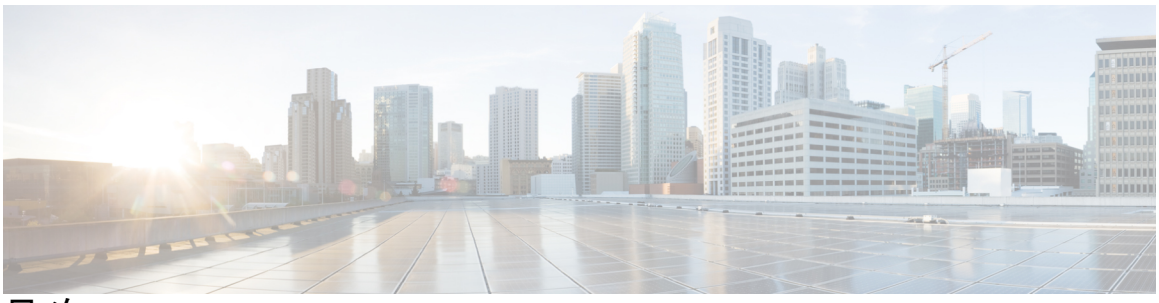
Cisco DNA Spaces：コネクタ コマンドリファレンスガイド

初版：2019 年 3 月 9 日

最終更新：2021 年 8 月 23 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



目 次

はじめに

対象読者

このドキュメントは、組織内の資産の使用状況を監視、管理、および最適化するために Cisco DNA Spaces を展開する Cisco Digital Network Architecture（DNA）Spaces ネットワーク管理者および IT 管理者を対象としています。

表記法

このマニュアルでは、次の表記法を使用しています。

表 *1* : 表記法

表記法	説明
太字	コマンド、キーワード、およびユーザーが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザーが値を指定する関数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。文字列を引用符で囲まないでください。引用符で囲むと、文字列に引用符が含まれます。

表記法	説明
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

はじめに

第 I 部

コマンドライン インターフェイスの使用

CLI の使用

コマンドライン インターフェイスの使用

コマンドライン インターフェイスの使用

Cisco DNA Spaces：コネクタ にはコマンドライン インターフェイスからアクセスできます。

制限されたコマンド ライン インターフェイス

制限された CLI

Cisco DNA Spaces：コネクタ では、Linux コマンドは、権限のないユーザーが不注意でシステム設定を変更することを防ぐために制限されています。このようにアクセスを制限することで、問題を引き起こす可能性のあるシステム構成をユーザーが変更できないようにしています。

制限されたコマンドラインでは次のコマンドが許可されます。

表 *2:* 制限コマンドのリスト

コマンド	説明
cat	ファイルの内容を出力します。
cp	ファイルをコピーします。
df	ファイルシステムのディスク領域の使用状況を出力します。
du	ファイルスペースの使用状況を出力します。
grep	パターンに一致する行を出力します。
ip	ネットワーク インターフェイス設定を表示します。
ls	ディレクトリの内容をリストします。
nslookup	インターネット ネーム サーバーに問い合わせます。
passwd	dnasadmin パスワードを変更します。
ping	Internet Control Message Protocol（ICMP）エコー要求をネットワークデバイスに送信します。
pwd	現在または作業中のディレクトリを出力します。
rm	ファイルを削除します。
scp	リモートコピーファイルを保護します。
sftp	ファイル転送を保護します。
ssh	クライアントに SSH 接続します。
tail	ファイルの最後の部分を出力します。

コマンド	説明
top	Linux プロセスを表示します。
route	IPルーティングテーブルルールを設定します。
clear	画面をクリアします。
wget	インターネットからファイルをダウンロードします。
who	ユーザーを表示します。

第 II 部

設定コマンド

設定コマンド

connectorctl lockinterval

このコマンドは、アカウントがロックされるまでに失敗できるログイン試行の許容回数を設定します。アカウントのロックアウト間隔も分単位で設定されます。最小試行回数は3回です。最大試行回数は 5 回です。デフォルトの試行回数は 3 回です。

パラメータ

なし。

connectorctl lockinterval

使用上のガイドライン

```
[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

このコマンドは、コネクタ Web UI のパスワードポリシーを設定し、脆弱なパスワードが設定されないようにして、強力なパスワードの設定を推奨します。

パラメータ

表 *3:* パラメータ

パラメータ	説明
Enable strong password	大文字、小文字、特殊文字、数字を含む強力なパスワードの設定を有効にします。
Minimum password length	パスワードの長さを指定できます。最小長は 8、最大長は 127、デフォルトの長さは 8 です。
Reject weak passwords	脆弱なパスワード（一般的な単語など）に警告を発行するだけではなく、拒否できるようにします。
Allow password to expire	パスワードの有効期限を 60 日に設定し、警告期間を 7 日に設定します。

使用上のガイドライン

connectorctl passwordpolicy

```
[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

このコマンドは、ネットワーク設定を行うか、コネクタ上で行われたネットワーク設定を表示します。このコマンドは、シングルインターフェイス展開とデュアルインターフェイス展開の両方で機能します。

（注） このコマンドを使用してホスト名または IP アドレスを変更する場合は、自己署名証明書を確実に再生成してください。システムを再起動した後に connectorctl generatecert コマンドを使用します。

パラメータ

表 *4:* パラメータ

パラメータ	説明
cloud	シングルインターフェイス展開でインターフェイスを設定します。クラウドインターフェイス、またはデュアルインターフェイス展開で外部ネットワークに接続するインターフェイス（最初のインターフェイス）を設定します。
cloudstatus	シングルインターフェイス展開でのインターフェイスのステータスを表示します。デュアルインターフェイス展開（最初のインターフェイス）でのクラウドインターフェイスのステータスを表示します。

connectorctl networkconfig { cloud | cloudstatus }

使用上のガイドライン

```
 [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

このコマンドは、ネットワーク設定を行うか、Cisco DNA Spaces：コネクタ 上で行われたネットワーク設定を表示します。このコマンドはデュアルインターフェイス展開でのみ機能します。シングルインターフェイス展開でこのコマンドを実行すると、エラーがスローされます。

（注） このコマンドを使用してホスト名または IP アドレスを変更する場合は、自己署名証明書を確実に再生成してください。システムを再起動した後に connectorctl generatecert コマンドを使用します。

パラメータ

表 *5:* パラメータ

パラメータ	説明
device	デュアルインターフェイス展開で、デバイスが存在するインターフェイス（デバイスインターフェイス）を設定します。
devicestatus	デュアルインターフェイス展開でのデバイスインターフェイスのステータスを表示します。

connectorctl networkconfig { device | devicestatus }

使用上のガイドライン

```
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.
```

（注） [Add Subnet] オプションを使用して、さらにサブネットを追加できます。Cisco DNA Spaces：コネクタ では、デバイスインターフェイスを使用してこれらのサブネットに到達できます。

```
[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 ~]$
```

第 III 部

アップグレード コマンド

アップグレード コマンド

connectorctl upgrade

このコマンドは、インストールされているオープン仮想アプライアンス（OVA）をアップグレードし、イメージ名をパラメーターとして受け取ります。

CSCvr74830 では、アップグレード中にエラーメッセージが表示されます。
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvr74830

パラメータ

cisco.com からダウンロードしたアップグレードイメージ

connectorctl upgrade *image*

使用上のガイドライン

```
[cmxadmin@connector ~]$ connectorctl upgrade cisco-dna-spaces-connector-v2.0-.connector
```

第 IV 部

証明書コマンド

証明書コマンド

connectorctl generatecert

このコマンドは、新しいセキュアソケットレイヤ（SSL）証明書を生成します。証明書のタイプは Rivest–Shamir–Adleman（RSA）または楕円曲線デジタル署名アルゴリズム（ECDSA）です。自己署名証明書を展開したら、**connectorctl showcert** コマンドを使用して証明書を表示できます。

connectorctl generatecert

コマンド履歴

リリース 2.3.2 より前	Connector SSL 証明書では、CSR の [Subject Alternative Name (SAN)] フィールドに IP アドレスが含まれます。
リリース 2.3.2	2.3.2 以降、コネクタ SSL 証明書では、CSR の [Subject Alternative Name (SAN)] フィールドに完全修飾ドメイン名（FQDN）またはホスト名が含まれます。

使用上のガイドライン

FQDN とホスト名は、CA 署名付き証明書の証明書署名要求（CSR）を設定します。CSR が CA によって署名されている場合、作成された証明書では、[SAN] フィールドに FQDN またはホスト名が含まれます。

CSCvt29826 の場合、IPSec を使用する AAA は、connectorctl generatecert コマンドを使用して生成される、キータイプが楕円曲線デジタル署名アルゴリズム（ECDSA）の Connector で生成される証明書と互換性がありません。https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvx40536

例

次に、以下のコマンドの出力例を示します。

```
[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"
```

関連トピック

connectorctl showcert （27 ページ）
connectorctl rsyslogconfig restart （80 ページ）

connectorctl showcert

このコマンドは、展開された証明書の詳細を表示します。

connectorctl showcert

コマンド履歴

リリース 2.2	このコマンドが導入されました。

例

次に、以下のコマンドの出力例を示します。

```
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.
================================================================================
```

関連トピック

connectorctl generatecert （26 ページ）
connectorctl createcsr （30 ページ）

connectorctl createcsr

このコマンドは、新しいセキュアソケットレイヤ（SSL）証明書の証明書署名要求（CSR）を作成します。認証局（CA）によって署名されたCSRを取得し、CA署名付きSSL証明書を取得できます。CA署名付き証明書を展開したら、**connectorctl showcert**コマンドを使用して証明書を表示できます。

connectorctl createcsr

コマンド履歴

リリース 2.3.2 より前	コネクタSSL証明書では、CSRの[Subject Alternative Name (SAN)]フィールドにIPアドレスが含まれます。
リリース 2.3.2	2.3.2以降、コネクタSSL証明書では、CSRの[Subject Alternative Name (SAN)]フィールドに完全修飾ドメイン名（FQDN）またはホスト名が含まれます。

使用上のガイドライン

FQDNとホスト名は、CA署名付き証明書の証明書署名要求（CSR）を設定します。CSRがCAによって署名されている場合、作成された証明書では、[SAN]フィールドにFQDNまたはホスト名が含まれます。

例

次に、以下のコマンドの出力例を示します。

```
[[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
```

関連トピック

connectorctl showcert （27 ページ）

connectorctl setproxycert

このコマンドは、HTTPS プロキシの証明書を設定します。

パラメータ

証明書のファイル名。

connectorctl setproxycert *filename*

構文の説明

filename	証明書のファイル名。

使用上のガイドライン

コマンドを実行する前に、まず証明書ファイルを dnasadmin ユーザーがアクセスできる（Cisco Unified Computing System（Cisco UCS） 上の）任意のフォルダにコピーする必要があります。

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

connectorctl validatecert

このコマンドは、認証局（CA） によって署名された証明書を検証します。

connectorctl validatecert *{ CA_certificate | root_certificate }*

構文の説明

CA_certificate	CA 証明書
root_certificate	ルート証明書

例

次に、 コマンドの出力例を示します。

```
[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

このコマンドは、署名付き証明書を コネクタ の正確な場所にインポートし、 コネクタ との接続のセキュリティを確保します。

connectorctl createcsr では、認証局（CA） による署名が必要な証明書が作成されます。この署名付き証明書は、connectorctl validatecert コマンドを使用して検証できます。署名付き証明書をインポートするには、connectorctl importcacert コマンドを使用できます。この手順により、コネクタ GUI にログインしようとしたときに表示される「Your connection is not private」というメッセージも削除されます。

connectorctl importcacert *certificate*

構文の説明

certificate	署名および検証済みの証明書。

コマンド履歴

リリース 2.2	このコマンドが導入されました。

例

次に、以下のコマンドの出力例を示します。

```
[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
```

使用上のガイドライン

CSCvy62400 では、サードパーティ CA による証明書またはデバイス証明書をインポートできない場合があります。https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy62400このような場合、証明書のインポートにいくつかのエラーが発生し、GUI が終了することがあります。次の出力が表示されます。

```
[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
```

この問題は、connectorctl generatecert コマンドを使用して自己署名証明書を再生成することで解決できます。この手順により、互換性のない証明書形式に関連する問題がすべて解消されます。

関連トピック

connectorctl validatecert （33 ページ）
connectorctl createcsr （30 ページ）
connectorctl generatecert （26 ページ）

connectorctl dockersubnet

デフォルトでは、コネクタ の Docker コンテナには 172.17.0.0/16 サブネットの IP アドレスが割り当てられます。サブネットがアドレス空間と重複している場合は、connectorctl dockersubnet コマンドを使用して、Docker サブネットを追加または削除できます。

connectorctl dockersubnet

例

次に、 コマンドの出力例を示します。

```
[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 ~]$
```

第 V 部

タイムゾーンコマンド

タイムゾーンコマンド

connectorctl checktimezone

このコマンドは、設定されたタイムゾーンの詳細を表示します。

パラメータ

なし

connectorctl checktimezone

使用上のガイドライン

```
[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

このコマンドは、使用可能なすべてのタイムゾーンを一覧表示します。

パラメータ

なし。

```
connectorctl listtimezone
```

使用上のガイドライン

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

connectorctl changetimezone

このコマンドを使用すると、タイムゾーンを利用可能なタイムゾーンのいずれかに変更できます。

パラメータ

なし。

connectorctl validatecert *CA_certificate root_certificate*

使用上のガイドライン

```
[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'.
```

関連トピック

connectorctl checktimezone （40 ページ）
connectorctl listtimezone （41 ページ）

第 VI 部

NTP コマンド

NTP コマンド

connectorctl ntprestrict

このコマンドは、IP アドレスによる Network Time Protocol（NTP）サーバーへのアクセスを制限します。

パラメータ

IP アドレス

connectorctl ntprestrict *ipaddress*

使用上のガイドライン

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

関連トピック

connectorctl ntpunrestrict （47 ページ）

connectorctl ntpunrestrict

このコマンドは、IP アドレスに対する Network Time Protocol（NTP）サーバーのアクセス制限をすべて削除します。

パラメータ

IP アドレス

connectorctl ntpunrestrict *ipaddress*

使用上のガイドライン

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

connectorctl ntpconfig

このコマンドは、Network Time Protocol（NTP）サーバーを追加、編集、削除、または表示します。

パラメータ

なし

connectorctl ntpconfig

使用上のガイドライン

以下は、NTP サーバーが設定されていない場合の [Show NTP Server Details (Press 4)] オプションのコマンド出力サンプルです。

```
[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)
```

以下は、NTP サーバーが設定されている場合の [Show NTP Server Details (Press 4)] オプションのコマンド出力サンプルです。

```
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

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

以下は、設定されている NTP サーバーがない場合の [Add NTP Server Details (Press 1)] オプションのコマンド出力サンプルです。

```
[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
```

以下は、1 つの NTP サーバーが既に設定されている場合の [Add NTP Server Details (Press 1)] オプションのコマンド出力サンプルです。参照用に、すでに追加されている NTP サーバーが最初に表示されます。

```
[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
```

以下は、[Edit NTP Server Details (Press 2)] オプションのコマンド出力サンプルです。参照用に、すでに追加されている NTP サーバーが最初に表示されます。

```
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
```

以下は、[Remove NTP Server Details (Press 3)] オプションのコマンド出力サンプルです。

```
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
```

第 VII 部

AAA コマンド

AAA コマンド

connectorctl aaa show

このコマンドは、Cisco DNA Spaces：コネクタ 上で行われた AAA サーバーの設定を表示します。

パラメータ

なし。

connectorctl aaa show

使用上のガイドライン

次の例は、AAA サーバーが IPSec なしで設定されている場合の出力を示しています。

```
[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

このコマンドは、Cisco DNA Spaces：コネクタ の既存の認証、許可、およびアカウンティング（AAA）設定を編集します。

パラメータ

パラメータ	説明
Do you want to CHANGE AAA Server settings	既存の AAA 設定の変更を選択します。
Enter AAA Server Host IP	AAA サーバの IP アドレス。
Enter AAA Server Port	AAA サーバーへの接続に使用されるポート。デフォルト値は 1812 です。
Enter AAA Server's shared secret key	AAA サーバーへの接続に使用される共有秘密鍵。
Do you want to enable IPSec?	IPSec を有効にするか無効にするかを選択します。IPSec の無効化を選択した場合、外部 AAA サーバーに確立された接続は暗号化されず、UDP 経由になります。
Enter AAA Server's DNS name	AAA サーバーのドメインネームサーバー（DNS）の名前。
Select IPSec Auth Type: (pubkey/psk)	2 種類の IPSec 認証、つまり pubkey または PSK から選択します。
Do you want to auto-generate ('a') OR provide ('p') PSK from Radius Server ?	• a：PSK の自動生成を選択します。 • p：AAA サーバーで設定された PSK の提供を選択します。
Enter PSK from Radius Server	AAA サーバーに存在する PSK 値を入力します。

connectorctl aaa edit

使用上のガイドライン

次の出力例では、AAA と Internet Protocol Security（IPSec）の両方が有効になっています。IPSec は事前共有キー（PSK）ありで有効になっています。[provide] オプションを選択すると、AAA サーバーで使用可能な PSK を指定できます。

```
[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
.
------------------------------------------------------------------
```

次の出力例では、AAA と Internet Protocol Security（IPSec）の両方が有効になっています。IPSec は事前共有キー（PSK）ありで有効になっています。[auto-generate] オプションを選択すると、AAA サーバーで使用可能な PSK を指定できます。

```
[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
```

自動生成された PSK 値が出力に表示されます。IPSec を有効にしても、出力の次のセクションに示されているように、IPSec トンネルがすぐに確立されない場合があります。

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

connectorctl aaa show コマンドを数分後に使用することで、IPSec トンネルが確立されているかどうかを確認できます。両方の出力の PSK 値を比較して、同じ値であることを確認できます。

```
[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.
```

関連トピック

- connectorctl aaa show （54 ページ）
- connector aaa restart （61 ページ）
- connectorctl aaa disable （60 ページ）
- connectorctl aaa edit （55 ページ）
- connectorctl aaa enable （58 ページ）

connectorctl aaa enable

このコマンドは、認証、許可、およびアカウンティング（AAA）サーバーを使用して認証を設定および有効化します。インターネットプロトコルセキュリティ（IPSec）プロトコルの有効化を選択できます。pubkey と PSK の 2 種類の IPSec プロトコルがサポートされています。

IPSec の無効化を選択した場合、外部 AAA サーバーに確立された接続は暗号化されず、UDP 経由になります。

パラメータ

パラメータ	説明
Do you want to configure a AAA server.	AAA サーバーの設定を選択します。
Enter AAA Server Host IP	AAA サーバの IP アドレス。
Enter AAA Server Port	AAA サーバーへの接続に使用されるポート。デフォルト値は 1812 です。
Enter AAA Server's shared secret key	AAA サーバーへの接続に使用される共有秘密鍵。
Do you want to enable IPSec?	IPSec を有効にするか無効にするかを選択します。IPSec の無効化を選択した場合、外部 AAA サーバーに確立された接続は暗号化されず、UDP 経由になります。
Enter AAA Server's DNS name	AAA サーバーのドメインネームサーバー（DNS）の名前。
Select IPSec Auth Type: (pubkey/psk)	2 種類の IPSec 認証、つまり pubkey または PSK から選択します。
Do you want to auto-generate ('a') OR provide ('p') PSK from Radius Server ?	• a：PSK の自動生成を選択します。 • p：AAA サーバーで設定された PSK の提供を選択します。
Enter PSK from Radius Server	AAA サーバーの既存の PSK の名前を入力します。

connectorctl aaa enable

使用上のガイドライン

次の出力例は、IPSec セキュリティプロトコルなしで有効になっている AAA サーバーを示しています。

```
[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.
-------------------------------------------------------------------
```

次の出力例は、IPSecセキュリティプロトコルありで有効になっているAAAサーバーを示しています。

```
[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.
-------------------------------------------------------------------
```

関連トピック

connectorctl aaa show （54 ページ）
connectorctl aaa disable （60 ページ）
connectorctl aaa edit （55 ページ）
connector aaa restart （61 ページ）
connectorctl aaa enable （58 ページ）

connectorctl aaa disable

このコマンドは、Cisco DNA Spaces：コネクタ での認証、許可、およびアカウンティング（AAA）設定と、インターネット プロトコル セキュリティ（IPSec）設定を無効にします。

パラメータ

なし。

connectorctl aaa disable

使用上のガイドライン

次のサンプルは、認証、許可、およびアカウンティング（AAA）とインターネット プロトコル セキュリティ（IPSec）の両方が有効になっている場合のコマンド出力です。connectorctl aaa disable コマンドは、両方のプロトコルを無効にします。

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

次のサンプルは、IPSec なしで AAA だけが有効になっている場合のコマンド出力です。

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

connector aaa restart

このコマンドは、Cisco DNA Spaces：コネクタから既存の認証、許可、およびアカウンティング（AAA）サーバーに確立された IP セキュリティトンネルを再起動します。

パラメータ

なし

connectorctl aaa restart

使用上のガイドライン

AAA が無効になっている場合、connectorctl aaa restart コマンドは次の出力例を表示します。

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

AAA が有効で IPSec が無効の場合、connectorctl aaa restart コマンドは次の出力例を表示します。

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

AAA と IPSec の両方が有効になっている場合、connectorctl aaa restart コマンドは次の出力例を表示します。

```
[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
```

関連トピック

connectorctl aaa show （54 ページ）

第 VIII 部

debug コマンド

debug コマンド

connectorctl enabledebug

このコマンドは、Cisco DNA Spaces：コネクタ のデバッグモードを有効にします。

パラメータ

なし。

connectorctl enabledebug

使用上のガイドライン

```
[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$
```

関連トピック

connectorctl viewdebuglogs （67 ページ）
connectorctl disabledebug （68 ページ）

connectorctl viewdebuglogs

このコマンドは、デバッグログを表示します。

パラメータ

なし。

connectorctl viewdebuglogs

使用上のガイドライン

```
[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 - tenantld: "427"
macAddress: "00: 0c :xx: xx: xx : xx"
controllerlpAddress: "10.22.244.28"
messageld: 15
measurementNotification {
    tenantld: "427"
    tenantld: "427"
    macAddress: "00:0c:xx:xx:xx:xx"
    controllerlpAddress: "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

このコマンドは、Cisco DNA Spaces：コネクタ のデバッグモードを無効にします。

パラメータ

なし。

connectorctl disabledebug

使用上のガイドライン

```
[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$
```

第 IX 部

サービスコマンド

サービスコマンド

connectorctl restartservices

このコマンドは、すべての Cisco DNA Spaces：コネクタ サービスを再起動します。

パラメータ

なし。

connectorctl restartservices

使用上のガイドライン

```
[cmxadmin@cmxnew ~]$ connectorctl restartservices
Restart services? [yes/no] [yes]: yes
Restart AGENT service?[yes/no] [yes]: yes
Restart DOCKER service?[yes/no] [yes]: yes
Restart HAPROXY service?[yes/no] [yes]: yes
Restart NGINX service?[yes/no] [yes]: yes
Restarting services....
```

関連トピック

connectorctl servicestatus （73 ページ）

connectorctl servicestatus

このコマンドは、Cisco DNA Spaces：コネクタ で実行されているすべてのサービスのステータスを表示します。

パラメータ

なし。

connectorctl servicestatus

使用上のガイドライン

```
[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/713a1fed5f06283b48771e699ca6082b3b7a39eeb8f28776aae97b914c78afa
 -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
```

関連トピック

connectorctl restartservices （72 ページ）

第 X 部

syslog コマンド

syslog コマンド

connectorctl rsyslogconfig restart

このコマンドは、リモート Syslog サーバーを再起動します。

connectorctl rsyslogconfig restart

コマンド履歴		
	リリース 2.3.2	このコマンドが導入されました。

例

次に、以下のコマンドの出力例を示します。

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

connectorctl rsyslogconfig

このコマンドは、リモート Syslog サーバーの設定を表示します。このコマンドで設定を更新することもできます。

connectorctl rsyslogconfig

コマンド履歴		
	リリース 2.3.2	このコマンドが導入されました。

例

次に、以下のコマンドの出力例を示します。

```
[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.
```

第 XI 部

クラウド接続コマンド

クラウド接続コマンド

connectorctl testconnectivity

このコマンドは、コネクタから米国またはEUのクラウドでホストされているCisco DNA Spacesへの接続をテストします。このコマンドは、**curl** の出力を詳細に出力します。

コマンド履歴

リリース 2.3.2	このコマンドが導入されました。

例

次に、以下のコマンドの出力例を示します。

```
[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 .
==========================================================================================
```

第 XII 部

その他のコマンド

その他のコマンド

connectorctl techsupport

このコマンドは、テクニカルサポート情報を表示します。ネットワークとシステムの詳細、実行中のDockerコンテナ、ダウンロードしたイメージを含むログファイルが作成されます。データの表示を選択すると、データが表示されます。

パラメータ

なし。

connectorctl techsupport

使用上のガイドライン

```
[cmxadmin@connector ~]$ connectorctl techsupport
Show data? [yes/no] [yes]: yes
################################################################################################################
CMX Tech Support Started At: Wed Sep 25 17:23:41 2019
################################################################################################################
################################################################################################################

CMX Tech Support Started At: Wed Sep 25 17:23:41 2019
################################################################################################################
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
################################################################################################################

CMX Tech Support Started At: Wed Sep 25 17:23:42 2019
################################################################################################################
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
SAR Memory Utilization

SAR Memory Statistics
################################################################################################################

CMX Tech Support Started At: Wed Sep 25 17:23:50 2019
################################################################################################################
Docker Downloaded Images
Docker Running Containers
Docker Service Status
```

```
HAProxy Service Status
NGINX Service Status
Connector Agent Service Status
Docker journalctl Status
```

connectorctl containerstatus

このコマンドは、Cisco DNA Spaces：コネクタ を実行しているコンテナステータスを表示します。

パラメータ

なし。

connectorctl containerstatus

使用上のガイドライン 以下は、実行されていないコンテナステータスの出力です。

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

connector container is not running
```

以下は、実行中のコンテナステータスの出力です。


```
[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

このコマンドは コネクタ のバージョンを表示します。

コマンド履歴

リリース 2.2	このコマンドが導入されました。

例

次に、 コマンドの出力例を示します。

```
[dnasadmin@conn171 ~]$ connectorctl version
2.3.494
```

connectorctl help

このコマンドは、DNA Spaces Connector コマンド ライン インターフェイスで使用可能なコマンドを表示します。

パラメータ

なし。

connectorctl help

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。