

Configurare GETVPN con i server chiavi COOP e l'autenticazione dei certificati

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[PKI per autenticazione](#)

[Configura GETVPN](#)

[Configurazione di COOP](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare Group Encrypted Transport VPN (GETVPN) in modo che utilizzi i certificati digitali per l'autenticazione e i server chiavi COOP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Group Encrypted Transport VPN (GETVPN)
- PKI (Public Key Infrastructure)
- CA (Certification Authority)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- CSR1000V - Cisco IOS® XE, versione 16.12.03 - come Cisco IOS® XE Key Server, Group Member e CA Server.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

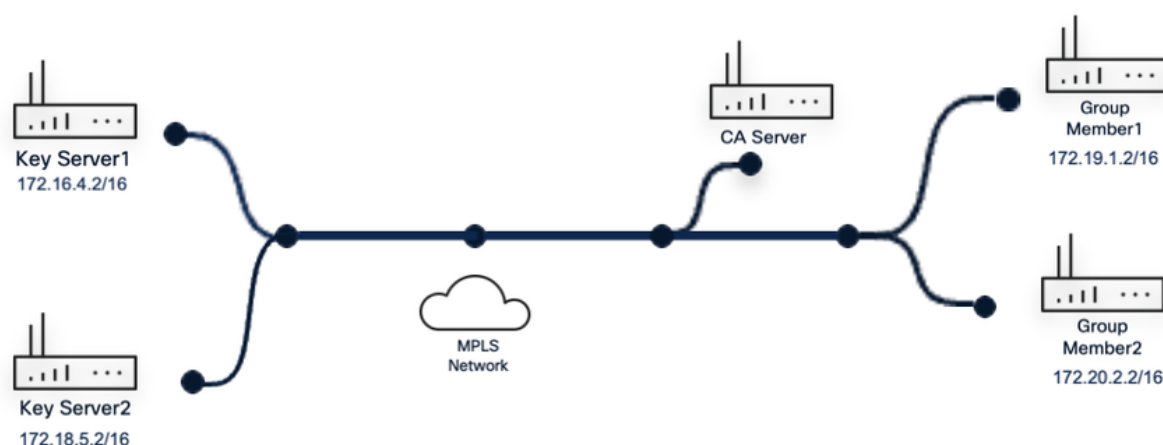
Premesse

In una distribuzione GETVPN, il server chiave è l'entità più importante perché il KS gestisce il control plane. Con un singolo dispositivo per gestire un gruppo GETVPN completo, crea un singolo punto di errore.

Per ridurre questo scenario, GETVPN supporta più Key Server denominati COOP (Cooperative) KS che forniscono ridondanza e ripristino se un Key Server diventa irraggiungibile.

Configurazione

Esempio di rete



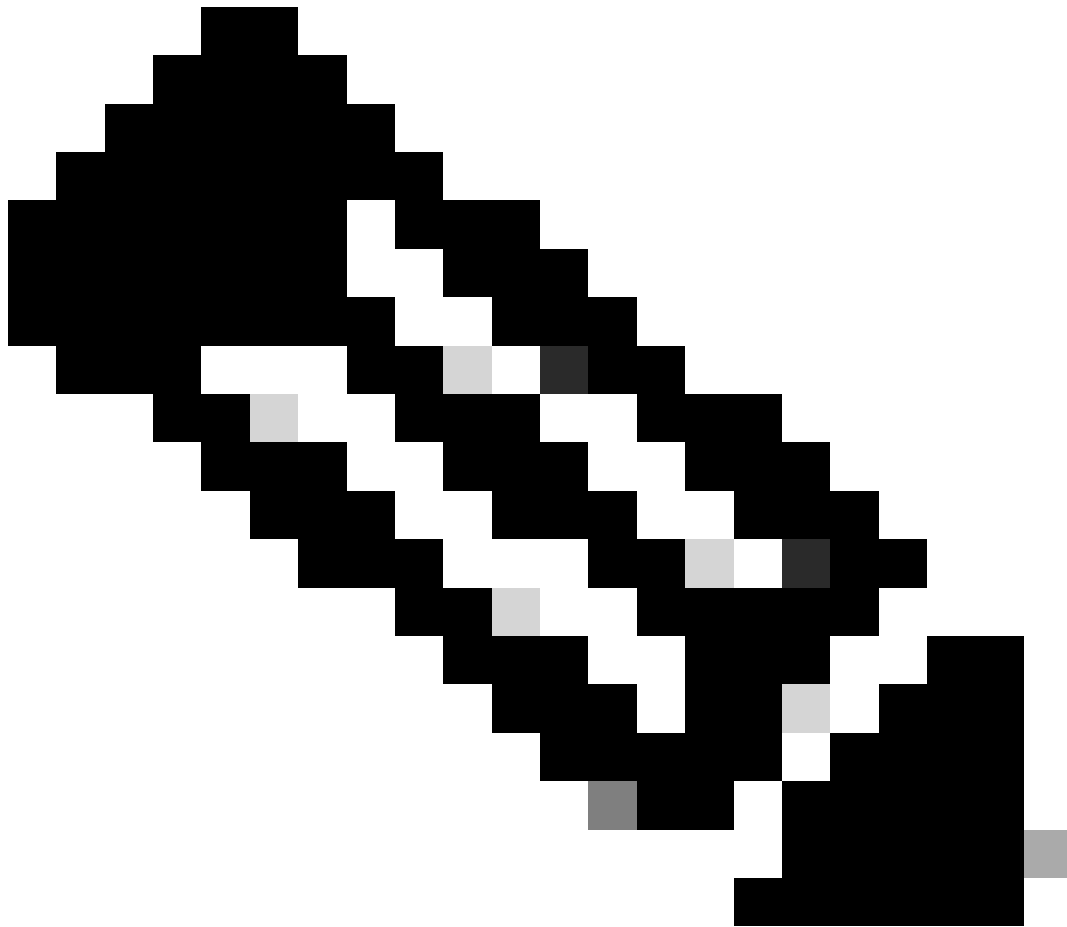
GETVPN Topology

Configurazioni

PKI per autenticazione

PKI utilizza la propria infrastruttura per superare le principali difficoltà di gestione incontrate durante l'utilizzo delle PSK. L'infrastruttura PKI funge da autorità di certificazione (CA) che rilascia (e quindi mantiene) i certificati di identità.

Qualsiasi router membro del gruppo le cui informazioni sul certificato corrispondono all'identità ISAKMP è autorizzato e può registrarsi al servizio KS.



Nota: I certificati possono essere rilasciati da qualsiasi CA. Per questa guida, un CSR1000V è configurato come CA per il rilascio di certificati a tutti i dispositivi nella distribuzione per autenticare la propria identità.

CA# show crypto pki server

server ca crypto pki server

livello database completato

archivio database pkcs12 password 7 1511021F07257A767B73

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

concedi hash automatico sha255

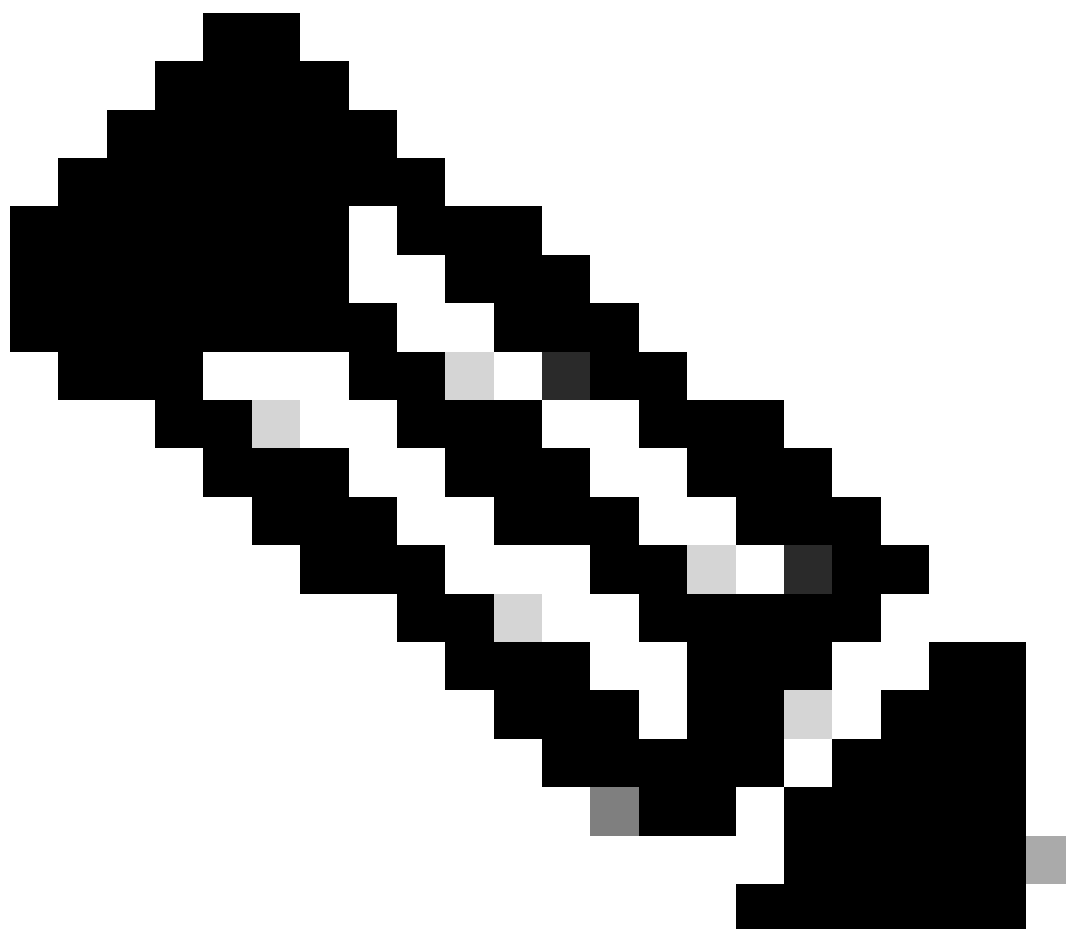
certificato di durata 5000

life ca-certificate 7300

eku server-auth client-auth

nvram url database

1.- Nelle distribuzioni basate su PKI, è necessario ottenere il certificato di identità da un'autorità di certificazione (CA) per ogni dispositivo. Nei router server di chiavi e membri del gruppo, creare una coppia di chiavi RSA utilizzata nella configurazione del trust point.



Nota: Ai fini della dimostrazione di questa guida, tutti i router dei server chiave e dei membri del gruppo in questa topologia condividono la stessa configurazione.

Server chiave

```
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**

Membro del gruppo

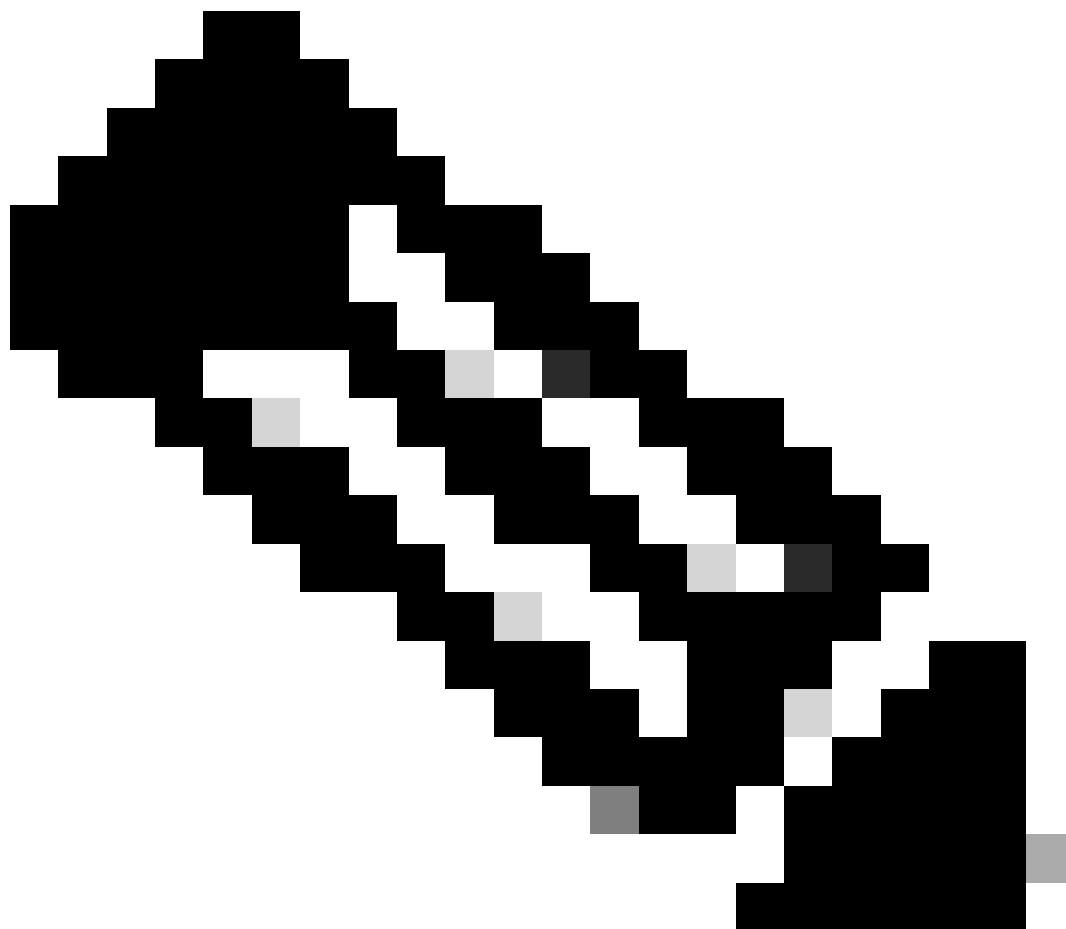
GM(config)# **crypto key generate rsa modulus 2049 general-keys label pkikey** The name for the keys will be: **pkikey** % The key modulus size is 2049 bits % Generating 2049 bit RSA keys, keys are non-exportable... [OK] (elapsed time was 0 seconds) GM(config)# **crypto pki trustpoint GETVPN** GM(ca-trustpoint)#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



Nota: Il nome della chiave RSA viene riutilizzato su tutti i dispositivi per mantenere la coerenza e non influisce sulle altre impostazioni perché ogni chiave RSA ha un valore computazionale univoco.

2.- Il certificato della CA deve essere installato prima nel trustpoint. Ciò può essere fatto autenticando il trustpoint o registrando direttamente. Poiché in precedenza non è installato alcun certificato CA, viene attivata per prima la procedura di autenticazione del trust point.

Server chiave

```
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.

Membro del gruppo

```
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' command will show the fingerprint.

3-Verificare su entrambi i dispositivi che i nuovi certificati rilasciati siano importati nei rispettivi trust point autenticati (è necessario importare anche il certificato CA) utilizzando il comando 'show

crypto pki certificates verbose'.

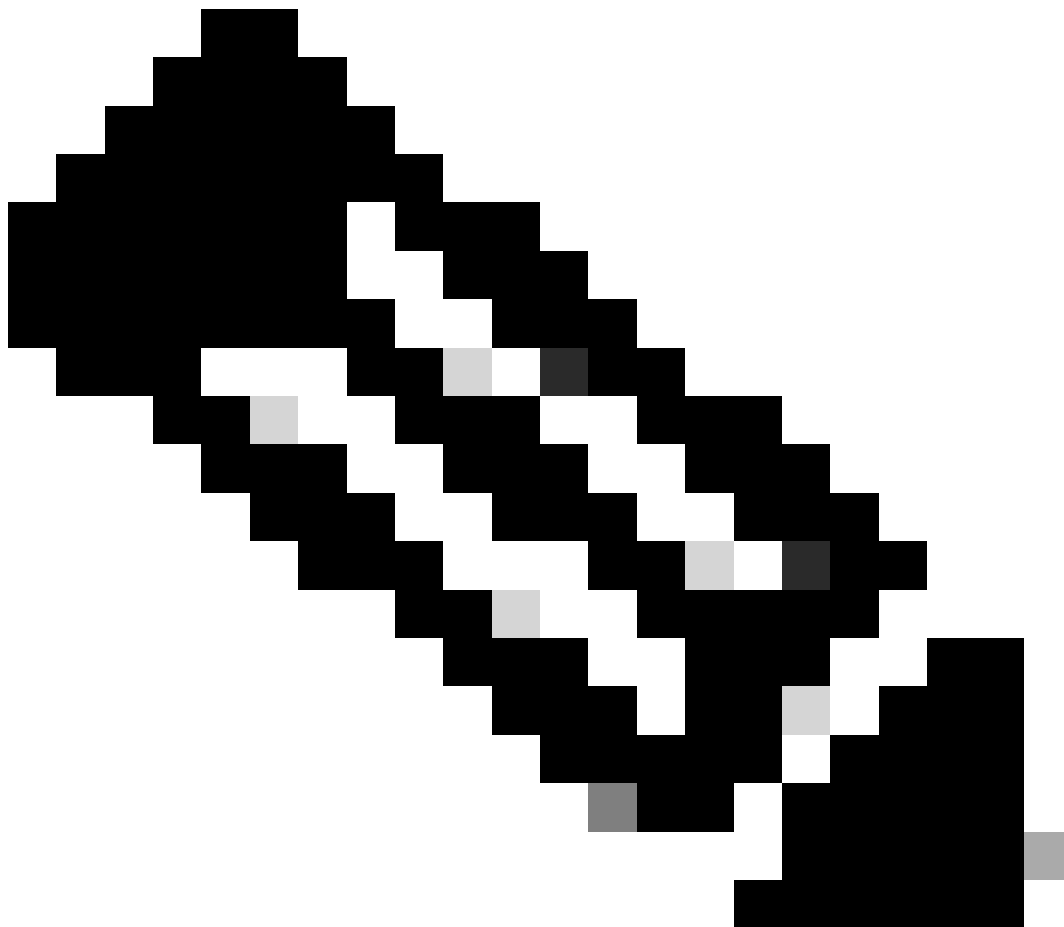
Server chiave

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

Membro del gruppo

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



Nota: Per l'autenticazione del certificato, verificare che il certificato fornito disponga dei parametri corretti per convalidare l'identità del dispositivo, ad esempio il nome comune (CN), l'utilizzo chiavi esteso (EKU), la data di validità.

Configura GETVPN

Caratteristiche importanti di GETVPN si basano sulla configurazione precedente che si consiglia di configurare prima delle funzionalità ISAKMP e GDOI.

4.- Sul server principale, generare una chiave RSA esportabile con l'etichetta 'getKey'. La chiave deve essere identica in tutti i server delle chiavi. Pertanto, la funzione esportabile è essenziale per le fasi successive:

```
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.- Definire un elenco degli accessi esteso con il traffico interessante che i router dei membri del

gruppo devono crittografare quando passano. Sul server chiavi secondario definire lo stesso elenco degli accessi utilizzando lo stesso nome.

Server chiavi primarie

```
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
```

Server chiavi secondario

```
KS2(config)# ip access-list extended data_plane KS2(config-ext-nacl)# 10 permit ip 10.0.0.0 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- Configurare il criterio ISAKMP, IPsec Transform-set e il profilo IPsec utilizzati per stabilire la connettività sicura con gli oggetti GM a partire dallo scambio di messaggi del gruppo GDOI.

```
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
```

Configurazione di COOP

7.- In un'implementazione cooperativa, i server principali coinvolti devono avere una configurazione identica. Esportare la chiave RSA esportabile creata in precedenza dal server di chiavi primario e importare le chiavi private e pubbliche nel server di chiavi secondario (KS2). In uno scenario in cui il server di chiavi primario non risponde, il server di chiavi secondario continua a controllare la reimpostazione della chiave per tutti i dispositivi GM all'interno del gruppo.

Server chiavi primarie

```
KS(config)# crypto key export rsa getKey pem terminal 3des cisco123 % Key name: getKey Usage: General Purpose Key Key data: -----
BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFtHBAAdGV3ZPaGQcsAqO
1H9gmJWJNEeQvTND/oSrhN+jSSm+8f27RvDnIMYLDl9MndZ+rPqCPM/3NXE07
5bOsrT7B2uOpCBmAJK9iiTsfr01Qc4Izu5fwWcK2CN5OvLhyR2pKPviqwkSmGS zbaErQCH7evvjutYHE6DhOTTLubxQIDAQAB -----END
PUBLIC KEY----- -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-
CBC,AA98923B28E00DCCto1Wym6cRvqEXBl97UZdGyusf3cW/iumb7oD9/09q5if4ouoE

brPykL3No0WMI7h56WQPiAHzLu5IZ+CTQHwwgYvXwHNpOHjmTMOgf9FG856GosM3kjP58QDupSc1W70+C9

zsCM3QmwbRs6JGBP5Rb36f+895xoyqzWA8G5sQlize1oP4lM3Zx5DukgTXLzIDL7w0dPEYBd1aDhAJQf8dB/Zu

GvQWxad4gL6SssEyzigbzdSdRwBS+0DLOm05hOUU8rNiWit1TCsTPflwuTjlyxgRbyKvtXdoURvuTP3M6/Doppe2

n26bXC2DcURk8nMtIrIHAPvvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb

AI286GHqCOW2AxDcoMzcanQYw1VNgHG7SUsbaday7enuJtwbf2Pjfk9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C

2PkLiQvQwuYi8J9SgM+391aFrf0NRXFHrM7T9MQcBBIcbo0BtfG4ICBuItpG+BpCty/XW99dvuhqh9hjyfy2sKqF4H
```

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwwvWQjewrA0K

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

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

Server chiavi secondario

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,AA98923B28E00DCCto1Wym6cRvqEXBlr97UZdGysuf3cW/iumb7oD9/09q5if4ouoE

brPykL3No0WMI7h56WQPiAhZLu5IZ+CTQHwwgYvXwHNpOHjmTMOgf9FG856GosM3kjP58QDupSc1W70+C9

zsCM3QmwbRs6JGBP5Rb36f+895xoyqzWA8G5sQlize1oP4lM3Zx5DukgTXLzIDL7w0dPEYBd1aDhAJQf8dB/Zu

GvQWxad4gL6SssEyzigbzdSdRwBS+0DLOm05hOUU8rNiWit1TCsTPflwuTjlyxgRbyKvtXdoURvuTP3M6/DOppe2

n26bXC2DcURk8nMtIrIHAPvvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb

AI286GHqCOW2AxDcoMzcanQYw1VNgHG7SUsbaday7enuJtwbf2Pjkf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C

2PkLiQvQwuYi8J9SgM+391aFr0NRXFHrM7T9MQcBBIcbo0BtfG4ICBuItpG+BpCty/XW99dvuhqh9hjfy2sKqF4H

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwwvWQjewrA0K

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

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

quit

% Key pair import succeeded.

8- È necessario configurare ISAKMP periodici per gli KS COOP. In questo modo, l'KS primario

può monitorare i server chiave secondari

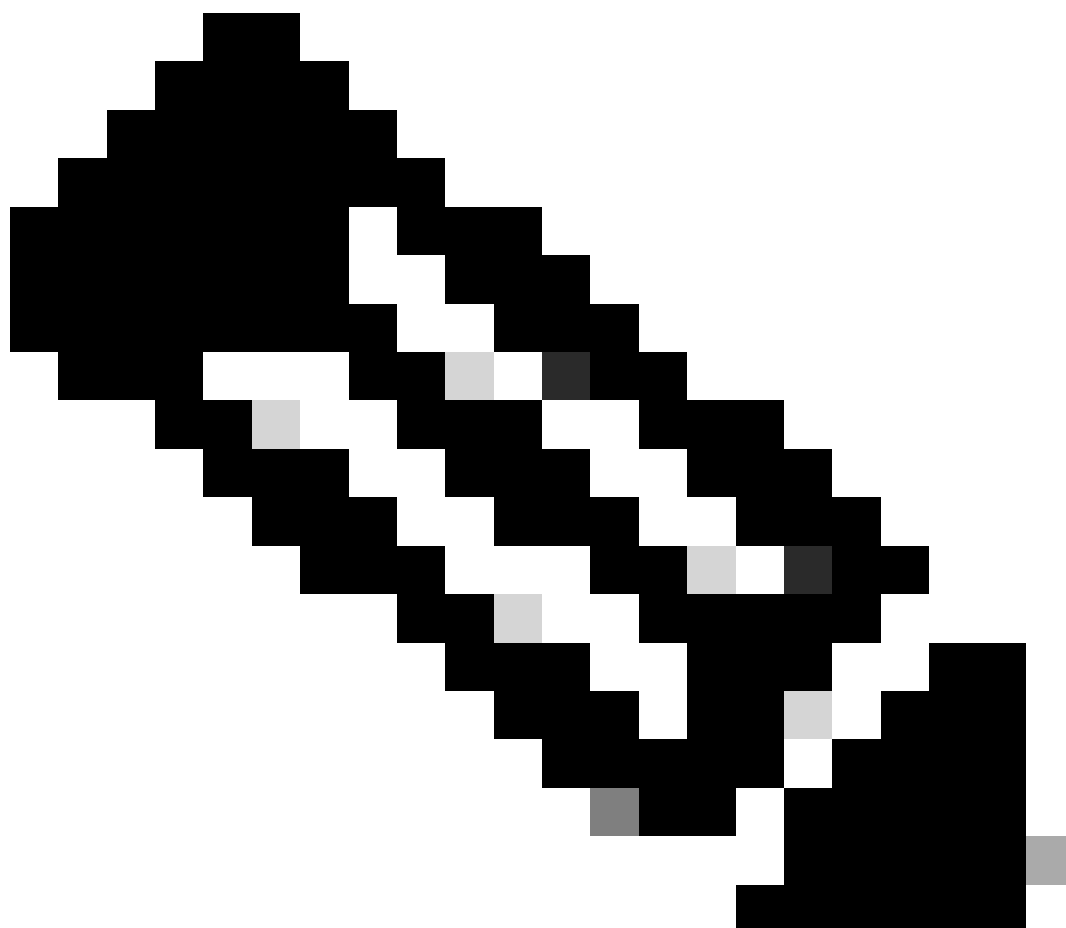
Server chiavi primarie

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

Server chiave secondari

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

I server chiave COOP scambiano comunicazioni unidirezionali dal server primario a quello secondario. Se un KS secondario non riceve l'audio dal KS primario in un intervallo di 30 secondi, il KS secondario tenta di contattare il KS primario e richiede informazioni aggiornate. Se il KS secondario non riceve l'audio dal KS primario in un intervallo di 60 secondi, viene avviato un processo di rielezione COOP e viene scelto un nuovo KS primario.



Nota: La DPD periodica tra GM e KS non è richiesta.

La scelta tra i server chiave si basa sul valore di priorità più alta configurato. Se sono uguali, si basa sull'indirizzo IP più alto. Configurare su ciascun Key Server lo stesso gruppo GDOI utilizzando gli stessi criteri di crittografia ed elenchi degli accessi estesi.

Server chiavi primarie

```
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.- All'interno delle stesse impostazioni del server locale, abilitare i criteri di crittografia previsti per il traffico del piano dati e l'elenco degli accessi precedentemente configurati.

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

Rispetto alle impostazioni del server locale è il livello di configurazione in cui la funzione del server chiave COOP è abilitata, la priorità definita determina il ruolo per questo server chiave. I server chiave secondari devono essere configurati in modo esplicito in modo che tutti i KS siano a conoscenza l'uno dell'altro.

```
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
```

La parte finale della configurazione del server chiavi COOP è la definizione dell'indirizzo IP di origine del pacchetto chiave, ossia un indirizzo IP configurato in una delle interfacce del router del server chiavi.

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

Replicare gli stessi passaggi di configurazione sul server di chiave secondaria, configurando una priorità inferiore per identificare il router come server secondario e registrare l'indirizzo del servizio di chiave primaria.

Server chiavi secondario

```
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.- Su un router membro del gruppo, le impostazioni del gruppo GDOI prevedono una configurazione inferiore rispetto ai server delle chiavi. Un membro del gruppo deve solo avere il criterio ISAKMP configurato, usare lo stesso metodo di autenticazione, il gruppo GDOI e avere gli indirizzi IP dei server chiavi su cui il router GM può registrarsi.

Membro del gruppo

```
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
```

Membro del gruppo 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
```

Verifica

Verificare le impostazioni da ogni fase della configurazione come segue:

ACL per il traffico del piano dati sui server chiave

Questo comando show viene usato per confermare che non ci sono errori nel traffico interessante definito.

```
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
```

Stato registrazione COOP:

Il comando 'show crypto gkm ks coop' visualizza lo stato COOP corrente tra i server chiavi, indicando chi è il server chiave primario, il gruppo GDOI a cui appartengono, la loro priorità individuale e peer e i timer relativi ai successivi messaggi da inviare dai server primari a quelli secondari.

Server chiavi primarie

```
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 rcv: 32 Ann msgs rcv with reply request: 4 Packet sent drops: 3 Packet Recv drops: 0 Total bytes sent: 42550002 Total bytes rcv: 22677

Server chiavi secondario

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 rcvd: 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 rcv: 28 Ann msgs rcv with reply request: 1
Packet sent drops: 1 Packet Recv drops: 0 Total bytes sent: 468 Total bytes rcv: 16913

Visualizza le informazioni sul gruppo GETVPN e sulla versione relative al server delle chiavi della modalità cooperativa.

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

Registrazione dei membri del gruppo

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 sent : 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 check P2P POLICY: REG_GM: local_addr
10.191.61.116

Risoluzione dei problemi

Scelta del server chiave COOP

I messaggi syslog consentono di tenere traccia e identificare i problemi relativi al processo COOP. Abilitare il debug GDOI nei server chiave COOP per visualizzare solo le informazioni correlate a questo processo.

KS# **debug crypto gdoi ks coop**

All'inizio del processo di selezione COOP, il messaggio syslog successivo viene visualizzato su tutti i server principali.

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

Al termine del processo di selezione, il messaggio "COOP_KS_TRANS_TO_PRI" visualizza le informazioni sul nuovo server di chiavi primario e il messaggio viene visualizzato sui server di chiavi primario e secondario. La Primaria precedente dovrebbe mostrare "NONE" al primo momento del processo elettorale.

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

In caso di rielezione del server di chiavi, il messaggio include l'indirizzo IP del server primario precedente.

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

Quando la connettività ai server chiave secondari COOP viene persa, viene visualizzato il messaggio "COOP_KS_UNREACH". Il KS primario tiene traccia dello stato di tutti i KS secondari e utilizza questo messaggio per indicare la perdita di connettività a un KS secondario. Un KS secondario tiene traccia solo dello stato del KS primario. Questo messaggio sul KS secondario indica la perdita di connettività con il KS primario.

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

Quando viene ripristinata la connettività tra i COOP KS, viene visualizzato il messaggio "COOP_KS_REACH".

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

Problemi di registrazione PKI

Quando si esegue il debug di problemi di registrazione o autenticazione del trust point, utilizzare i debug PKI.

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).