CLIを使用したSD-WANでのUTDエンジンのインストールとアンインストール

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[コンセプト](#)
[設定](#)
[UTDのアンインストール](#)
[事前チェック](#)
[設定](#)
[確認](#)
[設定](#)
[UTDのインストール](#)
[事前チェック](#)
[設定](#)
[確認](#)
[トラブルシュート](#)
[関連情報](#)

概要

このドキュメントでは、SDWANルータでCLIを使用してUnified Threat Defense(UTD)をインストールおよびアンインストールする手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Software-Defined Wide Area Network(SD-WAN)
- Cisco IOS® XEコマンドラインインターフェイス(CLI)

使用するコンポーネント

このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- ルータISR4461/K9
- ソフトウェアバージョン17.3.4

- コントローラモードのルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

cedgeがCLIモードであるか、vManageとcedgeの間に制御接続がない場合は、次の手順を適用する必要があります。

ただし、コントロールプレーンがあり、cedgeがvManageモードになっている場合は、この別の記事を参照してください（図11を参照）。

コンセプト

このドキュメントの具体的な要件は次のとおりです。

- Cisco vManageリリース20.3以降。
- Ciscoサービス統合型ルータ4431リリース17.3.4

サポートされているプラットフォームの詳細については、『SDWANでサポートされているプラットフォームと制限事項に関するUTD』を参照してください。

設定

UTDのアンインストール

事前チェック

これは、cedgeルータが以前にUTDをアンインストールした場合の例です。

> *デバイスはコントローラモードであり、テンプレートは添付されていませんが、UTD設定が適用されます。

```
cedge#show sdwan system Viptela (tm) vEdge Operating System Software Copyright (c) 2013-2022 by
Viptela, Inc. Controller Compatibility: 20.3 Version: 17.03.04a.0.5574 Build: Not applicable
```

> **注**:UTD設定をアンインストールする前に、まずUTD設定を削除する必要があります。

設定

1. UTDサービスを停止します。

```
cedge#config-transaction
cedge(config)# app-hosting appid utd
cedge(config-app-hosting)# no start
cedge(config-app-hosting)# commit
```

```
Commit complete.
```

注：開始が適用されないと、UTDのステータスが[Running]から[Deployed] に変わります。

```
cedge#show app-hosting list App id State ----------------------------------------------------
-- utd DEPLOYED cedge#
```

2. UTD設定を削除します。

```
cedge#config-transaction
cedge(config)# utd engine standard multi-tenancy
cedge(config-utd-multi-tenancy)# no policy utd-policy-vrf-1
cedge(config-utd-multi-tenancy)# commit
Commit complete.
cedge(config-utd-multi-tenancy)#
cedge#config-transaction
cedge(config)# utd multi-tenancy
cedge(config)# utd engine standard multi-tenancy
cedge(config-utd-multi-tenancy)# no threat-inspection whitelist profile Sig-white-list
cedge(config-utd-multi-tenancy)# no threat-inspection profile IPS-POLICY
cedge(config-utd-multi-tenancy)# exit
cedge(config)# commit
Commit complete.
cedge(config)# no utd engine standard multi-tenancy
cedge(config)# commit
Commit complete.
cedge(config)#
cedge#config-transaction
cedge(config)# no utd multi-tenancy
cedge(config)# commit
Commit complete.
cedge(config)#
cedge(config)# app-hosting appid utd
cedge(config-app-hosting)# no app-vnic gateway0 virtualportgroup 0 guest-interface 0
cedge(config-app-hosting)# no app-vnic gateway1 virtualportgroup 1 guest-interface 1
cedge(config-app-hosting)# no app-resource package-profile urlf-low
cedge(config-app-hosting)# commit
Commit complete.
cedge(config-app-hosting)#exit
cedge(config)# no app-hosting appid utd
cedge(config)# commit
Commit complete.
cedge(config)#
cedge(config)# no interface VirtualPortGroup0
cedge(config)# no interface VirtualPortGroup1
cedge(config)# commit
Commit complete.
cedge(config)#
cedge(config)# no iox
cedge(config)# commit
Commit complete.
cedge(config)#
```

3.検証。

次に、UTD設定が削除された後のエッジルータの表示例を示します。

```
cedge#show running-config | section iox
cedge#show running-config | section VirtualPortGroup0
cedge#show running-config | section VirtualPortGroup1
```

```
cedge#show running-config | section utd
cedge#
cedge#show platform software utd global
UTD Global state
=========================
Engine : Standard
Global Inspection : Disabled
Operational Mode : Intrusion Detection
Fail Policy : Fail-open
Container technology : LXC
Redirect interface : Not specified
UTD interfaces
No interfaces are protected by UTD
<snipped>
```

注：設定が削除された場合でも、UTDにはinstalledと表示されます。これは予想どおりの結果です。

```
cedge#show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.16_SV2.9.16.1_XE17.3
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.3$
UTD Installed Version: 1.0.16_SV2.9.16.1_XE17.3

cedge#show virtual-service
Virtual Service Global State and Virtualization Limits:
Infrastructure version : 1.7
Total virtual services installed : 1
Total virtual services activated : 0
<snipped>

cedge#show app-hosting list
The process for the command is not responding or is otherwise unavailable >>>> Expected because
UTD config was removed but UTD engine remains installed

** Before to remove Configuration **
cedge#show virtual-service version name utd running
Virtual service utd running version:
Name : UTD-Snort-Feature
Version : 1.0.16_SV2.9.16.1_XE17.3

** After configuration is removed **
cedge#
cedge#show virtual-service version name utd running
Virtual service utd running version:
Name : UTD-Snort-Feature
Version : None
```

4. UTDエンジンを取り外す。

ヒント:UTDエンジンをアンインストールするには、**ioxとapp-hosting appid utd**をアクティブにする必要があります。

UTDがioxとアプリケーションホスティングのアクティベーションなしで削除された場合に発生する状況の例を次に示します。

```
cedge#app-hosting uninstall appid utd    >>>> No action is taken.
cedge#
```

次に、UTDを正常にアンインストールする例を示します。

```
cedge#config-transaction
cedge(config)# iox
cedge(config)# app-hosting appid utd
cedge(config-app-hosting)# commit
Commit complete.
cedge(config-app-hosting)#
*Mar 3 20:25:24.889: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server iox has been notified
to start
*Mar 3 20:25:50.268: %IM-6-IOX_RECONCILE_INFO: R0/0: ioxman: App-hosting application reconcile
process start
*Mar 3 20:25:51.956: %IM-6-IOX_ENABLEMENT: R0/0: ioxman: IOX is ready.
cedge#
cedge#app-hosting uninstall appid utd
Uninstalling 'utd'. Use 'show app-hosting list' for progress.

cedge#
*Mar 3 20:26:31.653: %VIRT_SERVICE-5-INSTALL_STATE: Successfully uninstalled virtual service utd
*Mar 3 20:26:32.706: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Uninstall succeeded: utd
uninstalled successfully
cedge#
```

確認

次のコマンドを実行して、UTDが削除されたかどうかを確認します。

```
cedge#show app-hosting list
No App found

cedge#show virtual-service version name utd running
% Error: Virtual-service utd is not found

cedge#show utd engine standard version
IOS-XE Recommended UTD Version: 1.0.16_SV2.9.16.1_XE17.3
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.3$

cedge#show virtual-service
Virtual Service Global State and Virtualization Limits:
Infrastructure version : 1.7
Total virtual services installed : 0
Total virtual services activated : 0
<snipped>
```

設定

UTDのインストール

事前チェック

UTDでサポートされているバージョンを確認し、ブートフラッシュにダウンロードします。

```
cedge#
cedge#show utd engine standard version
IOS-XE Recommended UTD Version: 1.0.16_SV2.9.16.1_XE17.3
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.3$
```

```
cedge#
cedge#dir bootflash: | i utd
36 -rw- 55050240 Mar 1 2022 01:08:29 +00:00 secapp-
utd.17.03.04a.1.0.16_SV2.9.16.1_XE17.3.x86_64.tar
cedge#
```

設定

1. ioxとアプリケーションホスティングを有効にします。

```
cedge#config-transaction
cedge(config)# iox
cedge(config)# app-hosting appid utd
cedge(config-app-hosting)# commit
Commit complete.
cedge(config-app-hosting)#
*Mar 3 20:25:24.889: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server iox has been notified
to start
*Mar 3 20:25:50.268: %IM-6-IOX_RECONCILE_INFO: R0/0: ioxman: App-hosting application reconcile
process start
*Mar 3 20:25:51.956: %IM-6-IOX_ENABLEMENT: R0/0: ioxman: IOX is ready.
cedge#
```

2. UTDエンジンをインストールします。

```
cedge#app-hosting install appid utd package bootflash:secapp-
utd.17.03.04a.1.0.16_SV2.9.16.1_XE17.3.x86_64.tar
Installing package 'bootflash:secapp-utd.17.03.04a.1.0.16_SV2.9.16.1_XE17.3.x86_64.tar' for
'utd'. Use 'show app-hosting list' for progress.
cedge#
*Mar 3 21:07:43.529: %VMAN-5-PACKAGE_SIGNING_LEVEL_ON_INSTALL: R0/0: vman: Package 'secapp-
utd.17.03.04a.1.0.16_SV2.9.16.1_XE17.3.x86_64.tar' for service container 'utd' is 'Cisco
signed', signing level cached on original install is 'Cisco signed'
*Mar 3 21:07:56.332: %VIRT_SERVICE-5-INSTALL_STATE: Successfully installed virtual service utd
*Mar 3 21:07:56.922: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install succeeded: utd
installed successfully Current state is deployed
cedge#
```

3. UTDエンジンがインストールされていることを確認します。次のコマンドを実行します。

> **注：***DEPLOYED*状態とは、*UTDがインストールされているが設定されていないことを意味*します。*RUNNING*状態とは、*UTDがインストールされ設定されていることを意味します。*

```
cedge#show app-hosting list App id State ----------------------------------------------------------
-- utd DEPLOYED cedge#show virtual-service version name utd running Virtual service utd running
version: Name : UTD-Snort-Feature Version : None >>>> "None", it is expected due to the fact
that no config yet cedge#show utd engine standard version UTD Virtual-service Name: utd IOS-XE
Recommended UTD Version: 1.0.16_SV2.9.16.1_XE17.3 IOS-XE Supported UTD Regex: ^1\.0\.([0-
9]+)_SV(.*)_XE17.3$ UTD Installed Version: 1.0.16_SV2.9.16.1_XE17.3 >>>> UTD Package installed
cedge# cedge#show virtual-service Virtual Service Global State and Virtualization Limits:
Infrastructure version : 1.7 Total virtual services installed : 1 >>>> Installed 1 but Activated
0 as expected Total virtual services activated : 0
```

4. UTDをRUNNING状態にするには、IPS/URLの設定に進みます。これはラボの例です。

```
cedge#config-transaction
cedge(config)# interface VirtualPortGroup0
```

```
cedge(config-if)# description Management interface
cedge(config-if)# vrf forwarding 65529
cedge(config-if)# ip address 192.168.1.1 255.255.255.252
cedge(config-if)# exit
cedge(config)# commit
Commit complete.
cedge(config)#
cedge(config)# interface VirtualPortGroup1
cedge(config-if)# description Data interface
cedge(config-if)# ip address 192.168.2.1 255.255.255.252
cedge(config-if)# exit
cedge(config)# commit
Commit complete.
cedge(config)#
cedge(config)# app-hosting appid utd
cedge(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 0
cedge(config-app-hosting-gateway)# guest-ipaddress 192.168.1.2 netmask 255.255.255.252
cedge(config-app-hosting-gateway)# exit
cedge(config-app-hosting)# app-vnic gateway1 virtualportgroup 1 guest-interface 1
cedge(config-app-hosting-gateway)# guest-ipaddress 192.168.2.2 netmask 255.255.255.252
cedge(config-app-hosting-gateway)# exit
cedge(config-app-hosting)# app-resource package-profile urlf-low
cedge(config-app-hosting)# start
cedge(config-app-hosting)# commit
Commit complete.
cedge(config-app-hosting)#
cedge(config-app-hosting)# exit
cedge(config)# utd multi-tenancy
cedge(config)# utd engine standard multi-tenancy
cedge(config-utd-multi-tenancy)# threat-inspection whitelist profile Sig-white-list
cedge(config-utd-mt-whitelist)# generator id 3 signature id 22089
cedge(config-utd-mt-whitelist)# generator id 3 signature id 36208
cedge(config-utd-mt-whitelist)# exit
cedge(config-utd-multi-tenancy)# threat-inspection profile IPS-POLICY
cedge(config-utd-mt-threat)# threat detection
cedge(config-utd-mt-threat)# policy balanced
cedge(config-utd-mt-threat)# whitelist profile Sig-white-list
cedge(config-utd-mt-threat)# logging level alert
cedge(config-utd-mt-threat)# exit
cedge(config-utd-multi-tenancy)# commit
Commit complete.
cedge(config-utd-multi-tenancy)#
cedge(config-utd-multi-tenancy)# policy utd-policy-vrf-1
cedge(config-utd-mt-policy)# vrf 511
cedge(config-utd-mt-policy)# all-interfaces
cedge(config-utd-mt-policy)# fail close
cedge(config-utd-mt-policy)# threat-inspection profile IPS-POLICY
cedge(config-utd-mt-policy)# exit
cedge(config-utd-multi-tenancy)# commit
Commit complete.
cedge(config-utd-multi-tenancy)#
cedge(config-utd-multi-tenancy)# end
cedge#
```

5.設定が完了していることを確認します。

```
cedge#show run | section utd
utd multi-tenancy
utd engine standard multi-tenancy
threat-inspection whitelist profile Sig-white-list
generator id 3 signature id 22089
generator id 3 signature id 36208
threat-inspection profile IPS-POLICY
```

```
threat detection
policy balanced
logging level alert
whitelist profile Sig-white-list
policy utd-policy-vrf-1
vrf 511
all-interfaces
threat-inspection profile IPS-POLICY
fail close
app-hosting appid utd
app-vnic gateway0 virtualportgroup 0 guest-interface 0
guest-ipaddress 192.168.1.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 1 guest-interface 1
guest-ipaddress 192.168.2.2 netmask 255.255.255.252
app-resource package-profile urlf-low
start
cedge#
```

確認

1. show loggingを実行し、次に示すようなログが記録されていることを確認します。

```
*Mar 3 23:17:17.573: %LINK-3-UPDOWN: Interface VirtualPortGroup0, changed state to up *Mar 3
23:17:18.094: %LINK-3-UPDOWN: Interface VirtualPortGroup1, changed state to up *Mar 3
23:17:18.572: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup0, changed state
to up *Mar 3 23:17:19.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup1,
changed state to up *Mar 3 23:17:25.630: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel2000000001, changed state to up *Mar 3 23:19:36.863: %VIRT_SERVICE-5-ACTIVATION_STATE:
Successfully activated virtual service utd *Mar 3 23:19:37.577: %IM-6-START_MSG: R0/0: ioxman:
app-hosting: Start succeeded: utd started successfully Current state is running *Mar 3
23:19:38.318: %ONEP_BASE-6-CONNECT: [Element]: ONEP session Application:utd_snort Host:cedge
ID:6633 User: has connected. *Mar 3 23:19:50.428: %IOSXE_UTD-4-MT_CONFIG_DOWNLOAD: UTD MT
configuration download has started *Mar 3 23:20:06.460: %IOSXE_UTD-4-MT_CONFIG_DOWNLOAD: UTD MT
configuration download has completed *Mar 3 23:20:08.389: %IOSXE-5-PLATFORM: R0/0: cpp_cp:
QFP:0.0 Thread:011 TS:00000780131568867961 %SDVT-5-SDVT_HEALTH_UP: Service node is up for
channel Threat Defense. Current Health: Green, Previous Health: Down
```

注：設定が正常に完了すると、現在の状態が**ダウン**から**グリーン**に変わります。

2.次のコマンドを実行して、UTDのインストールを確認します。

```
cedge#show app-hosting list App id State ----------------------------------------------------------
-- utd RUNNING >>> State change from Deployed to Running cedge#show utd engine standard version
UTD Virtual-service Name: utd IOS-XE Recommended UTD Version: 1.0.16_SV2.9.16.1_XE17.3 IOS-XE
Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.3$ UTD Installed Version:
1.0.16_SV2.9.16.1_XE17.3 cedge#show virtual-service version name utd running Virtual service utd
running version: Name : UTD-Snort-Feature Version : 1.0.16_SV2.9.16.1_XE17.3 >>>> Changed from
NONE to "1.0.16_SV2.9.16.1_XE17.3" after config. cedge# cedge#show virtual-service Virtual
Service Global State and Virtualization Limits: Infrastructure version : 1.7 Total virtual
services installed : 1 Total virtual services activated : 1 >>>>>>>>> Now it is activated
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

便利なコマンド

```
show platform software device-mode
show app-hosting list
show virtual-service version name utd running
show utd engine standard version
show utd engine standard status
show virtual-service
```

関連情報

- セキュリティ設定ガイド：Unified Threat Defense、Cisco IOS XE 17
- セキュリティ設定ガイド：Unified Threat Defense、Cisco IOS XE 16
- SDWAN対応プラットフォームおよび制約事項のためのUTD.
- UTDとvManageをインストールします。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。