

Instalar e desinstalar o mecanismo UTD no SD-WAN com CLI

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Conceitos](#)

[Configurar](#)

[Desinstalar UTD](#)

[Pré-verificação](#)

[Configurações](#)

[Verificar](#)

[Configurar](#)

[Instalar UTD](#)

[Pré-verificação](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve o procedimento para instalar e desinstalar o Unified Threat Defense (UTD) via CLI em roteadores SDWAN.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida por software da Cisco (SD-WAN)
- Interface de linha de comando (CLI) do Cisco IOS® XE

Componentes Utilizados

Este documento é baseado nestas versões de software e hardware:

- Roteador ISR4461/K9
- Software versão 17.3.4

- Roteador no modo controlador

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Essas etapas precisam ser aplicadas quando o cedge está no modo CLI ou não há conexão de controle entre o vManage e o cedge.

Mas se você tiver o plano de controle e seu cedge estiver no modo vManage, continue a rever esse outro artigo .

Conceitos

Os requisitos específicos deste documento incluem:

- Cisco vManage versão 20.3 ou posterior.
- Cisco Integrated Services Routers 4431 versão 17.3.4

Para obter mais informações sobre plataformas suportadas, navegue para [UTD para plataformas e restrições suportadas por SDWAN](#).

Configurar

Desinstalar UTD

Pré-verificação

Este é um exemplo de como o roteador de cedge se parece com a desinstalação UTD anterior.

* O dispositivo está no modo de controlador e nenhum modelo está anexado, mas a configuração UTD é aplicada.

```
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
```

Observação: a configuração do UTD precisa ser removida antes de ser desinstalada.

Configurações

1. Parar o serviço UTD.

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

Observação: O status UTD muda de Em Execução para Implantado quando nenhum início é aplicado.

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

2. Remova a configuração de UTD.

```
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. Validação.

Este é um exemplo de como o roteador de cedge fica após a remoção da configuração do UTD.

```
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>
```

Observação: mesmo que a configuração tenha sido removida, o UTD mostra instalado. Isso é esperado.

```
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. Remova o mecanismo UTD.

Dica: você precisa ter **iox** e **app-hosting appid utd** ativados para desinstalar o mecanismo UTD.

Aqui está um exemplo do que ocorre se o UTD for excluído sem a ativação do iox e da hospedagem de aplicativos.

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

Este é um exemplo para desinstalar o UTD com sucesso.

```
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#
```

Verificar

Execute os próximos comandos para verificar se o UTD foi removido.

```
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>
```

Configurar

Instalar UTD

Pré-verificação

Reveja a versão suportada de UTD e faça o download para o bootflash.

```
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#
```

Configurações

1. Ative o iox e a hospedagem de aplicativos.

```
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. Instale o mecanismo UTD.

```
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. Verifique se o mecanismo UTD está instalado. Execute os próximos comandos.

Observação: o estado *DEPLOYED* significa UTD instalado, mas não configurado. Estado *RUNNING* significa UTD Instalado e configurado.

```
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. Para ter o UTD no estado RUNNING, continue para configurar o IPS/URL. Este é um exemplo do laboratório.

```
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. Certifique-se de que a configuração esteja concluída.

```

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#

```

Verificar

1. Execute **show logging** e certifique-se de que você tenha logs semelhantes, como mostrado a seguir.

```

*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

```

Observação: a integridade atual mudará de **Down** para **Green** se a configuração tiver sido feita com êxito.

2. Execute estes comandos para verificar a Instalação do UTD.

```

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

```

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos úteis

```
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
```

Informações Relacionadas

- [Guia de configuração de segurança: defesa unificada contra ameaças, Cisco IOS XE 17](#)
- [Guia de configuração de segurança: defesa unificada contra ameaças, Cisco IOS XE 16](#)
- [UTD para plataformas e restrições suportadas por SDWAN.](#)
- [Instale o UTD com o vManage.](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.