Extraire la liste de contrôle d'accès de CSM au format CSV via la méthode API

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Diagramme du réseau Installation/vérification de la licence de l'API CSM Configuration Steps Utilisation de l'API CSM Méthode de connexion Obtenir les règles ACL Vérification Dépannage

Introduction

Ce document décrit comment extraire les listes de contrôle d'accès (ACL), au format CSV (Comma-Separated Values), d'un périphérique géré par Cisco Security Manager (CSM) via la méthode API CSM.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Security Manager (CSM)
- API CSM
- Connaissances de base de l'API

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur CSM
- Licence API CSM Product Name: L-CSMPR-API Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
- Dispositif de sécurité adaptatif (ASA) géré par CSM

 Un client API. Vous pouvez utiliser cURL, Python ou Postman. Cet article démontre tout le processus avec Postman. L'application cliente CSM doit être fermée. Si une application cliente CSM est ouverte, doit être effectuée par un utilisateur différent de celui qui utilise la méthode API. Sinon, l'API renvoie une erreur. Pour connaître les conditions préalables supplémentaires à l'utilisation de la fonction API, reportez-vous au guide suivant. <u>Conditions</u> requises pour l'API

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cisco Security Manager (CSM) possède certaines fonctionnalités pour la configuration des périphériques gérés qui doivent être mises en oeuvre via l'API.

L'une de ces options de configuration est la méthode d'extraction d'une liste de la liste de contrôle d'accès (ACL) configurée dans chaque périphérique géré par CSM. L'utilisation de l'API CSM est le seul moyen d'atteindre cette exigence jusqu'à présent.

Àces fins, Postman a utilisé comme client API et CSM version 4.19 SP1, ASA 5515 version 9.8(4).

Diagramme du réseau



CSM GUI Client

Installation/vérification de la licence de l'API CSM

L'API CSM est une fonctionnalité sous licence. Vous pouvez vérifier que le CSM dispose d'une licence API, dans le client CSM, accédez à **Outils > Administration du Gestionnaire de sécurité > Licence** pour confirmer que vous avez déjà installé une licence.



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

	Cisco	o Security Manager - Ad	ministration	
ning				
CSM IPS				
	License Information			
	Edition		Security Manager Professional	
	Туре		Permanent	
	Number of devices licensed for this Se	curity Manager installation	50	
	Number of devices currently covered	by license	37	
	API License Available		Tes (Expires On 28 Apr 2020, 12:00:00 PDT)	
	Install License			
	License File	Installed on	Expire's On	
	SecurityManager419_Api_0_1.lc	29 Jan 2020, 02:11:25 PST	28 Apr 2020, 12:00:00 PDT	1
	SecurityManager411_StdToProLipgr	31 May 2016, 01:29:21 PDT	Never	
			Instal a License	
			Install a License	

Si aucune licence API n'est appliquée mais que vous disposez déjà du fichier .lic que vous pouvez installer votre licence, cliquez sur le bouton **Installer une licence**, vous devez stocker le fichier de licence sous le même disque où se trouve le serveur CSM.

Pour installer une nouvelle licence Cisco Security Manager, procédez comme suit :

Étape 1. Enregistrez le fichier de licence joint (.lic) à partir de l'e-mail que vous avez reçu dans votre système de fichiers.

Étape 2. Copiez le fichier de licence enregistré à un emplacement connu sur le système de fichiers du serveur Cisco Security Manager.

Étape 3. Lancez le client Cisco Security Manager.

Étape 4. Accédez à Outils->Administration de Security Manager...

Étape 5. Dans la fenêtre Cisco Security Manager - Administration, sélectionnez Licensing

Étape 6. Cliquez sur le bouton Installer une licence.

Étape 7. Dans la boîte de dialogue Installer la licence, sélectionnez le bouton Parcourir.

Étape 8. Accédez au fichier de licence enregistré sur le système de fichiers du serveur Cisco Security Manager et sélectionnez le bouton **OK**.

Étape 9. Dans la boîte de dialogue Installer la licence, cliquez sur le bouton OK.

Étape 10. Confirmez les informations de résumé de licence affichées et cliquez sur le bouton **Fermer**.

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					
	\\W9N-A73U18QCA72\C:\Program Files (x8I)\/CSCOpx\etc\kcenses\CSM						
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 License File: enses/CSMI/CSM2020012907092676-	A.Ic Browse
SecurityMan OK	Cancel Help
SecurityManager413_Pro_50_1.lc 26 Jun 2017, 03:24:26 PDT	Never

La licence API ne peut être appliquée que sur un serveur sous licence pour l'édition professionnelle CSM. La licence ne peut pas être appliquée à CSM exécutant une édition Standard de la licence. Exigences de licence API

Configuration Steps

Paramètres du client API

Si vous utilisez Postman, il y a des paramètres que vous devez configurer, cela dépend de chaque client d'API mais doit être similaire.

Proxy désactivé

Vérification SSL - DÉSACTIVÉ

Paramètres CSM

 API activée. Sous Outils > Administration de Security Manager > API Paramètres API

4	Cisco Security Manager - Administration	- • ×
-• 🕅	APT.	
- AutoLink	,	
ACL HitCount Settings	425	
- CCO Settings	C Finable API Service	
Configuration Archive		
- e CS-MARS	Result Set Page Size:* 500	
GSM Mobile		
Oustomize Desktop	Active cient sessions:" 5	
Debug Options	Request Payload Max Size (NB):* 2	
Deployment		
Device Communication		
Device Groups	50	Reset Restore Defaults
Discovery		
Event Ranagement		
 Health and Performance Monitor 		
Report Manager		
 Denoty Settings 		
Printergence settings		
Evening Notification Settings		
Dis Optimies		
Ide Seturgs		
- Certary		
Policy Management		
Policy Objects		
Process Monitoring Settings		
Sindle Sign on Configuration		
- Rule Expiration		
- Server Security		
Take Over User Session		
- Token Management		
VPN Policy Defaults		
Workflow		
wal Settings		
	A stimula MC	
	Activate will	luows
		Control Panel to activate Windows

Utilisation de l'API CSM

Vous devez configurer dans le client API les deux appels suivants :

- 1. Méthode de connexion
- 2. Obtenir les valeurs ACL

Pour référence au cours du processus :

Détails d'accès CSM utilisés dans ces travaux pratiques :

Nom d'hôte CSM (adresse IP) : **192.168.66.116**. Dans l'API, nous utilisons le nom d'hôte dans l'URL.

Utilisateur : admin

Mot de passe : Admin123

Méthode de connexion

Cette méthode doit être appelée avant toute autre méthode appelée sur d'autres services.

Guide d'API CSM : Méthode de connexion

Demander

- 1. Méthode HTTP : POST
- 2. URL: https://<hostname>/nbi/login
- 3. Body (Corps) :

Where:

username (nom d'utilisateur) : Nom d'utilisateur du client CSM associé à la session

Mot de passe : Mot de passe client CSM associé à la session.

reqld : Cet attribut identifie de manière unique une requête effectuée par le client. Cette valeur est reprise par le serveur CSM dans la réponse associée. Il peut être défini sur tout ce que l'utilisateur souhaite utiliser comme identificateur.

heartbeatRequested : Cet attribut peut être éventuellement défini. Si l'attribut est défini sur true, le client CSM reçoit un rappel de pulsation du serveur CSM. Le serveur tente d'envoyer une requête ping au client avec une fréquence proche de (délai d'inactivité) / 2 minutes. Si le client ne répond pas à la pulsation, l'API recommence la pulsation au cours de l'intervalle suivant. Si la pulsation réussit, le délai d'inactivité de la session est réinitialisé.

callbackUrl : URL à laquelle le serveur CSM effectue le rappel. Ceci doit être spécifié si heartbeatRequested a la valeur true. Seules les URL de rappel basées sur HTTPS sont autorisées

4. Envoyer

▶ 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	4	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 <password>Admin123</password> 7 <heartbeatrequested>true</heartbeatrequested> 8 <callbackurl>https://192.168.66.116/nbi/login</callbackurl> 9 </csm:loginrequest> 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3</pre>		

Sélectionnez l'option brute à afficher comme dans cet exemple.

Réponse

L'API de connexion valide les informations d'identification de l'utilisateur et renvoie un jeton de session sous la forme d'un cookie sécurisé. La valeur de session est stockée sous la clé **asCookie**, vous devez enregistrer cette **valeur asCookie**.

POST * https://192.168.30.17/nbi/login	Save 👻
Params Authorization Headers (10) Body Pre-request Script Tests Settings	
● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● GraphQL XML ▼	
1 (Anni Version=1.0" encoding="UFF-B*3> 2 < csn:logindscreet: walns:csm*csm* 3 cprotVersio=31.0C/protVersio> 4 credio1224(redio) 5 customariana/addin(sprome)	
<pre>6 Caster>:Lixal2X(pather2) 7 CasterDetReaderStree(/eartDetReader2) 8 CallerCult Stree(/eartDetReader2) 9 (/CasterDetReader2) 9</pre>	
Body Cookles (1) Headers (11) Test Results	
Pretty Raw Preview Visualize X0/IL =	a a
1 Bytwit version="1.0" encoding="Uff-8" }B 2 (nsl:loginResponse willstime"(sm") 3 (cprotVersion).10"(protVersion) 4 (cregId=123:/regId) 5 (serviceVersion)2.0"(protVersion) 6 (cesionTimeoutInVins) 7 7	A strate Mf a dama
	Activate Windows Go to System in Control Panel to activate Windows.
	🕞 Bootcamp Build Browse M 🙀

Body	Cookies (1) Headers (11) 1	Fest Results	asCookie Valu	ie		
	Name	Value	Domain	Path	HttpOnly	

Obtenir les règles ACL

Méthode execDeviceReadOnlyCLICmds. Le jeu de commandes qui peut être exécuté par cette méthode est constitué de commandes en lecture seule telles que les statistiques, les commandes de surveillance qui fournissent des informations supplémentaires sur le fonctionnement du périphérique particulier.

Détails de la méthode du guide de l'utilisateur de l'API CSM

Demander

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

3. En-tête HTTP : Le cookie retourné par la méthode de connexion qui identifie la session d'authentification.

Entrez asCookie valeur obtenue précédemment à partir de la connexion de méthode.

Clé : " de " d'entrée asCookie

Valeur: Valeur d'entrée obtenue.

Cochez cette case pour l'activer.

4. Body (Corps) :

Note: Le corps XML ci-dessus peut être utilisé pour exécuter n'importe quelle commande « show », par exemple : « show run all », « show run object », « show run nat », etc. L'élément XML "<deviceReadOnlyCLICmd>" indique que la commande spécifiée dans "<cmd>" et "<argument>" DOIT être en lecture seule.

Where:

deviceIP : Adresse IP du périphérique sur laquelle la commande doit être exécutée.

cmd : Commande fixe " show ". Le regex autorise la combinaison de majuscules [sS][hH][oO][wW]

argument : Arguments de la commande show. Comme " exécuter " pour afficher la configuration en cours du périphérique ou la **" liste d'accès "** pour afficher les détails de la liste d'accès.

5. Envoyer

$\left \right $		POST login	POST Get ACL	× + •••	No Environment	• • •
	▶ Get ACL				📮 Comments o	Examples 1 🔻
י 	POST - https://192.	.168.66.116/nbi/utilservice/execDev	riceReadOnlyCLICmds		Send	✓ Save ▼
	Params Authorization H	leaders (10) Body • Pre-	request Script Tests	Settings	5	Cookies Code
	🔵 none 🛛 form-data 🔍 >	<-www-form-urlencoded 🛛 🔘 raw	🔵 binary 🛛 🔵 GraphQL	XML 👻		
	1 k?xml version="1.0" d 2 < ccsm:execDeviceReadOT 3 <protversion>1.0 4 <reqid>1235 < deviceReadOnlyCLIC 6 <deviceip>192.168.60 7 <ccmd>show 8 <argument>access-lis 9 10 <th><pre>encoding="UTF-8"?> ilyCLICmdsRequest xmlns:csm= rotVersion> nd> 5.1</pre></th></argument></ccmd></deviceip> st Cmd> OnlyCLICmdsRequest><th>="csm"></th><td>4</td><td></td><th></th></reqid></protversion>	<pre>encoding="UTF-8"?> ilyCLICmdsRequest xmlns:csm= rotVersion> nd> 5.1</pre>	="csm">	4		
-						

Réponse



Vérification

Vous pouvez enregistrer la réponse sous forme de fichier. Accédez à **Enregistrer la réponse > Enregistrer dans un fichier.** Sélectionnez ensuite l'emplacement du fichier et enregistrez-le en tant que type .csv.

Sel	lect path to save file		x	Postman					- 0 X
💿 💿 🗉 🕆 🔳 Desitop →	× ¢	Search Desktop	ρ						_
Organize - New folder		8: •		My Workspace 🔹	🕹 Invite		0	* * * *	🜍 Upgrade 💌
★ Favorites A Favorit	<u></u>	Shortcut 1.74 KB	^	POST la chida act	POST https://1	92.168.30.17/nb//con_ 0 POST antGroupList		No Environment	
Desktop	1	fcs-csm-419-win-k9							
This PC	ervice_Pack1.exe here Self-Extractor ware	C5M20200129070926754.zip		nto				Send	• Save •
Documents fcs-csm-419	-win-k9.zip	FileZilla_3.44.1_win64_sponsored-se tup.exe FileZilla FTP Client	=	est Script Tests Settings					
Music Postman Postman Videos Videos		response.csv CSV File 1.36 KB	~) binary 🔘 GraphQL XML +					
File name response.csv			v						
Save as type: All Files (".")			~						
Alida Soldarr		Save Cancel							
- Proce Portoers			- /						
	Body Cookies (1) Headers								
	KEY					VALUE		Sav	e as example
	Date ()					Thu, 02 Apr 2020 01:43:47 GMT		San	e to a file
	Server @					Apache			
	Allow ()								
	Content-Length					253			
	Keep-Alive ①					timeout=20, max=10000			
	Connection ()					Keep-Alive			
	Content-Type					text/html; charset=iso-8859-1			
							Activate Wind Go to System in Co	OWS ontrol Panel to activat	
1 9 🖬									

Vous devez ensuite pouvoir ouvrir ce fichier .csv avec Excel Application, par exemple. À partir du type de fichier .csv, vous pouvez enregistrer la sortie sous d'autres types de fichier, tels que PDF, TXT, etc.

Dépannage

Réponses possibles en cas d'échec à l'aide de l'API.

1. Aucune licence API installée.

Motif: Licence API expirée, non installée ou non activée.

Solution possible : Vérifiez la date d'expiration de la licence, sous **Outils > Administration du Gestionnaire de sécurité > Page Licences.**

Vérifiez que la fonctionnalité API est activée sous **Outils > Administration du gestionnaire de sécurité > API**

Confirmez les paramètres de la section **Installation/Vérification de la licence de l'API CSM** cidessus de ce guide.

2. Mauvaise utilisation de l'adresse IP CSM pour la connexion à l'API.

Motif: L'adresse IP du serveur CSM est incorrecte dans l'URL de l'appel API.

Solution possible : Vérifiez dans l'URL du client API que le nom d'hôte est l'adresse IP correcte du serveur CSM.

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

3. Adresse IP ASA incorrecte.

Motif: L'adresse IP définie sur le corps entre les balises <deviceIP></deviceIP> ne doit pas être la bonne.

Solution possible : Vérifiez que l'adresse IP du périphérique approprié est définie dans la syntaxe Body.

4. Aucune connexion au pare-feu.

Motif: Le périphérique n'a aucune connexion avec le CSM

Solution possible : Exécutez un test de connectivité à partir du serveur CSM et dépannez une connectivité supplémentaire au périphérique.

Pour plus d'informations sur les codes d'erreur et la description, reportez-vous au Guide de spécification de l'API de Cisco Security Manager dans le <u>lien</u> suivant.