Radius Change of Authorization

This chapter contains the following sections:

aaa server radius dynamic-author

Use the aaa server radius dynamic-author global configuration mode command to enter into the dynamic authorization local server configuration mode, and configure the Change of Authorization (CoA) clients and parameters.

Syntax

aaa server radius dynamic-author

Parameters

This command has no arguments or keywords.

Command Mode

Global configuration mode

User Guidelines

Dynamic authorization allows an external policy server to dynamically send updates to the device via PoD (Packet of Disconnect) or CoA (Change of Authorization) Requests. This command enters the dynamic authorization local server configuration mode. Once in this mode, Dynamic RADIUS related commands (like client address or key) can be configured.

Examples

The following example enters the dynamic authorization local server configuration mode context:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)#
```

attribute event-timestamp drop-packet

To configure the device to discard a Packet of Disconnect (POD) Request or Change of Authorization (CoA) Request that do not include an Event-Timestamp Attribute use the attribute event-timestamp drop-packet command in dynamic authorization local server configuration mode. To restore the default configuration, use the no form of this command.

Syntax

attribute event-timestamp drop-packet

no attribute event-timestamp drop-packet

Parameters

This command does not have any parameters.

Default Configuration

The device does not discard PoD or CoA requests even if they do not contain the event-timestamp attribute.

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

User Guidelines

The Event-Timestamp (RADIUS attribute 55 - [RFC2869]) is used by the Switch to check if the Requests are current. If requests are not current, they are silently discarded (RFC 5176). It is not mandatory for CoA clients to send this attribute. To enhance CoA security, use the attribute event-timestamp drop-packet command to discard PoD or CoA requests that do not include the Event-Timestamp RADIUS attribute.

Examples

In the following example the device is configured to discard PoD or CoA Requests that do not include the Event-Timestamp RADIUS attribute:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# attribute event-timestamp drop-packet
```

authentication command bounce-port ignore

To configure the device to ignore a RADIUS Change of Authorization (CoA) bounce port command, use the authentication command bounce-port ignore command in global configuration mode. Use the no form of this command to return to the default status.

Syntax

authentication command bounce-port ignore

no authentication command bounce-port ignore

Parameters

This command has no arguments or keywords.

Default Configuration

The device accepts a RADIUS CoA bounce port command.

Command Mode

Global configuration mode

User Guidelines

which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer), that does not have a mechanism to detect a change on this authentication port. The authentication command bounce-port ignore command configures the device to ignore the RADIUS CoA bounce port command to prevent a link flap from occurring on any host(s) that are connected to an authentication port.

Examples

The following example shows how to configure the device to ignore a CoA bounce port command:

```
Switch010203(config)# authentication command bounce-port ignore
```

authentication command disable-port ignore

To configure the device to ignore a RADIUS Change of Authorization (CoA) disable-port command, use the authentication command disable-port ignore command in global configuration mode. Use the no form of this command to return to the default status.

Syntax

authentication command disable-port ignore

no authentication command bounce-port ignore

Parameters

This command has no arguments or keywords.

Default Configuration

The device accepts a RADIUS CoA disable port command.

Command Mode

Global configuration mode

User Guidelines

The RADIUS CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. Use the authentication command disable-port ignore command to configure the device to ignore the RADIUS CoA disable port command so that the authentication port and other hosts on this authentication port are not disconnected.

Examples

Example 1

The following example shows how to configure the device to ignore a CoA disable port command:

```
Switch010203(config)# authentication command disable-port ignore
```

client

To specify a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests, use the client command in dynamic authorization local server configuration mode. To remove a client, use the no form of this command.

Syntax

client *ip-addres*s *[***server-key** *key-string*]

encrypted client *ip-address* **server-key** *encrypted-key-string*

no client *ip-address*

Parameters

- *ip-address* - Specifies the CoA client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address
- **server-key** *key-string* – (optional) - Configures the RADIUS key to be shared between the device and a CoA client (Range: 0–128 characters). To specify an empty string, enter "".
- **server-key** *encrypted-key-string* - Same as the key-string parameter, but the key is in encrypted form.

Default Configuration

CoA clients are not configured on the device.

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

User Guidelines

Use the client command to allow an external policy server (configured in this command) to dynamically send updates to the device. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling the device and an external policy server each to act as a CoA server and client. Use the client command to specify the CoA clients for which the device will act as a server.

Use the optional server-key parameter to specify the key for RADIUS communications between the device and the specified CoA client. This key must match the key used by the CoA client. To specify an empty string, enter "". If this parameter is omitted, the global CoA key (command server-key) is used. If a global key was not configured the RADIUS exchange between the device and CoA client will fail.

If the ignore server-key command is configured then the RADIUS exchange between the device and CoA client will succeed even if there is a key mismatch or if a key was not configured.

Examples

Example 1

In the following example a CoA client with IP address 1.1.1.1 is added with a server key of “key1”:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# client 1.1.1.1 server-key key1
```

Example 2

In the following example a CoA client with IP address 2.2.2.2 is added without configuring a client server-key. In this case the global server-key (if configured) is used:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# client 2.2.2.2
```

domain delimiter

To configure the username domain delimitator for received PoD and CoA Requests use the domain delimiter command in dynamic authorization local server configuration mode. To return to the default delimiter, use the no form of this command.

Syntax

domain delimiter *character*

no domain delimiter

Parameters

- delimiter character — Specifies the domain delimiter. One of the following options can be specified: @, /, $, %, \, # or -

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

Default Configuration

The default delimiter is the @ character.

User Guidelines

Use the domain delimiter command to configure the delimiter to use when stripping the full username for AAA or 802.1x user sessions, to compare to the username provided in the packet of disconnect (POD) or Change of Authorization (CoA) requests. See command domain delimiter for details of full username domain section stripping.

Examples

Example 1

In this example the $ character is configured as a delimiter:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# domain delimiter $
```

domain stripping

To enable and define the behavior for username domain stripping for received PoD and CoA Requests use the domain stripping command in dynamic authorization local server configuration mode. To return to the default setting, use the no form of this command.

Syntax

domain stripping [right-to-left]

no domain stripping

Parameters

stripping — Compares the incoming username with the names oriented to the left of the domain delimiter

stripping [right-to-left] (optional) - Terminates the string at the first delimiter going from right to left

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

Default Configuration

Stripping is disabled by default. Stripping default direction is left-to-right.

User Guidelines

Use the domain stripping command to enable username domain stripping based on the delimiter configured in the domain delimiter command. Domain stripping allows to compare the incoming username with the names oriented to the left of the @ domain delimiter.

Configuring domain stripping allows you to send disconnect messages with only the username present before the @ domain delimiter (or other delimiter configured using the command domain delimiter. The switch then compares and matches this username with any session username on the switch with a potential domain. For example, when domain stripping is configured and you send packet of disconnect (POD) or Change of Authorization (CoA) Requests with the username "test," a comparison between the PoD/CoA message and device session username takes place, and sessions with the username "test@example.com" or "test" match the specified username "test.".

If domain stripping is not configured (the default behavior), the username provided in the PoD and COA Requests are compared with the full usernames included on the device active sessions.

Use the right-to-left keyword to specify that the username string should be terminated the string at the first delimiter going from right to left.

Examples

Example 1:

In this example the $ character is configured as a delimiter, and stripping is performed to the left of the delimiter. In this case, if the session user-name is user1$my_users then the username to be matched in the PoD or CoA Request is "user1":

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# domain delimiter $
Switch010203(config-locsvr-da-radius)# domain stripping
```

Example 2:

In this example stripping is performed up to the 1st delimiter to the left of the first delimiter going from right to left, using the default delimiter of @. In this case, if the session user-name is user1@test.com@example.com then the username to be matched in the PoD or CoA Request is “user1@test.com”:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# domain stripping right-to-left
```

ignore server-key

To configure the device to ignore the CoA server-key use the ignore server-key command in dynamic authorization local server configuration mode. To restore the default configuration, use the no form of this command.

Syntax

ignore server-key

no ignore server-key

Default Configuration

The server-key is not ignored.

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius).

User Guidelines

Use the ignore server-key command to configure the device to ignore the server key sent in the PoD or CoA Requests. If the server-key is ignored the RADIUS exchange with the CoA client will succeed even in a CoA server-key was not configured on the device (commands client or server-key) or if the key configured on the device does not match the key provided in the PoD or CoA Requests.

The default behavior is not to ignore the server key, meaning that PoD or CoA Requests will be discarded in case of a key mis-match or if a key was not configured for the CoA client.

Examples

Example 1:

In the following example the device is configured to ignore the server key:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# ignore server-key
```

port

To specify the port on which a device listens for Change of Authority (CoA) and Packet of Disconnect (PoD) Requests from configured CoA clients, use the port command in dynamic authorization local server configuration mode. To restore the default configuration, use the no form of this command.

Syntax

port udp-port

no port

Parameters

- *udp-port*—Specifies the UDP port number for authentication requests. (Range: 0–59,999)

Default Configuration

The device listens for CoA and PoD Requests on UDP port 1700.

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

User Guidelines

Use the port command to specify the port on which the device will listen for requests from CoA clients. This configuration applies to RADIUS PoD or CoA Requests from all CoA clients. If the port number is set to 0, PoD and CoA Requests are dropped even if CoA clients have been configured.

Examples

Example 1:

In the following example a port 1648 is specified as the port on which the device listens for RADIUS PoD and CoA requests:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# port 1648
```

server-key

To configure the default RADIUS key to be shared between the device and the CoA, use the server-key command in dynamic authorization local server configuration mode. To remove the configuration, use the no form of this command.

Syntax

server-key *key-string*

encrypted server-key *encrypted-key-string*

no server key

Parameters

- *key-string*—Specifies the authentication and encryption key for all RADIUS communications between the device and the CoA client's server (Range: 0–128 characters). The key provided in the PoD or CoA request must match this key. To specify an empty string, enter "".
- *encrypted-key-string*—Same as the key-string parameter, but the key is in encrypted form

Default Configuration

default server key is not configured.

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

User Guidelines

Use the server-key command to define the default RADIUS key to be used in communications between the device and the CoA client. This key is used by clients that were not configured with a specific client key (command client)

This key must match the key used by the CoA client. To specify an empty string, enter "".

If the ignore server-key command is configured then the RADIUS exchange between the device and CoA client will succeed even if there is a key mismatch or if a key was not configured

Examples

Example 1:

In the following example a default server key “key123” is configured:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# server-key key123
```

show aaa clients

Use the show aaa clients Privilege EXEC mode command to show AAA (CoA) client's statistics.

- ip-address (optional) —Displays the statistics for a specific CoA client host. The IP address can be an IPv4, IPv6 or IPv6z address.

Default Configuration

By default, the statistics of all CoA hosts are display.

Command Mode

Privileged EXEC mode

Examples

```
Switch010203# show aaa clients

Dynamic Author Client 1.1.1.1
CoA: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
PoD: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
Average Ack response time: 0 msec

Dynamic Author Client 2.2.2.2
CoA: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
PoD: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
Average Ack response time: 0 msec

Details of counters displayed:
1. Requests – Counts the Requests received from CoA clients
2. transactions – Counts CoA completed transactions. A Completed transaction occurs once
the Switch send an ACK or NAK in response to a Request from a CoA client.
3. Retransmissions – Counts received retransmitted CoA Requests. A retransmitted CoA Requests
 is a Request in which the Request identifier is identical to the identifier of a previous
 Request.
4. active transactions – Transactions that are currently active. An active transaction is
a transaction in which a Request from a COA Client has been received but an ACK or NAK
response has not been sent yet. Once an ACK or NAK is sent this counter is decremented.
5. Ack responses - Counts the number of Ack responses sent by the switch.
6. Nak responses - Counts the number of Nak responses sent by the switch
7. invalid requests – Counts invalid requests received by the switch. An invalid request
is one of the following
    a) A Request in which the secret in the Request does not match the Secret configured
on the device,
    b) A Request with no session identifier
    c) A Request with an unsupported attribute
    d) A Request in which a supported attribute is empty
    e) A Request which is discarded because the event-timestamp is not current, or if
event-timestamp is mandatory and received request does not include this attribute
    f) A Request with a not current or missing Event-Timestamp attribute
    g) A request received with “disable port” or “bounce port” command that are dropped due
 to user configuration.
8. errors – Counts errors. an error can be an internal error in which a request cannot be
processed due to resource issue, or if a secret has not been configured for the CoA client
9. Average Ack response time – in milliseconds
```

show aaa server radius dynamic-author

Use the show aaa server radius dynamic-author Privilege EXEC mode command to show CoA configuration.

Syntax

show aaa server radius dynamic-author *[ip-address]*

Parameters

ip-address—Specifies the CoA client host IP address to display. The IP address can be an IPv4, IPv6 or IPv6z address.

Command Mode

Privileged EXEC mode

Default Configuration

By default, the command displays the information for all configured CoA clients.

Examples

Example 1

```
Switch010203# show aaa server radius dynamic-author
CoA UDP port: 1700
Default Server-Key MD5: 9aa6e5f2256c17d2d430b100032b997c
Ignore Server-Key: disabled
Domain delimiter: @
Domain stripping: disabled
“disable port” command: process
“bounce port” command: process
Event-Timestamp attribute drop packet: disabled
```

CoA Client Address	Server-Key's MD5
1.1.1.1	02cea75e335fcb814cd81932f1c15dc2
1111::1100	default

Example 2

```
Switch010203# show aaa server radius dynamic-author
CoA UDP port: 1968
Default Server-Key MD5: Not configured
Ignore Server-Key: enabled Domain delimiter: $
Domain stripping: enabled (left to right) “disable port” command: ignore
“bounce port” command: process
Event-Timestamp attribute drop packet: enabled
```

CoA Client Address	Server-Key's MD5
1.1.1.1	02cea75e335fcb814cd81932f1c15dc2

CoA Client Address	Server-Key's MD5
1111::1100	default

Example 3

```
Switch010203# show aaa server radius dynamic-author 1.1.1.1
CoA UDP port: 1977
Default Key MD5: Not configured
Ignore Server-Key: enabled Domain delimiter: $
Domain stripping: enabled (left to right)
“disable port” command: process
“bounce port” command: ignore
Event-Timestamp attribute drop packet: disabled
```

CoA Client Address	Server-Key's MD5
1.1.1.1	02cea75e335fcb814cd81932f1c15dc2