在边缘路由器上安装UTD安全虚拟映像

目录

简介

本文档介绍如何安装统一威胁防御(UTD)安全虚拟映像以在Cisco IOS XE SD-WAN设备上启用安全功能。

先决条件

- 使用这些功能之前，请将相关的安全虚拟映像上传到vManage存储库。
- 边缘路由器必须处于vmanage模式，且已附加模板。
- 为入侵防御系统(IPS)、入侵检测系统(IDS)、URL过滤(URL-F)或高级恶意软件防护(AMP)过滤创建安全策略模板。

要求

- 4000集成服务路由器Cisco IOS XE SD-WAN(ISR4000)
- 1000集成服务路由器Cisco IOS XE SD-WAN(ISR1k)
- 1000v云服务路由器(CSR1kv),
- 1000v集成多业务路由器(ISRv)
- 支持8GB DRAM的边缘平台。

使用的组件

- 思科UTD虚拟映像
- vManage控制器
- 边缘路由器与控制连接。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

思科UTD映像需要在要安装的设备模板上安装安全策略，并启用安全功能，例如入侵防御系统(IPS)、入侵检测系统(IDS)、URL过滤(URL-F)和cEdge路由器上的高级恶意软件防护(AMP)。

从软件Cisco下载Cisco UTD Snort IP引擎软件

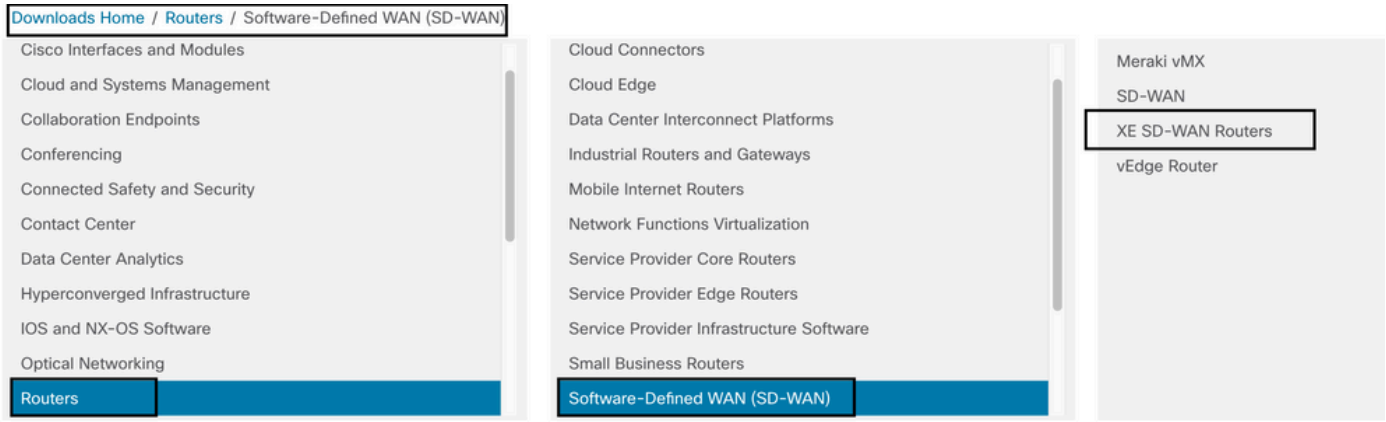
使用当前Cisco IOS XE版本支持的Cisco UTD虚拟映像regex。使用命令**show utd engine standard** version验证推荐的和支持的UTD映像。

```
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$
```

> **注意**下载映像的路径取决于路由器是运行Cisco IOS XE SDWAN软件(16.x)还是通用Cisco IOS XE软件(17.x)。

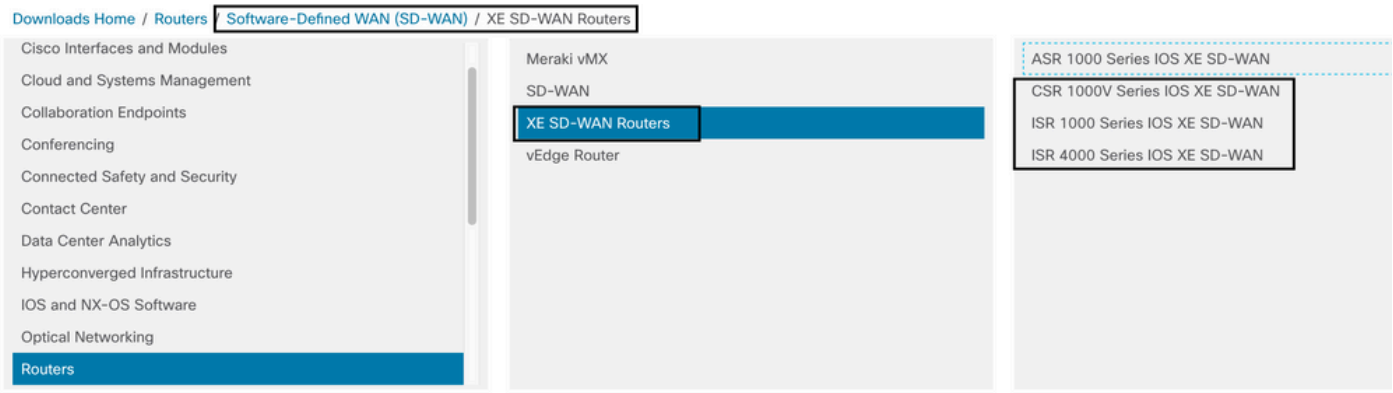
运行Cisco IOS XE SDWAN软件(16.x)的路由器

获取Cisco UTD Snort IPS引擎软件的路径为路由器/软件定义广域网(SD-WAN)/XE SD-WAN路由器/和系列集成路由器。



选择cEdge路由器的型号类型。

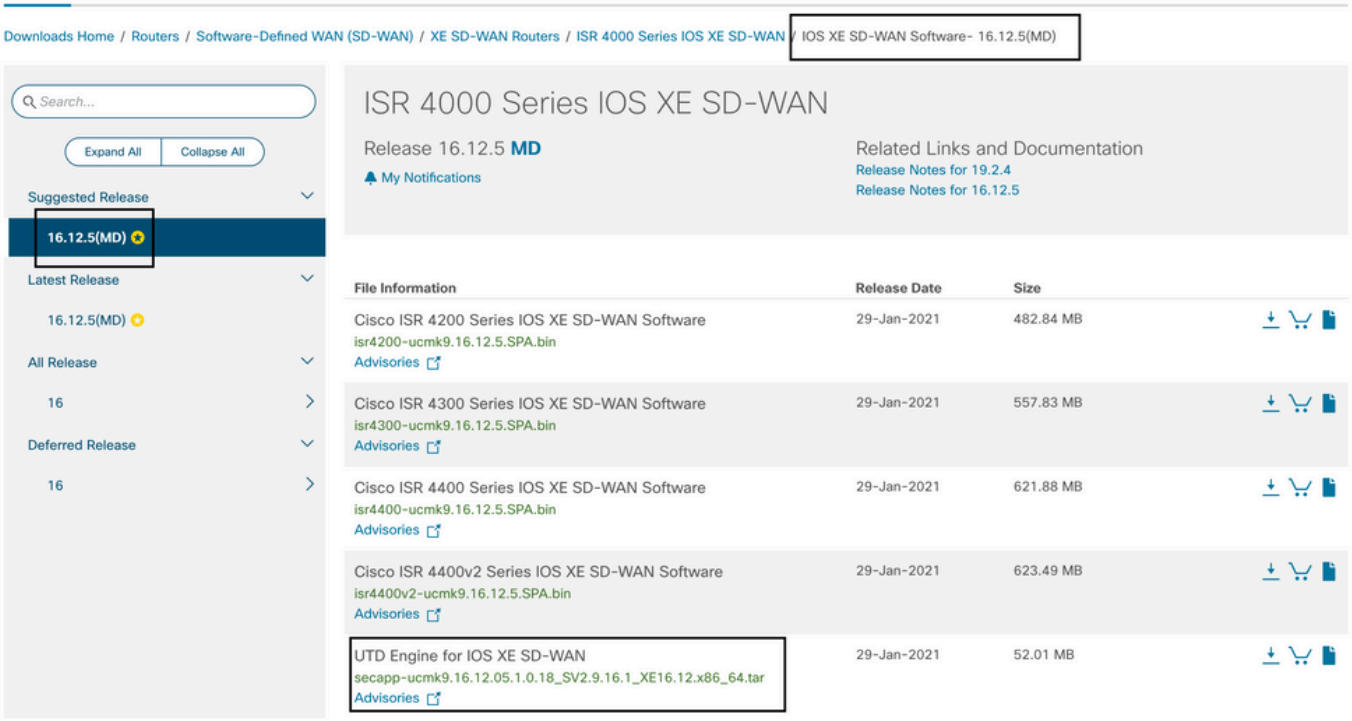
> **注意**系列聚合服务路由器(ASR)不适用于UTD功能。



选择类型路由器型号后，选择**Cisco IOS XE SD-WAN软件选项**以获取16.x版本的cEdge的UTD包。

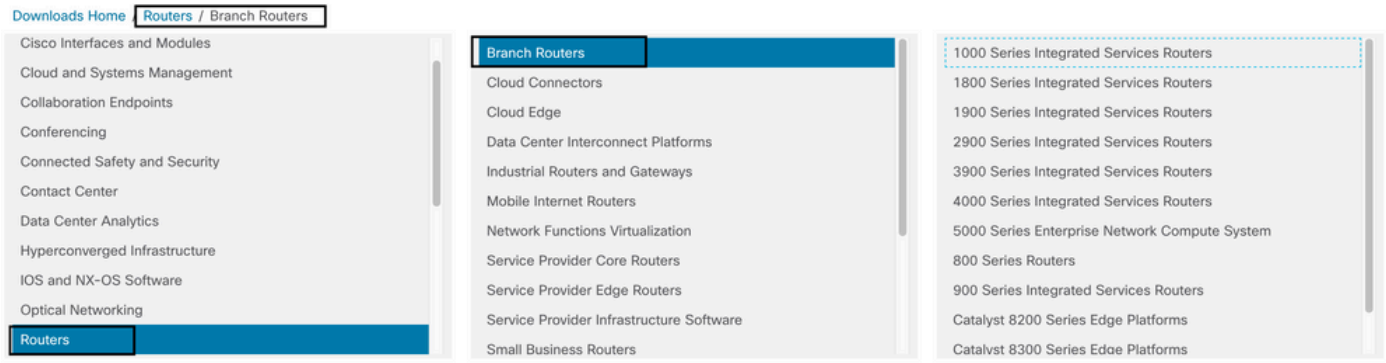
注意：为cEdge路由器的16.x代码选择Cisco UTD虚拟映像的下载路径还显示**Cisco IOS XE软件**选项。此路径仅用于为17.x选择cEdge的升级代码，但找不到版本17.x的UTD虚拟映像。17.x和最新版本上的Cisco unified常规Cisco IOS XE和Cisco IOS XE SDWAN代码，因此获取17.x的Cisco UTD虚拟映像的路径与常规Cisco IOS XE代码相同。

选择cEdge的当前版本，并下载该版本的UTD软件包。

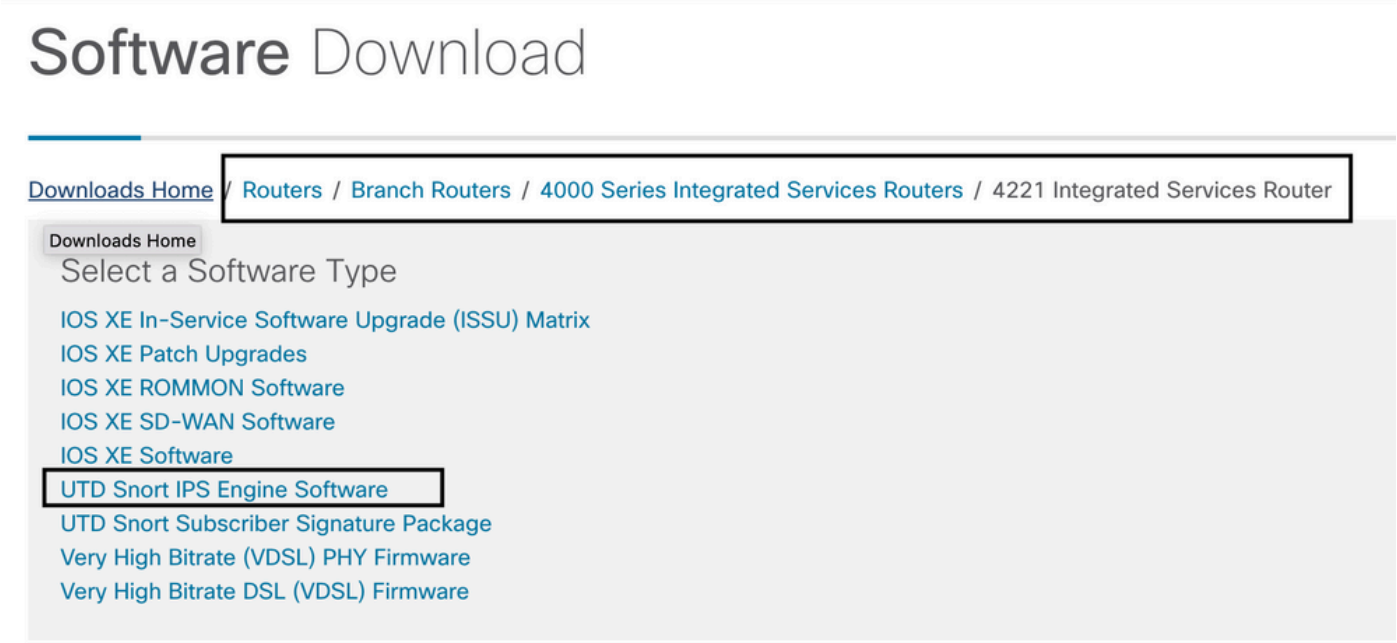


运行Cisco IOS XE软件(17.x)的路由器

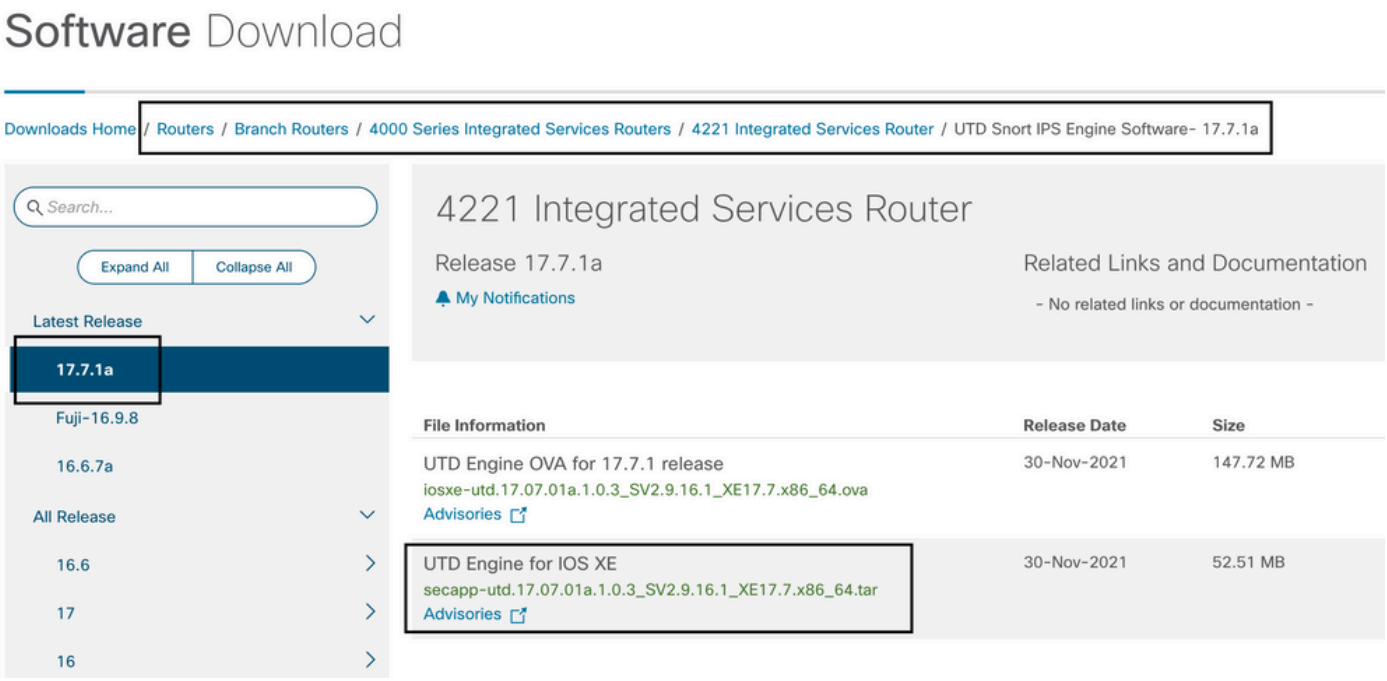
Cisco IOS XE版本17.2.1r和最新版本使用universalk9映像在Cisco IOS XE设备上部署Cisco IOS XE SD-WAN和Cisco IOS XE。
UTD Snort IPS引擎软件位于Routers > Branch Routers > Series Integrated Router中。



选择路由器的型号类型后，选择**UTD Snort IPS Engine Software**。



选择路由器的当前版本，并为所选版本下载UTD软件包。

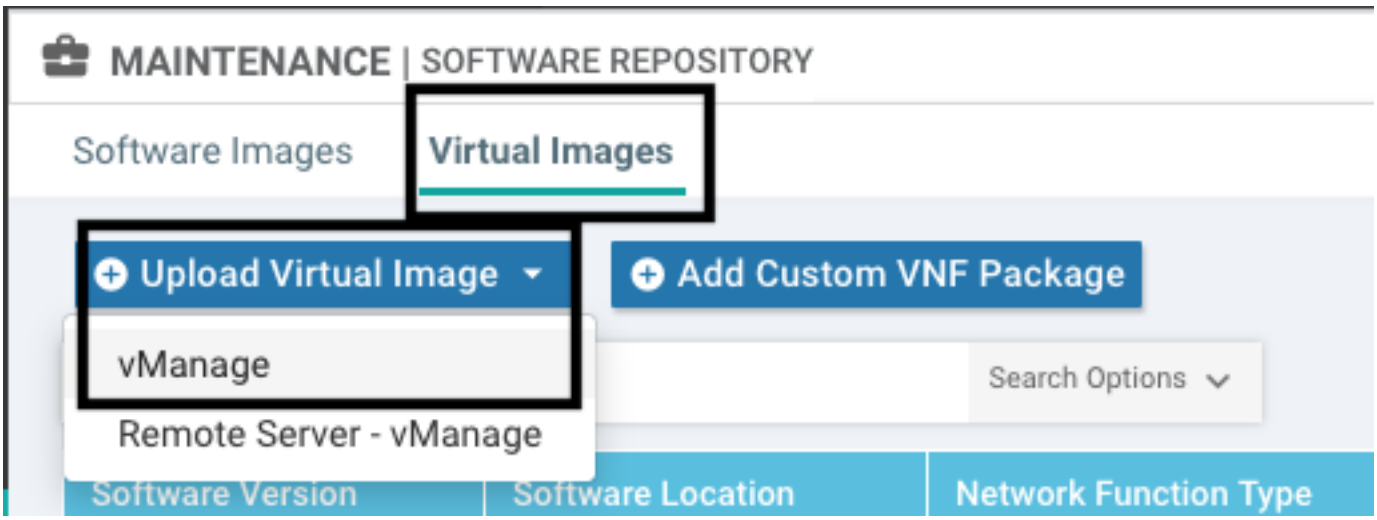


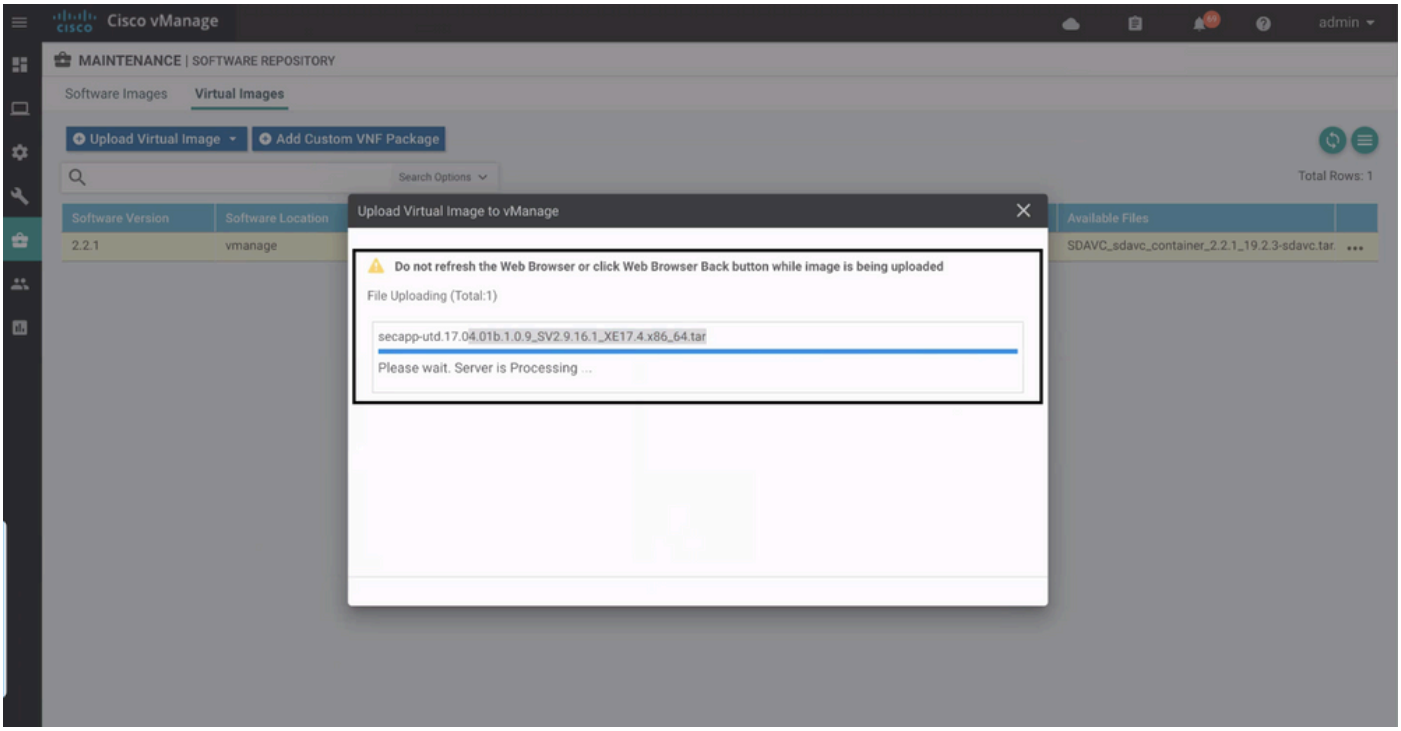
注意：运行Cisco IOS XE软件而非Viptela代码的Cisco ISR1100X系列路由器（Cisco Nutella路由器SR1100X-4G/6G）基于x86_x64。为ISR4K发布的Cisco UTD虚拟映像可以在这些路由器上运行。您可以在Nutella路由器上安装当前Cisco IOS XE SDWAN版本支持的相同Cisco UTD映像代码版本regex。使用命令**show utd engine standard version**验证推荐的和支持的Cisco UTD正则表达式。

配置

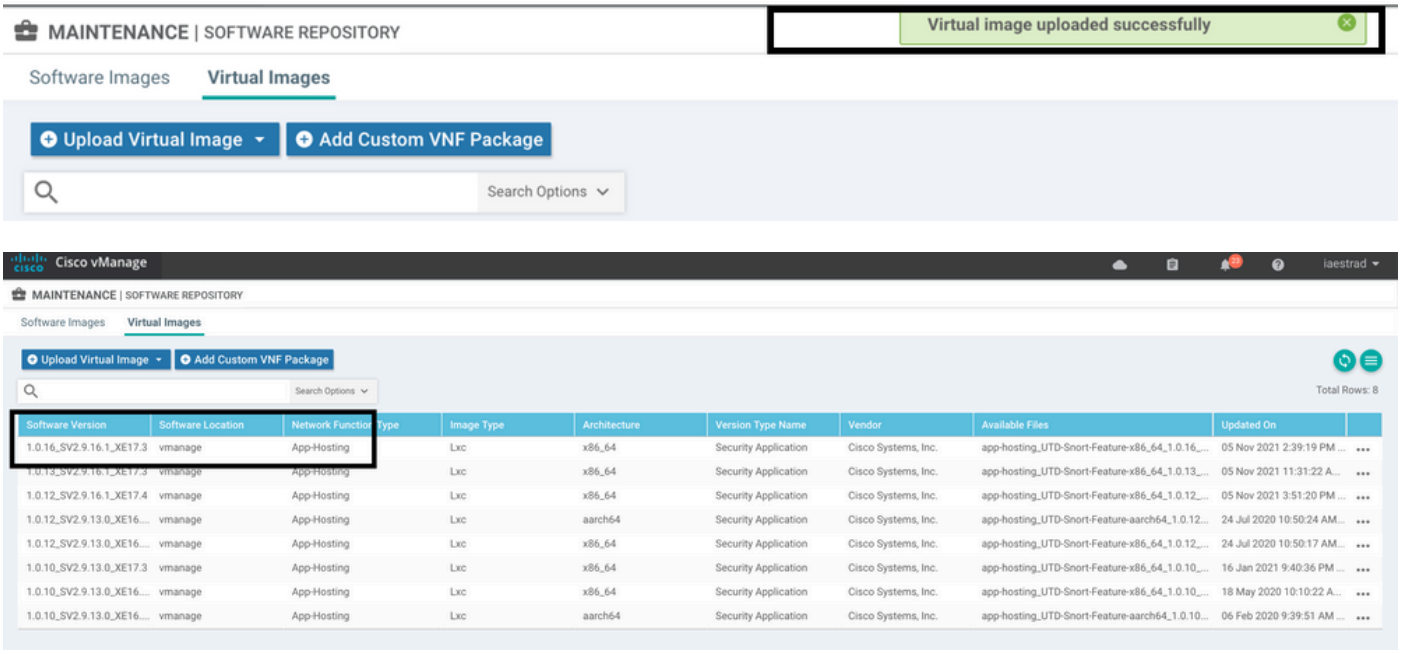
步骤1.上传虚拟映像

确保虚拟映像与cEdge上当前的Cisco IOS XE SDWAN代码相匹配，然后将其上传到vmanage存储库。
导航到**维护>软件存储库>虚拟映像>上传虚拟映像> vManage。**



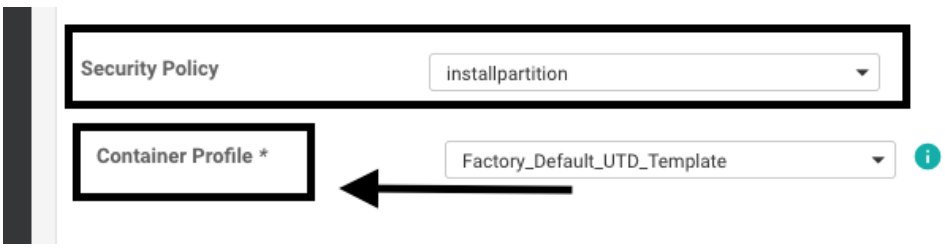


成功上传思科UTD虚拟映像后，请仔细检查其是否位于存储库中。



步骤2.将安全策略和容器配置文件子模板添加到设备模板

将之前创建的安全策略添加到设备模板。安全策略必须具有IPS/IDS、URL-F或AMP过滤策略才能将其添加到设备模板。自动打开容器配置文件。使用默认容器配置文件或在需要时对其进行修改。

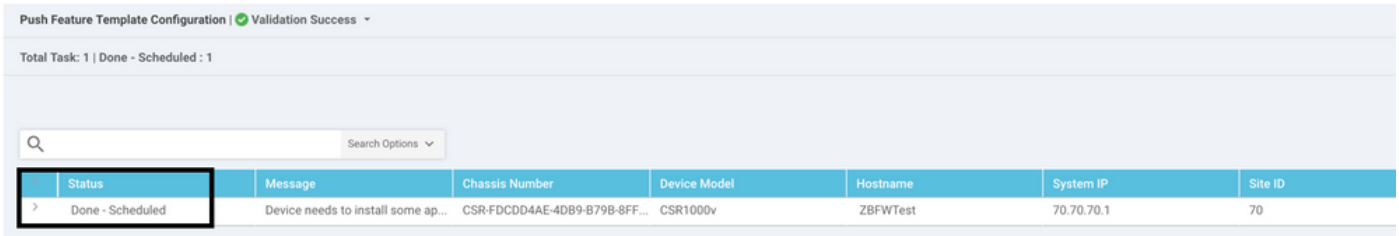


步骤3.使用安全策略和容器配置文件更新或附加设备模板

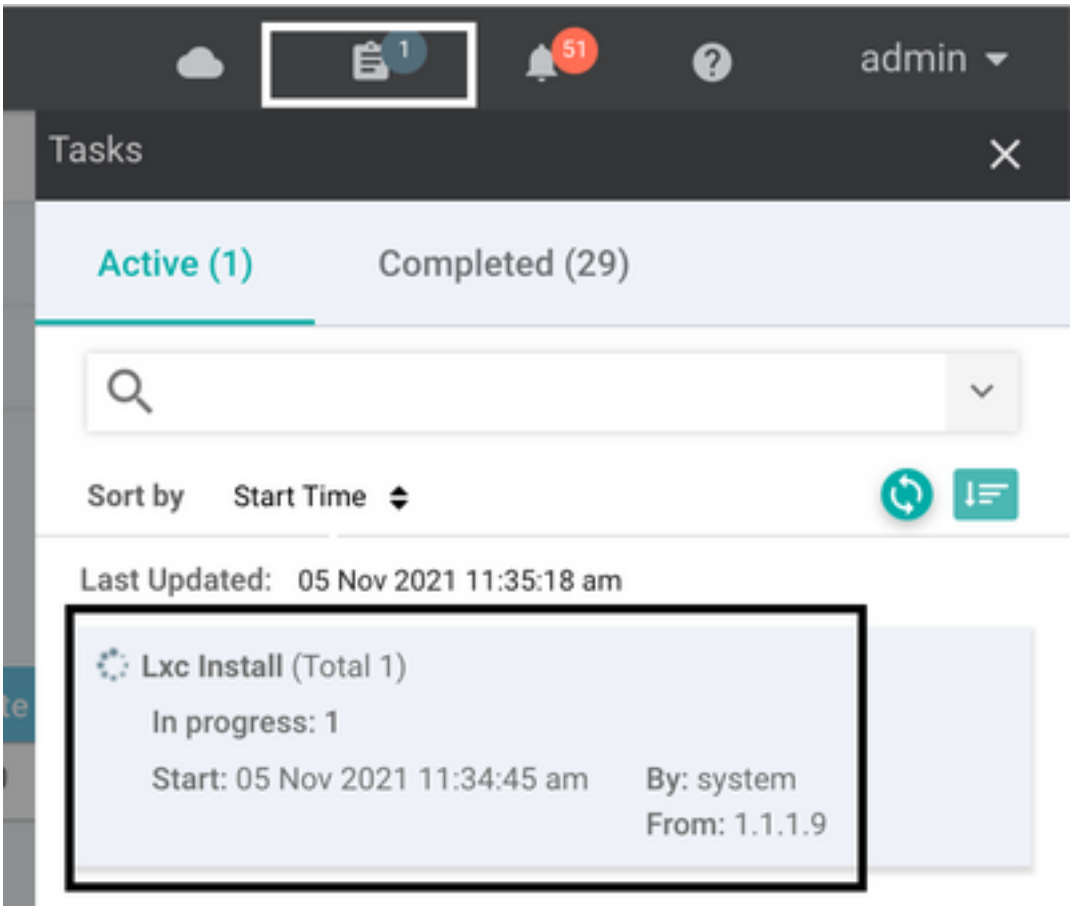
将模板更新或附加到cEdge路由器。请注意，在config diff中，已配置功能IPS/IDS、URL-F或AMP过滤的应用托管配置和UTD引擎。

```
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  lldp run
259 269  nat64 translation timeout tcp 60
260 270  nat64 translation timeout udp 1
271  utd multi-tenancy
272  utd engine standard multi-tenancy
273   threat-inspection profile GPC_IPS_v06_copy_copy
274    threat detection
275    policy security
276    logging level warning
277   !
278   utd global
279   !
280  !
281  policy
282   no app-visibility
283   no flow-visibility
284   no implicit-acl-logging
285   log-frequency        1000
286  !
```

模板状态更改为**Done-scheduled**，因为vmanage注意到应用的配置具有UTD引擎功能，因此vmanage确定cEdge需要安装虚拟映像才能使用UTD安全功能。



将模板移至计划状态后，任务菜单中会**显示一个正在进行的新任务。新任务是Lxc安装**，这意味着vmanage在推送新配置之前自动开始将虚拟映像安装到cEdge。

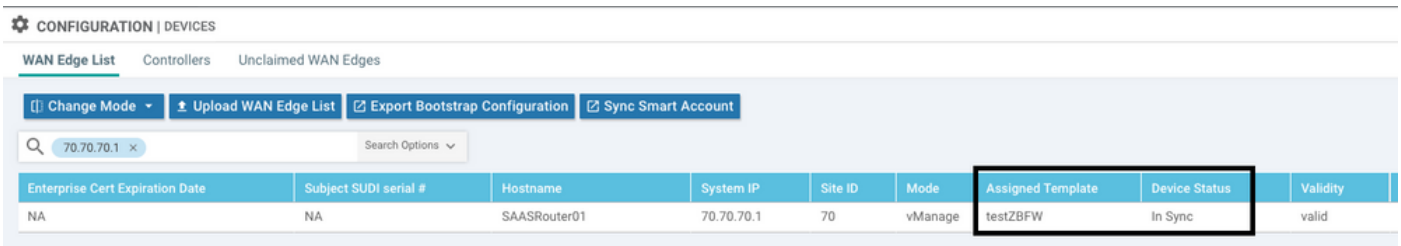


安装LX容器后，vManage会推送带有UTD功能的预定配置。由于之前已计划配置，因此没有新任务。

验证

验证cEdge是否与vManage同步，是否附加了模板。

导航到**配置>设备**



验证是否已安装Cisco UTD版本：

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

注意:UTD安装的版本不能处于**UNSUPPORTED**状态。

检查UTD是否处于运行状**态**，并返回下一个输出：

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

下一个命令汇总了之前的命令并显示当前状态和版本：

```
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命令显示UTD引擎的运行状况以及获取签名更新的列表时间。

```
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
```

使用下一命令验证启用的功能：

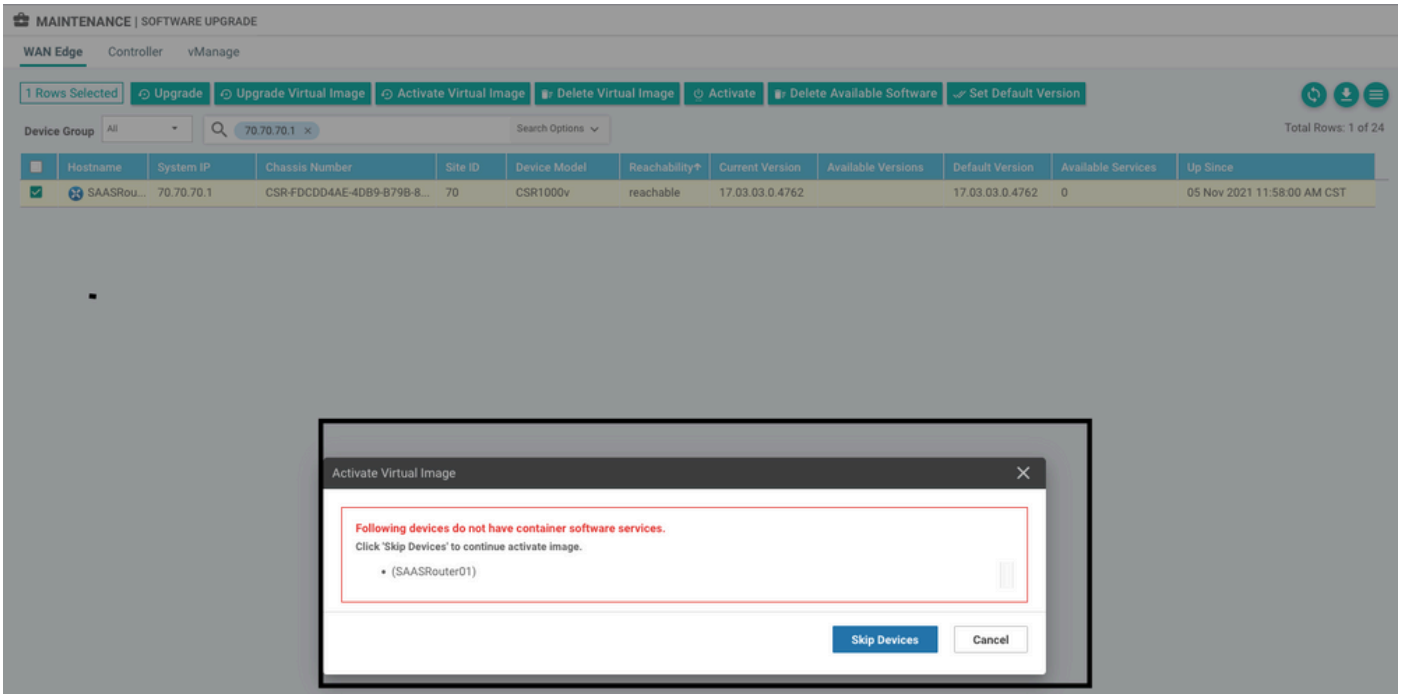
```
Router02# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
  Divert controller mode: enabled
  SN threads: 12
  CFT inst_id 0 feat id 2 fo id 2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

常见问题

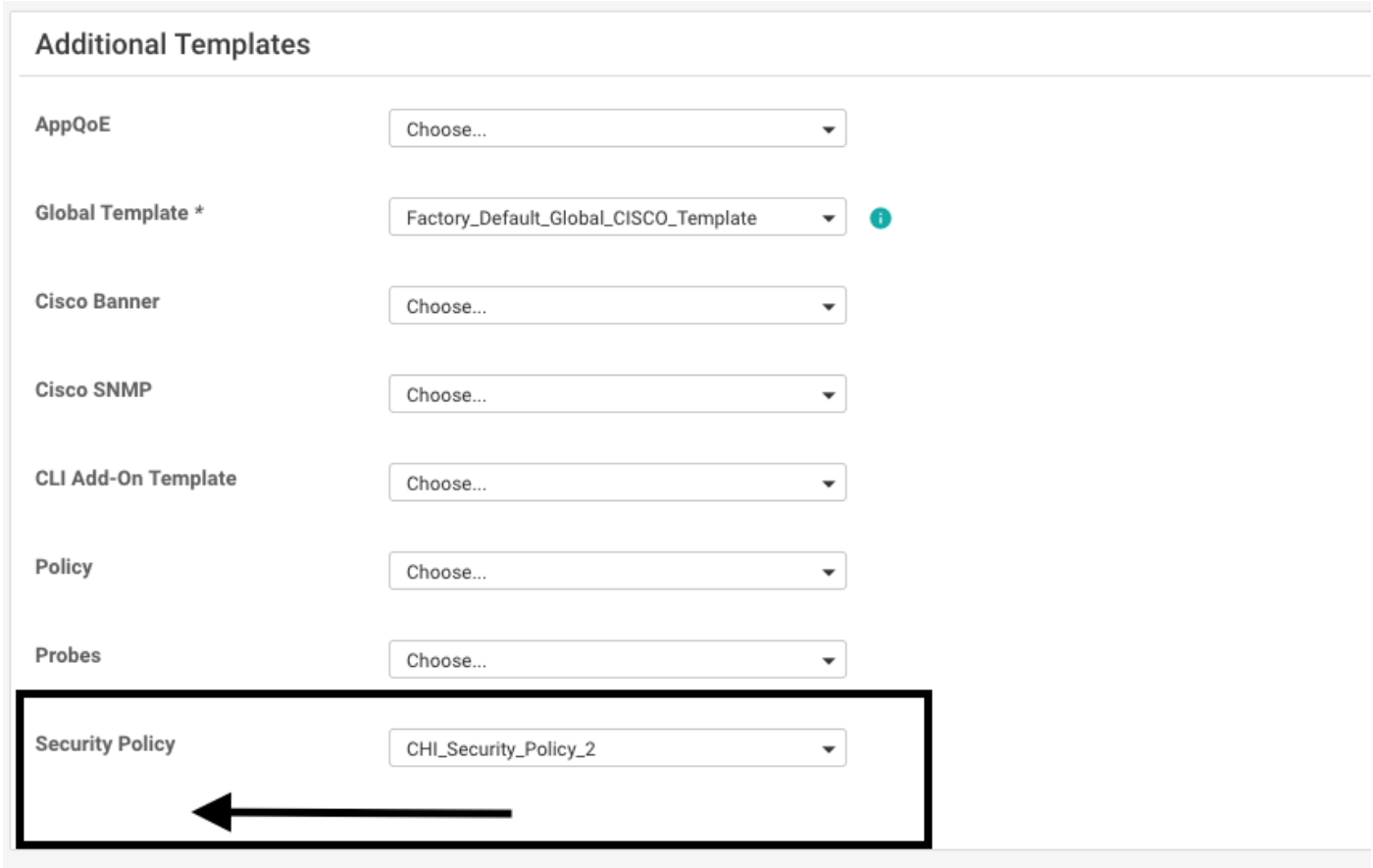
问题1.错误：以下设备没有容器软件服务

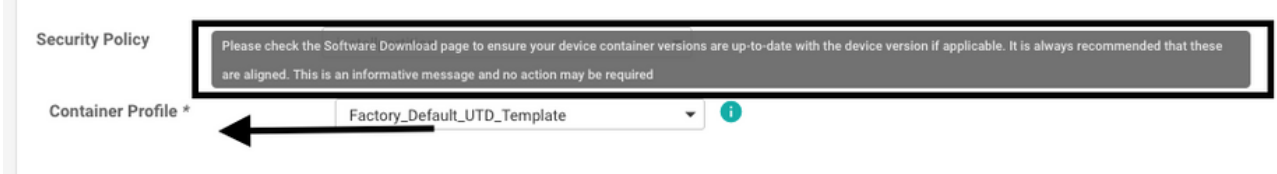
激活虚拟映像。

导航到**维护>软件>激活**



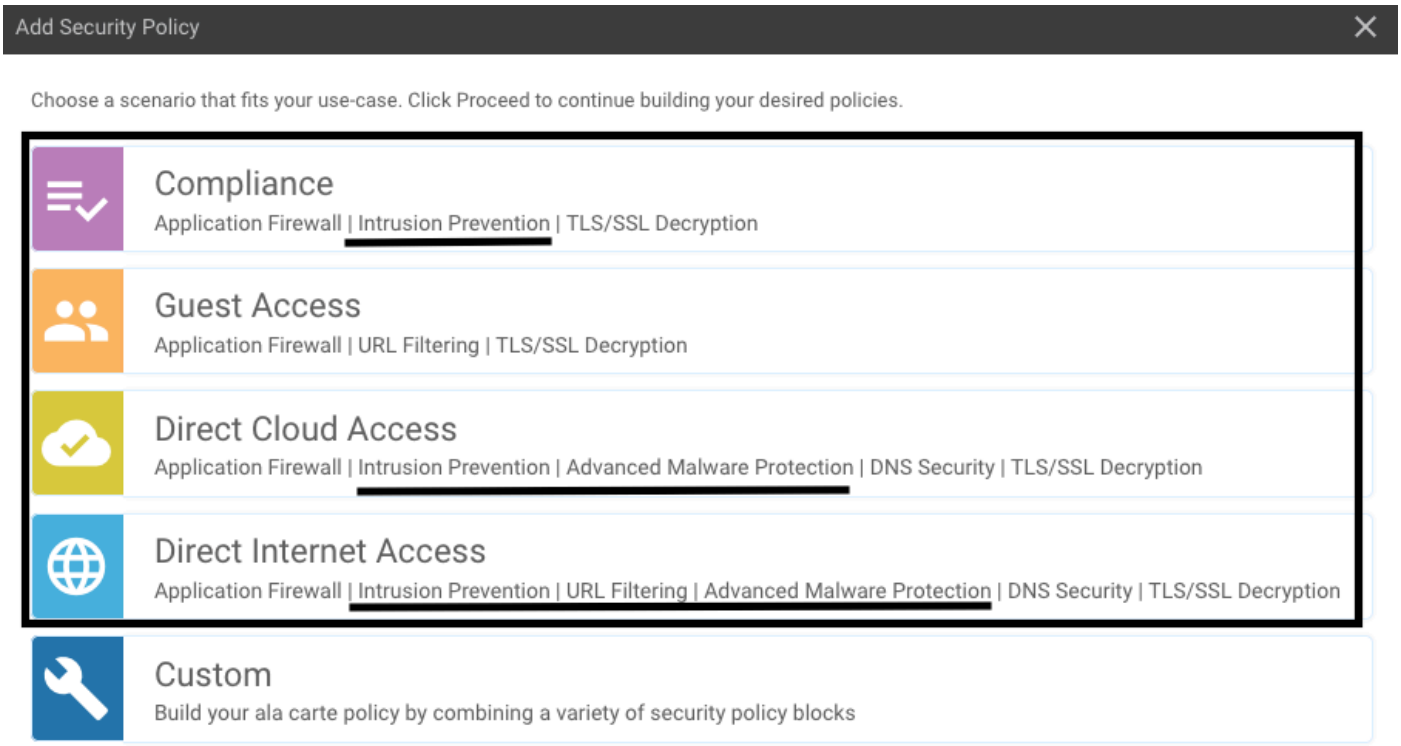
虚拟映像发送错误：**设备没有容器软件版本**，如果所选的cEdge路由器没有容器配置文件子模板的安全策略。





如果您使用的安全策略包括需要UTD软件包的安全功能，例如入侵防御系统(IPS)、入侵检测系统(IDS)、URL过滤(URL-F)和高级恶意软件防护(AMP)，则系统会自动添加此模板。并非所有可用的

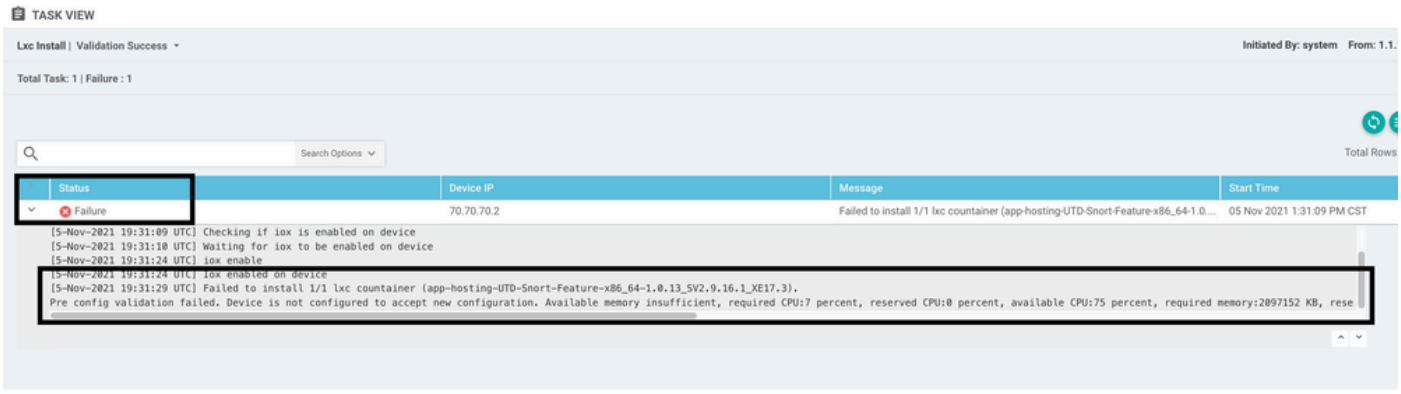
安全功能都需要UTD引擎，例如简单ZBFW功能。



使用容器配置文件子模板推送模板后，vmanage将自动安装虚拟映像。

问题2.可用内存不足

确保cEdge路由器具有8 GB DRAM内存，否则，Lxc Install进程发送**Device is not configured to accept new configuration。可用内存不足**错误。使用UTD功能的cEdge路由器的要求是至少有8 GB的DRAM。



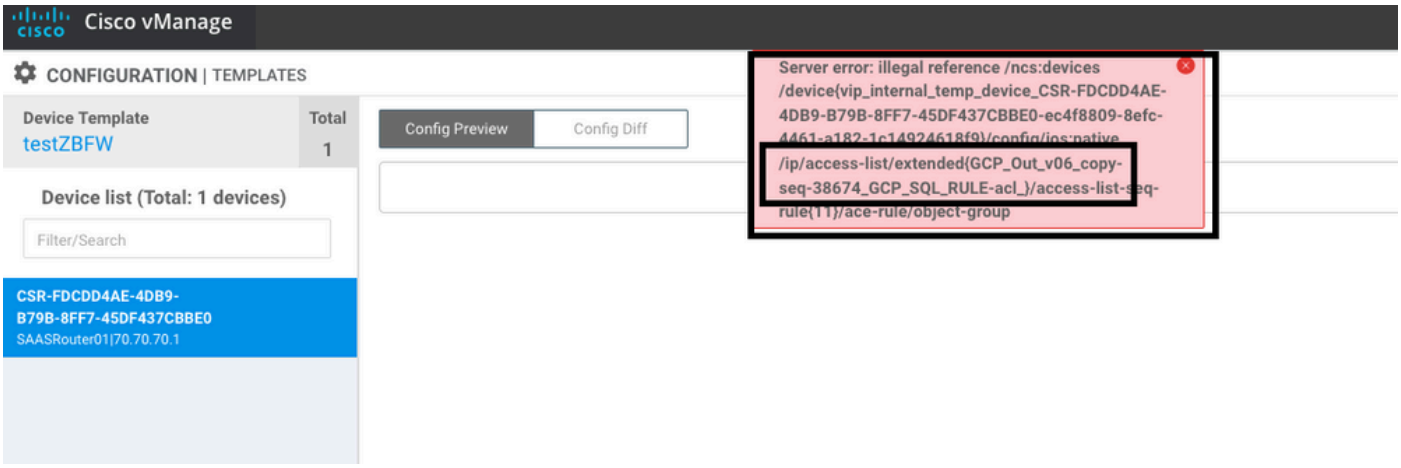
在本例中，CSRv只有4 GB的DRAM。将内存升级到8GB DRAM后，安装成功。

使用**show sdwan system status**输出验证当前的总内存：

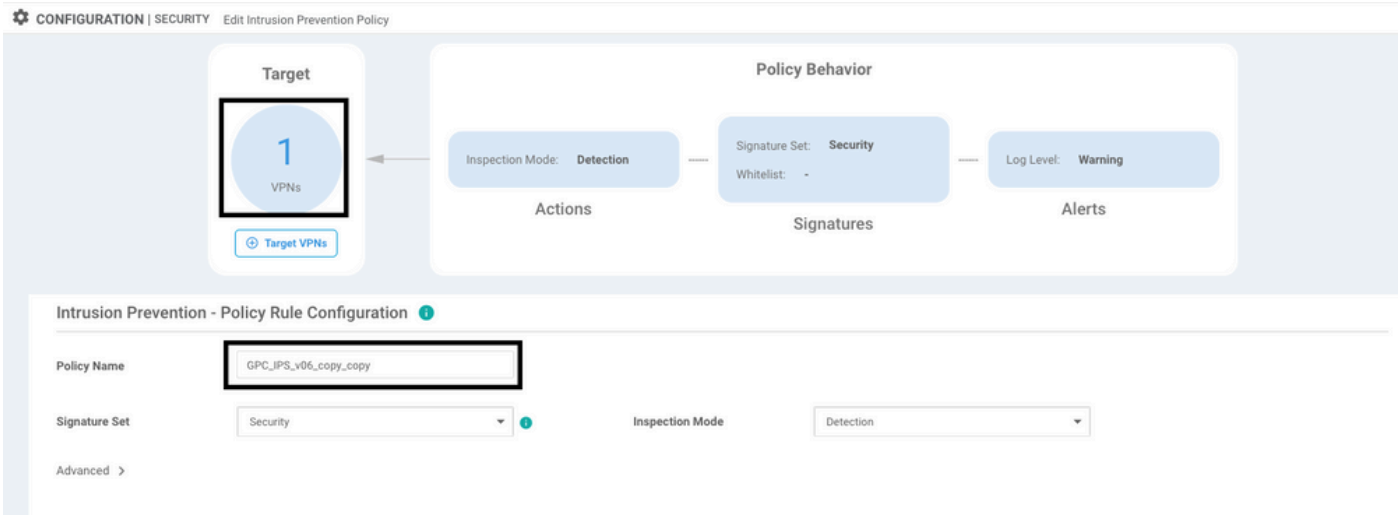
```
Router01# show sdwan system status

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

问题3.非法引用

确保在cEdge路由器中已经配置了用于任何安全策略功能的VPN/VRF，以避免安全策略序列的非法引用。



在本示例中，安全策略具有适用于VPN/VRF 1的入侵防御策略，但设备未配置任何VRF 1。因此，vmanage会为该策略序列发送非法引用。



配置安全策略上提到的VRF后，不会出现Illegal引用，并成功推送模板。

问题4. UTD已安装并已激活，但未启用

设备已配置安全策略，UTD已安装并处于活动状态，但未启用。

此问题与问题3相关，但vManage允许配置引用未在设备中配置的VRF，并且策略未应用于任何VRF。

要确定路由器是否遇到此问题，您需要看到UTD处于活动状态。UTD未启用消息，并且策略未引用任何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
```

对于解决方案，请验证目标VPN并确保将策略应用于配置的VRF。

相关信息

- 路由器安全：路由器上的Snort IPS
- Cisco SD-WAN安全配置指南，Cisco IOS XE版本
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。