# 使用CLI在SD-WAN中安装和卸载UTD引擎

## 目录



## 简介

本文档介绍在SDWAN路由器中通过CLI安装和卸载统一威胁防御(UTD)的过程。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科软件定义的广域网(SD-WAN)
- Cisco IOS® XE命令行界面(CLI)

### 使用的组件

本文档基于以下软件和硬件版本：

- 路由器ISR4461/K9
- 软件版本17.3.4
- 处于控制器模式的路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# 背景信息

当cedge处于CLI模式或vManage和cedge之间没有控制连接时，需要应用这些步骤。

但是，如果您有控制平面，并且您的边缘处于vManage模式，则继续查看此其他文章。

### 概念

本文档的具体要求包括：

- Cisco vManage 20.3版或更高版本。
- 思科集成多业务路由器4431版本17.3.4

有关支持的平台的详细信息，请导航至适用于SDWAN支持的平台和限制的UTD。

# 配置

## *卸载UTD*

### 预检查

这是在UTD卸载之前的cedge路由器的示例。

*设备处于控制器模式，未连接任何模板，但应用了UTD配置。

```
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
```

**注意**:必须先删除UTD配置，然后才能将其卸载。

### 配置

1. 停止UTD服务。

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

**注意**：未应用启动后，UTD状态将从Running**更改为**Deployed。

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

2.删除UTD配置。

```
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.验证。

本示例展示了边缘路由器在删除UTD配置后如何进行查找。

```
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>
```

**注意**:即使删除了配置，UTD仍显示已安装。这是预期结果。

```
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.删除UTD引擎。

**提示**：您需要激活**iox**和**应用托管appid utd**才能卸载UTD引擎。

以下示例展示在不激活iox和应用托管的情况下删除UTD时会发生什么情况。

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

这是一个成功卸载UTD的示例。

```
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#
```

# 验证

运行以下命令以验证是否已删除UTD。

```
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>
```

# 配置

## *安装UTD*

### 预检查

查看UTD支持的版本，并将其下载到bootflash中。

```
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#
```

### 配置

1.激活iox和应用托管。

```
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.安装UTD引擎。

```
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.确保已安装UTD引擎。运行下一个命令。

**注意**:*DEPLOYED状态指已安装UTD但未配置。RUNNING状态表示UTD已安装和配置。*

```
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.要使UTD处于运行状态，请继续配置IPS/URL。这是实验中的示例。

```
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.确保配置完成。

```
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#
```

# 验证

1.运行**show logging**并确保您获得类似日志，如下所示。

```
*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
```

**注意**：如果配置成功，当前运行状况将**从**Down**更改为**Green**。**

2.运行这些命令以验证UTD安装。

```
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
```

# 故障排除

本部分提供的信息可用于对配置进行故障排除。

有用的命令

```
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
```

# 相关信息

- 安全配置指南：统一威胁防御，Cisco IOS XE 17
- 安全配置指南：统一威胁防御，Cisco IOS XE 16
- 适用于SDWAN支持的平台和限制的UTD.

- 使用vManage安装UTD。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。