Netsh commands for remote access (ras)

Updated: January 21, 2005

Netsh commands for remote access (ras)

You can administer remote access servers by typing commands at the command prompt for the **Netsh ras** context. By using the **Netsh ras** command prompt, you can administer servers more quickly over slow network connections, and you can create scripts that automate the administration of many servers.

For more information on Netsh, see Netsh overview [http://technet.microsoft.com/en-us/library/61427fbd-de1f-4c8a-b613-321f7a3cca6a] and Enter a netsh context [http://technet.microsoft.com/en-us/library/d9b4eed7-f79b-4daf-8c22-ffd9428ddea5] .

To view the command syntax, click a command:

- help
- show activeservers
- show client
- dump
- show tracing
- set tracing
- show authmode
- set authmode
- add authtype
- delete authtype
- show authtype
- add link
- delete link
- show link
- add multilink
- delete multilink
- show multilink
- add registeredserver
- delete registeredserver
- show registeredserver
- show user
- set user
- Netsh ras diagnostics context commands
- Netsh ras IP context commands
- Netsh ras AppleTalk context commands
- Netsh ras AAAA context commands

help

Displays command-line help for commands you can use in the Netsh ras context.

Syntax

help

Parameters

Remarks

- You can also display command-line help by typing any of the following at the command prompt for the Netsh ras context: **?**, **/?**, or **-?**.

show_activeservers

Displays a list of remote access server advertisements.

Syntax

show activeservers

Parameters

show_client

Lists remote access clients connected to this server.

Syntax

show client

Parameters

dump

Displays the configuration of the remote access server in script form.

Syntax

dump

Parameters

show_tracing

Shows whether tracing is enabled for the specified component. Used without parameters, **show tracing** lists all installed components and whether tracing is enabled for each.

Syntax

show tracing [*Component*]

Parameters
Component
      Specifies the component for which to display information.

set_tracing

Enables or disables tracing for the specified component.

Syntax

set tracing *Component* {**enabled** | **disabled**}

Parameters
Component
      Required. Specifies the component for which you want to enable or disable tracing. Use * to specify all components.

{ enabled| disabled}
      Required. Specifies whether to enable or disable tracing for the specified component.

Remarks

- To see a list of all installed components, use the **show tracing** command without parameters.

Examples

To set tracing for the PPP component, type:

set tracing ppp enabled

show_authmode

Shows whether dial-up clients using certain types of devices should be authenticated.

Syntax

show authmode

Parameters

set_authmode

Specifies whether dial-up clients using certain types of devices should be authenticated.

Syntax

set authmode {**standard** | **nodcc** | **bypass**}

Parameters

{ standard| nodcc| bypass}
> Required. Specifies whether dial-up clients using certain types of devices should be authenticated. The parameter **standard** specifies that clients using any type of device should be authenticated. The parameter **nodcc** specifies that clients using any type of device except a direct-connect device should be authenticated. The parameter **bypass** specifies that no clients should be authenticated.

add_authtype

Adds an authentication type to the list of types through which the remote access server should attempt to negotiate authentication.

Syntax

add authtype {**pap** | **spap** | **md5chap** | **mschap** | **mschapv2** | **eap**}

Parameters

{ pap| spap| md5chap| mschap| mschapv2| eap}
> Required. Specifies which authentication type to add to the list of types through which the remote access server should attempt to negotiate authentication. The **pap** parameter specifies that the remote access server should use the Password Authentication Protocol (plaintext). The **spap** parameter specifies that the remote access server should use the Shiva Password Authentication Protocol. The **md5chap** parameter specifies that the remote access server should use the Challenge Handshake Authentication Protocol (using the Message Digest 5 hashing scheme to encrypt the response). The **mschap** parameter specifies that the remote access server should use the Microsoft Challenge-Handshake Authentication Protocol. The **mschapv2** parameter specifies that the remote access server should use Version 2 of MSCHAP. The **eap** parameter specifies that the remote access server should use Extensible Authentication Protocol.

Remarks

- The remote access server will attempt to negotiate authentication by using protocols in order from the most secure to the least secure. After both the client and the server have agreed on an authentication type, PPP negotiation proceeds according to the appropriate RFCs.

delete_authtype

Deletes an authentication type from the list of types through which the remote access server should attempt to negotiate authentication.

Syntax

delete authtype{**pap** | **spap** | **md5chap** | **mschap** | **mschapv2** | **eap**}

Parameters

{ pap| spap| md5chap| mschap| mschapv2| eap}
> Required. Specifies which authentication type to delete from the list of types through which the remote access server should attempt to negotiate authentication. The **pap** parameter specifies that the remote access server should not use the Password Authentication Protocol (plaintext). The **spap** parameter specifies that the remote access server should not use the Shiva Password Authentication Protocol. The **md5chap** parameter specifies that the remote access server should not use the Challenge Handshake Authentication Protocol (using the Message Digest 5 hashing scheme to encrypt the response). The **mschap** parameter specifies that the remote access server should not use the Microsoft Challenge-Handshake Authentication Protocol. The **mschapv2** parameter specifies that the remote access server should not use Version 2 of MSCHAP. The **eap** parameter specifies that the remote access server should not use Extensible Authentication Protocol.

show_authtype

Lists the authentication type (or types) that the remote access server uses to attempt to negotiate authentication.

Syntax

show authtype

Parameters

add_link

Adds a link property to the list of link properties PPP should negotiate.

Syntax

add link {**swc** | **lcp**}

Parameters
{ swc| lcp}
      Required. Specifies which link property to add to the list of link properties PPP should negotiate. The parameter **swc** specifies that software compression (MPPC) should be added. The parameter **lcp** specifies that Link Control Protocol extensions from the PPP suite of protocols should be added.

delete_link

Deletes a link property from the list of link properties PPP should negotiate.

Syntax

delete link {**swc** | **lcp**}

Parameters
{ swc| lcp}
      Required. Specifies which link property to delete from the list of link properties PPP should negotiate. The parameter **swc** specifies that software compression (MPPC) should be deleted. The parameter **lcp** specifies that Link Control Protocol extensions from the PPP suite of protocols should be deleted.

show link

Displays the link properties PPP should negotiate.

Syntax

show link

Parameters

add multilink

Adds a multilink type to the list of multilink types PPP should negotiate.

Syntax

add multilink {**multi** | **bacp**}

Parameters
{ multi| bacp}
      Required. Specifies which multilink type to add to the list of multilink types PPP should negotiate. The parameter **multi** specifies that multilink PPP sessions should be added. The parameter **bacp** specifies that Bandwidth Allocation Control Protocol should be added.

delete multilink

Deletes a multilink type from the list of multilink types PPP should negotiate.

Syntax

delete multilink {**multi** | **bacp**}

Parameters
{ multi| bacp}
      Required. Specifies which multilink type to delete from the list of multilink types PPP should negotiate. The

parameter **multi** specifies that multilink PPP sessions should be deleted. The parameter **bacp** specifies that Bandwidth Allocation Control Protocol should be deleted.

show multilink

Shows the multilink types PPP should negotiate.

Syntax

show multilink

Parameters

add registeredserver

Registers the specified server as a remote access server in the specified Active Directory domain. Used without parameters, **add registeredserver** registers the computer from which you type the command in its primary domain.

Syntax

add registeredserver [[**domain=**]*DomainName*] [[**server=**]*ServerName*]

Parameters
[domain=] *DomainName*
　　Specifies, by domain name, the domain in which to register the server. If you do not specify a domain, the server is registered in its primary domain.

[server=] *ServerName*
　　Specifies, by DNS name or IP address, the server to register. If you do not specify a server, the computer from which you type the command is registered.

delete registeredserver

Deletes the registration of the specified server as a remote access server from the specified Active Directory domain. Used without parameters, **delete registeredserver** deletes the registration of the computer from which you type the command from its primary domain.

Syntax

delete registeredserver [[**domain=**]*DomainName*] [[**server=**]*ServerName*]

Parameters
[domain=] *DomainName*
　　Specifies, by domain name, the domain from which to remove the registration. If you do not specify a domain, the registration is removed from the primary domain of the computer from which you type the command.

[server=] *ServerName*
　　Specifies, by IP address or DNS name, the server whose registration you want to remove. If you do not specify a server, the registration is removed for the computer from which you type the command.

show registeredserver

Displays status information about the specified server registered as a remote access server in the specified Active Directory domain. Used without parameters, **show registeredserver** displays information about the computer from which you type the command in its primary domain.

Syntax

show registeredserver [[**domain=**]*DomainName*] [[**server=**]*ServerName*]

Parameters
[domain=] *DomainName*
　　Specifies, by domain name, the domain in which the server about which you want to display information is registered. If you do not specify a domain, information is displayed about the server as it is registered in the primary domain of the computer from which you type the command.

[server=] *ServerName*
　　Specifies, by IP address or DNS name, the server about which you want to display information. If you do not specify a server, information about the computer from which you typed the command is displayed.

show user

Displays the properties of a specified remote access user or users. Used without parameters, **show user** displays the properties of all remote access users.

Syntax

show user [**name=***UserName*] [[**mode=**] {**permit** | **report**}]

Parameters

name= *UserName*

Specifies, by logon name, the user whose properties you want to display. If you do not specify a user, the properties of all users are displayed.

mode={ permit| report}

Specifies whether to show properties for all users or only those whose dial-up permission is set to permit. The **permit** parameter specifies that properties should be displayed only for users whose dial-up permission is permit. The **report** parameter specifies that properties should be displayed for all users.

setuser

Sets the properties of the specified remote access user.

Syntax

set user [**name=**]*UserName* [**dialin**] {**permit** | **deny** | **policy**} [**cbpolicy**] {**none** | **caller** | **admin** [**cbnumber=**] *CallbackNumber*}

Parameters

name= *UserName*

Required. Specifies, by logon name, the user for which you want to set properties.

[dialin] { permit| deny| policy}

Required. Specifies under what circumstances the user should be allowed to connect. The **permit** parameter specifies that the user should always be allowed to connect. The **deny** parameter specifies that the user should never be allowed to connect. The **policy** parameter specifies that remote access policies should determine whether the user is allowed to connect.

[cbpolicy] { none| caller| admin[cbnumber=] *CallbackNumber***}**

Required. Specifies the callback policy for the user. The callback feature saves the user the cost of the phone call used to connect to a remote access server. The **none** parameter specifies that the user should not be called back. The **caller** parameter specifies that the user should be called back at a number specified by the user at connection time. The **admin** parameter specifies that the user should be called back at the number specified by the *CallbackNumber* parameter.

Remarks

- For users in a mixed-mode domain, the **policy** parameter and the **deny** parameter are equivalent.

Examples

To allow GuestUser to connect and be called back at 4255550110, type:

set user guestuser permit admin 4255550110

Netsh ras diagnostics context commands

The following commands are specific to the **ras diagnostics** context within the Netsh environment.

To view the command syntax, click a command:

- dump
- show installation
- show logs
- show configuration
- show all
- show cmtracing
- set cmtracing
- show modemtracing
- set modemtracing
- show rastracing
- set rastracing
- show securityeventlog
- set securityeventlog
- show tracefacilities
- set tracefacilities

dump

Displays the configuration of Remote Access Diagnostics in script form.

Syntax

dump

Parameters

show installation

Creates a Remote Access Diagnostic Report that includes only diagnostics results for Information Files, Installation Check, Installed Networking Components, and Registry Check and delivers the report to a location you specify.

Syntax

show installation [**type**=] {**file** | **email**} [**destination**=] {*FileLocation* | *E-mailAddress*} [[**compression**=] {**enabled** | **disabled**}] [[**hours**=] *NumberOfHours*] [[**verbose**=] {**enabled** | **disabled**}]

Parameters

[type=] { file| email}
    Required. Specifies whether you want to save the report to a file or you want to send it to an e-mail address.

[destination=] { *FileLocation| E-mailAddress***}**
    Required. Specifies the full path and file name to which the report should be saved or the full e-mail address to which the report should be sent.

[[compression=] { enabled| disabled}]
    Specifies whether to compress the report into a .cab file. If you do not specify this parameter, the report is compressed if you send it to an e-mail address but not if you save it to a file.

[[hours=] *NumberOfHours***]**
    Specifies the number of past hours for which to show activity in the report. This parameter must be an integer between 1 and 24. If you do not specify this parameter, all past information is included.

[[verbose=] { enabled| disabled}]
    Specifies the amount of data to include in the report. If you do not specify this parameter, only minimal data is included.

Remarks

- The Remote Access Diagnostic Report is saved as an HTML file (.htm).

show logs

Creates a Remote Access Diagnostic Report that contains only diagnostics results for Tracing Logs, Modem Logs, Connection Manager Logs, IP Security Log, Remote Access Event Logs, and Security Event Logs and delivers the report to a location you specify.

Syntax

show logs [**type**=] {**file** | **email**} [**destination**=] {*FileLocation* | *E-mailAddress*} [[**compression**=] {**enabled** | **disabled**}] [[**hours**=] *NumberOfHours*] [[**verbose**=] {**enabled** | **disabled**}]

Parameters

[type=] { file| email}
    Required. Specifies whether you want to save the report to a file or you want to sent it to an e-mail address.

[destination=] { *FileLocation| E-mailAddress***}**
    Required. Specifies the full path and file name to which the report should be saved or the full e-mail address to which the report should be sent.

[[compression=] { enabled| disabled}]
    Specifies whether to compress the report into a .cab file. If you do not specify this parameter, the report is compressed if you send it to an e-mail address but not if you save it to a file.

[[hours=] *NumberOfHours***]**
    Specifies the number of past hours for which to show activity in the report. This parameter must be an integer between 1 and 24. If you do not specify this parameter, all past information will be included in the report.

[[verbose=] { enabled| disabled}]
    Specifies the amount of data to include in the report. If you do not specify this parameter, minimal data is included.

Remarks

- The Remote Access Diagnostic Report is saved as an HTML file (.htm).

show configuration

Creates a Remote Access Diagnostic Report that includes only diagnostics results for Installed Devices, Process Information, Command-Line Utilities, and Phone Book Files and delivers the report to a location you specify.

Syntax

show configuration [**type=**] {**file** | **email**} [**destination=**] {*FileLocation* | *E-mailAddress*} [[**compression=**] {**enabled** | **disabled**}] [[**hours=**] *NumberOfHours*] [[**verbose=**] {**enabled** | **disabled**}]

Parameters

[type=] { file| email}
      Required. Specifies whether the report should be saved to a file or sent to an e-mail address.

[destination=] { *FileLocation*| *E-mailAddress*}
      Required. Specifies the full path and file name to which the report should be saved or the full e-mail address to which the report should be sent.

[[compression=] { enabled| disabled}]
      Specifies whether to compress the report into a .cab file. If you do not specify this parameter, the report is compressed if you send it to an e-mail address but not if you save it to a file.

[[hours=] *NumberOfHours*]
      Specifies the number of past hours for which to show activity in the report. This parameter must be an integer between 1 and 24. If you do not specify this parameter, all past information is included.

[[verbose=] { enabled| disabled}]
      Specifies the amount of data to include in the report. If you do not specify this parameter, minimal data is included.

Remarks

- The Remote Access Diagnostic Report is saved as an HTML file (.htm).

show all

Creates a Remote Access Diagnostic Report for all remote access logs and delivers the report to a location you specify.

Syntax

show all [**type=**] {**file** | **email**} [**destination=**] {*FileLocation* | *E-mailAddress*} [[**compression=**] {**enabled** | **disabled**}] [[**hours=**] *NumberOfHours*] [[**verbose=**] {**enabled** | **disabled**}]

Parameters

[type=] { file| email}
      Required. Specifies whether you want to save the report to a file or sent it to an e-mail address.

[destination=] { *FileLocation*| *E-mailAddress*}
      Required. Specifies the full path and file name to which the report should be saved or the full e-mail address to which the report should be sent.

[[compression=] { enabled| disabled}]
      Specifies whether to compress the report into a .cab file. If you do not specify this parameter, the report is compressed if you send it to an e-mail address but not if you save it to a file.

[[hours=] *NumberOfHours*]
      Specifies the number of past hours for which to show activity in the report. This parameter must be an integer between 1 and 24. If you do not specify this parameter, all past information is included.

[[verbose=] { enabled| disabled}]
      Specifies the amount of data to include in the report. If you do not specify this parameter, minimal data is included.

Remarks

- The Remote Access Diagnostic Report is saved as an HTML file (.htm).
- The Remote Access Diagnostic Report that you create by using the **show all** command contains all diagnostic information available. You can use other commands, such as **show configuration**, to create reports that contain a narrower scope of information.

show cmtracing

Shows whether information about Connection Manager connections is being logged.

Syntax

show cmtracing

Parameters

set cmtracing

Enables or disables logging of information about all Connection Manager connections.

Syntax

set cmtracing {**enabled** | **disabled**}

Parameters

{ enabled| disabled}
  Required. Specifies whether you want information about Connection Manager connections to be logged. The **enabled** parameter specifies that you want information to be logged. The **disabled** parameter specifies that you do not want information to be logged.

Remarks

- Each log file for a Connection Manager connection contains information that is specific to the history of that connection. Each Connection Manager connection generates a unique log file. Depending on the configuration of the connection, the log file might be saved in any of various locations. For more information, see Connection Manager Administration Kit [http://technet.microsoft.com/en-us/library/be5c1c37-109e-49bc-943e-6595832d5761] and Troubleshooting process [http://technet.microsoft.com/en-us/library/fe348deb-f065-4eb1-a23f-44f076cfcbcd] .

- This command will be be overridden for a particular connection if the user enables or disables logging for that connection or if the user installs and uses a Connection Manager profile for which an administrator has enabled or disabled logging.

show modemtracing

Shows whether modem tracing is enabled or disabled.

Syntax

show modemtracing

Parameters

set modemtracing

Enables or disables modem tracing for all modems installed for the local computer.

Syntax

set modemtracing {**enabled** | **disabled**}

Parameters

{ enabled| disabled}
  Required. Specifies whether you want modem activity for each modem to be logged. The **enabled** parameter specifies that you want activity to be logged. The **disabled** parameter specifies that you do not want activity to be logged.

Remarks

- This command enables or disables the logging of modem activity for all modems. If you want to enable or disable modem logging for a specific modem, you should configure the modem in Device Manager.

show rastracing

Shows whether all activity for remote access components is traced.

Syntax

show rastracing

Parameters

set rastracing

Enables or disables tracing and logging of all activity for all remote access components or for a specific remote access component.

Syntax

set rastracing [**component=**] {*Component* | *} {**enabled** | **disabled**}

Parameters

[component=] { *Component* **| *}**
    Required. Specifies whether you want to enable or disable tracing and logging for a component that you specify or for all components. The *Component* parameter specifies the component for which you want to enable or disable tracing and logging.

{ enabled| disabled}
    Required. Specifies whether you want activity to be traced and logged. The **enabled** parameter specifies that you want activity to be traced and logged. The **disabled** parameter specifies that you do not want activity to be traced and logged.

Remarks

- If you enable tracing and logging, a log file named *Component*.txt is created in the %windir%\tracing directory for each component being traced.

show securityeventlog

Shows whether security events are being logged.

Syntax

show securityeventlog

Parameters

set securityeventlog

Enables or disables logging of all security events.

Syntax

set securityeventlog {**enabled** | **disabled**}

Parameters

{ enabled| disabled}
    Required. Specifies whether you want security events to be logged. The **enabled** parameter specifies that you want security events to be logged. The **disabled** parameter specifies that you do not want security events to be logged.

show tracefacilities

Shows whether all activity for all remote access components or for a remote access component that you specify is being traced and logged.

Syntax

show tracefacilities

Parameters

set tracefacilities

Enables or disables tracing and logging of all activity for all remote access components that are configured on the local computer.

Syntax

set tracefacilities [**state=**] {**enabled** | **disabled** | **clear**}

Parameters

[state=] { enabled| disabled| clear}
    Required. Specifies whether you want to enable tracing for all remote access components, to disable tracing, or

to clear all logs generated by tracefacilities. The **enabled** parameter specifies that you want to enable tracing. The **disabled** parameter specifies that you want to disable tracing. The **clear** parameter specifies that you want to clear all logs.

Netsh ras IP context commands

The following commands are specific to the **ras IP** context within the Netsh environment.

To view the command syntax, click a command:

- dump
- show config
- set negotiation
- set access
- set addassign
- set addrreq
- set broadcastnameresolution
- show broadcastnameresolution
- add range
- delete range
- delete pool

dump

Creates a script that contains the IP configuration of a remote access server. If you save this script to a file, you can use it to restore IP configuration settings.

Syntax

dump

Parameters

show config

Displays the current IP configuration of the remote access server.

Syntax

show config

Parameters

set negotiation

Specifies whether the remote access server should allow IP to be configured for any client connections the server accepts.

Syntax

set negotiation {**allow** | **deny**}

Parameters
{ allow| deny}
Required. Specifies whether to permit IP over client connections. The **allow** parameter allows IP over client connections. The **deny** parameter prevents IP over client connections.

set access

Specifies whether IP network traffic from any client should be forwarded to the network or networks to which the remote access server is connected.

Syntax

set access {**all** | **serveronly**}

Parameters

{ all| serveronly}
> Required. Specifies whether clients should be able to reach the remote access server and any networks to which it is connected. The **all** parameter allows clients to reach networks through the server. The **serveronly** parameter allows clients to reach only the server.

set addrassign

Sets the method by which the remote access server should assign IP addresses to its clients.

Syntax

set addrassign {**auto** | **pool**}

Parameters
{ auto| pool}
> Required. Specifies whether IP addresses should be assigned by using DHCP or from a pool of addresses held by the remote access server. The **auto** parameter specifies that addresses should be assigned by using DHCP. If no DHCP server is available, a random, private address is assigned. The **pool** parameter specifies that addresses should be assigned from a pool.

set addrreq

Specifies whether dial-up clients should be able to request their own IP addresses.

Syntax

set addrreq {**allow** | **deny**}

Parameters
{ allow| deny}
> Required. Specifies whether clients should be able to request their own IP addresses. The **allow** parameter allows clients to request addresses. The **deny** parameter prevents clients from requesting addresses.

set broadcastnameresolution

Enables or disables broadcast name resolution using NetBIOS over TCP/IP.

Syntax

set broadcastnameresolution {**enabled** | **disabled**}

Parameters
{ enabled| disabled}
> Required. Specifies whether to enable or disable broadcast name resolution using NetBIOS over TCP/IP.

show broadcastnameresolution

Displays whether broadcast name resolution using NetBIOS over TCP/IP has been enabled or disabled for the remote access server.

Syntax

show broadcastnameresolution

Parameters

add range

Adds a range of addresses to the pool of static IP addresses that the remote access server can assign to clients.

Syntax

add range [**from=**]*StartingIPAddress* [**to=**]*EndingIPAddress*

Parameters
[from=] *StartingIPAddress***[to=]** *EndingIPAddress*
> Required. Specifies the range of IP addresses to add. The *StartingIPAddress* parameter specifies the first IP address in the range. The *EndingIPAddress* parameter specifies the last IP address in the range.

Examples

To add the range of IP addresses 10.2.2.10 to 10.2.2.20 to the static pool of IP addresses that the remote access server can assign, type:

add range from=10.2.2.10 to=10.2.2.20

delete range

Deletes a range of addresses from the pool of static IP addresses that the remote access server can assign to clients.

Syntax

delete range [**from=**]*StartingIPAddress* [**to=**]*EndingIPAddress*

Parameters

[from=] *StartingIPAddress***[to=]** *EndingIPAddress*
> Required. Specifies the range of IP addresses to delete. The *StartingIPAddress* parameter specifies the first IP address in the range. The *EndingIPAddress* parameter specifies the last IP address in the range.

Examples

To delete the range of IP addresses 10.2.2.10 to 10.2.2.20 from the pool of static IP addresses that the remote access server can assign, type:

delete range from=10.2.2.10 to=10.2.2.20

delete pool

Deletes all addresses from the pool of static IP addresses that the remote access server can assign to clients.

Syntax

delete pool

Parameters

Netsh ras AppleTalk context commands

The following commands are specific to the **ras AppleTalk** context within the Netsh environment.

This feature is not available on the Itanium-based versions of the Windows operating systems. This content is not available in this preliminary release.

To view the command syntax, click a command:

- dump
- show config
- set negotiation

dump

Creates a script that contains the AppleTalk configuration of the remote access server. If you save this script to a file, you can use it to restore AppleTalk configuration settings.

Syntax

dump

Parameters

show config

Displays the current AppleTalk configuration of the remote access server.

Syntax

show config

Parameters

set negotiation

Specifies whether the remote access server should allow AppleTalk to be configured for any client connections the server accepts.

Syntax

set negotiation {**allow** | **deny**}

Parameters

{ allow| deny}

> Required. Specifies whether to allow AppleTalk configuration. The **allow** parameter allows configuration. The **deny** parameter prevents configuration.

Netsh ras AAAA context commands

The following commands are specific to the **ras AAAA** context within the Netsh environment.

To view the command syntax, click a command:

- dump
- add acctserv
- delete acctserv
- set acctserv
- show authserv
- add authserv
- delete authserv
- set authserv
- show authserv
- set acco
- show acco
- set authe
- show authe

dump

Displays the AAAA configuration of a remote access server in script form.

Syntax

dump

Parameters

add acctserv

Specifies the IP address or the DNS name of a RADIUS server to use for accounting and specifies accounting options.

Syntax

add acctserv [**name=**]*ServerID*[[**secret=**]*SharedSecret*] [[**init-score=**]*ServerPriority*] [[**port=**]*Port*] [[**timeout=**]*Seconds*] [[**messages**] {**enabled** | **disabled**}]

Parameters

[name=] *ServerID*

> Required. Specifies, by IP address or DNS name, the RADIUS server.

[secret=] *SharedSecret*

> Specifies the shared secret.

[init-score=] *ServerPriority*

> Specifies the initial score (server priority).

[port=] *Port*

> Specifies the port to which accounting requests should be sent.

[timeout=] *Seconds*

> Specifies the timeout period, in seconds, during which the RADIUS server can be idle before it should be marked unavailable.

[messages] { **enabled**| **disabled}**

> Specifies whether to send accounting on/off messages. The **enabled** parameter specifies that messages should be sent. The **disabled** parameter specifies that messages should not be sent.

delete acctserv

Deletes a RADIUS accounting server.

Syntax

delete acctserv [**name**=]*ServerID*

Parameters

[name=] *ServerID*
    Required. Specifies, by DNS name or IP address, which server to delete.

set acctserv

Provides the IP address or the DNS name of a RADIUS server to use for accounting.

Syntax

add acctserv [**name**=]*ServerID* [[**secret**=]*SharedSecret*] [[**init-score**=]*ServerPriority*] [[**port**=]*Port*] [[**timeout**=] *Seconds*] [[**messages**] {**enabled** | **disabled**}]

Parameters

[name=] *ServerID*
    Required. Specifies, by IP address or DNS name, the RADIUS server.

[secret=] *SharedSecret*
    Specifies the shared secret.

[init-score=] *ServerPriority*
    Specifies the initial score (server priority).

[port=] *Port*
    Specifies the port on which to send the authentication requests.

[timeout=] *Seconds*
    Specifies, in seconds, the amount of time that should elapse before the RADIUS server is marked unavailable.

[messages=] { enabled| disabled}
    Specifies whether accounting on/off messages should be sent.

show acctserv

Displays detailed information about an accounting server. Used without parameters, **show acctserv** displays information about all configured accounting servers.

Syntax

show acctserv [[**name**=]*ServerID*]

Parameters

[name=] *ServerID*
    Specifies, by DNS name or IP address, the RADIUS server about which to display information.

add authserv

Provides the IP address or the DNS name of a RADIUS server to which authentication requests should be passed.

Syntax

add authserv [**name**=]*ServerID*[[**secret**=]*SharedSecret*] [[**init-score**=]*ServerPriority*] [[**port**=]*Port*] [[**timeout**=] *Seconds*] [[**signature**] {**enabled** | **disabled**}]

Parameters

[name=] *ServerID*
    Required. Specifies, by IP address or DNS name, the RADIUS server.

[secret=] *SharedSecret*
    Specifies the shared secret.

[init-score=] *ServerPriority*
    Specifies the initial score (server priority).

[port=] *Port*
    Specifies the port to which authentication requests should be sent.

[timeout=] *Seconds*
    Specifies the timeout period, in seconds, during which the RADIUS server can be idle before it should be marked unavailable.

[signature] { enabled| disabled}
    Specifies whether to use digital signatures. The **enabled** parameter specifies that digital signatures should be

used. The **disabled** parameter specifies that digital signatures should not be used.

delete authserv

Deletes a RADIUS authentication server.

Syntax

delete authserv [**name=**]*ServerID*

Parameters

[name=] *ServerID*
      Required. Specifies, by DNS name or IP address, which server to delete.

set authserv

Provides the IP address or the DNS name of a RADIUS server to which authentication requests should be passed.

Syntax

set authserv [**name=**]*ServerID* [[**secret=**]*SharedSecret*] [[**init-score=**]*ServerPriority*] [[**port=**]*Port*] [[**timeout=**]*Seconds*] [[**signature**] {**enabled** | **disabled**}]

Parameters

[name=] *ServerID*
      Required. Specifies, by IP address or DNS name, the RADIUS server.

[secret=] *SharedSecret*
      Specifies the shared secret.

[init-score=] *ServerPriority*
      Specifies the initial score (server priority).

[port=] *Port*
      Specifies the port on which to send the authentication requests.

[timeout=] *Seconds*
      Specifies the amount of time, in seconds, that should elapse before the RADIUS server is marked unavailable.

[signature=] { enabled| disabled}
      Specifies whether digital signatures should be used.

show authserv

Displays detailed information about an authentication server. Used without parameters, **show authserv** displays information about all configured authentication servers.

Syntax

show authserv [[**name=**]*ServerID*]

Parameters

[name=] *ServerID*
      Specifies, by DNS name or IP address, the RADIUS server about which to display information.

set acco

Specifies the accounting provider.

Syntax

set acco {**windows** | **radius** | **none**}

Parameters

{ windows| radius| none}
      Required. Specifies whether accounting should be performed and by which server. The **windows** parameter specifies that Windows security should perform accounting. The **radius** parameter specifies that a RADIUS server should perform accounting. The **none** parameter specifies that no accounting should be performed.

show acco

Displays the accounting provider.

Syntax

show acco

Parameters

set authe

Specifies the authentication provider.

Syntax

set authe {**windows | radius**}

Parameters

{ windows| radius}

> Required. Specifies which technology should perform authentication. The **windows** parameter specifies that Windows security should perform authentication. The **radius** parameter specifies that a RADIUS server should perform authentication.

show authe

Displays the authentication provider.

Syntax

show authe

Parameters

Formatting legend

Format	Meaning
Italic	Information that the user must supply
Bold	Elements that the user must type exactly as shown
Ellipsis (...)	Parameter that can be repeated several times in a command line
Between brackets ([])	Optional items
Between braces ({}); choices separated by pipe (|). Example: {even|odd}	Set of choices from which the user must choose only one
Courier font	Code or program output

See Also

Concepts

Netsh commands for AAAA [http://technet.microsoft.com/en-us/library/9ffd261c-62e4-4f41-aa35-2790bd253477]
Netsh commands for DHCP [http://technet.microsoft.com/en-us/library/df9ecef3-7d85-49e6-a2aa-ff84a5bd3a39]
Netsh diagnostic (diag) commands [http://technet.microsoft.com/en-us/library/036aad0f-36b1-4f69-9c83-7983fb956fd2]
Netsh commands for Interface IP [http://technet.microsoft.com/en-us/library/b2c92af5-425a-4c0b-8604-7a8c4ac497e0]
Netsh commands for WINS [http://technet.microsoft.com/en-us/library/670bdec4-fe5b-45f5-aeae-4b13021d2006]
Command-line reference A-Z [http://technet.microsoft.com/en-us/library/552ed70a-208d-48c4-8da8-2e27b530eac7]
Command shell overview [http://technet.microsoft.com/en-us/library/44500063-fdaf-4e4f-8dac-476c497a166f]

Tags:

Community Content