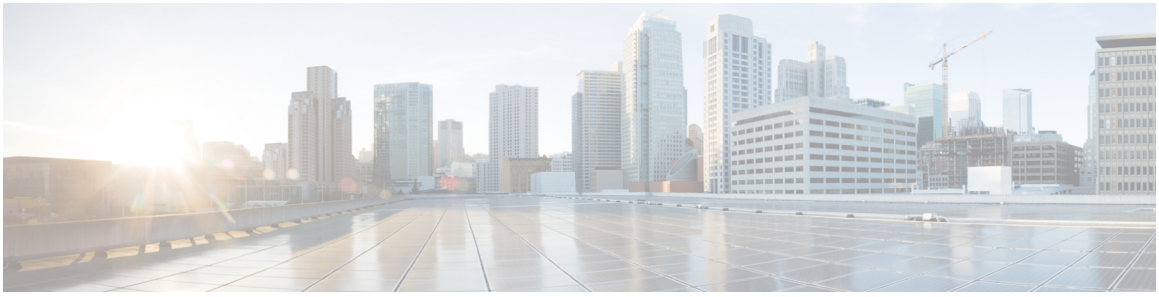
Cisco Spaces: Connector 2.x Command Reference Guide

First Published: 2019-03-09

Last Modified: 2022-06-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

Preface

Audience

This document is meant for Cisco Spaces network and IT administrators who deploy Cisco Spaces to monitor, manage, and optimize usage of assets in an organization.

Conventions

This document uses the following conventions:

Table 1: Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string. Otherwise, the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.

Convention	Indication
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means the following information will help you solve a problem.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Related Documentation

Cisco Spaces: Connector3 Configuration Guide

Cisco Spaces: Connector3 Command Reference Guide

Release Notes for Cisco Spaces: Connector

Cisco Spaces: IoT Service Configuration Guide (Wireless)

Cisco Spaces: IoT Service Configuration Guide (Wired)

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

PART I

Using the Command-Line Interface

Using the CLI

Using the Command-Line Interface

You can access Cisco Spaces: Connector via the command line interface.

Note **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

Restricted Command-Line Interface

Restricted CLI

In Cisco Spaces: Connector, Linux commands are restricted to prevent unauthorized users from inadvertently modifying the system configuration. This restricted access prevents users from modifying system configuration that are likely to cause issues.

The following commands are allowed on the restricted command line:

Table 2: List of Restricted Commands

Command	Description
cat	Prints file contents.
cp	Copies file.
df	Prints file system disk space usage.
du	Prints file space usage.
grep	Prints lines matching a pattern.
ip	Displays network interface configuration.
ls	Lists directory contents.
nslookup	Queries internet-name servers.
passwd	Changes the **spacesadmin** password.
ping	Sends Internet Control Message Protocol (ICMP) echo requests to network device.
pwd	Prints the current or working directory.
rm	Removes files.
scp	Secures remote copy files.
sftp	Secures file transfer.
ssh	Connects with SSH into a client.
tail	Outputs the last part of a file.
top	Displays linux processes.
route	Configure IP routing table rules.
clear	Clears screen.
wget	Downloads files from the internet.
who	Displays the user.

PART II

Configure Commands

Configure Commands

connectorctl lockinterval

This command sets the permitted number of unsuccessful login attempts before the account is locked. The command also sets the account lockout interval in minutes. The minimum number of tries is three. The maximum of tries is five. The default number of tries is three.

Parameters

None.

connectorctl lockinterval

Usage Guidelines

```
[cmxadmin@connector ~]$ connectorctl lockinterval
Unsuccessful login attempts before account lock [3-5] [3]: 4
Account lockout interval in minutes [1-120] [30]: 30|
```

connectorctl passwordpolicy

This command sets the password policy for the Connector Web UI, prevents the configuration of weak passwords, and encourages the setting of a strong password.

Parameters

Table 3: Parameters

Parameter	Description
Enable strong password	Enables the setting of a strong password that includes uppercase, lowercase, special characters, and digits.
Minimum password length	Enables you to specify a password length. Minimum length is eight, maximum length is 127, and the default length is 8
Reject weak passwords	Enables rejection of a weak password (such as a dictionary word), instead of merely issuing a warning.
Allow password to expire	Sets the password expiration period to 60 days and warning period to seven days.

connectorctl passwordpolicy

Usage Guidelines

```
[cmxadmin@connector ~]$ connectorctl passwordpolicy
Enable strong password [yes / no] [yes]: yes
Minimum password length [8-127] [8]: 10
Reject weak passwords? [Y/N] [yes]: Y
Allow password to expire [yes / no] [yes]: yes
```

connectorctl networkconfig cloud

This command configures or displays the network configurations made on the connector. This command works both on single and dual interface deployments.

Note If you change the hostname or the IP address using this command, ensure that you regenerate the self-signed certificate. Use the **connectorctl generatecert** command after you reboot the system.

Parameters.

Table 4: Parameters

Parameter	Description
cloud	Configures the interface in a single-interface deployement. Configures the cloud interface or the interface that connects to the external network (first interface) in a dual-interface deployment.
cloudstatus	Displays the status of the interface in a single-interface deployement. Displays the status of the cloud interface in a dual-interface deployment (first interface).

connectorctl networkconfig { cloud | cloudstatus }

Usage Guidelines

```
 [dnasadmin@conn170 ~]$ connectorctl networkconfig cloud
HOSTNAME=conn170
IPADDR=10.22.x.x
NETMASK=255.255.255.0
GATEWAY=10.22.x.x
DNS1=171.x.x.x
DOMAIN=cisco.com
HWADDR=00:0x:xx:xx:xx:xx
Do you want to edit any of the above information? [y/n] [n]: n
================================================================================
 Hostname Configuration
================================================================================
Do you want to edit the Hostname? [y/n] [n]: n
Please enter the new Hostname : cmxadmin
================================================================================
 IP Address Configuration
================================================================================
Do you want to edit the IP Address? [y/n] [n]: yes
Please enter the new IP Address : 10.22.244.11
================================================================================
 Netmask Configuration
================================================================================
Do you want to edit the Netmask? [y/n] [n]: n
================================================================================
Gateway Configuration
================================================================================
Do you want to edit the Gateway? [y/n] [n]: n
================================================================================
 DNS Server Configuration
```

```
================================================================================
DNS Servers can be added, edited, or removed
1. Add DNS Server                       Press 1
2. Edit DNS Server                      Press 2
3. Remove DNS Server                    Press 3
4. Exit                                 Press 4
Please select an option from the list above: (Default value is 4)

Added DNS Servers:
DNS1=10.x.x.x
Please enter the DNS Server IP Address: 10.x.x.x
[4]: 1

================================================================================
Domain Configuration
================================================================================
Do you want to edit the Domain? [y/n] [n]: n
New Network Changes:
HOSTNAME cmxadmin
IPADDR 10.x.x.x
DNS2 10.x.x.x
Confirm the above details? [y/n] [n]: y

Successfully restarted network service
LATEST NETWORK CONFIGURATION
HOSTNAME= cmxadmin
IPADDR=10.x.x.x
NETMASK=255.255.255.0
GATEWAY=10.x.x.x
DNS1=192.x.x.x.x
DOMAIN=test.com
System will reboot in 5 seconds...


[dnasadmin@conn170 ~]$ connectorctl networkconfig cloudstatus
Interface Name = ens33
IP = 10.22.x.x
NETMASK = 255.255.255.0
DOMAIN = cisco.com
DNS = 171.70.x.x
SUBNETS not configured

Routing Table
=============
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface    MSS
Window irtt
0.0.0.0         10.22.x.x     0.0.0.0         UG    0      0        0 ens33    0      0
  0
10.22.x.0     0.0.0.0         255.255.255.0   U     0      0        0 ens33    0      0
  0

Firewall rules
==============
Allowed port/protocol
443/tcp
1812/tcp
1813/tcp
8000/tcp
8004/tcp
2003/udp
```

connectorctl networkconfig device

This command configures or displays the network configurations that are made on the Cisco Spaces: Connector. This command works only on dual interface deployments. Running the command on a single-interface deployment throws an error.

Note If you change the hostname or the IP address using this command, ensure that you regenerate the self-signed certificate. Use the **connectorctl generatecert** command after you reboot the system.

Parameters

Table 5: Parameters

Parameter	Description
device	In a dual-interface deployment, it configures the interface where the devices are present (device interface).
devicestatus	Displays the status of the device interface in a dual-interface deployment.

connectorctl networkconfig { device | devicestatus }

Usage Guidelines

```
dnasadmin@conn171 ~]$ connectorctl networkconfig device
Do you want to (C)onfigure or (D)elete the Device Interface or (E)xit? (c/d/e): d
Are you sure you want to delete the Device Interface? (y/n) [n]: y
Deleting Device Interface ...
Device Interface deleted successfully.
System will reboot in 5 seconds...
Connection to 10.22.x.x closed by remote host.
Connection to 10.22.x.x closed.
rmadira@RMADIRA-M-L2BK Downloads % ssh dnasadmin@10.22.x.x
ssh: connect to host 10.22.x.x port 22: Operation timed out
rmadira@RMADIRA-M-L2BK Downloads % ssh dnasadmin@10.22.x.x
Password:
Password:
Last failed login: Mon Aug  9 13:35:57 PDT 2021 from 10.24.127.162 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Mon Aug  9 13:32:12 2021 from 10.24.x.x
[dnasadmin@conn171 ~]$ connectorctl networkconfig device
Configuring the Device Interface ...
Please enter IP []: 2.1.0.x
Please enter Netmask []: 255.255.255.0
Please enter Gateway []: 2.1.0.x
Please enter Domain []: cisco.com
================================================================================
 DNS Server Configuration
================================================================================
DNS Servers can be added, edited, or removed
1. Add DNS Server                       Press 1
2. Edit DNS Server                      Press 2
3. Remove DNS Server                    Press 3
4. Exit                                 Press 4
```

```
Please select an option from the list above [4]: 4

================================================================================
 Subnet Configuration
================================================================================
Current Subnet List:
2.1.x.x/24        (Auto-populated)
--------------------------------------------------------------------------------
Subnets can be added, edited, or removed
1. Add Subnet                           Press 1
2. Edit Subnet                          Press 2
3. Remove Subnet                        Press 3
4. Exit                                 Press 4
Please select an option from the list above [4]: 4

================================================================================
Do you want to block ports (8000, 8004 and 2003) on Cloud Interface? [y/n] [n]: n
================================================================================
Following configuration will be saved:
IPADDR=2.1.x.x
NETMASK=255.255.255.0
GATEWAY=2.1.0.x
DOMAIN=cisco.com
SUBNET1=2.1.0.0/24
CLOUD_PORTS_BLOCKED = No
Confirm the above details? [yes/no]: yes
Saving configutation...
Configuring Device Interface ...
Device Interface configured successfully.
System will reboot in 5 seconds...
Connection to 10.22.212.171 closed by remote host.
Connection to 10.22.212.171 closed.
```

Note You can add more subnets using the **Add Subnet** option. The Cisco Spaces: Connector can reach these subnets using the device interface.

```
[dnasadmin@conn170 ~]$ connectorctl networkconfig devicestatus
Interface Name = ens160
IP = 2.1.0.x
NETMASK = 255.255.255.0
DOMAIN = cisco.com
DNS =
SUBNET(s) configured:
---------------------
SUBNET1 = 2.1.0.0/24

Routing Table
=============
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface    MSS
Window irtt
2.1.0.0         2.1.0.x         255.255.255.0   UG    0      0        0 ens160   0     0
    0
2.1.0.0         0.0.0.0         255.255.255.0   U     0      0        0 ens160   0     0
    0

Firewall rules
==============
Subnets allowed     port/protocols allowed
---------------     ----------------------
2.1.0.0/24          2003/udp, 443/tcp, 8000/tcp, 8004/tcp
CLOUD_PORTS_BLOCKED = No
```

```
[dnasadmin@conn170 ~]$
```

connectorctl dnsconfig

This command configures or displays the DNS configurations that are made on the Cisco Spaces: Connector.

Table 6: Parameters

Parameter	Description
cloud	
device	

connectorctl dnsconfig [cloud | device]

Usage Guidelines

```
[dnasadmin@AMIMARKETPLACE ~]$ connectorctl dnsconfig
================================================================================
 DNS Server Configuration
================================================================================
DNS Servers can be added, edited, or removed
1. Add DNS Server                       Press 1
2. Edit DNS Server                      Press 2
3. Remove DNS Server                    Press 3
4. Exit                                 Press 4
Please select an option from the list above [4]: 1


Added DNS Servers:
Please enter the DNS Server: 10.8.8.8
================================================================================
 DNS Server Configuration
================================================================================
DNS Servers can be added, edited, or removed
1. Add DNS Server                       Press 1
2. Edit DNS Server                      Press 2
3. Remove DNS Server                    Press 3
4. Exit                                 Press 4
Please select an option from the list above [4]: 4
```

```
Following configuration will be saved:

DNS1=10.8.8.8

Confirm the above details? [yes/no]: yes

Saved changes successfully

System needs to reboot for changes to take effect.
```

PART III

Certificate Commands

Certificate Commands

connectorctl cert generate

This command regenerates a connector self-signed certificate. Once you deploy the self-signed certficate, you can view the certificate with the **connectorctl showcert** command.

connectorctl cert generate

Command History

Earlier than Release 2.3.2	The Connector SSL certificate contains the IP address in the **Subject Alternative Name (SAN)** field of the CSR.
Release 2.3.2	From 2.3.2, the connector SSL certificate contains the Fully Qualified Domain Name (FQDN) or the hostname in the **Subject Alternative Name (SAN)** field of the CSR.

Usage Guidelines

The FQDN and hostname configures the Certificate Signing Request (CSR) of a CA-signed certificate. When the CSR is signed by the CA, the created certificate contains the FQDN or the hostname in the SAN field.

With CSCvt29826, AAA with IPSec is not compatible with a certificate that is generated on a Connector of key type Elliptic Curve Digital Signature Algorithm (ECDSA) that is generated with the **connectorctl generatecert** command.

Examples

The following is a sample output of the command:

```
[dnasadmin@conn171 ~]$ connectorctl generatecert
Key Type [RSA/ECDSA] [RSA]:
Generating RSA private key, 2048 bit long modulus
.
........
e is 65537 (0x10001)
generatecert successful.
Note: Rsyslog service is enabled with TLS protocol.
You may need to deploy connector's CA certificate into Remote Syslog Server.
You can use "connectorctl exportcacert" command to extract the CA certitifcate.
Afterwards, you may need to restart rsyslog service. using "connectorctl rsyslogconfig
restart"
```

Related Topics

connectorctl showcert, on page 21
connectorctl rsyslogconfig restart, on page 76

connectorctl showcert

This command displays the deployed certificate details.

connectorctl showcert

Command History

Release 2.2	This command is introduced.

Examples

The following is a sample output of the command:

```
dnasadmin@conn171 ~]$ connectorctl showcert

Certificate details
================================================================================
                                    Certificate
================================================================================
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            a2:b6:8f:39:9e:b3:e5:19
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=CA, L=San Jose, O=Cisco, CN=conn171
        Validity
            Not Before: Aug 17 21:29:13 2021 GMT
            Not After : Aug 17 21:29:13 2023 GMT
        Subject: C=US, ST=CA, L=San Jose, O=Cisco, CN=conn171
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:aa:2f:26:cb:37:d0:d9:d8:bc:83:42:ea:fe:fc:
                    e3:21:62:12:57:40:4e:73:fa:6d:82:8c:eb:00:37:
                    43:60:5b:70:30:09:a5:33:57:71:13:33:62:3d:de:
                    bb:51:39:b5:0b:f2:bc:2d:fc:20:38:b7:8c:ca:1b:
                    6a:9c:d3:84:dc:7d:ed:31:ca:96:e7:7e:dd:59:b5:
                    ee:ea:4b:f2:ec:9a:9a:58:65:8f:f6:05:ef:ee:40:
                    4f:78:37:09:a5:6b:79:e8:4a:df:17:2e:84:76:8c:
                    c4:59:30:6c:a3:9e:63:f5:f2:a0:5e:e0:0e:38:bd:
                    86:e2:f7:48:fb:7a:85:06:2f:37:a2:e8:c9:f0:b4:
                    85:99:65:91:a0:8d:ab:55:b0:cd:0a:69:26:9f:d3:
                    39:11:66:ea:1e:22:ce:59:3e:a2:c4:25:d6:07:74:
                    71:71:f1:1b:78:36:4d:28:57:2c:fd:5d:0d:f0:20:
                    3b:d4:bb:c7:90:4a:02:d1:f5:0d:49:1d:7a:10:7d:
                    ca:c3:ae:43:bc:7f:cf:a3:84:8f:0d:0f:b3:2e:48:
                    c8:61:d5:18:7e:d6:27:e7:e2:b2:17:d2:2e:57:05:
                    d1:22:c6:74:23:ee:d9:6e:c6:9f:cc:30:0a:be:f3:
                    b2:03:bf:bb:e7:ea:b1:e1:53:01:62:5b:ca:05:98:
                    e8:db
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                DA:2E:75:E3:F1:64:F4:35:5F:4C:B6:63:E2:E1:F1:E5:03:89:D3:CA
            X509v3 Authority Key Identifier:
                keyid:DA:2E:75:E3:F1:64:F4:35:5F:4C:B6:63:E2:E1:F1:E5:03:89:D3:CA

            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Extended Key Usage:
```

```
                TLS Web Server Authentication
            X509v3 Subject Alternative Name:
                DNS:conn171
    Signature Algorithm: sha256WithRSAEncryption
         4c:63:b0:f7:37:24:7c:b5:5d:f9:b0:c2:3e:dc:8b:c9:27:ab:
         7e:e9:00:1b:b3:49:9e:62:de:e1:eb:1c:8c:46:ad:96:ed:82:
         04:e4:f9:02:39:7f:6d:b6:4f:cb:49:87:03:aa:2c:75:37:0f:
         52:03:85:66:37:23:29:16:68:65:4a:f6:c7:8a:9e:df:c7:a9:
         e8:43:96:cc:4b:47:69:b7:ff:17:f6:8f:82:05:b2:d8:51:84:
         b4:56:85:99:31:7b:3a:ee:c5:e4:dd:f1:24:7a:d8:6d:b1:79:
         86:a8:1e:08:cf:be:3e:0d:2a:78:9b:23:7c:12:68:ce:c9:fd:
         49:39:5b:74:80:98:d0:cb:6f:7e:5a:5b:f2:65:77:04:22:3f:
         99:fe:cb:7e:08:bd:76:3b:91:3f:5f:a8:fa:8b:06:6f:f7:57:
         46:2f:73:ac:22:00:3a:e1:49:3c:dc:71:c2:db:e6:8a:00:de:
         d2:56:12:7b:ca:15:f7:29:89:11:8d:71:64:87:e0:75:7b:9e:
         a0:35:12:48:76:8f:11:9f:d5:3c:28:6b:e7:8a:d4:10:50:b1:
         b8:92:5e:61:98:d5:ac:56:82:75:38:cb:58:d3:3e:e4:13:27:
         b3:60:7a:b3:19:c7:6c:a8:76:0c:b2:0f:c8:a8:9a:a2:59:5c:
         26:b7:64:eb
================================================================================
                           Certificate for IOT interface
================================================================================
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cc:68:8e:6e:a7:26:a7:66
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=CA, L=San Jose, O=Cisco, CN=conn171
        Validity
            Not Before: Jul 15 20:28:15 2021 GMT
            Not After : Jul 15 20:28:15 2023 GMT
        Subject: C=US, ST=CA, L=San Jose, O=Cisco, CN=conn171
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:8b:30:3b:f5:6d:33:60:3f:63:0b:be:a4:b0:49:
                    b3:7f:bc:69:d3:ea:ab:e3:be:0b:43:da:f6:2c:40:
                    4e:7f:41:70:62:83:ae:cf:e5:ab:35:b5:e5:99:8a:
                    61:03:89:0f:c7:6f:26:d6:d4:b7:aa:d9:98:23:f3:
                    a4:da:8a:6b:59:0d:05:cf:17:3f:06:e2:41:10:f4:
                    4a:f6:96:99:58:57:27:b7:0a:4e:b5:5d:93:55:26:
                    fd:f6:51:f1:17:c5:a6:44:42:ae:18:1e:73:41:16:
                    ab:68:83:26:7f:45:3f:c1:b8:5e:0c:eb:a6:03:16:
                    64:41:95:92:b2:d8:a2:df:05:92:22:68:ec:dc:28:
                    85:5a:0c:aa:63:b6:e3:a1:41:08:04:5b:99:46:51:
                    c2:79:3d:8f:4c:b1:e8:f1:12:9c:45:a5:11:8b:40:
                    ff:dd:7f:ba:07:5e:d8:b9:0a:87:f9:81:4b:ed:f6:
                    ae:8d:52:e6:4c:85:66:ee:1c:a4:f8:a3:c8:af:3a:
                    5d:70:f3:26:a7:09:9f:b3:4f:5c:ac:04:35:44:6b:
                    ff:d5:31:07:d3:f7:27:c8:5a:34:93:77:bb:97:d4:
                    88:7c:fa:01:6b:32:6b:be:7a:ab:8e:fd:bf:15:10:
                    2b:66:46:b4:0d:43:2b:63:3e:9e:c1:7b:ad:dc:61:
                    d4:13
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                A9:52:B9:CF:B9:F5:24:2F:02:DE:EC:65:5C:94:31:44:C0:C2:16:A9
            X509v3 Authority Key Identifier:
                keyid:A9:52:B9:CF:B9:F5:24:2F:02:DE:EC:65:5C:94:31:44:C0:C2:16:A9

            X509v3 Basic Constraints:
                CA:TRUE
```

```
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Subject Alternative Name:
                IP Address:10.x.x.x    Signature Algorithm: sha256WithRSAEncryption
          13:1d:a7:31:54:b4:b4:6c:de:7f:2a:7a:27:c7:46:6a:bf:2a:
          61:6d:0e:7e:23:c1:2c:b6:15:35:a6:79:86:59:85:8e:39:ff:
          9e:fc:a9:95:6b:99:23:78:e2:24:46:a3:bc:18:b8:df:b9:bc:
          80:2a:42:90:56:56:55:a7:3f:34:90:8a:f4:48:13:5a:af:36:
          7f:8b:71:57:97:76:3f:59:2d:be:8a:28:e9:0d:58:53:16:d0:
          a1:24:bb:be:32:67:e3:98:9b:f2:93:50:b3:c1:b3:56:e4:dc:
          e8:a3:35:63:51:a1:2c:ce:9f:99:fb:7a:51:92:2c:30:e0:17:
          1c:28:b4:2d:ad:1d:ca:0a:53:1f:da:d9:c5:ad:0d:24:a9:53:
          fa:18:f5:5d:17:d1:3c:cb:0c:be:04:7b:1a:d6:96:ce:6c:6b:
          21:a1:ba:2f:9a:5c:8e:5f:f3:8d:1f:69:bd:e1:8b:73:53:d8:
          f1:69:b2:bf:23:bb:af:f5:87:b4:66:5c:e1:47:a7:3f:12:aa:
          4b:55:35:78:04:e5:f7:ae:76:9c:ba:4a:15:c2:85:60:2a:b3:
          a8:00:51:bf:23:82:b8:95:eb:f9:75:4c:ba:31:43:dc:98:dd:
          a3:ab:f3:60:7a:e0:60:cc:d8:8b:91:90:8e:56:2c:d1:16:1a:
          6c:a5:c7:79
==========================================================================================
No Certificate available for WSA interface.
==========================================================================================
```

Related Topics

connectorctl cert generate, on page 20
connectorctl createcsr, on page 24

connectorctl createcsr

This command creates a Certificate Signing Request (CSR) for a new Secure Sockets Layer (SSL) certificate. You can get the CSR signed by a Certification Authority (CA) and obtain a CA-signed SSL certificate. Once you deploy the CA-signed certfficate, you can view the certificate with the **connectorctl showcert** command.

connectorctl createcsr

Command History

Earlier than Release 2.3.2	The connector SSL certificate contains the IP address in the **Subject Alternative Name (SAN)** field of the CSR.
Release 2.3.2	From 2.3.2, the connector SSL certificate contains the Fully Qualified Domain Name (FQDN) or the hostname in the **Subject Alternative Name (SAN)** field of the CSR.

Usage Guidelines

The FQDN and hostname configures the Certificate Signing Request (CSR) of a CA-signed certificate. When the CSR is signed by the CA, the created certificate contains the FQDN or the hostname in the SAN field.

Examples

The following is a sample output of the command:

```
[[cmxadmin@cmxnew ~]$ connectorctl createcsr

Creating Certificate Signing Request (CSR)

[For SAN field of CSR, enter IP Address for CMX server []: 10.x.x.x
Keytype is RSA, so generating RSA key with length 2048

Generating RSA private key, 2048 bit long modulus

e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank

For some fields there will be a default value,
If you enter '.', the field will be left blank.

[Country Name (2 letter code) [AU]:US
[State or Province Name (full name) [Some-State]:CA
[Locality Name (eg, city) []:San Jose
Organization Name (eg, company) []:Cisco Systems Inc.
Organizational Unit Name (eg, section) []:DNA_Spaces_Connector_01
[Common Name (e.g. server FQDN or YOUR name) [10.x.x.x]:
[Email Address []:
Please enter the following 'extra' attributes
 to be sent with your certificate request

[A challenge password []:
[An optional company name []:
The CSR is stored in : /etc/ssl/private/dnaspacescsr.pem
The Private key is stored in: /etc/ssl/private/dnaspaceskey.pem
Certificate Signing Request created successfully
```

Observe that the certificate is stored at /etc/ssl/private/dnaspaceskey.pem. This location is not owned by the **dnasadmin** user, and hence you cannot use GUI tools to download this file.

However, you can use the **scp** command to download the file.

```
user@home-machine % scp dnasadmin@x.x.x.x:///etc/ssl/private/dnaspacescsr.pem ./
(dnasadmin@x.x.x.x) Password:
dnaspacescsr.pem

100% 1135   338.2KB/s   00:00
```

Note The **root** user is disabled by default.

Related Topics

connectorctl showcert, on page 21

connectorctl setproxycert

This command sets the certificate of the HTTPS proxy.

Parameters

Filename of certificate.

connectorctl setproxycert *filename*

Syntax Description

filename	Filename of the certificate.

Usage Guidelines

You must first copy the certificate file into any folder (on the Cisco Unified Computing System (Cisco UCS)) that the **dnasadmin** user can access, before running the command.

```
[cmxadmin@connector ~]$ connectorctl setproxycert cert.pem
New cert exists.
Restarting connector container ...
Connector container was restarted.
setProxyCert successful.
```

connectorctl validatecert

This command validates a certificate signed by a Certification Authority (CA).

connectorctl validatecert *{ CA_certificate | root_certificate }*

Syntax Description

CA_certificate	CA certificate.
root_certificate	Root certificate

Examples

The following is a sample output of the command:

```
[cmxadmin@cmxnew ~]$ connectorctl validatecert 10.22.244.80.cert.pem
root-cal-ca2-chain.cert.pem

Validating certificate
root-cal-ca2-chain.cert.pem amd 10.22.244.80.cert.pern exists

Validation of server certificate is successful

[cmxadmin@cmxnew ~]$
```

connectorctl importcacert

This command imports a signed certificate to the accurate location on the connector and ensures the security of the connection with the connector.

The **connectorctl createcsr** creates a certificate which you must get signed by a Certification Authority (CA). You can validate this signed certificate with the **connectorctl validatecert** command. You can use the **connectorctl importcacert** command to import the signed certificate. This step also removes the "Your connection is not private" message that is displayed when trying to log in to the connector GUI.

connectorctl importcacert *certificate*

Syntax Description

certificate	Signed and validated certificate.

Command History

Release 2.2	This command is introduced.

Examples

The following is a sample output of the command:

```
[cmxadminÇcmxnew ~]$ connectorctl importcacert 10.x.x.x.cert.pem
Importing CA certificate
10.x.x.x.cert.pem exists

Certificate Imported Successfully!
Restarting HAProxy...
HA Proxy restarted successfully!
CA certificate import process executed successfully
```

Usage Guidelines

With CSCvy62400, you may find that you are unable to import a certificate by a third-party CA or a device certificate. In such a case, the certificate may get imported with a few errors and result in the termination of GUI. The following output is displayed.

```
[dnasadmin@dnasc-1 ~]$ connectorctl importcacert 20210609-063645839_Roche_G3_Root_CA.pem
Importing CA certificate.....
20210609-063645839_Roche_G3_Root_CA.pem exists
Certificate Imported Successfully!
Restarting HAProxy...
Job for haproxy.service failed because the control process exited with error code. See
"systemctl status haproxy.service" and "journalctl -xe" for details.
HAProxy restarted successfully!
CA certificate import process executed successfully

[dnasadmin@dnasc-1 ~]$ su -
Password:
Last login: Wed Jun  9 13:10:35 CDT 2021 on pts/0
```

You can resolve this issue by regenerating a selfsigned certificate using the **connectorctl generatecert** command. This step removes any problems that are associated with incompatible certificate formats.

Related Topics

connectorctl validatecert, on page 27

connectorctl createcsr, on page 24
connectorctl cert generate, on page 20

connectorctl exportcacert

This command exports a signed certificate from the connector to the location `/etc/ssl/private/` and ensures the security of the connection with the connector.

connectorctl exportcacert

Command History

Release 2.2	This command is introduced.

Examples

The following is a sample output of the command:

```
[cmxadminÇcmxnew ~]$ connectorctl exportcacert
CA certificate is exported successfully into /etc/ssl/private/ca-cert.pem
```

connectorctl dockersubnet

By default, the connector's docker container is assigned an IP address in the 172.17.0.0/16 subnet. If the subnet overlaps with your address space, you can use the **connectorctl dockersubnet** command to add or remove the docker subnet.

connectorctl dockersubnet

Examples

The following is a sample output of the command:

```
[cmxadminQcmxnew ~]$ connectorctl dockersubnet
Do you want to add or remove the subnet? [Insert a to add, r to remove] [a]: a

Please insert the Netmask IP: 10.22.244.1
Please insert CIDR [1-32] [16]:
Successfully changed the docker subnet
[cmxadminpcmxnew ~]$
```

PART IV

Timezone Commands

Timezone Commands

connectorctl checktimezone

This command displays details of the configured time zone.

Parameters

None

connectorctl checktimezone

Usage Guidelines

```
[cmxadmin@cmxnew ~]$ connectorctl checktimezone
      Local time: Wed 2020-02-19 04:02:02 UTC
  Universal time: Wed 2020-02-19 04:02:02 UTC
        RTC time: Wed 2020-02-19 04:02:02
       Time zone: UTC (UTC, +0000)
     NTP enabled: no
NTP synchronized: yes
 RTC in local TZ: yes
      DST active: n/a

Warning: The system is configured to read the RTC time in the local time zone.
         This mode can not be fully supported. It will create various problems
         with time zone changes and daylight saving time adjustments. The RTC
         time is never updated, it relies on external facilities to maintain it.
         If at all possible, use RTC in UTC by calling
         'timedatectl set-local-rtc 0'.
```

connectorctl listtimezone

This command lists all available time zones.

Parameters

None.

```
connectorctl listtimezone
```

Usage Guidelines

```
[cmxadmin@cmxnew ~]$ connectorctl listtimezone
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
...
...
UTC
```

connectorctl changetimezone

This command allows you to change the time zone to one of the available ones.

Parameters

None.

connectorctl validatecert *CA_certificate root_certificate*

Usage Guidelines

```
[cmxadmin@cmxnew ~]$ connectorctl changetimezone
...
Pacific/Saipan
Pacific/Tahiti
Pacific/Tarawa
Pacific/Tongatapu
Pacific/Wake
Pacific/Wallis
UTC

Please enter a timezone from the above list:: Pacific/Tahiti
Restarting services....
Timezone was successfully set!
      Local time: Tue 2020-02-18 18:11:43 -10
  Universal time: Wed 2020-02-19 04:11:43 UTC
        RTC time: Tue 2020-02-18 18:11:43
       Time zone: Pacific/Tahiti (-10, -1000)
     NTP enabled: no
NTP synchronized: yes
 RTC in local TZ: yes
      DST active: n/a

Warning: The system is configured to read the RTC time in the local time zone.
         This mode can not be fully supported. It will create various problems
         with time zone changes and daylight saving time adjustments. The RTC
         time is never updated, it relies on external facilities to maintain it.
         If at all possible, use RTC in UTC by calling
         'timedatectl set-local-rtc 0'.
```

Related Topics

connectorctl checktimezone, on page 36
connectorctl listtimezone, on page 37

PART V

NTP Commands

NTP Commands

The NTP commands are not supported on connector AMI.

connectorctl ntprestrict

This command restricts an IP address from accessing the Network Time Protocol (NTP) server.

Parameters

IP address

connectorctl ntprestrict *ipaddress*

Usage Guidelines

```
[cmxadmin@connector ~]$ connectorctl ntprestrict 10.22.244.34
```

Related Topics

connectorctl ntpunrestrict, on page 43

connectorctl ntpunrestrict

This command removes any Network Time Protocol (NTP) server access restriction on an IP address.

Parameters

IP address

connectorctl ntpunrestrict *ipaddress*

Usage Guidelines

```
[cmxadmin@connector ~]$ connectorctl ntpunrestrict 10.22.244.34
```

connectorctl ntpconfig

This command adds, edits, removes, or displays the Network Time Protocol (NTP) server.

Parameters

None

connectorctl ntpconfig

Usage Guidelines

The following is the sample command output for the **Show NTP Server Details (Press 4)** option when an NTP server is not configured.

```
[cmxadmin@cmxnew-01 ~]$ connectorctl ntpconfig

[Please select an option from the list above: (Default value is 4) [5]: 4
• ntpd.service - Network Time Service
Loaded: loaded (/usr/lib/systemd/system/ntpd.service ; disabled; vendor preset: disabled)

Active: inactive (dead)
```

The following is the sample command output for the **Show NTP Server Details (Press 4)** option when an NTP server is configured.

```
Please select an option from the list above: (Default value is 5) [5]: 4
● ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2020-02-17 19:50:05 -10; 1 day 7h ago
 Main PID: 675 (ntpd)
   Memory: 4.7M
   CGroup: /system.slice/ntpd.service
           └─675 /usr/sbin/ntpd -u ntp:ntp -g

Feb 18 18:11:45 cmxnew-01 ntpd[675]: new interface(s) found: waking up resolver
Feb 18 18:53:36 cmxnew-01 ntpd[675]: Deleting interface #10 veth438ff12,
fe80::607a:10ff:fe0f:1145#123, interface stats: received=0, sent=0, dropped=0,
active_time=2511 secs
Feb 18 18:53:38 cmxnew-01 ntpd[675]: Listen normally on 11 veth660497a
fe80::3836:acff:fe0c:c279 UDP 123
Feb 18 18:53:38 cmxnew-01 ntpd[675]: new interface(s) found: waking up resolver
Feb 18 20:35:06 cmxnew-01 ntpd[675]: Deleting interface #11 veth660497a,
fe80::3836:acff:fe0c:c279#123, interface stats: received=0, sent=0, dropped=0,
active_time=6088 secs
Feb 18 20:35:10 cmxnew-01 ntpd[675]: Listen normally on 12 vethb301b1d
fe80::d0a9:e5ff:fef2:8223 UDP 123
Feb 18 20:35:10 cmxnew-01 ntpd[675]: new interface(s) found: waking up resolver
Feb 18 20:35:15 cmxnew-01 ntpd[675]: Listen normally on 13 veth7636c9b
fe80::40a7:e2ff:fed9:d5a3 UDP 123
Feb 18 20:35:15 cmxnew-01 ntpd[675]: Deleting interface #12 vethb301b1d,
fe80::d0a9:e5ff:fef2:8223#123, interface stats: received=0, sent=0, dropped=0, active_time=5
 secs
Feb 18 20:35:15 cmxnew-01 ntpd[675]: new interface(s) found: waking up resolver

===============================================================================
     remote           refid      st t when poll reach   delay   offset  jitter
===============================================================================
*172.22.38.66    .GNSS.           1 u  880 1024  377    2.090   -0.092   0.159

===============================================================================
```

The following is the sample command output for the **Add NTP Server Details (Press 1)** option when no NTP server has been configured.

```
[cmxadmin@ccmxnew-01 ~]$ connectorctl ntpconfig
...
Configure NTP
[Please enter the NTP server name (blank for no NTP server): 1.ntp.esl.test.co
10 Feb 22:07:28 ntpdate[18062]: step time server 172.22.38.65 offset 17.924716 sec
NTP setup finishe
New NTP Change
1.ntp.esl.test.com
```

The following is the sample command output for the **Add NTP Server Details (Press 1)** option when one NTP server has already been configured. The NTP servers that are already added are first displayed for your reference.

```
[cmxadmin@cmxnew-01 ~]$ connectorctl ntpconfig
...
[Please select an option from the list above: (Default value is 4) [5]: 1

Added NTP Servers:
1.ntp.esl.test.com
[Please enter the NTP Server: 2.ntp.esl.test.com
Adding NTP Server: 2.ntp.esl.test.com
[Confirm the above details? [y/n] [n]: y
10 Feb 22:32:13 ntpdate[19105]: adjust time server 172.22.38.66 offset 0.099035 sec
Restarting the NTP Service
NTP Service restarted successfully!
New NTP Changes
1. ntp.esl.test.com
2. ntp.esl.test.com
```

The following is the sample command output for the **Edit NTP Server Details (Press 2)** option. The NTP servers that are already added are first displayed for your reference.

```
Please select an option from the list above: (Default value is 4) [5]: 2

Available NTP Servers:
2.ntp.esl.test.com
1. server 2.ntp.esl.test.com Press 1

Which NTP Server would you like to edit? [1]: 1
Please enter the new NTP Server : 1.ntp.esl.test.com
New NTP Server: 1.ntp.esl.test.com
Confirm the above details? [y/nl [n]: y
10 Feb 23:38:53 ntpdate[21024]: adjust time server 172.22.38.65 offset 0.002521 sec
Restarting the NTP Service
NTP Service restarted successfully!
New NTP Changes
1.ntp.esl.test.com
```

The following is the sample command output for the **Remove NTP Server Details (Press 3)** option.

```
Please select an option from the list above: (Default value is 4) [5]: 3
Available NTP Servers:
1. ntp.esl.test.com
2. ntp.esl.test.com
1. server 1.ntp.esl.test.com.    Press 1
2. server 2.ntp.esl.test.com     Press 2
```

```
Which NTP Server would you like to remove?

Removing NTP Server: 2.ntp.esl.test.com

Confirm the above details? [y/n] [n]: y

Successfully removed the NTP
Restarting the NTP Service
NTP Service restarted successfully!
New NTP Changes
1.ntp.esl.test.com
```

PART VI

AAA Commands

AAA Commands

connectorctl aaa show

This command shows the AAA configuration made on Cisco Spaces: Connector.

Parameters

None.

connectorctl aaa show

Usage Guidelines

The following sample displays the output when AAA server is configured without IPSec.

```
[cmxadmin@connector-01 ~]$ connectorctl aaa show
------------------------------------------------------------
AAA Server is Enabled
AAA Server IP: 10.22.244.114
AAA Server Port: 1812
Shared Secret: **<<masked>>**

IPSec is Disabled
Connection to AAA Server Successful. AAA Settings are correct.
.
------------------------------------------------------------------
```

connectorctl aaa edit

This command edits an existing Authentication, Authorization, and Accounting (AAA) configuration on Cisco Spaces: Connector.

Parameters

Parameter	Description
Do you want to CHANGE AAA Server settings	Choose to change the existing AAA configurations.
Enter AAA Server Host IP	IP address of the AAA server.
Enter AAA Server Port	Port used to connect to the AAA server. Default value is 1812.
Enter AAA Server's shared secret key	Shared secret key used to connect to the AAA server.
Do you want to enable IPSec?	Choose to enable or disable IPSec. If you chose to disable IPSec, the connection established to the external AAA server is un-encrypted and over UDP.
Enter AAA Server's DNS name	Domain Name Server (DNS) name of the AAA server.
Select IPSec Auth Type: (pubkey/psk)	Choose between two types of IPSec Authentication, namely **pubkey** or **PSK**.
Do you want to auto-generate ('a') OR provide ('p') PSK from Radius Server ?	• a: Choose to auto-generate the PSK. • p: Choose to provide PSK configured on the AAA server.
Enter PSK from Radius Server	Enter a PSK value existing on the AAA server.

connectorctl aaa edit

Usage Guidelines

The following sample output has both AAA and Internet Protocol Security (IPSec) enabled. IPSec is enabled with pre-shared key (PSK). Choosing the provide option allows you to specify a PSK that is available on the AAA server.

```
[cmxadmin@connector-01 ~]$ connectorctl aaa edit
------------------------------------------------------------
Do you want to CHANGE AAA Server settings? [yes/no] [yes]:
Enter AAA Server Host IP  [10.22.244.114]:
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [y]:
Enter AAA Server's DNS name  [aaa-srv-01]:
Select IPSec Auth Type: (pubkey/psk) [pubkey]: psk
Do you want to auto-generate ('a') OR provide ('p') PSK from Radius Server ? [a]: p
Enter PSK from Radius Server : 7dBoZXAkhadFMsyJ8e9HsBxdajnUPcxS

AAA Server configured successfully
```

```
Connection to AAA Server Successful. AAA Settings are correct.
IPSec is Enabled
IPSec Status:
Security Associations (1 up, 0 connecting):
         aaa[1]: ESTABLISHED 1 second ago,
10.22.244.100[connector-01]...10.22.244.114[aaa-srv-01]
         aaa{1}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c59d3960_i cf338432_o
         aaa{1}:   10.22.244.100/32 === 10.22.244.114/32
         aaa{2}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c75d414b_i c7e495e2_o
         aaa{2}:   10.22.244.100/32 === 10.22.244.114/32
.
------------------------------------------------------------
```

The folllowing sample output has both AAA and Internet Protocol Security (IPSec) enabled. IPSec is enabled with a pre-shared key (PSK). Choosing the auto-generate option allows you to specify a PSK that is available on the AAA server.

```
[cmxadmin@connector-01 ~]$ connectorctl aaa edit
Do you want to CHANGE AAA Server settings? [yes/no] [yes]:
Enter AAA Server Host IP  [10.22.244.114]:
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [y]:
Enter AAA Server's DNS name  [aaa-srv-01]:
Select IPSec Auth Type: (pubkey/psk) [psk]:
Do you want to auto-generate ('a') OR provide ('p') PSK from Radius Server ? [a]: a
Generated PSK value = 3AhBgueQQ6YBkKMwqIr6jyxIuG9ekw8g

AAA Server configured successfully
Connection to AAA Server Successful. AAA Settings are correct.
IPSec is Enabled
IPSec Status:
Security Associations (0 up, 0 connecting):
  no match
```

The auto-generated PSK value is displayed in the output. While IPSec is enabled, the IPSec tunnel may not be established immediately as indicated by the following section of the output.

```
IPSec Status:
Security Associations (0 up, 0 connecting):
  no match
```

You can use the **connectorctl aaa show** command after a few minutes to check if the IPSec tunnel has been established. You can compare the PSK values in both outputs and verify that they are the same.

```
[cmxadmin@connector-01 ~]$ connectorctl aaa show
AAA Server is Enabled
AAA Server IP: 10.22.244.114
AAA Server Port: 1812
Shared Secret: **<<masked>>**

IPSec is Enabled
AAA Server DNS: aaa-srv-01
IPSec Auth type: psk
IPSec PSK: 3AhBgueQQ6YBkKMwqIr6jyxIuG9ekw8g
IPSec Status:
Security Associations (1 up, 0 connecting):
         aaa[3]: ESTABLISHED 20 seconds ago,
10.22.244.100[connector-01]...10.22.244.114[aaa-srv-01]
         aaa{3}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: ca4688d1_i c24be7d9_o
         aaa{3}:   10.22.244.100/32 === 10.22.244.114/32

Connection to AAA Server Successful. AAA Settings are correct.
```

Related Topics

connectorctl aaa show, on page 50
connector aaa restart, on page 57
connectorctl aaa disable, on page 56
connectorctl aaa edit, on page 51
connectorctl aaa enable, on page 54

connectorctl aaa enable

This command configures and enables authentication using a Authentication, Authorization, and Accounting (AAA) server. You can choose to enable the Internet Protocol Security (IPSec) protocol. Two types of IPSec protocols are supported, namely pubkey and PSK.

If you chose to disable IPSec, the connection established to the external AAA server is un-encrypted and over UDP.

Parameters

Parameter	Description
Do you want to configure a AAA server.	Choose to configure a AAA server.
Enter AAA Server Host IP	IP address of the AAA server.
Enter AAA Server Port	Port used to connect to the AAA server. Default value is 1812.
Enter AAA Server's shared secret key	Shared secret key used to connect to the AAA server.
Do you want to enable IPSec?	Choose to enable or disable IPSec. If you chose to disable IPSec, the connection established to the external AAA server is un-encrypted and over UDP.
Enter AAA Server's DNS name	Domain Name Server (DNS) name of the AAA server.
Select IPSec Auth Type: (pubkey/psk)	Choose between two types of IPSec Authentication, namely **pubkey** or **PSK**.
Do you want to auto-generate ('a') OR provide ('p') PSK from Radius Server ?	• a: Choose to auto-generate the PSK. • p: Choose to provide the PSK configured on the AAA server.
Enter PSK from Radius Server	Enter the name of the existing PSK on the AAA server.

connectorctl aaa enable

Usage Guidelines

The following sample output shows a AAA server enabled without IPSec security protocol.

```
[cmxadmin@connector-01 ~]$ connectorctl aaa enable
------------------------------------------------------------
Do you want to configure AAA Server? [yes/no] [yes]:
Enter AAA Server Host IP : 10.22.244.114
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [n]:

AAA Server configured successfully
```

```
Connection to AAA Server Successful. AAA Settings are correct.
----------------------------------------------------------------
```

The following sample output shows a AAA server enabled with IPSec security protocol.

```
[cmxadmin@connector-01 ~]$ connectorctl aaa enable
------------------------------------------------------------
Do you want to configure AAA Server? [yes/no] [yes]:
Enter AAA Server Host IP : 10.22.244.114
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [n]: y
Enter AAA Server's DNS name : aaa-srv-01
Select IPSec Auth Type: (pubkey/psk) [pubkey]:
AAA Server's CA Certificate file : radiusca.pem

Connection to AAA Server Successful. AAA Settings are correct.

IPSec is Enabled
IPSec Status:
Security Associations (1 up, 0 connecting):
         aaa[1]: ESTABLISHED 0 seconds ago,
10.30.114.46[10.30.114.46]...10.22.244.114[aaa-srv-01]
         aaa{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: ca07f0e2_i cd4dcf30_o
         aaa{1}:   10.30.114.46/32 === 10.22.244.114/32

Restarting cmx-agent ...  Done
AAA Server configured successfully
Please wait for 2 minutes to login to the UI.
----------------------------------------------------------------
```

Related Topics

connectorctl aaa show, on page 50
connectorctl aaa disable, on page 56
connectorctl aaa edit, on page 51
connector aaa restart, on page 57
connectorctl aaa enable, on page 54

connectorctl aaa disable

This command disables the Authentication, Authorization, and Accounting (AAA) configurations as well any Internet Protocol Security (IPSec) configurations on Cisco Spaces: Connector.

Parameters

None.

connectorctl aaa disable

Usage Guidelines

The following sample is the command output when both Authentication, Authorization, and Accounting (AAA) and Internet Protocol Security (IPSec) are enabled. The **connectorctl aaa disable** command disables both protocols.

```
[cmxadmin@cmxkeyhashlll ~]$ connectorctl aaa disable
------------------------------------------------------------
Do you want to disable AAA Server? [yes/no] [yes]:
IPSec tunnel disabled
AAA Server is Disabled
------------------------------------------------------------------
```

The following sample is the command output when only AAA is enabled without IPSec.

```
[cmxadmin@cmxkeyhashlll ~]$ connectorctl aaa disable
------------------------------------------------------------
Do you want to disable AAA Server? [yes/no] [yes]:
AAA Server is Disabled
------------------------------------------------------------------
```

connector aaa restart

This command restarts the IP Security tunnel established from the Cisco Spaces: Connector to the existing Authentication, Authorization, and Accounting (AAA) server.

Parameters

None

connectorctl aaa restart

Usage Guidelines

When AAA is disabled, the **connectorctl aaa restart** command displays the following sample output.

```
[dnasadmin@cisco-dna-spaces-connector-7 ~]$ connectorctl aaa restart
Error: Cannot restart IPSec tunnel as AAA is disabled.
```

When AAA is enabled but IPSec is disabled, the **connectorctl aaa restart** command displays the following sample output.

```
[dnasadmin@cisco-dna-spaces-connector-7 ~]$ connectorctl aaa restart
Error: Cannot restart IPSec tunnel as IPSec is disabled.
```

When AAA and IPSec are both enabled, the **connectorctl aaa restart** command displays the following sample output.

```
[dnasadmin@cisco-dna-spaces-connector-7 ~]$ connectorctl aaa restart
Restarted IPSec tunnel

IPSec Status:
Security Associations (1 up, 0 connecting):
         aaa[1]: ESTABLISHED 0 seconds ago,
10.30.114.46[cisco-dna-spaces-connector-7]...10.22.244.114[aaa-srv-01]
         aaa{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c32e5888_i c9e2ab84_o
         aaa{1}:   10.30.114.46/32 === 10.22.244.114/32
```

Related Topics

connectorctl aaa show, on page 50

PART VII

Debug Commands

Debug Commands

connectorctl enabledebug

This command enables the debug mode for the Cisco Spaces: Connector.

Parameters

None.

connectorctl enabledebug

Usage Guidelines

```
[cmxadmin@cmxnew ~]$ connectorctl enabledebug
Please enter a Valid MAC Address [Format: xx:xx:xx:xx:xx:xx]: 00:0c:xx:xx:xx:xx
Please choose a debug level [Default: MESSAGE] [MESSAGE]:
Debug enabled successfully: MESSAGE$
```

Related Topics

connectorctl viewdebuglogs, on page 63
connectorctl disabledebug, on page 64

connectorctl viewdebuglogs

This command displays the debugs logs.

Parameters

None.

connectorctl viewdebuglogs

Usage Guidelines

```
[cmxadminQcmxadmin ~]$ connectorctl viewdebuglogs
Please enter the mac address:: 00:0c:xx:xx:xx:xx
2019-11-21 23:15:55 [nioEventLoopGroup-6-1] INFO com.cisco.cmx.nmsp.protomapping.MappingEngine
 - tenantId: "427"
macAddress: "00: 0c :xx: xx: xx : xx"
controllerIpAddress: "10.22.244.28"
messageId: 15
measurementNotification {
    tenantId: "427"
    tenantId: "427"
    macAddress: "00:0c:xx:xx:xx:xx"
    controllerIpAddress: "10.22.244.28"
    deviceCategory {
        deviceClass: TAGS_2
    }
    transmitPower {
        value: 19
    }
    apRssiMeasurements {
        entries {
            apMacAddress: "08 :cc: xx : xx : xx :xx"
            rssi: -29
            timestamp: 278
```

connectorctl disabledebug

This command disables the debug mode for the Cisco Spaces: Connector.

Parameters

None.

connectorctl disabledebug

Usage Guidelines

```
[cmxadmin@cmxnew ~]$ connectorctl disabledebug
Please enter a Valid MAC Address [Format: xx:xx:xx:xx:xx:xx]: 00:0c:xx:xx:xx:xx
Please choose a debug level [Default: MESSAGE] [MESSAGE]:
Debug disabled successfully: MESSAGE$
```

PART VIII

Services Commands

Services Commands

connectorctl service restart

This command restarts all the Cisco Spaces: Connector services. To enable debug logs, use the -l keyword is specified.

connectorctl service restart **-s** *service-name* [**-l** *debug-level* [**-d** *debug-period-in-minutes*]]

Syntax Description

Keyword and Variable	Description
-s *service-name*	Configure the service that needs to be restarted.
-l *debug-level*	(Optional) Configure the debug level. Values are DEBUG, INFO, and WARNING. • If *debug-level* is unspecified, the default value is DEBUG. **Note** Running the service at DEBUG log level would significantly impact performance
-d *debug-period-in-minutes*	(Optional) Specify the debug period in minutes. If unspecified, the default value is 10 minutes. • If **-l** is unspecified, service is restarted but debugging is not logged.

Command History

Release 3	This command is introduced.

Examples

You can also restart a specified service. The following is a sample output of the command:

```
$[spacesadmin@connector ~]$ connectorctl service restart -s location -l DEBUG
Executing command:service
Command execution status: Success

Status:Successfully started location
```

Related Topics

connectorctl servicestatus, on page 69

connectorctl servicestatus

This command displays the status of all the services running on the Cisco Spaces: Connector.

Parameters

None.

connectorctl servicestatus

Usage Guidelines

```
[cmxadmin@cmxnew ~]$ connectorctl servicestatus
================================================================================================================
Docker Downloaded Images
================================================================================================================

REPOSITORY                                TAG                 IMAGE ID            CREATED
         SIZE
connector.dev-dnaspaces.io/connector   v2.0.226            3e961019b481        30 hours ago
        837MB
codekoala/pypi                            latest              9d1395575eb8        2 years ago
         59.7MB


================================================================================================================
Docker Running Containers
================================================================================================================

CONTAINER ID        IMAGE                                                COMMAND
CREATED             STATUS              PORTS
                                                                                                  NAMES
713a1fed5f06        connector.dev-dnaspaces.io/connector:v2.0.226   "./entrypoint.sh"   19
 hours ago        Up 10 minutes       0.0.0.0:8002-8003->8002-8003/tcp,
0.0.0.0:2003->2003/udp, 0.0.0.0:8186->8186/tcp, 127.0.0.1:8185->8185/tcp,
0.0.0.0:8004->25103/tcp   connector


================================================================================================================
Docker Service Status
================================================================================================================

● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; vendor preset: disabled)

   Active: active (running) since Tue 2020-02-18 18:53:35 -10; 10min ago
     Docs: https://docs.docker.com
 Main PID: 29575 (dockerd)
   Memory: 55.9M
   CGroup: /system.slice/docker.service
           ├─29575 /usr/bin/dockerd
           ├─29582 docker-containerd --config /var/run/docker/containerd/containerd.toml
           └─29739 docker-containerd-shim -namespace moby -workdir
/var/lib/docker/containerd/daemon/io.containerd.runtime.v1.linux/moby/713a1fed5f06283b48771e699ca6082b3b7a39ceeb8f28776aae97b914c78afa
 -address /var/run/docker/containerd/docker-containerd.sock -containerd-binary
/usr/bin/docker-containerd -runtime-root /var/run/docker/runtime-runc

Feb 18 18:53:33 cmxnew dockerd[29575]: time="2020-02-18T18:53:33.454920975-10:00" level=info
 msg="pickfirstBalancer: HandleSubConnStateChange: 0xc4204074f0, READY" module=grpc
Feb 18 18:53:33 cmxnew dockerd[29575]: time="2020-02-18T18:53:33.454943957-10:00" level=info
 msg="Loading containers: start."
Feb 18 18:53:34 cmxnew dockerd[29575]: time="2020-02-18T18:53:34.198905851-10:00" level=info
```

```
 msg="Default bridge (docker0) is assigned with an IP address 172.17.0.0/16. Daemon option
 --bip can be used to set a preferred IP address"
Feb 18 18:53:35 cmxnew dockerd[29575]: time="2020-02-18T18:53:35-10:00" level=info msg="shim
 docker-containerd-shim started"
address="/containerd-shim/moby/713a1fed5f06283b48771e699ca6082b3b7a39ceeb8f28776aae97b914c78afa/shim.sock"
 debug=false pid=29739
Feb 18 18:53:35 cmxnew dockerd[29575]: time="2020-02-18T18:53:35.313599290-10:00" level=info
 msg="Loading containers: done."
Feb 18 18:53:35 cmxnew dockerd[29575]: time="2020-02-18T18:53:35.446434997-10:00" level=info
 msg="Docker daemon" commit=e68fc7a graphdriver(s)=overlay2 version=18.06.1-ce
Feb 18 18:53:35 cmxnew dockerd[29575]: time="2020-02-18T18:53:35.446524264-10:00" level=info
 msg="Daemon has completed initialization"
Feb 18 18:53:35 cmxnew dockerd[29575]: time="2020-02-18T18:53:35.463099648-10:00"
level=warning msg="Could not register builder git source: failed to find git binary: exec:
 \"git\": executable file not found in $PATH"
Feb 18 18:53:35 cmxnew dockerd[29575]: time="2020-02-18T18:53:35.480241781-10:00" level=info
 msg="API listen on /var/run/docker.sock"
Feb 18 18:53:35 cmxnew systemd[1]: Started Docker Application Container Engine.


================================================================================================
HAProxy Service Status
================================================================================================

● haproxy.service - HAProxy Load Balancer
   Loaded: loaded (/usr/lib/systemd/system/haproxy.service; enabled; vendor preset: disabled)

   Active: active (running) since Tue 2020-02-18 18:53:35 -10; 10min ago
  Process: 29815 ExecStartPre=/usr/sbin/haproxy -f $CONFIG -c -q (code=exited,
status=0/SUCCESS)
 Main PID: 29817 (haproxy)
   Memory: 7.7M
   CGroup: /system.slice/haproxy.service
           ├─29817 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -p /run/haproxy.pid
           └─29820 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -p /run/haproxy.pid

Feb 18 18:53:35 cmxnew haproxy[29817]: [WARNING] 048/185335 (29817) : config : log format
ignored for frontend 'https' since it has no log address.
Feb 18 18:53:35 cmxnew haproxy[29817]: [WARNING] 048/185335 (29817) : config : log format
ignored for frontend 'grpchttps' since it has no log address.
Feb 18 18:53:35 cmxnew haproxy[29817]: [NOTICE] 048/185335 (29817) : New worker #1 (29820)
 forked
Feb 18 18:53:35 cmxnew systemd[1]: Started HAProxy Load Balancer.
Feb 18 18:53:35 cmxnew haproxy[29817]: [WARNING] 048/185335 (29820) : Server
grpcserver/grpcserver is DOWN, reason: Layer4 connection problem, info: "Connection refused",
 check duration: 0ms. 0 active and 0 backup servers left. 0 sessions active, 0 requeued, 0
 remaining in queue.
Feb 18 18:53:35 cmxnew haproxy[29817]: [ALERT] 048/185335 (29820) : backend 'grpcserver'
has no server available!
Feb 18 18:53:36 cmxnew haproxy[29817]: [WARNING] 048/185336 (29820) : Server dsapapi/dsapapi
 is DOWN, reason: Layer4 connection problem, info: "Connection refused", check duration:
0ms. 0 active and 0 backup servers left. 0 sessions active, 0 requeued, 0 remaining in
queue.
Feb 18 18:53:36 cmxnew haproxy[29817]: [ALERT] 048/185336 (29820) : backend 'dsapapi' has
no server available!
Feb 18 18:53:36 cmxnew haproxy[29817]: [WARNING] 048/185336 (29820) : Server firehose/firehose
 is DOWN, reason: Layer4 connection problem, info: "Connection refused", check duration:
0ms. 0 active and 0 backup servers left. 0 sessions active, 0 requeued, 0 remaining in
queue.
Feb 18 18:53:36 cmxnew haproxy[29817]: [ALERT] 048/185336 (29820) : backend 'firehose' has
 no server available!


================================================================================================
```

```
NGINX Service Status
================================================================================================================

● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)

   Active: active (running) since Tue 2020-02-18 18:53:35 -10; 10min ago
  Process: 29836 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
  Process: 29832 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
  Process: 29831 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)

 Main PID: 29839 (nginx)
   Memory: 2.1M
   CGroup: /system.slice/nginx.service
           ├─29839 nginx: master process /usr/sbin/nginx
           └─29840 nginx: worker process

Feb 18 18:53:35 cmxnew systemd[1]: Starting The nginx HTTP and reverse proxy server...
Feb 18 18:53:35 cmxnew nginx[29832]: nginx: the configuration file /etc/nginx/nginx.conf
syntax is ok
Feb 18 18:53:35 cmxnew nginx[29832]: nginx: configuration file /etc/nginx/nginx.conf test
is successful
Feb 18 18:53:35 cmxnew systemd[1]: Started The nginx HTTP and reverse proxy server.


================================================================================================================
Connector Agent Service Status
================================================================================================================

● cmx-agent.service - uWSGI instance to serve dna-spaces-agent
   Loaded: loaded (/etc/systemd/system/cmx-agent.service; enabled; vendor preset: disabled)

   Active: active (running) since Tue 2020-02-18 18:53:21 -10; 10min ago
 Main PID: 29480 (uwsgi)
   Memory: 35.4M
   CGroup: /system.slice/cmx-agent.service
           ├─29480 /usr/bin/uwsgi --ini agent_wsgi.ini
           └─29497 /usr/bin/uwsgi --ini agent_wsgi.ini

Feb 18 18:53:21 cmxnew systemd[1]: Started uWSGI instance to serve dna-spaces-agent.
Feb 18 18:53:21 cmxnew systemd[1]: Starting uWSGI instance to serve dna-spaces-agent...
Feb 18 18:53:21 cmxnew uwsgi[29480]: [uWSGI] getting INI configuration from agent_wsgi.ini
```

Related Topics

connectorctl service restart, on page 68

PART IX

Syslog Commands

Syslog Commands

connectorctl rsyslogconfig restart

This command restarts the remote syslog server.

connectorctl rsyslogconfig restart

Command History

Release 2.3.2	This command is introduced.

Examples

The following is a sample output of the command:

```
[dnasadmin@conn171 ~]$ connectorctl rsyslogconfig restart
Do you want to restart the rsyslog service? (yes/no)  [yes]: yes
rsyslog service restarted successfully
```

connectorctl rsyslogconfig

This command displays the remote syslog server configurations. The command also allows you to update the configurations.

connectorctl rsyslogconfig

Command History

Release 2.3.2	This command is introduced.

Examples

The following is a sample output of the command:

```
[dnasadmin@conn171 ~]$ connectorctl rsyslogconfig
Rsyslog Enabled = yes
Rsyslog Protocol = TLS
Rsyslog IP = 172.19.28.161
Rsyslog PORT = 4514
Rsyslog SAN = cisco-cmx-ova-81
Do you want to update the configuration? (yes/no)  [yes]: yes
Enable Rsyslog feature ?  [yes]: ]
Error: invalid choice: ]. (choose from yes, no)
Enable Rsyslog feature ?  [yes]:
Please select Protocol (TCP/TLS/UDP)  [TLS]:
Please enter Rsyslog IP [172.19.28.161]:
Please enter Rsyslog PORT [4514]:
Please enter Rsyslog Server SAN [cisco-cmx-ova-81]:
Do you want to replace existing Rsyslog CA Certificate? (y/n) [n]: y
Please enter Rsyslog Server CA File: /etc/ssl/private/ca-cert.pem
Do you want to confirm ? (y/n)  [n]: y
Rsyslog configuration saved.
rsyslog service restarted successfully.
```

PART X

Cloud Connectivity Commands

Cloud Connectivity Commands

connectorctl testconnectivity

This command tests the connectivity from the connector to the Cisco Spaces hosted on the U.S. or the EU cloud. The command prints the output of the **curl** output in detail.

Command History

Release 2.3.2	This command is introduced.

Examples

The following is a sample output of the command:

```
[dnasadmin@conn171 ~]$ connectorctl testconnectivity
This utility tests connectivity to DNASpaces Cloud.
Choose a DNASpaces Cloud region [US / EU] [US]: US
Performing connectivity test, this may take up to 10 seconds...
```

```
Testing connectivity to https://connector.dnaspaces.io, Using proxy http://a.b.c.d:e
--------------------------------------------------------------------------------------------------------------
* About to connect() to proxy a.b.c.d port 80 (#0)
*   Trying a.b.c.d...
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0* Connected
to a.b.c.d (a.b.c.d) port 80 (#0)
* Establish HTTP proxy tunnel to connector.dnaspaces.io:443
> CONNECT connector.dnaspaces.io:443 HTTP/1.1
> Host: connector.dnaspaces.io:443
> User-Agent: curl/7.29.0
> Proxy-Connection: Keep-Alive
>
< HTTP/1.1 200 Connection established
<
* Proxy replied OK to CONNECT request
* Initializing NSS with certpath: sql:/etc/pki/nssdb
*   CAfile: /etc/pki/tls/certs/ca-bundle.crt
  CApath: none
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0* SSL connection
 using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate:
*    subject: CN=connector.dnaspaces.io,O="Cisco Systems, Inc.",L=San Jose,ST=California,C=US
*     start date: Sep 19 03:31:46 2019 GMT
*     expire date: Sep 19 03:41:00 2021 GMT
*     common name: connector.dnaspaces.io
*     issuer: CN=HydrantID SSL ICA G2,O=HydrantID (Avalanche Cloud Corporation),C=US
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: connector.dnaspaces.io
> Accept: */*
>
< HTTP/1.1 200 OK
< content-length: 0
<
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
* Connection #0 to host a.b.c.d left intact
https://connector.dnaspaces.io/ | Status code: 200 | local_ip: 10.f.g.e | lookuptime: 0.000
 | time_connect: 0.005 | time_toal: 0.466 .
```

PART XI

Miscellaneous Commands

Miscellaneous Commands

connectorctl techsupport

This command gathers and displays technical support information. The command creates a TAR file with information about the network, system, running docker containers, and downloaded images.

connectorctl techsupport

Syntax Description

This command has no keywords or arguments.

Examples

```
[spacesadmin@connector ~]$ connectorctl techsupport
Executing command:techsupport
Command execution status:Success
-----------------------
##################################################################################################
DNA Spaces Connector 3.0 Tech Support Started At: Tue Aug  2 23:46:19 2022
##################################################################################################

Interface Configuration
Ethernet Tool Stats
Ethernet Tool Ring Buffer Sizes
Network Interface Stats
Network Connection Stats
Route Configuration
NTP Stats
NTP Status
DNS Configuration
Domain Information Groper
ARP hosts
SAR Network
File System Usage
Partition Tables
Current Processes
Top Processes
Processor Related Stats
I/O Related Stats
Memory Stats
List Open Files Count
Up Time
SAR CPU
SAR CPU ALL
SAR I/O
SAR Paging and Memory Statistics
SAR Memory Utilization
Docker Downloaded Images
Docker Containers
Docker Service Status
Docker Stats
Service Manager Service Status
Service Agent Service Status
Docker journalctl Status
Connector Service Status
tech support saved to
/home/dnasadmin/techsupport/connector_tech_support_2022-08-02T23-46-19.gz
```

Command History

Release 3	This command is introduced.

connectorctl containerstatus

This command displays the status of the container running the Cisco Spaces: Connector.

Parameters

None.

connectorctl containerstatus

Usage Guidelines

The following is the output for a container status that is not running:

```
[cmxadmin@cmxTrial02 ~]$ connectorctl containerstatus

connector container is not running
```

The following is the output for a container status that is running:


```
[cmxadmin@cmxnew ~]$ connectorctl containerstatus
{
  "connector": {
    "authInfo": {
      "ctrlHost": "https://connector.dev-dnaspaces.io/api/dms/v1/ctrl",
      "dataHost": "https://connector.dev-dnaspaces.io/data",
      "tenantId": "1570",
      "connectorId": "81257079417762970000",
      "issueTime": 1582088017,
      "expiration": 1582174417
    },
    "macAddress": "00:0c:29:0d:d1:e5",
    "keyHash": "315b43d153e39b6d604f1547d47ab2ed725581712f9eb9f6095e76f2b27fa9bf",
    "currentTime": 1582088972317,
    "timezone": "Coordinated Universal Time",
    "osArch": "amd64",
    "osName": "Linux",
    "osVersion": "5.5.1-1.el7.elrepo.x86_64",
    "ipAddress": "10.22.244.100",
    "uptime": 956381,
    "numberOfAps": 0,
    "cpu": 2
  },
  "controllers": [],
  "upgrade": {
    "gold": "v2.0.139",
    "latest": "v2.0.226"
  },
  "controlChannel": {
    "connectionStatus": "Connected",
    "connectionTime": 1582088018141,
    "connectionCount": 1,
    "connectionErrorTime": 0,
    "connectionErrorCount": 0,
    "connectionLastRequestTime": 1582088018176,
    "connectionRequestCount": 3,
    "channelTotal": 0,
    "channelActive": 0
  },
  "dataChannel": {
    "connectionStatus": "Connected",
    "connectionTime": 1582088018211,
```

```
    "connectionCount": 2,
    "connectionErrorTime": 0,
    "connectionErrorCount": 0,
    "connectionLastRequestTime": 0,
    "connectionRequestCount": 0,
    "channelTotal": 2,
    "channelActive": 2,
    "connectionMetrics": {
      "connectionCount": {
        "count": 2,
        "m15_rate": 0.1399750996444616,
        "m1_rate": 5.779920984437031e-08,
        "m5_rate": 0.017140850746816084,
        "mean_rate": 0.002095201454175875,
        "units": "events/second"
      },
      "nmspDropped": {
        "count": 0,
        "m15_rate": 0.0,
        "m1_rate": 0.0,
        "m5_rate": 0.0,
        "mean_rate": 0.0,
        "units": "events/second"
      },
      "nmspMessages": {
        "count": 0,
        "m15_rate": 0.0,
        "m1_rate": 0.0,
        "m5_rate": 0.0,
        "mean_rate": 0.0,
        "units": "events/second"
      },
      "bytesSent": {
        "count": 0,
        "m15_rate": 0.0,
        "m1_rate": 0.0,
        "m5_rate": 0.0,
        "mean_rate": 0.0,
        "units": "events/second"
      }
    }
  },
  "controllerStats": {
    "nmspByteReceived": {
      "count": 0
    },
    "nmspMessageReceived": {
      "count": 0,
      "m15_rate": 0.0,
      "m1_rate": 0.0,
      "m5_rate": 0.0,
      "mean_rate": 0.0,
      "units": "events/second"
    }
  },
  "current_version": "v2.0.226",
  "gold_version": "v2.0.139"
}
```

connectorctl version

This command displays the versions of **service-manager** and **service-agent** services on the connector.

connectorctl version

Syntax Description

This command has no keywords or arguments.

Examples

The following is a sample output of the command to view the versions of service-manager and service-agent.

```
[spacesadmin@connector ~]$ connectorctl version
Executing command:version
Command execution status:Success
----------------------
Package:connector3-p82-sep2022
System Version:8.4.0.82
Service Agent Version:8.4.0.97
Service Manager Version:3.0.1.96
```

Command History

Release 3	This command is introduced.

connectorctl help

This command displays the commands available on the Cisco Spaces: Connector CLI.

connectorctl help

Parameters

None

Command History		
	Release 3	This command is introduced.