

Related Commands

add cs policylabel

rm cs policylabel

bind cs policylabel

show cs policylabel

show cs policylabel

Synopsis

```
show cs policylabel [<labelName>]
```

Description

Display policy label or policies bound to content switching policylabel.

Arguments

labelName
Name of the content switching policy label.

summary

fullValues

format

level

Output

cspolicylabeltype
The type of the policy label.

state

numpol
number of polices bound to label.

hits
Number of times policy label was invoked.

policyName
Name of the content switching policy.

priority
Specifies the priority of the policy.

targetVserver
The virtual server name (created with the add lb vserver command) to which content will be switched.

gotoPriorityExpression
Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType
Type of policy label invocation.

labelName
Name of the label to invoke if the current policy rule evaluates to TRUE.

Example

i) show cs policylabel cs_lab ii) show cs policylabel

Related Commands

add cs policylabel
rm cs policylabel
bind cs policylabel
unbind cs policylabel

add cs vserver

Synopsis

```
add cs vserver <name> <serviceType> ((<IPAddress>  [-
range <positive_integer>]) | (-IPPattern <ippat>  -
IPMask <ipmask>)) <port> [-state ( ENABLED | DISABLED
)] [-stateupdate ( ENABLED | DISABLED )] [-cacheable (
YES | NO )] [-redirectURL <URL>] [-cltTimeout <secs>]
[-precedence ( RULE | URL )] [-caseSensitive ( ON | OFF
)] [-soMethod <soMethod>] [-soPersistence ( ENABLED |
DISABLED )] [-soPersistenceTimeOut <positive_integer>]
[-soThreshold <positive_integer>] [-
redirectPortRewrite ( ENABLED | DISABLED )] [-
downStateFlush ( ENABLED | DISABLED )] [-backupVServer
<string>] [-disablePrimaryOnDown ( ENABLED | DISABLED
)] [-insertVserverIPPort <insertVserverIPPort>
[<vipHeader>] ] [-rtspNat ( ON | OFF )] [-
AuthenticationHost <string>] [-Authentication ( ON |
OFF )] [-push ( ENABLED | DISABLED )] [-pushVserver
<string>] [-pushLabel <expression>] [-pushMultiClients
( YES | NO )]
```

Description

Add a content switching virtual server.

Arguments

name

The virtual server name. The name can be a maximum of 31 characters long.

serviceType

The service type of the virtual server. Possible values: HTTP, SSL, TCP, FTP, RTSP, SSL_TCP

IPAddress

The IP address of the virtual server.

IPPattern
The IP Pattern of the virtual server.

range
An IP address range. Default value: 1 Minimum value: 1

port
A port number for the virtual server. Minimum value: 1

state
The initial state, enabled or disabled, of the virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

stateupdate
To enable the state update for a CSW vserver Possible values: ENABLED, DISABLED Default value: DISABLED

cacheable
Use this option to specify whether a virtual server, used for load balancing or content switching, routes requests to the cache redirection virtual server before sending it to the configured servers. Possible values: YES, NO Default value: NO

redirectURL
The URL where traffic is redirected if the virtual server in the system becomes unavailable. You can enter up to 127 characters as the URL argument.WARNING!Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the add cs policy CLI command. If the same domain is specified in both arguments, the request will be continuously redirected to the same unavailable virtual server in the system - then the user may not get the requested content.

cltTimeout
The timeout value in seconds for idle client connection Maximum value: 31536000

precedence
This sets the precedence between RULE-based and URL-based policies on the content switching virtual server. The default precedence is RULE. With the precedence set to RULE, incoming requests are evaluated against the content switching policies created with the -rule argument (using the add cs policy CLI command). If none of the rules match, the URL in the request is

evaluated against the content switching policies created with the -url argument (using the add cs policy CLI command). Possible values: RULE, URL Default value: CS_PRIORITY_RULE

caseSensitive
The URL lookup case option on the content switching vserver. If the case sensitivity of a content switching virtual server is set to 'ON', the URLs /a/1.html and /A/1.HTML are treated differently, and can be switched to different targets with appropriate content switching policies. If the case sensitivity is set to 'OFF', the URLs /a/1.html and /A/1.HTML are treated the same, and are switched to the same target. Possible values: ON, OFF Default value: ON

soMethod
The spillover factor based on which the traffic will be given to the backupvserver once the main virtual server reaches the spillover threshold. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence
The state of the spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut

soThreshold
If the spillover method is set to CONNECTION or DYNAMICCONNECTION, this value is treated as the maximum number of connections a lb vserver will handle before spillover takes place. If the spillover method is set to BANDWIDTH, this value is treated as the amount of incoming and outgoing traffic (in Kbps) a vserver will handle before spillover takes place. Minimum value: 1 Maximum value: 0xFFFFFFF7

redirectPortRewrite
Enable port rewrite while performing HTTP redirect. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush
Perform delayed cleanup of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer
The backup virtual server for content switching.

disablePrimaryOnDown
When this argument is enabled, traffic will continue reaching backup vservers even after primary comes UP from DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort
The virtual IP and port header insertion option for the vserver. VIPADDR- Header contains the vserver's IP address and port number without any translation. OFF- The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4 address corresponding to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values: OFF, VIPADDR, V6TOV4MAPPING Default value: OFF

rtspNat
Use this parameter to enable natting for RTSP data connection. Possible values: ON, OFF Default value: OFF

AuthenticationHost
FQDN of authentication vserver Maximum value: 252

Authentication
This option toggles on or off the application of authentication of incoming users to the vserver. Possible values: ON, OFF Default value: OFF

push
Process traffic on bound Push vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver
The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

pushLabel
Use this parameter to specify the expression to extract the label in response from server. The string can be either a named expression (configured using add policy expression command) or else it can be an in-line expression with a maximum of 63 characters. Default value: "none"

pushMultiClients

Specify if multiple web 2.0 connections from the same client can connect to this vserver and expect updates. Possible values: YES, NO Default value: NO

Example

1.You can use precedence when certain client attributes (e.g., browser type) require to be served with different content. All other clients can then be served from content distributed among the servers. If the precedence is configured as URL, the incoming request URL is evaluated against the content switching policies created with the -url argument. If none of the policies match, the request is applied against the content any switching policies created with the -rule argument. 2.Precedence can also be used when certain content (such as images) is the same for all clients, but other content (such as text) is different for different clients. In this case, the images will be served to all clients, but the text will be served to specific clients based on attributes such as Accept-Language.

Related Commands

add cs policy

rm cs vserver

set cs vserver

unset cs vserver

enable cs vserver

disable cs vserver

show cs vserver

stat cs vserver

rm cs vserver

Synopsis

```
rm cs vserver <name>@ ...
```

Description

Remove a virtual server.

Arguments

name

The name of the virtual server to be removed.

Example

rm vserver cs_vip

Related Commands

add cs vserver

set cs vserver

unset cs vserver

enable cs vserver

disable cs vserver

show cs vserver

stat cs vserver

set cs vserver

Synopsis

```
set cs vserver <name> [-IPAddress
<ip_addr|ipv6_addr|*>] [-IPPattern <ippat>] [-IPMask
<ipmask>] [-stateupdate ( ENABLED | DISABLED )] [-
precedence ( RULE | URL )] [-caseSensitive ( ON | OFF
)] [-backupVServer <string>] [-redirectURL <URL>] [-
cacheable ( YES | NO )] [-cltTimeout <secs>] [-soMethod
<soMethod>] [-soPersistence ( ENABLED | DISABLED )] [-
soPersistenceTimeOut <positive_integer>] [-soThreshold
<positive_integer>] [-redirectPortRewrite ( ENABLED |
DISABLED )] [-downStateFlush ( ENABLED | DISABLED )] [-
disablePrimaryOnDown ( ENABLED | DISABLED )] [-
insertVserverIPPort <insertVserverIPPort>
[<vipHeader>] ] [-rtspNat ( ON | OFF )] [-
AuthenticationHost <string>] [-Authentication ( ON |
OFF )] [-push ( ENABLED | DISABLED )] [-pushVserver
<string>] [-pushLabel <expression>] [-pushMultiClients
( YES | NO )]
```

Description

Change the parameters of a content switching virtual server.

Arguments

name

Identifies the virtual server name (created with the add cs vserver command).

IPAddress

The new IP address of the virtual server.

IPPattern

The IP Pattern of the virtual server.

IPMask

The IP Mask of the virtual server IP Pattern

stateupdate
To enable the state update for a CSW vserver Possible values: ENABLED, DISABLED Default value: ENABLED

precedence
The precedence on the content switching virtual server between rule-based and URL-based policies. The default precedence is set to RULE. If the precedence is configured as RULE, the incoming request is applied against the content switching policies created with the -rule argument. If none of the rules match, then the URL in the request is applied against the content switching policies created with the -url option. For example, this precedence can be used if certain client attributes (such as a specific type of browser) need to be served different content and all other clients can be served from the content distributed among the servers. If the precedence is configured as URL, the incoming request URL is applied against the content switching policies created with the -url option. If none of the policies match, then the request is applied against the content switching policies created with the -rule option. Also, this precedence can be used if some content (such as images) is the same for all clients, but other content (such as text) is different for different clients. In this case, the images will be served to all clients, but the text will be served to specific clients based on specific attributes, such as Accept-Language. Possible values: RULE, URL Default value: CS_PRIORITY_RULE

caseSensitive
The URL lookup case option on the content switching vserver. If case sensitivity of a content switching virtual server is set to 'ON', the URLs /a/1.html and /A/1.HTML are treated differently and may have different targets (set by content switching policies). If case sensitivity is set to 'OFF', the URLs /a/1.html and /A/1.HTML are treated the same, and will be switched to the same target. Possible values: ON, OFF Default value: ON

backupVServer
The backup virtual server for content switching.

redirectURL
The redirect URL for content switching.

cacheable
The option to specify whether a virtual server used for content switching will route requests to the cache redirection virtual server before sending it to the configured servers. Possible values: YES, NO Default value: NO

cltTimeout
Client timeout in seconds. Maximum value: 31536000

soMethod
The spillover factor. When traffic on the main virtual server reaches this threshold, additional traffic is sent to the backupvserver. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence
The state of the spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut
The spillover persistency entry timeout. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold
If the spillover method is set to CONNECTION or DYNAMICCONNECTION, this value is treated as the maximum number of connections a lb vserver will handle before spillover takes place. If the spillover method is set to BANDWIDTH, this value is treated as the amount of incoming and outgoing traffic (in Kbps) a vserver will handle before spillover takes place. Minimum value: 1 Maximum value: 0xFFFFFFFE

redirectPortRewrite
SSL redirect port rewrite. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush
Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

disablePrimaryOnDown
When this argument is enabled, traffic will continue reaching backup vservers even after primary comes UP from DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort
The virtual IP and port header insertion option for the vserver. VIPADDR-Header contains the vserver's IP address and port number without any translation. OFF- The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4 address that corresponds to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values: OFF, VIPADDR, V6TOV4MAPPING Default value: OFF

rtspNat
Use this parameter to enable natting for RTSP data connection. Possible values: ON, OFF Default value: OFF

AuthenticationHost
FQDN of authentication vserver Maximum value: 252

Authentication
This option toggles on or off the application of authentication of incoming users to the vserver. Possible values: ON, OFF Default value: OFF

push
Process traffic on bound Push vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver
The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

pushLabel
Use this parameter to specify the expression to extract the label in response from server. The string can be either a named expression (configured using add policy expression command) or else it can be an in-line expression with a maximum of 63 characters. Default value: "none"

pushMultiClients
Specify if multiple web 2.0 connections from the same client can connect to this vserver and expect updates. Possible values: YES, NO Default value: NO

Related Commands

add cs policy

show cs policy

add cs vserver
rm cs vserver
unset cs vserver
enable cs vserver
disable cs vserver
show cs vserver

stat cs vserver

unset cs vserver

Synopsis

```
unset cs vserver <name> [-caseSensitive] [-
backupVServer] [-redirectURL] [-AuthenticationHost] [-
pushVserver] [-pushLabel] [-stateupdate] [-precedence]
[-cacheable] [-cltTimeout] [-soMethod] [-
soPersistence] [-soPersistenceTimeOut] [-soThreshold]
[-redirectPortRewrite] [-downStateFlush] [-
disablePrimaryOnDown] [-insertVserverIPPort] [-
vipHeader] [-rtspNat] [-Authentication] [-push] [-
pushMultiClients]
```

Description

Unset the parameters of a content switching virtual server..Refer to the set cs vserver command for meanings of the arguments.

Related Commands

add cs policy

show cs policy

add cs vserver

set cs vserver

rm cs vserver

enable cs vserver

disable cs vserver

show cs vserver

stat cs vserver

bind cs vserver

Synopsis

```
bind cs vserver <name> [<targetVserver>] [-policyName
<string>  [-priority <positive_integer>]  [-
gotoPriorityExpression <expression>]  [-type ( REQUEST
| RESPONSE )]  [-invoke  (<labelType>  <labelName>) ]
]
```

Description

Bind a content switching policy between a content-based virtual server and an address-based virtual server. You can assign multiple policies to the virtual server pair. Do not specify the optional policyName when adding a default policy on the content switching virtual server. When binding policies to the content-based virtual server, GotoPriorityExpression applies only to content switching policies with advance policy expression in the rule part. It also applies to rewrite and responder policies. Flowtype and invoke apply only to rewrite and responder policies.

Arguments

name

The virtual server name (created with the add cs vserver or add cr vserver command) for which the content switching policy will be set.

targetVserver

The virtual server name (created with the add lb vserver command) to which content will be switched.

Example

i) bind cs vserver csw-vip1 -policyname csw-policy1 -priority 13 ii) bind cs vserver csw-vip2 -policyname csw-ape-policy2 -priority 14 -gotoPriorityExpression NEXT iii) bind cs vserver csw-vip3 -policyname rewrite-policy1 -priority 17 -gotoPriorityExpression 'q.header("a").count' -flowtype REQUEST -invoke policylabel label1

Related Commands

add cs policy

show cs policy
unbind cs vserver

unbind cs vserver

Synopsis

```
unbind cs vserver <name> [-policyName <string>  [-type
( REQUEST | RESPONSE )]] [-priority <positive_integer>]
```

Description

Remove all content switching policies for the specified content switching virtual server. To remove the default policy, do not specify the optional policy name.

Arguments

`name`

The virtual server name (created with the add cs vserver or add cr vserver command) for which the content switching policy will be set.

`policyName`

The content switch policy name (created with the add cs policy command).

`priority`

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Related Commands

bind cs vserver

enable cs vserver

Synopsis

```
enable cs vserver <name>@
```

Description

Enable a virtual cs server. Note:Virtual servers, when added, are enabled by default.

Arguments

name

The name of the virtual server to be enabled.

Example

enable vserver cs_vip

Related Commands

add cs vserver

rm cs vserver

set cs vserver

unset cs vserver

disable cs vserver

show cs vserver

stat cs vserver

disable cs vserver

Synopsis

```
disable cs vserver <name>@
```

Description

Disable (makes out of service) a virtual cs server.

Arguments

name

The name of the virtual server to be disabled.

Example

disable vserver cs_vip

Related Commands

add cs vserver

rm cs vserver

set cs vserver

unset cs vserver

enable cs vserver

show cs vserver

stat cs vserver

show cs vserver

Synopsis

```
show cs vserver [<name>] show cs vserver stats - alias
for 'stat cs vserver'
```

Description

Display the list of content switching virtual servers configured in the system. To show the information for a particular virtual server and the content policies bound to that virtual server, enter the name of the content switching virtual server.

Arguments

name
The name of the content switching virtual server.

summary

fullValues

format

level

Output

insertVserverIPPort
The virtual IP and port header insertion option for the vserver.

vipHeader
The name of the virtual IP and port header.

IPAddress

IPAddress
The IP address of the virtual server.

IPPattern
The IP address of the virtual server.

IPMask
The IP address mask of the virtual server.

state

value
The ssl card status for the transparent ssl cs vserver.

port

range

serviceType

type
Virtual server type.

state
The state of the cs vserver.

sc
The state of SureConnect the specified virtual server.

stateupdate
To enable the state update for a CSW vserver

status
Status.

cacheType
Cache type.

redirect
Redirect URL string.

precedence

redirectURL
The redirect URL for content switching.

Authentication
Authentication.

caseSensitive

homePage
Home page.

dnsVserverName
DNS vserver name.

domain
Domain.

rule
Rule.

policyName
Policies bound to this vserver.

hits
Number of hits.

serviceName
Service name.

weight
Weight for this service.

cacheVserver
Cache vserver name.

backupVServer

priority
Priority for the policy.

cltTimeout

soMethod

soPersistence

soPersistenceTimeOut

soThreshold
If the spillover method is set to CONNECTION or DYNAMICCONNECTION, this value is treated as the maximum number of connections a lb vserver will handle before spillover takes place. If the spillover method is set to BANDWIDTH, this value is treated as the amount of incoming and outgoing traffic (in Kbps) a vserver will handle before spillover takes place.

cacheable
The state of caching.

url
URL string.

gotoPriorityExpression
Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

redirectPortRewrite
Redirect port rewrite.

downStateFlush
Perform delayed clean up of connections on this vserver.

disablePrimaryOnDown
Tells whether traffic will continue reaching backup vservers even after primary comes UP from DOWN state.

type
The bindpoint to which the policy is bound

invoke
Invoke flag.

labelType
The invocation type.

labelName
Name of the label invoked.

gt2GB
This argument has no effect.

stateChangeTimeSec
Time when last state change happened. Seconds part.

stateChangeTimemSec
Time at which last state change happened. Milliseconds part.

ticksSinceLastStateChange
Time in 10 millisecond ticks since the last state change.

rtspNat
Use this parameter to enable natting for RTSP data connection.

AuthenticationHost
FQDN of authentication vserver

push
Process traffic on bound Push vserver.

pushVserver
The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

pushLabel
Use this parameter to specify the expression to extract the label in response from server. The string can be either a named expression (configured using add policy expression command) or else it can be an in-line expression with a maximum of 63 characters.

pushMultiClients
Specify if multiple web 2.0 connections from the same client can connect to this vserver and expect updates.

Related Commands

show cs policy

add cs vserver

rm cs vserver

set cs vserver
unset cs vserver
enable cs vserver
disable cs vserver

stat cs vserver

stat cs vserver

Synopsis

```
stat cs vserver [<name>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display content switch vserver statistics.

Arguments

name

The name of the vserver for which statistics will be displayed. If not given statistics are shown for all cs vservers.

Output

Counters

IP address (IP)

The ip address at which the service is running.

Port (port)

The port at which the service is running.

Vserver protocol (Protocol)

Protocol associated with the vserver

State

Current state of the server.

Requests (Req)

The total number of requests received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Responses (Rsp)

Number of responses received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Request bytes (Reqb)
The total number of request bytes received on this service/vserver.

Response bytes (Rspb)
Number of response bytes received on this service/vserver.

Labelled Connection (LblConn)
Number of Labelled connection on this vserver

Push Labelled Connection (PushLbl)
Number of labels for this push vserver.

Deferred Request (DefReq)
Number of deferred request on this vserver

Related Commands

add cs vserver
rm cs vserver
set cs vserver
unset cs vserver
enable cs vserver
disable cs vserver
show cs vserver

CHAPTER 14

DNS Commands

This chapter covers the DNS commands.

flush dns proxyRecords

Synopsis

```
flush dns proxyRecords
```

Description

Flush all the DNS proxy records.

Related Commands

stat dns

Synopsis

```
stat dns [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display DNS statistics.

Arguments

Output

Counters

Dns queries (Q)
Total number of DNS queries received.

NS queries (NSQ)
Total number of NS queries received.

SOA queries (SOAQ)
Total number of SOA queries received.

PTR queries (PTRQ)
Total number of PTR queries received.

SRV queries (SRVQ)
Total number of SRV queries received.

Multi queries (MtQ)
Total number of Multi Query request received.

Dns responses (Rsp)
Total number of DNS responses received

A responses (ARsp)
Total number of A responses received.

CNAME responses (CNRsp)
Total number of CNAME responses received.

MX responses (MXRsp)
Total number of MX responses received.

Server responses (SvrRsp)
Total number of Server responses received.

ANY responses (ANYRsp)
Total number of ANY responses received.

NS updates (NSUp)
Total number of NS record updates.

SOA updates (SOAUp)
Total number of SOA record updates.

PTR updates (PTRUp)
Total number of PTR record updates.

SRV updates (SRVUp)
Total number of SRV record updates.

Total Record updates (TotRecUp)
Total number of record updates.

Cache entries flushed (CaEntFsh)
Total number of cache entries flushed.

Auth answers (AuthAns)
Number of queries which were authoritatively answered.

AAAA queries (AAAAQ)
Total number of AAAA queries received.

A queries (AQ)
Total number of A queries received.

CNAME queries (CNQ)
Total number of CNAME queries received.

MX queries (MXQ)
Total number of MX queries received.

ANY queries (ANYQ)
Total number of ANY queries received.

Server queries (SvrQ)
Total number of Server queries sent.

AAAA responses (AAAARsp)
Total number of AAAA responses received.

NS responses (NSRsp)
Total number of NS responses received.

SOA responses (SOARsp)
Total number of SOA responses received.

PTR responses (PTRRsp)
Total number of PTR responses received.

SRV responses (SRVRsp)
Total number of SRV responses received.

AAAA updates (AAAAUp)
Total number of AAAA record updates.

A updates (AUp)
Total number of A record updates.

MX updates (MXUp)
Total number of MX record updates.

CNAME updates (CNUp)
Total number of CNAME record updates.

Cache flush called (CaFsh)
Total number of times cache was flushed.

AAAA records (AAAARec)
Total number of AAAA records.

A records (ARec)
Total number of A records.

MX records (MXRec)
Total number of MX records.

CNAME records (CNRec)
Total number of CNAME records.

Non-authoritative entries (PxyEnt)
Total number of non-authoritative entries.

NS records (NSRec)
Total number of NS records.

SOA records (SOARec)
Total number of SOA records.

PTR records (PTRRec)
Total number of PTR records.

SRV records (SRVRec)
Total number of SRV records.

Authoritative entries (AthEnt)
Total number of authoritative entries.

Nonexistent domain (NoDomain)
Number of queries for which no record was found.

No AAAA records (NoAAAARec)
Total number of times AAAA record lookup failed.

No A records (NoARec)
Total number of times A record lookup failed.

No MX records (NoMXRec)
Total number of times MX record lookup failed.

No PTR records (NoPTRRec)
Total number of times PTR record lookup failed.

Unsupported queries (NotSupQ)
Total number of requests for which query type requested was unsupported.

Response class unsupported (RspClsEr)
Total number of responses for which response types were unsupported.

Invalid query format (InQFmt)
Total number of queries whose format was invalid.

Stray answers (StryRsp)
Total number of stray answers.

Incorrect RD length (BadRDlen)
Number of DNS responses received with invalid resoure data length.

Requests refused (ReqRefused)
Number of DNS requests refused.

No NS records (NoNSRec)
Total number of times NS record lookup failed.

No CNAME records (NoCNRec)
Total number of times CNAME record lookup failed.

No SOA records (NoSOARec)
Total number of times SOA record lookup failed.

No SRV records (NoSRVRec)
Total number of times SRV record lookup failed.

No ANY records (NoANYrec)
Total number of times ANY query lookup failed.

Response type unsupported (RspNoSup)
Total number of responses for which response type requested was unsupported.

Query class unsupported (QClsEr)
Total number of queries for which query class was unsupported.

Invalid response format (InRspFmt)
Total number of responses for which there was a format error.

No answer responses (NoAnswer)
Number of DNS responses received without answer.

Multi queries disabled (MtQErr)
Total number of times a multi query was disabled and received a multi query.

Other errors (OtherErr)
Total number of other errors.

Related Commands

show dns stats

Synopsis

```
show dns stats - alias for 'stat dns'
```

Description

show dns stats is an alias for stat dns

Related Commands

stat dns

add dns aaaaRec

Synopsis

```
add dns aaaaRec <hostName> <IPv6Address> ... [-TTL
<secs>]
```

Description

Add an AAAA address record for the specified domain name.

Arguments

hostName

The domain name for which the address record is added.

IPv6Address

Specify one or more IP addresses for the domain name.

TTL

Specify the time to live, in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Example

add dns aaaarec www.mynw.com 3::4:5 -ttl 10

Related Commands

rm dns aaaaRec

show dns aaaaRec

rm dns aaaaRec

Synopsis

```
rm dns aaaaRec <hostName> [<IPv6Address> ...]
```

Description

This command removes the specified IPv6 address from the address record for the given domain name. If IPv6 address is not specified, the entire address record for the given domain name is removed.

Arguments

hostName

The host name for which the AAAA record is to be removed.

IPv6Address

Specify one or more IPv6 addresses for the AAAA record to be removed. If all IPv6 records within a domain are removed, the domain name entry is also removed.

Example

rm dns aaaarec www.mynw.com

Related Commands

add dns aaaaRec

show dns aaaaRec

show dns aaaaRec

Synopsis

```
show dns aaaaRec [<hostName> | -type <type>]
```

Description

Show the IPv6 address0 record for the specified host name. If a host name is not specified, all IPv6 address records are displayed.

Arguments

hostName

The domain name for which the address record is to be displayed.

type

Specify the address record type. The record type can take 3 values: ADNS - If this is specified, all of the authoritative address records will be displayed. PROXY - If this is specified, all of the proxy address records will be displayed. ALL - If this is specified, all of the address records will be displayed. Possible values: ALL, ADNS, PROXY

summary

fullValues

format

level

Output

IPv6Address

TTL

authType

Authentication type.

Related Commands

add dns aaaaRec

rm dns aaaaRec

add dns addRec

Synopsis

```
add dns addRec <hostName> <IPAddress> ... [-TTL <secs>]
```

Description

Add an address record for the specified domain name.

Arguments

hostName

The domain name for which the address record is being added.

IPAddress

One or more IP addresses for the domain name.

TTL

Time to live, in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Example

Add dns addrec www.mynw.com 65.200.211.139 -ttl 10

Related Commands

rm dns addRec

show dns addRec

rm dns addRec

Synopsis

```
rm dns addRec <hostName> [<IPAddress> ...]
```

Description

Remove the specified ipaddress from the address record for the given domain name. If IP address is not specified, the entire address record for the given domain name is removed.

Arguments

hostName

The host name for which the address record is to be removed.

IPAddress

One or more IP addresses for the address record to be removed. If all address records within a domain are removed, the domain name entry is also removed.

Example

rm dns addrec www.mynw.com

Related Commands

add dns addRec

show dns addRec

show dns addRec

Synopsis

```
show dns addRec [<hostName> | -type <type>]
```

Description

Display the address record for the specified host name. If a host name is not specified, all address records are displayed.

Arguments

hostName
The domain name.

type
The address record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative address records will be displayed. PROXY - If this is specified, all of the proxy address records will be displayed. ALL - If this is specified, all of the address records will be displayed. Possible values: ALL, ADNS, PROXY

summary

fullValues

format

level

Output

IPAddress
IP addresses for the domain name.

TTL
The time to live, in seconds.

vServerName
Vitual server name.

authType
Authentication type.

Related Commands

add dns addRec

rm dns addRec

add dns cnameRec

Synopsis

```
add dns cnameRec <aliasName> <canonicalName> [-TTL
<secs>]
```

Description

Add a canonical name record.

Arguments

aliasName

Alias name for the specified domain.

canonicalName

The domain for which cnamerec is created.

TTL

Time to live, in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Example

add dns cnameRec www.mynw.org www.mynw.com -ttl 20

Related Commands

rm dns cnameRec

show dns cnameRec

rm dns cnameRec

Synopsis

```
rm dns cnameRec <aliasName>
```

Description

Remove the canonical name record.

Arguments

aliasName

The name of the alias to be removed.

Example

rm dns cnamerec www.mynw.org

Related Commands

add dns cnameRec

show dns cnameRec

show dns cnameRec

Synopsis

```
show dns cnameRec [<aliasName> | -type <type>]
```

Description

Display the cname records. If no alias name is specified, all "cname" records are displayed.

Arguments

aliasName

The alias name. If an alias name is not specified, all "cname" records are displayed.

type

The cname record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative cname records will be displayed. PROXY - If this is specified, all of the proxy cname records will be displayed. ALL - If this is specified, all of the cname records will be displayed. Possible values: ALL, ADNS, PROXY Default value: NSDNS_AUTH_HOST

summary

fullValues

format

level

Output

canonicalName

TTL

Time to live, in seconds.

Example

show dns cnameRec www.mynw.org

Related Commands

add dns cnameRec

rm dns cnameRec

add dns mxRec

Synopsis

```
add dns mxRec <domain> -mx <string> -pref
<positive_integer> [-TTL <secs>]
```

Description

Add the DNS mail exchange (MX) record.

Arguments

domain

The domain for which the added MX record is added.

mx

The MX record name.

pref

The route priority number. Note:A domain name can have multiple mail routes, with a priority number assigned to each. The mail route with the lowest number identifies the server responsible for the domain. Other mail servers listed are used as backups. Minimum value: 0 Maximum value: 65535

TTL

Time to live, in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Related Commands

rm dns mxRec

set dns mxRec

unset dns mxRec

show dns mxRec

rm dns mxRec

Synopsis

```
rm dns mxRec <domain> <mx>
```

Description

Remove the DNS mail exchange record.

Arguments

`domain`

The domain for the mail exchange record to be removed.

`mx`

The mail exchange record name.

Related Commands

add dns mxRec

set dns mxRec

unset dns mxRec

show dns mxRec

set dns mxRec

Synopsis

```
set dns mxRec <domain> -mx <string> [-pref
<positive_integer>] [-TTL <secs>]
```

Description

Set the DNS MX (mail exchange) record parameters.

Arguments

domain

The domain to be associated with the MX record.

mx

The name of the MX record.

pref

The priority number of the domain's mail route. Because one domain name can have multiple mail routes, you must specify a priority number for each domain's route. The mail route with the lowest number identifies the server responsible for the domain. Other mail servers listed are used as backups. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 65535

TTL

The time to live, in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Related Commands

add dns mxRec

rm dns mxRec

unset dns mxRec

show dns mxRec

unset dns mxRec

Synopsis

```
unset dns mxRec <domain> -TTL
```

Description

Use this command to remove dns mxRec settings.Refer to the set dns mxRec command for meanings of the arguments.

Related Commands

add dns mxRec

rm dns mxRec

set dns mxRec

show dns mxRec

show dns mxRec

Synopsis

```
show dns mxRec [<domain> | -type <type>]
```

Description

Display the mail exchange (MX) record for the specified domain. If a domain name is not specified, all mail exchange records are displayed.

Arguments

domain

The domain name.

type

The MX record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative MX records will be displayed. PROXY - If this is specified, all of the proxy MX records will be displayed. ALL - If this is specified, all of the MX records will be displayed. Possible values: ALL, ADNS, PROXY Default value: NSDNS_AUTH_HOST

summary

fullValues

format

level

Output

mx

pref

TTL

Related Commands

add dns mxRec

rm dns mxRec

set dns mxRec

unset dns mxRec

add dns nsRec

Synopsis

```
add dns nsRec <domain> <nameServer> [-TTL <secs>]
```

Description

Add the name server record for a given domain name.

Arguments

domain

The domain name for which a name server record is added.

nameServer

The nameserver for the domain.

TTL

Time to live, in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Related Commands

rm dns nsRec

show dns nsRec

rm dns nsRec

Synopsis

```
rm dns nsRec <domain> <nameServer>
```

Description

Remove the name server record for a domain.

Arguments

`domain`

The domain name whose name server record is to be removed.

`nameServer`

The name server for the domain to be removed.

Related Commands

add dns nsRec

show dns nsRec

show dns nsRec

Synopsis

```
show dns nsRec [<domain> | -type <type>]
```

Description

Display the name server record for a domain. If no domain name is specified, all of the name server records are displayed.

Arguments

domain

The domain name for the name server record.

type

The name server record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative name server records will be displayed. PROXY - If this is specified, all of the proxy name server records will be displayed. ALL - If this is specified, all of the name server records will be displayed. Possible values: ALL, ADNS, PROXY

summary

fullValues

format

level

Output

nameServer

TTL

Related Commands

add dns nsRec

rm dns nsRec

add dns ptrRec

Synopsis

```
add dns ptrRec <reverseDomain> <domain> ... [-TTL
<secs>]
```

Description

Add a PTR record for the specified reverse domain name.

Arguments

reverseDomain

Reverse domain name with suffixes, e.g.: in-addr.arpa. or ip6.arpa..

domain

The domain name for which reverse mapping is being done.

TTL

Time to live, in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Example

add dns ptrrec 1.1.1.in-addr.arpa. abc.com

Related Commands

rm dns ptrRec

show dns ptrRec

rm dns ptrRec

Synopsis

```
rm dns ptrRec <reverseDomain> [<domain> ...]
```

Description

Remove a PTR record corresponding to a given reverse domain name and domain name.

Arguments

`reverseDomain`

The reverse domain name of the PTR record being removed.

`domain`

The domain name whose reverse mapping is being removed.

Example

rm dns ptrrec 1.1.1.1.in-addr.arpa. ptr.com

Related Commands

add dns ptrRec

show dns ptrRec

show dns ptrRec

Synopsis

```
show dns ptrRec [<reverseDomain> | -type <type>]
```

Description

Display the PTR record for the specified reverse domain name and domain name.

Arguments

reverseDomain

The reverse domain name of the PTR record being displayed.

type

PTR record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative ptr records will be displayed. PROXY - If this is specified, all of the proxy ptr records will be displayed. ALL - If this is specified, all of the ptr records will be displayed. Possible values: ALL, ADNS, PROXY

summary

fullValues

format

level

Output

domain

The domain name for which reverse mapping is being done.

TTL

Time to live, in seconds.

authType

Authentication type.

Related Commands

add dns ptrRec

rm dns ptrRec

add dns srvRec

Synopsis

```
add dns srvRec <domain> <target> -priority
<positive_integer> -weight <positive_integer> -port
<positive_integer> [-TTL <secs>]
```

Description

Add an SRV record for the specified domain name.

Arguments

domain

The domain name that is offering the services. The domain name includes the service offered and transport layer protocol, e.g.: _ftp._tcp.abc.com.

target

The target host that is hosting the specified service.

priority

The target host priority. This helps in server selection by the client. Minimum value: 0 Maximum value: 65535

weight

Weight for the target host. This helps in server selection by the client in case of same priority Minimum value: 0 Maximum value: 65535

port

Port on which the target host is listening for client requests. Minimum value: 0 Maximum value: 65535

TTL

The time to live, measured in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Related Commands

rm dns srvRec

set dns srvRec

unset dns srvRec

show dns srvRec

rm dns srvRec

Synopsis

```
rm dns srvRec <domain> <target> ...
```

Description

Remove the SRV record for a given domain name and target.

Arguments

domain

The domain name of the SRV record to be removed.

target

The target host that is hosting the service to be removed.

Related Commands

add dns srvRec

set dns srvRec

unset dns srvRec

show dns srvRec

set dns srvRec

Synopsis

```
set dns srvRec <domain> <target> [-priority
<positive_integer>] [-weight <positive_integer>] [-
port <positive_integer>] [-TTL <secs>]
```

Description

Set the SRV record attributes.

Arguments

`domain`
The domain name for which the service is configured.

`target`
The target host that is hosting the service whose attributes are to be changed

`priority`
Priority of the target host. This helps in server selection by the client. Minimum value: 0 Maximum value: 65535

`weight`
Weight for the target host. This helps in server selection by the client in case of same priority Minimum value: 0 Maximum value: 65535

`port`
Port on which the target host is listening for client requests. Minimum value: 0 Maximum value: 65535

`TTL`
The time to live, measured in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Related Commands

add dns srvRec

rm dns srvRec

unset dns srvRec

show dns srvRec

unset dns srvRec

Synopsis

```
unset dns srvRec <domain> <target> -TTL
```

Description

Use this command to remove dns srvRec settings.Refer to the set dns srvRec command for meanings of the arguments.

Related Commands

add dns srvRec

rm dns srvRec

set dns srvRec

show dns srvRec

show dns srvRec

Synopsis

```
show dns srvRec [(<domain>  [<target>]) | -type <type>]
```

Description

Display the SRV record for the specified domain. If the domain name is not specified, all of the SRV records are displayed.

Arguments

`domain`

The domain name for which the SRV record will be displayed.

`target`

The target host that is hosting the service whose attributes are to be displayed

`type`

SRV record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative SRV records will be displayed. PROXY - If this is specified, all of the proxy SRV records will be displayed. ALL - If this is specified, all of the SRV records will be displayed. Possible values: ALL, ADNS, PROXY

`summary`

`fullValues`

`format`

`level`

Output

`priority`

Priority of the target host. This helps in server selection by the client.

`weight`

Weight for the target host. This helps in server selection by the client in case of same priority

port
Port on which the target host is listening for client requests.

TTL
The time to live, measured in seconds.

Related Commands

add dns srvRec
rm dns srvRec
set dns srvRec
unset dns srvRec

set dns parameter

Synopsis

```
set dns parameter [-retries <positive_integer>] [-
minTTL <secs>] [-maxTTL <secs>] [-cacheRecords ( YES |
NO )] [-nameLookupPriority ( WINS | DNS )] [-recursion
( ENABLED | DISABLED )]
```

Description

Set TTL parameters.

Arguments

retries

The DNS resolver request retry count. Default value: 5 Minimum value: 1 Maximum value: 5

minTTL

The minimum time to live value, in seconds. If any DNS entry has a time to live value of less than the minimum, it is saved as the minimum time to live value. Minimum value: 0 Maximum value: 604800

maxTTL

The maximum time to live value allowed, in seconds. If the DNS entry has a time to live value of more than the maximum, it is saved as the maximum time to live value. Default value: 604800 Minimum value: 1 Maximum value: 604800

cacheRecords

The state of dns records caching. Possible values: YES, NO Default value: ENABLED

nameLookupPriority

The name lookup priority, as DNS or WINS. Possible values: WINS, DNS Default value: NS_WINSFIRST

recursion

Allow recursive name resolution by NetScaler. Possible values: ENABLED, DISABLED Default value: DISABLED

Related Commands

unset dns parameter

show dns parameter

unset dns parameter

Synopsis

```
unset dns parameter [-retries] [-minTTL] [-maxTTL] [-
cacheRecords] [-nameLookupPriority] [-recursion]
```

Description

Use this command to remove dns parameter settings.Refer to the set dns parameter command for meanings of the arguments.

Related Commands

set dns parameter

show dns parameter

show dns parameter

Synopsis

```
show dns parameter
```

Description

Display dns parameter. Displays the following value: DNS Retries - The DNS resolver request timeout. minTTL - The minimum allowed value for time to live. If a DNS entry has a time to live value less than the minimum, it is saved as the minimum time to live. maxTTL - The maximum allowed value for time to live. If any DNS entry has a time to live value less than the maximum, it is saved as the maximum time to live.

Arguments

format

level

Output

retries

minTTL

maxTTL

nameLookupPriority

cacheRecords

recursion

Related Commands

set dns parameter

unset dns parameter

add dns soaRec

Synopsis

```
add dns soaRec <domain> -originServer <string> -contact
<string> [-serial <positive_integer>] [-refresh <secs>]
[-retry <secs>] [-expire <secs>] [-minimum <secs>] [-
TTL <secs>]
```

Description

Add the Start of Authority (SOA) record.

Arguments

domain

The domain name for which the SOA record is added.

originServer

The name of the origin server for the given domain.

contact

The contact person for this ADNS. Typically this is an email address for which the at sign (@) has been replaced by a period (.).

serial

The secondary server uses this parameter to determine if it requires a zone transfer from the primary server. If the secondary server's number is lower than the primary's, the secondary server knows that its records are out of date. This parameter is not used by a primary server. Default value: 100 Minimum value: 0 Maximum value: 0xFFFFFFFE

refresh

The number of seconds between a successful serial number check on the primary server's zone, and the next attempt. It is usually 2-24 hours. This value is not used by a primary server. Default value: 3600 Minimum value: 0 Maximum value: 0xFFFFFFFE

retry
When a refresh attempt fails, a server will retry after the specified number of seconds. This parameter is not used by a primary server. Default value: 3 Minimum value: 0 Maximum value: 0xFFFFFFFE

expire
Measured in seconds. If the refresh and retry attempts fail after the specified number of seconds, the server will stop serving the zone. The typical value is 1 week. This parameter is not used by a primary server. Default value: 3600 Minimum value: 0 Maximum value: 0xFFFFFFFE

minimum
The default TTL for every record in the zone. You can override this value for a particular record. Typical values range from eight hours to four days. This value is often set at ten minutes or less when changes are being made to a zone. Default value: 5 Minimum value: 0 Maximum value: 2147483647

TTL
The time to live, in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Related Commands

rm dns soaRec

set dns soaRec

unset dns soaRec

show dns soaRec

rm dns soaRec

Synopsis

```
rm dns soaRec <domain>
```

Description

Remove the Start of Authority (SOA) record for a given domain name.

Arguments

domain

The domain name for the SOA record to be removed.

Related Commands

add dns soaRec

set dns soaRec

unset dns soaRec

show dns soaRec

set dns soaRec

Synopsis

```
set dns soaRec <domain> [-originServer <string>] [-
contact <string>] [-serial <positive_integer>] [-
refresh <secs>] [-retry <secs>] [-expire <secs>] [-
minimum <secs>] [-TTL <secs>]
```

Description

Set the DNS Start Of Authority (SOA) record attributes.

Arguments

domain

The domain name for which the SOA record attributes are set.

originServer

The origin server name for the given domain.

contact

The contact person for this ADNS. Typically it is the email address, with the at sign (@) replaced by a period (.).

serial

The secondary server number. This number is used by a secondary server to determine if it requires a zone transfer from the primary server. If the secondary server's number is lower than the primary's, the secondary server determines that its records are out of date. This parameter is not used by a primary server. Default value: 100 Minimum value: 1

refresh

The refresh time in seconds. Refresh determines the number of seconds between a successful check on the serial number on the zone of the primary, and the next attempt (usually 2-24 hours). This parameter is used by a primary server. Default value: 3600 Minimum value: 0 Maximum value: 0xFFFFFFFE

retry
The retry time in seconds. If a refresh attempt fails, a server will retry after the specified number of seconds. Not used by a primary server. Default value: 3 Minimum value: 0 Maximum value: 0xFFFFFFFE

expire
The expire time in seconds. If the refresh and retry attempts fail after the specified number of seconds, the server will stop serving the zone. The typical value is 1 week. Not used by a primary server. Default value: 3600 Minimum value: 0 Maximum value: 0xFFFFFFFE

minimum
The default TTL for every record in the zone. You can override this value for a specific record. Typical values range from eight hours to four days. This value is often set to 10 minutes or less when changes are being made to a zone. Default value: 5 Minimum value: 0 Maximum value: 2147483647

TTL
The time to live, measured in seconds. Default value: 3600 Minimum value: 0 Maximum value: 2147483647

Related Commands

add dns soaRec

rm dns soaRec

unset dns soaRec

show dns soaRec

unset dns soaRec

Synopsis

```
unset dns soaRec <domain> [-serial] [-refresh] [-retry]
[-expire] [-minimum] [-TTL]
```

Description

Use this command to remove dns soaRec settings.Refer to the set dns soaRec command for meanings of the arguments.

Related Commands

add dns soaRec

rm dns soaRec

set dns soaRec

show dns soaRec

show dns soaRec

Synopsis

```
show dns soaRec [<domain> | -type <type>]
```

Description

Display the specified Start of Authority record. If the domain name is not specified, all of the SOA records are displayed.

Arguments

domain

The domain name.

type

The SOA record type. The type can take 3 values : ADNS - If this is specified, all of the authoritative SOA records will be displayed. PROXY - If this is specified, all the proxy SOA records will be displayed. ALL - If this is specified, all the SOA records will be displayed. Possible values: ALL, ADNS, PROXY

summary

fullValues

format

level

Output

originServer

contact

serial

refresh

retry

expire

minimum

TTL

Related Commands

add dns soaRec
rm dns soaRec
set dns soaRec
unset dns soaRec

add dns suffix

Synopsis

```
add dns suffix <dnsSuffix>
```

Description

Append suffixes while resolving the domain names.

Arguments

dnsSuffix

Suffix to be appended while resolving the domain name.

Example

add dns suffix netscaler.com If the incoming domain name "engineering" is not resolved by itself, the system will append the suffix netscaler.com and attempt to resolve the name engineering.netscaler.com.

Related Commands

rm dns suffix

show dns suffix

rm dns suffix

Synopsis

```
rm dns suffix <dnsSuffix>
```

Description

Remove the DNS suffixes.

Arguments

dnsSuffix

Suffix name to be removed.

Related Commands

add dns suffix

show dns suffix

show dns suffix

Synopsis

```
show dns suffix [<dnsSuffix>]
```

Description

Display all the configured DNS suffixes.

Arguments

dnsSuffix

summary

fullValues

format

level

Output

Related Commands

add dns suffix

rm dns suffix

add dns nameServer

Synopsis

```
add dns nameServer ((<IP>  [-local]) |
<dnsVserverName>) [-state ( ENABLED | DISABLED )]
```

Description

Add a name server. Two types of name servers can be added: 1.IP Address-based name server. In this case, the user must specify the Ipaddress of the name server to be contacted. 2.Vserver-based name server. In this case, the user must specify the name of the DNS vserver configured in the System.

Arguments

IP

The IP address of the name server.

dnsVserverName

The name of the dns vserver

local

IP is a local recursive nameserver. Default value: NSAPSET_LOCALFLAG

state

The administrative state of the nameserver. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

Adding an-IP based nameserver IP: add nameserver 10.102.4.1, Adding a vserver-based name server: add nameserver dns_vsvr where dns_vsvr is the name of a DNS vserver created in the system.

Related Commands

rm dns nameServer

enable dns nameServer

disable dns nameServer

show dns nameServer

rm dns nameServer

Synopsis

```
rm dns nameServer (<IP> | <dnsVserverName>)
```

Description

Remove the NameServer.

Arguments

IP

The IP address of the name server.

dnsVserverName

The name of the dns vserver.

Example

Deleting an IP-based nameserver: rm nameserver 10.102.4.1, Deleting a vserver-based nameserver: rm nameserver dns_vsvr

Related Commands

add dns nameServer

enable dns nameServer

disable dns nameServer

show dns nameServer

enable dns nameServer

Synopsis

```
enable dns nameServer (<IP> | <dnsVserverName>)
```

Description

Enable a nameserver.

Arguments

IP

The IP address of the name server.

dnsVserverName

The name of the dns vserver.

Example

enable dns nameserver 10.14.43.149

Related Commands

add dns nameServer

rm dns nameServer

disable dns nameServer

show dns nameServer

disable dns nameServer

Synopsis

```
disable dns nameServer (<IP> | <dnsVserverName>)
```

Description

Disable a nameserver.

Arguments

IP

The IP address of the name server.

dnsVserverName

The name of the dns vserver

Example

disable dns nameserver 10.14.43.149

Related Commands

add dns nameServer

rm dns nameServer

enable dns nameServer

show dns nameServer

show dns nameServer

Synopsis

```
show dns nameServer [<IP> | <dnsVserverName>]
```

Description

Display the name servers configured in the system and the state of the name servers.

Arguments

IP

The IP address of the name server.

dnsVserverName

The name of the dns vserver.

summary

fullValues

format

level

Output

serviceName

The name of the dns vserver.

port

Port of the service.

state

State of the server.

local

ip is a local recursive nameserver.

Related Commands

add dns nameServer

rm dns nameServer
enable dns nameServer
disable dns nameServer

add dns view

Synopsis

```
add dns view <viewName>
```

Description

Adds a dns view, used for dns view-based policies and for binding a view-specific IP for a gslb service.

Arguments

viewName

Name of the view name.

Example

add dns view privateview

Related Commands

rm dns view

show dns view

rm dns view

Synopsis

```
rm dns view <viewName>
```

Description

Removes a dns view that is used for dns view-based policies, and for binding a view-specific IP for a gslb service.

Arguments

viewName

Name of the view name.

Example

rm dns view privateview

Related Commands

add dns view

show dns view

show dns view

Synopsis

```
show dns view [<viewName>]
```

Description

Displays the dns views configured in the system.

Arguments

viewName

The name of the view to be displayed.

summary

fullValues

format

level

Output

serviceName

Service name of the service using this view.

IPAddress

IP of the service corresponding to the given view.

flags

Flags controlling display.NOTE: This attribute is deprecated.This is deprecated attribute.

state

flags controlling display

Related Commands

add dns view

rm dns view

add dns policy

Synopsis

```
add dns policy <name> <rule> (-viewName <string> | -
preferredLocation <string> | -drop ( YES | NO ))
```

Description

Add a dns policy. DNS policies that can be added are Interface, IP,VLAN expressions.

Arguments

`name`
Name of the dns policy.

`rule`
Expression to be used by the dns policy.

`viewName`
The view name that must be used for the given policy.

`preferredLocation`
The location used for the given policy.

`drop`
The dns packet must be dropped. Possible values: YES, NO

Example

add dns policy pol1 "CLIENT.IP.SRC.EQ(1.1.1.1)" -view privatesubnet1 add dns policy pol2 "CLIENT.IP.SRC.IN_SUBNET(1.1.1.1/24)" -view privatesubnet2 add dns policy pol1 CLIENT.ETHER.SRCMAC.EQ(00:0b:2b:0c:75:12) -view private

Related Commands

rm dns policy

set dns policy

show dns policy

rm dns policy

Synopsis

```
rm dns policy <name>
```

Description

Removes a dns policy.

Arguments

name

Name of the dns policy.

Related Commands

add dns policy

set dns policy

show dns policy

set dns policy

Synopsis

```
set dns policy <name> [<rule>] [-viewName <string> | -
preferredLocation <string> | -drop ( YES | NO )]
```

Description

Used to change the expression or view name of an already existing policy. DNS policies that can be set are Interface,IP,VLAN expressions.

Arguments

`name`
Name of the dns policy.

`rule`
Expression to be used by dns policy.

`viewName`
The view name that must be used for the given policy

`preferredLocation`
The location used for the given policy.

`drop`
The dns packet must be dropped. Possible values: YES, NO

Example

set dns policy pol1 -rule "CLIENT.IP.SRC.EQ(1.1.1.1)" set dns policy pol2 -rule "CLIENT.IP.SRC.IN_SUBNET(1.1.1.1/24)" set dns policy pol1 -rule CLIENT.ETHER.SRCMAC.EQ(00:0b:2b:0c:75:12)

Related Commands

add dns policy

rm dns policy

show dns policy

show dns policy

Synopsis

```
show dns policy [<name>]
```

Description

Used to display the policy-related information.

Arguments

`name`
Name of the dns policy.

`summary`

`fullValues`

`format`

`level`

Output

`rule`
The expression to be used by the dns policy.

`viewName`
The view name that must be used for the given policy

`preferredLocation`
The location used for the given policy.

`hits`
The number of times the policy has been hit.

`drop`
The dns packet must be dropped.

Related Commands

add dns policy
rm dns policy

set dns policy

bind dns global

Synopsis

```
bind dns global <policyName> <priority> [-
gotoPriorityExpression <string>]
```

Description

Binds the DNS policy with the given priority.

Arguments

policyName

The name of the policy to be bound to dns global.

Example

bind dns global pol9 9

Related Commands

unbind dns global

show dns global

unbind dns global

Synopsis

```
unbind dns global <policyName>
```

Description

Unbinds the DNS policy with the given priority.

Arguments

policyName

Name of the policy to be bound to dns global.

Example

unbind dns global pol9

Related Commands

bind dns global

show dns global

show dns global

Synopsis

```
show dns global
```

Description

Display the DNS global bindings.

Arguments

summary

fullValues

format

level

Output

policyName
Name of the dns policy.

priority
Specifies the priority of the policy.

gotoPriorityExpression
Expression which evaluates to a priority which must be executed next. Byt default it goes to priority 65535.

upgraded
It is internally used to tell that the policy is a upgraded policy.

Example

show dns global

Related Commands

bind dns global

unbind dns global

CHAPTER 15

DoS Commands

This chapter covers the DoS commands.

stat dos

Synopsis

```
stat dos [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display DOS statistics.

Arguments

Output

Counters

DOS condition triggered (CndMatch)

This counter gives the number of times Netscaler triggered the DOS JavaScript due to a condition match

Valid DOS clients (ValidClt)

This counter gives the number of clients from whom Netscaler received a valid DOS cookie.

DOS priority clients (DosPriCl)

This counter gives the number of valid clients that were given DOS priority.

Related Commands

stat dos policy

show dos stats

Synopsis

```
show dos stats - alias for 'stat dos'
```

Description

show dos stats is an alias for stat dos

Related Commands

stat dos

add dos policy

Synopsis

```
add dos policy <name> -qDepth <positive_integer> [-
cltDetectRate <positive_integer>]
```

Description

Add a DoS protection policy to the system.

Arguments

name

The name of the DoS protection policy.

qDepth

The queue size (the number of outstanding service requests on the system) that must be reached before DoS protection is activated on the service to which the DoS protection policy is bound. Note:For the DoS protection to be applied on a service, the service must have a DoS policy bound to it. This is done with the ###bind service### command. Minimum value: 21

cltDetectRate

The client detect rate is the percentage of traffic to apply the DOS policy. Minimum value: 0 Maximum value: 100

Example

add dos policy dospol -qdepth 100 -cltDetectRate 90

Related Commands

rm dos policy

set dos policy

unset dos policy

show dos policy

stat dos policy

rm dos policy

Synopsis

```
rm dos policy <name>
```

Description

Remove the specified DoS protection policy.

Arguments

name

The name of the DoS protection policy.

Example

rm dos policy dospol

Related Commands

add dos policy
set dos policy
unset dos policy
show dos policy
stat dos policy

set dos policy

Synopsis

```
set dos policy <name> [-qDepth <positive_integer>] [-
cltDetectRate <positive_integer>]
```

Description

Modify the parameters for the specified DoS protection policy.

Arguments

name

The name of the DoS protection policy to be modified.

qDepth

The queue size (the outstanding requests on this service queued in the system, waiting to be sent to the server) that must be reached before DoS protection is activated on the service. For DoS protection to be activated on a service, this policy needs to be bound to the service using the ###bind service### command. Minimum value: 21

cltDetectRate

The client detect rate. Client detect rate is the percentage of traffic to apply the DOS policy. Minimum value: 1 Maximum value: 100

Example

set dos policy dospol -qdepth 1000

Related Commands

add dos policy

rm dos policy

unset dos policy

show dos policy

stat dos policy

unset dos policy

Synopsis

```
unset dos policy <name> [-qDepth] [-cltDetectRate]
```

Description

Use this command to remove dos policy settings.Refer to the set dos policy command for meanings of the arguments.

Related Commands

add dos policy

rm dos policy

set dos policy

show dos policy

stat dos policy

show dos policy

Synopsis

```
show dos policy [<name>]
```

Description

Display the configured DoS protection policy.

Arguments

`name`

The name of DoS policy.

`summary`

`fullValues`

`format`

`level`

Output

`qDepth`

The queue size (the outstanding requests on this service queued in the system, waiting to be sent to the server) that must be reached before DoS protection is activated on the service. For DoS protection to be activated on a service, this policy needs to be bound to the service using the ###bind service### command.

`cltDetectRate`

The client detect rate is the percentage of traffic to apply the DOS policy.

Example

> show dos policy 1 configured DoS policy: 1) Policy: dospol QDepth: 100 ClientDetectRate: 90 Done

Related Commands

add dos policy

rm dos policy

set dos policy
unset dos policy
stat dos policy

stat dos policy

Synopsis

```
stat dos policy [<name>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display DOS policy statistics.

Arguments

name

The name of the DoS policy for which statistics will be displayed. If a name is not given, statistics are shown for all DoS policies.

Output

Counters

Client detect rate (ClDtRate)

This counter gives the current ratio of JS send rate to the server response rate (Client detect rate)

Physical service port (SvcPort)

Port address of the physical service to which this policy is bound.

Physical service IP (SvcIP)

IP address of the physical service to which this policy is bound.

Current server queue size (CurQSize)

This counter gives the current queue size of the server to which this policy is bound.

DOS transactions (DosTrans)

This counter gives the total number of DOS JavaScript transactions performed for this policy.

Client detect rate mismatch (JsRefusd)

This counter gives the number of times the DOS JS was not sent because the set JS rate was not met for this policy.

Valid clients (TotValCl)
This counter gives the total number of valid DOS cookies reveived for this policy.

DOS JavaScript bytes served (JsBytSnt)
This counter gives the total number of DOS JS bytes sent for this policy.

Non GET, POST requests
This counter gives the number of non GET, POST requests for which DOS JS was sent.

Physical service port (SvcPort)
Port address of the physical service to which this policy is bound.

DOS JavaScript send rate (JSRate)
This counter gives the current rate at which JS is being sent in response to client requests.

Server response rate (RespRate)
This counter gives the current rate at which the server to which this policy is bound is responding.

Related Commands

add dos policy
rm dos policy
set dos policy
unset dos policy
show dos policy
stat dos

CHAPTER 16

Filter Commands

This chapter covers the filter commands.

set filter prebodyInjection

Synopsis

```
set filter prebodyInjection <prebody>
```

Description

Set file name for prebody

Arguments

prebody

The file name for prebody.

Example

set htmlinjection prebody myprebody.dat

Related Commands

unset filter prebodyInjection

show filter prebodyInjection

unset filter prebodyInjection

Synopsis

```
unset filter prebodyInjection
```

Description

Unset file name for prebody.Refer to the set filter prebodyInjection command for meanings of the arguments.

Example

unset htmlinjection prebody

Related Commands

set filter prebodyInjection

show filter prebodyInjection

show filter prebodyInjection

Synopsis

```
show filter prebodyInjection
```

Description

Display the file for prebody.

Arguments

format

level

Output

prebody

The name of the prebody file.

systemIID

The system IID of the current NetScaler system.

Example

show htmlinjection prebody

Related Commands

set filter prebodyInjection

unset filter prebodyInjection

set filter postbodyInjection

Synopsis

```
set filter postbodyInjection <postbody>
```

Description

Unset file name for postbody

Arguments

postbody

The file name for postbody.

Example

set htmlinjection postbody postbody.dat

Related Commands

unset filter postbodyInjection

show filter postbodyInjection

unset filter postbodyInjection

Synopsis

```
unset filter postbodyInjection
```

Description

Remove file name for prebody.Refer to the set filter postbodyInjection command for meanings of the arguments.

Example

unset htmlinjection prebody

Related Commands

set filter postbodyInjection

show filter postbodyInjection

show filter postbodyInjection

Synopsis

```
show filter postbodyInjection
```

Description

Display the file for postbody.

Arguments

format

level

Output

postbody

The name of the postbody file.

systemIID

The system IID of the current NetScaler system.

Example

show htmlinjection postbody

Related Commands

set filter postbodyInjection

unset filter postbodyInjection

add filter action

Synopsis

```
add filter action <name> <qual> [<serviceName>]
[<value>] [<respCode>] [<page>]
```

Description

Create a content filtering action. The action thus created can be associated with the content filtering policy. The two built-in filter actions RESET and DROP are always present on the system. Use the RESET filter action to send a TCP reset for the HTTP requests. Use the DROP filter action to drop the HTTP requests silently without sending a TCP FIN for closing the connection.

Arguments

name

The name for the filter action.

qual

The name of the qualifier. Possible values: reset, add, corrupt, forward, errorcode, drop

serviceName

The service to which HTTP requests are forwarded. This parameter is required when the qualifier is FORWARD.

value

The string containing the header_name and header_value. When the qualifier is ADD use this option as header_name:header_value. When the qualifier is Corrupt use this option to specify only the header_name.

respCode

The response code to be returned for HTTP requests. Use this parameter when the qualifier is ERRORCODE. Minimum value: 1

page

The HTML page that will be returned for the HTTP requests. Use this parameter when the qualifier is ERRORCODE.

Example

add filter action bad_url_action errorcode 400 "<HTML>Bad URL.</HTML>" add filter action forw_action FORWARD service1 add filter action add_header_action add "HEADER:value"

Related Commands

rm filter action

set filter action

unset filter action

show filter action

rm filter action

Synopsis

```
rm filter action <name>
```

Description

Remove a created filter action.

Arguments

name

The name of the filter action.

Example

rm filter action filter_action_name

Related Commands

add filter action

set filter action

unset filter action

show filter action

set filter action

Synopsis

```
set filter action <name> [-serviceName <string>] [-
value <string>] [-respCode <positive_integer>] [-page
<string>]
```

Description

Modify an existing content filtering action.

Arguments

name

The name for the filter action.

serviceName

The service to which HTTP requests are forwarded. This parameter can be set only when the action qualifier is FORWARD.

value

The string containing the header_name and header_value. When the qualifier is ADD use this option as header_name:header_value. When the qualifier is Corrupt use this option to specify only the header_name.

respCode

The response code to be returned for HTTP requests. Use this parameter when the qualifier is ERRORCODE. Minimum value: 1

page

The HTML page that will be returned for the HTTP requests. Use this parameter when the action qualifier is ERRORCODE.

Example

set filter action bad_url_action -respcode 400 -page "<HTML>Bad URL.</HTML>" set filter action forw_action -serviceName service1 set filter action add_header_action -value "HEADER:value"

Related Commands

add filter action

rm filter action
unset filter action
show filter action

unset filter action

Synopsis

```
unset filter action <name> -page
```

Description

Use this command to remove filter action settings.Refer to the set filter action command for meanings of the arguments.

Related Commands

add filter action

rm filter action

set filter action

show filter action

show filter action

Synopsis

```
show filter action [<name>]
```

Description

Display the created filter actions. The filter actions RESET and DROP are always displayed, irrespective of whether an action has been defined. They are built-in actions and cannot be modified.

Arguments

`name`

`summary`

`fullValues`

`format`

`level`

Output

`qual`
The name of the qualifier.

`serviceName`
The service to which HTTP requests are forwarded. This parameter will exist when the qualifier is FORWARD.

`value`
The string containing the header_name and header_value. When the qualifier is ADD it will have header_name:header_value. When the qualifier is Corrupt this will have header_name.

`respCode`
The response code to be returned for HTTP requests. This parameter will exist when the qualifier is ERRORCODE.

page

The HTML page that will be returned for the HTTP requests. This parameter will exist when the qualifier is ERRORCODE.

Example

Example 1 The following shows an example of the output of the show filter action command when no filter actions have been defined: 1) Name: RESET Filter Type: reset 2) Name: DROP Filter Type: drop Done Example 2 The following command creates a filter action: add filter action bad_url_action errorcode 400 "<HTML>Bad URL.</HTML>" The following shows an example of the output of the show filter action command after the previous command has been issued: Name: bad_url_action Filter Type: errorcode StatusCode: 400 Response Page: <HTML>Bad URL.</HTML> Done

Related Commands

add filter action

rm filter action

set filter action

unset filter action

add filter htmlinjectionvariable

Synopsis

```
add filter htmlinjectionvariable <variable> [-value
<string>]
```

Description

Add a new HTML injection variable

Arguments

`variable`

The name of the HTML injection variable to be added.

`value`

Value to be assigned to the new variable.

Example

add htmlinjectionvariable EDGESIGHT_SERVER_IP -value 1.1.1.1

Related Commands

rm filter htmlinjectionvariable

set filter htmlinjectionvariable

unset filter htmlinjectionvariable

show filter htmlinjectionvariable

rm filter htmlinjectionvariable

Synopsis

```
rm filter htmlinjectionvariable <variable>
```

Description

Remove a HTML injection variable

Arguments

variable

The name of the HTML injection variable to be removed.

Example

rm htmlinjectionvariable EDGESIGHT_SERVER_IP

Related Commands

add filter htmlinjectionvariable
set filter htmlinjectionvariable
unset filter htmlinjectionvariable
show filter htmlinjectionvariable

set filter htmlinjectionvariable

Synopsis

```
set filter htmlinjectionvariable <variable> [-value
<string>]
```

Description

Set the value of a HTML injection variable

Arguments

`variable`

The name of the HTML injection variable to be set.

`value`

Value to be set in the new variable. Default value:

Example

set htmlinjectionvariable EDGESIGHT_SERVER_IP -value 2.2.2.2

Related Commands

add filter htmlinjectionvariable

rm filter htmlinjectionvariable

unset filter htmlinjectionvariable

show filter htmlinjectionvariable

unset filter htmlinjectionvariable

Synopsis

```
unset filter htmlinjectionvariable <variable> -value
```

Description

Use this command to remove filter htmlinjectionvariable settings.Refer to the set filter htmlinjectionvariable command for meanings of the arguments.

Related Commands

add filter htmlinjectionvariable

rm filter htmlinjectionvariable

set filter htmlinjectionvariable

show filter htmlinjectionvariable

show filter htmlinjectionvariable

Synopsis

```
show filter htmlinjectionvariable [<variable>]
```

Description

Display HTML injection variable

Arguments

variable

The name of the HTML injection variable to be displayed.

summary

fullValues

format

level

Output

value

Value of the HTML injection variable

type

Type of the HTML injection variable

Example

show htmlinjectionvariable EDGESIGHT_SERVER_IP

Related Commands

add filter htmlinjectionvariable

rm filter htmlinjectionvariable

set filter htmlinjectionvariable

unset filter htmlinjectionvariable

set filter htmlinjectionparameter

Synopsis

```
set filter htmlinjectionparameter [-rate
<positive_integer>] [-frequency <positive_integer>]
```

Description

Set the various HTML injection parameters

Arguments

rate

if rate is X, HTML injection will be done for 1 out of X policy matches
Default value: 1 Minimum value: 1

frequency

if frequency is X, HTML injection will be done atleast once per X milisecond
Default value: 1 Minimum value: 1

Example

set htmlinjection parameter -rate 10 -frequency 1

Related Commands

unset filter htmlinjectionparameter

show filter htmlinjectionparameter

unset filter htmlinjectionparameter

Synopsis

```
unset filter htmlinjectionparameter [-rate] [-
frequency]
```

Description

Unset the previously set HTML injection parameters.Refer to the set filter htmlinjectionparameter command for meanings of the arguments.

Example

a) unset htmlinjectionparameter -rate b) unset htmlinjectionparameter -frequency c) unset htmlinjectionparameter -rate -frequency

Related Commands

set filter htmlinjectionparameter

show filter htmlinjectionparameter

show filter htmlinjectionparameter

Synopsis

```
show filter htmlinjectionparameter
```

Description

Display the HTML injection parameters

Arguments

format

level

Output

rate

if rate is X, HTML injection will be done for 1 out of X policy matches

frequency

if frequency is X, HTML injection will be done atleast once per X milisecond

Example

rate:10

Related Commands

set filter htmlinjectionparameter

unset filter htmlinjectionparameter

add filter policy

Synopsis

```
add filter policy <name> -rule <expression> (-reqAction
<string> | -resAction <string>)
```

Description

Create a content filtering policy.

Arguments

name

The name of the new filter policy.

rule

The expression which sets the condition for application of the policy.

reqAction

The name of the action to be performed on the request. The string value can be a created filter action or one of the following built-in actions: RESET - Sends the TCP reset and closes the connection to the peer. DROP - Silently closes the connection to the peer without sending the TCP FIN. Note that the request action can not be specified if the rule has some condition to be evaluated for response.

resAction

The action to be performed on the response. The string value can be a filter action created filter action or a built-in action.

Example

Example 1: add policy expression e1 "sourceip == 66.33.22.0 -netmask 255.255.255.0" add policy expression e2 "URL == /admin/account.asp" add filter policy ip_filter -rule "e1 && e2" -reqAction RESET After creating above filter policy, it can be activated by binding it globally: bind filter global ip_filter With the configured ip_filter (name of the filter policy), the NetScaler system sends a TCP reset to all HTTP requests for the /admin/account.asp URL from 66.33.22.0 Class C network. This action is applied at the HTTP request time. Example 2: To silently drop (without sending FIN) all the HTTP requests in which the URL has root.exe or cmd.exe, below filter

policy can be configured: add filter policy nimda_filter -rule "URL contains root.exe || URL contains cmd.exe" -reqAction DROP bind filter global nimda_filter Example 3: add filter policy url_filter -rule "url == /foo/secure.asp && SOURCEIP != 65.186.55.0 -netmask 255.255.255.0 && SOURCEIP != 65.202.35.0 -netmask 255.255.255.0" -reqaction RESET bind filter global url_filter With the above configured filter policy named url_filter, the NetScaler system sends RESET to all HTTP requests for the URL /foo/secure.asp from all the networks except from 65.186.55.0 and 65.202.35.0 Class C networks. This action is applied at the HTTP request time. Note: In above examples, the RESET and DROP are built-in actions in the NetScaler system. "show filter action" and "show filter policy" CLI commands show the configured filter actions and policies in NetScaler system respectively. "show filter global" command shows all the globallyactive filter policies.

Related Commands

rm filter policy

set filter policy

unset filter policy

show filter policy

rm filter policy

Synopsis

```
rm filter policy <name>
```

Description

Remove a filter policy.

Arguments

name

The name of filter policy.

Example

rm filter policy filter_policy_name The "show filter policy" command shows all filter policies that are currently defined.

Related Commands

add filter policy

set filter policy

unset filter policy

show filter policy

set filter policy

Synopsis

```
set filter policy <name> [-rule <expression>] [-
reqAction <string> | -resAction <string>]
```

Description

Modify the created filter policy.

Arguments

name

The name of the filter policy.

rule

The expression which sets the condition for application of the policy.

reqAction

Request action.

resAction

Response action.

Example

Example 1: A filter policy to allow access of URL /foo/secure.asp only from 65.186.55.0 network can be created using below command: add filter policy url_filter -rule "URL == /foo/secure.asp && SOURCEIP != 65.186.55.0 -netmask 255.255.255.0" -reqAction RESET This policy is activated using: bind filter global url_filter Later, to allow access of this url from second network 65.202.35.0 too, above filter policy can be changed by issuing below command: set filter policy url_filter -rule "URL == /foo/secure.asp && SOURCEIP != 65.186.55.0 -netmask 255.255.255.0 && SOURCEIP != 65.202.35.0 -netmask 255.255.255.0" Changed filter policy can be viewed by using following command: show filter policy url_filter Name: url_filter Rule: (URL == /foo/secure.asp && (SOURCEIP != 65.186.55.0 -netmask 255.255.255.0 && SOURCEIP != 65.202.35.0 -netmask 255.255.255.0)) Request action: RESET Response action: Hits: 0 Done

Related Commands

add filter policy
rm filter policy
unset filter policy
show filter policy

unset filter policy

Synopsis

```
unset filter policy <name> [-rule] [-reqAction] [-
resAction]
```

Description

Use this command to remove filter policy settings.Refer to the set filter policy command for meanings of the arguments.

Related Commands

add filter policy

rm filter policy

set filter policy

show filter policy

show filter policy

Synopsis

```
show filter policy [<name>]
```

Description

Display the filter policies.

Arguments

name

The name of the filter policy.

summary

fullValues

format

level

Output

rule

The expression which sets the condition for application of the policy.

reqAction

The name of the action to be performed on the request.

resAction

The action to be performed on the response.

boundTo

The entity name to which policy is bound

Example

show filter policy 1) Name: nimda_filter Rule: (URL CONTAINS root.exe || URL CONTAINS cmd.exe) Request action: RESET Response action: Hits: 0 2) Name: ip_filter Rule: (src_ips && URL == /admin/account.asp) Request action: RESET Response action: Hits: 0 Done Individual filter policy can also be viewed by giving filter policy name

as argument: show filter policy ip_filter Name: ip_filter Rule: (src_ips && URL == /admin/account.asp) Request action: RESET Response action: Hits: 0 Done

Related Commands

add filter policy
rm filter policy
set filter policy
unset filter policy

bind filter global

Synopsis

```
bind filter global (<policyName>  [-priority
<positive_integer>]) [-state ( ENABLED | DISABLED )]
```

Description

Activate the filter policy globally.Note that the content filtering license is required for filtering.

Arguments

policyName

The name of the filter policy to be bound.

Example

To send RESET for all the HTTP requests which are not get or head type, following filter policy can be created: add filter policy reset_invalid_req -rule "METHOD != GET && METHOD != HEAD" -reqAction RESET This filter policy can be activated globally for NetScaler system by giving command: bind filter global reset_invalid_req Globally active filter policies can be seen using command: show filter global 1) Policy Name: reset_invalid_req Priority: 0 Done

Related Commands

unbind filter global

show filter global

unbind filter global

Synopsis

```
unbind filter global <policyName>
```

Description

Deactivate a filter policy globally.

Arguments

policyName

The name of the filter policy to be unbound.

Example

Globally active filter policies can be seen using command: show filter global 1) Policy Name: reset_invalid_req Priority: 0 Done This globally active filter policy can be deactivated on NetScaler system by giving command: unbind filter global reset_invalid_req

Related Commands

bind filter global

show filter global

show filter global

Synopsis

```
show filter global
```

Description

Display the globally activated filter policies.

Arguments

summary

fullValues

format

level

Output

policyName
The name of teh filter policy.

priority
The priority of the policy.

state
The state of the binding.

Example

show filter global 1) Policy Name: url_filter Priority: 0 2) Policy Name: reset_invalid_req Priority: 0 Done

Related Commands

bind filter global

unbind filter global

CHAPTER 17

GSLB Commands

This chapter covers the GSLB commands.

show gslb runningConfig

Synopsis

```
show gslb runningConfig
```

Description

Display the information pertaining to all the configuration that has been applied to the system, including settings that have not yet been saved to the system's ns.conf file using the save config command.

Arguments

Output

Related Commands

show ns.conf

stat gslb domain

Synopsis

```
stat gslb domain [<name>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display statistics of a gslb domain.

Arguments

name

The name of the gslb domain for which statistics will be displayed. If not given statistics are shown for all gslb domain.

Output

Counters

domainHits (Hits)

Total number of DNS queries received.

domainHits (Hits)

Total number of DNS queries received.

Related Commands

stat gslb site

stat gslb service

stat gslb vserver

add gslb site

Synopsis

```
add gslb site <siteName> [<siteType>] <siteIPAddress>
[-publicIP <ip_addr>] [-metricExchange ( ENABLED |
DISABLED )] [-nwMetricExchange ( ENABLED | DISABLED )]
[-sessionExchange ( ENABLED | DISABLED )] [-
triggerMonitor <triggerMonitor>] [-parentSite
<string>]
```

Description

Add the site entity participating in GSLB in system

Arguments

siteName

The name of the site that is participating in the GSLB

siteType

Specify whether the site is LOCAL or REMOTE. If this option is not specified, then it will be automatically detected whether the site should be considered LOCAL or REMOTE. This decision is based on whether the siteIPAddress is found to be already configured in the system, for e.g., MIP or SNIP Possible values: REMOTE, LOCAL Default value: NS_NORMAL

siteIPAddress

The IP address of the site. This IP address will be a System owned IP address. SNIP or MIP can be used as Site IP address

publicIP

The Public IP. This parameter is in effect only for a LOCAL site. This parameter is required only if the local System is in a private address space and has a public IP hosted on an external FW or NAT device.

metricExchange

The state of MEP. When metric exchange is DISABLED, then the site does not exchange metrics with other sites. When this option is disabled, a simple ROUNDROBIN method will be used for Global Server Load Balancing. Possible values: ENABLED, DISABLED Default value: ENABLED

nwMetricExchange
Disable or enable exchange of network metrics like RTT. Possible values: ENABLED, DISABLED Default value: ENABLED

sessionExchange
Disable or enable exchange of persistence session entries. Possible values: ENABLED, DISABLED Default value: ENABLED

triggerMonitor
A setting that defines when bound monitors if any should be triggered for services belonging to this site. Possible values: ALWAYS, MEPDOWN, MEPDOWN_SVCDOWN Default value: NSGSLB_TRIGMON_ALWAYS

parentSite
Parent site of this site.

Example

add site new_york LOCAL 192.168.100.12 -publicIP 65.200.211.139

Related Commands

rm gslb site
set gslb site
unset gslb site
show gslb site
stat gslb site

rm gslb site

Synopsis

```
rm gslb site <siteName>
```

Description

Remove the site entity configured in system

Arguments

siteName

The name of the site entity to be removed. When the site is removed, all the services created under that site will be removed.

Example

rm gslb site new_york

Related Commands

add gslb site

set gslb site

unset gslb site

show gslb site

stat gslb site

set gslb site

Synopsis

```
set gslb site <siteName> [-metricExchange ( ENABLED |
DISABLED )] [-nwMetricExchange ( ENABLED | DISABLED )]
[-sessionExchange ( ENABLED | DISABLED )] [-
triggerMonitor <triggerMonitor>]
```

Description

Enable or disable the Metric Exchange between sites

Arguments

siteName

The name of the site.

metricExchange

State of metric exchange for the site. If metric exchange is disabled, a simple ROUNDROBIN method is used to perform Global Server load balancing Possible values: ENABLED, DISABLED Default value: ENABLED

nwMetricExchange

Disable or enable exchange of network metrics like RTT. Possible values: ENABLED, DISABLED Default value: ENABLED

sessionExchange

Disable or enable exchange of persistence session entries. Possible values: ENABLED, DISABLED Default value: ENABLED

triggerMonitor

A setting that defines when bound monitors if any should be triggered for services belonging to this site. Possible values: ALWAYS, MEPDOWN, MEPDOWN_SVCDOWN Default value: NSGSLB_TRIGMON_ALWAYS

Example

set gslb site new_york - metricExchange DISABLED

Related Commands

add gslb site

rm gslb site
unset gslb site
show gslb site
stat gslb site

unset gslb site

Synopsis

```
unset gslb site <siteName> [-metricExchange] [-
nwMetricExchange] [-sessionExchange] [-triggerMonitor]
```

Description

Use this command to remove gslb site settings.Refer to the set gslb site command for meanings of the arguments.

Related Commands

add gslb site

rm gslb site

set gslb site

show gslb site

stat gslb site

show gslb site

Synopsis

```
show gslb site [<siteName>] show gslb site stats -
alias for 'stat gslb site'
```

Description

Display the configured site entities in system

Arguments

siteName

The name of the site. If sitename is specified, all the services created under that site will be displayed.

summary

fullValues

format

level

Output

siteType

Specifies whether the site is LOCAL or REMOTE.

siteIPAddress

The IP address of the site.

publicIP

The Public IP of the gslb site.

metricExchange

The state of MEP. When metric exchange is DISABLED, then the site does not exchange metrics with other sites. When this option is disabled, a simple ROUNDROBIN method will be used for Global Server Load Balancing.

serviceName

Service name.

IPAddress
IP Address of the gslb service.

port
Port number of the gslb service.

state
State of the gslb service.

status
Current metric exchange status.

serviceType
Service type.

nwMetricExchange
Specifies whether the exchange of network metrics like RTT is enabled or disabled.

sessionExchange
Specifies whether the exchange of persistence session entries is enabled or disabled.

triggerMonitor
A setting that defines when bound monitors if any should be triggered for services belonging to this site.

parentSite
Parent site of this site.

cnameEntry
The cname of the gslb service.

Example

show site new_york

Related Commands

add gslb site
rm gslb site
set gslb site
unset gslb site
stat gslb site

stat gslb site

Synopsis

```
stat gslb site [<siteName>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display Gslb site statistics.

Arguments

siteName

The name of the GSLB site for which statistics will be displayed. If not given statistics are shown for all gslb sites.

Output

Counters

Metric Exchange State (MEPstate)

This indicates the status of the Metric Exchange Policy at the site.

Metric Exchange (MEP)

This indicates whether metric exchange is enabled or disabled at this site.

GSLB Site type (sitetype)

This indicates whether the Gslb site is local or remote.

Gslb Site Public IP address (Public IP)

This is the public IP address of the GSLB site.

Gslb Site private IP address (Private IP)

This is the private IP address of the site

Requests (Req)

The total number of requests received on the Vservers represented by all GSLB services associated with this site.

Responses (Rsp)
Number of responses received on the Vservers represented by all GSLB services associated with this site.

Request bytes (Reqb)
The total number of request bytes received on the Vservers represented by all GSLB services associated with this site.

Response bytes (Rspb)
Number of response bytes received on the Vservers represented by all GSLB services associated with this site.

Current client connections (ClntConn)
The number of current client connections to the Vservers represented by all GSLB services associated with this site.

Current server connections (SvrConn)
The number of current connections to the real servers behind the Vservers represented by all the GSLB services associated with this site.

Related Commands

add gslb site
rm gslb site
set gslb site
unset gslb site
show gslb site

stat gslb domain
stat gslb service
stat gslb vserver

add gslb service

Synopsis

```
add gslb service <serviceName> [-cnameEntry <string> |
<IP> | <serverName> | <serviceType> | <port> | -
publicIP <ip_addr> | -publicPort <port> | -
sitePersistence <sitePersistence> | -sitePrefix
<string>] [-maxClient <positive_integer>] [-siteName
<string>] [-state ( ENABLED | DISABLED )] [-cip (
ENABLED | DISABLED )  [<cipHeader>]] [-cookieTimeout
<mins>] [-cltTimeout <secs>] [-svrTimeout <secs>] [-
maxBandwidth <positive_integer>] [-downStateFlush (
ENABLED | DISABLED )] [-maxAAAUsers <positive_integer>]
[-monThreshold <positive_integer>]
```

Description

Add a GSLB service in the system.

Arguments

serviceName

The name of the service.

cnameEntry

The cname of the gslb service.

IP

The IP address of the server for which the service will be added

serverName

The name of the server for which the service will be added

serviceType

The type of service that is being added Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP Default value: NSSVC_SERVICE_UNKNOWN

port
The port on which the service is running Minimum value: 1

publicIP
The IP address on a NAT box in front of the system to which a private IP of the service maps. This is applicable to GSLB local services. This is optional Default value: VAL_NOT_SET

publicPort
The port on a NAT box in front of the system to which the private port of service maps. This is applicable to GSLB local services.This is optional Default value: VAL_NOT_SET

maxClient
The maximum number of open connections to the service. This argument is optional Default value: VAL_NOT_SET Maximum value: 0xFFFFFFFE

siteName
The GSLB site name. This parameter is mandatory. This option specifies whether the service is a local GSLB service or remote GSLB service

state
The state of the service(s). This parameter is optional. This is not applicable to the local GSLB services. Possible values: ENABLED, DISABLED Default value: ENABLED

cip
State of insertion of the Client IP header for the service. This parameter is used while connection proxy based Site persistency is enabled, and it inserts real client's IP address in the HTTP request Possible values: ENABLED, DISABLED Default value: DISABLED

cipHeader
The client IP header to be used in the HTTP request. If client IP insertion is enabled and the client IP header is not specified then the value that has been set by the set ns config CLI command will be used as the Client IP header.

sitePersistence
The state of cookie based Site persistency. Possible values: ConnectionProxy, HTTPRedirect, NONE

cookieTimeout
The timeout value in minutes for the cookie when cookie based Site persistency is enabled Default value: 0 Maximum value: 1440

sitePrefix
Specify the site prefix string. When the service is bound to a GSLB vserver, then for each bound service-domain pair, a GSLB Site domain will be generated internally by concatenating the service's siteprefix and the domain's name. If a special string "NONE" is specified, the siteprefix string will be unset

cltTimeout
The idle time in seconds after which the client connection is terminated. This will be used while doing site persistency Default value: VAL_NOT_SET Maximum value: 31536000

svrTimeout
The idle time in seconds after which the server connection is terminated. This will be used while doing site persistency Default value: VAL_NOT_SET Maximum value: 31536000

maxBandwidth
A positive integer to identify the maximum bandwidth allowed for the service

downStateFlush
Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: VAL_NOT_SET

maxAAAUsers
The maximum number of concurrent SSLVPN users allowed to login at a time. Maximum value: 65535

monThreshold
The monitoring threshold. Default value: 0 Minimum value: 0 Maximum value: 65535

Example

add gslb service sj_svc 203.12.123.12 http 80 -site san_jos

Related Commands

rm gslb service

set gslb service
unset gslb service
bind gslb service
unbind gslb service
show gslb service
stat gslb service

rm gslb service

Synopsis

```
rm gslb service <serviceName>
```

Description

Remove a gslb service configured in system.

Arguments

`serviceName`

The name of the service entity to be removed

Example

rm gslb service sj_svc

Related Commands

add gslb service
set gslb service
unset gslb service
bind gslb service
unbind gslb service
show gslb service
stat gslb service

set gslb service

Synopsis

```
set gslb service <serviceName> [-IPAddress <ip_addr|*>]
[-publicIP <ip_addr>] [-publicPort <port>] [-cip (
ENABLED | DISABLED )  [<cipHeader>]] [-sitePersistence
<sitePersistence>] [-sitePrefix <string>] [-maxClient
<positive_integer>] [-maxBandwidth <positive_integer>]
[-downStateFlush ( ENABLED | DISABLED )] [-maxAAAUsers
<positive_integer>] [-viewName <string>  <viewIP>] [-
monThreshold <positive_integer>] [-weight
<positive_integer>  <monitorName>]
```

Description

Set parameters in the gslb service

Arguments

serviceName

The name of the gslb service.

IPAddress

The new IP address of the service.

publicIP

The IP address on a NAT box in front of the system to which a private IP service maps. This is optional. It is only valid for LOCAL GSLB service

publicPort

The port on a NAT box in front of the system to which the private port of service maps. This is optional. It is only valid for local service Minimum value: 1

cip

Insertion of the Client IP header for the service. This option is used while connection proxy based Site persistency is enabled Possible values: ENABLED, DISABLED Default value: DISABLED

sitePersistence
The state of cookie based Site persistency. Possible values: ConnectionProxy, HTTPRedirect, NONE

sitePrefix
The site prefix string.

maxClient
Maximum number of Clients.

maxBandwidth
Maximum bandwidth.

downStateFlush
Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

maxAAAUsers
The maximum number of concurrent SSLVPN users allowed to login at a time. Maximum value: 65535

viewName
The name of view for the given IP

monThreshold
The monitoring threshold. Minimum value: 0 Maximum value: 65535

weight
The weight for the specified monitor. Minimum value: 1 Maximum value: 100

Example

set gslb service sj_svc -sitePersistence ConnectionProxy

Related Commands

add gslb service

rm gslb service

unset gslb service

bind gslb service

unbind gslb service

show gslb service

stat gslb service

unset gslb service

Synopsis

```
unset gslb service <serviceName> [-publicIP] [-
publicPort] [-cip] [-cipHeader] [-sitePersistence] [-
sitePrefix] [-maxClient] [-maxBandwidth] [-
downStateFlush] [-maxAAAUsers] [-viewIP] [-
monThreshold] [-monitorName]
```

Description

Use this command to remove gslb service settings.Refer to the set gslb service command for meanings of the arguments.

Related Commands

add gslb service

rm gslb service

set gslb service

bind gslb service

unbind gslb service

show gslb service

stat gslb service

bind gslb service

Synopsis

```
bind gslb service <serviceName> [-viewName <string>
<viewIP>]
```

Description

Binding a view specific IP to this service

Arguments

serviceName

The name of the gslb service

viewName

The name of view for the given IP

Example

bind gslb service -viewName privateview 1.2.3.4

Related Commands

add gslb service
rm gslb service
set gslb service
unset gslb service
unbind gslb service
show gslb service
stat gslb service

unbind gslb service

Synopsis

```
unbind gslb service <serviceName> -viewName <string>
```

Description

Unbinding a view from the service

Arguments

serviceName

The name of the gslb service

viewName

The name of view for the given IP

Example

unbind gslb service -viewName privateview

Related Commands

add gslb service

rm gslb service

set gslb service

unset gslb service

bind gslb service

show gslb service

stat gslb service

show gslb service

Synopsis

```
show gslb service [<serviceName>] show gslb service
stats - alias for 'stat gslb service'
```

Description

Display the gslb services configured in the system.

Arguments

serviceName
The name of the gslb service.

summary

fullValues

format

level

Output

gslb

IPAddress
IP address of the service

serverName
The name of the server for which the service will be added

serviceType
Service type.

port
Port number of the service.

publicIP
Public ip of the service

publicPort
Public port of the service

maxClient
Maximum number of clients.

maxAAAUsers
The maximum number of concurrent SSLVPN users allowed to login at a time.

siteName
Name of the site to which the service belongs.

svrState
Server state.

svrEffGslbState
Effective state of the gslb svc

gslbthreshold
Indicates if gslb svc has reached threshold

gslbsvcStats
Indicates if gslb svc has stats of the primary or the whole chain

state

monitorName
Monitor name.

monState
State of the monitor bound to gslb service.

cip
Indicates if Client IP option is enabled

cipHeader
The client IP header used in the HTTP request.

sitePersistence
Indicates the type of cookie persistence set

sitePrefix
The site prefix string.

cltTimeout
Client timeout in seconds.

svrTimeout
Server timeout in seconds.

totalfailedprobes
The total number of failed probs.

preferredLocation
Prefered location.

maxBandwidth
Maximum bandwidth.

downStateFlush
Perform delayed clean up of connections on this vserver.

cnameEntry
The cname of the gslb service.

viewName
The name of view for the given IP

viewIP
IP address to be used for the given view

weight
The Weight of monitor

monThreshold
The monitoring threshold.

failedprobes
Number of the current failed monitoring probes.

monStatCode
The code indicating the monitor response.

monStatParam1
First parameter for use with message code.

monStatParam2
Second parameter for use with message code.

monStatParam3
Third parameter for use with message code.

responseTime
Response time of this monitor.

monState
The running state of the monitor on this service.

Example

show gslb service sj_svc

Related Commands

add gslb service
rm gslb service
set gslb service
unset gslb service
bind gslb service
unbind gslb service
stat gslb service

stat gslb service

Synopsis

```
stat gslb service [<serviceName>] [-detail] [-
fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>]
```

Description

Display statistics of a service.

Arguments

serviceName

Output

Counters

IP address (IP)
The ip address at which the service is running.

Port (port)
The port at which the service is running.

Service type (Type)
The type of the service.

State
Current state of the server.

Requests (Req)
The total number of requests received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Responses (Rsp)
Number of responses received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Request bytes (Reqb)
The total number of request bytes received on this service/vserver.

Response bytes (Rspb)
Number of response bytes received on this service/vserver.

Current client connections (ClntConn)
The number of current client connections.

Current server connections (SvrConn)
The number of current connections to the real servers behind the vserver.

Current load on the service (Load)
The load on the service that is calculated from bound load based monitor.

Related Commands

add gslb service
rm gslb service
set gslb service
unset gslb service
bind gslb service
unbind gslb service
show gslb service

stat gslb domain
stat gslb site
stat gslb vserver

add gslb vserver

Synopsis

```
add gslb vserver <name> <serviceType> [-lbMethod
<lbMethod>  [-backupLBMethod <backupLBMethod>] ] [-
backupSessionTimeout <mins>] [-netmask <netmask>] [-
tolerance <positive_integer>] [-persistenceType (
SOURCEIP | NONE )] [-persistenceId <positive_integer>]
[-persistMask <netmask>] [-timeout <mins>] [-EDR (
ENABLED | DISABLED )] [-MIR ( ENABLED | DISABLED )] [-
disablePrimaryOnDown ( ENABLED | DISABLED )] [-
dynamicWeight <dynamicWeight>] [-state ( ENABLED |
DISABLED )] [-considerEffectiveState ( NONE |
STATE_ONLY )]
```

Description

Add a GSLB vserver in the system.

Arguments

name

The virtual server name.

serviceType

The service type of the virtual server Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP

lbMethod

The load balancing method for the virtual server.The valid options for this parameter are: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT , CUSTOMLOAD Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD Default value: PEMGMT_LB_LEASTCONNS

backupSessionTimeout
A non zero value enables the feature whose minimum value is 2 minutes. The feature can be disabled by setting the value to zero. The created session is in effect for a specific client per domain. Default value: 0 Minimum value: 0 Maximum value: 1440

backupLBMethod
The load balancing method for the virtual server, in case the primary lb method fails. The valid options for this parameter are: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT , CUSTOMLOAD. The backup lb method can be set only if the primary method is RTT or STATICPROXIMITY. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD

netmask
The netmask to be used in the SOURCEIPHASH policy. The default is 255.255.255.255 Default value: 0xFFFFFFFF

tolerance
The Site selection tolerance is the maximum deviation (in milliseconds) in the RTT value, which the system can tolerate, while deciding the best site for a domain. This value enables the system to implement the Round Robin method of GSLB between sites that have RTT values within this permissible limit. The tolerance value is required only if the LB method is RTT. The default tolerance value is 0 Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 100

persistenceType
The persistence type for the virtual server. This has 2 options: SOURCEIP and NONE Possible values: SOURCEIP, NONE

persistenceId
The Persistence Id. This parameter is a positive integer which is used to identify the GSLB VIP on all sites. This is a required argument if SOURCEIP based persistency is enabled. Maximum value: 65535

persistMask
The netmask to be used while SOURCEIP based persistency is ENABLED.This is an optional argument. Default value: 0xFFFFFFFF

timeout
The idle time out in minutes for the persistence entries Default value: 2 Minimum value: 2 Maximum value: 1440

EDR
Use this parameter to specify whether System will send empty DNS response when all the sites participating in GSLB are down Possible values: ENABLED, DISABLED Default value: DISABLED

MIR
Use this parameter to specify whether System can send Multiple IP addresses in the DNS response or not. Possible values: ENABLED, DISABLED Default value: DISABLED

disablePrimaryOnDown
When this feature is enabled we will continue to direct traffic to the backup chain even after the primary comes UP. Ideally one should use backup persistence if they want to stick to the same vserver in the chain. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicWeight
Specifies whether we want to consider the svc count or the svc weights or ignore both Possible values: SERVICECOUNT, SERVICEWEIGHT, DISABLED Default value: DISABLED

state
State of the virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

considerEffectiveState
Specifies which backup to consider when the primary state of all gslb services bound to the vip are down. By specifying NONE we will not consider the effective state of the gslb service to determine the state of the gslb vip. If STATE_ONLY is chosen we will consider the effective state obtained via MEP to determine the state of the gslb vip Possible values: NONE, STATE_ONLY Default value: NS_GSLB_DONOT_CONSIDER_BKPS

Example
add gslb vserver gvip http

Related Commands
rm gslb vserver

set gslb vserver
unset gslb vserver
bind gslb vserver
unbind gslb vserver
enable gslb vserver
disable gslb vserver
show gslb vserver
stat gslb vserver

rm gslb vserver

Synopsis

```
rm gslb vserver <name>
```

Description

Remove a GSLB vserver configured in system.

Arguments

name

The name of the GSLB virtual server to be removed

Example

rm gslb vserver gvip

Related Commands

add gslb vserver
set gslb vserver
unset gslb vserver
bind gslb vserver
unbind gslb vserver
enable gslb vserver
disable gslb vserver
show gslb vserver
stat gslb vserver

set gslb vserver

Synopsis

```
set gslb vserver <name> [-backupVServer <string>] [-
backupSessionTimeout <mins>] [-lbMethod <lbMethod>  [-
backupLBMethod <backupLBMethod>] ] [-netmask <netmask>]
[-tolerance <positive_integer>] [-persistenceType (
SOURCEIP | NONE )] [-persistenceId <positive_integer>]
[-persistMask <netmask>] [-timeout <mins>] [-EDR (
ENABLED | DISABLED )] [-MIR ( ENABLED | DISABLED )] [-
disablePrimaryOnDown ( ENABLED | DISABLED )] [-
dynamicWeight <dynamicWeight>] [-
considerEffectiveState ( NONE | STATE_ONLY )] [-
serviceName <string>  -weight <positive_integer>] [-
domainName <string>  [-TTL <secs>]  [-backupIP
<ip_addr>]  [-cookieDomain <string>]  [-cookieTimeout
<mins>]  [-sitedomainTTL <secs>]]
```

Description

Specify different settings on GSLB vserver

Arguments

name

The virtual server name.

backupVServer

Backup server.

backupSessionTimeout

A non zero value enables the feature whose minimum value is 2 minutes. The feature can be disabled by setting the value to zero. The created session is in effect for a specific client per domain. Minimum value: 0 Maximum value: 1440

lbMethod
The load balancing method for the virtual server. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD Default value: PEMGMT_LB_LEASTCONNS

netmask
The netmask to be used in the SOURCEIPHASH policy. Default value: 0xFFFFFFFF

tolerance
The Site selectionn tolerance. Site selection tolerance is the maximum deviation (in milliseconds) in the RTT value, which the System system can tolerate, while deciding the best site for a domain. This value enables the system to implement the Round Robin method of GSLB between sites that have RTT values within this permissible limit. The tolerance value is required only if the LB method is RTT. Maximum value: 100

persistenceType
The persistence type for the virtual server. Possible values: SOURCEIP, NONE

persistenceId
The Persistence Id. This parameter is a positive integer which is used to identify the GSLB VIP on all sites Maximum value: 65535

persistMask
The netmask to be used while SOURCEIP based persistency is ENABLED.This is an optional argument. Default is 255.255.255.255 Default value: 0xFFFFFFFF

timeout
The idle time out in minutes for the persistence entries Default value: 2 Minimum value: 2 Maximum value: 1440

EDR
The state of the System in sending empty DNS response when all the sites participating in GSLB are down. Possible values: ENABLED, DISABLED Default value: DISABLED

MIR
The state of the System in sending Multiple IP addresses in the DNS response. Possible values: ENABLED, DISABLED Default value: DISABLED

disablePrimaryOnDown
When this feature is enabled we will continue to direct traffic to the backup chain even after the primary comes UP. Ideally one should use backup persistence if they want to stick to the same vserver in the chain. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicWeight
The state to consider the svc count or the svc weights or ignore both. Possible values: SERVICECOUNT, SERVICEWEIGHT, DISABLED Default value: DISABLED

considerEffectiveState
Specifies which backup to consider when the primary state of all gslb services bound to the vip are down. By specifying NONE we will not consider the effective state of the gslb service to determine the state of the gslb vip. If STATE_ONLY is chosen we will consider the effective state obtained via MEP to determine the state of the gslb vip Possible values: NONE, STATE_ONLY Default value: NS_GSLB_DONOT_CONSIDER_BKPS

serviceName
The service for which the weight needs to be changed.

domainName
The name of the domain for which TTL and/or backupIP has to be changed.

Example

set gslb vserver gvip -persistenceType SOURCEIP

Related Commands

add gslb vserver
rm gslb vserver
unset gslb vserver
bind gslb vserver
unbind gslb vserver
enable gslb vserver
disable gslb vserver

show gslb vserver
stat gslb vserver

unset gslb vserver

Synopsis

```
unset gslb vserver <name>@ [-backupVServer] [-
backupSessionTimeout] [-lbMethod] [-backupLBMethod] [-
netmask] [-tolerance] [-persistenceType] [-
persistenceId] [-persistMask] [-timeout] [-EDR] [-MIR]
[-disablePrimaryOnDown] [-dynamicWeight] [-
considerEffectiveState] [-serviceName] [-weight]
```

Description

Unset the backup virtual server or redirectURL set on the virtual server..Refer to the set gslb vserver command for meanings of the arguments.

Example

unset gslb vserver lb_vip -backupVServer

Related Commands

add gslb vserver
rm gslb vserver
set gslb vserver
bind gslb vserver
unbind gslb vserver
enable gslb vserver
disable gslb vserver
show gslb vserver
stat gslb vserver

bind gslb vserver

Synopsis

```
bind gslb vserver <name> [(-serviceName <string>  [-
weight <positive_integer>]) | (-domainName <string>  [-
TTL <secs>]  [-backupIP <ip_addr>]  [-cookieDomain
<string>]  [-cookieTimeout <mins>]  [-sitedomainTTL
<secs>])]
```

Description

Bind a domain or service to a GSLB vserver

Arguments

name

The vserver for which the binding operation is to be done

serviceName

The name of the service to be bound with the gslb vserver

domainName

The domain to be bound with this vserver

Example

bind gslb vserver gvip -domainName www.mynw.com

Related Commands

add gslb vserver
rm gslb vserver
set gslb vserver
unset gslb vserver
unbind gslb vserver
enable gslb vserver
disable gslb vserver
show gslb vserver
stat gslb vserver

unbind gslb vserver

Synopsis

```
unbind gslb vserver <name> [-serviceName <string> | (-
domainName <string>  [-backupIP]  [-cookieDomain])]
```

Description

Unbind the domain or service from the gslb vserver

Arguments

name

The vserver for which the unbinding operation is to be performed

serviceName

The service to be unbound from the gslb vserver

domainName

The domain to be unbound from this vserver

Example

unbind gslb vserver gvip -domainName www.mynw.com

Related Commands

add gslb vserver
rm gslb vserver
set gslb vserver
unset gslb vserver
bind gslb vserver
enable gslb vserver
disable gslb vserver
show gslb vserver
stat gslb vserver

enable gslb vserver

Synopsis

```
enable gslb vserver <name>@
```

Description

Enable a virtual server. Note:Virtual servers, when added, are enabled by default.

Arguments

name

The name of the virtual server to be enabled.

Example

enable gslb vserver gslb_vip

Related Commands

add gslb vserver
rm gslb vserver
set gslb vserver
unset gslb vserver
bind gslb vserver
unbind gslb vserver
disable gslb vserver
show gslb vserver
stat gslb vserver

disable gslb vserver

Synopsis

```
disable gslb vserver <name>@
```

Description

Disable (makes out of service) a virtual server.

Arguments

name

The name of the virtual server to be disabled. Notes: 1.The system still responds to ARP and/or ping requests for the IP address of this virtual server. 2.As the virtual server is still configured in the system, you can enable the virtual server using enable vserver CLI command.

Example

disable gslb vserver gslb_vip

Related Commands

add gslb vserver
rm gslb vserver
set gslb vserver
unset gslb vserver
bind gslb vserver
unbind gslb vserver
enable gslb vserver
show gslb vserver
stat gslb vserver

show gslb vserver

Synopsis

```
show gslb vserver [<name>] show gslb vserver stats -
alias for 'stat gslb vserver'
```

Description

Display the GSLB virtual server attributes

Arguments

name

The name of the GSLB virtual server.

summary

fullValues

format

level

Output

serviceType

The service type of the virtual server

persistenceType

Indicates if persistence is set on the gslb vserver

persistenceId

Persistence id of the gslb vserver

lbMethod

The load balancing method set for the virtual server

backupLBMethod

Indicates the backup method in case the primary fails

tolerance

Indicates the deviation we can tolerate when we have the LB method as RTT

timeout
Idle timeout for persistence entries.

state
State of the gslb vserver.

netmask
The netmask used in the SOURCEIPHASH policy.

persistMask
The netmask used while SOURCEIP based persistency is ENABLED.

serviceName
The service name.

weight
Weight for the service.

domainName
The name of the domain for which TTL and/or backupIP has changed.

TTL
TTL for the given domain.

backupIP
Backup IP for the given domain.

cookieDomain

cookieTimeout
Time out value of the cookie in minutes

sitedomainTTL
Site domain TTL.

IPAddress
IP address.

port
Port number.

status
Current status of the gslb vserver. During the initial phase if the configured lb method is not round robin , the vserver will adopt round robin to distribute traffic for a predefined number of requests.

lbrrreason
Reason why a vserver is in RR.

preferredLocation
The target site to be returned in the DNS response when a policy is successfully evaluated against the incoming DNS request. Target site is specified in dotted notation with up to 6 qualifiers. Wildcard `*' is accepted as a valid qualifier token.

backupVServer
Backup vserver in case the primary fails

backupSessionTimeout
A non zero value enables the feature. The minimum value is 2 minutes. To disable the feature set the value to zero. The created session is in effect for a specific client per domain.

EDR
Indicates if Empty Down Response is enabled/disabled

MIR
Indicates if Multi IP Response is enabled/disabled

disablePrimaryOnDown
When this feature is enabled we will continue to direct traffic to the backup chain even after the primary comes UP. Ideally one should use backup persistence if they want to stick to the same vserver in the chain.

dynamicWeight
Dynamic weight method. Possible values are, the svc count or the svc weights or ignore both.

isCname
is cname feature set on vserver

cumulativeWeight
NSA_DYNAMIC_CONF_WT * NSA_WEIGHT

dynamicConfWt
Weight obtained by the virtue of bound service count or weight

thresholdValue
Tells whether threshold exceeded for this service participating in CUSTOMLB

sitePersistence
Type of Site Persistence set

svrEffGslbState
Effective state of the gslb svc

gslbthreshold
Indicates if gslb svc has reached threshold

considerEffectiveState
Specifies which backup to consider when the primary state of all gslb services bound to the vip are down. By specifying NONE we will not consider the effective state of the gslb service to determine the state of the gslb vip. If STATE_ONLY is chosen we will consider the effective state obtained via MEP to determine the state of the gslb vip

cnameEntry
The cname of the gslb service.

totalServices
Total number of services bound to the vserver.

activeServices
Total number of active services bound to the vserver.

stateChangeTimeSec
Time when last state change happened. Seconds part.

stateChangeTimemSec
Time at which last state change happened. Milliseconds part.

ticksSinceLastStateChange
Time in 10 millisecond ticks since the last state change.

Example

show gslb vserver gvip

Related Commands

add gslb vserver
rm gslb vserver
set gslb vserver
unset gslb vserver
bind gslb vserver
unbind gslb vserver
enable gslb vserver
disable gslb vserver
stat gslb vserver

stat gslb vserver

Synopsis

```
stat gslb vserver [<name>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display statistics of a gslb vserver.

Arguments

name

The name of the gslb vserver for which statistics will be displayed. If not given statistics are shown for all gslb vservers.

Output

Counters

Vserver Health (Health)

Health of the vserver. This gives percentage of UP services bound to this vserver.

Vserver protocol (Protocol)

Protocol associated with the vserver

State

Current state of the server.

Vserver hits (Hits)

Total vserver hits

Requests (Req)

The total number of requests received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Responses (Rsp)

Number of responses received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Request bytes (Reqb)
The total number of request bytes received on this service/vserver.

Response bytes (Rspb)
Number of response bytes received on this service/vserver.

Current client connections (ClntConn)
The number of current client connections.

Current server connections (SvrConn)
The number of current connections to the real servers behind the vserver.

Related Commands

add gslb vserver
rm gslb vserver
set gslb vserver
unset gslb vserver
bind gslb vserver
unbind gslb vserver
enable gslb vserver
disable gslb vserver
show gslb vserver

stat gslb domain
stat gslb site
stat gslb service

set gslb parameter

Synopsis

```
set gslb parameter [-ldnsEntryTimeout
<positive_integer>] [-RTTTolerance <positive_integer>]
[-ldnsMask <netmask>]
```

Description

Set different GSLB parameters

Arguments

ldnsEntryTimeout

The idle timeout in seconds of the learnt LDNS entry. If no new DNS request is made within this interval, then the LDNS entry is aged out. Default value: 180

RTTTolerance

The RTT Tolerance in milli seconds. When the RTT is calculated for an LDNS entry, and if the difference between the old RTT and the newly computed one is less than or equal to the RTT Tolerance value, the network metric table is not updated with the new value for this LDNS entry. This is done to prevent exchange of metric when there is small variation in RTT. Default value: 5 Minimum value: 1 Maximum value: 100

ldnsMask

The Netmask. The Netmask specified here is used to store the LDNS IP addresses in the hash table and these are used in dynamic proximity-based GSLB Default value: 0xFFFFFFFF

Example

set gslb parameter -ldnsMask 255.255.0.0

Related Commands

unset gslb parameter

show gslb parameter

unset gslb parameter

Synopsis

```
unset gslb parameter [-ldnsEntryTimeout] [-
RTTTolerance] [-ldnsMask]
```

Description

Use this command to remove gslb parameter settings.Refer to the set gslb parameter command for meanings of the arguments.

Related Commands

set gslb parameter

show gslb parameter

show gslb parameter

Synopsis

```
show gslb parameter
```

Description

Display the GSLB parameters

Arguments

format

level

Output

flags
State of the GSLB parameter.

ldnsEntryTimeout

RTTTolerance

ldnsMask

Example

show gslb parameter

Related Commands

set gslb parameter

unset gslb parameter

add gslb policy

Synopsis

Description

Add GSLB policy NOTE: This command is deprecated.

Arguments

`name`
The name of the GSLB policy

`reqRule`
The expression rule

`action`
The GSLB action to be used when the reqrule is matched

Example

add gslb policy gslb_redirect -reqRule client_Japan -action pref_site

Related Commands

rm gslb policy
set gslb policy
show gslb policy

rm gslb policy

Synopsis

Description

Remove the gslb policy configured in the system NOTE: This command is deprecated.

Arguments

name

The name of the policy to be removed

Example

rm gslb policy gslb_redirect

Related Commands

add gslb policy

set gslb policy

show gslb policy

set gslb policy

Synopsis

Description

Change the action for the given gslb policy NOTE: This command is deprecated.

Arguments

`name`

The name of the gslb policy.

`action`

The action to be taken for the given gslb policy

Example

set gslb policy gslb_redirect -action redirect_asia

Related Commands

add gslb policy

rm gslb policy

show gslb policy

show gslb policy

Synopsis

Description

Display the configured GSLB policy NOTE: This command is deprecated.

Arguments

name

The name of the GSLB policy.

format

level

Output

reqRule

action

The action taken for the given gslb policy.

hits

Number of policy hits for the gslb policy.

Example

show gslb policy

Related Commands

add gslb policy

rm gslb policy

set gslb policy

add gslb action

Synopsis

Description

Add GSLB action used in the GSLB policy NOTE: This command is deprecated.

Arguments

`name`

The name of the GSLB action

`preferredLocation`

The target site to be returned in the DNS response when a policy is successfully evaluated against the incoming DNS request. Target site is specified in dotted notation with up to 6 qualifiers. Wildcard `*' is accepted as a valid qualifier token.

Example

add gslb action pref_site -preferredlocation NorthAmerica.US.*.*.*.*

Related Commands

rm gslb action

set gslb action

show gslb action

rm gslb action

Synopsis

Description

Remove the gslb action configured in the system NOTE: This command is deprecated.

Arguments

name

The name of the action to be removed

Example

rm gslb action redirect_asia

Related Commands

add gslb action

set gslb action

show gslb action

set gslb action

Synopsis

Description

Change the preferredlocation of the given gslb action NOTE: This command is deprecated.

Arguments

`name`

The name of the GSLB action

`preferredLocation`

The target site to be returned in the DNS response when a policy is successfully evaluated against the incoming DNS request. Target site is specified in dotted notation with up to 6 qualifiers. Wildcard `*' is accepted as a valid qualifier token.

Example

set gslb action pref_site -preferredlocation NorthAmerica.US.*.*.*.*

Related Commands

add gslb action

rm gslb action

show gslb action

show gslb action

Synopsis

Description

Display the GSLB actions configured NOTE: This command is deprecated.

Arguments

`name`

The name of the action.

`format`

`level`

Output

`preferredLocation`

Example

show gslb action

Related Commands

add gslb action

rm gslb action

set gslb action

show gslb ldnsentries

Synopsis

```
show gslb ldnsentries
```

Description

Displays the LDNS entries.

Arguments

summary

fullValues

Output

IPAddress
IP address of the LDNS server

TTL
TTL value of the LDNS entry

name
Monitor that is currently being used to monitor the LDNS ip..

Example

show gslb ldnsentries

Related Commands

rm gslb ldnsentry

Synopsis

```
rm gslb ldnsentry <IPAddress>
```

Description

Removes the LDNS entry corresponding to the IP address given

Arguments

IPAddress

IP address of the LDNS server

Example

rm gslb ldnsentry 10.102.27.226

Related Commands

sync gslb config

Synopsis

```
sync gslb config [-preview | -forceSync <string>] [-
debug]
```

Description

Synchronize the GSLB running configuration on all NetScalers participating in GSLB. The NetScaler on which this command is run is considered the "master node". All GSLB sites configured on the master, which do not have a parent, will be brought in sync with the master node.

Arguments

preview

Preview of the commands that are applied on the slave node. This won't initiate the gslb auto sync.

debug

A more verbose output of gslb auto sync.

forceSync

Forcibly sync the config from master to slave. The slave is identified with the sitename supplied as part of the argument. If the supplied argument is "all-sites", the config will be pushed to all slave nodes.

Related Commands

show gslb syncStatus

Synopsis

```
show gslb syncStatus
```

Description

Shows the status of the master and slave nodes configured for GSLB Auto Sync.

Arguments

Output

Related Commands

CHAPTER 18

Load Balancing Commands

This chapter covers the load balancing commands.

show lb monbindings

Synopsis

```
show lb monbindings <monitorName>
```

Description

Display the services to which this monitor is bound

Arguments

monitorName
The name of the monitor.

summary

fullValues

Output

type
The type of monitor.

state
The state of the monitor.

monState
The configured state (enable/disable) of Monitor on this service.

IPAddress
The IPAddress of the service.

port
The port of the service.

serviceName
The name of the service.

serviceType
The type of service

svrState
The state of the service

state

Related Commands

rm lb monitor

Synopsis

```
rm lb monitor <monitorName> <type> [-respCode <int[-int]> ...]
```

Description

Remove either a specified monitor or response code for the HTTP monitor. While the response codes for a specified monitor are removed, the monitor itself is not removed. Built-in monitors can not be removed.

Arguments

`monitorName`
The name of the monitor.

`type`
The type of monitor. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC

`respCode`
The response codes to be deleted from the response codes list of the HTTP monitor.

Example

rm monitor http_mon http

Related Commands

enable lb monitor

disable lb monitor

add lb monitor

set lb monitor

unset lb monitor

show lb monitor

enable lb monitor

Synopsis

```
enable lb monitor (<serviceName>@ |
<serviceGroupName>@) [<monitorName>]
```

Description

Enable the monitor that is bound to a specific service. If no monitor name is specified, all monitors bound to the service are enabled.

Arguments

`serviceName`
The name of the service to which the monitor is bound.

`serviceGroupName`
The name of the service group to which the monitor is to be bound.

`monitorName`
The name of the monitor.

Example

enable monitor http_svc http_mon

Related Commands

add service
rm lb monitor
disable lb monitor
add lb monitor
set lb monitor
unset lb monitor
show lb monitor

disable lb monitor

Synopsis

```
disable lb monitor (<serviceName>@ |
<serviceGroupName>@) [<monitorName>]
```

Description

Disable the monitor for a service. If the monitor name is not specified, all monitors bound to the service are disabled.

Arguments

`serviceName`
The name of the service being monitored.

`serviceGroupName`
The name of the service group being monitored.

`monitorName`
The name of the monitor.

Example

disable monitor http_svc http_mon

Related Commands

add service
rm lb monitor
enable lb monitor
add lb monitor
set lb monitor
unset lb monitor
show lb monitor

show lb persistentSessions

Synopsis

```
show lb persistentSessions [<vServer>]
```

Description

Get all vserver persistent sessions

Arguments

vServer
The name of the virtual server.

summary

fullValues

Output

type
The netmask of this IP.

srcIP
SOURCE IP.

srcIPv6
SOURCE IPv6 ADDRESS.

destIP
DESTINATION IP.

destIPv6
DESTINATION IPv6 ADDRESS.

flags
IPv6 FLAGS.

destPort
Destination port.

vServerName
Virtual server name.

timeout
Persistent Session timeout.

referenceCount
Reference Count.

sipCallID
SIP CALLID.NOTE: This attribute is deprecated.Replaced by "persistenceParam" field

persistenceParam
Specific persistence information . Callid in case of SIP_CALLID persistence entry , RTSP session id in case of RTSP_SESSIONID persistence entry.

Related Commands

clear lb persistentSessions

clear lb persistentSessions

Synopsis

```
clear lb persistentSessions [<vServer>]
```

Description

Use this command to clear/flush persistent sessions

Arguments

vServer

The name of the LB vserver whose persistence sessions are to be flushed. If not specified, all persistence sessions will be flushed .

Related Commands

show lb persistentSessions

set lb group

Synopsis

```
set lb group <name>@ [-persistenceType
<persistenceType>] [-persistenceBackup ( SOURCEIP |
NONE )] [-backupPersistenceTimeout <mins>] [-
persistMask <netmask>] [-cookieDomain <string>] [-
timeout <mins>]
```

Description

Set the persistence for the group (used in the system's load balancing feature). Persistence is set for the connections between a client and a server that is being load balanced by the system. The client will be directed to the same server until client's transactions have completed (or until the time period that you have specified has passed). Before using this command, the group must be created. The group is created implicitly when binding a load balancing virtual server to a group using the bind lb group CLI command. Similarly a group is removed when the last load balancing virtual server is unbound from it using the unbind lb group CLI command.

Arguments

name

The name of the group.

persistenceType

The persistence type for the group. Select SOURCEIP - This option is used to maintain persistency based on the client IP. COOKIEINSERT- This option is used to maintain persistency based on the cookie in the client request.This cookie is inserted by the system in the first response to the client. NONE - To disable the persistency. Possible values: SOURCEIP, COOKIEINSERT, NONE

persistenceBackup

The backup persistence type for the group. Possible values: SOURCEIP, NONE

backupPersistenceTimeout
The maximum time backup persistence is in effect for a specific client. Default value: 2 Minimum value: 2 Maximum value: 1440

persistMask
The netmask to be applied when the persistency type is SOURCEIP.

cookieDomain
The domain attribute of the HTTP cookie.

timeout
The maximum time that persistence is in effect for a specific client. Default value: 2 Maximum value: 1440

Example

set lb group webgrp -persistenceType COOKIEINSERT

Related Commands

unset lb group

bind lb group

unbind lb group

show lb group

unset lb group

Synopsis

```
unset lb group <name>@ [-persistenceType] [-
persistenceBackup] [-backupPersistenceTimeout] [-
persistMask] [-cookieDomain] [-timeout]
```

Description

Use this command to remove lb group settings.Refer to the set lb group command for meanings of the arguments.

Related Commands

set lb group

bind lb group

unbind lb group

show lb group

bind lb group

Synopsis

```
bind lb group <name>@ <vServerName>@ ...
```

Description

Create a group of virtual servers in the system. This group supports server persistence. Only address-based (not content-based) virtual servers can be added to a group. Each virtual server can only be assigned to one group. When moving a virtual server from one group to another, the virtual server must be removed from the original group with the unbind lb group command.

Arguments

name

The name of the group. A maximum of 31 characters can be used to specify a new name to a group of virtual servers that you are creating (or to specify an existing group name if you are adding the virtual server to an existing group of virtual servers.

vServerName

The name of the virtual server that will belong to the named group.

Example

bind lb group webgrp http_vip

Related Commands

set lb group

unset lb group

unbind lb group

show lb group

unbind lb group

Synopsis

```
unbind lb group <name> <vServerName>@ ...
```

Description

Unbind the virtual server from a group. When the last vserver is unbound, the group is deleted from system.

Arguments

name

The name of the group.

vServerName

The name of the virtual server to be removed from the group. Multiple names can be specified.

Example

unbind lb group webgroup http_vip

Related Commands

set lb group

unset lb group

bind lb group

show lb group

show lb group

Synopsis

```
show lb group [<name>]
```

Description

Display the names of the virtual servers associated to the specified group. The virtual servers were created using the ###add vserver### command.

Arguments

name

The name of the group.

summary

fullValues

format

level

Output

vServerName

Virtual server name.

persistenceType

The type of the persistence set for the group.

persistenceBackup

The type of the backup persistence set for the group.

backupPersistenceTimeout

The maximum time backup persistence is in effect for a specific client.

persistMask

The netmask applied when the persistency type is SOURCEIP.

cookieDomain

`timeout`
The maximum time that persistence is in effect for a specific client.

Example

show lb group webgrp

Related Commands

add vserver
set lb group
unset lb group
bind lb group
unbind lb group

add lb monitor

Synopsis

```
add lb monitor <monitorName> <type> [-action <action>]
[-respCode <int[-int]> ...] [-httpRequest <string>] [-
rtspRequest <string>] [-customHeaders <string>] [-
maxForwards <integer>] [-sipMethod <sipMethod>] [-
sipURI <string>] [-sipregURI <string>] [-send <string>]
[-recv <string>] [-query <string>] [-queryType
<queryType>] [-scriptName <string>] [-scriptArgs
<string>] [-dispatcherIP <ip_addr>] [-dispatcherPort
<port>] [-userName <string>] {-password } {-
secondaryPassword } [-logonpointName <string>] [-
lasVersion <string>] {-radKey } [-radNASid <string>] [-
radNASip <ip_addr>] [-LRTM ( ENABLED | DISABLED )] [-
deviation <integer>  [<units>]] [-interval <integer>
[<units>]] [-resptimeout <integer>  [<units>]] [-
resptimeoutThresh <positive_integer>] [-retries
<integer>] [-failureRetries <integer>] [-alertRetries
<integer>] [-successRetries <integer>] [-downTime
<integer>  [<units>]] [-destIP <ip_addr|ipv6_addr|*>]
[-destPort <port>] [-state ( ENABLED | DISABLED )] [-
reverse ( YES | NO )] [-transparent ( YES | NO )] [-
ipTunnel ( YES | NO )] [-tos ( YES | NO )] [-tosId
<positive_integer>] [-secure ( YES | NO )] [-IPAddress
<ip_addr|ipv6_addr|*> ...] [-group <string>] [-fileName
<string>] [-baseDN <string>] [-bindDN <string>] [-
filter <string>] [-attribute <string>] [-database
<string>] [-sqlQuery <text>] [-snmpOID <string>] [-
snmpCommunity <string>] [-snmpThreshold <string>] [-
snmpVersion ( V1 | V2 )] [-metricTable <string>] [-
application <string>] [-sitePath <string>]
```

Description

Add a monitor to the system.

Arguments

monitorName

The name of the monitor.

type

The type of monitor. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC

action

The action to be taken in INLINE monitors. Possible values: NONE, LOG, DOWN Default value: SM_DOWN

respCode

The response codes. For the probe to succeed, the HTTP/RADIUS response from the server must be of one of the types specified.

httpRequest

The HTTP request that is sent to the server (for example, "HEAD /file.html"). Default value: "\007"

rtspRequest

The RTSP request that is sent to the server (for example, "OPTIONS *"). Default value: "\007"

customHeaders

The custom header string, attached to the monitoring probes.

maxForwards

SIP packet max-forwards Default value: 1 Minimum value: 0 Maximum value: 255

sipMethod

SIP method to be used for the query Possible values: OPTIONS, INVITE, REGISTER Default value: NS_T_OPTIONS

sipURI
SIP method string, sent to the server. For example "OPTIONS sip:sip.test".

sipregURI
SIP user to be registered

send
The string that is sent to the service. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitor types. Default value: "\007"

recv
The string that is expected from the server to mark the server as UP. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitor types.

query
The DNS query (domain name) sent to the DNS service that is being monitored. Default value: "\007"

queryType
The type of DNS query that is sent. Possible values: Address, Zone, AAAA, Address

scriptName
The path and name of the script to execute.

scriptArgs
The string that are put in the POST data - they are copied to the request verbatim.

dispatcherIP
The IP Address of the dispatcher to which the probe is sent.

dispatcherPort
The port of the dispatcher to which the probe is sent.

userName
Username on the RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/ CITRIX_AG server. This user name is used in the probe.

password
Password used in RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/ LDAP/CITRIX-AG server monitoring.

secondaryPassword
Secondary password used in Citrix Access Gateway server monitoring. Default value:

logonpointName
Logonpoint name used in Citrix AAC login page and logon agent service monitoring.

lasVersion
The version of the Citrix AAC logon agent service required by CITRIX-AAC-LAS monitor.

radKey
The radius key.

radNASid
The NAS ID to be used in Radius monitoring.

radNASip
The NAS IP to be used in Radius monitoring.

LRTM
The state of response time calculation of probes. Possible values: ENABLED, DISABLED Default value: VAL_NOT_SET

deviation
Deviation from the learnt response time for Dynamic Response Time monitoring. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes.

interval
The frequency at which the probe is sent to a service.The interval should be greater than the response timeout. The minimum value is 20 msec.The maximum value is 20940000 in milliseconds , 20940 in seconds and 349 in minutes Default value: 5 Minimum value: 1

resptimeout
The interval for which the system waits before it marks the probe as FAILED. The response timeout should be less than the value specified in -interval parameter. The UDP-ECV monitor type does not decide the probe failure by the response timeout. System considers the probe successful for UDP-ECV monitor type, when the server response matches the criteria set by the -send and -recv options or if the response is not received from the server (unless the

-reverse option is set to yes). Note:The -send option specifies what data is to be sent to the server in the probe and -recv specifies the server response criteria for the probe to succeed. The probe failure is caused by the ICMP port unreachable error from the service. The minimum value is 10 msec. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes Default value: 2 Minimum value: 1

resptimeoutThresh
Monitor response timeout threshold , a trap will be sent if the response time for the monitoring probes exceeds the thereshold. It is given in percentage. Minimum value: 0 Maximum value: 100

retries
The maximum number of most recent probes considered to decide whether to mark the service as DOWN. Minimum value of retries is 1. Default value: 3

failureRetries
The number of failed probes out of most recent "retries" number of probes required to mark the service as DOWN. By default, the system requires "retries" number of consecutive probe failures to mark the service as DOWN. Default value: 0 Minimum value: 0 Maximum value: 32

alertRetries
The number of probes failures after which the system generates a snmp trap. Default value: 0 Minimum value: 0 Maximum value: 32

successRetries
The number of consecutive sucessful probes required to mark the service as UP. Default value: 1 Minimum value: 1 Maximum value: 32

downTime
The duration for which the system waits to make the next probe once the service is marked as DOWN. The minimum value is 10 msec. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes Default value: 30 Minimum value: 1

destIP
The IP address to which the probe is sent. If the destination IP address is set to 0, the destination IP address is that of the server to which the monitor is bound. Default value: 0

destPort
The TCP/UDP port to which the probe is sent. If the destination port is set to 0, the destination port is of the service to which the monitor is bound. For a USER monitor, however, this will be the port sent in the HTTP request to the dispatcher. This option is ignored if the monitor is of the PING type.

state
The state of the monitor. If the monitor is disabled, this monitor-type probe is not sent for all services. If the monitor is bound, the state of this monitor is not taken into account when the service of this state is determined. Possible values: ENABLED, DISABLED Default value: ENABLED

reverse
The state of reverse probe's criterion check. Possible values: YES, NO Default value: NO

transparent
The state of the monitor for transparent devices, such as firewalls, based on the responsiveness of the services behind them. If the monitoring of transparent devices is enabled, the destination IP address should be specified. The probe is sent to the specified destination IP address using the MAC address of the transparent device. Possible values: YES, NO Default value: NO

ipTunnel
The state of the monitor for tunneled devices. If the monitoring of tunneled devices is enabled, the destination IP address should be specified. The probe is sent to the specified destination IP address by tunneling it to the device. Possible values: YES, NO Default value: NO

tos
If enabled, the probe is sent to the service by encoding the specified destination IP address in the IP TOS (6)bits. Possible values: YES, NO

tosId
Use this parameter to specify the TOS ID of the specified destination IP. Applicable only when the -tos is enabled Minimum value: 1 Maximum value: 63

secure
The state of the secure monitoring of services. SSL handshake will be done on the TCP connection established. Applicable only for TCP based monitors.

This option can't be used in conjuction with CITRIX-AG monitor as this monitor is a secure monitor by default. Possible values: YES, NO Default value: NO

IPAddress
List of IP address to be checked against the response to the DNS monitoring probe. Applicable only to the DNS monitors.

group
Group name to be queried for NNTP monitor.

fileName
File name to be used for FTP-EXTENDED monitor.

baseDN
Base name for the LDAP monitor.

bindDN
BDN name for the LDAP monitor.

filter
Filter for the LDAP monitor.

attribute
Attribute for the LDAP monitor.

database
Database to be used for the MYSQL monitor.

sqlQuery
SQL query to be used for the MYSQL monitor.

snmpOID
OID to be used for the SNMP monitor.

snmpCommunity
Community to be used for the SNMP monitor.

snmpThreshold
Threshold to be used for the SNMP monitor.

snmpVersion
SNMP version to be used for LOAD monitoring. Possible values: V1, V2

`metricTable`
Metric table to use for the metrics that are going to be bound. Maximum value: 99

`application`
Name of the application that has to be executed to check the state of the service

`sitePath`
URL of the logon page

Example

add monitor http_mon http

Related Commands

rm lb monitor
enable lb monitor
disable lb monitor
set lb monitor
unset lb monitor
show lb monitor

set lb monitor

Synopsis

```
set lb monitor <monitorName> <type> [-action <action>]
[-respCode <int[-int]> ...] [-httpRequest <string>] [-
rtspRequest <string>] [-customHeaders <string>] [-
maxForwards <integer>] [-sipMethod <sipMethod>] [-
sipregURI <string>] [-sipURI <string>] [-send <string>]
[-recv <string>] [-query <string>] [-queryType
<queryType>] [-userName <string>] {-password } {-
secondaryPassword } [-logonpointName <string>] [-
lasVersion <string>] {-radKey } [-radNASid <string>] [-
radNASip <ip_addr>] [-LRTM ( ENABLED | DISABLED )] [-
deviation <integer>  [<units>]] [-scriptName <string>]
[-scriptArgs <string>] [-dispatcherIP <ip_addr>] [-
dispatcherPort <port>] [-interval <integer>  [<units>]]
[-resptimeout <integer>  [<units>]] [-resptimeoutThresh
<positive_integer>] [-retries <integer>] [-
failureRetries <integer>] [-alertRetries <integer>] [-
successRetries <integer>] [-downTime <integer>
[<units>]] [-destIP <ip_addr|ipv6_addr|*>] [-destPort
<port>] [-state ( ENABLED | DISABLED )] [-reverse ( YES
| NO )] [-transparent ( YES | NO )] [-ipTunnel ( YES |
NO )] [-tos ( YES | NO )] [-tosId <positive_integer>]
[-secure ( YES | NO )] [-IPAddress
<ip_addr|ipv6_addr|*> ...] [-group <string>] [-fileName
<string>] [-baseDN <string>] [-bindDN <string>] [-
filter <string>] [-attribute <string>] [-database
<string>] [-sqlQuery <text>] [-snmpOID <string>] [-
snmpCommunity <string>] [-snmpThreshold <string>] [-
snmpVersion ( V1 | V2 )] [-metricTable <string>] [-
metric <string>  [-metricThreshold <positive_integer>]
[-metricWeight <positive_integer>]] [-application
<string>] [-sitePath <string>]
```

Description

Use this command to modify the parameters of a specific monitor.

Arguments

monitorName
The name of the monitor that is being set.

type
The type of monitor. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC

action
The action to be taken in INLINE monitors. Possible values: NONE, LOG, DOWN Default value: SM_DOWN

respCode
The response codes.

httpRequest
The HTTP request that is sent to the server. Default value: "\007"

rtspRequest
The RTSP request that is sent to the server (for example, "OPTIONS *"). Default value: "\007"

customHeaders
The string that is sent to the service. Applicable to HTTP and HTTP-ECV monitor types.

maxForwards
SIP packet max-forwards Default value: 1 Minimum value: 0 Maximum value: 255

sipMethod
SIP method to be used for the query Possible values: OPTIONS, INVITE, REGISTER Default value: NS_T_OPTIONS

sipURI
SIP uri string, sent to the server. For example "sip:sip.test".

send
The string that is sent to the service. Default value: "\007"

recv
The string that is expected from the server to mark the server as UP.

query
The DNS query (domain name) sent to the DNS service that is being monitored. Default value: "\007"

queryType
The type of DNS query that is sent. Possible values: Address, Zone, AAAA, Address

userName
Username on the RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/ CITRIX-AG server. This user name is used in the probe.

password
Password used in RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/ LDAP/CITRIX-AG server monitoring.

secondaryPassword
Secondary password used in Citrix Access Gateway server monitoring.

logonpointName
Logonpoint name used in Citrix AAC login page and logon agent service monitoring.

lasVersion
The version of the Citrix AAC logon agent service required by CITRIX-AAC-LAS monitor.

radKey
The radius key.

radNASid
The NAS ID to be used in Radius monitoring.

radNASip
The NAS IP to be used in Radius monitoring.

LRTM
The state of response time calculation of probes. Possible values: ENABLED, DISABLED

deviation
Deviation from the learnt response time for Dynamic Response Time monitoring. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes.

scriptName
The path and name of the script to execute.

scriptArgs
The string that are put in the POST data - they are copied to the request verbatim.

dispatcherIP
The IP Address of the dispatcher to which the probe is sent.

dispatcherPort
The port of the dispatcher to which the probe is sent.

interval
The frequency at which the probe is sent to the service.The minimum value is 20 msec.The maximum value is 20940000 in milliseconds , 20940 in seconds and 349 in minutes Default value: 5 Minimum value: 1

resptimeout
The interval for which the system waits before it marks the probe as FAILED. The minimum value is 10 msec. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes. Default value: 2 Minimum value: 1

resptimeoutThresh
Monitor response timeout threshold , a trap will be sent if the response time for the monitoring probes exceeds the thereshold. It is given in percentage. Minimum value: 0 Maximum value: 100

retries
The maximum number of most recent probes considered to decide whether to mark the service as DOWN. Minimum value of retries is 1. Default value: 3

failureRetries
The number of failed probes out of most recent "retries" number of probes required to mark the service as DOWN. By default, the system requires "retries" number of consecutive probe failures to mark the service as DOWN. Minimum value: 0 Maximum value: 32

alertRetries
The number of probes failures after which the system generates a snmp trap. Minimum value: 0 Maximum value: 32

successRetries
The number of consecutive sucessful probes required to mark the service as UP. Default value: 1 Minimum value: 1 Maximum value: 32

downTime
The duration for which the system waits to make the next probe once the service is marked as DOWN. The minimum value is 10 msec. The maximum value is 20939000 in milliseconds , 20939 in seconds and 348 in minutes Default value: 30 Minimum value: 1

destIP
The IP address to which the probe is sent. Default value: 0

destPort
The TCP/UDP port to which the probe is sent.

state
The state of the monitor. Possible values: ENABLED, DISABLED Default value: ENABLED

reverse
The state of reverse probe's criterion check. Possible values: YES, NO Default value: NO

transparent
The state of the monitor for transparent devices. Possible values: YES, NO Default value: NO

ipTunnel
The state of the monitor for tunneled devices. Possible values: YES, NO Default value: NO

tos
If enabled, the probe is sent to the service by encoding the specified destination IP address in the IP TOS (6)bits. Possible values: YES, NO

tosId
Use this parameter to specify the TOS ID of the specified destination IP. Applicable only when the -tos is enabled Minimum value: 1 Maximum value: 63

secure
The state of the secure monitoring of services. Possible values: YES, NO Default value: NO

IPAddress
List of IP address to be checked against the response to the DNS monitoring probe. Applicable only to the DNS monitors.

group
Group name to be queried for NNTP monitor.

fileName
File name to be used for FTP-EXTENDED monitor.

baseDN
Base name for the LDAP monitor.

bindDN
BDN name for the LDAP monitor.

filter
Filter for the LDAP monitor.

attribute
Attribute for the LDAP monitor.

database
Database to be used for the MYSQL monitor.

sqlQuery
SQL query to be used for the MYSQL monitor.

snmpOID
OID to be used for the SNMP monitor.

snmpCommunity
Community to be used for the SNMP monitor.

snmpThreshold
Threshold to be used for the SNMP monitor.

snmpVersion
SNMP version to be used for SNMP monitoring. Possible values: V1, V2

metricTable
Metric table to use for the metrics that are going to be bound.

metric
Metric name in the metric table, whose setting is changed. A value zero disables the metric and it will not be used for load calculation Maximum value: 37

application
Name of the application that has to be executed to check the state of the service

sitePath
URL of the logon page

Example

set monitor http_mon http -respcode 100

Related Commands

rm lb monitor
enable lb monitor
disable lb monitor
add lb monitor
unset lb monitor
show lb monitor

unset lb monitor

Synopsis

```
unset lb monitor <monitorName> <type> [-IPAddress
<ip_addr|ipv6_addr|*> ...] [-action] [-respCode] [-
httpRequest] [-rtspRequest] [-customHeaders] [-
maxForwards] [-sipMethod] [-sipregURI] [-sipURI] [-
send] [-recv] [-query] [-queryType] [-userName] [-
password] [-secondaryPassword] [-logonpointName] [-
lasVersion] [-radKey] [-radNASid] [-radNASip] [-LRTM]
[-deviation] [-scriptName] [-scriptArgs] [-
dispatcherIP] [-dispatcherPort] [-interval] [-
resptimeout] [-resptimeoutThresh] [-retries] [-
failureRetries] [-alertRetries] [-successRetries] [-
downTime] [-destIP] [-destPort] [-state] [-reverse] [-
transparent] [-ipTunnel] [-tos] [-tosId] [-secure] [-
group] [-fileName] [-baseDN] [-bindDN] [-filter] [-
attribute] [-database] [-sqlQuery] [-snmpOID] [-
snmpCommunity] [-snmpThreshold] [-snmpVersion] [-
metricTable]
```

Description

Use this command to modify the parameters of a specific monitor..Refer to the set lb monitor command for meanings of the arguments.

Example

set monitor dns_mon dns -ipaddress 10.102.27.230

Related Commands

rm lb monitor

enable lb monitor

disable lb monitor

add lb monitor

set lb monitor

show lb monitor

bind lb monitor

Synopsis

```
bind lb monitor <monitorName> ((<serviceName>@ [-state
( ENABLED | DISABLED )] [-weight <positive_integer>])
| ((<serviceGroupName>@ [-state ( ENABLED | DISABLED
)] [-weight <positive_integer>]) | (-metric <string>
-metricThreshold <positive_integer> [-metricWeight
<positive_integer>])))
```

Description

Use this command to bind a monitor to a service. Multiple monitors can be bound to the service. The server's state is determined by the state of all the bound monitors using the AND condition. All monitor's probes have to succeed for the service to be in the UP state.

Arguments

monitorName
The name of the monitor to be bound.

serviceName
The name of the service or a service group to which the monitor is to be bound.

serviceGroupName
The name of the service group to which the monitor is to be bound.

metric
The name of the metric from the table to be used for this monitor.

Example

bind monitor http_mon http_svc

Related Commands

unbind lb monitor

unbind lb monitor

Synopsis

```
unbind lb monitor <monitorName> (<serviceName>@ |
<serviceGroupName>@ | -metric <string>)
```

Description

Use this command to unbind a specified monitor from the service.

Arguments

monitorName
The name of the monitor to be unbound.

serviceName
The service name from which the monitor is to be unbound.

serviceGroupName
The service group name from which the monitor is to be unbound.

metric
The name of the metric from the table to be used for this monitor.

Example

unbind monitor http_mon http_svc

Related Commands

bind lb monitor

show lb monitor

Synopsis

```
show lb monitor [<monitorName>] [<type>] show lb
monitor bindings - alias for 'show lb monbindings'
```

Description

Display the parameters for the specified monitor. If the monitor_name argument is not specified, a list of all existing monitors is returned.

Arguments

monitorName
The name of the monitor.

type
The type of monitor. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC

summary

fullValues

format

level

Output

interval
The frequency at which the probe is sent to the service.

units
monitor interval units

resptimeout
The interval for which the system waits before it marks the probe as FAILED.

resptimeoutThresh
Monitor response timeout threshold , a trap will be sent if the response time for the monitoring probes exceeds the thereshold. It is given in percentage.

units
monitor response timeout units

retries
The maximum number of most recent probes considered to decide whether to mark the service as DOWN. Minimum value of retries is 1.

failureRetries
The number of failed probes out of most recent "retries" number of probes required to mark the service as DOWN. By default, the system requires "retries" number of consecutive probe failures to mark the service as DOWN.

alertRetries
The number of failures after which the system generates a SNMP trap.

successRetries
The number of consecutive sucessful probes required to mark the service as UP.

downTime
The duration in seconds for which the system waits to make the next probe once the service is marked as DOWN.

units
monitor downtime units

destIP
The IP address to which the probe is sent.

destPort
The TCP/UDP port to which the probe is sent.

state
The state of the monitor.

reverse
The state of reverse probe's criterion check.

transparent
The state of the monitor for transparent devices.

ipTunnel
The state of the monitor for tunneled devices.

tos
TOS setting.

tosId
TOS ID

secure
The state of the secure monitoring of services.

action
The action to be taken in INLINE monitors.

respCode
The response codes.

httpRequest
The HTTP request that is sent to the server.

rtspRequest
The RTSP request that is sent to the server.

send
The string that is sent to the service.

recv
The string that is expected from the server to mark the server as UP.

query
The DNS query (domain name) sent to the DNS service that is being monitored.

queryType
The type of DNS query that is sent.

userName
Username on the RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3 server. This user name is used in the probe.

password
Password used in RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/ LDAP server monitoring.

secondaryPassword
Secondary password used in Citrix Access Gateway server monitoring.

logonpointName
Logonpoint name used in Citrix AAC login page monitoring.

lasVersion
The version of the Citrix AAC logon agent service required by CITRIX-AAC-LAS monitor.

radKey
The radius key.

radNASid
The NAS ID to be used in Radius monitoring.

radNASip
The NAS IP to be used in Radius monitoring.

LRTM
The state of response time calculation of probes.

lrtmConf
State of LRTM configuration on the monitor.

deviation
Deviation from the learnt response time for Dynamic Response Time monitoring.

units
Deviation units.

dynamicResponseTimeout
Response timeout of the DRTM enabled monitor , calculated dynamically based on the history and current response time.

dynamicInterval
Interval between monitoring probes for DRTM enabled monitor , calculated dynamically based monitor response time.

scriptName
The path and name of the script to execute.

scriptArgs
The string that are put in the POST data - they are copied to the request verbatim.

dispatcherIP
The IP Address of the dispatcher to which the probe is sent.

dispatcherPort
The port of the dispatcher to which the probe is sent.

sipURI

sipMethod
Specifies SIP method to be used for the query

maxForwards
Maximum number of hops a sip monitor packet can go.

sipregURI
Specifies SIP user to be registered

customHeaders
The string that is sent to the service. Applicable to HTTP ,HTTP-ECV and RTSP monitor types.

IPAddress
List of IP address to be checked against the response to the DNS monitoring probe. Applicable only to the DNS monitors.

group
Group name to be queried for NNTP monitor.

fileName
File name to be used for FTP-EXTENDED monitor.

baseDN
Base name for the LDAP monitor.

bindDN
BDN name for the LDAP monitor.

filter
Filter for the LDAP monitor.

attribute
Attribute for the LDAP monitor.

database
Database to be used for the MYSQL monitor.

sqlQuery
SQL query to be used for the MYSQL monitor.

snmpOID
OID to be used for the SNMP monitor.

snmpCommunity
Community to be used for the SNMP monitor.

snmpThreshold
Threshold to be used for the SNMP monitor.

snmpVersion
SNMP version to be used for SNMP monitoring.

metric
Metric name in the metric table, whose setting is changed

metricTable
Metric table, whose setting is changed

metricThreshold
Threshold to be used for that metric.

metricWeight
The weight for the specified service metric with respect to others.

flags
Flags controlling the display.NOTE: This attribute is deprecated.This is deprecated attribute.

state
Flags controlling the display.

application
Name of the application that has to be executed to check the state of the service

sitePath
URL of the logon page

units
Giving the unit of the metric

Example

An example of the show monitor command output is as follows: 8 configured monitors: 1) Name.....: ping Type.....: PING State....ENABLED 2) Name.....: tcp Type.....: TCP State....ENABLED 3) Name.....: http Type.....: HTTP State....ENABLED 4) Name.....: tcp-ecv Type.....: TCP-ECV State....ENABLED 5) Name.....: http-ecv Type.....: HTTP-ECV State....ENABLED 6) Name.....: udp-ecv Type.....: UDP-ECV State....ENABLED 7) Name.....: dns Type.....: DNS State....ENABLED 8) Name.....: ftp Type.....: FTP State....ENABLED

Related Commands

rm lb monitor
enable lb monitor
disable lb monitor
add lb monitor
set lb monitor
unset lb monitor

add lb route

Synopsis

```
add lb route <network> <netmask> <gatewayName>
```

Description

Bind the route VIP to the route structure.

Arguments

network

The IP address of the network to which the route belongs.

netmask

The netmask to which the route belongs.

gatewayName

The name of the route.

Related Commands

rm lb route

show lb route

rm lb route

Synopsis

```
rm lb route <network> <netmask>
```

Description

Remove the route VIP from the route structure.

Arguments

network

The IP address of the network to which the route VIP belongs.

netmask

The netmask of the destination network.

Related Commands

add lb route

show lb route

show lb route

Synopsis

```
show lb route [<network>  <netmask>]
```

Description

Display the names of the routes associated to the route structure using the ###add lb route### command.

Arguments

network
The destination network or host.

summary

fullValues

format

level

Output

gatewayName

flags
State of the configured gateway.

Related Commands

add lb route
rm lb route

add lb vserver

Synopsis

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@  [-
range <positive_integer>]) | (-IPPattern <ippat>  -
IPMask <ipmask>)] [<port>] [-persistenceType
<persistenceType>] [-timeout <mins>] [-
persistenceBackup ( SOURCEIP | NONE )] [-
backupPersistenceTimeout <mins>] [-lbMethod <lbMethod>
[-hashLength <positive_integer>]  [-netmask <netmask>]
] [-rule <expression>] [-resRule <expression>] [-
persistMask <netmask>] [-pq ( ON | OFF )] [-sc ( ON |
OFF )] [-rtspNat ( ON | OFF )] [-m <m>] [-tosId
<positive_integer>] [-dataLength <positive_integer>]
[-dataOffset <positive_integer>] [-sessionless (
ENABLED | DISABLED )] [-state ( ENABLED | DISABLED )]
[-connfailover <connfailover>] [-redirectURL <URL>] [-
cacheable ( YES | NO )] [-cltTimeout <secs>] [-soMethod
<soMethod>] [-soPersistence ( ENABLED | DISABLED )] [-
soPersistenceTimeOut <positive_integer>] [-soThreshold
<positive_integer>] [-redirectPortRewrite ( ENABLED |
DISABLED )] [-downStateFlush ( ENABLED | DISABLED )] [-
backupVServer <string>] [-disablePrimaryOnDown (
ENABLED | DISABLED )] [-insertVserverIPPort
<insertVserverIPPort>  [<vipHeader>] ] [-
AuthenticationHost <string>] [-Authentication ( ON |
OFF )] [-push ( ENABLED | DISABLED )] [-pushVserver
<string>] [-pushLabel <expression>] [-pushMultiClients
( YES | NO )]
```

Description

Add a load balancing virtual server.

Arguments

name
The name of the load balancing virtual server being added.

serviceType
The service type. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH

IPAddress
The IP address of the virtual server.

IPPattern
The IP Pattern of the virtual server.

port
A port number for the virtual server.

range
The IP range for the network vserver. Default value: 1 Minimum value: 1

persistenceType
Persistence type for the virtual server. Note: The <persistenceType> parameter can take one of the following options: SOURCEIP - When configured, the system selects a physical service based on the Load Balancing method, and then directs all the subsequent requests arriving from the same IP as the first request to the same physical service. COOKIEINSERT - When configured, the system inserts an HTTP cookie into the client responses. The cookie is inserted into the "Cookie" header field of the HTTP response. The client stores the cookie (if enabled) and includes it in all the subsequent requests, which then match the cookie criteria. The cookie contains information about the service where the requests have to be sent. SSLSESSION ID - When configured, the system creates a persistence that is session based on the arriving SSL Session ID, which is part of the SSL handshake process. All requests with the same SSL session ID are directed to the initially selected physical service. CUSTOM SERVER ID -This mode of Persistence requires the server to provide its Server-ID in such a way that it can be extracted from subsequent requests. The system extracts the Server-ID from subsequent client requests and uses it to select a server. The server embeds the Server-ID into the URL query of the HTML links, accessible from the initial page that has to generate persistent HTTP requests. RULE - When

configured, the system maintains persistence based on the contents of the matched rule. This persistence requires an expression to be configured. The expression is created using the add expression CLI command and is configured on a virtual server, using the -rule option of the add lb vserver or set lb vserver CLI command.After successful evaluation of the expression, a persistence session is created and all subsequent matching client requests are directed to the previously selected server. URLPASSIVE - This mode of Persistence requires the server to provide its Server-ID in such a way that it can be extracted from subsequent requests.The system extracts the Server-ID from subsequent client requests and uses it to select a server. The servers which require persistence, embed the Server-ID into the URL query of the HTML links, accessible from the initial page. The Server-ID is its IP address and port specified as a hexadecimal number.URL Passive persistence type requires an expression to be configured that specifies the location of the Server-ID in the client's requests. The expression is created using the CLI command add expression. This expression is configured on a virtual server, using option -rule of the add lb vserver or set lb vserver CLI command. DESTIP -When configured, the system selects a physical service based on the Load Balancing method, and then directs all the subsequent requests with the same destination as the first packet to the same physical service. This will be used in LLB deployment scenarios. SRCIPDESTIP - When configured, the system selects a physical service based on the Load Balancing method, and then directs all the subsequent requests with the same Source IP and Destination IP as the first packet to the same physical service. This will be used in IDS LB depolyments. Possible values: SOURCEIP, COOKIEINSERT, SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPSID, NONE Default value: VAL_NOT_SET

`timeout`

The time period for which the persistence is in effect for a specific client. The value ranges from 2 to 1440 minutes. Default value: 2 Maximum value: 1440

`persistenceBackup`

Use this parameter to specify a backup persistence type for the virtual server. The Backup persistence option is used when the primary configured persistence mechanism on virtual server fails. The <persistenceBacup> parameter can take one of the following options: lSOURCEIP lNONE Possible values: SOURCEIP, NONE

backupPersistenceTimeout

The maximum time backup persistence is in effect for a specific client. Default value: 2 Minimum value: 2 Maximum value: 1440

lbMethod

The load balancing method for the virtual server. The valid options for this parameter are: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH,LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPDESTIPHASH,CUSTOMLOAD. When the load balancing policy is configured as: ROUNDROBIN - When configured, the system distributes incoming requests to each server in rotation, regardless of the load. When different weights are assigned to services then weighted round robin occurs and requests go to services according to how much weighting has been set. LEASTCONNECTION (default value)- When configured, the system selects the service that has the least number of connections. For TCP, HTTP, HTTPS and SSL_TCP services the least number of connections includes: Established, active connections to a service. Connection reuse applies to HTTP and HTTPS. Hence the count includes only those connections which have outstanding HTTP or HTTPS requests, and does not include inactive, reusable connections. Connections to a service waiting in the Surge Queue, which exists only if the Surge Protection feature is enabled. For UDP services the least number of connections includes: The number of sessions between client and a physical service. These sessions are the logical, time-based entities, created on first arriving UDP packet. If configured, weights are taken into account when server selection is performed. LEASTRESPONSETIME - When configured, the system selects the service with the minimum average response time. The response time is the time interval taken when a request is sent to a service and first response packet comes back from the service, that is Time to First Byte (TTFB). URLHASH - The system selects the service based on the hashed value of the incoming URL.To specify the number of bytes of the URL that is used to calculate the hash value use the optional argument [-hashLength <positive_integer>] in either the add lb vserver or set lb vserver CLI command. The default value is 80. DOMAINHASH - When configured with this load balancing method, the system selects the service based on the hashed value of the domain name in the HTTP request. The domain name is taken either from the incoming URL or from the Host header of the HTTP request. Note:The system defaults to LEASTCONNECTION if the request does not contain a domain name. If the domain name appears in both the URL

and the host header, the system gives preference to the URL domain. DESTINATIONIPHASH - The system selects the service based on the hashed value of the destination IP address in the TCP IP header. SOURCEIPHASH - The system selects the service based on the hashed value of the client's IP address in the TCP IP header. LEASTBANDWIDTH - The system selects the service that is currently serving the least traffic, measured in megabits per second. LEASTPACKETS - The system selects the service that is currently serving the lowest number of packets per second. Token -The system selects the service based on the value, calculated from a token, extracted from the client's request (location and size of the token is configurable). For subsequent requests with the same token, the systems will select the same physical server. SRCIPDESTIPHASH - The system selects the service based on the hashed value of the client's SOURCE IP and DESTINATION IP address in the TCP IP header. CUSTOMLOAD - The system selects the service based on the it load which was determined by the LOAD monitors bound to the service. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORTHASH, LRTM, CALLIDHASH, CUSTOMLOAD Default value: PEMGMT_LB_LEASTCONNS

rule

Use this parameter to specify the string value used to set the RULE persistence type. The string can be either an existing rule name (configured using add rule command) or else it can be an in-line expression with a maximum of 256 characters. Default value: "none"

resRule

Use this parameter to specify the expression to be used in response for RULE persistence type. The string is an in-line expression with a maximum of 1500 characters. Default value: "none"

persistMask

Use this parameter to specify if the persistency is IP based. This parameter is Optional. Default value: 0xFFFFFFFF

pq

Use this parameter to enable priority queuing on the specified virtual server. Possible values: ON, OFF Default value: OFF

sc
Use this parameter to enable SureConnect on the specified virtual server. Possible values: ON, OFF Default value: OFF

rtspNat
Use this parameter to enable natting for RTSP data connection. Possible values: ON, OFF Default value: OFF

m
Use this parameter to specify the LB mode. If the value is specified as IP then the traffic is sent to the physical servers by changing the destination IP address to that of the physical server. If the value is MAC then the traffic is sent to the physical servers , by changing the destination MAC address to that of one of the physical servers, the destination IP is not changed. MAC mode is used mostly in Firewall Load Balancing scenario. Possible values: IP, MAC, IPTUNNEL, TOS Default value: NSFWD_IP

tosId
Use this parameter to specify the TOS ID of this vserver. Applicable only when the LB mode is TOS Minimum value: 1 Maximum value: 63

dataLength
Use this parameter to specify the length of the token in bytes. Applicable to TCP virtual servers, when Token Load Balancing method is selected. The datalength should not be more than 24k. Minimum value: 0 Maximum value: 100

dataOffset
Use this parameter to specifies offset of the data to be taken as token. Applicable to the TCP type virtual servers, when Token load balancing method is used. Must be within the first 24k of the client TCP data. Minimum value: 0 Maximum value: 25400

sessionless
Use this parameter to enable sessionless load balancing. Possible values: ENABLED, DISABLED Default value: DISABLED

state
The state of the load balancing virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

connfailover
Specifies the connection failover mode of the virtual server Possible values: DISABLED, STATEFUL, STATELESS Default value: DISABLED

redirectURL
The URL where traffic is redirected if the virtual server in the system becomes unavailable. You can enter up to 127 characters as the URL argument. WARNING!Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the add cs policy CLI command. If the same domain is specified in both arguments, the request will be continuously redirected to the same unavailable virtual server in the system - then the user may not get the requested content.

cacheable
Use this option to specify whether a virtual server, used for load balancing or content switching, routes requests to the cache redirection virtual server before sending it to the configured servers. Possible values: YES, NO Default value: NO

cltTimeout
The timeout value in seconds for idle client connection Maximum value: 31536000

soMethod
The spillover factor based on which the traffic will be given to the backupvserver once the main virtual server reaches the spillover threshold. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence
The state of the spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut
The spillover persistency entry timeout. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold
In case of CONNECTION (or) DYNAMICCONNECTION type spillover method this value is treated as Maximum number of connections a lb vserver will handle before spillover takes place. In case of BANDWIDTH type

spillover method this value is treated as the amount of incoming and outgoing traffic (in Kbps) a Vserver will handle before spillover takes place. In case of HEALTH type spillover method if the percentage of active services (by weight) becomes lower than this value, spillover takes place Minimum value: 1 Maximum value: 0xFFFFFFF7

redirectPortRewrite
The state of port rewrite while performing HTTP redirect. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush
Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer
The Backup Virtual Server.

disablePrimaryOnDown
When this argument is enabled, traffic will continue reaching backup vservers even after primary comes UP from DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort
The virtual IP and port header insertion option for the vserver. VIPADDR-Header contains the vserver's IP address and port number without any translation. OFF- The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4 address corresponding to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values: OFF, VIPADDR, V6TOV4MAPPING Default value: OFF

AuthenticationHost
FQDN of authentication vserver Maximum value: 252

Authentication
This option toggles on or off the application of authentication of incoming users to the vserver. Possible values: ON, OFF Default value: OFF

push
Process traffic on bound Push vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver
The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

pushLabel
Use this parameter to specify the expression to extract the label in response from server. The string can be either a named expression (configured using add policy expression command) or else it can be an in-line expression with a maximum of 63 characters. Default value: "none"

pushMultiClients
Specify if multiple web 2.0 connections from the same client can connect to this vserver and expect updates. Possible values: YES, NO Default value: NO

Example

add lb vserver http_vsvr http 10.102.1.10 80

Related Commands

rm lb vserver
set lb vserver
unset lb vserver
enable lb vserver
disable lb vserver
show lb vserver

stat lb vserver

rm lb vserver

Synopsis

```
rm lb vserver <name>@ ...
```

Description

Remove a virtual server.

Arguments

name

The name of the virtual server to be removed.

Example

rm vserver lb_vip

Related Commands

add lb vserver

set lb vserver

unset lb vserver

enable lb vserver

disable lb vserver

show lb vserver

stat lb vserver

set lb vserver

Synopsis

```
set lb vserver <name>@ [-IPAddress
<ip_addr|ipv6_addr|*>@] [-IPPattern <ippat>] [-IPMask
<ipmask>] [-weight <positive_integer>  <serviceName>@]
[-persistenceType <persistenceType>] [-timeout <mins>]
[-persistenceBackup ( SOURCEIP | NONE )] [-
backupPersistenceTimeout <mins>] [-lbMethod <lbMethod>
[-hashLength <positive_integer>]  [-netmask <netmask>]
] [-rule <expression>] [-resRule <expression>] [-
persistMask <netmask>] [-pq ( ON | OFF )] [-sc ( ON |
OFF )] [-rtspNat ( ON | OFF )] [-m <m>] [-tosId
<positive_integer>] [-dataLength <positive_integer>]
[-dataOffset <positive_integer>] [-sessionless (
ENABLED | DISABLED )] [-connfailover <connfailover>] [-
backupVServer <string>] [-redirectURL <URL>] [-
cacheable ( YES | NO )] [-cltTimeout <secs>] [-soMethod
<soMethod>] [-soThreshold <positive_integer>] [-
soPersistence ( ENABLED | DISABLED )] [-
soPersistenceTimeOut <positive_integer>] [-
redirectPortRewrite ( ENABLED | DISABLED )] [-
downStateFlush ( ENABLED | DISABLED )] [-
insertVserverIPPort <insertVserverIPPort>
[<vipHeader>] ] [-disablePrimaryOnDown ( ENABLED |
DISABLED )] [-AuthenticationHost <string>] [-
Authentication ( ON | OFF )] [-push ( ENABLED |
DISABLED )] [-pushVserver <string>] [-pushLabel
<expression>] [-pushMultiClients ( YES | NO )]
```

Description

Set load balancing virtual server attributes.

Arguments

name
The name of the load balancing virtual server.

IPAddress
The new IP address of the virtual server.

IPPattern
The IP Pattern of the virtual server.

IPMask
The IP Mask of the virtual server IP Pattern Default value: 0xFFFFFFFF

weight
The weight for the specified service. Minimum value: 1

persistenceType
The persistence type for the specified virtual server: SOURCEIP - Specify a server that can use any or all protocols. COOKIEINSERT - The system inserts a cookie when a cookie is being sent from the server. Each subsequent client request lwill have that cookie. The system extracts the cookie and sends the client request to the same server. In this mode, the system inserts and reads the inserted cookie. SSLSESSION - Specify for an SSL server. RULE - Specify this when the persistence is based on a rule. URLPASSIVE - Specify this when the destination server is selected from the URL. CUSTOMSERVERID - Specify this when the destination server is selected based on the server ID configured using set service or add service command. NONE - Disables session persistence. This setting is the default. Possible values: SOURCEIP, COOKIEINSERT, SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPSID, NONE

timeout
The maximum time persistence is in effect for a specific client. Default value: 2 Maximum value: 1440

persistenceBackup
The backup persistency to be used when the primary persistency fails. For the backup persistency to be active the primary persistency must be COOKIEINSERT. Possible values: SOURCEIP, NONE

backupPersistenceTimeout
The maximum time backup persistence is in effect for a specific client. Default value: 2 Minimum value: 2 Maximum value: 1440

lbMethod
The load balancing method to be in effect: ROUNDROBIN: When selected, determines the destination of a request based on the performance weight (configured by the -weight argument of the ###set lb vserver### command). LEASTCONNECTION: When selected, determines the destination of a request based on the least number of active connections from the system to each physical service bound to the virtual server. LEASTRESPONSETIME: When selected, determines the destination of a request based on the average response time. URLHASH: When selected, determines the destination of a request by hashing the URL. DOMAINHASH: When selected, determines the destination of a request by hashing the domain name DESTINATIONHASH: When selected, determines the destination of a request by hashing the destination IP address or destination network. SOURCEIPHASH: When selected, determines the destination of a request by hashing the source IP address or source network. LEASTBANDWIDTH: When selected, determines the destination of a request based on the bandwidth utilization. LEASTPACKETS: When selected, determines the destination of a request based on number of packets. Token: When selected, determines the destination of a request based on the value, calculated from a token, extracted from the client's request (location and size of the token is configurable). CUSTOMLOAD: The system selects the service based on the it load which w as determined by the LOAD monitors bound to the service. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORTHASH, LRTM, CALLIDHASH, CUSTOMLOAD Default value: PEMGMT_LB_LEASTCONNS

rule
The RULE persistence type. The string can be either a existing rule name (configured using ###add rule### command) or else it could it be an inline expression with a maximum of 1500 characters. Default value: "none"

resRule
Use this parameter to specify the expression to be used in response for RULE persistence type. The string is an in-line expression with a maximum of 1500 characters. Default value: "none"

persistMask
The persistence mask. Use this parameter if you are using IP based persistence type. Default value: 0xFFFFFFFF

pq
The state of priority queuing on the specified virtual server. Possible values: ON, OFF Default value: OFF

sc
The state of SureConnect the specified virtual server. Possible values: ON, OFF Default value: OFF

rtspNat
Use this parameter to enable natting for RTSP data connection. Possible values: ON, OFF Default value: OFF

m
The LB mode. This option is designed for firewall load balancing and cache redirection. IP - Communicate to the server using server's IP address. MAC - Communicate to the server using server's MAC address. TUNNEL - Communicate to the server through an IP tunnel. TOS - Communicate to server using TOS ID. Possible values: IP, MAC, IPTUNNEL, TOS Default value: NSFWD_IP

tosId
Use this parameter to specify the TOS ID of this vserver. Applicable only when the LB mode is TOS Minimum value: 1 Maximum value: 63

dataLength
The data length when TOKEN load balancing method is selected. Minimum value: 1

dataOffset
The data offset length when TOKEN load balancing method is selected.

sessionless
The state of sessionless load balancing. Possible values: ENABLED, DISABLED Default value: DISABLED

connfailover
Specifies the connection failover mode of the virtual server Possible values: DISABLED, STATEFUL, STATELESS Default value: DISABLED

backupVServer
The Backup Virtual Server.

redirectURL
The redirect URL.

cacheable
The state of caching. Possible values: YES, NO Default value: NO

cltTimeout
The client timeout in seconds. Maximum value: 31536000

soMethod
The spillover method to be in effect. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence
State of spillover persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut
The maximum time persistence is in effect for a specific client on a spillover vserver. Default value: 2 Minimum value: 2 Maximum value: 1440

redirectPortRewrite
The state of port rewrite while performing HTTP redirect. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush
Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

insertVserverIPPort
The virtual IP and port header insertion option for the vserver. VIPADDR- Header contains the vserver's IP address and port number without any translation. OFF- The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4 address corresponding to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values: OFF, VIPADDR, V6TOV4MAPPING Default value: OFF

disablePrimaryOnDown
When this argument is enabled, traffic will continue reaching backup vservers even after primary comes UP from DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

AuthenticationHost
FQDN of authentication vserver Maximum value: 252

Authentication
This option toggles on or off the application of authentication of incoming users to the vserver. Possible values: ON, OFF Default value: OFF

push
Process traffic on bound Push vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver
The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

pushLabel
Use this parameter to specify the expression to extract the label in response from server. The string can be either a named expression (configured using add policy expression command) or else it can be an in-line expression with a maximum of 63 characters. Default value: "none"

pushMultiClients
Specify if multiple web 2.0 connections from the same client can connect to this vserver and expect updates. Possible values: YES, NO Default value: NO

Example

set lb vserver http_vip -lbmethod LEASTRESPONSETIME

Related Commands

add lb vserver

rm lb vserver

unset lb vserver

enable lb vserver

disable lb vserver

show lb vserver

stat lb vserver

unset lb vserver

Synopsis

unset lb vserver <name>@ [-backupVServer] [-redirectURL] [-AuthenticationHost] [-pushVserver] [-pushLabel] [-serviceName] [-persistenceType] [-timeout] [-persistenceBackup] [-backupPersistenceTimeout] [-lbMethod] [-hashLength] [-netmask] [-rule] [-resRule] [-persistMask] [-pq] [-sc] [-rtspNat] [-m] [-tosId] [-dataLength] [-dataOffset] [-sessionless] [-connfailover] [-redirectURL] [-cacheable] [-soMethod] [-soThreshold] [-soPersistence] [-soPersistenceTimeOut] [-redirectPortRewrite] [-downStateFlush] [-insertVserverIPPort] [-vipHeader] [-disablePrimaryOnDown] [-Authentication] [-push] [-pushMultiClients]

Description

Unset the backup virtual server or redirectURL set on the virtual server..Refer to the set lb vserver command for meanings of the arguments.

Example

unset lb vserver lb_vip -backupVServer

Related Commands

add lb vserver

rm lb vserver

set lb vserver

enable lb vserver

disable lb vserver

show lb vserver

stat lb vserver

bind lb vserver

Synopsis

```
bind lb vserver <name>@ ((<serviceName>@  [-weight
<positive_integer>]) | <serviceGroupName>@ | (-
policyName <string>@  [-priority <positive_integer>]
[-gotoPriorityExpression <expression>]  [-type (
REQUEST | RESPONSE )]  [-invoke  (<labelType>
<labelName>) ]  ))
```

Description

Bind a physical service to a virtual server.

Arguments

name

The virtual server name to which the service is bound.

serviceName

The name of the service that is bound.

serviceGroupName

The name of the service group that is bound.

policyName

The SureConnect or priority queuing policy that needs to be bound to the specified load balancing virtual server for SureConnect or priority queuing to be activated on a load balancing virtual server.

Example

bind lb vserver http_vip http_svc

Related Commands

unbind lb vserver

unbind lb vserver

Synopsis

```
unbind lb vserver <name>@ (<serviceName>@ |
<serviceGroupName>@ | (-policyName <string>@  [-type (
REQUEST | RESPONSE )])) [-priority <positive_integer>]
```

Description

Unbind a service or policy from a virtual server that has been configured for use in system's load balancing.

Arguments

name

The virtual server name from which the service will be unbound.

serviceName

The service name (created with the addService command) that will be unbound.

serviceGroupName

The name of the service group that is unbound.

policyName

The SureConnect or priority queuing policy that has been bound to this load balancing virtual server, using the ###bind lb vserver### command.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind lb vserver http_vip http_svc

Related Commands

bind lb vserver

enable lb vserver

Synopsis

```
enable lb vserver <name>@
```

Description

Enable a virtual server. Note:Virtual servers, when added, are enabled by default.

Arguments

name

The name of the virtual server to be enabled.

Example

enable vserver lb_vip

Related Commands

add lb vserver

rm lb vserver

set lb vserver

unset lb vserver

disable lb vserver

show lb vserver

stat lb vserver

disable lb vserver

Synopsis

```
disable lb vserver <name>@
```

Description

Disable (makes out of service) a virtual server.

Arguments

name

The name of the virtual server to be disabled. Notes: 1.The system still responds to ARP and/or ping requests for the IP address of this virtual server. 2.As the virtual server is still configured in the system, you can enable the virtual server using ###enable vserver### command.

Example

disable vserver lb_vip

Related Commands

add lb vserver

rm lb vserver

set lb vserver

unset lb vserver

enable lb vserver

show lb vserver

stat lb vserver

show lb vserver

Synopsis

```
show lb vserver [<name>] show lb vserver stats - alias
for 'stat lb vserver'
```

Description

Display load balancing virtual servers information.

Arguments

name

The name of the load balancing server. If no load balancing virtual server name is entered, a list of all configured load balancing virtual servers is displayed. All the services and priority queuing/SureConnect policies that are bound to this virtual server are also displayed.

summary

fullValues

format

level

Output

insertVserverIPPort

The virtual IP and port header insertion option for the vserver.

vipHeader

The name of virtual IP and port header.

value

SSL status.

state

IPAddress

The IP address of the virtual server.

IPAddress
The IP address of the virtual server.

IPPattern
The IP pattern of the virtual server.

IPMask
The IP address mask of the virtual server.

IPMapping
The permanent mapping for the V6 Address

port
A port number for the virtual server.

range
The IP range for the network vserver.

serviceType
The service type.

type
Type of LB vserver.

state
Current LB vserver state.

effectiveState
Effective state of the LB vserver , based on the state of backup vservers.

status
Current status of the lb vserver. During the initial phase if the configured lb method is not round robin , the vserver will adopt round robin to distribute traffic for a predefined number of requests.

lbrrreason
Reason why a vserver is in RR.

cacheType
Cache type.

redirect
Cache redirect type.

precedence
Precedence.

redirectURL
The redirect URL.

Authentication
Authentication.

homePage
Home page.

dnsVserverName
DNS vserver name.

domain
Domain.

policyName
Name of the policy bound to the LB vserver.

serviceName
The service name bound to the selected load balancing virtual server.

weight
The weight for the specified service.

dynamicWeight
Dynamic weight

cacheVserver
Cache virtual server.

backupVServer
The Backup Virtual Server.

priority
Priority.

cltTimeout
The client timeout in seconds.

soMethod
The spillover method to be in effect.

soPersistence
State of spillover persistence.

soPersistenceTimeOut
The maximum time persistence is in effect for a specific client on a spillover vserver.

soThreshold
In case of CONNECTION (or) DYNAMICCONNECTION type spillover method this value is treated as Maximum number of connections a lb vserver will handle before spillover takes place. In case of BANDWIDTH type spillover method this value is treated as the amount of incoming and outgoing traffic (in Kbps) a Vserver will handle before spillover takes place. In case of HEALTH type spillover method if the percentage of active services (by weight) becomes lower than this value, spillover takes place

lbMethod
The load balancing method to be in effect

hashLength
The hash length.

dataOffset
The data offset length for TOKEN load balancing method.

health
Health of vserver based on percentage of weights of active svcs/all svcs. This does not consider administratively disabled svcs

dataLength
The data length for TOKEN load balancing method.

netmask
The netmask of the destination network.

rule
Rule type.

resRule
Use this parameter to specify the expression to be used in response for RULE persistence type. The string is an in-line expression with a maximum of 1500 characters.

gotoPriorityExpression
Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

ruleType
Rule type.

groupName
LB group to which the lb vserver is to be bound.

m
The LB mode.

tosId
TOS ID

persistenceType
The persistence type for the specified virtual server

timeout
The maximum time persistence is in effect for a specific client.

cookieDomain
Domain name to be used in the set cookie header in case of cookie persistence.

persistMask
The persistence mask.

persistenceBackup
The maximum time backup persistence is in effect for a specific client.

backupPersistenceTimeout
The maximum time backup persistence is in effect for a specific client.

cacheable
The state of caching.

pq
The state of priority queuing on the specified virtual server.

sc
The state of SureConnect the specified virtual server.

rtspNat
Use this parameter to enable natting for RTSP data connection.

sessionless
To enable sessionless load balancing, enable this option

map
Map.

connfailover
The connection failover mode of the virtual server

redirectPortRewrite
The state of port rewrite while performing HTTP redirect.

downStateFlush
Perform delayed clean up of connections on this vserver.

disablePrimaryOnDown
Tells whether traffic will continue reaching backup vservers even after primary comes UP from DOWN state.

gt2GB
Allow for greater than 2 GB transactions on this vserver.

thresholdValue
Tells whether threshold exceeded for this service participating in CUSTOMLB

type
The bindpoint to which the policy is bound

invoke
Invoke flag.

labelType
The invocation type.

labelName
Name of the label invoked.

cookieIpPort
Encryped Ip address and port of the service that is inserted into the set-cookie http header

vserverId
Vserver Id

version
Cookie version

totalServices
Total number of services bound to the vserver.

activeServices
Total number of active services bound to the vserver.

stateChangeTimeSec
Time when last state change happened. Seconds part.

stateChangeTimemSec
Time at which last state change happened. Milliseconds part.

ticksSinceLastStateChange
Time in 10 millisecond ticks since the last state change.

hits
Number of hits.

AuthenticationHost
FQDN of authentication vserver

push
Process traffic on bound Push vserver.

pushVserver
The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

pushLabel
Use this parameter to specify the expression to extract the label in response from server. The string can be either a named expression (configured using add policy expression command) or else it can be an in-line expression with a maximum of 63 characters.

pushMultiClients
Specify if multiple web 2.0 connections from the same client can connect to this vserver and expect updates.

Related Commands

add lb vserver
rm lb vserver
set lb vserver
unset lb vserver
enable lb vserver
disable lb vserver

stat lb vserver

stat lb vserver

Synopsis

```
stat lb vserver [<name>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display load-balancing vserver statistics.

Arguments

name

The name of the vserver for which statistics will be displayed. If not given statistics are shown for all vservers.

Output

Counters

Current Client Est connections (ClntEstConn)

The number of Client connections in established state.

Vserver Health (Health)

Health of the vserver. This gives percentage of UP services bound to this vserver.

Vserver IP address (vsvrIP)

IP address of the vserver

Port (port)

The port at which the service is running.

Vserver protocol (Protocol)

Protocol associated with the vserver

State

Current state of the server.

Vserver hits (Hits)

Total vserver hits

Requests (Req)
The total number of requests received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Responses (Rsp)
Number of responses received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Request bytes (Reqb)
The total number of request bytes received on this service/vserver.

Response bytes (Rspb)
Number of response bytes received on this service/vserver.

Total Packets rcvd (PktRx)
The total number of packets received on this service/vserver.

Total Packets sent (PktTx)
The total number of packets sent.

Current client connections (ClntConn)
The number of current client connections.

Current server connections (SvrConn)
The number of current connections to the real servers behind the vserver.

Spill Over Threshold (SOThresh)
Spill Over Threshold set on the VServer.

Spill Over Hits (NumSo)
Number of times vserver expereinced spill over.

Labelled Connection (LblConn)
Number of Labelled connection on this vserver

Push Labelled Connection (PushLbl)
Number of labels for this push vserver.

Deferred Request (DefReq)
Number of deferred request on this vserver

Current Server Est connections (SvrEstConn)
The number of Server connections in established state.

Related Commands

add lb vserver
rm lb vserver
set lb vserver
unset lb vserver
enable lb vserver
disable lb vserver
show lb vserver

set lb sipParameters

Synopsis

```
set lb sipParameters [-rnatSrcPort <port>] [-
rnatDstPort <port>] [-retryDur <integer>] [-addRportVip
( ENABLED | DISABLED )]
```

Description

Set different SIP parameters

Arguments

rnatSrcPort
Source port of SIP packets on RNAT path Minimum value: 1

rnatDstPort
Destination port of SIP packets on RNAT path Minimum value: 1

retryDur
Retry Duration for SIP packets sent by NetScaler Default value: 120 Minimum value: 1

addRportVip
Add rport to SIP requests coming on VIP Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set sip parameter

Related Commands

unset lb sipParameters
show lb sipParameters

unset lb sipParameters

Synopsis

```
unset lb sipParameters [-rnatSrcPort] [-rnatDstPort] [-
retryDur] [-addRportVip]
```

Description

Use this command to remove lb sipParameters settings.Refer to the set lb sipParameters command for meanings of the arguments.

Related Commands

set lb sipParameters

show lb sipParameters

show lb sipParameters

Synopsis

```
show lb sipParameters
```

Description

Display the SIP parameters

Arguments

format

level

Output

rnatSrcPort

rnatDstPort

retryDur

addRportVip

Example

show sip parameter

Related Commands

set lb sipParameters

unset lb sipParameters

add lb metricTable

Synopsis

```
add lb metricTable <metricTable>
```

Description

Use this command to add a metric table.

Arguments

`metricTable`
The name of the metric table. Maximum value: 31

Example

add metrictable newtable

Related Commands

rm lb metricTable
set lb metricTable
bind lb metricTable
unbind lb metricTable
show lb metricTable

rm lb metricTable

Synopsis

```
rm lb metricTable <metricTable>
```

Description

Use this command to remove a metric table.

Arguments

metricTable

The name of the metric table.

Example

rm metric table netscaler

Related Commands

add lb metricTable

set lb metricTable

bind lb metricTable

unbind lb metricTable

show lb metricTable

set lb metricTable

Synopsis

```
set lb metricTable <metricTable> <metric> <snmpOID>
```

Description

Use this command to set a metric table.

Arguments

`metricTable`

The name of the metric table.

Example

set metrictable table met1 aliasname oidstr

Related Commands

add lb metricTable

rm lb metricTable

bind lb metricTable

unbind lb metricTable

show lb metricTable

bind lb metricTable

Synopsis

```
bind lb metricTable <metricTable> <metric> <snmpOID>
```

Description

Use this command to bind metric and OID to the metrictable.

Arguments

`metricTable`

The name of the metric table.

`metric`

metric name of the oid.

Example

bind metrictable tablename aliasname 1.2.3.4

Related Commands

add lb metricTable

rm lb metricTable

set lb metricTable

unbind lb metricTable

show lb metricTable

unbind lb metricTable

Synopsis

```
unbind lb metricTable <metricTable> <metric>
```

Description

Use this command to unbind metric from the metrictable.

Arguments

`metricTable`

The name of the metric table.

`metric`

Metric name from the table that has to be unbound.

Example

unbind metrictable tablename aliasname

Related Commands

add lb metricTable

rm lb metricTable

set lb metricTable

bind lb metricTable

show lb metricTable

show lb metricTable

Synopsis

```
show lb metricTable [<metricTable>]
```

Description

Display the parameters for the specified metrictable. If the monitor_name argument is not specified, a list of all existing metrictable is returned.

Arguments

`metricTable`
The name of the metric table.

`summary`

`fullValues`

`format`

`level`

Output

`metric`
Metric name of the oid.

`snmpOID`
OID corresponding to the metric

`flags`
flags controlling displayNOTE: This attribute is deprecated.This is deprecated attribute.

`state`
flags controlling display

`type`
Indication if it is a permanent or temporary

Example

TODO

Related Commands

add lb metricTable
rm lb metricTable
set lb metricTable
bind lb metricTable
unbind lb metricTable

add lb wlm

Synopsis

```
add lb wlm <wlmName> [<IPAddress>  <port>] -LBUID
<string> [-KATimeout <mins>]
```

Description

Add a Work Load Manager.

Arguments

wlmName

The name of the Work Load Manager.

IPAddress

The IP address of the WLM.

LBUID

The LBUID for the Load Balancer to communicate to the Work Load Manager.

KATimeout

The idle time period after which NS would probe the WLM. The value ranges from 2 to 1440 minutes. Default value: 2 Maximum value: 1440

Example

add lb wlm ibm_wlm 10.102.1.10 3060

Related Commands

rm lb wlm

set lb wlm

unset lb wlm

show lb wlm

rm lb wlm

Synopsis

```
rm lb wlm <wlmName>
```

Description

Removes a Work Load Manager.

Arguments

wlmName

The name of the Work Load Manager to be removed.

Example

rm lb wlm ibm_wlm

Related Commands

add lb wlm

set lb wlm

unset lb wlm

show lb wlm

set lb wlm

Synopsis

```
set lb wlm <wlmName> [-KATimeout <mins>]
```

Description

set Work Load Manager attributes

Arguments

wlmName

The name of the work load manager.

KATimeout

The idle time period after which NS would probe the WLM. The value ranges from 2 to 1440 minutes. Default value: 2 Maximum value: 1440

Example

set lb wlm ibm_wlm -ka_timeout 6

Related Commands

add lb wlm

rm lb wlm

unset lb wlm

show lb wlm

unset lb wlm

Synopsis

```
unset lb wlm <wlmName> -KATimeout
```

Description

Use this command to remove lb wlm settings.Refer to the set lb wlm command for meanings of the arguments.

Related Commands

add lb wlm

rm lb wlm

set lb wlm

show lb wlm

show lb wlm

Synopsis

```
show lb wlm [<wlmName>]
```

Description

show Work Load Manager details

Arguments

wlmName
The name of the work load manager.

summary

fullValues

format

level

Output

IPAddress
The IP address of the WLM.

port
A port number for the virtual server.

state

secure
Use this parameter to enable secure mode of communication with WLM.

KATimeout
The idle time period after which NS would probe the WLM. The value ranges from 2 to 1440 minutes.

LBUID
The LBUID for the Load Balancer to communicate to the Work Load Manager.

state
State of the WLM.

vServerName
Name of the virtual server which is to be bound to the WLM.

Example

show lb wlm ibm_wlm

Related Commands

add lb wlm
rm lb wlm
set lb wlm
unset lb wlm

bind lb wlm

Synopsis

```
bind lb wlm <wlmName> <vServerName>@
```

Description

Bind a vserver to Work Load Manager.

Arguments

wlmName

The name of the Work Load Manager.

vServerName

Name of the virtual server which is to be bound to the WLM.

Example

bind lb wlm ibm_wlm http_vip

Related Commands

unbind lb wlm

unbind lb wlm

Synopsis

```
unbind lb wlm <wlmName> <vServerName>@
```

Description

Unbind a vserver from Work Load Manager.

Arguments

wlmName

The name of the Work Load Manager.

vServerName

Name of the virtual server which is to be unbound from the WLM.

Example

unbind lb wlm ibm_wlm http_vip

Related Commands

bind lb wlm

CHAPTER 19

NetScaler Commands

This chapter covers the NetScaler commands.

stat ns

Synopsis

```
stat ns [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display general system statistics.

Arguments

Output

Counters

Average CPU usage (CPU)
Average CPU utilization percentage.

CPU usage (CPU)
CPU utilization percentage

Memory usage (MemUsage)
This represents the percentage of memory utilization on NetScaler.

Total HTTP compression ratio
Ratio of total HTTP data received to total HTTP data transmitted (uncmp:1.0).

Delta compression ratio (DlCmpRt)
Ratio of compressible data received to compressed data transmitted (uncmp:1.0).

HTTP compression ratio
Ratio of the compressible data received from the server to the compressed data sent to the client.

Utilized memory(KB) (UtiMem)
Amount of memory the integrated cache is currently using.

Maximum memory(KB) (MaxMem)
Largest amount of memory the NetScaler can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the caching module continues to run.

Origin bandwidth saved(%) (POrBan)
Percentage of origin bandwidth saved, expressed as number of bytes served from the integrated cache divided by all bytes served. The assumption is that all compression is done in the NetScaler.

Misses (TotMiss)
Intercepted HTTP requests requiring fetches from origin server.

Hits (TotHit)
Responses served from the integrated cache. These responses match a policy with a CACHE action.

 # SSL cards UP (SSLCardUP)
Number of ssl cards UP. If number of cards UP is lower than a threshold, a failover will be initiated.

Memory usage (%) (MemUsage)
This represents the percentage of memory utilization on NetScaler.

Memory usage (MB) (MemUseMB)
Main memory currently in use, in megabytes.

Management CPU usage (%) (CPU)
Management CPU utilization percentage.

Packet CPU usage (%) (CPU)
Packet CPU utilization percentage.

Average CPU usage (%) (CPU)
Average CPU utilization percentage.

CPU usage (%) (CPU)
CPU utilization percentage

Up since (Since)
Time when the system last started

Last Transition time (TransTime)
Time when the last master state transition occurred. You can use this statistic for debugging.

System state (HAState)
State of the node, based on its health, in a high availability setup. Possible values are: UP ? Indicates that the node is accessible and can function as either a primary or secondary node. DISABLED ? Indicates that the high availability status of the node has been manually disabled. Synchronization and propagation cannot take place between the peer nodes. INIT ? Indicates that the node is in the process of becoming part of the high availability configuration. PARTIALFAIL ? Indicates that one of the high availability monitored interfaces has failed because of a card or link failure. This state triggers a failover. COMPLETEFAIL ? Indicates that all the interfaces of the node are unusable, because the interfaces on which high availability monitoring is enabled are not connected or are manually disabled. This state triggers a failover. DUMB ? Indicates that the node is in listening mode. It does not participate in high availability transitions or transfer configuration from the peer node. This is a configured value, not a statistic. PARTIALFAILSSL ? Indicates that the SSL card has failed. This state triggers a failover. ROUTEMONITORFAIL ? Indicates that the route monitor has failed. This state triggers a failover.

Master state (mastate)
Indicates the high availability state of the node. Possible values are: STAYSECONDARY ? Indicates that the selected node remains the secondary node in a high availability setup. In this case a forced failover does not change the state but, instead, returns an appropriate error message. This is a configured value and not a statistic. PRIMARY ? Indicates that the selected node is the primary node in a high availability setup. SECONDARY ? Indicates that the selected node is the secondary node in a high availability setup. CLAIMING ? Indicates that the secondary node is in the process of taking over as the primary node. This is the intermediate state in the transition of the secondary node to primary status. FORCE CHANGE - Indicates that the secondary node is forcibly changing its status to primary due to a forced failover issued on the secondary node.

 # SSL cards present (SSLCards)
Number of SSL crypto cards present in the system

/flash Used (%) (disk0PerUsage)
Used space in /flash partition of the disk, as a percentage. This is a critical counter. You can configure /flash Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.

/var Used (%) (disk1PerUsage)
Used space in /var partition of the disk, as a percentage. This is a critical counter. You can configure /var Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.

/flash Available (MB) (disk0Avail)
Available space in /flash partition of the disk.

/var Available (MB) (disk1Avail)
Available space in /var partition of the disk.

Megabits received (RxMb)
Number of megabits received by the system

Megabits transmitted (TxMb)
Number of megabits transmitted by the system

All client connections (CltCx)
Client connections, including connections in the Opening, Established, and Closing state.

Established client connections (CltCxE)
Current client connections in the Established state, which indicates that data transfer can occur between the NetScaler and the client.

All server connections (SvrCx)
Server connections, including connections in the Opening, Established, and Closing state.

Established server connections (SvrCxE)
Current server connections in the Established state, which indicates that data transfer can occur between the NetScaler and the server.

Total requests (HTReqRx)
HTTP requests received, including HTTP/1.0 and HTTP/1.1 requests.

Total responses (HTRspRx)
HTTP responses sent including HTTP/1.0 and HTTP/1.1 responses.

Request bytes received (HTReqbRx)
Bytes of HTTP data received.

Response bytes received (HTRspbRx)
Bytes received as response data.

SSL transactions (SSLTrn)
Number of SSL transactions

SSL session hits (SeHit)
Number of SSL session reuse hits

requests (reqs)
Number of requests received by the application firewall

responses (resps)
Number of responses handled by the application firewall

aborts
Number of requests aborted by the application firewall

redirects (redirect)
Number of requests redirected by the application firewall (HTTP 302)

Misc. Counter 0 (misc0)
Miscellaneous Counter 0

Misc. Counter 1 (misc1)
Miscellaneous Counter 1

Misc. Counter 2 (misc2)
Miscellaneous Counter 2

Misc. Counter 3 (misc3)
Miscellaneous Counter 3

The number of CPUs on the system

CPU usage (CPU)
CPU utilization, percentage * 10

Management CPU usage (CPU)
Management CPU utilization, percentage * 10

SSL crypto card status (SSLCardSt)
Status of the SSL card (1=UP, 0=DOWN)

304 hits (304Hit)
Object not modified responses served from the cache. (Status code 304 served instead of the full response.)

Non-304 hits (Non304Hit)
Total number of full (non-304) responses served from the cache. A 304 status code indicates that a response has not been modified since the last time it was served

Requests (CacReq)
Total cache hits plus total cache misses.

Compressed bytes transmitted
Number of bytes the NetScaler sends to the client after compressing the response from the server.

Compressible bytes received
Number of bytes that can be compressed, which the NetScaler receives from the server. This gives the content length of the response that the NetScaler receives from server.

Compressed bytes transmitted (DlCmpTxB)
Total number of delta-compressed bytes transmitted by NetScaler.

Compressible bytes received (DlCmpRxB)
Total number of delta-compressible bytes received by NetScaler.

Related Commands

config ns

stat ns acl

stat ns acl6

stat ns simpleacl

show ns stats

Synopsis

```
show ns stats - alias for 'stat ns'
```

Description

show ns stats is an alias for stat ns

Related Commands

stat ns

show ns ns.conf

Synopsis

```
show ns ns.conf
```

Description

Display the last saved configuration.

Arguments

Output

textBlob

Text of the last saved configuration.

Related Commands

save config, show runningconfig

config ns

Synopsis

```
config ns
```

Description

Use this command to display the system's configuration menu. By choosing items from the menu and following the instructions on the screen, each of the configuration parameters can be modified. On entering the config CLI command, the following menu is displayed: Note:The values inside the square brackets indicate the current value of the parameters. > config ns NSCONFIG NS6.1. Reading the system configuration from the file /etc/ns.conf REVIEW CONFIGURATION PARAMETERS MENU ---------- This menu allows you to view and/or modify the system's configuration. Each configuration parameter displays its current value within brackets if it has been set. To change a value, enter the number that is displayed next to it. ---------- 1. System's IP address: [10.102.7.101] 2. Netmask: [255.255.255.0] 3. Advanced Network Configuration. 4. Time zone. 5. Cancel all the changes and exit. 6. Applychanges and exit. Select a menu item from 1 to 6 [6]: System is running. Writing the System configuration into the file /etc/ns.conf System must be rebooted to apply configuration changes. Do you want to reboot System now? [NO]: Done Notes: 1.The system needs to be rebooted every time an item on this menu is changed and the changes saved. 2.This command only modifies and saves the basic configuration set in the ns.conf file (using the set ns config command). It does not save the running configuration changes applied after the last invocation of the save ns config command. If you have applied changes to your running configuration, then you should save them with save ns config command before using the config ns command. See the note on the reboot ns command.

Arguments

Related Commands

reboot ns

stat ns

show ns runningConfig

Synopsis

```
show ns runningConfig [-withDefaults]
```

Description

Display the information pertaining to all the configuration that has been applied to the system, including settings that have not yet been saved to the system's ns.conf file using the save config command.

Arguments

withDefaults

Output

Related Commands

show ns.conf

renumber ns acls

Synopsis

```
renumber ns acls
```

Description

Reorganize ACL priorities. This will introduce gaps between ACL priorities. This command does not affect the behaviour of ACLs.

Example

renumber acls

Related Commands

apply ns acls

clear ns acls

clear ns acls

Synopsis

```
clear ns acls
```

Description

Clear all configured ACLs. This operation does not require an explicit apply.

Example

clear ns acls

Related Commands

add ns acl

rm ns acl

renumber ns acls

apply ns acls

clear ns simpleacl

Synopsis

```
clear ns simpleacl
```

Description

Clear all configured SimpleACL rules.

Example

clear ns simpleacl

Related Commands

add ns simpleacl

rm ns simpleacl

show ns simpleacl

stat ns simpleacl

apply ns acls

Synopsis

```
apply ns acls
```

Description

Commit the ACL in the configuration space to the system. This is required after you add ACLs or modify the ACLs.

Example

apply ns acls

Related Commands

add ns acl

rm ns acl

set ns acl

enable ns acl

disable ns acl

renumber ns acls

clear ns acls

show ns info

Synopsis

```
show ns info
```

Description

Display the most relevant information about a system, including: lSoftware version lFeatures that are enabled and disabled lModes that are enabled and disabled lWhether the system is acting as a normal or master node lThe system IP address and mapped IP.

Example

An example of this command's output is shown below: System Rainier: Build 24, Date: Apr 25 2002, 21:13:25 System IP: 10.101.4.22(mask: 255.255.0.0) Mapped IP: 10.101.4.23 Node: Standalone HTTP port(s): (none) Max connections: 0 Max requests per connection: 0 Client IP insertion enabled: NO Cookie version: 0 Feature status: Web Logging: ON Surge Protection: ON Load Balancing: ON Content Switching: ON Cache Redirection: ON Sure Connect: ON Compression Control: OFF Priority Queuing: ON SSL Offloading: ON Global Server Load Balancing: ON HTTP DoS Protection: OFF N+1: OFF Dynamic Routing: OFF Content Filtering: ON Internal Caching: ON SSL VPN: OFF Mode status: Fast Ramp: ON Layer 2 mode: ON Use Source IP: OFF Client Keep-alive: ON TCP Buffering: OFF MAC-based forwarding: ON Edge configuration: OFF Use Subnet IP: OFF Layer 3 mode (ip forwarding): ON

Related Commands

show ns license

Synopsis

```
show ns license
```

Description

Display information about the current system license.

Arguments

Output

WL
Web Logging.

SP
Surge Protection.

LB
Load Balancing.

CS
Content Switching.

CR
Cache Redirect.

SC
Sure Connect.

CMP
Compression.

DELTA
Delta Compression.

PQ
Priority Queuing.

SSL
Secure Sockets Layer.

GSLB
Global Server Load Balancing.

GSLBP
GSLB Proximity.

HDOSP
DOS Protection.

Routing
Routing.

CF
Content Filter.

IC
Integrated Caching.

SSLVPN
SSL VPN.

AAA
AAA

OSPF
OSPF Routing.

RIP
RIP Routing.

BGP
BGP Routing.

REWRITE
Rewrite.

IPv6PT
IPv6 protocol translation

AppFw
Application Firewall.

RESPONDER
Responder.

HTMLInjection
HTML Injection.

ModelID
Model Number ID.

push
NetScaler Push.

Related Commands

show ns version

Synopsis

```
show ns version
```

Description

Display the version and build number of the system.

Arguments

Output

`version`
Version.

`Mode`
Kernel mode (KMPE/VMPE).

Related Commands

reboot

Synopsis

```
reboot
```

Description

Use this command to restart a system. Notes: 1.When a standalone system is rebooted, all configuration changes made since the last save ns config command was issued are lost. 2.In High Availability mode, on running this command on the primary system, the secondary system takes over and will have the configuration changes made since the last time that the save ns config command was issued on the primary system. In this case, log on to the new primary system, then issue the save ns config CLI command to save these changes.

Arguments

Related Commands

shutdown

Synopsis

shutdown

Description

Use this command to stop the operations of the system on which you are issuing this command. After you enter this command, you can turn off power to the system. Notes 1.When a standalone system is rebooted, all configuration changes made since the last save ns config command was issued are lost. 2.In High Availability mode, on running this command on the primary system, the secondary system takes over and will have the configuration changes made since the last time that the save ns config command was issued on the primary system. In this case, log on to the new primary system, then issue the save ns config CLI command to save these changes.

Arguments

Related Commands

clear ns config

Synopsis

```
clear ns config [-force] <level>
```

Description

Clear NS Config.

Arguments

force

Clear the configuration without prompting confirmation.

level

Clear the configuration according to the levels. Possible values: basic, extended, full

Related Commands

set ns config

unset ns config

save ns config

show ns config

diff ns config

clear ns acls6

Synopsis

```
clear ns acls6
```

Description

Clear all configured ACL6. This operation does not require an explicit apply.

Example

clear ns acls6

Related Commands

add ns acl6

rm ns acl6

apply ns acls6

renumber ns acls6

apply ns acls6

Synopsis

```
apply ns acls6
```

Description

Commit the ACL6 in the configuration space to the system. This is required after an ACL6 is added or modified.

Example

apply ns acls6

Related Commands

add ns acl6

rm ns acl6

set ns acl6

enable ns acl6

disable ns acl6

clear ns acls6

renumber ns acls6

renumber ns acls6

Synopsis

```
renumber ns acls6
```

Description

Reorganize ACL6 priorities. This will introduce gaps between ACL6 priorities. This command does not affect the behaviour of ACLs.

Example

renumber acls6

Related Commands

apply acls6

clear acls6

clear ns acls6

apply ns acls6

show ns connectiontable

Synopsis

```
show ns connectiontable [<filterexpression>] [-detail
<detail> ...]
```

Description

Display the current TCP/IP connection table

Arguments

`filterexpression`

The maximum length of filter expression is 255 and it can be of following format: <expression> [<relop> <expression>] <relop> = (&& | ||) <expression> = the expression string in the format: <qualifier> <operator> <qualifier-value> <qualifier> = SOURCEIP. <qualifier-value> = A valid IP address. <qualifier> = SOURCEPORT. <qualifier-value> = A valid port number. <qualifier> = DESTIP. <qualifier-value> = A valid IP address. <qualifier> = DESTPORT. <qualifier-value> = A valid port number. <qualifier> = IDLETIME. <qualifier-value> = A positive integer indicating the idle time. <qualifier> = SVCNAME. <qualifier-value> = The name of a service. <qualifier> = VSVRNAME. <qualifier-value> = The name of a vserver. <qualifier> = STATE. <qualifier-value> = (CLOSE_WAIT | CLOSED | CLOSING | ESTABLISHED | FIN_WAIT_1 | FIN_WAIT_2 | LAST_ACK | LISTEN | SYN_RECEIVED | SYN_SENT | TIME_WAIT) <qualifier> = SVCTYPE. <qualifier-value> = (HTTP | FTP | TCP | UDP | SSL | SSL_BRIDGE | SSL_TCP | NNTP | RPCSVR | RPCSVRS | RPCCLNT | DNS | ADNS | SNMP | RTSP | DHCPRA | ANY | MONITOR | MONITOR_UDP | MONITOR_PING | SIP_UDP | UNKNOWN) <operator> = (== | eq | != | neq | > | gt | < | lt | >= | ge | <= | le | BETWEEN)

`link`

Display link information if available Default value: NS_CONFILTER_FILTERLNK

`name`

Display name instead of IP for local entities Default value: NS_CONFILTER_FILTERNAME

detail
Display options for the connection table.

summary

fullValues

Output

SOURCEIP
Source IP of the connection.

SOURCEPORT
Source port of the connection.

DESTIP
Destination IP of the connection.

DESTPORT
Destination port of the connection.

SVCTYPE
Protocol supported by the connection.

IDLETIME
Time since last activity was detected on the connection.

STATE
Current TCP/IP state of the connection.

linkSourceIP
Source IP of the link connection.

linkSourcePort
Source port of the link connection.

linkDestIP
Destination IP of the link connection.

linkDestPort
Destination port of the link connection.

linkServiceType
Protocol supported by the link connection.

linkIdleTime
Time since last activity was detected on link connection.

linkState
TCP/IP current state of link connection.

entityName
NetScaler entity name for the connection.

linkEntityName
NetScaler entity name for link connection.

connectionNumber
Connection numberNOTE: This attribute is deprecated.Deprecated in favour of NSA_CONNID.

linkConnectionNumber
Link connection numberNOTE: This attribute is deprecated.Deprecated in favour of NSA_LINK_CONNID.

connid
Unique transaction number for the connection.

linkConnid
Unique transaction number for the peer connection.

filterFlags
flags used to store display options

optionFlags
flags used to store TCP options like Sack, WS

mss
Client side MSS for the connection - used in server SYN.

retxRetryCnt
Retransmission retry count for the connection.

rcvWnd
Received Advertised Window for the connection.

advWnd
Sent advertised window for the connection.

sndCwnd
sent congestion window for the connection.

iss
Initial send sequence number for the connection.

irs
Initial receive sequence number for the connection.

rcvNxt
next expecting seq number for the connection.

maxAck
current running max ack sent for the connection.

sndNxt
next bytes seq number for the connection.

sndUnAck
Most recently received ACK for the connection.

httpEndSeq
HTTP parsing tracking seq number for the connection.

httpState
HTTP Protocol state for the connection.

trCount
Max reuests allowed per connection.

priority
priority of the connection.

httpReqVer
current HTTP request version on the connection.

httpRequest
current HTTP request type on the connection.

httpRspCode
current response type on the connection.

rttSmoothed
smoothed RTT value of the connection.

rttVariance
RTT variance for the connection.

outoforderPkts
held packets on the connection.

count
count

linkOptionFlag
Link connection's TCP option flag for Sack and WS

linkMSS
Client side MSS for the Link connection - used in server SYN

linkRetxRetryCnt
Retransmission retry count for the Link connection.

linkRcvWnd
Received Advertised Window for the Link connection.

linkAdvWnd
Sent advertised window for the Link connection.

linkSndCwnd
Send congestion window for the Link connection.

linkISS
Initial send seq number for the Link connection.

linkIRS
Initial receive seq number for the Link connection.

linkRcvNxt
Next expecting seq number on the Link connection.

linkMaxAck
Current running maximum ack sent on the Link connection.

linkSndNxt
Next bytes seq number for the Link connection.

linkSndUnAck
Most recently received ACK on the Link connection.

linkHttpEndSeq
HTTP parsing tracking seq number on the Link connection.

linkHttpState
HTTP protocol state on the Link connection.

linkTrCount
Max requests per connection for Link connection.

linkPriority
Priority for the Link connection.

linkHttpReqVer
HTTP current request version on Link connection.

linkHttpReq
HTTP current request type on Link connection.

linkHttpRspCode
Current response type on link connection.

linkRttSmoothed
Smoothed RTT value on link connection.

linkRttVariance
RTT variance on Link connection.

linkHeldPkts
Held packets on Link connection.

Related Commands

show ns limitSessions

Synopsis

```
show ns limitSessions <limitIdentifier> [-detail]
```

Description

Display rate limit sessions.

Arguments

limitIdentifier
The name of the rate limit identifer.

detail
Displays the individual hash values Default value: NSA_CLIDETAIL

Output

timeout
The time remaining on the session before a flush can be attempted. If active transactions are present the session will not be flushed

hits
The number of times this entry was hit.

drop
The number of times action was taken.

number
The hash of the matched selectlets.

name
The string formed by gathering selectlet values.

unit
Total computed hash of the matched selectlets.

flags
Used internally to identify ip addresses.

referenceCount
Total number of transactions pointing to this entry. Its the sum total of the connection and bandwidth references

maxBandwidth
The current bandwidth

limitSelectorIPV61
First IPV6 address gathered.

limitSelectorIPV62
Second IPV6 address gathered.

flag
Used internally to identify ipv6 addresses.

Related Commands

clear ns limitSessions

clear ns limitSessions

Synopsis

```
clear ns limitSessions <limitIdentifier>
```

Description

Arguments

`limitIdentifier`
The name of the rate limit identifer.

Related Commands

show ns limitSessions

show ns persistencesession

Synopsis

Description

Get all Sessions corresponding to a Vserver NOTE: This command is deprecated.Moved to LB command group

Arguments

name
The name of the virtual server.

summary

fullValues

Output

type
The netmask of this IP.

srcIP
SOURCE IP.

srcIPv6
SOURCE IPv6 ADDRESS.

destIP
DESTINATION IP.

destIPv6
DESTINATION IPv6 ADDRESS.

flags
IPv6 FLAGS.

destPort
Destination port.

vServerName
Virtual server name.

timeout
Persistent Session timeout.

referenceCount
Reference Count.

sipCallID
SIP CALLID.NOTE: This attribute is deprecated.Replaced by "persistenceParam" field

persistenceParam
Specific persistence information . Callid in case of SIP_CALLID persistence entry , RTSP session id in case of RTSP_SESSIONID persistence entry.

Example

show ns persistencesession vipname

Related Commands

clear ns persistencesession

clear ns persistencesession

Synopsis

Description

Use this command to clear/flush persistence sessions NOTE: This command is deprecated.Moved to LB command group

Arguments

vServer

The name of the LB vserver whose persistence sessions are to be flushed. If not specified, all persistence sessions will be flushed .

Example

clear persistenceSessions -vserver vip1

Related Commands

show ns persistencesession

set ns config

Synopsis

```
set ns config [-IPAddress <ip_addr>  -netmask
<netmask>] [-nsvlan <positive_integer>  -ifnum
<interface_name> ...] [-httpPort <port> ...] [-maxConn
<positive_integer>] [-maxReq <positive_integer>] [-cip
( ENABLED | DISABLED )  <cipHeader>] [-cookieversion (
0 | 1 )] [-pmtuMin <positive_integer>] [-pmtuTimeout
<mins>] [-ftpPortRange <int[-int]>] [-timezone
<timezone>]
```

Description

Set the system parameters.

Arguments

IPAddress

The IP address of the system.

nsvlan

The VLAN (NSVLAN) for the subnet on which the IP resides. Minimum value: 2 Maximum value: 4095

httpPort

The HTTP ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value: 1

maxConn

The maximum number of connections that will be made from the system to the web server(s) attached to it. The value entered here is applied globally to all attached servers. Maximum value: 0xFFFFFFFE

maxReq

The maximum number of requests that the system can pass on a particular connection between the system and a server attached to it. Setting this value to

0 allows an unlimited number of requests to be passed. Minimum value: 0 Maximum value: 65535

cip
The option to control (enable or disable) the insertion of the actual client IP address into the HTTP header request passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a minor modification to the server. lIf cipHeader is specified, it will be used as the client IP header. lIf it is not specified, then the value that has been set by the set ns config CLI command will be used as the client IP header. Possible values: ENABLED, DISABLED

cookieversion
The version of the cookie inserted by system. Possible values: 0, 1

pmtuMin
The minimum Path MTU. Default value: 576 Minimum value: 168 Maximum value: 1500

pmtuTimeout
The timeout value in minutes. Default value: 10 Minimum value: 1 Maximum value: 1440

ftpPortRange
Port range configured for FTP services. Minimum value: 1024 Maximum value: 64000

timezone
Name of the timezone Possible values: GMT-11:00-SST-Pacific/Pago_Pago, GMT-11:00-NUT-Pacific/Niue, GMT-11:00-SST-Pacific/Midway, GMT-11:00-WST-Pacific/Apia, GMT-10:00-CKT-Pacific/Rarotonga, GMT-10:00-TAHT-Pacific/Tahiti, GMT-10:00-TKT-Pacific/Fakaofo, GMT-10:00-HST-Pacific/Johnston, GMT-10:00-HST-Pacific/Honolulu, GMT-09:30-MART-Pacific/Marquesas, GMT-09:00-GAMT-Pacific/Gambier, GMT-09:00-HADT-America/Adak, GMT-08:00-PST-Pacific/Pitcairn, GMT-08:00-AKDT-America/Anchorage, GMT-08:00-AKDT-America/Juneau, GMT-08:00-AKDT-America/Yakutat, GMT-08:00-AKDT-America/Nome, GMT-07:00-MST-America/Dawson_Creek, GMT-07:00-PDT-America/Vancouver, GMT-07:00-PDT-America/Whitehorse, GMT-07:00-PDT-America/Dawson, GMT-07:00-MST-America/Hermosillo, GMT-07:00-PDT-America/Tijuana, GMT-07:00-MST-America/Phoenix, GMT-07:00-PDT-America/Los_Angeles, GMT-06:00-CST-America/Belize, GMT-06:00-CST-America/

Regina, GMT-06:00-CST-America/Swift_Current, GMT-06:00-MDT-America/Edmonton, GMT-06:00-MDT-America/Cambridge_Bay, GMT-06:00-MDT-America/Yellowknife, GMT-06:00-MDT-America/Inuvik, GMT-06:00-EAST-Pacific/Easter, GMT-06:00-CST-America/Costa_Rica, GMT-06:00-GALT-Pacific/Galapagos, GMT-06:00-CST-America/Guatemala, GMT-06:00-CST-America/Tegucigalpa, GMT-06:00-MDT-America/Mazatlan, GMT-06:00-MDT-America/Chihuahua, GMT-06:00-CST-America/Managua, GMT-06:00-CST-America/El_Salvador, GMT-06:00-MDT-America/Denver, GMT-06:00-MDT-America/Boise, GMT-06:00-MDT-America/Shiprock, GMT-05:00-ACT-America/Eirunepe, GMT-05:00-ACT-America/Rio_Branco, GMT-05:00-EST-America/Resolute, GMT-05:00-EST-America/Atikokan, GMT-05:00-CDT-America/Rankin_Inlet, GMT-05:00-CDT-America/Winnipeg, GMT-05:00-CDT-America/Rainy_River, GMT-05:00-COT-America/Bogota, GMT-05:00-ECT-America/Guayaquil, GMT-05:00-EST-America/Port-au-Prince, GMT-05:00-EST-America/Jamaica, GMT-05:00-EST-America/Cayman, GMT-05:00-CDT-America/Mexico_City, GMT-05:00-CDT-America/Cancun, GMT-05:00-CDT-America/Merida, GMT-05:00-CDT-America/Monterrey, GMT-05:00-EST-America/Panama, GMT-05:00-PET-America/Lima, GMT-05:00-CDT-America/Indiana/Knox, GMT-05:00-CDT-America/Chicago, GMT-05:00-CDT-America/Indiana/Tell_City, GMT-05:00-CDT-America/Menominee, GMT-05:00-CDT-America/North_Dakota/Center, GMT-05:00-CDT-America/North_Dakota/New_Salem, GMT-04:00-AST-America/Antigua, GMT-04:00-AST-America/Anguilla, GMT-04:00-AST-America/Curacao, GMT-04:00-CLT-Antarctica/Palmer, GMT-04:00-AST-America/Aruba, GMT-04:00-AST-America/Barbados, GMT-04:00-AST-America/St_Barthelemy, GMT-04:00-BOT-America/La_Paz, GMT-04:00-AMT-America/Campo_Grande, GMT-04:00-AMT-America/Cuiaba, GMT-04:00-AMT-America/Porto_Velho, GMT-04:00-AMT-America/Boa_Vista, GMT-04:00-AMT-America/Manaus, GMT-04:00-EDT-America/Nassau, GMT-04:00-AST-America/Blanc-Sablon, GMT-04:00-EDT-America/Montreal, GMT-04:00-EDT-America/Toronto, GMT-04:00-EDT-America/Nipigon, GMT-04:00-EDT-America/Thunder_Bay, GMT-04:00-EDT-America/Iqaluit, GMT-04:00-EDT-America/Pangnirtung, GMT-04:00-CLT-America/Santiago, GMT-04:00-CDT-America/Havana, GMT-04:00-AST-America/Dominica, GMT-04:00-AST-America/Santo_Domingo, GMT-04:00-FKT-Atlantic/Stanley, GMT-04:00-AST-America/Grenada, GMT-04:00-AST-America/Guadeloupe, GMT-04:00-GYT-America/Guyana, GMT-04:00-AST-America/St_Kitts, GMT-04:00-AST-America/St_Lucia, GMT-04:00-AST-America/Marigot, GMT-04:00-AST-America/Martinique, GMT-04:00-AST-America/Montserrat, GMT-

04:00-AST-America/Puerto_Rico, GMT-04:00-PYT-America/Asuncion, GMT-04:00-EDT-America/Grand_Turk, GMT-04:00-AST-America/Port_of_Spain, GMT-04:00-EDT-America/New_York, GMT-04:00-EDT-America/Detroit, GMT-04:00-EDT-America/Kentucky/Louisville, GMT-04:00-EDT-America/Kentucky/Monticello, GMT-04:00-EDT-America/Indiana/Indianapolis, GMT-04:00-EDT-America/Indiana/Vincennes, GMT-04:00-EDT-America/Indiana/Winamac, GMT-04:00-EDT-America/Indiana/Marengo, GMT-04:00-EDT-America/Indiana/Vevay, GMT-04:00-EDT-America/Indiana/Petersburg, GMT-04:00-AST-America/St_Vincent, GMT-04:30-VET-America/Caracas, GMT-04:00-AST-America/Tortola, GMT-04:00-AST-America/St_Thomas, GMT-03:00-ROTT-Antarctica/Rothera, GMT-03:00-ART-America/Argentina/Buenos_Aires, GMT-03:00-ART-America/Argentina/Cordoba, GMT-03:00-ART-America/Argentina/Jujuy, GMT-03:00-ART-America/Argentina/Tucuman, GMT-03:00-ART-America/Argentina/Catamarca, GMT-03:00-ART-America/Argentina/La_Rioja, GMT-03:00-ART-America/Argentina/San_Juan, GMT-03:00-ART-America/Argentina/Mendoza, GMT-03:00-ART-America/Argentina/Rio_Gallegos, GMT-03:00-ART-America/Argentina/Ushuaia, GMT-03:00-ADT-Atlantic/Bermuda, GMT-03:00-BRT-America/Belem, GMT-03:00-BRT-America/Fortaleza, GMT-03:00-BRT-America/Recife, GMT-03:00-BRT-America/Araguaina, GMT-03:00-BRT-America/Maceio, GMT-03:00-BRT-America/Bahia, GMT-03:00-BRT-America/Sao_Paulo, GMT-03:00-ADT-America/Halifax, GMT-03:00-ADT-America/Glace_Bay, GMT-03:00-ADT-America/Moncton, GMT-03:00-ADT-America/Goose_Bay, GMT-03:00-GFT-America/Cayenne, GMT-03:00-ADT-America/Thule, GMT-03:00-SRT-America/Paramaribo, GMT-03:00-UYT-America/Montevideo, GMT-02:00-FNT-America/Noronha, GMT-02:30-NDT-America/St_Johns, GMT-02:00-WGST-America/Godthab, GMT-02:00-GST-Atlantic/South_Georgia, GMT-02:00-PMDT-America/Miquelon, GMT-01:00-CVT-Atlantic/Cape_Verde, GMT+00:00-GMT-Africa/Ouagadougou, GMT+00:00-GMT-Africa/Abidjan, GMT+00:00-WET-Africa/El_Aaiun, GMT+00:00-GMT-Africa/Accra, GMT+00:00-GMT-America/Danmarkshavn, GMT+00:00-EGST-America/Scoresbysund, GMT+00:00-GMT-Africa/Banjul, GMT+00:00-GMT-Africa/Conakry, GMT+00:00-GMT-Africa/Bissau, GMT+00:00-GMT-Atlantic/Reykjavik, GMT+00:00-GMT-Africa/Monrovia, GMT+00:00-WET-Africa/Casablanca, GMT+00:00-GMT-Africa/Bamako, GMT+00:00-GMT-Africa/Nouakchott, GMT+00:00-AZOST-Atlantic/Azores, GMT+00:00-GMT-Atlantic/St_Helena, GMT+00:00-GMT-Africa/Freetown, GMT+00:00-GMT-Africa/Dakar, GMT+00:00-GMT-Africa/Sao_Tome, GMT+00:00-GMT-Africa/Lome, GMT+01:00-WAT-Africa/Luanda, GMT+01:00-WAT-Africa/

Porto-Novo, GMT+01:00-WAT-Africa/Kinshasa, GMT+01:00-WAT-Africa/Bangui, GMT+01:00-WAT-Africa/Brazzaville, GMT+01:00-WAT-Africa/Douala, GMT+01:00-CET-Africa/Algiers, GMT+01:00-WEST-Atlantic/Canary, GMT+01:00-WEST-Atlantic/Faroe, GMT+01:00-WAT-Africa/Libreville, GMT+01:00-BST-Europe/London, GMT+01:00-BST-Europe/Guernsey, GMT+01:00-WAT-Africa/Malabo, GMT+01:00-IST-Europe/Dublin, GMT+01:00-BST-Europe/Isle_of_Man, GMT+01:00-BST-Europe/Jersey, GMT+01:00-WAT-Africa/Windhoek, GMT+01:00-WAT-Africa/Niamey, GMT+01:00-WAT-Africa/Lagos, GMT+01:00-WEST-Europe/Lisbon, GMT+01:00-WEST-Atlantic/Madeira, GMT+01:00-WAT-Africa/Ndjamena, GMT+02:00-CEST-Europe/Andorra, GMT+02:00-CEST-Europe/Tirane, GMT+02:00-CEST-Europe/Vienna, GMT+02:00-CEST-Europe/Sarajevo, GMT+02:00-CEST-Europe/Brussels, GMT+02:00-CAT-Africa/Bujumbura, GMT+02:00-CAT-Africa/Gaborone, GMT+02:00-CAT-Africa/Lubumbashi, GMT+02:00-CEST-Europe/Zurich, GMT+02:00-CEST-Europe/Prague, GMT+02:00-CEST-Europe/Berlin, GMT+02:00-CEST-Europe/Copenhagen, GMT+02:00-CEST-Europe/Madrid, GMT+02:00-CEST-Africa/Ceuta, GMT+02:00-CEST-Europe/Paris, GMT+02:00-CEST-Europe/Gibraltar, GMT+02:00-CEST-Europe/Zagreb, GMT+02:00-CEST-Europe/Budapest, GMT+02:00-CEST-Europe/Rome, GMT+02:00-CEST-Europe/Vaduz, GMT+02:00-SAST-Africa/Maseru, GMT+02:00-CEST-Europe/Luxembourg, GMT+02:00-EET-Africa/Tripoli, GMT+02:00-CEST-Europe/Monaco, GMT+02:00-CEST-Europe/Podgorica, GMT+02:00-CEST-Europe/Skopje, GMT+02:00-CEST-Europe/Malta, GMT+02:00-CAT-Africa/Blantyre, GMT+02:00-CAT-Africa/Maputo, GMT+02:00-CEST-Europe/Amsterdam, GMT+02:00-CEST-Europe/Oslo, GMT+02:00-CEST-Europe/Warsaw, GMT+02:00-CEST-Europe/Belgrade, GMT+02:00-CAT-Africa/Kigali, GMT+02:00-CEST-Europe/Stockholm, GMT+02:00-CEST-Europe/Ljubljana, GMT+02:00-CEST-Arctic/Longyearbyen, GMT+02:00-CEST-Europe/Bratislava, GMT+02:00-CEST-Europe/San_Marino, GMT+02:00-SAST-Africa/Mbabane, GMT+02:00-CEST-Africa/Tunis, GMT+02:00-CEST-Europe/Vatican, GMT+02:00-SAST-Africa/Johannesburg, GMT+02:00-CAT-Africa/Lusaka, GMT+02:00-CAT-Africa/Harare, GMT+03:00-SYOT-Antarctica/Syowa, GMT+03:00-EEST-Europe/Mariehamn, GMT+03:00-EEST-Europe/Sofia, GMT+03:00-AST-Asia/Bahrain, GMT+03:00-EEST-Europe/Minsk, GMT+03:00-EEST-Asia/Nicosia, GMT+03:00-EAT-Africa/Djibouti, GMT+03:00-EEST-Europe/Tallinn, GMT+03:00-EEST-Africa/Cairo, GMT+03:00-EAT-Africa/Asmara, GMT+03:00-EAT-Africa/Addis_Ababa, GMT+03:00-EEST-Europe/Helsinki, GMT+03:00-EEST-Europe/Athens, GMT+03:00-IDT-Asia/Jerusalem,

GMT+03:00-EEST-Asia/Amman, GMT+03:00-EAT-Africa/Nairobi, GMT+03:00-EAT-Indian/Comoro, GMT+03:00-AST-Asia/Kuwait, GMT+03:00-EEST-Asia/Beirut, GMT+03:00-EEST-Europe/Vilnius, GMT+03:00-EEST-Europe/Riga, GMT+03:00-EEST-Europe/Chisinau, GMT+03:00-EAT-Indian/Antananarivo, GMT+03:00-EEST-Asia/Gaza, GMT+03:00-AST-Asia/Qatar, GMT+03:00-EEST-Europe/Bucharest, GMT+03:00-EEST-Europe/Kaliningrad, GMT+03:00-AST-Asia/Riyadh, GMT+03:00-EAT-Africa/Khartoum, GMT+03:00-EAT-Africa/Mogadishu, GMT+03:00-EEST-Asia/Damascus, GMT+03:00-EEST-Europe/Istanbul, GMT+03:00-EAT-Africa/Dar_es_Salaam, GMT+03:00-EEST-Europe/Kiev, GMT+03:00-EEST-Europe/Uzhgorod, GMT+03:00-EEST-Europe/ Zaporozhye, GMT+03:00-EEST-Europe/Simferopol, GMT+03:00-EAT-Africa/Kampala, GMT+03:00-AST-Asia/Aden, GMT+03:00-EAT-Indian/ Mayotte, GMT+04:00-GST-Asia/Dubai, GMT+04:30-AFT-Asia/Kabul, GMT+04:00-GET-Asia/Tbilisi, GMT+04:00-ADT-Asia/Baghdad, GMT+04:30-IRDT-Asia/Tehran, GMT+04:00-MUT-Indian/Mauritius, GMT+04:00-GST-Asia/Muscat, GMT+04:00-RET-Indian/Reunion, GMT+04:00-MSD-Europe/Moscow, GMT+04:00-VOLST-Europe/ Volgograd, GMT+04:00-SCT-Indian/Mahe, GMT+05:00-AMST-Asia/ Yerevan, GMT+05:00-AZST-Asia/Baku, GMT+05:30-IST-Asia/Calcutta, GMT+05:00-AQTT-Asia/Aqtobe, GMT+05:00-AQTT-Asia/Aqtau, GMT+05:00-ORAT-Asia/Oral, GMT+05:30-IST-Asia/Colombo, GMT+05:00-MVT-Indian/Maldives, GMT+05:45-NPT-Asia/Katmandu, GMT+05:00-PKT-Asia/Karachi, GMT+05:00-SAMST-Europe/Samara, GMT+05:00-TFT-Indian/Kerguelen, GMT+05:00-TJT-Asia/Dushanbe, GMT+05:00-TMT-Asia/Ashgabat, GMT+05:00-UZT-Asia/Samarkand, GMT+05:00-UZT-Asia/Tashkent, GMT+06:00-MAWT-Antarctica/Mawson, GMT+06:00-VOST-Antarctica/Vostok, GMT+06:00-BDT-Asia/Dhaka, GMT+06:00-BTT-Asia/Thimphu, GMT+06:30-CCT-Indian/Cocos, GMT+06:00-IOT-Indian/Chagos, GMT+06:00-KGT-Asia/Bishkek, GMT+06:00-ALMT-Asia/Almaty, GMT+06:00-QYZT-Asia/Qyzylorda, GMT+06:30-MMT-Asia/Rangoon, GMT+06:00-YEKST-Asia/Yekaterinburg, GMT+07:00-DAVT-Antarctica/Davis, GMT+07:00-CXT-Indian/Christmas, GMT+07:00-WIT-Asia/Jakarta, GMT+07:00-WIT-Asia/Pontianak, GMT+07:00-ICT-Asia/Phnom_Penh, GMT+07:00-ICT-Asia/Vientiane, GMT+07:00-HOVT-Asia/Hovd, GMT+07:00-OMSST-Asia/Omsk, GMT+07:00-NOVST-Asia/Novosibirsk, GMT+07:00-ICT-Asia/Bangkok, GMT+07:00-ICT-Asia/Saigon, GMT+08:00-WST-Antarctica/Casey, GMT+08:00-WST-Australia/Perth, GMT+08:45-CWST-Australia/Eucla, GMT+08:00-BNT-Asia/Brunei, GMT+08:00-CST-Asia/Shanghai,

GMT+08:00-CST-Asia/Harbin, GMT+08:00-CST-Asia/Chongqing, GMT+08:00-CST-Asia/Urumqi, GMT+08:00-CST-Asia/Kashgar, GMT+08:00-HKT-Asia/Hong_Kong, GMT+08:00-CIT-Asia/Makassar, GMT+08:00-ULAT-Asia/Ulaanbaatar, GMT+08:00-CST-Asia/Macau, GMT+08:00-MYT-Asia/Kuala_Lumpur, GMT+08:00-MYT-Asia/Kuching, GMT+08:00-PHT-Asia/Manila, GMT+08:00-KRAST-Asia/Krasnoyarsk, GMT+08:00-SGT-Asia/Singapore, GMT+08:00-CST-Asia/Taipei, GMT+09:30-CST-Australia/Broken_Hill, GMT+09:30-CST-Australia/Adelaide, GMT+09:30-CST-Australia/Darwin, GMT+09:00-EIT-Asia/Jayapura, GMT+09:00-JST-Asia/Tokyo, GMT+09:00-KST-Asia/Pyongyang, GMT+09:00-KST-Asia/Seoul, GMT+09:00-CHOT-Asia/Choibalsan, GMT+09:00-PWT-Pacific/Palau, GMT+09:00-IRKST-Asia/Irkutsk, GMT+09:00-TLT-Asia/Dili, GMT+10:00-DDUT-Antarctica/DumontDUrville, GMT+10:30-LHST-Australia/Lord_Howe, GMT+10:00-EST-Australia/Hobart, GMT+10:00-EST-Australia/Currie, GMT+10:00-EST-Australia/Melbourne, GMT+10:00-EST-Australia/Sydney, GMT+10:00-EST-Australia/Brisbane, GMT+10:00-EST-Australia/Lindeman, GMT+10:00-TRUT-Pacific/Truk, GMT+10:00-ChST-Pacific/Guam, GMT+10:00-ChST-Pacific/Saipan, GMT+10:00-PGT-Pacific/Port_Moresby, GMT+10:00-YAKST-Asia/Yakutsk, GMT+11:00-PONT-Pacific/Ponape, GMT+11:00-KOST-Pacific/Kosrae, GMT+11:00-NCT-Pacific/Noumea, GMT+11:30-NFT-Pacific/Norfolk, GMT+11:00-VLAST-Asia/Vladivostok, GMT+11:00-SAKST-Asia/Sakhalin, GMT+11:00-SBT-Pacific/Guadalcanal, GMT+11:00-VUT-Pacific/Efate, GMT+12:00-NZST-Antarctica/McMurdo, GMT+12:00-NZST-Antarctica/South_Pole, GMT+12:00-FJT-Pacific/Fiji, GMT+12:00-GILT-Pacific/Tarawa, GMT+12:00-MHT-Pacific/Majuro, GMT+12:00-MHT-Pacific/Kwajalein, GMT+12:00-NRT-Pacific/Nauru, GMT+12:00-NZST-Pacific/Auckland, GMT+12:45-CHAST-Pacific/Chatham, GMT+12:00-MAGST-Asia/Magadan, GMT+12:00-TVT-Pacific/Funafuti, GMT+12:00-WAKT-Pacific/Wake, GMT+12:00-WFT-Pacific/Wallis, GMT+13:00-PHOT-Pacific/Enderbury, GMT+13:00-PETST-Asia/Kamchatka, GMT+13:00-ANAST-Asia/Anadyr, GMT+13:00-TOT-Pacific/Tongatapu, GMT+14:00-LINT-Pacific/Kiritimati

Related Commands

clear ns config

unset ns config

save ns config

show ns config

diff ns config

unset ns config

Synopsis

```
unset ns config [-nsvlan] [-ftpPortRange] [-timezone]
[-IPAddress] [-netmask] [-ifnum] [-httpPort] [-maxConn]
[-maxReq] [-cip] [-cipHeader] [-cookieversion] [-
pmtuMin] [-pmtuTimeout]
```

Description

Unset the system parameters..Refer to the set ns config command for meanings of the arguments.

Related Commands

clear ns config

set ns config

save ns config

show ns config

diff ns config

save ns config

Synopsis

```
save ns config
```

Description

Save the system configuration to the system's FLASH. In a high availability setup, the command is sent to the primary system. The primary system then forwards the command to the secondary system. The entire system configuration is saved to the ns.conf file located in the /nsconfig directory. Backup configuration files are named ns.conf.n. The most recent backup file has the smallest value for n.

Output

Related Commands

clear ns config

set ns config

unset ns config

show ns config

diff ns config

show ns config

Synopsis

```
show ns config
```

Description

Display the version, build, and feature information of the system. Note:If you want to see the complete configuration parameters that have been set for the system, use ns runningconfig.

Arguments

format

level

Output

IPAddress
IP Address of the System.

netmask
Net Mask Address of the System.

mappedIP
Mapped IP Address of the System.

range
The range of Mapped IP addresses to be configured.

nsvlan
The VLAN (NSVLAN) for the subnet on which the system IP resides.

ifnum
This option is used to bind the given ports to the NSVLAN.

httpPort
The HTTP ports on the Web server.

maxConn
Maximum Number of Connections.

maxReq
Maxmimum Number of requests that can be handled.

cip
Insertion of client IP address into the HTTP header.

cipHeader
The text that is used as the client IP header.

cookieversion
The version of the cookie inserted by system.

failover
Standalone node.

primaryIP
HA Master Node IP address.

pmtuMin
The minimum Path MTU.

pmtuTimeout
The timeout value in minutes.

ftpPortRange
Port range configured for FTP services.

flags
The flags for this entry.

timezone
Name of the timezone

Related Commands

clear ns config
set ns config
unset ns config
save ns config
diff ns config

set ns hostName

Synopsis

```
set ns hostName <hostName>
```

Description

Sets the host name for the system.

Arguments

hostName

Desired host name. Maximum value: 255

Example

set ns hostname nspri

Related Commands

show ns hostName

show ns hostName

Synopsis

```
show ns hostName
```

Description

Display the host name of the system.

Arguments

format

level

Output

hostName
Host name

Example

show ns hostname

Related Commands

set ns hostName

add ns limitIdentifier

Synopsis

```
add ns limitIdentifier <limitIdentifier> [-threshold
<positive_integer>] [-timeSlice <positive_integer>] [-
mode <mode>  [-limitType ( BURSTY | SMOOTH )]] [-
selectorName <string>] [-maxBandwidth
<positive_integer>] [-trapsInTimeSlice
<positive_integer>]
```

Description

Create a limit identifier.

Arguments

limitIdentifier

The name of rate limit identifier.

threshold

The maximum number of requests that are allowed in the given timeslice when requests are tracked per timeslice. When connections (-mode CONNECTION)are tracked its the total number of connections that would be let through Default value: 1 Minimum value: 1

timeSlice

Defines the time interval in msecs specified in multiples of 10 msec during which the requests are tracked to see if they cross the threshold. It is used only when the mode is REQUEST_RATE while tracking request rate and for defining the trap timeslice Default value: 1000 Minimum value: 10

mode

Defines what is tracked - request rate, connections or none. Request rate is used to track requests/timeslice, connections will track active transactions. For DNS please use the mode as either NONE or REQUEST_RATE as CONNECTION is not supported. Eg: 1) add limitidentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200 will permit 20 requests in 10 ms and 2 Traps in 10 ms 2) set limitidentifier limit_req -timeslice 1000 -Threshold 5000 -

limitType smooTH will permit 50 Requests in 10 ms 3) set limitidentifier limit_req -mode smooth -timeslice 2000 -Threshold 50 will permit 1 request in 40 ms 4) set limitidentifier limit_req -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8 will permit 1 request in 200 ms and 1 Trap in 130 ms 5) set limitidentifier limit_req -timeslice 1000 -Threshold 5000 -limitType BURSTY will permit 5000 Requests in 1000 ms and 200 Traps in 1000 ms As you see in the above examples smooth mode is used when one wants the permitted number of requests in a given interval of time to be spread evenly across the timeslice while bursty is used when one is ok to let the permitted number of requests to exhaust the quota anytime within the timeslice. Possible values: CONNECTION, REQUEST_RATE, NONE Default value: PEMGMT_RLT_MODE_REQ_RATE

limitType

Specifies if it is a smooth or bursty request type. If the smooth mode of operation is chosen requests are tracked at the rate of 10 ms. To be specified with -mode REQUEST_RATE . Possible values: BURSTY, SMOOTH Default value: PEMGMT_RLT_REQ_RATE_TYPE_BURSTY

selectorName

The name of rate limit selector.

maxBandwidth

The maximum bandwidth permitted in kbps Default value: 0 Minimum value: 0 Maximum value: 0xFFFFFFF7

trapsInTimeSlice

Number of traps that would be sent in the timeslice configured. A value of zero means that the traps are disabled. Default value: 0 Minimum value: 0 Maximum value: 65535

Example

add ns limitIdentifier limit_id -threshold 2 -timeSlice 5000 -mode CONNECTION -selectorName sel_1 -maxBandwidth 24 -trapsInTimeSlice 8

Related Commands

rm ns limitIdentifier

set ns limitIdentifier

unset ns limitIdentifier

show ns limitIdentifier

rm ns limitIdentifier

Synopsis

```
rm ns limitIdentifier <limitIdentifier>
```

Description

The command deletes the rate limit identifier.

Arguments

`limitIdentifier`

The name of rate limit identifier.

Example

rm ns limitIdentifier limit_id

Related Commands

add ns limitIdentifier

set ns limitIdentifier

unset ns limitIdentifier

show ns limitIdentifier

set ns limitIdentifier

Synopsis

```
set ns limitIdentifier <limitIdentifier> [-threshold
<positive_integer>] [-timeSlice <positive_integer>] [-
mode <mode>  [-limitType ( BURSTY | SMOOTH )]] [-
selectorName <string>] [-maxBandwidth
<positive_integer>] [-trapsInTimeSlice
<positive_integer>]
```

Description

set limit identifier params.

Arguments

limitIdentifier

The name of rate limit identifier.

threshold

The maximum number of requests that are allowed in the given timeslice when requests are tracked per timeslice. When connections (-mode CONNECTION)are tracked its the total number of connections that would be let through Default value: 1 Minimum value: 1

timeSlice

Defines the time interval in msecs specified in multiples of 10 msec during which the requests are tracked to see if they cross the threshold. It is used only when the mode is REQUEST_RATE while tracking request rate and for defining the trap timeslice Default value: 1000 Minimum value: 10

mode

Defines what is tracked - request rate, connections or none. Request rate is used to track requests/timeslice, connections will track active transactions. For DNS please use the mode as either NONE or REQUEST_RATE as CONNECTION is not supported. Eg: 1) add limitidentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200 will permit 20 requests in 10 ms and 2 Traps in 10 ms 2) set limitidentifier limit_req -timeslice 1000 -Threshold 5000 -

limitType smooTH will permit 50 Requests in 10 ms 3) set limitidentifier limit_req -mode smooth -timeslice 2000 -Threshold 50 will permit 1 request in 40 ms 4) set limitidentifier limit_req -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8 will permit 1 request in 200 ms and 1 Trap in 130 ms 5) set limitidentifier limit_req -timeslice 1000 -Threshold 5000 -limitType BURSTY will permit 5000 Requests in 1000 ms and 200 Traps in 1000 ms As you see in the above examples smooth mode is used when one wants the permitted number of requests in a given interval of time to be spread evenly across the timeslice while bursty is used when one is ok to let the permitted number of requests to exhaust the quota anytime within the timeslice. Possible values: CONNECTION, REQUEST_RATE, NONE Default value: PEMGMT_RLT_MODE_REQ_RATE

selectorName

The name of rate limit selector.

maxBandwidth

The maximum bandwidth permitted in kbps Minimum value: 0 Maximum value: 0xFFFFFFF7

trapsInTimeSlice

Number of traps that would be sent in the timeslice configured. A value of zero means that the traps are disabled. Default value: 0 Minimum value: 0 Maximum value: 65535

Example

set ns limitIdentifier limit_id -threshold 2 -timeSlice 5000 -mode CONNECTION -selectorName sel_1 -maxBandwidth 24 -trapsInTimeSlice 8

Related Commands

add ns limitIdentifier

rm ns limitIdentifier

unset ns limitIdentifier

show ns limitIdentifier

unset ns limitIdentifier

Synopsis

```
unset ns limitIdentifier <limitIdentifier> [-
selectorName] [-threshold] [-timeSlice] [-mode] [-
limitType] [-maxBandwidth] [-trapsInTimeSlice]
```

Description

Use this command to remove ns limitIdentifier settings.Refer to the set ns limitIdentifier command for meanings of the arguments.

Related Commands

add ns limitIdentifier

rm ns limitIdentifier

set ns limitIdentifier

show ns limitIdentifier

show ns limitIdentifier

Synopsis

```
show ns limitIdentifier [<limitIdentifier>]
```

Description

Display rate limit identifiers.

Arguments

limitIdentifier

The name of the rate limit identifier.

summary

fullValues

format

level

Output

threshold

The maximum number of requests that are allowed in the given timeslice when requests are tracked per timeslice. When connections (-mode CONNECTION)are tracked its the total number of connections that would be let through

timeSlice

Defines the time interval in msecs specified in multiples of 10 msec during which the requests are tracked to see if they cross the threshold. It is used and displayed only when the mode is REQUEST_RATE while tracking request rate and for defining the trap timeslice.

mode

Defines what is tracked - request rate, connections or none. Request rate is used to track requests/timeslice, connections will track active transactions. For DNS please use the mode as either NONE or REQUEST_RATE as CONNECTION is not supported. Eg: 1) add limitidentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -

trapsInTimeSlice 200 will permit 20 requests in 10 ms and 2 Traps in 10 ms 2) set limitidentifier limit_req -timeslice 1000 -Threshold 5000 -limitType smooTH will permit 50 Requests in 10 ms 3) set limitidentifier limit_req -mode smooth -timeslice 2000 -Threshold 50 will permit 1 request in 40 ms 4) set limitidentifier limit_req -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8 will permit 1 request in 200 ms and 1 Trap in 130 ms 5) set limitidentifier limit_req -timeslice 1000 -Threshold 5000 -limitType BURSTY will permit 5000 Requests in 1000 ms and 200 Traps in 1000 ms As you see in the above examples smooth mode is used when one wants the permitted number of requests in a given interval of time to be spread evenly across the timeslice while bursty is used when one is ok to let the permitted number of requests to exhaust the quota anytime within the timeslice.

limitType
Specifies if it is a smooth or bursty request type. If the smooth mode of operation is chosen requests are tracked at the rate of 10 ms. To be specified with -mode REQUEST_RATE .

selectorName
The name of rate limit selector.

flags
This is used internally to identify ip addresses returned.

hits
The number of times this identifier was evaluated.

drop
The number of times action was taken.

rule
Rule.

time
Time interval considered for rate limiting

total
Maximum number of requests permitted in the computed timeslice

maxBandwidth
The maximum bandwidth in kbps permitted

trapsInTimeSlice
The maximum bandwidth permitted in kbps

trapsComputedInTimeSlice
The number of traps that would be sent in the timeslice configured.

computedTrapTimeSlice
The time interval computed for sending traps.

referenceCount
Total number of transactions pointing to this entry.

Example

show ns limitIdentifier limit_id

Related Commands

add ns limitIdentifier
rm ns limitIdentifier
set ns limitIdentifier
unset ns limitIdentifier

add ns limitSelector

Synopsis

```
add ns limitSelector <selectorName> <rule> ...
```

Description

Create rate limit selectors. A selector is an abstraction for a collection of PIXL expressions.

Arguments

`selectorName`

The name of rate limit selector.

`rule`

The set of PIXL expressions.

Example

add ns limitSelector sel_subnet Q.URL CLIENT.IP.SRC.SUBNET(24)

Related Commands

rm ns limitSelector

set ns limitSelector

show ns limitSelector

rm ns limitSelector

Synopsis

```
rm ns limitSelector <selectorName>
```

Description

The command deletes the rate limit selector.

Arguments

`selectorName`

The name of rate limit selector.

Example

rm ns limitSelector sel_subnet

Related Commands

add ns limitSelector

set ns limitSelector

show ns limitSelector

set ns limitSelector

Synopsis

```
set ns limitSelector <selectorName> <rule> ...
```

Description

Change the set of expressions associated with the rate limit selector.

Arguments

`selectorName`

The name of rate limit selector.

`rule`

The set of PIXL expressions.

Example

set ns limitSelector sel_subnet Q.URL CLIENT.IP.SRC

Related Commands

add ns limitSelector

rm ns limitSelector

show ns limitSelector

show ns limitSelector

Synopsis

```
show ns limitSelector [<selectorName>]
```

Description

Display rate limit selectors.

Arguments

selectorName

The name of the rate limit selector.

summary

fullValues

format

level

Output

flags

Flags.

rule

Rule.

Example

show ns limitSelector sel_subnet

Related Commands

add ns limitSelector

rm ns limitSelector

set ns limitSelector

add ns acl

Synopsis

```
add ns acl <aclname> <aclaction> [-srcIP  [<operator>]
<srcIPVal>] [-srcPort  [<operator>]  <srcPortVal>] [-
destIP  [<operator>]  <destIPVal>] [-destPort
[<operator>]  <destPortVal>] [-TTL <positive_integer>]
[-srcMac <mac_addr>] [(-protocol <protocol>  [-
established]) | -protocolNumber <positive_integer>] [-
vlan <positive_integer>] [-interface <interface_name>]
[-icmpType <positive_integer>  [-icmpCode
<positive_integer>]] [-priority <positive_integer>] [-
state ( ENABLED | DISABLED )] [-logstate ( ENABLED |
DISABLED )  [-ratelimit <positive_integer>]]
```

Description

Add an ACL to the System configuration. Each inbound packet is matched against configured ACLs and the specified action is applied to the packet. This command adds the acl to the configuration space. To commit this ACL, one should apply the ACL.

Arguments

aclname

The alphanumeric name of the ACL.

aclaction

The action associated with the ACL. Possible values: BRIDGE, DENY, ALLOW

srcIP

The source IP address (range).

srcPort

The source Port (range).

destIP

The destination IP address (range).

destPort
The destination Port (range).

TTL
The time to expire this ACL(in seconds). Minimum value: 1 Maximum value: 0x7FFFFFFF

srcMac
The source MAC address.

protocol
The IP protocol name. Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS

protocolNumber
The IP protocol number (decimal). Minimum value: 1 Maximum value: 255

vlan
The VLAN number. Minimum value: 1 Maximum value: 4094

interface
The physical interface.

established
This argument indicates that the ACL should be used for TCP response traffic only. Default value: NSACL_ESTABLISHED

icmpType
The ICMP message type Default value: 65536 Minimum value: 0 Maximum value: 255

icmpCode
The ICMP message code Default value: 65536 Minimum value: 0 Maximum value: 255

priority
The priority of the ACL. Minimum value: 1 Maximum value: 10240

state
The state of the ACL. Possible values: ENABLED, DISABLED Default value: XACLENABLED

logstate

The logging state of the ACL. Possible values: ENABLED, DISABLED Default value: GENDISABLED

ratelimit

log message rate limit for acl rule Default value: 100 Minimum value: 1 Maximum value: 10000

Example

add ns acl restrict DENY -srcport 45-1024 -destIP 192.168.1.1 -protocol TCP

Related Commands

clear acls

apply acls

rm ns acl

set ns acl

unset ns acl

enable ns acl

disable ns acl

stat ns acl

show ns acl

rm ns acl

Synopsis

```
rm ns acl <aclname> ...
```

Description

Remove an ACL. To commit this operation, one should apply the ACL.

Arguments

aclname

The name of the ACL to be deleted.

Example

rm ns acl restrict

Related Commands

apply acls
clear acls
add ns acl
set ns acl
unset ns acl
enable ns acl
disable ns acl
stat ns acl
show ns acl

set ns acl

Synopsis

```
set ns acl <aclname> [-aclaction <aclaction>] [-srcIP
[<operator>]  <srcIPVal>] [-srcPort  [<operator>]
<srcPortVal>] [-destIP  [<operator>]  <destIPVal>] [-
destPort  [<operator>]  <destPortVal>] [-srcMac
<mac_addr>] [-protocol <protocol> | -protocolNumber
<positive_integer>] [-icmpType <positive_integer>  [-
icmpCode <positive_integer>]] [-vlan
<positive_integer>] [-interface <interface_name>] [-
priority <positive_integer>] [-state ( ENABLED |
DISABLED )] [-logstate ( ENABLED | DISABLED )] [-
ratelimit <positive_integer>]
```

Description

Modify an ACL. To commit this modified ACL, use the 'apply acls' command.

Arguments

aclname

The alphanumeric name of the ACL.

aclaction

The action associated with the ACL. Possible values: BRIDGE, DENY, ALLOW

srcIP

The source IP address (range).

srcPort

The source Port (range).

destIP

The destination IP address (range).

destPort
The destination Port (range).

srcMac
The source MAC address.

protocol
The IP protocol name. Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS

protocolNumber
The IP protocol number (decimal). Minimum value: 1 Maximum value: 255

icmpType
The ICMP message type Default value: 65536 Minimum value: 0 Maximum value: 255

vlan
The VLAN number. Minimum value: 1 Maximum value: 4094

interface
The physical interface.

priority
The priority of the ACL. Minimum value: 1 Maximum value: 10240

state
The state of the ACL. Possible values: ENABLED, DISABLED Default value: XACLENABLED

logstate
The logging state of the ACL. Possible values: ENABLED, DISABLED Default value: GENDISABLED

Example

set ns acl restrict -srcPort 50

Related Commands

clear acls

apply acls

add ns acl

rm ns acl

unset ns acl
enable ns acl
disable ns acl
stat ns acl
show ns acl

unset ns acl

Synopsis

```
unset ns acl <aclname> [-srcIP] [-srcPort] [-destIP] [-
destPort] [-srcMac] [-protocol] [-icmpType] [-icmpCode]
[-vlan] [-interface] [-logstate] [-ratelimit]
```

Description

Modify an ACL. To commit this modified ACL, use the 'apply acls' command..Refer to the set ns acl command for meanings of the arguments.

Example

unset ns acl rule1 -srcPort

Related Commands

set ns acl
clear acls
apply acls
add ns acl
rm ns acl
enable ns acl
disable ns acl
stat ns acl
show ns acl

enable ns acl

Synopsis

```
enable ns acl <aclname> ...
```

Description

Enable an ACL. To commit this operation, one should apply the ACL.

Arguments

aclname

The name of the ACL to be enabled.

Example

enable ns acl foo

Related Commands

apply acls
clear acls
add ns acl
rm ns acl
set ns acl
unset ns acl
disable ns acl
stat ns acl
show ns acl

disable ns acl

Synopsis

```
disable ns acl <aclname> ...
```

Description

Disable an ACL. To commit this operation, one should apply the ACL.

Arguments

aclname

The name of the ACL to be disabled.

Example

disable ns acl foo

Related Commands

apply acls
clear acls
add ns acl
rm ns acl
set ns acl
unset ns acl
enable ns acl
stat ns acl
show ns acl

stat ns acl

Synopsis

```
stat ns acl [<aclname>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display ACL statistics.

Arguments

aclname
The ACL.

Output

Counters

Bridge ACL hits (ACLBdg)
Packets matching a bridge ACL, which in transparent mode bypasses service processing.

Deny ACL hits (ACLDeny)
Packets dropped because they match ACLs with processing mode set to DENY.

Allow ACL hits (ACLAllow)
Packets matching ACLs with processing mode set to ALLOW. NetScaler processes these packets.

NAT ACL hits (ACLNAT)
Packets matching a NAT ACL, resulting in a NAT session.

ACL hits (ACLHits)
Packets matching an ACL.

ACL misses (ACLMiss)
Packets not matching any ACL.

Hits for this ACL (Hits)
Number of times the acl was hit

Example

stat acl

Related Commands

add ns acl
rm ns acl
set ns acl
unset ns acl
enable ns acl
disable ns acl
show ns acl
stat ns
stat ns acl6
stat ns simpleacl

show ns acl

Synopsis

```
show ns acl [<aclname>]
```

Description

Display the ACLs.If name is specified, then only that particular ACL information is displayed. If it is not specified, all configured ACLs are displayed.

Arguments

aclname
The name of the ACL.

summary

fullValues

format

level

Output

aclaction
The action associated with the ACL.

srcMac
The source MAC address.

state
ACL state flag.

protocol
The protocol number in IP header or name.

protocolNumber
The protocol number in IP header or name.

srcPortVal
The source Port (range).

destPortVal
The destination Port (range).

srcIPVal
The source IP address (range).

destIPVal
The destination IP address (range).

vlan
The VLAN number.

state
The state of the ACL.

TTL
The time to expire this ACL(in seconds).

icmpType
The ICMP message type

icmpCode
The ICMP message code

interface
The physical interface.

hits
The hits of this ACL.

established
This flag indicates that the ACL should be used for TCP response traffic only.

priority
The priority of the ACL.

operator
Logical operator.

operator
Logical operator.

operator
Logical operator.

operator
Logical operator.

kernelstate
The commit status of the ACL.

logstate
The logging state of the ACL.

ratelimit
Packet rate limit for acl logging

Example

sh acl foo Name: foo Action: ALLOWHits: 0 srcIP = 10.102.1.150 destIP = 202.54.12.47 srcMac: Protocol: TCP srcPort destPort = 110 Vlan: Interface: Active Status: ENABLED Applied Status: NOTAPPLIED Priority: 1027

Related Commands

add ns acl

rm ns acl

set ns acl

unset ns acl

enable ns acl

disable ns acl

stat ns acl

add ns acl6

Synopsis

```
add ns acl6 <acl6name> <acl6action> [-srcIPv6
[<operator>]  <srcIPv6Val>] [-srcPort  [<operator>]
<srcPortVal>] [-destIPv6  [<operator>]  <destIPv6Val>]
[-destPort  [<operator>]  <destPortVal>] [-TTL
<positive_integer>] [-srcMac <mac_addr>] [(-protocol
<protocol>  [-established]) | -protocolNumber
<positive_integer>] [-vlan <positive_integer>] [-
interface <interface_name>] [-icmpType
<positive_integer>  [-icmpCode <positive_integer>]] [-
priority <positive_integer>] [-state ( ENABLED |
DISABLED )]
```

Description

Add an IPv6 ACL to the System configuration. Each inbound packet is matched against configured ACLs and the specified action is applied to the packet. This command adds the IPv6 ACL to the configuration space. To commit this ACL, one should apply the ACL.

Arguments

acl6name
Alphanumeric name of the ACL6.

acl6action
Action associated with the ACL6. Possible values: BRIDGE, DENY, ALLOW

srcIPv6
Source IPv6 address (range).

srcPort
Source port (range).

destIPv6
Destination IPv6 address (range).

destPort
Destination port (range).

TTL
Time to expire this ACL6 (in seconds). Minimum value: 1 Maximum value: 0x7FFFFFFF

srcMac
Source MAC address.

protocol
IPv6 protocol name. Possible values: ICMPV6, TCP, UDP

protocolNumber
IPv6 protocol number (decimal). Minimum value: 1 Maximum value: 255

vlan
VLAN number. Minimum value: 1 Maximum value: 4094

interface
Physical interface name.

established
This argument indicates that the ACL6 should be used for TCP response traffic only. Default value: NSACL_ESTABLISHED

icmpType
ICMPv6 message type Default value: 65536 Minimum value: 0 Maximum value: 255

icmpCode
ICMPv6 message code Default value: 65536 Minimum value: 0 Maximum value: 255

priority
Priority of the ACL6. (Sequence of execution) Minimum value: 1 Maximum value: 10240

state
State of the ACL6. Possible values: ENABLED, DISABLED Default value: XACLENABLED

Example

add ns acl6 rule1 DENY -srcport 45-1024 -destIPv6 2001::45 -protocol TCP

Related Commands

clear ns acls6
apply ns acls6
rm ns acl6
set ns acl6
unset ns acl6
enable ns acl6
disable ns acl6
stat ns acl6
show ns acl6

rm ns acl6

Synopsis

```
rm ns acl6 <acl6name> ...
```

Description

Remove an ACL6. To commit this operation, one should apply the ACL6.

Arguments

acl6name

Name of the ACL6 to be deleted.

Example

rm ns acl6 rule1

Related Commands

apply ns acls6
clear ns acls6
add ns acl6
set ns acl6
unset ns acl6
enable ns acl6
disable ns acl6
stat ns acl6
show ns acl6

set ns acl6

Synopsis

```
set ns acl6 <acl6name> [-aclaction <aclaction>] [-
srcIPv6 [<operator>] <srcIPv6Val>] [-srcPort
[<operator>] <srcPortVal>] [-destIPv6 [<operator>]
<destIPv6Val>] [-destPort [<operator>] <destPortVal>]
[-srcMac <mac_addr>] [-protocol <protocol> | -
protocolNumber <positive_integer>] [-icmpType
<positive_integer> [-icmpCode <positive_integer>]] [-
vlan <positive_integer>] [-interface <interface_name>]
[-priority <positive_integer>] [-state ( ENABLED |
DISABLED )]
```

Description

Modify an ACL6. To commit this modified ACL6, use 'apply acls6' command.

Arguments

acl6name
Alphanumeric name of the ACL6.

aclaction
Action associated with the ACL6. Possible values: BRIDGE, DENY, ALLOW

srcIPv6
Source IPv6 address (range).

srcPort
Source Port (range).

destIPv6
Destination IPv6 address (range).

destPort
Destination Port (range).

srcMac
Source MAC address.

protocol
IPv6 protocol name. Possible values: ICMPV6, TCP, UDP

protocolNumber
IPv6 protocol number (decimal). Minimum value: 1 Maximum value: 255

icmpType
ICMPv6 message type Default value: 65536 Minimum value: 0 Maximum value: 255

vlan
VLAN number. Minimum value: 1 Maximum value: 4094

interface
Physical interface name.

priority
Priority of the ACL6. (Sequence of execution) Minimum value: 1 Maximum value: 10240

state
State of the ACL6. Possible values: ENABLED, DISABLED Default value: XACLENABLED

Example

set ns acl6 rule1 -srcPort 50

Related Commands

clear ns acls6
apply ns acls6
add ns acl6
rm ns acl6
unset ns acl6
enable ns acl6
disable ns acl6
stat ns acl6
show ns acl6

unset ns acl6

Synopsis

```
unset ns acl6 <acl6name> [-srcIPv6] [-srcPort] [-
destIPv6] [-destPort] [-srcMac] [-protocol] [-icmpType]
[-icmpCode] [-vlan] [-interface]
```

Description

Modify an ACL6. To commit this modified ACL6, use 'apply acls6' command..Refer to the set ns acl6 command for meanings of the arguments.

Example

unset ns acl6 rule1 -srcPort

Related Commands

set ns acl6
clear ns acls6
apply ns acls6
add ns acl6
rm ns acl6
enable ns acl6
disable ns acl6
stat ns acl6
show ns acl6

enable ns acl6

Synopsis

```
enable ns acl6 <acl6name> ...
```

Description

Enable an ACL6. To commit this operation, one should apply the ACL6.

Arguments

acl6name

Name of the ACL6 to be enabled.

Example

enable ns acl6 rule1

Related Commands

apply ns acls6

clear ns acls6

add ns acl6

rm ns acl6

set ns acl6

unset ns acl6

disable ns acl6

stat ns acl6

show ns acl6

disable ns acl6

Synopsis

```
disable ns acl6 <acl6name> ...
```

Description

Disable an ACL6. To commit this operation, one should apply the ACL6.

Arguments

acl6name

Name of the ACL6 to be disabled.

Example

disable ns acl6 rule1

Related Commands

apply ns acls6
clear ns acls6
add ns acl6
rm ns acl6
set ns acl6
unset ns acl6
enable ns acl6
stat ns acl6
show ns acl6

stat ns acl6

Synopsis

```
stat ns acl6 [<acl6name>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display ACL6 statistics.

Arguments

acl6name
ACL6 Name.

Output

Counters

Bridge ACL6 hits (ACL6Bdg)
Packets matching a bridge IPv6 ACL, which in transparent mode bypasses service processing.

Deny ACL6 hits (ACL6Deny)
Packets dropped because they match IPv6 ACLs with processing mode set to DENY.

Allow ACL6 hits (ACL6Allow)
Packets matching IPv6 ACLs with processing mode set to ALLOW. NetScaler processes these packets.

NAT ACL6 hits (ACL6NAT)
Packets matching a NAT ACL6, resulting in a NAT session.

ACL6 hits (ACL6Hits)
Packets matching an IPv6 ACL.

ACL6 misses (ACL6Miss)
Packets not matching any IPv6 ACL.

Hits for this ACL6 (Hits)
Number of times the acl6 was hit

Example

stat acl6

Related Commands

add ns acl6
rm ns acl6
set ns acl6
unset ns acl6
enable ns acl6
disable ns acl6
show ns acl6
stat ns
stat ns acl
stat ns simpleacl

show ns acl6

Synopsis

```
show ns acl6 [<acl6name>]
```

Description

Display the ACL6. If name is specified, then only that particular ACL6 information is displayed. If it is not specified, all configured ACL6 are displayed.

Arguments

acl6name
Name of the ACL6.

summary

fullValues

format

level

Output

acl6action
Action associated with the ACL6.

srcMac
Source MAC address.

state
ACL6 state flag.

protocol
Protocol number in IPv6 header or name.

protocolNumber
Protocol number in IPv6 header or name.

srcPortVal
Source Port (range).

destPortVal
Destination Port (range).

srcIPv6Val
Source IPv6 address (range).

destIPv6Val
Destination IPv6 address (range).

vlan
VLAN number.

state
State of the ACL6.

kernelstate
Commit status of the ACL6.

TTL
Time left to expire ACL6 (in seconds).

icmpType
ICMPv6 message type

icmpCode
ICMPv6 message code

interface
Physical interface name.

hits
Number of hits of this ACL6.

established
This flag indicates that the ACL6 should be used for TCP response traffic only.

priority
Priority of the ACL6. (Sequence of execution)

operator
Logical operator.

operator
Logical operator.

operator
Logical operator.

operator
Logical operator.

Example

show ns acl6 rule1 1) Name: r1 Action: DENY srcIPv6 = 2001::1 destIPv6 srcMac: Protocol: Vlan: Interface: Active Status: ENABLED Applied Status: NOTAPPLIED Priority: 10 Hits: 0 TTL:

Related Commands

add ns acl6
rm ns acl6
set ns acl6
unset ns acl6
enable ns acl6
disable ns acl6
stat ns acl6

enable ns feature

Synopsis

```
enable ns feature <feature> ...
```

Description

Enable a specific feature.

Arguments

`feature`

The feature to be enabled.

Output

`reqFeature`

Required Feature.

Example

enable ns feature sc This CLI command enables the SureConnect feature.

Related Commands

disable ns feature

show ns feature

disable ns feature

Synopsis

```
disable ns feature <feature> ...
```

Description

Disable a specified feature or features.

Arguments

`feature`

The name of the feature to be disabled.

Output

`reqFeature`

Required Feature.

Related Commands

disable ns mode

enable ns feature

show ns feature

show ns feature

Synopsis

```
show ns feature
```

Description

Display the current status of System features.

Arguments

Output

WL
Web Logging.

SP
Surge Protection.

LB
Load Balancing.

CS
Content Switching.

CR
Cache Redirect.

SC
Sure Connect.

CMP
Compression.

PQ
Priority Queuing.

SSL
Secure Sockets Layer.

GSLB
Global Server Load Balancing.

HDOSP
DOS Protection.

Routing
Routing.NOTE: This attribute is deprecated.

CF
Content Filter.

IC
Integrated Caching.

SSLVPN
SSL VPN.

AAA
AAA

OSPF
OSPF Routing.

RIP
RIP Routing.

BGP
BGP Routing.

REWRITE
Rewrite.

IPv6PT
IPv6 protocol translation

AppFw
Application Firewall.

RESPONDER
Responder.

HTMLInjection
HTML Injection.

push
NetScaler Push.

Related Commands

enable ns feature

disable ns feature

add ns ip6

Synopsis

```
add ns ip6 <IPv6Address>@ [-scope ( global | link-local
)] [-type <type>  [-hostRoute ( ENABLED | DISABLED )
[-ip6hostRtGw <ipv6_addr|*>]  [-metric <integer>]  [-
vserverRHILevel <vserverRHILevel>]  [-ospf6LSAType (
INTRA_AREA | EXTERNAL )  [-ospfArea
<positive_integer>]]]] [-nd ( ENABLED | DISABLED )] [-
icmp ( ENABLED | DISABLED )] [-vServer ( ENABLED |
DISABLED )] [-telnet ( ENABLED | DISABLED )] [-ftp (
ENABLED | DISABLED )] [-gui <gui>] [-ssh ( ENABLED |
DISABLED )] [-snmp ( ENABLED | DISABLED )] [-mgmtAccess
( ENABLED | DISABLED )] [-dynamicRouting ( ENABLED |
DISABLED )] [-state ( DISABLED | ENABLED )] [-map
<ip_addr>]
```

Description

Add an IPV6 address.

Arguments

IPv6Address

The IPV6 address

scope

The scope of the IPV6 address Possible values: global, link-local Default value: NS_GLOBAL

type

The type of the IPV6 address. Possible values: NSIP, VIP, SNIP Default value: NS_IPV6_SNIP

nd

Use this option to set (enable or disable) ND responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp
Use this option to set (enable or disable) ICMP responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer
Use this option to set (enable or disable) the vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet
Use this option to set (enable or disable) the state of telnet access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp
Use this option to set (enable or disable) the state of ftp access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

gui
Use this option to set (enable|Secureonly|disable) GUI access to this IP entity. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh
Use this option to set (enable or disable) the state of SSH access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp
Use this option to set (enable or disable) the state of SNMP access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess
Use this option to set (enable or disable) the state of management access to this IP entity. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting
Use this option to enable or disable dynamic routing on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute
The state of advertisement of a hostroute to this IPv6 entity. Possible values: ENABLED, DISABLED

ip6hostRtGw
The gateway for the hostroute to be advertised for this IPv6 entity. Default value: 0

metric
The metric value to be added or subtracted from the cost of the hostroute advertised for this IP entity. Minimum value: -16777215

vserverRHILevel
The state of per VIP RHI controls. Possible values: ONE_VSERVER, ALL_VSERVERS, NONE Default value: RHI_STATE_ONE

ospf6LSAType
The OSPF6's route advertisement type. Possible values: INTRA_AREA, EXTERNAL Default value: DISABLED

ospfArea
The area ID of the area in which OSPF intra area prefix LSAs should be advertised. Default value: -1 Minimum value: 0

state
Use this option to enable or disable the entity. Possible values: DISABLED, ENABLED Default value: ENABLED

map
The mapped IPV4 address for IPV6.

Example

add ns ip6 2001::a/96 -scope GLOBAL

Related Commands

rm ns ip6

set ns ip6

unset ns ip6

show ns ip6

rm ns ip6

Synopsis

```
rm ns ip6 <IPv6Address>@
```

Description

Remove an IPv6 entity.

Arguments

IPv6Address

The IPV6 address of the entity.

Example

rm ns ip6 2002::5

Related Commands

add ns ip6

set ns ip6

unset ns ip6

show ns ip6

set ns ip6

Synopsis

```
set ns ip6 <IPv6Address>@ [-nd ( ENABLED | DISABLED )]
[-icmp ( ENABLED | DISABLED )] [-vServer ( ENABLED |
DISABLED )] [-telnet ( ENABLED | DISABLED )] [-ftp (
ENABLED | DISABLED )] [-gui <gui>] [-ssh ( ENABLED |
DISABLED )] [-snmp ( ENABLED | DISABLED )] [-mgmtAccess
( ENABLED | DISABLED )] [-state ( DISABLED | ENABLED )]
[-map <ip_addr>] [-dynamicRouting ( ENABLED | DISABLED
)] [-hostRoute ( ENABLED | DISABLED )  [-ip6hostRtGw
<ipv6_addr|*>]  [-metric <integer>]  [-vserverRHILevel
<vserverRHILevel>]  [-ospf6LSAType ( INTRA_AREA |
EXTERNAL )  [-ospfArea <positive_integer>]]]
```

Description

Set IP6 address options.

Arguments

IPv6Address

The IPV6 address

nd

The state of ND responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

The state of ICMP responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer

The state of vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet

The state of telnet access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp
The state of ftp access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

gui
The state of GUI access to this IP entity. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh
The state of SSH access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp
The state of SNMP access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess
The state of management access to this IP entity. Possible values: ENABLED, DISABLED Default value: DISABLED

state
Use this option to enable or disable the entity. Possible values: DISABLED, ENABLED Default value: ENABLED

map
The mapped IPV4 address for IPV6.

dynamicRouting
Use this option to enable or disable dynamic routing on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute
The state of advertisement of a hostroute to this IPv6 entity. Possible values: ENABLED, DISABLED

Example

set ns ip6 2001::a -map 10.102.33.27

Related Commands

add ns ip6

rm ns ip6

unset ns ip6

show ns ip6

unset ns ip6

Synopsis

```
unset ns ip6 <IPv6Address>@ [-nd] [-icmp] [-vServer] [-
telnet] [-ftp] [-gui] [-ssh] [-snmp] [-mgmtAccess] [-
state] [-map] [-dynamicRouting] [-hostRoute] [-
ip6hostRtGw] [-metric] [-vserverRHILevel] [-
ospf6LSAType] [-ospfArea]
```

Description

Use this command to remove ns ip6 settings.Refer to the set ns ip6 command for meanings of the arguments.

Related Commands

add ns ip6

rm ns ip6

set ns ip6

show ns ip6

show ns ip6

Synopsis

```
show ns ip6 [<IPv6Address>]
```

Description

Display all IPV6 addresses

Arguments

IPv6Address
The IPV6 address

format

level

Output

scope
The scope of the IPV6 address

type
The type of the IPV6 address

nd
Whether ND is enabled or disabled.

icmp
Whether icmp is enabled or disabled.

vServer
Whether vserver is enabled or disabled.

telnet
Whether telnet is enabled or disabled.

ssh
Whether ssh is enabled or disabled.

gui
Whether gui is (enabled|SecureOnly|disabled).

snmp
Whether snmp is enabled or disabled.

ftp
Whether ftp is enabled or disabled.

mgmtAccess
Whether management access is enabled or disabled.

state
The state of the IPV6 address

map
The mapped IPV4 address for IPV6.

dynamicRouting
Use this option to enable or disable dynamic routing on this IP address for the entity.

hostRoute
The state of advertisement of a hostroute to this IPv6 entity.

ip6hostRtGw
The gateway for the hostroute to be advertised for this IPv6 entity.

metric
The metric value to be added or subtracted from the cost of the hostroute advertised for this IPv6 entity.

vserverRHILevel
The state of per VIP RHI controls.

ospf6LSAType
The OSPF's route advertisement type.

ospfArea
The area ID of the area in which OSPF INTRA AREA PREFIX LSAs should be advertised.

Example

show ns ip6

Related Commands

add ns ip6

rm ns ip6

set ns ip6

unset ns ip6

add ns ip

Synopsis

```
add ns ip <IPAddress>@ <netmask> [-type <type>  [-
hostRoute ( ENABLED | DISABLED )  [-hostRtGw <ip_addr>]
[-metric <integer>]  [-vserverRHILevel
<vserverRHILevel>]  [-ospfLSAType ( TYPE1 | TYPE5 )  [-
ospfArea <positive_integer>]]] ] [-arp ( ENABLED |
DISABLED )] [-icmp ( ENABLED | DISABLED )] [-vServer (
ENABLED | DISABLED )] [-telnet ( ENABLED | DISABLED )]
[-ftp ( ENABLED | DISABLED )] [-gui <gui>] [-ssh (
ENABLED | DISABLED )] [-snmp ( ENABLED | DISABLED )] [-
mgmtAccess ( ENABLED | DISABLED )] [-dynamicRouting (
ENABLED | DISABLED )] [-state ( ENABLED | DISABLED )]
```

Description

Add an IP address.

Arguments

IPAddress

The IP address of the entity.

netmask

The netmask of the IP.

type

The type of the IP address. Possible values: SNIP, VIP, MIP, NSIP, GSLBsiteIP Default value: NSADDR_SNIP

arp

Use this option to set (enable or disable) ARP and gratuitous ARP for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

Use this option to set (enable or disable) ICMP responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer
Use this option to set (enable or disable) the vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet
Use this option to set (enable or disable) the state of telnet access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp
Use this option to set (enable or disable) the state of ftp access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

gui
Use this option to set (enable|Secureonly|disable) GUI access to this IP entity. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh
Use this option to set (enable or disable) the state of SSH access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp
Use this option to set (enable or disable) the state of SNMP access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess
Use this option to set (enable or disable) the state of management access to this IP entity. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting
Use this option to enable or disable dynamic routing on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

ospf
Use this option to enable or disable OSPF on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

bgp
Use this option to enable or disable BGP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

rip
Use this option to enable or disable RIP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute
The state of advertisement of a hostroute to this IP entity. Possible values: ENABLED, DISABLED

hostRtGw
The gateway for the hostroute to be advertised for this IP entity. Default value: -1

metric
The metric value to be added or subtracted from the cost of the hostroute advertised for this IP entity. Minimum value: -16777215

vserverRHILevel
The state of per VIP RHI controls. Possible values: ONE_VSERVER, ALL_VSERVERS, NONE Default value: RHI_STATE_ONE

ospfLSAType
The OSPF's route advertisement type. Possible values: TYPE1, TYPE5 Default value: DISABLED

ospfArea
The area ID of the area in which OSPF Type1 LSAs should be advertised. Default value: -1 Minimum value: 0

state
Use this option to enable or disable the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add ns ip 10.102.4.123 255.255.255.0

Related Commands

rm ns ip

set ns ip

unset ns ip

enable ns ip

disable ns ip

show ns ip

rm ns ip

Synopsis

```
rm ns ip <IPAddress>@
```

Description

Remove an IP entity.

Arguments

IPAddress

The IP address of the entity.

Example

rm ns ip 10.102.4.123

Related Commands

add ns ip
set ns ip
unset ns ip
enable ns ip
disable ns ip
show ns ip

set ns ip

Synopsis

```
set ns ip <IPAddress>@ [-netmask <netmask>] [-arp (
ENABLED | DISABLED )] [-icmp ( ENABLED | DISABLED )] [-
vServer ( ENABLED | DISABLED )] [-telnet ( ENABLED |
DISABLED )] [-ftp ( ENABLED | DISABLED )] [-gui <gui>]
[-ssh ( ENABLED | DISABLED )] [-snmp ( ENABLED |
DISABLED )] [-mgmtAccess ( ENABLED | DISABLED )] [-
dynamicRouting ( ENABLED | DISABLED )] [-hostRoute (
ENABLED | DISABLED )  [-hostRtGw <ip_addr>]  [-metric
<integer>]  [-vserverRHILevel <vserverRHILevel>]  [-
ospfLSAType ( TYPE1 | TYPE5 )  [-ospfArea
<positive_integer>]]]
```

Description

Set the attributes of an IP entity.

Arguments

IPAddress

The IP address of the entity.

netmask

The netmask of the IP.

arp

The state of ARP and gratuitous ARP for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

The state of ICMP responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer

The state of vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet
The state of telnet access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp
The state of ftp access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

gui
The state of GUI access to this IP entity. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh
The state of SSH access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp
The state of SNMP access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess
The state of management access to this IP entity. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting
Use this option to enable or disable dynamic routing on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

ospf
The state of OSPF on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

bgp
The state of BGP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

rip
The state of RIP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute
The state of advertisement of a hostroute to this IP entity. Possible values: ENABLED, DISABLED

Example

set ns ip 10.102.4.123 -arp ENABLED

Related Commands

add ns ip
rm ns ip
unset ns ip
enable ns ip
disable ns ip
show ns ip

unset ns ip

Synopsis

```
unset ns ip <IPAddress>@ [-netmask] [-arp] [-icmp] [-
vServer] [-telnet] [-ftp] [-gui] [-ssh] [-snmp] [-
mgmtAccess] [-dynamicRouting] [-hostRoute] [-hostRtGw]
[-metric] [-vserverRHILevel] [-ospfLSAType] [-
ospfArea]
```

Description

Use this command to remove ns ip settings.Refer to the set ns ip command for meanings of the arguments.

Related Commands

add ns ip

rm ns ip

set ns ip

enable ns ip

disable ns ip

show ns ip

enable ns ip

Synopsis

```
enable ns ip <IPAddress>@
```

Description

Enable an IP entity.

Arguments

IPAddress

The IP address of the entity.

Example

enable ns ip 10.10.10.10

Related Commands

add ns ip
rm ns ip
set ns ip
unset ns ip
disable ns ip
show ns ip

disable ns ip

Synopsis

```
disable ns ip <IPAddress>@
```

Description

Disable an IP entity.

Arguments

IPAddress

The IP address of the entity.

Example

disable ns ip 10.10.10.10

Related Commands

add ns ip
rm ns ip
set ns ip
unset ns ip
enable ns ip
show ns ip

show ns ip

Synopsis

```
show ns ip [<IPAddress>] [-type <type>]
```

Description

Display all the IP addresses such as VIP,MIP,NSIP, and SNIP.

Arguments

IPAddress
The IP address of the entity.

type
The type of this IP. Possible values: SNIP, VIP, MIP, NSIP, GSLBsiteIP

format

level

Output

netmask
The netmask of this IP.

flags
The flags for this entry.

arp
Whether arp is enabled or disabled.

icmp
Whether icmp is enabled or disabled.

vServer
Whether vserver is enabled or disabled.

telnet
Whether telnet is enabled or disabled.

ssh
Whether ssh is enabled or disabled.

gui
Whether gui is (enabled|SecureOnly|disabled).

snmp
Whether snmp is enabled or disabled.

ftp
Whether ftp is enabled or disabled.

mgmtAccess
Whether management access is enabled or disabled.

dynamicRouting
Whether dynamic routing is enabled or disabled.

bgp
Whether bgp is enabled or disabled.NOTE: This attribute is deprecated.

ospf
Whether ospf is enabled or disabled.NOTE: This attribute is deprecated.

rip
Whether rip is enabled or disabled.NOTE: This attribute is deprecated.

hostRoute
Whether host route is enabled or disabled.

hostRtGw
Gateway used for advertising host route.

metric
The metric value added or subtracted from the cost of the hostroute.

ospfArea
The area ID of the area in which OSPF Type1 LSAs are advertised.

vserverRHILevel
The rhi level for this IP.

VIPrtadv2BSD
Whether this route is advertised to FreeBSD

VIPvserCount
Number of vservers bound to this VIP

VIPvserDownCount
Number of vservers bound to this VIP, which are down

ospfLSAType
The ospf lsa type to use while advertising this IP.

state
Whether this ip is enabled or disabled.

freePorts
Number of free Ports available on this IP

Example

show ns ip Ipaddress Type ModeArp IcmpVserver State --------- ---- ------- ---------- ----- 1)10.102.4.123 NetScaler IP ActiveEnabled Enabled NA Enabled 2)10.102.4.237 MIPPassive Enabled Enabled NAEnabled 3)10.102.1.131 VIPPassive Enabled Enabled Enabled Enabled

Related Commands

add ns ip

rm ns ip

set ns ip

unset ns ip

enable ns ip

disable ns ip

enable ns mode

Synopsis

```
enable ns mode <Mode> ...
```

Description

Enable a specified mode.

Arguments

Mode

The name of the mode to be enabled.

Output

reqFeature

Required feature.

Example

This CLI command enables the system's client keep-alive feature: enable ns mode CKA

Related Commands

disable ns mode

show ns mode

disable ns mode

Synopsis

```
disable ns mode <Mode> ...
```

Description

Disable the specified feature or features.

Arguments

Mode

The feature to be disabled.

Output

reqFeature

Required feature.

Example

This example shows the command to disable the system's client keep-alive feature: disable ns mode CKA

Related Commands

enable ns mode

show ns mode

show ns mode

Synopsis

```
show ns mode
```

Description

Display the state of Fast Ramp, Layer 2, USIP, client keep-alive, TCP buffering, and MAC-based forwarding features.

Arguments

Output

FR
Fast Ramp.

L2
Layer 2 mode.

USIP
Use Source IP.

CKA
Client Keep-alive.

TCPB
TCP Buffering.

MBF
MAC-based forwarding.

Edge
Edge configuration.

USNIP
Use Subnet IP.

L3
Layer 3 mode (ip forwarding).

PMTUD
Path MTU Discovery.

SRADV
Static Route Advertisement.

DRADV
Direct Route Advertisement.

IRADV
Intranet Route Advertisement.

SRADV6
Ipv6 Static Route Advertisement.

DRADV6
Ipv6 Direct Route Advertisement.

BridgeBPDUs
BPDU Bridging Mode.

Related Commands

enable ns mode
disable ns mode

set ns dhcpParams

Synopsis

```
set ns dhcpParams -dhcpClient ( ON | OFF )
```

Description

Set the dhcp-client parameters.

Arguments

dhcpClient

Setting this argument to ON makes the netscaler to enable dhcp-client for acquiring IP from the DHCP server in the next boot. Setting it to OFF disables the dhcp-client in the next boot. Possible values: ON, OFF Default value: OFF

Related Commands

unset ns dhcpParams

show ns dhcpParams

unset ns dhcpParams

Synopsis

```
unset ns dhcpParams -dhcpClient
```

Description

Use this command to remove ns dhcpParams settings.Refer to the set ns dhcpParams command for meanings of the arguments.

Related Commands

set ns dhcpParams

show ns dhcpParams

show ns dhcpParams

Synopsis

```
show ns dhcpParams
```

Description

Show dhcp-client parameters.

Arguments

format

level

Output

dhcpClient
ON, if DHCP client active on next reboot, else OFF

IPAddress
DHCP acquired IP

netmask
DHCP acquired Netmask

hostRtGw
DHCP acquired Gateway

Related Commands

set ns dhcpParams

unset ns dhcpParams

release ns dhcpIp

Synopsis

```
release ns dhcpIp
```

Description

Release IP acquired by DHCP client

Related Commands

set ns spParams

Synopsis

```
set ns spParams [-baseThreshold <integer>] [-throttle
<throttle>]
```

Description

Set the base threshold and/or the throttle rate for surge protection.

Arguments

baseThreshold

The base threshold. This is the maximum number of server connections that can be opened before surge protection is activated. Minimum value: 0 Maximum value: 0x7FFF

throttle

The throttle rate, which is the rate at which the system opens connections to the server. The different names of throttle are the keywords: relaxed, normal, and aggressive. Possible values: Aggressive, Normal, Relaxed

Example

set ns spparams -baseThreshold 1000 -throttle aggressive set ns spparams -throttle relaxed

Related Commands

unset ns spParams

show ns spParams

unset ns spParams

Synopsis

```
unset ns spParams [-baseThreshold] [-throttle]
```

Description

Use this command to remove ns spParams settings.Refer to the set ns spParams command for meanings of the arguments.

Related Commands

set ns spParams

show ns spParams

show ns spParams

Synopsis

```
show ns spParams
```

Description

Display the surge protection configuration on the system. This includes the base threshold value and throttle value. These values are set using the setnsparams command.

Arguments

format

level

Output

baseThreshold

The base threshold. This is the maximum number of server connections that can be open before surge protection is activated.

throttle

The throttle rate, which is the rate at which the system opens connections to the server. The different names of throttle are the keywords: relaxed, normal, and aggressive.

Table

Table.

Example

> show ns spparams Surge Protection parameters: BaseThreshold:200 Throttle: Normal Done

Related Commands

set ns spParams

unset ns spParams

set ns tcpbufParam

Synopsis

```
set ns tcpbufParam [-size <KBytes>] [-memLimit
<MBytes>]
```

Description

Display the current TCP buffer size. The command also displays the percentage of the system memory that is used for buffering.

Arguments

size

The size (in KBytes) of the TCP buffer per connection. Default value: 64 Minimum value: 4 Maximum value: 20480

memLimit

The maximum memory that can be used for buffering, in megabytes. Default value: 64 Minimum value: 0

Related Commands

unset ns tcpbufParam

show ns tcpbufParam

unset ns tcpbufParam

Synopsis

```
unset ns tcpbufParam [-size] [-memLimit]
```

Description

Use this command to remove ns tcpbufParam settings.Refer to the set ns tcpbufParam command for meanings of the arguments.

Related Commands

set ns tcpbufParam

show ns tcpbufParam

show ns tcpbufParam

Synopsis

```
show ns tcpbufParam
```

Description

Display the current TCP buffer size. The command also displays the percentage of the system memory that is used for buffering.

Arguments

format

level

Output

size

The size (in KBytes) of the TCP buffer per connection.

memLimit

The maximum memory that can be used for buffering, in megabytes.

Example

An example of this command's output is as follows: TCP buffer size: 64KBytes TCP buffer percentage: 50%

Related Commands

set ns tcpbufParam

unset ns tcpbufParam

set ns tcpParam

Synopsis

```
set ns tcpParam [-WS ( ENABLED | DISABLED )] [-WSVal
<positive_integer>] [-SACK ( ENABLED | DISABLED )] [-
maxBurst <positive_integer>] [-initialCwnd
<positive_integer>] [-recvBuffSize <positive_integer>]
[-delayedAck <positive_integer>] [-downStateRST (
ENABLED | DISABLED )] [-nagle ( ENABLED | DISABLED )]
[-limitedPersist ( ENABLED | DISABLED )] [-oooQSize
<positive_integer>]
```

Description

Set the TCP settings on the NetScaler

Arguments

WS

The state of WS Possible values: ENABLED, DISABLED Default value: DISABLED

WSVal

Window Scaling Factor used Default value: 4 Minimum value: 0 Maximum value: 8

SACK

The state of SACK Possible values: ENABLED, DISABLED Default value: DISABLED

maxBurst

Max-Burst Factor used Default value: 6 Minimum value: 2 Maximum value: 10

initialCwnd

Intial value of TCP cwnd used Default value: 4 Minimum value: 2 Maximum value: 6

recvBuffSize
TCP Receive buffer size Default value: 8190 Minimum value: 8190 Maximum value: 20971520

delayedAck
Delayed acknowledgement timeout (in millisec) Default value: 200 Minimum value: 10 Maximum value: 300

downStateRST
Flag to switch on RST on down services Possible values: ENABLED, DISABLED Default value: DISABLED

nagle
Whether to enable Nagle's algorithm on connections Possible values: ENABLED, DISABLED Default value: DISABLED

limitedPersist
Whether to limit the number of persist(zero window) probes Possible values: ENABLED, DISABLED Default value: ENABLED

oooQSize
Maximum size of out-of-order packet queue (0 means infinite) Default value: 64 Minimum value: 0 Maximum value: 512

Related Commands

unset ns tcpParam

show ns tcpParam

unset ns tcpParam

Synopsis

```
unset ns tcpParam [-WS] [-WSVal] [-SACK] [-maxBurst] [-
initialCwnd] [-recvBuffSize] [-delayedAck] [-
downStateRST] [-nagle] [-limitedPersist] [-oooQSize]
```

Description

Use this command to remove ns tcpParam settings.Refer to the set ns tcpParam command for meanings of the arguments.

Related Commands

set ns tcpParam

show ns tcpParam

show ns tcpParam

Synopsis

```
show ns tcpParam
```

Description

Display the TCP settings on the NetScaler

Arguments

format

level

Output

WS
The state of WS

WSVal
Window Scaling Factor used

SACK
The state of SACK

maxBurst
Max-Burst Factor used

initialCwnd
Intial value of TCP cwnd used

recvBuffSize
TCP Receive buffer size

downStateRST
Flag to switch on RST on down services

Related Commands

set ns tcpParam

unset ns tcpParam

set ns httpParam

Synopsis

```
set ns httpParam [-dropInvalReqs ( ON | OFF )] [-
markHttp09Inval ( ON | OFF )] [-markConnReqInval ( ON |
OFF )] [-insNsSrvrHdr ( ON | OFF )  [<nsSrvrHdr>]] [-
logErrResp ( ON | OFF )]
```

Description

Set configurable HTTP parameters on the NetScaler

Arguments

dropInvalReqs

Whether to drop invalid HTTP requests Possible values: ON, OFF Default value: OFF

markHttp09Inval

Whether to mark HTTP/0.9 requests as invalid Possible values: ON, OFF Default value: OFF

markConnReqInval

Whether to mark CONNECT requests as invalid Possible values: ON, OFF Default value: OFF

insNsSrvrHdr

Enable/disable NetScaler server header insertion for NetScaler generated HTTP responses. Possible values: ON, OFF Default value: OFF

logErrResp

Whether to log HTTP error responses generated by NetScaler Possible values: ON, OFF Default value: ON

Example

set ns httpParam -dropInvalReqs ON

Related Commands

unset ns httpParam

show ns httpParam

unset ns httpParam

Synopsis

```
unset ns httpParam [-dropInvalReqs] [-markHttp09Inval]
[-markConnReqInval] [-insNsSrvrHdr] [-nsSrvrHdr] [-
logErrResp]
```

Description

Use this command to remove ns httpParam settings.Refer to the set ns httpParam command for meanings of the arguments.

Related Commands

set ns httpParam

show ns httpParam

show ns httpParam

Synopsis

```
show ns httpParam
```

Description

Display configured HTTP parameters on the NetScaler

Arguments

format

level

Output

dropInvalReqs
Whether to drop invalid HTTP requests

markHttp09Inval
Whether to mark HTTP/0.9 requests as invalid

markConnReqInval
Whether to mark CONNECT requests as invalid

insNsSrvrHdr
Enable/disable NetScaler server header insertion for NetScaler generated HTTP responses.

nsSrvrHdr
The server header value to be inserted.

logErrResp
Whether to log HTTP error responses

Related Commands

set ns httpParam

unset ns httpParam

set ns weblogparam

Synopsis

```
set ns weblogparam -bufferSizeMB <positive_integer>
```

Description

Set the current web log buffer size.

Arguments

bufferSizeMB

The buffer size (in MB) allocated for log transaction data on the system.
Minimum value: 1 Maximum value: 0xFFFFFFFE

Related Commands

show ns weblogparam

show ns weblogparam

Synopsis

```
show ns weblogparam
```

Description

Display the current size of the buffer, which is used to store log transactions.

Arguments

format

level

Output

bufferSizeMB
Buffer size in MB.

Related Commands

set ns weblogparam

set ns rateControl

Synopsis

```
set ns rateControl [-tcpThreshold <positive_integer>]
[-udpThreshold <positive_integer>] [-icmpThreshold
<positive_integer>]
```

Description

Configure udp/tcp/icmp packet rate controls for any application that is not configured at System(ie., direct access to the backend through System). This rate limit should be specified in the number of packets to allow per 10ms.

Arguments

tcpThreshold

The number of SYNs permitted per 10 milli second.

udpThreshold

The number of UDP packets permitted per 10 milli second.

icmpThreshold

The number of ICMP packets permitted per 10 milli second. Default value: 100

Example

The following command will set the SYN rate to 100, icmp rate to 10 and the udp rate to unlimited. set ns ratecontrol -tcpThreshold 100 -udpThreshold 0 -icmpThreshold 10 The 'show ns rate control' command can be used to view the current settings of the rate controls. > show ns ratecontrol UDP threshold: 0 per 10 ms TCP threshold:0 per 10 ms ICMP threshold: 100 per 10 ms Done

Related Commands

unset ns rateControl

show ns rateControl

unset ns rateControl

Synopsis

```
unset ns rateControl [-tcpThreshold] [-udpThreshold] [-
icmpThreshold]
```

Description

Use this command to remove ns rateControl settings.Refer to the set ns rateControl command for meanings of the arguments.

Related Commands

set ns rateControl

show ns rateControl

show ns rateControl

Synopsis

```
show ns rateControl
```

Description

Check the current rate control values.

Arguments

format

level

Output

tcpThreshold

The number of SYNs permitted per 10 milli second.

udpThreshold

The number of UDP packets permitted per 10 milli second.

icmpThreshold

The number of ICMP packets permitted per 10 milli second.

Example

By default, there is no rate control for TCP/UDP and for ICMP it will be 100. The output of the "show ns ratecontrol" command, with default setting, > show ns ratecontrol UDP threshold:0 per 10 ms TCP threshold:0 per 10 ms ICMP threshold: 100 per 10 ms Done

Related Commands

set ns rateControl

unset ns rateControl

set ns rpcNode

Synopsis

```
set ns rpcNode <IPAddress> {-password } [-srcIP
<ip_addr|*>] [-secure ( YES | NO )]
```

Description

Set the authentication attributes associated with peer System node. All System nodes use remote procedure calls to communicate.

Arguments

IPAddress

The IP address of the node. This has to be in same subnet as NSIP.

password

The password to be used in authentication with the peer System node.

srcIP

The src ip to be used in communiction with the peer System node. Default value: 0xFFFFFFFF

secure

The state of the channel when talking to the node. Channel can be secure or insecure. Possible values: YES, NO

Example

Example-1: Failover configuration In a failover configuration define peer NS as: add node 1 10.101.4.87 Set peer ha-unit's password as: set ns rpcnode 10.101.4.87 -password testpass -secure yes System will now use the configured password to authenticate with its failover unit. Example-2: GSLB configuration In a GSLB configuration define peer NS GSLB site as: add gslb site us_east_coast remote 206.123.3.4 Set peer GSLB-NS's password as: set ns rpcnode 206.123.3.4 -password testrun System will now use the configured password to authenticate with east-coast GSLB site.

Related Commands

unset ns rpcNode

show ns rpcNode

unset ns rpcNode

Synopsis

```
unset ns rpcNode [-password] [-srcIP] [-secure]
```

Description

Use this command to remove ns rpcNode settings.Refer to the set ns rpcNode command for meanings of the arguments.

Related Commands

set ns rpcNode

show ns rpcNode

show ns rpcNode

Synopsis

show ns rpcNode

Description

Display a list of nodes currently communicating using RPC. All nodes use remote procedure calls to communicate.

Arguments

summary

fullValues

format

level

Output

IPAddress
The IP address of the node. This has to be in same subnet as NSIP.

password
Password.

retry
The reference count.

srcIP
The src ip used in communiction with the peer System node.

Example

Following example shows list of nodes communicating using RPC: > sh rpcnode 1)IPAddress:10.101.4.84 Password: ..8a7b474124957776b56cf03b28 Srcip: 1.1.1.1 2)IPAddress:10.101.4.87 Password: ..ca2a035465d22c Srcip: 2.2.2.2 Done

Related Commands

set ns rpcNode

unset ns rpcNode

set ns idletimeout

Synopsis

Description

Set the pcb/natpcb idletimeout. NOTE: This command is deprecated.

Arguments

`tcpsvr`
Set the idletimeout for server side pcb.

`tcpclt`
Set the idletimeout for client side pcb.

`nontcpsvrclt`
Set the idletimeout for natpcb. Default value: 120 Minimum value: 1

Example

set ns idletimeout -tcpsvr 120 set ns idletimeout -tcpclt 120 set ns idletimeout -nontcpsvrclt 120

Related Commands

unset ns idletimeout

show ns idletimeout

unset ns idletimeout

Synopsis

Description

Use this command to remove ns idletimeout settings.Refer to the set ns idletimeout command for meanings of the arguments.NOTE: This command is deprecated.

Related Commands

set ns idletimeout

show ns idletimeout

show ns idletimeout

Synopsis

Description

Display the global setting of pcb/natpcb idletimeout. NOTE: This command is deprecated.This command is deprecated in favour of 'set ns timeout'

Arguments

format

level

Output

tcpsvr
Set the idletimeout for server side pcb.

tcpclt
Set the idletimeout for client side pcb.

nontcpsvrclt
Set the idletimeout for natpcb.

Related Commands

set ns idletimeout

unset ns idletimeout

set ns timeout

Synopsis

```
set ns timeout [-zombie <positive_integer>] [-
httpClient <positive_integer>] [-httpServer
<positive_integer>] [-tcpClient <positive_integer>] [-
tcpServer <positive_integer>] [-anyClient
<positive_integer>] [-anyServer <positive_integer>] [-
halfclose <positive_integer>] [-nontcpZombie
<positive_integer>]
```

Description

Set various timeout values for NetScaler device. Caution: Modifying these values may affect system performance.

Arguments

zombie

Inactive TCP connection timeout (in seconds) Default value: 120 Minimum value: 1 Maximum value: 600

client

Client idle timeout (in seconds). If zero, the service-type default value is taken when service is created. Minimum value: 0 Maximum value: 18000

server

Server idle timeout (in seconds). If zero, the service-type default is taken when service is created. Minimum value: 0 Maximum value: 18000

httpClient

HTTP client idle timeout (in seconds) Minimum value: 0 Maximum value: 18000

httpServer

HTTP server idle timeout (in seconds) Minimum value: 0 Maximum value: 18000

tcpClient
TCP client idle timeout (in seconds) Minimum value: 0 Maximum value: 18000

tcpServer
TCP server idle timeout (in seconds) Minimum value: 0 Maximum value: 18000

anyClient
ANY client idle timeout (in seconds) Minimum value: 0 Maximum value: 18000

anyServer
ANY server idle timeout (in seconds) Minimum value: 0 Maximum value: 18000

halfclose
Half-closed connection timeout (in seconds) Default value: 10 Minimum value: 1 Maximum value: 600

nontcpZombie
Inactive non-TCP connection timeout (in seconds) Default value: 60 Minimum value: 1 Maximum value: 600

Example

set ns timeout -zombie 200

Related Commands

unset ns timeout

show ns timeout

unset ns timeout

Synopsis

```
unset ns timeout [-zombie] [-httpClient] [-httpServer]
[-tcpClient] [-tcpServer] [-anyClient] [-anyServer] [-
halfclose] [-nontcpZombie]
```

Description

Use this command to remove ns timeout settings.Refer to the set ns timeout command for meanings of the arguments.

Related Commands

set ns timeout

show ns timeout

show ns timeout

Synopsis

```
show ns timeout
```

Description

Display various timeout values for NetScaler device. The timeouts having default values are not displayed.

Arguments

format

level

Output

zombie
Inactive TCP connection timer (in seconds)

httpClient
HTTP client idle timeout (in seconds)

httpServer
HTTP server idle timeout (in seconds)

tcpClient
TCP client idle timeout (in seconds)

tcpServer
TCP server idle timeout (in seconds)

anyClient
ANY client idle timeout (in seconds)

anyServer
ANY server timeout (in seconds)

halfclose
Half-closed connection timeout (in seconds)

nontcpZombie
Inactive non-TCP connection timeout (in seconds)

Example

show ns timeout

Related Commands

set ns timeout
unset ns timeout

add ns simpleacl

Synopsis

```
add ns simpleacl <aclname> <aclaction> -srcIP <ip_addr>
[-destPort <port>  -protocol ( TCP | UDP )] [-TTL
<positive_integer>]
```

Description

Add a SimpleACL rule to the system configuration, every inbound packet is matched against configured SimpleACL rules and specified action is applied.

Arguments

aclname

Alphanumeric name of the ACL rule.

aclaction

Action associated with the ACL rule. Possible values: DENY

srcIP

Source ip for the ACL rule.

destPort

Destination port for the ACL rule.

TTL

Time to expire this ACL rule(in seconds). Timer granularity is 4 seconds. Minimum value: 4 Maximum value: 0x7FFFFFFF

Example

add simpleacl rule1 DENY -srcIP 1.1.1.1 -port 80 -protocol TCP add simpleacl rule2 DENY -srcIP 2.2.2.2 -TTL 600

Related Commands

add ns acl

rm ns acl

clear ns simpleacl

rm ns simpleacl

show ns simpleacl

stat ns simpleacl

rm ns simpleacl

Synopsis

```
rm ns simpleacl <aclname> ...
```

Description

Remove a SimpleACL rule.

Arguments

aclname

Name of the ACL rule to be deleted.

Example

rm ns simpleacl rule1

Related Commands

add ns simpleacl

rm ns acl

clear ns simpleacl

show ns simpleacl

stat ns simpleacl

show ns simpleacl

Synopsis

```
show ns simpleacl [<aclname>]
```

Description

Display all the SimpleACL rules. If a rule name is specified, then only that SimpleACL rule is shown.

Arguments

aclname
Name of the ACL rule.

summary

fullValues

format

level

Output

aclaction
Action associated with the ACL rule.

srcIP
Source IP address.

state
SACL state flag.

destPort
Destination Port.

TTL
Time to expire this ACL rule(in seconds).

hits
Number of hits for this ACL rule.

Example

show simpleacl rule1 Name: rule1 Action: DENY srcIP = 10.102.1.150 Protocol = TCP DestPort = 110 Hits: 5 TTL: 200(seconds)

Related Commands

clear ns simpleacl

add ns simpleacl

rm ns simpleacl

stat ns simpleacl

stat ns simpleacl

Synopsis

```
stat ns simpleacl [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display SimpleACL statistics.

Arguments

Output

Counters

Allow SimpleACL hits (SACLAllow)
Total packets that matched a SimpleACL with action ALLOW and got consumed by NetScaler.

Bridge SimpleACL hits (SACLBdg)
Total packets that matched a SimpleACL with action BRIDGE and got bridged by NetScaler.

Deny SimpleACL hits (SACLDeny)
Packets dropped because they match deny simple ACL.

SimpleACL hits (SACLHits)
Packets matching a simple ACL.

SimpleACL misses (SACLMiss)
Packets not matching any simple ACL.

SimpleACLs count (SACLsCount)
Number of simple ACLs configured.

Example

stat simpleacl

Related Commands

clear ns simpleacl

add ns simpleacl
rm ns simpleacl
show ns simpleacl
stat ns
stat ns acl
stat ns acl6

show ns hardware

Synopsis

```
show ns hardware
```

Description

Displays hardware and product related information like SystemId, HostId, SerialId.

Arguments

Output

hwdescription
Hardware and it's ports detail.

sysId
System id.

manufactureDay
Manufacturing day.

manufactureMonth
Manufacturing month.

manufactureYear
Manufacturing year.

cpufrequncy
CPU Frequency.

hostId
host id.

serialNo
Serial no.

encodedSerialNo
Encoded serial no.

Related Commands

diff ns config

Synopsis

```
diff ns config [<config1>] [<config2>] [-outtype ( cli
| xml )] [-template]
```

Description

Difference between two configuration

Arguments

config1

Config options.

config2

Config options.

outtype

The format in which result is desired. Possible values: cli, xml

template

Enable template diff.This will only compare commands given in template file.

Example

diff ns config runningconfig savedConfig

Related Commands

clear ns config

set ns config

unset ns config

save ns config

show ns config

show ns events

Synopsis

```
show ns events [<eventNo>]
```

Description

display the events

Arguments

eventNo
Last retrieved event no. This command will return all events after that.

summary

fullValues

Output

time
Event no.

eventcode
event Code.

devid
Device Name.

devname
Device Name.

text
Event no.

data0
additional event information.

data1
additional event information.

data2
additional event information.

`data3`
additional event information.

Example

show ns events

Related Commands

CHAPTER 20

Policy Commands

This chapter covers the policy commands.

add policy expression

Synopsis

```
add policy expression <name> <value> [-description
<string>] [-clientSecurityMessage <string>]
```

Description

Create an expression.

Arguments

`name`

The name of the expression that will be created.

`value`

The expression string.

`description`

Description for the expression.

`clientSecurityMessage`

The client security message that will be displayed on failure of this expression.Only relevant for end point check expressions.

Related Commands

rm policy expression

set policy expression

unset policy expression

show policy expression

rm policy expression

Synopsis

```
rm policy expression <name> ...
```

Description

Remove a previously defined expression. If the expression is part of a policy or filter, you must remove the policy or filter before removing the expression.

Arguments

name

The name of the expression.

Related Commands

add policy expression

set policy expression

unset policy expression

show policy expression

set policy expression

Synopsis

```
set policy expression <name> [<value>] [-description
<string>] [-clientSecurityMessage <string>]
```

Description

This command modifies an existing expression.

Arguments

`name`
The name of the expression.

`value`
The expression string.

`description`
Description for the expression.

`clientSecurityMessage`
The client security message that will be displayed on failure of this expression. Only relevant for end point check expressions. Default value:

Related Commands

add policy expression
rm policy expression
unset policy expression
show policy expression

unset policy expression

Synopsis

```
unset policy expression <name> [-description] [-
clientSecurityMessage]
```

Description

Use this command to remove policy expression settings.Refer to the set policy expression command for meanings of the arguments.

Related Commands

add policy expression

rm policy expression

set policy expression

show policy expression

show policy expression

Synopsis

```
show policy expression [<name> | -type ( CLASSIC |
ADVANCED )]
```

Description

Display the expressions defined in the system.

Arguments

name

The name of the expression. if no name is given then all expressions will be displayed.

type

The type of expression. This is for input only. Possible values: CLASSIC, ADVANCED

summary

fullValues

format

level

Output

value

The expression string.

hits

The total number of hits.

piHits

The total number of hits.

type

The type of expression. This is for output only.

clientSecurityMessage
The client security message that will be displayed on failure of the client security check.

description
Description for the expression.

state

Related Commands

add policy expression
rm policy expression
set policy expression
unset policy expression

add policy map

Synopsis

```
add policy map <mapPolicyName> -sd <string> [-su
<string>] [-td <string>] [-tu <string>]
```

Description

Create a policy to map publicly-known domain name to a target domain name for a reverse proxy virtual server used in the cache redirection feature. Optionally, a source and target URL can also be specified. The map policy created can be associated with a reverse proxy cache redirection virtual server using the ###bind cr vserver### command. There can be only one default map policy for a domain.

Arguments

mapPolicyName

The name of the map policy to be created.

sd

The source domain name which is publicly known. This is the domain name with which a client request arrives to a reverse proxy virtual server for cache redirection on the system.

su

The source URL. The format to specify the argument is: / [[prefix] [*]] [.suffix]

td

The domain name sent to the server. It replaces the source domain name.

tu

The target URL.The format to specify the argument is: / [[prefix] [*]] [.suffix]

Example

Example 1 The following example creates a default map policy (map1) for the source domain www.a.com. Any client requests with this source domain in the host header is changed to www.real_a.com. add policy map map2 -sd www.a.com -td www.real.a.com Example 2 This example shows how to

create a URL map policy (map2) if you want to translate /sports.html in the incoming request to /news.html in addition to mapping the source domain www.a.com to www.real_a.com in the outgoing request. add policy map map2 -sd www.a.com -td www.real_a.com -su /sports.html -tu /news.html These type of map policies, called "URL map policies," have the following restrictions: lURL map policies belonging to www.a.com cannot be added without first adding a default map policy as described in Example 1. lIf a source suffix has been specified for URL map policy, a destination suffix must also be specified. lIf an exact URL has been specified as the source, then the target URL should also be exact URL. lIf there is a source prefix in the URL, there must be also a destination prefix in the URL.

Related Commands

rm policy map

show policy map

rm policy map

Synopsis

```
rm policy map <mapPolicyName>
```

Description

Remove the map policies. Note:Before removing the map policy, you must first unbind the map policy from the reverse proxy virtual server.

Arguments

mapPolicyName

The name of the map policy.

Related Commands

add policy map

show policy map

show policy map

Synopsis

```
show policy map [<mapPolicyName>]
```

Description

Display the map policies that have been configured and the related map policy information.

Arguments

mapPolicyName
The name of the map policy to be displayed.

summary

fullValues

format

level

Output

sd
The source domain name which is publicly known. This is the domain name with which a client request arrives to a reverse proxy virtual server for cache redirection on the system.

su
The source URL.

td
The domain name sent to the server.

tu
The target URL.

targetName
The expression string.

Related Commands

add policy map

rm policy map

add policy patClass

Synopsis

Description

Add a patclass. Each patclass is identified by a name. More patterns(strings) can be associated with it later. NOTE: This command is deprecated.This command is deprecated in favor of 'add policy patset'

Arguments

`name`

The name of the patclass. The name must not exceed 31 characters.

`string`

The string associated with the patclass.

Example

add policy patclass pat1 foo

Related Commands

rm policy patClass

bind policy patClass

unbind policy patClass

show policy patClass

rm policy patClass

Synopsis

Description

Remove the patclass created by the add patclass command. Once the patclass is removed, all the expressions referring it would have undefined value.
NOTE: This command is deprecated.This command is deprecated in favor of 'rm policy patset'

Arguments

name
The name of the patclass.

Example

rm policy patclass pat1

Related Commands

add policy patClass
bind policy patClass
unbind policy patClass
show policy patClass

bind policy patClass

Synopsis

Description

Bind string(s) to a patclass. NOTE: This command is deprecated.This command is deprecated in favor of 'bind policy patset'

Arguments

`name`
The name of the patclass.

`string`
The string associated with the patclass.

Example

bind policy patclass pat1 bar xyz

Related Commands

add policy patClass
rm policy patClass
unbind policy patClass
show policy patClass

unbind policy patClass

Synopsis

Description

Unbind string(s) from a patclass. NOTE: This command is deprecated.This command is deprecated in favor of 'unbind policy patset'

Arguments

`name`

The name of the patclass.

`string`

The string associated with the patclass.

Example

unbind policy patclass pat1 bar xyz

Related Commands

add policy patClass

rm policy patClass

bind policy patClass

show policy patClass

show policy patClass

Synopsis

Description

Display the configured patclass(s). NOTE: This command is deprecated.This command is deprecated in favor of 'show policy patset'

Arguments

`name`
The name of the patclass.

`summary`

`fullValues`

`format`

`level`

Output

`state`

`string`
The string associated with the patclass.

`index`
The index of the string associated with the patclass.

`description`
Description of the patclass

`isDefault`

Example

show policy patclass pat1

Related Commands

add policy patClass
rm policy patClass
bind policy patClass
unbind policy patClass

add policy patset

Synopsis

```
add policy patset <name>
```

Description

Add a patset. Each patset is identified by a name.

Arguments

name

The name of the patset. The name must not exceed 31 characters.

Example

add policy patset pat1

Related Commands

rm policy patset

bind policy patset

unbind policy patset

show policy patset

rm policy patset

Synopsis

```
rm policy patset <name>
```

Description

Remove the patset created by the add patset command. Once the patset is removed, all the expressions referring it would have undefined value.

Arguments

name

The name of the patset.

Example

rm policy patset pat1

Related Commands

add policy patset

bind policy patset

unbind policy patset

show policy patset

bind policy patset

Synopsis

```
bind policy patset <name> <string> [-index
<positive_integer>]
```

Description

Bind string to a patset. If first patern(string) is bound using index label then next bind statements to that patset should provide index, and vice versa

Arguments

`name`
The name of the patset.

`string`
The string associated with the patset.

Example

bind policy patset pat1 bar -index 2

Related Commands

add policy patset
rm policy patset
unbind policy patset
show policy patset

unbind policy patset

Synopsis

```
unbind policy patset <name> <string> ...
```

Description

Unbind string(s) from a patset.

Arguments

`name`

The name of the patset.

`string`

The string associated with the patset.

Example

unbind policy patset pat1 bar xyz

Related Commands

add policy patset

rm policy patset

bind policy patset

show policy patset

show policy patset

Synopsis

```
show policy patset [<name>]
```

Description

Display the configured patset(s).

Arguments

name

The name of the patset.

summary

fullValues

format

level

Output

state

string

The string associated with the patset.

index

The index of the string associated with the patset.

description

Description of the patset

isDefault

Example

show policy patset pat1

Related Commands

add policy patset
rm policy patset
bind policy patset
unbind policy patset

add policy httpCallout

Synopsis

```
add policy httpCallout <name>
```

Description

Add a httpcallout. Each httpcallout is identified by a name.

Arguments

name

The name of the httpcallout. The name must not exceed 31 characters.

Example

add policy httpcallout h1

Related Commands

rm policy httpCallout
set policy httpCallout
unset policy httpCallout
show policy httpCallout

rm policy httpCallout

Synopsis

```
rm policy httpCallout <name>
```

Description

Removes the httpcallout entity

Arguments

name

The name of the httpcallout.

Example

rm policy httpcallout h1

Related Commands

add policy httpCallout

set policy httpCallout

unset policy httpCallout

show policy httpCallout

set policy httpCallout

Synopsis

```
set policy httpCallout <name> [-IPAddress
<ip_addr|ipv6_addr|*>] [-port <port|*>] [-vServer
<string>] [-returnType <returnType>] [-httpMethod ( GET
| POST )] [-hostExpr <string>] [-urlStemExpr <string>]
[-headers <name(value)> ...] [-parameters <name(value)>
...] [-fullReqExpr <string>] [-resultExpr <string>]
```

Description

Sets attributes for an httpcallout policy. You invoke this policy by specifying the SYS.HTTP_CALLOUT expression prefix in an advanced expression.

Arguments

`name`

The name of the httpcallout.

`IPAddress`

IPv4 or IPv6 address of the server to which the callout is sent, or a wildcard. Mutually exclusive with the -vserver argument.

`port`

If you specify an IP address, this is the port on the server to which the callout is sent, or a wildcard.

`vServer`

The name of a load balancing, content switching, or cache redirection virtual server with a service type of HTTP. This is where the callout is sent. This option is mutually exclusive with IP address and port.

`returnType`

Type of data that the target application returns in the response to the callout. Possible values: BOOL, NUM, TEXT

`httpMethod`

Method used in the HTTP request that this callout sends. Mutually exclusive with -fullReqExpr. Possible values: GET, POST

hostExpr
Advanced text expression to configure the Host header. The expression can contain a literal value (10.101.10.11) or a derived value (for example, http.req.header. . .). Mutually exclusive with -fullReqExpr.

urlStemExpr
An advanced string expression for generating the URL stem. The expression can contain a literal string (for example, /mysite/index.html) or an expression that derives the value (for example, http.req.url). Mutually exclusive with -fullReqExpr.

headers
Advanced text expression to insert HTTP headers and their values in the HTTP callout request. You must specify a value for every header. You specify the header name as a string and the header value as an advanced expression. Mutually exclusive with -fullReqExpr.

parameters
Advanced expression to insert query parameters in the HTTP request that the callout sends. You must specify a value for every parameter that you configure. If the callout request uses the GET method, these parameters are inserted in the URL. If the callout request uses the POST method, these parameters are inserted in the POST body. You configure the query parameter name as a string, and the value as an advanced expression. The parameter values are URL encoded. Mutually exclusive with -fullReqExpr.

fullReqExpr
Exact HTTP request that the NetScaler is to send, as an advanced expression of up to 8191 characters. If you specify this parameter, you must omit the httpMethod, hostExpr, urlStemExpr, headers, and parameters arguments. The request expression is constrained by the feature where the callout is used. For example, an HTTP.RES expression cannot be used in a request-time policy bank or in a TCP content switching policy bank. The NetScaler does not check the validity of this request. You must manually validate the request.

resultExpr
Advanced expression that extracts HTTP.RES objects from the response to the HTTP callout. The maximum length is 8191. The operations in this expression must match the return type. For example, if you configure a return type of TEXT, the result expression must be a text-based expression. If the

return type is NUM, the result expression (resultExpr) must return a numeric value, as in the following: http.res.body(10000).length.

Example

set policy httpcallout h1 -vip v1

Related Commands

add policy httpCallout

rm policy httpCallout

unset policy httpCallout

show policy httpCallout

unset policy httpCallout

Synopsis

```
unset policy httpCallout <name> [-IPAddress] [-port] [-
vServer] [-httpMethod] [-hostExpr] [-urlStemExpr] [-
headers] [-parameters] [-fullReqExpr] [-resultExpr]
```

Description

Use this command to remove policy httpCallout settings.Refer to the set policy httpCallout command for meanings of the arguments.

Related Commands

add policy httpCallout

rm policy httpCallout

set policy httpCallout

show policy httpCallout

show policy httpCallout

Synopsis

```
show policy httpCallout [<name>]
```

Description

Display the configured httpcallout(s).

Arguments

name
The name of the httpcallout.

summary

fullValues

format

level

Output

state

IPAddress
Server IP address.

port
Server port.

vServer
Vserver name

returnType
Return type of the http callout

httpMethod
Http callout request type

hostExpr
PI string expression for Host

urlStemExpr
PI string expression for URL stem

headers
PI string expression for request http headers

parameters
PI string expression for request query parameters

fullReqExpr
PI string expression for full http callout request

resultExpr
PI string expression for http callout response

hits
Total hits

undefHits
Total undefs

svrState
The state of the service

undefReason
Reason for last undef

recursiveCallout
Number of recursive callouts

Example

show policy httpcallout h1

Related Commands

add policy httpCallout
rm policy httpCallout
set policy httpCallout
unset policy httpCallout

CHAPTER 21

Priority Queuing Commands

This chapter covers the Priority Queuing commands.

stat pq

Synopsis

```
stat pq [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display Priority Queuing statistics.

Arguments

Output

Counters

Policy hits (PolMatch)

This counter gives the number of times Netscaler matched an incoming request with any PQ policy.

Threshold failed (ThrsFail)

This counter gives the number of times the priority queue threshold criteria was not met.

Priority 1 requests (Pri1Req)

This counter gives the number of priority 1 requests that Netscaler received.

Priority 2 requests (Pri2Req)

This counter gives the number of priority 2 requests that Netscaler received.

Priority 3 requests (Pri3Req)

This counter gives the number of priority 3 requests that Netscaler received.

Related Commands

stat pq policy

show pq binding

Synopsis

```
show pq binding <vServerName>
```

Description

Display binding information for the system's priority queuing feature. This applies to the specified load balancing virtual server (previously bound during priority queuing configuration).

Arguments

vServerName
The load balancing virtual server.

summary

fullValues

Output

state

policyName
The name of the priority queuing policy.

rule
The condition for applying the policy.

priority
The priority of queuing the request.

weight
Weight.

qDepth
Queue Depth.

polqDepth
Policy Queue Depth.

`hits`
Total number of hits.

Related Commands

show pq stats

Synopsis

```
show pq stats - alias for 'stat pq'
```

Description

show pq stats is an alias for stat pq

Related Commands

stat pq

add pq policy

Synopsis

```
add pq policy <policyName> -rule <expression> -priority
<positive_integer> [-weight <positive_integer>] [-
qDepth <positive_integer> | -polqDepth
<positive_integer>]
```

Description

Add a priority queueing policy. Note: In order to activate priority queuing on a virtual server, this policy needs to be bound to the virtual server using the bindlbvserver command. This virtual server must also have priority queuing turned on using the setvserver CLI command

Arguments

`policyName`

The name of the priority queuing policy.

`rule`

The condition for applying the policy. When requests are received by a system, they are classified into different priority levels based on the expression_logic that they match. Specifies the condition for applying the policy. Expression logic is expression names, separated by the logical operators || and &&, and possibly grouped using parenthesis. If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes. The following are valid expression logic: ns_ext_cgi||ns_ext_asp ?ns_non_get && (ns_header_cookie||ns_header_pragma)? When a request comes to the system, it is prioritized based on the expression_list that is matches.

`priority`

The priority of queuing the request. When a request matches the configured rule and if server resources are not available, this option specifies a priority for queuing the request until the server resources are available again. Enter the value of positive_integer as 1, 2 or 3. The highest priority level is 1 and the lowest priority value is 3. Minimum value: 0 Maximum value: 3

weight
The weight for the priorty level. Each priority level is assigned a weight according to which it is served when server resources are available. The weight for a higher priority request must be set higher than that of a lower priority request. The default weights for the priority queues 1, 2, and 3 are 3, 2, and 1 respectively. Specify the weights as 0 through 101. A weight of 0 indicates that the particular priority level should be served only when there are no requests in any of the priority queues. A weight of 101 specifies a weight of infinity. This means that this priority level is served irrespective of the number of clients waiting in other priority queues. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 101

qDepth
The queue depth threshold value. When the number of waiting requests in the queue (or queue size) on the virtual server to which this policy is bound, increases to the specified qdepth value, any subsequent requests are dropped to the lowest priority level. Default value: 0 Minimum value: 0 Maximum value: 0xFFFFFFFE

polqDepth
The policy queue depth threshold value. When the number of waiting requests in all the queue belonging to this policy (or the policy queue size) increases to the specified polqdepth value all subsequent requests are dropped to the lowest priority level. Default value: 0 Minimum value: 0 Maximum value: 0xFFFFFFFE

Related Commands

bind lb vserver
set vserver
rm pq policy
set pq policy
unset pq policy
show pq policy
stat pq policy

rm pq policy

Synopsis

```
rm pq policy <policyName> ...
```

Description

Remove the priority queuing policy that was added using the add pq policy command.

Arguments

policyName

The name of the priority queuing policy to be removed.

Related Commands

add pq policy

set pq policy

unset pq policy

show pq policy

stat pq policy

set pq policy

Synopsis

```
set pq policy <policyName> [-weight <positive_integer>]
[-qDepth <positive_integer> | -polqDepth
<positive_integer>]
```

Description

Modify priority queuing policies that was set using the add pq policy command.

Arguments

policyName

The name of the priority queuing policy that is to be modified.

weight

The Weight of priority queuing policy. Default value: VAL_NOT_SET Minimum value: 0 Maximum value: 101

qDepth

Queue Depth of priority queuing policy. Minimum value: 0 Maximum value: 0xFFFFFFFE

polqDepth

Policy Queue Depth of priority queuing policy. Minimum value: 0 Maximum value: 0xFFFFFFFE

Related Commands

add pq policy

rm pq policy

unset pq policy

show pq policy

stat pq policy

unset pq policy

Synopsis

```
unset pq policy <policyName> [-weight] [-qDepth] [-
polqDepth]
```

Description

Use this command to remove pq policy settings.Refer to the set pq policy command for meanings of the arguments.

Related Commands

add pq policy

rm pq policy

set pq policy

show pq policy

stat pq policy

show pq policy

Synopsis

```
show pq policy [<policyName>]
```

Description

Display all priority queuing policies added using the add pq policy command.

Arguments

policyName
Policy Name

summary

fullValues

format

level

Output

rule
The condition for applying the policy.

priority
The priority of queuing the request.

weight
Weight.

qDepth
Queue Depth.

polqDepth
Policy Queue Depth.

hits
Total number of hits.

Related Commands

add pq policy
rm pq policy
set pq policy
unset pq policy
stat pq policy

stat pq policy

Synopsis

```
stat pq policy [<policyName>] [-detail] [-fullValues]
[-ntimes <positive_integer>] [-logFile
<input_filename>]
```

Description

Display Priority Queuing policy statistics.

Arguments

policyName

The name of the PQ policy for which statistics will be displayed. If not given statistics are shown for all PQ policies.

Output

Counters

Toatal queue wait time (QWaitTim)

This counter gives the amount of time spent by PQ clients in the priority queue.

Toatal queue wait time (QWaitTim)

This counter gives the amount of time spent by PQ clients in the priority queue.

Avg queue wait time (AvWtTime)

This counter gives the average waiting time for this priority queue policy.

Avg clt transaction time (AvgTime)

This counter gives the average time taken by a PQ client to complete its transaction.

Vserver port (VsPort)

Gives the port of the vserver to which this policy is bound.

Vserver IP (VsIP)

Gives the IP address of the vserver to which this policy is bound.

Current queue depth (Qdepth)
Number of waiting clients.

Current server connections (CltCons)
This counter gives the current number of server connections established for this policy.

Server TCP connections (TotCltCon)
This counter gives the total number of server connections established for this policy.

Client requests dropped (Dropped)
Number of dropped transactions.

Client HTTP transactions (CltTrns)
Total number of client transactions.

Queue depth (TotQLen)
This counter gives the total queue depth for this policy.

Vserver port (VsPort)
Gives the port of the vserver to which this policy is bound.

Avg clt transaction time (us) (AvgTime)
This counter gives the average time taken by a PQ client to complete its transaction.

Toatal queue wait time (QWaitTim)
This counter gives the amount of time spent by PQ clients in the priority queue.

Related Commands

add pq policy
rm pq policy
set pq policy
unset pq policy
show pq policy
stat pq

CHAPTER 22

Protocols Commands

This chapter covers the protocols commands.

stat protocol tcp

Synopsis

```
stat protocol tcp [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display TCP protocol statistics

Arguments

Output

Counters

Server active connections (ActSvrCo)
Connections to a server currently responding to requests.

Opening server connections (SvrCxO)
Server connections in the Opening state, which indicates that the handshakes are not yet complete.

Opening client connections (CltCxO)
Client connections in the Opening state, which indicates that the handshakes are not yet complete.

Established client connections (CltCxE)
Current client connections in the Established state, which indicates that data transfer can occur between the NetScaler and the client.

Established server connections (SvrCxE)
Current server connections in the Established state, which indicates that data transfer can occur between the NetScaler and the server.

TCP packets received (TCPPktRx)
TCP packets received.

TCP bytes received (TCPbRx)
Bytes of TCP data received.

TCP packets transmitted (TCPPktTx)
TCP packets transmitted.

TCP bytes transmitted (TCPbTx)
Bytes of TCP data transmitted.

All client connections (CltCx)
Client connections, including connections in the Opening, Established, and Closing state.

Closing client connections (CltCxCl)
Client connections in the Closing state, which indicates that the connection termination process has initiated but is not complete.

Opened client connections (TotCltO)
Client connections initiated on the NetScaler since startup. This counter is reset when the NetScaler is restarted.

All server connections (SvrCx)
Server connections, including connections in the Opening, Established, and Closing state.

Closing server connections (SvrCxCl)
Server connections in the Closing state, which indicates that the connection termination process has initiated but is not complete.

Opened server connections (TotSvrO)
Server connections initiated by the NetScaler since startup. This counter is reset when the NetScaler is restarted.

Surge queue (SQlen)
Connections in the surge queue. When the NetScaler cannot open a connection to the server, for example when maximum connections have been reached, the NetScaler queues these requests.

Spare connections (SpConn)
Spare connections available. To save time and resources in establishing another connection for a new client, the connection on the server is not closed after completing the request from the first client and is available for serving future requests.

Client idle flushed (ZomCltF)
Client connections that are flushed because the client has been idle for some time.

Client half opened flushed (ZCltFHo)
Half-opened client connections that are flushed because the three-way handshakes are not complete.

Client active half closed flushed (ZCltFAhc)
Active half-closed client connections that are flushed because the client has closed the connection and there has been no activity on the connection.

Client passive half closed flushed (ZCltFPhc)
Passive half-closed client connections that are flushed because the NetScaler has closed the connection and there has been no activity on the connection.

Server idle connections flushed (ZSvrF)
Server connections that are flushed because there have been no client requests in the queue for some time.

Server half opened flushed (ZSvrFHo)
Half-opened server connections that are flushed because the three-way handshakes are not complete.

Server active half closed flushed (ZSvrFAhc)
Active half-closed server connections that are flushed because the server has closed the connection and there has been no activity on the connection.

Server passive half closed flushed (ZSrvFPhc)
Passive half-closed server connections that are flushed because the NetScaler has closed the connection and there has been no activity on the connection.

Zombie cleanup calls (ZmbCall)
Times the Zombie cleanup function is called. Every time a connection is flushed, it is marked for cleanup. The Zombie cleanup function clears all these connections at predefined intervals.

SYN packets received (TCPSYN)
SYN packets received

Server probes (SYNProbe)
Probes from the NetScaler to a server. The NetScaler sends a SYN packet to the server to check its availability and expects a SYN_ACK packet from the server before a specified response timeout.

FIN packets from server (SvrFin)
FIN packets received from the server.

FIN packets from client (CltFin)
FIN packets received from the clients.

Time wait to SYN (WaToSyn)
SYN packets received on connections that are in the TIME_WAIT state. Packets cannot be transferred on a connection in this state.

Data in TIME_WAIT (WaDat)
Bytes of data received on connections that are in the TIME_WAIT state. Data cannot be transferred on a connection that is in this state.

SYN packets held (SYNHeld)
SYN packets held on the NetScaler that are waiting for a server connection.

SYN packets flushed (SYNFlush)
SYN packets flushed on the NetScaler because of no response from the server for three or more seconds.

TIME_WAIT connections closed (FinWaitC)
Connections closed on the NetScaler because the number of connections in the TIME_WAIT state has exceeded the default value of 7000.

Bad TCP checksum (TCPBadCk)
Packets received with a TCP checksum error.

Data after FIN (TCPDtFin)
Bytes received following a connection termination request. This error is usually caused by a reordering of packets during transmission.

SYN in SYN_RCVD state (TCPSYNRv)
SYN packets received on a connection that is in the SYN_RCVD state. A connection goes into the SYN_RCVD state after receiving a SYN packet.

SYN in ESTABLISHED state (TCPSYNEs)
SYN packets received on a connection that is in the ESTABLISHED state. A SYN packet is not expected on an ESTABLISHED connection.

SYN_SENT incorrect ACK packet (TCPBadAk)
Incorrect ACK packets received on a connection that is in the SYN_SENT state. An incorrect ACK packet is the third packet in the three-way handshake that has an incorrect sequence number.

RST packets received (TCPRST)
Reset packets received from a client or a server.

RST on not ESTABLISHED (TCPRSTNE)
Reset packets received on a connection that is not in the ESTABLISHED state.

RST out of window (TCPRSTOW)
Reset packets received on a connection that is out of the current TCP window.

RST in TIME_WAIT (TCPRSTTi)
Reset packets received on a connection that is in the TIME_WAIT state. Packets cannot be transferred on a connection in the TIME_WAIT state.

Server out of order packets (SvrOOO)
Out of order TCP packets received from a server.

Client out of order packets (CltOOO)
Out of order TCP packets received from a client.

TCP hole on client connection (CltHole)
TCP holes created on a client connection. When out of order packets are received from a client, a hole is created on the NetScaler for each group of missing packets.

TCP hole on server connection (SvrHole)
TCP holes created on a server connection. When out of order packets are received from a server, a hole is created on the NetScaler for each group of missing packets.

Seq number SYN cookie reject (CSeqRej)
SYN cookie packets rejected because they contain an incorrect sequence number.

Signature SYN cookie reject (CSigRej)
SYN cookie packets rejected because they contain an incorrect signature.

Seq number SYN cookie drop (CSigDrp)
SYN cookie packets dropped because the sequence number specified in the packets is outside the current window.

MSS SYN cookie reject (CMssRej)
SYN cookie packets rejected because the maximum segment size (MSS) specified in the packets is incorrect.

Any IP port allocation failure (PortFal)
Port allocations that have failed on a mapped IP address because the maximum limit of 65536 has been exceeded, or the mapped IP is not configured.

IP port allocation failure (PortFalI)
Port allocations that have failed on a subnet IP address or vserver IP address because the maximum limit of 65536 has been exceeded.

Stray packets (StrayPkt)
Packets received on a connection whose state is not maintained on the NetScaler.

RST packets sent (SentRst)
Reset packets sent to a client or a server.

Bad state connections (BadConn)
Connections that are not in a valid TCP state.

RST threshold dropped (RstThre)
Reset packets dropped because the default threshold of 100 resets per 10 milliseconds has been exceeded. This is a configurable value using the set rateControl command.

Packets out of window (OOWPkt)
Packets received that are out of the current advertised window.

SYNs dropped (Congestion) (SynCng)
SYN packets dropped because of network congestion.

Client retransmissions (TCPCltRe)
Packets retransmitted by a client. This usually occurs because the acknowledgement from the NetScaler has not reached the client.

Full packet retransmissions (TCPFulRe)
Full packets retransmitted by the client or the server.

SYN packet retries (TCPSYNRe)
SYN packets resent to a server.

SYN packets timeout (TCPSYNG)
Attempts to establish a connection on the NetScaler that timed out.

TCP retransmission (Retr)
TCP packets retransmitted. The NetScaler attempts to retransmit the packet up to seven times, after which it resets the other half of the TCP connection.

1st retransmission (1stRetr)
Packets retransmitted once by the NetScaler.

3rd retransmission (3rdRetr)
Packets retransmitted three times by the NetScaler.

5th retransmission (5thRetr)
Packets retransmitted five times by the NetScaler.

7th retransmission (7thRetr)
Packets retransmitted seven times by the NetScaler. If this fails, the NetScaler terminates the connection.

Fast retransmits (FastRetr)
TCP packets on which the NetScaler performs a fast retransmission in response to three duplicate acknowledgements or a partial acknowledgement. The NetScaler assumes that the packet is lost and retransmits the packet before its time-out.

Server retransmissions (TCPSvrRe)
Packets retransmitted by a server. This usually occurs because the acknowledgement from the NetScaler has not reached the server.

Partial packet retransmissions (TCPParRe)
Partial packet retransmits by a client or server due to congestion on the connection. This usually occurs because the window advertised by the NetScaler is not big enough to hold the full packet.

FIN packet retries (TCPFINRe)
FIN packets resent to a server or a client.

FIN packets timeout (TCPFING)
Connections that were timed out by the NetScaler because of not receiving the ACK packet after retransmitting the FIN packet four times.

2nd retransmission (2ndRetr)
Packets retransmitted twice by the NetScaler.

4th retransmission (4thRetr)
Packets retransmitted four times by the NetScaler.

6th retransmission (6thRetr)
Packets retransmitted six times by the NetScaler.

TCP retransmission giveup (RetrG)
Times the NetScaler terminates a connection after retransmitting the packet seven times on that connection.

TCP level cip failure (CltHdrEr)
Number of times TCP level client header insertion failure

Related Commands

stat protocol http
stat protocol icmp
stat protocol ipv6
stat protocol icmpv6
stat protocol ip
stat protocol udp

stat protocol http

Synopsis

```
stat protocol http [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display HTTP protocol statistics

Arguments

Output

Counters

`Total requests (HTReqRx)`
HTTP requests received, including HTTP/1.0 and HTTP/1.1 requests.

`Total responses (HTRspRx)`
HTTP responses sent including HTTP/1.0 and HTTP/1.1 responses.

`Request bytes received (HTReqbRx)`
Bytes of HTTP data received.

`Response bytes received (HTRspbRx)`
Bytes received as response data.

`GETs (HTGETs)`
HTTP requests received using the GET method.

`POSTs (HTPOSTs)`
HTTP requests received using the POST method.

`Other methods (HTOthers)`
HTTP requests received using methods other than GET and POST. Some of the other well-defined HTTP methods are HEAD, PUT, DELETE, OPTIONS, and TRACE. User-defined methods are also allowed.

`HTTP/1.0 requests (HT10ReqRx)`
HTTP/1.0 requests received.

HTTP/1.1 requests (HT11ReqRx)
HTTP/1.1 requests received.

Content-length requests (HTCLnReq)
HTTP requests in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.

Chunked requests (HTChkReq)
HTTP requests in which the Transfer-Encoding field of the HTTP header has been set to chunked.

Request bytes transmitted (HTReqbTx)
Bytes of HTTP data transmitted.

HTTP/1.0 responses (HT10RspRx)
HTTP/1.0 responses sent.

HTTP/1.1 responses (HT11RspRx)
HTTP/1.1 responses sent.

Content-length responses (HTCLnRsp)
HTTP responses sent in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.

Chunked responses (HTChunk)
HTTP responses sent in which the Transfer-Encoding field of the HTTP header has been set to chunked. This setting is used when the server wants to start sending the response before knowing its total length. The server breaks the response into chunks and sends them in sequence, inserting the length of each chunk before the actual data. The message ends with a chunk of size zero.

Multi-part responses (HTMPrtHd)
HTTP multi-part responses sent. In multi-part responses, one or more entities are encapsulated within the body of a single message.

FIN-terminated responses (HTNoCLnChunk)
FIN-terminated responses sent. In FIN-terminated responses, the server finishes sending the data and closes the connection.

Response bytes transmitted (HTRspbTx)
Bytes transmitted as response data.

Incomplete headers (HTIncHd)
HTTP requests and responses received in which the HTTP header spans more than one packet.

Incomplete request headers (HTIncReqHd)
HTTP requests received in which the header spans more than one packet.

Incomplete response headers (HTIncRspHd)
HTTP responses received in which the header spans more than one packet.

HTTP 500 Server-busy Responses (HT500Rsp)
Error responses received. Some of the error responses are: 500 Internal Server Error 501 Not Implemented 502 Bad Gateway 503 Service Unavailable 504 Gateway Timeout 505 HTTP Version Not Supported

Large/Invalid messages (HTInvReq)
Large or invalid requests and responses received.

Large/Invalid chunk requests (HTInvChkRx)
Large or invalid requests received in which the Transfer-Encoding field of the HTTP header has been set to chunked.

Large/Invalid content-length (HTInvCLn)
Large or invalid requests received in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.

Related Commands

stat protocol tcp
stat protocol icmp
stat protocol ipv6
stat protocol icmpv6
stat protocol ip
stat protocol udp

stat protocol icmp

Synopsis

```
stat protocol icmp [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display ICMP protocol statistics

Arguments

Output

Counters

ICMP packets received (ICPktRx)
ICMP packets received.

ICMP bytes received (ICbRx)
Bytes of ICMP data received.

ICMP packets transmitted (ICPktTx)
ICMP packets transmitted.

ICMP bytes transmitted (ICbTx)
Bytes of ICMP data transmitted.

ICMP echo replies received (ECORepRx)
ICMP Ping echo replies received.

ICMP echo replies transmitted (ECORepTx)
ICMP Ping echo replies transmitted.

ICMP echos received (ECORx)
ICMP Ping Echo Request and Echo Reply packets received.

ICMP rate threshold (pkts/sec) (ICThs)
Limit for ICMP packets handled every 10 milliseconds. Default value, 0, applies no limit. This is a configurable value using the set rateControl command.

ICMP port unreachable received (PortUnRx)
ICMP Port Unreachable error messages received. This error is generated when there is no service is running on the port.

ICMP port unreachable generated (PortUnTx)
ICMP Port Unreachable error messages generated. This error is generated when there is no service is running on the port.

Need fragmentation received (NeedFrag)
ICMP Fragmentation Needed error messages received for packets that need to be fragmented but for which Don't Fragment is specified the header.

ICMP rate threshold exceeded (ICRtEx)
Times the ICMP rate threshold is exceeded. If this counter continuously increases, first make sure the ICMP packets received are genuine. If they are, increase the current rate threshold.

ICMP packets dropped (ICPktDr)
ICMP packets dropped because the rate threshold has been exceeded.

Bad ICMP checksum (BadCkSum)
ICMP Fragmentation Needed error messages received with an ICMP checksum error.

PMTU non-first IP fragments (PMTUerr)
ICMP Fragmentation Needed error messages received that were generated by an IP fragment other than the first one.

PMTU Invalid body len received (IvBdyLen)
ICMP Fragmentation Needed error messages received that specified an invalid body length.

PMTU no tcp connection (NoTcpCon)
ICMP Need Fragmentation error messages received for TCP packets. The state of the connection for these packets is not maintained on the NetScaler.

PMTU no udp conection (NoUdpCon)
ICMP Need Fragmentation error messages received for UDP packets. The state of the connection for these packets is not maintained on the NetScaler.

PMTU invalid tcp seqno recvd (InvSeqNo)
ICMP Fragmentation Needed error messages received for packets that contain an invalid TCP address.

Invalid next MTU value recvd (IvNxtMTU)
ICMP Fragmentation Needed error messages received in which the Maximum Transmission Unit (MTU) for the next hop is out of range. The range for the MTU is 576-1500.

Next MTU > Current MTU (BigNxMTU)
ICMP Fragmentation Needed error messages received in which the value for the next MTU is higher than that of the current MTU.

PMTU Invalid protocol recvd (IvPrtRx)
ICMP Fragmentation Needed error messages received that contain a protocol other than TCP and UDP.

PMTU IP check sum error (CkSumErr)
ICMP Fragmentation Needed error messages received with an IP checksum error.

PMTU pcb with no link (NoLnkErr)
ICMP Fragmentation Needed error messages received on a Protocol Control Block (PCB) with no link. The PCB maintains the state of the connection.

PMTU Discovery not enabled (PMTUdis)
ICMP Need Fragmentation error messages received when the PMTU Discovery mode is not enabled.

Related Commands

stat protocol tcp

stat protocol http

stat protocol ipv6

stat protocol icmpv6

stat protocol ip

stat protocol udp

stat protocol ipv6

Synopsis

```
stat protocol ipv6 [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display ipv6 protocol statistics

Arguments

Output

Counters

IPv6 packets received (ipv6RxPkts)
IPv6 packets received.

IPv6 bytes received (ipv6RxBytes)
Bytes of IPv6 data received.

IPv6 packets transmitted (ipv6TxPkts)
IPv6 packets transmitted

IPv6 bytes transmitted (ipv6TxBytes)
Bytes of IPv6 data transmitted.

IPv6 Fragments received. (ipv6FragRxPkts)
IPv6 fragments received.

TCP Fragments reassembled. (ipv6FragTcpReass)
TCP fragments processed after reassembly.

UDP Fragments reassembled. (ipv6FragUdpReass)
UDP fragments processed after reassembly.

IPv6 Fragments processed without reassembly. (ipv6FragPktsProcessNoReass)
IPv6 fragments processed without reassembly.

IPv6 Fragments bridged. (ipv6FragPktsForward)
IPv6 fragments forwarded to the client or server without reassembly.

IPv6 error hdr packets (RxErrHdr)
Packets received that contain an error in one or more components of the IPv6 header.

IPv6 unsupported next header (Errnxthdr)
Packets received that contain an unsupported next header. The supported next headers are TCP, ICMP, UDP, OSPF, and FRAGMENT.

IPv6 Land-attacks (land attack)
Land-attack packets received. The source and destination addresses are the same. If not dropped, these packets can lock up the appliance.

Reassembled data too big (AssembledPktTooBig)
Packets received for which the reassembled data exceeds the Ethernet packet data length of 1500 bytes.

Zero fragment length received (ZeroLenFramentedPkt)
Packets received with a fragment length of 0 bytes.

ICMPv6 NA packets received
Number of ICMPv6 NA packets received by NetScaler (OBSOLETE).

ICMPv6 NS packets received
Number of ICMPv6 NS packets received by NetScaler (OBSOLETE).

ICMPv6 NA packets transmitted
Number of ICMPv6 NA packets transmitted by NetScaler (OBSOLETE).

ICMPv6 NS packets transmitted
Number of ICMPv6 NS packets transmitted by NetScaler (OBSOLETE).

ICMPv6 RA packets received
Number of ICMPv6 RA packets received by NetScaler (OBSOLETE).

ICMPv6 RS packets transmitted
Number of ICMPv6 RS packets transmitted by NetScaler (OBSOLETE).

ICMPv6 packets received
Number of ICMPv6 packets received by NetScaler (OBSOLETE).

ICMPv6 packets transmitted
Number of ICMPv6 packets transmitted by NetScaler (OBSOLETE).

IPv6 error hdr packets
Number of erroneous header packets received (OBSOLETE).

IPv6 error packets
Number of erroneous packets received (OBSOLETE).

IPv6 bad checksum
Number of bad checksum packets received (OBSOLETE).

ICMPv6 error packets
Number of erroneous ICMPv6 packets received (OBSOLETE).

unsupported ICMPv6 packets
Number of ICMPv6 unsupported packets received (OBSOLETE).

Rate threshold exceeded packets
Number of ICMPv6 packets dropped for rate threshold exceeded (OBSOLETE).

Related Commands

stat protocol tcp
stat protocol http
stat protocol icmp
stat protocol icmpv6
stat protocol ip
stat protocol udp

stat protocol icmpv6

Synopsis

```
stat protocol icmpv6 [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display icmpv6 protocol statistics

Arguments

Output

Counters

ICMPv6 packets received (icmpv6RxPkts)
ICMPv6 packets received.

ICMPv6 bytes received (icmpv6RxBytes)
Bytes of ICMPv6 data received.

ICMPv6 packets transmitted (icmpv6TxPkts)
ICMPv6 packets transmitted.

ICMPv6 bytes transmitted (icmpv6TxBytes)
Bytes of ICMPv6 data transmitted.

ICMPv6 NA packets received (icmpv6RxNa)
ICMPv6 neighbor advertisement packets received. These packets are received in response to a neighbor solicitation message sent out by this node, or if the link layer address of a neighbor has changed.

ICMPv6 NS packets received (icmpv6RxNs)
ICMPv6 neighbor solicitation packets received. These packets are received if the link layer address of a neighbor has changed, or in response to a neighbor solicitation message sent out by this node.

ICMPv6 RA packets received (icmpv6RxRa)
ICMPv6 router advertisement packets received. These are received at defined intervals or in response to a router solicitation message.

ICMPv6 RS packets received (icmpv6RxRs)
ICMPv6 router solicitation packets received. These could be sent by a neighboring router to initiate address resolution.

ICMPv6 Echo Request packets received (icmpv6RxEchoReq)
ICMPv6 Ping Echo Request packets received.

ICMPv6 Echo Reply packets received (icmpv6RxEchoReply)
ICMPv6 Ping Echo Reply packets received.

ICMPv6 NA packets transmitted (icmpv6TxNa)
ICMPv6 neighbor advertisement packets transmitted. These packets are sent in response to a neighbor solicitation packet, or if the link layer address of this node has changed.

ICMPv6 NS packets transmitted (icmpv6TxNs)
ICMPv6 neighbor solicitation packets transmitted. These packets are sent to get the link layer addresses of neighboring nodes or to confirm that they are reachable.

ICMPv6 RA packets transmitted (icmpv6TxRa)
ICMPv6 router advertisement packets transmitted. These packets are sent at regular intervals or in response to a router solicitation packet from a neighbor.

ICMPv6 RS packets transmitted (icmpv6TxRs)
ICMPv6 router solicitation packets transmitted. These packets are sent to request neighboring routers to generate router advertisements immediately rather than wait for the next defined time.

ICMPv6 Echo Request packets transmitted (icmpv6TxEchoReq)
ICMPv6 Ping Echo Request packets transmitted.

ICMPv6 Echo Reply packets transmitted (icmpv6TxEchoReply)
ICMP Ping Echo Reply packets transmitted.

ICMPv6 RA error packets (Error in RA packet)
ICMPv6 router advertisement error packets received that contain an error in the header, such as an incorrect source IP address, destination IP address, or packet length.

ICMPv6 NA error packets (Error in NA packet)
ICMPv6 neighbor advertisement error packets received that contain an error in the header, such as an incorrect source IP address, destination IP address, or packet length.

ICMPv6 NS error packets (Error in NS packet)
ICMPv6 neighbor solicitation error packets received that contain an error in the header, such as an incorrect source IP address, destination IP address, or packet length.

ICMPv6 bad checksum (Cksumerr)
Packets received with an ICMPv6 checksum error.

unsupported ICMPv6 packets (icmpv6Unspt)
ICMPv6 packets received that are not supported by the NetScaler.

Rate threshold exceeded packets (icmpv6thsld)
Packets dropped because the default threshold of 100 requests per 10 milliseconds has been exceeded. This is a configurable value using the set rateControl command.

Related Commands

stat protocol tcp
stat protocol http
stat protocol icmp
stat protocol ipv6
stat protocol ip
stat protocol udp

stat protocol ip

Synopsis

```
stat protocol ip [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display IP protocol statistics

Arguments

Output

Counters

IP packets received (IPPktRx)
IP packets received.

IP bytes received (IPbRx)
Bytes of IP data received.

IP packets transmitted (IPPktTx)
IP packets transmitted.

IP bytes transmitted (IPbTx)
Bytes of IP data transmitted.

Megabits received (IPMbRx)
Megabits of IP data received.

Megabits transmitted (IPMbTx)
Megabits of IP data transmitted.

IP fragments received (IPFragRx)
IP fragments received.

Successful reassembly (reasSucc)
Fragmented IP packets successfully reassembled on the NetScaler.

Reassembly attempted (reasAtmp)
IP packets that the NetScaler attempts to reassemble. If one of the fragments is missing, the whole packet is dropped.

IP address lookups (IpLkUp)
IP address lookups performed by the NetScaler. When a packet is received on a non-established session, the NetScaler checks if the destination IP address is one of the NetScaler owned IP addresses.

IP address lookup failure (IpLkFail)
IP address lookups performed by the NetScaler that have failed because the destination IP address of the packet does not match any of the NetScaler owned IP addresses.

UDP fragments forwarded (udpFgFwd)
UDP fragments forwarded to the client or the server.

TCP fragments forwarded (tcpFgFwd)
TCP fragments forwarded to the client or the server.

Fragmentation packets created (frgPktCr)
Fragmented packets created by the NetScaler.

Bad IP checksums (badCksum)
Packets received with an IP checksum error.

Unsuccessful reassembly (reasFail)
Packets received that could not be reassembled. This can occur when there is a checksum failure, an identification field mismatch, or when one of the fragments is missing.

Reassembled data too big (reasBig)
Packets received for which the reassembled data exceeds the Ethernet packet data length of 1500 bytes.

Zero fragment length received (zeroLen)
Packets received with a fragment length of 0 bytes.

Duplicate fragments received (dupFrag)
Duplicate IP fragments received. This can occur when the acknowledgement was not received within the expected time.

Out of order fragment received (oooFrag)
Fragments received that are out of order.

Unknown destination received (UnkDst)
Packets received in which the destination IP address was not reachable or not owned by the NetScaler.

Bad Transport (badTran)
Packets received in which the protocol specified in the IP header is unknown to the NetScaler.

VIP down (vipDown)
Packets received for which the VIP is down. This can occur when all the services bound to the VIP are down or the VIP is manually disabled.

Fix header failure (hdrFail)
Packets received that contain an error in one or more components of the IP header.

TTL expired during transit (ttlExp)
Packets for which the time-to-live (TTL) expired during transit. These packets are dropped.

max non-TCP clients (maxClt)
Attempts to open a new connection to a service for which the maximum limit has been exceeded. Default value, 0, applies no limit.

Unknown services (UnkSvc)
Packets received on a port or service that is not configured.

land-attacks (LndAtk)
Land-attack packets received. The source and destination addresses are the same.

Invalid IP header size (errHdrSz)
Packets received in which an invalid data length is specified, or the value in the length field and the actual data length do not match. The range for the Ethernet packet data length is 0-1500 bytes.

Invalid IP packet size (errPktLen)
Total number of packets received by NetScaler with invalid IP packet size.

Truncated IP packet (trIP)
Truncated IP packets received. An overflow in the routers along the path can truncate IP packets.

Truncated non-IP packet (trNonIp)
Truncated non-IP packets received.

ZERO next hop (zrNxtHop)
Packets received that contain a 0 value in the next hop field. These packets are dropped.

Packets with len > 1514 rcvd (BadLenTx)
Packets received with a length greater than the normal maximum transmission unit of 1514 bytes.

Packets with bad MAC sent (BadMacTx)
IP packets transmitted with a bad MAC address.

Related Commands

stat protocol tcp
stat protocol http
stat protocol icmp
stat protocol ipv6
stat protocol icmpv6
stat protocol udp

stat protocol udp

Synopsis

```
stat protocol udp [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display UDP protocol statistics

Arguments

Output

Counters

Packets received (UDPPktRx)
UDP packets received.

Bytes received (UDPbRx)
Bytes of UDP data received.

Packets transmitted (UDPPktTx)
UDP packets transmitted.

Bytes transmitted (UDPbTx)
Bytes of UDP data transmitted.

Current rate threshold (UDPThs)
Limit for UDP packets handled every 10 milliseconds. Default value, 0, applies no limit. This is a configurable value using the set rateControl command.

Unknown service (UDPUnSvc)
UDP packets received (but dropped) on a NetScaler port number that is not assigned to any service.

Bad UDP checksum (UDPBadCkSum)
Packets received with a UDP checksum error.

`Rate threshold exceeded (UDPRtEx)`
Number of times the UDP rate threshold is exceeded. If this counter continuously increases, first make sure the UDP packets received are genuine. If they are, increase the current rate threshold.

Related Commands

stat protocol tcp
stat protocol http
stat protocol icmp
stat protocol ipv6
stat protocol icmpv6
stat protocol ip

CHAPTER 23

Routing Commands

This chapter covers the routing commands.

clear router bgp

Synopsis

```
clear router bgp [<autonomousSystem>] (-neighbor
<ip_addr> | -all)
```

Description

Clear the BGP connection to a specified neighbor.

Arguments

autonomousSystem

The autonomous system for BGP. Minimum value: 1

neighbor

The neighbor associated with the connection that needs to be torn down.

all

Reset TCP connections to all neighbors.

Example

clear ip bgp neighbor 10.102.10.10

Related Commands

add router bgp

rm router bgp

set router bgp

unset router bgp

show router bgp

vtysh

Synopsis

```
vtysh
```

Description

Enter this comamand to enter vtysh (the routing shell). Vtysh is the integrated shell of the dynamic routing suite from which all the routing protocols can be configured.

Related Commands

set router ospf

Synopsis

```
set router ospf [-routerID <ip_addr>] [-
passiveInterface <string>] [-staticRedistribute  [-
staticMetricType <integer>]] [-kernelRedistribute  [-
kernelMetricType <integer>]] [-conRedistribute  [-
conMetricType <integer>]] [-learnRoute] [-network
<ip_addr>  <netmask>  -area <integer>] [-host <ip_addr>
-cost <integer>]
```

Description

Configure different OSPF parameters.

Arguments

`routerID`

The router ID.

`passiveInterface`

The mode of the Interface. Use this option to change the mode of the interface to listen only.

`staticRedistribute`

The state of the router in redistributing static routes. Use this option to enable the redistribution of static routes. Default value:
NS_OSPF_REDISTRIBUTE_STATIC

`kernelRedistribute`

The state of the router in redistributing kernel routes. Use this option to enable the redistribution of kernel routes. Default value:
NS_OSPF_REDISTRIBUTE_KERNEL

`conRedistribute`

The state of the router in redistributing connected routes. Use this option to enable the redistribution of connected routes. Default value:
NS_OSPF_REDISTRIBUTE_CON

learnRoute
The state of the router in learning routes from OSPF. Use this option to enable route learning from OSPF. Default value: NS_OSPF_SET_LEARNING

network
The broadcast network on which OSPF is to be run.

host
The stub link.

Example

set ospf -routerID 1.2.3.4

Related Commands

unset router ospf

show router ospf

unset router ospf

Synopsis

```
unset router ospf [-routerID] [-learnRoute] [-
conRedistribute] [-kernelRedistribute] [-
staticRedistribute] [-network <ip_addr>  <netmask>  -
area <integer>] [-host <ip_addr>  -cost <integer>] [-
passiveInterface <string>] [-staticMetricType] [-
kernelMetricType] [-conMetricType]
```

Description

Unset the OSPF parameters that were configured using the ###set ospf### command..Refer to the set router ospf command for meanings of the arguments.

Example

unset ospf -router-id

Related Commands

set router ospf

show router ospf

show router ospf

Synopsis

```
show router ospf [<ospfoptions>]
```

Description

Display the state of the OSPF daemon.

Arguments

ospfoptions

The Router OSPF option. Use this option to display one of border-routers, database, interface, neighbor, route, and virtual-links. Possible values: border-routers, database, interface, neighbor, route, virtual-links

format

level

Output

network

The network on which OSPF is running.

netmask

Netmask of the network on which OSPF is running

Example

show ospf neighbor

Related Commands

set router ospf

unset router ospf

set router rip

Synopsis

```
set router rip [-defaultMetric <integer>] [-
passiveInterface <string>] [-learnRoute] [-
staticRedistribute] [-kernelRedistribute] [-network
<ip_addr>  <netmask>]
```

Description

Configure the RIP daemon.

Arguments

`defaultMetric`

The default metrics when advertising routes. Default value: 1 Minimum value: 1 Maximum value: 16

`passiveInterface`

The mode of the interface to listen only.

`learnRoute`

The state of Route learning. Use this option to enable route learning and installation in the kernel. Default value: NS_RIP_SET_LEARNING

`staticRedistribute`

The state of redistributing static routes. Default value: NS_RIP_SETREDISTRIBUTE_STATIC

`kernelRedistribute`

The state of redistributing kernel routes. Default value: NS_RIP_SETREDISTRIBUTE_KERNEL

`network`

The broadcast network on which RIP must run.

Example

set router rip -kernelRedistribute

Related Commands

unset router rip

show router rip

unset router rip

Synopsis

```
unset router rip [-defaultMetric] [-staticRedistribute]
[-learnRoute] [-kernelRedistribute] [-passiveInterface
<string>] [-network <ip_addr>  <netmask>]
```

Description

Unset the RIP parameters..Refer to the set router rip command for meanings of the arguments.

Example

unset rip -default-metric

Related Commands

set router rip

show router rip

show router rip

Synopsis

```
show router rip [<ripOptions>]
```

Description

Display the RIP configuration.

Arguments

`ripOptions`

RIP option in show command, one of database or interface. Possible values: database, interface

`format`

`level`

Output

`network`

`netmask`

Example

show rip interface

Related Commands

set router rip

unset router rip

add router bgp

Synopsis

```
add router bgp <autonomousSystem> [-routerID <ip_addr>]
[-learnRoute] [-staticRedistribute  [-staticRouteMap
<string>]] [-kernelRedistribute  [-kernelRouteMap
<string>]] [-conRedistribute  [-connectedRouteMap
<string>]] [-neighbor <ip_addr>  <remoteAS>  [-
neighborRouteMap <string>]] [-network <ip_addr>
<netmask>]
```

Description

Add BGP neighbors.

Arguments

autonomousSystem

The BGP autonomous system. Minimum value: 1

routerID

The router ID of the router.

learnRoute

The state of route learning from BGP. Default value: NS_BGP_SET_LEARNING

staticRedistribute

The state of router in redistribution of static routes. Default value: NS_BGP_REDISTRIBUTE_STATIC

kernelRedistribute

The state of router in redistribution of kernel routes. Default value: NS_BGP_REDISTRIBUTE_KERNEL

conRedistribute

The state of router in redistribution of connected routes. Default value: NS_BGP_REDISTRIBUTE_CON

`neighbor`
Add a BGP neighbor.

`network`
The neighbor to be advertised.

Example

add router bgp 10 neighbor 10.102.10.10 10

Related Commands

clear router bgp
rm router bgp
set router bgp
unset router bgp
show router bgp

rm router bgp

Synopsis

```
rm router bgp <autonomousSystem> [-neighbor <ip_addr>]
```

Description

Remove the BGP configuration.

Arguments

autonomousSystem

The autonomous system for BGP. Minimum value: 1

neighbor

To remove a particular neighbor.

Example

rm router bgp 3535

Related Commands

clear router bgp

add router bgp

set router bgp

unset router bgp

show router bgp

set router bgp

Synopsis

```
set router bgp <autonomousSystem> [-routerID <ip_addr>]
[-learnRoute] [-staticRedistribute  [-staticRouteMap
<string>]] [-kernelRedistribute  [-kernelRouteMap
<string>]] [-conRedistribute  [-connectedRouteMap
<string>]] [-neighbor <ip_addr>  [<remoteAS>]  [-
neighborRouteMap <string>]] [-network <ip_addr>
<netmask>]
```

Description

Configure BGP on the NetScaler system.

Arguments

autonomousSystem

The autonomous system for BGP. Minimum value: 1

routerID

The Router ID of this router.

learnRoute

The state of the router in learning routes from BGP. Use this option to enable route learning and installation from BGP. Default value: NS_BGP_SET_LEARNING

staticRedistribute

The state of the router in redistributing static routes. Use this option to enable the redistribution of static routes. Default value: NS_BGP_REDISTRIBUTE_STATIC

kernelRedistribute

The state of the router in redistribution of kernel routes. Default value: NS_BGP_REDISTRIBUTE_KERNEL

conRedistribute
The state of the router in redistributing connected routes. Use this option to enable the redistribution of connected routes into the BGP domain. Default value: NS_BGP_REDISTRIBUTE_CON

neighbor
The IP address of a BGP peer for the router.

network
The network to be advertized.

Example

set router bgp -kernelRedistribute

Related Commands

clear router bgp
add router bgp
rm router bgp
unset router bgp
show router bgp

unset router bgp

Synopsis

```
unset router bgp <autonomousSystem> [-routerID
<ip_addr>] [-learnRoute] [-staticRedistribute  [-
staticRouteMap <string>]] [-kernelRedistribute  [-
kernelRouteMap <string>]] [-conRedistribute  [-
connectedRouteMap <string>]] [-neighbor <ip_addr>  -
neighborRouteMap <string>] [-network <ip_addr>
<netmask>] [-remoteAS]
```

Description

Unset the BGP parameters..Refer to the set router bgp command for meanings of the arguments.

Example

unset router bgp -kernelRedistribute

Related Commands

clear router bgp

add router bgp

rm router bgp

set router bgp

show router bgp

show router bgp

Synopsis

```
show router bgp [<autonomousSystem>] (<bgpOptions> | -
routeMap <string>)
```

Description

Display the BGP configuration.

Arguments

autonomousSystem

The autonomous system for BGP. Minimum value: 1

bgpOptions

option to show BGP command either neighbors or summary Possible values: neighbors, summary

routeMap

The BGP route map.

summary

fullValues

format

level

Output

Example

show router bgp summary

Related Commands

clear router bgp

add router bgp

rm router bgp

set router bgp

unset router bgp

CHAPTER 24

SureConnect Commands

This chapter covers the SureConnect commands.

stat sc

Synopsis

```
stat sc [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display SureConnect statistics.

Arguments

Output

Counters

SC condition triggered (ScTrigd)

This counter gives the number of times the SC conditions were triggered.

Policy matches

This counter gives the number of times netscaler matched an incoming request with a Configured sureconnect policy.

SC responses sent

This counter gives the number of times netscaler served the in-memory java script which throws up the pop up window.

Reissued requests (ReissReq)

This counter gives the number of SC reissued requests that Netscaler received.

Valid reissued requests

This counter gives the number of requests which came in a SureConnect session.

Alternate content requests

This gives the number of requests which are required to load the alternate content in the pop up window.

SC POST requests

This counter gives the number of times a post request triggered SureConnect.

SC statistics timeout
This gives the number of times SureConnect statistics were reset.

Unsupported browsers
This counter gives the number of times requests came from unsupported browsers.

Tampered SC cookies
This counter gives the number of times netscaler encountered corrupted SureConnect Cookies.

SC trigger condition failed
This counter gives the number of times netscaler did not serve the in-memory response because the thresholds conditions had failed.

Related Commands

stat sc policy

show sc stats

Synopsis

```
show sc stats - alias for 'stat sc'
```

Description

show sc stats is an alias for stat sc

Related Commands

stat sc

set sc parameter

Synopsis

```
set sc parameter [-sessionLife <secs>] [-vsr
<input_filename>]
```

Description

set the SureConnect parameters.

Arguments

sessionLife

The time between the first time and next time the sureconnect alternet window display.The SureConnect alternate content window is displayed only once during a session. For the same browser accessing a configured URL.The value is in seconds. Minimum value: 1 Maximum value: 0xFFFFFFFE

vsr

The file containing the customized response that is to be displayed with ACTION as NS in the SureConnect policy.

Example

set sc parameter -sessionlife 200 -vsr /etc/vsr.htm

Related Commands

unset sc parameter

show sc parameter

unset sc parameter

Synopsis

```
unset sc parameter [-sessionLife] [-vsr]
```

Description

Use this command to remove sc parameter settings.Refer to the set sc parameter command for meanings of the arguments.

Related Commands

set sc parameter

show sc parameter

show sc parameter

Synopsis

```
show sc parameter
```

Description

Display the SureConnect parameters set through the use of the ###set sc parameter### command.

Arguments

format

level

Output

sessionLife

The time between first time the Sureconnect aternate content window displays and the next time it displays.The SureConnect alternate content window is displayed only once during a session. For the same browser accessing a configured URL.The value is in seconds.

vsr

The customized response will be displayed to the user if the alternate content server has been determined by the system to have failed. If you have created a customized response that you want the system to use, enter its filename (if you renamed the vsr.htm file supplied by system). If you have not renamed the file, enter /etc/vsr.htm as the filename.

Example

> show sc parameter Sure Connect Parameters: Sessionlife: 300 Vsr: DEFAULT Done

Related Commands

set sc parameter

unset sc parameter

add sc policy

Synopsis

```
add sc policy <name> [-url <URL> | -rule <expression>]
[-delay <usecs>] [-maxConn <positive_integer>] [-action
<action>  (<altContentSvcName>  <altContentPath>)]
```

Description

Add the SureConnect policy.

Arguments

`name`

The name of the SureConnect policy.

`url`

The URL name. The system matches the incoming client request against the URL you enter here. If the incoming request does not match any of the configured URLs or the rules that have been configured, then SureConnect does not trigger.

`rule`

The rule that the system matches with the incoming request. The system matches the incoming request against the rules you enter here. Before matching against the configured rules, the system matches the requests with any of the configured URLs. Thus, URLs have a higher precedence over rules. If the incoming request does not match any of the configured URLs or the rules that have been configured, then SureConnect does not trigger. Expression logic is expression names, separated by the logical operators || and && , and possibly grouped using parenthesis. If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes.The following are valid expression logic: ns_ext_cgi||ns_ext_asp ns_non_get && (ns_header_cookie||ns_header_pragma)

`delay`

The delay threshold in microseconds for the configured URL or the rule. If the delay statistics gathered for the configured URL or rule exceeds the configured delay, then SureConnect is triggered on the incoming request

which matched the corresponding delay. Minimum value: 1 Maximum value: 599999999

maxConn

The maximum number of concurrent connections that can be open for the configured URL or rule. You can enter this argument as any integer value greater than zero. Minimum value: 1 Maximum value: 0xFFFFFFFE

action

The action to be taken when the thresholds are met. The valid options are ACS , NS and NOACTION . ACS - Specifies that alternate content is to be served from altContSvcName with the path altContPath . NS - Specifies that alternate content is to be served from the system. See the set sc parameter command to customize the response served from the system. NOACTION - Specifies that no alternate content is to be served. However, delay statistics are still collected for the configured URLs. If the - maxconn argument is specified, the number of connections is limited to that specified value for that configured URL or rule (alternate content will not served even if the - maxconn threshold is met). Possible values: ACS, NS, NOACTION

altContentSvcName

The alternate content service name used in the ACS action.

altContentPath

The alternate content path for the ACS action.

Example

add sc policy scpol_ns -delay 1000000 -url /delay.asp -action NS add policy expression exp_acs "url == /mc_acs.asp" add service svc_acs 10.110.100.253 http 80 add scpolicy scpol_acs -maxconn 10 -rule exp_acs -action ACS svc_acs /altcont.htm

Related Commands

rm sc policy

set sc policy

unset sc policy

show sc policy

stat sc policy

rm sc policy

Synopsis

```
rm sc policy <name>
```

Description

Remove the SureConnect policy.

Arguments

name

The name of the SureConnect policy.

Example

rm sc policy scpol_ns rm sc policy scpol_acs

Related Commands

add sc policy

set sc policy

unset sc policy

show sc policy

stat sc policy

set sc policy

Synopsis

```
set sc policy <name> [-url <URL> | -rule <expression>]
[-delay <usecs>] [-maxConn <positive_integer>] [-action
<action>  (<altContentSvcName>  <altContentPath>)]
```

Description

Set the delay and maxConn parameters for the specified SureConnect policy.

Arguments

name

The name of the SureConnect policy.

url

The URL name. The system matches the incoming client request against the URL you enter here. If the incoming request does not match any of the configured URLs or the rules that have been configured, then SureConnect does not trigger.

rule

The rule that the system matches with the incoming request. The system matches the incoming request against the rules you enter here. Before matching against the configured rules, the system matches the requests with any of the configured URLs. Thus, URLs have a higher precedence over rules. If the incoming request does not match any of the configured URLs or the rules that have been configured, then SureConnect does not trigger. Expression logic is expression names, separated by the logical operators || and && , and possibly grouped using parenthesis. If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes.The following are valid expression logic: ns_ext_cgi||ns_ext_asp ns_non_get && (ns_header_cookie||ns_header_pragma)

delay

The delay threshold in microseconds for the configured URL or the rule. Minimum value: 1 Maximum value: 599999999

maxConn

The maximum number of concurrent connections that can be open for the configured URL or rule. Minimum value: 1 Maximum value: 0xFFFFFFFE

action

The action to be taken when the thresholds are met. The valid options are ACS , NS and NOACTION . ACS - Specifies that alternate content is to be served from altContSvcName with the path altContPath . NS - Specifies that alternate content is to be served from the system. See the set sc parameter command to customize the response served from the system. NOACTION - Specifies that no alternate content is to be served. However, delay statistics are still collected for the configured URLs. If the - maxconn argument is specified, the number of connections is limited to that specified value for that configured URL or rule (alternate content will not served even if the - maxconn threshold is met). Possible values: ACS, NS, NOACTION

Example

set sc policy scpol_ns -delay 2000000 set sc policy scpol_acs -maxconn 100

Related Commands

add sc policy

rm sc policy

unset sc policy

show sc policy

stat sc policy

unset sc policy

Synopsis

```
unset sc policy <name> [-delay] [-maxConn]
```

Description

Use this command to remove sc policy settings.Refer to the set sc policy command for meanings of the arguments.

Related Commands

add sc policy

rm sc policy

set sc policy

show sc policy

stat sc policy

show sc policy

Synopsis

```
show sc policy [<name>]
```

Description

Display all of the Configured SureConnect policies.

Arguments

name

The name of the SureConnect policy.

summary

fullValues

format

level

Output

url

The URL name. The system matches the incoming client request against the URL you enter here.

rule

The rule that the system matches with the incoming request. The system matches the incoming request against the rules you enter here. Before matching against the configured rules, the NetScaler 9000 system matches the requests with any of the configured URLs. Thus, URLs have a higher precedence over rules. If the incoming request does not match any of the configured URLs or the rules that have been configured, then SureConnect does not trigger. Expression logic is expression names, separated by the logical operators || and && , and possibly grouped using parenthesis. If the expression contains blanks (for example, between an expression name and a logical operator), then the entire argument must be enclosed in double quotes.The following are valid expression logic: ns_ext_cgi||ns_ext_asp ns_non_get && (ns_header_cookie||ns_header_pragma)

delay
The delay threshold in microseconds for the configured URL or the rule. If the delay statistics gathered for the configured URL or rule exceeds the configured delay, then SureConnect is triggered on the incoming request which matched the corresponding delay.

maxConn
The maximum number of concurrent connections that can be open for the configured URL or rule. You can enter this argument as any integer value greater than zero.

action
The action to be taken when the thresholds are met. The valid options are ACS , NS and NOACTION . ACS - Specifies that alternate content is to be served from altContSvcName with the path altContPath . NS - Specifies that alternate content is to be served from the NetScaler 9000 system. See the set sc parameter command to customize the response served from the system. NOACTION - Specifies that no alternate content is to be served. However, delay statistics are still collected for the configured URLs. If the - maxconn argument is specified, the number of connections is limited to that specified value for that configured URL or rule (alternate content will not served even if the - maxconn threshold is met).

altContentSvcName
The alternate content service name used in the ACS action.

altContentPath
The alternate content path for the ACS action.

Example

> show sc policy 2 monitored Sure Connect Policies: 1) Name: scpol_ns RULE: exp1 Delay: 1000000 microsecs Alternate Content from NS 2) Name: scpol_acs RULE: exp_acs Max Conn: 10 Alternate Content from ACS, svc_acs /delay/alcont.htm Done

Related Commands

add sc policy

rm sc policy

set sc policy

unset sc policy

stat sc policy

stat sc policy

Synopsis

```
stat sc policy [<name>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display SureConnect policy statistics.

Arguments

name

The name of the SC policy for which statistics will be displayed. If not given stati stics are shown for all SC policies.

Output

Counters

Server TTLB (SvrTTLB)

This counter gives the server TTLB calculated for this policy.

Server TTLB (SvrTTLB)

This counter gives the server TTLB calculated for this policy.

Average server TTLB

Average Server transaction time.

Average client TTLB (AvClTTLB)

This counter gives the average value of the client TTLB for this policy.

Physical service port (SvcPort)

The port of the physical service for which this statistics is maintained.

Physical service IP (SvcIP)

The IP address of the physical service for which this statistics is maintained.

Current client connections (CurClts)

This counter gives the number of clients that were allowed a server connection for this policy.

Current SC queue length (WaitClts)
This counter gives the current number of SC priority clients that are waiting for a server connection for this policy.

Current server connections (CurSvrs)
Total number of open connections for this policy.

Estimated waiting time (Sec) (WaitTime)
This counter gives the value of the currently estimated waiting time for the configured URL.

Client TCP connections (TotClt)
This counter gives the total number of clients that were allowed a server connection for this policy.

Server TCP connections (TotSvr)
This counter gives the total number of server connections that were established for this policy.

Client HTTP transactions
Total number of client transactions for this policy.

Server HTTP transactions (SrvTrans)
This counter gives the number of 200 OK responses received from the server for this policy.

Requests received (TotReq)
This counter gives the total number of requests received for this policy.

Request bytes received (ReqBytes)
This counter gives the total number of request bytes received for this policy.

Server responses received (TotResp)
This counter gives the total number of server responses received for this policy.

Response bytes received (RspBytes)
This counter gives the total number of response bytes received for this policy.

Physical service port (SvcPort)
The port of the physical service for which this statistics is maintained.

Average client TTLB (AvClTTLB)
This counter gives the average value of the client TTLB for this policy.

Server TTLB (SvrTTLB)
This counter gives the server TTLB calculated for this policy.

Related Commands

add sc policy
rm sc policy
set sc policy
unset sc policy
show sc policy
stat sc

CHAPTER 25

SNMP Commands

This chapter covers the SNMP commands.

show snmp oid

Synopsis

```
show snmp oid <entityType> [<name>]
```

Description

Display the SNMP OID index for entities of given type.

Arguments

entityType
The entity type. Possible values: VSERVER, SERVICE, SERVICEGROUP

name
The name of the entity.

summary

fullValues

Output

snmpOID
The snmp oid.

state
state flag

Example

show snmp oid VSERVER vs1

Related Commands

stat snmp

Synopsis

```
stat snmp [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display snmp statistics.

Arguments

Output

Counters

SNMP packets received (PktsRx)
SNMP packets received.

SNMP packets sent (PktsTx)
SNMP packets transmitted.

Get requests receieved (GetReqRx)
SNMP Get-Request PDUs that have been accepted and processed.

Get-next requests receieved (GtNextRx)
SNMP Get-Next PDUs that have been accepted and processed.

Get-bulk requests received (GtBulkRx)
SNMP Get-Bulk PDUs that have been accepted and pro?cessed.

Responses sent (RspTx)
SNMP Get-Response PDUs that have been generated by the NetScaler.

Traps messages sent (TrapsTx)
SNMP Trap PDUs that have been generated by the NetScaler.

Requests dropped (ReqDrop)
SNMP requests dropped.

ASN.1/BER errors in requests (PrsErrRx)
Number of ASN.1 or BER errors encountered when decoding received SNMP Messages.

Unsupported SNMP version (UnkVrsRx)
Number of SNMP messages received, which were for an unsupported SNMP version.

Unknown community name (UnkCNRx)
SNMP messages received, which used an SNMP community name not known to the NetScaler.

No permission on community (BadCURx)
The total number of SNMP Messages received that represented an SNMP operation which was not allowed by the SNMP community named in the Message.

Unsupported security level (UnkSecLv)
SNMP packets that were dropped because they requested a security level that was unknown to the NetScaler or otherwise unavailable.

Not in time window (NtTimeWd)
SNMP packets that were dropped because they appeared outside of the authoritative SNMP engine's window.

Unknown user name (UnkUser)
SNMP packets that were dropped because they referenced a user that was not known to the SNMP engine.

Unknown engine Id (UnkEngId)
SNMP packets that were dropped because they referenced an SNMP engine ID that was not known to the NetScaler.

Wrong digest value (WrgDgst)
SNMP packets that were dropped because they did not contain the expected digest value.

Decryption errors (DcrptErr)
SNMP packets that were dropped because they could not be decrypted.

Example

stat snmp

Related Commands

show snmp stats

Synopsis

```
show snmp stats - alias for 'stat snmp'
```

Description

show snmp stats is an alias for stat snmp

Related Commands

stat snmp

set snmp alarm

Synopsis

```
set snmp alarm <trapName> [-thresholdValue
<positive_integer>  [-normalValue <positive_integer>]]
[-time <secs>] [-state ( ENABLED | DISABLED )] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Description

Configure the user-configurable SNMP alarms. For each configured alarm, an SNMP trap is sent when the value exceeds the specified high threshold. When the value falls below the normal threshold, another SNMP trap is sent indicating a return-to-normal state. Note: For any alarm, after a high threshold trap has been sent, it is not sent again until the monitored value falls back to normal. System supports thirteen user configurable alarms - HA-STATE-CHANGE:Change to primary/secondary CPU:High CPU usage ENTITY-STATE:Entity state change SYNFLOOD:Global unacknowledged SYN count MEMORY:Memory usage VSERVER-REQRATE:Vserver specific request rate SERVICE-REQRATE: Service specific request rate ENTITY-RXRATE: Entity specific Rx bytes per second ENTITY-TXRATE:Entity specific Tx bytes per second ENTITY-SYNFLOOD:Entity specific unacknowledged SYN count CONFIG-CHANGESystem configuration changed SERVICE-MAXCLIENTS:Service hit max-client limit CONFIG-SAVESystem configuration was saved For the purposes of this command, entity includes vservers and services. Note: 1. These traps are sent to "specific" trap destinations added via the 'add snmp trap specific'. 2. Thresholds for SERVICE-MAXCLIENTS should be set through 'set service <name> -maxClients <n>'.

Arguments

trapName

The name of the alarm. Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-

THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED

thresholdValue
The high threshold value that triggers the alarm. Minimum value: 1

time
The time interval for SYNFLOOD, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS or HA-BAD-SECONDARY-STATE alarms only. Default value: 1

state
The current state of the alarm. Possible values: ENABLED, DISABLED Default value: ENABLED

severity
The severity level of this alarm. Possible values: Critical, Major, Minor, Warning, Informational Default value: SNMP_SEV_UNKNOWN

logging
The logging status of the alarm. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set snmp alarm VSERVER-REQRATE -thresholdValue 10000 -normalValue 100

Related Commands

add snmp trap

unset snmp alarm

enable snmp alarm

disable snmp alarm

show snmp alarm

unset snmp alarm

Synopsis

```
unset snmp alarm <trapName> [-thresholdValue | -
normalValue | -time | -state | -severity | -logging]
```

Description

Unset a user-configurable SNMP alarm..Refer to the set snmp alarm command for meanings of the arguments.

Example

unset snmp alarm VSERVER-REQRATE

Related Commands

set snmp alarm

enable snmp alarm

disable snmp alarm

show snmp alarm

enable snmp alarm

Synopsis

```
enable snmp alarm <trapName> ...
```

Description

Enable the specified SNMP alarm.

Arguments

trapName

The alarm to be enabled. Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED

Example

enable snmp alarm VSERVER-REQRATE enable snmp alarm CPU SYNFLOOD

Related Commands

set snmp alarm

unset snmp alarm

disable snmp alarm

show snmp alarm

disable snmp alarm

Synopsis

```
disable snmp alarm <trapName> ...
```

Description

Disable the specified SNMP alarm.

Arguments

trapName

The alarm to be disabled. Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED

Example

disable snmp alarm VSERVER-REQRATE disable snmp alarm CPU SYNFLOOD

Related Commands

set snmp alarm

unset snmp alarm

enable snmp alarm

show snmp alarm

show snmp alarm

Synopsis

```
show snmp alarm [<trapName>]
```

Description

Displays the alarm thresholds for the user-configurable traps.

Arguments

trapName

The name of the alarm. Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED

summary

fullValues

format

level

Output

thresholdValue

The high threshold value.

normalValue

The normal threshold value.

time
The time interval for the SYNFLOOD alarm.

state
The current state of the alarm.

severity
The severity of this alarm.

logging
The log status of the alarm.

Related Commands

set snmp alarm
unset snmp alarm
enable snmp alarm
disable snmp alarm

add snmp community

Synopsis

```
add snmp community <communityName> <permissions>
```

Description

Set the SNMP community string to grant access to an SNMP network management application to manage the system. It also defines the specific management tasks that this user can perform. Tip: Use the add SNMP manager command to set the management privileges for the network management application.

Arguments

`communityName`
The SNMP community string.

`permissions`
The access privileges. Possible values: GET, GET_NEXT, GET_BULK, ALL

Example

add snmp community public ALL add snmp community a#12ab GET_BULK

Related Commands

rm snmp community

show snmp community

rm snmp community

Synopsis

```
rm snmp community <communityName>
```

Description

Remove the specified SNMP community string. Once the string is deleted, the user will not be able to use the community to manage the system.

Arguments

communityName
SNMP community string

Example

rm snmp community public

Related Commands

add snmp community

show snmp community

show snmp community

Synopsis

```
show snmp community [<communityName>]
```

Description

Display the access privileges set for all the SNMP community strings configured on the system.

Arguments

communityName
SNMP community string

summary

fullValues

format

level

Output

permissions
The access privileges.

Example

show snmp community

Related Commands

add snmp community

rm snmp community

add snmp manager

Synopsis

```
add snmp manager <IPAddress> ... [-netmask <netmask>]
```

Description

Configure the management application, which complies with SNMP version 1 or SNMP version 2, to access to the system. If at least one management station is not added through this command, network management applications from any host computer can access the system. The netmask parameter can be used to grant access from entire subnets. Up to a maximum of 100 network management hosts or networks can be added.

Arguments

`IPAddress`

The IP/Network address of the management station(s).

`netmask`

The subnet of management stations. Default value: 0xFFFFFFFF

Example

add snmp manager 192.168.1.20 192.168.2.42 add snmp manager 192.168.2.16 -netmask 255.255.255.240

Related Commands

rm snmp manager

show snmp manager

rm snmp manager

Synopsis

```
rm snmp manager <IPAddress> ... [-netmask <netmask>]
```

Description

Remove the access privileges from a management station, so that the management station no longer has access to the system.

Arguments

IPAddress

The IP/Network address of the management station.

netmask

The subnet of the management station.

Example

rm snmp manager 192.168.1.20 rm snmp manager 192.168.2.16 -netmask 255.255.255.240

Related Commands

add snmp manager

show snmp manager

show snmp manager

Synopsis

```
show snmp manager [<IPAddress>  [-netmask <netmask>]]
```

Description

Display the management stations that are allowed to manage the system. The managers are listed by their IP addresses and netmasks.

Arguments

IPAddress

The IP/Network address of the management station.

summary

fullValues

format

level

Output

Example

show snmp manager

Related Commands

add snmp manager

rm snmp manager

set snmp mib

Synopsis

```
set snmp mib [-contact <string>] [-name <string>] [-
location <string>] [-customID <string>]
```

Description

Set the system SNMP MIB information of the system.

Arguments

contact

The contact person for the system. Default value: "WebMaster (default)"

name

The name of the system. Default value: "NetScaler"

location

The physical location of the system. Default value: "POP (default)"

customID

Custom ID for the system. Default value: "Default"

Related Commands

unset snmp mib

show snmp mib

unset snmp mib

Synopsis

```
unset snmp mib [-contact] [-name] [-location] [-
customID]
```

Description

Use this command to remove snmp mib settings.Refer to the set snmp mib command for meanings of the arguments.

Related Commands

set snmp mib

show snmp mib

show snmp mib

Synopsis

```
show snmp mib
```

Description

Display the information from the SNMP system MIB in the system. The information that is displayed depends on what was specified when the set snmp mib CLI command was issued.

Arguments

format

level

Output

contact
The contact person for the system.

name
The name of the system.

location
The physical location of the system.

sysDesc
The description of the system.

sysUptime
The UP time of the system in 100th of a second.

sysServices
The services offered by the system.

sysOID
The OID of the system's management system.

customID
Custom ID for the system.

Example

show snmp mib

Related Commands

set snmp mib

unset snmp mib

add snmp trap

Synopsis

```
add snmp trap <trapClass> <trapDestination> ... [-
version ( V1 | V2 )] [-destPort <port>] [-communityName
<string>] [-srcIP <ip_addr>] [-severity <severity>]
```

Description

Create SNMP traps. The SNMP traps are asynchronous events generated by the agent to indicate the state of the system. The destination to which these traps should be sent by the system is configured via this command.

Arguments

trapClass
The Trap type. The Generic type causes the standard SNMP traps supported by the system to be sent to the destination, while the Specific trap type sets the destination for specific traps. Possible values: generic, specific

trapDestination
The IP address of the trap destination.

version
The SNMP version of the trap PDU to be sent. Possible values: V1, V2 Default value: TRAP_VERSION_2

destPort
The destination port of the SNMP trap. Default value: 162 Minimum value: 1

communityName
SNMP trap community string Default value: "public"

srcIP
The source IP of the SNMP traps. By default it is the NetScaler IP.

severity
The minimum severity of the alarms to be sent to this trap destination. By default all traps will be sent to this trap destination. Possible values: Critical, Major, Minor, Warning, Informational Default value: SNMP_SEV_UNKNOWN

Related Commands

rm snmp trap

set snmp trap

unset snmp trap

show snmp trap

rm snmp trap

Synopsis

```
rm snmp trap <trapClass> <trapDestination> ...
```

Description

Remove a trap destination that has been set.

Arguments

trapClass

The Trap type. Possible values: generic, specific

trapDestination

The IP address of the trap destination.

Related Commands

add snmp trap

set snmp trap

unset snmp trap

show snmp trap

set snmp trap

Synopsis

```
set snmp trap <trapClass> <trapDestination> [-destPort
<port>] [-version ( V1 | V2 )] [-communityName
<string>] [-srcIP <ip_addr>] [-severity <severity>]
```

Description

Set the SNMP version of trap PDU and source IP of SNMP traps for configured trap destinations.

Arguments

trapClass
The Trap type. Possible values: generic, specific

trapDestination
The IP address of the trap destination.

destPort
The destination port of the SNMP trap. Default value: 162 Minimum value: 1

version
The SNMP version of the trap PDU to be sent. Possible values: V1, V2 Default value: TRAP_VERSION_2

communityName
SNMP trap community string Default value: "public"

srcIP
The source IP of the SNMP traps. By default it is the NetScaler IP.

severity
The minimum severity of the alarms to be sent to the trap destination. Possible values: Critical, Major, Minor, Warning, Informational Default value: SNMP_SEV_UNKNOWN

Example

set snmp trap generic 192.168.3.4 -version V1

Related Commands

add snmp trap

rm snmp trap

unset snmp trap

show snmp trap

unset snmp trap

Synopsis

```
unset snmp trap <trapClass> <trapDestination> [-
destPort] [-version] [-communityName] [-srcIP] [-
severity]
```

Description

Unset the SNMP version of trap PDU and source IP of SNMP traps for configured trap destinations..Refer to the set snmp trap command for meanings of the arguments.

Example

unset snmp trap generic 192.168.3.4 -version

Related Commands

add snmp trap

rm snmp trap

set snmp trap

show snmp trap

show snmp trap

Synopsis

```
show snmp trap [<trapClass>  <trapDestination>]
```

Description

Display the IP addresses of the SNMP managers to which the system sends traps and the version of the PDU to be used for these destinations.

Arguments

trapClass
The trap type. Possible values: generic, specific

summary

fullValues

format

level

Output

destPort
The destination port of the SNMP trap.

version
The SNMP version of the trap to be sent.

communityName
SNMP trap community string

srcIP
The source IP of the SNMP trap to be sent.

severity
The minimum severity of traps to be sent to this destination.

Example

show snmp trap

Related Commands

add snmp trap

rm snmp trap

set snmp trap

unset snmp trap

add snmp group

Synopsis

```
add snmp group <name> <securityLevel> -readViewName
<string>
```

Description

Use this command to add an snmp group.

Arguments

`name`

The name of the SNMP group.

`securityLevel`

The security level of the group. Possible values: noAuthNoPriv, authNoPriv, authPriv

`readViewName`

The name of the read view associated with this view.

Related Commands

rm snmp group

set snmp group

show snmp group

rm snmp group

Synopsis

```
rm snmp group <name> <securityLevel>
```

Description

Use this command to delete an snmp group.

Arguments

name

The name of the SNMP group.

securityLevel

The security level of the group. Possible values: noAuthNoPriv, authNoPriv, authPriv

Related Commands

add snmp group

set snmp group

show snmp group

set snmp group

Synopsis

```
set snmp group <name> <securityLevel> -readViewName
<string>
```

Description

Use this command to set snmp group parameters.

Arguments

name

The name of the SNMP group.

securityLevel

The security level of the group. Possible values: noAuthNoPriv, authNoPriv, authPriv

readViewName

The name of the read view associated with this view.

Related Commands

add snmp group

rm snmp group

show snmp group

show snmp group

Synopsis

```
show snmp group [<name>  <securityLevel>]
```

Description

Display the configured SNMP groups.

Arguments

`name`

The name of the SNMP group.

`securityLevel`

The security level of the group. Possible values: noAuthNoPriv, authNoPriv, authPriv

`summary`

`fullValues`

`format`

`level`

Output

`readViewName`

The name of the read view associated with this view.

`storageType`

The storage type for this group.

`status`

The status of this group.

Related Commands

add snmp group

rm snmp group

set snmp group

add snmp view

Synopsis

```
add snmp view <name> <subtree> -type ( included |
excluded )
```

Description

Use this command to add an snmp view.

Arguments

name

The name of the SNMP view.

subtree

The subtree which is a part of the view.

type

The sutree needs to be included or excluded. Possible values: included, excluded

Related Commands

rm snmp view

set snmp view

show snmp view

rm snmp view

Synopsis

```
rm snmp view <name> <subtree>
```

Description

Use this command to delete an snmp view.

Arguments

name

The name of the SNMP view.

subtree

The subtree which is a part of the view.

Related Commands

add snmp view

set snmp view

show snmp view

set snmp view

Synopsis

```
set snmp view <name> <subtree> -type ( included |
excluded )
```

Description

Use this command to set snmp view parameters.

Arguments

name

The name of the SNMP view.

subtree

The subtree which is a part of the view.

type

The sutree needs to be included or excluded. Possible values: included, excluded

Related Commands

add snmp view

rm snmp view

show snmp view

show snmp view

Synopsis

```
show snmp view [<name>  [<subtree>]]
```

Description

Display the configured SNMP views.

Arguments

name

The name of the SNMP view.

summary

fullValues

format

level

Output

type

The type of sutree.

storageType

The storage type for this view.

status

The status of this view.

Related Commands

add snmp view

rm snmp view

set snmp view

add snmp user

Synopsis

```
add snmp user <name> -group <string> [-authType ( MD5 |
SHA )  {-authPasswd }  [-privType ( DES | AES )  {-
privPasswd }]]
```

Description

Use this command to create a SNMP user.

Arguments

name

The name of the SNMP user.

group

The name of the group to which user belongs.

authType

The authentication type. Possible values: MD5, SHA

privType

The encryption type. Possible values: DES, AES

Related Commands

rm snmp user

set snmp user

unset snmp user

show snmp user

rm snmp user

Synopsis

```
rm snmp user <name>
```

Description

Use this command to delete an SNMP user.

Arguments

name

The name of the SNMP user.

Related Commands

add snmp user

set snmp user

unset snmp user

show snmp user

set snmp user

Synopsis

```
set snmp user <name> [-group <string>] [-authType ( MD5 | SHA )  {-authPasswd }] [-privType ( DES | AES )  {-privPasswd }]
```

Description

Use this command to set parameters of an SNMP user.

Arguments

name

The name of the SNMP user.

group

The name of the group to which user belongs.

authType

The authentication type. Possible values: MD5, SHA

privType

The encryption type. Possible values: DES, AES

Related Commands

add snmp user

rm snmp user

unset snmp user

show snmp user

unset snmp user

Synopsis

```
unset snmp user <name> (-authType | -privType) [-
authPasswd] [-privPasswd]
```

Description

Use this command to unset parameters of an SNMP user..Refer to the set snmp user command for meanings of the arguments.

Related Commands

add snmp user

rm snmp user

set snmp user

show snmp user

show snmp user

Synopsis

```
show snmp user [<name>]
```

Description

Display configured SNMP users.

Arguments

name
The name of the SNMP user.

summary

fullValues

format

level

Output

group
The name of the group to which user belongs.

authType
The authentication type.

privType
The encryption type.

engineID
The context engine ID of the user.

storageType
The storage type for this user.

status
The status of this user.

Related Commands

add snmp user

rm snmp user

set snmp user

unset snmp user

set snmp engineId

Synopsis

```
set snmp engineId <engineID>
```

Description

Use this command to set the SNMP engine ID.

Arguments

engineID

The engine ID of the SNMP agent. Maximum value: 31

Related Commands

unset snmp engineId

show snmp engineId

unset snmp engineId

Synopsis

```
unset snmp engineId
```

Description

Use this command to unset the SNMP engine ID..Refer to the set snmp engineId command for meanings of the arguments.

Related Commands

set snmp engineId

show snmp engineId

show snmp engineId

Synopsis

```
show snmp engineId
```

Description

Use this command to display the SNMP engine ID.

Arguments

format

level

Output

engineID

The engine ID of the SNMP agent.

Related Commands

set snmp engineId

unset snmp engineId

CHAPTER 26

SSL Commands

This chapter covers the SSL commands.

create ssl wrapkey

Synopsis

```
create ssl wrapkey <wrapKeyName> -password <string> -
salt <string>
```

Description

Generate a wrap key.

Arguments

wrapKeyName

The object name for the wrap key.

password

The password string for the wrap key.

salt

The salt string for the wrap key.

Example

create wrapkey wrap1 -password wrapkey123 -salt wrapsalt123

Related Commands

rm ssl wrapkey

show ssl wrapkey

create ssl rsakey

Synopsis

```
create ssl rsakey <keyFile> <bits> [-exponent ( 3 | F4 )] [-keyform ( DER | PEM )] [-des] [-des3] [-password <string>]
```

Description

Generate an RSA key.

Arguments

keyFile

The file in which the generated RSA key is stored. The default output path for the key file is /nsconfig/ssl/. Maximum value: 64 -1

bits

The bit value (key length) for the RSA key. Minimum value: 512 Maximum value: 4096

exponent

The public exponent value for the RSA key. The supported values are F4 (Hex: 0x10001) or 3 (Hex: 0x3). Possible values: 3, F4 Default value: FIPSEXP_F4

keyform

The format for the key file: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

des

Encrypt the generated RSA key using DES algorithm. You will be prompted to enter the pass-phrase (password) that will be used to encrypt the key.

des3

Encrypt the generated RSA key using the Triple-DES algorithm. You will be prompted to enter the pass-phrase (password) that will be used to encrypt the key.

password
The pass-phrase to use for encryption if '-des' or '-des3' option is selected.
Maximum value: 32 -1

Example

create ssl rsakey /nsconfig/ssl/rsa1024.pem 1024 -exp F4

Related Commands

create ssl cert

create ssl certreq

add ssl certkey

convert ssl pkcs12

Synopsis

```
convert ssl pkcs12 <outfile> [-import  [-pkcs12File
<input_filename>]  [-des | -des3] ] [-export  [-
certFile <input_filename>]  [-keyFile
<input_filename>]]
```

Description

Convert the end-user certificate (Client-certificate/Server-Certificate) from PEM encoding format to PKCS#12 format. These certificates can then be distributed and installed in browsers as Client certificates.

Arguments

outfile

The output file to be generated. If the -import option is used, this file will be used to store the certificate and the private-key in PEM format. If the -export option is used, the certificate and private-key will be stored in the PKCS12 format. The default output path for the file is /nsconfig/ssl/. Maximum value: 64 -1

import

Convert the certificate and private-key from PKCS12 format to PEM format.

export

Convert the certificate and private-key from PEM format to PKCS12 format. Note: During the export operation, you will be prompted to enter the 'Export password'

Example

1)convert ssl pkcs12 /nsconfig/ssl/client_certkey.p12 -export -cert / nsconfig/ssl/client_certcert.pem -key /nsconfig/ssl/client_key.pem The above example CLI command converts the PEM encoded certificate and key file to PKCS#12. 2)convert ssl pkcs12 /nsconfig/ssl/client_certkey.pem -import -pkcs12 /nsconfig/ssl/client_certcertkey.p12 The above example CLI command converts the PKCS12 file to PEM format. 3)convert ssl pkcs12 / nsconfig/ssl/client_certkey.pem -import -pkcs12 /nsconfig/ssl/

client_certcertkey.p12 -des The above example CLI command converts the PKCS12 file to PEM format, with encrypted key. Note:The -des option will encrypt the output key using DES algorithm. User will be prompted to enter the pass-phrase to be used for encryption.

Related Commands

create ssl rsakey

create ssl dsakey

create ssl certreq

create ssl cert

convert ssl pkcs8

Synopsis

```
convert ssl pkcs8 <pkcs8File> <keyFile> [-keyform ( DER | PEM )] [-password <string>]
```

Description

Convert a PEM or DER encoded key file to PKCS#8 format before importing it into the System's FIPS system.

Arguments

`pkcs8File`
The name of the output file where the PKCS8 format key file will be stored. The default output path for the PKCS8 file is /nsconfig/ssl/. Maximum value: 64 -1

`keyFile`
The input key file. The default input path for the key file is /nsconfig/ssl/. Maximum value: 64 -1

`keyform`
The format of the keyFile. PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

`password`
The password if the key is encrypted. Valid for PEM encoded files only. Maximum value: 32 -1

Example

convert ssl pkcs8 /nsconfig/ssl/key.pk8 /nsconfig/ssl/key.pem

Related Commands

create ssl fipsKey

Synopsis

```
create ssl fipsKey <fipsKeyName> -modulus
<positive_integer> [-exponent ( 3 | F4 )]
```

Description

Generate a FIPS key within the Hardware Security Module (HSM)-FIPS card.

Arguments

fipsKeyName

The object name for the FIPS key.

modulus

The modulus of the key to be created. The modulus value should be a multiple of 64. Minimum value: 512 Maximum value: 2048

exponent

The exponent value for the key to be created. 3: Hex value 0x3 F4: Hex value 0x10001 Possible values: 3, F4 Default value: 3

Example

create fipskey fips1 -modulus 1024 -exp f4

Related Commands

rm ssl fipsKey

show ssl fipsKey

import ssl fipsKey

export ssl fipsKey

create ssl dhParam

Synopsis

```
create ssl dhParam [<dhFile>] [<bits>] [-gen ( 2 | 5 )]
```

Description

Generate the Diffie-Hellman (DH) parameters.

Arguments

dhFile

The name of the output file where the generated DH parameter is stored. Maximum value: 64 -1

bits

The bit value for the DH parameters. Minimum value: 512 Maximum value: 2048

gen

The DH generator value (g) to be used. Possible values: 2, 5 Default value: 2

Example

1)create ssl dhparam /nsconfig/ssl/dh1024.pem 1024 -gen 5

Related Commands

set ssl vserver

show ssl vserver

create ssl dsaKey

Synopsis

```
create ssl dsaKey <keyFile> <bits> [-keyform ( DER |
PEM )] [-des] [-des3] {-password }
```

Description

Generate a DSA key.

Arguments

keyFile

The name of the output file where the generated DSA key is stored. The default output path for the DH file is /nsconfig/ssl/. Maximum value: 64 -1

bits

The bit value (key length) for the DSA key. Minimum value: 512 Maximum value: 2048

keyform

The format of the key file: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule. Possible values: DER, PEM Default value: FORMAT_PEM

des

Encrypt the generated DSA key using the DES algorithm. It prompts you to enter the pass-phrase (password) that is used to encrypt the key.

des3

Encrypt the generated DSA key using Triple-DES algorithm. You will be prompted to enter the pass-phrase (password) that is used to encrypt the key.

password

The pass-phrase to use for encryption if '-des' or '-des3' option is selected. Maximum value: 32 -1

Example

create ssl dsakey /nsconfig/ssl/dsa1024.pem 1024

Related Commands

create ssl cert

create ssl certreq
add ssl certkey

show ssl certLink

Synopsis

```
show ssl certLink
```

Description

Display all the linked certificate-key pairs in the system.

Arguments

summary

fullValues

Output

certkeyName
Certificate key name.

linkCertKeyName
Name of the Certificate-Authority.

Example

The following shows an example of the output of the show ssl certlink command: linked certificate: 1) Cert Name: siteAcertkey CA Cert Name: CAcertkey

Related Commands

link ssl certkey

unlink ssl certkey

create ssl crl

Synopsis

```
create ssl crl <CAcertFile> <CAkeyFile> <indexFile> (-
revoke <input_filename> | -genCRL <output_filename>) [-
password <string>]
```

Description

Revoke a certificate or list of certificates or generate a CRL for the list of certificates that are revoked.

Arguments

`CAcertFile`

Path to the CA certificate file. The default input path for the CA certificate is /nsconfig/ssl/. Maximum value: 64 -1

`CAkeyFile`

Path to the CA key file. The default input path for the CA key is /nsconfig/ssl/. Maximum value: 64 -1

`indexFile`

This file contains the serial number of all the certificates that are revoked. This file is created the first time. New certificate revocation will be added to it subsequently. The default input path for the index file is /nsconfig/ssl/. Maximum value: 64 -1

`revoke`

The certificate file to be revoked. The default input path for the certificate(s) is /nsconfig/ssl/. Maximum value: 64 -1

`genCRL`

The CRL file to be created. The list of certificates that have been revoked is obtained from the index file. The default output path for the CRL file is /var/netscaler/ssl/. Maximum value: 64 -1

`password`

The password for the CA key file. Maximum value: 32 -1

Example

1)create crl /nsconfig/ssl/cacert.pem /nsconfig/ssl/cakey.pem /nsconfig/ssl/index.txt -gencrl /var/netscaler/ssl/crl.pem

Related Commands

add ssl crl

rm ssl crl

set ssl crl

unset ssl crl

show ssl crl

create ssl certReq

Synopsis

```
create ssl certReq <reqFile> [-keyFile
<input_filename>] [-fipsKeyName <string>] [-keyform (
DER | PEM )]
```

Description

Generate a new Certificate Signing Request (CSR). The generated CSR can be sent to a Certificate-Authority (CA) to obtain an X509 certificate for the user domain (web site).

Arguments

reqFile

The file name where the generated Certificate Signing Requests are stored. The default output path for the CSR file is /nsconfig/ssl/. Maximum value: 64 -1

keyFile

The key file name to be used. The key can be an RSA or a DSA key. The default input path for the key file is /nsconfig/ssl/. Maximum value: 64 -1

fipsKeyName

The FIPS key name to be used. FIPS keys are created inside the FIPS HSM (Hardware Security Module). This is applicable only to the SSL FIPS system. Maximum value: 31

keyform

The format for the input key file specified in the keyFileName: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule The command prompts the user for information that is incorporated in the Certificate Signing Request. For example, this information forms the Distinguished Name (DN) for the domain or the site. Country Name - Two letter ISO code for your country. For example, US for United States. State or Province Name - Full name for the state or province where your organization is located. Do not abbreviate. Locality Name - Name of the city or town in which your organization's head office is located. Organization Name - Name of the organization. The organization name (corporation, limited partnership,

university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which the organization is registered. Do not abbreviate the organization name and do not use the following characters in the name: < > ~ ! @ # 0 ^ * / ( )?. Organization Unit Name - Division or Section name in the organization that will use the certificate. Common Name - Fully qualified domain name for the company/Web site. The common name is the fully qualified domain name (FQDN) for the company/Web site. The common name must match the name used by DNS servers to do a DNS lookup of your server (for example, www.mywebsite.com <http://www.mywebsite.com>). Most browsers use this information for authenticating the server's certificate during the SSL handshake. If the server name does not match the common name as given in the server certificate, the browsers will terminate the SSL handshake or prompt the user with a warning message. CAUTION: Do not use wildcard characters such as * or ? and do not use an IP address as the common name. The common name should be without the protocol specifier <http://> or <https://>. Challenge Password - Challenge password for this certificate. Optional Company Name - Additional name of the company/web-site. Challenge Password - The contact person's E-mail address. Note: If the input key specified is an encrypted key, the user will be prompted to enter the PEM pass-phrase that was used to encrypt the key. Possible values: DER, PEM Default value: FORMAT_PEM

Example

create ssl certreq /nsconfig/ssl/csr.pem -keyFile /nsconfig/ssl/rsa1024.pem

Related Commands

create ssl cert

create ssl rsakey

create ssl dsakey

create ssl cert

Synopsis

```
create ssl cert <certFile> <reqFile> <certType> [-
keyFile <input_filename>] [-keyform ( DER | PEM )] [-
days <positive_integer>] [-certForm ( DER | PEM )] [-
CAcert <input_filename>] [-CAcertForm ( DER | PEM )] [-
CAkey <input_filename>] [-CAkeyForm ( DER | PEM )] [-
CAserial <output_filename>]
```

Description

Generate a signed X509 Certificate.

Arguments

certFile

The name of the generated certificate file. The default path of the certificate file is /nsconfig/ssl/. Maximum value: 64 -1

reqFile

The Certificate Signing Request (CSR) file that is used to generate the certificate. This file is created using the "create ssl certreq" command or an existing CSR. The default input path for the CSR file is /nsconfig/ssl/. Maximum value: 64 -1

certType

The type of the certificate to be generated. ROOT_CERT : The certificate generated will be a self-signed Root-CA certificate. For this, you need to specify the -keyfile parameter. The generated Root-CA certificate can be used for signing end-user certificates (Client/Server) or to create Intermediate-CA certificates. INTM_CERT : The certificate generated will be an Intermediate-CA certificate. For this, you need to specify the following parameters: -CAcert , -CAkey, and -CAserial. NOTE:The three parameters are also mandatory for the CLNT_CERT or SRVR_CERT certificate types. CLNT_CERT : The certificate generated will be an end-user client certificate. This can be used in a Client-Authentication setup. SRVR_CERT : The certificate generated will be an end-user Server certificate. This can be used as an SSL server certificate on the backend SSL servers for an SSL backend-

encryption setup with the system. NOTE:Avoid using the Server certificate (generated above) for a front-end SSL virtual server (or SSL service) on a system or on any frontend SSL server if the certificate is signed by System. The same is true with System generated Intermediate-CA or Root-CA certificate. The reason being, the System generated CA certificates will not be present in browsers (such as IE, Netscape, and other browsers) by default. So during the SSL handshake the Server Certificate verification will fail. Browsers generally display a warning message and prompt the user to either continue with the SSL handshake or terminate it. If the System generated CA certificates are installed in the browsers as trusted CA certificates, the SSL handshake will proceed without any errors or warnings. Possible values: ROOT_CERT, INTM_CERT, CLNT_CERT, SRVR_CERT

keyFile

The input keyFile to sign the certificate being generated. This keyFile is created using the "create ssl rsakey" or "create ssl dsakey" commands, or an existing RSA/DSA key. This file is required only when creating a self-signed Root-CA certificate. The default input path for the keyFile is /nsconfig/ssl/. Note: If the input key specified is an encrypted key, the user will be prompted to enter the PEM pass-phrase that was used for encrypting the key. Maximum value: 64 -1

keyform

The format for the input key file: PEM : Privacy Enhanced Mail DER : Distinguished Encoding Rule. Possible values: DER, PEM Default value: FORMAT_PEM

days

The number of days for which the certificate will be valid. The certificate is valid from the time and day (system time) of the creation, to the number of days specified in the -days field. Default value: 365 Minimum value: 1

certForm

The output certificate format: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

CAcert

The CA certificate file that will issue and sign the Intermediate-CA certificate or the end-user certificates (Client/Server). The default input path for the CA certificate file is /nsconfig/ssl/. Maximum value: 64 -1

CAcertForm

The format of the input CA certificate file: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

CAkey

The CA key file that will be used to sign the Intermediate-CA certificate or the end-user certificates (Client/Server). The default input path for the CA key file is /nsconfig/ssl/. Note: If the CA key file is password protected, the user will be prompted to enter the pass-phrase used for encrypting the key. Maximum value: 64 -1

CAkeyForm

The format of the input CA key file: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

CAserial

The Serial number file maintained for the CA certificate. This will contain the serial number of the next certificate to be issued/signed by the CA (-CAcert). If the specified file does not exist, a new file will be created. The default input path for the CAserial file name is /nsconfig/ssl/. Note: Specify the proper path of the existing serial file; else a new serial file will be created. This may change the certificate serial numbers assigned by the CA certificate to each of the certificate it signs. Maximum value: 64 -1

Example

1) create ssl cert /nsconfig/ssl/root_cert.pem /nsconfig/ssl/root_csr.pem ROOT_CERT -keyFile /nsconfig/ssl/root_key.pem -days 1000 The above example creates a self signed Root-CA certificate. 2) create ssl cert /nsconfig/ssl/server_cert.pem /nsconfig/ssl/server_csr.pem SRVR_CERT -CAcert /nsconfig/ssl/root_cert.pem -CAkey /nsconfig/ssl/root_key.pem -CAserial /nsconfig/ssl/root.srl The above example creates a Server certificate which is signed by the Root-CA certificate: root_cert.pem

Related Commands

create ssl certreq

create ssl rsakey

create ssl dsakey

add ssl certkey

stat ssl

Synopsis

```
stat ssl [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display ssl statistics.

Arguments

Output

Counters

 # SSL cards UP (SSLCardUP)

Number of ssl cards UP. If number of cards UP is lower than a threshold, a failover will be initiated.

SSL crypto card status (SSLCardSt)

Status of the SSL card (1=UP, 0=DOWN)

 # SSL cards present (SSLCards)

Number of SSL crypto cards present in the system

SSL engine status (SSLEngSt)

Status of the SSL Engine (1=UP/0=DOWN). This state is decided based on SSL Feature/License status and minimum number of cards UP

SSL sessions (SSLSe)

Number of SSL sessions

SSL transactions (SSLTrn)

Number of SSL transactions

SSLv2 transactions (SSL2Trn)

Number of SSLv2 transactions

SSLv3 transactions (SSL3Trn)

Total number of SSLv3 Transactions.

TLSv1 transactions (TLS1Trn)
Number of TLSv1 transactions

SSLv2 sessions (SSL2Se)
Number of SSLv2 sessions

SSLv3 sessions (SSL3Se)
Number of SSLv3 sessions

TLSv1 sessions (TLS1Se)
Number of TLSv1 sessions

new SSL sessions (NewSe)
Number of new SSL sessions created.

SSL session misses (SeMiss)
Number of SSL session reuse misses

SSL session hits (SeHit)
Number of SSL session reuse hits

SSL sessions (BSSLSe)
Number of Backend SSL sessions

SSLv3 sessions (BSSL3Se)
Number of Backend SSLv3 sessions

TLSv1 sessions (BTLS1Se)
Number of Backend TLSv1 sessions

Session multiplex attempts (BSeMx)
Number of Backend SSL session multiplex attempts

Session multiplex successes (BSeMxS)
Number of Backend SSL session multiplex successes

Session multiplex failures (BSeMxF)
Number of Backend SSL session multiplex failures

Bytes encrypted (Enc)
Number of bytes encrypted

Bytes decrypted (Dec)
Number of bytes decrypted

SSL session renegotiations (SSLRn)
Number of SSL session renegotiations

SSLv3 session renegotiations (SSL3Rn)
Number of session renegotiations done on SSLv3

TLSv1 session renegotiations (TLS1Rn)
Number of SSL session renegotiations done on TLSv1

RSA 512-bit key exchanges (RSAKx5)
Number of RSA 512-bit key exchanges

RSA 1024-bit key exchanges (RSAKx1)
Number of RSA 1024-bit key exchanges

RSA 2048-bit key exchanges (RSAKx2)
Number of RSA 2048-bit key exchanges

RSA 4096-bit key exchanges (RSAKx4)
Number of RSA 4096-bit key exchanges

DH 512-bit key exchanges (DHKx5)
Number of Diffie-Helman 512-bit key exchanges

DH 1024-bit key exchanges (DHKx1)
Number of Diffie-Helman 1024-bit key exchanges

DH 2048-bit key exchanges (DHKx2)
Number of Diffie-Helman 2048-bit key exchanges

RC4 40-bit encryptions (RC4En4)
Number of RC4 40-bit cipher encryptions

RC4 56-bit encryptions (RC4En5)
Number of RC4 56-bit cipher encryptions

RC4 64-bit encryptions (RC4En6)
Number of RC4 64-bit cipher encryptions

RC4 128-bit encryptions (RC4En1)
Number of RC4 128-bit cipher encryptions

DES 40-bit encryptions (DESEn4)
Number of DES 40-bit cipher encryptions

DES 56-bit encryptions (DESEn5)
Number of DES 56-bit cipher encryptions

3DES 168-bit encryptions (3DESEn1)
Number of DES 168-bit cipher encryptions

AES 128-bit encryptions (AESEn1)
Number of AES 128-bit cipher encryptions

AES 256-bit encryptions (AESEn2)
Number of AES 256-bit cipher encryptions

RC2 40-bit encryptions (RC2En4)
Number of RC2 40-bit cipher encryptions

RC2 56-bit encryptions (RC2En5)
Number of RC2 56-bit cipher encryptions

RC2 128-bit encryptions (RC2En1)
Number of RC2 128-bit cipher encryptions

IDEA 128-bit encryptions (IDEAEn1)
Number of IDEA 128-bit cipher encryptions

Null cipher encryptions (NullEn)
Number of Null cipher encryptions

MD5 hashes (MD5Hsh)
Number of MD5 hashes

SHA hashes (SHAHsh)
Number of SHA hashes

SSLv2 SSL handshakes (SSL2Hs)
Number of handshakes on SSLv2

SSLv3 SSL handshakes (SSL3Hs)
Number of handshakes on SSLv3

TLSv1 SSL handshakes (TLS1Hs)
Number of SSL handshakes on TLSv1

SSLv2 client authentications (SSL2CAt)
Number of client authentications done on SSLv2

SSLv3 client authentications (SSL3CAt)
Number of client authentications done on SSLv3

TLSv1 client authentications (TLS1CAt)
Number of client authentications done on TLSv1

RSA authentications (RSAAt)
Number of RSA authentications

DH authentications (DHAt)
Number of Diffie-Helman authentications

DSS (DSA) authentications (DSSAt)
Total number of times DSS authorization used.

Null authentications (NullAt)
Number of Null authentications

SSL session renegotiations (BSSLRn)
Number of Backend SSL session renegotiations

SSLv3 session renegotiations (BSSL3Rn)
Number of Backend SSLv3 session renegotiations

TLSv1 session renegotiations (BTLS1Rn)
Number of Backend TLSv1 session renegotiations

RSA 512-bit key exchanges (BRSAKx5)
Number of Backend RSA 512-bit key exchanges

RSA 1024-bit key exchanges (BRSAKx1)
Number of Backend RSA 1024-bit key exchanges

RSA 2048-bit key exchanges (BRSAKx2)
Number of Backend RSA 2048-bit key exchanges

DH 512-bit key exchanges (BDHKx5)
Number of Backend DH 512-bit key exchanges

DH 1024-bit key exchanges (BDHKx1)
Number of Backend DH 1024-bit key exchanges

DH 2048-bit key exchanges (BDHKx2)
Number of Backend DH 2048-bit key exchanges

RC4 40-bit encryptions (BRC4En4)
Number of Backend RC4 40-bit cipher encryptions

RC4 56-bit encryptions (BRC4En5)
Number of Backend RC4 56-bit cipher encryptions

RC4 64-bit encryptions (BRC4En6)
Number of Backend RC4 64-bit cipher encryptions

RC4 128-bit encryptions (BRC4En1)
Number of Backend RC4 128-bit cipher encryptions

DES 40-bit encryptions (BDESEn4)
Number of Backend DES 40-bit cipher encryptions

DES 56-bit encryptions (BDESEn5)
Number of Backend DES 56-bit cipher encryptions

3DES 168-bit encryptions (B3DESE1n)
Number of Backend 3DES 168-bit cipher encryptions

AES 128-bit encryptions (BAESEn1)
Backend AES 128-bit cipher encryptions

AES 256-bit encryptions (BAESEn2)
Backend AES 256-bit cipher encryptions

RC2 40-bit encryptions (BRC2En4)
Number of Backend RC2 40-bit cipher encryptions

RC2 56-bit encryptions (BRC2En5)
Number of Backend RC2 56-bit cipher encryptions

RC2 128-bit encryptions (BRC2En1)
Number of Backend RC2 128-bit cipher encryptions

IDEA 128-bit encryptions (BIDEAEn1)
Number of Backend IDEA 128-bit cipher encryptions

null encryptions (BNullEn)
Number of Backend null cipher encryptions

MD5 hashes (BMD5Hsh)
Number of Backend MD5 hashes

SHA hashes (BSHAHsh)
Number of Backend SHA hashes

SSLv3 handshakes (BSSL3Hs)
Number of Backend SSLv3 handshakes

TLSv1 handshakes (BTLS1Hs)
Number of Backend TLSv1 handshakes

SSLv3 client authentications (BSSL3CAt)
Number of Backend SSLv3 client authentications

TLSv1 client authentications (BTLS1CAt)
Number of Backend TLSv1 client authentications

RSA authentications (BRSAAt)
Number of Backend RSA authentications

DH authentications (BDHAt)
Number of Backend DH authentications

DSS authentications (BDSSAt)
Number of Backend DSS authentications

Null authentications (BNullAt)
Number of Backend null authentications

RSA key exchanges offloaded (RSAkxOf)
Number of RSA key exchanges offloaded to crypto card

RSA sign operations offloaded (RSASnOf)
Number of RSA sign operations offloaded to crypto card

DH key exchanges offloaded (DHkxOf)
Number of DH key exchanges offloaded to crypto card

RC4 encryptions offloaded (RC4EnOf)
Number of RC4 encryptions offloaded to crypto card

DES encryptions offloaded (DESEnOf)
Number of DES encryptions offloaded to crypto card

AES encryptions offloaded (AESEnOf)
Number of AES encryptions offloaded to crypto card

Bytes encrypted in hardware (EncHw)
Number of bytes encrypted in hardware

Bytes encrypted in software (EncSw)
Number of bytes encrypted in software

Bytes encrypted on front-end (EncFe)
Number of bytes encrypted on front-end

Bytes encrypted in hardware on front-end (EncHwFe)
Number of bytes encrypted in hardware on front-end

Bytes encrypted in software on front-end (EncSwFe)
Number of bytes encrypted in software on front-end

Bytes encrypted on back-end (EncBe)
Number of bytes encrypted on back-end

Bytes encrypted in hardware on back-end (EncHwBe)
Number of bytes encrypted in hardware on back-end

Bytes encrypted in software on back-end (EncSwBe)
Number of bytes encrypted in software on back-end

Bytes decrypted in hardware (DecHw)
Number of bytes decrypted in hardware

Bytes decrypted in software (DecSw)
Number of bytes decrypted in software

Bytes decrypted on front-end (DecFe)
Number of bytes decrypted on front-end

Bytes decrypted in hardware on front-end (DecHwFe)
Number of bytes decrypted in hardware on front-end

Bytes decrypted in software on front-end (DecSwFe)
Number of bytes decrypted in software on front-end

Bytes decrypted on back-end (DecBe)
Number of bytes decrypted on back-end

Bytes decrypted in hardware on back-end (DecHwBe)
Number of bytes decrypted in hardware on back-end

Bytes decrypted in software on back-end (DecSwBe)
Number of bytes decrypted in software on back-end

Backend SSL sessions reused (BSeRe)
Number of Backend SSL sessions reused

Related Commands

show ssl stats

Synopsis

```
show ssl stats - alias for 'stat ssl'
```

Description

show ssl stats is an alias for stat ssl

Related Commands

stat ssl

bind ssl cipher

Synopsis

```
bind ssl cipher (<vServerName>@ | <serviceName>@ |
<serviceGroupName>@) [-vServer | -service]
<cipherOperation> <cipherAliasName/cipherName/
cipherGroupName>
```

Description

Change the default cipher-suite defined for an SSL virtual server. By default, the predefined cipher alias on the system is bound to all SSL virtual servers. The DEFAULT alias contains all ciphers with encryption strength >=128bit. Note:To view the individual ciphers in the alias DEFAULT, use the show ssl cipher DEFAULT CLI command

Arguments

vServerName

The name of the SSL virtual server to which the cipher-suite is to be bound.

serviceName

The name of the SSL service name to which the cipher-suite is to be bound.

serviceGroupName

The name of the SSL service name to which the cipher-suite is to be bound.

cipherOperation

The operation that is performed when adding the cipher-suite. Possible cipher operations are: ADD - Appends the given cipher-suite to the existing one configured for the virtual server. REM - Removes the given cipher-suite from the existing one configured for the virtual server. ORD - Overrides the current configured cipher-suite for the virtual server with the given cipher-suite. Possible values: ADD, REM, ORD

cipherAliasName/cipherName/cipherGroupName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

Example

1)bind ssl cipher sslvip ADD SSL3-RC4-SHA The above example appends the cipher SSL3-RC4-SHA to the cipher-suite already configured for the SSL virtual server sslvip. 2)bind ssl cipher sslvip REM NULL The above example removes the ciphers identified by the system's predefined cipher-alias -NULL from the cipher-suite already configured for the SSL virtual server sslvip. 3) bind ssl cipher sslvip ORD HIGH The above example overrides the existing cipher-suite configured for the SSL virtual server with ciphers, having HIGH encryption strength (ciphers supporting 168-bit encryption). Note: The individual ciphers contained in a system predefined cipher-alias can beviewed by using the following command: show ssl cipher <cipherAlaisName>

Related Commands

show ssl vserver

show ssl cipher

add ssl cipher

rm ssl cipher

show ssl cipher

Synopsis

```
show ssl cipher [<cipherAliasName/cipherName/
cipherGroupName>]
```

Description

Display the details of a cipher, cipher-group, or cipher-alias defined on the system. If no argument is specified, the command displays all the predefined cipher-aliases and user-defined cipher-groups on the system. If a cipher name is specified, the details of the cipher are displayed. If a user defined cipher-group name is specified, all the individual ciphers in the group are displayed along with the individual cipher description. If a system predefined cipher-alias name is specified, all the individual ciphers in the alias are displayed along with the individual cipher description.

Arguments

`cipherAliasName/cipherName/cipherGroupName`
cipherName: The individual cipher name. cipherGroupName: The user defined cipher-group name for which the cipher details are displayed. cipherAliasName: The system predefined cipher-alias name for which the cipher details aredisplayed.

`summary`

`fullValues`

`format`

`level`

Output

`cipherGroupName`
The name of cipher group/alias/individual cipher name.

`description`
Cipher suite description.

cipherName
Cipher name.

Example

1) An example of the output of the show ssl cipher SSL3-RC4-MD5 command is as follows: Cipher Name: SSL3-RC4-MD5 Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5 2) This example displays the details of individual ciphers in the system predefinedcipher-alias: SSLv2 (the command show ssl cipher SSLv2 has been entered): 8 configured cipher(s)in alias 1) Cipher Name: SSL2-RC4-MD5 Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5 2) Cipher Name: SSL2-EXP-RC4-MD5 Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export 3) Cipher Name: SSL2-RC2-CBC-MD5 Description: SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5 4) Cipher Name: SSL2-EXP-RC2-CBC-MD5 Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export 5) Cipher Name: SSL2-DES-CBC-MD5 Description: SSLv2 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5 6) Cipher Name: SSL2-DES-CBC3-MD5 Description: SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5 7) Cipher Name: SSL2-RC4-64-MD5 Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(64) Mac=MD5

Related Commands

bind ssl cipher

add ssl cipher

rm ssl cipher

add ssl certKey

Synopsis

```
add ssl certKey <certkeyName> -cert <string> [(-key
<string>  [-password]) | -fipsKey <string>] [-inform (
DER | PEM )] [-expiryMonitor ( ENABLED | DISABLED )  [-
notificationPeriod <positive_integer>]]
```

Description

Add a certificate-key pair object. Notes: 1)For server certificate-key pair, use both -cert and -key arguments. 2)The command ###bind ssl certkey###, used for binding a certificate-key pair to an SSL virtual server, fails if the certificate-key pair does not include the private key. 3)In an HA configuration, the certificate should be located as specified in the -cert <string> parameter, on both the primary and secondary nodes. If the optional parameter -key is used, the key must be located as specified in the -key <string> parameter.

Arguments

certkeyName

The name of the certificate and private-key pair.

cert

The file name and path for the X509 certificate file. The certificate file should be present on the system device (HDD). The default input path for the certificate file is /nsconfig/ssl/.

key

The file name and path for the private-key file. The private-key file should be present on the system device (HDD). The default input path for the key file is /nsconfig/ssl/. Notes: 1) This argument is optional when adding a Certificate-Authority (CA) certificate file. In this case the CA's private-key will not be available to the user. 2) The System's FIPS system does not support external keys (non-FIPS keys). On a System's FIPS system, you will not be able to load keys from a local storage device such as a hard disc or flash memory.

fipsKey
The name of the FIPS key. The FIPS key is created inside the FIPS HSM (Hardware Security Module). This is applicable only to the SSL FIPS system.

inform
The input format of the certificate and the private-key files. The two formats supported by the system are: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

expiryMonitor
Alert before the certificate is about to expire. Possible values: ENABLED, DISABLED Default value: DISABLED

notificationPeriod
Number of days in advance when an alert needs to be generated for a certificate which is about to expire. Default value: 30 Minimum value: 10 Maximum value: 100

Example

1)add ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem The above command loads a certificate and private key file. 2)add ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem -password Password: ******** The above command loads a certificate and private key file. Here the private key file is an encrypted key. 3)add ssl certkey fipscert -cert /nsconfig/ssl/cert.pem -fipskey fips1024 The above command loads a certificate and associates it with the corresponding FIPS key that resides within the HSM.

Related Commands

rm ssl certKey

set ssl certKey

unset ssl certKey

bind ssl certKey

unbind ssl certKey

link ssl certKey

unlink ssl certKey

show ssl certKey

update ssl certKey

rm ssl certKey

Synopsis

```
rm ssl certKey <certkeyName> ...
```

Description

Remove the specified certificate-key pair from the system.

Arguments

certkeyName

The name of the certificate-key pair. Note: The certificate-key pair is removed only when it is not referenced by any other object. The reference count is updated when the certificate-key pair is bound to an SSL virtual server (using the ###bind ssl certkey### command) or linked to another certificate-key pair (using the ###link ssl certkey### command).

Example

1)rm ssl certkey siteAcertkey The above command removes the certificate-key pair siteAcertkey from the system.

Related Commands

add ssl certKey

set ssl certKey

unset ssl certKey

bind ssl certKey

unbind ssl certKey

link ssl certKey

unlink ssl certKey

show ssl certKey

update ssl certKey

set ssl certKey

Synopsis

```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED
| DISABLED )  [-notificationPeriod <positive_integer>]]
```

Description

Change attributes of a certificate-key pair object.

Arguments

certkeyName

The name of the certificate and private-key pair.

expiryMonitor

Alert before the certificate is about to expire. Possible values: ENABLED, DISABLED Default value: DISABLED

Related Commands

add ssl certKey

rm ssl certKey

unset ssl certKey

bind ssl certKey

unbind ssl certKey

link ssl certKey

unlink ssl certKey

show ssl certKey

update ssl certKey

unset ssl certKey

Synopsis

```
unset ssl certKey <certkeyName> [-expiryMonitor] [-
notificationPeriod]
```

Description

Use this command to remove ssl certKey settings.Refer to the set ssl certKey command for meanings of the arguments.

Related Commands

add ssl certKey
rm ssl certKey
set ssl certKey
bind ssl certKey
unbind ssl certKey
link ssl certKey
unlink ssl certKey
show ssl certKey

update ssl certKey

bind ssl certKey

Synopsis

```
bind ssl certKey (<vServerName>@ | <serviceName>@ |
<serviceGroupName>@) [-vServer | -service]
<certkeyName> [-CA  [-crlCheck ( Mandatory | Optional
)]]
```

Description

Bind a certificate-key pair to an SSL virtual server or an SSL service

Arguments

vServerName

The name of the SSL virtual server name to which the certificate-key pair needs to be bound.

serviceName

The name of the SSL service to which the certificate-key pair needs to be bound. Use the ###add service### command to create this service.

serviceGroupName

The name of the SSL service group to which the certificate-key pair needs to be bound. Use the "add servicegroup" command to create this service.

certkeyName

The object name for the certificate-key pair.

CA

If this option is specified, it indicates that the certificate-key pair being bound to the SSL virtual server is a CA certificate. If this option is not specified, the certificate-key pair is bound as a normal server certificate. Note: In case of a normal server certificate, the certificate-key pair should consist of both the certificate and the private-key. Minimum value: 0

Example

1)bind ssl certkey sslvip siteAcertkey In the above example, the certificate-key pair siteAcertkey is bound to the SSL virtual sever as server certificate. 2) bind ssl certkey sslvip CAcertkey -CA In the above example, the certificate-

key pair CAcertkey is bound to the SSL virtual sever as CA certificate. 3)bind ssl certkey sslsvc siteAcertkey -service In the above example, the certificate-key pair CAcertkey is bound to the SSL Service as server certificate.

Related Commands

show ssl vserver
add ssl certKey
rm ssl certKey
set ssl certKey
unset ssl certKey
unbind ssl certKey
link ssl certKey
unlink ssl certKey
show ssl certKey

update ssl certKey

unbind ssl certKey

Synopsis

```
unbind ssl certKey (<vServerName>@ | <serviceName>@ |
<serviceGroupName>@) [-vServer | -service]
<certkeyName> [-CA]
```

Description

Unbind the certificate-key pair from the specified SSL vserver or SSL service. Use the "bind ssl certkey " command to bind the certificate-key pair to the specified SSL vserver or SSL service.

Arguments

vServerName
The name of the SSL virtual server.

serviceName
The name of the SSL service

serviceGroupName
The name of the service group.

certkeyName
The certificate-key object name that needs to be unbound from the SSL virtual server or SSL service.

CA
The certificate-key pair being unbound is a Certificate Authority (CA) certificate. If you choose this option, the certificate-key pair is unbound from the list of CA certificates that were bound to the specified SSL virtual server or SSL service.

Example

1)unbind ssl certkey sslvip siteAcertkey In the above example, the server certificate siteAcertkey is unbound from the SSL virtual server. 2) unbind ssl certkey sslvip CAcertkey -CA In the above example, the CA certificate CAcertkey is unbound from the SSL virtual server.

Related Commands

show ssl vserver
add ssl certKey
rm ssl certKey
set ssl certKey
unset ssl certKey
bind ssl certKey
link ssl certKey
unlink ssl certKey
show ssl certKey

update ssl certKey

link ssl certKey

Synopsis

```
link ssl certKey <certkeyName> <linkCertKeyName>
```

Description

Link a certificate-key pair to its Certificate Authority (CA) certificate-key pair. Note:The two certificate-key pairs are linked only if the certificate specified in the certKeyName parameter is issued by the Certificate-Authority specified in the linkCertKeyName parameter.

Arguments

certkeyName

The certificate-key name that is to be bound to its issuer certificate-key pair.

linkCertKeyName

The name of the Certificate-Authority.

Example

1)link ssl certkey siteAcertkey CAcertkey In the above example, the certificate-key siteAcertkey is bound to its issuer certificate-key pair CAcertkey.

Related Commands

show ssl certlink

add ssl certKey

rm ssl certKey

set ssl certKey

unset ssl certKey

bind ssl certKey

unbind ssl certKey

unlink ssl certKey

show ssl certKey

update ssl certKey

unlink ssl certKey

Synopsis

```
unlink ssl certKey <certkeyName>
```

Description

Unlink the certificate-key name from its Certificate-Authority (CA) certificate-key pair.

Arguments

certkeyName

The certificate-key object name that has to be unlinked from the CA certificate. The CA certificate name is taken internally.

Example

1)unlink ssl certkey siteAcertkey The above example unlinks the certificate 'siteAcertkey' from its Certificate-Authority (CA) certificate.

Related Commands

show ssl certlink

add ssl certKey

rm ssl certKey

set ssl certKey

unset ssl certKey

bind ssl certKey

unbind ssl certKey

link ssl certKey

show ssl certKey

update ssl certKey

show ssl certKey

Synopsis

```
show ssl certKey [<certkeyName>]
```

Description

Display the information pertaining to the certificate-key pairs configured on the system: 1)If no argument is specified, the command will display all the certificate-key pairs configured on the system. 2)If the certKeyName argument is specified, the command will display the details of the certificate.

Arguments

certkeyName
The certificate-key pair object name.

summary

fullValues

format

level

Output

cert
The name and location of the file containing the certificate.

key
The name and location of the file containing the key.

inform
The encoding format of the certificate and key (PEM or DER).

signatureAlg
Signature algorithm.

serial
Serial number.

issuer
Issuer name.

clientCertNotBefore
Not-Before date.

clientCertNotAfter
Not-After date.

daysToExpiration
Days remaining for the certificate to expire.

subject
Subject name.

publickey
Public key algorithm.

publickeysize
Size of the public key.

version
Version.

status
Status of the certificate.

fipsKey
FIPS key ID.

passcrypt
Passcrypt.

data
Vserver Id

serverName
Vserver name to which the certificate key pair is bound.

serviceName
Service name to which the certificate key pair is bound.

expiryMonitor
Certificate expiry monitor

notificationPeriod
Certificate expiry notification period

Example

1) An example of the output of the show ssl certkey command is shown below: 2 configured certkeys: 1)Name: siteAcertkey Cert Path: /nsconfig/ssl/siteA-cert.pem Key Path: /nsconfig/ssl/siteA-key.pem Format: PEM Status: Valid 2)Name: cert1 Cert Path: /nsconfig/ssl/server_cert.pem Key Path: /nsconfig/ssl/server_key.pem Format: PEM Status: Valid 2) An example of the output of the show ssl certkey siteAcertkey command is shown below: Name: siteAcertkeyStatus: Valid Version: 3 Serial Number: 02 Signature Algorithm: md5WithRSAEncryption Issuer: /C=US/ST=CA/L=Santa Clara/O=siteA/OU=Tech Validity Not Before: Nov 11 14:58:18 2001 GMT Not After: Aug 7 14:58:18 2004 GMT Subject: /C=US/ST-CA/L=San Jose/O=CA/OU=Security Public Key Algorithm: rsaEncryption Public Key size: 1024

Related Commands

add ssl certKey
rm ssl certKey
set ssl certKey
unset ssl certKey
bind ssl certKey
unbind ssl certKey
link ssl certKey
unlink ssl certKey

update ssl certKey

update ssl certKey

Synopsis

```
update ssl certKey <certkeyName> [-cert <string>] [(-
key <string>  [-password]) | -fipsKey <string>] [-
inform ( DER | PEM )] [-noDomainCheck]
```

Description

Update a certificate-key pair object. Notes: 1)In a HA configuration, the certificate should be located as specified in the -cert <string> parameter, on both the primary and secondary nodes. If the optional parameter -key is used, the key must be located as specified in the -key <string> parameter.

Arguments

certkeyName
The name of the certificate and private-key pair.

cert
The file name and pathfor the X509 certificate file. The certificate file should be present on the system device (HDD). The default input path for the certificate file is /nsconfig/ssl/.

key
The file name and pathfor the private-key file. The private-key file should be present on the system device (HDD). The default input path for the key file is /nsconfig/ssl/.

fipsKey
The name of the FIPS key. The FIPS key is created inside the FIPS HSM (Hardware Security Module). This is applicable only to the SSL FIPS system.

inform
The input format of the certificate and the private-key files. The two formats supported by the system are: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

noDomainCheck

Specify this option to override the check for matching domain names during certificate update operation

Example

1) update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key / nsconfig/ssl/pkey.pem The above command updates a certificate and private key file. 2) update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem -password Password: ******** The above command updates a certificate and private key file. Here the private key file is an encrypted key. 3) update ssl certkey mydomaincert The above command updates the certificate using the same parameters (-cert path/-key path) that it was added with.

Related Commands

add ssl certkey

rm ssl certkey

add ssl certKey

rm ssl certKey

set ssl certKey

unset ssl certKey

bind ssl certKey

unbind ssl certKey

link ssl certKey

unlink ssl certKey

show ssl certKey

add ssl cipher

Synopsis

```
add ssl cipher <cipherGroupName> <cipherAliasName/
cipherName/cipherGroupName> ...
```

Description

Create a user-defined cipher group or to add ciphers to an existing group. The cipher group can be used to set the cipher-suite of an SSL virtual server.

Arguments

cipherGroupName

The name of the user-defined cipher group. If the cipher group does not exist on the system, a new group is created with the specified name. The ciphers are added to this group. If a group identified by cipherGroupName already exists on the system, the ciphers are added to it.

cipherAliasName/cipherName/cipherGroupName

The individual cipher name(s), a user-defined cipher group, or a system predefined cipher alias that will be added to the predefined cipher alias that will be added to the group cipherGroupName. If a cipher alias or a cipher group is specified, all the individual ciphers in the cipher alias or group will be added to the user-defined cipher group.

Example

1)add ssl cipher mygroup SSL2-RC4-MD5 SSL2-EXP-RC4-MD5 The above command creates a new cipher-group by the name: mygroup, with the two ciphers SSL2-RC4-MD5 and SSL2-EXP-RC4-MD5, as part of the cipher-group. If a cipher-group by the name: mygroup already exists in system, then the two ciphers is added to the list of ciphers contained in the group. 2)add ssl cipher mygroup HIGH MEDIUM The above command creates a new cipher-group by the name: mygroup, with the ciphers from the cipher alias "HIGH" and "MEDIUM" as part of the cipher group. If a cipher-group by the name, mygroup, already exists in system, then the ciphers from the two aliases is added to the list of ciphers contained in the group.

Related Commands

bind ssl cipher

show ssl cipher

rm ssl cipher

rm ssl cipher

Synopsis

```
rm ssl cipher <cipherGroupName> [<cipherName> ...]
```

Description

Remove cipher(s) from a user-defined cipher group. It can also remove an entire cipher group from the system. If there is no cipherName included with the cipherGroupName, the cipher group specified by cipherGroupName is deleted. If there is a cipherName included, the specified cipher(s) are removed from the cipher group.

Arguments

`cipherGroupName`

The user defined cipher group on the system.

`cipherName`

The cipher(s) to be removed from the cipher group.

Example

1)rm ssl cipher mygroup SSL2-RC4-MD5 The above example removes the cipher SSL2-RC4-MD5 from the cipher group mygroup. 2)rm ssl cipher mygroup The above example will remove the cipher group 'mygroup' from the system.

Related Commands

bind ssl cipher

show ssl cipher

add ssl cipher

set ssl parameter

Synopsis

```
set ssl parameter [-quantumSize <quantumSize>] [-
crlMemorySizeMB <positive_integer>] [-strictCAChecks (
YES | NO )] [-sslTriggerTimeout <positive_integer>] [-
sendCloseNotify ( YES | NO )] [-encryptTriggerPktCount
<positive_integer>]
```

Description

Arguments

quantumSize
SSL quantum size Possible values: 4096, 8192, 16384 Default value: 8192

crlMemorySizeMB
Memory size to use for CRLs Default value: 256 Minimum value: 10 Maximum value: 1024

strictCAChecks
Enable strict CA certificate checks. Possible values: YES, NO Default value: NO

sslTriggerTimeout
Encryption trigger timer Default value: 100 Minimum value: 1 Maximum value: 200

sendCloseNotify
Enable sending SSL Close-Notify at the end of a transaction Possible values: YES, NO Default value: YES

encryptTriggerPktCount
Number of queued packets that force encryption to occur. Default value: 50 Minimum value: 10 Maximum value: 50

Related Commands

unset ssl parameter

show ssl parameter

unset ssl parameter

Synopsis

```
unset ssl parameter [-quantumSize] [-crlMemorySizeMB]
[-strictCAChecks] [-sslTriggerTimeout] [-
sendCloseNotify] [-encryptTriggerPktCount]
```

Description

Use this command to remove ssl parameter settings.Refer to the set ssl parameter command for meanings of the arguments.

Related Commands

set ssl parameter

show ssl parameter

show ssl parameter

Synopsis

```
show ssl parameter
```

Description

Display ssl advanced parameters.

Arguments

format

level

Output

quantumSize
SSL quantum size

crlMemorySizeMB
Memory size to use for CRLs

strictCAChecks
Memory size to use for CRLs

sslTriggerTimeout
Encryption trigger timer

sendCloseNotify
Enable sending SSL Close-Notify at the end of a transaction

encryptTriggerPktCount
Number of queued packets that force encryption to occur.

Related Commands

set ssl parameter

unset ssl parameter

add ssl crl

Synopsis

```
add ssl crl <crlName> <crlPath> [-inform ( DER | PEM )]
[-refresh ( ENABLED | DISABLED )] [-CAcert <string>] [-
method ( HTTP | LDAP )] [-server <ip_addr|ipv6_addr|*>
| -url <URL>] [-port <port>] [-baseDN <string>] [-scope
( Base | One )] [-interval <interval>] [-day <integer>]
[-time <HH:MM>] [-bindDN <string>] [-password <string>]
[-binary ( YES | NO )]
```

Description

Add a Certificate Revocation List (CRL) object. Note:In an HA configuration, the CRL on both the primary and secondary nodes must be present in the location specified by <crlPath>.

Arguments

`crlName`
The object name for the CRL.

`crlPath`
The file name and path for the CRL file. The default input path for the CRL is /var/netscaler/ssl/.

`inform`
The input format of the CRL file. PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM

`refresh`
Enables or disables the auto refresh feature for the CRL identified by the crlName Possible values: ENABLED, DISABLED Default value: VAL_NOT_SET

`CAcert`
The corresponding CA certificate that has issued the CRL. This is the System object identifying the CA certificate that is loaded in System. Note: This is a

mandatory field when the "-refresh" option is enabled. The CA certificate needs to be installed before loading the CRL.

method
The method for CRL refresh - HTTP or LDAP. Possible values: HTTP, LDAP Default value: MTHD_LDAP

server
The IP address of the LDAP server from which the CRLs are to be fetched.

url
URI of the CRL Distribution Point.

port
The port for the LDAP server. Minimum value: 1

baseDN
The baseDN attribute used by LDAP search to query for the attribute certificateRevocationList. Note: It is recommended to use the baseDN attribute over the Issuer Name from the CA certificate for the CRL, if the Issuer-Name fields does not exactly match the LDAP directory structure's DN.

scope
Extent of the search operation on the LDAP server. Base: Exactly the same level as basedn One : One level below basedn Possible values: Base, One Default value: NSAPI_ONESCOPE

interval
The CRL refresh interval. The valid values are monthly, weekly, and daily. This along with the -days and -time option will identify the exact time/time-interval for CRL refresh. -interval NONE can be used to reset previously set interval settings. Possible values: MONTHLY, WEEKLY, DAILY, NONE Default value: VAL_NOT_SET

day
The purpose of this option varies with the usage of the -interval option. If the -interval option has been set to MONTHLY, the -days option can be used to set a particular day of the month (1-30/31/28) on which the CRL needs to be refreshed. If the -interval option has been set to WEEKLY, the -days option can be used to set a particular day of the week, i.e. 1...7 (Sun=1,Sat=7) on which the CRL needs to be refreshed. The system handles the valid number

of days in a Month or Week, if the input value for the corresponding -day option is set incorrectly. If the -interval option has been set to DAILY, the -days parameter is not used. If the -days option is used without the -interval option, it specifies the number of days after which the refresh is to be done. Default value: VAL_NOT_SET Maximum value: 0xFFFE

time

The exact time of the day when the CRL is to be refreshed. The time is specified in 24-hour time format, where HH stands for Hours and MM stands for minutes. Default value: VAL_NOT_SET

bindDN

The bindDN to be used to access the CRL object in the LDAP repository. This is required if the access to the LDAP repository is restricted, i.e. anonymous access is not allowed.

password

The password to be used to access the CRL object in the LDAP repository. This is required if the access to the LDAP repository is restricted i.e. anonymous access is not allowed.

binary

Set the LDAP based CRL retrieval mode to binary. Possible values: YES, NO Default value: NO

Example

1)add ssl certkey CAcert -cert /nsconfig/ssl/ca_cert.pem add ssl crl crl_file /var/netscaler/ssl/crl.pem -cacert CAcert The above command adds a CRL from local storage system (HDD) with no refresh set. 2)add ssl certkey CAcert -cert /nsconfig/ssl/ca_cert.pem add ssl crl crl_file /var/netscaler/ssl/crl_new.pem -cacert Cacert -refresh ENABLED -server 10.102.1.100 -port 389 -interval DAILY -baseDN o=example.com,ou=security,c=US The above command adds a CRL to the system by fetching the CRL from the LDAP server and setting the refresh interval as daily.

Related Commands

create ssl crl

rm ssl crl

set ssl crl

unset ssl crl

show ssl crl

rm ssl crl

Synopsis

```
rm ssl crl <crlName> ...
```

Description

Remove the specified CRL object from the system.

Arguments

crlName

The name of the CRL object to be removed from the system.

Example

1)rm ssl crl ca_crl The above CLI command to delete the CRL object ca_crl from the system is.

Related Commands

create ssl crl

add ssl crl

set ssl crl

unset ssl crl

show ssl crl

set ssl crl

Synopsis

```
set ssl crl <crlName> [-refresh ( ENABLED | DISABLED )]
[-CAcert <string>] [-server <ip_addr|ipv6_addr|*> | -
url <URL>] [-method ( HTTP | LDAP )] [-port <port>] [-
baseDN <string>] [-scope ( Base | One )] [-interval
<interval>] [-day <integer>] [-time <HH:MM>] [-bindDN
<string>] [-password <string>] [-binary ( YES | NO )]
```

Description

Enable the automatic refresh option on a CRL and set different refresh parameters.

Arguments

crlName

The object name for the CRL.

refresh

The state of the auto refresh feature for the CRL. Possible values: ENABLED, DISABLED

CAcert

The corresponding CA certificate that has issued the CRL. This is the System object identifying the CA certificate that is loaded in System.

server

The IP address of the LDAP server from which the CRLs are to be fetched.

method

The method for CRL refresh. Possible values: HTTP, LDAP Default value: MTHD_LDAP

port

The port of the LDAP server. Minimum value: 1

baseDN

The baseDN attribute used by LDAP search to query for the attribute certificateRevocationList. Note: It is recommended to use the baseDN attribute over the Issuer Name from the CA certificate for the CRL, if the Issuer-Name fields does not exactly match the LDAP directory structure's DN.

scope

Extent of the search operation on the LDAP server. Base: Exactly the same level as basedn One : One level below basedn Possible values: Base, One Default value: NSAPI_ONESCOPE

interval

The CRL refresh interval. This option, when used in conjunction with the -days and -time option, can identify the exact time/time-interval for the CRL refresh. -interval NONE can be used to reset previously set interval settings. -interval NOW can be used to force a instantaneous CRL refresh. This is a one time operation. Possible values: MONTHLY, WEEKLY, DAILY, NOW, NONE

day

The purpose of this option varies with the usage of the -interval option. If the -interval option has been set to MONTHLY, the -days option can be used to set a particular day of the month (1-30/31/28) on which the CRL needs to be refreshed. If the -interval option has been set to WEEKLY, the -days option can be used to set a particular day of the week, i.e. 1...7 (Sun=1,Sat=7) on which the CRL needs to be refreshed. Sytem handles the valid number of days in a Month or Week, if the input value for the corresponding -day option is set incorrectly. For -interval daily, the -days parameter is not used. If -days is used without the -interval option, it specifies the number of days after which the refresh is to be performed.

time

The exact time of the day when the CRL is to be refreshed. The time is specified in 24-hour time format, where HH stands for Hours and MM stands for minutes.

bindDN

The bindDN to be used to access the CRL object in the LDAP repository. This is required if the access to the LDAP repository is restricted, i.e. anonymous access is not allowed.

password

The password to be is used to access the CRL object in the LDAP repository. This is required if the access to the LDAP repository is restricted, i.e. anonymous access is not allowed.

binary

Set the LDAP based CRL retrieval mode to binary. Possible values: YES, NO Default value: NO

Example

1)set ssl crl crl_file -refresh ENABLE -interval MONTHLY -days 10 -time 12:00 The above example sets the CRL refresh to every Month, on date=10, and time=12:00hrs. 2)set ssl crl crl_file -refresh ENABLE -interval WEEKLY -days 1 -time 00:10 The above example sets the CRL refresh every Week, on weekday=Sunday, and at time 10 past midnight. 3)set ssl crl crl_file -refresh ENABLE -interval DAILY -days 1 -time 12:00 The above example sets the CRL refresh every Day, at 12:00hrs. 4)set ssl crl crl_file -refresh ENABLE -days 10 The above example sets the CRL refresh after every 10 days. Note: The CRL will be refreshed after every 10 days. The time for CRL refresh will be 00:00 hrs. 5)set ssl crl crl_file -refresh ENABLE -time 01:00 The above example sets the CRL refresh after every 1 hour. 6)set ssl crl crl_file -refresh ENABLE -interval NOW The above example sets the CRL refresh instantaneously.

Related Commands

create ssl crl

add ssl crl

rm ssl crl

unset ssl crl

show ssl crl

unset ssl crl

Synopsis

```
unset ssl crl <crlName> [-refresh] [-CAcert] [-server]
[-method] [-url] [-port] [-baseDN] [-scope] [-interval]
[-day] [-time] [-bindDN] [-password] [-binary]
```

Description

Use this command to remove ssl crl settings.Refer to the set ssl crl command for meanings of the arguments.

Related Commands

create ssl crl

add ssl crl

rm ssl crl

set ssl crl

show ssl crl

show ssl crl

Synopsis

```
show ssl crl [<crlName>]
```

Description

Display the information pertaining to the Certificate Revocation Lists (CRL) configured on the system: If the crlName argument is specified, the command displays the details of the CRL. If the crlName argument is not specified, the command displays all the CRLs.

Arguments

`crlName`
The CRL object name.

`summary`

`fullValues`

`format`

`level`

Output

`crlPath`
The name and path to the file containing the CRL.

`inform`
The encoding format of the CRL (PEM or DER).

`CAcert`
The CA certificate that issued the CRL.

`refresh`
The state of the auto refresh feature for the CRL.

`scope`
Extent of the search operation on the LDAP server. Base: Exactly the same level as basedn One : One level below basedn.

server
The IP address of the LDAP/HTTP server from which the CRLs are to be fetched.

port
The port of the LDAP/HTTP server.

url
URI of the CRL Distribution Point.

method
The method for CRL refresh (LDAP or HTTP).

baseDN
The baseDN to be used to fetch the CRL object from the LDAP server.

interval
The CRL refresh interval.

day
The day when the CRL is to be refreshed.

time
The time when the CRL is to be refreshed.

bindDN
The bindDN to be used to access the CRL object in the LDAP repository.

password
The password to be is used to access the CRL object in the LDAP repository.

flags
CRL status flag.

lastupdatetime
Last CRL refresh time.

version
CRL version.

signaturealgo
Signature algorithm.

issuer
Issuer name.

lastupdate
Last update time.

nextupdate
Next update time.

date
Certificate Revocation date

number
Certificate Serial number.

binary
Mode of retrieval of CRL from LDAP server.

daysToExpiration
Number of days remaining for the CRL to expire.

Example

1) An example output of the show ssl crl command is as follows: 1 configured CRL(s) 1 Name: ca_crl CRL Path: /var/netscaler/ssl/cr1.der Format: DER Cacert: ca_cert Refresh: DISABLED 2) An example of the output of the show ssl crl ca_crl command is as follows: Name: ca_crl Status: Valid, Days to expiration: 21 CRL Path: /var/netscaler/ssl/cr1.der Format: DERCAcert: ca_cert Refresh: DISABLED Version: 1 Signature Algorithm: md5WithRSAEncryption Issuer: /C=US/ST=CA/L=santa clara /O=CA/OU=security Last_update:Dec 21 09:47:16 2001 GMT Next_update:Jan 20 09:47:16 2002 GMT Revoked Certificates: Serial Number: 01 Revocation Date:Dec 21 09:47:02 2001 GMT Serial Number: 02 Revocation Date:Dec 21 09:47:02 2001 GMT

Related Commands

create ssl crl

add ssl crl

rm ssl crl

set ssl crl

unset ssl crl

set ssl fips

Synopsis

```
set ssl fips -initHSM Level-2 [-hsmLabel <string>]
```

Description

Initialize the Hardware Security Module (HSM) or the FIPS card and set a new Security Officer password and User password. CAUTION: This command will erase all data on the FIPS card. You will be prompted before proceeding with the command execution. Save the current configuration after executing this command.

Arguments

`initHSM`
The FIPS initialization level. The system currently supports Level-2 (FIPS 140-2 Level-2). Possible values: Level-2

`soPassword`
The Hardware Security Module's (HSM) Security Officer password.

`oldSoPassword`
The old Security Officer password. This is used for authentication.

`userPassword`
The Hardware Security Module's (HSM) User password.

`hsmLabel`
The label to identify the Hardware Security Module (HSM).

Example

1) set fips -initHSM Level-2 fipsso123 oldfipsso123 fipuser123 -hsmLabel FIPS-140-2 >This command will erase all data on the FIPS card. You must save the configuration (saveconfig) after executing this command.Do you want to continue?(Y/N)y The above command initializes the FIPS card to FIPS-140-2 Level-2 and sets the HSM's Security Officer and User passwords.

Related Commands

unset ssl fips

reset ssl fips
show ssl fips

unset ssl fips

Synopsis

```
unset ssl fips -hsmLabel
```

Description

Use this command to remove ssl fips settings.Refer to the set ssl fips command for meanings of the arguments.

Related Commands

set ssl fips

reset ssl fips

show ssl fips

reset ssl fips

Synopsis

```
reset ssl fips
```

Description

Reset the FIPS card to default password for SO and User accounts. Note: This command can be used only if the FIPS card has been locked due to three or more unsuccessful login attempts

Arguments

Example

reset fips

Related Commands

set ssl fips

unset ssl fips

show ssl fips

show ssl fips

Synopsis

```
show ssl fips
```

Description

Display the information on the FIPS card.

Arguments

format

level

Output

initHSM
The level of the FIPS initialization.

eraseData
Erase data.

hsmLabel
FIPS card (HSM) label

serial
FIPS card serial number.

majorVersion
Firmware major version.

minorVersion
Firmware minor version.

flashMemoryTotal
Total size of the flash memory on card.

flashMemoryFree
Total size of free flash memory.

sramTotal
Total size of the SRAM memory on card.

sramFree
Total size of free SRAM memory.

status
Status.

Example

An example of the output for show ssl fips command is as follows: FIPS HSM Info: HSM Label : FIPS1 Initialization : FIPS-140-2 Level-2 HSM Serial Number : 238180016 Firmware Version : 4.3.0 Total Flash Memory : 1900428 Free Flash Memory : 1899720 Total SRAM Memory : 26210216 Free SRAM Memory : 17857232

Related Commands

set ssl fips

unset ssl fips

reset ssl fips

rm ssl fipsKey

Synopsis

```
rm ssl fipsKey <fipsKeyName> ...
```

Description

Remove the specified FIPS key(s) from the system.

Arguments

fipsKeyName

The name of the FIPS key(s) to be removed from the system.

Example

rm fipskey fips1

Related Commands

create ssl fipsKey
show ssl fipsKey

import ssl fipsKey
export ssl fipsKey

show ssl fipsKey

Synopsis

```
show ssl fipsKey [<fipsKeyName>]
```

Description

Display the information on the FIPS keys configured on the system. If no FIPS key name is specified then the command will list all the FIPS keys configured in the system. If a FIPS key name is specified, the command will display the details of the FIPS key.

Arguments

`fipsKeyName`
The name of the FIPS key.

`summary`

`fullValues`

`format`

`level`

Output

`modulus`
The modulus of the key.

`exponent`
The exponent value for the key.

`size`
Size.

Example

1) An example of output of show ssl fipskey command is as follows: show fipskey 2 FIPS keys: 1) FIPS Key Name: fips1 2) FIPS Key Name: fips2 2) An example of output of show fipskey command with FIPS key name specified is as follows: show fipskey fips1 FIPS Key Name: fips1 Modulus: 1024 Public Exponent: 3 (Hex: 0x3)

Related Commands

create ssl fipsKey
rm ssl fipsKey

import ssl fipsKey
export ssl fipsKey

import ssl fipsKey

Synopsis

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform
( SIM | DER )] [-wrapKeyName <string>] [-iv <string>]
```

Description

Import a key into the Hardware Security Module (HSM) -FIPS card. You can also use this command to import a FIPS key from another System's FIPS system (example Primary system), or for importing a non-FIPS key from an external Web server (Apache/IIS).

Arguments

`fipsKeyName`
The object name for the FIPS key being imported.

`key`
The path to the key file. The default input path for the key is /nsconfig/ssl/.

`inform`
The input format of the key file. SIM: Secure Information Management. This is used when a FIPS key is transferred from one FIPS system to other. DER: Distinguished Encoding Rule. This is used when a non-FIPS key is to be imported inside a FIPS system. The non-FIPS key has to be converted to PKCS#8 form using the CLI command "convert pkcs8". Possible values: SIM, DER Default value: FORMAT_SIM

`wrapKeyName`
The object name of the wrapkey to use for importing the key. The wrapkey is created using the CLI command "create ssl wrapkey". This is required if the key being imported is a non-FIPS key.

`iv`
The Initialization Vector (IV) to use for importing the key. This is required if the key being imported is a non-FIPS key.

Example

1)import fipskey fips1 -key /nsconfig/ssl/fipskey.sim The above example imports a FIPS key stored in the file fipskey.sim in the system. 2)import fipskey fips2 -key /nsconfig/ssl/key.der -inform DER -wrapKeyName wrapkey1 -iv wrap123 The above example imports a non-FIPS key stored in the file key.der in the system.

Related Commands

create ssl fipsKey

rm ssl fipsKey

show ssl fipsKey

export ssl fipsKey

export ssl fipsKey

Synopsis

```
export ssl fipsKey <fipsKeyName> -key <string>
```

Description

Export a FIPS key from one system to another or to backup the FIPS key in a secure manner. The exported key is secured using a strong asymmetric key encryption methods.

Arguments

fipsKeyName

The name of the FIPS key to be exported.

key

The path and file name to store the exported key. The default output path for the key is /nsconfig/ssl/.

Example

export fipskey fips1 -key /nsconfig/ssl/fips1.key

Related Commands

create ssl fipsKey

rm ssl fipsKey

show ssl fipsKey

import ssl fipsKey

set ssl service

Synopsis

```
set ssl service [<serviceName>@] [-dh ( ENABLED |
DISABLED )  -dhFile <string>] [-dhCount
<positive_integer>] [-eRSA ( ENABLED | DISABLED )  [-
eRSACount <positive_integer>]] [-sessReuse ( ENABLED |
DISABLED )  [-sessTimeout <positive_integer>]] [-
cipherRedirect ( ENABLED | DISABLED )  [-cipherURL
<URL>]] [-sslv2Redirect ( ENABLED | DISABLED )  [-
sslv2URL <URL>]] [-clientAuth ( ENABLED | DISABLED )
[-clientCert ( Mandatory | Optional )]] [-sslRedirect (
ENABLED | DISABLED )] [-redirectPortRewrite ( ENABLED |
DISABLED )] [-nonFipsCiphers ( ENABLED | DISABLED )] [-
ssl2 ( ENABLED | DISABLED )] [-ssl3 ( ENABLED |
DISABLED )] [-tls1 ( ENABLED | DISABLED )] [-serverAuth
( ENABLED | DISABLED )]
```

Description

Set the Advance SSL Configurations for an SSL service.

Arguments

serviceName

The SSL service name for which the advance configurations are to be set.

dh

The state of Diffie-Hellman (DH) key exchange support for the SSL service. Possible values: ENABLED, DISABLED Default value: DISABLED

dhCount

The refresh count for regeneration of DH public-key and private-key from the DH parameter. Zero means infinite usage (no refresh). Option '-dh' has to be enabled Default value: 0 Minimum value: 0 Maximum value: 65534

eRSA
The state of Ephemeral RSA key exchange support for the SSL service. Possible values: ENABLED, DISABLED Default value: ENABLED

sessReuse
The state of session reuse support for the SSL service. Possible values: ENABLED, DISABLED Default value: ENABLED

cipherRedirect
The state of Cipher Redirect feature. Possible values: ENABLED, DISABLED Default value: ENABLED

sslv2Redirect
The state of SSLv2 Redirect feature. Possible values: ENABLED, DISABLED Default value: ENABLED

clientAuth
The state of Client-Authentication support for the SSL service. Possible values: ENABLED, DISABLED Default value: DISABLED

sslRedirect
The state of HTTPS redirects for the SSL service. This is required for the proper functioning of the redirect messages from the server. The redirect message from the server provides the new location for the moved object. This is contained in the HTTP header field: Location, e.g. Location: http://www.moved.org/here.html For the SSL session, if the client browser receives this message, the browser will try to connect to the new location. This will break the secure SSL session, as the object has moved from a secure site (https://) to an un-secure one (http://). Generally browsers flash a warning message on the screen and prompt the user, either to continue or disconnect. The above feature, when enabled will automatically convert all such http:// redirect message to https://. This will not break the client SSL session. Note: The set ssl service command can be used for configuring a front-end SSL service for service based SSL Off-Loading, or a backend SSL service for backend-encryption setup. Some of the command options are not applicable while configuring a backend service. System will not report an error if these options are used for a backend SSL service. These are: [-dh (ENABLED|DISABLED) (-dhFile < file_name >)] [(-dhCount <pos_int>)] [-eRSA (ENABLED|DISABLED)] [(-eRSACount <pos_int>)] [-cipherRedirect (ENABLED | DISABLED) [-cipherURL <URL>]] [-sslv2Redirect (ENABLED | DISABLED) [-sslv2URL <URL>]] [-

clientAuth (ENABLED | DISABLED) [-clientCert (Mandatory | Optional)]] [-sslRedirect (ENABLED | DISABLED)] [-ssl2 (ENABLED|DISABLED)]. Possible values: ENABLED, DISABLED Default value: DISABLED

redirectPortRewrite

The state of the port in rewrite while performing HTTPS redirect. Possible values: ENABLED, DISABLED Default value: DISABLED

nonFipsCiphers

The state of usage of non FIPS approved ciphers. Valid only for an SSL service bound with a FIPS key and certificate. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl2

The state of SSLv2 protocol support for the SSL service. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3

The state of SSLv3 protocol support for the SSL service. Possible values: ENABLED, DISABLED Default value: ENABLED

tls1

The state of TLSv1 protocol support for the SSL service. Possible values: ENABLED, DISABLED Default value: ENABLED

serverAuth

The state of Server-Authentication support for the SSL service. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

1)set ssl service sslsvc -dh ENABLED -dhFile /nsconfig/ssl/dh1024.pem -dhCount 500 The above example sets the DH parameters for the SSL service 'sslsvc'. 2.set ssl service sslsvc -ssl2 DISABLED The above example disables the support for SSLv2 protocol for the SSL service 'sslsvc'.

Related Commands

unset ssl service

bind ssl service

unbind ssl service

show ssl service

unset ssl service

Synopsis

```
unset ssl service [<serviceName>@] [-dh] [-dhFile] [-
dhCount] [-eRSA] [-eRSACount] [-sessReuse] [-
sessTimeout] [-cipherRedirect] [-cipherURL] [-
sslv2Redirect] [-sslv2URL] [-clientAuth] [-clientCert]
[-sslRedirect] [-redirectPortRewrite] [-
nonFipsCiphers] [-ssl2] [-ssl3] [-tls1] [-serverAuth]
```

Description

Use this command to remove ssl service settings.Refer to the set ssl service command for meanings of the arguments.

Related Commands

set ssl service

bind ssl service

unbind ssl service

show ssl service

bind ssl service

Synopsis

```
bind ssl service <serviceName>@ ((-policyName <string>
[-priority <positive_integer>]) | (-certkeyName
<string>  [-CA  [-crlCheck ( Mandatory | Optional )]]))
```

Description

Bind a SSL certkey or a SSL policy to a SSL service.

Arguments

serviceName
The name of the SSL service to which the SSL policy needs to be bound.

policyName
The name of the SSL policy.

certkeyName
The name of the CertKey

Example

bind ssl service ssl_svc -policyName certInsert_pol -priority 10

Related Commands

set ssl service
unset ssl service
unbind ssl service

show ssl service

unbind ssl service

Synopsis

```
unbind ssl service <serviceName>@ (-policyName <string>
| (-certkeyName <string>  [-CA  [-crlCheck ( Mandatory
| Optional )]]))
```

Description

Unbind a SSL policy from a SSL service.

Arguments

serviceName

The name of the SSL service from which the SSL policy needs to be unbound.

policyName

The name of the SSL policy.

certkeyName

Example

unbind ssl service ssl_svc -policyName certInsert_pol

Related Commands

set ssl service

unset ssl service

bind ssl service

show ssl service

show ssl service

Synopsis

```
show ssl service <serviceName> [-cipherDetails]
```

Description

View the advanced SSL settings for an SSL service.

Arguments

serviceName
The name of the SSL service.

cipherDetails
Details of the individual ciphers bound to the SSL service. Select this flag value to display the details of the individual ciphers bound to the SSL service.

summary

fullValues

format

level

Output

crlCheck
The state of the CRL check parameter. (Mandatory/Optional)

dh
The state of Diffie-Hellman (DH) key exchange support.

dhFile
The file name and path for the DH parameter.

dhCount
The refresh count for regeneration of DH public-key and private-key from the DH parameter.

eRSA
The state of Ephemeral RSA key exchange support.

eRSACount
The refresh count for re-generation of RSA public-key and pri-vate-key pair.

sessReuse
The state of session reuse support.

sessTimeout
The session timeout value in seconds.

cipherRedirect
The state of Cipher Redirect feature.

cipherURL
The redirect URL to be used with the Cipher Redirect feature.

sslv2Redirect
The state of SSLv2 Redirect feature.

sslv2URL
The redirect URL to be used with the SSLv2 Redirect feature.

clientAuth
The state of Client-Authentication support.

clientCert
The rule for client certificate requirement in client authentication.

sslRedirect
The state of HTTPS redirect feature.

redirectPortRewrite
The state of port rewrite feature.

nonFipsCiphers
The state of usage of non FIPS approved ciphers.

ssl2
The state of SSLv2 protocol support.

ssl3
The state of SSLv3 protocol support.

tls1
The state of TLSv1 protocol support.

serverAuth
The state of Server-Authentication support.

cipherAliasName/cipherName/cipherGroupName
The cipher group/alias/individual cipher configuration.

description
The cipher suite description.

certkeyName
The certificate key pair binding.

policyName
The SSL policy binding.

clearTextPort
The clearTextPort settings.

priority
The priority of the policies bound to this SSL service

polinherit
Whether the bound policy is a inherited policy or not

Example

An example of output of show ssl service command is as shown below show ssl service svc1 Advanced SSL configuration for Back-end SSL Service svc1: DH: DISABLED Ephemeral RSA: ENABLED Refresh Count: 0 Session Reuse: ENABLED Timeout: 300 seconds Cipher Redirect: DISABLED SSLv2 Redirect: DISABLED Server Auth: DISABLED SSL Redirect: DISABLED Non FIPS Ciphers: DISABLED SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED 1) Cipher Name: ALL Description: Predefined Cipher Alias

Related Commands

set ssl service

unset ssl service

bind ssl service

unbind ssl service

set ssl serviceGroup

Synopsis

```
set ssl serviceGroup <serviceGroupName>@ [-sessReuse (
ENABLED | DISABLED )  [-sessTimeout
<positive_integer>]] [-nonFipsCiphers ( ENABLED |
DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1 (
ENABLED | DISABLED )] [-serverAuth ( ENABLED | DISABLED
)]
```

Description

Set the Advance SSL Configurations for a SSL service group.

Arguments

serviceGroupName

The SSL service group name for which the advance configurations are to be set.

sessReuse

The state of session reuse support for the SSL service group. Possible values: ENABLED, DISABLED Default value: ENABLED

nonFipsCiphers

The state of usage of non FIPS approved ciphers. Valid only for an SSL service group bound with a FIPS key and certificate. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3

The state of SSLv3 protocol support for the SSL service group. Possible values: ENABLED, DISABLED Default value: ENABLED

tls1

The state of TLSv1 protocol support for the SSL service group. Possible values: ENABLED, DISABLED Default value: ENABLED

serverAuth

The state of Server-Authentication support for the SSL service group. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

1)set ssl servicegroup svcg1 -sessReuse DISABLED The above example disables session reuse for the service group 'svcg1'.

Related Commands

unset ssl serviceGroup

show ssl serviceGroup

unset ssl serviceGroup

Synopsis

```
unset ssl serviceGroup <serviceGroupName>@ [-sessReuse]
[-sessTimeout] [-nonFipsCiphers] [-ssl3] [-tls1] [-
serverAuth]
```

Description

Use this command to remove ssl serviceGroup settings.Refer to the set ssl serviceGroup command for meanings of the arguments.

Related Commands

set ssl serviceGroup

show ssl serviceGroup

show ssl serviceGroup

Synopsis

```
show ssl serviceGroup <serviceGroupName> [-
cipherDetails]
```

Description

View the advanced SSL settings for an SSL service group.

Arguments

serviceGroupName

The name of the SSL service group.

cipherDetails

Display the details of the individual ciphers bound to the SSL service group.

summary

fullValues

format

level

Output

dh

The state of DH key exchange support for the SSL service group.

dhFile

The file name and path for the DH parameter.

dhCount

The refresh count for the re-generation of DH public-key and private-key from the DH parameter.

eRSA

The state of Ephemeral RSA key exchange support for the SSL service group.

eRSACount
The refresh count for the re-generation of RSA public-key and private-key pair.

sessReuse
The state of session re-use support for the SSL service group.

sessTimeout
The Session timeout value in seconds.

cipherRedirect
The state of Cipher Redirect feature.

cipherURL
The redirect URL to be used with the Cipher Redirect feature.

sslv2Redirect
The state of SSLv2 Redirect feature.

sslv2URL
The redirect URL to be used with SSLv2 Redirect feature.

clientAuth
The state of Client-Authentication support for the SSL service group.

clientCert
The rule for client certificate requirement in client authentication.

sslRedirect
The state of HTTPS redirects for the SSL service group.

redirectPortRewrite
The state of port-rewrite feature.

nonFipsCiphers
The state of usage of non FIPS approved ciphers.

ssl2
The state of SSLv2 protocol support for the SSL service group.

ssl3
The state of SSLv3 protocol support for the SSL service group.

tls1
The state of TLSv1 protocol support for the SSL service group.

serverAuth
The state of the server authentication configuration for the SSL service group.

cipherAliasName/cipherName/cipherGroupName
The name of the cipher group/alias/name configured for the SSL service group.

description
The description of the cipher.

certkeyName
The name of the certificate bound to the SSL service group.

clearTextPort
The clear-text port for the SSL service group.

serviceName
The service name.

Example

An example of output of show ssl servicegroup command is as shown below show ssl servicegroup ssl_svcg Advanced SSL configuration for Back-end SSL Service Group ssl_svcg: Session Reuse: ENABLED Timeout: 300 seconds Server Auth: DISABLED Non FIPS Ciphers: DISABLED SSLv3: ENABLED TLSv1: ENABLED 1) Cipher Name: ALL Description: Predefined Cipher Alias

Related Commands

set ssl serviceGroup

unset ssl serviceGroup

set ssl vserver

Synopsis

```
set ssl vserver <vServerName>@ [-clearTextPort <port>]
[-dh ( ENABLED | DISABLED )  -dhFile <string>] [-
dhCount <positive_integer>] [-eRSA ( ENABLED | DISABLED
)  [-eRSACount <positive_integer>]] [-sessReuse (
ENABLED | DISABLED )  [-sessTimeout
<positive_integer>]] [-cipherRedirect ( ENABLED |
DISABLED )  [-cipherURL <URL>]] [-sslv2Redirect (
ENABLED | DISABLED )  [-sslv2URL <URL>]] [-clientAuth (
ENABLED | DISABLED )  [-clientCert ( Mandatory |
Optional )]] [-sslRedirect ( ENABLED | DISABLED )] [-
redirectPortRewrite ( ENABLED | DISABLED )] [-
nonFipsCiphers ( ENABLED | DISABLED )] [-ssl2 ( ENABLED
| DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1 (
ENABLED | DISABLED )]
```

Description

Set Advance SSL Configurations for an SSL virtual server.

Arguments

vServerName

The name of the SSL virtual server.

clearTextPort

The port on the back-end web-servers where the clear-text data is sent by system. Use this setting for the wildcard IP based SSL Acceleration configuration (*:443). Minimum value: 1

dh

The state of DH key exchange support for the specified SSL virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

dhCount
The refresh count for the re-generation of DH public-key and private-key from the DH parameter. Zero means infinite usage (no refresh). Note: The '-dh' argument must be enabled if this argument is specified. Default value: 0 Minimum value: 0 Maximum value: 65534

eRSA
The state of Ephemeral RSA key exchange support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

sessReuse
The state of session re-use support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

cipherRedirect
The state of Cipher Redirect feature. Possible values: ENABLED, DISABLED Default value: ENABLED

sslv2Redirect
The state of SSLv2 Redirect feature. Possible values: ENABLED, DISABLED Default value: ENABLED

clientAuth
The state of Client-Authentication support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

sslRedirect
The state of HTTPS redirects for the SSL virtual server. This is required for proper working of the redirect messages from the web server. The redirect message from the server gives the new location for the moved object. This is contained in the HTTP header field: Location (for example, Location: http://www.moved.org/here.html). For an SSL session, if the client browser receives this message, the browser will try to connect to the new location. This will break the secure SSL session, as the object has moved from a secure site (https://) to an unsecured one (http://). Browsers usually flash a warning message on the screen and prompt the user to either continue or disconnect. When the above feature is enabled, all such http:// redirect messages are automatically converted to https://. This does not break the client SSL session. Possible values: ENABLED, DISABLED Default value: DISABLED

redirectPortRewrite
The state of port in rewrite while performing HTTPS redirect. Possible values: ENABLED, DISABLED Default value: DISABLED

nonFipsCiphers
The state of usage of non FIPS approved ciphers. Valid only for an SSL vserver bound with a FIPS key and certificate. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl2
The state of SSLv2 protocol support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3
The state of SSLv3 protocol support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

tls1
The state of TLSv1 protocol support for the SSL virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

1)set ssl vserver sslvip -dh ENABLED -dhFile /siteA/dh1024.pem -dhCount 500 The above example set the DH parameters for the SSL virtual server 'sslvip'. 3)set ssl vserver sslvip -ssl2 DISABLED The above example disables the support for SSLv2 protocol for the SSL virtual server 'sslvip'.

Related Commands

unset ssl vserver

bind ssl vserver

unbind ssl vserver

show ssl vserver

unset ssl vserver

Synopsis

```
unset ssl vserver <vServerName>@ [-clearTextPort] [-dh]
[-dhFile] [-dhCount] [-eRSA] [-eRSACount] [-sessReuse]
[-sessTimeout] [-cipherRedirect] [-cipherURL] [-
sslv2Redirect] [-sslv2URL] [-clientAuth] [-clientCert]
[-sslRedirect] [-redirectPortRewrite] [-
nonFipsCiphers] [-ssl2] [-ssl3] [-tls1]
```

Description

Use this command to remove ssl vserver settings.Refer to the set ssl vserver command for meanings of the arguments.

Related Commands

set ssl vserver

bind ssl vserver

unbind ssl vserver

show ssl vserver

bind ssl vserver

Synopsis

```
bind ssl vserver <vServerName>@ ((-policyName <string>
[-priority <positive_integer>]) | (-certkeyName
<string>  [-CA  [-crlCheck ( Mandatory | Optional )]]))
```

Description

Bind a SSL certkey or a SSL policy to a SSL virtual server.

Arguments

vServerName

The name of the SSL virtual server to which the SSL policy needs to be bound.

policyName

The name of the SSL policy.

certkeyName

The name of the CertKey

Example

bind ssl vserver ssl_vip -policyName certInsert_pol -priority 10

Related Commands

set ssl vserver

unset ssl vserver

unbind ssl vserver

show ssl vserver

unbind ssl vserver

Synopsis

```
unbind ssl vserver <vServerName>@ (-policyName <string>
| (-certkeyName <string>  [-CA  [-crlCheck ( Mandatory
| Optional )]]))
```

Description

Unbind a SSL policy from a SSL virtual server.

Arguments

vServerName

The name of the SSL virtual server from which the SSL policy needs to be unbound.

policyName

The name of the SSL policy.

certkeyName

Example

unbind ssl vserver ssl_vip -policyName certInsert_pol

Related Commands

set ssl vserver

unset ssl vserver

bind ssl vserver

show ssl vserver

show ssl vserver

Synopsis

```
show ssl vserver <vServerName> [-cipherDetails]
```

Description

Display all the SSL specific configurations for an SSL virtual server. This includes information about the Advance SSL configurations, certificate bindings, and cipher-suite configurations.

Arguments

vServerName
The name of the SSL virtual server.

cipherDetails
Details of the individual ciphers bound to the SSL vserver. Select this flag value to display the details of the individual ciphers bound to the SSL vserver.

summary

fullValues

format

level

Output

clearTextPort
The clearTextPort settings.

dh
The state of Diffie-Hellman (DH) key exchange support.

dhFile
The file name and path for the DH parameter.

dhCount
The refresh count for the re-generation of DH public-key and private-key from the DH parameter.

eRSA
The state of Ephemeral RSA key exchange support.

eRSACount
The refresh count for the re-generation of RSA public-key and private-key pair.

sessReuse
The state of session re-use support.

sessTimeout
The Session timeout value in seconds.

cipherRedirect
The state of Cipher Redirect feature.

crlCheck
The state of the CRL check parameter. (Mandatory/Optional)

cipherURL
The redirect URL to be used with the Cipher Redirect feature.

sslv2Redirect
The state of SSLv2 Redirect feature.

sslv2URL
The redirect URL to be used with SSLv2 Redirect feature.

clientAuth
The state of Client-Authentication support.

clientCert
The rule for client certificate requirement in client authentication.

sslRedirect
The state of HTTPS redirect feature support.

priority
The priority of the policies bound to this SSL service

polinherit
Whether the bound policy is a inherited policy or not

redirectPortRewrite
The state of port rewrite feature support.

nonFipsCiphers
The state of usage of non FIPS approved ciphers.

ssl2
The state of SSLv2 protocol support.

ssl3
The state of SSLv3 protocol support.

tls1
The state of TLSv1 protocol support.

cipherAliasName/cipherName/cipherGroupName
The name of the cipher group/alias/individual cipheri bindings.

description
The cipher suite description.

service
Service

certkeyName
The name of the certificate key pair binding.

policyName
The name of the SSL policy binding.

serviceName
Service name.

Example

An example of the output of the show vserver sslvip command is as follows:
sh ssl vserver va1 Advanced SSL configuration for VServer va1: DH: DISABLED Ephemeral RSA: ENABLED Refresh Count: 0 Session Reuse: ENABLED Timeout: 120 seconds Cipher Redirect: DISABLED SSLv2 Redirect: DISABLED ClearText Port: 0 Client Auth: DISABLED SSL Redirect: DISABLED Non FIPS Ciphers: DISABLED SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED 1 bound certificate: 1) CertKey Name: buy Server Certificate 1 bound CA certificate: 1) CertKey Name: rtca CA

Certificate 1) Cipher Name: DEFAULT Description: Predefined Cipher Alias

Related Commands

bind ssl certkey

bind ssl cipher

set ssl vserver

unset ssl vserver

bind ssl vserver

unbind ssl vserver

rm ssl wrapkey

Synopsis

```
rm ssl wrapkey <wrapKeyName> ...
```

Description

Remove the specified wrapkey(s) from the system.

Arguments

wrapKeyName

The name of the wrapkey(s) to be removed from the system.

Example

rm wrapkey wrap1

Related Commands

create ssl wrapkey

show ssl wrapkey

show ssl wrapkey

Synopsis

```
show ssl wrapkey
```

Description

Display the wrap keys.

Arguments

summary

fullValues

format

level

Output

wrapKeyName
Wrap key name.

Example

An example of output of 'show wrapkey' command is as shown below: sh wrapkey 1 WRAP key: 1)WRAP Key Name: wrap1

Related Commands

create ssl wrapkey

rm ssl wrapkey

enable ssl fipsSIMTarget

Synopsis

```
enable ssl fipsSIMTarget <keyVector> <sourceSecret>
```

Description

Enable the target FIPS system to participate in secure exchange of keys with another FIPS system. The command is used for secure transfer of FIPS keys from the Primary system to the Secondary system.

Arguments

keyVector

The file name and path for storing the target FIPS system's key-vector. The default output path for the secret data is /nsconfig/ssl/.

sourceSecret

The file name and path for the source FIPS system's secret data. The default input path for the secret data is /nsconfig/ssl/.

Example

enable fipsSIMtarget /nsconfig/ssl/target.key /nsconfig/ssl/source.secret

Related Commands

init ssl fipsSIMTarget

init ssl fipsSIMTarget

Synopsis

```
init ssl fipsSIMTarget <certFile> <keyVector>
<targetSecret>
```

Description

Initialize the target FIPS system for participating in secure exchange of keys with another FIPS system. The command is used for secure transfer of FIPS keys from the primary system to the Secondary system.

Arguments

certFile

The source FIPS system's certificate file name and path. The default input path for the certificate file is /nsconfig/ssl/.

keyVector

The file name and path for storing the target FIPS system's key-vector. The default output path for the key-vector is /nsconfig/ssl/.

targetSecret

The file name and path for storing the target FIPS system's secret data. The default output path for the secret data is /nsconfig/ssl/.

Example

init fipsSIMtarget /nsconfig/ssl/source.cert /nsconfig/ssl/target.key /nsconfig/ssl/target.secret

Related Commands

enable ssl fipsSIMTarget

enable ssl fipsSIMSource

Synopsis

```
enable ssl fipsSIMSource <targetSecret> <sourceSecret>
```

Description

Enable the source FIPS system for participating in secure exchange of keys with another FIPS system. The command is used for secure transfer of FIPS keys from the Primary system to the Secondary system.

Arguments

`targetSecret`

The file name and path for the target FIPS system's secret data. The default input path for the secret data is /nsconfig/ssl/.

`sourceSecret`

The file name and path for storing the source FIPS system's secret data. The default output path for the secret data is /nsconfig/ssl/.

Example

enable fipsSIMsource /nsconfig/ssl/target.secret /nsconfig/ssl/source.secret

Related Commands

init ssl fipsSIMSource

init ssl fipsSIMSource

Synopsis

```
init ssl fipsSIMSource <certFile>
```

Description

Initialize the source FIPS system for participating in secure exchange of keys with another FIPS system. The command is used for secure transfer of FIPS keys from the primary system to the secondary system.

Arguments

certFile

The file name and path where the source FIPS system's certificate is to be stored. The default output path for the certificate file is /nsconfig/ssl/.

Example

init fipsSIMsource /nsconfig/ssl/source.cert

Related Commands

enable ssl fipsSIMSource

add ssl action

Synopsis

```
add ssl action <name> [-clientAuth ( DOCLIENTAUTH |
NOCLIENTAUTH )] [-clientCert ( ENABLED | DISABLED )  -
certHeader <string>] [-clientCertSerialNumber ( ENABLED
| DISABLED )  -certSerialHeader <string>] [-
clientCertSubject ( ENABLED | DISABLED )  -
certSubjectHeader <string>] [-clientCertHash ( ENABLED
| DISABLED )  -certHashHeader <string>] [-
clientCertIssuer ( ENABLED | DISABLED )  -
certIssuerHeader <string>] [-sessionID ( ENABLED |
DISABLED )  -sessionIDHeader <string>] [-cipher (
ENABLED | DISABLED )  -cipherHeader <string>] [-
clientCertNotBefore ( ENABLED | DISABLED )  -
certNotBeforeHeader <string>] [-clientCertNotAfter (
ENABLED | DISABLED )  -certNotAfterHeader <string>] [-
OWASupport ( ENABLED | DISABLED )]
```

Description

Create a new SSL action.

Arguments

name

The name for the new SSL action. Maximum Length: 32

clientAuth

Set action to do client certificate authentication or no authentication. DOCLIENTAUTH: Perform client certificate authentication. NOCLIENTAUTH: No client certificate authentication. Possible values: DOCLIENTAUTH, NOCLIENTAUTH

clientCert

The state of insertion of the client certificate in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertSerialNumber
The state of insertion of the client certificate's Serial Number in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertSubject
The state of insertion of the client certificate's Subject Name in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertHash
The state of insertion of the client certificate's hash (signature) in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertIssuer
The state of insertion of the client certificate's Issuer Name in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

sessionID
The state of insertion of the Session-ID in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

cipher
The state of insertion of the cipher details in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertNotBefore
The state of insertion of the client certificate's Not-Before date in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

clientCertNotAfter
The state of insertion of the client certificate's Not-After in the HTTP header when the request is sent to the web-server. Possible values: ENABLED, DISABLED

OWASupport
The state of Outlook Web-Access support. If the system is in front of an Outlook Web Access (OWA) server, a special header field, 'FRONT-END-HTTPS: ON', needs to be inserted in the HTTP requests going to the OWA

server. Note: This parameter is required as the SSL requests (HTTPS) arrives at the back-end Exchange-2000 server on the configured HTTP port (80) instead of arriving at the front-end Exchange 2000 server. Possible values: ENABLED, DISABLED

Example

add ssl action certInsert_act -clientCert ENABLED -certHeader CERT

Related Commands

rm ssl action

show ssl action

rm ssl action

Synopsis

```
rm ssl action <name>
```

Description

Remove the specified SSL action.

Arguments

name

The name of the SSL action.

Example

rm ssl action certInsert_act

Related Commands

add ssl action

show ssl action

show ssl action

Synopsis

```
show ssl action [<name>]
```

Description

Display the SSL actions.

Arguments

name

The name of the SSL action.

summary

fullValues

format

level

Output

Example

sh ssl action 1 Configured SSL action: 1) Name: certInsert_act Data Insertion Action: Cert Header: ENABLED Cert Tag: CERT

Related Commands

add ssl action

rm ssl action

add ssl policy

Synopsis

```
add ssl policy <name> -rule <expression> -reqAction
<string>
```

Description

Add an SSL policy.

Arguments

name

The name for the new SSL policy. Maximum Length: 32

rule

The expression that sets the condition for application of the SSL policy. Maximum Length:1500

reqAction

The name of the action to be performed on the request. Refer to 'add ssl action' command to add a new action.

Example

add ssl action certInsert_act -clientCert ENABLED -certHeader CERT add ssl policy certInsert_pol -rule "URL == /secure/*" -reqAction certInsert_act The above example adds an SSL policy to do Client certificate insertion into the HTTP requests for any web-objects under /secure/.

Related Commands

rm ssl policy

show ssl policy

rm ssl policy

Synopsis

```
rm ssl policy <name>
```

Description

Remove an SSL policy.

Arguments

name

The name of the SSL policy.

Example

rm ssl policy certInsert_pol

Related Commands

add ssl policy

show ssl policy

show ssl policy

Synopsis

```
show ssl policy [<name>]
```

Description

Display the created SSL policies.

Arguments

name

The name of the SSL policy.

summary

fullValues

format

level

Output

rule

The expression that sets the condition for application of the SSL policy.

action

The name of the action to be performed on the request.

hits

Number of hits for this policy.

boundTo

The entity name to which policy is bound

Example

show ssl policy 1 SSL policy: 1) Name: certInsert_pol Rule: URL == /*
Action: certInsert_act Hits: 0

Related Commands

add ssl policy

rm ssl policy

bind ssl global

Synopsis

```
bind ssl global [-policyName <string>  [-priority
<positive_integer>]]
```

Description

Bind an SSL policy globally.

Arguments

policyName

The name of the SSL policy.

Example

bind ssl global -policyName certInsert_pol -priority 100

Related Commands

unbind ssl global

show ssl global

unbind ssl global

Synopsis

```
unbind ssl global -policyName <string>
```

Description

Unbind a globally bound SSL policy.

Arguments

policyName

The name of the SSL policy.

Example

unbind ssl global -policyName certInsert_pol

Related Commands

bind ssl global

show ssl global

show ssl global

Synopsis

```
show ssl global
```

Description

Display globally bound SSL policies.

Arguments

summary

fullValues

format

level

Output

policyName
The name for the SSL policy.

priority
The priority of the policy binding.

Example

sh ssl global 1 Globally Active SSL Policy: 1) Name: certInsert_pol Priority: 100

Related Commands

bind ssl global

unbind ssl global

CHAPTER 27

System Commands

This chapter covers the system commands.

stat system

Synopsis

```
stat system [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

This command displays system statistics

Arguments

Output

Counters

`CPU usage (CPU)`
CPU utilization percentage

`Average CPU usage (CPU)`
Average CPU utilization percentage.

`CPU1`
CPU 1 (currently the slave CPU) utilization, as percentage of capacity. Not applicable for a single-CPU system.

`CPU0`
CPU 0 (currently the master CPU) utilization, as percentage of capacity.

`Voltage 7 (Volts) (volt7)`
Voltage of a device connected to health monitoring chip through pin 7.

`Voltage 6 (Volts) (volt6)`
Voltage of a device connected to health monitoring chip through pin 6.

`Voltage 5 (Volts) (volt5)`
Voltage of a device connected to health monitoring chip through pin 5.

`Voltage 4 (Volts) (volt4)`
Voltage of a device connected to health monitoring chip through pin 4.

Voltage 3 (Volts) (volt3)
Voltage of a device connected to health monitoring chip through pin 3.

Voltage 2 (Volts) (volt2)
Voltage of a device connected to health monitoring chip through pin 2.

Voltage 1 (Volts) (volt1)
Voltage of a device connected to health monitoring chip through pin 1.

Voltage 0 (Volts) (volt0)
Voltage of a device connected to health monitoring chip through pin 0.

Voltage Sensor2(Volts) (VSEN2)
Voltage Sensor 2 Input. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

5V Standby Voltage(Volts) (V5SB)
Power Supply 5V Standby Voltage. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

Intel CPU Vtt Power(Volts) (VTT)
Intel CPU Vtt power. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

Battery Voltage (Volts) (VBAT)
Onboard battery power supply output. 9800 and 9950 platforms display standard value of 5.0V.

-12.0 V Supply Voltage (V12n)
Power supply -12V output. Acceptable range is -13.20 through -10.80 volts. 9800 and 9960 platforms display standard value of -12.0V.

+12.0 V Supply Voltage (V+12)
Power supply +12V output. Acceptable range is 10.80 through 13.20 volts.

-5.0 V Supply Voltage (V50n)
Power supply -5V output. Acceptable range is -5.50 through -4.50 volts. 9800 and 9960 platforms display standard value of -5.0V.

+5.0 V Supply Voltage (V50)
Power supply +5V output. Acceptable range is 4.50 through 5.50 volts.

Standby 3.3 V Supply Voltage (V33Stby)
Standby power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts. 9800 and 9960 platforms display standard value of 3.3V. You can configure Standby 3.3V Supply Voltage by using the Set snmp alarm VOLTAGE-LOW command to set the lower limit and the Set snmp alarm VOLTAGE-HIGH command to set the upper limit.

Main 3.3 V Supply Voltage (V33Main)
Main power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts. This is a critical counter. You can configure Main 3.3V Supply Voltage, by using the Set snmp alarm VOLTAGE-LOW command to set the lower limit and the Set snmp alarm VOLTAGE-HIGH command to set the upper limit.

CPU 1 Core Voltage (Volts) (VCC1)
CPU core 1 voltage. Acceptable range is 1.080 through 1.650 volts. If CPU 1 is not connected to the health monitoring chip, display shows voltage of CPU 0.

CPU 0 Core Voltage (Volts) (VCC0)
CPU core 0 voltage. Acceptable range is 1.080 through 1.650 volts.

Number of CPUs (CPUs)
The number of CPUs on the system

Memory usage (%) (MemUsage)
This represents the percentage of memory utilization on NetScaler.

Memory usage (MB) (MemUseMB)
Main memory currently in use, in megabytes.

Management CPU usage (%) (CPU)
Management CPU utilization percentage.

Packet CPU usage (%) (CPU)
Packet CPU utilization percentage.

CPU usage (%) (CPU)
CPU utilization percentage

Average CPU usage (%) (CPU)
Average CPU utilization percentage.

Up since (Since)
Time when the system last started

/flash Used (%) (disk0PerUsage)
Used space in /flash partition of the disk, as a percentage. This is a critical counter. You can configure /flash Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.

/var Used (%) (disk1PerUsage)
Used space in /var partition of the disk, as a percentage. This is a critical counter. You can configure /var Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.

CPU Fan 0 Speed (RPM) (CPUFan0)
CPU Fan 0 speed. Acceptable range is 3000 through 6000 RPM. This is a critical counter. You can configure CPU Fan 0 Speed by using the Set snmp alarm FAN-SPEED-LOW command to set the lower limit.

CPU Fan 1 Speed (RPM) (CPUFan1)
CPU Fan 1 speed. Acceptable range is 3000 through 6000 RPM. 7000 platform displays speed of CPU fan 0. This is a critical counter. You can configure CPU Fan 1 Speed by using the Set snmp alarm FAN-SPEED-LOW command to set the lower limit.

System Fan Speed (RPM) (systemFan)
System fan speed. Acceptable range is 3000 through 6000 RPM. This is a critical counter. You can configure System Fan Speed by using the Set snmp alarm FAN-SPEED-LOW command to set the lower limit.

System Fan 1 Speed (RPM) (systemFan1)
System fan 1 speed. For new platforms associated pin is connected to CPU supporting fans. For platforms in which it is not connected, it will point to System Fan.

System Fan 2 Speed (RPM) (systemFan2)
System fan 2 speed. For new platforms associated pin is connected to CPU supporting fans. For platforms in which it is not connected, it will point to System Fan

CPU 0 Temperature (Celsius) (TCPU0)
CPU 0 temperature. 9800 and 9960 platforms display internal chip temperature. This is a critical counter. You can configure CPU 0 Temperature

by using the Set snmp alarm TEMPERATURE-HIGH command to set the upper limit.

CPU 1 Temperature (Celsius) (TCPU1)
CPU 1 temperature. 9800 and 9960 platforms display internal chip temperature. 7000, 9010 and 10010 platforms display CPU 0 temperature. This is a critical counter. You can configure CPU 1 Temperature by using the Set snmp alarm TEMPERATURE-HIGH command to set the upper limit.

Internal Temperature (Celsius) (intTemp)
Internal temperature of health monitoring chip. This is a critical counter. You can configure Internal Temperature by using the Set snmp alarm TEMPERATURE-HIGH command to set the upper limit.

Power supply 1 status (PS1FAIL)
Power supply 1 failure status

Power supply 2 status (PS2FAIL)
Power supply 2 failure status

/flash Size (MB) (disk0Size)
Size of /flash partition of the disk.

/flash Used (MB) (disk0Used)
Used space in /flash partition of the disk.

/flash Available (MB) (disk0Avail)
Available space in /flash partition of the disk.

/var Size (MB) (disk1Size)
Size of /var partition of the disk.

/var Used (MB) (disk1Used)
Used space in /var partition of the disk.

/var Available (MB) (disk1Avail)
Available space in /var partition of the disk.

Fan 0 Speed (RPM) (Fan0)
Speed of Fan 0 if associated pin is connected to health monitoring chip.

Fan 1 Speed (RPM) (Fan1)
Speed of Fan 1 if associated pin is connected to health monitoring chip.

Fan 2 Speed (RPM) (Fan2)
Speed of Fan 2 if associated pin is connected to health monitoring chip.

Fan 3 Speed (RPM) (Fan3)
Speed of Fan 3 if associated pin is connected to health monitoring chip.

Temperature 0 (Celsius) (temp0)
Temperature of a device connected to health monitoring chip through pin 0.

Temperature 1 (Celsius) (temp1)
Temperature of a device connected to health monitoring chip through pin 1.

Temperature 2 (Celsius) (temp2)
Temperature of a device connected to health monitoring chip through pin 2.

Temperature 3 (Celsius) (temp3)
Temperature of a device connected to health monitoring chip through pin 3.

Up time (UP)
Seconds since the system started

System memory (MB) (Memory)
Total amount of system memory, in megabytes

CPU usage (CPU)
CPU utilization, percentage * 10

The number of CPUs on the system

Management CPU usage (CPU)
Management CPU utilization, percentage * 10

CPU 0 Core Voltage (Volts) (VCC0)
CPU core 0 voltage. Acceptable range is 1.080 through 1.650 volts.

CPU 1 Core Voltage (Volts) (VCC1)
CPU core 1 voltage. Acceptable range is 1.080 through 1.650 volts. If CPU 1 is not connected to the health monitoring chip, display shows voltage of CPU 0.

Main 3.3 V Supply Voltage (V33Main)
Main power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts. This is a critical counter. You can configure Main 3.3V Supply Voltage,

by using the Set snmp alarm VOLTAGE-LOW command to set the lower limit and the Set snmp alarm VOLTAGE-HIGH command to set the upper limit.

Standby 3.3 V Supply Voltage (V33Stby)
Standby power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts. 9800 and 9960 platforms display standard value of 3.3V. You can configure Standby 3.3V Supply Voltage by using the Set snmp alarm VOLTAGE-LOW command to set the lower limit and the Set snmp alarm VOLTAGE-HIGH command to set the upper limit.

+5.0 V Supply Voltage (V50)
Power supply +5V output. Acceptable range is 4.50 through 5.50 volts.

-5.0 V Supply Voltage (V50n)
Power supply -5V output. Acceptable range is -5.50 through -4.50 volts. 9800 and 9960 platforms display standard value of -5.0V.

+12.0 V Supply Voltage (V+12)
Power supply +12V output. Acceptable range is 10.80 through 13.20 volts.

-12.0 V Supply Voltage (V12n)
Power supply -12V output. Acceptable range is -13.20 through -10.80 volts. 9800 and 9960 platforms display standard value of -12.0V.

Battery Voltage (Volts) (VBAT)
Onboard battery power supply output. 9800 and 9950 platforms display standard value of 5.0V.

Intel CPU Vtt Power(Volts) (VTT)
Intel CPU Vtt power. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

5V Standby Voltage(Volts) (V5SB)
Power Supply 5V Standby Voltage. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

Voltage Sensor2(Volts) (VSEN2)
Voltage Sensor 2 Input. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

Voltage 0 (Volts) (volt0)
Voltage of a device connected to health monitoring chip through pin 0.

Voltage 1 (Volts) (volt1)
Voltage of a device connected to health monitoring chip through pin 1.

Voltage 2 (Volts) (volt2)
Voltage of a device connected to health monitoring chip through pin 2.

Voltage 3 (Volts) (volt3)
Voltage of a device connected to health monitoring chip through pin 3.

Voltage 4 (Volts) (volt4)
Voltage of a device connected to health monitoring chip through pin 4.

Voltage 5 (Volts) (volt5)
Voltage of a device connected to health monitoring chip through pin 5.

Voltage 6 (Volts) (volt6)
Voltage of a device connected to health monitoring chip through pin 6.

Voltage 7 (Volts) (volt7)
Voltage of a device connected to health monitoring chip through pin 7.

Master CPU usage (CPU0)
CPU0 utilization, percentage * 10

Slave CPU usage (CPU1)
CPU1 utilization, percentage * 10

Related Commands

stat system cpu

show system session

Synopsis

```
show system session [<sid>]
```

Description

Display system sessions. System may reclaim sessions with no active connections before expiry time

Arguments

sid
The session id. Minimum value: 1

summary

fullValues

Output

userName
user name of the session

logintime
logged-in time of this session

lastactivitytime
last activity time of on this session

expirytime
Time left in expire the session in seconds

numOfconnections
number of connection using this token

currentconn
True if the token is used for current session

Related Commands

kill system session

kill system session

Synopsis

```
kill system session [<sid> | -all]
```

Description

Kill system sessions.

Arguments

sid

The session id. Minimum value: 1

all

Specify this if you want to kill all sessions except self.

Related Commands

show system session

stat system cpu

Synopsis

```
stat system cpu [<id>] [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

This command displays CPU statistics

Arguments

id

Specifies the CPU ID. Default value: 65535 Maximum value: 65534

Output

Counters

CPU Usage (Usage)

CPU utilization percentage

CPU Usage (Usage)

CPU utilization percentage

Related Commands

stat system

rm system entitydata

Synopsis

```
rm system entitydata [<type>] [<name>] [-allDeleted] [-
allInactive] [-dataSource <string>] [-core <integer>]
```

Description

Arguments

type
Specify the entity type.

name
Specify the entity name.

allDeleted
Specify this if you would like to deleted all deleted entity database.

allInactive
Specify this if you would like to deleted all inactive entity database.

dataSource
Specify data source name.

core
Specify core. Default value: VAL_NOT_SET

Related Commands

show system entitydata

show system entity

Synopsis

```
show system entity <type> [-dataSource <string>] [-core
<integer>]
```

Description

Display entities in historical data.

Arguments

type

Specify the entity type.

dataSource

Specify Data source name.

core

Specify core. Default value: VAL_NOT_SET

Output

Related Commands

show system globaldata

Synopsis

```
show system globaldata <counters> [<countergroup>] [-
startTime <string> | (-last <integer>  [<unit>])] [-
endTime <string>] [-dataSource <string>] [-core
<integer>]
```

Description

Display historical data for global counters.

Arguments

counters
Specify the counters.

countergroup
Specify the counter group.

startTime
Specify start time in mmddyyyyhhmm.

endTime
Specify end time in mmddyyyyhhmm.

last
Specify the counters. Default value: 1

dataSource
Specify data source name.

core
Specify core. Default value: VAL_NOT_SET

Output

Related Commands

show system entitydata

Synopsis

```
show system entitydata <type> <name> <counters> [-
startTime <string> | (-last <integer>  [<unit>])] [-
endTime <string>] [-dataSource <string>] [-core
<integer>]
```

Description

Display historical data for global counters.

Arguments

type

Specify the entity type.

name

Specify the entity name.

counters

Specify the counters.

startTime

Specify end time in mmddyyyyhhmm.

endTime

Specify end time in mmddyyyyhhmm.

last

Specify the counters. Default value: 1

dataSource

Specify Data source name.

core

Specify core. Default value: VAL_NOT_SET

Output

Related Commands

rm system entitydata

show system counters

Synopsis

```
show system counters <countergroup> [-dataSource
<string>]
```

Description

Display entities in historical data.

Arguments

countergroup

Specify the group name.

dataSource

Specify Data source name.

Output

Related Commands

show system countergroup

Synopsis

```
show system countergroup [-dataSource <string>]
```

Description

Display available counter groups.

Arguments

dataSource

Specify Data source name.

Output

Related Commands

add system cmdPolicy

Synopsis

```
add system cmdPolicy <policyName> <action> <cmdSpec>
```

Description

Add a system command Policy to the system.

Arguments

`policyName`

The name for the command policy.

`action`

The action the policy need to apply when the cmdSpec pattern matches. Possible values: ALLOW, DENY

`cmdSpec`

The matching rule that the policy will utilize. This rule is a regular expression which the policy uses to pattern match.

Related Commands

rm system cmdPolicy

set system cmdPolicy

show system cmdPolicy

rm system cmdPolicy

Synopsis

```
rm system cmdPolicy <policyName>
```

Description

Remove a system command policy.

Arguments

policyName

The name of the policy.

Related Commands

add system cmdPolicy

set system cmdPolicy

show system cmdPolicy

set system cmdPolicy

Synopsis

```
set system cmdPolicy <policyName> <action> <cmdSpec>
```

Description

Modify an already configured command Policy.

Arguments

`policyName`

The name for the command policy.

`action`

The action the policy need to apply when the cmdSpec pattern matches. Possible values: ALLOW, DENY

`cmdSpec`

The matching rule that the policy will utilize. This rule is a regular expression which the policy uses to pattern match.

Related Commands

add system cmdPolicy

rm system cmdPolicy

show system cmdPolicy

show system cmdPolicy

Synopsis

```
show system cmdPolicy [<policyName>]
```

Description

Display configured command policies.

Arguments

policyName
The name of a policy.

summary

fullValues

format

level

Output

action
The policy action.

cmdSpec
The matching rule that the policy will utilize.

Related Commands

add system cmdPolicy
rm system cmdPolicy
set system cmdPolicy

add system user

Synopsis

```
add system user <userName>
```

Description

Add a new system user to the system.

Arguments

`userName`

The name for the system user.

`password`

The system user's password.

Related Commands

rm system user

set system user

show system user

rm system user

Synopsis

```
rm system user <userName>
```

Description

Remove a system user.

Arguments

userName

The name of the system user.

Related Commands

add system user

set system user

show system user

set system user

Synopsis

```
set system user <userName>
```

Description

Set a system user's password.

Arguments

`userName`

The name for the system user.

`password`

The system user's password.

Related Commands

add system user

rm system user

show system user

bind system user

Synopsis

```
bind system user <userName> <policyName> <priority>
```

Description

Bind the command policy to a system user.

Arguments

userName

The name of the system user.

policyName

The name of the command policy being bound to the system user.

Related Commands

unbind system user

unbind system user

Synopsis

```
unbind system user <userName> <policyName>
```

Description

Unbind attributes of a system user.

Arguments

`userName`

The name of the system user.

`policyName`

The name of the command policy to be unbound.

Related Commands

bind system user

show system user

Synopsis

```
show system user [<userName>]
```

Description

Display configured system users.

Arguments

userName

The name of a system user.

summary

fullValues

format

level

Output

groupName

The system group.

policyName

The name of command policy.

priority

The priority of the policy.

Related Commands

add system user

rm system user

set system user

show system core

Synopsis

```
show system core [-dataSource <string>]
```

Description

Display entities in historical data.

Arguments

dataSource

Specify Data source name.

Output

Related Commands

show system dataSource

Synopsis

```
show system dataSource [<dataSource>]
```

Description

Display entities in historical data.

Arguments

dataSource

Specify Data source name.

Output

Related Commands

add system group

Synopsis

```
add system group <groupName>
```

Description

Add a new system group.

Arguments

groupName

The name of system group.

Related Commands

rm system group

show system group

rm system group

Synopsis

```
rm system group <groupName>
```

Description

Remove a system group.

Arguments

groupName

The name of the system group.

Related Commands

add system group

show system group

bind system group

Synopsis

```
bind system group <groupName> [-userName <string>] [-
policyName <string>  <priority>]
```

Description

Bind entities to a system group.

Arguments

groupName

The name of the system group.

userName

The name of a system user to be bound to the group.

policyName

The name of the command policy to be bound to the group.

Related Commands

unbind system group

unbind system group

Synopsis

```
unbind system group <groupName> [-userName <string>] [-
policyName <string>]
```

Description

Unbind entities from a system group.

Arguments

groupName

The system group name.

userName

The name of a system user to be unbound from the group.

policyName

The command policy to be be unbound from the group.

Related Commands

bind system group

show system group

Synopsis

```
show system group [<groupName>]
```

Description

Display the configured system groups.

Arguments

groupName
The name of the system group.

summary

fullValues

format

level

Output

userName
The system user.

policyName
The name of command policy.

priority
The priority of the command policy.

Related Commands

add system group
rm system group

bind system global

Synopsis

```
bind system global [<policyName>  [-priority
<positive_integer>]]
```

Description

Bind entities to system global.

Arguments

policyName

The name of the command policy to be bound to system global.

Related Commands

unbind system global

show system global

unbind system global

Synopsis

```
unbind system global <policyName>
```

Description

Unbind entities from system global.

Arguments

`policyName`

The name of the command policy to be unnbound.

Related Commands

bind system global

show system global

show system global

Synopsis

```
show system global
```

Description

Display system global bindings.

Arguments

summary

fullValues

format

level

Output

policyName

The name of the command policy.

priority

The priority of the command policy.

Related Commands

bind system global

unbind system global

set system collectionparam

Synopsis

```
set system collectionparam [-communityName <string>] [-
dataPath <string>]
```

Description

Set a collection parameters.

Arguments

communityName

dataPath

specify the data path

Related Commands

unset system collectionparam

show system collectionparam

unset system collectionparam

Synopsis

```
unset system collectionparam [-communityName] [-
dataPath]
```

Description

Use this command to remove system collectionparam settings.Refer to the set system collectionparam command for meanings of the arguments.

Related Commands

set system collectionparam

show system collectionparam

show system collectionparam

Synopsis

```
show system collectionparam
```

Description

Display collection parameter

Arguments

format

level

Output

communityName

specify the snmp community which is used to collect the data.

logLevel

specify the log level. Possible values
CRITICAL,WARNING,INFO,DEBUG1,DEBUG2

dataPath

specify the data path

Related Commands

set system collectionparam

unset system collectionparam

CHAPTER 28

Tunnel Commands

This chapter covers the tunnel commands.

add tunnel trafficPolicy

Synopsis

```
add tunnel trafficPolicy <name> <rule> <action>
```

Description

Create a tunnel trafficpolicy.

Arguments

`name`

The name of the new tunnel trafficpolicy.

`rule`

The expression specifying the condition under which this policy is applied.

`action`

The name of the action to be performed. The string value may be one of the following built-in compression actions: COMPRESS: Enables default compression (DEFLATE). NOCOMPRESS: Disables compression. GZIP: Enables GZIP compression. DEFLATE: Enables DEFLATE compression.

Example

Example 1: add tunnel trafficpolicy cmp_all_destport "REQ.TCP.DESTPORT == 0-65535" GZIP After creating above tunnel policy, it can be activated by binding it globally: bind tunnel global cmp_all_destport The policy is evaluated for all traffic flowing through the ssl-vpn tunnel, and compresses traffic for all TCP application ports. Example 2: The following tunnel policy disables compression for all access from a specific subnet: add tunnel trafficpolicy local_sub_nocmp "SOURCEIP == 10.1.1.0 -netmask 255.255.255.0" NOCOMPRESS bind tunnel global local_sub_nocmp

Related Commands

rm tunnel trafficPolicy

set tunnel trafficPolicy

unset tunnel trafficPolicy

show tunnel trafficPolicy

rm tunnel trafficPolicy

Synopsis

```
rm tunnel trafficPolicy <name>
```

Description

Remove a tunnel traffic policy.

Arguments

name

The name of the tunnel traffic policy.

Example

rm tunnel trafficpolicy tunnel_policy_name The "show tunnel trafficpolicy" command shows all tunnel policies that are currently defined.

Related Commands

add tunnel trafficPolicy

set tunnel trafficPolicy

unset tunnel trafficPolicy

show tunnel trafficPolicy

set tunnel trafficPolicy

Synopsis

```
set tunnel trafficPolicy <name> [-rule <expression>] [-
action <string>]
```

Description

Modify the rule and/or action of an existing tunnel traffic policy, created using the "add tunnel trafficpolicy" command.

Arguments

`name`
The name of the policy to be modified.

`rule`
The new rule to be used in the policy.

`action`
The new action to be applied by the policy.

Example

add tunnel trafficpolicy cmp_all_destport "REQ.TCP.DESTPORT == 0-65535" GZIP set tunnel trafficpolicy cmp_all_destport -action NOCOMPRESS Above 'set' command changes action for policy cmp_all_destport from GZIP to NOCOMPRESS

Related Commands

add tunnel trafficPolicy

rm tunnel trafficPolicy

unset tunnel trafficPolicy

show tunnel trafficPolicy

unset tunnel trafficPolicy

Synopsis

```
unset tunnel trafficPolicy <name> [-rule] [-action]
```

Description

Use this command to remove tunnel trafficPolicy settings.Refer to the set tunnel trafficPolicy command for meanings of the arguments.

Related Commands

add tunnel trafficPolicy

rm tunnel trafficPolicy

set tunnel trafficPolicy

show tunnel trafficPolicy

show tunnel trafficPolicy

Synopsis

```
show tunnel trafficPolicy [<name>]
```

Description

Display all tunnel policies that are currently defined.

Arguments

name
The name of the tunnel traffic policy.

summary

fullValues

format

level

Output

rule

action

hits
No of hits.

txbytes
Number of bytes transmitted.

rxbytes
Number of bytes received.

clientTTLB
Total client TTLB value.

clientTransactions
Number of client transactions.

serverTTLB
Total server TTLB value.

serverTransactions
Number of server transactions.

boundTo
The entity name to which policy is bound

Example

> show tunnel trafficpolicy 2 Tunnel policies: 1) Name: local_sub_nocmp Rule: SOURCEIP == 10.1.1.0 -netmask 255.255.255.0 Action: NOCOMPRESS Hits: 3 2) Name: cmp_all Rule: REQ.TCP.DESTPORT == 0-65535 Action: GZIP Hits: 57125 Bytes In:...796160 Bytes Out:... 197730 Bandwidth saving...75.16% Ratio 4.03:1 Done

Related Commands

add tunnel trafficPolicy

rm tunnel trafficPolicy

set tunnel trafficPolicy

unset tunnel trafficPolicy

bind tunnel global

Synopsis

```
bind tunnel global (<policyName>  [-priority
<positive_integer>]) [-state ( ENABLED | DISABLED )]
```

Description

Activate the tunnel traffic policy globally. The tunnel policies are created using the "add tunnel trafficpolicy" command. The command "show tunnel trafficpolicy" shows all the existing tunnel policies and the command "show tunnel global" shows all the globally active tunnel policies. Note that the ssl-vpn license is required for tunnel compression feature to work.

Arguments

policyName

The name of the tunnel traffic policy to be bound.

Example

add tunnel trafficpolicy cmp_all_destport "REQ.TCP.DESTPORT == 0-65535" GZIP After creating above tunnel policy, it can be activated by binding it globally: bind tunnel global cmp_all_destport After binding cmp_all_destport compression policy globally, the policy gets activated and the NetScaler will compress all TCP traffic accessed through ssl-vpn tunnel. Globally active tunnel policies can be seen using command: > show tunnel global 1 Globally Active Tunnel Policies: 1) Policy Name: cmp_all_destport Priority: 0 Done

Related Commands

unbind tunnel global

show tunnel global

unbind tunnel global

Synopsis

```
unbind tunnel global <policyName>
```

Description

Deactivate an active tunnel traffic policy. Use command "show tunnel global" to see all the globally active tunnel policies.

Arguments

policyName

The name of the tunnel traffic policy.

Example

Globally active tunnel policies can be seen using command: > show tunnel global 1 Globally Active Tunnel Policies: 1) Policy Name: cmp_all_destport Priority: 0 Done The globally active tunnel traffic policy can be deactivated on the NetScaler system by issuing the command: unbind tunnel global cmp_all_destport

Related Commands

bind tunnel global

show tunnel global

show tunnel global

Synopsis

```
show tunnel global
```

Description

Display global active tunnel policies.

Arguments

summary

fullValues

format

level

Output

policyName
Policy name.

priority
Priority.

state
The current state of the binding.

Example

> sh tunnel global 1) Policy Name: cmp_all_destport Priority: 0 2) Policy Name: local_sub_nocmp Priority: 500 Done

Related Commands

bind tunnel global

unbind tunnel global

CHAPTER 29

High Availability Commands

This chapter covers the High Availability commands.

force HA sync

Synopsis

```
force HA sync [-force  [-save ( YES | NO )]]
```

Description

Force the configuration to be synchronized between the HA pair.

Arguments

force

Initiate force sync irrespective of haprop/hasync states

save

Save/NoSave option for config after sync, without prompts Possible values: YES, NO Default value: VAL_NOT_SET

Example

Can be used in following formats: >force sync <cr> >force sync -force <cr> >force sync -force -save [yes|no]<cr>

Related Commands

sync HA files

Synopsis

```
sync HA files [<Mode> ...]
```

Description

Synchronize SSL Certificates, SSL CRL lists, and SSL VPN bookmarks from the primary node to the secondary node in a high-availability pair. The node in primary state is always considered authoritative. Files are copied from primary to secondary overwriting all differences, even when the command is invoked from a node in secondary state. The sync command supports three modes; all, bookmarks, and ssl. The following paths correspond to the synchronization mode: Mode Paths all /nsconfig/ssl/ /var/vpn/bookmarks/ /nsconfig/htmlinjection/ ssl / nsconfig/ssl/ bookmarks /var/vpn/bookmarks/ htmlinjection / nsconfig/htmlinjection/

Arguments

Mode

The sync mode.

Example

sync files all

Related Commands

force HA failover

Synopsis

```
force HA failover [-force]
```

Description

Trigger a failover.

Arguments

force

Initiate force failover without confirmation.

Related Commands

add HA node

Synopsis

```
add HA node <id> <IPAddress> [-inc ( ENABLED | DISABLED )]
```

Description

Add the IP address of the other system in the high availability configuration. The IP addresses of the both the systems must belong to the same subnet.

Arguments

`id`

The unique number that identifies the node. Minimum value: 1 Maximum value: 64

`IPAddress`

The IP address of the node to be added. This should be in same subnet as NSIP.

`inc`

The state of INC mode. Possible values: ENABLED, DISABLED Default value: DISABLED

Related Commands

rm HA node

set HA node

unset HA node

bind HA node

unbind HA node

show HA node

stat HA node

rm HA node

Synopsis

```
rm HA node <id>
```

Description

Remove a node.

Arguments

id

The unique number that identifies the node. Minimum value: 1 Maximum value: 64

Related Commands

add HA node

set HA node

unset HA node

bind HA node

unbind HA node

show HA node

stat HA node

set HA node

Synopsis

```
set HA node [-haStatus <haStatus>] [-haSync ( ENABLED |
DISABLED )] [-haProp ( ENABLED | DISABLED )] [-
helloInterval <msecs>] [-deadInterval <secs>]
```

Description

Set the HA status of the current node and configure synchronization.

Arguments

id

The unique number that identifies the node. Default value: 0 Minimum value: 0 Maximum value: 64

haStatus

The HA status of the node. The HA status STAYSECONDARY is used to force the secondary device stay as secondary independent of the state of the Primary device. For example, in an existing HA setup, the Primary node has to be upgraded and this process would take few seconds. During the upgradation, it is possible that the Primary node may suffer from a downtime for a few seconds. However, the Secondary should not take over as the Primary node. Thus, the Secondary node should remain as Secondary even if there is a failure in the Primary node. Possible values: ENABLED, STAYSECONDARY, DISABLED, STAYPRIMARY

haSync

The state of synchronization. Possible values: ENABLED, DISABLED Default value: ENABLED

haProp

The state of propagation. The valid values are Enabled and Disabled. Possible values: ENABLED, DISABLED Default value: ENABLED

helloInterval

The Hello Interval in milliseconds. Default value: 200 Minimum value: 200 Maximum value: 1000

`deadInterval`
The Dead Interval in seconds. Default value: 3 Minimum value: 3 Maximum value: 60

Related Commands

add HA node
rm HA node
unset HA node
bind HA node
unbind HA node
show HA node
stat HA node

unset HA node

Synopsis

```
unset HA node [-haStatus] [-haSync] [-haProp] [-
helloInterval] [-deadInterval]
```

Description

Use this command to remove HA node settings.Refer to the set HA node command for meanings of the arguments.

Related Commands

add HA node
rm HA node
set HA node
bind HA node
unbind HA node
show HA node
stat HA node

bind HA node

Synopsis

```
bind HA node [<id>] -routeMonitor <ip_addr|*> <netmask>
```

Description

Monitor the presence of a route in the FIB.

Arguments

id

The unique number that identifies the node. Default value: 0 Minimum value: 1 Maximum value: 64

routeMonitor

Route monitor.

Related Commands

add HA node

rm HA node

set HA node

unset HA node

unbind HA node

show HA node

stat HA node

unbind HA node

Synopsis

```
unbind HA node [<id>] -routeMonitor <ip_addr|*>
<netmask>
```

Description

Unbind a route monitor from the node.

Arguments

id

The unique number that identifies the node. Default value: 0 Minimum value: 1 Maximum value: 64

routeMonitor

Route monitor.

Related Commands

add HA node
rm HA node
set HA node
unset HA node
bind HA node
show HA node
stat HA node

show HA node

Synopsis

```
show HA node [<id>]
```

Description

Display all nodes. It also displays the number of additional nodes, ID, IP address, and the state of all nodes.

Arguments

id
Node id.

summary

fullValues

format

level

Output

name
Node Name.

IPAddress
IP Address of the node.

flags
The flags for this entry.

haStatus
HA status.

state
HA Master State.

haSync
HA Sync State.

haProp
HA Propagation Status.

enaifaces
Enabled interfaces.

disifaces
Disabled interfaces.

hamonifaces
HAMON ON interfaces.

pfifaces
Interfaces causing Partial Failure.

ifaces
Interfaces on which non-multicast is not seen.

network
The network.

netmask
The netmask.

inc
INC state.

ssl2
SSL card status.

helloInterval
Hello Interval.

deadInterval
Dead Interval.

masterStateTime
Time elapsed in current master state

Example

An example of the command's output is as follows: 2 configured nodes: 1) Node ID: 0 IP: 192.168.100.5 Primary node 2) Node ID: 2 IP: 192.168.100.112 Secondary node

Related Commands

add HA node
rm HA node
set HA node
unset HA node
bind HA node
unbind HA node
stat HA node

stat HA node

Synopsis

```
stat HA node [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display high-availability protocol statistics.

Arguments

Output

Counters

High Availability (HA)

Indicates whether a NetScaler is set up for high availability. Possible values are YES and NO. If the value is NO, the high availability statistics below are invalid.

System state (HAState)

State of the node, based on its health, in a high availability setup. Possible values are: UP ? Indicates that the node is accessible and can function as either a primary or secondary node. DISABLED ? Indicates that the high availability status of the node has been manually disabled. Synchronization and propagation cannot take place between the peer nodes. INIT ? Indicates that the node is in the process of becoming part of the high availability configuration. PARTIALFAIL ? Indicates that one of the high availability monitored interfaces has failed because of a card or link failure. This state triggers a failover. COMPLETEFAIL ? Indicates that all the interfaces of the node are unusable, because the interfaces on which high availability monitoring is enabled are not connected or are manually disabled. This state triggers a failover. DUMB ? Indicates that the node is in listening mode. It does not participate in high availability transitions or transfer configuration from the peer node. This is a configured value, not a statistic. PARTIALFAILSSL ? Indicates that the SSL card has failed. This state triggers a failover. ROUTEMONITORFAIL ? Indicates that the route monitor has failed. This state triggers a failover.

Master state (mastate)
Indicates the high availability state of the node. Possible values are: STAYSECONDARY ? Indicates that the selected node remains the secondary node in a high availability setup. In this case a forced failover does not change the state but, instead, returns an appropriate error message. This is a configured value and not a statistic. PRIMARY ? Indicates that the selected node is the primary node in a high availability setup. SECONDARY ? Indicates that the selected node is the secondary node in a high availability setup. CLAIMING ? Indicates that the secondary node is in the process of taking over as the primary node. This is the intermediate state in the transition of the secondary node to primary status. FORCE CHANGE - Indicates that the secondary node is forcibly changing its status to primary due to a forced failover issued on the secondary node.

Last Transition time (TransTime)
Time when the last master state transition occurred. You can use this statistic for debugging.

Heartbeats received (HApktrx)
Number of heartbeat packets received from the peer node. Heartbeats are sent at regular intervals (default is 200 milliseconds) to determine the state of the peer node.

Heartbeats sent (HApkttx)
Number of heartbeat packets sent to the peer node. Heartbeats are sent at regular intervals (default is 200 milliseconds) to determine the state of the peer node.

Propagation timeouts (ptimeout)
Number of times propagation timed out

Sync failure (syncfail)
Number of times the configuration of the primary and secondary nodes failed to synchronize since that last transition. A synchronization failure results in mismatched configuration. It can be caused by a mismatch in the Remote Procedural Call (RPC) password on the two nodes forming the high availability pair.

Related Commands

add HA node

rm HA node

set HA node
unset HA node
bind HA node
unbind HA node
show HA node

CHAPTER 30

Networking Commands

This chapter covers the networking commands.

clear nd6

Synopsis

```
clear nd6
```

Description

Clear all the dynamically learnt IPv6 neighbor entries (ND6)

Example

clear nd6

Related Commands

add nd6

rm nd6

show nd6

add arp

Synopsis

```
add arp -IPAddress <ip_addr> -mac <mac_addr> -ifnum
<interface_name>
```

Description

Add a static entry to the system's ARP table. This ARP entry never times out.

Arguments

IPAddress

The IP address of the server.

mac

The MAC address of the server. Enter the MAC address with the colons (:) as the example shows.

ifnum

The physical interface for the ARP entry. Use the show interface command to view the valid interface names.

Example

add arp -ip 10.100.0.48 -mac 00:a0:cc:5f:76:3a -ifnum 1/1

Related Commands

rm arp

send arp

show arp

rm arp

Synopsis

```
rm arp (<IPAddress> | -all)
```

Description

Remove an entry from the system's ARP table.

Arguments

IPAddress

The IP address whose entry is to be removed.

all

Remove all entries from the system's ARP table.

Related Commands

add arp

send arp

show arp

send arp

Synopsis

```
send arp (<IPAddress> | -all)
```

Description

Send out an ARP for an IP address or for all IP addresses.

Arguments

IPAddress

The IP address for which the ARP needs to be sent.

all

Send an ARP out for all System-owned IP addresses for which ARP is enabled.

Example

send arp 10.10.10.10

Related Commands

add arp

rm arp

show arp

show arp

Synopsis

```
show arp [<IPAddress>]
```

Description

Display all the entries in the system's ARP table.

Arguments

`IPAddress`
The IP address corresponding to an ARP entry.

`summary`

`fullValues`

`format`

`level`

Output

`mac`
The MAC address corresponding to an ARP entry.

`ifnum`
The interface on which this MAC address resides.

`timeout`
The time when this entry will timeout.

`state`
The state of this ARP entry.

`flags`
The flags for this entry.

`type`
The flags for this entry.

vlan

The VLAN for this ARP entry.

Example

The output of the sh arp command is as follows: 5 configured arps: IP MAC Inface VLAN Origin ------- ------- ------- ---- ------- 1) 10.250.11.1 00:04:76:dc:f1:b9 1/2 2 dynamic 2) 10.11.0.254 00:30:19:c1:7e:f4 1/1 1 dynamic 3) 10.11.0.41 00:d0:a8:00:7c:e4 0/1 1 dynamic 4) 10.11.222.2 00:ee:ff:22:00:01 0/1 1 dynamic 5) 10.11.201.12 00:30:48:31:23:49 0/1 1 dynamic

Related Commands

add arp

rm arp

send arp

show ci

Synopsis

```
show ci
```

Description

Displays the CIs.

Arguments

summary

fullValues

Output

ifaces

Interfaces that are critical.

Example

>show ci Critical Interfaces: LO/1 1/2

Related Commands

clear interface

Synopsis

```
clear interface <id>
```

Description

Clear the statistics of the specified interface. It does not reset the interface. Note:Resetting the interface will not clear the statistics.

Arguments

id

The number of the interface to be cleared.

Related Commands

set interface

unset interface

enable interface

disable interface

reset interface

show interface

stat interface

clear route

Synopsis

```
clear route <routeType>
```

Description

Clear the Routes.

Arguments

routeType

The type of routes to be cleared.

Related Commands

add route

rm route

set route

unset route

show route

clear route6

Synopsis

```
clear route6 <routeType>
```

Description

Clear the ipv6 routes.

Arguments

routeType

The type of routes to be cleared.

Related Commands

add route6

rm route6

set route6

unset route6

show route6

clear rnat

Synopsis

```
clear rnat ((<network>  [<netmask>]) | (<aclname>  [-
redirectPort])) [-natIP <ip_addr|*> ...]
```

Description

Clear the Reverse NAT configuration.

Arguments

network

The network or subnet from which the traffic is flowing.

netmask

The netmask of the network.

aclname

The acl name.

redirectPort

The redirect port. Default value: NS_REDIRECTPORT

natIP

The NAT IP(s) assigned to a source IP or System IP.

Related Commands

set rnat

unset rnat

stat rnat

show rnat

set bridgetable

Synopsis

```
set bridgetable -bridgeAge <positive_integer>
```

Description

Set the aging time for bridge table entries. Dynamic bridge entries are automatically removed after a specified time, the ageing time, has elapsed since the entry was created or last updated.

Arguments

bridgeAge

The bridge ageing time in seconds. Default value: 300 Minimum value: 60 Maximum value: 300

Example

set bridgetable -bridgeAge 200

Related Commands

unset bridgetable

show bridgetable

unset bridgetable

Synopsis

```
unset bridgetable -bridgeAge
```

Description

Use this command to remove bridgetable settings.Refer to the set bridgetable command for meanings of the arguments.

Related Commands

set bridgetable

show bridgetable

show bridgetable

Synopsis

```
show bridgetable
```

Description

Display the bridge ageing time and bridging table.

Arguments

summary

fullValues

format

level

Output

bridgeAge
The bridge ageing time in seconds.

mac
The MAC address of target.

ifnum
The interface on which the address was learnt.

vlan
The VLAN in which this MAC address lies.

Example

show bridgetable

Related Commands

set bridgetable
unset bridgetable

stat bridge

Synopsis

```
stat bridge [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display bridging statistics.

Arguments

Output

Counters

`Loops`

The number of times bridging registered MAC moved

`Collisions (Collisns)`

The number of bridging table collisions

`Interface muted (Mutes)`

The number of bridging related interface mutes

Related Commands

stat interface

stat rnat

stat rnatip

stat vlan

add channel

Synopsis

```
add channel <id> [-ifnum <interface_name> ...] [-state
( ENABLED | DISABLED )] [-Mode <Mode>] [-connDistr (
DISABLED | ENABLED )] [-macdistr <macdistr>] [-speed
<speed>] [-flowControl <flowControl>] [-haMonitor ( ON
| OFF )] [-trunk ( ON | OFF )] [-ifAlias <string>] [-
throughput <positive_integer>] [-bandwidthHigh
<positive_integer>  [-bandwidthNormal
<positive_integer>]]
```

Description

Add the specified Link Aggregate channel in the system.

Arguments

id

LA channel name (in form LA/*)

ifnum

the interfaces to be bound to Link Aggregate channel.

state

The initial state for the LA channel. Possible values: ENABLED, DISABLED Default value: NSA_DVC_ENABLE

Mode

The initital mode for the LA channel. Possible values: MANUAL, AUTO, DESIRED

connDistr

The 'connection' distribution mode for the LA channel. Possible values: DISABLED, ENABLED

macdistr

The 'MAC' distribution mode for the LA channel. Possible values: SOURCE, DESTINATION, BOTH

speed
The speed for the LA channel. Possible values: AUTO, 10, 100, 1000, 10000

flowControl
Flow control for the LA channel. Possible values: OFF, RX, TX, RXTX

haMonitor
The HA-monitoring for the LA channel. Possible values: ON, OFF

trunk
The option to select whether this port is a trunk port or not..By default, this is set to OFF for all interfaces. When ON, the port membership in all vlans will be tagged.If one wants 802.1q behaviour with native vlan use the OFF setting for this variable. Possible values: ON, OFF Default value: OFF

ifAlias
The alias name for the channel.

throughput
Minimum required throughput for the interface. Default value: VAL_NOT_SET

bandwidthHigh
Configured high threshold of the interface bandwidth usage in Mbits/s. Trap will be sent if bandwidth usage of the interface crosses this limit. Default value: VAL_NOT_SET

Related Commands

rm channel

set channel

unset channel

bind channel

unbind channel

show channel

rm channel

Synopsis

```
rm channel <id>
```

Description

Remove the specified Link Aggregate channel from the system.

Arguments

`id`

LA channel name (in form LA/*)

Related Commands

add channel

set channel

unset channel

bind channel

unbind channel

show channel

set channel

Synopsis

set channel <id> [-state (ENABLED | DISABLED)] [-Mode <Mode>] [-connDistr (DISABLED | ENABLED)] [-macdistr <macdistr>] [-speed <speed>] [-flowControl <flowControl>] [-haMonitor (ON | OFF)] [-trunk (ON | OFF)] [-ifAlias <string>] [-throughput <positive_integer>] [-bandwidthHigh <positive_integer> [-bandwidthNormal <positive_integer>]]

Description

This command sets configuration of the specified Link Aggregate channel.

Arguments

id

LA channel name (in form LA/*)

state

The packet processing state for the LA channel. Possible values: ENABLED, DISABLED Default value: NSA_DVC_ENABLE

Mode

The mode for the LA channel. Possible values: MANUAL, AUTO, DESIRED

connDistr

The 'connection' distribution mode for the LA channel. Possible values: DISABLED, ENABLED

macdistr

The 'MAC' distribution mode for the LA channel. Possible values: SOURCE, DESTINATION, BOTH

speed

The speed for the LA channel. Possible values: AUTO, 10, 100, 1000, 10000

flowControl
Sets required flow control for the LA channel. Possible values: OFF, RX, TX, RXTX

haMonitor
The state of HA-monitoring for the LA channel. Possible values: ON, OFF

trunk
The option to select whether this port is a trunk port or not. By default, this is set to OFF for all interfaces. When ON, all the vlans will be tagged. If one wants 802.1q with native vlan behaviour use the OFF setting for this variable. Possible values: ON, OFF Default value: OFF

ifAlias
The alias name for the interface.

throughput
Minimum required throughput for the interface. Default value: VAL_NOT_SET

bandwidthHigh
Configured high threshold of the interface bandwidth usage in Mbits/s. Trap will be sent if bandwidth usage of the interface crosses this limit. Default value: VAL_NOT_SET

Related Commands

add channel

rm channel

unset channel

bind channel

unbind channel

show channel

unset channel

Synopsis

```
unset channel <id> [-state] [-Mode] [-connDistr] [-
macdistr] [-speed] [-flowControl] [-haMonitor] [-trunk]
[-ifAlias] [-throughput] [-bandwidthHigh] [-
bandwidthNormal]
```

Description

Use this command to remove channel settings.Refer to the set channel command for meanings of the arguments.

Related Commands

add channel

rm channel

set channel

bind channel

unbind channel

show channel

bind channel

Synopsis

```
bind channel <id> <ifnum> ...
```

Description

This command binds specified interfaces to the Link Aggregate channel.

Arguments

`id`

LA channel name (in form LA/*)

`ifnum`

Interfaces to be bound to the LA channel.

Related Commands

add channel

rm channel

set channel

unset channel

unbind channel

show channel

unbind channel

Synopsis

```
unbind channel <id> <ifnum> ...
```

Description

This command unbinds specified interfaces from the Link Aggregate channel.

Arguments

`id`

LA channel name (in form LA/*)

`ifnum`

Interfaces to be unbound to the LA channel.

Related Commands

add channel

rm channel

set channel

unset channel

bind channel

show channel

show channel

Synopsis

```
show channel [<id>]
```

Description

show the Link Aggregate channel settings configured in the system for the specified channel. If channel is not specified, the settings are shown for all channels in a brief format.

Arguments

`id`
LA channel name (in form LA/*) Minimum value: 1

`summary`

`fullValues`

`format`

`level`

Output

`deviceName`
Name of the channel.

`unit`
Unit number of this channel.

`description`
Device descriptor.

`flags`
Flags of this channel.

`mtu`
Mtu of the channel.

`vlan`
Native vlan of the channel.

mac
Mac address of the channel.

uptime
Uptime of the channel (Example: 3 hours 1 minute 1 second).

reqMedia
Requested media for this channel.

reqSpeed
Requested speed for this channel.

reqDuplex
Requested duplex setting for this channel.

reqFlowcontrol
Requested flow control for this channel.

media
Actual media for this channel.

speed

duplex
Actual duplex setting for this channel.

flowControl

connDistr

macdistr

Mode

haMonitor

state

autoneg
Requested auto negotiation setting for this channel.

autonegResult
Actual auto negotiation setting for this channel.

tagged
Vlan tags setting on this channel.

trunk

taggedAny
Channel setting to accept/drop all tagged packets.

taggedAutolearn
Dynaminc vlan membership on this channel.

hangDetect
Hang detect for this channel.

hangReset
Hang reset for this channel.

rxpackets
Total number of packets recevied on this channel.

rxbytes
Total number of bytes recevied on this channel.

rxerrors
Total number of receive errors reported on this channel.

rxdrops
Total number of receive drops reported on this channel.

txpackets
Total number of packets transmitted on this channel.

txbytes
Total number of bytes transmitted on this channel.

txerrors
Total number of transmit errors on this channel.

txdrops
Total number of transmit drops on this channel.

inDisc
Total number of inbound error-free packets discarded in the channel.

outDisc
Total number of outbound error-free packets discarded in the channel.

fctls
Total number of times flow control is done on this channel.

hangs
Number of hangs on this channel.

stsStalls

txStalls

rxStalls

bdgMuted
NIC muted.

vmac
Virtual MAC of this channel.

vmac6
Virtual MAC for IPv6 of this interface.

ifAlias
The alias name for the interface.

reqThroughput
Minimum required throughput for the interface.

throughput
Actual throughput for the interface.

`bandwidthHigh`
Configured high threshold of the interface bandwidth usage in Mbits/s. Trap will be sent if bandwidth usage of the interface crosses this limit.

`bandwidthNormal`
Configured normal threshold of the interface bandwidth usage in Mbits/s. Trap will be sent if bandwidth usage of the interface comes back to this limit.

Related Commands

add channel

rm channel

set channel

unset channel

bind channel

unbind channel

add fis

Synopsis

```
add fis <name>
```

Description

Add an FIS. Each FIS is identified by a name (string max 31 letters). The FIS created is empty (without members).

Arguments

name

The name of the FIS. This name must not exceed 31 characters.

Related Commands

rm fis

bind fis

unbind fis

show fis

rm fis

Synopsis

```
rm fis <name>
```

Description

Removes the FIS created by the add fis command. Once the FIS is removed, its interfaces become CIs.

Arguments

name

The name of the FIS.

Related Commands

add fis

bind fis

unbind fis

show fis

bind fis

Synopsis

```
bind fis <name> <ifnum> ...
```

Description

Bind interfaces to a FIS. Adding an interface to an FIS deletes it from CIs and adds it to the new FIS.

Arguments

`name`

The name of the FIS.

`ifnum`

The interface name represented in the <slot/port> notation. For example 1/1. Use the ###show interface### command to view the system interfaces.

Related Commands

add fis

rm fis

unbind fis

show fis

unbind fis

Synopsis

```
unbind fis <name> <ifnum> ...
```

Description

Unbind the specified interface from the FIS. The interface unbound becomes a CI.

Arguments

`name`

The name of the FIS.

`ifnum`

The interface name represented in the <slot/port> notation. For example 1/1. Use the ###show interface### command to view the system interfaces.

Related Commands

add fis

rm fis

bind fis

show fis

show fis

Synopsis

```
show fis [<name>]
```

Description

Displays the configured FISs.

Arguments

name

The name of the FIS.

summary

fullValues

format

level

Output

ifaces

Interfaces bound to theFIS.

Example

>show fis 1) FIS: fis1 Member Interfaces : 1/1 Done

Related Commands

add fis

rm fis

bind fis

unbind fis

set interface

Synopsis

```
set interface <id> [-speed <speed>] [-duplex <duplex>]
[-flowControl <flowControl>] [-autoneg ( DISABLED |
ENABLED )] [-haMonitor ( ON | OFF )] [-trunk ( ON | OFF
)] [-lacpMode <lacpMode>] [-lacpKey <positive_integer>]
[-lacpPriority <positive_integer>] [-lacpTimeout ( LONG
| SHORT )] [-ifAlias <string>] [-throughput
<positive_integer>] [-bandwidthHigh <positive_integer>
[-bandwidthNormal <positive_integer>]]
```

Description

This command sets attributes for the system interface specified by the ifnum variable.

Arguments

id

The number of the interface.

speed

The Ethernet speed for the interface specified by ifnum. The default setting is AUTO. This means that the system will attempt auto-negotiate or auto-sense the line speed on this interface when this interface is brought up. Setting a speed other than AUTO on an interface requires the device at the other end of the link to be configured identically. Mismatching speed and/or duplex configurations on two ends will lead to link errors, packet losses, and so on. It must be avoided. Some interfaces do not support certain speeds. If you try to set a speed on an interface that does not support it, it is reported as an error. Possible values: AUTO, 10, 100, 1000, 10000 Default value: NSA_DVC_SPEED_AUTO

duplex

The duplex mode for the interface. The default setting is AUTO. This means that the system will attempt auto-negotiate for the duplex mode on this interface when this interface is brought up. Other duplex modes you can specify are half and full duplex. The system recommends that the speed

remain as AUTO. If you need to force the duplex mode, then set both the duplex mode and speed manually identically on both side of the link. Possible values: AUTO, HALF, FULL Default value: NSA_DVC_DUPLEX_AUTO

`flowControl`
The required 802.3x flow control for the system interface. You can specify OFF (the default), RX, TX, RXTX and ON (which means "forced RXTX"). For Fast Ethernet interfaces, only OFF is available. 802.3x specification does not define the flow control for speeds 10 and 100 MB but Gigabit Ethernet interfaces still support it for all three possible speeds. Real flow control status depend on the auto-negotiation results. Option ON still use the auto-negotiation to give the peer opportunity to negotiate the flow control but then force the two-way flow control for this interface. As for any other link parameters mismatches it sometimes can cause problems and should be avoided and checked throughly. Possible values: OFF, RX, TX, RXTX Default value: NSA_DVC_FC_OFF

`autoneg`
The state of the auto negotiation for the specified interface. Possible values: DISABLED, ENABLED Default value: NSA_DVC_AUTONEG_ON

`haMonitor`
The state of high availability configuration to specify which interfaces to monitor for failing events. By default, this is set to ON for all interfaces. When ON, in a HA configuration the failover occurs when an interface fails. If an interface is not being used, or if failover is not required, select the value as OFF. Also if interface is not used in current configuration than it is advisable to completely disable it using the disable interface command. Possible values: ON, OFF Default value: NSA_DVC_MONITOR_ON

`trunk`
The option to select whether this port is a trunk port or not for the interface. By default, this is set to OFF for all interfaces. When ON, the traffic will be tagged for all vlans bound to this interface. If one wants 802.1q behaviour with backward compatibility the OFF setting for this variable. Possible values: ON, OFF Default value: NSA_DVC_VTRUNK_OFF

`lacpMode`
LACP mode Possible values: DISABLED, ACTIVE, PASSIVE Default value: DISABLED

lacpKey
LACP key Minimum value: 1 Maximum value: 4

lacpPriority
LACP port priority Default value: 32768 Minimum value: 1 Maximum value: 65535

lacpTimeout
LACP timeout Possible values: LONG, SHORT Default value: NSA_LACP_TIMEOUT_LONG

ifAlias
The alias name for the interface.

throughput
Minimum required throughput for the interface. Default value: VAL_NOT_SET

bandwidthHigh
Configured high threshold of the interface bandwidth usage in Mbits/s. Trap will be sent if bandwidth usage of the interface crosses this limit. Default value: VAL_NOT_SET

Related Commands

clear interface
unset interface
enable interface
disable interface
reset interface
show interface
stat interface

unset interface

Synopsis

```
unset interface <id> [-speed] [-duplex] [-flowControl]
[-autoneg] [-haMonitor] [-trunk] [-lacpMode] [-lacpKey]
[-lacpPriority] [-lacpTimeout] [-ifAlias] [-
throughput] [-bandwidthHigh] [-bandwidthNormal]
```

Description

Use this command to remove interface settings.Refer to the set interface command for meanings of the arguments.

Related Commands

clear interface

set interface

enable interface

disable interface

reset interface

show interface

stat interface

enable interface

Synopsis

```
enable interface <id>
```

Description

Enable the interface.All interfaces are enabled by default.This command to used if interface is disabled.

Arguments

id

The interface name.

Related Commands

clear interface

set interface

unset interface

disable interface

reset interface

show interface

stat interface

disable interface

Synopsis

```
disable interface <id>
```

Description

Disable the interface specified by the ifnum argument. Interface monitoring for high availability mode is also disabled. The system does not receive or transmit any packets on this interface and LCD indicator does not shows "link down" alerts for this disabled interface. Note:To see the status of an interface, use the show interface command.

Arguments

id

The number of the interface to be disabled.

Related Commands

clear interface

set interface

unset interface

enable interface

reset interface

show interface

stat interface

reset interface

Synopsis

```
reset interface <id>
```

Description

Reset the specified interface. The interface saves the configured settings of duplex, speed, and so on. Interface breaks the connection and then tries to reestablish the link using the current settings. If Ethernet autonegotiation is enabled for this interface then resulting link state depends on the counterpart Ethernet port settings.

Arguments

`id`
The number of the interface.

Related Commands

clear interface
set interface
unset interface
enable interface
disable interface
show interface
stat interface

show interface

Synopsis

```
show interface [<id>] show interface stats - alias for
'stat interface'
```

Description

Show the interface settings configured in the system for the specified interface number. If ifnum is not specified, the settings are shown for all interfaces (in a brief format).

Arguments

id
The number of the interface. Minimum value: 1

summary

fullValues

format

level

Output

state

deviceName
Name of the interface.

unit
Unit number of this interface.

description
Device descriptor.

flags
Flags of this interface.

mtu
MTU of the interface.

vlan
Native vlan of the interface.

mac
Mac address of the interface.

uptime
Uptime of the interface (Example: 3 hours 1 minute 1 second).

downTime
Downtime of the interface.

reqMedia
Requested media for this interface.

reqSpeed
Requested speed for this interface.

reqDuplex
Requested duplex setting for this interface.

reqFlowcontrol
Requested flow control for this interface.

media
Media for this interface.

speed

duplex

flowControl

connDistr
Connection distribution setting on this interface.

macdistr
MAC distribuition setting on this interface.

Mode
Interface mode setting.

haMonitor

state
State of the interface.

autoneg

autonegResult
Actual auto negotiation setting for this interface.

tagged
Vlan tags setting on this channel.

trunk

taggedAny
Interface setting to accept/drop all tagged packets.

taggedAutolearn
Dynaminc vlan membership on this interface.

hangDetect
Hang detect for this interface.

hangReset
Hang reset for this interface.

rxpackets
Total number of packets recevied on this interface.

rxbytes
Total number of bytes recevied on this interface.

rxerrors
Total number of receive errors reported on this interface.

rxdrops
Total number of receive drops reported on this interface.

txpackets
Total number of packets transmitted on this interface.

txbytes
Total number of bytes transmitted on this interface.

txerrors
Total number of transmit errors on this interface.

txdrops
Total number of transmit drops on this interface.

inDisc
Total number of inbound error-free packets discarded in the interface.

outDisc
Total number of outbound error-free packets discarded in the interface.

fctls
Total number of times flow control is done on this interface.

hangs
Number of hangs on this interface.

stsStalls
Total number of status stalls on this interface.

txStalls
Total number oftransmit stalls on this interface.

rxStalls
Total number of receive stalls on this interface.

bdgMacMoved
Mac moved.

bdgMuted
NIC muted.

vmac
Virtual MAC of this interface.

vmac6
Virtual MAC for IPv6 of this interface.

lacpMode
lacp mode

lacpKey
lacp key

lacpPriority
lacp priority

lacpTimeout
lacp timeout

ifAlias
The alias name for the interface.

reqThroughput
Minimum required throughput for the interface.

throughput
Actual throughput for the interface.

bandwidthHigh
Configured high threshold of the interface bandwidth usage in Mbits/s. Trap will be sent if bandwidth usage of the interface crosses this limit.

bandwidthNormal
Configured normal threshold of the interface bandwidth usage in Mbits/s. Trap will be sent if bandwidth usage of the interface comes back to this limit.

Example

The output for the show interface command is as follows: 5 interfaces: 1) Interface 0/1 (NIC 0/bx0) Broadcom BCM5701A10 1000Base-T flags=0x2c081 <ENABLE, UP, autoneg on, HAMONITOR ON, 802.1q support> mtu=1514, native vlan=1, eaddr=00:30:48:31:22:f6, uptime 2h24m03s Requested: media AUTO, speed AUTO, duplex AUTO, fctl RXTX, throughput 0 Actual: media UTP, speed 1000, duplex FULL, fctl RXTX, throughput 1000 2) Interface 1/1 (NIC 1/bx1) 3Com 3C996BT Gigabit Server NIC flags=0x2c081 <ENABLE, UP, autoneg on, HAMONITOR ON, 802.1q support> mtu=1514, native vlan=1, eaddr=00:04:76:ef:03:33, uptime 2h24m03s Requested: media AUTO, speed AUTO, duplex AUTO, fctl RXTX, throughput 0 Actual: media UTP, speed 1000, duplex FULL, fctl RXTX, throughput 1000 3) Interface 1/3 (NIC 2/

bx2) 3Com 3C996BT Gigabit Server NIC flags=0x2c081 <ENABLE, UP, autoneg on, HAMONITOR ON, 802.1q support> mtu=1514, native vlan=3, eaddr=00:04:76:eb:d4:46, uptime 2h24m03s Requested: media AUTO, speed AUTO, duplex AUTO, fctl RXTX, throughput 0 Actual: media UTP, speed 1000, duplex FULL, fctl RXTX, throughput 1000 4) Interface 1/2 (NIC 3/ bx3) 3Com 3C996BT Gigabit Server NIC flags=0x2c081 <ENABLE, UP, autoneg on, HAMONITOR ON, 802.1q support> mtu=1514, native vlan=2, eaddr=00:04:76:ef:03:32, uptime 2h24m03s Requested: media AUTO, speed AUTO, duplex AUTO, fctl RXTX, throughput 0 Actual: media UTP, speed 1000, duplex FULL, fctl RXTX, throughput 1000 5) Interface 1/4 (NIC 4/ bx4) 3Com 3C996BT Gigabit Server NIC flags=0x24000 <disable, down, autoneg on, 802.1q support> mtu=1514, native vlan=1, eaddr=00:04:76:eb:cd:d0, uptime 2h24m03s Requested: media AUTO, speed AUTO, duplex AUTO, fctl RXTX, throughput 0 Actual: media AUTO, speed AUTO, duplex AUTO, fctl RXTX, throughput 100 The output for the show interface 1/1 command is as follows: Interface 1/1 (NIC 1/bx1) 3Com 3C996BT Gigabit Server NIC flags=0x2c081 <ENABLE, UP, autoneg on, HAMONITOR ON, 802.1q support> mtu=1514, native vlan=1, eaddr=00:04:76:ef:03:33, uptime 2h24m33s Requested: media AUTO, speed AUTO, duplex AUTO, fctl RXTX, throughput 0 Actual: media UTP, speed 1000, duplex FULL, fctl RXTX, throughput 1000 RX: Pkts(16010) Bytes(1386354) Errs(3) Drops(5261) TX: Pkts(17132) Bytes(2344334) Errs(0) Drops(0) NIC: InDisc(0) OutDisc(0) Fctls(0) Hangs(0)

Related Commands

clear interface

set interface

unset interface

enable interface

disable interface

reset interface

stat interface

stat interface

Synopsis

```
stat interface [<id>] [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display statistics of interface(s).

Arguments

id

Specifies the number of the interface.

Output

Counters

Link State (State)

Current state of the link or logical interface.

Link uptime (UpTime)

Duration for which the link is UP. Counter is reset when the state changes to DOWN.

Link downtime (DnTime)

Duration for which the link is DOWN. Counter is reset when the state changes to UP.

Bytes received (Rx Bytes)

Bytes received on the interface.

Bytes transmitted (Tx Bytes)

Bytes transmitted from the interface.

Packets received (Rx Pkts)

Packets received on the interface.

Packets transmitted (Tx Pkts)

Packets transmitted from the interface.

Multicast packets (McastPkt)
Packets, received on the interface, which are destined for multiple hosts.

NetScaler packets (NSPkt)
Packets (received on this interface) in which the destination MAC address is either the address of one of the NetScaler interfaces or the VMAC address configured by the user.

LACPDUs received (RxLacpdu)
Total Link Aggregation Control Protocol Data Units (LACPDUs) received on the selected port. To transmit a LACPDU, the port has to be a member of dynamic link aggregation.

LACPDUs transmitted (TxLacpdu)
Total LACPDUs transmitted by the selected port. To transmit a LACPDU, the port has to be a member of dynamic link aggregation.

Error packets received (hw) (ErrRx)
Erroneous packets received on the interface. For example, a packet consisting of fewer than 64 bytes, is in an oversized frame, or has a checksum error.

Error packets transmitted (hw) (ErrTx)
Erroneous packets transmitted on the interface. For example, a packet consisting of fewer than 64 bytes, is in an oversized frame, or is the result of a collision error.

Inbound packets discarded(hw) (InDisc)
Error-free inbound packets discarded on the interface due to a lack of resources, for example, NIC buffers.

Outbound packets discarded(hw) (OutDisc)
Error-free outbound packets discarded on the interface due to a lack of resources.

Packets dropped in Rx (sw) (DrpRxPkt)
Packets dropped on the interface. Commonly dropped packets are multicast frames, spanning tree BPDUs, packets destined to a MAC not owned by the system when L2 mode is disabled, or packets tagged for a vlan that isn?t bound to the interface. This counter will increment in most healthy networks at a steady rate regardless of traffic load. If a sharp spike in dropped packets occurs, it generally indicates an issue with connected L2 switches, such as a

forwarding database overflow resulting in packets being broadcast on all ports.

Packets dropped in Tx (sw) (DrpTxPkt)
Error-free outbound packets dropped in transmission on the interface due to a VLAN mismatch, an oversized packet, or a disabled network interface card.

NIC hangs (Hangs)
Number of network interface card hangs because the NetScaler software detects an error on the transmission or reception path of the NIC.

Status stalls (StsStall)
System detected stalls in the transmission or reception of packets on the NIC. When the status is not updated within 0.8 seconds by the NIC hardware, the NIC is said to be in a status stall state.

Transmit stalls (TxStall)
System detected stalls in the transmission of packets on the NIC. When a packet posted for transmission has not been transmitted in 4 seconds, the NIC is said to be in a transmit stall state.

Receive stalls (RxStall)
System registered stalls in the reception of packets on the network interface card. When the link is up for more than 10 minutes and packets have been transmitted, but no packets have been received for 16 seconds, the network interface card is said to be in a receive stall state. This commonly occurs in lab environments when no packets, including spanning tree, are being received on the wire.

Error-disables (ErrDis)
Number of times the interface has been disabled due to an error, such as a stall in the transmission or reception of packets. A disabled interface will not receive or transmit any packets.

Duplex mismatches (DupMism)
Number of duplex mismatches detected on the interface. A mismatch will occur if the duplex mode is not identically set on both ends of the link.

Link re-initializations (LnkReint)
Number of times the link has been re-initialized. A re-initialization occurs when the link goes from the DOWN state to the UP state, or when an interface configuration parameter, such as speed or duplex, changes.

MAC moves registered (MacMvd)
Number of MAC moves between ports. Usually, a MAC address is seen on only one port. However, if there is a high rate of MAC moves registered, it is likely that there is a bridge loop between two interfaces on the system, which can cause performance and reliability issues.

Times NIC become muted (ErrMtd)
Number of times the interface stopped transmitting and receiving packets. For example, there are too many MAC moves on this interface due to a suspected configuration issue.

Related Commands

clear interface
set interface
unset interface
enable interface
disable interface
reset interface
show interface
stat bridge
stat rnat
stat rnatip
stat vlan

set lacp

Synopsis

```
set lacp -sysPriority <positive_integer>
```

Description

Set the LACP system priority.

Arguments

sysPriority

LACP system priority Default value: 32768 Minimum value: 1 Maximum value: 65535

Related Commands

show lacp

show lacp

Synopsis

```
show lacp
```

Description

Display the LACP configuration.

Arguments

`format`

`level`

Output

`deviceName`
Name of the channel.

`sysPriority`

`mac`
LACP system mac.

`flags`
Flags of this channel.

`lacpKey`
LACP key of this channel.

Related Commands

set lacp

set rnatparam

Synopsis

```
set rnatparam -tcpproxy ( ENABLED | DISABLED )
```

Description

set the rnat parameter

Arguments

tcpproxy

The state of tcpproxy. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set rnat parameter -tcpproxy ENABLED

Related Commands

unset rnatparam

show rnatparam

unset rnatparam

Synopsis

```
unset rnatparam -tcpproxy
```

Description

Use this command to remove rnatparam settings.Refer to the set rnatparam command for meanings of the arguments.

Related Commands

set rnatparam

show rnatparam

show rnatparam

Synopsis

```
show rnatparam
```

Description

show the rnat parameter.

Arguments

format

level

Output

tcpproxy

The state of tcpproxy.

Example

show rnat parameter

Related Commands

set rnatparam

unset rnatparam

add route

Synopsis

```
add route <network> <netmask> <gateway> [-distance
<positive_integer>] [-cost <positive_integer>] [-
weight <positive_integer>] [-advertise ( DISABLED |
ENABLED )] [-protocol <protocol> ...] [-msr ( ENABLED |
DISABLED )  [-monitor <string>]]
```

Description

Add a static route to the forwarding table.

Arguments

`network`
The destination network.

`netmask`
The netmask of the destination network.

`gateway`
The gateway for this route. It can either be the ip address of the gateway or null to specify a null interface route.

`cost`
The cost metric of this route. Default value: 0 Maximum value: 65535

`distance`
Distance of this route. Default value: STATIC_ROUTE_DEFAULT_DISTANCE Minimum value: 1 Maximum value: 255

`cost`
The cost metric of this route. Default value: 0 Maximum value: 65535

`weight`
The weight of this route. It will be used to do a weighted hash-based traffic distribution, in case of ECMP routes. Default value: ROUTE_DEFAULT_WEIGHT Minimum value: 1 Maximum value: 65535

`advertise`
The state of advertisement of this route. Possible values: DISABLED, ENABLED

`protocol`
The routing protocols for advertisement of this route.

`msr`
Enable/disable MSR on this route. Possible values: ENABLED, DISABLED
Default value: DISABLED

Example

add route 10.10.10.0 255.255.255.0 10.10.10.1

Related Commands

show arp
rm arp
clear route
rm route
set route
unset route
show route

rm route

Synopsis

```
rm route <network> <netmask> <gateway>
```

Description

Remove a configured static route from the system. Routes added via VLAN configuration cannot be deleted using this command. Use the rmvlan or clearvlan command instead.

Arguments

`network`
The network of the route to be removed.

`netmask`
The netmask of the route to be removed.

`gateway`
The gateway address of the route to be removed.

Related Commands

clear vlan

clear route

add route

set route

unset route

show route

set route

Synopsis

```
set route <network> <netmask> <gateway> [-distance
<positive_integer>] [-cost <positive_integer>] [-
weight <positive_integer>] [-advertise ( DISABLED |
ENABLED ) | -protocol <protocol> ...] [-msr ( ENABLED |
DISABLED )  [-monitor <string>]]
```

Description

Set the attributes of a route that was added via the add route command.

Arguments

network
The destination network for the route.

netmask
The netmask for this destination network.

gateway
The gateway for the destination network of the route.

distance
Distance of this route. Default value: STATIC_ROUTE_DEFAULT_DISTANCE Minimum value: 1 Maximum value: 255

cost
The cost metric of this route. Default value: 0 Maximum value: 65535

weight
The weight of this route. It will be used to do a weighted hash-based traffic distribution, in case of ECMP routes. Default value: ROUTE_DEFAULT_WEIGHT Minimum value: 1 Maximum value: 65535

advertise
The state of advertisement of this route. Possible values: DISABLED, ENABLED

protocol
The routing protocols for advertisement of this route.

msr
Enable/disable MSR on this route. Possible values: ENABLED, DISABLED
Default value: DISABLED

Example

set route 10.10.10.0 255.255.255.0 10.10.10.1 -advertise enable

Related Commands

clear route
add route
rm route
unset route
show route

unset route

Synopsis

```
unset route <network> <netmask> <gateway> [-advertise (
DISABLED | ENABLED ) | -protocol <protocol> ...] [-
distance] [-cost] [-weight] [-msr] [-monitor]
```

Description

Unset the attributes of a route that were added via the add/set route command..Refer to the set route command for meanings of the arguments.

Example

unset route 10.10.10.0 255.255.255.0 10.10.10.1 -advertise enable

Related Commands

clear route

add route

rm route

set route

show route

show route

Synopsis

```
show route [<network> <netmask> [<gateway>]]
[<routeType>] [-detail]
```

Description

Display the configured routing information.

Arguments

network
The destination network or host.

routeType
The type of routes to be shown.

detail
To get a detailed view. Default value: NSA_CLIDETAIL

summary

fullValues

format

level

Output

gatewayName
The name of the gateway for this route.

advertise
Whether advertisement is enabled or disabled.

type
State of the RNAT.

state

dynamic
State of the RNAT.

STATIC
State of the RNAT.

PERMANENT
State of the RNAT.

DIRECT
State of the RNAT.

DYNAMIC
State of the RNAT.

NAT
State of the RNAT.

LBROUTE
State of the RNAT.

ADV
State of the RNAT.

TUNNEL
Whether this route is dynamically learnt or not.

cost
Cost of this route.

distance
Distance of this route.

cost
The cost metric of this route.

weight
The weight of this route.

data
Internal data of this route.

flags
If this route is dynamic then which routing protocol was it learnt from.

OSPF
If this route is dynamic then which routing protocol was it learnt from.

RIP
If this route is dynamic then which routing protocol was it learnt from.

BGP
If this route is dynamic then which routing protocol was it learnt from.

msr
Whether MSR is enabled or disabled.

monitor
The name of the monitor.

state
If this route is UP/DOWN.

totalprobes
The total number of probes sent.

totalfailedprobes
The total number of failed probes.

failedprobes
Number of the current failed monitoring probes.

monStatCode
The code indicating the monitor response.

monStatParam1
First parameter for use with message code.

monStatParam2
Second parameter for use with message code.

monStatParam3
Third parameter for use with message code.

Example

An example of the output of the show route command is as follows: 3 configured routes: Network Netmask Gateway/OwnedIP Type
------- ------- --------------- ---- 1) 0.0.0.0 0.0.0.0 10.11.0.254

STATIC 2) 127.0.0.0 255.0.0.0 127.0.0.1 PERMANENT 3)
10.251.0.0 255.255.0.0 10.251.0.254 NAT

Related Commands

clear route

add route

rm route

set route

unset route

set rnat

Synopsis

```
set rnat ((<network> [<netmask>] [-natIP <ip_addr|*>
...]) | (<aclname> [-redirectPort <port>] [-natIP
<ip_addr|*> ...]))
```

Description

Configure Reverse NAT on the system.

Arguments

network

The network or subnet from which the traffic is flowing.

aclname

The acl name.

Related Commands

clear rnat

unset rnat

stat rnat

show rnat

unset rnat

Synopsis

```
unset rnat [-network] [-netmask] [-natIP] [-aclname] [-
redirectPort] [-natIP]
```

Description

Use this command to remove rnat settings.Refer to the set rnat command for meanings of the arguments.

Related Commands

clear rnat

set rnat

stat rnat

show rnat

stat rnat

Synopsis

```
stat rnat [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display statistics for rnat sessions.

Arguments

Output

Counters

Bytes Received (rnatRxBytes)
Bytes received during RNAT sessions.

Bytes Sent (rnatTxBytes)
Bytes sent during RNAT sessions.

Packets Received (rnatRxPkts)
Packets received during RNAT sessions.

Packets Sent (rnatTxPkts)
Packets sent during RNAT sessions.

Syn Sent (rnatTxSyn)
Requests for connections sent during RNAT sessions.

Current RNAT sessions (rnatSessions)
Currently active RNAT sessions.

Example

stat rnat

Related Commands

clear rnat

set rnat

unset rnat

show rnat
stat bridge
stat interface
stat rnatip
stat vlan

stat rnatip

Synopsis

```
stat rnatip [<rnatip>] [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display statistics for rnat sessions.

Arguments

rnatip
Specifies the natip

Output

Counters

Bytes Received (rxBytes)
Bytes received on this IP address during RNAT sessions.

Bytes Sent (txBytes)
Bytes sent from this IP address during RNAT sessions.

Packets Received (rxPkts)
Packets received on this IP address during RNAT sessions.

Packets Sent (txPkts)
Packets sent from this IP address during RNAT sessions.

Syn Sent (txSyn)
Requests for connections sent from this IP address during RNAT sessions.

Current RNAT sessions (sessions)
Currently active RNAT sessions started from this IP address.

Example

stat rnatip 1.1.1.1

Related Commands

stat bridge

stat interface

stat rnat

stat vlan

show rnat

Synopsis

```
show rnat
```

Description

Display the Reverse NAT configuration.

Arguments

summary

fullValues

format

level

Output

network
The network address.

netmask
The netmask of the network.

natIP
Nat IP Address.

aclname
The acl name.

redirectPort
The redirect port.

Related Commands

clear rnat

set rnat

unset rnat

stat rnat

add vlan

Synopsis

```
add vlan <id> [-ipv6DynamicRouting ( ENABLED | DISABLED )]
```

Description

Create a VLAN. Each VLAN is identified by a VID (integer from 1-4094). The VLAN created is empty (without members). This VLAN is not active until interfaces are bound to it. VLAN 1 is created by default and cannot be added or deleted.

Arguments

`id`

The VLAN id. Minimum value: 0 Maximum value: 4094

`ipv6DynamicRouting`

Use this option to enable or disable dynamic routing on this vlan. Possible values: ENABLED, DISABLED Default value: DISABLED

Related Commands

rm vlan

set vlan

unset vlan

bind vlan

unbind vlan

show vlan

stat vlan

rm vlan

Synopsis

```
rm vlan <id>
```

Description

Removes the VLAN created by the add vlan command. Once the VLAN is removed, its interfaces become members of VLAN 1.

Arguments

id

The VLAN Id. Minimum value: 2 Maximum value: 4094

Related Commands

add vlan

set vlan

unset vlan

bind vlan

unbind vlan

show vlan

stat vlan

set vlan

Synopsis

```
set vlan <id> -ipv6DynamicRouting ( ENABLED | DISABLED
)
```

Description

Set VLAN parameters.

Arguments

id

The VLAN id. Minimum value: 0 Maximum value: 4094

ipv6DynamicRouting

Use this option to enable or disable dynamic routing on this vlan. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set vlan 2 -dynamicRouting ENABLED

Related Commands

add vlan

rm vlan

unset vlan

bind vlan

unbind vlan

show vlan

stat vlan

unset vlan

Synopsis

```
unset vlan <id> -ipv6DynamicRouting
```

Description

Use this command to remove vlan settings.Refer to the set vlan command for meanings of the arguments.

Related Commands

add vlan

rm vlan

set vlan

bind vlan

unbind vlan

show vlan

stat vlan

bind vlan

Synopsis

```
bind vlan <id> [-ifnum <interface_name> ... [-tagged]]
[-IPAddress <ip_addr|ipv6_addr|*> [<netmask>]]
```

Description

Bind an interface or an ip address to a VLAN. An interface can be bound to a VLAN as a tagged or an untagged interface. Adding an interface as an untagged member (default) deletes it from its current native VLAN and adds it to the new VLAN. If an interface is added as a tagged member to a VLAN, it still remains a member of its native VLAN.

Arguments

id

Specifies the virtual LAN ID.

ifnum

The interface name represented in the <slot/port> notation. For example 1/1. Use the ###show interface### command to view the system interfaces. Minimum value: 1

IPAddress

The IP address that is to be assigned to the VLAN. An entry for this subnet is to be added in the routing table prior to the issue of this command. Overlapping subnets are not allowed. The VLAN specified by id should already have been created by the add command. The IP address specified can be used as the default gateway among the hosts in the subnet to allow for IP forwarding between VLANs. In a high availability configuration, this IP address is shared by the systems and is active in the master. CAUTION:DO NOT specify an IP address for VLAN 1.

Related Commands

add vlan

rm vlan

set vlan

unset vlan

unbind vlan
show vlan
stat vlan

unbind vlan

Synopsis

```
unbind vlan <id> [-ifnum <interface_name> ...  [-
tagged]] [-IPAddress <ip_addr|ipv6_addr|*>
[<netmask>]]
```

Description

Unbind the specified interface from the VLAN. If the interface was an untagged member of this VLAN, it is added to the default VLAN (VLAN 1).

Arguments

id

The virtual LAN (VLAN) id. Minimum value: 1 Maximum value: 4094

ifnum

The interface number represented in the <slot/port> notation. For example, 1/1. Use the ###show interface### command to view the system interfaces.

IPAddress

Related Commands

add vlan

rm vlan

set vlan

unset vlan

bind vlan

show vlan

stat vlan

show vlan

Synopsis

```
show vlan [<id>] show vlan stats - alias for 'stat vlan'
```

Description

Displays the configured VLANs. If id is specified, then only that particular VLAN information is displayed. If it is not specified, all configured VLANs are displayed.

Arguments

`id`
The VLAN id Minimum value: 1 Maximum value: 4094

`summary`

`fullValues`

`format`

`level`

Output

`IPAddress`
The IP address assigned to the VLAN.

`netmask`
The network mask for the subnet defined for the VLAN.

`rnat`
Temporary flag used for internal purpose.

`state`
state flag

`portbitmap`
Member interfaces of this vlan.

tagbitmap
Tagged members of this vlan.

ifaces
Names of all member interfaces of this vlan.

tagIfaces
Names of all tagged member interfaces of this vlan.

ipv6DynamicRouting
Whether dynamic routing is enabled or disabled.

Example

An example of the output of the show vlan command is as follows: 3 configured VLANs: 1) VLAN ID: 1 Member Interfaces : 0/1 1/1 1/4 Tagged: None 2) VLAN ID: 2 IP: 10.250.0.254 Mask: 255.255.0.0 ReverseNAT: YES Member Interfaces : 1/2 Tagged: None 3) VLAN ID: 3 IP: 10.251.0.254 Mask: 255.255.0.0 ReverseNAT: YES Member Interfaces : 1/3 Tagged: None

Related Commands

add vlan
rm vlan
set vlan
unset vlan
bind vlan
unbind vlan
stat vlan

stat vlan

Synopsis

```
stat vlan [<id>] [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display statistics for VLAN(s).

Arguments

id

Specifies the VID (VLAN identification number). Enter an integer from 1 to 4094. Minimum value: 1

Output

Counters

Packets received (RxPkts)

Packets received on the VLAN.

Bytes received (RxBytes)

Bytes of data received on the VLAN.

Packets sent (TxPkts)

Packets transmitted on the VLAN.

Bytes sent (TxBytes)

Bytes of data transmitted on the VLAN.

Packets dropped (DropPkts)

Inbound packets dropped by the VLAN upon reception.

Broadcast pkts sent & received (BcastPkt)

Broadcast packets sent and received on the VLAN.

Example

stat vlan 1

Related Commands

add vlan
rm vlan
set vlan
unset vlan
bind vlan
unbind vlan
show vlan
stat bridge
stat interface
stat rnat
stat rnatip

add vrID

Synopsis

```
add vrID <id>
```

Description

This command creates a Virtual Mac address.Each VMAC is identified by a VRID(integer from 1-255).The VMAC created is empty (without members). This VMAC is not active until interfaces are bound to it.

Arguments

id

The virtual Router ID. Minimum value: 1 Maximum value: 255

Example

add vrID 1

Related Commands

rm vrID

bind vrID

unbind vrID

show vrID

rm vrID

Synopsis

```
rm vrID (<id> | -all)
```

Description

Remove the VRID created by the add command.

Arguments

id

The virtual Router ID whose entry is to be removed. Minimum value: 1 Maximum value: 255

all

Remove all entries from the system's vrid table.

Related Commands

add vrID

bind vrID

unbind vrID

show vrID

bind vrID

Synopsis

```
bind vrID <id> -ifnum <interface_name> ...
```

Description

Bind an interface to a vrID.

Arguments

`id`

The virtual Router ID.

`ifnum`

Interfaces to be bound to this vrID.

Example

add vrID 1

Related Commands

add vrID

rm vrID

unbind vrID

show vrID

unbind vrID

Synopsis

```
unbind vrID <id> -ifnum <interface_name> ...
```

Description

Unbind specified interfaces from the VRID.

Arguments

`id`

The virtual Router ID.

`ifnum`

Interfaces to be bound to this vrID.

Related Commands

add vrID

rm vrID

bind vrID

show vrID

show vrID

Synopsis

```
show vrID [<id>]
```

Description

Display vrid table.

Arguments

id

The VRID. Enter an integer from 1 to 255. Minimum value: 1 Maximum value: 255

summary

fullValues

format

level

Output

ifaces

Interfaces bound to this vrid.

type

Type (static or dynamic) of this vrid.

vlan

The VLAN in which this VRID lies.

Example

show vrid

Related Commands

add vrID

rm vrID

bind vrID

unbind vrID

add vrID6

Synopsis

```
add vrID6 <id>
```

Description

This command creates a Virtual Mac address.Each VMAC is identified by a VRID(integer from 1-255).The VMAC created is empty (without members). This VMAC is not active until interfaces are bound to it.

Arguments

id

The virtual Router ID. Minimum value: 1 Maximum value: 255

Example

add vrID6 1

Related Commands

rm vrID6

bind vrID6

unbind vrID6

show vrID6

rm vrID6

Synopsis

```
rm vrID6 (<id> | -all)
```

Description

Remove the VRID created by the add command.

Arguments

id

The virtual Router ID whose entry is to be removed. Minimum value: 1 Maximum value: 255

all

Remove all entries from the system's vrid table.

Related Commands

add vrID6

bind vrID6

unbind vrID6

show vrID6

bind vrID6

Synopsis

```
bind vrID6 <id> -ifnum <interface_name> ...
```

Description

Arguments

id
The virtual Router ID.

ifnum
Interfaces to be bound to this vrID.

Example

add vrID6 1

Related Commands

add vrID6
rm vrID6
unbind vrID6
show vrID6

unbind vrID6

Synopsis

```
unbind vrID6 <id> -ifnum <interface_name> ...
```

Description

Unbind specified interfaces from the VRID.

Arguments

`id`

The virtual Router ID.

`ifnum`

Interfaces to be bound to this vrID.

Related Commands

add vrID6

rm vrID6

bind vrID6

show vrID6

show vrID6

Synopsis

```
show vrID6 [<id>]
```

Description

Display vrid6 table.

Arguments

id

The VRID. Enter an integer from 1 to 255. Minimum value: 1 Maximum value: 255

summary

fullValues

format

level

Output

ifaces

Interfaces bound to this vrid.

type

Type (static or dynamic) of this vrid.

vlan

The VLAN in which this VRID lies.

Example

show vrid6

Related Commands

add vrID6

rm vrID6

bind vrID6

unbind vrID6

add route6

Synopsis

```
add route6 <network> <gateway> [-vlan
<positive_integer>] [-weight <positive_integer>] [-
distance <positive_integer>] [-cost
<positive_integer>] [-advertise ( DISABLED | ENABLED )]
```

Description

Add a IPv6 static route to the forwarding table. VLAN number is needed only for link local addresses

Arguments

network
The destination network.

gateway
The gateway for this route.

vlan
The VLAN number. Default value: 0 Minimum value: 1 Maximum value: 4094

weight
The weight of this route. Default value: 1 Minimum value: 1 Maximum value: 65535

distance
Distance of this route. Default value: 1 Minimum value: 1 Maximum value: 254

cost
The cost metric of this route. Default value: 1 Maximum value: 65535

advertise
The state of advertisement of this route. Possible values: DISABLED, ENABLED

Example

add route6 ::/0 2004::1 add route6 ::/0 FE80::67 -vlan 5

Related Commands

show route6

rm route6

clear route6

set route6

unset route6

rm route6

Synopsis

```
rm route6 <network> <gateway> [-vlan
<positive_integer>]
```

Description

Remove a configured static route from the system.

Arguments

network

The network of the route to be removed.

gateway

The gateway address of the route to be removed.

vlan

The VLAN number. Default value: 0 Minimum value: 1 Maximum value: 4094

Example

rm route6 ::/0 2004::1 rm route6 ::/0 FE80::67 -vlan 5

Related Commands

rm route6

clear route6

add route6

set route6

unset route6

show route6

set route6

Synopsis

```
set route6 <network> <gateway> [-vlan
<positive_integer>] [-weight <positive_integer>] [-
distance <positive_integer>] [-cost
<positive_integer>] [-advertise ( DISABLED | ENABLED )]
```

Description

Set the attributes of a route that was added via the add route command.

Arguments

network

The destination network for the route.

gateway

The gateway for the destination network of the route.

vlan

The VLAN number. Default value: 0 Minimum value: 1 Maximum value: 4094

weight

The weight of this route. Default value: 1 Minimum value: 1 Maximum value: 65535

distance

Distance of this route. Default value: 1 Minimum value: 1 Maximum value: 254

cost

The cost metric of this route. Default value: 1 Maximum value: 65535

advertise

The state of advertisement of this route. Possible values: DISABLED, ENABLED

Example

set route 1::1/100 2000::1 -advertise enable

Related Commands

clear route6

add route6

rm route6

unset route6

show route6

unset route6

Synopsis

```
unset route6 <network> <gateway> [-vlan
<positive_integer>] [-weight] [-distance] [-cost] [-
advertise]
```

Description

Unset the attributes of a route that were added via the add/set route command..Refer to the set route6 command for meanings of the arguments.

Example

unset route 2000::1/100 3000::1 -advertise enable

Related Commands

clear route6

add route6

rm route6

set route6

show route6

show route6

Synopsis

```
show route6 [<network>  [<gateway>  [-vlan
<positive_integer>]]] [<routeType>] [-detail]
```

Description

Display the configured routing information.

Arguments

network
The destination network or host.

routeType
The type of routes to be shown.

detail
To get a detailed view. Default value: NSA_CLIDETAIL

summary

fullValues

format

level

Output

gatewayName
The name of the gateway for this route.

advertise
Whether advertisement is enabled or disabled.

type
State of the RNAT.

state

dynamic
Whether this route is dynamically learnt or not.

weight
Weight of this route.

distance
Distance of this route.

cost
The cost metric of this route.

data
Internal data of this route.

flags
If this route is dynamic then which routing protocol was it learnt from.

Example

An example of the output of the show route6 command is as follows:
Flags: Static(S), Dynamic(D), Active(A) ----------
Network Gateway(vlan) Flags ------- ----------- ----- 0::0/0 2001::1 S(A) 0::0/0 FE80::90(4) D(A)

Related Commands

clear route6
add route6
rm route6
set route6
unset route6

add nd6

Synopsis

```
add nd6 <neighbor> <mac> <ifnum> [-vlan <integer>]
```

Description

Add a static entry to the NetScaler nd6 table

Arguments

neighbor
IPv6 Neighbor

mac
MAC address

ifnum
The interface on which this MAC address resides

vlan
The VLAN number. Default value: 0

Example

add nd6 2001::1 00:04:23:be:3c:06 5 1/1

Related Commands

clear nd6
rm nd6
show nd6

rm nd6

Synopsis

```
rm nd6 <neighbor> [-vlan <integer>]
```

Description

Remove a static entry from the NetScaler nd6 table

Arguments

neighbor
IPv6 Neighbor

vlan
The VLAN number. Default value: 0

Example

rm nd6 2001::1 5 1/1

Related Commands

clear nd6
add nd6
show nd6

show nd6

Synopsis

```
show nd6
```

Description

Display the neighbor discovery information.

Arguments

summary

fullValues

format

level

Output

neighbor
IPv6 Neighbor

mac
MAC address

state
ND6 state

timeout
Time elapsed

ifnum
The interface on which this MAC address resides

vlan
The VLAN number.

flags
flag for static/permanent entry.

Example

An example of the output for show nd6 command is as follows: Neighbor MAC-Address(Vlan, Interface) State TIME(hh:mm:ss) -------- -- ------------------------ ----- ------------- 2001::1
00:04:23:be:3c:06(5, 1/1) REACHABLE 00:00:24 FE80::123:1
00:04:23:be:3c:07(4, 1/2) STALE 00:03:34

Related Commands

clear nd6

add nd6

rm nd6

set ipv6

Synopsis

```
set ipv6 -ralearning ( ENABLED | DISABLED )
```

Description

Enable IPv6 RA learning to start learning default routers, other properties through router advertisement messages.

Arguments

ralearning

IPv6 router advertisement learning Possible values: ENABLED, DISABLED Default value: DISABLED

Related Commands

unset ipv6

show ipv6

unset ipv6

Synopsis

```
unset ipv6 -ralearning
```

Description

Use this command to remove ipv6 settings.Refer to the set ipv6 command for meanings of the arguments.

Related Commands

set ipv6

show ipv6

show ipv6

Synopsis

```
show ipv6
```

Description

Display IPv6 settings

Arguments

format

level

Output

flags
IPv6 flags

basereachtime
ND6 base reachable time (ms)

reachtime
ND6 computed reachable time (ms)

retransmissiontime
ND6 retransmission time (ms)

Example

show ipv6

Related Commands

set ipv6

unset ipv6

add inat

Synopsis

```
add inat <name>@ <publicIP>@ <privateIP>@ [-tcpproxy ( ENABLED | DISABLED )] [-ftp ( ENABLED | DISABLED )] [-usip ( ON | OFF )] [-usnip ( ON | OFF )] [-proxyIP <ip_addr>]
```

Description

Create an inbound NAT with given public and private IP.

Arguments

name
Name of inbound NAT being added.

publicIP
NetScaler owned public IP (VIP).

privateIP
IP address of the server.

tcpproxy
To enable/disable TCP engine (Default DISABLED). Possible values: ENABLED, DISABLED Default value: DISABLED

ftp
To enable/disable FTP (Default DISABLED). Possible values: ENABLED, DISABLED Default value: DISABLED

usip
To switch on use source IP mode (Default ON). Possible values: ON, OFF Default value: ON

usnip
To switch on use subnet IP mode (Default ON). Possible values: ON, OFF Default value: ON

proxyIP
Source IP address for backend connection to server.

Example

add nat mynat 1.2.3.4 192.168.1.100

Related Commands

rm inat

set inat

unset inat

show inat

rm inat

Synopsis

```
rm inat <name>@
```

Description

Remove the Inbound NAT configured.

Arguments

name

Name of inbound NAT being added.

Example

rm nat mynat.

Related Commands

add inat

set inat

unset inat

show inat

set inat

Synopsis

```
set inat <name>@ [-privateIP <ip_addr>@] [-tcpproxy (
ENABLED | DISABLED )] [-ftp ( ENABLED | DISABLED )] [-
usip ( ON | OFF )] [-usnip ( ON | OFF )] [-proxyIP
<ip_addr>]
```

Description

Modify some of the inbound NAT attributes.

Arguments

name

Name of inbound NAT being added.

privateIP

IP address of the server.

tcpproxy

To enable/disable TCP engine (Default DISABLED). Possible values: ENABLED, DISABLED Default value: DISABLED

ftp

To enable/disable FTP (Default DISABLED). Possible values: ENABLED, DISABLED Default value: DISABLED

usip

To switch on use source IP mode (Default ON). Possible values: ON, OFF Default value: ON

usnip

To switch on use subnet IP mode (Default ON). Possible values: ON, OFF Default value: ON

proxyIP

Source IP address for backend connection to server.

Example

set nat mynat -tcpproxy ENABLED

Related Commands

add inat

rm inat

unset inat

show inat

unset inat

Synopsis

```
unset inat <name>@ [-tcpproxy] [-ftp] [-usip] [-usnip]
[-proxyIP]
```

Description

Use this command to remove inat settings.Refer to the set inat command for meanings of the arguments.

Related Commands

add inat

rm inat

set inat

show inat

show inat

Synopsis

```
show inat [<name>]
```

Description

show all configured inbound NAT.

Arguments

name
Name of inbound NAT being added.

summary

fullValues

format

level

Output

publicIP
NetScaler owned public IP (VIP).

privateIP
IP address of the server.

proxyIP
Source IP address for backend connection to server.

tcpproxy
To enable/disable TCP engine (Default DISABLED).

ftp
To enable/disable FTP (Default DISABLED).

usip
To switch on use source IP mode (Default ON).

usnip
To switch on use subnet IP mode (Default ON).

flags
Flags for different modes

Example

show nat

Related Commands

add inat
rm inat
set inat
unset inat

set ipTunnelParam

Synopsis

```
set ipTunnelParam [-srcIP <ip_addr>] [-dropFrag ( YES | NO )] [-dropFragCpuThreshold <positive_integer>]
```

Description

Set the IP Tunnel global settings on the NetScaler

Arguments

srcIP

The source IP used for all IP tunnels, unless configured using 'add iptunnel' command.

dropFrag

To drop an IP packet, if fragmentation is required to tunnel it. Possible values: YES, NO Default value: NO

dropFragCpuThreshold

To drop an IP packet, if fragmentation is required to tunnel it and cpu usage is above this configured threshold. Default value: 0 Minimum value: 1 Maximum value: 100

Example

set ipTunnelParam -srcIP 10.100.20.48 -dropFrag YES -dropFragCpuThreshold 95

Related Commands

add iptunnel

rm iptunnel

show iptunnel

unset ipTunnelParam

show ipTunnelParam

unset ipTunnelParam

Synopsis

```
unset ipTunnelParam [-srcIP] [-dropFrag] [-
dropFragCpuThreshold]
```

Description

Use this command to remove ipTunnelParam settings.Refer to the set ipTunnelParam command for meanings of the arguments.

Related Commands

set ipTunnelParam

show ipTunnelParam

show ipTunnelParam

Synopsis

```
show ipTunnelParam
```

Description

Display the IP Tunnel global settings on the NetScaler

Arguments

format

level

Output

srcIP

The source IP used for all IP tunnels, unless configured using 'add iptunnel' command.

dropFrag

To drop an IP packet, if fragmentation is required to tunnel it.

dropFragCpuThreshold

To drop an IP packet, if fragmentation is required to tunnel it and cpu usage is above this configured threshold.

Example

Tunnel Source IP: 10.100.20.48 Drop if Fragmentation Needed: YES CPU usage threshold to avoid fragmentation: 95

Related Commands

add iptunnel

rm iptunnel

show iptunnel

set ipTunnelParam

unset ipTunnelParam

add ipTunnel

Synopsis

```
add ipTunnel <name> <remote> <remoteSubnetMask> <local>
[-protocol IPIP]
```

Description

Add an ip tunnel.

Arguments

`name`

The name of the ip tunnel.

`remote`

The remote-ip or subnet of the tunnel.

`remoteSubnetMask`

The remote-subnet mask of the tunnel.

`local`

The local-ip of the tunnel.

`protocol`

The IP tunneling protocol. Possible values: IPIP Default value: TNL_IPIP

Example

add iptunnel tunnel1 10.100.20.0 255.255.255.0 *

Related Commands

set iptunnelParam

rm ipTunnel

show ipTunnel

rm ipTunnel

Synopsis

```
rm ipTunnel <name>
```

Description

Remove a configured ip tunnel from the system.

Arguments

`name`

The name of the ip tunnel.

Example

rm iptunnel tunnel1

Related Commands

set iptunnelParam

show iptunnelParam

add ipTunnel

show ipTunnel

show ipTunnel

Synopsis

```
show ipTunnel [(<remote>  <remoteSubnetMask>) | <name>]
```

Description

Display the configured IP tunnels.

Arguments

`remote`
The remote-ip or subnet of the tunnel.

`name`
The name of the ip tunnel.

`format`

`level`

Output

`name`
The name of the ip tunnel.

`local`
The local-ip of the tunnel.

`protocol`
The IP tunneling protocol.

`type`
The type of this tunnel.

`encapIp`
The effective local-ip of the tunnel. Used as the source of the encapsulated packets.

Example

1) Name.....: t1 Remote.....: 10.102.33.0 Mask.....: 255.255.255.0
Local.....: * Encap.....: 0.0.0.0 Protocol.....: IPIP

```
Type.....:              C 2) Name.....: tunnel1    Remote.....:    10.100.20.0
Mask.....:  255.255.255.0    Local.....:          *  Encap.....:       0.0.0.0
Protocol.....:          IPIP  Type.....:          C 3) Name.....:    Remote.....:
10.102.33.190  Mask.....: 255.255.255.255    Local.....:          *
Encap.....:   10.102.33.85    Protocol.....:          IPIP  Type.....:          I
```

Related Commands

set iptunnelParam

show iptunnelParam

add ipTunnel

rm ipTunnel

CHAPTER 31

Responder Commands

This chapter covers the responder commands.

add responder policy

Synopsis

```
add responder policy <name> <rule> <action>
[<undefAction>]
```

Description

Add a responder policy.

Arguments

`name`

Name of the responder policy

`rule`

Expression to be used by responder policy. It has to be a boolean PI rule expression.

`action`

Responder action to be used by the policy.

`undefAction`

Responder action to be taken in the case of UNDEF event during policy evaluation. Should be NOOP, RESET or DROP.

Example

i) add responder policy pol9
"Q.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_respondwith

Related Commands

rm responder policy

set responder policy

unset responder policy

show responder policy

stat responder policy

rm responder policy

Synopsis

```
rm responder policy <name>
```

Description

Remove a responder policy.

Arguments

name

Name of the responder policy to be removed.

Example

rm responder policy pol9

Related Commands

add responder policy

set responder policy

unset responder policy

show responder policy

stat responder policy

set responder policy

Synopsis

```
set responder policy <name> [-rule <expression>] [-
action <string>] [-undefAction <string>]
```

Description

Set a new rule/action for existing unbound responder policy.

Arguments

`name`

Name of the responder policy

`rule`

Expression to be used by responder policy. It has to be a boolean PI rule expression.

`action`

Responder action to be used by the policy.

`undefAction`

Responder action to be taken in the case of UNDEF event during policy evaluation. Should be NOOP, RESET or DROP.

Example

set responder policy pol9 -rule
"HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

Related Commands

add responder policy

rm responder policy

unset responder policy

show responder policy

stat responder policy

unset responder policy

Synopsis

```
unset responder policy <name> [-rule] [-action] [-undefAction]
```

Description

Unset undefAction for existing responder policy..Refer to the set responder policy command for meanings of the arguments.

Example

unset responder policy respol9 -undefAction

Related Commands

add responder policy

rm responder policy

set responder policy

show responder policy

stat responder policy

show responder policy

Synopsis

show responder policy [<name>] show responder policy stats - alias for 'stat responder policy'

Description

Display all the configured responder policies.

Arguments

name
Name of the responder policy.

summary

fullValues

format

level

Output

state

rule
Rule of the policy.

action
Responder action associated with the policy.

undefAction
UNDEF action associated with the policy.

hits
Number of hits.

undefHits
Number of policy UNDEF hits.

activePolicy
Indicates whether policy is bound or not.

boundTo
Location where policy is bound

priority
Specifies the priority of the policy.

Example

show responder policy

Related Commands

add responder policy
rm responder policy
set responder policy
unset responder policy
stat responder policy

add responder action

Synopsis

```
add responder action <name> <type> <target> [-
bypassSafetyCheck ( YES | NO )]
```

Description

Creates a responder action. The action thus created can be associated with responder policy by using "add responder policy" command. The system has following built-in action entities: NOOP - the no-op action. RESET - reset the current client and server connection. DROP - drop packets when rate exceeds the rate-limiting threshold

Arguments

name

Name of the responder action to be added.

type

Type of responder action. It can be: (respondwith|redirect). For each action type the <target> is as defined below. o RESPONDWITH: Send the specified response. <target> = SNIT expression to be sent as the response. o REDIRECT: Generates an 'HTTP Redirect' to a specified URL. <target> = where to redirect to. Possible values: respondwith, redirect

target

Expression specifying what to to respond with. Maximum length of the input expression is 8191. Maximum size of string that can be used inside the expression is 1499.

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions Possible values: YES, NO Default value: NO

Example

i) add responder action act1 respondwith "\\"HTTP/1.1 200 OK\\r\\n\\r\\n\\"" ii) add responder action redir_action redirect "'http://backupsite2.com" + q.url' -bypassSafetyCheck YES

Related Commands

rm responder action
set responder action
show responder action

rm responder action

Synopsis

```
rm responder action <name>
```

Description

Remove a configured responder action.

Arguments

name

Name of the responder action.

Example

rm responder action act_before

Related Commands

add responder action

set responder action

show responder action

set responder action

Synopsis

```
set responder action <name> (-target <string>  [-
bypassSafetyCheck ( YES | NO )])
```

Description

Modify a responder action.

Arguments

name

Name of the responder action.

target

Expression specifying what to respond with. Maximum length of the input expression is 8191. Maximum size of string that can be used inside the expression is 1499.

Example

set responder action act_responder -target 'HTTP.REQ.HEADER("MYURL")' -bypassSafetyCheck YES

Related Commands

add responder action

rm responder action

show responder action

show responder action

Synopsis

```
show responder action [<name>]
```

Description

Display configured responder action(s).

Arguments

name
Name of the responder action.

summary

fullValues

format

level

Output

state

type
Type of responder action. It can be: (respondwith).

target
Expression specifying what to to respond with

bypassSafetyCheck
The safety check to allow unsafe expressions.

hits
The number of times the action has been taken.

referenceCount
The number of references to the action.

undefHits
The number of times the action resulted in UNDEF.

Example

1. show responder action 2. show responder action act_insert

Related Commands

add responder action
rm responder action
set responder action

bind responder global

Synopsis

```
bind responder global <policyName> <priority>
[<gotoPriorityExpression>] [-type <type>] [-invoke
(<labelType>  <labelName>) ]
```

Description

Binds the responder policy with given priority

Arguments

policyName

Name of the policy to be bound to responder global.

Example

i)bind responder global pol9 9

Related Commands

unbind responder global

show responder global

unbind responder global

Synopsis

```
unbind responder global <policyName> [-type <type>] [-
priority <positive_integer>]
```

Description

Unbind entities from responder global.

Arguments

policyName

The name of the policy to be unbound.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind responder global pol9

Related Commands

bind responder global

show responder global

show responder global

Synopsis

```
show responder global [-type <type>]
```

Description

Display the responder global bindings.

Arguments

type

The bindpoint to which policy is bound. Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT

summary

fullValues

format

level

Output

state

policyName

Name of the responder policy.

priority

Specifies the priority of the policy.

gotoPriorityExpression

Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType

Type of policy label invocation.

labelName

Name of the label to invoke if the current policy rule evaluates to TRUE.

flowType
flowtype of the bound responder policy.

numpol
number of polices bound to label.

Example

show responder global

Related Commands

bind responder global
unbind responder global

set responder param

Synopsis

```
set responder param -undefAction <string>
```

Description

Set the default responder undef action. If an UNDEF event is triggered during policy evaluation and if the current policy's undefAction is not specified, then this global undefAction value is used. NOOP is the default value of default responder undef action

Arguments

undefAction

can be NOOP, RESET or DROP

Example

set responder param -undefAction RESET

Related Commands

unset responder param

show responder param

unset responder param

Synopsis

```
unset responder param -undefAction
```

Description

Unset responder params..Refer to the set responder param command for meanings of the arguments.

Example

unset responder param -undefAction

Related Commands

set responder param

show responder param

show responder param

Synopsis

```
show responder param
```

Description

Display default responder undef action.

Arguments

format

level

Output

undefAction

Name of the responder action.

Example

show responder param

Related Commands

set responder param

unset responder param

add responder policylabel

Synopsis

```
add responder policylabel <labelName>
```

Description

Add a responder policy label.

Arguments

labelName

Name of the responder policy label.

Example

add responder policylabel resp_lab

Related Commands

rm responder policylabel

bind responder policylabel

unbind responder policylabel

show responder policylabel

rm responder policylabel

Synopsis

```
rm responder policylabel <labelName>
```

Description

Remove a responder policy label.

Arguments

labelName

Name of the responder policy label.

Example

rm responder policylabel resp_lab

Related Commands

add responder policylabel

bind responder policylabel

unbind responder policylabel

show responder policylabel

bind responder policylabel

Synopsis

```
bind responder policylabel <labelName> <policyName>
<priority> [<gotoPriorityExpression>] [-invoke
(<labelType>  <labelName>) ]
```

Description

Bind the responder policy to one of the labels.

Arguments

labelName

Name of the responder policy label.

policyName

Name of the policy to be bound to responder policy label.

Example

i)bind responder policylabel resp_lab pol_resp 1 2 ii)bind responder policylabel resp_lab pol_resp 1 2 -invoke vserver CURRENT

Related Commands

add responder policylabel

rm responder policylabel

unbind responder policylabel

show responder policylabel

unbind responder policylabel

Synopsis

```
unbind responder policylabel <labelName> <policyName>
[-priority <positive_integer>]
```

Description

Unbind entities from responder label.

Arguments

labelName

Name of the responder policy label.

policyName

The name of the policy to be unbound.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind responder policylabel resp_lab pol_resp

Related Commands

add responder policylabel

rm responder policylabel

bind responder policylabel

show responder policylabel

show responder policylabel

Synopsis

```
show responder policylabel [<labelName>]
```

Description

Display policy label or policies bound to responder policylabel.

Arguments

labelName
Name of the responder policy label.

summary

fullValues

format

level

Output

state

numpol
number of polices bound to label.

hits
Number of times policy label was invoked.

policyName
Name of the responder policy.

priority
Specifies the priority of the policy.

gotoPriorityExpression
Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType
Type of policy label invocation.

labelName
Name of the label to invoke if the current policy rule evaluates to TRUE.

Example

i)show responder policylabel resp_lab ii)show responder policylabel

Related Commands

add responder policylabel
rm responder policylabel
bind responder policylabel
unbind responder policylabel

stat responder policy

Synopsis

```
stat responder policy [<name>] [-detail] [-fullValues]
[-ntimes <positive_integer>] [-logFile
<input_filename>]
```

Description

Display responder policy statistics.

Arguments

name

The name of the responder policy for which statistics will be displayed. If not given statistics are shown for all responder policies.

Output

Counters

Policy hits (Hits)

Number of hits on the policy

Policy undef hits (Undefhits)

Number of undef hits on the policy

Related Commands

add responder policy
rm responder policy
set responder policy
unset responder policy
show responder policy

CHAPTER 32

Rewrite Commands

This chapter covers the rewrite commands.

add rewrite policy

Synopsis

```
add rewrite policy <name> <rule> <action>
[<undefAction>]
```

Description

Add a rewrite policy.

Arguments

`name`

Name of the rewrite policy

`rule`

Expression to be used by rewrite policy. It has to be a boolean PI rule expression.

`action`

Rewrite action to be used by the policy.

`undefAction`

A rewrite action, to be used by the policy when the rule evaluation turns out to be undefined. The undef action can be NOREWRITE, RESET or DROP

Example

i)add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert ii)add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert NOREWRITE iii)add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert RESET iii)add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert DROP

Related Commands

rm rewrite policy

set rewrite policy

unset rewrite policy
show rewrite policy
stat rewrite policy

rm rewrite policy

Synopsis

```
rm rewrite policy <name>
```

Description

Remove a rewrite policy.

Arguments

name

Name of the rewrite policy to be removed.

Example

rm rewrite policy pol9

Related Commands

add rewrite policy
set rewrite policy
unset rewrite policy
show rewrite policy
stat rewrite policy

set rewrite policy

Synopsis

```
set rewrite policy <name> [-rule <expression>] [-action
<string>] [-undefAction <string>]
```

Description

Set a new rule/action/undefAction for existing rewrite policy. The rule flow type can change only if: .action and undefAction(if present) are of NEUTRAL flow type

Arguments

`name`
Name of the rewrite policy

`rule`
Expression to be used by rewrite policy. It has to be a boolean PI rule expression.

`action`
Rewrite action to be used by the policy.

`undefAction`
A rewrite action, to be used by the policy when the rule evaluation turns out to be undefined. The undef action can be NOREWRITE, RESET or DROP

Example

set rewrite policy pol9 -rule
"HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

Related Commands

add rewrite policy
rm rewrite policy
unset rewrite policy
show rewrite policy
stat rewrite policy

unset rewrite policy

Synopsis

```
unset rewrite policy <name> -undefAction
```

Description

Unset undefAction for existing rewrite policy..Refer to the set rewrite policy command for meanings of the arguments.

Example

unset rewrite policy pol9 -undefAction

Related Commands

add rewrite policy

rm rewrite policy

set rewrite policy

show rewrite policy

stat rewrite policy

show rewrite policy

Synopsis

```
show rewrite policy [<name>] show rewrite policy stats
- alias for 'stat rewrite policy'
```

Description

Display all the configured rewrite policies.

Arguments

name

Name of the rewrite policy.

summary

fullValues

format

level

Output

state

rule

Expression to be used by rewrite policy. It has to be a boolean PI rule expression.

action

Rewrite action associated with the policy.

undefAction

Undef Action associated with the policy.

hits

Number of hits.

undefHits

Number of Undef hits.

activePolicy
Indicates whether policy is bound or not.

boundTo
Location where policy is bound

priority
Specifies the priority of the policy.

gotoPriorityExpression
Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType
Type of policy label invocation.

labelName
Name of the label to invoke if the current policy rule evaluates to TRUE.

description
Description of the policy

Example

show rewrite policy

Related Commands

add rewrite policy
rm rewrite policy
set rewrite policy
unset rewrite policy
stat rewrite policy

add rewrite action

Synopsis

```
add rewrite action <name> <type> <target>
[<stringBuilderExpr>] (-pattern <expression> | -patset
<string>) [-bypassSafetyCheck ( YES | NO )]
```

Description

Creates a rewrite action. The action thus created can be associated with rewrite policy by using "add rewrite policy" command. The system has three built-in action entities: NOREWRITE - no-op action RESET - reset the current client and server connection DROP - drop packets when rate exceeds the rate-limiting threshold A flow type is implicitly associated with every action.Following 3 flow types are possible: 1. Neutral : the action can be request or response time action 2. Request : the action can only be executed at request time 3. Response : the action can only be executed at response time

Arguments

name

Name of the rewrite action to be added.

type

Type of rewrite action. It can be: (replace|insert_http_header|delete_http_header|insert_before|insert_after|delete|replace_http_res). For each action type the <target> and <string builder expr> are defined below. oINSERT_HTTP_HEADER: Will insert a HTTP header. <target> = header name. <string builder expr> = header value specified as a compound text expression. oDELETE_HTTP_HEADER: Will delete all occurrence of HTTP header. <target> = header name. oREPLACE: Will replace the target text reference with the value specified in attr. <target> = Advanced text expression <string builder expr> = Compound text expression oINSERT_BEFORE: Will insert the value specified by attr before the target text reference. <target> = Advanced text expression <string builder expr> = Compound text expression oINSERT_AFTER: Will insert the value specified by attr after the target text reference. <target> = Advanced text expression <string builder expr> = Compound text expression oDELETE:

Delete the target text reference. <target> = Advanced text expression o REPLACE_HTTP_RES: Replace the http response with value specified in target. <target> = Compound text expression oREPLACE_ALL: Replaces all occurrence of the pattern in the text provided in the target with the text provided in the stringBuilderExpr, wit a string defined in the -pattern argument. For example, you can replace all occurences of abcd with -pattern efgh. <target> = text in a request or a response, for example http.req.body(1000) <stringBuilderExpr> = Compound text expression -pattern <expression> = string constant, for example -pattern efgh o INSERT_BEFORE_ALL: Will insert the value specified by stringBuilderExpr before all the occurrence of pattern in the target text reference. <target> = Advanced text expression <stringBuilderExpr> = Compound text expression -pattern <expression> = string constant or advanced regular expression oINSERT_AFTER_ALL: Will insert the value specified by stringBuilderExpr after all the occurrence of pattern in the target text reference. <target> = Advanced text expression <stringBuilderExpr> = Compound text expression -pattern <expression> = string constant or advanced regular expression oDELETE_ALL: Delete all the occurrence of pattern in the target text reference. <target> = Advanced text expression -pattern <expression> = string constant or advanced regular expression Possible values: delete, insert_http_header, delete_http_header, insert_before, insert_after, replace, replace_http_res, delete_all, replace_all, insert_before_all, insert_after_all, clientless_vpn_encode, clientless_vpn_encode_all, clientless_vpn_decode, clientless_vpn_decode_all

`target`
Expression specifying which part of HTTP packet needs to be rewritten.

`stringBuilderExpr`
Expression specifying new value of the rewritten HTTP packet. Maximum length of the input expression is 8191. Maximum size of string that can be used inside the expression is 1499.

`pattern`
Pattern to be used for insert_before_all, insert_after_all, replace_all, delete_all action types.

`patset`
Patset to be used for insert_before_all, insert_after_all, replace_all, delete_all action types.

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. Possible values: YES, NO Default value: NO

Example

i)add rewrite action act_insert INSERT_HTTP_HEADER change_req "\\"no change\\"" .This Adds to http header will add the header change_req: no change. ii)add rewrite action act_replace REPLACE "HTTP.REQ.URL.PREFIX(1)" "HTTP.REQ.URL.PREFIX(1)+\\"citrix/\\"" -bypassSafetyCheck YES .If Q.URL.PREFIX(1) is / the result would be /citrix/ iii)add rewrite action act_before INSERT_BEFORE "HTTP.REQ.HEADER(\\"host\\").VALUE(0)" "\\"india\\"" .If Q.HEADER(\\"host\\").VALUE(0) is netscaler.com the result would be indianetscaler.com iv)add rewrite action act_after INSERT_AFTER "HTTP.REQ.HEADER(\\"host\\").TYPECAST_LIST_T('.').GET(0)" "\\"-india\\"" .If Q.HEADER(\\"host\\").VALUE(0) is support.netscaler.com then the result would be support-india.netscaler.com v)add rewrite action act_delete DELETE "HTTP.REQ.HEADER(\\"host\\").VALUE(0)" will leave the Host header looking like "HOST: ". vi)add rewrite action act_delete_header DELETE_HTTP_HEADER Host will delete the Host header. If Host header occurs more than once all occurrence of the header will be deleted.

Related Commands

rm rewrite action

set rewrite action

unset rewrite action

show rewrite action

rm rewrite action

Synopsis

```
rm rewrite action <name>
```

Description

Remove a configured rewrite action.

Arguments

name

Name of the rewrite action.

Example

rm rewrite action act_before

Related Commands

add rewrite action

set rewrite action

unset rewrite action

show rewrite action

set rewrite action

Synopsis

```
set rewrite action <name> [-target <string>] [-
stringBuilderExpr <string>] (-pattern <expression> | -
patset <string>) [-bypassSafetyCheck ( YES | NO )]
```

Description

Modify rewrite action.

Arguments

name

The name of rewrite action to be modified.

target

Expression specifying which part of the HTTP packet is to be rewritten.

stringBuilderExpr

Expression specifying new value of the rewritten HTTP packet. Maximum length of the input expression is 8191. Maximum size of string that can be used inside the expression is 1499.

pattern

Pattern to be used for insert_before_all, insert_after_all, replace_all, delete_all action types.

patset

Patset to be used for insert_before_all, insert_after_all, replace_all, delete_all action types.

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. Possible values: YES, NO Default value: NO

Example

set rewrite action rwact1 -target "HTTP.REQ.HEADER(\\"MyHdr\\")" -stringBuilderExpr "HTTP.REQ.URL.MARK_SAFE"

Related Commands

add rewrite action
rm rewrite action
unset rewrite action
show rewrite action

unset rewrite action

Synopsis

```
unset rewrite action <name> [-stringBuilderExpr] [-
pattern] [-patset]
```

Description

Use this command to remove rewrite action settings.Refer to the set rewrite action command for meanings of the arguments.

Related Commands

add rewrite action

rm rewrite action

set rewrite action

show rewrite action

show rewrite action

Synopsis

```
show rewrite action [<name>]
```

Description

Display configured rewrite action(s).

Arguments

name
Name of the rewrite action.

summary

fullValues

format

level

Output

state

type
Type of rewrite action. It can be:
(delete|replace|insert_http_header|insert_before|insert_after|replace_http_res).

target
Expression specifying which part of HTTP header needs to be rewritten.

stringBuilderExpr
Expression specifying the value of rewritten HTTP header.

pattern
Pattern used for insert_before_all, insert_after_all, replace_all, delete_all action types.

patset
Patset to be used for insert_before_all, insert_after_all, replace_all, delete_all action types.

bypassSafetyCheck
The safety check to allow unsafe expressions.

hits
The number of times the action has been taken.

undefHits
The number of times the action resulted in UNDEF.

referenceCount
The number of references to the action.

description
Description of the action

Example

1. show rewrite action 2. show rewrite action act_insert

Related Commands

add rewrite action

rm rewrite action

set rewrite action

unset rewrite action

bind rewrite global

Synopsis

```
bind rewrite global <policyName> <priority>
[<gotoPriorityExpression>] [-type <type>] [-invoke
(<labelType>  <labelName>) ]
```

Description

Bind the rewrite policy to one of the two global lists of rewrite policies. A policy becomes active only after it is bound. All HTTP traffic will be evaluated against these two policy banks. There is a request time policy bank and a response time policy bank. The flow type of the policy implicitly determines which bank it gets bound to. Each bank of policies is an ordered list ordered by policies priority values. Policy Bank Evaluation The goal of evaluation is to traverse the ordered list of policies in the bank, find out which policies match and build a result set that will contain the actions of all the matching policies. While evaluating a policy if any advanced expression cannot be evaluated then UNDEF processing will get triggered. There are also other scenarios during policy traversal when UNDEF processing can get triggered. If an UNDEF event occurs while processing a policy, then (i) policy bank traversal ends, (ii) the result set of actions that was built so far is wiped out (iii) the current policy's undefAction is put in the result set and the evaluation ends.

Arguments

`policyName`

The rewrite policy name.

Example

i)bind rewrite global pol9 9 ii)bind rewrite global pol9 9 120 iii)bind rewrite global pol9 9
"HTTP.REQ.HEADER(\\"qh3\\").TYPECAST_NUM_T(DECIMAL)"

Related Commands

unbind rewrite global

show rewrite global

unbind rewrite global

Synopsis

```
unbind rewrite global <policyName> [-type <type>] [-
priority <positive_integer>]
```

Description

Unbind entities from rewrite global.

Arguments

policyName

The rewrite policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind rewrite global pol9

Related Commands

bind rewrite global

show rewrite global

show rewrite global

Synopsis

```
show rewrite global [-type <type>]
```

Description

Display the rewrite global bindings.

Arguments

type
The bindpoint to which to policy is bound. Possible values:
REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

summary

fullValues

format

level

Output

state

policyName
Name of the rewrite policy.

priority
Specifies the priority of the policy.

gotoPriorityExpression
Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType
Type of policy label invocation.

labelName
Name of the label to invoke if the current policy rule evaluates to TRUE.

numpol
The number of policies bound to the bindpoint.

flowType
flowtype of the bound rewrite policy.

Example

show rewrite global

Related Commands

bind rewrite global
unbind rewrite global

set rewrite param

Synopsis

```
set rewrite param -undefAction <string>
```

Description

Set the default rewrite undef action. If an UNDEF event is triggered during policy evaluation and if the current policy.s undefAction is not specified, then this global undefAction value is used. NOREWRITE is the default value of default rewrite undef action

Arguments

undefAction

can be NOREWRITE, RESET or DROP

Example

set rewrite param -undefAction RESET

Related Commands

unset rewrite param

show rewrite param

unset rewrite param

Synopsis

```
unset rewrite param -undefAction
```

Description

Unset rewrite params..Refer to the set rewrite param command for meanings of the arguments.

Example

unset rewrite param -undefAction

Related Commands

set rewrite param

show rewrite param

show rewrite param

Synopsis

```
show rewrite param
```

Description

Display default rewrite undef action.

Arguments

format

level

Output

undefAction

Name of the rewrite action.

Example

show rewrite param

Related Commands

set rewrite param

unset rewrite param

add rewrite policylabel

Synopsis

```
add rewrite policylabel <labelName> <transform>
```

Description

Add a rewrite policy label.

Arguments

`labelName`

Name of the rewrite policy label.

`transform`

The type of transformations allowed by the policies bound to the label. Possible values: http_req, http_res, url, text, clientless_vpn_req, clientless_vpn_res

Example

add rewrite policylabel trans_http_url http_req

Related Commands

rm rewrite policylabel

bind rewrite policylabel

unbind rewrite policylabel

show rewrite policylabel

rm rewrite policylabel

Synopsis

```
rm rewrite policylabel <labelName>
```

Description

Remove a rewrite policy label.

Arguments

`labelName`

Name of the rewrite policy label.

Example

rm rewrite policylabel trans_http_url

Related Commands

add rewrite policylabel

bind rewrite policylabel

unbind rewrite policylabel

show rewrite policylabel

bind rewrite policylabel

Synopsis

```
bind rewrite policylabel <labelName> <policyName>
<priority> [<gotoPriorityExpression>] [-invoke
(<labelType>  <labelName>) ]
```

Description

Bind the rewrite policy to one of the labels.

Arguments

labelName

Name of the rewrite policy label.

policyName

The rewrite policy name.

Example

i)bind rewrite policylabel trans_http_url pol_1 1 2 -invoke reqvserver CURRENT ii)bind rewrite policylabel trans_http_url pol_2 2

Related Commands

add rewrite policylabel

rm rewrite policylabel

unbind rewrite policylabel

show rewrite policylabel

unbind rewrite policylabel

Synopsis

```
unbind rewrite policylabel <labelName> <policyName> [-
priority <positive_integer>]
```

Description

Unbind entities from rewrite label.

Arguments

labelName

Name of the rewrite policy label.

policyName

The rewrite policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind rewrite policylabel trans_http_url pol_1

Related Commands

add rewrite policylabel

rm rewrite policylabel

bind rewrite policylabel

show rewrite policylabel

show rewrite policylabel

Synopsis

```
show rewrite policylabel [<labelName>]
```

Description

Display policy label or policies bound to rewrite policylabel.

Arguments

labelName
Name of the rewrite policy label.

summary

fullValues

format

level

Output

state

transform
The type of transformations allowed by the policies bound to the label.

numpol
Number of polices bound to label.

hits
Number of times policy label was invoked.

policyName
The rewrite policy name.

priority
Specifies the priority of the policy.

gotoPriorityExpression
Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType
Type of policy label invocation.

labelName
Name of the label to invoke if the current policy rule evaluates to TRUE.

flowType
Flowtype of the bound rewrite policy.

description
Description of the policylabel

Example

i)show rewrite policylabel trans_http_url ii)show rewrite policylabel

Related Commands

add rewrite policylabel
rm rewrite policylabel
bind rewrite policylabel
unbind rewrite policylabel

stat rewrite policy

Synopsis

```
stat rewrite policy [<name>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display rewrite policy statistics.

Arguments

name

The name of the rewrite policy for which statistics will be displayed. If not given statistics are shown for all rewrite policies.

Output

Counters

Policy hits (Hits)

Number of hits on the policy

Policy undef hits (Undefhits)

Number of undef hits on the policy

Example

stat rewrite policy

Related Commands

add rewrite policy

rm rewrite policy

set rewrite policy

unset rewrite policy

show rewrite policy

CHAPTER 33

NTP Commands

This chapter covers the NTP commands.

enable ntp sync

Synopsis

```
enable ntp sync
```

Description

Enable NTP synchronization

Related Commands

disable ntp sync

show ntp sync

disable ntp sync

Synopsis

```
disable ntp sync
```

Description

Disable NTP synchronization

Related Commands

enable ntp sync

show ntp sync

show ntp sync

Synopsis

```
show ntp sync
```

Description

Show NTP sync info

Arguments

Output

state

Show NTP status

Related Commands

enable ntp sync

disable ntp sync

add ntp server

Synopsis

```
add ntp server (<serverIP> | <serverName>) [-minpoll
<positive_integer>] [-maxpoll <positive_integer>]
```

Description

Add NTP server

Arguments

serverIP

IP address of the NTP server.

serverName

Fully qualified domain name of the NTP server.

minpoll

Specifies the minimum poll intervals for NTP messages, in seconds to the power of two. Value defaults to 6 (64 s), but can be decreased to a lower limit of 4 (16 s). Default value: NS_NTP_MINPOLL_DEFAULT_VALUE Minimum value: 4

maxpoll

Specifies the maximum poll intervals for NTP messages, in seconds to the power of two. Value defaults to 10 (1,024 s), but can be increased to an upper limit of 17 (36.4 h). Default value: NS_NTP_MAXPOLL_DEFAULT_VALUE Maximum value: 17

Related Commands

rm ntp server

set ntp server

unset ntp server

show ntp server

rm ntp server

Synopsis

```
rm ntp server (<serverIP> | <serverName>)
```

Description

Remove NTP server entry

Arguments

`serverIP`

IP address of the NTP server.

`serverName`

Fully qualified domain name of the NTP server.

Related Commands

add ntp server

set ntp server

unset ntp server

show ntp server

set ntp server

Synopsis

```
set ntp server (<serverIP> | <serverName>) [-minpoll
<positive_integer>] [-maxpoll <positive_integer>]
```

Description

Modify the NTP server entries.

Arguments

serverIP

IP address of the NTP server.

serverName

Fully qualified domain name of the NTP server.

minpoll

Specifies the minimum poll intervals for NTP messages, in seconds to the power of two. Value defaults to 6 (64 s), but can be decreased to a lower limit of 4 (16 s) Default value: NS_NTP_MINPOLL_DEFAULT_VALUE Minimum value: 4

maxpoll

Specifies the maximum poll intervals for NTP messages, in seconds to the power of two. Value defaults to 10 (1,024 s), but can be increased to an upper limit of 17 (36.4 h). Default value: NS_NTP_MAXPOLL_DEFAULT_VALUE Maximum value: 17

Related Commands

add ntp server

rm ntp server

unset ntp server

show ntp server

unset ntp server

Synopsis

```
unset ntp server [<serverIP>] [<serverName>] [-minpoll]
[-maxpoll]
```

Description

Use this command to remove ntp server settings.Refer to the set ntp server command for meanings of the arguments.

Related Commands

add ntp server

rm ntp server

set ntp server

show ntp server

show ntp server

Synopsis

```
show ntp server [<serverIP> | <serverName>]
```

Description

Show NTP server information.

Arguments

serverIP

IP address of the NTP server.

serverName

Fully qualified domain name of the NTP server.

summary

fullValues

format

level

Output

minpoll

Minimum poll interval of the server in secs.

maxpoll

Maximum poll interval of the server in secs.

Related Commands

add ntp server

rm ntp server

set ntp server

unset ntp server

CHAPTER 34

URL Transforms Commands

This chapter covers the url transforms commands.

add transform profile

Synopsis

```
add transform profile <name> [-type URL]
```

Description

Create a URL Transformation profile.

Arguments

name

URL Transformation profile name.

type

Type of transformation. Possible values: URL

Related Commands

rm transform profile

set transform profile

unset transform profile

show transform profile

rm transform profile

Synopsis

```
rm transform profile <name>
```

Description

Remove a URL Transformation profile.

Arguments

name

URL Transformation profile name.

Related Commands

add transform profile

set transform profile

unset transform profile

show transform profile

set transform profile

Synopsis

```
set transform profile <name> [-type URL] [-
onlyTransformAbsURLinBody ( ON | OFF )] [-comment
<string>]
```

Description

Modify URL Transformation action settings.

Arguments

name

URL Transformation action name.

type

Type of transformation. Possible values: URL

onlyTransformAbsURLinBody

Flag to only perform transformations of absolute URLs in HTTP body. Possible values: ON, OFF

comment

Comments.

Related Commands

add transform profile

rm transform profile

unset transform profile

show transform profile

unset transform profile

Synopsis

```
unset transform profile <name> [-type] [-
onlyTransformAbsURLinBody] [-comment]
```

Description

Use this command to remove transform profile settings.Refer to the set transform profile command for meanings of the arguments.

Related Commands

add transform profile

rm transform profile

set transform profile

show transform profile

show transform profile

Synopsis

```
show transform profile [<name>]
```

Description

Display the configured URL Transformation profiles.

Arguments

name
URL Transformation profile name.

summary

fullValues

format

level

Output

type
Type of transformation.

RegexForFindingURLinJavaScript
Patclass having regexes to find the URLs in JavaScript.

RegexForFindingURLinCSS
Patclass having regexes to find the URLs in CSS.

RegexForFindingURLinXComponent
Patclass having regexes to find the URLs in X-Component.

RegexForFindingURLinXML
Patclass having regexes to find the URLs in XML.

additionalReqHeadersList
Patclass having a list of additional request header names that should transformed.

additionalRespHeadersList
Patclass having a list of additional response header names that should transformed.

onlyTransformAbsURLinBody
Flag to only perform transformations of absolute URLs in HTTP body.

comment
Comments.

priority
Priority of the Action within the Profile.

state
Enabled flag.

Related Commands

add transform profile
rm transform profile
set transform profile
unset transform profile

add transform action

Synopsis

```
add transform action <name> <profileName> <priority>
```

Description

Create a URL Transformation action.

Arguments

`name`

URL Transformation action name.

`profileName`

URL Transformation profile name.

`priority`

Priority of the Action within the Profile. Minimum value: 1 Maximum value: 2147483647

Related Commands

rm transform action

set transform action

unset transform action

show transform action

rm transform action

Synopsis

```
rm transform action <name>
```

Description

Remove a URL Transformation action.

Arguments

name

URL Transformation action name.

Related Commands

add transform action

set transform action

unset transform action

show transform action

set transform action

Synopsis

```
set transform action <name> [-priority
<positive_integer>] [-reqUrlFrom <expression>] [-
reqUrlInto <expression>] [-resUrlFrom <expression>] [-
resUrlInto <expression>] [-cookieDomainInto
<expression>] [-state ( ENABLED | DISABLED )] [-comment
<string>]
```

Description

Modify URL Transformation action settings.

Arguments

name

URL Transformation action name.

priority

Priority of the Action within the Profile. Minimum value: 1 Maximum value: 2147483647

reqUrlFrom

Pattern of original request URLs. It corresponds to the way external users view the server, and acts as a source for request transformations.

reqUrlInto

Pattern of transformed request URLs. It corresponds to internal addresses and indicates how they are created.

resUrlFrom

Pattern of original response URLs. It corresponds to the way external users view the server, and acts as a source for response transformations.

resUrlInto

Pattern of transformed response URLs. It corresponds to internal addresses and indicates how they are created.

cookieDomainInto
Pattern of transformed request URLs. It corresponds to internal addresses and indicates how they are created.

state
Enabled flag. Possible values: ENABLED, DISABLED

comment
Comments.

Related Commands

add transform action
rm transform action
unset transform action
show transform action

unset transform action

Synopsis

```
unset transform action <name> [-priority] [-reqUrlFrom]
[-reqUrlInto] [-resUrlFrom] [-resUrlInto] [-
cookieDomainInto] [-state] [-comment]
```

Description

Use this command to remove transform action settings.Refer to the set transform action command for meanings of the arguments.

Related Commands

add transform action

rm transform action

set transform action

show transform action

show transform action

Synopsis

```
show transform action [<name>]
```

Description

Display the configured URL Transformation action.

Arguments

`name`
URL Transformation profile name.

`summary`

`fullValues`

`format`

`level`

Output

`profileName`
URL Transformation profile name.

`priority`
Priority of the Action within the Profile.

`reqUrlFrom`
Pattern of original request URLs. It corresponds to the way external users view the server, and acts as a source for request transformations.

`reqUrlInto`
Pattern of transformed request URLs. It corresponds to internal addresses and indicates how they are created.

`resUrlFrom`
Pattern of original response URLs. It corresponds to the way external users view the server, and acts as a source for response transformations.

resUrlInto
Pattern of transformed response URLs. It corresponds to internal addresses and indicates how they are created.

cookieDomainInto
Pattern of transformed request URLs. It corresponds to internal addresses and indicates how they are created.

continueMatching
Continue transforming using the next rule in the list.

state
Enabled flag.

comment
Comments.

Related Commands

add transform action

rm transform action

set transform action

unset transform action

add transform policy

Synopsis

```
add transform policy <name> <rule> <profileName>
```

Description

Create a URL Transformation policy.

Arguments

`name`
URL Transformation policy name.

`rule`
The rule associated with the policy.

`profileName`
URL Transformation profile name.

Related Commands

rm transform policy
show transform policy

rm transform policy

Synopsis

```
rm transform policy <name>
```

Description

Remove a URL Transformation policy.

Arguments

name

URL Transformation policy name.

Related Commands

add transform policy

show transform policy

show transform policy

Synopsis

```
show transform policy [<name>]
```

Description

Display the Url Transform policies.

Arguments

name
URL Transformation policy name.

summary

fullValues

format

level

Output

state

rule
The rule associated with the policy.

profileName
URL Transformation profile name.

priority
Specifies the priority of the policy.

hits
Number of hits.

Related Commands

add transform policy
rm transform policy

bind transform global

Synopsis

```
bind transform global <policyName> <priority>
```

Description

Bind the Url Transform policy globally

Arguments

policyName

The Url Transform policy name.

Example

bind transform global pol9 9

Related Commands

unbind transform global

show transform global

unbind transform global

Synopsis

```
unbind transform global <policyName>
```

Description

Unbind globally bound Url Transfrom policy.

Arguments

policyName

The Url Transform policy name.

Example

unbind transform global pol9

Related Commands

bind transform global

show transform global

show transform global

Synopsis

```
show transform global
```

Description

Display the rewrite global bindings.

Arguments

summary

fullValues

format

level

Output

state

policyName
Name of the Url Transfrom policy.

priority
Specifies the priority of the policy.

Example

show rewrite global

Related Commands

bind transform global

unbind transform global

CHAPTER 35

Utility Commands

This chapter covers the utility commands.

ping

Synopsis

```
ping [-c <count>] [-i <interval>] [-I <interface>] [-n]
[-p <pattern>] [-q] [-s <size>] [-S <src_addr>] [-t
<timeout>] <hostname>
```

Description

Invoke the UNIX ping command. The <hostName> option is used if the name is in /etc/hosts file directory or is otherwise known in DNS.

Arguments

c

Number of packets to send (default is infinite)

i

Waiting time in seconds (default is 1 sec)

I

Network interface on which to ping, if you have multiple interfaces

n

Numeric output only - no name resolution

p

Pattern to fill in packets. Can be up to 16 bytes, useful for diagnosing data-dependent problems.

q

Quiet output - only summary is printed

s

Data size in bytes (default is 56)

S

The source IP address to be used in the outgoing query packets. If the IP addrESS Is not one of this machine's addresses, an error is returned and nothing is sent.

t
Timeout in seconds before ping exits

hostName
Address of host to ping

Example

ping -p ff -I rl0 -c 4 10.102.4.107

Related Commands

ping6

Synopsis

```
ping6 [-c <count>] [-i <interval>] [-I <interface>] [-
n] [-p <pattern>] [-q] [-S sourceaddr] [-s <size>] [-t
<timeout>] Hostname
```

Description

Invoke the UNIX ping6 command. The <hostName> option is used if the name is in /etc/hosts file directory or is otherwise known in DNS.

Arguments

c

Number of packets to send (default is infinite)

i

Waiting time in seconds (default is 1 sec)

I

Network interface on which to ping6, if you have multiple interfaces

n

Numeric output only - no name resolution

p

Pattern to fill in packets. Can be up to 16 bytes, useful for diagnosing data-dependent problems.

q

Quiet output - only summary is printed

s

Data size in bytes (default is 56)

S

The source IP address to be used in the outgoing query packets.

t

Timeout in seconds before ping6 exits

hostName
Address of host to ping6

Example

ping6 -p ff -I 1/1 -c 4 2002::1

Related Commands

traceroute

Synopsis

```
traceroute [-S] [-n] [-r] [-v] [-M <min_ttl] [-m
<max_ttl>] [-P <protocol>][-p <portno>] [-q <nqueries>]
[-s <src_addr>] [-t <tos>]  [-w <wait>] <host>
[<packetlen>]
```

Description

Invoke the UNIX traceroute command. Traceroute attempts to track the route that the packets follow to reach the destination host.

Arguments

S

Print a summary of how many probes were not answered for each hop.

n

Print hop addresses numerically rather than symbolically andnumerically.

r

Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned.

v

Verbose output. Received ICMP packets other than TIME_EXCEEDED and UNREACHABLEs are listed.

M

The minimum ttl value used in outgoing probe packets. Default value: 1

m

The maximum TTL value used in outgoing probe packets. Default value: 64

P

Send packets of specified IP protocol. The currently supported protocols are UDP and ICMP.

p
The base port number used in probes. Default value: 33434

q
The number of queries per hop. Default value: 3

s
The source IP address to be used in the outgoing query packets. If the IP address is not one of this machine's addresses, an error is returned and nothing is sent.

t
The type-of-service in query packets. Default value: 0 Minimum value: 0 Maximum value: 255

w
The time (in seconds) to wait for a response to a query. Default value: 5 Minimum value: 2 Maximum value: 86399

host
The destination host ip address or name.

packetlen
The packet length (in bytes) of the query packets. Default value: 44 Minimum value: 44 Maximum value: 32768

Example

traceroute 10.102.4.107

Related Commands

traceroute6

Synopsis

```
traceroute6 [-n] [I] [-r] [-v] [-m <hoplimit>]  [-p
<port>] [-q <probes>] [-s <src_addr>] [-w <waittime>]
<target> [<packetlen>]
```

Description

Invoke the UNIX traceroute6 command. Traceroute6 attempts to track the route that the packets follow to reach the destination host.

Arguments

n

Print hop addresses numerically rather than symbolically andnumerically.

I

Use ICMP ECHO for probes

r

Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned.

v

Verbose output. Received ICMP packets other than TIME_EXCEEDED and UNREACHABLEs are listed.

m

The maximum hop value used in outgoing probe packets. Default value: 64

p

The base port number used in probes. Default value: 33434

q

The number of probe per hop. Default value: 3

s
The source IP address to be used in the outgoing query packets. If the IP address is not one of this machine's addresses, an error is returned and nothing is sent.

w
The time (in seconds) to wait for a response to a query. Default value: 5 Minimum value: 2 Maximum value: 86399

host
The destination host ip address or name.

packetlen
The packet length (in bytes) of the query packets. Default value: 44 Minimum value: 44 Maximum value: 32768

Example

traceroute6 2002::7

Related Commands

grep

Synopsis

```
grep [-c] [-E] [-i] [-v] [-w] [-x] <pattern>
```

Description

grep to search files or output for lines containing a match to the given <pattern>. By default, grep prints the matching lines.

Arguments

c

Suppress normal output; instead print a count of matching lines. With the -v option, count non-matching lines.

E

Interpret <pattern> as an extended regular expression.

i

Ignore case distinctions.

v

Invert the sense of matching, to select non-matching lines.

w

Select only those lines containing matches that form whole words.

x

Select only those matches that exactly match the whole line.

pattern

The pattern (regular expression or text string) being sought.

Example

show ns info | grep off -i

Related Commands

install

Synopsis

```
install <url> [-c] [-y]
```

Description

Install a version of NetScaler software on the system. The command takes a single argument consisting of a valid URL for the HTTP, HTTPS, FTP, and SFTP protocols. Local files may be specified using the file:// URL variation. http://[user]:[password]@host/path/to/file https://[user]:[password]@host/path/to/file sftp://[user]:[password]@host/path/to/file scp://[user]:[password]@host/path/to/file ftp://[user]:[password]@host/path/to/file file://path/to/file

Arguments

url

http://[user]:[password]@host/path/to/file https://[user]:[password]@host/path/to/file sftp://[user]:[password]@host/path/to/file scp://[user]:[password]@host/path/to/file ftp://[user]:[password]@host/path/to/file file://path/to/file

c

Specifiy this option to backup existing kernel.

y

Specify this option to avoid prompt for yes/no i.e. reboot.

Example

install http://host.netscaler.com/ns-6.0-41.2.tgz

Related Commands

shell

Synopsis

shell [(command)]

Description

Exit to the FreeBSD command prompt, where FreeBSD commands may be entered. Press the <Control> + <D> keys or type exit to return to the NetScaler system CLI prompt.

Arguments

command

The shell command(s) to be invoked.

Example

> shell # ps | grep nscli 485 p0 S 0:01.12 -nscli (nscli) 590 p0 S+ 0:00.00 grep nscli # ^D Done > shell ps -aux |grep nscli 485 p0 S 0:01.12 -nscli (nscli) 590 p0 S+ 0:00.00 grep nscli

Related Commands

scp

Synopsis

```
scp [-r] [-C] [-q] <sourceString> <destString>
```

Description

Securely copy data from one computer to another via the ssh protocol.

Arguments

r

Recursively copy subdirectories

C

Enable compression

q

Quiet output - disable progress meter

sourceString

The source user, host and file path, specified as user@host:path/to/copy/from. User and host parts are optional.

destString

The destination user, host and file path, specified as user@host:path/to/copy/to. User and host parts are optional.

Example

scp /nsconfig/ns.conf nsroot@10.102.4.107:/nsconfig/

Related Commands

nstrace

Synopsis

```
nstrace [-nf <positive_integer>] [-time <secs>] [-size
<positive_integer>] [-mode <mode> ...] [-tcpdump (
ENABLED | DISABLED )  [-perNIC ( ENABLED | DISABLED )]]
[-name <string>  [-id <string>]] [-filter <expression>
[-link ( ENABLED | DISABLED )]]
```

Description

Invoke nstrace program to log traffic flowing through netscaler

Arguments

h

prints this message - exclusive option

nf

number of files to be generated in cycle Default value: 24

time

Log in each trace file for 'time' seconds. (could be an expression) Default value: 3600

size

size of the packet to be logged(should be in the range of 60 to 1514 bytes). Setting size as zero, logs full packet. Default value: 164 Maximum value: 1514

m

Capturing mode: sum of the values: 1 - Transmitted packets (TX) 2 - Packets buffered for transmission (TXB) 4 - Received packets (RX) Default value: 6

tcpDump

nstrace-format, tcpdump-format Possible values: NSTRACE, TCPDUMP Default value: 0

mode

Capturing mode for trace. Mode can be any of the following values or combination of these values: RXReceived packets before NIC pipelining NEW_RXReceived packets after NIC pipelining TXTransmitted packets TXBPackets buffered for transmission IPV6 Translated IPv6 packets Default mode: NEW_RX TXB Default value: ARRAY(0x8968240)

tcpdump

Log files format supported:nstrace-format, tcpdump-format. default:nstrace-format Possible values: ENABLED, DISABLED Default value: DISABLED

name

Custom file name for nstrace files

filter

Filter expression for nstrace. Maximum length of filter is 255.

Example

nstrace -nf 10 -time 100 -mode RX IPV6 TXB -name abc -tcpdump ENABLED -perNIC ENABLED

Related Commands

show techsupport

Synopsis

```
show techsupport [<fileName>]
```

Description

This command generates a tar archive of system configuration data and statistics for submission to Citrix ANG technical support. The archive is always named /var/tmp/support.tgz for each invocation of the command.

Arguments

`fileName`
Name of support file.

Output

`serverName`

Example

show techsupport

Related Commands

config audit

Synopsis

Description

audit and verify the commands in file against running config. NOTE: This command is deprecated.Command deprecated. Use diff ns config command

Arguments

commandStr

specify the options.

Example

config audit -diff -f <filename>

Related Commands

CHAPTER 36

AAA for Application Traffic Commands

This chapter covers the AAA for application traffic commands.

add tm sessionPolicy

Synopsis

```
add tm sessionPolicy <name> <rule> <action>
```

Description

Add a tm session policy, which conditionally sets characteristics of a tm session upon session establishment.

Arguments

name

The name for the new tm session policy.

rule

The rule to be evaluated in the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The action to be performed when the rule is matched.

Related Commands

rm tm sessionPolicy

set tm sessionPolicy

unset tm sessionPolicy

show tm sessionPolicy

rm tm sessionPolicy

Synopsis

```
rm tm sessionPolicy <name>
```

Description

Remove a previously created tm session policy.

Arguments

name

The name of the policy to be removed.

Related Commands

add tm sessionPolicy

set tm sessionPolicy

unset tm sessionPolicy

show tm sessionPolicy

set tm sessionPolicy

Synopsis

```
set tm sessionPolicy <name> [-rule <expression>] [-
action <string>]
```

Description

Modify the rule or action of a tm session policy.

Arguments

name

The name of the tm session policy.

rule

The new rule to be associated with the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The new tm session action for the policy.

Related Commands

add tm sessionPolicy

rm tm sessionPolicy

unset tm sessionPolicy

show tm sessionPolicy

unset tm sessionPolicy

Synopsis

```
unset tm sessionPolicy <name> [-rule] [-action]
```

Description

Use this command to remove tm sessionPolicy settings.Refer to the set tm sessionPolicy command for meanings of the arguments.

Related Commands

add tm sessionPolicy

rm tm sessionPolicy

set tm sessionPolicy

show tm sessionPolicy

show tm sessionPolicy

Synopsis

```
show tm sessionPolicy [<name>]
```

Description

Display the configured tm session policies.

Arguments

`name`

The name of the tm session policy.

`summary`

`fullValues`

`format`

`level`

Output

`rule`

The new rule associated with the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

`action`

The new tm session action the policy is using.

`boundTo`

The entity name to which policy is bound

Related Commands

add tm sessionPolicy

rm tm sessionPolicy

set tm sessionPolicy

unset tm sessionPolicy

add tm sessionAction

Synopsis

```
add tm sessionAction <name> [-sessTimeout <mins>] [-
defaultAuthorizationAction ( ALLOW | DENY )] [-SSO ( ON
| OFF )] [-ssoCredential ( PRIMARY | SECONDARY )]
```

Description

Create a session action, which defines the properties of a TM session.

Arguments

name

The name for the new tm session action.

sessTimeout

The session timeout, in minutes, to be set by the action. Minimum value: 1

defaultAuthorizationAction

This toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY

SSO

Enables or disables the use of Single Sign-on for the session. Possible values: ON, OFF Default value: OFF

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY Default value: 0

Related Commands

rm tm sessionAction

set tm sessionAction

unset tm sessionAction

show tm sessionAction

rm tm sessionAction

Synopsis

```
rm tm sessionAction <name>
```

Description

Delete a previously created session action.

Arguments

name

The tm session action to be removed.

Related Commands

add tm sessionAction

set tm sessionAction

unset tm sessionAction

show tm sessionAction

set tm sessionAction

Synopsis

```
set tm sessionAction <name> [-sessTimeout <mins>] [-
defaultAuthorizationAction ( ALLOW | DENY )] [-SSO ( ON
| OFF )] [-ssoCredential ( PRIMARY | SECONDARY )]
```

Description

Modify a session action, which defines the properties of a TM session.

Arguments

name

The name of the tm session action.

sessTimeout

The session timeout, in minutes, to be set by the action. Minimum value: 1

defaultAuthorizationAction

This toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY

SSO

Enables or disables the use of Single Sign-on for the session. Possible values: ON, OFF Default value: OFF

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY

Related Commands

add tm sessionAction

rm tm sessionAction

unset tm sessionAction

show tm sessionAction

unset tm sessionAction

Synopsis

```
unset tm sessionAction <name> [-sessTimeout] [-
defaultAuthorizationAction] [-SSO] [-ssoCredential]
```

Description

Use this command to remove tm sessionAction settings.Refer to the set tm sessionAction command for meanings of the arguments.

Related Commands

add tm sessionAction

rm tm sessionAction

set tm sessionAction

show tm sessionAction

show tm sessionAction

Synopsis

```
show tm sessionAction [<name>]
```

Description

Display tm session action details.

Arguments

name

The name of the tm session action.

summary

fullValues

format

level

Output

sessTimeout

The session timeout, in minutes, set by the action.

defaultAuthorizationAction

The Authorization Action, e.g. allow or deny

SSO

Whether or not Single Sign-On is used for this session.

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On

Related Commands

add tm sessionAction

rm tm sessionAction

set tm sessionAction

unset tm sessionAction

bind tm global

Synopsis

```
bind tm global [-policyName <string>  [-priority
<positive_integer>]]
```

Description

Bind session/audit policies to tm global.

Arguments

policyName

The name of the policy to be bound to tm global.

Related Commands

unbind tm global

show tm global

unbind tm global

Synopsis

```
unbind tm global -policyName <string>
```

Description

Unbind audit/session policies from tm global.

Arguments

policyName

The name of the policy to be unbound.

Related Commands

bind tm global

show tm global

show tm global

Synopsis

```
show tm global
```

Description

Display the tm global bindings.

Arguments

summary

fullValues

format

level

Output

policyName
The name of the policy.

priority
The priority of the policy.

type
Bindpoint to which the policy is bound

Related Commands

bind tm global
unbind tm global

set tm sessionParameter

Synopsis

```
set tm sessionParameter [-sessTimeout <mins>] [-
defaultAuthorizationAction ( ALLOW | DENY )] [-SSO ( ON
| OFF )] [-ssoCredential ( PRIMARY | SECONDARY )]
```

Description

Set global parameters for the tm session

Arguments

sessTimeout

The session idle timeout value in minutes. This idle timeout meters the overall network inactivity for a session. Default value: 30 Minimum value: 1

defaultAuthorizationAction

The authorization action state. Toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY Default value: NS_ALLOW

SSO

Whether or not Single Sign-On is used Possible values: ON, OFF Default value: OFF

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY Default value: VPN_SESS_ACT_USE_PRIMARY_CREDENTIALS

Related Commands

unset tm sessionParameter

show tm sessionParameter

unset tm sessionParameter

Synopsis

```
unset tm sessionParameter [-sessTimeout] [-SSO] [-
defaultAuthorizationAction] [-ssoCredential]
```

Description

Unset parameters for the tm session.Refer to the set tm sessionParameter command for meanings of the arguments.

Related Commands

set tm sessionParameter

show tm sessionParameter

show tm sessionParameter

Synopsis

```
show tm sessionParameter
```

Description

Display the configured tm session parameters.

Arguments

format

level

Output

sessTimeout
The session timeout, in minutes.

defaultAuthorizationAction
The Authentication Action, e.g. allow or deny.

SSO
Whether or not Single Sign-On is used for this session.

ssoCredential
The set of user credentials (primary or secondary) to use for Single Sign-On

Related Commands

set tm sessionParameter

unset tm sessionParameter

CHAPTER 37

SSL VPN Commands

This chapter covers the SSL VPN commands.

stat vpn

Synopsis

```
stat vpn [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>]
```

Description

Display VPN statistics.

Arguments

Output

Counters

Login-page requests received (iHtHit)
Total number of login-page request received by SSLVPN server.

Login-page delivery failures (iHtFail)
Number of times login-page has not been delivered by SSLVPN server.

Client-configuration requests (cfgHit)
Total number of SSLVPN-client configuration request received by SSLVPN-server. In response to this SSLVPN-server returns information to configure SSLVPN-client.

DNS queries resolved (dnsHit)
Total number of DNS query(s) resolved by SSLVPN server.

WINS queries resolved (winsHit)
Total number of WINS query(s) resolved by SSLVPN server.

Number of SSLVPN tunnels (csHit)
Total number of SSLVPN tunnels created between SSLVPN client and server.

Backend non-HTTP server probes (csNoHttp)
Number of probes from NetScaler to backend non-HTTP servers. The backend servers are those servers which has been accessed by VPN client. This is an application debug counter.

Backend HTTP server probes (csHttp)
Number of probes from NetScaler to backend HTTP server. The backend servers are those servers which has been accessed by VPN client. This is an application debug counter.

Backend server probe successes (csConSuc)
Number of successful probes to backend servers (both HTTP and non-HTTP). This is an application debug counter.

File-system requests received (totFsHit)
Total number of file-system request received by SSLVPN server.

IIP disabled and MIP used (IIPdMIPu)
Number of times MIP is used as IIP is disabled.

IIP failed and MIP used (IIPfMIPu)
Number of times MIP is used as IIP assignment failed.

IIP spillover and MIP used (IIPsMIPu)
Number of times MIP is used on IIP Spillover.

IIP disabled and MIP disabled (IIPdMIPd)
Both IIP and MIP is disabled.

IIP failed and MIP disabled (IIPfMIPd)
Number of times IIP assignment failed and MIP is disabled.

SOCKS method request received (SOCKSmReqR)
Number of received SOCKS method request.

SOCKS method request sent (SOCKSmReqS)
Number of sent SOCKS method request.

SOCKS method response received (SOCKSmRespR)
Number of received SOCKS method response.

SOCKS method response sent (SOCKSmRespS)
Number of sent SOCKS method response.

SOCKS connect request received (SOCKScReqR)
Number of received SOCKS connect request.

SOCKS connect request sent (SOCKScReqS)
Number of sent SOCKS connect request.

SOCKS connect response received (SOCKScRespR)
Number of received SOCKS connect response.

SOCKS connect response sent (SOCKScRespS)
Number of sent SOCKS connect response.

SOCKS server error (SOCKSserverErr)
Number of SOCKS server error.

SOCKS client error (SOCKSclientErr)
Number of SOCKS client error.

STA connection success (STAconnSucc)
Number of STA connection success.

STA connection failure (STAconnFail)
Number of STA connection failure.

CPS connection success (CPSconnSucc)
Number of CPS connection success.

CPS connection failure (CPSconnFail)
Number of CPS connection failure.

STA request sent (STAreqSent)
Number of STA request sent.

STA response received (STArespRecvd)
Number of STA response received.

ICA license failure (ICAlicenseFail)
Number of ICA license failure.

Related Commands

stat vpn vserver

show vpn stats

Synopsis

```
show vpn stats - alias for 'stat vpn'
```

Description

show vpn stats is an alias for stat vpn

Related Commands

stat vpn

add vpn vserver

Synopsis

```
add vpn vserver <name> <serviceType> (<IPAddress>  [-
range <positive_integer>]) <port> [-state ( ENABLED |
DISABLED )] [-authentication ( ON | OFF )] [-
maxAAAUsers <positive_integer>] [-downStateFlush (
ENABLED | DISABLED )]
```

Description

Add a VPN virtual server.

Arguments

`name`

The name for the new vpn vserver.

`serviceType`

The vpn vserver's protocol type, e.g. SSL Possible values: SSL Default value: NSSVC_SSL

`IPAddress`

The IP address for the vpn vserver.

`port`

The TCP port on which the vserver listens. Minimum value: 1

`state`

The intital vserver server state, e.g. ENABLED or DISABLED Possible values: ENABLED, DISABLED Default value: ENABLED

`authentication`

This option toggles on or off the application of authentication of incoming users to the VPN. Possible values: ON, OFF Default value: ON

`maxAAAUsers`

The maximum number of concurrent users allowed to login into this vserver at a time. The administrator can configure any number between 0 and 65535 for this virtual server, but the actual number of users allowed to login into this

virtual server will also depend on the total number of user licenses and the total number of currently logged in users. Minimum value: 0 Maximum value: 65535

downStateFlush

Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

The following example creates a VPN vserver named myvpnvip which supports SSL portocol and with AAA functionality enabled: vserver myvpnvip SSL 65.219.17.34 443 -aaa ON

Related Commands

rm vpn vserver

set vpn vserver

unset vpn vserver

enable vpn vserver

disable vpn vserver

show vpn vserver

stat vpn vserver

rm vpn vserver

Synopsis

```
rm vpn vserver <name>@ ...
```

Description

Remove a virtual server.

Arguments

name

The name of the virtual server to be removed.

Example

rm vserver vpn_vip

Related Commands

add vpn vserver

set vpn vserver

unset vpn vserver

enable vpn vserver

disable vpn vserver

show vpn vserver

stat vpn vserver

set vpn vserver

Synopsis

```
set vpn vserver <name> [-IPAddress
<ip_addr|ipv6_addr|*>] [-authentication ( ON | OFF )]
[-maxAAAUsers <positive_integer>] [-downStateFlush (
ENABLED | DISABLED )]
```

Description

Change the parameters of a VPN virtual server.

Arguments

name

The name of the vserver to be modified.

IPAddress

The new IP address of the virtual server.

authentication

Indicates whether or not authentication is being applied to incoming users to the VPN. Possible values: ON, OFF Default value: ON

maxAAAUsers

The maximum number of concurrent users allowed to login into this vserver at a time. The administrator can configure any number between 0 and 65535 for this virtual server, but the actual number of users allowed to login into this virtual server will also depend on the total number of user licenses and the total number of currently logged in users. Minimum value: 0 Maximum value: 65535

downStateFlush

Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

Related Commands

add vpn vserver

rm vpn vserver

unset vpn vserver

enable vpn vserver
disable vpn vserver
show vpn vserver

stat vpn vserver

unset vpn vserver

Synopsis

```
unset vpn vserver <name> [-authentication] [-
maxAAAUsers] [-downStateFlush]
```

Description

Use this command to remove vpn vserver settings.Refer to the set vpn vserver command for meanings of the arguments.

Related Commands

add vpn vserver

rm vpn vserver

set vpn vserver

enable vpn vserver

disable vpn vserver

show vpn vserver

stat vpn vserver

bind vpn vserver

Synopsis

```
bind vpn vserver <name> [-policy <string>  [-priority
<positive_integer>]  [-secondary]] [-
intranetApplication <string>] [-nextHopServer
<string>] [-urlName <string>] [-intranetIP <ip_addr>
<netmask>] [-staServer <URL>]
```

Description

Bind attributes to a vserver.

Arguments

name

The vserver to which this command shall bind parameters.

policy

The name of the policy to be bound to the vserver.

intranetApplication

The name of the intranet application to be bound to the vserver.

nextHopServer

The name of the next hop server to be bound to the vserver.

urlName

The name of the vpn url to be bound.

intranetIP

The network id for the range of intranet IP addresses or individual intranet ip to be bound to the vserver.

staServer

Secure Ticketing Authority (STA) server, in the format 'http(s)://IP/FQDN/URLPATH'

Related Commands

unbind vpn vserver

unbind vpn vserver

Synopsis

```
unbind vpn vserver <name> [-policy <string>  [-
secondary]] [-intranetApplication <string>] [-
nextHopServer <string>] [-urlName <string>] [-
intranetIP <ip_addr>  <netmask>] [-staServer <URL>]
```

Description

Unbind attributes from a vserver.

Arguments

name

The name of the vserver from which an attribute is to be unbound.

policy

The name of the policy to be unbound.

intranetApplication

The intranet application to be unbound.

nextHopServer

The name of the next hop server to be unbound.

urlName

The vpn url to be unbound.

intranetIP

The network id for the range of intranet IP addresses or the individually bound intranet IP address to be unbound.

staServer

Secure Ticketing Authority (STA) server to be removed, in the format 'http(s)://IP/FQDN/URLPATH'

Related Commands

bind vpn vserver

enable vpn vserver

Synopsis

```
enable vpn vserver <name>@
```

Description

Enable a virtual vpn server. Note:Virtual servers, when added, are enabled by default.

Arguments

name

The name of the virtual server to be enabled.

Example

enable vserver vpn1

Related Commands

add vpn vserver

rm vpn vserver

set vpn vserver

unset vpn vserver

disable vpn vserver

show vpn vserver

stat vpn vserver

disable vpn vserver

Synopsis

```
disable vpn vserver <name>@
```

Description

Disable (take out of service) a virtual server.

Arguments

name

The name of the virtual server to be disabled. Notes: 1.The system still responds to ARP and/or ping requests for the IP address of this virtual server. 2.As the virtual server is still configured in the system, you can enable the virtual server using ###enable vserver### command.

Example

disable vserver lb_vip

Related Commands

add vpn vserver

rm vpn vserver

set vpn vserver

unset vpn vserver

enable vpn vserver

show vpn vserver

stat vpn vserver

show vpn vserver

Synopsis

```
show vpn vserver [<name>] show vpn vserver stats -
alias for 'stat vpn vserver'
```

Description

Display all of the configured VPN virtual servers.

Arguments

`name`
The name of the VPN vserver.

`summary`

`fullValues`

`format`

`level`

Output

`IPAddress`
The Virtual IP address of the VPN vserver.

`IPAddress`
The IP address of the virtual server.

`value`
Indicates whether or not the certificate is bound or if SSL offload is disabled.

`port`
The virtual TCP port of the VPN vserver.

`range`
The range of vpn vserver IP addresses. The new range of vpn vservers will have IP addresses consecutively numbered, starting with the primary address specified with the <ipaddress> argument.

serviceType
The vpn vserver's protocol type, Currently the only possible value is SSL.

type
The type of Virtual Server, e.g. CONTENT based or ADDRESS based.

state
The current state of the Virtual server, e.g. UP, DOWN, BUSY, etc.

status
Whether or not this vserver responds to ARPs and whether or not round-robin selection is temporarily in effect.

cacheType
Virtual server's cache type. The options are: TRANSPARENT, REVERSE and FORWARD.

redirect
The cache redirect policy. The valid redirect policies are: l.CACHE - Directs all requests to the cache. 2.POLICY - Applies cache redirection policy to determine whether the request should be directed to the cache or origin. This is the default setting. 3.ORIGIN - Directs all requests to the origin server.

precedence
This argument is used only when configuring content switching on the specified virtual server. This is applicable only if both the URL and RULE-based policies have been configured on the same virtual server. It specifies the type of policy (URL or RULE) that takes precedence on the content switching virtual server. The default setting is RULE. lURL - In this case, the incoming request is matched against the URL-based policies before the rule-based policies. lRULE - In this case, the incoming request is matched against the rule-based policies before the URL-based policies. For all URL-based policies, the precedence hierarchy is: 1.Domain and exact URL 2.Domain, prefix and suffix 3.Domain and suffix 4.Domain and prefix 5.Domain only 6. Exact URL 7.Prefix and suffix 8.Suffix only 9.Prefix only 10.Default

redirectURL
The URL where traffic is redirected if the virtual server in system becomes unavailable. WARNING!Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the ###add cs policy### command. If the same domain is specified in both

arguments, the request will be continuously redirected to the same unavailable virtual server in the system. If so, the user may not get the requested content.

authentication
Indicates whether or not authentication is being applied to incoming users to the VPN.

maxAAAUsers
The maximum number of concurrent users allowed to login into this vserver at a time.

curAAAUsers
The number of current users logged in to this vserver.

domain
The domain name of the server for which a service needs to be added. If the IP Address has been specified, the domain name does not need to be specified.

rule
The name of the rule, or expression, if any, that policy for the vpn server is to use. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide. The default rule is ns_true.

policyName
The name of the policy, if any, bound to the vpn vserver.

serviceName
The name of the service, if any, to which the vserver policy is bound.

weight
Weight for this service, if any. This weight is used when the system performs load balancing, giving greater priority to a specific service. It is useful when the services bound to a virtual server are of different capacity.

cacheVserver
The name of the default target cache virtual server, if any, to which requests are redirected.

backupVServer
The name of the backup vpn virtual server for this vpn virtual server.

priority
The priority, if any, of the vpn vserver policy.

cltTimeout
The idle time, if any, in seconds after which the client connection is terminated.

soMethod
VPN client applications are allocated from a block of Intranet IP addresses. That block may be exhausted after a certain number of connections. This switch specifies the method used to determine whether or not a new connection will spillover, or exhaust, the allocated block of Intranet IP addresses for that application. Possible values are CONNECTION or DYNAMICCONNECTION. CONNECTION means that a static integer value is the hard limit for the spillover threshold. The spillover threshold is described below. DYNAMICCONNECTION means that the spillover threshold is set according to the maximum number of connections defined for the vpn vserver.

soThreshold
VPN client applications are allocated from a block of Intranet IP addresses. That block may be exhausted after a certain number of connections. The value of this option is number of client connections after which the Mapped IP address is used as the client source IP address instead of an address from the allocated block of Intranet IP addresses.

soPersistence
Whether or not cookie-based site persistance is enabled for this VPN vserver. Possible values are 'ConnectionProxy', HTTPRedirect, or NONE

soPersistenceTimeOut
The timeout, if any, for cookie-based site persistance of this VPN vserver.

intranetApplication
The intranet vpn application.

nextHopServer
The name of the next hop server bound to vpn vserver.

urlName
The intranet url.

intranetIP
The network id for the range of intranet IP addresses or individual intranet ip to be bound to the vserver.

netmask
The netmask of the intranet ip or range.

staServer
Configured Secure Ticketing Authority (STA) server.

staAuthID
Authority ID of the STA Server. Authority ID is used to match incoming STA Tickets in the SOCKS/CGP protocol with the right STA Server.

useMIP
Deprecated. See 'map' below.

map
Whether or not Mapped IP Addresses are ON or OFF. Mapped IP addresses are source IP addresses for the virtual servers running on the NetScaler. Mapped IP addresses are used by the system to connect to the backend servers.

downStateFlush
Perform delayed clean up of connections on this vserver.

type
Bindpoint to which the policy is bound

gotoPriorityExpression
Next priority expression.

disablePrimaryOnDown
Tells whether traffic will continue reaching backup vservers even after primary comes UP from DOWN state.

Example

show vpn vserver

Related Commands

add vpn vserver

rm vpn vserver

set vpn vserver
unset vpn vserver
enable vpn vserver
disable vpn vserver

stat vpn vserver

add vpn intranetApplication

Synopsis

```
add vpn intranetApplication <intranetApplication>
[<protocol>] ((<destIP>  [-netmask <netmask>]) |
<IPRange> | <hostName> | (-clientApplication <string>
...  [-spoofIIP ( ON | OFF )])) [-destPort <port[-
port]>] [-interception ( PROXY | TRANSPARENT )  [-srcIP
<ip_addr>]  [-srcPort <port>]]
```

Description

Add an intranet application.

Arguments

`intranetApplication`
The name for the new vpn intranet application.

`protocol`
The protocol of the intranet application, e.g. TCP, UDP or ANY. Possible values: TCP, UDP, ANY

`destIP`
The destination IP address for the application. This address is the real application server IP address.

`clientApplication`
The names of the client applications

`destPort`
The destination TCP or UDP port range. Minimum value: 1

`interception`
The interception type, e.g. proxy or transparent Possible values: PROXY, TRANSPARENT

`srcIP`
This is the source IP address of the client application. If not optionally specified, the default is 127.0.0.1.

srcPort
The source application TCP or UDP port. Minimum value: 1

Related Commands

rm vpn intranetApplication
show vpn intranetApplication

rm vpn intranetApplication

Synopsis

```
rm vpn intranetApplication <intranetApplication>
```

Description

Remove a configured intranet application.

Arguments

`intranetApplication`

The name of the vpn intranet application to remove.

Related Commands

add vpn intranetApplication

show vpn intranetApplication

show vpn intranetApplication

Synopsis

```
show vpn intranetApplication [<intranetApplication>]
```

Description

Display the configured vpn intranet applications.

Arguments

intranetApplication

summary

fullValues

format

level

Output

protocol
The IP protocol, e.g. TCP, UDP or ANY

destIP
The destination IP address.

netmask
The destination netmask.

IPAddress
The IP address for the application. This address is the real application server IP address.

hostName
Name based interception. Names should be valid dns or wins names and will be resolved during interception on the sslvpn.

destPort
The destination port.

clientApplication
The names of the client applications

spoofIIP
This specifies whether to spoof this application on the client.

interception
The interception type, e.g. proxy or transparent.

srcIP
The source IP address.

srcPort
The source port.

Related Commands

add vpn intranetApplication
rm vpn intranetApplication

add vpn nextHopServer

Synopsis

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort>
[-secure ( ON | OFF )]
```

Description

Add an next hop server.

Arguments

name

Configures new vpn next hop server.

nextHopIP

Configures next hop IP address.

nextHopPort

Configures next hop port number.

secure

Configures next hop over secure connection. Possible values: ON, OFF
Default value: OFF

Example

add vpn nexthopserver dh1 10.1.1.1 80 -secure OFF

Related Commands

rm vpn nextHopServer

show vpn nextHopServer

rm vpn nextHopServer

Synopsis

```
rm vpn nextHopServer <name>
```

Description

Remove vpn next hop server.

Arguments

name

The name of the vpn next hop server to be removed.

Example

rm vpn nexthopserver dh1

Related Commands

add vpn nextHopServer

show vpn nextHopServer

show vpn nextHopServer

Synopsis

```
show vpn nextHopServer [<name>]
```

Description

Display the configured vpn next hop servers.

Arguments

name

summary

fullValues

format

level

Output

nextHopIP
Next hop IP address.

nextHopPort
Next hop port number.

secure
Next hop over secure connection.

Example

show vpn nexthopserver dh1

Related Commands

add vpn nextHopServer

rm vpn nextHopServer

show vpn icaConnection

Synopsis

```
show vpn icaConnection [-userName <string>]
```

Description

Display the active ICA connections.

Arguments

userName
The user name.

summary

fullValues

Output

domain
The domain name.

srcIP
The client IP address.

srcPort
The client port.

destIP
The CPS server IP address.

destPort
The CPS server port.

Related Commands

bind vpn global

Synopsis

```
bind vpn global [-policyName <string>  [-priority
<positive_integer>]  [-secondary]] [-intranetDomain
<string>] [-intranetApplication <string>] [-
nextHopServer <string>] [-urlName <string>] [-
intranetIP <ip_addr>  <netmask>] [-staServer <URL>]
```

Description

Bind vpn entities to vpn global.

Arguments

policyName
The name of the policy to be bound to vpn global.

intranetDomain
A conflicting intranet domain name.

intranetApplication
The vpn intranet application to be bound.

nextHopServer
The name of the next hop server to be bound globally.

urlName
The vpn url to be bound.

intranetIP
The intranet ip or range to be bound to VPN global.

staServer
Secure Ticketing Authority (STA) server, in the format 'http(s)://IP/FQDN/URLPATH'

Related Commands

unbind vpn global
show vpn global

unbind vpn global

Synopsis

```
unbind vpn global [-policyName <string>  [-secondary]]
[-intranetDomain <string>] [-intranetApplication
<string>] [-nextHopServer <string>] [-urlName <string>]
[-intranetIP <ip_addr>  <netmask>] [-staServer <URL>]
```

Description

Unbind entities from vpn global.

Arguments

policyName
The name of the policy to be unbound.

intranetDomain
A conflicting intranet domain name to be unbound.

intranetApplication
The name of a vpn intranet application to be unbound.

nextHopServer
The name of the next hop server to be unbound globally.

urlName
The name of a vpn url to be unbound from vpn global.

intranetIP
The intranet ip address or range to be unbound.

staServer
Secure Ticketing Authority (STA) server to be removed, in the format 'http(s)://IP/FQDN/URLPATH'

Related Commands

bind vpn global

show vpn global

show vpn global

Synopsis

```
show vpn global
```

Description

Display the vpn global bindings.

Arguments

summary

fullValues

format

level

Output

state

policyName
The name of the policy.

priority
The priority of the policy.

intranetDomain
The conflicting intranet domain name.

intranetApplication
The intranet vpn application.

nextHopServer
The name of the next hop server bound to vpn global.

urlName
The intranet url.

intranetIP
The intranet ip address or range.

netmask
The intranet ip address or range's netmask.

staServer
Configured Secure Ticketing Authority (STA) server.

staAuthID
Authority ID of the STA Server. Authority ID is used to match incoming STA Tickets in the SOCKS/CGP protocol with the right STA Server.

type
Bindpoint to which the policy is bound

Related Commands

bind vpn global
unbind vpn global

add vpn trafficPolicy

Synopsis

```
add vpn trafficPolicy <name> <rule> <action>
```

Description

Add a traffic policy. A traffic policy conditionally sets VPN traffic characteristics at run time.

Arguments

`name`

The name for the new vpn traffic policy.

`rule`

The rule to be used by the vpn traffic policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

`action`

The action to be applied by the policy if its rule is matched.

Related Commands

rm vpn trafficPolicy

set vpn trafficPolicy

unset vpn trafficPolicy

show vpn trafficPolicy

rm vpn trafficPolicy

Synopsis

```
rm vpn trafficPolicy <name>
```

Description

Remove a vpn traffic policy.

Arguments

name

The name of the vpn traffic policy to be removed.

Related Commands

add vpn trafficPolicy

set vpn trafficPolicy

unset vpn trafficPolicy

show vpn trafficPolicy

set vpn trafficPolicy

Synopsis

```
set vpn trafficPolicy <name> [-rule <expression>] [-
action <string>]
```

Description

Change the properties of an existing traffic policy.

Arguments

name

The name of the policy.

rule

The new rule to be used in the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The new action to be applied by the policy.

Related Commands

add vpn trafficPolicy

rm vpn trafficPolicy

unset vpn trafficPolicy

show vpn trafficPolicy

unset vpn trafficPolicy

Synopsis

```
unset vpn trafficPolicy <name> [-rule] [-action]
```

Description

Use this command to remove vpn trafficPolicy settings.Refer to the set vpn trafficPolicy command for meanings of the arguments.

Related Commands

add vpn trafficPolicy

rm vpn trafficPolicy

set vpn trafficPolicy

show vpn trafficPolicy

show vpn trafficPolicy

Synopsis

```
show vpn trafficPolicy [<name>]
```

Description

Display vpn traffic policies.

Arguments

`name`
The name of the vpn trafiic policy.

`summary`

`fullValues`

`format`

`level`

Output

`rule`
The rule used by the vpn traffic policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide

`action`
The action to be performed when the rule is matched.

`boundTo`
The entity name to which policy is bound

Related Commands

add vpn trafficPolicy
rm vpn trafficPolicy
set vpn trafficPolicy
unset vpn trafficPolicy

add vpn trafficAction

Synopsis

```
add vpn trafficAction <name> <qual> [-appTimeout
<mins>] [-SSO ( ON | OFF ) | -wanscaler ( ON | OFF )] [-
fta ( ON | OFF )]
```

Description

Create a vpn traffic action. A vpn traffic action defines the characteristics of run time VPN traffic.

Arguments

name

The name for the action.

qual

The protocol to be set with the action, e.g. http or tcp. Possible values: http, tcp

appTimeout

The inactivity timeout after which the system closes a connection. Minimum value: 1 Maximum value: 715827

SSO

Enable or disable Single Sign-On Possible values: ON, OFF

fta

Enable or disable file-type association Possible values: ON, OFF

wanscaler

Enable or disable wanscaler Possible values: ON, OFF

Related Commands

rm vpn trafficAction

set vpn trafficAction

unset vpn trafficAction

show vpn trafficAction

rm vpn trafficAction

Synopsis

```
rm vpn trafficAction <name>
```

Description

Remove a previously created traffic action.

Arguments

name

The name of the action to be removed.

Related Commands

add vpn trafficAction

set vpn trafficAction

unset vpn trafficAction

show vpn trafficAction

set vpn trafficAction

Synopsis

```
set vpn trafficAction <name> [-appTimeout <mins>] [-SSO ( ON | OFF ) | -wanscaler ( ON | OFF )] [-fta ( ON | OFF )]
```

Description

Modifies a vpn traffic action. A vpn traffic action defines the characteristics of run time VPN traffic.

Arguments

`name`

The name for the action.

`appTimeout`

The inactivity timeout after which the system closes a connection. Minimum value: 1 Maximum value: 715827

`SSO`

switch to turn on the SSO engine for HTTP traffic. Possible values: ON, OFF

`fta`

Enable or disable file-type association Possible values: ON, OFF

`wanscaler`

Enable or disable wanscaler Possible values: ON, OFF

Related Commands

add vpn trafficAction

rm vpn trafficAction

unset vpn trafficAction

show vpn trafficAction

unset vpn trafficAction

Synopsis

```
unset vpn trafficAction <name> -wanscaler
```

Description

Use this command to remove vpn trafficAction settings.Refer to the set vpn trafficAction command for meanings of the arguments.

Related Commands

add vpn trafficAction

rm vpn trafficAction

set vpn trafficAction

show vpn trafficAction

show vpn trafficAction

Synopsis

```
show vpn trafficAction [<name>]
```

Description

Display the configured vpn traffic action(s).

Arguments

name
The name of the vpn trafiic action.

summary

fullValues

format

level

Output

qual
The protocol that is set with the action, e.g. http or tcp.

appTimeout
The application timeout

SSO
Whether or not Single Sign On is enabled.

fta
Whether or not file-type association is enabled.

wanscaler
Enable or disable wanscaler

Related Commands

add vpn trafficAction

rm vpn trafficAction

set vpn trafficAction
unset vpn trafficAction

add vpn url

Synopsis

```
add vpn url <urlName> <linkName> <actualURL> [-
clientlessAccess ( ON | OFF )]
```

Description

Add vpn urls. A vpn url provides a link to intranet resources on the vpn portal page.

Arguments

urlName

The name for the new vpn url.

linkName

The display name for the vpn url. This is the name that will display in the bookmark links in the vpn portal page.

actualURL

The actual URL that the vpn url points to.

clientlessAccess

Enable clientless access for the URL in other VPN modes if permitted. In clientless mode of VPN, it is enabled by default. Possible values: ON, OFF Default value: OFF

Example

add vpn url ggl search www.google.com.

Related Commands

rm vpn url

set vpn url

unset vpn url

show vpn url

rm vpn url

Synopsis

```
rm vpn url <urlName>
```

Description

Remove vpn urls.

Arguments

urlName

The name of the vpn url to be removed.

Example

rm vpn url ggl

Related Commands

add vpn url

set vpn url

unset vpn url

show vpn url

set vpn url

Synopsis

```
set vpn url <urlName> [-linkName <string>] [-actualURL
<string>] [-clientlessAccess ( ON | OFF )]
```

Description

Modifies a vpn url. A vpn url provides a link to intranet resources on the vpn portal page.

Arguments

urlName

The name of the vpn url to be modified.

linkName

The display name for the vpn url. This is the name that will display in the bookmark links in the vpn portal page.

actualURL

The actual URL that the vpn url points to.

clientlessAccess

Enable or disable clientless access mode for the url in other modes. Possible values: ON, OFF Default value: OFF

Example

set vpn url wiurl -clientlessAccess on

Related Commands

add vpn url

rm vpn url

unset vpn url

show vpn url

unset vpn url

Synopsis

```
unset vpn url <urlName> -clientlessAccess
```

Description

Use this command to remove vpn url settings.Refer to the set vpn url command for meanings of the arguments.

Related Commands

add vpn url

rm vpn url

set vpn url

show vpn url

show vpn url

Synopsis

```
show vpn url [<urlName>]
```

Description

Display the configured vpn urls.

Arguments

urlName

summary

fullValues

format

level

Output

clientlessAccess

Whether clientless access is enabled for the url in other modes or not.

Related Commands

add vpn url

rm vpn url

set vpn url

unset vpn url

add vpn sessionPolicy

Synopsis

```
add vpn sessionPolicy <name> <rule> <action>
```

Description

Add a vpn session policy, which conditionally sets characteristics of a vpn session upon session establishment.

Arguments

`name`

The name for the new vpn session policy.

`rule`

The rule to be evaluated in the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

`action`

The action to be performed when the rule is matched.

Related Commands

rm vpn sessionPolicy

set vpn sessionPolicy

unset vpn sessionPolicy

show vpn sessionPolicy

rm vpn sessionPolicy

Synopsis

```
rm vpn sessionPolicy <name>
```

Description

Remove a previously created vpn session policy.

Arguments

name

The name of the policy to be removed.

Related Commands

add vpn sessionPolicy

set vpn sessionPolicy

unset vpn sessionPolicy

show vpn sessionPolicy

set vpn sessionPolicy

Synopsis

```
set vpn sessionPolicy <name> [-rule <expression>] [-
action <string>]
```

Description

Modify the rule or action of a vpn session policy.

Arguments

name

The name of the vpn session policy.

rule

The new rule to be associated with the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action

The new vpn session action for the policy.

Related Commands

add vpn sessionPolicy

rm vpn sessionPolicy

unset vpn sessionPolicy

show vpn sessionPolicy

unset vpn sessionPolicy

Synopsis

```
unset vpn sessionPolicy <name> [-rule] [-action]
```

Description

Use this command to remove vpn sessionPolicy settings.Refer to the set vpn sessionPolicy command for meanings of the arguments.

Related Commands

add vpn sessionPolicy

rm vpn sessionPolicy

set vpn sessionPolicy

show vpn sessionPolicy

show vpn sessionPolicy

Synopsis

```
show vpn sessionPolicy [<name>]
```

Description

Display the configured vpn session policies.

Arguments

`name`
The name of the vpn session policy.

`summary`

`fullValues`

`format`

`level`

Output

`rule`
The new rule associated with the policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

`action`
The new vpn session action the policy is using.

`boundTo`
The entity name to which policy is bound

Related Commands

add vpn sessionPolicy
rm vpn sessionPolicy
set vpn sessionPolicy
unset vpn sessionPolicy

add vpn sessionAction

Synopsis

```
add vpn sessionAction <name> [-httpPort <port> ...] [-
winsIP <ip_addr>] [-dnsVserverName <string>] [-splitDns
<splitDns>] [-sessTimeout <mins>] [-clientSecurity
<expression>  [-clientSecurityGroup <string>]  [-
clientSecurityMessage <string>]] [-clientSecurityLog (
ON | OFF )] [-splitTunnel <splitTunnel>] [-
localLanAccess ( ON | OFF )] [-rfc1918 ( ON | OFF )] [-
spoofIIP ( ON | OFF )] [-killConnections ( ON | OFF )]
[-transparentInterception ( ON | OFF )] [-
windowsClientType ( AGENT | PLUGIN )] [-
defaultAuthorizationAction ( ALLOW | DENY )] [-
authorizationGroup <string>] [-clientIdleTimeout
<mins>] [-proxy <proxy>] [-allProtocolProxy <string> |
-httpProxy <string> | -ftpProxy <string> | -socksProxy
<string> | -gopherProxy <string> | -sslProxy <string>]
[-proxyException <string>] [-proxyLocalBypass ( ENABLED
| DISABLED )] [-clientCleanupPrompt ( ON | OFF )] [-
forceCleanup <forceCleanup> ...] [-clientOptions
<clientOptions> ...] [-clientConfiguration
<clientConfiguration> ...] [-SSO ( ON | OFF )] [-
ssoCredential ( PRIMARY | SECONDARY )] [-
windowsAutoLogon ( ON | OFF )] [-useMIP ( NS | OFF )]
[-useIIP <useIIP>] [-clientDebug <clientDebug>] [-
loginScript <input_filename>] [-logoutScript
<input_filename>] [-homePage <URL>] [-icaProxy ( ON |
OFF )] [-wihome <URL>] [-citrixReceiverHome <URL>] [-
wiPortalMode ( NORMAL | COMPACT )] [-ClientChoices ( ON
| OFF )] [-iipDnsSuffix <string>] [-forcedTimeout
<mins>] [-forcedTimeoutWarning <mins>] [-ntDomain
<string>] [-clientlessVpnMode <clientlessVpnMode>] [-
```

```
emailHome <URL>] [-clientlessModeUrlEncoding
<clientlessModeUrlEncoding>] [-
clientlessPersistentCookie
<clientlessPersistentCookie>]
```

Description

Create a session action, which defines the properties of a VPN session.

Arguments

`name`
The name for the new vpn session action.

`httpPort`
The http port number for this session. Minimum value: 1

`winsIP`
The WINS server ip address for this session.

`dnsVserverName`
The name of the DNS vserver to be configured by the session action.

`splitDns`
Set the VPN client to route the DNS requests to remote network or local network or both. Possible values: LOCAL, REMOTE, BOTH

`sessTimeout`
The session timeout, in minutes, to be set by the action. Minimum value: 1

`clientSecurity`
The client security check string to be applied. This is in the form of an Expression. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

`clientSecurityLog`
Controls client side logging of security checks. Possible values: ON, OFF

`splitTunnel`
The split tunnel state, e.g. ON, OFF or REVERSE. Split Tunnelling ON enables the VPN client to route non-VPN traffic through its local network interface. When Split Tunnelling is OFF, no traffic may go to the local

interface while the client session is active. Split tunneling can also be set to REVERSE. In this case all traffic directed to domains configured on the system will bypass the VPN tunnel. All other traffic is forced through the VPN tunnel. Possible values: ON, OFF, REVERSE

localLanAccess
Finer grained local lan access. ON or OFF. splitTunnel, when OFF, permits no traffic to be routed to the client's local interface. But if, in addition, localLanAccess is turned ON, the client MAY route traffic to its local interface. This combination of switches is useful primarily when the rfc1918 switch is also specified. In this fashion, the client may restrict local lan access to devices which commonly have non-routable addresses, such as local printers or local file servers. Possible values: ON, OFF

rfc1918
Only allow RFC1918 local addresses when local LAN access feature is enabled. Possible values: ON, OFF

spoofIIP
Controls the Spoofing of Intranet IP to the Windows Applications by Windows VPN client when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF

killConnections
Determines whether Windows VPN client should kill all pre-existing connections (ie, the connections existing before the end user logged in to SSL VPN) and prevent new incoming connections on the Windows Client system when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF

transparentInterception
The transparent interception state, e.g. ON or OFF. Possible values: ON, OFF

windowsClientType
Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed\ b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

defaultAuthorizationAction
This toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY

authorizationGroup
The authorization group to be applied to the session.

clientIdleTimeout
Defines the client idle timeout value. Measured in minutes, the client idle timeout default is 20 minutes and meters a client session's keyboard and mouse inactivity. Minimum value: 1 Maximum value: 9999

proxy
Enables or disables use of a proxy configuration in the session. Possible values: BROWSER, NS, OFF

allProtocolProxy
Sets the address to use for all proxies.

httpProxy
Sets the HTTP proxy IP address.

ftpProxy
Defines the FTP proxy IP address.

socksProxy
The SOCKS proxy IP address.

gopherProxy
Sets the Gopher proxy IP address.

sslProxy
Sets the HTTPS proxy IP address.

proxyException
Proxy Exception string that will be configured in the Browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass
Bypass proxy server for local addresses option in IE proxy server settings will be enabled Possible values: ENABLED, DISABLED

clientCleanupPrompt
Toggles the prompt for client clean up on a client intitiated session close. Possible values: ON, OFF

forceCleanup
The client side items for force cleanup on session close. Options are: none, all, cookie, addressbar, plugin, filesystemapplication, addressbar, application, clientcertificate, applicationdata, and autocomplete. You may specify all or none alone or any combination of the client side items.

clientOptions
Display only configured buttons(and/or menu options in the docked client) in the Windows VPN client.\ Options:\ none\ none of the Windows Client's buttons/menu options (except logout) are displayed.\ all\ all of the Windows Client's buttons/menu options are displayed.\ \ One or more of the following\ services\ only the "Services" button/menu option is displayed.\ filetransfer\ only the "File Transfer" button/menu option is displayed.\ configuration\ only the "Configuration" button/menu option is displayed.

clientConfiguration
Display only configured tabs in the Windows VPN client.\ Options:\ none\ none of the Windows Client's tabs(except About) are displayed.\ all\ all of the Windows Client's tabs (except "Resptime") are displayed.\ \ One or more of the following\ general\ only the "General" tab is displayed.\ tunnel\ only the "Tunnel" tab is displayed.\ trace\ only the "Trace" tab is displayed.\ compression\ only the "Compression" tab is displayed.\ resptime\ only the "Resptime" tab is displayed.

SSO
Enables or disables the use of Single Sign-on for the session. Possible values: ON, OFF

ssoCredential
The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY Default value: 0

windowsAutoLogon
Enables or disables the Windows Auto Logon for the session. Possible values: ON, OFF

useMIP
Enables or disables the use of a Mapped IP address for the session Possible values: NS, OFF

useIIP
Controls how the intranet IP module is configured for usage. \ Options:\ SPILLOVER\ specifies that iip is ON and when we can't assign an intranet IP to an entity, which has other instances active, we spill over to using Mapped IP.\ NOSPILLOVER\ specifies that iip is ON and when we can't assign intranet IP to an entity, which has other instances active, then we initiate transfer login.\ OFFnspecifies that intranet IP module won't be activated for this entity. Possible values: NOSPILLOVER, SPILLOVER, OFF

clientDebug
Sets the trace level on the Windows VPN Client.\ Options:\ debugn\ Detailed debug messages are collected are written into the specified file.\ stats\ Application audit level error messages and debug statistic counters are written into the specified file.\ events\ Application audit level error messages are written into the specified file.\ off\ Only critical events are logged into the Windows Application Log. Possible values: debug, stats, events, OFF

loginScript
Login script path.

logoutScript
Logout script path.

homePage
Sets the client home page. Setting this parameter overrides serving the default portal page to SSL VPN users with the URL specified here.

icaProxy
Enable ICA proxy mode. This can be used to enable Secure Gateway functionality for the Web Interface. If enabled, a VPN homepage that points to a Web Interface in SG mode, has to be configured. Possible values: ON, OFF

wihome
Sets the home page of wi interface. Used only in conjunction with icaProxy ON. If clientChoices is ON, wiHome has to be configured. Since the end user is given a choice between FullClient and ICAProxy the homepage/landing page for each of these options could be different i.e. for FullClient it could be

a Intranet web site and for the ICAProxy choice it will be a Web Interface web site. Hence we don't presume wihome == homepage.

citrixReceiverHome
Sets the home page of apprecvr interface.

wiPortalMode
WI layout on the VPN portal. Possible values: NORMAL, COMPACT

ClientChoices
Enables user to select different clients by displaying a set of options in a html page. The different client can be a) agent b) plugin c) wimode. Possible values: ON, OFF

epaClientType
Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

iipDnsSuffix
Configure the IntranetIP DNS suffix. When a user logs into SSL-VPN, an A record is added to the DNS cache, after appending the configured IntranetIP DNS suffix to the username.

forcedTimeout
Maximum number of minutes a session is allowed to persist. Minimum value: 1 Maximum value: 255

forcedTimeoutWarning
Number of minutes to warn a user before their session is removed by a forced time out. Minimum value: 1 Maximum value: 255

ntDomain
NT domain to use with Smart Access when User Principle Name is not extracted from Active Directory Maximum value: 32

clientlessVpnMode
Whether clientlessVPN is available to the session. ON will make the session clientless and no client will be downloaded OFF will download the client but the clientlessVPN will also be available DISABLED will disable clientlessVPN altogether. Possible values: ON, OFF, DISABLED

`emailHome`
Sets the EMail home for the portal

`clientlessModeUrlEncoding`
URL encoding to be used in clientless mode. No encoding will be done for TRANSPARENT. Protocol and domain will be encoded or encrypted with OPAQUE or ENCRYPT respectively. Possible values: TRANSPARENT, OPAQUE, ENCRYPT

`clientlessPersistentCookie`
Controls the use of persistent cookie in clientless mode. ALLOW lets cookie to be stored on disk. DENY prevents usage of persistent cookie. PROMPT lets VPN user choose whether persistent cookie should be used or not. Possible values: ALLOW, DENY, PROMPT

Related Commands

rm vpn sessionAction

set vpn sessionAction

unset vpn sessionAction

show vpn sessionAction

rm vpn sessionAction

Synopsis

```
rm vpn sessionAction <name>
```

Description

Delete a previously created session action.

Arguments

name

The vpn session action to be removed.

Related Commands

add vpn sessionAction

set vpn sessionAction

unset vpn sessionAction

show vpn sessionAction

set vpn sessionAction

Synopsis

```
set vpn sessionAction <name> [-httpPort <port> ...] [-
winsIP <ip_addr>] [-dnsVserverName <string>] [-splitDns
<splitDns>] [-sessTimeout <mins>] [-clientSecurity
<expression>  [-clientSecurityGroup <string>]  [-
clientSecurityMessage <string>]] [-clientSecurityLog (
ON | OFF )] [-splitTunnel <splitTunnel>] [-
localLanAccess ( ON | OFF )] [-rfc1918 ( ON | OFF )] [-
spoofIIP ( ON | OFF )] [-killConnections ( ON | OFF )]
[-transparentInterception ( ON | OFF )] [-
windowsClientType ( AGENT | PLUGIN )] [-
defaultAuthorizationAction ( ALLOW | DENY )] [-
authorizationGroup <string>] [-clientIdleTimeout
<mins>] [-proxy <proxy>] [-allProtocolProxy <string> |
-httpProxy <string> | -ftpProxy <string> | -socksProxy
<string> | -gopherProxy <string> | -sslProxy <string>]
[-proxyException <string>] [-proxyLocalBypass ( ENABLED
| DISABLED )] [-clientCleanupPrompt ( ON | OFF )] [-
forceCleanup <forceCleanup> ...] [-clientOptions
<clientOptions> ...] [-clientConfiguration
<clientConfiguration> ...] [-SSO ( ON | OFF )] [-
ssoCredential ( PRIMARY | SECONDARY )] [-
windowsAutoLogon ( ON | OFF )] [-useMIP ( NS | OFF )]
[-useIIP <useIIP>] [-clientDebug <clientDebug>] [-
loginScript <input_filename>] [-logoutScript
<input_filename>] [-homePage <URL>] [-icaProxy ( ON |
OFF )] [-wihome <URL>] [-citrixReceiverHome <URL>] [-
wiPortalMode ( NORMAL | COMPACT )] [-ClientChoices ( ON
| OFF )] [-iipDnsSuffix <string>] [-forcedTimeout
<mins>] [-forcedTimeoutWarning <mins>] [-ntDomain
<string>] [-clientlessVpnMode <clientlessVpnMode>] [-
```

emailHome <URL>] [-clientlessModeUrlEncoding <clientlessModeUrlEncoding>] [-clientlessPersistentCookie <clientlessPersistentCookie>]

Description

Modify a session action, which defines the properties of a VPN session.

Arguments

name
The name of the vpn session action.

httpPort
The http port number for this session. Minimum value: 1

winsIP
The WINS server ip address.

dnsVserverName
The name of the DNS vserver to be configured by the session action.

splitDns
Set the VPN client to route the DNS requests to remote network or local network or both. Possible values: LOCAL, REMOTE, BOTH

sessTimeout
The session timeout, in minutes, to be set by the action. Minimum value: 1

clientSecurity
The client security check string to be applied. This is in the form of an Expression. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

clientSecurityLog
Controls client side logging of security checks. Possible values: ON, OFF

splitTunnel
The split tunnel state, e.g. ON, OFF or REVERSE. Split Tunnelling ON enables the VPN client to route non-VPN traffic through its local network interface. When Split Tunnelling is OFF, no traffic may go to the local

interface while the client session is active. Split tunneling can also be set to REVERSE. In this case all traffic directed to domains configured on the system will bypass the VPN tunnel. All other traffic is forced through the VPN tunnel. Possible values: ON, OFF, REVERSE

`localLanAccess`
Finer grained local lan access. ON or OFF. splitTunnel, when OFF, permits no traffic to be routed to the client's local interface. But if, in addition, localLanAccess is turned ON, the client MAY route traffic to its local interface. This combination of switches is useful primarily when the rfc1918 switch is also specified. In this fashion, the client may restrict local lan access to devices which commonly have non-routable addresses, such as local printers or local file servers. Possible values: ON, OFF

`rfc1918`
Only allow RFC1918 local addresses when local LAN access feature is enabled Possible values: ON, OFF

`spoofIIP`
Controls the Spoofing of Intranet IP to the Windows Applications by Windows VPN client when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF

`killConnections`
Determines whether Windows VPN client should kill all pre-existing connections (ie, the connections existing before the end user logged in to SSL VPN) and prevent new incoming connections on the Windows Client system when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF

`transparentInterception`
The transparent interception state, e.g. ON or OFF. Possible values: ON, OFF

`windowsClientType`
Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed\ b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

defaultAuthorizationAction
This toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY

authorizationGroup
The authorization group to be applied to the session.

clientIdleTimeout
Defines the client idle timeout value. Measured in minutes, the client idle timeout default is 20 minutes and meters a client session's keyboard and mouse inactivity. Minimum value: 1 Maximum value: 9999

proxy
Enables or disables use of a proxy configuration in the session. Possible values: BROWSER, NS, OFF

allProtocolProxy
Sets the address to use for all proxies.

httpProxy
Sets the HTTP proxy IP address.

ftpProxy
Defines the FTP proxy IP address.

socksProxy
The SOCKS proxy IP address.

gopherProxy
Sets the Gopher proxy IP address.

sslProxy
Sets the HTTPS proxy IP address.

proxyException
Proxy Exception string that will be configured in the Browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass
Bypass proxy server for local addresses option in IE proxy server settings will be enabled Possible values: ENABLED, DISABLED

clientCleanupPrompt
Toggles the prompt for client clean up on a client intitiated session close. Possible values: ON, OFF

forceCleanup
The client side items for force cleanup on session close. Options are: none, all, cookie, addressbar, plugin, filesystemapplication, addressbar, application, clientcertificate, applicationdata, and autocomplete. You may specify all or none alone or any combination of the client side items.

clientOptions
Display only configured buttons(and/or menu options in the docked client) in the Windows VPN client.\ Options:\ none\ none of the Windows Client's buttons/menu options (except logout) are displayed.\ all\ all of the Windows Client's buttons/menu options are displayed.\ \ One or more of the following\ services\ only the "Services" button/menu option is displayed.\ filetransfer\ only the "File Transfer" button/menu option is displayed.\ configuration\ only the "Configuration" button/menu option is displayed.

clientConfiguration
Display only configured tabs in the Windows VPN client.\ Options:\ none\ none of the Windows Client's tabs(except About) are displayed.\ all\ all of the Windows Client's tabs (except "Resptime") are displayed.\ \ One or more of the following\ general\ only the "General" tab is displayed.\ tunnel\ only the "Tunnel" tab is displayed.\ trace\ only the "Trace" tab is displayed.\ compression\ only the "Compression" tab is displayed.\ resptime\ only the "Resptime" tab is displayed.

SSO
Enables or disables the use of Single Sign-on for the session. Possible values: ON, OFF

ssoCredential
The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY

windowsAutoLogon
Enables or disables the Windows Auto Logon for the session. Possible values: ON, OFF

useMIP
Enables or disables the use of a Mapped IP address for the session Possible values: NS, OFF

useIIP
Controls how the intranet IP module is configured for usage. \ Options:\ SPILLOVER\ specifies that iip is ON and when we can't assign an intranet IP to an entity, which has other instances active, we spill over to using Mapped IP.\ NOSPILLOVER\ specifies that iip is ON and when we can't assign intranet IP to an entity, which has other instances active, then we initiate transfer login.\ OFFnspecifies that intranet IP module won't be activated for this entity. Possible values: NOSPILLOVER, SPILLOVER, OFF

clientDebug
Sets the trace level on the Windows VPN Client.\ Options:\ debugn\ Detailed debug messages are collected are written into the specified file.\ stats\ Application audit level error messages and debug statistic counters are written into the specified file.\ events\ Application audit level error messages are written into the specified file.\ off\ Only critical events are logged into the Windows Application Log. Possible values: debug, stats, events, OFF

loginScript
Login script path.

logoutScript
Logout script path.

homePage
Sets the client home page. Setting this parameter overrides serving the default portal page to SSL VPN users with the URL specified here.

icaProxy
Enable ICA proxy mode. This can be used to enable Secure Gateway functionality for the Web Interface. If enabled, a VPN homepage that points to a Web Interface in SG mode, has to be configured. Possible values: ON, OFF Default value: OFF

wihome
Sets the home page of wi interface. Used only in conjunction with icaProxy ON. If clientChoices is ON, wiHome has to be configured. Since the end user is given a choice between FullClient and ICAProxy the homepage/landing page for each of these options could be different i.e. for FullClient it could be

a Intranet web site and for the ICAProxy choice it will be a Web Interface web site. Hence we don't presume wihome == homepage.

citrixReceiverHome
Sets the home page of apprecvr interface.

wiPortalMode
WI layout on the VPN portal. Possible values: NORMAL, COMPACT

ClientChoices
Enables user to select different clients by displaying a set of options in a html page. The different client can be a) agent b) plugin c) wimode. Possible values: ON, OFF

epaClientType
Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

iipDnsSuffix
Configure the IntranetIP DNS suffix. When a user logs into SSL-VPN, an A record is added to the DNS cache, after appending the configured IntranetIP DNS suffix to the username.

forcedTimeout
Maximum number of minutes a session is allowed to persist. Minimum value: 1 Maximum value: 255

forcedTimeoutWarning
Number of minutes to warn a user before their session is removed by a forced time out. Minimum value: 1 Maximum value: 255

ntDomain
NT domain to use with Smart Access when User Principle Name is not extracted from Active Directory Maximum value: 32

clientlessVpnMode
Whether clientlessVPN is available to the session. ON will make the session clientless and no client will be downloaded OFF will download the client but the clientlessVPN will also be available DISABLED will disable

clientlessVPN altogether. Possible values: ON, OFF, DISABLED Default value: VPN_SESS_ACT_CVPNMODE_OFF

emailHome

Sets the EMail home for the portal

clientlessModeUrlEncoding

URL encoding to be used in clientless mode. No encoding will be done for TRANSPARENT. Protocol and domain will be encoded or encrypted with OPAQUE or ENCRYPT respectively. Possible values: TRANSPARENT, OPAQUE, ENCRYPT

clientlessPersistentCookie

Controls the use of persistent cookie in clientless mode. ALLOW lets cookie to be stored on disk. DENY prevents usage of persistent cookie. PROMPT lets VPN user choose whether persistent cookie should be used or not. Possible values: ALLOW, DENY, PROMPT Default value: VPN_SESS_ACT_CVPN_PERSCOOKIE_DENY

Related Commands

add vpn sessionAction

rm vpn sessionAction

unset vpn sessionAction

show vpn sessionAction

unset vpn sessionAction

Synopsis

```
unset vpn sessionAction <name> [-httpPort] [-winsIP] [-
dnsVserverName] [-splitDns] [-sessTimeout] [-
clientSecurity] [-clientSecurityGroup] [-
clientSecurityMessage] [-clientSecurityLog] [-
splitTunnel] [-localLanAccess] [-rfc1918] [-spoofIIP]
[-killConnections] [-transparentInterception] [-
windowsClientType] [-defaultAuthorizationAction] [-
authorizationGroup] [-clientIdleTimeout] [-proxy] [-
allProtocolProxy] [-httpProxy] [-ftpProxy] [-
socksProxy] [-gopherProxy] [-sslProxy] [-
proxyException] [-proxyLocalBypass] [-
clientCleanupPrompt] [-forceCleanup] [-clientOptions]
[-clientConfiguration] [-SSO] [-ssoCredential] [-
windowsAutoLogon] [-useMIP] [-useIIP] [-clientDebug] [-
loginScript] [-logoutScript] [-homePage] [-icaProxy] [-
wihome] [-citrixReceiverHome] [-wiPortalMode] [-
ClientChoices] [-iipDnsSuffix] [-forcedTimeout] [-
forcedTimeoutWarning] [-ntDomain] [-clientlessVpnMode]
[-emailHome] [-clientlessModeUrlEncoding] [-
clientlessPersistentCookie]
```

Description

Use this command to remove vpn sessionAction settings.Refer to the set vpn sessionAction command for meanings of the arguments.

Related Commands

add vpn sessionAction

rm vpn sessionAction

set vpn sessionAction

show vpn sessionAction

show vpn sessionAction

Synopsis

```
show vpn sessionAction [<name>]
```

Description

Display vpn session action details.

Arguments

name
The name of the vpn session action.

summary

fullValues

format

level

Output

httpPort
The HTTP port for this session action

winsIP
The WINS server IP address for this session action.

dnsVserverName
The name of the DNS vserver configured by the session action.

splitDns
The VPN client SplitDns state.

sessTimeout
The session timeout, in minutes, set by the action.

clientSecurity
The client security check string being applied. This is in the form of an Expression. Expressions are simple conditions, such as a test for equality,

applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

clientSecurityGroup
The client security group that will be assigned on failure of the client security check. Users can in general be organized into Groups. In this case, the Client Security Group may have a more restrictive security policy.

clientSecurityMessage
The client security message that will be displayed on failure of the client security check.

clientSecurityLog
Controls client side logging of security checks.

splitTunnel
The split tunnel state, e.g. ON, OFF or REVERSE. Split Tunnelling ON enables the VPN client to route non-VPN traffic through its local network interface. When Split Tunnelling is OFF, no traffic may go to the local interface while the client session is active. Split tunneling can also be set to REVERSE. In this case all traffic directed to domains configured on the system will bypass the VPN tunnel. All other traffic is forced through the VPN tunnel.

localLanAccess
Finer grained local lan access. ON or OFF. splitTunnel, when OFF, permits no traffic to be routed to the client's local interface. But if, in addition, localLanAccess is turned ON, the client MAY route traffic to its local interface. This combination of switches is useful primarily when the rfc1918 switch is also specified. In this fashion, the client may restrict local lan access to devices which commonly have non-routable addresses, such as local printers or local file servers.

rfc1918
Only allow RFC1918 local addresses when local LAN access feature is enabled.

spoofIIP
Controls the Spoofing of Intranet IP to the Windows Applications by Windows VPN client when the end-user is connected to SSL VPN in '-splittunnel OFF' mode.

killConnections
Determines whether Windows VPN client should kill all pre-existing connections (ie, the connections existing before the end user logged in to SSL VPN) and prevent new incoming connections on the Windows Client system when the end-user is connected to SSL VPN in '-splittunnel OFF' mode.

transparentInterception
The transparent interception state, e.g. ON or OFF.

windowsClientType
Windows client type, e.g. Agent or ActiveX

defaultAuthorizationAction
The Authorization Action, e.g. allow or deny

authorizationGroup
The authorization group applied to client sessions.

clientIdleTimeout
The client idle timeout, in minutes.

clientIdleTimeoutWarning
The time after which the client gets a timeout warning, in minutes.

proxy
The state of proxy configuration for the session.

allProtocolProxy
The address set for all proxies.

httpProxy
The HTTP proxy IP address.

ftpProxy
The FTP proxy IP address.

socksProxy
The SOCKS proxy IP address.

gopherProxy
The Gopher proxy IP address.

sslProxy
The HTTPS proxy IP address.

proxyException
Proxy Exception string that will be configured in the Browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass
Bypass proxy server for local addresses option in IE proxy server settings will be enabled

clientCleanupPrompt

forceCleanup

clientOptions
List of configured buttons(and/or menu options in the docked client) in the Windows VPN client.

clientConfiguration
List of configured tabs in the Windows VPN client.

SSO
Whether or not Single Sign-On is used for this session.

ssoCredential
The set of user credentials (primary or secondary) to use for Single Sign-On

windowsAutoLogon
Whether or not Windows Auto Logon is enabled for this session.

useMIP
Whether or not a Mapped IP address is used for the session

useIIP
Controls how the intranet IP module is configured for usage. \ Options:\ SPILLOVER\ specifies that iip is ON and when we can't assign an intranet IP to an entity, which has other instances active, we spill over to using Mapped IP.\ NOSPILLOVER\ specifies that iip is ON and when we can't assign intranet IP to an entity, which has other instances active, then we initiate transfer login.\ OFFnspecifies that intranet IP module won't be activated for this entity.

clientDebug
Trace level on the Windows VPN Client.

loginScript
Login script path.

logoutScript
Logout script path.

homePage
The client home page.

icaProxy
Enable ICA proxy mode. This can be used to enable Secure Gateway functionality for the Web Interface. If enabled, a VPN homepage that points to a Web Interface in SG mode, has to be configured.

wihome
Sets the home page of wi interface. Used only in conjunction with icaProxy ON. If clientChoices is ON, wiHome has to be configured. Since the end user is given a choice between FullClient and ICAProxy the homepage/landing page for each of these options could be different i.e. for FullClient it could be a Intranet web site and for the ICAProxy choice it will be a Web Interface web site. Hence we don't presume wihome == homepage.

citrixReceiverHome
Sets the home page of apprecvr interface.

wiPortalMode
WI layout on the VPN portal.

ClientChoices
Enables user to select different clients by displaying a set of options in a html page. The different client can be a) agent b) plugin c) wimode.

epaClientType
Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer.NOTE: This attribute is deprecated.This argument is not supported

iipDnsSuffix
The IntranetIP DNS suffix.

forcedTimeout

forcedTimeoutWarning

ntDomain

clientlessVpnMode
Whether clientlessVPN is available to the session.

clientlessModeUrlEncoding
URL encoding used in clientless mode.

clientlessPersistentCookie
Controls the use of persistent cookie in clientless mode. ALLOW lets cookie to be stored on disk. DENY prevents usage of persistent cookie. PROMPT lets VPN user choose whether persistent cookie should be used or not.

emailHome
The EMail home for the portal

Related Commands

add vpn sessionAction
rm vpn sessionAction
set vpn sessionAction
unset vpn sessionAction

set vpn parameter

Synopsis

```
set vpn parameter [-httpPort <port> ...] [-winsIP
<ip_addr>] [-dnsVserverName <string>] [-splitDns
<splitDns>] [-sessTimeout <mins>] [-clientSecurity
<expression>  [-clientSecurityGroup <string>]  [-
clientSecurityMessage <string>]] [-clientSecurityLog (
ON | OFF )] [-splitTunnel <splitTunnel>] [-
localLanAccess ( ON | OFF )] [-rfc1918 ( ON | OFF )] [-
spoofIIP ( ON | OFF )] [-killConnections ( ON | OFF )]
[-transparentInterception ( ON | OFF )] [-
windowsClientType ( AGENT | PLUGIN )] [-
defaultAuthorizationAction ( ALLOW | DENY )] [-
authorizationGroup <string>] [-clientIdleTimeout
<mins>] [-proxy <proxy>] [-allProtocolProxy <string> |
-httpProxy <string> | -ftpProxy <string> | -socksProxy
<string> | -gopherProxy <string> | -sslProxy <string>]
[-proxyException <string>] [-proxyLocalBypass ( ENABLED
| DISABLED )] [-clientCleanupPrompt ( ON | OFF )] [-
forceCleanup <forceCleanup> ...] [-clientOptions
<clientOptions> ...] [-clientConfiguration
<clientConfiguration> ...] [-SSO ( ON | OFF )] [-
ssoCredential ( PRIMARY | SECONDARY )] [-
windowsAutoLogon ( ON | OFF )] [-useMIP ( NS | OFF )]
[-useIIP <useIIP>] [-clientDebug <clientDebug>] [-
loginScript <input_filename>] [-logoutScript
<input_filename>] [-homePage <URL>] [-icaProxy ( ON |
OFF )] [-wihome <URL>] [-citrixReceiverHome <URL>] [-
wiPortalMode ( NORMAL | COMPACT )] [-ClientChoices ( ON
| OFF )] [-iipDnsSuffix <string>] [-forcedTimeout
<mins>] [-forcedTimeoutWarning <mins>] [-ntDomain
```

<string>] [-clientlessVpnMode <clientlessVpnMode>] [-clientlessModeUrlEncoding <clientlessModeUrlEncoding>] [-clientlessPersistentCookie <clientlessPersistentCookie>] [-emailHome <URL>]

Description

Set global parameters for the SSL VPN feature.

Arguments

httpPort
The SSL VPN HTTP port. Minimum value: 1

winsIP
The WINS server IP address to be used for WINS host resolution by the VPN.

dnsVserverName
The configured DNS vserver to be used for DNS host resolution by the VPN.

splitDns
Set the VPN client to route the DNS requests to remote network or local network or both. Possible values: LOCAL, REMOTE, BOTH

sessTimeout
The session idle timeout value in minutes. This idle timeout meters the overall network inactivity for a session. Default value: 30 Minimum value: 1

clientSecurity
The client security check string to be applied to client sessions. This is in the form of an Expression. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

clientSecurityLog
Controls client side logging of security checks. Possible values: ON, OFF Default value: VPN_SESS_ACT_ON

splitTunnel
The split tunnel state, e.g. ON, OFF or REVERSE. Split Tunnelling ON enables the VPN client to route non-VPN traffic through its local network interface. When Split Tunnelling is OFF, no traffic may go to the local interface while the client session is active. Split tunneling can also be set to

REVERSE. In this case all traffic directed to domains configured on the system will bypass the VPN tunnel. All other traffic is forced through the VPN tunnel. Possible values: ON, OFF, REVERSE Default value: VPN_SESS_ACT_OFF

localLanAccess

Finer grained local lan access. ON or OFF. splitTunnel, when OFF, permits no traffic to be routed to the client's local interface. But if, in addition, localLanAccess is turned ON, the client MAY route traffic to its local interface. This combination of switches is useful primarily when the rfc1918 switch is also specified. In this fashion, the client may restrict local lan access to devices which commonly have non-routable addresses, such as local printers or local file servers. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

rfc1918

Only allow RFC1918 local addresses when local LAN access feature is enabled Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

spoofIIP

The Spoof IP Address. Controls the Spoofing of Intranet IP to the Windows Applications by Windows VPN client when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF Default value: ON

killConnections

The state of kill connections. Determines whether Windows VPN client should kill all pre-existing connections (ie, the connections existing before the end user logged in to SSL VPN) and prevent new incoming connections on the Windows Client system when the end-user is connected to SSL VPN in '-splittunnel OFF' mode. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

transparentInterception

The transparent interception state, e.g. ON or OFF. Possible values: ON, OFF Default value: VPN_SESS_ACT_ON

windowsClientType

The Windows client type. Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed\ b) Activex Control - ActiveX control run by Microsoft's Internet

Explorer. Possible values: AGENT, PLUGIN Default value: VPN_SESS_ACT_CLT_AGENT

defaultAuthorizationAction
The authorization action state. Toggles the default authorization action to either ALLOW or DENY. Possible values: ALLOW, DENY

authorizationGroup
The authorization group to be applied to client sessions.

clientIdleTimeout
The client idle time out interval, which meters the client session's mouse and keyboard inactivity. The value is specified in minutes. Minimum value: 1 Maximum value: 9999

proxy
The usage of proxy configuration. Possible values: BROWSER, NS, OFF

allProtocolProxy
The address to be used for all proxies.

httpProxy
The HTTP proxy IP address.

ftpProxy
The FTP proxy IP address.

socksProxy
The SOCKS proxy IP address.

gopherProxy
The Gopher proxy IP address.

sslProxy
The HTTPS proxy IP address.

proxyException
The Proxy Exception string that will be configured in the Browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass

Bypass proxy server for local addresses option in IE proxy server settings will be enabled Possible values: ENABLED, DISABLED Default value: VPN_SESS_ACT_DISABLED

clientCleanupPrompt

The state for prompting for client clean up on session close. Possible values: ON, OFF Default value: VPN_SESS_ACT_ON

forceCleanup

The client side items for force cleanup on session close. You may specify all or none alone or any combination of the client side items.

clientOptions

Configured buttons(and/or menu options in the docked client) in the Windows VPN client.\ Possible options \ none \ none of the Windows Client's buttons/ menu options (except logout) are displayed. \ all \ all of the Windows Client's buttons/menu options are displayed. \ \ One or more of the following \ services \ only the "Services" button/menu option is displayed. \ filetransfer \ only the "File Transfer" button/menu option is displayed. \ configuration \ only the "Configuration" button/menu option is displayed.

clientConfiguration

Configured tabs in the Windows VPN client. \ Options: \ none \ none of the Windows Client's tabs(except About) are displayed. \ all \ all of the Windows Client's tabs (except "Resptime") are displayed. \ \ One or more of the following \ general \ only the "General" tab is displayed. \ tunnel \ only the "Tunnel" tab is displayed. \ trace \ only the "Trace" tab is displayed. \ compression \ only the "Compression" tab is displayed. \ resptime \ only the "Resptime" tab is displayed.

SSO

Whether or not Single Sign-On is used Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

ssoCredential

The set of user credentials (primary or secondary) to use for Single Sign-On Possible values: PRIMARY, SECONDARY Default value: VPN_SESS_ACT_USE_PRIMARY_CREDENTIALS

windowsAutoLogon
Whether or not Windows Auto Logon is enabled Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

useMIP
Whether or not a Mapped IP address is used Possible values: NS, OFF Default value: VPN_SESS_ACT_NS

useIIP
Controls how the intranet IP module is configured for usage. \ Options:\ SPILLOVER\ specifies that iip is ON and when we can't assign an intranet IP to an entity, which has other instances active, we spill over to using Mapped IP.\ NOSPILLOVER\ specifies that iip is ON and when we can't assign intranet IP to an entity, which has other instances active, then we initiate transfer login.\ OFFnspecifies that intranet IP module won't be activated for this entity. Possible values: NOSPILLOVER, SPILLOVER, OFF Default value: VPN_SESS_ACT_NOSPILLOVER

clientDebug
The trace level on the Windows VPN Client.\ Options:\ debugn\ Detailed debug messages are collected are written into the specified file.\ stats\ Application audit level error messages and debug statistic counters are written into the specified file.\ events\ Application audit level error messages are written into the specified file.\ off\ Only critical events are logged into the Windows Application Log. Possible values: debug, stats, events, OFF Default value: VPN_SESS_ACT_OFF

loginScript
Login script path.

logoutScript
Logout script path.

homePage
The client home page. Setting this parameter overrides the serving of the default portal page with the URL specified here.

icaProxy
Enable ICA proxy mode. This can be used to enable Secure Gateway functionality for the Web Interface. If enabled, a VPN homepage that points to a Web Interface in SG mode, has to be configured. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

wihome
Sets the home page of wi interface. Used only in conjunction with icaProxy ON. If clientChoices is ON, wiHome has to be configured. Since the end user is given a choice between FullClient and ICAProxy the homepage/landing page for each of these options could be different i.e. for FullClient it could be a Intranet web site and for the ICAProxy choice it will be a Web Interface web site. Hence we don't presume wihome == homepage.

citrixReceiverHome
Sets the home page of apprecvr interface.

wiPortalMode
WI layout on the VPN portal. Possible values: NORMAL, COMPACT

ClientChoices
Enables user to select different clients by displaying a set of options in a html page. The different client can be a) agent b) plugin c) wimode. Possible values: ON, OFF Default value: VPN_SESS_ACT_ON

epaClientType
Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

iipDnsSuffix
The IntranetIP DNS suffix. When a user logs into SSL-VPN, an A record is added to the DNS cache, after appending the configured IntranetIP DNS suffix to the username.

forcedTimeout
Maximum number of minutes a session is allowed to persist. Minimum value: 1 Maximum value: 255

forcedTimeoutWarning
Number of minutes to warn a user before their session is removed by a forced time out. Minimum value: 1 Maximum value: 255

ntDomain
NT domain to use with Smart Access when User Principle Name is not extracted from Active Directory Maximum value: 32

clientlessVpnMode

Whether clientlessVPN is available to the session. ON will make the session clientless and no client will be downloaded OFF will download the client but the clientlessVPN will also be available DISABLED will disable clientlessVPN altogether. Possible values: ON, OFF, DISABLED Default value: VPN_SESS_ACT_CVPNMODE_OFF

clientlessModeUrlEncoding

URL encoding to be used in clientless mode. No encoding will be done for TRANSPARENT. Protocol and domain will be encoded or encrypted with OPAQUE or ENCRYPT respectively. Possible values: TRANSPARENT, OPAQUE, ENCRYPT Default value: VPN_SESS_ACT_CVPN_ENC_OPAQUE

clientlessPersistentCookie

Controls the use of persistent cookie in clientless mode. ALLOW lets cookie to be stored on disk. DENY prevents usage of persistent cookie. PROMPT lets VPN user choose whether persistent cookie should be used or not. Possible values: ALLOW, DENY, PROMPT Default value: VPN_SESS_ACT_CVPN_PERSCOOKIE_DENY

emailHome

Sets the EMail home for the portal

Example

set vpn parameter -httpport 80 90 -winsIP 192.168.0.220 -dnsVserverName mydns -sessTimeout 240

Related Commands

unset vpn parameter

show vpn parameter

unset vpn parameter

Synopsis

```
unset vpn parameter [-httpPort] [-winsIP] [-
dnsVserverName] [-splitDns] [-sessTimeout] [-
clientSecurity] [-clientSecurityGroup] [-
clientSecurityMessage] [-clientSecurityLog] [-
authorizationGroup] [-clientIdleTimeout] [-
allProtocolProxy | -httpProxy | -ftpProxy | -socksProxy
| -gopherProxy | -sslProxy] [-proxyException] [-
forceCleanup] [-clientOptions] [-clientConfiguration]
[-loginScript] [-logoutScript] [-homePage] [-proxy] [-
wihome] [-citrixReceiverHome] [-wiPortalMode] [-
iipDnsSuffix] [-forcedTimeout] [-forcedTimeoutWarning]
[-defaultAuthorizationAction] [-ntDomain] [-
clientlessVpnMode] [-emailHome] [-
clientlessModeUrlEncoding] [-
clientlessPersistentCookie] [-splitTunnel] [-
localLanAccess] [-rfc1918] [-spoofIIP] [-
killConnections] [-transparentInterception] [-
windowsClientType] [-proxyLocalBypass] [-
clientCleanupPrompt] [-SSO] [-ssoCredential] [-
windowsAutoLogon] [-useMIP] [-useIIP] [-clientDebug] [-
icaProxy] [-ClientChoices]
```

Description

Unset parameters for the SSL VPN feature..Refer to the set vpn parameter command for meanings of the arguments.

Related Commands

set vpn parameter

show vpn parameter

show vpn parameter

Synopsis

```
show vpn parameter
```

Description

Display the configured vpn parameters.

Arguments

format

level

Output

name
The VPN name.

httpPort
The HTTP Port.

winsIP
The WINS server IP address used for WINS host resolution by the VPN.

dnsVserverName
The configured DNS vserver used for DNS host resolution by the VPN.

splitDns
The VPN client SplitDns state.

sessTimeout
The session timeout, in minutes.

clientSecurity
The client security check applied to client sessions. This is in the form of an Expression. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

clientSecurityGroup
The client security group that will be assigned on failure of the client security check. Users can in general be organized into Groups. In this case, the Client Security Group may have a more restrictive security policy.

clientSecurityMessage
The client security message that will be displayed on failure of the client security check.

clientSecurityLog
Controls client side logging of security checks.

splitTunnel
The split tunnel state, e.g. ON, OFF or REVERSE. Split Tunnelling ON enables the VPN client to route non-VPN traffic through its local network interface. When Split Tunnelling is OFF, no traffic may go to the local interface while the client session is active. Split tunneling can also be set to REVERSE. In this case all traffic directed to domains configured on the system will bypass the VPN tunnel. All other traffic is forced through the VPN tunnel.

localLanAccess
Finer grained local lan access. ON or OFF. splitTunnel, when OFF, permits no traffic to be routed to the client's local interface. But if, in addition, localLanAccess is turned ON, the client MAY route traffic to its local interface. This combination of switches is useful primarily when the rfc1918 switch is also specified. In this fashion, the client may restrict local lan access to devices which commonly have non-routable addresses, such as local printers or local file servers.

rfc1918
Only allow RFC1918 local addresses when local LAN access feature is enabled.

spoofIIP
Controls the Spoofing of Intranet IP to the Windows Applications by Windows VPN client when the end-user is connected to SSL VPN in '-splittunnel OFF' mode.

killConnections
Determines whether Windows VPN client should kill all pre-existing connections (ie, the connections existing before the end user logged in to SSL

VPN) and prevent new incoming connections on the Windows Client system when the end-user is connected to SSL VPN in '-splittunnel OFF' mode.

transparentInterception
The transparent interception state, e.g. ON or OFF.

windowsClientType
The windows client type.

defaultAuthorizationAction
The Authentication Action, e.g. allow or deny.

authorizationGroup
The authorization group applied to the session.

clientIdleTimeout
The client idle timeout, in minutes.

clientIdleTimeoutWarning
The time after which the client gets a timeout warning, in minutes.

proxy
Proxy configuration for the session.

allProtocolProxy
Address set for all proxies.

httpProxy
The HTTP proxy IP address.

ftpProxy
The FTP proxy IP address.

socksProxy
The SOCKS proxy IP address.

gopherProxy
The Gopher proxy IP address.

sslProxy
The HTTPS proxy IP address.

proxyException
The Proxy Exception string that is configured in the Browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass
Bypass proxy server for local addresses option in IE proxy server settings will be enabled

clientCleanupPrompt
The state for prompting for client clean up on session close.

forceCleanup
Whether or not to force a cleanup on exit from the VPN session.

clientOptions
List of configured buttons(and/or menu options in the docked client) in the Windows VPN client.

clientConfiguration
List of configured tabs in the Windows VPN client.

SSO
Enable or Disable Single Sign-On.

ssoCredential
The set of user credentials (primary or secondary) to use for Single Sign-On

windowsAutoLogon
Enable or Disable Windows Auto Logon.

useMIP
Enables or disables the use of a Mapped IP address for the session.

useIIP
Controls how the intranet IP module is configured for usage. \ Options:\ SPILLOVER\ specifies that iip is ON and when we can't assign an intranet IP to an entity, which has other instances active, we spill over to using Mapped IP.\ NOSPILLOVER\ specifies that iip is ON and when we can't assign intranet IP to an entity, which has other instances active, then we initiate transfer login.\ OFFnspecifies that intranet IP module won't be activated for this entity.

clientDebug
Whether or not to add debugging information to the activity log on the client.

loginScript
Login script path.

logoutScript
Logout script path.

homePage
The home page URL, or 'none'. 'none' is case sensitive.

icaProxy
Enable ICA proxy mode. This can be used to enable Secure Gateway functionality for the Web Interface. If enabled, a VPN homepage that points to a Web Interface in SG mode, has to be configured.

wihome
Sets the home page of wi interface. Used only in conjunction with icaProxy ON. If clientChoices is ON, wiHome has to be configured. Since the end user is given a choice between FullClient and ICAProxy the homepage/landing page for each of these options could be different i.e. for FullClient it could be a Intranet web site and for the ICAProxy choice it will be a Web Interface web site. Hence we don't presume wihome == homepage.

citrixReceiverHome
Sets the home page of apprecvr interface.

wiPortalMode
WI layout on the VPN portal.

ClientChoices
Enables user to select different clients by displaying a set of options in a html page. The different client can be a) agent b) plugin c) wimode.

epaClientType
Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer.NOTE: This attribute is deprecated.This argument is not supported

iipDnsSuffix
The DNS suffix for the intranet IP address.

forcedTimeout
The time, in minutes after which a timeout is forced.

forcedTimeoutWarning
The time, in minutes, after which a timeout warning is issued.

ntDomain

clientlessVpnMode
Whether clientlessVPN is available to the session.

clientlessModeUrlEncoding
URL encoding to be used for clientless mode.

clientlessPersistentCookie
Controls the use of persistent cookie in clientless mode. ALLOW lets cookie to be stored on disk. DENY prevents usage of persistent cookie. PROMPT lets VPN user choose whether persistent cookie should be used or not.

emailHome
Sets the EMail home for the portal

Related Commands

set vpn parameter

unset vpn parameter

add vpn clientlessAccessPolicy

Synopsis

```
add vpn clientlessAccessPolicy <name> <rule>
<profileName>
```

Description

Add a clientless access policy.

Arguments

`name`

The name for the new clientless access policy.

`rule`

The rule to be used by the clientless access policy.

`profileName`

The profile to be invoked for clientless access.

Related Commands

rm vpn clientlessAccessPolicy

set vpn clientlessAccessPolicy

show vpn clientlessAccessPolicy

rm vpn clientlessAccessPolicy

Synopsis

```
rm vpn clientlessAccessPolicy <name>
```

Description

Remove a clientless access policy.

Arguments

name

The name of the clientless access policy to be removed.

Related Commands

add vpn clientlessAccessPolicy

set vpn clientlessAccessPolicy

show vpn clientlessAccessPolicy

set vpn clientlessAccessPolicy

Synopsis

```
set vpn clientlessAccessPolicy <name> [-rule
<expression>] [-profileName <string>]
```

Description

Set a new rule/profile for existing clientless access policy.

Arguments

name

The name of the existing clientless access policy.

rule

The rule to be used by the clientless access policy.

profileName

The profile to be invoked for clientless access.

Related Commands

add vpn clientlessAccessPolicy

rm vpn clientlessAccessPolicy

show vpn clientlessAccessPolicy

show vpn clientlessAccessPolicy

Synopsis

```
show vpn clientlessAccessPolicy [<name>]
```

Description

Display clientless access policies.

Arguments

`name`
The name of the clientless access policy.

`summary`

`fullValues`

`format`

`level`

Output

`rule`
The rule used by the clientless access policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide

`profileName`
The profile to invoked for the clientless access.

`undefAction`
The UNDEF action.

`hits`
The number of times the policy evaluated to true.

`undefHits`
The number of times the policy evaluation resulted in undefined processing.

activePolicy
Indicates whether policy is bound or not.

boundTo
Location where policy is bound.

priority
Specifies the priority of the policy.

description
Description of the clientless access policy.

Related Commands

add vpn clientlessAccessPolicy
rm vpn clientlessAccessPolicy
set vpn clientlessAccessPolicy

stat vpn vserver

Synopsis

```
stat vpn vserver [<name>] [-detail] [-fullValues] [-
ntimes <positive_integer>] [-logFile <input_filename>]
```

Description

Display vpn vserver statistics.

Arguments

name

The name of the vserver for which statistics will be displayed. If not given statistics are shown for all vpn vservers.

Output

Counters

IP address (IP)

The ip address at which the service is running.

Port (port)

The port at which the service is running.

Vserver protocol (Protocol)

Protocol associated with the vserver

State

Current state of the server.

Requests (Req)

The total number of requests received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Responses (Rsp)

Number of responses received on this service/vserver(This is applicable for HTTP/SSL servicetype).

Request bytes (Reqb)
The total number of request bytes received on this service/vserver.

Response bytes (Rspb)
Number of response bytes received on this service/vserver.

Related Commands

add vpn vserver
rm vpn vserver
set vpn vserver
unset vpn vserver
enable vpn vserver
disable vpn vserver
show vpn vserver

stat vpn

add vpn clientlessAccessProfile

Synopsis

```
add vpn clientlessAccessProfile <profileName>
```

Description

Add a clientless access profile.

Arguments

`profileName`

The name of the clientless access profile.

Related Commands

rm vpn clientlessAccessProfile

set vpn clientlessAccessProfile

unset vpn clientlessAccessProfile

show vpn clientlessAccessProfile

rm vpn clientlessAccessProfile

Synopsis

```
rm vpn clientlessAccessProfile <profileName>
```

Description

Remove a clientless access profile.

Arguments

profileName

The name of the clientless access profile.

Related Commands

add vpn clientlessAccessProfile

set vpn clientlessAccessProfile

unset vpn clientlessAccessProfile

show vpn clientlessAccessProfile

set vpn clientlessAccessProfile

Synopsis

```
set vpn clientlessAccessProfile <profileName> [-
URLRewritePolicyLabel <string>] [-
JavaScriptRewritePolicyLabel <string>] [-
ReqHdrRewritePolicyLabel <string>] [-
ResHdrRewritePolicyLabel <string>] [-
RegexForFindingURLinJavaScript <string>] [-
RegexForFindingURLinCSS <string>] [-
RegexForFindingURLinXComponent <string>] [-
RegexForFindingURLinXML <string>] [-
ClientConsumedCookies <string>] [-
requirePersistentCookie ( ON | OFF )]
```

Description

Set a policylabel on the clientless access profile.

Arguments

profileName
The name of the clientless vpn profile.

URLRewritePolicyLabel
The configured URL rewrite policylabel.

JavaScriptRewritePolicyLabel
The configured JavaScript rewrite policylabel.

ReqHdrRewritePolicyLabel
The configured Request Header rewrite policylabel.

ResHdrRewritePolicyLabel
The configured Response rewrite policylabel.

RegexForFindingURLinJavaScript
Patclass having regexes to find the URLs in JavaScript.

RegexForFindingURLinCSS
Patclass having regexes to find the URLs in CSS.

RegexForFindingURLinXComponent
Patclass having regexes to find the URLs in X-Component.

RegexForFindingURLinXML
Patclass having regexes to find the URLs in XML.

ClientConsumedCookies
Patclass having the client consumed Cookie names.

requirePersistentCookie
The flag to select Persistent cookie for the profile Possible values: ON, OFF Default value: OFF

Related Commands

add vpn clientlessAccessProfile
rm vpn clientlessAccessProfile
unset vpn clientlessAccessProfile
show vpn clientlessAccessProfile

unset vpn clientlessAccessProfile

Synopsis

```
unset vpn clientlessAccessProfile <profileName> [-
URLRewritePolicyLabel] [-JavaScriptRewritePolicyLabel]
[-ReqHdrRewritePolicyLabel] [-
ResHdrRewritePolicyLabel] [-
RegexForFindingURLinJavaScript] [-
RegexForFindingURLinCSS] [-
RegexForFindingURLinXComponent] [-
RegexForFindingURLinXML] [-ClientConsumedCookies] [-
requirePersistentCookie]
```

Description

Unset a policylabel on a clientless access profile..Refer to the set vpn clientlessAccessProfile command for meanings of the arguments.

Related Commands

add vpn clientlessAccessProfile

rm vpn clientlessAccessProfile

set vpn clientlessAccessProfile

show vpn clientlessAccessProfile

show vpn clientlessAccessProfile

Synopsis

```
show vpn clientlessAccessProfile [<profileName>]
```

Description

Show clientless access profile.

Arguments

profileName
The name of the clientless vpn profile.

summary

fullValues

format

level

Output

state

URLRewritePolicyLabel
The configured URL rewrite policylabel.

JavaScriptRewritePolicyLabel
The configured JavaScript rewrite policylabel.

CSSRewritePolicyLabel
The configured CSS rewrite policylabel.

XMLRewritePolicyLabel
The configured XML rewrite policylabel.

XComponentRewritePolicyLabel
The configured X-Component rewrite policylabel.

ReqHdrRewritePolicyLabel
The configured Request Header rewrite policylabel.

ResHdrRewritePolicyLabel
The configured Response rewrite policylabel.

RegexForFindingURLinJavaScript
Patclass having regexes to find the URLs in JavaScript.

RegexForFindingURLinCSS
Patclass having regexes to find the URLs in CSS.

RegexForFindingURLinXComponent
Patclass having regexes to find the URLs in X-Component.

RegexForFindingURLinXML
Patclass having regexes to find the URLs in XML.

ClientConsumedCookies
Patclass having the client consumed Cookie names.

requirePersistentCookie
The flag to select Persistent cookie for the profile

description
Description of the clientless access profile.

Related Commands

add vpn clientlessAccessProfile
rm vpn clientlessAccessProfile
set vpn clientlessAccessProfile
unset vpn clientlessAccessProfile