APIC-EM 1.3 - Generación de certificados: eliminación mediante API

Contenido

Introducción Antecedentes ¿Cómo sabrá cuál es el estado actual del dispositivo? ¿Cómo se asegura de que APIC-EM también tenga el mismo certificado o de que APIC-EM haya entendido o no el mismo certificado? ¿Cómo se elimina el certificado del dispositivo? ¿Cómo se aplica el certificado de APIC - EM? A veces APIC-EM tiene el certificado pero el dispositivo no. ¿Cómo puede resolverlo?

Introducción

Este documento describe cómo utilizar la API Cisco Application Policy Infrastructure Controller (APIC) - Extension Mobility (EM) para crear y eliminar el certificado. Con IWAN, todo se configura automáticamente. Sin embargo, IWAN en este momento no tiene ningún flujo para recuperar automáticamente el dispositivo del certificado caducado.

Lo bueno es que hay algún tipo de flujo en la automatización en términos de RestAPI. Sin embargo, la automatización se realiza por dispositivo y necesita cierta información sobre el dispositivo. El flujo RestAPI que está fuera del flujo IWAN, utiliza algún mecanismo para automatizar el certificado para el dispositivo.

Antecedentes

Topología habitual del cliente.

SPOKE — HUB — APIC_EM [Controller]

Estas son las tres situaciones:

- El certificado ha caducado.
- El certificado no se está renovando.
- El certificado no está disponible en absoluto.

¿Cómo sabrá cuál es el estado actual del dispositivo?

Ejecute el comando Switch# sh cry pki cert.

```
HUB2#sh cry pki cert
Certificate
 Status: Available
 Certificate Serial Number (hex): 3C276CE6B6ABFA8D
 Certificate Usage: General Purpose
 Issuer:
   cn=sdn-network-infra-subca
 Subject:
   Name: HUB2
   cn=ASR1001 SSI161908CX sdn-network-infra-iwan
   hostname=HUB2
 Validity Date:
   start date: 06:42:03 UTC Mar 28 2017
   end date: 07:42:03 UTC Mar 28 2017
 Associated Trustpoints: sdn-network-infra-iwan
CA Certificate
 Status: Available
 Certificate Serial Number (hex): 04
 Certificate Usage: General Purpose
 Issuer:
   cn=ca
 Subject:
   cn=sdn-network-infra-subca
 Validity Date:
   start date: 06:42:03 UTC Mar 28 2017
   end date: 07:42:03 UTC Mar 28 2017
 Associated Trustpoints: sdn-network-infra-iwan
```

Si ve, hay dos certificados y aquí debe marcar el punto de confianza asociado .

La fecha de finalización será normalmente de un año y debe ser posterior a la fecha de inicio.

Si se trata de sdn-network-infra-iwan, significa desde APIC-EM que tiene ID y certificado CA registrados.

¿Cómo se asegura de que APIC-EM también tenga el mismo certificado o de que APIC-EM haya entendido o no el mismo certificado?

a. Mostrar la versión del dispositivo y recopilar el número de serie:

```
If you require further assistance please contact us by sending email to
export@cisco.com.
License Type: RightToUse
License Level: adventerprise
Next reload license Level: adventerprise
cisco ASR1001 (1RU) processor (revision 1RU) with 1062861K/6147K bytes of memory.
Processor board ID SSI 61908CX
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7741439K bytes of eUSB flash at bootflash:.
Configuration register is 0x0
```

Con la ayuda de este número de serie, puede realizar una consulta APIC-EM para averiguar qué piensa APIC-EM sobre este dispositivo.

b. Vaya a Documentación de API.

CISCO DNA Center						admin 👩 😷 💽
	1	Design, A	NA Cer	nter 1	1-1-	AMICLEM Settings Settings New Controller Admin Controller Management Auto Logs
Applications				Q	Search Applications	Re Audit Logs New
🔀 Design	8,	Provision	Policy			Re User Change Password
Tools						
\$	m	8	:	*	÷	
Discovery	Dashboard	Device Inventory	Host Inventory	Topology	Path Trace	
	₩	e,	B , N			0

c. Haga clic en Agente de infraestructura de clave pública (PKI).

d. Haga clic en First API (Primera API), que nos ayudará a conocer el estado desde el lado de la API.

cisco DNA Center	API Documentation	а
Policy Administration Role Based Access Control	cert /certificate-authority/idcert/ca/{id}/{type}	getDefaultCaPem
Scheduler Service Provision Engine	рит /certificate-authority/update/{id}/{type}	updateDefaultCaPem
Site Profile Service Swim	рит /certificate-authority/{id}/(type)	updateDefaultCaPem
Task Topology	GET /trust-point	pkiTrustPointListGet
default Title	Post /trust-point	pkiTrustPointPost
	GET /trust-point/count	pkiTrustPointListGet
	GET /trust-point/pkcs12/{trustPointid}/{token}	pkiTrustPointPkcs12Download
	DELETE /trust-point/serial-number/{serialNumber}	pkiTrustPointDeleteByDeviceSN
	GET /trust-point/serial-number/(serialNumber)	pkiTrustPointGetByDeviceSN
	GET /trust-point/{startindex}/{recordsToReturn}	getCertificateBriefList
	DELETE //trust-point/{trustPoint/d}	pkiTrustPointDelete
	Post //trust-point/{trustPoint/d}	pkiTrustPointPush

Haga clic en GET.

En una casilla de verificación, haga clic en el número de serie recopilado de la salida show version del Dispositivo.

Haga clic en Prueba!.

Compare el valor de salida con el resultado sh crp pki cert del dispositivo.

¿Cómo se elimina el certificado del dispositivo?

A veces ocurre que en el dispositivo, el certificado está ahí y en el APIC-EM no está ahí. Por eso, cuando ejecuta **GET API** obtiene un mensaje de error.



La solución es sólo una y es eliminar el certificado del dispositivo:

a. Switch# show run | I trustpoint

```
HUB2#sh run | i trustpoint
crypto pki trustpoint zxz
crypto pki trustpoint <mark>sdn-network-infra-iwan</mark>
HUB2#
```

Ejecute el comando Switch# no crypto pki trustpoint <trustpoint name>.

```
HUB2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
HUB2(config)#no crypto pki trustpoint sdn-network-infra-iwan
% Removing an enrolled trustpoint will destroy all certificates
received from the related Certificate Authority.
Are you sure you want to do this? [yes/no]: yes
% Be sure to ask the CA administrator to revoke your certificates.
```

HUB2(config)#

Este comando elimina todo el certificado en el dispositivo asociado con el punto de confianza seleccionado.

Vuelva a comprobar si se elimina el certificado.

Use el comando: Switch# sh cry pki cert.

No debe mostrar el punto de confianza sdn que se eliminó.

b. Eliminación de clave:

Ejecute el comando en el dispositivo: Switch# sh cry key mypubkey all.

Aquí verá que el nombre de la clave comienza con sdn-network-infra.

Comando para eliminar la clave:

HUB2(config)#cry key zeroize rsa sdn-network-infra-iwan % Keys to be removed are named 'sdn-network-infra-iwan'. % All router certs issued using these keys will also be removed. Do you really want to remove these keys? [yes/no]: yes HUB2(config)#

2. Asegúrese de que la interfaz APIC-EM conectada al dispositivo sea Pingable.

Puede ocurrir que APIC-EM tenga dos interfaces de las cuales una es pública y la otra es privada. En ese caso, asegúrese de que la interfaz APIC-EM que se comunica con el dispositivo haga ping entre sí.

```
HUB2#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HUB2#
```

¿Cómo se aplica el certificado de APIC - EM?

En APIC-EM, cuando se hace clic en Documentación de API y se selecciona Agente PKI, esta opción está disponible.

POST/trust-point

(I Broker Service	GET /certificate-authority/ca/(id)/(type)	getDefaultCaPemChai
olicy Administration ole Based Access Control	GET /certificate-authority/idcert/ca/{id}/{type}	getDefaultCaPer
cheduler ervice Provision Engine	рит /certificate-authority/update/{id}//type}	updateDefaultCaPer
te Profile Service wim	рит /certificate-suthority/{id}//type}	updateDefaultCaPer
sk pology	cer /trust-point	pkiTrustPointListG
fault Title	Post /trust-point	pkiTrustPointPo
	Response Class	
	Implementation Notes This method is used to create a trust-point Response Class Model Model Schema TaskidResuit { version (string, optional), response (TaskidResponse, optional) } TaskidResponse {	
	taskid (Taskid, optional), url (string, optional) } Taskid {	

A continuación, debe tener información sobre el dispositivo y hacer clic en la opción de probarlo.

Response Class				
Model Model Sch	nema			
TaskidResuit { version (string, op response (Taskidi TaskidResponse { taskid (Taskid, opt url (string, optional Taskid {	tional), Response, optional) tional), I)			
esponse Conter	nt Type: application/json			
Parameter	Value	Description	Parameter Type	Data Type
pkiTrustPointInput	(pkiTrustPoi	ntlnput body	Model Model Schema
	"Battellumbar" "Aschuku!. "senablumbar" "SSII81808CX" "itusEPcolleName" "sgn.network-infra-iwan". "entityType" "router". "entityName" "HUR2"	R		PkiTrustPoint { serialNumber (string): Devices serial-number, entityName (string): Devices hostname, id (string, optional): Trust-point identification.

Automatically generated,

platformId (string): Platform identification. Eg. ASR1008. trustProfileName (string): Name of trust-profile (must already exist). Default: sdn-network-infra-iwan, entityType (string, optional): Available options: router,

Ejemplo:

{

"platformId":"ASR1001", "serialNumber":"SSI161908CX", "trustProfileName":"sdn-network-infra-iwan", "entityType":"router", "entityName":"HUB2"

}

- La información resaltada es ESTÁTICA y el resto es Dinámica.
- El nombre de entidad es el nombre de host del dispositivo.

Parameter content type: application/json *

- Número de serie que obtuvo de la versión show del dispositivo.
- Tipo de entidad que puede cambiar en función del tipo de dispositivo.
- Esta información es necesaria para indicar a APIC-EM que configure el dispositivo. Aquí APIC-EM comprende el número de serie.

Salida de Try it out!:

Response Body	
<pre>{ "response": "taskId": "url": "/ }, "version": }</pre>	: { : "la395edl-1730-43fa-9527-327ed3e6e12b", /api/v1/task/la395ed121730-43fa-9527-327ed3e6e12b" "l.0"
Response Code	
202	
Response Head	ters
<pre>{ "Pragma": "r "Content-Sec "X-Frame-Opt "Date": "Tue "Strict-Tran "Content-Typ "Access-Cont "Cache-Contr "Transfer-Er "Access-Cont }</pre>	no-cache, no-cache", curity-Policy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bd50 tions": "SAMEORIGIN, SAMEORIGIN", e, 28 Mar 2017 10:10:06 GNT", nsport-Security": "max-age=31536000; includeSubDomains, max-age=31536000; includeSubDomains", pe": "application/json;charset=UTF-8", trol-Allow-Origin": "https://10.78.106.45", rol": "no-cache, no-store, no-cache, no-store", ncoding": "chunked", trol-Allow-Credentials": "false"

Esta salida significa que APIC-EM crea el archivo internamente y que ahora está listo para implementarlo en el dispositivo. El siguiente paso es introducir este dispositivo en el paquete. Para pulsar, necesita obtener una ID de punto de confianza. Esto se puede hacer a través de GET API CALL.

<u>GET/trust-point/serial-number/{serialNumber}</u> - Consulta

CET /trus	t-point/serial-number/(serial/\umber)			pkiTrustPointGetByDeviceSN
Implementatio	an Notes			
This method is	s used to return a specific trust-point by	its device serial-number		
Response Cla	305			
Model Model	Schema			
PkiTrustPointR version (strin response (Pi) PkiTrustPoint (serialNumber entityName () id (string.opti platformid (st trustProfileN entityType () networkDevi certificateAut controllertpA attributeInfo }	esuit (g. optional), iTrustPoint, optional) r (string): Devices setial-number, string): Devices hostname, onal): Trust-point identification. Automatically g tring): Platform identification. Eg. ASR1006, ame (string): Name of trust-profile (must alread tring, optional): Available options: router, switcl celd (string, optional): Device identification. Ci thorityld (string, optional): CA identification. A iddress (string, optional): IP address device u (object, optional)	renerated. by exist). Default: sdn-network-initra-iwan. h. Currently not used. arrently not used. utomatically populated. ses to connect to APIC-EM. Eg. Proxy server IP add	ress. Automatically populi	alled if not set.
Response Co	ntent Type: application/json			
Parameters				
Parameter	Value	Description	Parameter Type	Dela Type
serialNumber	551151508CX	Device serial number	path	ating
Server Statute C	odes.			

Le dará este resultado. Significa que el APIC-EM tiene el certificado con esto para presionar el dispositivo.

esponse Body		
{		
"response": {		
"platformId": "ASR1001",		
"serialNumber": "SSI1619)8CX",	
"trustProfileName": "sdr	network-infra-iwan",	
"entityName": "HUB2",		
"entityType": "router",		
"certificateAuthorityId"	"f0bd5040-3f04-4e44-94d8-de97b8829e8d",	
"attributeInfo": {},		
"id": "2b832bf6-9061-44b	1-a773-fb5256e544fb"	
3,		
"version": "1.0"		
}		
	N	
	A	
esponse Code		
200		

Empuje el certificado al dispositivo.

<u>POST/trust-point/{trustPointId}</u> // trustPointId debe copiarse de la consulta del número de serie de GET

{"response": { "platformId": "ASR1001", "serialNumber": "SSI161908CX", "trustProfileName": "sdnnetwork-infra-iwan", "entityName": "HUB2", "EntityType": "router", "certificateAuthorityId": "f0bd5040-3f04-4e44-94d8-de97b8829e8d", "attributeInfo": {}, "id": "c4c7d612-9752-4be5-88e5e2b6f137ea13" }, "versión": "1.0" }

Esto llevará el certificado al dispositivo, siempre que haya una conectividad adecuada.

POST /trust-point/{trustPoint/d}	pkiTrustPointPush
GET /trust-point/{trustPointId}	pkiTrustPointGet
GET /trust-point/{trustPointId}/config	pkiTrustPointConfigGet
GET //trust-point/{trustPointid}/downloaded	checkPKCS12Downloaded

[BASE URL: https://10.78.106.45/abi/v1/abi-docs/bki-broker-service . API VERSION: 1.0]

rameter V	alue	Description	Parameter Type	Data Type
trustPointId 2	b832bf6-9061-44bd-a773-fb5256e544fb	Trust-point ID	path	string
rror Status Code	s			
HTTP Status Code	Reason			
200	The request was successful. The result is conta	ined in the response body.		
201	The POST/PUT request was fulfilled and a new	resource has been created. Information about	the resource is in the response boo	ly.
202	The request was accepted for processing, but ti	he processing has not been completed.		
204	The request was successful, however no conter	nt was returned.		
206	The GET request included a Range Header, an	d the server responded with the partial content	matching the range.	
400	The client made a request that the server could	not understand (for example, the request synt	ax is incorrect).	
401	The client's authentication credentials included	with the request are missing or invalid.		
403	The server recognizes the authentication crede	ntials, but the client is not authorized to perform	n this request.	
484	The client made a request for a resource that d	oes not exist.		
500	The server could not fulfill the request.			
501	The server has not implemented the functionalit	y required to fulfill the request.		
503	The server is (temporarily) unavailable.			
504	The server did not respond inside time restriction	ns and timed-out.		
489	The target resource is in a conflicted state (for e	xample, an edit conflict where a resource is be	ing edited by multiple users). Retryir	ng the request later might succeed.
415	The client sent a request body in a format that t	he server does not support (for example, XML	to a server that only accepts JSON)	

Mensaje de respuesta correcta:

Try it out! Hide Response	
Request URL	
https://10.78.106.45/api/v1/trust-point/2b832bf6-9061-44bd-a773-fb5256e544fb	
Response Body	
<pre>{ "response": { "taskId":]_"f10022bd-8f45-4597-8160-bcc07fd55898", "url": "/api/v1/task/f10022bd-8f45-4597-8160-bcc07fd55898" }, "version": "1.0" }</pre>	
Response Code	
202	
Response Headers	

Vuelva a comprobar el dispositivo:

Ya ve que ambos certificados se han pegado:

```
HUB2#sh cry pki cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 2AD39646370CACC7
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: HUB2
    cn=ASR1001 SSI161908CX sdn-network-infra-iwan
    hostname=HUB2
  Validity Date:
    start date: 10:00:07 UTC Mar 28 2017
    end
         date: 10:00:07 UTC Mar 28 2018
    renew date: 10:00:06 UTC Jan 14 2018
  Associated Trustpoints: sdn-network-infra-iwan
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 5676260082D447A3
  Certificate Usage: Signature
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    cn=sdn-network-infra-ca
  Validity Date:
    start date: 09:20:26 UTC Mar 28 2017
    end date: 09:20:26 UTC Mar 27 2022
  Associated Trustpoints: sdn-network-infra-iwan
```

```
HUB2#
```

A veces APIC-EM tiene el certificado pero el dispositivo no. ¿Cómo puede resolverlo?

Hay una tarea en segundo plano a través de la cual sólo puede eliminar el certificado de APIC-EM. A veces, el cliente elimina por error el certificado del dispositivo, pero en APIC-EM, sigue ahí. Haga clic en **ELIMINAR.**

DELETE/trust-point/serial-number/{serialNumber} - Eliminar.

GET	/trust-point/count	pkiTrustPointListGet
GET	/trust-point/pkcs12/{trustPointid}//token)	pkiTrustPointPkcs12Download
00.55	/trust-point/serial-number/(serialNumber)	phiTrustPointDeleteByDeviceSN
GET	/trust-point/serial-number/[serialNumber]	pNTrustPointGetByDeviceSN
Respo	ethod is used to return a specific trust-point by its device serial-number	
Model	Model Schema	
PkiTrus versi respo	stPointResult { ion (string, optional), onse (PkiTrustPoint, optional)	

Introduzca el número de serie y haga clic en Try out!.

Value	Description	Parameter Type	Data Type
SSI161908CX	Device serial-number	path	string
odes			
Reason			
The request was successful. The resu	It is contained in the response body.		
The request was successful, however	no content was returned.		
The GET request included a Range H	leader, and the server responded with the partial content ma	tching the range.	
The client made a request that the se	rver could not understand (for example, the request syntax is	s incorrect).	
The client's authentication credentials	included with the request are missing or invalid.		
The server recognizes the authentica	tion credentials, but the client is not authorized to perform thi	s request.	
The client made a request for a resou	ree that does not exist.		
The server could not fulfill the reques			
The server has not implemented the t	unctionality required to fulfill the request.		
The server is (temporarily) unavailable			
The server did not respond inside tim	e restrictions and timed-out.		
The target resource is in a conflicted	state (for example, an edit conflict where a resource is being	edited by multiple users). Retryi	ng the request later might succeed.
The client sent a request body in a fo	rmat that the server does not support (for example, XML to a	server that only accepts JSON	
	Value SSI161908CX COES Reason The request was successful. The resul The request was successful. however The GET request included a Range H The client made a request that the se The client's authentication credentials The client made a request for a resou The server recognizes the authentical The server recould not fulfill the request The server has not implemented the f The server did not respond inside time The target resource is in a conflicted s The client sent a request body in a for	Value Description SS161908CX Device serial-number CCES Reason The request was successful. The result is contained in the response body. The request was successful. The result is contained in the response body. The request was successful. The result is contained in the response body. The request was successful, however no content was returned. The GET request included a Range Header, and the server responded with the partial content ma The client made a request that the server could not understand (for example, the request syntax is The client made a request that the server could not understand (for example, the request syntax is The client made a request for a resource that does not exist. The server recognizes the authentication credentials, but the client is not authorized to perform the the client made a request for a resource that does not exist. The server could not fulfill the request. The server has not implemented the functionality required to fulfill the request. The server is (temporarily) unavailable. The server did not respond inside time restrictions and timed-out. The target resource is in a conflicted state (for example, an edit conflict where a resource is being The client sent a request body in a format that the server does not support (for example, XML to a state)	Value Description Parameter Type STIE1308CX Device serial-number path

<pre>{ "response": { "taskId": "33ab0da8-9be1-40b7-86c2-cf2e501ebbb5", "url": "/api/v1/task/33ab0da8-9be1-40b7-86c2-cf2e501ebbb5" }, "version": "1.0" }</pre>	
Response Code	
202	
Response Headers	
<pre>{ "Pragma": "no-cache, no-cache", "Content-Security-Policy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce "X-Frame-Options": "SAMEORIGIN, SAMEORIGIN", "Date": "Tue, 28 Mar 2017 10:15:23 GMT", "Strict-Transport-Security": "max-age=31536000; includeSubDomains, max-age=31536000; includeSubDomains", "Content-Type": "application/json;charset=UTF-8", "Access-Control-Allow-Origin": "https://10.78.106.45", "Cache-Control": "no-cache, no-store, no-cache, no-store", "Transfer-Encoding": "chunked", "Access-Control-Allow-Credentials": "false" }</pre>	:-f59e75bb-2a28-4fe8-a954-