oneP Communication

Communication between IOS-XR and a WSG service is based on the oneP (StarOS Connected Apps) infrastructure. This bidirectional communication allows the service to send and receive information to/from IOS-XR.

This chapter describes the configuration of oneP client communication.

Overview

The oneP infrastructure supported by IOS-XR on the ASR 9000 is used to communicate with StarOS service virtual machines (VMs). OneP libraries consists a set of "C" libraries running as Linux user space processes so that a WSG service can interface with IOS-XR. An instance of the oneP (StarOS Connected Apps [CA]) library running within a wsg-service VM is completely independent from another instance running as part of a different wsg-service VM. A StarOS **connectedaspps** command allows an operator to configure and initiate a oneP (Connected Apps) session with the IOS-XR server.

For additional information on the ASR 9000 and the oneP infrastructure refer to:

- *Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide – Configuring Virtual Services on the Cisco ASR 9000 Series Router*
- *Implementing CGv6 over VSM*

Connected Apps Sessions

The StarOS client Connected Apps (oneP) application running on the wsg-service VM can set up a TLS (Transport Layer Security) session with the oneP server running on the ASR 9000 route processor (RP).

Enabling oneP on ASR 9000 RSP

To enable oneP communication with the VSM, the corresponding oneP server configuration should be done on the ASR 9000 Route Switch Processor (RSP). For IOS-XR 5.2.0 version onwards, only TLS transport type is supported for oneP connection. The basic configuration sequence is:

```
onep
 transport type tls localcert onep-tp disable-remotecert-validation
 !

 crypto ca trustpoint onep-tp
 crl optional
 subject-name CN=ASR9K-8.cisco.com
 enrollment url terminal
!
```

By default, OneP flows are blocked at the LPTS layer on the VSM. That is why you must configure a policer rate for OneP flow for VSM.

For additional information, refer to the *Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide – Configuring Virtual Services on the Cisco ASR 9000 Series Router*

Configuring a Client CA Session

Before a CA session can be activated via StarOS, the operator must configure the session parameters – IP address, session name, username and password.

Important A client CA session must be configured via StarOS on each VPC-VSM instance running on the VSM (one per CPU).

The following sample StarOS CA mode CLI command sequence configures the CA session parameters:

```
configure
   connectedapps
     ca-certificate-name cert_name
     ha-chassis-mode inter
     ha-network-mode L2
     rri-mode BOTH
     sess-ip-address ip_address
     sess-name session_name
     sess-passwd { encrypted | password } password
     sess-userid username
     activate
```

ip_address may be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal format.

For a complete description of these command keywords, see the *Global Configuration Mode Commands* and *Connected Apps Configuration Mode Commands* chapters of the *Command Line Interface Reference*.

Activating a Client Connected Apps Session

Important You must configure HA Mode, on page 3 on each VPC-VSM instance before activating a client CA session via StarOS.

To activate a CA session with the IOS-XR oneP server execute the following StarOS command sequence:

```
configure
   connectedapps
     activate
```

For a complete description this command, see the *Global Configuration Mode Commands* and *Connected Apps Configuration Mode Commands* chapters of the *Command Line Interface Reference*.

For additional information on IOS-XR commands, refer to ASR 9000 user documentation.

HA Mode

High Availability (HA) mode for a wsg-service VM is configured via StarOS Connected Apps mode commands as described below.

Configuring HA Chassis Mode

High Availability can be configured between ASR 9000 chassis (inter), within a single chassis (intra) [VSM-to-VSM] or standalone VSM.

The following StarOS CA mode command sequence enables the preferred HA chassis mode:

```
configure
   connectedapps
     ha-chassis-mode { inter | intra | standalone }
```

For a complete description this command, see the *Global Configuration Mode Commands* and *Connected Apps Configuration Mode Commands* chapters of the *Command Line Interface Reference*.

Configuring HA Network Mode

HA network mode can be specified as:

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

The following StarOS CA mode command sequence enables the preferred HA network mode:

```
configure
   connectedapps
      ha-network mode { L2 | L3 | NA }
```

For a complete description this command, see the *Global Configuration Mode Commands* and *Connected Apps Configuration Mode Commands* chapters of the *Command Line Interface Reference*.

show connectedapps Command

The StarOS **show connectedapps** command displays information about the current CA configuration.

The following is a sample output of this command:

```
Current connectedapps controller configuration
    CA session userid : iosxr01
    CA session password : db1jvk4
    CA session name : vm0-1
    CA session IP address : 192.168.120.1
    CA session ca certificate name : test
    RRI mode : S2S & RAS
    HA chassis mode : inter
    HA network mode : L2
    CA session Activation : YES
    CA session ID : 28677
    CA SRP Status : ACTIVE
    CA SRP State : SOCK_ACTIVE
```

SRP refers to the Session Redundancy Protocol supported by the StarOS Interchassis Session Recovery (ICSR) function. For additional information on SRP and ICSR, refer to the *VPC-VSM System Administration Guide*.

For additional information about this command, see the *Exec Mode show Commands* chapter in the *Command Line Interface Reference*.