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

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。

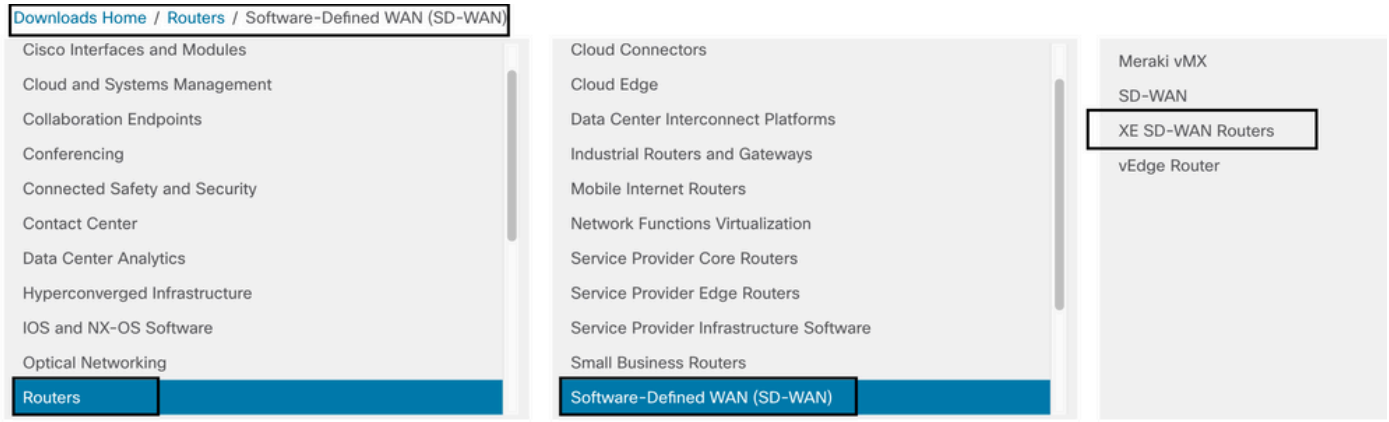
現在のCisco IOS XEバージョンでサポートされているCisco UTD仮想イメージの正規表現を使用します。**show utd engine standard**コマンドを使用して、推奨およびサポートされているUTDイメージを検証します。

```
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。

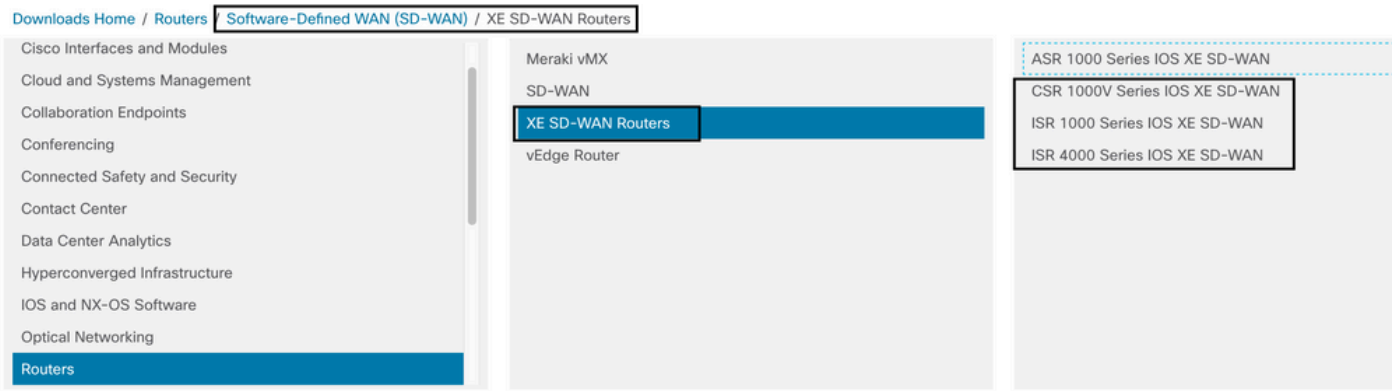
Cisco IOS XE SDWANソフトウェア(16.x)が稼働するルータ

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。

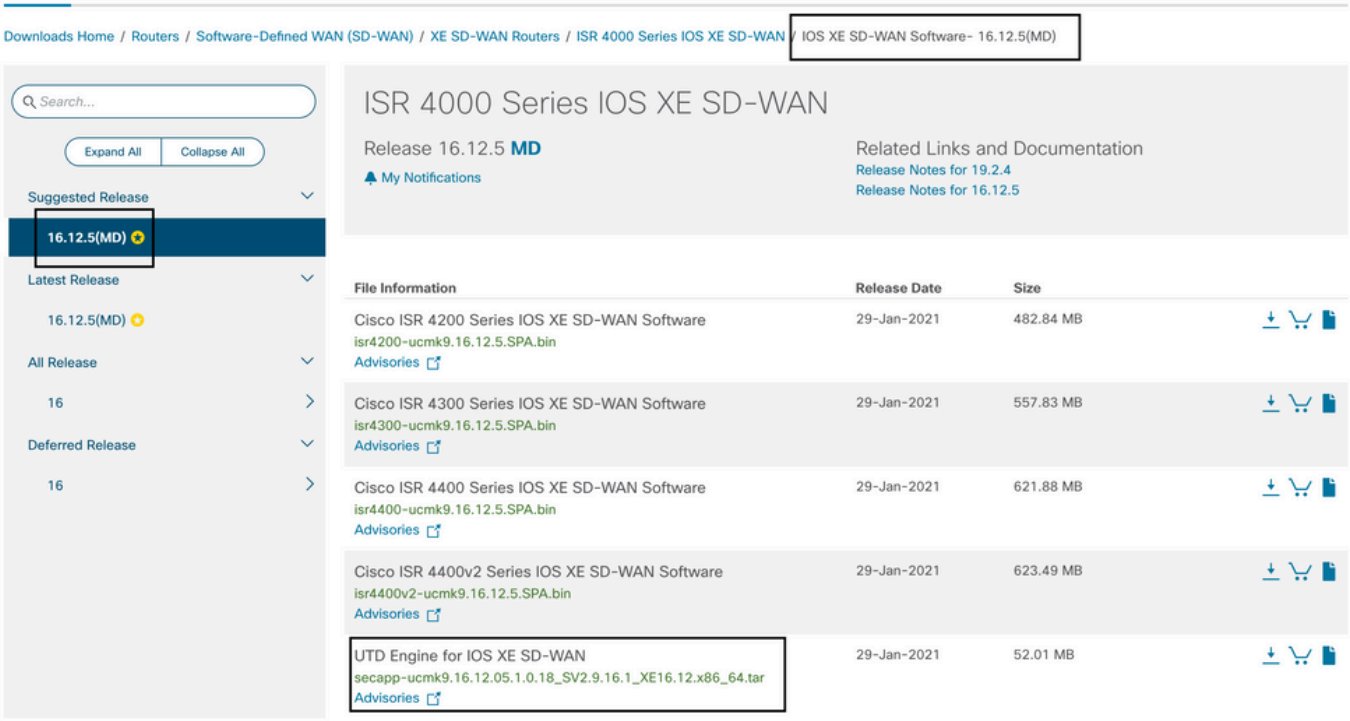
注シリーズアグリゲーションサービスルータ(ASR)は、UTD機能では使用できません。



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。

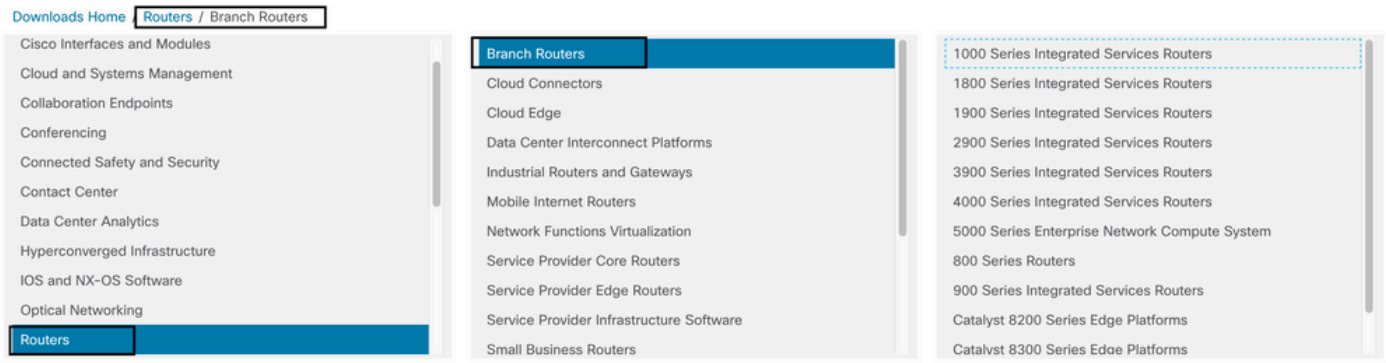
注 cEdgesルータ用に16.xコード用のCisco UTD仮想イメージを選択するダウンロードパスには、**Cisco IOS XEソフトウェアオプションも示されて**います。これは17.x用のcEdgeのアップグレードコードを選択するパスですが、バージョン17.x用のUTD仮想イメージが見つかりません。Cisco Unifiedの通常のCisco IOS XEおよびCisco IOS XE SDWANコードは17.xおよび最新であるため、17.x用のCisco UTD仮想イメージを取得するパスは、通常のCisco IOS XEコードと同じです。

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。

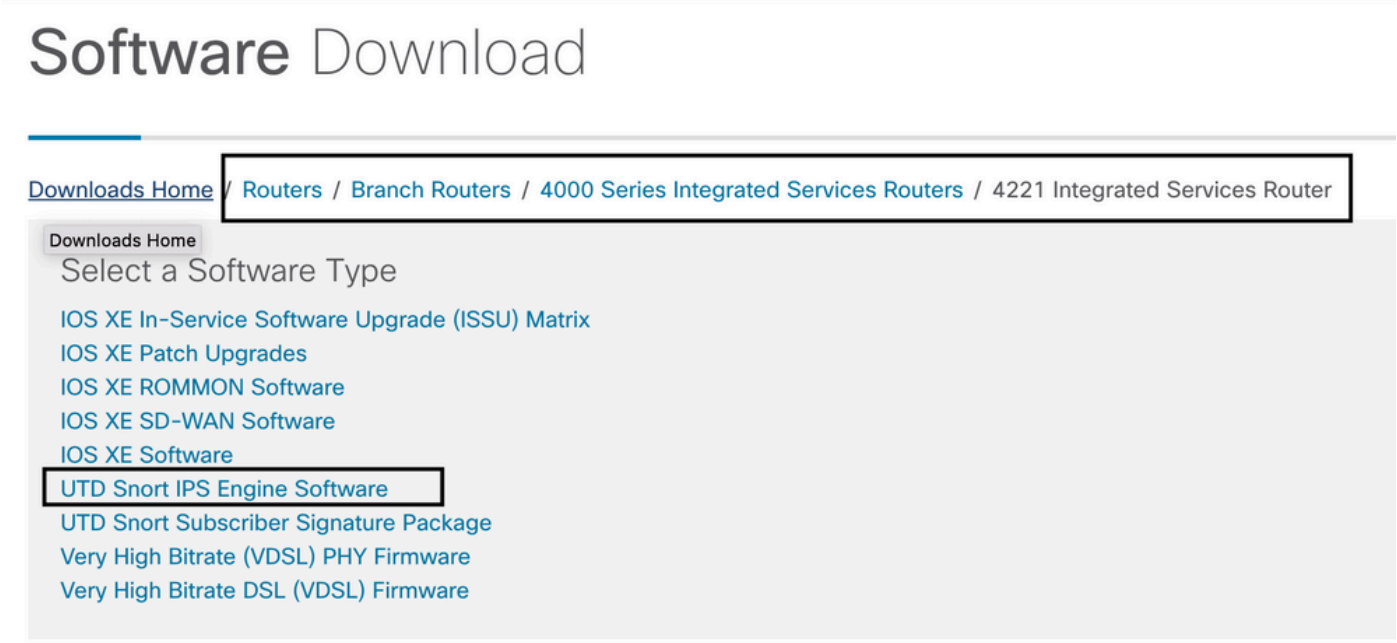


Cisco IOS XEソフトウェア(17.x)が稼働するルータ

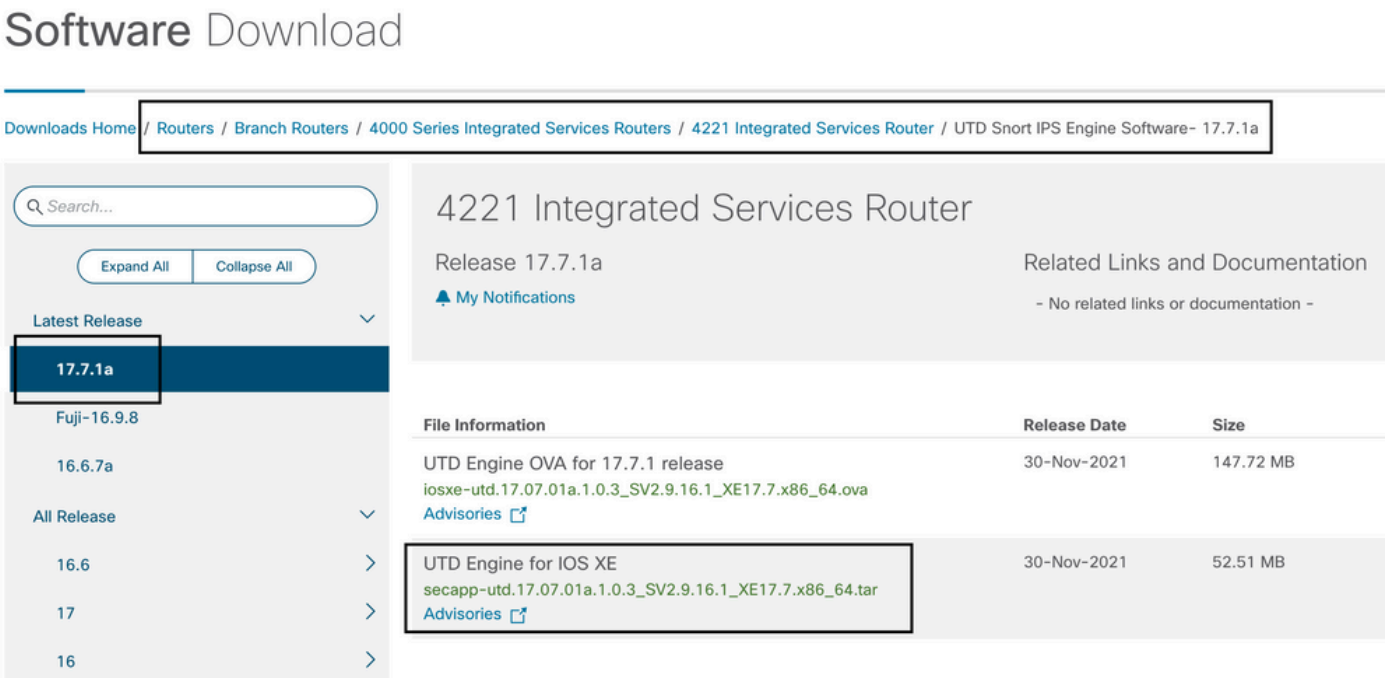
Cisco IOS XEリリース17.2.1rおよび最新バージョンでは、universalk9イメージを使用して、Cisco IOS XE SD-WANとCisco IOS XEの両方をCisco IOS XEデバイスに導入します。**UTD Snort IPSエンジンソフトウェア**は、**[Routers] > [Branch Routers] > [Series Integrated Router]にあります。**



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。



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。

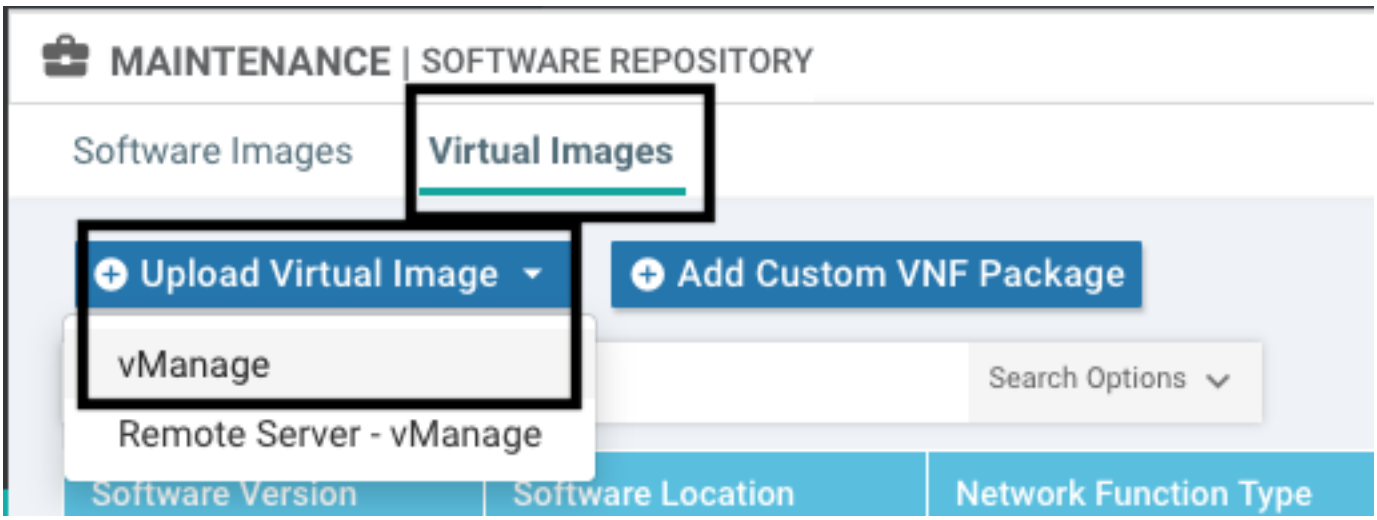


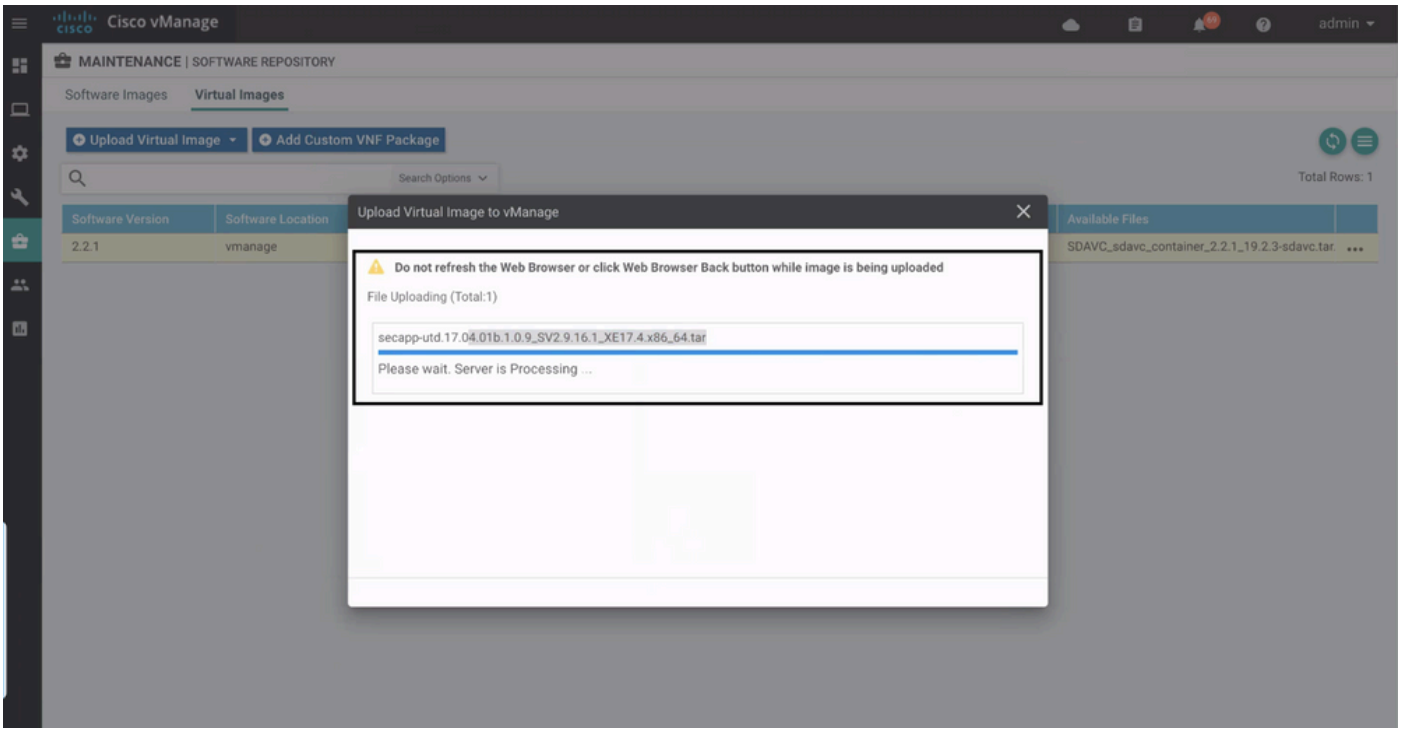
注：Viptelaコードの代わりにCisco IOS XEソフトウェアを実行するCisco ISR1100Xシリーズルータ（Cisco NutellaルータSR1100X-4G/6G）は、x86_x64に基づいています。ISR4K用に公開されたCisco UTD仮想イメージは、このルータで動作します。現在のCisco IOS XE SDWANバージョンと同じCisco UTDイメージコードバージョンをNutellaルータにインストールできます。**show utd engine standard version**コマンドを使用して、推奨およびサポートされる正規表現のCisco UTDイメージ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

設定

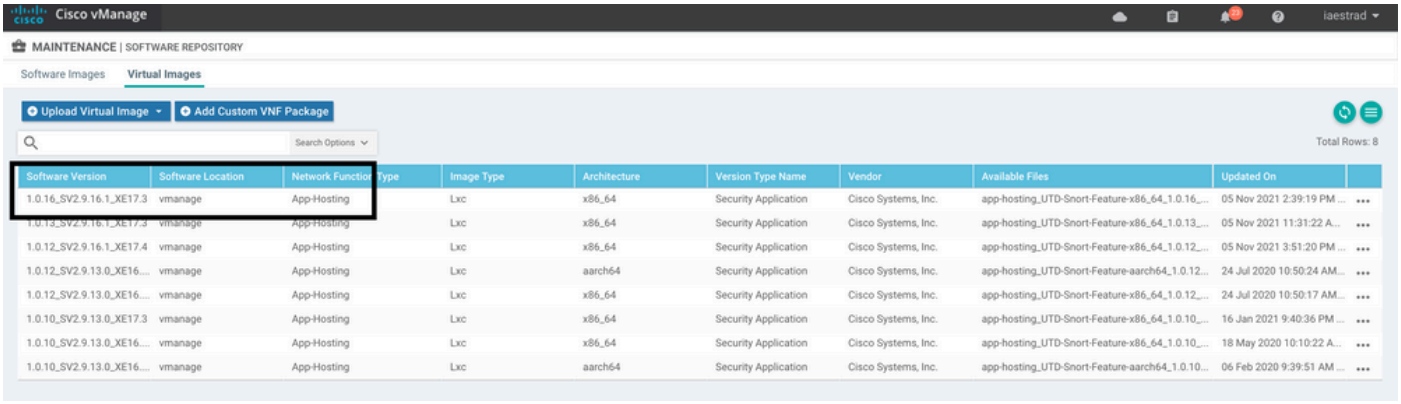
ステップ1：仮想イメージのアップロード

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。



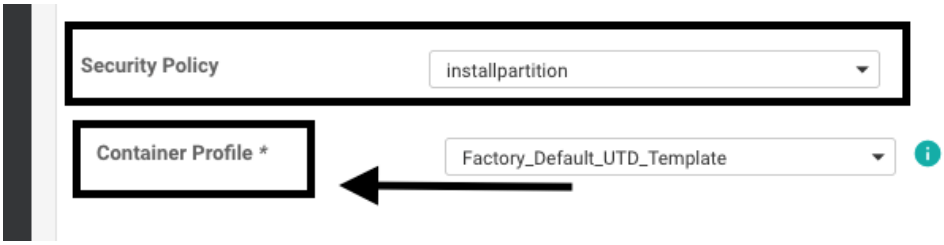


Cisco UTD仮想イメージが正常にアップロードされたら、リポジトリ上にあることを再確認します。



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。

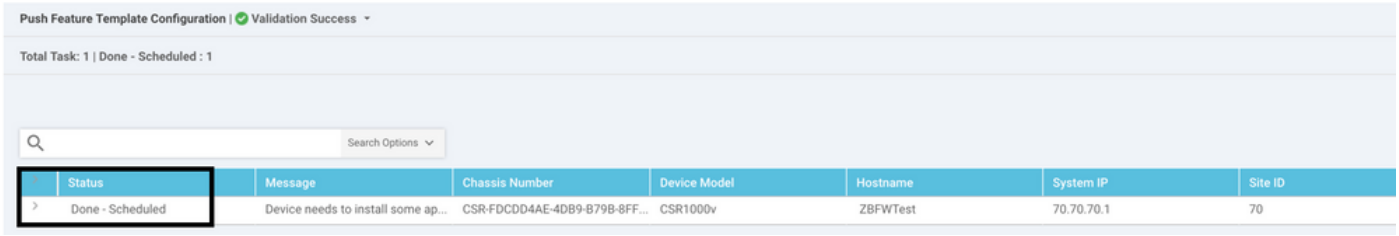


ステップ3：セキュリティポリシーとコンテナプロファイルでデバイステンプレートを更新または添付する

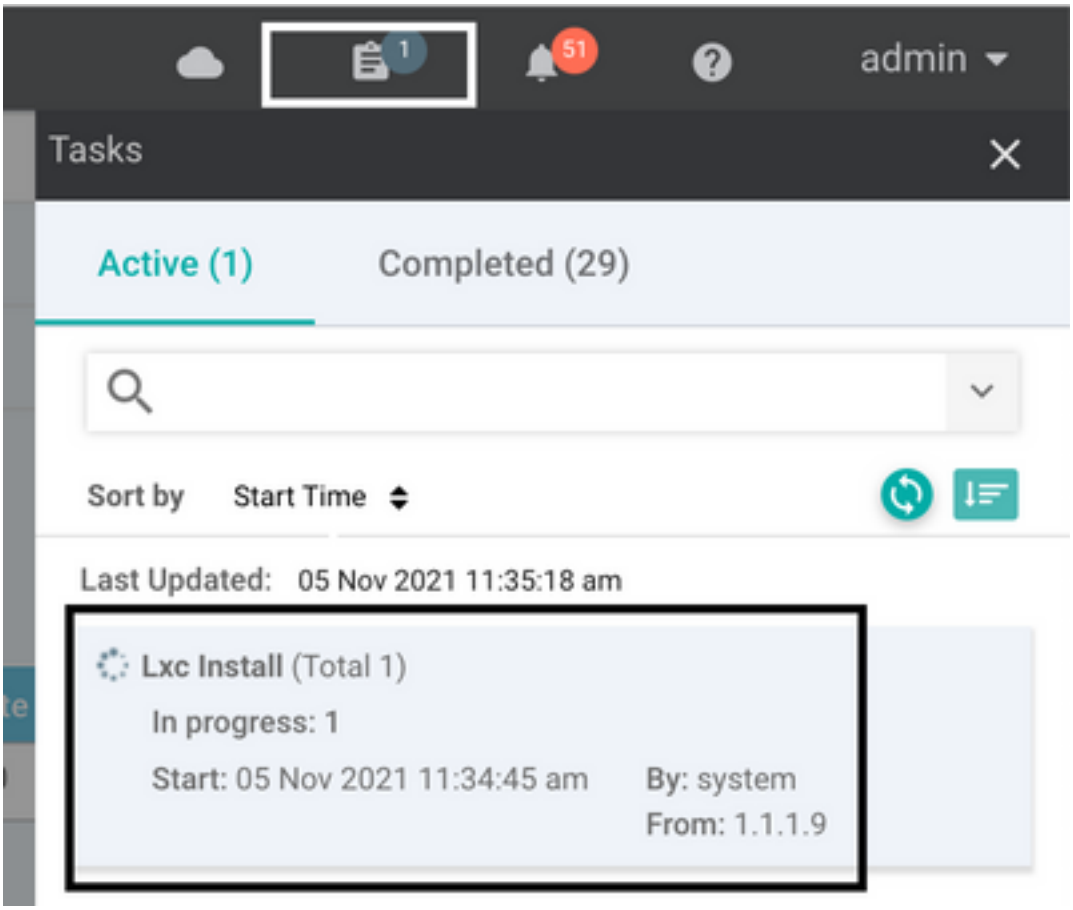
テンプレートを更新するか、cEdgeルータに添付します。config diffで、IPS/IDS、URL-F、またはAMPフィルタリング機能のアプリケーションホスティング設定とUTDエンジンが設定されていることに注目してください。

```
app-hosting appid utd
 app-resource package-profile cloud-low
 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 192.0.2.2 netmask 255.255.255.252
 !
 start
!
lldp run
nat64 translation timeout tcp 60
nat64 translation timeout udp 1
utd multi-tenancy
utd engine standard multi-tenancy
 threat-inspection profile GPC_IPS_v06_copy_copy
  threat detection
  policy security
  logging level warning
 !
 utd global
 !
!
policy
 no app-visibility
 no flow-visibility
 no implicit-acl-logging
 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に必要であると判断します。



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。

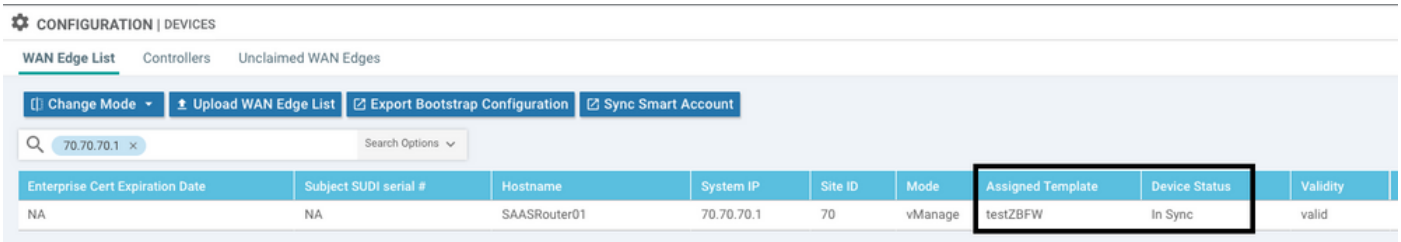


LXコンテナがインストールされると、vManageはUTD機能を使用して事前にスケジュールされた設定をプッシュします。以前に設定がスケジュールされたため、このタスクには新しいタスクはありません。

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。



Cisco UTDバージョンがインストールされているかどうかを確認します。

```
Router02# show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.12_SV2.9.16.1_XE17.4
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.4$
UTD Installed Version: 1.0.12_SV2.9.16.1_XE17.4         <<<<<<<<<<<<<<<<<<
```

注：UTDのインストール済みバージョンを**UNSUPPORTED**状態にすることはできません。

次の出力で、UTDが実行状態で**ある**かどうかを確認します。

```
Router02# show app-hosting list
App id                                   State
---------------------------------------------------------
utd                                      RUNNING      <<<<<<<<<<<<<<<<<<
```

次のコマンドは、前のコマンドを要約し、現在のステータスとバージョンを表示します。

```
Router02# show app-hosting detail appid utd
App id                 : utd
Owner                  : ioxm
State                  : RUNNING      <<<<<<<<<<<<<<<<<<<<<<<<
Application
  Type                 : LXC
  Name                 : UTD-Snort-Feature
  Version              : 1.0.12_SV2.9.16.1_XE17.4    <<<<<<<<<<<<<<<<<
  Description          : Unified Threat Defense
  Path                 : /bootflash/.UTD_IMAGES/iox-utd_1.0.12_SV2.9.16.1_XE17.4.tar
  URL Path             :
Activated profile name : cloud-low

Resource reservation
  Memory               : 2048 MB
  Disk                 : 861 MB
  CPU                  :
  CPU-percent          : 7 %
  VCPU                 : 0
```

Show utd engine standard statusコマンドは、UTDエンジンのヘルスステータスと、シグニチャアップデートを取得するリスト時間を表示します。

```
Router02# show utd engine standard status
Engine version       : 1.0.6_SV2.9.13.0_XE17.2
Profile              : Cloud-Low
System memory        :
              Usage  : 20.10 %
              Status : Green
Number of engines    : 1

Engine        Running    Health     Reason
=======================================
Engine(#1):   Yes        Green      None      <<<<<<<<<<<<<<<<<<<<<<<<<<<
=====================================================

Overall system status: Green    <<<<<<<<<<<<<<<<<<<<<<<<<<

Signature update status:
```

```
=========================
Current signature package version: 29130.156.s
Last update status: Successful
Last successful update time: Wed Nov 25 07:27:35 2020 EDT   <<<<<<<<<<<<<<<<<<<
Last failed update time: None
Last failed update reason: None
Next update scheduled at: None
Current status: Idle
```

次のコマンドを使用して、有効になっている機能を確認します。

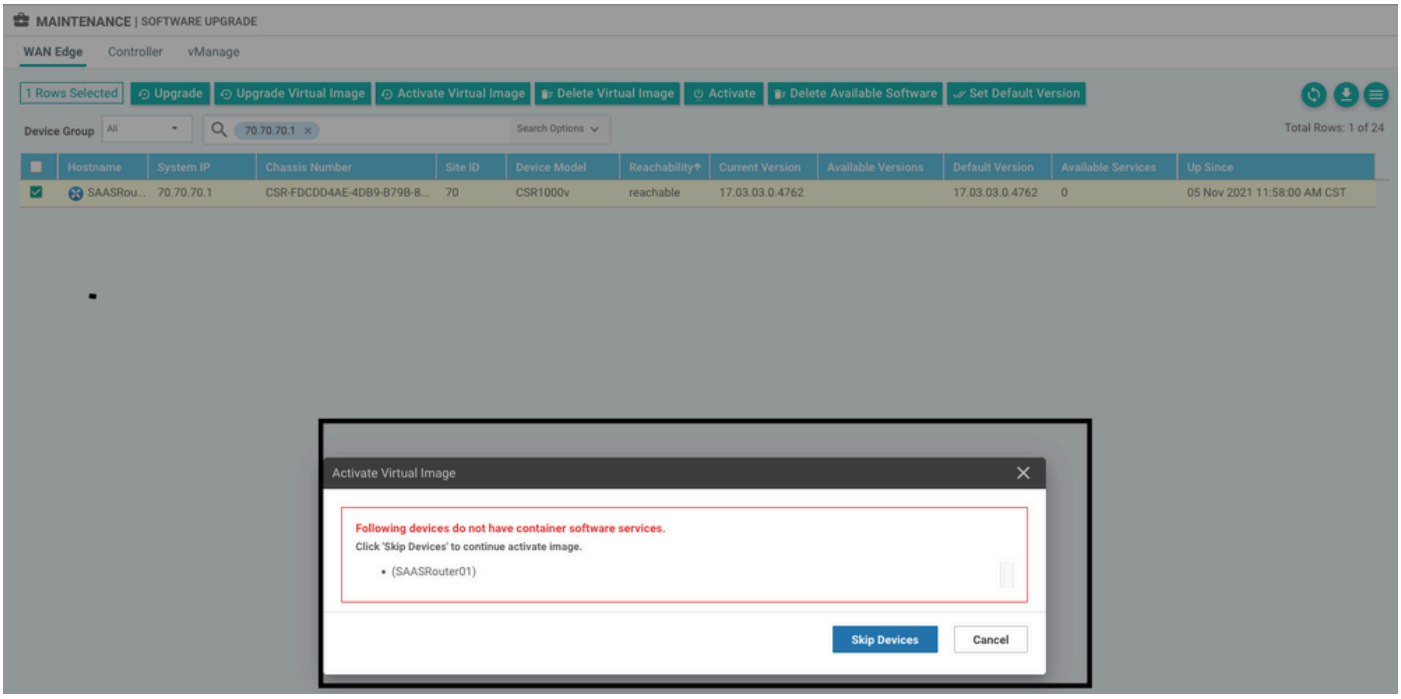
```
Router02# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
  Divert controller mode: enabled
  SN threads: 12
  CFT inst_id 0 feat id 2 fo id 2 chunk id 13
  Max flows: 55000
  SN Health: channel: Threat Defense : Green
  SN Health: channel: Service : Down

  Context Id: 0, Name: Global domain Security Context

   Ctx Flags: (0x1c70001)
        Engine: Standard
        State            : Enabled
        SN Redirect Mode : Fail-open, Divert
        Threat-inspection: Enabled, Mode: IPS
        Domain Filtering : Not Enabled
        URL Filtering    : Enabled   <<<<<<<<<<<
        File Inspection  : Enabled   <<<<<<<<<<<
        All Interfaces   : Enabled
```

一般的な問題

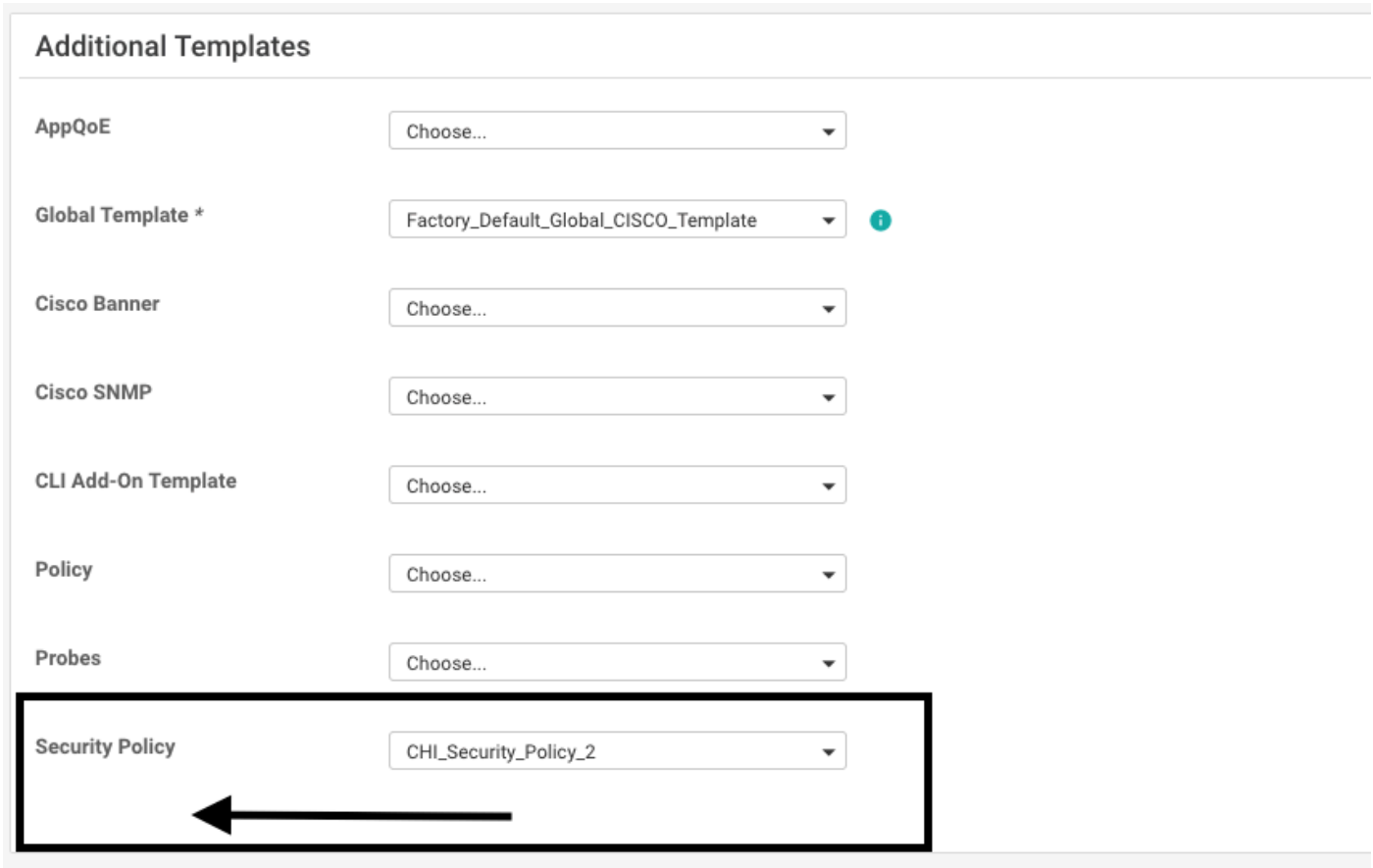
問題1：エラー：次のデバイスにはコンテナソフトウェアサービスがありません

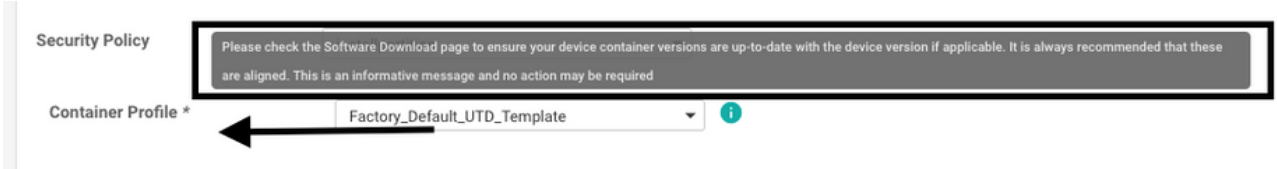
仮想イメージをアクティブにします。

[maintenance] > [software] > [activate]に移動します。



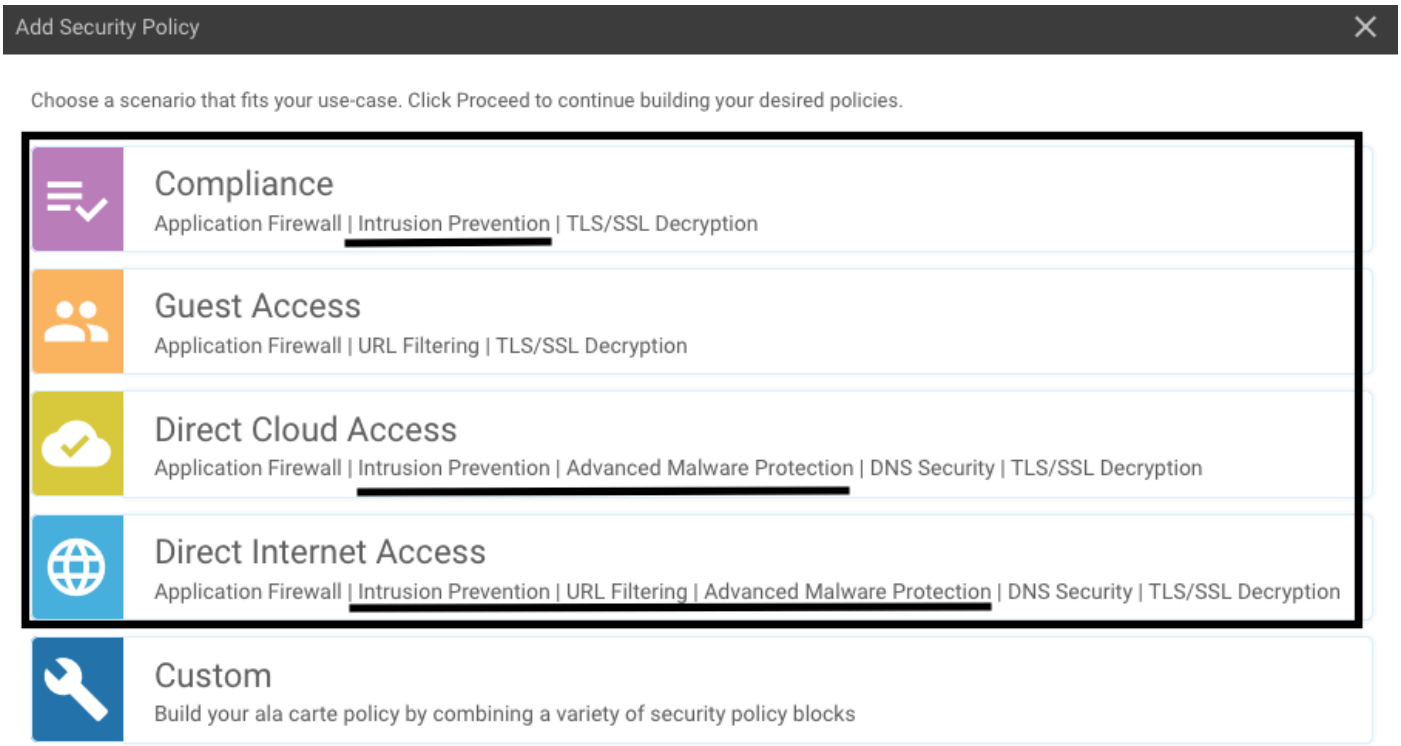
仮想イメージがエラーを送信しました：**選択したcEdgeルータにコンテナプロファ**イルのサブテンプレートを持つセキュリティポリシーがない場合、デバイスにはコンテナソフトウェアサービスがありません。





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

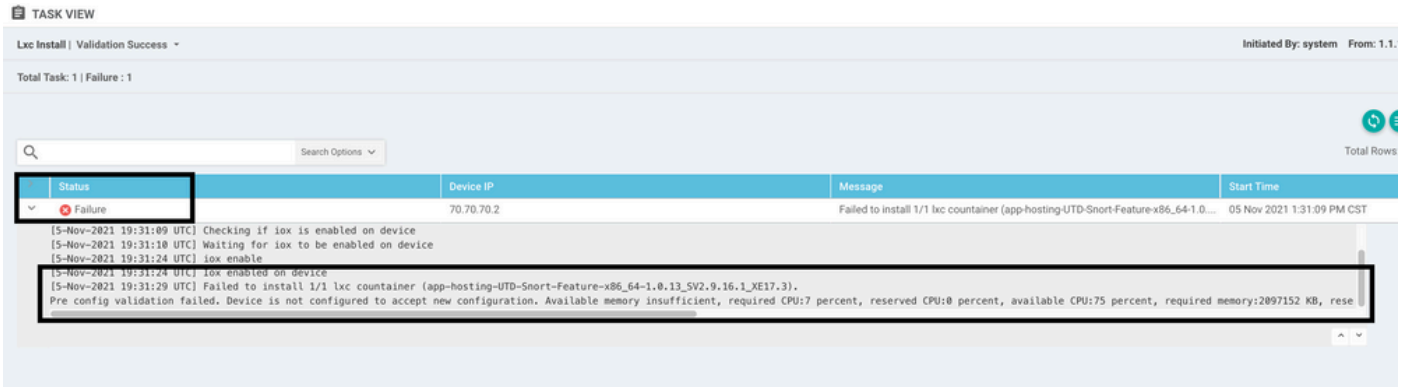
ング(URL-F)、高度なマルウェア防御(AMP)などのセキュリティ機能を含むセキュリティポリシーを使用すると、このテンプレートが自動的に追加されます。利用できるセキュリティ機能のすべてが、単純なZBFW機能のようなUTDエンジンを必要とするわけではありません。



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。



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。

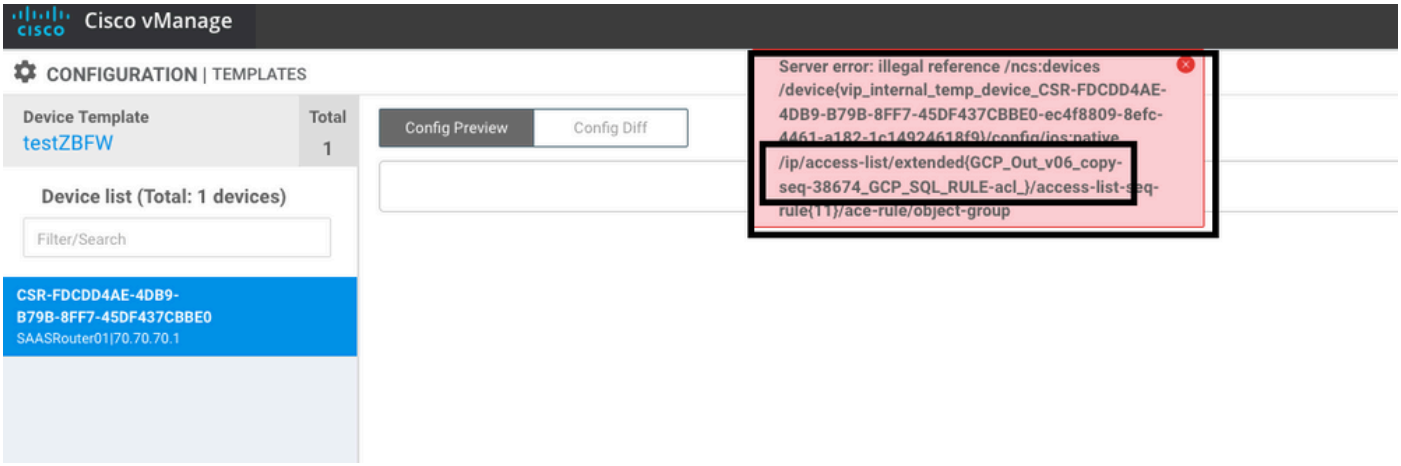
show sdwan system statusの出力で、現在の合計メモリを確認します。

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

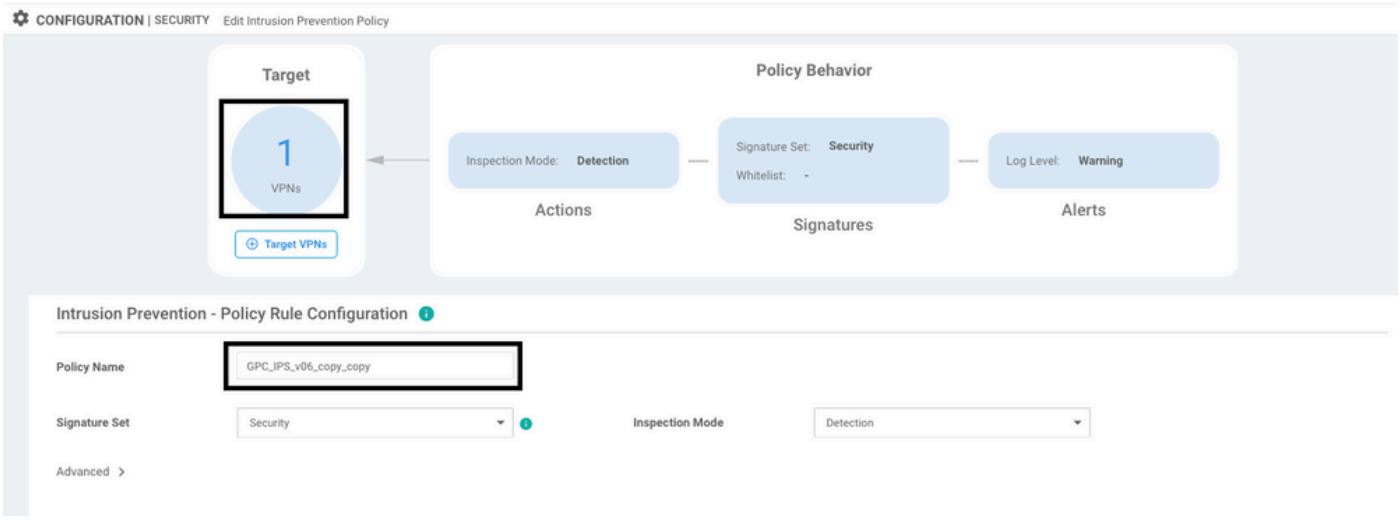
```
Memory usage:            8107024K total,    3598816K used,    4508208K free
                         349492K buffers,  2787420K cache
```

問題3.不正参照

セキュリティポリシー機能で使用されるVPN/VRFがcEdgeルータで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。