APIC-EM 1.3. – 証明書の生成 – APIによる削除

内容

<u>概要</u>

<u>背景説明</u>

<u>デバイスの現在の状態を確認するには、どうすればよいですか。</u> APIC-EM にも同じ証明書があるかどうか、または APIC-EM が同じ証明書を認識したどうかを確 認するには、どうすればよいですか。 デバイスから証明書を削除するには、どうすればよいですか。 APIC-EM から証明書を適用するには、どうすればよいですか。 APIC-EM には証明書があっても、デバイスにはない場合があります。これを解決するには、どう すればよいですか。

概要

このドキュメントでは、Cisco Application Policy Infrastructure Controller(APIC)- エクステンション モビリティ(EM)API を使用して証明書を作成または削除する方法について説明します。 IWAN では、これがすべて自動的に設定されます。ただし、現時点では、期限切れの証明書から デバイスを自動的に復旧するためのフローが IWAN にはありません。

なお、RestAPIに関するある種の自動化フローが存在します。ただし、この自動化はデバイスご とに行われ、デバイスに関する情報が必要です。IWANフローの外部にあるRestAPIフローは、デ バイスの証明書を自動化するメカニズムを使用します。

背景説明

標準的な顧客トポロジ。

SPOKE — HUB — APIC_EM [コントローラ]

以下の3つの状況があります。

- •証明書の有効期限が切れている。
- •証明書が更新されない。
- •証明書をまったく使用できない。

デバイスの現在の状態を確認するには、どうすればよいですか。

コマンド Switch# sh cry pki cert を実行します。

```
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
        date: 07:42:03 UTC Mar 28 2017
   end
 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
```

結果を見ると 2 つの証明書があり、ここでは関連するトラストポイント(Associated Trustpoint)を確認する必要があります。

終了日は通常1年であり、開始日より後である必要があります。

これが sdn-network-infra-iwan である場合は、APIC-EM から、ID および CA 証明書が登録されて いることを意味します。

APIC-EM にも同じ証明書があるかどうか、または APIC-EM が 同じ証明書を認識したどうかを確認するには、どうすればよいで すか。

a.デバイスからバージョンを表示し、シリアル番号を次のように収集します。

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
```

このシリアル番号を使って APIC-EM クエリを実行し、APIC-EM がこのデバイスをどのように認 識しているかを確認できます。

b.API ドキュメントに移動します。

CISCO DNA Center						admin 📋 😷 💽
	1	Design, A	NA Cer	nter 1	1	Additional Settings Settings New Controller Admin Controller Management Add Logs
Applications				Q	Search Applications	Re Audit Logs New
🔀 Design	8,	Provision	🛃 Policy			Re User Change Password
Tools						
\$	m	9		*	÷	
Discovery	Dashboard	Device Inventory	Host Inventory	Topology	Path Trace	
	\$	₿ _A	A , N	00		0

c. [Public Key Infrastructure (PKI) Broker]をクリックします。

d.最初の API をクリックします。これにより、API 側からのステータスを確認できます。

cisco DNA Center	API Documentation	ad
Policy Administration Role Based Access Control	cerr /certificate-authority/idcert/ca/{id}/{type}	getDefaultCaPem
Scheduler Service Provision Engine	PUT /certificate-authority/update/{id}/{type}	updateDefaultCaPem
Site Profile Service Swim	PUT /certificate-authority/{id}/{type}	updateDefaultCaPem
Task Topology	SET /trust-point	pkiTrustPointListGet
default Title	POST /trust-point	pkiTrustPointPost
	GET /trust-point/count	pkiTrustPointListGet
	cet /trust-point/pkcs12/{trustPoint/d}/{token}	pkiTrustPointPkcs12Download
	DELETE //trust-point/serial-number/{serialNumber}	pkiTrustPointDeleteByDeviceSN
	cer /trust-point/serial-number/{serialNumber}	pkiTrustPointGetByDeviceSN
	<pre>/trust-point/{startIndex}/{recordsToReturn}</pre>	getCertificateBriefList
	DELETE /trust-point/(trustPointid)	pkiTrustPointDelete
	POST //trust-point/{trustPoint/d}	pkiTrustPointPush

[GET] をクリックします。

チェックボックスで、デバイスの show version の出力から収集されたシリアル番号をクリックします。

[Try it out!] をクリックします。

出力値を、デバイスの sh crp pki cert 出力と比較します。

デバイスから証明書を削除するには、どうすればよいですか。

デバイスには証明書があっても、APIC-EM には証明書がない場合があります。これが原因で、 GET API を実行するとエラー メッセージが表示されます。



解決法は1つのみ、つまりデバイスから証明書を削除することです。

a.Switch# show run | I trustpoint



コマンド Switch# no crypto pki trustpoint <trustpoint name> を実行します。

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)#

このコマンドは、選択したトラストポイントに関連付けられているデバイス上のすべての証明書 を削除します。

証明書が削除されたことを再確認します。

コマンドを使用しますSwitch# sh cry pki cert

削除された sdn トラストポイントは表示されないはずです。

b.キーの削除:

デバイス上でコマンドを実行します。Switch# sh cry key mypubkey all。

ここで、キー名が sdn-network-infra で始まることが分かります。

キーを削除するコマンド:

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.デバイスに接続されているAPIC-EMインターフェイスがping可能であることを確認します。

APIC-EM に 2 つのインターフェイス(1 つは公開、もう 1 つは非公開)が存在する場合がありま す。この場合、デバイスと通信する APIC-EM インターフェイスが互いに ping 可能であることを 確認してください。

```
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#
```

APIC-EM から証明書を適用するには、どうすればよいですか。

APIC-EM で [API Documentation] をクリックして [PKI Broker] を選択すると、このオプションが 使用可能になります。

POST/trust-point

KI Broker Service	GET /certificate-authority/ca/(id}/(type)	getDefaultCaPemChain
olicy Administration	GET /certificate-authority/idcert/ca/{id}/(type}	getDefaultCaPem
cheduler ervice Provision Engine	Put /certificate-authority/update/{id}/(type}	updateDefaultCaPem
te Profile Service	Put /certificate-authonity/{id}/(type}	updateDefaultCaPem
<u>sk</u> pology	GET /trust-point	pkiTrustPointListGet
sfault Title	Pacific /trust-point	pkiTrustPointPost
	This method is used to create a trust-point Response Class	
	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 { }	

[try it out]

Response Class					
Model Model Sc	hema				
TaskidResult { version (string, op response (Taskid	otional), Response, optional)				
TaskidResponse (taskid (Taskid, op url (string, optiona	tional), il)				
}					
Taskid {					
ł					
Response Conte	nt Type: application/json				
Parameters					
Parameter	Value		Description	Parameter Type	Data Type
pkiTrustPointInput	l.		pkiTrustPointInput	body	Model Model Schema
	"platfacmid""ASR1901". "asnathumber""SSI181808CX". "tustEchieName""San-network-infra-iwan". "anthyTyns"."router. "anthyTyns"."HUB2" J	A7			PkiTrustPoint (serialNumber (sting): Devices serial-number, entityName (string): Devices hostname, id (string, optional): Trust-point identification. Automatically generated,

serialNumber (sting): Devices serial-number, entityName (sting): Devices hostname, id (sting, ordonal): Trush-point identification. Automatically generated, platformid (sting): Platform identification. Eg. ASR1000, KutaRFordieName (string): Name of trust-profile (must already exist). Default scin-network-infra-iwan, entityType (string, optional): Available options: router, 2

{

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

Parameter content type: application/json 🔻

"entityName":"HUB2"

}

- •
- .
- show version

•

• APIC-EM APIC-EM

[Try it out!]

{	
"response": {	
"taskId": "la395e	dl-1730-43fa-9527-327ed3e6e12b",
"url": "/api/v1/t	ask/1a395ed1x2730-43fa-9527-327ed3e6e12b"
},	
"version": "1.0"	
}	
spanse Cade	
02	
sponse Headers	
sponse Headers	
sponse Headers	
"Pragma": "no-cache,	no-cache",
"Pragma": "no-cache, "Content-Security-Po	. no-cache", ulicy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bd
<pre>sponse Headers "Pragma": "no-cache, "Content-Security-Pc "X-Frame-Options": " "Total Security Total Security</pre>	. no-cache", llicy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bd 'SAMEORIGIN, SAMEORIGIN",
<pre>sponse Headers "Pragma": "no-cache, "Content-Security-Pc "X-Frame-Options": " "Date": "Tue, 28 Mar "statict Topacroots So</pre>	. no-cache", licy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bc 'SAMEORIGIN, SAMEORIGIN", ' 2017 10:10:06 GMTT, runite": "max-are-31536000; includeSubDomains, max-are-31536000; includeSubDomains"
"Pragma": "no-cache, "Content-Security-Pc "X-Frame-Options": " "Date": "Tue, 28 Mar "Strict-Transport-Sec	no-cache", Plicy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bo SAMEORIGIN, SAMEORIGIN", 2017 10:10:06 GMT", Picurity": "max-age=31536000; includeSubDomains, max-age=31536000; includeSubDomains",
"Pragma": "no-cache, "Content-Security-Pc "X-Frame-Options": " "Date": "Tue, 28 Mar "Strict-Transport-Se "Content-Type": "app "Access-Control-Allo	no-cache", licy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bd 'SAMEORIGIN, SAMEORIGIN", ' 2017 10:10:06 GMT", :curity": "max-age=31536600; includeSubDomains, max-age=31536000; includeSubDomains", :lication/json;charset=UTF-8", w=Oriein": "https://10.78.106.45".
"Pragma": "no-cache, "Content-Security-Pc "X-Frame-Options": "Date": "Tue, 28 Mar "Strict-Transport-Se "Content-Type": "app "Access-Control-Allo "cache-Control": "no	no-cache", Nicy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bd SAMEORIGIN, SAMEORIGIN", ' 2017 10:10:06 GMT", :curity": "max-age=31536000; includeSubDomains, max-age=31536000; includeSubDomains", Nication/json;charset=UTF-8", ww-Origin": "https://10.78.106.45", -cache, no-store, no-cache, no-store".
"Pragma": "no-cache, "Content-Security-Pc "X-Frame-Options": " "Date": "Tue, 28 Mar "Strict-Transport-Se "Content-Type": "app "Access-Control-AllC "Cache-Control": "no "Transfer-Encoding";	no-cache", blicy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bd 'SAMEORIGIN, SAMEORIGIN", '2017 10:10:06 GMT", scurity": "max-age=31536000; includeSubDomains, max-age=31536000; includeSubDomains", blication/json;charset=UTF-8", w=Origin": "https://10.78.106.45", i-cache, no-store, no-cache, no-store", "chunked",
<pre> Pragma": "no-cache, "Content-Security-Pc "X-Frame-Options": ' "Date": "Tue, 28 Mar "Strict-Transport-Se "Content-Type": "app "Access-Control-Allc "Transfer-Encoding": "Access-Control-Allc "Access-Control-Allc "Access-Control-Allc "Access-Control-Allc "Access-Control-Allc "Access-Control-Allc "Access-Control-Allc "Access-Control-Allc "Access-Control-Allc "Content-Secontrol-Allc "Transfer-Encoding": "Access-Control-Allc "Content-Secontrol-Allc "Access-Control-Allc "Acces</pre>	no-cache", blicy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bd 'SAMEORIGIN, SAMEORIGIN", 2017 10:10:06 GMT", scurity": "max-age=31536000; includeSubDomains, max-age=31536000; includeSubDomains", blication/json;charset=UTF-8", ww-Origin": "https://10.78.106.45", u-cache, no-store, no-cache, no-store", "chunked", ww-Credentials": "false"
"Pragma": "no-cache, "Content-Security-Pc "X-Frame-Options": ' "Date": "Tue, 28 Mar "Strict-Transport-Se "Content-Type": "app "Access-Control-Alle "Transfer-Encoding": "Access-Control-Alle	no-cache", blicy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bd 'SAMEORIGIN, SAMEORIGIN", '2017 10:10:06 GMT", scurity": "max-age=31536000; includeSubDomains, max-age=31536000; includeSubDomains", blication/json;charset=UTF-8", ww-Origin": "https://10.78.106.45", -cache, no-store, no-cache, no-store", "chunked", ww-Credentials": "false"

APIC-EM ID GET API CALL

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

Contraction of the local division of the loc	st-point/serial-number/{serialNun	ber)		pk/TrustPointGetByDeviceSN
	12			
Implementati	ion Notes			
This method is	s used to return a specific trust-poir	t by its device serial-number		
Response Cl	laos			
Model Mode	i Schema			
PkiTrustPointF version (strin response (Pi) PkiTrustPoint (serialNumbe entityName (id (string, opt platformid (s trustProfileN entityType () networkDev/ certificateAu controllertp/ attributeInfo	Result { ng, optional); si/TrustPoint, optional) f r (string): Devices serial-number, (string): Devices hostname, ironal): Trust-point identification. Automativ firing): Platform identification. Eg. ASR100 fame (string): Name of trust-profile (must itting, optional): Name of trust-profile (must itting, optional): Device identificati thorityId (string, optional): CA identificati Address (string, optional): IP address dev (object, optional)	ally generated. 6. Iready exist). Default: sdn-network-infra-iwan. witch. Currently not used. n. Currently not used. on. Automatically populated. ice uses to connect to APIC-EM. Eg. Proxy server IP add	ress. Automatically popula	sted if not set.
Response Co	ontent Type: application/json			
Response Co Parameters	ontent Type: application/json			
Response Co Parameters Parameter	ontent Type: application/json	Description	Parameter Type	Dela Type

APIC-EM

Response Body	
{	
"response": {	
"platformId": "ASR1001",	
"serialNumber": "SSI161908CX",	
"trustProfileName": "sdn-network-infra-iwan",	
"entityName": "HUB2",	
"entityType": "router",	
"certificateAuthorityId": "f0bd5040-3f04-4e44-94d8-de97b8829e8d",	
"attributeInfo": {},	
"id": "2b832bf6-9061-44bd-a773-fb5256e544fb"	
h	
"version": "1.0"	
}	
Response Code	
200	

<u>シリアル番号取得クエリから POST/trust-point/{trustPointId}</u> // trustPointId をコピーする必要が あります。

{ "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" }, "version":"1.0" }

(
POST	/trust-point/{trustPointid}	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/pki-broker-service . API VERSION: 1.0]

arameter Va	lue	Description	Parameter Type	Data Type
trustPointId 21	832bf6-9061-44bd-a773-fb5256e544fb	Trust-point ID	path	string
rror Status Code	5			
HTTP Status Code	Reason			
200	The request was successful. The result is contain	ed in the response body.		
201	The POST/PUT request was fulfilled and a new r	esource has been created. Information about	the resource is in the response boo	ly.
202	The request was accepted for processing, but the	e processing has not been completed.		
204	The request was successful, however no content	was returned.		
206	The GET request included a Range Header, and	the server responded with the partial content	matching the range.	
490	The client made a request that the server could r	ot understand (for example, the request synta	ax is incorrect).	
401	The client's authentication credentials included w	ith the request are missing or invalid.		
403	The server recognizes the authentication creden	ials, but the client is not authorized to perform	this request.	
484	The client made a request for a resource that do	es not exist.		
500	The server could not fulfill the request.			
501	The server has not implemented the functionality	required to fulfill the request.		
503	The server is (temporarily) unavailable.			
504	The server did not respond inside time restriction	s and timed-out.		
489	The target resource is in a conflicted state (for ex	ample, an edit conflict where a resource is bei	ng edited by multiple users). Retryir	ng the request later might succeed.
415	The client sent a request body in a format that th	e server does not support (for example, XML t	o a server that only accepts JSON	

成功応答メッセージ:

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	

```
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#

APIC-EM には証明書があっても、デバイスにはない場合があり ます。これを解決するには、どうすればよいですか。

1 APIC-EM APIC-EM [DELETE]

DELETE/trust-point/serial-number/{serialNumber} - 削除。

GET	/trust-point/count	pkiTrustPointListGet
GET	/trust-point/pkcs12/{trustPointid}//{token}	pHTrustPointPkcs12Download
00.57	/trust-point/serial-number/(serialNumber)	pkiTrustPointDeleteByDeviceSN
GET	/trust-point/serial-number/(serialNumber)	pluTrustPointGetByDeviceSN
Resoo	ense Class	
Respo	inse Class	
PkiTrus versi respo	stPointResult { ion (string, optional), onse (PkiTrustPoint, optional)	

[Try it out!]

Parameters					
Parameter	Value	Description	Parameter Type	Data Type	
serialNumber	SSI161908CX	Device serial-number	path	string	
Error Status Co	odes				
HTTP Status Code	Reason				
200	The request was successful. The result	s contained in the response body.			
204	The request was successful, however n	o content was returned.			
206	The GET request included a Range He	der, and the server responded with the partial content mate	ching the range.		
400	The client made a request that the serv	er could not understand (for example, the request syntax is	incorrect).		
401	The client's authentication credentials in	cluded with the request are missing or invalid.			
403	The server recognizes the authenticatio	n credentials, but the client is not authorized to perform this	request.		
484	The client made a request for a resource	that does not exist.			
500	The server could not fulfill the request.				
501	The server has not implemented the fur	ctionality required to fulfill the request.			
503	The server is (temporarily) unavailable.				

504	The server did not respond inside time restrictions and timed-out.
409	The target resource is in a conflicted state (for example, an edit conflict where a resource is being edited by multiple users). Retrying the request later might succeed.
415 Try jt out!	The client sent a request body in a format that the server does not support (for example, XML to a server that only accepts JSON).

<pre>{ "response": { "taskId": "33ab0da8- "url": "/api/v1/task }, "version": "1.0" }</pre>	9be1-40b7-86c2-cf2e501ebbb5", /33ab0da8-9be1-40b7-86c2-cf2e501ebbb5"
Response Code	
Response Headers	
<pre>{ "Pragma": "no-cache, no "Content-Security-Polic "X-Frame-Options": "SAM "Date": "Tue, 28 Mar 20 "Strict-Transport-Secur "Content-Type": "applic "Access-Control-Allow-O "Cache-Control": "no-ca "Transfer-Encoding": "c "Access-Control-Allow-C }</pre>	-cache", y": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-f59e75bb-2a28-4fe8-a95 EORIGIN, SAMEORIGIN", 17 10:15:23 GMT", ity": "max-age=31536000; includeSubDomains, max-age=31536000; includeSubDomains", ation/json;charset=UTF-8", rigin": "https://10.78.106.45", che, no-store, no-store", hunked", redentials": "false"