

cEdgeルータへのUTDセキュリティ仮想イメージのインストール

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Cisco IOS XE SDWANソフトウェア\(16.x\)が稼働するルータ](#)

[Cisco IOS XEソフトウェア\(17.x\)が稼働するルータ](#)

[設定](#)

[ステップ1：仮想イメージのアップロード](#)

[ステップ2：セキュリティポリシーとコンテナプロファイルサブテンプレートデバイステンプレートに追加する](#)

[ステップ3：セキュリティポリシーとコンテナプロファイルでデバイステンプレートを更新または添付する](#)

[確認](#)

[一般的な問題](#)

[問題1：エラー：次のデバイスにはコンテナソフトウェアサービスがありません](#)

[問題2：使用可能なメモリが不十分](#)

[問題3.不正参照](#)

[問題4:UTDがインストールされ、アクティブだが、有効になっていない](#)

[関連情報](#)

概要

このドキュメントでは、Cisco IOS XE SD-WANデバイスでセキュリティ機能を有効にするためにUnified Threat Defense(UTD)セキュリティ仮想イメージをインストールする方法について説明します。

前提条件

- これらの機能を使用する前に、関連するセキュリティ仮想イメージをvManageリポジトリにアップロードします。
- cEdgeルータは、テンプレートが事前に添付されたvmanageモードである必要があります。
- 侵入防御システム(IPS)、侵入検知システム(IDS)、URLフィルタリング(URL-F)、または高度なマルウェア防御(AMP)フィルタリングのセキュリティポリシーテンプレートを作成します。
- 。

要件

- 4000サービス統合型ルータCisco IOS XE SD-WAN(ISR4k)

- 1000サービス統合型ルータCisco IOS XE SD-WAN(ISR1k)
- 1000vクラウドサービスルータ(CSR1kv)
- 1000vサービス統合型ルータ(ISRv)
- 8 GB DRAMをサポートするcEdgeプラットフォーム

使用するコンポーネント

- Cisco UTD仮想イメージ
- vManageコントローラ
- コントローラとの制御接続を持つcEdgeルータ。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco UTDイメージをインストールするには、デバイステンプレートにセキュリティポリシーが必要です。また、cEdgeルータでは、Intrusion Prevention System(IPS)、Intrusion Detection System(IDS)、URL Filtering(URL-F)、Advanced Malware Protection(AMP)などのセキュリティ機能が有効になっている必要があります。

[Software Cisco](#)からCisco UTD Snort IP Engineソフトウェアをダウンロードします。

現在のCisco IOS XEバージョンでサポートされているCisco UTD仮想イメージの正規表現を使用します。**show utd engine standard**コマンドを使用して、推奨およびサポートされているUTDイメージを検証します。

```
Router01# show utd engine standard version
IOS-XE Recommended UTD Version: 1.0.13_SV2.9.16.1_XE17.3
IOS-XE Supported UTD Regex: ^1\.0\.[0-9]+\_SV(\.*)_XE17.3$
```

注イメージをダウンロードするパスは、ルータでCisco IOS XE SDWANソフトウェア(16.x)またはユニバーサルCisco IOS XEソフトウェア(17.x)が稼働しているかどうかによって異なります。

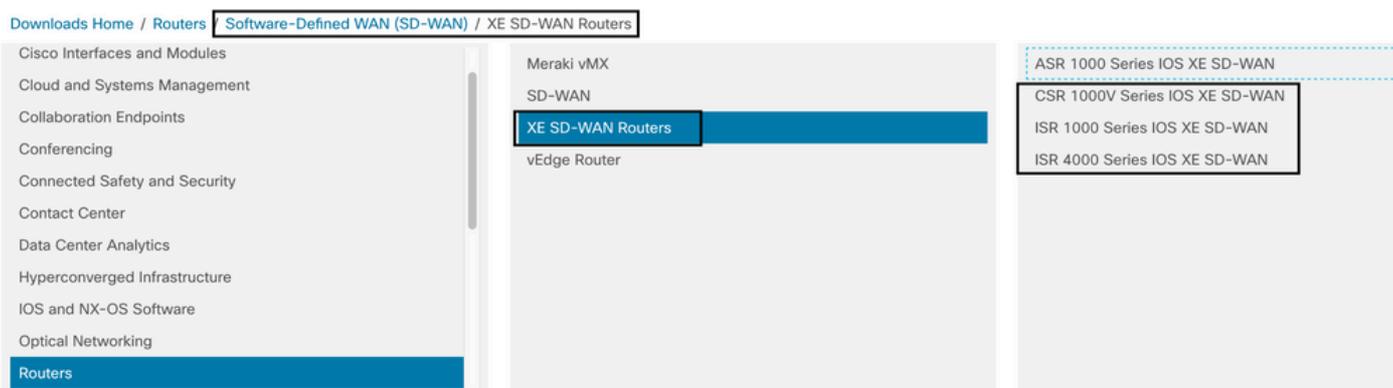
Cisco IOS XE SDWANソフトウェア(16.x)が稼働するルータ

Cisco UTD Snort IPS Engineソフトウェアを入手する方法は、ルータ/ソフトウェア定義型WAN(SD-WAN)/XE SD-WANルータ/およびシリーズ統合型ルータです。



cEdgeルータのモデルタイプを選択します。

注シリーズアグリゲーションサービスルータ(ASR)は、UTD機能では使用できません。



ルータモデルのタイプを選択したら、[Cisco IOS XE SD-WAN software] オプションを選択して、16.xバージョンのcEdge用のUTDパッケージを取得します。

Downloads Home / Routers / Software-Defined WAN (SD-WAN) / XE SD-WAN Routers / ISR 4000 Series IOS XE SD-WAN

Select a Software Type

[IOS XE In-Service Software Upgrade \(ISSU\) Matrix](#)

[IOS XE SD-WAN Software](#)

[IOS XE Software](#)

注 cEdgesルータ用に16.xコード用のCisco UTD仮想イメージを選択するダウンロードパスには、Cisco IOS XEソフトウェアオプションも示されています。これは17.x用のcEdgeのアップグレードコードを選択するパスですが、バージョン17.x用のUTD仮想イメージが見つかりません。Cisco Unifiedの通常のCisco IOS XEおよびCisco IOS XE SDWANコードは17.xおよび最新であるため、17.x用のCisco UTD仮想イメージを取得するパスは、通常のCisco IOS XEコードと同じです。

cEdgeの現在のバージョンを選択し、そのバージョンのUTDパッケージをダウンロードします。

Search...

Expand All Collapse All

Suggested Release

16.12.5(MD)

Latest Release

16.12.5(MD)

All Release

16

Deferred Release

16

ISR 4000 Series IOS XE SD-WAN

Release 16.12.5 **MD**

My Notifications

Related Links and Documentation

[Release Notes for 19.2.4](#)

[Release Notes for 16.12.5](#)

File Information	Release Date	Size	
Cisco ISR 4200 Series IOS XE SD-WAN Software isr4200-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	482.84 MB	↓ 🛒 📄
Cisco ISR 4300 Series IOS XE SD-WAN Software isr4300-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	557.83 MB	↓ 🛒 📄
Cisco ISR 4400 Series IOS XE SD-WAN Software isr4400-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	621.88 MB	↓ 🛒 📄
Cisco ISR 4400v2 Series IOS XE SD-WAN Software isr4400v2-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	623.49 MB	↓ 🛒 📄
UTD Engine for IOS XE SD-WAN secapp-ucmk9.16.12.05.1.0.18_SV2.9.16.1_XE16.12.x86_64.tar Advisories	29-Jan-2021	52.01 MB	↓ 🛒 📄

Cisco IOS XEソフトウェア(17.x)が稼働するルータ

Cisco IOS XEリリース17.2.1rおよび最新バージョンでは、universalk9イメージを使用して、Cisco IOS XE SD-WANとCisco IOS XEの両方をCisco IOS XEデバイスに導入します。UTD Snort IPSエンジンソフトウェアは、[Routers] > [Branch Routers] > [Series Integrated Router]にあります。

Downloads Home **Routers / Branch Routers**

- Cisco Interfaces and Modules
- Cloud and Systems Management
- Collaboration Endpoints
- Conferencing
- Connected Safety and Security
- Contact Center
- Data Center Analytics
- Hyperconverged Infrastructure
- IOS and NX-OS Software
- Optical Networking
- Routers**

Branch Routers

- Cloud Connectors
- Cloud Edge
- Data Center Interconnect Platforms
- Industrial Routers and Gateways
- Mobile Internet Routers
- Network Functions Virtualization
- Service Provider Core Routers
- Service Provider Edge Routers
- Service Provider Infrastructure Software
- Small Business Routers

- 1000 Series Integrated Services Routers**
- 1800 Series Integrated Services Routers
- 1900 Series Integrated Services Routers
- 2900 Series Integrated Services Routers
- 3900 Series Integrated Services Routers
- 4000 Series Integrated Services Routers
- 5000 Series Enterprise Network Compute System
- 800 Series Routers
- 900 Series Integrated Services Routers
- Catalyst 8200 Series Edge Platforms
- Catalyst 8300 Series Edge Platforms

ルータのモデルタイプを選択したら、UTD Snort IPS Engine Softwareを選択します。

Software Download

[Downloads Home](#) / [Routers](#) / [Branch Routers](#) / [4000 Series Integrated Services Routers](#) / [4221 Integrated Services Router](#)

Downloads Home

Select a Software Type

[IOS XE In-Service Software Upgrade \(ISSU\) Matrix](#)

[IOS XE Patch Upgrades](#)

[IOS XE ROMMON Software](#)

[IOS XE SD-WAN Software](#)

[IOS XE Software](#)

[UTD Snort IPS Engine Software](#)

[UTD Snort Subscriber Signature Package](#)

[Very High Bitrate \(VDSL\) PHY Firmware](#)

[Very High Bitrate DSL \(VDSL\) Firmware](#)

ルータの現在のバージョンを選択し、選択したバージョンのUTDパッケージをダウンロードします。

Software Download

[Downloads Home](#) / [Routers](#) / [Branch Routers](#) / [4000 Series Integrated Services Routers](#) / [4221 Integrated Services Router](#) / [UTD Snort IPS Engine Software- 17.7.1a](#)

[Expand All](#) [Collapse All](#)

Latest Release

- 17.7.1a**
- Fuji-16.9.8
- 16.6.7a

All Release

- 16.6
- 17
- 16

4221 Integrated Services Router

Release 17.7.1a

[My Notifications](#)

[Related Links and Documentation](#)
- No related links or documentation -

File Information	Release Date	Size
UTD Engine OVA for 17.7.1 release iosxe-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.ova Advisories	30-Nov-2021	147.72 MB
UTD Engine for IOS XE secapp-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.tar Advisories	30-Nov-2021	52.51 MB

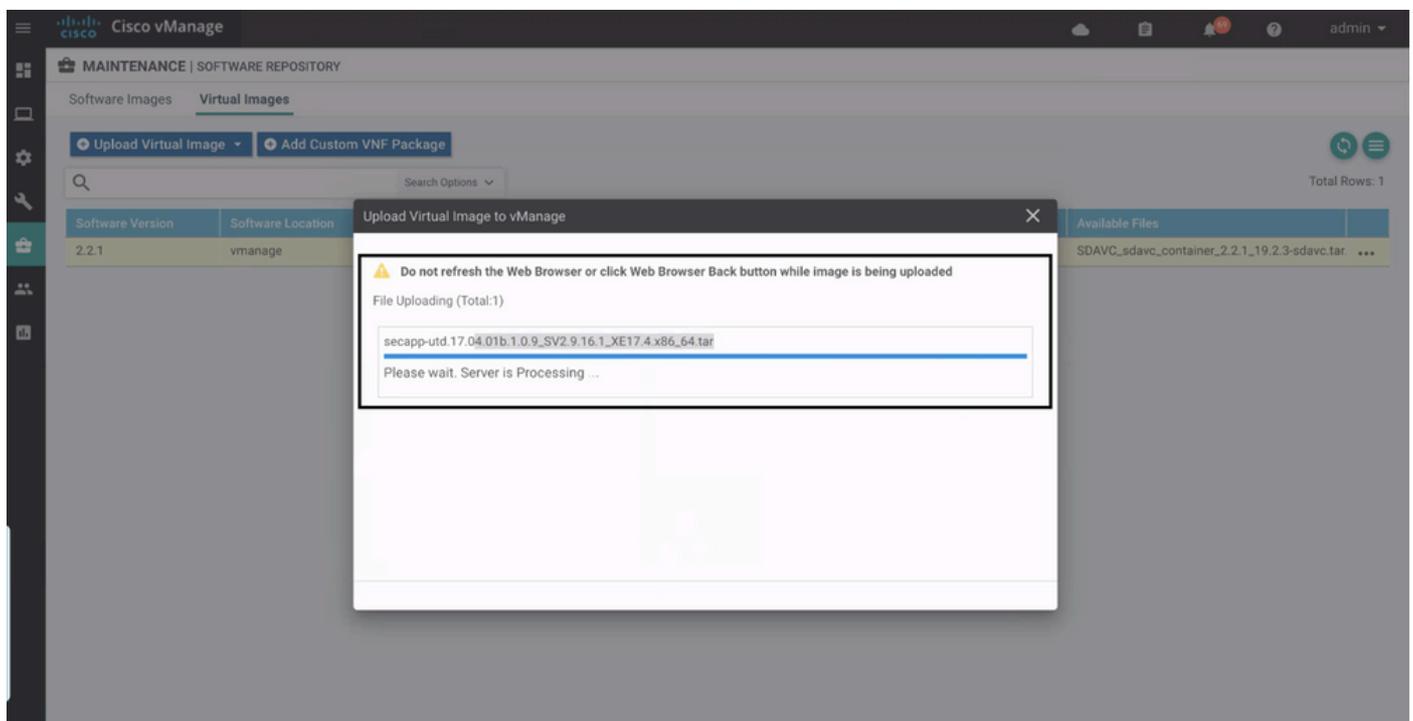
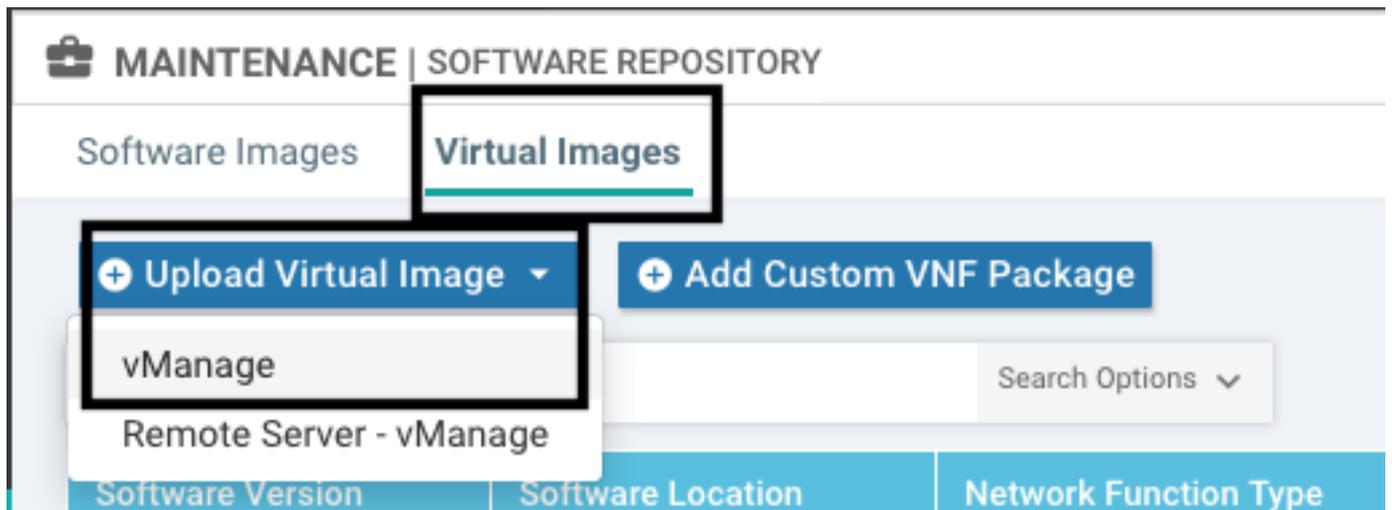
注：Viptelaコードの代わりにCisco IOS XEソフトウェアを実行するCisco ISR1100Xシリーズルータ（Cisco NutellaルータSR1100X-4G/6G）は、x86_x64に基づいています。ISR4K用に公開されたCisco UTD仮想イメージは、このルータで動作します。現在のCisco IOS XE SDWANバージョンと同じCisco UTDイメージコードバージョンをNutellaルータにインストールできます。**show utd engine standard version**コマンドを使用して、推奨およびサポートされる正規表現のCisco UTDイメージを検証します。

設定

ステップ1：仮想イメージのアップロード

仮想イメージがcEdge上の現在のCisco IOS XE SDWANコードと一致していることを確認し、それをvmanageリポジトリにアップロードします。

[Maintenance] > [Software Repository] > [Virtual Image] > [Upload Virtual Image] > [vManage] に移動します。



Cisco UTD仮想イメージが正常にアップロードされたら、リポジトリ上にあることを再確認します。



Cisco vManage MAINTENANCE | SOFTWARE REPOSITORY

Software Images Virtual Images

Upload Virtual Image Add Custom VNF Package

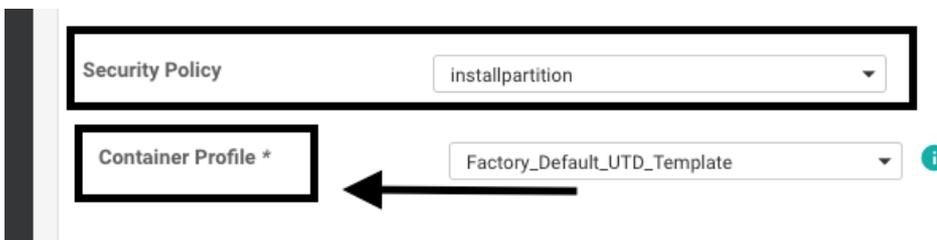
Search Options

Total Rows: 8

Software Version	Software Location	Network Function	Type	Image Type	Architecture	Version Type Name	Vendor	Available Files	Updated On
1.0.16_SV2.9.16.1_XE17.3	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.16...	05 Nov 2021 2:39:19 PM ...
1.0.13_SV2.9.16.1_XE17.2	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.13...	05 Nov 2021 11:31:22 A...
1.0.12_SV2.9.16.1_XE17.4	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.12...	05 Nov 2021 3:51:20 PM...
1.0.12_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	aarch64	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aarch64_1.0.12...	24 Jul 2020 10:50:24 AM...
1.0.12_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.12...	24 Jul 2020 10:50:17 AM...
1.0.10_SV2.9.13.0_XE17.3	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.10...	16 Jan 2021 9:40:36 PM...
1.0.10_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.10...	18 May 2020 10:10:22 A...
1.0.10_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	aarch64	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aarch64_1.0.10...	06 Feb 2020 9:39:51 AM...

ステップ2: セキュリティポリシーとコンテナプロファイルサブテンプレートをデバイステンプレートに追加する

以前に作成したセキュリティポリシーをデバイステンプレートに追加します。セキュリティポリシーには、デバイステンプレートに対するIPS/IDS、URL-F、またはAMPフィルタリングポリシーが必要です。コンテナプロファイルを自動的に開きます。デフォルトのコンテナプロファイルを使用するか、必要に応じて変更します。



ステップ3: セキュリティポリシーとコンテナプロファイルでデバイステンプレートを更新または添付する

テンプレートを更新するか、cEdgeルータに添付します。config diffで、IPS/IDS、URL-F、またはAMPフィルタリング機能のアプリケーションホスティング設定とUTDエンジンが設定されていることに注目してください。

```

258 app-hosting appid utd
259 app-resource package-profile cloud-low
260 app-vnic gateway0 virtualportgroup 0 guest-interface 0
261 guest-ipaddress 192.168.1.2 netmask 255.255.255.252
262 !
263 app-vnic gateway1 virtualportgroup 1 guest-interface 1
264 guest-ipaddress 192.0.2.2 netmask 255.255.255.252
265 !
266 start
267 !
258 268 !ldp run
259 269 nat64 translation timeout tcp 60
260 270 nat64 translation timeout udp 1
271
272 utd multi-tenancy
273 utd engine standard multi-tenancy
274 threat-inspection profile GPC_IPS_v06_copy_copy
275 threat detection
276 policy security
277 logging level warning
278 !
279 utd global
280 !
281 !
282 policy
283 no app-visibility
284 no flow-visibility
285 no implicit-acl-logging
286 log-frequency 1000

```

vmanageは、適用された設定にUTDエンジン機能があることを認識したため、テンプレートのステータスをDone-scheduledに変更します。そのため、vmanageは、UTDセキュリティ機能を使用するためにインストールされた仮想イメージがcEdgeに必要なであると判断します。

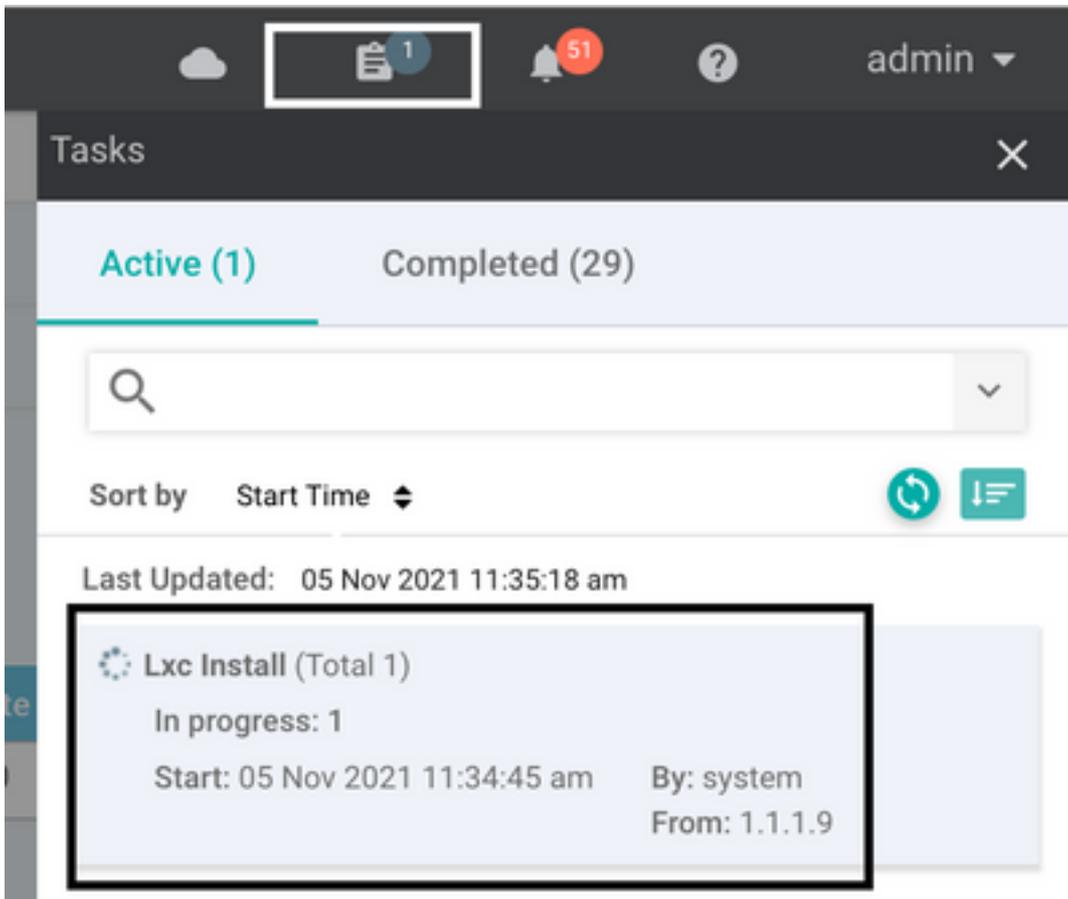
Push Feature Template Configuration | Validation Success

Total Task: 1 | Done - Scheduled : 1

Search Options

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID
Done - Scheduled	Device needs to install some ap...	CSR-FDCDD4AE-4DB9-B79B-8FF...	CSR1000v	ZBFWTest	70.70.70.1	70

テンプレートがスケジュール状態に移動すると、タスクメニューに新しい進行中のタスクが表示されます。新しいタスクはLxc installationです。これは、新しい設定をプッシュする前に、vmanageがcEdgeへの仮想イメージのインストールを自動的に開始することを意味します。



LXコンテナがインストールされると、vManageはUTD機能を使用して事前にスケジュールされた設定をプッシュします。以前に設定がスケジュールされたため、このタスクには新しいタスクはありません。



確認

cEdgeがvManageと同期し、テンプレートが添付されているかどうかを確認します。

[Configuration] > [Devices]に移動します。



MAINTENANCE | SOFTWARE UPGRADE

WAN Edge Controller vManage

1 Rows Selected Upgrade Upgrade Virtual Image Activate Virtual Image Delete Virtual Image Activate Delete Available Software Set Default Version

Device Group All 70.70.70.1 Search Options Total Rows: 1 of 24

Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability*	Current Version	Available Versions	Default Version	Available Services	Up Since
SAASRou...	70.70.70.1	CSR-FDCDD4AE-4DB9-B798-8...	70	CSR1000v	reachable	17.03.03.0.4762		17.03.03.0.4762	0	05 Nov 2021 11:58:00 AM CST

Activate Virtual Image

Following devices do not have container software services.
Click 'Skip Devices' to continue activate image.

- (SAASRouter01)

Skip Devices Cancel

仮想イメージがエラーを送信しました：選択したcEdgeルータにコンテナプロファイルのサブテンプレートを持つセキュリティポリシーがない場合、デバイスにはコンテナソフトウェアサービスがありません。

Additional Templates

AppQoE Choose...

Global Template * Factory_Default_Global_CISCO_Template ⓘ

Cisco Banner Choose...

Cisco SNMP Choose...

CLI Add-On Template Choose...

Policy Choose...

Probes Choose...

Security Policy CHI_Security_Policy_2

Security Policy

Please check the Software Download page to ensure your device container versions are up-to-date with the device version if applicable. It is always recommended that these are aligned. This is an informative message and no action may be required

Container Profile * Factory_Default_UTD_Template ⓘ

UTDパッケージを必要とする侵入防御システム(IPS)、侵入検知システム(IDS)、URLフィルタリ

ング(URL-F)、高度なマルウェア防御(AMP)などのセキュリティ機能を含むセキュリティポリシーを使用すると、このテンプレートが自動的に追加されます。利用できるセキュリティ機能のすべてが、単純なZFW機能のようなUTDエンジンを必要とするわけではありません。

Add Security Policy

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

- Compliance**
Application Firewall | Intrusion Prevention | TLS/SSL Decryption
- Guest Access**
Application Firewall | URL Filtering | TLS/SSL Decryption
- Direct Cloud Access**
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Direct Internet Access**
Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Custom**
Build your ala carte policy by combining a variety of security policy blocks

コンテナプロファイルのサブテンプレートを使用してテンプレートをプッシュすると、vmanageによって仮想イメージが自動的にインストールされます。

問題2：使用可能なメモリが不十分

cEdgeルータに8 GBのDRAMメモリが搭載されていることを確認します。搭載されていない場合は、Lxcインストールプロセスから「**Device is not configured to accept new configuration.Available memory insufficient**」エラーが表示されます。cEdgeルータがUTD機能を使用するための要件は、8 GB以上のDRAMを搭載することです。

The screenshot shows a 'TASK VIEW' window with a table of task results. The table has columns for Status, Device IP, Message, and Start Time. One task is highlighted with a red 'Failure' status. The message column contains the following text:

```
[5-Nov-2021 19:31:09 UTC] Checking if iox is enabled on device  
[5-Nov-2021 19:31:10 UTC] Waiting for iox to be enabled on device  
[5-Nov-2021 19:31:24 UTC] iox enable  
[5-Nov-2021 19:31:24 UTC] iox enabled on device  
[5-Nov-2021 19:31:29 UTC] Failed to install 1/1 lxc container (app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3).  
Pre config validation failed. Device is not configured to accept new configuration. Available memory insufficient, required CPU:7 percent, reserved CPU:0 percent, available CPU:75 percent, required memory:2897152 KB, rese
```

この場合、CSRvには4 GBのDRAMしかありません。メモリを8 GB DRAMにアップグレードすると、インストールは成功します。

`show sdwan system status`の出力で、現在の合計メモリを確認します。

```
Router01# show sdwan system status
```

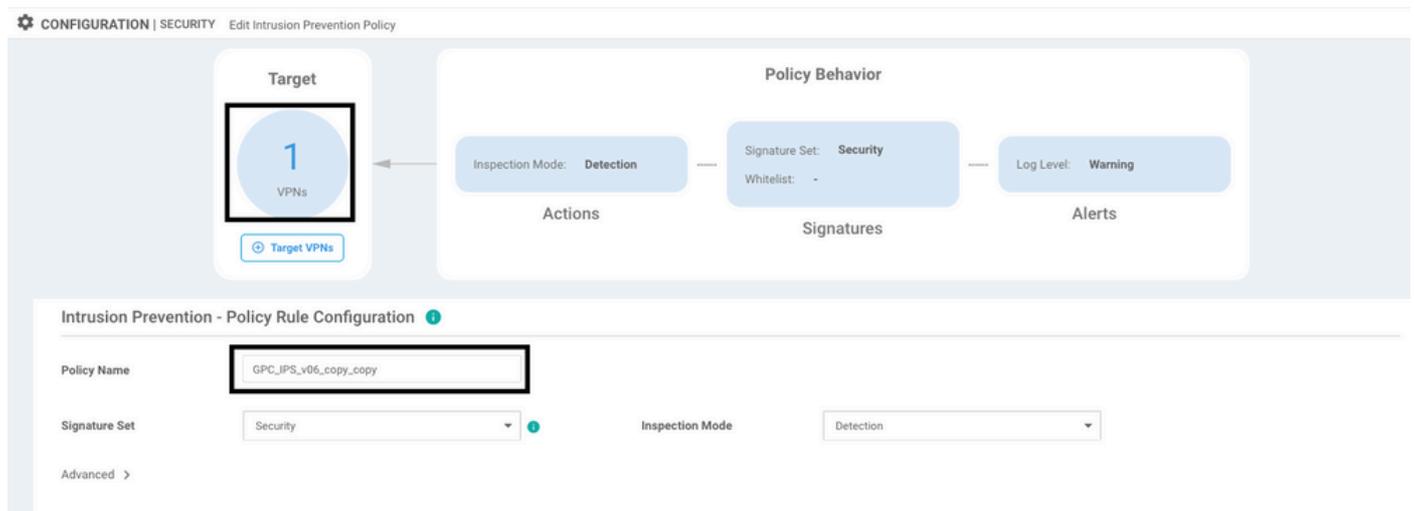
Memory usage: 8107024K total, 3598816K used, 4508208K free
349492K buffers, 2787420K cache

問題3.不正参照

セキュリティポリシー機能で使用するVPN/VRFがcEdgeルータですすでに設定されていることを確認して、セキュリティポリシーシーケンスの不正な参照を回避します。



この例では、セキュリティポリシーにVPN/VRF 1の侵入防御ポリシーがありますが、デバイスにはVRF 1が設定されていません。そのため、vmanageはそのポリシーシーケンスに対して不正な参照を送信します。



セキュリティポリシーに記載されているVRFを設定した後、不正な参照が表示されず、テンプレートが正常にプッシュされます。

問題4:UTDがインストールされ、アクティブだが、有効になっていない

デバイスにセキュリティポリシーが設定されており、UTDがインストールされてアクティブになっていますが、有効になっていません。

この問題は問題番号3に関連していますが、vManageでは、デバイスに設定されていないVRFを参照するように設定を許可しており、ポリシーはどのVRFにも適用されていません。

ルータがこの問題に直面しているかどうかを判別するには、UTDがアクティブであることを確認する必要があります。UTD not enabledメッセージとポリシーがVRFを参照しません。

```
Router01# show utd engine standard status
```

```
UTD engine standard is not enabled <<<<<<<<<<<<
```

```
ISR01#show sdwan virtual-application utd
```

```
VERSION ACTIVE PREVIOUS TIMESTAMP
```

```
-----  
1.0.16_SV2.9.16.1_XE17.3 true true 2022-06-10T13:29:43-00:00
```

この問題を解決するには、ターゲットVPNを確認し、設定したVRFにポリシーが適用されていることを確認します。

関連情報

- [ルータセキュリティ：ルータ上のSnort IPS](#)
- [Cisco SD-WANセキュリティ設定ガイド、Cisco IOS XEリリース](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。