配置ASA作为使用多份证书基于验证的AnyConnect客户端的SSL网关

目录

简介

本文描述如何配置可适应安全工具(ASA)作为使用多份证书基于验证Cisco AnyConnect安全移动客户端的安全套接字协议层(SSL)网关。

贡献用Shakti库马尔和Dhruv Goel， Cisco TAC工程师

先决条件

要求

Cisco 建议您了解以下主题：

- ASA CLI配置和SSL VPN配置基础知识
- X509证书基础知识

使用的组件

本文档中的信息基于以下软件版本：

- Cisco可适应安全工具(ASA)软件，版本9.7(1)和以上
- 与Cisco AnyConnect安全移动客户端4.4的Windows 10

  Note:请从 Cisco 软件下载中下载 AnyConnect VPN Client 程序包 (anyconnect-win*.pkg)（仅限注册用户）。将 AnyConnect VPN Client 复制到 ASA 的闪存中以供远程用户计算机下载，以便建立与 ASA 的 SSL VPN 连接。有关 ASA 配置指南的详细信息，请参阅安装 AnyConnect 客户端部分。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

在软件版本9.7(1)之前， ASA支持单个证书根据验证，含义用户或计算机可以验证，但是不是两个，单个连接尝试的。

多份证书基于验证给能力安排ASA验证计算机除验证用户的身份证书之外允许VPN访问，或设备证书，保证设备是一个公司发出的设备。

限制

- 多份证书验证当前限制证书编号到正确地两。
- AnyConnect客户端必须指示多份证书验证的支持。如果那不是实际情形网关然后使用其中一传统认证方法或请出故障连接。AnyConnect版本4.4.04030或以上支持多证书基于验证。
- 对于Windows平台，机器认证发送在聚集验证协议下的用户证书跟随的最初的SSL握手期间。不支持从Windows机器存储的两证书。
- 在意味着的XML配置文件下的多份证书验证忽略**Enable (event)自动证书Selectio**首选客户端设法所有组合验证两证书，直到发生故障。当Anyconnect设法连接时，这可能引入严重的延迟。因此，推荐给匹配在多个用户/机器认证的情况下使用身份验证在客户端机器。
- Anyconnect仅SSL VPN支持RSA根据证书。
- 在聚集验证期间，仅SHA256、SHA384和SHA512基于证书支持。

在Windows v/s非Windows平台的证书选择

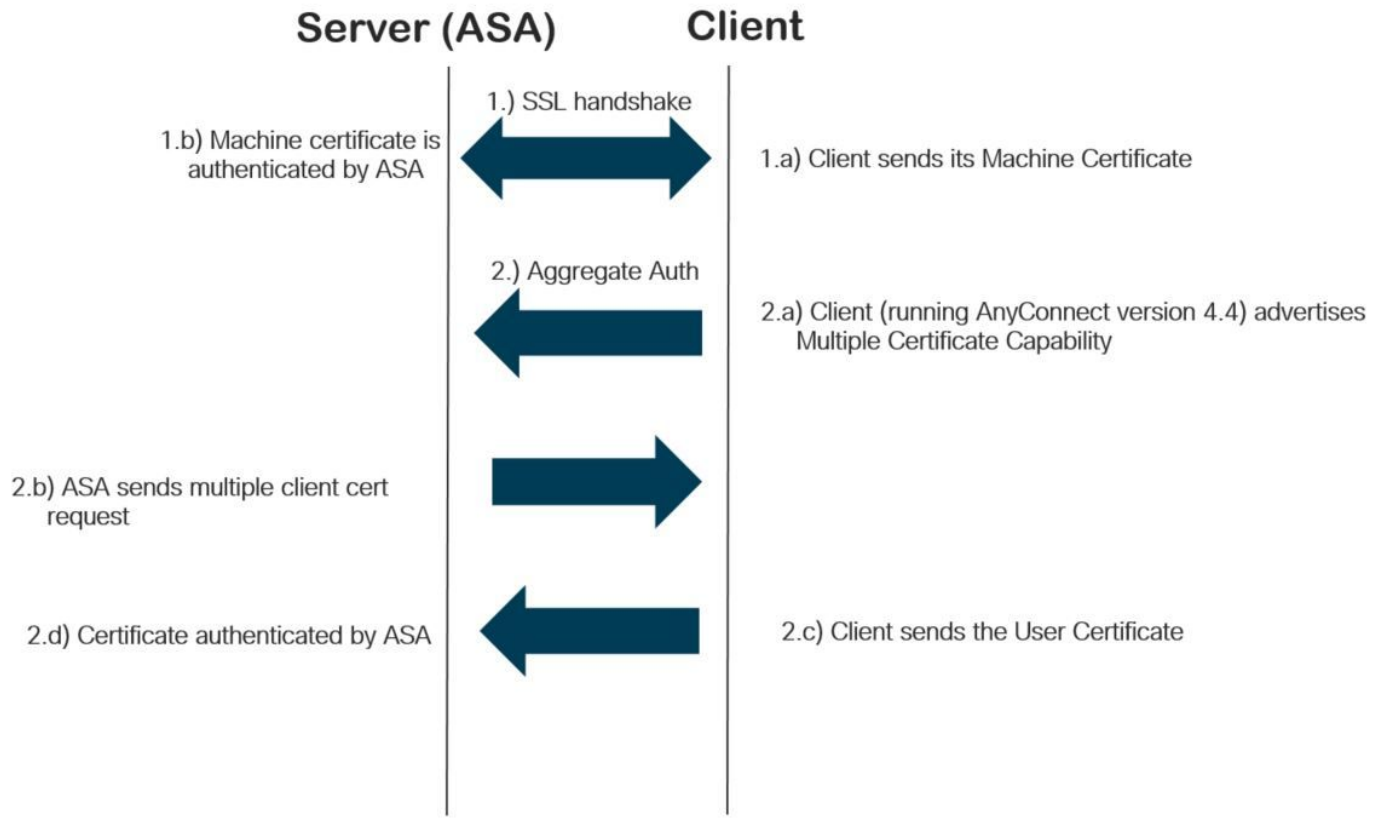
在Windows的AnyConnect区分在从计算机存储(仅可访问由特权进程)和用户存储获取的证书之间(仅可访问由登录用户拥有的进程)。 这样差异没有由AnyConnect做在非Windows平台。

ASA可能选择强制执行连接策略，配置由ASA管理员，根据接收的证书的实际类型。 对于Windows，类型可以是：

- 一计算机和一个用户或者
- 两用户。

对于非Windows平台，征兆总是两个用户证书。

多份证书验证的连接流



配置

通过ASDM配置多份证书验证

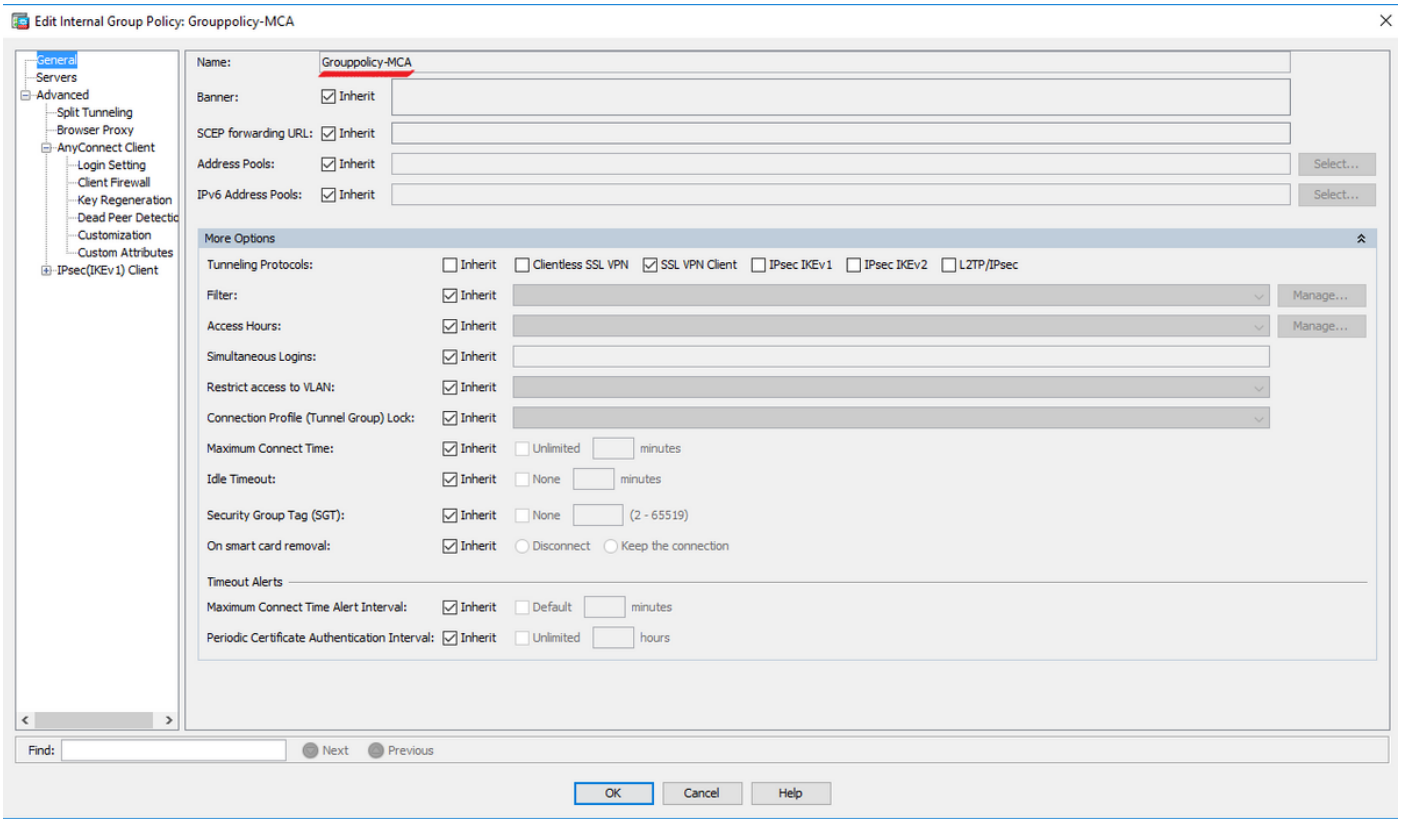
此部分描述如何配置思科ASA作为AnyConnect客户端的SSL网关有证书验证的。

通过ASDM完成这些步骤设置证书验证的Anyconnect客户端：

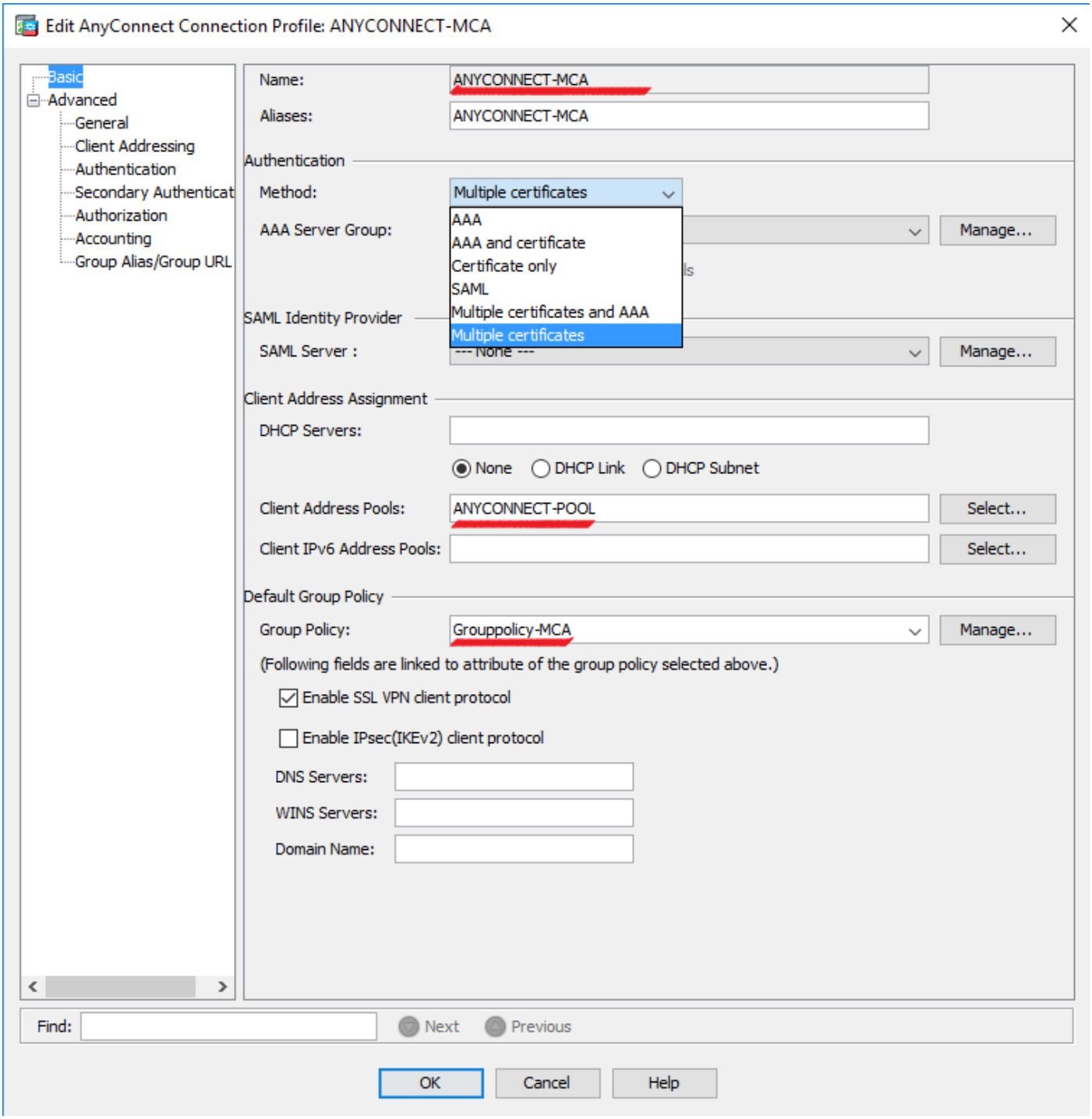
步骤1.用户和机器认证的安装CA证书在ASA。

对于参考的证书的安装请配置ASA ：SSL数字证书安装和续订

步骤2.导航对**Configuration>远程访问>组策略**并且配置组政策。



步骤3.配置新连接配置文件并且选择**认证方法**作为多份证书并且选择在step1创建的组政策。



第四步：对于其他详细配置，请参考toVPN客户端和AnyConnect访客接入对本地LAN配置示例

通过CLI配置多份证书验证的ASA

Note:使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

```
ASA Version 9.7(1)
!
hostname GCE-ASA
!
! Configure the VPN Pool
ip local pool ANYCONNECT-POOL 192.168.100.1-192.168.100.254 mask 255.255.255.0
```

```
!
interface GigabitEthernet0/0
nameif outside
security-level 100
ip address 10.197.223.81 255.255.254.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
! Configure Objects
object network obj-AnyConnect_pool
subnet 192.168.100.0 255.255.255.0
object network obj-Local_Lan
subnet 192.168.1.0 255.255.255.0
!
! Configure Split-tunnel access-list
access-list split standard permit 192.168.1.0 255.255.255.0
!
! Configure Nat-Exemption for VPN traffic
nat (inside,outside) source static obj-Local_Lan obj-Local_Lan destination static obj-
AnyConnect_pool obj-AnyConnect_pool no-proxy-arp route-lookup
!
! TrustPoint for User CA certificate
crypto ca trustpoint UserCA
enrollment terminal
crl configure
!
! Trustpoint for Machine CA certificate
crypto ca trustpoint MachineCA
enrollment terminal
crl configure
!
!
crypto ca certificate chain UserCA
certificate ca 00ea473dc301c2fdc7
30820385 3082026d a0030201 02020900 ea473dc3 01c2fdc7 300d0609 2a864886
<snip>
3d57bea7 3e30c8f0 f391bab4 855562fd 8e21891f 4acb6a46 281af1f2 20eb0592
012d7d99 e87f6742 d5
quit


crypto ca certificate chain MachineCA
certificate ca 00ba27b1f331aea6fc
30820399 30820281 a0030201 02020900 ba27b1f3 31aea6fc 300d0609 2a864886
f70d0101 0b050030 63310b30 09060355 04061302 494e3112 30100603 5504080c
<snip>
2c214c7a 79eb8651 6ad1eabd ae1ffbba d0750f3e 81ce5132 b5546f93 2c0d6ccf
606add30 2a73b927 7f4a73e5 2451a385 d9a96b50 6ebeba66 fc2e496b fa
quit
!
! Enable AnyConnect
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.4.00243-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
!
! Configure Group-Policy
group-policy Grouppolicy-MCA internal
group-policy Grouppolicy-MCA attributes
vpn-tunnel-protocol ssl-client
```

```
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
!
! Configure Tunnel-Group
tunnel-group ANYCONNECT-MCA type remote-access
tunnel-group ANYCONNECT-MCA general-attributes
address-pool ANYCONNECT-POOL
default-group-policy Grouppolicy-MCA
tunnel-group ANYCONNECT-MCA webvpn-attributes
authentication multiple-certificate
group-alias ANYCONNECT-MCA enable
group-url https://10.197.223.81/MCA enable
```

验证

使用本部分可确认配置能否正常运行。

> **Note**:命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

通过CLI查看在ASA的已安装证书

show crypto ca certificate

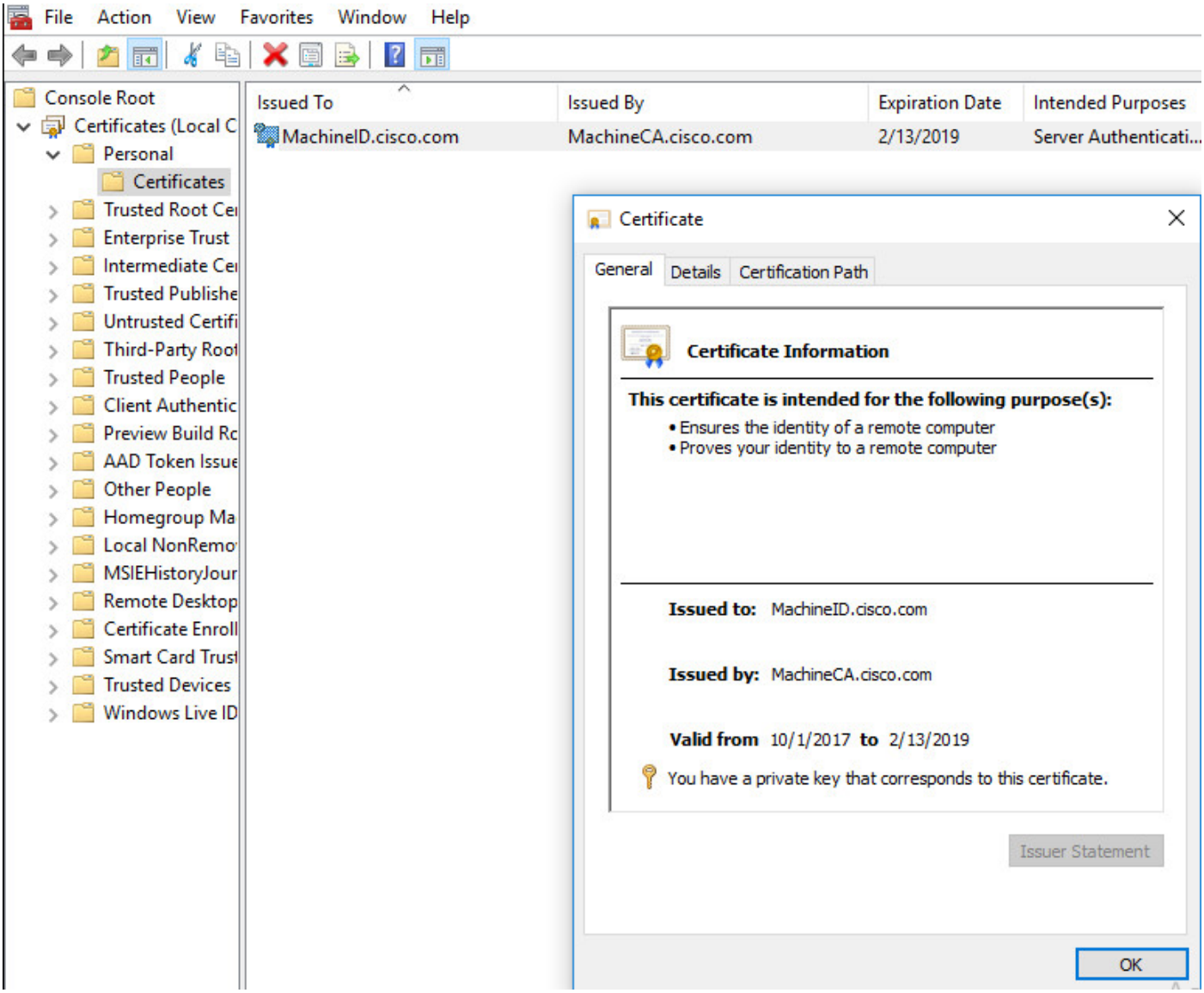
```
GCE-ASA(config)# show crypto ca certificate

CA Certificate

Status: Available
Certificate Serial Number: 00ea473dc301c2fdc7
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
cn=UserCA.cisco.com
o=Cisco
l=Dallas
st=Texas
c=IN
Subject Name:
cn=UserCA.cisco.com
o=Cisco
l=Dallas
st=Texas
c=IN
Validity Date:
start date: 15:40:28 UTC Sep 30 2017
enddate: 15:40:28 UTC Jul202020
Storage: config
Associated Trustpoints: UserCA


CA Certificate

Status: Available
```

```
Certificate Serial Number: 00ba27b1f331aea6fc
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
cn=MachineCA.cisco.com
o=Cisco
l=Bangalore
st=Karnataka
c=IN
Subject Name:
cn=MachineCA.cisco.com
o=Cisco
l=Bangalore
st=Karnataka
c=IN
Validity Date:
start date: 15:29:23 UTC Sep 30 2017
enddate: 15:29:23 UTC Jul202020
Storage: config
Associated Trustpoints: MachineCA
```

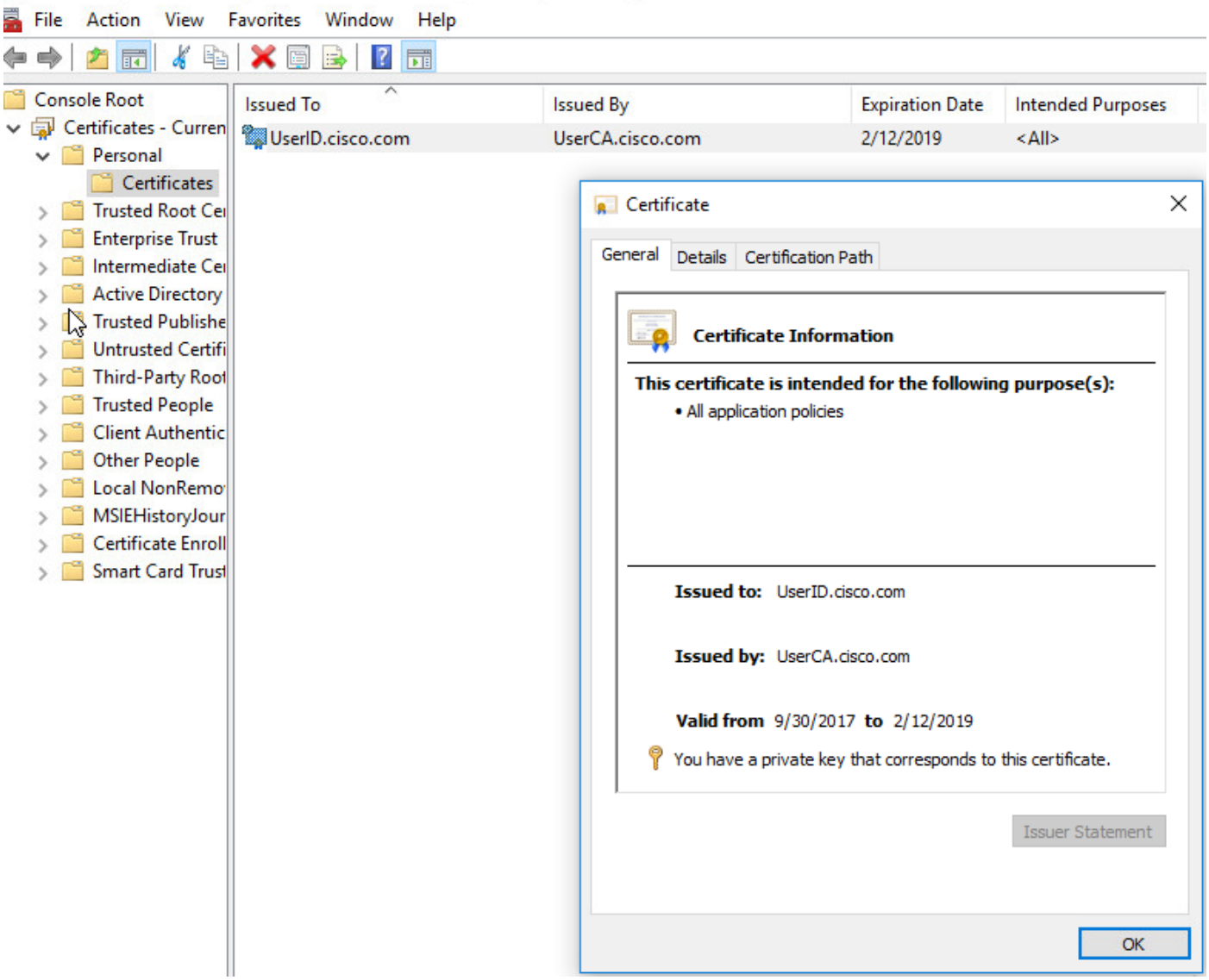
查看在客户端的已安装证书

为了验证安装，请使用认证管理器(certmgr.msc) ：

机器认证


File Action View Favorites Window Help
Console Root
Certificates (Local C
Personal
Certificates
Trusted Root Cer
Enterprise Trust
Intermediate Cer
Trusted Publishe
Untrusted Certifi
Third-Party Root
Trusted People
Client Authentic
Preview Build Rc
AAD Token Issue
Other People
Homegroup Ma
Local NonRemo
MSIEHistoryJour
Remote Desktop
Certificate Enroll
Smart Card Trust
Trusted Devices
Windows Live ID
Issued To
Issued By
Expiration Date
Intended Purposes
MachineID.cisco.com
MachineCA.cisco.com
2/13/2019
Server Authenticati...
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
Issued to: MachineID.cisco.com
Issued by: MachineCA.cisco.com
Valid from 10/1/2017 to 2/13/2019
You have a private key that corresponds to this certificate.
Issuer Statement
OK

用户证书



执行此命令验证连接：

```
GCE-ASA# sh vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : MachineID.cisco.com Index : 296
Assigned IP : 192.168.100.1 Public IP : 10.197.223.235
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES128 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11542 Bytes Rx : 2097
Pkts Tx : 8 Pkts Rx : 29
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : Grouppolicy-MCA Tunnel Group : ANYCONNECT-MCA
Login Time : 22:26:27 UTC Sun Oct 1 2017
Duration : 0h:00m:21s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0ac5df510012800059d16b93
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 296.1
Public IP : 10.197.223.235
Encryption : none Hashing : none
TCP Src Port : 51609 TCP Dst Port : 443
Auth Mode : Multiple-certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.14393
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.4.01054
Bytes Tx : 5771 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 296.2
Assigned IP : 192.168.100.1 Public IP : 10.197.223.235
Encryption : AES128 Hashing : SHA1
Ciphersuite : AES128-SHA
Encapsulation: TLSv1.2 TCP Src Port : 51612
TCP Dst Port : 443 Auth Mode : Multiple-certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.4.01054
Bytes Tx : 5771 Bytes Rx : 446
Pkts Tx : 4 Pkts Rx : 5
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 296.3
Assigned IP : 192.168.100.1 Public IP : 10.197.223.235
Encryption : AES256 Hashing : SHA1
Ciphersuite : AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 63385
UDP Dst Port : 443 Auth Mode : Multiple-certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.4.01054
Bytes Tx : 0 Bytes Rx : 1651
Pkts Tx : 0 Pkts Rx : 24
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

故障排除

此部分提供您能使用为了排除故障您的配置的信息。

> **Note**:使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。
>
> **Caution**:在ASA，您能设置多种调试级别;默认情况下，使用1级。如果改变调试级别，调试的冗余也许增加。执行此小心地，特别是在生产环境。

- **Debug crypto ca消息127**

- Debug crypto ca处理127

```
CRYPTO_PKI: Begin sorted cert chain
---------Certificate--------:
Serial:  00B6D609E1D68B9334
Subject: cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN
Issuer:  cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN

CRYPTO_PKI: End sorted cert chain
CRYPTO_PKI: Cert chain pre-processing: List size is 1, trustpool is not in use
CRYPTO_PKI: List pruning is not necessary.
CRYPTO_PKI: Sorted chain size is: 1
CRYPTO_PKI: Found ID cert. serial number: 00B6D609E1D68B9334, subject name:
cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN
CRYPTO_PKI: Verifying certificate with serial number: 00B6D609E1D68B9334, subject name:
cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN, issuer_name:
cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN, signature alg: SHA256/RSA.

CRYPTO_PKI(Cert Lookup) issuer="cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN"
serial number=00 b6 d6 09 e1 d6 8b 93 34                          |  ........4

CRYPTO_PKI: valid cert with warning.

CRYPTO_PKI: valid cert status.

CRYPTO_PKI: Begin sorted cert chain
---------Certificate--------:
Serial:  00B6D609E1D68B9334
Subject: cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN
Issuer:  cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN

CRYPTO_PKI: End sorted cert chain
CRYPTO_PKI: Cert chain pre-processing: List size is 1, trustpool is not in use
CRYPTO_PKI: List pruning is not necessary.
CRYPTO_PKI: Sorted chain size is: 1
CRYPTO_PKI: Found ID cert. serial number: 00B6D609E1D68B9334, subject name:
cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN
CRYPTO_PKI: Verifying certificate with serial number: 00B6D609E1D68B9334, subject name:
cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN, issuer_name:
cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN, signature alg: SHA256/RSA.

CRYPTO_PKI(Cert Lookup) issuer="cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN"
serial number=00 b6 d6 09 e1 d6 8b 93 34                          |  ........4

CRYPTO_PKI: valid cert with warning.

CRYPTO_PKI: valid cert status.

CRYPTO_PKI: Begin sorted cert chain
---------Certificate--------:
Serial:  00A5A42E24A345E11A
Subject: cn=UserID.cisco.com,ou=TAC,o=Cisco,l=Dallas,st=Texas,c=IN
Issuer:  cn=UserCA.cisco.com,o=Cisco,l=Dallas,st=Texas,c=IN

CRYPTO_PKI: End sorted cert chain
CRYPTO_PKI: Cert chain pre-processing: List size is 1, trustpool is not in use
CRYPTO_PKI: List pruning is not necessary.
CRYPTO_PKI: Sorted chain size is: 1
CRYPTO_PKI: Found ID cert. serial number: 00A5A42E24A345E11A, subject name:
cn=UserID.cisco.com,ou=TAC,o=Cisco,l=Dallas,st=Texas,c=IN
CRYPTO_PKI: Verifying certificate with serial number: 00A5A42E24A345E11A, subject name:
cn=UserID.cisco.com,ou=TAC,o=Cisco,l=Dallas,st=Texas,c=IN, issuer_name:
```

```
cn=UserCA.cisco.com,o=Cisco,l=Dallas,st=Texas,c=IN, signature alg: SHA256/RSA.

CRYPTO_PKI(Cert Lookup) issuer="cn=UserCA.cisco.com,o=Cisco,l=Dallas,st=Texas,c=IN" serial
number=00 a5 a4 2e 24 a3 45 e1 1a                          |  ....$.E..

CRYPTO_PKI: valid cert with warning.

CRYPTO_PKI: valid cert status.
```

- **调试聚合验证xml 127**

```
Received XML message below from the client <?xml version="1.0" encoding="UTF-8"?> <config-auth
client="vpn" type="init" aggregate-auth-version="2">
<version who="vpn">4.4.01054</version>
<device-id device-type="VMware, Inc. VMware Virtual Platform" platform-version="10.0.14393
#snip#  win</device-id>
<mac-address-list>
<mac-address>00-0c-29-e4-f5-bd</mac-address></mac-address-list>
<group-select>ANYCONNECT-MCA</group-select>
<group-access>https://10.197.223.81/MCA</group-access>
<capabilities>
<auth-method>single-sign-on</auth-method>
<auth-method>multiple-cert</auth-method></capabilities>
</config-auth>

Generated XML message below
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="auth-request" aggregate-auth-version="2">
<opaque is-for="sg">
<tunnel-group>ANYCONNECT-MCA</tunnel-group>
<aggauth-handle>136775778</aggauth-handle>
<auth-method>multiple-cert</auth-method>
<auth-method>single-sign-on</auth-method>
<config-hash>1506879881148</config-hash>
</opaque>
<multiple-client-cert-request>
<hash-algorithm>sha256</hash-algorithm>
<hash-algorithm>sha384</hash-algorithm>
<hash-algorithm>sha512</hash-algorithm>
</multiple-client-cert-request>
<random>FA4003BD87436B227####snip####C138A08FF724F0100015B863F750914839EE79C86DFE8F0B9A0199E2</r
andom>
</config-auth>

Received XML message below from the client
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="auth-reply" aggregate-auth-version="2">
<version who="vpn">4.4.01054</version>
<device-id device-type="VMware, Inc. VMware Virtual Platform" platform-version="10.0.14393
##snip## win</device-id>
<mac-address-list>
<mac-address>00-0c-29-e4-f5-bd</mac-address></mac-address-list>
<session-token></session-token>
<session-id></session-id>
<opaque is-for="sg">

<tunnel-group>ANYCONNECT-MCA</tunnel-group>
<aggauth-handle>608423386</aggauth-handle>
<auth-method>multiple-cert</auth-method>
<auth-method>single-sign-on</auth-method>
<config-hash>1506879881148</config-hash></opaque>
<auth>
```

```
<client-cert-chain cert-store="1M">
<client-cert-sent-via-protocol></client-cert-sent-via-protocol></client-cert-chain>
<client-cert-chain cert-store="1U">
<client-cert cert-format="pkcs7">MIIG+AYJKoZIhvcNAQcCoIIG6TCCBuU
yTCCAzwwggIkAgkApaQuJKNF4RowDQYJKoZIhvcNAQELBQAwWTELMAkGA1UEBhMC
#Snip#
gSCx8Luo9V76nPjDI8PORurSFVWL9jiGJH0rLakYoGv
</client-cert>
<client-cert-auth-signature hash-algorithm-
chosen="sha512">FIYur1Dzb4VPThVZtYwxSsCVRBUin/8MwWK+G5u2Phr4fJ
#snip#
EYt4G2hQ4hySySYqD4L4iV91uCT5b5Bmr5HZmSqKehg0zrDBjqxx7CLMSf2pSmQnjMwi6D0ygT=</client-cert-auth-
signature>
</client-cert-chain>
</auth>
</config-auth>
Received attribute hash-algorithm-chosen in XML message from client
Base64 Signature (len=349):
FIYur1Dzb4VPThVZtYwxSsCVRBUin/8MwWK+G5u2Phr4fJI9aWFqd1BbV9WhSTsF
EYt4G2hQ4hySySYqD4L4iV91uCT5b5Bmr5HZmSqKehg0zrDBjqxx7CLMSf2pSmQn
ABXv++cN7lNWGHK91EAvNRcpCX4TdZ+6ZKpL4sClu8vZJeW2jwGmPnYesG3sttrS
TFBRqg74+1TFSbUuIEzn8MLXZqHbOnA19B9gyXZJon8eh3Z7cDspFiR0xKBu8iYH
L+ES84UNtDQjatIN4EiS8SD/5QPAunCyvAUBvK5FZ4c4TpnF6MIEPhjMwi6D0ygT
sm2218mstLDNKBouaTjB3A==
Successful Base64 signature decode, len 256
Loading cert into PKI
Waiting for certificate validation result
Verifying signature
Successfully verified signature
```

- **调试聚合验证ssl 127**

```
/CSCOSSLC/config-auth
Processing client request
XML successfully parsed
Processing request (init)
INIT-no-cert: Client has not sent a certificate
Found TG ANYCONNECT-MCA by URL https://10.197.223.81/MCA
INIT-no-cert: Resolve tunnel group (ANYCONNECT-MCA) alias (NULL) Cert or URL mapped YES
INIT-no-cert: Client advertised multi-cert authentication support
[332565382] Created auth info for client 10.197.223.235
[332565382] Started timer (3 mins) for auth info for client 10.197.223.235
INIT-no-cert: Tunnel group ANYCONNECT-MCA requires multi-cert authentication
[332565382] Generating multiple certificate request
[332565382] Saved message of len 699 to verify signature
rcode from handler = 0
Sending response
/CSCOSSLC/config-auth
Processing client request
XML successfully parsed
Processing request (init)
INIT-cert: Client has certificate, groupSelect ANYCONNECT-MCA
Found TG ANYCONNECT-MCA by URL https://10.197.223.81/MCA
INIT-cert: Found tunnel group (ANYCONNECT-MCA) alias (NULL) url or certmap YES
INIT-cert: Client advertised multi-cert authentication support
[462466710] Created auth info for client 10.197.223.235
[462466710] Started timer (3 mins) for auth info for client 10.197.223.235
INIT-cert: Tunnel group ANYCONNECT-MCA requires multi-cert authentication
Resetting FCADB entry
[462466710] Generating multiple certificate request
[462466710] Saved message of len 741 to verify signature
rcode from handler = 0
Sending response
```

```
/CSCOSSLC/config-auth
Processing client request
XML successfully parsed
Processing request (auth-reply)
auth-reply:[462466710] searching for authinfo
[462466710] Found auth info for client 10.197.223.235, update expire timer (3 mins)
Found tunnel group (ANYCONNECT-MCA) alias ANYCONNECT-MCA
[462466710] Multi cert authentication
[462466710] First cert came in SSL protocol, len 891
[462466710] Success loading cert into PKI
[462466710] Authenticating second cert
[462466710] Sending Message AGGAUTH_MSG_ATHENTICATE_CERT(1)
[462466710] Fiber waiting
Aggauth Message handler received message AGGAUTH_MSG_ATHENTICATE_CERT
[462466710] Process certificate authentication request
[462466710] Waiting for async certificate verification
[462466710] Verify cert callback
[462466710] Certificate Authentication success - verifying signature
[462466710] Signature verify success
[462466710] Signalling fiber
[462466710] Fiber continuing
[462466710] Found auth info
[462466710] Resolved tunnel group (ANYCONNECT-MCA), Cert or URL mapped YES
Resetting FCADB entry
Attempting cert only login
Authorization username = MachineID.cisco.com
Opened AAA handle 335892526
Making AAA request
AAA request finished
Send auth complete
rcode from handler = 0
Sending response
Closing AAA handle 335892526
[462466710] Destroy auth info for 10.197.223.235
[462466710] Free auth info for 10.197.223.235
```

相关信息

- 思科ASA系列的版本注释， 9.7(x)
- Cisco AnyConnect安全移动客户端管理员指南，版本4.4
- AnyConnect VPN客户端故障排除指南-常见问题
- 技术支持和文档