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

<u>概要</u>

<u>前提条件</u>

<u>要件</u>

<u>使用するコンポーネント</u>

<u>背景説明</u>

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

<u>Cisco IOS XEソフトウェア(17.x)が稼働するルータ</u>

<u>設定</u>

<u>ステップ1:仮想イメージのアップロード</u>

<u>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</u> <u>ートに追加する</u>

<u>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</u> <u>添付する</u>

<u>確認</u>

<u>一般的な問題</u>

<u>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</u>

<u>問題2:使用可能なメモリが不十分</u>

<u>問題3.不正参照</u>

<u>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</u> 関連情報

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。

Downloads Home / Routers / Software-Defined WAN (SD-WAN)		
Cisco Interfaces and Modules	Cloud Connectors	Meraki vMX
Cloud and Systems Management	Cloud Edge	SD-WAN
Collaboration Endpoints	Data Center Interconnect Platforms	XE SD-WAN Routers
Conferencing	Industrial Routers and Gateways	vEdge Router
Connected Safety and Security	Mobile Internet Routers	
Contact Center	Network Functions Virtualization	
Data Center Analytics	Service Provider Core Routers	
Hyperconverged Infrastructure	Service Provider Edge Routers	
IOS and NX-OS Software	Service Provider Infrastructure Software	
Optical Networking	Small Business Routers	
Routers	Software-Defined WAN (SD-WAN)	

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。

Downloads Home / Routers / Software-Defined WAN (SD-WAN) / XE	SD-WAN Routers	
Cisco Interfaces and Modules	Meraki vMX	ASR 1000 Series IOS XE SD-WAN
Cloud and Systems Management	SD-WAN	CSR 1000V Series IOS XE SD-WAN
Collaboration Endpoints	XE SD-WAN Routers	ISR 1000 Series IOS XE SD-WAN
Conferencing	vEdge Router	ISR 4000 Series IOS XE SD-WAN
Connected Safety and Security		
Contact Center		
Data Center Analytics		
Hyperconverged Infrastructure		
IOS and NX-OS Software		
Optical Networking		
Routers		

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。

Downloads Home / Routers / Software-De	fined WAN	I (SD-WAN) / XE SD-WAN Routers / ISR 4000 Series IOS XE SD-WAN / I	OS XE SD-WAN Software- 16.	12.5(MD)	
Q Search Expand All Collapse All Suggested Release 15.12 5(UD)	~	ISR 4000 Series IOS XE SD-WA Release 16.12.5 MD My Notifications	N Related Links an Release Notes for 19.2 Release Notes for 16.1	d Documentation .4 2.5	
Latest Release	~	File Information	Release Date	Size	
16.12.5(MD) 😒 All Release	~	Cisco ISR 4200 Series IOS XE SD-WAN Software isr4200-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	482.84 MB	±₩∎
16 Deferred Release	> ~	Cisco ISR 4300 Series IOS XE SD-WAN Software isr4300-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	557.83 MB	±₩∎
16	>	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	±₩∎

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。

Software Download

Downloads Home / Routers / Bran	ch Routers / 4000 Series Integrated Services Routers / 4221 Integrated Services Router
Downloads Home Select a Software Type	
IOS XE In-Service Software Upg	rade (ISSU) Matrix
IOS XE Patch Upgrades	
IOS XE ROMMON Software	
IOS XE SD-WAN Software	
IOS XE Software	
UTD Snort IPS Engine Software	
UID Snort Subscriber Signature	Package
Very High Bitrate (VDSL) PHY Fir	mware mware

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。

Software Download

Downloads Home / Routers / Branch Route	rs / 400	0 Series Integrated Services Routers / 4221 Integrated Services Router / UTD S	nort IPS Engine Software-	- 17.7.1a
Q Search Expand All Collapse All Latest Release	~	4221 Integrated Services Router Release 17.7.1a My Notifications	Related Links an	d Documentation
17.7.1a				
16.6.7a		UTD Engine OVA for 17.7.1 release	30-Nov-2021	147.72 MB
All Release	\sim	Advisories 🗗		
16.6 17	> >	UTD Engine for IOS XE secapp-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.tar Advisories	30-Nov-2021	52.51 MB
16	>			

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。

	E SOFTWARE REPOSITO	DRY
Software Images	Virtual Images	
	al Image 👻 🛨 Add C	Custom VNF Package
vManage Remote Server	- vManage	Search Options 🗸
Software Version	Software Locatio	on Network Function Type
Cisco VManage MAINTENANCE SOFTWARE REPOSITORY Software Images Virtual Images Upload Virtual Image Outpload Virtual Image Add Custom Software Version Software Location 2.2.1 vmanage	VNF Package Search Options Upload Virtual Image to vManage O not refresh the Web Browser or click Web Browser Back button File Uploading (Total:1) secapp-utd.17.04.01b.10.9_SV2.9.16.1_XE17.4.x86_64.tar Please wait. Server is Processing	admin Image is being uploaded

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。

MAINTENANCE SOFTWARE REPOSITORY			Virtual image uploaded successfully	8
Software Images Virtual Images				
Opload Virtual Image → Opload Virtual Image → Opload Virtual Image → Opload Custom VNF	Package			
Q	Search Options 🗸			

cisco Cisco vManag	e						▲ ¹	# 0 📫	iaestrad 👻
MAINTENANCE SO	FTWARE REPOSITORY								
Software Images Vi	tual Images								
 Upload Virtual Imag Q. 	e 👻 🗢 Add Custom VN	F Package Search Options V							Co Co 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	Lice	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.16	05 Nov 2021 2:3	9:19 PM •••
1.0.13_SV2.9.16.1_XE17	3 vmanage	App-Hosting	Lixe	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	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.12	05 Nov 2021 3:5	1:20 PM ***
1.0.12_SV2.9.13.0_XE16	vmanage	App-Hosting	Lic	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aarch64_1.0.12.	24 Jul 2020 10:5	0:24 AM ***
1.0.12_SV2.9.13.0_XE16	vmanage	App-Hosting	Lic	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.12	24 Jul 2020 10:5	0:17 AM •••
1.0.10_SV2.9.13.0_XE17	3 vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.10	16 Jan 2021 9:4	0:36 PM ***
1.0.10_SV2.9.13.0_XE16	vmanage	App-Hosting	Lxc	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	Lice	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aarch64_1.0.10.	06 Feb 2020 9:3	9:51 AM •••

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。

Security Policy	installpartition	•
Container Profile *	Factory Default UTD Template	•

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。



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。

Push Feature Template Configuration 🖉 Validation Success 👻							
Total Task: 1 Done - Scheduled : 1							
Q Search Options ~							
> 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	

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。

Ê TA	SK VIEW			
Lxc In	stall Validation Success *			Initiated By: system From: 1.1.1.9
Total	Task: 1 Success : 1			
0				
Q	search uptions *			Total Hows. 1
- X	Status		Message	Start Time
~	Success	70.70.70.1	Done - Lxc Install	05 Nov 2021 12:06:03 PM CST
	15-Nov-2021 18:06:03 UTC] Total number of Container app [5-Nov-2021 18:06:03 UTC] Started 1/1 ixc countainer (5-Nov-2021 18:06:03 UTC] Checking if iox is enabled on [5-Nov-2021 18:06:04 UTC] Checking control on order	rs to be installed: 1. Container apps to be instal pp-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9. a device	<pre>lled are following: [app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE 16.1_XE17.3) installation</pre>	:17.3]
	[5-Nov-2021 18:06:09 UTC Container app image: app-hoss [5-Nov-2021 18:06:20 UTC Connection Instance: 4, Colo [5-Nov-2021 18:06:20 UTC Downloading http://l.ll.9:8/	<pre>ing_UTD-Snort-Feature-x86_64_1.0.13_SV2.9.16.1_XE : biz-internet 880/software/package/lxc/app-hosting_UTD-Snort-Fea</pre>	17.3_secapp-utd.17.03.03.1.0.13_SV2.9.16.1_KE17.3.x86_64.tar ture-x86_64_1.0.13_SV2.9.16.1_XE17.3_secapp-utd.17.03.03.1.0.13_SV2.9.16.1_XE	17.3.x86_64.tar?deviceId=70.70.70.1

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。

CONFIGURATION DEVICES								
WAN Edge List Controllers Unclaimed WAN Edges								
(1) Change Mode 🔹 🛨 Upload WAN Edge List 🔯 Export Bootstrap Configuration 🖾 Sync Smart Account								
Q 70.70.70.1 × Search Options V								
Enterprise Cert Expiration Date	Subject SUDI serial #	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Validity
NA	A NA		70.70.70.1	70	vManage	testZBFW	In Sync	valid

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		
Туре	:	LXC
Name	:	UTD-Snort-Feature
Version	:	1.0.12_SV2.9.16.1_XE17.4
Description	:	Unified Threat Defense
Path	:	<pre>/bootflash/.UTD_IMAGES/iox-utd_1.0.12_SV2.9.16.1_XE17.4.tar</pre>
URL Path	:	
Activated profile name	:	cloud-low

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	7 utd engi	ne standard	status	
Engine version	ı :	1.0.6_SV2.9.	13.0_XE17.2	2
Profile	:	Cloud-Low		
System memory	:			
	Usage :	20.10 %		
	Status :	Green		
Number of engi	nes :	1		
Engine	Running	Health	Reason	
Engine(#1):	Yes	Green	None	·····
Overall system	n status:	Green <<<		

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 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。

Ô.	🖆 MAINTENANCE SOFTWARE UPGRADE											
WA	N Edge Con	troller vMa	anage									
18	ows Selected	⊙ Upgrade	⊙ Upgrade V	irtual Image 💿 Activa	te Virtual In	nage 📑 Delete Vir	rtual Image _ ලු	Activate 📑 Del	ete Available Software	🛷 Set Default V	ersion	000
Dev	ice Group	•	Q 70.70.70.1	×		Search Options 🗸						Total Rows: 1 of 24
	Hostname						Reachability↑			Default Version		Up Since
	SAASRo	u 70.70.70.1	CSR-F	DCDD4AE-4DB9-B79B-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 Im Following devi Click 'Skip Devis • (SAASR	nage ces do not ha ces' to contínu outer01)	we container software ie activate image.	e services.		Skip Devices	X		

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。

Additional Templates		
AppQoE	Choose	▼
Global Template *	Factory_Default_Global_CISCO_Template	• 0
Cisco Banner	Choose	•
Cisco SNMP	Choose	•
CLI Add-On Template	Choose	•
Policy	Choose	•
Probes	Choose	•
Security Policy	CHI_Security_Policy_2	•
County Policy		
Please check the S are aligned. This is	oftware Download page to ensure your device container versions are up-to-date w an informative message and no action may be required	with the device version if applicable. It is always recommended that these
Container Profile *	Factory_Default_UTD_Template	

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。

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
3	Custom Build your ala carte policy by combining a variety of security policy blocks

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。

İ ТА	SK VIEW				
Lxc In	stall Validation Success ~				Initiated By: system From: 1.1.
Total	ask: 1 Failure : 1				
					00
Q		Search Options V			Total Rows
. 2	Status			Message	Start Time
~	S Failure		70.70.70.2	Failed to install 1/1 bxc countainer (app-hosting-UTD-Snort-Feature-x86_64-1.0	05 Nov 2021 1:31:09 PM CST
	<pre>[5-Nov-2021 19:31:09 UTC] Checking if iox [5-Nov-2021 19:31:10 UTC] Waiting for iox [5-Nov-2021 19:31:24 UTC] iox enable [5-Nov-2021 19:31:24 UTC] iox enabled on</pre>	<pre>c is enabled on device c to be enabled on device device</pre>			
	[5-Nov-2021 19:31:29 UTC] Failed to insta Pre config validation failed. Device is n	all 1/1 lxc countainer (ap not configured to accept n	p-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3). ew configuration. Available memory insufficient, required CPU:7 pe	rcent, reserved CPU:0 percent, available CPU:75 percent, required	nemory:2097152 KB, rese
					* *

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。

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。

cisco vManage								
	S		Server error: illegal reference /ncs:devices					
Device Template testZBFW	Total 1	Config Preview Config Diff	4DB9-B79B-8FF7-45DF437CBBE0-ec4f8809-8efc- 4461-a182-1r14924618f9)/config/ins-native /ip/access-list/extended(GCP_Out_v06_copy-					
Device list (Total: 1 devices) Filter/Search			seq-38674_GCP_SQL_RULE-acl_)/access-list-seq- rule(11)/ace-rule/object-group					
CSR-FDCDD4AE-4DB9- B79B-8FF7-45DF437CBBE0 SAASRouter01 70.70.70.1								

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。

NFIGURATION SECURITY Edit Intrusion Prevention Policy			
Target		Policy Behavior	
	Inspection Mode: Detection	Signature Set: Security Whitelist: -	Log Level: Warning
Target VPNs	Actions	Signatures	Alerts
Intrusion Prevention - Policy Rule Configuration 🚯			
Policy Name GPC_JPS_v06_copy_copy			
Signature Set Security	▼ Inspection Mod	de Detection	
Advanced >			

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 sta	cus				
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	/PNを確認し、設定したVRFにポリシ	ーが適用されている			
ここで唯認しまり。					

関連情報

- <u>ルータセキュリティ:ルータ上のSnort IPS</u>
- <u>Cisco SD-WANセキュリティ設定ガイド、Cisco IOS XEリリース</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

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。