Installa immagine virtuale di sicurezza UTD su router cEdge

Sommario

Introduzione

Questo documento descrive come installare l'immagine virtuale di sicurezza UTD (Unified Threat Defense) per abilitare le funzionalità di sicurezza sui dispositivi Cisco IOS® XE SD-WAN.

Prerequisiti

- Prima di utilizzare queste funzionalità, caricare l'immagine virtuale di sicurezza appropriata nel repository vManage.
- Il router Cisco Edge deve essere in modalità di gestione con il modello preallegato.
- Creare un modello di criteri di sicurezza per i filtri IPS (Intrusion Prevention System), IDS (Intrusion Detection System), URL-F (URL Filtering) o AMP (Advanced Malware Protection).

Requisiti

- 4000 Integrated Services Router Cisco IOS XE SD-WAN (ISR4k)

- 1000 Integrated Services Router Cisco IOS XE SD-WAN (ISR1k)
- 1000v Cloud Services Router (CSR1kv),
- ISRv (1000v Integrated Services Router)
- Piattaforme Cisco Edge che supportano DRAM da 8 GB.

Componenti usati

- Immagine virtuale UTD Cisco
- vManage controller
- Router Cisco Edge con connessioni di controllo con controller.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per installare l'immagine Cisco UTD, è necessario un criterio di sicurezza nel modello di dispositivo e le funzionalità di sicurezza abilitate, ad esempio IPS (Intrusion Prevention System), IDS (Intrusion Detection System), URL Filtering (URL-F) e AMP (Advanced Malware Protection), devono essere abilitate sui router Cisco Edge.

Scarica il software Cisco UTD Snort IP Engine dal software Cisco

Usare il regex supportato dall'immagine virtuale Cisco UTD per la versione corrente di Cisco IOS XE. Utilizzare il comando show utd engine standard version per convalidare l'immagine UTD consigliata e supportata.

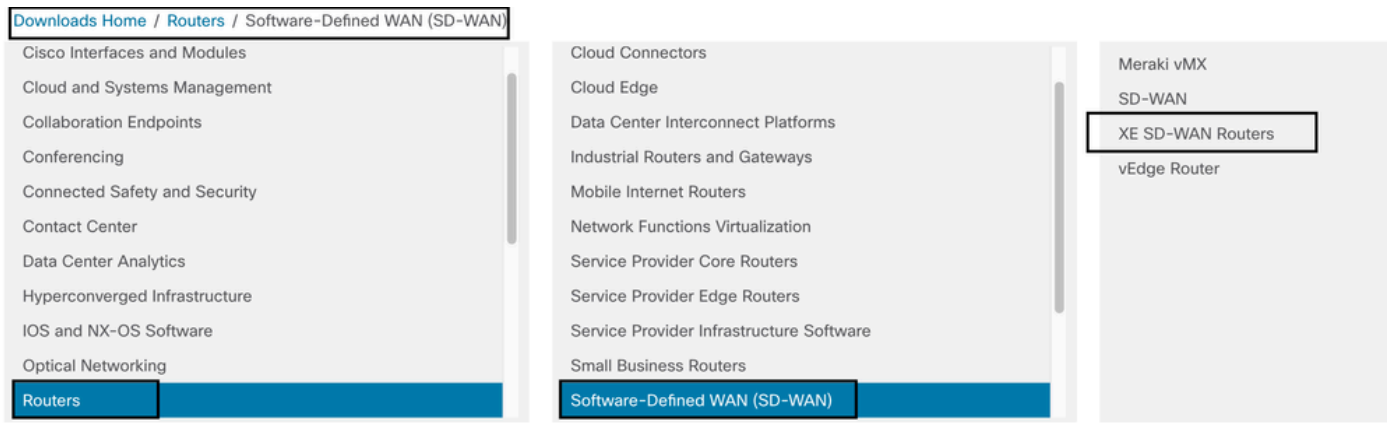
```
<#root>

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$
```

Nota Il percorso per il download dell'immagine dipende dal fatto che il router esegua il software Cisco IOS XE SD-WAN (16.x) o il software Cisco IOS XE universale (17.x).

Router che eseguono il software Cisco IOS XE SD-WAN (16.x)

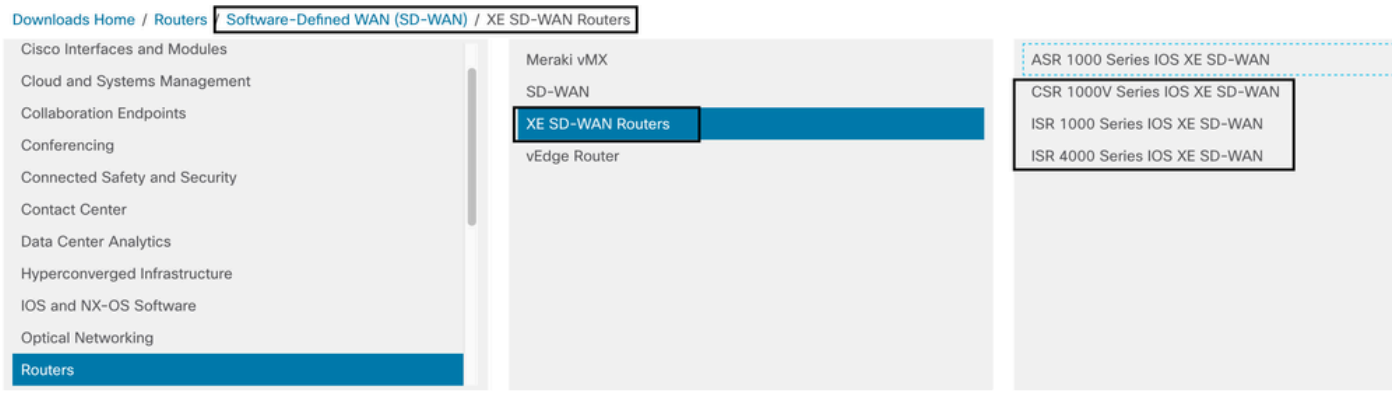
Il percorso per ottenere il software Cisco UTD Snort IPS Engine è Router/ Software-Defined WAN

(SD-WAN)/ Router XE SD-WAN / e router integrati della serie.



Selezionare il tipo di modello per il router Cisco Edge.

Nota: i router ASR (Series Aggregation Services Router) non sono disponibili per le funzionalità UTD.

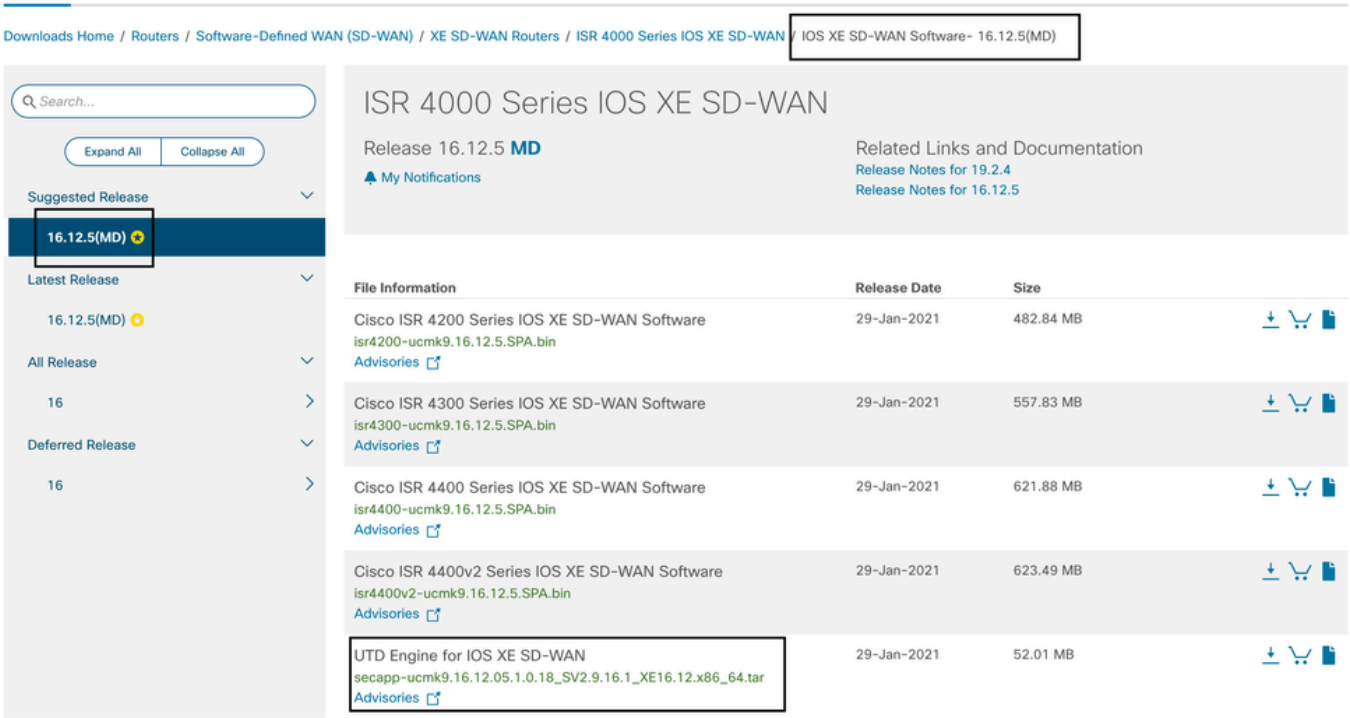


Dopo aver scelto il tipo di modello di router, selezionare l'opzione software Cisco IOS XE SD-WAN per ottenere il pacchetto UTD per Cisco Edges sulla versione 16.x.

Nota Il percorso di download per la scelta dell'immagine virtuale Cisco UTD per il codice 16.x per i router Cisco Edge mostra anche l'opzione software Cisco IOS XE. Questo è il percorso per scegliere i codici di aggiornamento di Cisco Edge solo per 17.x, ma non è presente l'immagine virtuale UTD per la versione 17.x. Cisco ha unificato i codici Cisco IOS XE e

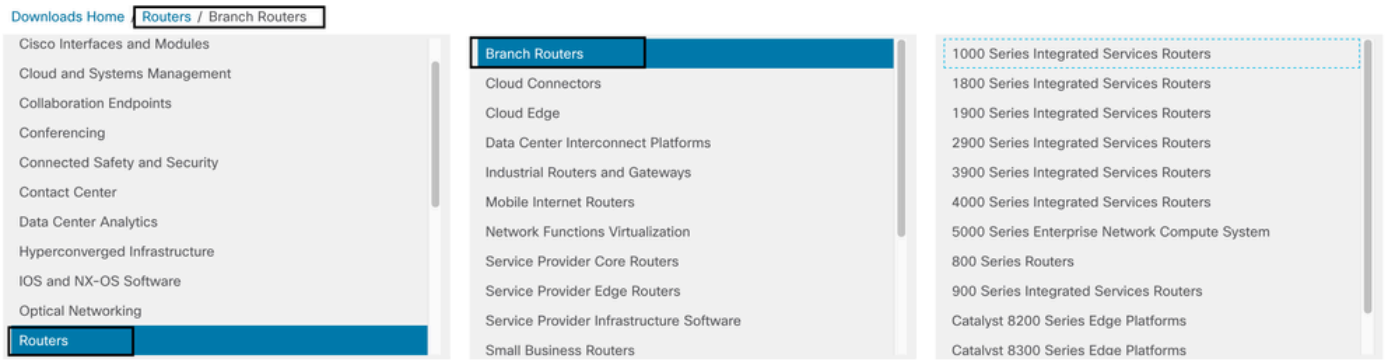
Cisco IOS XE SD-WAN regolari sulla versione 17.x e successive, quindi il percorso per ottenere l'immagine virtuale Cisco UTD per la versione 17.x è lo stesso dei normali codici Cisco IOS XE.

Scegliere la versione corrente di Cisco Edge e scaricare il pacchetto UTD per tale versione.

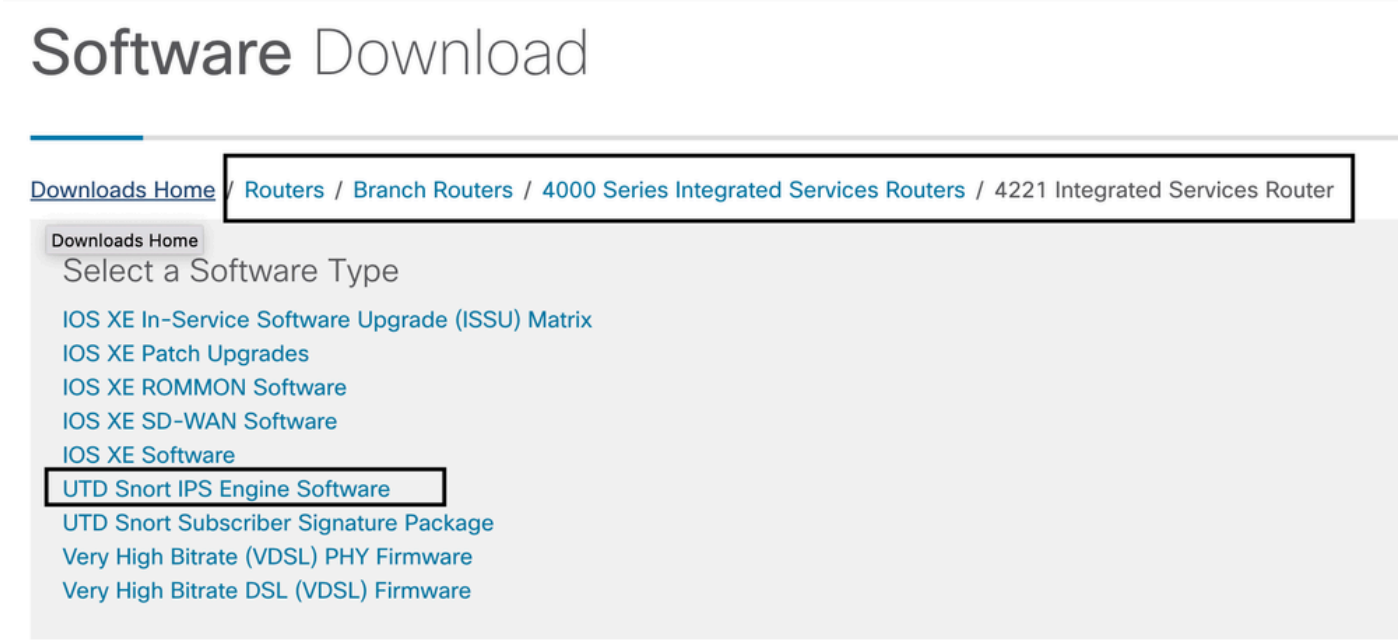


Router con software Cisco IOS XE (17.x)

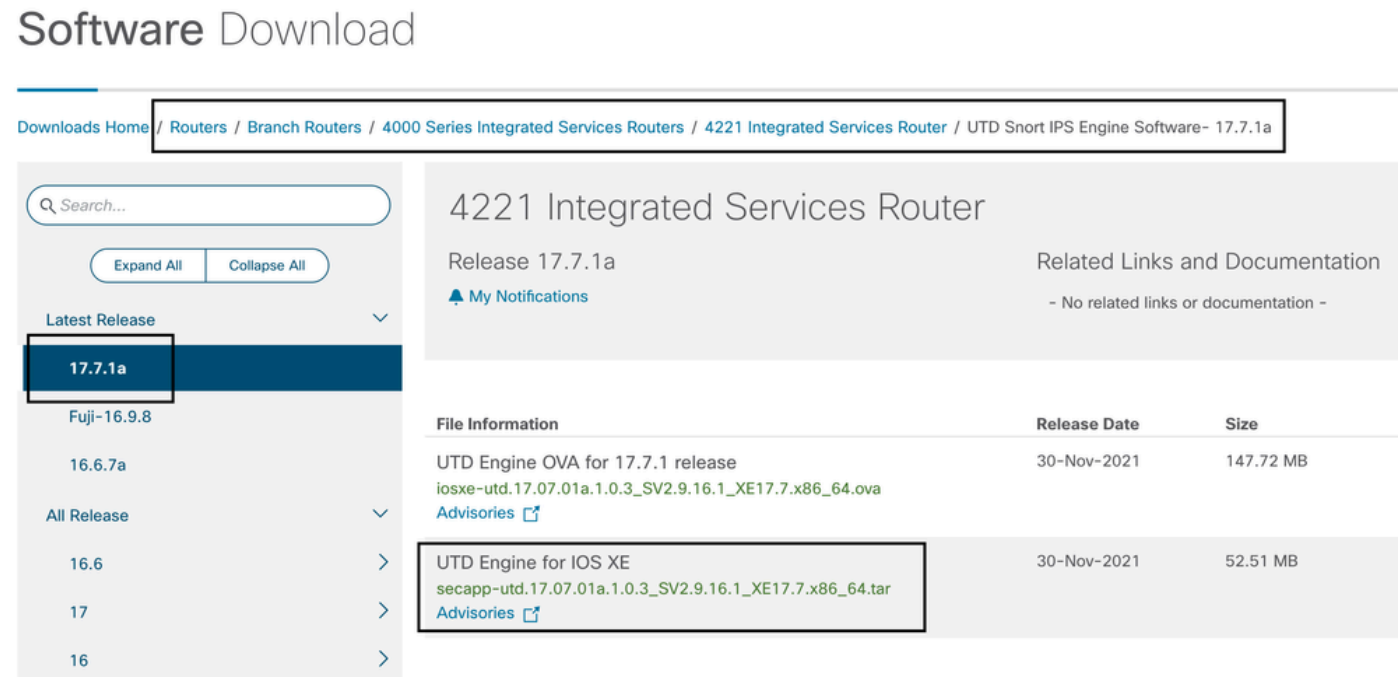
Cisco IOS XE versione 17.2.1r e la versione più recente usano l'immagine universalk9 per installare Cisco IOS XE SD-WAN e Cisco IOS XE sui dispositivi Cisco IOS XE.
Il software UTD Snort IPS Engine si trova in Router > Router per filiali > Router integrati in serie.



Dopo aver scelto il tipo di modello del router, selezionare il software UTD Snort IPS Engine.



Selezionare la versione corrente del router e scaricare il pacchetto UTD per la versione selezionata.

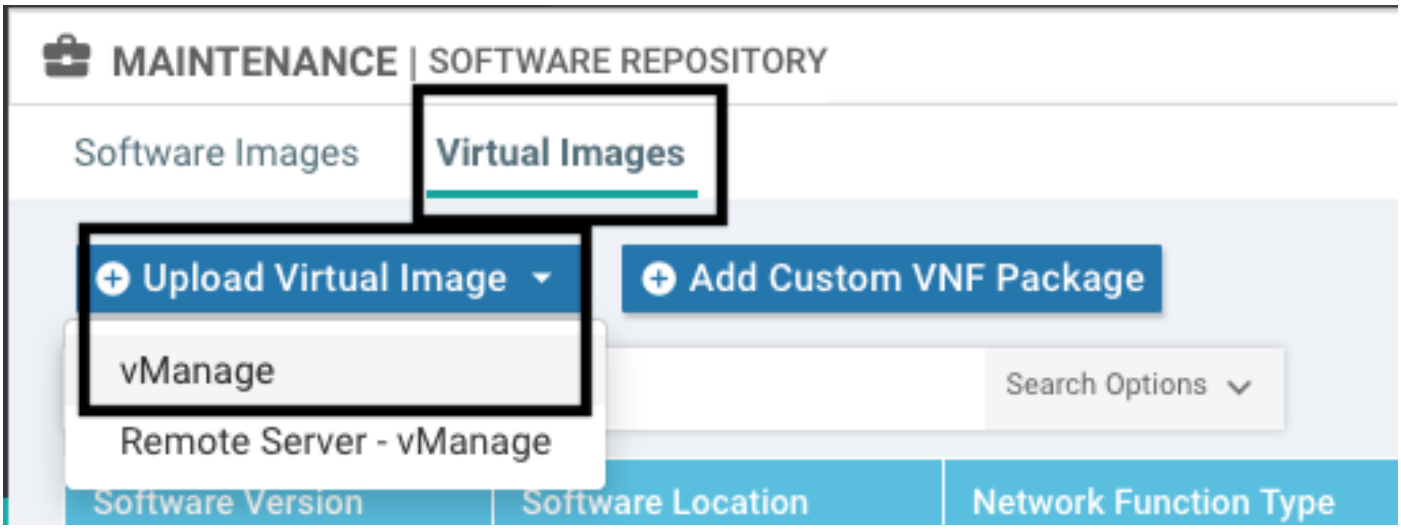


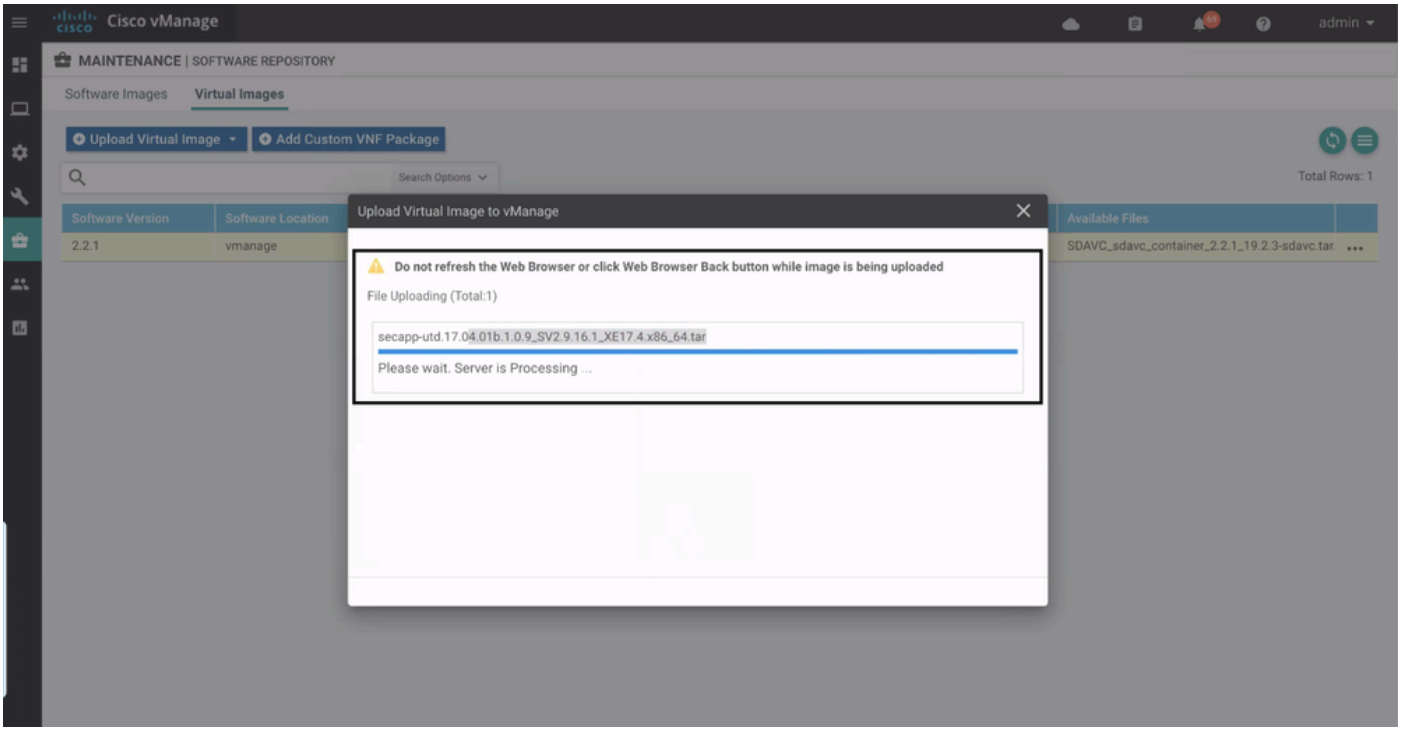
Nota: i router Cisco serie ISR1100X (Cisco Nutella SR1100X-4G/6G) con software Cisco IOS XE anziché con codice Viptela sono basati su x86_x64. È possibile utilizzare l'immagine virtuale UTD Cisco pubblicata per ISR4K. È possibile installare sul router Nutella la stessa versione del codice di immagine UTD Cisco supportata dal regex per la versione corrente di Cisco IOS XE SD-WAN. Utilizzare il comando show utd engine standard version per convalidare l'immagine UTD Cisco regex consigliata e supportata.

Configurazione

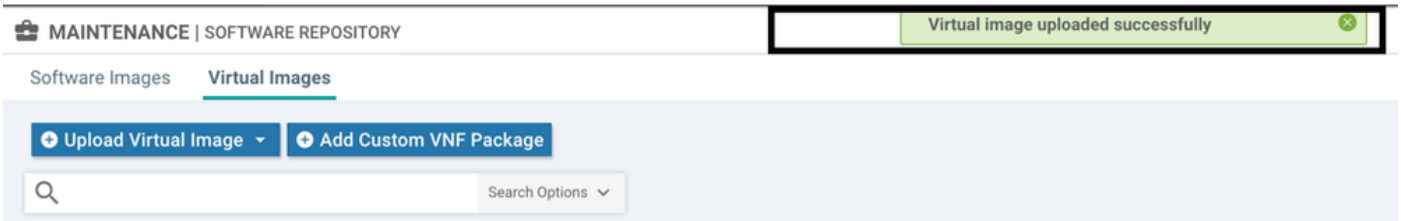
Passaggio 1. Carica immagine virtuale

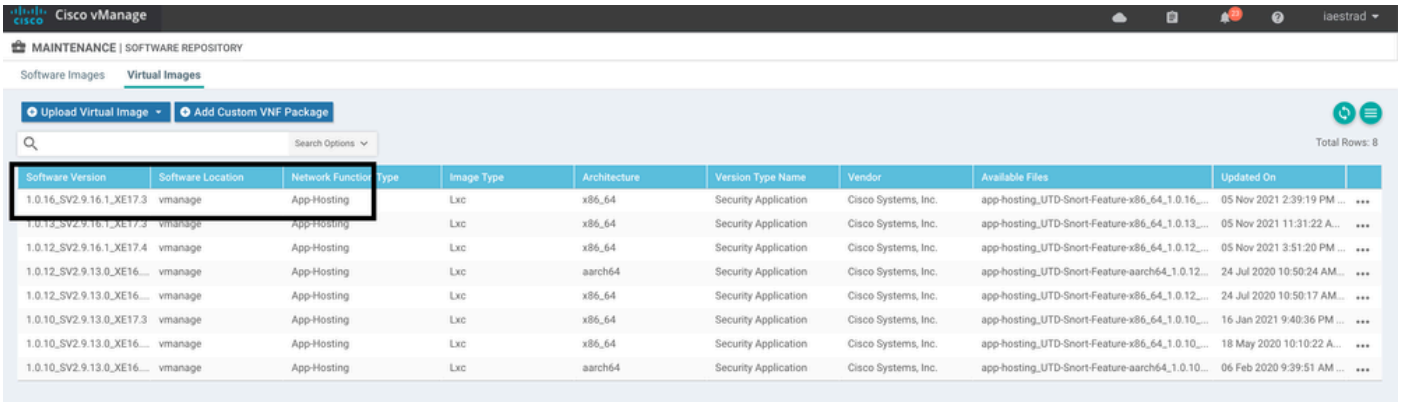
Verificare che l'immagine virtuale corrisponda al codice Cisco IOS XE SD-WAN corrente sul perimetro Cisco e caricarla in per gestire il repository.
Passare a Manutenzione > Repository software > Immagine virtuale > Carica immagine virtuale > vManage.





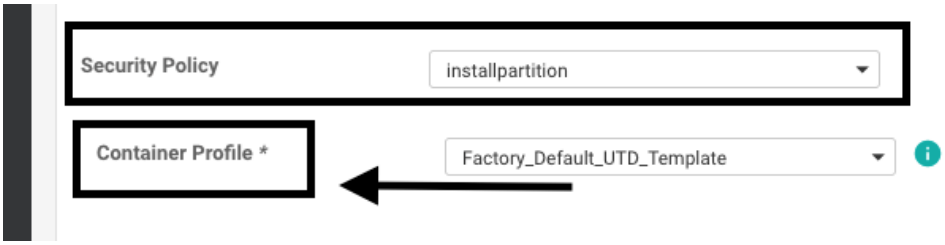
Una volta caricata correttamente l'immagine virtuale Cisco UTD, verificare che si trovi nel repository.





Passaggio 2. Aggiungi criterio di protezione e sottomodello di profilo contenitore al modello di dispositivo

Aggiungere il criterio di protezione creato in precedenza al modello di dispositivo. Il criterio di protezione deve includere un criterio di filtro IPS/IDS, URL-F o AMP nel modello del dispositivo. Aprire automaticamente il profilo contenitore. Utilizzare il profilo contenitore predefinito o modificarlo se necessario.

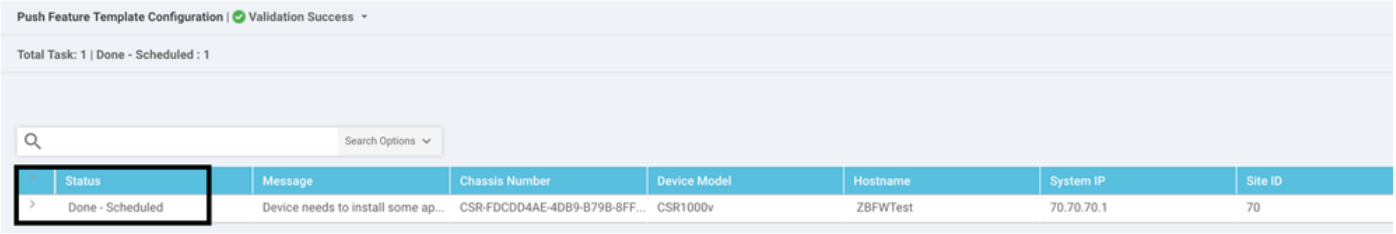


Passaggio 3. Aggiornare o collegare il modello di dispositivo con il criterio di protezione e il profilo del contenitore

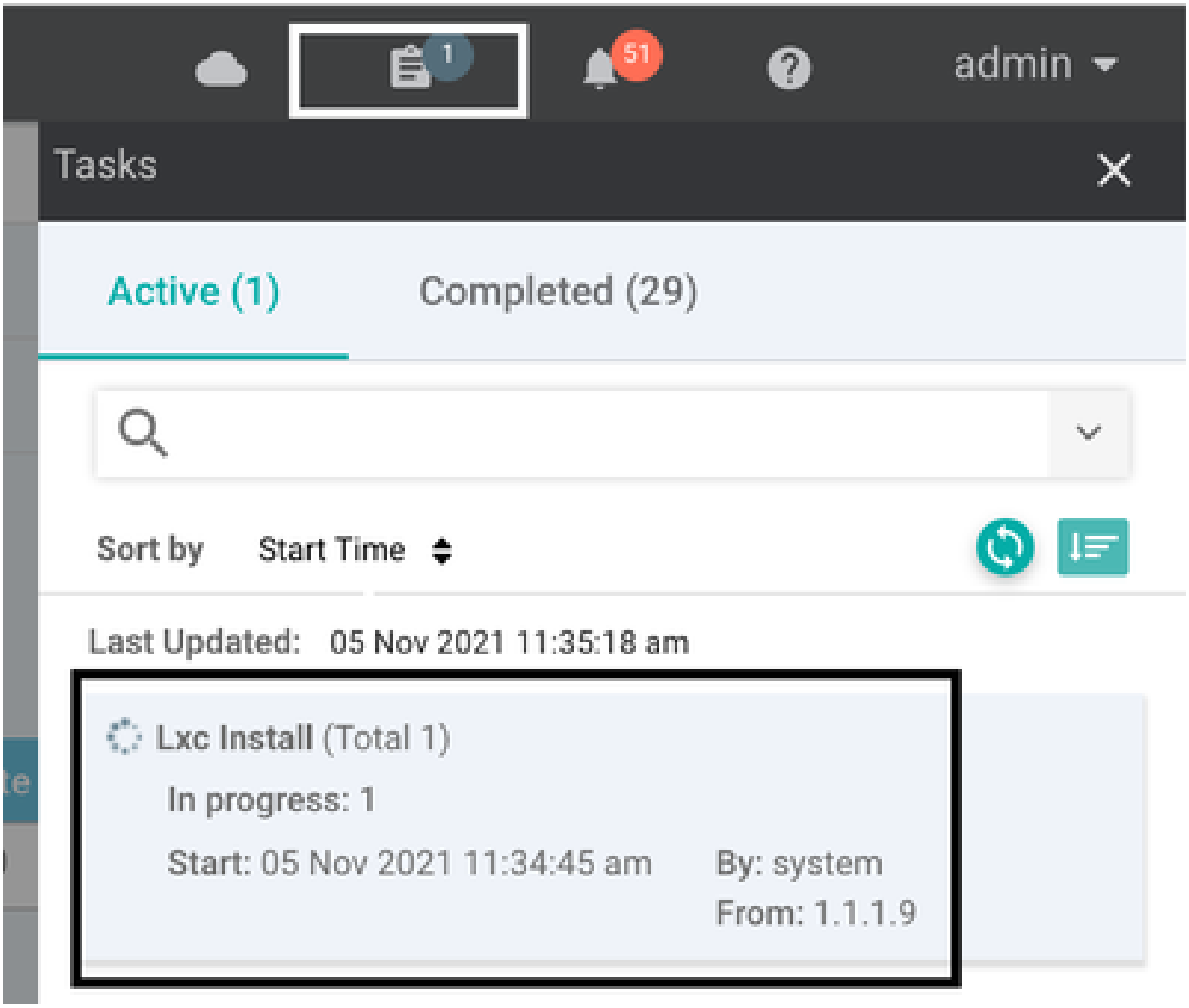
Aggiornare o collegare il modello al router Cisco Edge. Notare sulle differenze di configurazione che è configurata la configurazione di hosting dell'app e il motore UTD per la funzionalità IPS/IDS, URL-F o filtro AMP.

```
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
!
```

Lo stato del modello viene modificato in Fatto-pianificato perché il gestore ha notato che la configurazione applicata ha funzionalità del motore UTD, quindi il gestore determina che il Cisco Edge deve installare l'immagine virtuale per usare le funzionalità di sicurezza UTD.



Una volta che il modello è stato spostato allo stato di programmazione, nel menu delle operazioni viene visualizzata una nuova operazione in corso. La nuova attività è l'installazione Lxc, ovvero il gestore avvia automaticamente l'installazione dell'immagine virtuale sul Cisco Edge prima di eseguire il push della nuova configurazione.

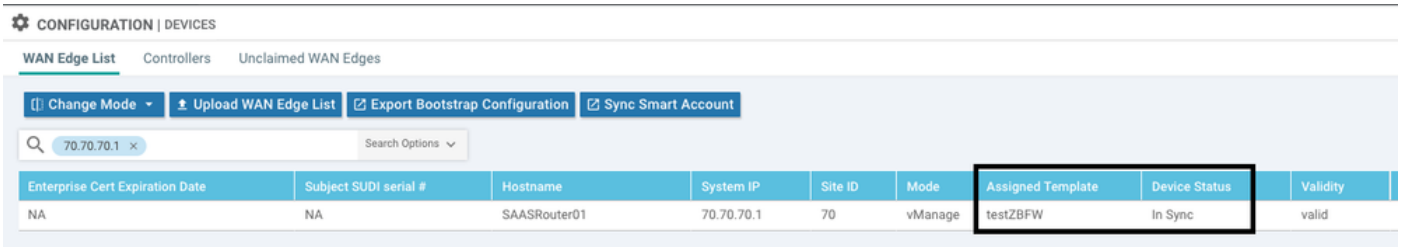


Una volta installato il contenitore LX, vManage esegue il push della configurazione pre-pianificazione con le funzionalità UTD. Non è disponibile una nuova attività per questa operazione perché la configurazione è stata pianificata in precedenza.

Verifica

Verificare che Cisco Edge sia sincronizzato con vManage e il modello associato.

Selezionare Configurazione > Dispositivi



Verificare se è installata la versione UTD di Cisco:

```
<#root>

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

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

Nota Lo stato della versione installata di UTD non può essere UNSUPPORTED.

Verificare se lo stato UTD è in esecuzione con l'output successivo:

```
<#root>

Router02#

show app-hosting list


App id                                   State
---------------------------------------------------------
utd                                      RUNNING

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

Il comando successivo riepiloga i comandi precedenti e mostra lo stato e la versione correnti:

```
<#root>

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
```

Il comando Mostra stato standard motore UTD visualizza lo stato di integrità del motore UTD e l'ora in cui viene ottenuto l'aggiornamento della firma.

<#root>

```
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
```

Verificare le funzionalità abilitate utilizzando il comando successivo:

<#root>

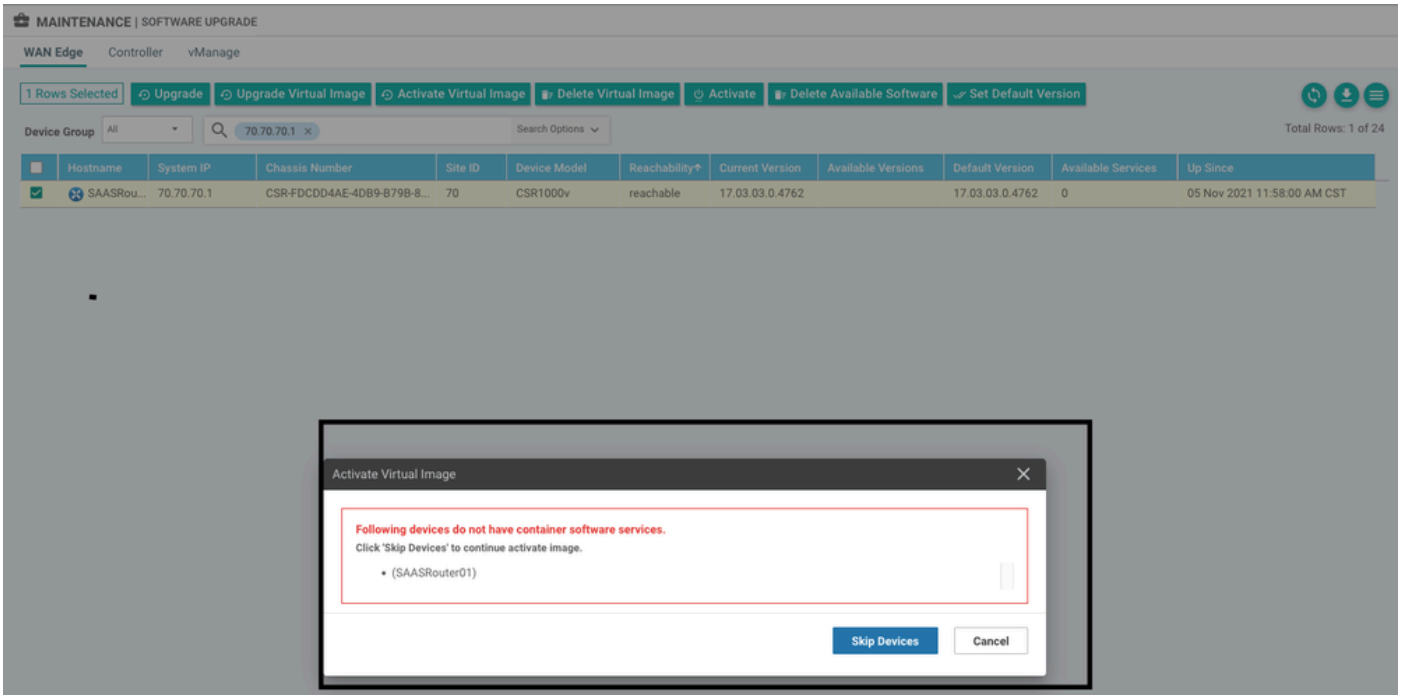
```
Router02#

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
```

Problemi comuni

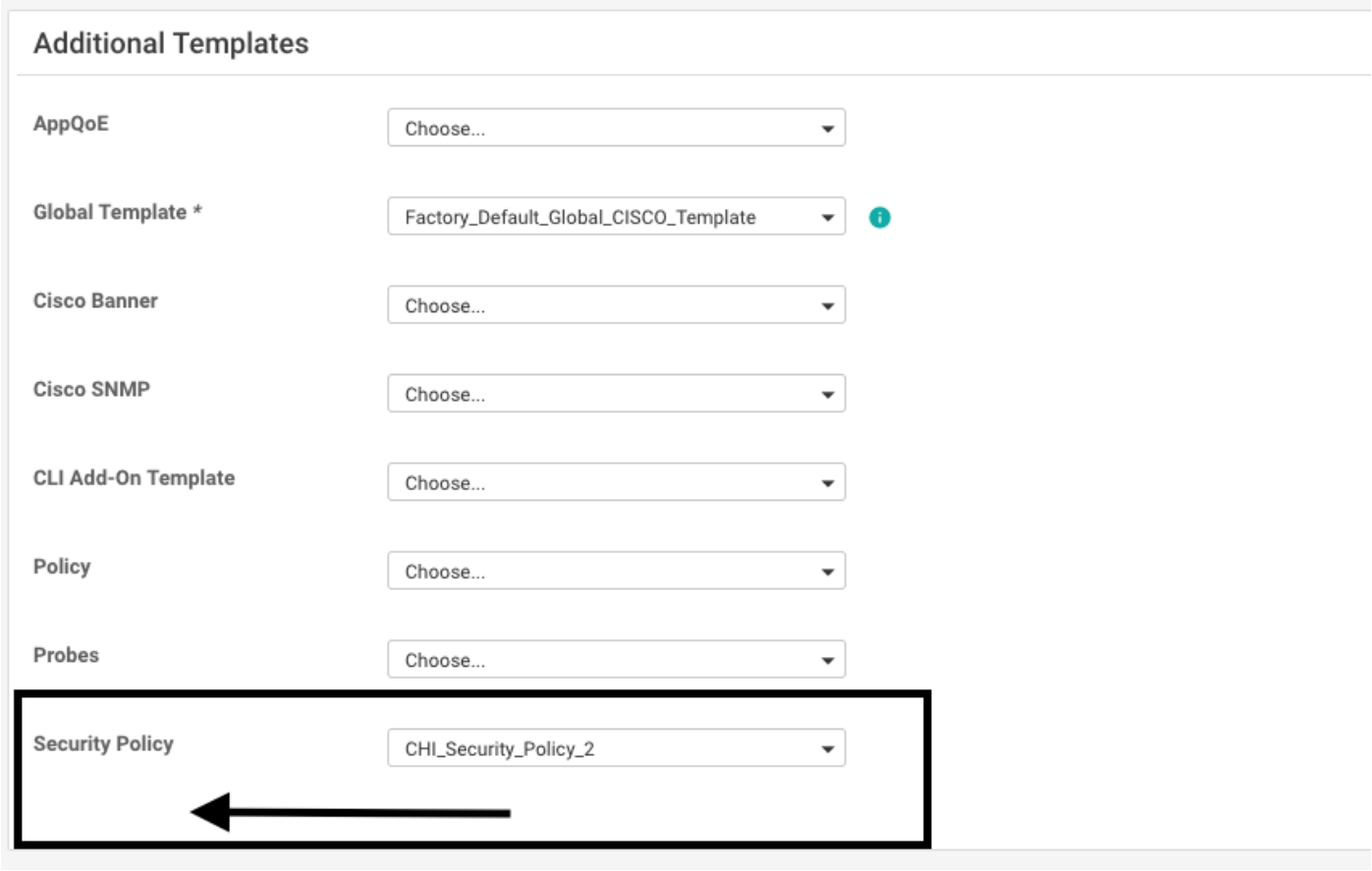
NUMERO 1. Errore: i seguenti dispositivi non dispongono di servizi software contenitore

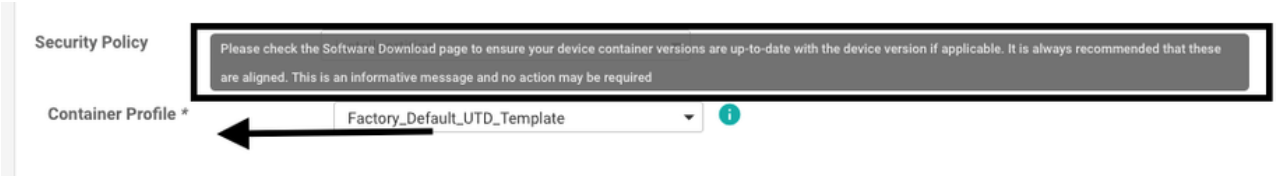
Attivare l'immagine virtuale.

Selezionare manutenzione > software > attiva

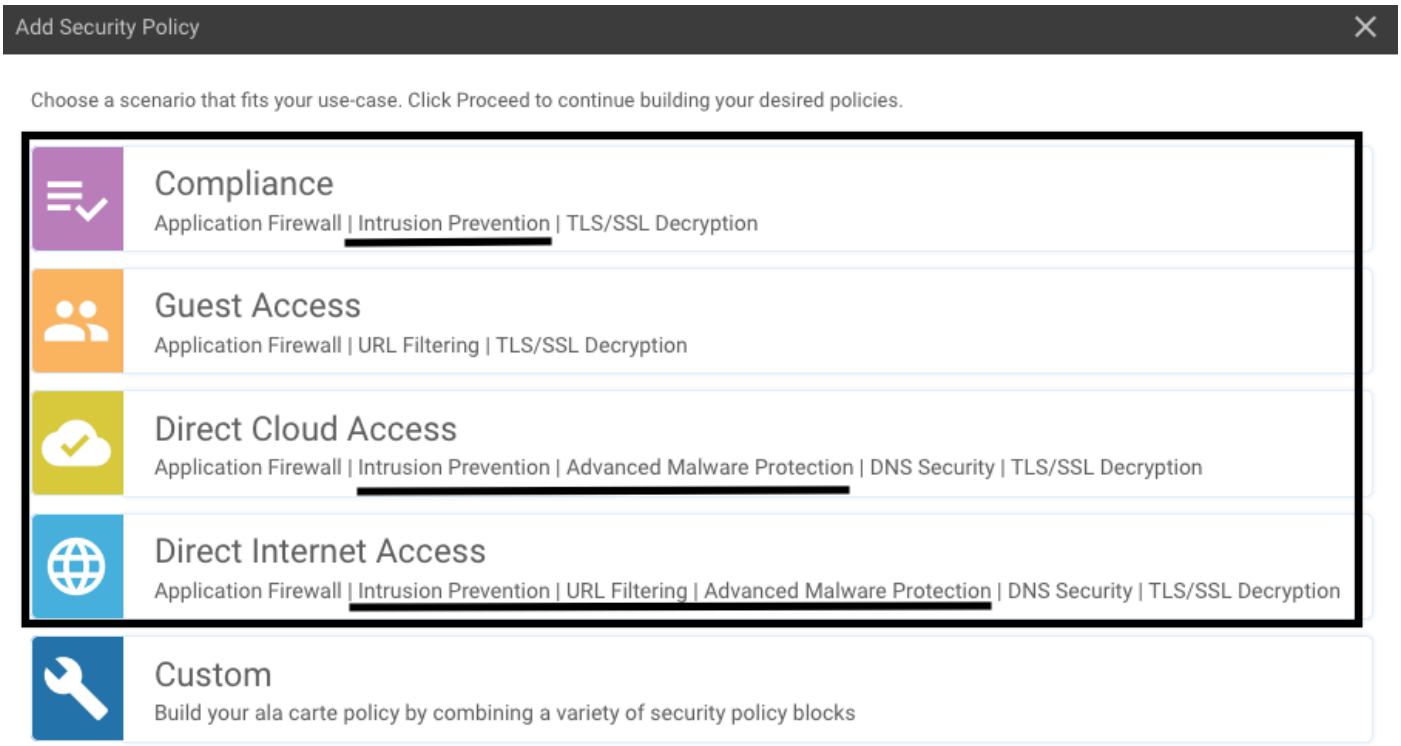


L'immagine virtuale invia un messaggio di errore: i dispositivi non dispongono di servizi software contenitore, se il router Cisco Edge selezionato non dispone di un criterio di sicurezza con il sottomodello del profilo del contenitore.





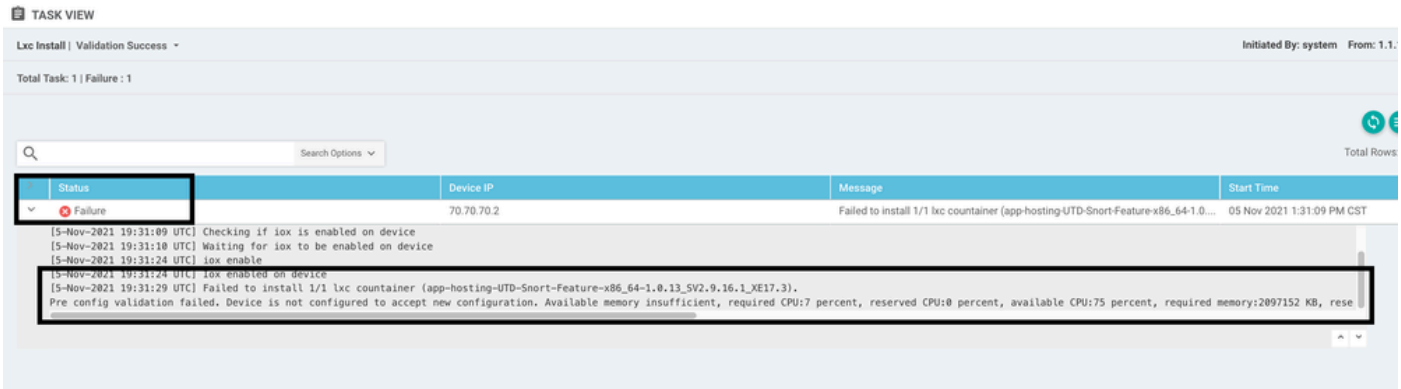
Questo modello viene aggiunto automaticamente se si utilizza un criterio di sicurezza che include funzionalità di sicurezza quali IPS (Intrusion Prevention System), IDS (Intrusion Detection System), URL Filtering (URL-F) e AMP (Advanced Malware Protection) che richiedono un pacchetto UTD. Non tutte le funzioni di sicurezza disponibili necessitano di un motore UTD come la semplice funzione ZBFW.



Una volta eseguito il push del modello con il sottomodello del profilo del contenitore, il gestore installa automaticamente l'immagine virtuale.

NUMERO 2. Memoria disponibile insufficiente

Verificare che il router Cisco Edge disponga di 8 GB di memoria DRAM. In caso contrario, il processo di installazione Lxc che invia un dispositivo non è configurato per accettare la nuova configurazione. Errore di memoria insufficiente. Per utilizzare le funzionalità UTD, i router Cisco Edge devono avere almeno 8 GB di DRAM.



In questo caso, i CSRv hanno solo 4 GB di DRAM. Dopo l'aggiornamento della memoria alla memoria DRAM da 8 GB, l'installazione è riuscita.

Verificare la memoria totale corrente con l'output show sdwan system status:

<#root>

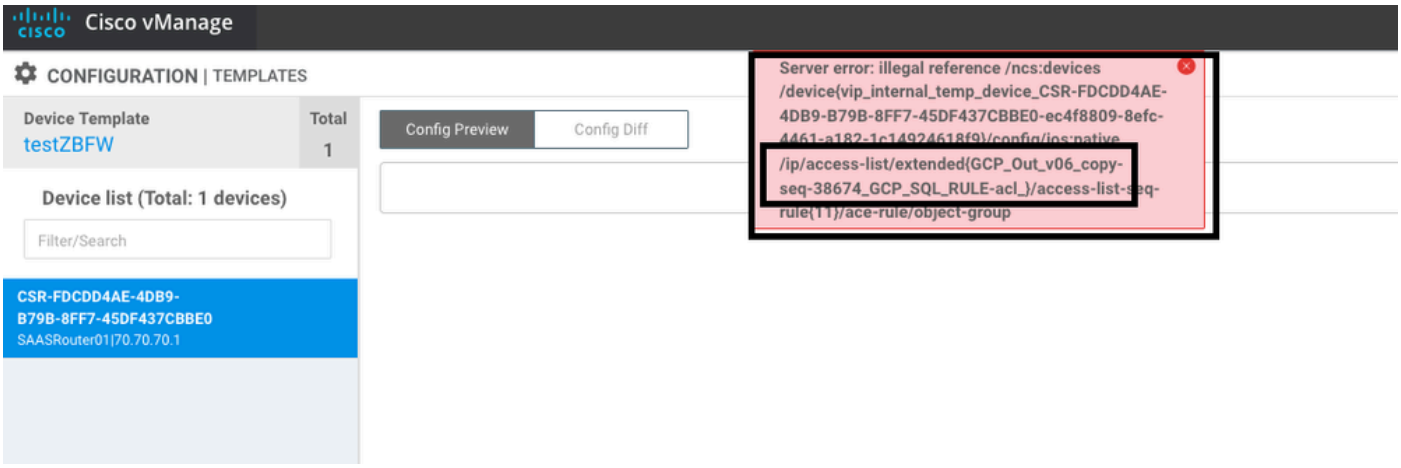
```
Router01#
```

```
show sdwan system status

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

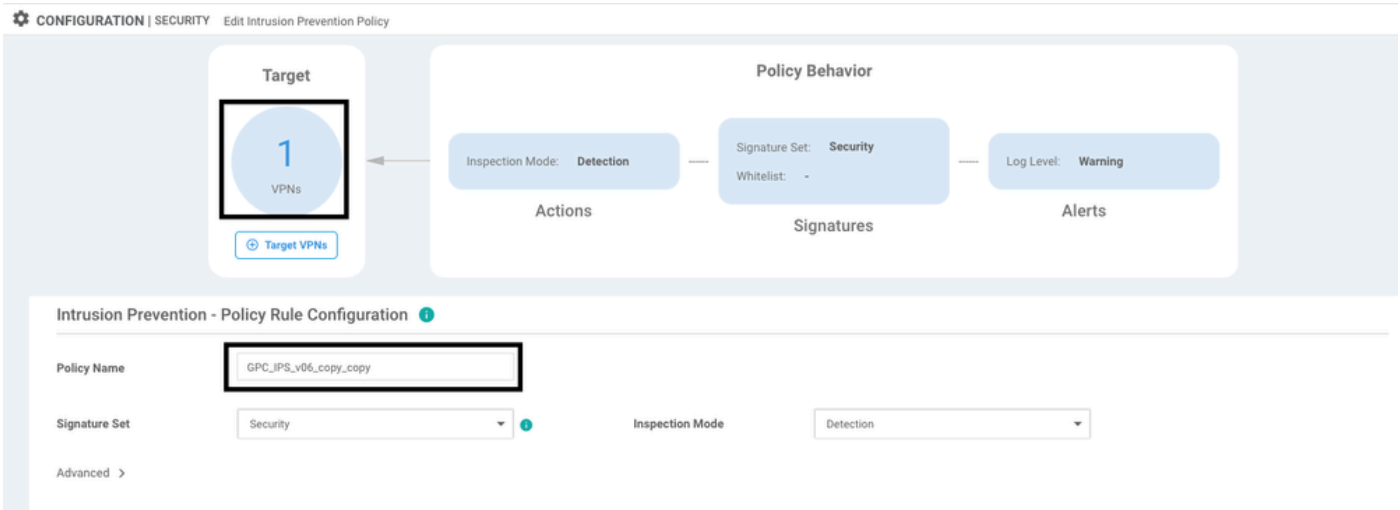
Nota Per installare UTD deve essere disponibile una quantità di memoria sufficiente. Se la DRAM installata è adeguata ma l'installazione non riesce a causa di memoria insufficiente, controllare l'utilizzo corrente in mostra processi piattaforma di memoria ordinata

NUMERO 3. Riferimento non valido

Verificare che le VPN/VRF utilizzate su una delle funzionalità dei criteri di sicurezza siano già configurate nel router perimetrale Cisco per evitare un riferimento non valido per le sequenze dei criteri di sicurezza.



In questo esempio, il criterio di sicurezza dispone di un criterio di prevenzione delle intrusioni per VPN/VRF 1, ma i dispositivi non dispongono di alcun VRF 1 configurato. Pertanto, il gestore invia un riferimento non valido per tale sequenza di criteri.



Dopo aver configurato il VRF indicato nei criteri di protezione, il riferimento Illegal non viene visualizzato e il modello viene sottoposto a push correttamente.

NUMERO 4. UTD installato e attivo ma non abilitato

Per il dispositivo è configurato un criterio di protezione e l'UTD è installato e attivo ma non è abilitato.

Questo problema è correlato al numero di problema 3. Tuttavia, vManage ha consentito alla configurazione di fare riferimento a VRF non configurati nel dispositivo e il criterio non viene applicato ad alcun VRF.

Per determinare se il router è in grado di risolvere il problema, è necessario che l'UTD sia attivo. UTD non abilitato messaggio e il criterio non fa riferimento ad alcun VRF.

```
<#root>

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
```

Per la risoluzione, verificare le VPN di destinazione e assicurarsi di applicare il criterio a un VRF configurato.

Video

Installa immagine virtuale di sicurezza UTD su router cEdge

Informazioni correlate

- Sicurezza router: bloccare IPS sui router
- Guida alla configurazione della sicurezza di Cisco SD-WAN, Cisco IOS XE release
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).