Installer l'image virtuelle de sécurité UTD sur les routeurs cEdge

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Informations générales
Routeurs exécutant le logiciel Cisco IOS XE SDWAN (16.x)
Routeurs exécutant le logiciel Cisco IOS XE (17.x)
Configuration
Étape 1. Télécharger l'image virtuelle
Étape 2. Ajouter le sous-modèle Stratégie de sécurité et profil de conteneur au modèle de périphérique
Étape 3. Mise à jour ou association du modèle de périphérique avec la stratégie de sécurité et le profil de conteneur
Vérification
Problèmes courants
PROBLÈME 1. Erreur : Les périphériques suivants n'ont pas de services logiciels de conteneur
PROBLÈME 2. Mémoire disponible insuffisante
QUESTION 3. Renvoi illégal
PROBLÈME 4. UTD est installé et actif mais pas activé
Informations connexes

Introduction

Ce document décrit comment installer l'image virtuelle de sécurité UTD (Unified Threat Defense) pour activer les fonctions de sécurité sur les périphériques SD-WAN Cisco IOS XE.

Conditions préalables

- Avant d'utiliser ces fonctionnalités, téléchargez l'image virtuelle de sécurité appropriée dans le référentiel vManage.
- Le routeur cEdge doit être en mode vmanage avec un modèle pré-joint.
- Créez un modèle de stratégie de sécurité pour le système de prévention des intrusions (IPS), le système de détection des intrusions (IDS), le filtrage des URL (URL-F) ou le filtrage AMP (Advanced Malware Protection).

Conditions requises

- Routeur à services intégrés 4000 Cisco IOS XE SD-WAN (ISR4k)
- Routeur à services intégrés 1000 Cisco IOS XE SD-WAN (ISR1k)

- Routeur de services cloud 1000v (CSR1kv),
- Routeur à services intégrés 1000v (ISRv)
- Plates-formes périphériques prenant en charge 8 Go de DRAM.

Components Used

- Image virtuelle Cisco UTD
- Contrôleur vManage
- Routeurs cEdge avec connexions de contrôle avec contrôleurs.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'image Cisco UTD nécessite une stratégie de sécurité sur le modèle de périphérique à installer et des fonctionnalités de sécurité activées telles que le système de prévention des intrusions (IPS), le système de détection des intrusions (IDS), le filtrage des URL (URL-F) et AMP (Advanced Malware Protection) sur les routeurs Edge.

Téléchargez le logiciel Cisco UTD Snort IP Engine à partir du logiciel Cisco

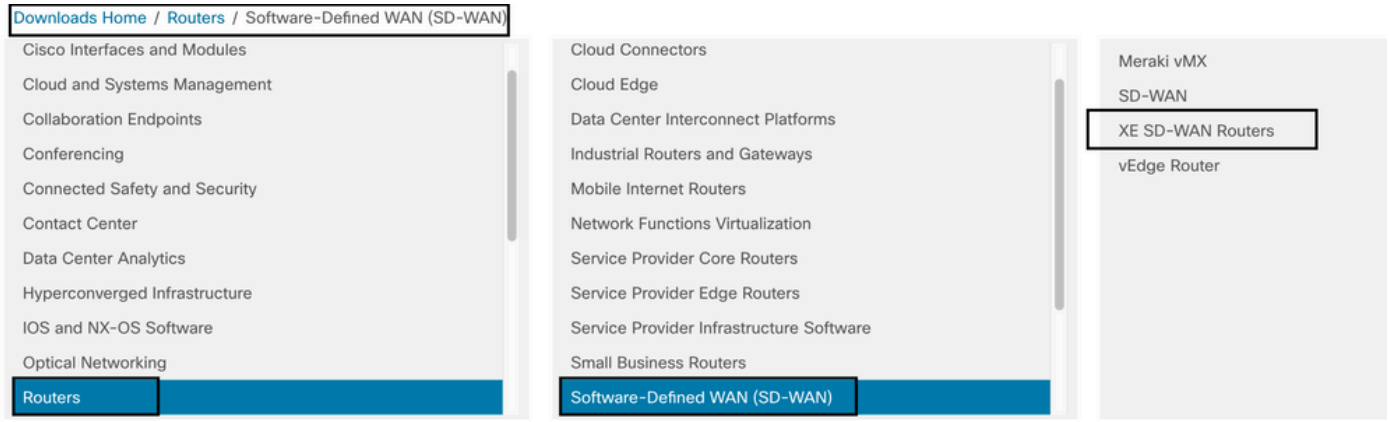
Utilisez l'expression régulière prise en charge de l'image virtuelle UTD Cisco pour la version actuelle de Cisco IOS XE. Utilisez la commande **show utd engine standard** version pour valider l'image UTD recommandée et prise en charge.

```
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$
```

> **Remarque** Le chemin de téléchargement de l'image dépend du routeur qui exécute le logiciel SDWAN Cisco IOS XE (16.x) ou le logiciel universel Cisco IOS XE (17.x).

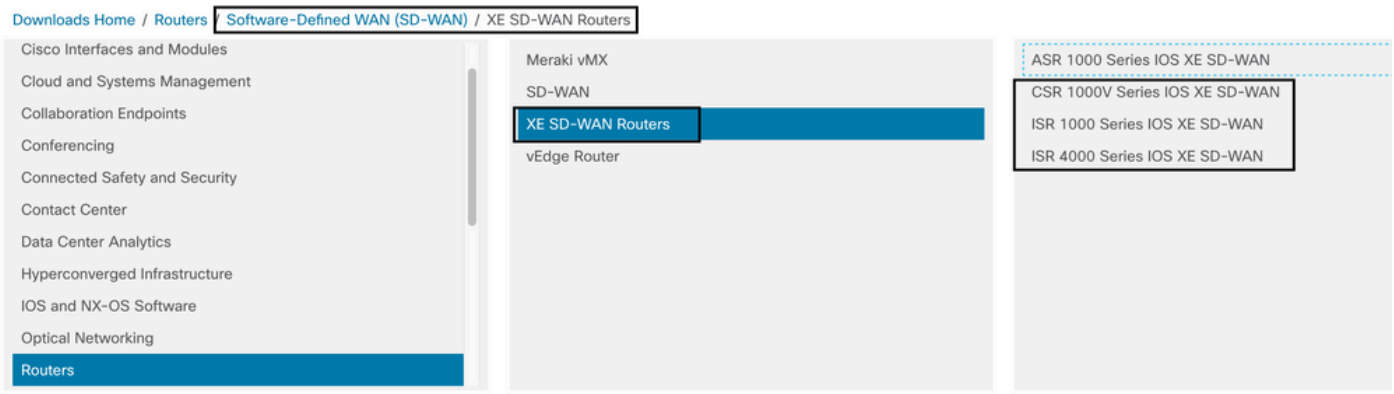
Routeurs exécutant le logiciel Cisco IOS XE SDWAN (16.x)

Le chemin pour obtenir le logiciel Cisco UTD Snort IPS Engine est Routers/ Software-Defined WAN (SD-WAN)/ XE SD-WAN Routers / et le routeur intégré de la gamme.



Sélectionnez le type de modèle du routeur McEdge.

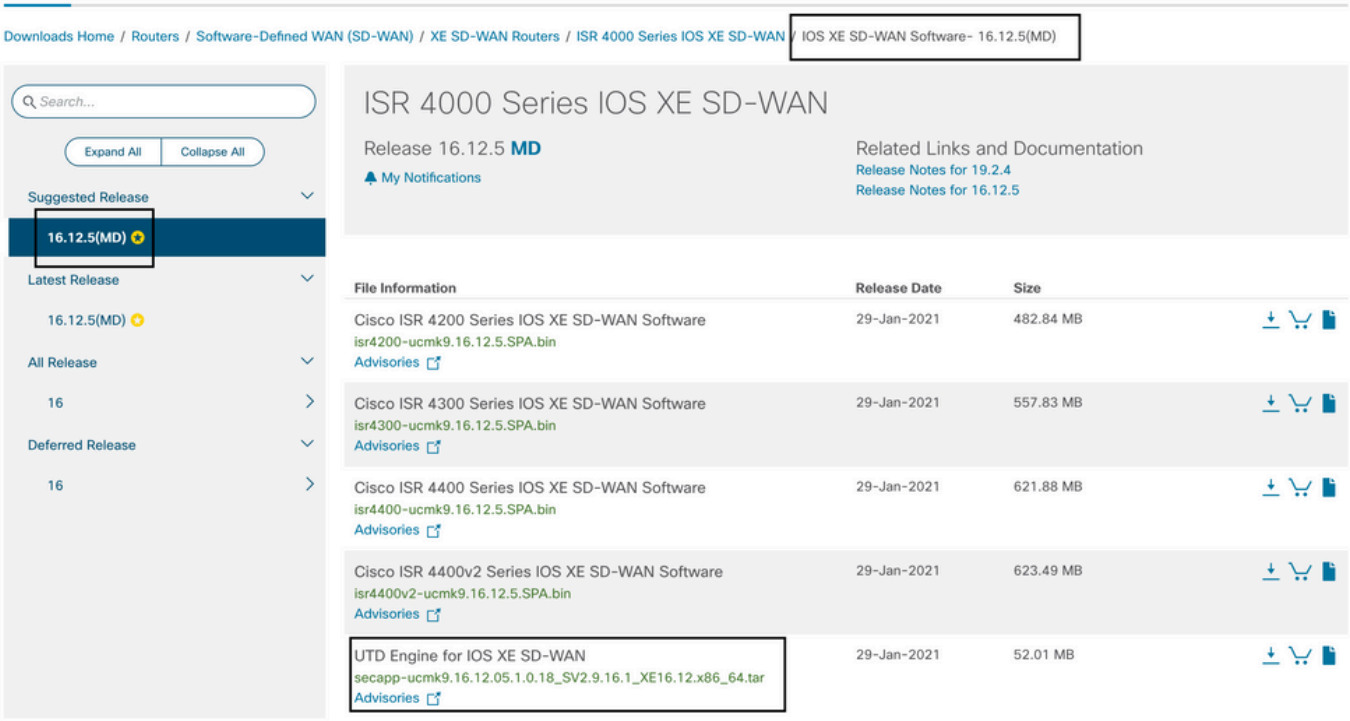
> **Remarque** Les routeurs ASR (Aggregation Services Routers) de la gamme ne sont pas disponibles pour les fonctionnalités UTD.



Après avoir choisi le modèle de routeur de type, sélectionnez l'option **logicielle Cisco IOS XE SD-WAN** pour obtenir le package UTD pour Edge sur la version 16.x.

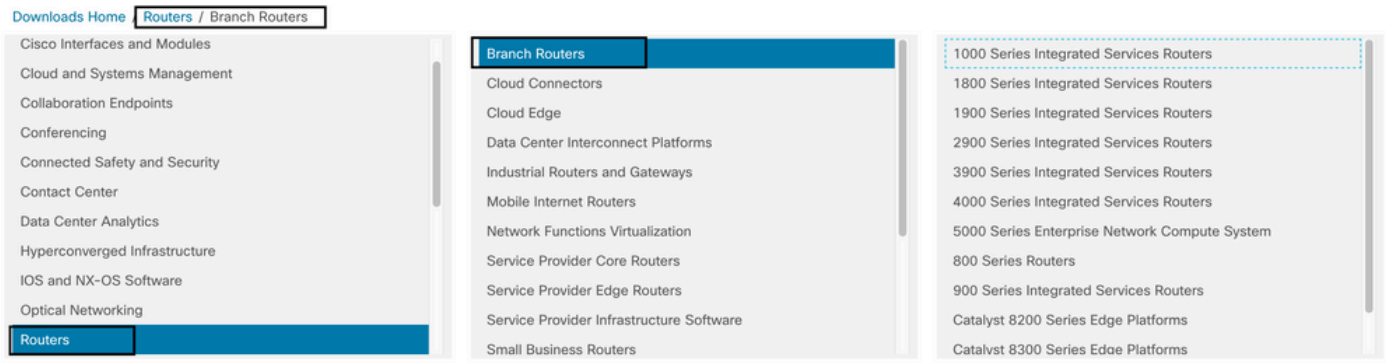
> **Remarque** Le chemin de téléchargement permettant de choisir l'image virtuelle Cisco UTD pour le code 16.x des routeurs Edge affiche également l'option du **logiciel Cisco IOS XE**. C'est le chemin pour choisir les codes de mise à niveau de cEdge pour 17.x seulement, mais il n'y a pas localisé l'image virtuelle UTD pour la version 17.x. Les codes SDWAN Cisco IOS XE et Cisco IOS XE standard unifiés sur 17.x et les versions ultérieures, de sorte que le chemin pour obtenir l'image virtuelle Cisco UTD pour 17.x est le même que les codes Cisco IOS XE standard.

Choisissez la version actuelle du serveur cEdge et téléchargez le package UTD correspondant.

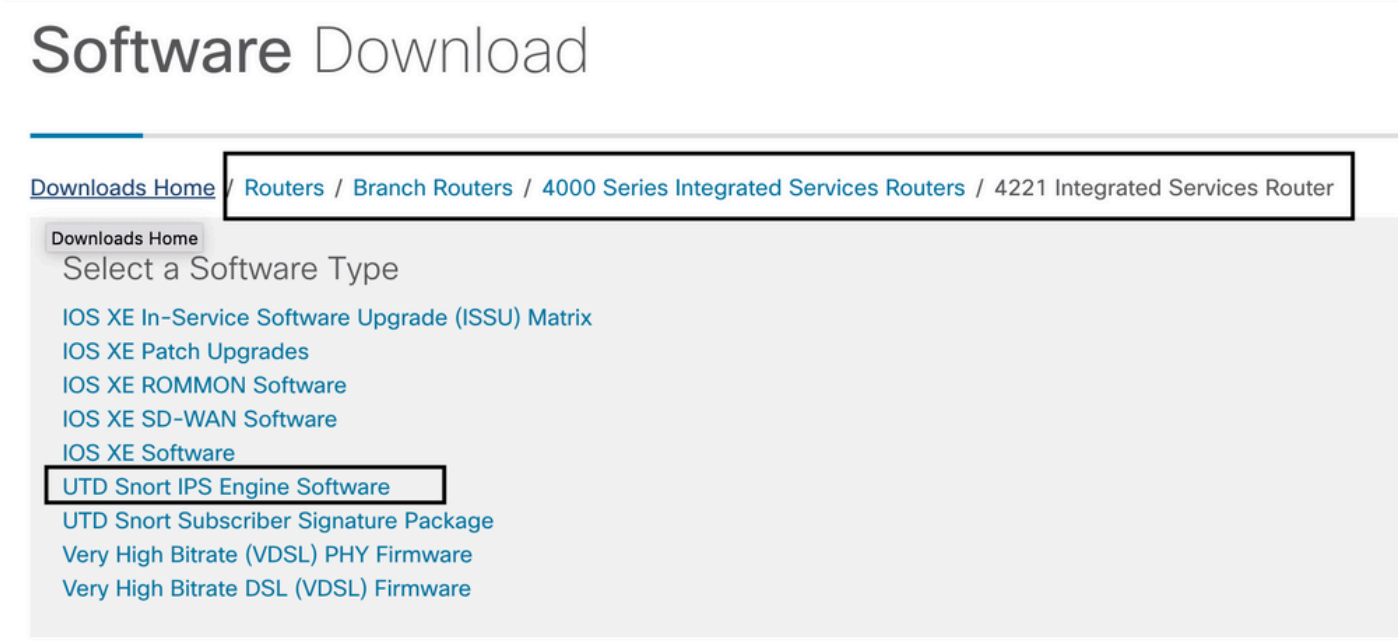


Routeurs exécutant le logiciel Cisco IOS XE (17.x)

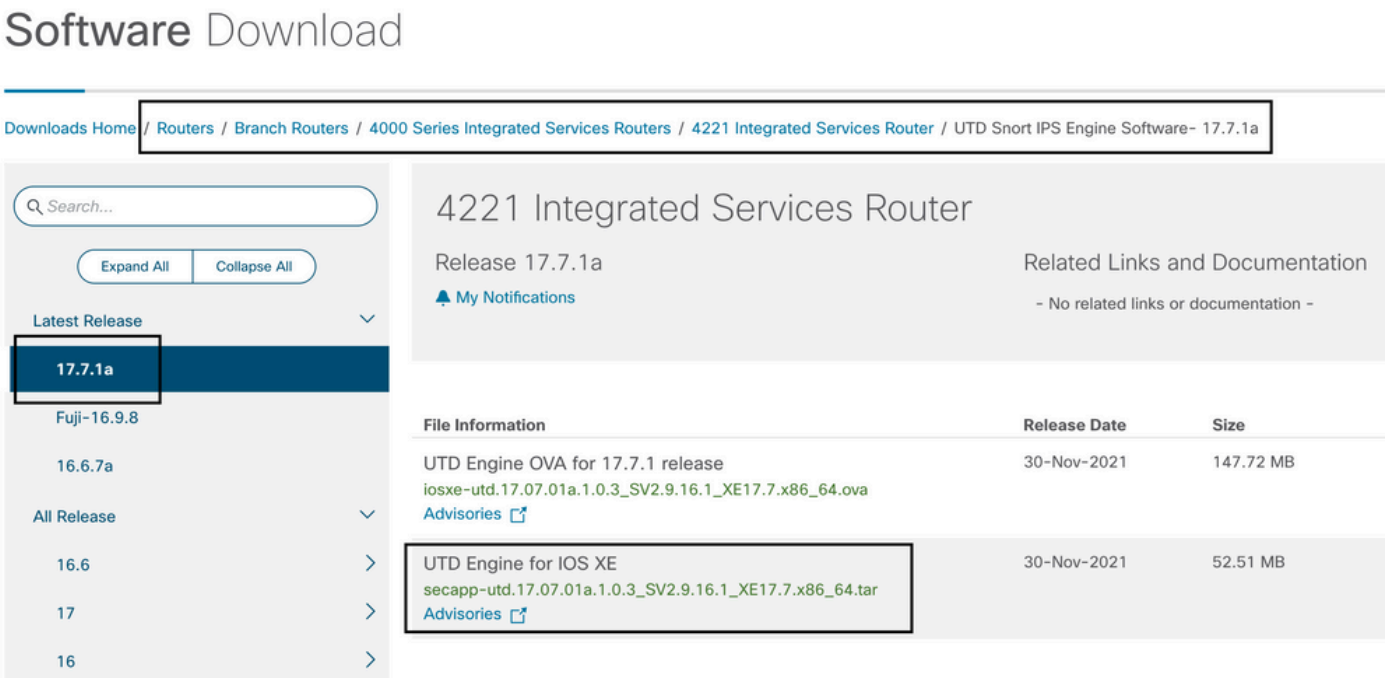
Cisco IOS XE version 17.2.1r et la dernière version utilisent l'image universalk9 pour déployer Cisco IOS XE SD-WAN et Cisco IOS XE sur les périphériques Cisco IOS XE.
Le logiciel UTD Snort IPS Engine se trouve dans **Routers > Branch Routers > Series Integrated Router**.



Après avoir choisi le type de modèle du routeur, sélectionnez le logiciel **UTD Snort IPS Engine**.



Sélectionnez la version actuelle du routeur et téléchargez le package UTD correspondant à la version sélectionnée.

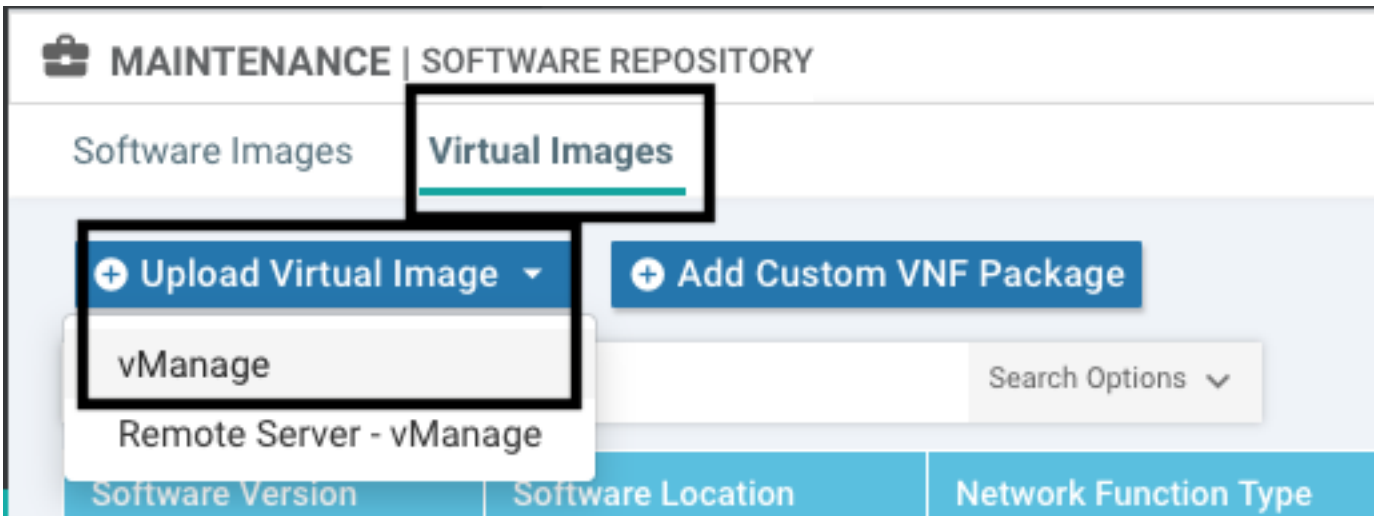


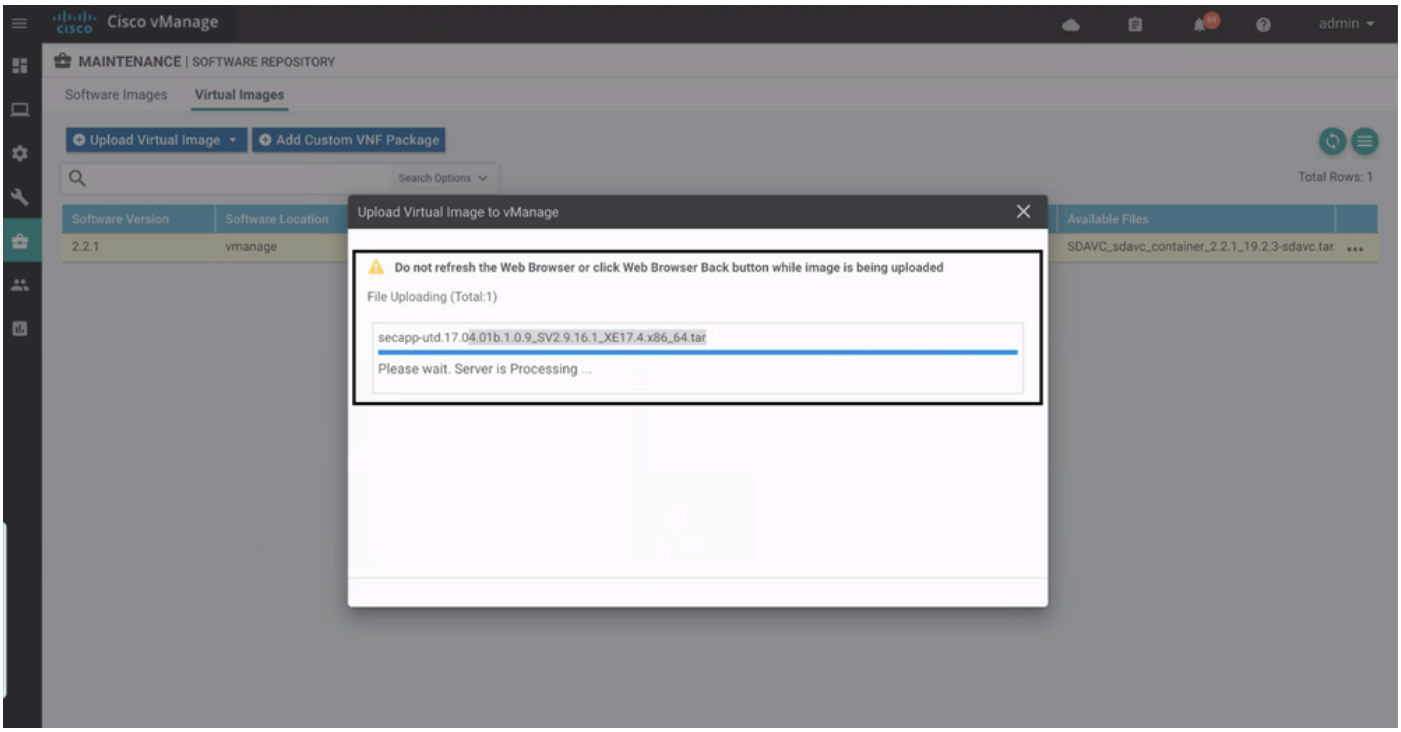
Note: Les routeurs de la gamme Cisco ISR1100X (routeurs Cisco Nutella SR1100X-4G/6G) qui exécutent le logiciel Cisco IOS XE au lieu du code Viptela sont basés sur x86_x64. L'image virtuelle Cisco UTD publiée pour ISR4K peut fonctionner dessus. Vous pouvez installer la même version de code d'image UTD prise en charge par regex pour la version SDWAN Cisco IOS XE actuelle sur le routeur Nutella. Utilisez la commande **show utd engine standard version** pour valider l'image UTD recommandée et prise en charge de l'expression régulière Cisco.

Configuration

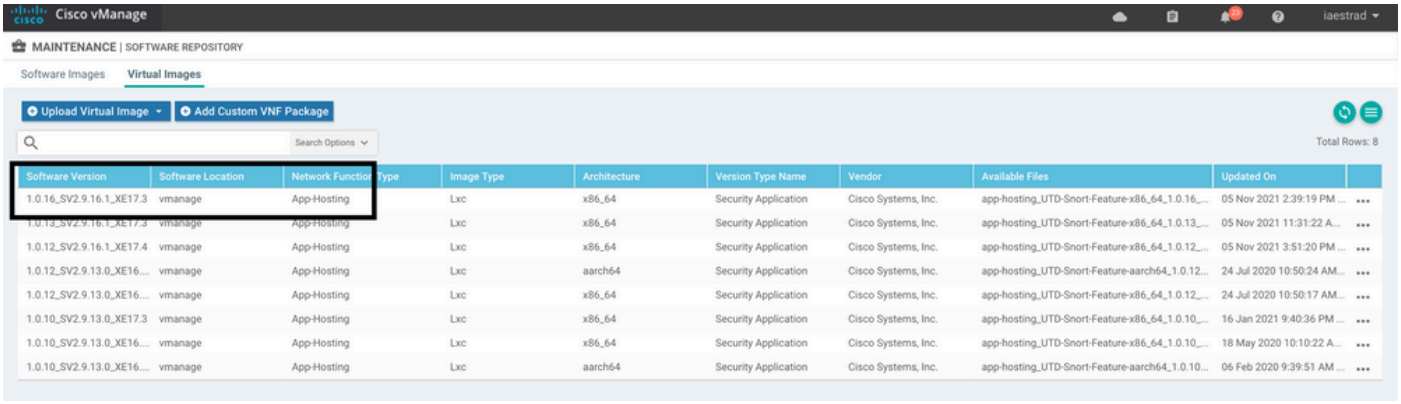
Étape 1. Télécharger l'image virtuelle

Assurez-vous que votre image virtuelle correspond au code SDWAN Cisco IOS XE actuel sur le serveur cEdge et téléchargez-le dans pour gérer le référentiel.
Accédez à **Maintenance > Référentiel de logiciels > Image virtuelle > Télécharger l'image virtuelle > vManage.**



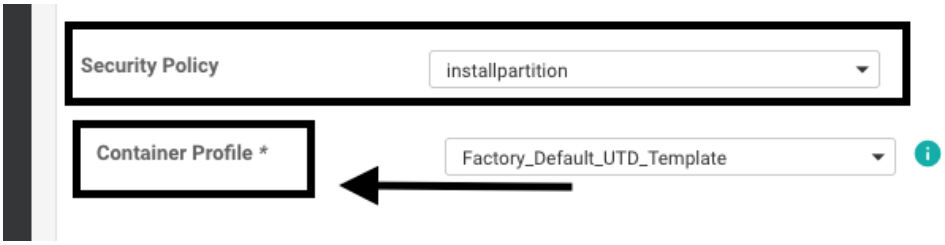


Une fois que l'image virtuelle Cisco UTD a été correctement téléchargée, vérifiez qu'elle se trouve dans le référentiel.



Étape 2. Ajouter le sous-modèle Stratégie de sécurité et profil de conteneur au modèle de périphérique

Ajoutez la stratégie de sécurité précédemment créée au modèle de périphérique. La stratégie de sécurité doit comporter une stratégie IPS/IDS, URL-F ou de filtrage AMP sur le modèle de périphérique. Ouvrez le profil de conteneur automatiquement. Utilisez le profil de conteneur par défaut ou modifiez-le si nécessaire.

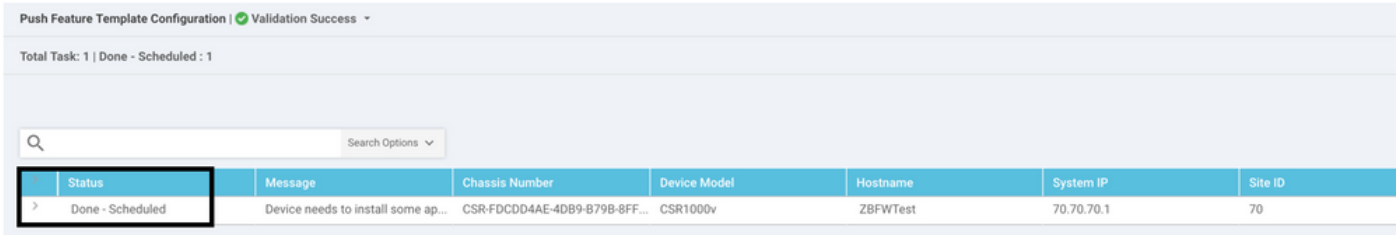


Étape 3. Mise à jour ou association du modèle de périphérique avec la stratégie de sécurité et le profil de conteneur

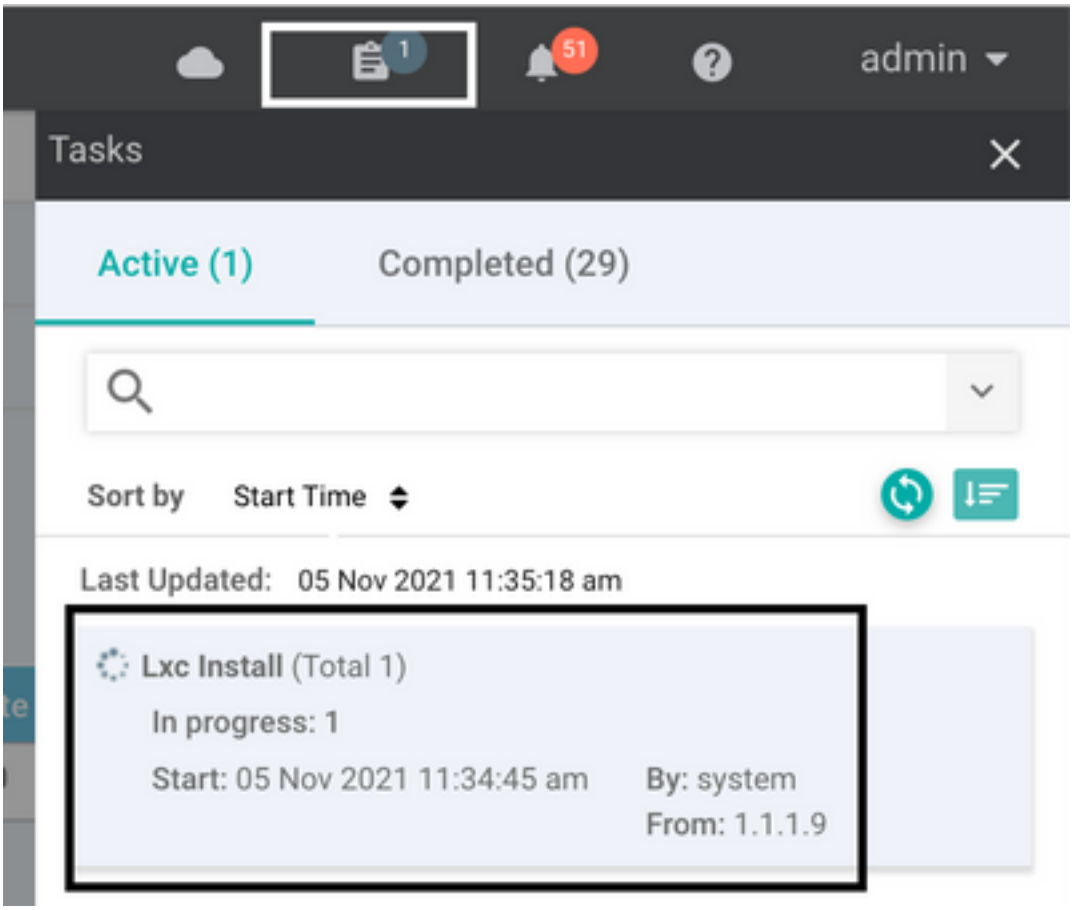
Mettez à jour ou joignez le modèle au routeur cEdge. Notez dans config diff que la configuration d'hébergement d'applications et le moteur UTD pour la fonctionnalité IPS/IDS, URL-F ou le filtrage AMP sont configurés.

```
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
!
```

L'état du modèle passe à **Terminé planifié** car vmanage a remarqué que la configuration appliquée comporte des fonctionnalités de moteur UTD, donc vmanage détermine que cEdge a besoin de l'image virtuelle installée pour utiliser les fonctionnalités de sécurité UTD.



Une fois que le modèle est passé à l'état de planification, une nouvelle tâche **en cours** apparaît dans le menu des tâches. La nouvelle tâche est l'**installation Lxc**, cela signifie que vmanage démarre automatiquement l'installation de l'image virtuelle sur le cEdge avant de pousser la nouvelle configuration.

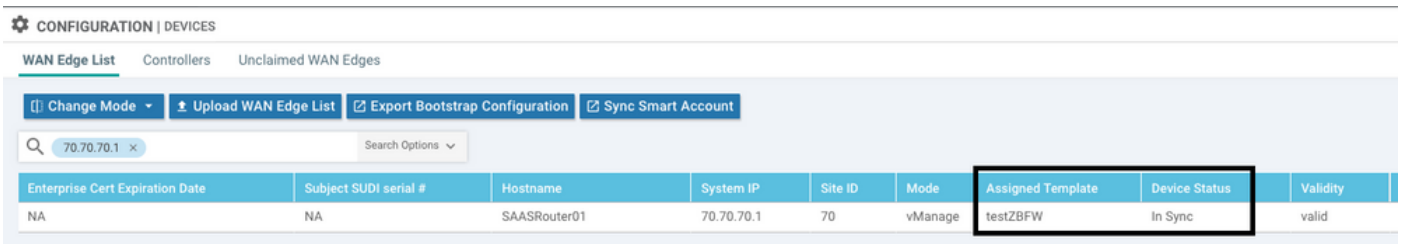


Une fois le conteneur LX installé, le vManage transmet la configuration pré-planifiée avec les fonctionnalités UTD. Il n'y a pas de nouvelle tâche pour cela car la configuration a déjà été planifiée.

Vérification

Vérifiez si le serveur cEdge est synchronisé avec vManage et le modèle joint.

Accédez à **Configuration > Devices**



Vérifiez si la version Cisco UTD est installée :

```
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         <<<<<<<<<<<<<<<<<<<
```

Remarque La version UTD installée ne peut pas être à l'état **UNSUPPORTED**.

Vérifiez si UTD est en **cours d'exécution** avec la sortie suivante :

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

La commande suivante récapitule les commandes précédentes et affiche l'état et la version actuels :

```
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
```

La commande **Show utd engine standard status** affiche l'état d'intégrité du moteur UTD et l'heure à laquelle il obtient la mise à jour de signature.

```
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
```

Vérifiez que les fonctionnalités activées utilisent la commande suivante :

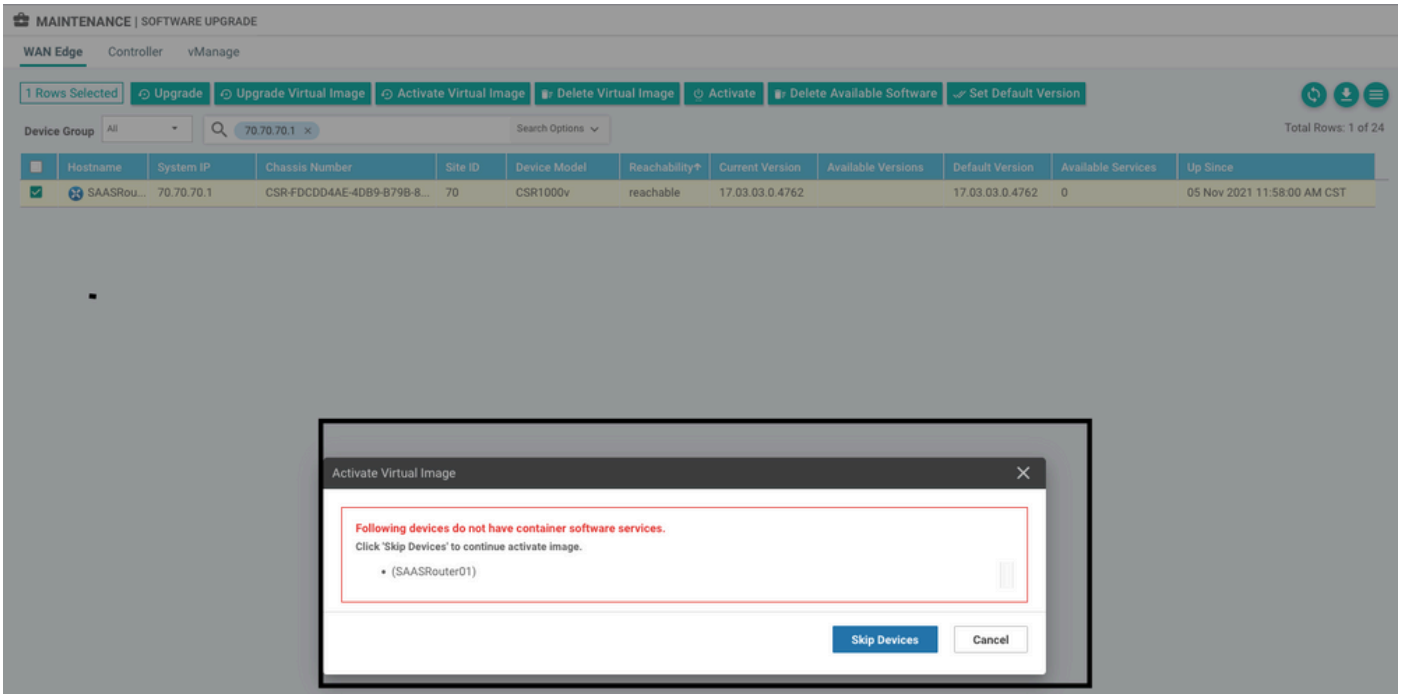
```
Router02# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
  Divert controller mode: enabled
  SN threads: 12
  CFT inst_id 0 feat id 2 fo id 2 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
```

Problèmes courants

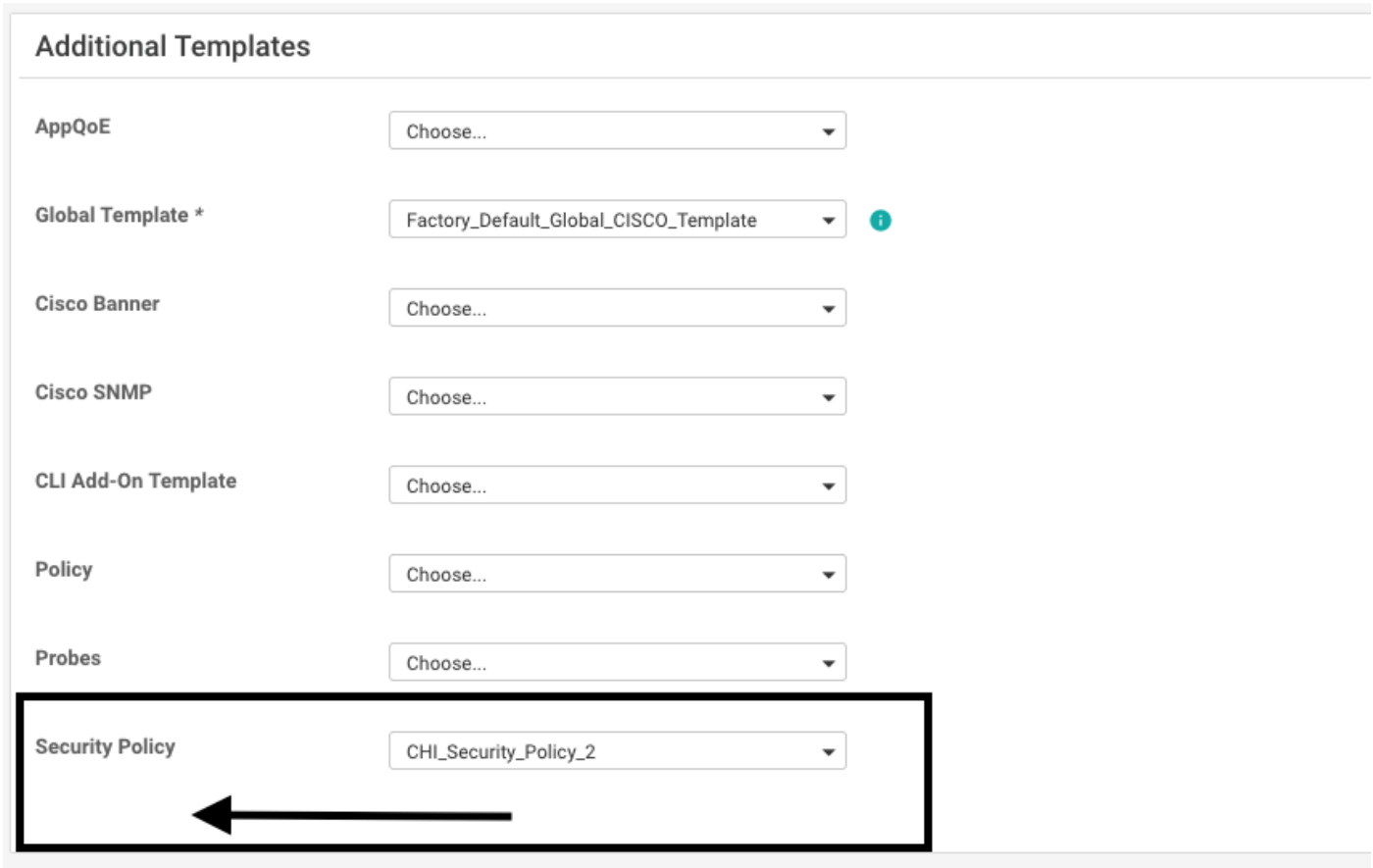
PROBLÈME 1. Erreur : Les périphériques suivants n'ont pas de services logiciels de conteneur

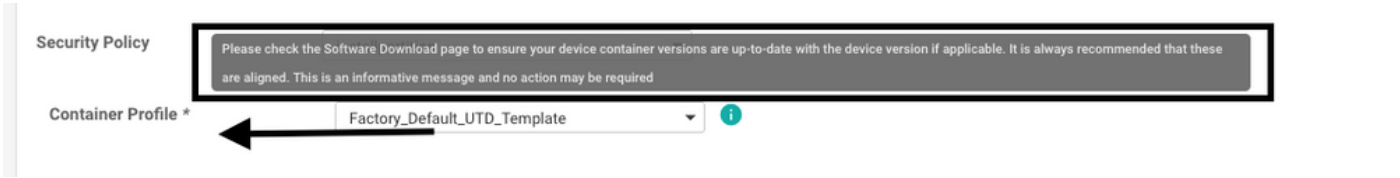
Activez l'image virtuelle.

Accédez à **maintenance > logiciel > activer**



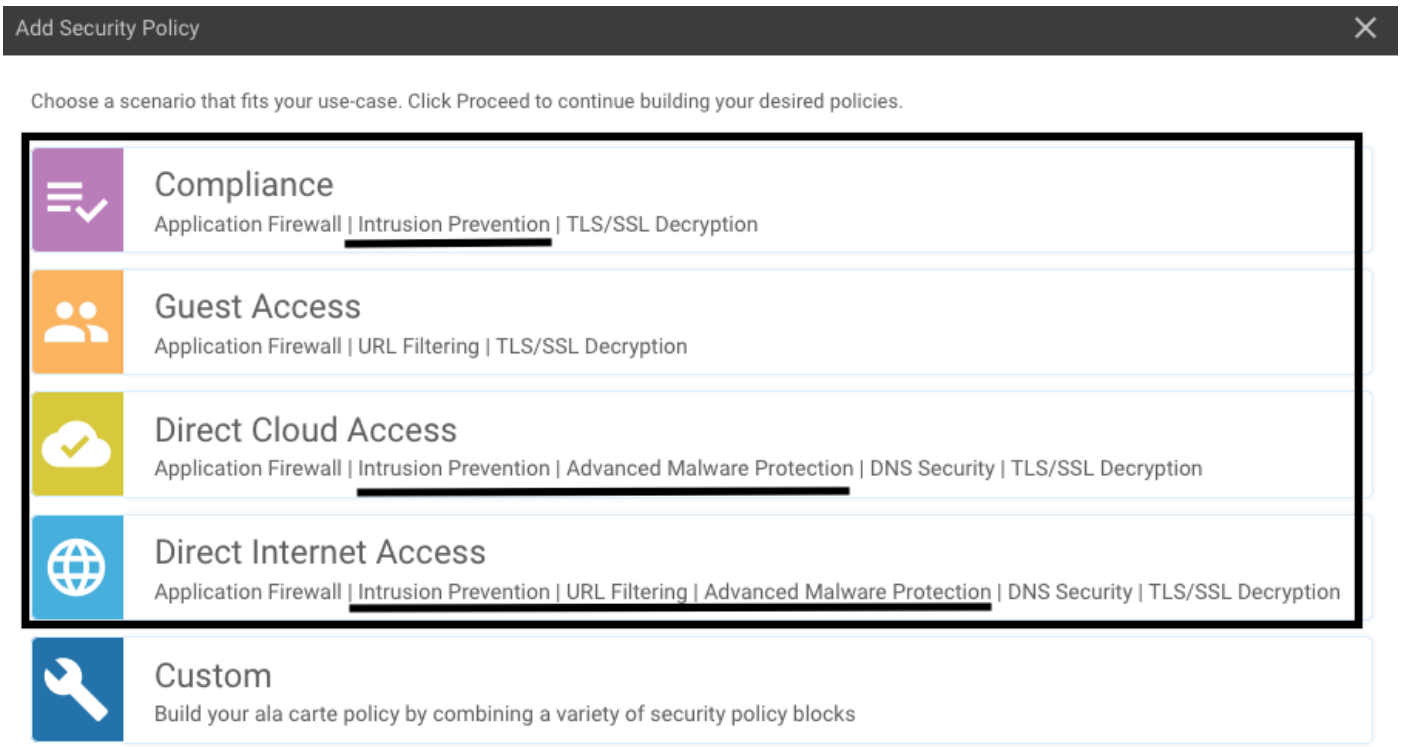
L'image virtuelle envoie une erreur : **Les périphériques n'ont donc pas de services logiciels de conteneur**, Si le routeur cEdge sélectionné n'a pas de stratégie de sécurité avec le sous-modèle de profil de conteneur.





Ce modèle est automatiquement ajouté si vous utilisez une stratégie de sécurité qui inclut des

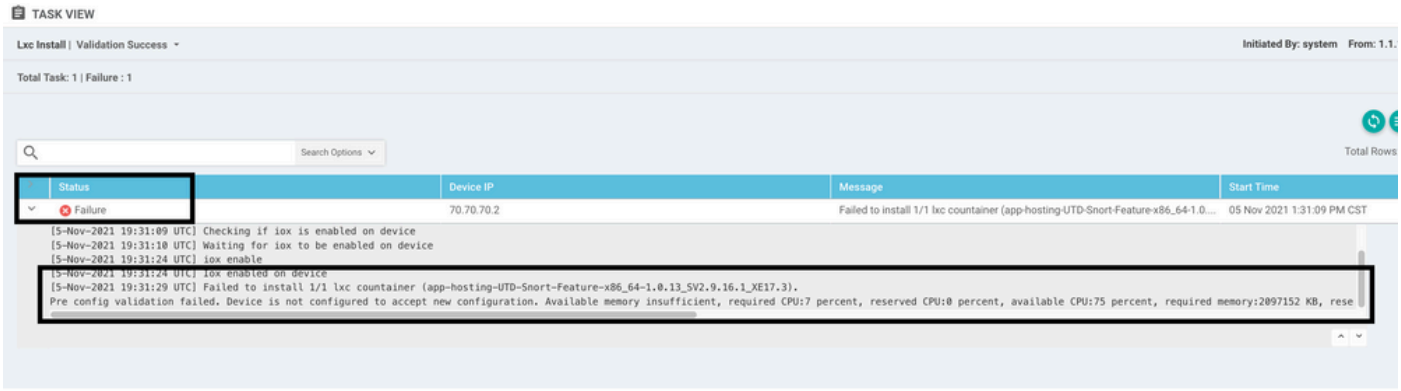
fonctionnalités de sécurité telles que le système de prévention des intrusions (IPS), le système de détection des intrusions (IDS), le filtrage des URL (URL-F) et Advanced Malware Protection (AMP) qui nécessite un package UTD. Toutes les fonctions de sécurité disponibles ne nécessitent pas de moteur UTD, comme la simple fonction ZBFW.



Une fois que vous avez envoyé le modèle avec le sous-modèle de profil de conteneur, vmanage installe automatiquement l'image virtuelle.

PROBLÈME 2. Mémoire disponible insuffisante

Assurez-vous que le routeur cEdge dispose de 8 Go de mémoire DRAM. Si ce n'est pas le cas, le processus d'installation Lxc envoie un **périphérique qui n'est pas configuré pour accepter la nouvelle configuration.** Erreur **mémoire disponible insuffisante**. Pour que les routeurs cEdge puissent utiliser les fonctions UTD, il faut disposer d'au moins 8 Go de DRAM.



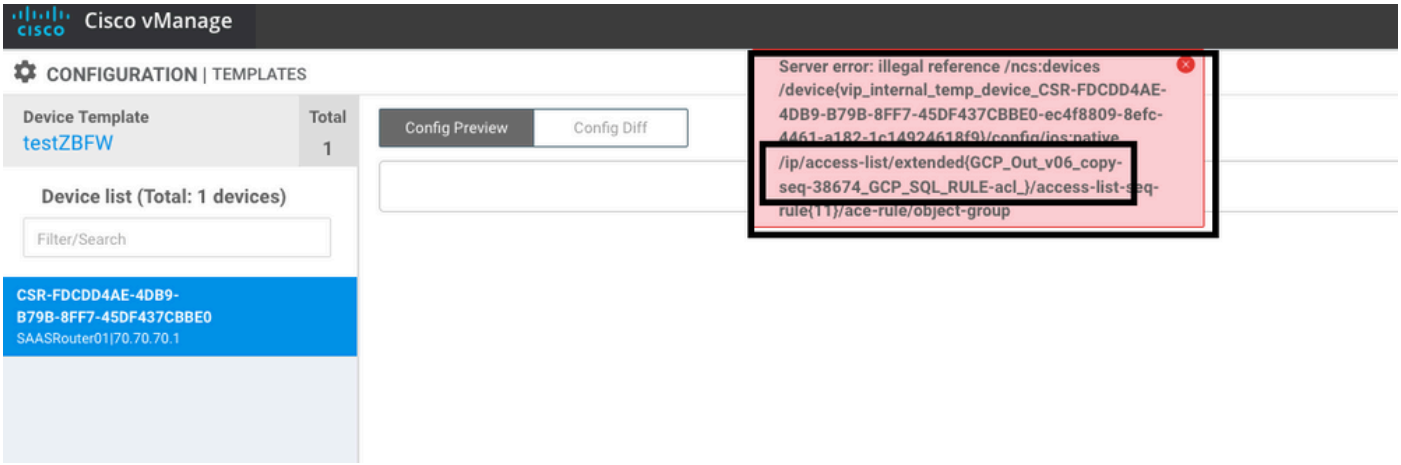
Dans ce cas, le CSRv dispose de seulement 4 Go de DRAM. Après la mise à niveau de la mémoire à 8 Go de DRAM, l'installation est un succès.

Vérifiez la mémoire totale actuelle avec la sortie **show sdwan system status** :

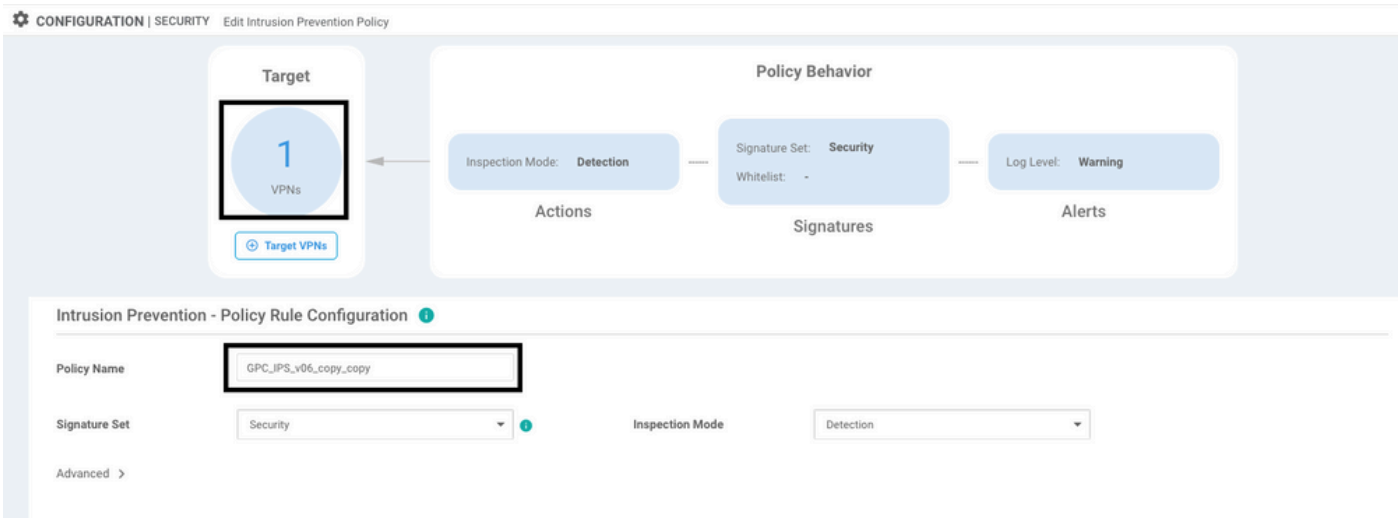
```
Router01# show sdwan system status

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

QUESTION 3. Renvoi illégal

Assurez-vous que les VPN/VRF utilisés sur l'une des fonctionnalités de stratégie de sécurité sont déjà configurés dans le routeur cEdge pour éviter une référence illégale pour les séquences de stratégie de sécurité.



Dans cet exemple, la stratégie de sécurité a une stratégie de prévention des intrusions pour VPN/VRF 1, mais aucun VRF 1 n'est configuré sur les périphériques. Ainsi, le vmanage envoie une référence illégale pour cette séquence de stratégie.



Après avoir configuré le VRF mentionné sur les stratégies de sécurité, la référence Illégal n'apparaît pas et le modèle est envoyé avec succès.

PROBLÈME 4. UTD est installé et actif mais pas activé

Une stratégie de sécurité est configurée pour le périphérique, et UTD est installé et actif, mais il n'est pas activé.

Ce problème est lié au problème numéro 3. Néanmoins, vManage a autorisé la configuration à faire référence à des VRF qui ne sont pas configurés dans le périphérique et la stratégie n'est appliquée à aucun VRF.

Pour déterminer si le routeur est confronté à ce problème, vous devez voir UTD active. Le message UTD n'est pas activé et la stratégie ne fait référence à aucun VRF.

```
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
```

Pour la résolution, vérifiez les VPN cibles et assurez-vous d'appliquer la stratégie à un VRF configuré.

Informations connexes

- Sécurité du routeur : Snort IPS sur les routeurs
- Guide de configuration de la sécurité Cisco SD-WAN, version Cisco IOS XE
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.