使用COOP金鑰伺服器和證書身份驗證配置GETVPN

目錄

簡介

本文檔介紹如何將組加密傳輸VPN(GETVPN)配置為使用數位證書進行身份驗證和COOP金鑰伺服器。

必要條件

需求

思科建議您瞭解以下主題：

— 群組加密傳輸VPN(GETVPN)

— 公開金鑰基礎架構(PKI)

— 證書頒發機構(CA)

採用元件

本檔案中的資訊是根據以下軟體版本：

- CSR1000V - Cisco IOS® XE版本16.12.03 - Cisco IOS® XE金鑰伺服器、組成員和CA伺服器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

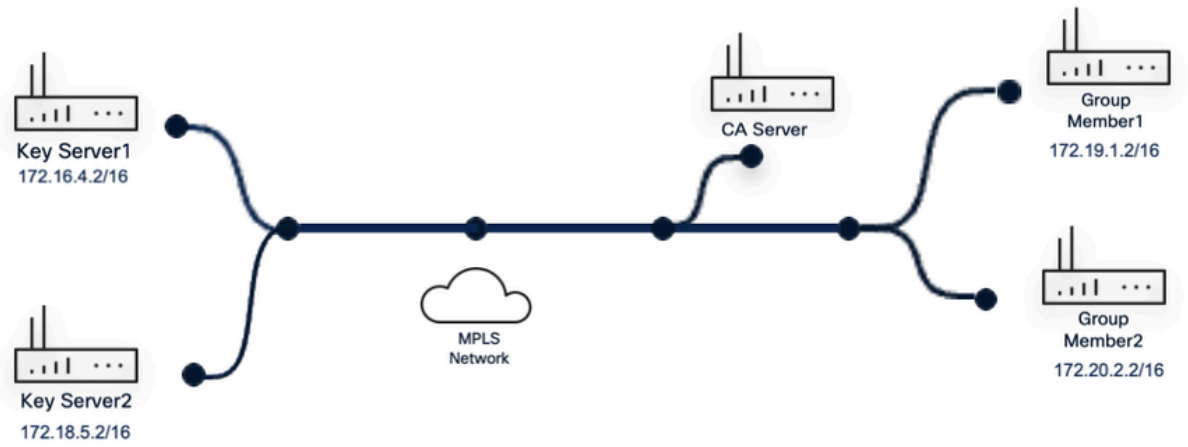
背景資訊

在GETVPN部署中，金鑰伺服器是最重要的實體，因為KS維護了控制平面。使用單個裝置管理完整的GETVPN組，會建立單點故障。

為了緩解此情況，GETVPN支援多個稱為合作(COOP)KS的金鑰伺服器，這些金鑰伺服器在金鑰伺服器不可達時提供冗餘和恢復。

設定

網路圖表



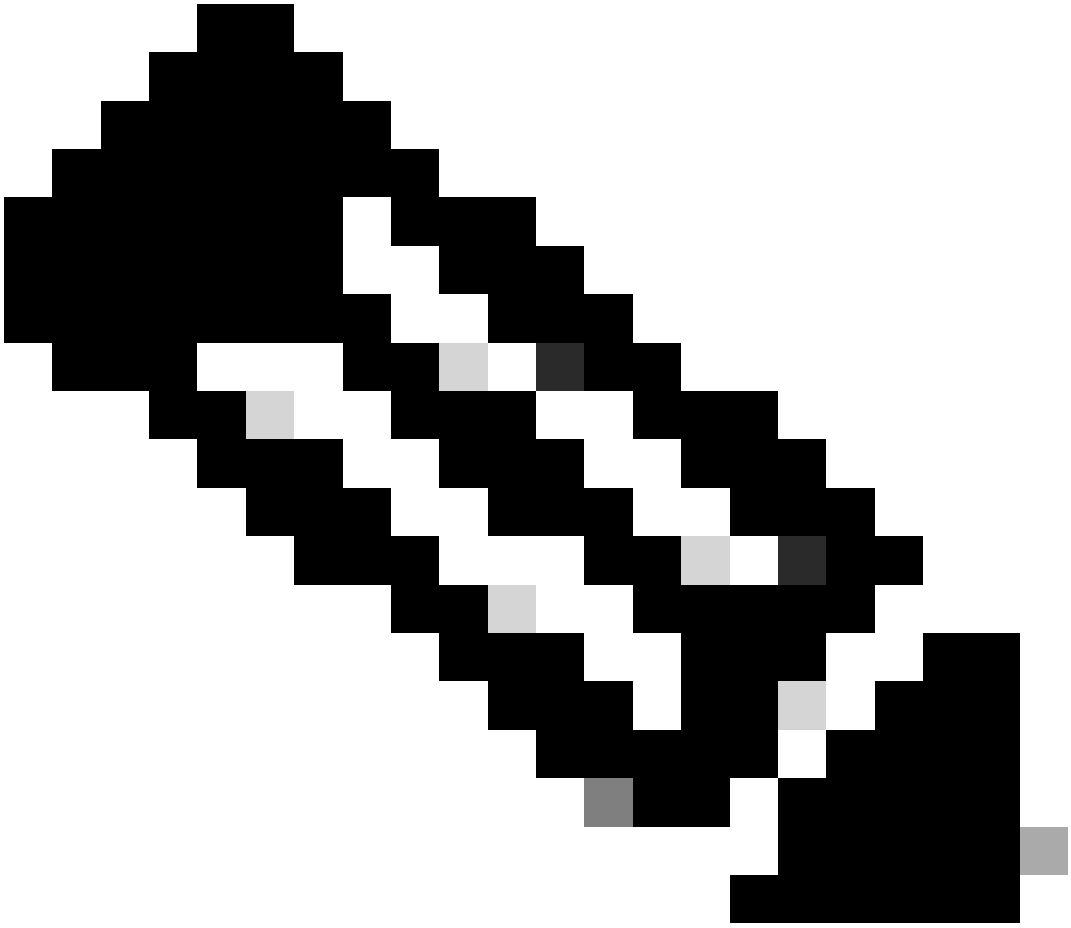
GETVPN拓撲

組態

用於身份驗證的PKI

PKI使用其基礎設施來克服使用PSK時遇到的金鑰管理困難。PKI基礎設施充當頒發（然後維護）身份證書的證書頒發機構(CA)。

其證書資訊與ISAKMP標識匹配的任何組成員路由器都經過授權，可以註冊到KS。



附註：證書可由任何CA頒發。在本指南中，CSR1000V被配置為CA，以向部署中的所有裝置頒發證書以驗證其身份。

CA# show crypto pki server

crypto pki server ca-server

資料庫級別完成

database archive pkcs12 password 7 1511021F07257A767B73

issuer-name CN=Root-CA.cisco.com OU=LAB

grant auto hash sha255

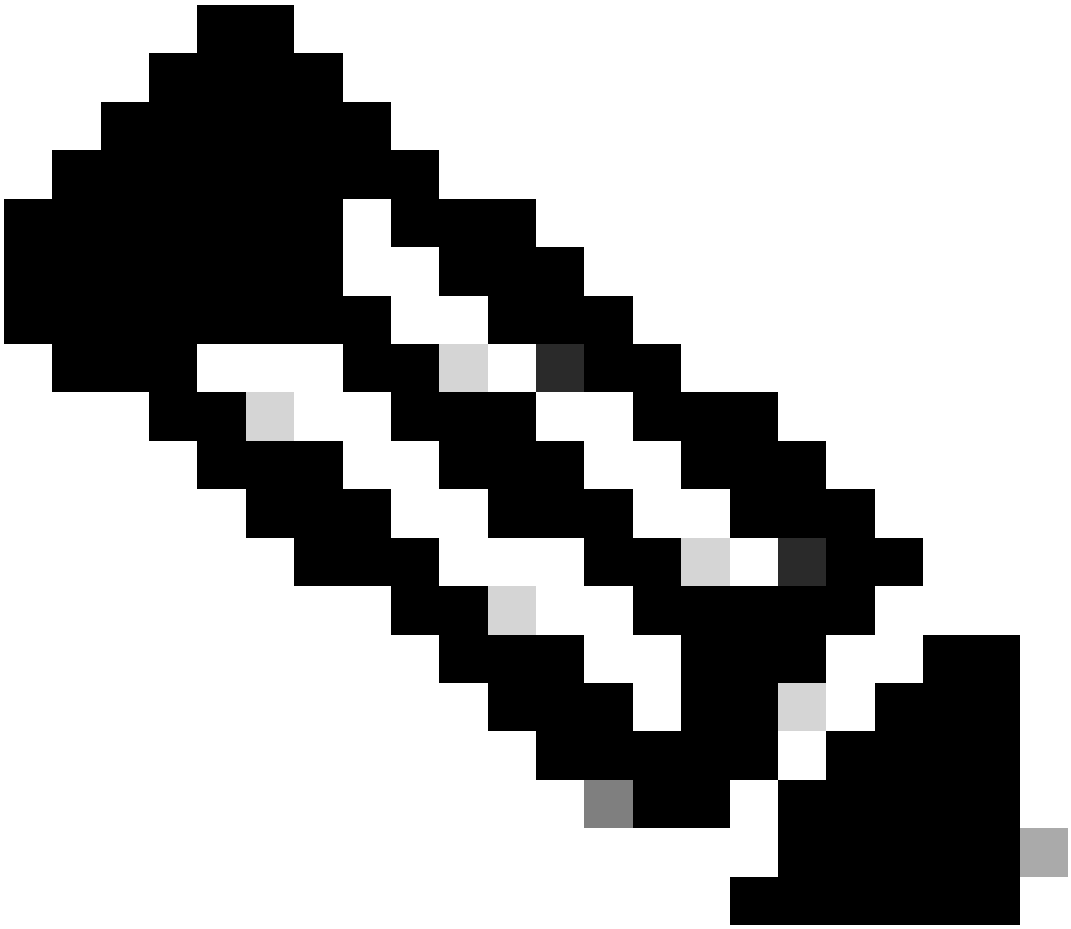
有效期證書5000

lifetime ca-certificate 7300

eku server-auth client-auth

資料庫url nvram

1. — 在基於PKI的部署中，必須獲得來自每個裝置的證書頒發機構(CA)的身份證書。在金鑰伺服器和組成員路由器中，建立用於其信任點配置的RSA金鑰對。



附註：為了演示本指南，此拓撲中的所有關鍵伺服器和組成員路由器共用相同的配置。

金鑰伺服器

KS(config)# **crypto key generate rsa modulus 2049 general-keys label pkikey** The name for the keys will be: **pkikey** % The key modulus size is 2049 bits % Generating 2049 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 0 seconds) KS(config)# **crypto pki trustpoint GETVPN** KS(config)# **enrollment url http://10.191.61.120:80** KS(config)# **subject-name OU=GETVPN_KS** KS(config)# **revocation-check none** KS(config)# **rsakeypair pkikey** KS(config)# **auto-enroll 70**

組成員

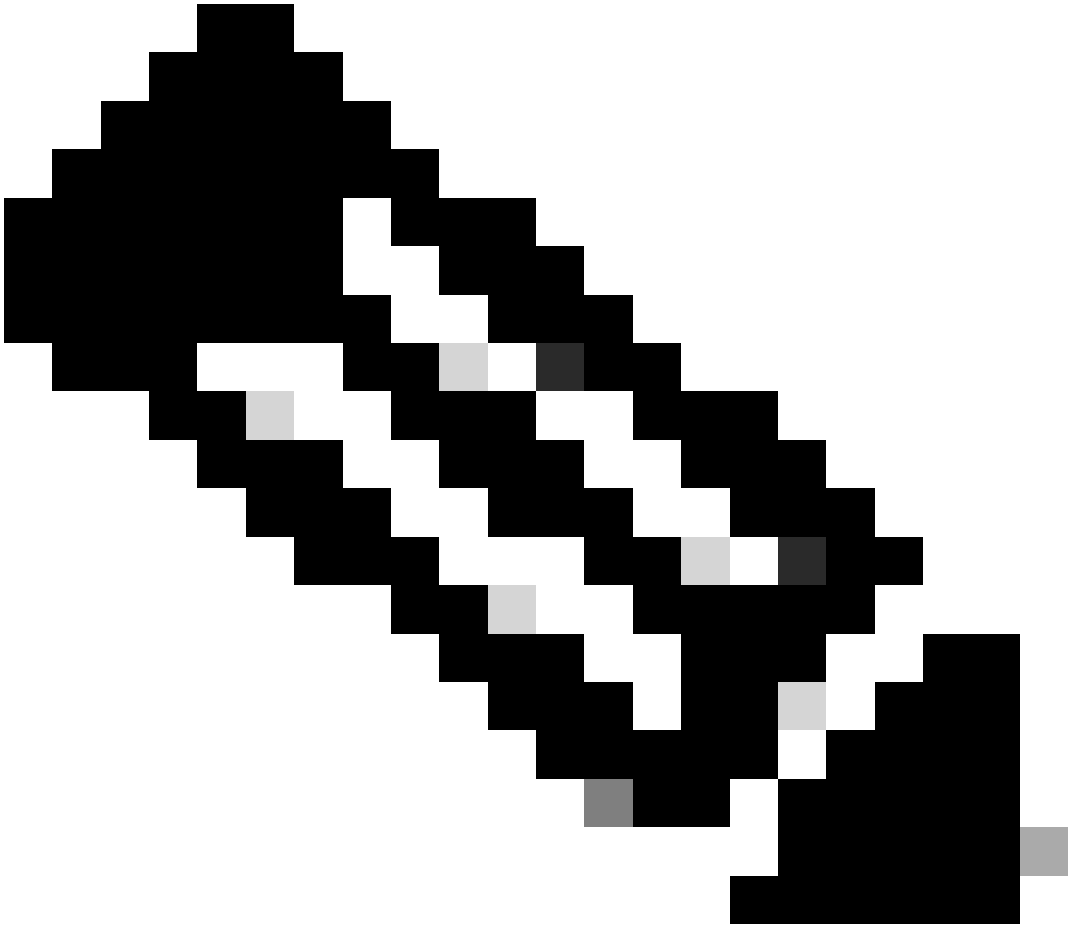
GM(config)# **crypto key generate rsa modulus 2049 general-keys label pkikey** The name for the keys will be: **pkikey** % The key modulus size is 2049 bits % Generating 2049 bit RSA keys, keys are non-exportable... [OK] (elapsed time was 0 seconds) GM(config)# **crypto pki trustpoint GETVPN** GM(ca-trustpoint)# **enrollment url http://10.191.61.120:80**

GM(ca-trustpoint)# **subject-name OU=GETVPN_GM**

GM(ca-trustpoint)# **revocation-check none**

GM(ca-trustpoint)# **rsakeypair pkikey**

GM(ca-trustpoint)# **auto-enroll 70**



附註：RSA金鑰名稱在所有裝置上重複使用以保持一致性，並且不影響其他設定，因為每個RSA金鑰在其計算值中都是唯一的。

---

2. — 必須首先在信任點中安裝CA的證書。這可以通過驗證信任點或直接註冊來完成。由於以前未

安裝CA證書，因此首先觸發信任點身份驗證過程。

金鑰伺服器

KS(config)# **crypto pki enroll GETVPN** % You must authenticate the Certificate Authority before

you can enroll with it. % Attempting authentication first.

Certificate has the following attributes: Fingerprint MD5: CD60821B 034ACFCF D1FD66D3 EA27D688 Fingerprint SHA1: 3F0C3A05 9BC786B4 8828007A 78A3973D B507F9C4 % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted. % Start certificate enrollment .. % Create a challenge password. You need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password is not saved in the configuration. Please make a note of it. Password: Re-enter password: % The subject name in the certificate includes: OU=GETVPN_KS % The subject name in the certificate includes: get-KS % Include the router serial number in the subject name? [yes/no]: no % Include an IP address in the subject name? [no]: no Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority % The 'show crypto pki certificate verbose GETVPN' command will show the fingerprint.

組成員

GM(config)# **crypto pki enroll GETVPN** % You must authenticate the Certificate Authority before

you can enroll with it. % Attempting authentication first.

Certificate has the following attributes: Fingerprint MD5: E184D9EC 2D6499B3 D5D78E8A CD0B910C Fingerprint SHA1: A31EE77D A4FFA2B7 90F39933 00337A6D 46CBE32E

% Do you accept this certificate? [yes/no]: y % Trustpoint CA certificate accepted. % Start certificate enrollment .. % Create a challenge password. You need to verbally provide this

password to the CA Administrator in order to revoke your certificate.

For security reasons your password is not saved in the configuration.

Please make a note of it.

Password:

Re-enter password:

% The subject name in the certificate will include: OU=GETVPN % The subject name in the certificate will include: get_GM % Include the router serial number in the subject name? [yes/no]: n % Include an IP address in the subject name? [no]: n Request certificate from CA? [yes/no]: y % Certificate request sent to Certificate Authority % The 'show crypto pki certificate verbose GETVPN' commandwill show the fingerprint.

3 — 使用show crypto pki certificates verbose命令，在兩台裝置上驗證新頒發的證書是否匯入到其各自的已驗證信任點中（也必須匯入CA證書）。

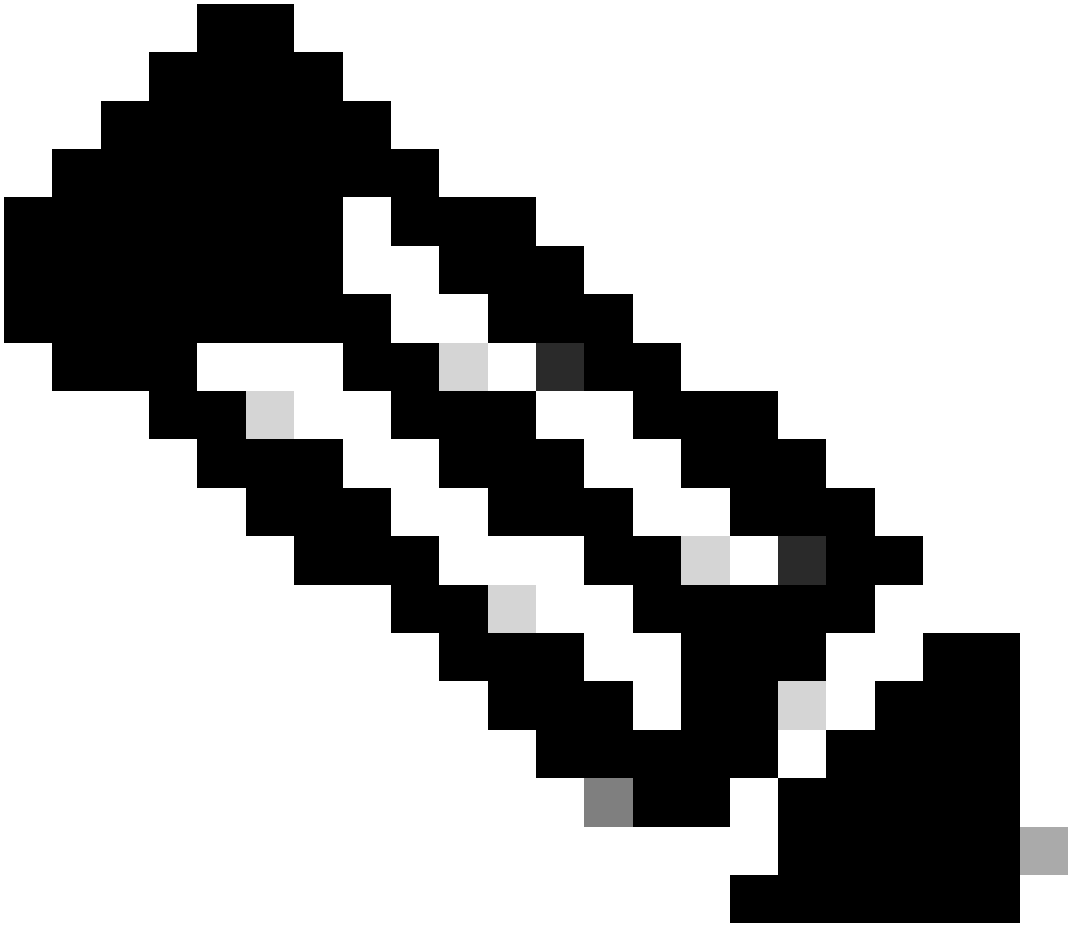
金鑰伺服器

KS# **show crypto pki certificates verbose GETVPN**

. **Certificate** Status: Available Version: 3 Certificate Serial Number (hex): 05 Certificate Usage: General Purpose **Issuer: cn=Root-CA.cisco.com OU=LAB Subject: Name: get-KS** hostname=get-KS ou=GETVPN_KS **Validity Date:** start date: 11:58:27 UTC Sep 9 2025 end date: 11:58:27 UTC May 19 2039 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2049 bit) Signature Algorithm: SHA256 with RSA Encryption Fingerprint MD5: 51576B28 1203C5EC 06FF408E F90B0E47 Fingerprint SHA1: 9D5B10E5 E9418C00 895E6DC7 9BE86624 B273CF15 X509v3 extensions: X509v3 Key Usage: A0000000 Digital Signature Key Encipherment X509v3 Subject Key ID: 3A1012CD 1FB41E07 5B64742B 778B1E24 E1F07A92 X509v3 Authority Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F Authority Info Access: **Extended Key Usage: Client Auth Server Auth** Cert install time: 11:58:28 UTC Sep 9 2025 **Associated Trustpoints: GETVPN** Storage: nvram:Root-CAcisco#5.cer **Key Label: pkikey** Key storage device: private config **CA Certificate** Status: Available Version: 3 Certificate Serial Number (hex): 01 Certificate Usage: Signature **Issuer: cn=Root-CA.cisco.com OU=LAB** Subject: cn=Root-CA.cisco.com OU=LAB **Validity Date:** start date: 11:28:11 UTC Sep 9 2025 end date: 11:28:11 UTC Sep 4 2045 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Signature Algorithm: SHA256 with RSA Encryption Fingerprint MD5: E184D9EC 2D6499B3 D5D78E8A CD0B910C Fingerprint SHA1: A31EE77D A4FFA2B7 90F39933 00337A6D 46CBE32E X509v3 extensions: X509v3 Key Usage: 86000000 Digital Signature Key Cert Sign CRL Signature X509v3 Subject Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F X509v3 Basic Constraints: **CA: TRUE** X509v3 Authority Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F Authority Info Access: Cert install time: 11:58:16 UTC Sep 9 2025 **Associated Trustpoints: GETVPN** Storage: nvram:Root-CAcisco#1CA.cer

組成員

GM# **show crypto pki certificates verbose GETVPN Certificate** Status: Available Version: 3 Certificate Serial Number (hex): 08 Certificate Usage: General Purpose Issuer: cn=Root-CA.cisco.com OU=LAB Subject: Name: get_GM hostname=get_GM ou=GETVPN Validity Date: start date: 12:05:19 UTC Sep 9 2025 end date: 12:05:19 UTC May 19 2039 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2049 bit) Signature Algorithm: SHA256 with RSA Encryption Fingerprint MD5: CA8AF53B B7424CD6 4C94F689 6FDD441F Fingerprint SHA1: 8ACE3BC0 5BC6BBF1 D9696805 2998AFDB 2A73A65E X509v3 extensions: X509v3 Key Usage: A0000000 Digital Signature Key Encipherment X509v3 Subject Key ID: F3C5E024 F93B09A0 4F99215E 34EB9C88 553C7CAD X509v3 Authority Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F Authority Info Access: Extended Key Usage: Client Auth Server Auth Associated Trustpoints: GETVPN Storage: nvram:Root-CAcisco#8.cer Key Label: **pkikey CA Certificate** Status: Available Version: 3 Certificate Serial Number (hex): 01 Certificate Usage: Signature Issuer: cn=Root-CA.cisco.com OU=LAB Subject: cn=Root-CA.cisco.com OU=LAB Validity Date: start date: 11:28:11 UTC Sep 9 2025 end date: 11:28:11 UTC Sep 4 2045 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Signature Algorithm: SHA256 with RSA Encryption Fingerprint MD5: E184D9EC 2D6499B3 D5D78E8A CD0B910C Fingerprint SHA1: A31EE77D A4FFA2B7 90F39933 00337A6D 46CBE32E X509v3 extensions: X509v3 Key Usage: 86000000 Digital Signature Key Cert Sign CRL Signature X509v3 Subject Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F X509v3 Basic Constraints: CA: TRUE X509v3 Authority Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F Authority Info Access: Associated Trustpoints: GETVPN Storage: nvram:Root-CAcisco#1CA.cer



附註：對於證書身份驗證，請確保所提供的證書具有用於驗證裝置身份的正確引數，例如公用名(CN)、擴展金鑰用法(EKU)和生效日期。

配置GETVPN

GETVPN的重要功能取決於以前的配置，建議在ISAKMP和GDOI功能之前配置該配置。

4. — 在主金鑰伺服器上，生成帶有標籤「getKey」的可匯出RSA金鑰。 此金鑰在所有金鑰伺服器上都必須相同。因此，可匯出功能對於後續步驟至關重要：

KS(config)# **crypto key generate rsa general-keys label getKey modulus 1024 exportable** The name for the keys will be: **getKey** % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys are exportable. .. [OK] (elapsed time was 0 seconds)

5. — 使用組成員路由器在傳遞時必須加密的相關流量定義擴展訪問清單。在輔助金鑰伺服器上，使用相同的名稱定義相同的訪問清單。

主鍵伺服器

KS(config)# **ip access-list extended data_plane** KS(config-ext-nacl)# 10 permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255 KS(config-ext-nacl)# 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255

輔助金鑰伺服器

KS2(config)# **ip access-list extended data_plane** KS2(config-ext-nacl)# 10 permit ip 10.0.0 0.0.0.255 172.16.0.0 0.0.255.255 KS2(config-ext-nacl)# 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255

6 — 配置用於與GM建立安全連線的ISAKMP策略、IPsec轉換集和IPsec配置檔案，以從GDOI組消息交換開始。

KS(config)# **crypto isakmp policy 10** KS(config-isakmp)# **encryption aes 256** KS(config-iskamp)# **hash sha256** KS(config-iskamp)# **group 14** KS(config-iskamp)# **lifetime 3600**

KS(config)# **crypto ipsec transform-set get-ts esp-aes esp-sha-hmac** KS(config)# **crypto ipsec profile gdoi-profile** KS(ipsec-profile)# **set security-association lifetime seconds 7200** KS(ipsec-profile)# **set transform-set get-ts**

配置合作伙

7. — 在合作實施中，所涉及的關鍵伺服器必須具有相同的配置。從主金鑰伺服器匯出先前建立的可匯出RSA金鑰，並將私鑰和公鑰匯入輔助金鑰伺服器(KS2)。 在主Key Server變得無響應的情況下，次Key Server繼續對組內的所有GM裝置控制重新生成金鑰。

主鍵伺服器

KS(config)# **crypto key export rsa getKey pem terminal 3des cisco123** % Key name: getKey Usage: General Purpose Key Key data: -----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFtHBAdGV3ZPaGQcsAqO
1H9gmJWJNEeQvTND/oSrhN+jSSm+8f27RvDnIMYLDl9MndZ+rPqCPM/3NXE07
5bOsrT7B2uOpCBmAJK9iiTsfr01Qc4Izu5fwWcK2CN5OvLhyR2pKPviqwkSmGS zbaErQCH7evvjutYHE6DhOTTLubxQIDAQAB -----END PUBLIC KEY----- -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,AA98923B28E00DCCto1Wym6cRvqEXBlt97UZdGyusf3cW/iumb7oD9/09q5if4ouoE

brPykL3No0WMI7h56WQPiAHzLu5IZ+CTQHwwgYvXwHNpOHjmTMOgf9FG856GosM3kjP58QDupSc1W70+C9

zsCM3QmwbRs6JGBP5Rb36f+895xoyqzWA8G5sQlizE1oP4lM3Zx5DukgTXLzIDL7w0dPEYBd1aDhAJQf8dB/Zu

GvQWxad4gL6SssEyzigbzdSdRwBS+0DLOm05hOUU8rNiWit1TCsTPflwuTjlyxgRbyKvtXdoURvuTP3M6/DOppe2

n26bXC2DcURk8nMtIrIHAPvvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb

AI286GHqCOw2AxDcoMzcanQYw1VNgHG7SUsbaday7enuJtwbf2Pjkf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C

2PkLiQvQwuYi8J9SgM+391aFrf0NRXFHrM7T9MQcBBIcbo0BtfG4ICBuIltpG+BpCty/XW99dvuhqh9hjqfy2sKqF4H

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwvvWQjewrA0K

5Bu+jzxSeQAxbUAXGiIfp9hCL8jq4ac/g+OafCqyHETJd8m5Yr6W9/0bGLnsEzNLbhgPR7A==

-----END RSA PRIVATE KEY-----

輔助金鑰伺服器

KS2(config)# **crypto key import rsa getKey pem exportable terminal cisco123**

% Enter PEM-formatted public General Purpose key or certificate.

% End with a blank line or "quit" on a line by itself. -----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFtHBAdGV3ZPaGQcsAqO
1H9gmJWJNEeQvTND/oSrhN+jSSm+8f27RvDnIMYLDl9MndZ+rPqCPM/3NXE07
5bOsrT7B2uOpCBmAJK9iiTsfr01Qc4Izu5fwWcK2CN5OvLhyR2pKPviqwkSmGSz baErQCH7evvjutYHE6DhOTTLubxQIDAQAB -----END PUBLIC KEY----- quit % Enter PEM-formatted encrypted private General Purpose key.

% End with "quit" on a line by itself. -----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,AA98923B28E00DCCto1Wym6cRvqEXBlt97UZdGyusf3cW/iumb7oD9/09q5if4ouoE

brPykL3No0WMI7h56WQPiAHzLu5IZ+CTQHwwgYvXwHNpOHjmTMOgf9FG856GosM3kjP58QDupSc1W70+C9

zsCM3QmwbRs6JGBP5Rb36f+895xoyqzWA8G5sQlizE1oP4lM3Zx5DukgTXLzIDL7w0dPEYBd1aDhAJQf8dB/Zu

GvQWxad4gL6SssEyzigbzdSdRwBS+0DLOm05hOUU8rNiWit1TCsTPflwuTjlyxgRbyKvtXdoURvuTP3M6/DOppe2

n26bXC2DcURk8nMtIrIHAPvvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb

AI286GHqCOw2AxDcoMzcanQYw1VNgHG7SUsbaday7enuJtwbf2Pjkf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C

2PkLiQvQwuYi8J9SgM+391aFrf0NRXFHrM7T9MQcBBIcbo0BtfG4ICBuIltpG+BpCty/XW99dvuhqh9hjqfy2sKqF4H

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwvvWQjewrA0K

5Bu+jzxSeQAxbUAXGiIfp9hCL8jq4ac/g+OafCqyHETJd8m5Yr6W9/0bGLnsEzNLbhgPR7A==

-----END RSA PRIVATE KEY-----

quit

% Key pair import succeeded.

8 — 必須為合作伙KS配置定期ISAKMP。這樣，主KS可以監視輔助金鑰伺服器

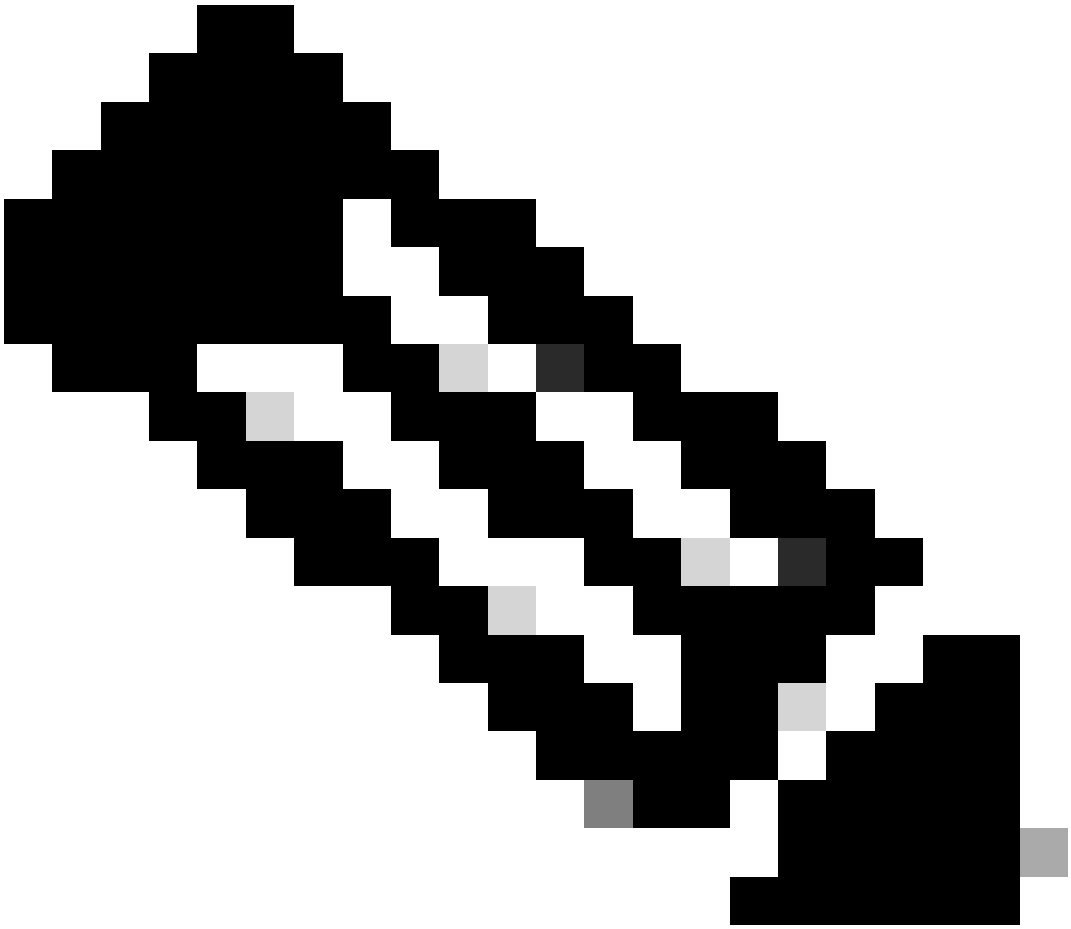
主鍵伺服器

KS(config)# **crypto isakmp keepalive 15 periodic**

輔助金鑰伺服器

KS2(config)# **crypto isakmp keepalive 15 periodic**

COOP金鑰伺服器從主伺服器交換單向通訊。如果輔助KS在30秒間隔內沒有從主KS聽到消息，輔助KS嘗試聯絡主KS並請求更新資訊。如果輔助KS在60秒間隔內沒有從主KS聽到消息，則觸發COOP重新選擇過程並選舉新的主KS。



附註：GM和KS之間不需要定期DPD。

關鍵伺服器之間的選擇基於配置的最高優先順序值。如果相同，則基於最高IP地址。在每個金鑰伺服器上使用相同的加密策略、擴展訪問清單配置相同的GDOI組。

主鍵伺服器

KS(config)# **crypto gdoi group GETVPN** KS(config-gkm-group)# **identity number 484** KS(config-gkm-group)# **server local** KS(gkm-local-server)# **rekey lifetime seconds 86400** KS(gkm-local-server)# **rekey retransmit 40 number 2** KS(gkm-local-server)#**rekey authentication mypubkey rsa getKey** KS(gkm-local-server)# **rekey transport unicast**

9. — 在同一本地伺服器設定中，啟用用於資料平面流量的加密策略和先前配置的訪問清單。

KS(gkm-local-server)# **sa ipsec 10** KS(gkm-sa-ipsec)# **profile gdoi-profile** KS(gkm-sa-ipsec)# **match address ipv4 data_plane**

本地伺服器設定是啟用COOP金鑰伺服器功能的配置級別，定義的優先順序決定此金鑰伺服器的角色。 必須顯式配置輔助金鑰伺服器，以便所有KS都能知道彼此的存在。

KS(gkm-sa-ipsec)# **exit** KS(gkm-local-server)# **redundancy** KS(gdoi-coop-ks-config)# **local priority 100** KS(gdoi-coop-ks-config)# **peer address ipv4 172.18.5.2**

COOP金鑰伺服器配置的最後一部分是金鑰資料包的源IP地址的定義，該地址是在金鑰伺服器路由器的一個介面中配置的IP地址。

KS(gdoi-coop-ks-config)# **exit** KS(gkm-local-server)# **address ipv4 172.16.4.2**

在輔助金鑰伺服器上複製相同的配置步驟，配置較低的優先順序以將路由器標識為輔助伺服器並註冊主KS地址。

輔助金鑰伺服器

KS2(config)# **crypto gdoi group GETVPN** KS2(config-gkm-group)# **identity number 484** KS2(config-gkm-group)# **server local** KS2(gkm-local-server)# **rekey lifetime seconds 86400** KS2(gkm-local-server)# **rekey retransmit 40 number 2** KS2(gkm-local-server)# **rekey authentication mypubkey rsa getKey** KS2(gkm-local-server)# **rekey transport unicast** KS2(gkm-local-server)# **sa ipsec 10** KS2(gkm-sa-ipsec)# **profile gdoi-profile** KS2(gkm-sa-ipsec)# **match address ipv4 data_plane** KS2(gkm-sa-ipsec)# **exit** KS2(gkm-local-server)# **redundancy** KS2(gdoi-coop-ks-config)# **local priority 78** KS2(gdoi-coop-ks-config)# **peer address ipv4 172.16.4.2** KS2(gdoi-coop-ks-config)# **exit** KS2(gkm-local-server)# **address ipv4 172.18.5.2**

10. — 在組成員路由器上，GDOI組設定與金鑰伺服器相比包含更少的配置。組成員只需要配置ISAKMP策略（使用相同的身份驗證方法GDOI組），並且具有GM路由器能夠向其註冊的金鑰伺服器的IP地址。

組成員

GM(config)# **crypto isakmp policy 10** GM(config-isakmp)# **encryption aes 256** GM(config-isakmp)# **hash sha256** GM(config-isakmp)# **group 14** GM(config-isakmp)# **lifetime 3600**

GM(config)# **crypto gdoi group GETVPN** GM(config-gkm-group)# **identity number 484** GM(config-gkm-group)# **server address ipv4 172.18.5.2**

GM(config)# **crypto map getvpn 10 gdoi** GM(config-crypto-map)# **set group GETVPN**

GM(config)# **interface GigabitEthernet1** GM(config-if)# **crypto map getvpn**

組成員2

GM2(config)# **crypto isakmp policy 10** GM2(config-isakmp)# **encryption aes 256** GM2(config-isakmp)# **hash sha256** GM2(config-isakmp)# **group 14** GM2(config-isakmp)# **lifetime 3600** GM2(config)# **crypto gdoi group GETVPN** GM2(config-gkm-group)# **identity number 484** GM2(config-gkm-group)# **server address ipv4 172.16.4.2** GM2(config-gkm-group)# **server address ipv4 172.18.5.2** GM2(config)# **crypto map getvpn 10 gdoi** GM2(config-crypto-map)# **set group GETVPN** GM2(config)# **interface GigabitEthernet1** GM2(config-if)# **crypto map getvpn**

驗證

按如下所示驗證配置每個階段的設定：

關鍵伺服器上資料平面流量的ACL

此show命令用於驗證所定義的相關流量是否無錯誤。

KS# **show ip access-lists data_plane Extended IP access list data_plane** 10 permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255 KS2# **show ip access-lists data_plane Extended IP access list data_plane** 10 permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255

COOP註冊狀態：

show crypto gkm ks coop命令顯示金鑰伺服器之間的當前COOP狀態，指示主金鑰伺服器是誰、它們所屬的GDOI組、它們的單獨和對等優先順序，以及有關從主伺服器傳送到輔助伺服器的下一條消息的計時器。

主鍵伺服器

KS# **show crypto gkm ks coop** Crypto Gdoi Group Name :GETVPN Group handle: 1073741826, Local Key Server handle: 1073741826 Local Address: 10.191.61.114 Local Priority: 100 Local KS Role: Primary , Local KS Status: Alive Local KS version: 1.0.27 Primary Timers: Primary Refresh Policy Time: 20 Remaining Time: 5 Per-user timer remaining time: 0 Antireplay Sequence Number: 63046 Peer Sessions: Session 1: Server handle: 1073741827 Peer Address: 10.191.61.115 Peer Version: 1.0.23 Peer Priority: 75 Peer KS Role: Secondary , Peer KS Status: Alive Antireplay Sequence Number: 0 IKE status: Established Counters: Ann msgs sent: 63040 Ann msgs sent with reply request: 3 Ann msgs recv: 32 Ann msgs recv with reply request: 4 Packet sent drops: 3 Packet Recv drops: 0 Total bytes sent: 42550002 Total bytes recv: 22677

輔助金鑰伺服器

KS2# **show crypto gkm ks coop** Crypto Gdoi Group Name :GETVPN Group handle: 1073741829, Local Key Server handle: 1073741827 Local Address: 10.191.61.115 Local Priority: 75 Local KS Role: Secondary , Local KS Status: Alive Local KS version: 1.0.23 Secondary Timers: Sec Primary Periodic Time: 30 Remaining Time: 11, Retries: 0 Invalid ANN PST recvd: 0 New GM Temporary Blocking Enforced?: No Per-user timer remaining time: 0 Antireplay Sequence Number: 4 Peer Sessions: Session 1: Server handle: 1073741828 Peer Address: 10.191.61.114 Peer Version: 1.0.27 Peer Priority: 100 Peer KS Role: Primary , Peer KS Status: Alive Antireplay Sequence Number: 30 IKE status: Established Counters: Ann msgs sent: 2 Ann msgs sent with reply request: 1 Ann msgs recv: 28 Ann msgs recv with reply request: 1 Packet sent drops: 1 Packet Recv drops: 0 Total bytes sent: 468 Total bytes recv: 16913

顯示組GETVPN的資訊以及有關合作金鑰伺服器的版本資訊。

KS# **show crypto gdoi group GETVPN ks coop version** Cooperative key server infra Version : 2.0.0 Client : KS_POLICY_CLIENT Version : 2.0.0 Client : GROUP_MEMBER_CLIENT Version : 2.0.1 Client : SID_CLIENT Version : 1.0.1

組成員註冊

GM# **show crypto gkm group GETVPN** Group Name : GETVPN Group Identity : 484 Group Type : GDOI (ISAKMP) Crypto Path : ipv4 Key Management Path : ipv4 Rekeys received : 0 IPSec SA Direction : Both Group Server list : 10.191.61.115 Group Member Information For Group GETVPN: IPSec SA Direction : Both ACL Received From KS : gdoi_group_GETVPN_temp_acl Group member : 10.191.61.116 vrf: None Local addr/port : 10.191.61.116/848 Remote addr/port : 10.191.61.115/848 fvrf/ivrf : None/None Version : 1.0.25 Registration status : Registered Registered with : 10.191.61.115 Re-registers in : 5642 sec Succeeded registration: 1 Attempted registration: 1 Last rekey from : UNKNOWN Last rekey seq num : 0 Unicast rekey received: 0 Rekey ACKs sent : 0 Rekey Received : never PFS Rekey received : 0 DP Error Monitoring : OFF IPSEC init reg executed : 0 IPSEC init reg postponed : 0 Active TEK Number : 1 SA Track (OID/status) : disabled Fail-Close Revert : Disabled allowable rekey cipher: any allowable rekey hash : any allowable transformtag: any ESP Rekeys cumulative Total received : 0 After latest register : 0 Rekey Acks sents : 0 ACL Downloaded From KS 10.191.61.115: access-list permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255 access-list permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255 KEK POLICY: Rekey Transport Type : Unicast Lifetime (secs) : 85185 Encrypt Algorithm : 3DES Key Size : 192 Sig Hash Algorithm : HMAC_AUTH_SHA Sig Key Length (bits) : 1296 TEK POLICY for the current KS-Policy ACEs Downloaded: GigabitEthernet1: IPsec SA: spi: 0x535F673B(1398761275) transform: esp-aes esp-sha-hmac sa timing:remaining key lifetime (sec): (5988) Anti-Replay(Counter Based) : 64 tag method : disabled alg key size: 16 (bytes) sig key size: 20 (bytes) encaps: ENCAPS_TUNNEL KGS POLICY: REG_GM: local_addr 10.191.61.116 overall chech P2P POLICY: REG_GM: local_addr 10.191.61.116

疑難排解

COOP金鑰伺服器選擇

系統日誌消息可幫助跟蹤和確定COOP流程的問題。在COOP金鑰伺服器上啟用GDOI調試，僅顯示與此進程相關的資訊。

KS# **debug crypto gdoi ks coop**

當COOP選擇過程開始時，所有關鍵伺服器上都會顯示下一條系統日誌消息。

```
%GDOI-5-COOP_KS_ELECTION: KS entering election mode in group GETVPN (Previous Primary = NONE)
```

完成選擇過程後，消息「COOP_KS_TRANS_TO_PRI」顯示有關新的主金鑰伺服器的資訊，該消息在主金鑰伺服器和輔助金鑰伺服器上可見。在選舉過程的第一天，上一個Primary將會顯示「NONE」。

```
%GDOI-5-COOP_KS_TRANS_TO_PRI: KS 172.16.4.2 in group GETVPN transitioned to Primary (Previous Primary =
```

如果存在Key Server重新選擇，則消息包括前一個主伺服器的IP地址。

```
%GDOI-5-COOP_KS_TRANS_TO_PRI: KS 172.18.5.2 in group GETVPN transitioned to Primary (Previous Primary =
```

當COOP次金鑰伺服器失去連線時，將顯示「COOP_KS_UNREACH」消息。主KS跟蹤所有輔助KS的狀態，並使用此消息表示與輔助KS的連線丟失。輔助KS僅跟蹤主KS的狀態。輔助KS上的此消息表示與主KS失去連線。

```
%GDOI-3-COOP_KS_UNREACH: Cooperative KS 172.18.5.2 Unreachable in group GETVPN
```

當在COOP KS之間恢復連線時，將顯示「COOP_KS_REACH」消息。

```
%GDOI-5-COOP_KS_REACH: Reachability restored with Cooperative KS 172.18.5.2 in group GETVPN.
```

PKI註冊問題

調試信任點註冊或身份驗證問題時，請使用PKI調試。

debug crypto pki messages debug crypto pki transactions debug crypto pki validation debug crypto pki api debug crypto pki callback

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。