Release 2.3.2

- What's New in Release 2.3.2, on page 1
- Upgrading the connector OVA to 2.3.2, on page 2
- Caveats, on page 2

What's New in Release 2.3.2

This release allows you to perform the following:

- Deploy the connector as a Amazon Web Services (AWS) instance. You can download an Amazon Machine Images (AMI) image from Amazon Web Services. The connector AMI has the following limitations:
  - Dual-interface mode is not supported.
  - Proxy configuration is not supported.
  - Enabling or disabling the AAA with IPSec feature is not supported.
  - Upgrading the connector from theGUI is not supported.

  For more information, see Downloading and Deploying the Cisco Spaces: Connector AMI.
- Install a connector in a dual-interface mode, where the connector has access to two different networks.
- Configure the connector to access an external network that can reach the cloud-hosted Cisco Spaces, and an internal network that connects to all your devices (dual-interface mode). For more information, see Downloading and Deploying the Cisco Spaces: Connector OVA (Dual Interface) .
- Deploy the connector as a Hyper-V instance. You can download a Virtual Hard Disk (VHDX) image from cisco.com . However, you cannot configure the Hyper-V connector in the dual-interface mode. For more information, see Downloading and Deploying Hyper-V.
- Configure a syslog server on the connector. For more information, see Syslog Commands in Connector Command Reference Guide.
- Mask a user's IP address on Cisco Spaces (along with username and MAC address). For more information, seeConfiguring Privacy Settings in the Connector Configuration Guide.
- Configure the HTTP proxy with basic authentication. See Configuring a Proxy in the Connector Configuration Guide.

- Test connectivity from connector to Cisco Spaces using the **connectorctl testconnectivity** command. For more information, see Cloud Connectivity Commands in the Connector Command Reference Guide.
- Configure the Subject Alternative Names (SANs) field of a self-signed certificate or a Certification Authority (CA)-signed certificate with either the Fully Qualified Domain Name (FQDN) or the hostname of the connector. The **connectorctl createcsr** and the **connectorctl generatecert** commands are now modified with the capability to configure Subject Alternative Names (SANs). For more information, see Certificate Commands in the Connector Configuration Guide.

Upgrading the connector OVA to 2.3.2

This task shows you how to upgrade the Cisco Spaces: Connector OVA to version 2.3.2.

Procedure

Step 1 Download Connector 2.3.2 from cisco.com.

Step 2 Copy the downloaded file on to the Cisco Unified Computing System (Cisco UCS) where the Cisco Spaces: Connector is hosted.

Step 3 Log in to the connector CLI.

Step 4 Run the **connectorctl upgrade** <<*upgrade_file_name*>> command.

This command starts the OVA upgrade process.

The **dnasadmin** user is created.

Step 5 Set a password for the newly created **dnasadmin** user when prompted.
Wait for a few seconds for the upgrade to be completed.

Step 6 After the upgrade is completed, log in to the connector as the **dnasadmin** user.

Observe that the connector is upgraded and restored to the same state as it was before the upgrade.

You can ignore the two known errors displayed during the upgrade. See CSCvr74830.

What to do next

To deploy connector 2.3.2 in a dual-interface configuration, ensure that the Cisco UCS device has an additional physical interface (device interface) defined. If not, add the device interface and restart the connector. For more details, see the Cisco DNA Spaces: Connector Configuration Guide.

Caveats

Caveats describe unexpected behavior in the Cisco Spaces: Connector.

Open Caveats in Cisco Spaces: Connector, Release 2.3.2

This section lists the bugs that are open in this release of Cisco Spaces: Connector.

Table 1: Open Caveats

Caveat	Description
CSCvt29826	AAA with IPSec enabled does not work when certificate generated on connector is of key type ECDSA.
CSCwa05499	ConnectorAMI2.3.2: Docker upgrade immediate instead of waiting for configured Upgrade window
CSCwa05506	ConnectorAMI2.3.2: **connectorctl dockersubnet** remove(r) command does not remove the docker subnet.
CSCwa22344	ConnectorAMI2.3.2 - Invalid SSL Certificate causes GUI login/render failure (Negative Test)
CSCwa42080	ConnectorAMI2.3.2: Authorization fails with valid user when IPSec tunnel is configured

Resolved Caveats in Cisco Spaces: Connector, Release 2.3.2

This section lists the bugs that are resolved in this release of Cisco Spaces: Connector.

Table 2: Resolved Caveats

Caveat	Description
CSCvy69125	Proxy Certificate Installation Fails in connector with 'Unknown File Format' Error.
CSCvz49630	**connectorctl networkconfig cloudstatus** not working when connector is installed as a Hyper-V instance using **cisco-dna-spaces-connector-2.3.495.connector**.