تثبيت محرك UTD وإلغاء تثبيته في SD-WAN مع CLI

المحتويات

المقدمة

يصف هذا المستند إجراء تثبيت "الدفاع الموحد عن التهديدات" (UTD) وإلغاء تثبيته عبر CLI في موجهات SDWAN.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة المنطقة الواسعة المعرفة من برنامج Cisco (SD-WAN)
- واجهة سطر الأوامر (CLI) ل Cisco IOS® XE

المكونات المستخدمة

يستند هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الموجه ISR461/K9
- برنامج صيغة 17.3.4

- موجه في وضع وحدة التحكم

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يلزم تطبيق هذه الخطوات عندما يكون الخادم في وضع واجهة سطر الأوامر (CLI) أو عندما لا يوجد اتصال تحكم بين vManage و cedge.

ولكن إذا كان لديك مستوى تحكم وكان الطراز cedge في وضع الإدارة الافتراضية، فواصل مراجعة هذه المقالة الأخرى .

المفاهيم

تتضمن المتطلبات الخاصة لهذا المستند:

- الإصدار 20.3 من Cisco vManage أو إصدار أحدث.
- Cisco Integrated Services Routers 4431، الإصدار 17.3.4

لمزيد من المعلومات حول الأنظمة الأساسية المدعومة، انتقل إلى [UTD ل SDWAN الأنظمة الأساسية والقيود المدعومة.]

التكوين

إزالة تثبيت UTD

معاينة

هذا مثال على كيفية إزالة تثبيت Cedge موجه لمثيل UTD السابق.

> * الجهاز في وضع وحدة التحكم ولا يتم إرفاق أي قالب ولكن يتم تطبيق تكوين 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
```

> **ملاحظة**: يلزم إزالة تكوين UTD أو القالب قبل إزالة تثبيته.

التكوينات

1. إيقاف خدمة UTD.

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

ملاحظة: تتغير حالة UTD من التشغيل إلى النشر بمجرد **عدم** تطبيق **أي بادئة**.

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

2. إزالة تكوين 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. التحقق من الصحة.

هذا مثال على كيفية إستجابة موجه Cedge بعد إزالة تكوين 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>
```

ملاحظة: على الرغم من إزالة التكوين، إلا أن UTD يظهر مثبتا. هذا متوقع.

```
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. إزالة محرك UTD.

تلميح: تحتاج إلى تنشيط IOx و**APPID الخاص باستضافة التطبيقات** لإزالة تثبيت محرك UTD.

وفيما يلي مثال على ما يحدث إذا تم حذف UTD دون تنشيط IOx واستضافة التطبيقات.

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

هذا مثال على إزالة تثبيت UTD بنجاح.

```
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#
```

التحقق من الصحة

قم بتشغيل الأوامر التالية للتحقق من إزالة 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>
```

التكوين

تثبيت UTD

معاينة

مراجعة الإصدار المعتمد من UTD وتنزيله في 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#
```

التكوينات

1. تنشيط الطرازان ioX واستضافة التطبيقات.

```
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. تثبيت محرك 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. تأكد من تثبيت محرك UTD. قم بتشغيل الأوامر التالية.

> **ملاحظة**: حالة *النشر تعني UTD الذي تم تثبيته ولكن لم يتم تكوينه*. تعني حالة *التشغيل UTD التي تم تثبيتها وتكوينها*.

```
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. للحصول على UTD في حالة التشغيل، قم بالمتابعة لتكوين IPS/URL. اذه مثال من المختبر.

```
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. تأكد من إجراء التكوين.

```
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#
```

التحقق من الصحة

1. قم بتشغيل **show logging** وتأكد من حصولك على سجلات مماثلة كما هو موضح بعد ذلك.

```
*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
```

ملاحظة: التغييرات الحالية في الصحة من **أسفل** إلى **أخضر** إذا تم إجراء التكوين بنجاح.

2. قم بتشغيل هذه الأوامر للتحقق من تثبيت 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
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر مفيدة

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
```

معلومات ذات صلة

- دليل تكوين الأمان: Unified Threat Defense، Cisco IOS XE 17
- دليل تكوين الأمان: Unified Threat Defense، Cisco IOS XE 16
- القيود والأنظمة الأساسية المدعومة UTD لـ SDWAN.
- تثبيت UTD باستخدام vManage.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).