

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).

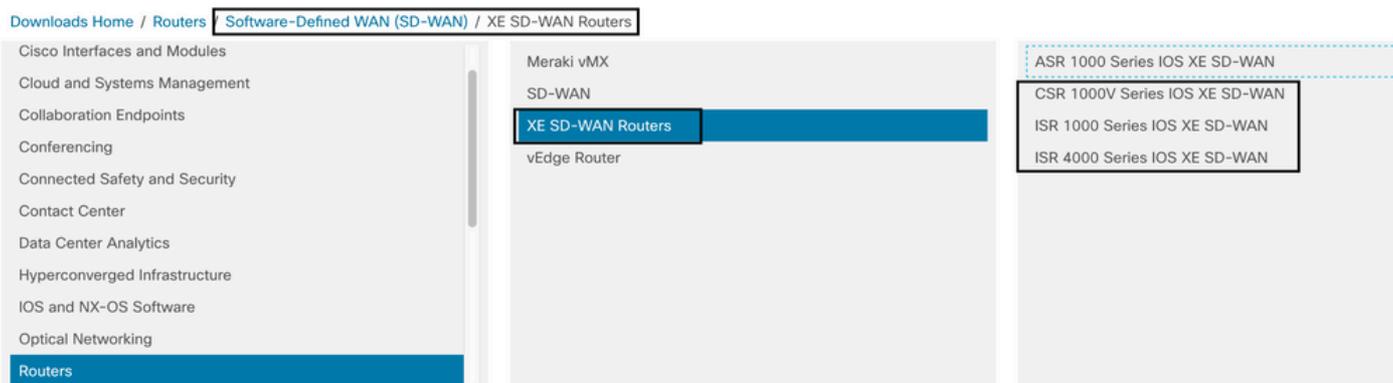
Routeurs exécutant le logiciel Cisco IOS XE SDWAN (16.x)

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.

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	↓ 🛒 📄

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.

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

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

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](#)

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

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 -

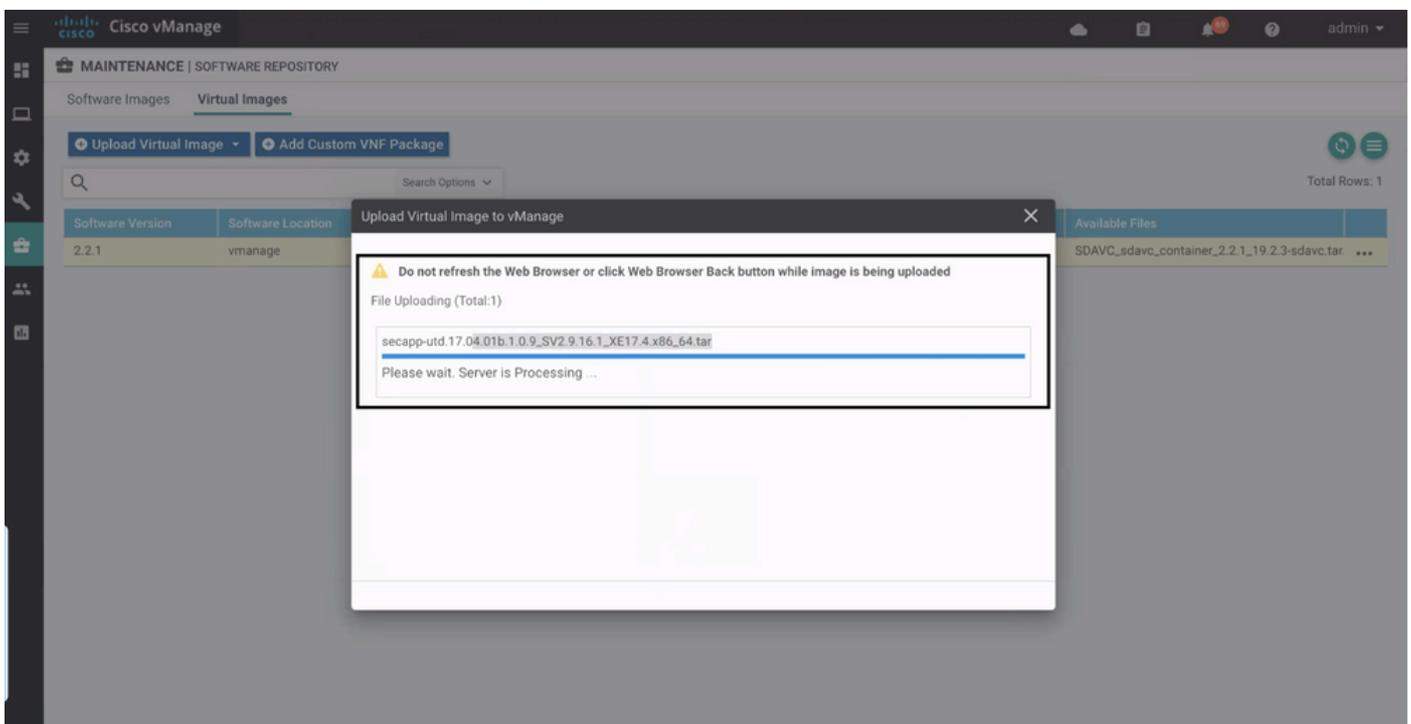
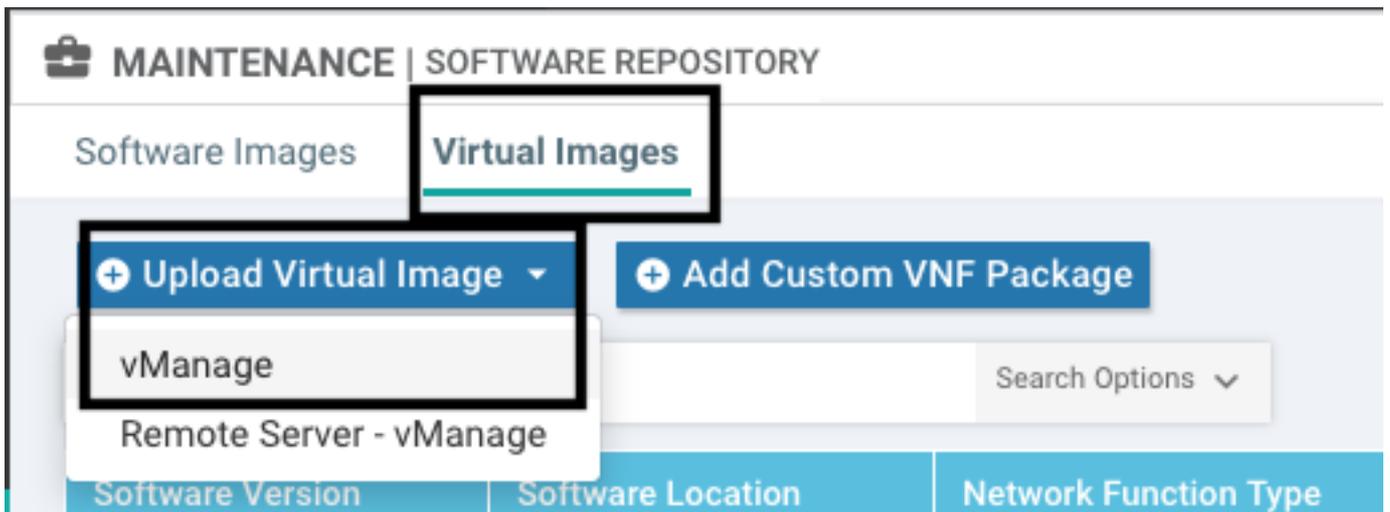
File Information	Release Date	Size
UTD Engine OVA for 17.7.1 release <code>iosxe-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.ova</code> Advisories	30-Nov-2021	147.72 MB
UTD Engine for IOS XE <code>secapp-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.tar</code> Advisories	30-Nov-2021	52.51 MB

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.



Cisco vManage MAINTENANCE | SOFTWARE REPOSITORY

Software Images Virtual Images

Upload Virtual Image Add Custom VNF Package

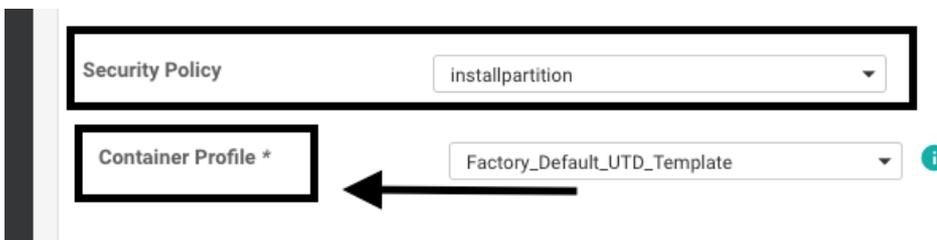
Search Options

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 ...

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.

```
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 policy
282   no app-visibility
283   no flow-visibility
284   no implicit-acl-logging
285   log-frequency 1000
286 !
```

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.

Push Feature Template Configuration | Validation Success

Total Task: 1 | Done - Scheduled : 1

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

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.

The screenshot shows the vManage interface with a 'Tasks' window open. At the top, there are icons for a cloud, a task list with a '1' notification, a bell with '51' notifications, a help icon, and the user 'admin'. The 'Tasks' window has a title bar with 'Tasks' and a close button. Below the title bar, there are two tabs: 'Active (1)' and 'Completed (29)'. A search bar is present with a magnifying glass icon and a dropdown arrow. Below the search bar, there is a 'Sort by' dropdown set to 'Start Time' and two icons: a refresh icon and a list icon. The main content area shows 'Last Updated: 05 Nov 2021 11:35:18 am'. A task card is highlighted with a black box, showing:

- Lxc Install (Total 1)
- In progress: 1
- Start: 05 Nov 2021 11:34:45 am
- By: system
- From: 1.1.1.9

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.

The screenshot shows the 'TASK VIEW' page in vManage. The task is 'Lxc Install | Validation Success'. The status is 'Success'. The device IP is '70.70.70.1'. The message is 'Done - Lxc Install'. The start time is '05 Nov 2021 12:06:03 PM CST'. Below the task details, there is a log of events:

- [5-Nov-2021 18:06:03 UTC] Total number of Container apps to be installed: 1. Container apps to be installed are following: [app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3]
- [5-Nov-2021 18:06:03 UTC] Started 1/1 Lxc container (app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3) installation
- [5-Nov-2021 18:06:03 UTC] Checking if lxc is enabled on device
- [5-Nov-2021 18:06:04 UTC] Downloading http://1.1.1.9:8888/software/package/lxc/app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3_secapp-utd.17.03.03.1.0.13_SV2.9.16.1_XE17.3.x86_64.tar
- [5-Nov-2021 18:06:09 UTC] Container app image: app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3_secapp-utd.17.03.03.1.0.13_SV2.9.16.1_XE17.3.x86_64.tar
- [5-Nov-2021 18:06:20 UTC] Connection Instance: 4, Color: biz-Internet
- [5-Nov-2021 18:06:20 UTC] Downloading http://1.1.1.9:8888/software/package/lxc/app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3_secapp-utd.17.03.03.1.0.13_SV2.9.16.1_XE17.3.x86_64.tar?deviceId=70.70.70.1

Vérification

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

Accédez à **Configuration > Devices**

The screenshot shows the 'CONFIGURATION | DEVICES' page in vManage. The 'WAN Edge List' tab is selected. There are buttons for 'Change Mode', 'Upload WAN Edge List', 'Export Bootstrap Configuration', and 'Sync Smart Account'. A search bar contains '70.70.70.1'. Below the search bar, there is a table with the following columns: Enterprise Cert Expiration Date, Subject SUDI serial #, Hostname, System IP, Site ID, Mode, Assigned Template, Device Status, and Validity. The table contains one row:

Enterprise Cert Expiration Date	Subject SUDI serial #	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Validity
NA	NA	SAASRouter01	70.70.70.1	70	vManage	testZBFW	In Sync	valid

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

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.

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 ⓘ

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.

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

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.

TASK VIEW

Lxc Install | Validation Success - Initiated By: system From: 1.1.

Total Task: 1 | Failure: 1

Status	Device IP	Message	Start Time
Failure	70.70.70.2	Failed to install 1/1 lxc container (app-hosting-UTD-Snort-Feature-x86_64-1.0...	05 Nov 2021 1:31:09 PM CST

```

[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:2097152 KB, reserved memory:1048576 KB, available memory:1048576 KB
```

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

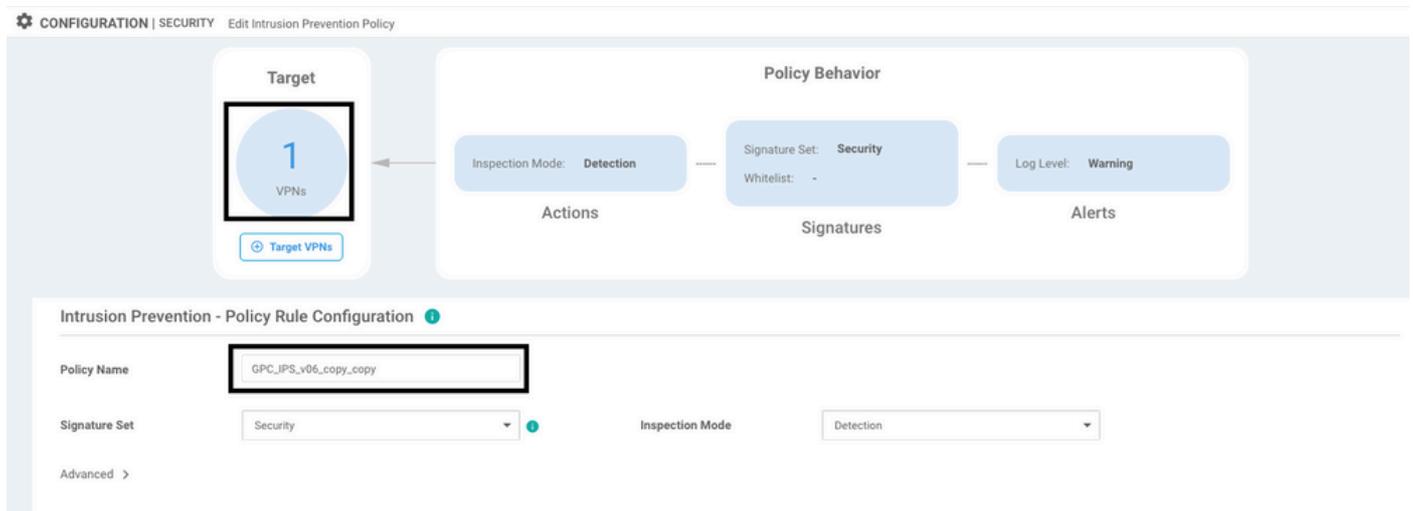
Memory usage: 8107024K total, 3598816K used, 4508208K free
349492K buffers, 2787420K cache

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 illégale 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.