Extraia a ACL do CSM no formato CSV através do método API

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Diagrama de Rede Instalação/verificação de licença de API CSM Configuration Steps Trabalhar com API CSM Método de login Obter regras de ACL Verificar Troubleshoot

Introduction

Este documento descreve como extrair a ACL (Access Control Lists, listas de controle de acesso), no formato CSV (Comma-Separated Values, valores separados por vírgula), de um dispositivo gerenciado pelo Cisco Security Manager (CSM) através do método de API do CSM.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Security Manager (CSM)
- API CSM
- conhecimento básico de API

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Servidor CSM
- licença de API CSM Product Name: L-CSMPR-API Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
- ASA (Adapative Security Appliance, dispositivo de segurança adaptável) gerenciado pelo CSM

Um cliente de API. Você pode usar cURL, Python ou Postman. Este artigo demonstra todo o
processo com o Postman. O aplicativo cliente CSM deve ser fechado. Se um aplicativo
cliente CSM estiver aberto, deve ser feito por um usuário diferente daquele que usa o método
API. Caso contrário, a API retorna um erro. Para pré-requisitos adicionais para usar o recurso
API, você pode usar o próximo guia. <u>Pré-requisitos de API</u>

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Security Manager (CSM) tem algumas funcionalidades para a configuração de dispositivos gerenciados que precisam ser implementadas através da API.

Uma dessas opções de configuração é o método para extrair uma lista da ACL (Access Control List, lista de controle de acesso) configurada em cada dispositivo gerenciado pelo CSM. O uso da API do CSM é a única forma de atingir esse requisito até agora.

Para esses fins, o Postman usou como Cliente API e CSM versão 4.19 SP1, ASA 5515 versão 9.8(4).

Diagrama de Rede



CSM GUI Client

Instalação/verificação de licença de API CSM

A API do CSM é um recurso licenciado. Você pode verificar se o CSM tem uma licença de API, no cliente do CSM, navegue para **Ferramentas > Administração do Security Manager > Licenciamento** para confirmar se você já tem uma licença instalada.



۵,

API

- AutoLink
- ACL HitCount Settings
- CCO Settings
- Configuration Archive
- CS-MARS
- CSM Mobile
- Customize Desktop
- Debug Options
- Deployment
- Device Communication
- Device Groups
- Discovery
- Event Management
- Health and Performance Monitor
- Report Manager
- Identity Settings
- Image Manager
- IP Intelligence Settings
- Eventing Notification Settings
- IPS Updates
- ISE Settings

Licensing

- Logs
- Policy Management
- Policy Objects
- Process Monitoring Settings
- Single Sign-on Configuration
- Rule Expiration
- Server Security
- Take Over User Session
- Ticket Management
- Token Management
- VPN Policy Defaults
- Workflow
- Wall Settings

	color becarry manager - r	koministration
nsing		
CSM [95]		
	License Information	
	Edition	Security Manager Professional
	Туре	Permanent
	Number of devices licensed for this Security Manager installation	50
	Number of devices currently covered by license	37
	API Licerse Available	Yes (Expires On 28 Apr 2020, 12:00:00 PDT)
	Instal License	
	Install License License File Installed on	Expire's On
	Install License License File SecurityManager419_Api_0_Lic 29 Jan 2020, 02:11:25 PST	Expire's On 28 Apr 2020, 12:00:00 PDT
	Distal License License File Installed on SecurityManager419_Api_0_1.ic 29 Jan 2020, 02:11:25 PST SecurityManager411_StdToProLippr 31 May 2016, 01:29:21 PDT	Expire's On 28 Apr 2020, 12:00:00 PDT Never
	Install License License File Installed on SecurityManager419_Api_0_1.lic 29 Jan 2020, 02:11:25 PST SecurityManager411_StdTeProLipgr 31 May 2016, 01:29:21 PDT	Expire's On 28 Apr 2020, 12:00:00 POT Never
	Install License License File Installed on SecurityManager419_Api_0_L1c 29 Jan 2020, 02:11:25 PST SecurityManager411_StdToProLipgr 31 May 2016, 01:29:21 PDT	Expire's On 28 Apr 2020, 12:00:00 PDT Never
	Instal License License File 2rstalled on SecurityManager419_Api_0_Lic 29 Jan 2020, 02:11:25 PST SecurityManager411_StdTsProLipgr 31 May 2016, 01:29:21 PDT	Expire's On 28 Apr 2020, 12:00:00 PDT Never
	Distal License License File Sistalled on SecurityManager419_Api_0_1.ic 29 Jan 2020, 02:11:25 PST SecurityManager411_StdTeProUpgr 31 May 2016, 01:29:21 PDT	Expire's On 28 Apr 2020, 12:00:00 PDT Never
	Distal License License File Installed on SecurityManager419_Api_0_1.ic 29 Jan 2020, 02:11:25 PST SecurityManager411_StdToProUpgr 31 May 2016, 01:29:21 PDT	Expire's On 28 Apr 2020, 12:00:00 POT Never Install a License
	Distal License License File Installed on SecurityManager419_Api_0_1.ic 29 Jan 2020, 02:11:25 PST SecurityManager411_StdToProLipgr 31 May 2016, 01:29:21 PDT	Expire's On 28 Apr 2020, 12:00:00 POT Never Statal a License
	Install License License File Installed on SecurityManager419_Api_0_1.ic 29 Jan 2020, 02:11:25 PST SecurityManager411_StdToProLipgr 31 May 2016, 01:29:21 PDT	Expire's On 28 Apr 2020, 12:00:00 POT Never Install a License
	Install License License File Installed on SecurityManager419_Api_0_1.ic 29 Jan 2020, 02:11:23 PST BecurityManager411_StdToProLipgr 31 May 2016, 01:29:21 POT Note: Please refer to "Device Count" in the Licensing	Expire's On 28 Apr 2020, 12:00:00 PDT Never Install a License

Se não houver licença de API aplicada, mas você já tiver o arquivo .lic que pode instalar sua licença, clique no botão **Instalar uma licença**, você deve armazenar o arquivo de licença no mesmo disco onde o servidor CSM está localizado.

Para instalar uma licença mais recente do Cisco Security Manager, siga estas etapas:

Etapa 1. Salve o arquivo de licença anexado (.lic) do e-mail que você recebeu no sistema de arquivos.

Etapa 2. Copie o arquivo de licença salvo para um local conhecido no sistema de arquivos do servidor do Cisco Security Manager.

Etapa 3. Inicie o Cisco Security Manager Client.

Etapa 4. Navegue até Ferramentas->Administração do Gerenciador de Segurança...

Etapa 5. Na janela Cisco Security Manager - Administration, selecione Licensing

Etapa 6. Clique no botão Instalar uma licença.

Passo 7. Na caixa de diálogo Instalar licença, selecione o botão Procurar.

Etapa 8. Navegue até o arquivo de licença salvo no sistema de arquivos do servidor do Cisco Security Manager e selecione o botão **OK**.

Etapa 9. Na caixa de diálogo Instalar licença, clique no botão OK.

Etapa 10. Confirme as informações de Resumo da licença exibidas e clique no botão Fechar.

License Information	
Edition	Security Manager Professional
Type	Permanent
Number of devices licensed for this Security Manager installation	200
Number of devices currently covered by license	10
API License Available	No
Ucense File License File CK	Browse Cancel Help
SecurityManager413_Pro_50_1.lc 26 Jun 2017, 03:24:26 PDT	Never

19 9 - 19		Choose The License File		
)III • 🎽 CSM			♥] Q,+ Search CSH	
Pro	gram Files	Name	Date modified	Size
4 🎍 Pro	gram Piles (x86)	🔮 CSM20200 1290 70926764.lc	29/01/2020 7:09 AM	10
	Common Files	SecurityManager413_Addon_100_1.lc	12/06/2020 4:30 AM	18
1 1	CSCOpx	SecurityManager413_Addon_50_1.1c	12/06/2020 4:30 AM	19
	cam-repository cpi-bin collect conf databases dbupdete etc copyright icenses	×		
File selected:*	C5M20200129070	926764.Ac		
	\\WIN-A73U18QC/	172\C:\Program Files (x86)\CSCOpx\etc\loenses	ýCSM	
Path:				

License Information	
Editon	Security Manager Professional
Туре	Permanent
Number of devices licensed for this Security Manager installation	200
Number of devices currently covered by license	10
API License Available	No
Install Licen License File: enses\CSM\CSM2020012907092676	4.lc Browse
License File SecurityMan	Cancel Help
SecurityManager413_Pro_50_1.lc 26 Jun 2017, 03:24:26 PDT	Never

A licença da API só pode ser aplicada em um servidor licenciado para a edição profissional do CSM. A licença não pode ser aplicada ao CSM que executa uma edição padrão da licença. Requisitos de licença de API

Configuration Steps

Configurações do cliente API

Se você usa o Postman, há algumas configurações que você precisa configurar, depende de cada cliente de API, mas deve ser semelhante.

Proxy desabilitado

• Verificação SSL - DESLIGADO

Configurações do CSM

 API ativada. Em Ferramentas > Administração do Security Manager > API Configurações de API

5		lisco Security Manager - Administration	_ _ X
-• M	491		
- • Autourk			
ACL HitCount Settings	421		
- CCO Settings	Finable API Service		
Configuration Archive			
- • CS-MARS	Result Set Page Size:* 500		
- CSM Mobile	tation doub exercises 2		
Oustomize Desktop	Active cient sessions:* 5		
Debug Options	Request Payload Max Size (M8):* 2		
Deployment			
Device Communication			
Device Groups		Save	Reset Restore Defaults
Discovery			
Event Management			
Pearth and Performance Monitor			
Report Manager			
Joenory Seconds			
D Intelligence Fallinge			
Functional Mathematical Sections			
Eliptates			
e ISE Settors			
- e Licensing			
@ Loos			
Policy Management			
Policy Objects			
- Process Monitoring Settings			
Single Sign on Configuration			
Rule Expiration			
Server Security			
Take Over User Session			
- Ticket Management			
Token Management			
VPN Policy Defaults			
- Workflow			
Wall Settings			
L			Panel to activate Miedowr
			Close Help

Trabalhar com API CSM

Você precisa configurar no cliente API as duas chamadas abaixo:

- 1. Método de login
- 2. Obter valores de ACL

Para referência através do processo:

Detalhes de acesso CSM usados neste laboratório:

Nome de host CSM (endereço IP): 192.168.66.116. Na API, usamos o nome de host na URL.

Usuário: admin

Senha: Admin123

Método de login

Esse método deve ser chamado antes de qualquer outro método chamado em outros serviços.

Guia de API do CSM: Login do método

Requisição

- 1. Método de HTTP: POST
- 2. URL: https://<hostname>/nbi/login
- 3. Corpo:

Where:

Nome de usuário: O nome de usuário do cliente CSM associado à sessão

Senha: A senha do cliente CSM associada à sessão.

reqld: Este atributo identifica exclusivamente uma solicitação feita pelo cliente, esse valor ecoa pelo servidor CSM na resposta associada. Ele pode ser definido para qualquer coisa que o usuário queira usar como um identificador.

heartbeat solicitado: Esse atributo pode ser opcionalmente definido. Se o atributo estiver definido como verdadeiro, o cliente CSM receberá um retorno de chamada de pulsação do servidor CSM. O servidor tenta fazer ping no cliente com uma frequência próxima a (tempo limite de inatividade) / 2 minutos. Se o cliente não responder ao ritmo cardíaco, a API repetirá o ritmo cardíaco durante o próximo intervalo. Se o heartbeat for bem-sucedido, o tempo limite de inatividade da sessão será redefinido.

callbackUrl: O URL no qual o servidor CSM faz o retorno de chamada. Isso precisa ser especificado se o heartbeatRequested é verdadeiro. Somente URLs de retorno de chamada baseados em HTTPS são permitidos

> login	📮 Comments o 🛛 Examples o 🔻
POST - https://192.168.66.116/nbi/login 2	Send 🔻 Save 🔻
Params Authorization Headers (9) Body Pre-request Script Tests Settings	Cookies Code
🔍 none 🔍 form-data 🌑 x-www-form-urlencoded 🥥 raw 🔍 binary 🔍 GraphQL XML 💌	
<pre>1 k?xml version="1.0" encoding="UTF-8"?> 2 < csm:loginRequest xmlns:csm="csm"> 3 <protversion>1.0</protversion> 4 <reqid>123</reqid> 5 <username>admin</username> 6 <pre>cpassword>Admin123</pre>/password> 7 <heartbeatrequested>true</heartbeatrequested> 8 <callbackurl>https://192.168.66.116/nbi/login</callbackurl> 9 3 </pre>	

4. Enviar

Selecione a opção bruta para ver como neste exemplo.

Resposta

A API de Logon valida as credenciais do usuário e retorna um token de sessão como um cookie seguro. O valor da sessão é armazenado na chave **asCookie**, você deve salvá-lo **comoCookie**.

POST v https://192.168.30.17/nbi/login	Send 🔻 Save 👻
Params Authorization Headers [10] Body Pre-request Script Tests Settings	
🔍 none 🔍 form-data 🔍 xwww-form-urlencoded 🛛 🌒 raw 🔍 binary 🔍 GraphQL XML *	
1 (Paul version="1.0" encoding="UIF=0">> 2 < <smiloginhecest milissicas"com"=""> 3 <crotion124(roots=)>> 4 <crotion124(roots=) 5 <clotename>admint/secreman></clotename></crotion124(roots=) </crotion124(roots=)></smiloginhecest>	
<pre>6 C-asser@stisol324/asser>> 7 C-artbestRequests>Prued/assttestRequests>> 8 C-allbeckUr:https://192.168.30.17/mbi/loginc/csllbackUr1> 9 (/CssloginRequest></pre>	
Body Cookies (1) Headers (11) Test Results Status: 200 200	
Pretty Raw Preview Visualize XML * 🛱	n 🗈 Q
1 Bysal version="1.0" encoding="UTF-8")B 2 (nslleginResponse zmlas.nsl="can") 3 (protVersion).10(protVersion) 4 (reqld)123(/reqld) 5 (serviceVersion)2 6 (sessionTimeoutInMins>)5(sessionTimeoutInMins>) 7 (/nslloginResponse)	
Activate Wi Go to System in	
ප Bootcamp	Build Browse 🖬 📩 (

Body	Cookies (1) Headers (11)	Test Results	asCookie Valu	Je		
	Name	Value	Domain	Path	HttpOnly	
	asCookie					

Obter regras de ACL

Método execDeviceReadOnlyCLICmds. O conjunto de comandos que podem ser executados por esse método são comandos somente leitura, como estatísticas, comandos de monitoramento que fornecem informações adicionais sobre a operação do dispositivo específico.

Detalhes do método no Guia do usuário da API do CSM

Requisição

- 1. Método de HTTP: POST
- 2. URL: https://hostname/nbi/utilservice/execDeviceReadOnlyCLICmds

3. Cabeçalho HTTP: O cookie retornado pelo método de login que identifica a sessão de autenticação.

Valor de entrada **asCookie** obtido anteriormente do Login do método.

Chave: Digite "asCookie"

Valor: Valor de entrada obtido.

Clique na caixa de seleção para ativá-la.

4. Corpo:

Note: O corpo XML acima pode ser usado para executar qualquer comando "show", por exemplo: "show run all", "show run object", "show run nat" etc.

O elemento XML "<deviceReadOnlyCLICmd>" indica que o comando especificado em "<cmd>" e "<argumento>" DEVE ser somente leitura.

Where:

IP do dispositivo: O endereço IP do dispositivo com o qual o comando deve ser executado.

cmd: Comando fixo "show". O regex permite maiúsculas/minúsculas [sS][hH][oO][wW]

argumento: Os argumentos do comando show. Como "executar" para mostrar a configuração atual do dispositivo ou **"lista de acesso"** para mostrar os detalhes da lista de acesso.

5. Enviar

D		POST login	POST Get ACL	× + •••	No Environment	• • *
	▶ Get ACL				📮 Comments 🛛	Examples 1 🔻
י 	POST 🔻 https://192.1	168.66.116/nbi/utilservice/execDev	viceReadOnlyCLICmds		Send	- Save -
	1 Params Authorization H	eaders (10) Body • Pre-	request Script Tests	Settings	5	Cookies Code
	🔵 none 🔍 form-data 🔍 x	-www-form-urlencoded 🛛 💿 raw	🔵 binary 🛛 🔵 GraphQL	XML 👻		
	<pre>2 < csm:execDeviceReadOn 3 <protversion>1.0</protversion></pre> 4 <reqid>123</reqid> 5 < deviceReadOnlyCLICm 6 <deviceip>192.168.666 7 <ccmd>show 8 <argument>access-lis 9 </argument></ccmd></deviceip>	<pre>llyCLICmdsRequest xmlns:csm otVersion> d> i.1 st ind> inlyCLICmdsRequest></pre>	="csm">	4		

Resposta



Verificar

Você tem a opção Salvar resposta como um arquivo. Navegue até Salvar resposta > Salvar em um arquivo. Em seguida, selecione o local do arquivo e salve-o como um tipo .csv.

Select path to save file	×	Postman		- 0 ×
③ ③ → ↑ ■ Desktop → ✓ Č	Search Desktop 🔎			
Organize • New folder	8 • 8	🖬 My Workspace 👻 🕹 Invite	🧿 🖌 🗜 I	🌲 🤎 🥑 Upgrade 💌
🖈 Favorites 📄 🌄 Shortcut 🚛 Sh	hortcut A		No Environm	ent • 0 🔅
Desktop	recond 10 win k0			
Secent places				
CSMA 19.05ervice, Pack Laee	5M20200129070926764.zip	nfo		Send • Save •
Documents fcs-csm-419-win-k9.zip	ileZilla_3.44.1_win64_sponsored-se up.exe	est Script Tests Settings		
Downloads Downloads Postman Postman	ileZilla FTP Client	binary 🔍 GraphQL XML 💌		
Pictures Shortcut CO	SV File 36 KB			
File name: response.co/	,			
Save as type: All Files (".")	v			
(a) Marketing	Save Cancel			
S Hot Polities	Jine Conto			
Both Costine (I) Header (I)	Tant Baradra			Save Response +
Body Council () Headers ()			Value	Save as example
Date @			Thu, 02 Apr 2020 01:43:47 GMT	Save to a file
Server ()			Apache	
Allow 0				
Content-Length			253	
Keep-Aine			timeout=20, max=10000	
Connection ()			Keep-Alive	
Content-Type			text/html; charset≈iso-8859-1	
			Go to System in Control Panel	
			😌 Bootcamp Build	Browse 🔛 🛅 🤅

Em seguida, você deve ser capaz de abrir esse arquivo .csv com o aplicativo Excel, por exemplo. No tipo de arquivo .csv, você pode salvar a saída como outros tipos de arquivo, como PDF, TXT etc.

Troubleshoot

Possíveis respostas de falha usando API.

1. Nenhuma licença de API instalada.

Causa: Licença de API expirada, não instalada ou não habilitada.

Possível solução: Verifique a data de validade da licença, em **Ferramentas > Administração do** Security Manager > Página de Licenciamento

Verifique se o recurso API está habilitado em Ferramentas > Administração do Security Manager > API

Confirme as configurações da seção Instalação/Verificação de Licenças de API CSM acima deste guia.

2. Uso de endereço IP CSM inválido para o login da API.

Causa: O endereço IP do servidor CSM está incorreto na URL da chamada da API.

Possível solução: Verifique na URL do cliente API se o nome do host é o endereço IP correto do servidor CSM.

URL: https:// <hostname>/nbi/login

3. Endereço IP ASA errado.

Causa: O endereço IP definido no corpo entre as marcas <deviceIP></deviceIP> não deve ser o correto.

Possível solução: Confirme se o endereço IP do dispositivo correto está definido na Sintaxe do corpo.

4. Nenhuma conexão com o firewall.

Causa: O dispositivo não tem conexão com o CSM

Possível solução: Execute um teste de conectividade do servidor CSM e solucione problemas de conectividade adicional com o dispositivo.

Para obter mais códigos de erro e descrição, consulte o Guia de especificação da API do Cisco Security Manager no próximo <u>link.</u>