UTD Engine installeren en verwijderen in SD-WAN met CLI

Inhoud

Inleiding

Dit document beschrijft de procedure voor het installeren en verwijderen van Unified Threat Defense (UTD) via CLI op SDWAN-routers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

Dit document is gebaseerd op deze software- en hardwareversies:

- Router ISR461/K9
- Software versie 17.3.4

- Router in controllermodus

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Deze stappen moeten worden toegepast wanneer de cedge zich in de CLI-modus bevindt of wanneer er geen bedieningsverbinding tussen vManager en cedge is.

Maar als u een besturingsplane hebt en uw cedge in vManager-modus staat, ga dan verder om dit andere artikel te bekijken.

Concepten

Specifieke eisen voor dit document zijn onder meer:

- Cisco vManager release 20.3 of hoger.
- Cisco geïntegreerde services routers 4431 release 17.3.4

Ga voor meer informatie over ondersteunde platforms naar UTD voor door SDWAN ondersteunde platforms en beperkingen.

Configureren

UTD verwijderen

Voorcontrole

Dit is een voorbeeld van hoe cedge router eruit ziet als eerdere UTD-desinstallatie.

> * Het apparaat is op Controllerwijze en geen Malplaatje is in bijlage maar de configuratie UTD wordt toegepast.

```
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
```

> **Opmerking**: UTD-configuratie moet eerst worden verwijderd voordat het kan worden verwijderd.

Configuraties

1. Stop de UTD-service.

```
cedge#config-transaction
cedge(config)# app-hosting appid utd
```

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

> **Opmerking**: de UTD-status verandert van Running naar Implementatie zodra **geen start** wordt toegepast.

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

2. Verwijder de UTD-configuratie.

```
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. Validering.

Dit is een voorbeeld van hoe cedge router eruit ziet nadat UTD-configuratie is verwijderd.

```
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>
```

Opmerking: ook al is de configuratie verwijderd, de UTD toont geïnstalleerd. Dit wordt verwacht.

```
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. Verwijder de UTD-engine.

Tip: Je moet jox en app-hosting applicatie utd geactiveerd hebben om UTD engine te verwijderen.

Hier is een voorbeeld van wat gebeurt als UTD wordt verwijderd zonder iox en app-hosting activering.

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

Dit is een voorbeeld om UTD succesvol te verwijderen.

```
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#
```

Verifiëren

Voer de volgende opdrachten uit om te controleren of de UTD is verwijderd.

```
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>
```

Configureren

Installeer UTD

Voorcontrole

Beoordeel UTD ondersteunde versie en download het 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#
```

Configuraties

1. Activeer jox en app-hosting.

```
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. Installeer de UTD-engine.

```
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. Controleer of de UTD-motor is geïnstalleerd. Voer de volgende opdrachten uit.

> **Opmerking**: *uitgerold* staat betekent *geïnstalleerd maar niet geconfigureerd UTD*. *Onder* actieve toestand wordt *verstaan: UTD geïnstalleerd en geconfigureerd*.

```
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. Ga verder met het configureren van IPS/URL om UTD in actieve staat te hebben. Dit is een

voorbeeld uit het lab.

```
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. Controleer of de configuratie is voltooid.

```
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#
```

Verifiëren

1. Start **show logging** en zorg ervoor dat je soortgelijke logbestanden hebt zoals hieronder wordt getoond.

```
*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
```

> **Opmerking**: de huidige status verandert van **Down** naar **Green** als de configuratie met succes is uitgevoerd.

2. Voer deze opdrachten uit om de UTD-installatie te controleren.

```
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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Handige opdrachten

```
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
```

Gerelateerde informatie

- Security Configuration Guide: Unified Threat Defense, Cisco IOS XE 17
- Security Configuration Guide: Unified Threat Defense, Cisco IOS XE 16
- UTD voor door SDWAN ondersteunde platforms en beperkingen.
- Installeer UTD met vManager.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.