Configuración de la trampa SNMPv3 en el router Cisco CEdge

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Configuraciones Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe la configuración para habilitar las trampas de SNMP (del inglés Simple Network Management Protocol, protocolo simple de administración de red) versión 3 mediante una plantilla de función vManage en un router de extremo c.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Solución Cisco SDWAN
- Comprensión básica de SNMP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router Cisco Cloud Services Router 1000V (CSR1000v) que ejecuta 16.12.3
- vManage versión que ejecuta 19.2.2.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Nota: Los extremos en general no necesitan grupos de trampa. En las versiones 20.x y posteriores de vManage, las plantillas de cEdge y vEdge son independientes, la dependencia de tener un grupo de trampa ya no está presente.

Configurar

Configuraciones

En vManage:

Paso 1. Para crear una plantilla de función SNMP, navegue hasta **CONFIGURATION > TEMPLATES > Feature Template > SNMP**.

Introduzca un nombre de plantilla y una descripción seguidos de SNMP no-shutdown, como se muestra en esta imagen.

cisco vManage	
	ES
Device Feature	
Feature Template > SNMP	
Template Name	CSR1000v-SNMP
Description	CSR1000v-SNMP
SNMP SNMP Vers	ion
ONIMD	
SNMP	
Shutdown	⊕ - Ves O No

Paso 2. Seleccione la versión SNMP. En este caso - versión 3.



Paso 3. Cree el grupo de trampa SNMP y rellene los módulos de trampa, como se muestra en esta imagen.

TRAP GROUP TRAP TARGET SE	RVER Update Trap Group		×
Trap Group Name SNMP-TRAP-GRP_VMANAGE	Trap Type Modules	1 Trap Type Modules	Cancel
VIEW & GROUP		Save Changes	
Trap Type Modules			×
Module Name		Severity Levels	
⊕ ▼ all	~	⊕	
		Save Changes	Cancel

Paso 4. Cree un servidor de destino de trampa SNMP.

Aquí se utiliza el reenvío de routing virtual (VRF) de mgmt-intf para obtener capturas SNMP.

interface GigabitEthernet1 vrf address dhcp negotiation auto a	forwarding Mgmt-intf ip dhcp arp timeout 1200 no mop enabl	client default-router distance 1 ip ed no mop sysid end
Update Trap Target		×
VPN ID	⊕ ▼ 512	Mark as Optional Row (i)
IP Address	⊕ - 10.48.35.219]
UDP Port	⊕ - 161	
Trap Group Name	⊕ ▼ SNMP-TRAP-GRP_VMANAGE ▼	
User Name	⊕	
Source Interface	⊕ - GigabitEthernet1	
		Save Changes Cancel

Paso 5. Cree la vista SNMP y agregue el identificador de objetos SNMP (OID).

	Object Identifiers		×
VIEW & GROUP	Object Identifier	Exclude OID	
VIEW GROUP	⊕ - 1.3.6.1.4.1	⊕ - ○ 0n ● 0ff	•
New View			1
Name	Add Object Identifer		
SNMP-VIEW_VMANAGE			
		Sav	e Changes Cancel

Paso 6. Cree el grupo SNMP y adjunte a él la vista SNMP creada previamente.

VIEW & GROUP	Update Group				×
VIEW GROUP	Name	۲	SNMP-GRP-VMANAGE		
New Group	Security Level	۲	AuthPriv		
Group Name OSNMP-GRP-VMANAGE	View	•	SNMP-VIEW_VMANAGE		
				Save Changes	Cancel

Paso 7. Agregue el usuario SNMPv3, como se muestra en esta imagen.

SNMP SNMP Version	Update User				×	
Group Name SNMP-GRP-VMANAGE	User	۲	SNMP_V3_USER_VMANAGE			
	Authentication Protocol	•	SHA			
	Authentication Password	•				
USER	Privacy Protocol	•	AES-CFB-128			
New User	Privacy Password	•				
Username Auth	Group	•	SNMP-GRP-VMANAGE			
				Save Chang	es Cancel	

Paso 8. Adjunte la plantilla de función SNMP en la sección plantilla adicional de la plantilla de dispositivo:

;		
ansport & Management VPN	Service VPN	Additional Templates
		†
Choose	•	
Choose	•	
Chaoca		
010036	•	
Choose	•	
Choose	•	
CSR1000v-SNMP	•	
test-1-sec	•	
	ansport & Management VPN Choose Choose Choose Choose Choose Choose Choose Choose test-1-sec	Ansport & Management VPN Service VPN Choose Choose Choose Choose Choose Choose Choose Choose

Paso 9. Conecte la plantilla de dispositivo al dispositivo correspondiente.

Verificación

En cEdge:

Habilitar estos debugs:

debug snmp packets debug snmp detail Generar trampa SNMP: **test snmp trap config**

cEdge#test snmp trap config Generating CONFIG-MAN-MIB Trap cEdge# Aug 19 14:26:03.124: SNMP: Queuing packet to 10.48.35.219 Aug 19 14:26:03.124: SNMP: V2 Trap, reqid 5563, errstat 0, erridx 0 sysUpTime.0 = 233535801 snmpTrapOID.0 = ciscoConfigManEvent ccmHistoryEventCommandSource.2 = 1 ccmHistoryEventConfigSource.2 = 2 ccmHistoryEventConfigDestination.2 = 2 ccmHistoryEventTerminalUser.2 = test Aug 19 14:26:03.374: SNMP: Packet sent via UDP to 10.48.35.219

Aquí se observa que la trampa SNMP se envía al servidor 10.48.35.219.

Captura de paquete:

<pre>k k k k k k k k k k k k k k k k k k k</pre>	2 2020-08-18 12:58:22.830950	10.48.62.184	10.48.35.219	SNMP	306 encryptedPDU: privKey Unknown
<pre>> Frame 2: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) > Ethernet II, Src: VMware_8d:61:ce (00:50:56:8d:61:ce), Dst: Cisco_5b:a6:1d (cc:7f:76:5b:a6:1d) > Internet Protocol Version 4, Src: 10.48.62.184, Dst: 10.48.35.219 > User Datagram Protocol, Src Port: 49444, Dst Port: 161 </pre> / Simple Network Management Protocol msgVersion: snmpv3 (3) > msgGlobalData > msgAuthoritativeEngineID: 766d616e6167652d0a151515 msgAuthoritativeEngineTime: 4490 msgUserName: SNMP_V3_USER_VMANAGE msgAuthoritatioteIngaremeters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)					
<pre>> Ethernet II, Src: VMware_8d:61:ce (00:50:56:8d:61:ce), Dst: Cisco_5b:a6:1d (cc:7f:76:5b:a6:1d) > Internet Protocol Version 4, Src: 10.48.62.184, Dst: 10.48.35.219 > User Datagram Protocol, Src Port: 49444, Dst Port: 161 </pre> <pre>> Simple Network Management Protocol msgVersion: snmpv3 (3) > msgGlobalData > msgAuthoritativeEngineID: 766d616e6167652d0a151515 msgAuthoritativeEngineTime: 4490 msgUserName: SNMP_V3_USER_VMANAGE msgAuthoritationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)</pre>	Frame 2: 306 bytes on wire (2448 b	its), 306 bytes cap	tured (2448 bits)		
Internet Protocol Version 4, Src: 10.48.62.184, Dst: 10.48.35.219 User Datagram Protocol, Src Port: 49444, Dst Port: 161 Simple Network Management Protocol msgUersion: snmpv3 (3) > msgGlobalData > msgAuthoritativeEngineID: 766d616e6167652d0a151515 msgAuthoritativeEngineBoots: 1 msgAuthoritativeEngineTime: 4490 msgUserName: SNMP_V3_USER_VMANAGE msgAuthenticationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)	Ethernet II, Src: VMware_8d:61:ce	(00:50:56:8d:61:ce)	, Dst: Cisco_5b:a6:1d	(cc:7f:76:5b:a6	::1d)
> User Datagram Protocol, Src Port: 49444, Dst Port: 161 > Simple Network Management Protocol msgVersion: snmpv3 (3) > msgGlobalData > msgAuthoritativeEngineID: 766d616e6167652d0a151515 msgAuthoritativeEngineBoots: 1 msgAuthoritativeEngineTime: 4490 msgUserName: SNMP_V3_USER_VMANAGE msgAuthenticationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 msgData: encryptedPDU (1)	Internet Protocol Version 4, Src: :	10.48.62.184, Dst:	10.48.35.219		
Simple Network Management Protocol msgVersion: snmpv3 (3) msgGlobalData msgAuthoritativeEngineID: 766d616e6167652d0a151515 msgAuthoritativeEngineBoots: 1 msgAuthoritativeEngineTime: 4490 msgUserName: SNMP_V3_USER_VMANAGE msgAuthenticationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 msgData: encryptedPDU (1)	User Datagram Protocol, Src Port:	49444, Dst Port: 16	1		
<pre>msgVersion: snmpv3 (3) > msgGlobalData > msgAuthoritativeEngineID: 766d616e6167652d0a151515 msgAuthoritativeEngineBoots: 1 msgAuthoritativeEngineTime: 4490 msgUserName: SNMP_V3_USER_VMANAGE msgAuthenticationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)</pre>	 Simple Network Management Protocol 				
<pre>> msgGlobalData > msgAuthoritativeEngineID: 766d616e6167652d0a151515 msgAuthoritativeEngineBoots: 1 msgAuthoritativeEngineTime: 4490 msgUserName: SNMP_V3_USER_VMANAGE msgAuthenticationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)</pre>	msgVersion: snmpv3 (3)				
<pre>> msgAuthoritativeEngineID: 766d616e6167652d0a151515 msgAuthoritativeEngineBoots: 1 msgAuthoritativeEngineTime: 4490 msgUserName: SNMP_V3_USER_VMANAGE msgAuthenticationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)</pre>	<pre>> msgGlobalData</pre>				
<pre>msgAuthoritativeEngineBoots: 1 msgAuthoritativeEngineTime: 4490 msgUserName: SNMP_V3_USER_VMANAGE msgAuthenticationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)</pre>	> msgAuthoritativeEngineID: 766d61	l6e6167652d0a151515			
<pre>msgAuthoritativeEngineTime: 4490 msgUserName: SNMP_V3_USER_VMANAGE msgAuthenticationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)</pre>	msgAuthoritativeEngineBoots: 1				
<pre>msgUserName: SNMP_V3_USER_VMANAGE msgAuthenticationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)</pre>	msgAuthoritativeEngineTime: 4490	3			
<pre>msgAuthenticationParameters: ecb71af6d4616f7944426464 msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)</pre>	msgUserName: SNMP_V3_USER_VMANAG	ŝΕ			
msgPrivacyParameters: d2c8f7ee670781e2 > msgData: encryptedPDU (1)	msgAuthenticationParameters: ect	71af6d4616f7944426	464		
> msgData: encryptedPDU (1)	msgPrivacyParameters: d2c8f7ee67	/0781e2			
	> msgData: encryptedPDU (1)				

A veces, puede notar "CheckMIBView: OID no en la vista MIB." error en las depuraciones.

Verifique la configuración de la vista SNMP anterior y añada OID (por ejemplo: 1.3.6.1.4.1).

Troubleshoot

debug snmp detail debug snmp packets cEdge#test snmp trap config Generating CONFIG-MAN-MIB Trap SPOKE-8#CheckMIBView: OID is in MIB view. CheckMIBView: OID is in MIB view. SrCheckNotificationFilter: OID is included. Aug 19 14:30:16.527: SNMP: Queuing packet to 10.48.35.219Sr_send_trap: trap sent to 10.48.35.219:161:Mgmt-intf Aug 19 14:30:16.527: SNMP: V2 Trap, reqid 5564, errstat 0, erridx 0 sysUpTime.0 = 233561141 snmpTrapOID.0 = ciscoConfigManEvent ccmHistoryEventCommandSource.2 = 1 ccmHistoryEventConfigSource.2 = 2 ccmHistoryEventConfigDestination.2 = 2 ccmHistoryEventTerminalUser.2 = test SrV2GenerateNotification:Function has reached clean up routine. Aug 19 14:30:16.777: SNMP: Packet sent via UDP to 10.48.35.219 cEdge#sh snmp | i sent Logging to 10.48.35.219.161, 0/10, 3316 sent, 2039 dropped. cEdge#sh snmp user User name: SNMP_V3_USER_VMANAGE Engine ID: 766D616E6167652D0A151515 storage-type: nonvolatile active Authentication Protocol: SHA Privacy Protocol: AES128 Group-name: SNMP-GRP-VMANAGE cEdge#show snmp group groupname: ILMI security model:v1 contextname:

Información Relacionada

- Ejemplo de Configuración de Captura de Paquetes Incrustada para Cisco IOS e IOS-XE
- Usar trampas SNMP
- Navegador de objeto SNMP
- Soporte Técnico y Documentación Cisco Systems