Connected Apps Configuration Mode Commands

The Connected Apps (CA) Configuration Mode is used to define CA client session parameters and High Availability (HA) settings for ASR 9000 VSMs supporting wsg-service virtual machines (VMs)

Important The StarOS commands described in this chapter are only supported for VPC running within a VM on the ASR 9000 VSM.

Command Modes Exec > Global Configuration > Connected Apps Configuration

`configure > connectedapps`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-connectedapps)#`

- activate, on page 1
- ca-certificate-name, on page 2
- end, on page 3
- exit, on page 3
- ha-chassis-mode, on page 3
- ha-network-mode, on page 4
- rri-mode, on page 5
- sess-ip-address, on page 6
- sess-name, on page 6
- sess-passwd, on page 7
- sess-userid, on page 8

activate

Initiates a ConnectedApps (CA) client session with the IOS-XR server on the ASR 9000.

Product SecGW (WSG)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-connectedapps)#`

Syntax Description

activate
no activate

no

Disconnects an established CA session.

Usage Guidelines

Use this command to establish or disconnect a ConnectedApps (CA) client session with the IOS-XR server on the ASR 9000. CA client session parameters must have been previously entered for this command to work.

Example

The following command establishes a CA client session:

activate

ca-certificate-name

Configures a ConnectedApps (CA) client session with the IOS-XR server using TLS (Transport Layer Security) and CA (Certification Authority) certificate. This is an IOS-XR 5.2.0 requirement.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-connectedapps)#`

Syntax Description

ca-certificate-name *cert_name*

cert_name

Specifies a CA certificate name as an alphanumeric string of 1 through 125 characters.

Usage Guidelines

Use this command to configure a ConnectedApps client session with the IOS-XR server using TLS (Transport Layer Security) and a specified CA certificate.

Example

The following command configures a ConnectedApps session using a CA certificate named *ux1345perm*:

```
ca-certificate-name ux1345perm
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.

ha-chassis-mode

Sets the High Availability (HA) mode for wsg-service virtual machines on VSMs in an ASR 9000.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-connectedapps)#

Syntax Description

ha-chassis-mode { inter | intra | standalone }
no ha-chassis-mode

no

Disables the current HA chassis mode

{ inter | intra | standalone }

Specifies the type of chassis mode as:

- **inter** – HA is established between VSMs in two ASR 9000 chassis.
- **intra** – HA is established between VSMs in a single ASR 9000 chassis.
- **standalone** – This is a standalone card; HA cannot be enabled.

Usage Guidelines

Use this command to set or disable HA for VSMs within or across ASR 9000 chassis. To complete HA configuration you must also set its network mode.

Example

The following command sets HA mode between two ASR 9000 chassis:

```
ha-chassis-mode inter
```

ha-network-mode

Sets the network mode for High Availability (HA) network configuration between VSMs in ASR 9000 chassis.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

```
configure > connectedapps
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-connectedapps)#
```

Syntax Description

```
ha-network mode { L2 | L3 | NA }
no ha-network mode
```

no

Deletes the current setting for HA network mode.

{ L2 | L3 | NA }

Specifies the desired HA network mode as:

- **L2** – Layer 2
- **L3** – Layer 3
- **NA** – Not Applicable (standalone VSM)

Usage Guidelines

Use this command to set the network mode for the HA network configuration between VSMs in ASR 9000 chassis.

Example

The following command sets the HA network mode to Layer 2:

```
ha-network-mode L2
```

rri-mode

Configures Reverse Route Injection (RRI) mode. (VPC-VSM only)

Product

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

```
configure > connectedapps
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-connectedapps)#
```

Syntax Description

```
rri-mode { both | none | ras | s2s }
no rri-mode
```

no

Disables the current RRI mode setting.

both

Support RAS and S2S modes.

none

Support neither RAS nor S2S mode.

ras

Support Remote Access Service mode only.

s2s

Support Site-to-Site mode only.

Usage Guidelines

Use this command to set the RRI mode.

Example

The following command sets the RRI mode to RAS.

```
rri-mode ras
```

sess-ip-address

Sets the IP address for a Connected Apps (CA) session.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-connectedapps)#`

Syntax Description

sess-ip-address *ip_address*
no sess-ip-address

no

Deletes the current CA session IP address.

ip_address

Specifies the IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to set the IP address for a Connected Apps (CA) session.

Example

The following command sets an IPv4 address for a CA session.

sess-ip-address 209.165.200.225

sess-name

Sets the name for a CA session.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-connectedapps)#`

Syntax Description

sess-name *session_name*
no sess-name

no

Deletes the current CA session name.

session_name

Specifies the CA session name as an alphanumeric string of 1 through 125 characters.

Usage Guidelines

Use this command to set the name for a CA client session.

Example

The following command sets the CA session name to *vsm0-1*:

```
sess-name vsm0-1
```

sess-passwd

Sets a password for a CA session.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-connectedapps)#

Syntax Description

sesss-passwd { encrypted | password } *password*
no sess-passwd

no

Deletes the current CA session password.

encrypted

This keyword is only used by StarOS when you save the configuration file. StarOS displays the encrypted keyword in the configuration file as a flag indicating that the variable following the keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

password

Specifies that the password will appear in plain text in the configuration file.

password

Specifies the password as an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage Guidelines

Use this password to set a password for a CA session.

Example

The following command sets a plain text password for a CA session:

```
sess-passwd password admin012
```

sess-userid

Defines a user identifier (username) for the CA session.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

```
configure > connectedapps
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-connectedapps)#
```

Syntax Description

```
sess-userid username
no sess-userid
```

no

Deletes the current user identifier for the CA session.

username

Specifies the user identifier for the CA session as an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to define a user identifier (username) for the CA session.

Example

The following command sets the user identifier to *vsm-admin02*:

```
sess-userid vsm-admin02
```