

Installazione e disinstallazione del motore UTD in SD-WAN con CLI

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Concetti](#)

[Configurazione](#)

[Disinstalla UTD](#)

[Verifica preliminare](#)

[Configurazioni](#)

[Verifica](#)

[Configurazione](#)

[Installa UTD](#)

[Verifica preliminare](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive la procedura per installare e disinstallare Unified Threat Defense (UTD) tramite CLI nei router SDWAN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SD-WAN (Wide Area Network) definito dal software Cisco
- Cisco IOS® XE Command Line Interface (CLI)

Componenti usati

Questo documento si basa sulle seguenti versioni software e hardware:

- Router ISR4461/K9
- Software versione 17.3.4

- Router in modalità controller

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questi passaggi devono essere applicati quando la cedge è in modalità CLI o non è disponibile una connessione di controllo tra vManage e cedge.

Se invece si dispone di un control plane e la coda è in modalità vManage, procedere con la revisione di questo altro articolo.

Concetti

I requisiti specifici per questo documento includono:

- Cisco vManage release 20.3 o successive.
- Cisco Integrated Services Router 4431 release 17.3.4

Per ulteriori informazioni sulle piattaforme supportate, passare a [UTD per le piattaforme e le restrizioni supportate da SDWAN.](#)

Configurazione

Disinstalla UTD

Verifica preliminare

Questo è un esempio di come appare cedge router prima della disinstallazione UTD.

* Il dispositivo è in modalità controller e non è collegato alcun modello ma è applicata la configurazione UTD.

```
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
```

Nota: prima di disinstallare la configurazione UTD, è necessario rimuoverla.

Configurazioni

1. Arrestare il servizio UTD.

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

Commit complete.

Nota: lo stato UTD passa da In esecuzione a Distribuito quando **non** viene applicato alcun avvio.

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

2. Rimuovere la configurazione 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. Convalida.

Questo è un esempio di come appare il router cedge dopo la rimozione della configurazione 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>

```

Nota: anche se la configurazione è stata rimossa, l'UTD mostra installato. Questo è previsto.

```

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. Rimuovere il motore UTD.

Suggerimento: per disinstallare il motore UTD, è necessario che **iox** e **app-hosting** appid siano attivati.

Di seguito è riportato un esempio di ciò che accade se l'UTD viene eliminato senza attivazione iox e hosting dell'app.

```

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

```

Questo è un esempio di disinstallazione di UTD completata.

```
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#
```

Verifica

Eseguire i comandi successivi per verificare se l'UTD è stato rimosso.

```
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>
```

Configurazione

Installa UTD

Verifica preliminare

Controllare la versione UTD supportata e scaricarla in 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#
```

Configurazioni

1. Attivare iox e l'hosting di app.

```
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. Installare il motore 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. Assicurarsi che il motore UTD sia installato. Eseguire i comandi successivi.

Nota: lo stato *DISTRIBUITO* indica che *UTD* è installato ma non configurato. Lo stato *RUNNING* indica che *UTD* è installato e configurato.

```
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. Per attivare lo stato RUNNING di UTD, procedere alla configurazione di IPS/URL. Questo è un esempio da un laboratorio.

```
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. Accertarsi che la configurazione sia stata eseguita.

```

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#

```

Verifica

1. Eseguire il comando **show logging** e assicurarsi di avere log simili a quelli mostrati di seguito.

```

*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

```

Nota: lo stato corrente passa da **Giù** a **Verde** se la configurazione è stata completata correttamente.

2. Eseguire questi comandi per verificare l'installazione di 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

```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi utili

```
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
```

Informazioni correlate

- [Guida alla configurazione della sicurezza: Unified Threat Defense, Cisco IOS XE 17](#)
- [Guida alla configurazione della sicurezza: Unified Threat Defense, Cisco IOS XE 16](#)
- [UTD per piattaforme supportate da SDWAN e limitazioni.](#)
- [Installare UTD con vManage.](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).