COOPキーサーバと証明書認証を使用したGETVPNの設定

内容

はじめに

このドキュメントでは、認証とCOOPキーサーバにデジタル証明書を使用するようにGroup Encrypted Transport VPN(GETVPN)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

– グループ暗号化トランスポートVPN(GETVPN)

-公開キー インフラストラクチャ（PKI）

-認証局（CA）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- CSR1000V:Cisco IOS® XEバージョン16.12.03:Cisco IOS® XEキーサーバ、グループメンバー、およびCAサーバとして機能

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

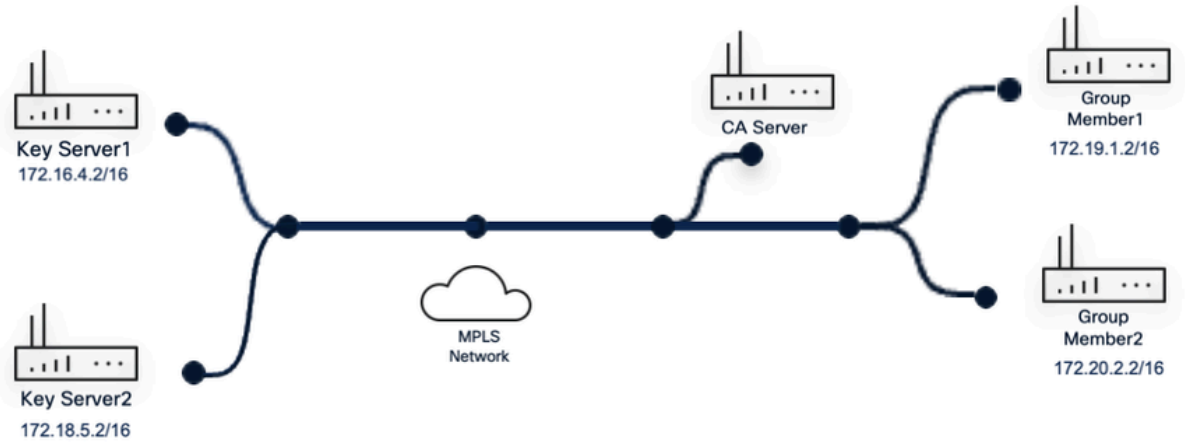
背景説明

GETVPN展開では、KSがコントロールプレーンを維持するため、キーサーバが最も重要なエンティティです。完全なGETVPNグループを1つのデバイスで管理すると、シングルポイント障害が発生します。

このシナリオを軽減するために、GETVPNはCooperative(COOP)KSと呼ばれる複数のキーサーバをサポートします。このキーサーバは、キーサーバに到達できなくなった場合に冗長性とリカバリを提供します。

設定

ネットワーク図



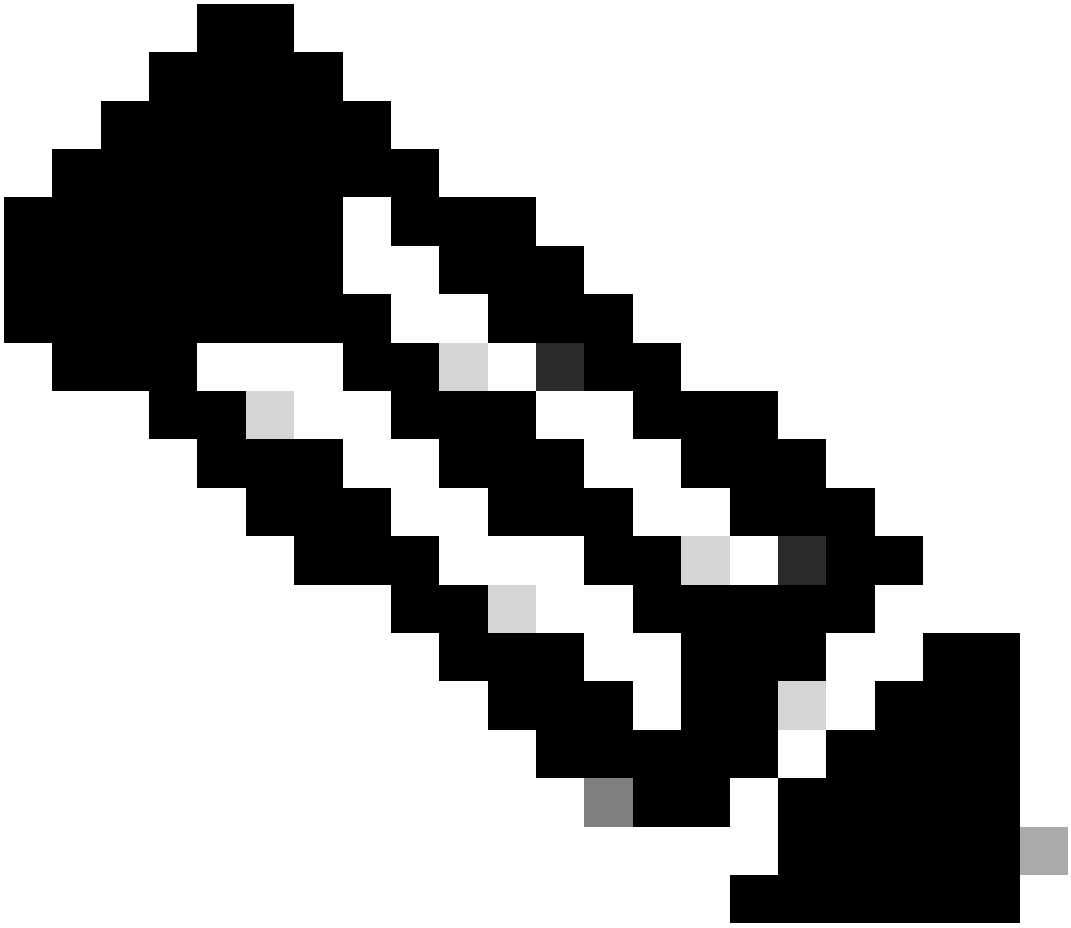
GETVPNトポロジ

コンフィギュレーション

認証用のPKI

PKIは、そのインフラストラクチャを使用して、PSKの使用時に発生する主要な管理の問題を解決します。PKIインフラストラクチャは、ID証明書を発行（および維持）する認証局(CA)として機能します。

証明書情報がISAKMP IDと一致するグループメンバールータはすべて承認され、KSに登録できます。



注：証明書は、任意のCAによって発行できます。このガイドでは、CSR1000VをCAとして設定し、導入環境内のすべてのデバイスに証明書を発行してIDを認証します。

CA# show crypto pki server

crypto pki server caサーバ

データベースレベル完了

database archive pkcs12 password 7 1511021F07257A767B73（データベースのアーカイブpkcs12パスワード7）

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

自動ハッシュsha255を許可

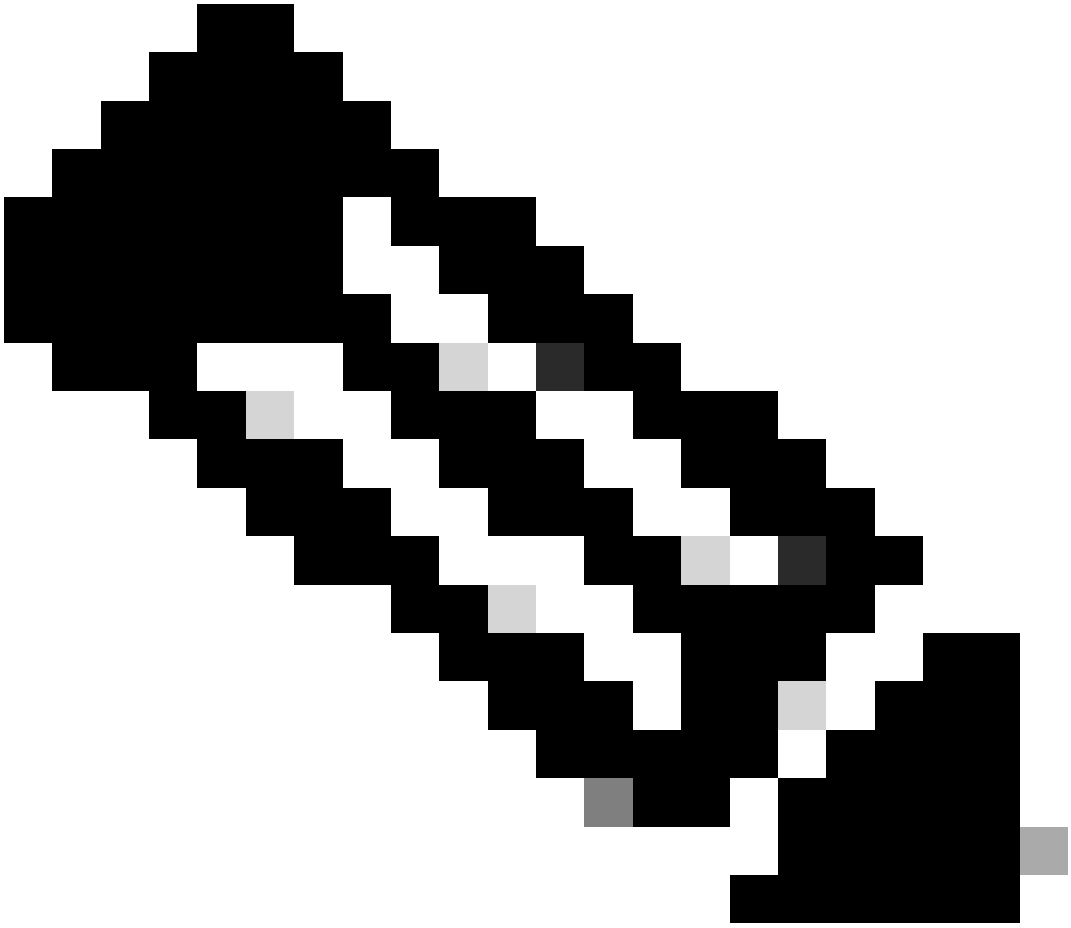
ライフタイム証明書5000

ライフタイムca証明書7300

ekuサーバ認証クライアント認証

データベースurl nvram

1.- PKIベースの導入では、各デバイスの認証局(CA)からID証明書を取得する必要があります。キーサーバおよびグループメンバーのルータで、トラストポイント設定で使用するRSAキーペアを作成します。



注：このガイドのデモンストレーションでは、このトポロジ内のすべてのキーサーバとグループメンバーのルータが同じ設定を共有しています。

キーサーバ

KS(config)# crypto key generate rsa modulus 2049 general-keys label pkikeyキーの名前は次のとおりです。pkikey %キーのモジュラスサイズは2049ビット%2049ビットRSAキーの生成、キーはエクスポートできません。 [OK]（経過時間0秒） KS(config)# **crypto pki trustpoint GETVPN KS(config)# enrollment url** http://10.191.61.120:80# subject-name OU=GETVPN KS KS(config)# revocation-check

none **KS(config)# rsakeypair pkikey** KS(config)# **auto-enroll 70**

グループメンバー

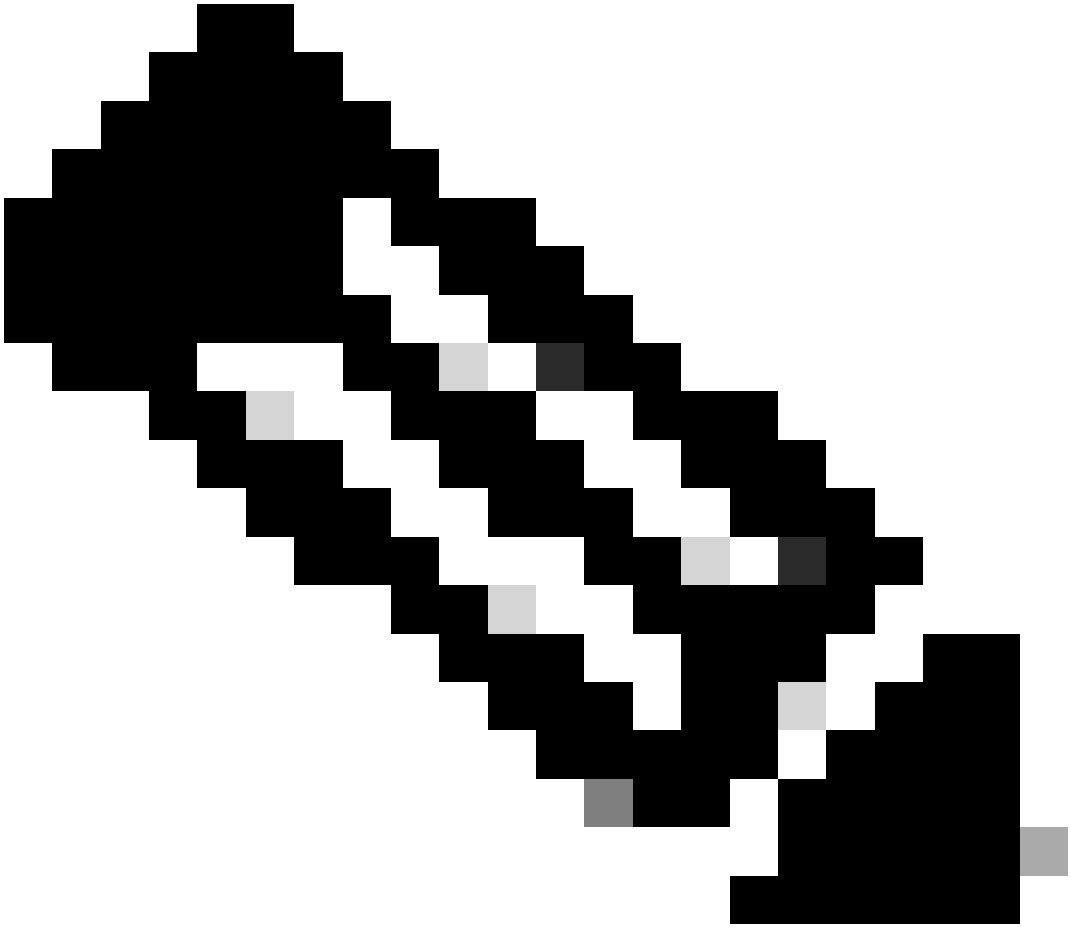
GM(config)# **crypto key generate rsa modulus 2049 general-keys label pkikey**キーの名前は次のとおりです。**pkikey** %キーのモジュラスサイズは2049ビット%2049ビットRSAキーの生成はエクスポートできません。 [OK]（経過時間は0秒）GM(config)# **crypto pki trustpoint GETVPN** GM(ca-trustpoint)# **enrollment url**http://10.191.61.120:80

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**



注:RSAキー名は、一貫性を維持するためにすべてのデバイスで再利用されます。各RSAキーはその計算値において一意であるため、他の設定には影響しません。

2.- CAからの証明書は、トラストポイントに最初にインストールする必要があります。 これは、トラストポイントを認証するか、直接登録することによって実行できます。以前にインストールされたCA証明書がないため、トラストポイント認証手順が最初にトリガーされます。

キーサーバ

KS(config)# **crypto pki enroll GETVPN** %

登録できます。%最初に認証を試行しています。

証明書には次の属性があります。フィンガープリントMD5: CD60821B 034ACFCF D1FD66D3 EA27D688フィンガープリントSHA1: 3F0C3A05 9BC786B4 8828007A 78A3973D B507F9C4 %この証明書を受け入れますか？[yes/no]：はい。トラストポイントCA証明書は受け入れられました。% Start certificate enrollment .. %チャレンジパスワードを作成します。証明書を失効させるには、CA管理者にこのパスワードを口頭で伝える必要があります。 セキュリティ上の理由から、パスワードは設定に保存されません。 メモしておいてください。パスワード：パスワードを再入力してください： %証明書のサブジェクト名には次が含まれます：OU=GETVPN_KS %証明書のサブジェクト名には次が含まれます： get-KS %サブジェクト名にルータのシリアル番号を含めますか？[yes/no]: no % IPアドレスをサブジェクト名に含めますか。[no]: CAから証明書を要求しますか？[yes/no]: yes %認証局に証明書要求が送信されました。 %「show crypto pki certificate verbose GETVPN」コマンドを実行すると、フィンガープリントが表示されます。

グループメンバー

GM(config)# **crypto pki enroll GETVPN** %

登録できます。%最初に認証を試行しています。

証明書には次の属性があります。指紋MD5: E184D9EC 2D6499B3 D5D78E8A CD0B910C指紋SHA1: A31EE77D A4FFA2B7 90F3993300337A6D 46CBE32E

%この証明書を受け入れますか？[yes/no]:y % Trustpoint CA certificate accepted.% Start certificate enrollment .. %チャレンジパスワードを作成します。口頭で提供する必要があります

CA管理者のパスワードを入力して、証明書を失効させます。

セキュリティ上の理由から、パスワードは設定に保存されません。

メモしておいてください。

パスワード：

パスワードの再入力：

%証明書のサブジェクト名には次が含まれます： OU=GETVPN %証明書のサブジェクト名には次が含まれます： get_GM %サブジェクト名にルータのシリアル番号を含めますか？[yes/no]: n %サブジェクト名にIPアドレスを含めますか？[no]: n CAから証明書を要求しますか？[yes/no]: y % Certificate request sent to Certificate Authority %「show crypto pki certificate verbose GETVPN」コマンドを実行すると、フィンガープリントが表示されます。

3 – 両方のデバイスで「show crypto pki certificates verbose」コマンドを使用して、新しく発行さ

れた証明書がそれぞれの認証されたトラストポイントにインポートされることを確認します（CA証明書もインポートする必要があります）。

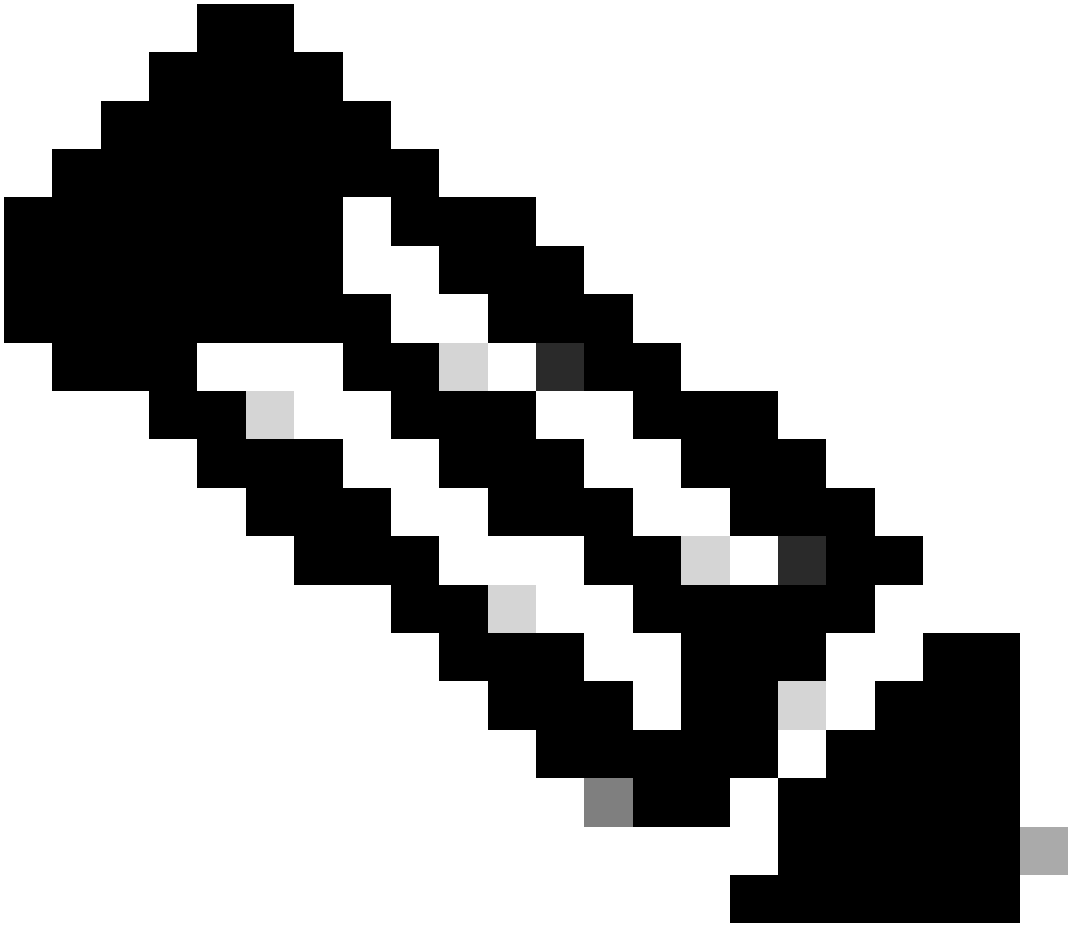
キーサーバ

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

.**証明書のステータス：利用可能なバージョン： 3証明書シリアル番号（16進数）: 05証明書の使用方法：汎用発行者： 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**サブジェクトキー9情報：公開キーアルゴリズム：** rsa**暗号化RSA公開キー：（2049ビット）署名アルゴリズム：** RSA**暗号化フィンガープリントを使用したSHA256 MD5: 51576B28 1203C5EC 06FF408E F90B0E47フィンガープリントSHA1: 9D5B10E5 E9418C000895E 6DC7 9BE86624 B273CF15 X509v3拡張：X509v3キー使用法：A0000000デジタル署名キー暗号化X509v3件名キー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: nvstorage: ram:Root-CAcisco#5.cer Key Label: pkikey キーストレージデバイス：private config CA証明書ステータス：使用可能なバージョン： 3証明書シリアル番号（16進数）: 01証明書の使用方法：署名の発行者： cn=Root-CA.cisco.com OU=LAB** Subject: cn=Root-CA.cisco.com OU=LAB**有効期間：** start date: 11:28:11 UTC Sep 9 2025 end date: 11:28:11 UTC Sep 4 045 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key:（1024ビット）Signature Algorithm: SHA256 with RSA Encryption Fingerprint MD5: E184D9EC 2D6499B3 D5D78E8A CD0B910C Fingerprint SHA1: A31EE77D4A FFA2B7 90F39933 00337A6D 46CBE32E X509v3**拡張：** X509v3**キーの使用方法：** 86000000**デジタル署名キー証明書の署名**CRL**署名** X509v3**件名キー**ID: 4F0F7126 6D21324A 585A0BF3 652EB5617D 1 8B2F X509v3**基本制約：** CA: TRUE X509v3 Authority Key ID: 4F0F7126 6D21324A 585A0BF3 652EB 561 17D18B2F Authority Info Access: Cert install time: 11:58:16 UTC Sep 9 2025**関連トラストポイント：** GETVPN Storage: nvram:Root-CAcisco#1CA.cer

グループメンバー

GM# **show crypto pki certificates verbose GETVPN Certificate**ステータス：入手可能バージョン： 3証明書シリアル番号（16進数）: 08証明書の使用方法：一般目的発行者： cn=Root-CA.cisco.com OU=LAB件名： 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 1920 39 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key:（2049ビット）署名アルゴリズム： SHA256 with RSA Encryption Fingerprint MD5: CA8AF53B B7424CD6 4C94F689 6FDD441F Fingerprint SHA1: 8ACE3BC0 5BC6BBF1 9696805 2998AFDB 2A73A65E X509v3拡張：X509v3キーの使用方法：A0000000デジタル署名キーの暗号化X509v3サブジェクトキーID:F3C5E024 F93B09A0 4F99215E 34EB9C8855C7CAD 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 ビット）署名アルゴリズム：SHA256 with RSA Encryption Fingerprint MD5: E184D9EC 2D6499B3 D5D78E8A CD0B910C Fingerprint SHA1: A31EE77D A4FFA2B7 90F3993300337A6D 46CBE32E X5 09v3拡張： X509v3キー使用法： 86000000デジタル署名キー証明書Sign CRL署名X509v3件名キー**ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F X509v3**基本制約： CA: TRUE X509v3 Authority Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F Authority Info Access: Associated Trustpoints: GETVPN Storage: nvram:Root-CAcisco#1CA.cer**



注：証明書認証の場合、共通名(CN)、拡張キー使用法(EKU)、有効期間などのデバイスのIDを検証するための正しいパラメータが、提供された証明書に含まれていることを確認してください。

GETVPNの設定

GETVPNの重要な機能は、ISAKMPおよびGDOI機能の前に設定しておくことをお勧めする以前の設定に依存します。

4. – プライマリキーサーバで、「getKey」というラベルを持つエクスポート可能なRSAキーを生成します。 このキーは、すべてのキーサーバで同一である必要があります。したがって、次の手順ではエクスポート可能な機能が不可欠です。

KS(config)# **crypto key generate rsa general-keys label getKey modulus 1024 exportable** キーの名前は次のとおりです。**getKey** %キーのモジュラスサイズは1024ビット%1024ビットのRSAキーを生成しています。キーはエクスポート可能です。 .. [OK]（経過時間0秒）

5. – グループメンバーのルータが通過する際に暗号化する必要のある対象トラフィックを含む拡張アクセスリストを定義します。セカンダリキーサーバで、同じ名前を使用して同じアクセスリストを定義します。

プライマリキーサーバ

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 0.0.0.0 255.255 KS(config-ext-nacl)# 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255

セカンダリキーサーバ

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 0.0.2 55.255 KS2(config-ext-nacl)# 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255

6- GDOIグループメッセージ交換で始まるGMとのセキュアな接続を確立するために使用されるISAKMPポリシー(IPsec-set)、IPsecトランスフォームセット、およびIPsecプロファイルを設定します。

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**

COOPの設定

7. – 協調的な実装では、関係するキーサーバは同じ設定である必要があります。以前作成したエクスポート可能なRSAキーをプライマリキーサーバからエクスポートし、秘密キーと公開キーの両方をセカンダリキーサーバ(KS2)にインポートします。 プライマリキーサーバが応答しなくなった場合、セカンダリキーサーバはグループ内のすべてのGMデバイスに対するキー再生成の制御を続行します。

プライマリキーサーバ

KS(config)# **crypto key export rsa getKey pem terminal 3des cisco123** %キー名： getKey使用方法： General Purpose Key Keyデータ：
-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFtHBAdGV3ZPaGQcs aqO
1H9gmJWJNEeQvTND/oSrhN+jSSm+8f27RvDnIMYLDl9MndZ+rPqCPM/3NXE07 5bOsrT7B2uOpCBmAJK9iiTsfr01Qc4IzuWcK2CN5Ov
LhyR2pKPviqwkSmGS zbaErQCH7evvjutYHE6DhOTLubxQIDAQAB -----END PUBLIC KEY----- -----BEGIN RSA PRIVATE KEY-----処理タイプ：4,ENCRYPTED DEK-Info:DES-EDE3-CBC,AA98923B28E00DCC1To
ym6cRvqEXBlt97UZdGyusf3cW/iumb7oD9/09q5if4ouoE

brPykL3No0WMI7h56WQPiAHzLu5IZ+CTQHwwgYvXwHNpOHjmTMOgf9FG856GosM3kjP58QDupSc1W70+C9

zsCM3QmwbRs6JGBP5Rb36f+895xoyqzWA8G5sQlizE1oP4lM3Zx5DukgTXLzIDL7w0dPEYBd1aDhAJQf8dB/Zu

GvQWxad4gL6SssEyzigbzdSdRwBS+0DLOm05hOUU8rNiWit1TCsTPflwuTjlyxgRbyKvtXdoURvuTP3M6/DOppe2

n26bXC2DcURk8nMtIrIHAPvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb

AI286GHqCOw2AxDcoMzcanQYw1VNgHG7SUsbaday7enuJtwbf2Pjkf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C

2PkLiQvQwuYi8J9SgM+391aFrf0NRXFHrM7T9MQcBBIcbo0BtfG4ICBuIltpG+BpCty/XW99dvuhqh9hjqfy2sKqF4H

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwvvWQjewrA0K

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

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

セカンダリキーサーバ

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

% PEM形式のパブリック汎用キーまたは証明書を入力します。

%空白行で終了するか、単独の行で「終了」します。-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFtHBAdGV3ZPaGQcsAqO 1H9gmJWJNEeQvTND/oSrhN+jSSm+8f27RvO
dnIMYLDl9MndZ+rPqCPM/3NXE07
5bOsrT7B2uOpCBmAJK9iiTsfr01Qc4Izu5fwWcK2CN5OvLhyR2pKPviqwkSmGSzBaErQCH7evjutYHE6DhDhOTTL ubxQIDAQAB -----
END PUBLIC KEY----- quit % PEM形式の暗号化された汎用鍵を入力します。

% 1行に「quit」が単独で含まれている場合に終了します。-----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

n26bXC2DcURk8nMtIrIHAPvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb

AI286GHqCOw2AxDcoMzcanQYw1VNgHG7SUsbaday7enuJtwbf2Pjkf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C

2PkLiQvQwuYi8J9SgM+391aFrf0NRXFHrM7T9MQcBBIcbo0BtfG4ICBuIltpG+BpCty/XW99dvuhqh9hjqfy2sKqF4H

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwvvWQjewrA0K

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

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

quit

%キーペアのインポートに成功しました。

8- COOP KSに対して定期的ISAKMPを設定する必要があります。 このようにして、プライマリKSはセカンダリキーサーバをモニタできます

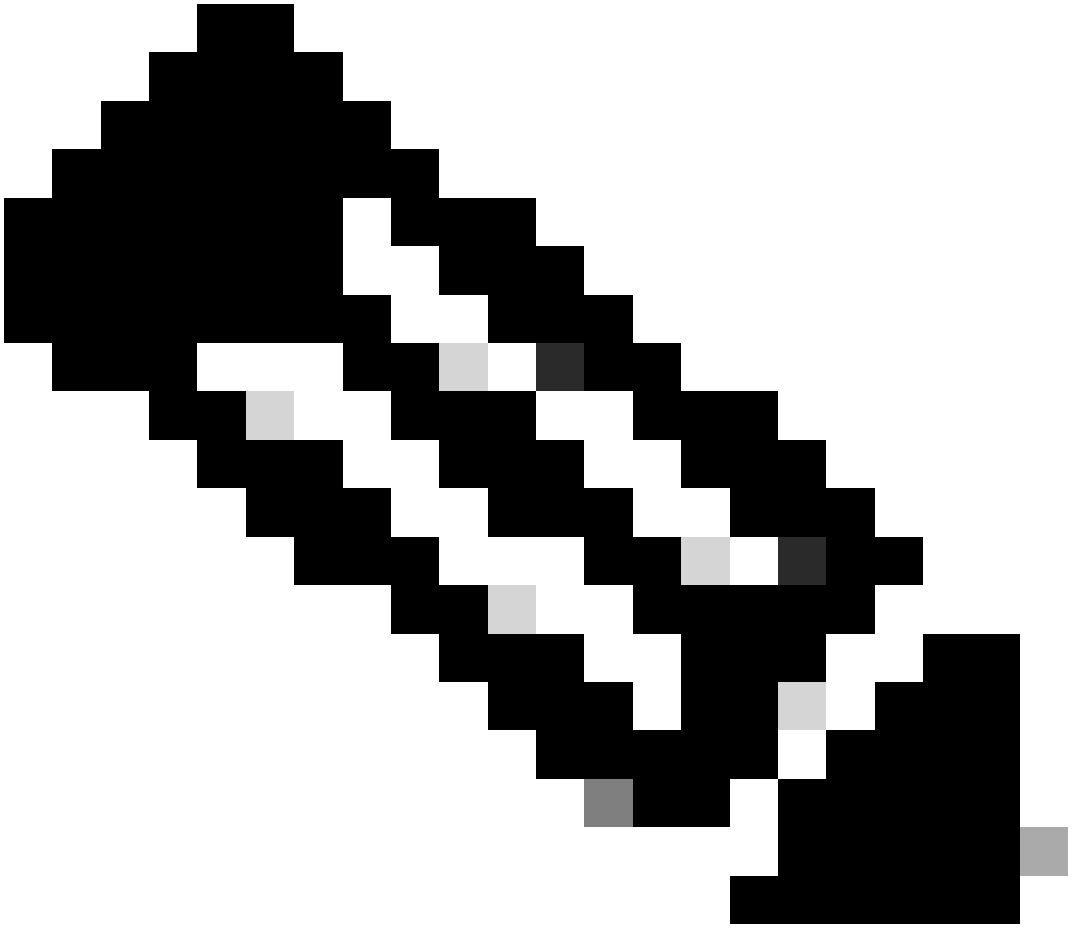
プライマリキーサーバ

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

セカンダリキーサーバ

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

COOPキーサーバは、プライマリからセカンダリへ一方向の通信を交換します。セカンダリKSが30秒の間隔でプライマリKSから応答を受信しない場合、セカンダリKSはプライマリKSへの接続を試行し、更新された情報を要求します。セカンダリKSがプライマリKSから60秒の間隔で受信しない場合、COOP再選択プロセスがトリガーされ、新しいプライマリKSが選択されます。



注:GMとKSの間の定期的なDPDは必要ありません。

キーサーバ間の選出は、設定された最も高いプライオリティ値に基づいて行われます。同じ場合は、最も高いIPアドレスに基づきます。同じクリプトポリシーの拡張アクセスリストを使用して、各キーサーバに同じGDOIグループを設定します。

プライマリキーサーバ

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 866 400 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. – 同じローカルサーバ設定で、データプレーントラフィック用の暗号化ポリシーと以前に設定したアクセスリストを有効にします。

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

ローカルサーバの設定では、COOPキーサーバ機能が有効になっている設定レベルが優先されます。定義された優先順位によって、このキーサーバの役割が決まります。 すべてのKSが互いを認識できるように、セカンダリキーサーバを明示的に設定する必要があります。

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キーサーバ設定の最後の部分は、キーパケットの送信元IPアドレスの定義です。これは、キーサーバルータのいずれかのインターフェイスで設定されたIPアドレスです。

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

セカンダリキーサーバで同じ設定手順を複製し、優先度を低く設定してルータをセカンダリサーバとして特定し、プライマリKSアドレスを登録します。

セカンダリキーサーバ

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 rsaKey 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 ipv4 172.16.14 .2 KS2(gdoi-coop-ks-config)# exit KS2(gkm-local-server)# address ipv4 172.18.5.2

10. – グループメンバールータでは、GDOIグループ設定はキーサーバに比べて少ない設定で構成されています。グループメンバーが必要とされるのは、ISAKMPポリシーを設定し（デフォルト設定）、同じ認証方式のGDOIグループを使用し、GMルータが登録可能なキーサーバのIPアドレスを持つことだけです。

グループメンバー

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**

グループメンバー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 484GM2 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

確認

設定の各段階の設定を次のように確認します。

主要サーバ上のデータプレーントラフィックのACL

このshowコマンドは、定義された対象トラフィックに間違いがないことを確認するために使用されます。

KS# **show ip access-lists data_plane Extended IP access list data_plane** 10 permit ip 10.0.0.0 0.0.255 172.16.0.0 0.0.255.255 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0.0.0.255 KS2# **show ip access-data_plane拡張IPアクセスリストdata_plane** 10 permit ip 10.0.0 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登録ステータス：

コマンド'show crypto gkm ks coop'は、キーサーバ間の現在のCOOPステータスを表示します。これにより、プライマリキーサーバの正体、キーサーバが属するGDOIグループ、個人およびピアの優先順位、およびプライマリからセカンダリサーバに送信される次のメッセージに関するタイマーが示されます。

プライマリキーサーバ

KS# **show crypto gkm ks coop** Crypto Gdoiグループ名：GETVPNグループハンドル：1073741826、ローカルキーサーバハンドル：1073741826ローカルアドレス：10.191.61.114ローカル優先度：100ローカルKSロール：プライマリ、ローカルKSステータス：Aliveローカルksバージョン：1.0.27プライマリタイマー：プライマリリフレッシュポリシー時間：20残り時間：ユーザあたり5タイマー残り時間：0 Anti リプレイシーケンス番号：63046ピアセッション：セッション1：サーバハンドル：1073741827ピアアドレス：10.191.61.115ピアバージョン：1.0.23ピア優先度：75ピアKSロール：セカンダリ（KS用）、ピアKSステータス：Aliveアンチリプレイシーケンス番号： 0 IKE状態：確立カウンタ： 63040 MSGS送信：応答要求でMSGS送信： 3 ANN MSGS recv: 32応答要求でMSGS recv: 4パケット送信ドロップ： 3パケット送信ドロップ： 0送信バイト合計： 42550002受信バイト合計：22677

セカンダリキーサーバ

KS2# **show crypto gkm ks coop** Crypto Gdoiグループ名：GETVPNグループハンドル： 1073741829、ローカルキーサーバハンドル： 1073741827ローカルアドレス： 10.191.61.115ローカル優先度： 75ローカルKSロール：セカンダリ、ローカルKSステータス： Aliveローカルバージョン： 1.0.23セカンダリタイマー： Secプライマリ平均時間： 30残り時間： 11、再試行： 0無効な 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 Status: Established counters: 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

グループGETVPNの情報と連携キーサーバのバージョン情報を表示します。

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

グループメンバーの登録

GM# **show crypto gkm group GETVPN**グループ名：GETVPNグループID:484グループタイプ：GDOI(ISAKMP)暗号化パス：ipv4 Key Management Path:ipv4 Rekeys received : 0 IPSec SA方向：両方のグループサーバリスト：10.191.61.115グループGETVPNのグループメンバー情報：IPSec SA方向：両方のACLを: 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 with : 10.191.61.115 Re-registers in : 5642 sec succeeded registration: 1 Attempted registration: 1 Last rekey from Unknown :最後のキー再生成シーケンス番号： 0ユニキャストキー再生成を受信： 0キー再生成を送信： 0キー再生成を受信： 0キー再生成を受信しませんでした： 0 DPエラー監視： 0 IPSEC init regを実行しました： 0 IPSEC init regを延期しました： 0アクティブTEK番号： 1 SAトラック（OID/ステータス）: 0フェールクローズ復元を無効にしました。 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 10.0.0.0.0.0.255 KEK POLICY: Rekey Transport Type : ユニキャストライフタイム（秒）:85185暗号化アルゴリズム：3DESキーサイズ：192シグニチャハッシュアルゴリズム：HMAC_AUTH_SHAシグニチャキー長（ビット）：ダウンロードされた現在のKSポリシーACEの1296 TEKポリシー：GigabitEthernet1:IPsec SA:spi: 0x535F673B(1398761275)変換： esp-aes-sha-hmac timing：残りのキーライフタイム（秒）: 5 988)アンチリプレイ（カウンタベース）:64タグメソッド：無効なalgキーサイズ：16（バイト）sigキーサイズ：20（バイト）encap:ENCAPS_TUNNEL KGSポリシー：REG_GM:local_addr 10.191.61.116 overall chech P2Pポリシー：REG_GM:local_addr 10.191.61.116

トラブルシュート

COOPキーサーバの選択

syslogメッセージは、COOPプロセスに関する問題の追跡と特定に役立ちます。このプロセスに関連する情報だけを表示するには、COOPキーサーバでGDOIデバッグを有効にします。

KS# **debug crypto gdoi ks coop**

COOP選択プロセスが開始されると、次のsyslogメッセージがすべてのキーサーバに表示されます。

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

選択プロセスが完了すると、メッセージ「COOP_KS_TRANS_TO_PRI」に新しいプライマリキーサーバの情報が表示されます。このメッセージはプライマリおよびセカンダリキーサーバに表示されます。選出プロセスの最初の時点で、以前のプライマリには「NONE」と表示されることが予想されます。

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

キーサーバの再選択がある場合、メッセージには前のプライマリサーバのIPアドレスが含まれます。

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

COOPセカンダリキーサーバへの接続が失われると、「COOP_KS_UNREACH」メッセージが表示されます。プライマリKSはすべてのセカンダリKSの状態を追跡し、このメッセージを使用してセカンダリKSへの接続が失われたことを示します。セカンダリKSは、プライマリKSの状態だけを追跡します。セカンダリKSのこのメッセージは、プライマリKSとの接続が失われたことを示します。

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

COOP KS間の接続が復元されると、「COOP_KS_REACH」メッセージが表示されます。

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

PKI登録の問題

トラストポイントの登録または認証の問題をデバッグする場合は、PKIデバッグを使用します。

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。