

Contrôle CRL HTTP sur un concentrateur Cisco VPN 3000

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Diagramme du réseau](#)

[Configurez le concentrateur VPN 3000](#)

[Instructions pas à pas](#)

[Surveillance](#)

[Vérifiez](#)

[Logs de concentrateur](#)

[Logs réussis de concentrateur](#)

[Logs défectueux](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment activer la Liste des révocations de certificat (CRL) vérifiant des Certificats de l'autorité de certification (CA) installés dans le concentrateur de Cisco VPN 3000 utilisant le mode de HTTP.

On s'attend à ce que normalement un certificat soit valable sa période entière de validité. Cependant, si un certificat devient dû non valide à des choses telles qu'un changement de nom, modification d'association entre le sujet et le CA, et compromission de Sécurité, le CA retire le certificat. Sous X.509, les CAs retirent des Certificats en émettant périodiquement un CRL signé, où chaque certificat retiré est identifié par son numéro de série. L'activation de vérifier CRL signifie que chaque fois que le concentrateur VPN utilise le certificat pour l'authentification, elle vérifie également le CRL pour s'assurer que le certificat étant vérifié n'a pas été retiré.

Bases de données du Protocole LDAP (Lightweight Directory Access Protocol) /HTTP d'utilisation CAs pour enregistrer et distribuer CRLs. Ils pourraient également utiliser des autres moyens, mais le concentrateur VPN se fonde sur l'accès LDAP/HTTP.

Vérifier du HTTP CRL est introduit dans la version 3.6 ou ultérieures de concentrateur VPN. Cependant, vérifier basé sur LDAP CRL a été introduit dans les releases 3.x plus tôt. Ce document discute seulement CRL vérifiant utilisant le HTTP.

Note: La taille de mise en cache CRL des concentrateurs VPN série 3000 dépend de la plateforme et elle ne peut pas être configurée selon le souhait de l'administrateur.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Vous avez avec succès établi le tunnel d'IPsec des clients matériels VPN 3.x utilisant des Certificats pour l'authentification d'Échange de clés Internet (IKE) (sans vérifier CRL activé).
- Votre concentrateur VPN a la Connectivité au serveur CA à tout moment.
- Si votre serveur CA est connecté à l'interface publique, alors vous avez ouvert des règles nécessaires dans le filtre (par défaut) public.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C de version 4.0.1 de concentrateur VPN 3000
- Client matériel VPN 3.x
- Serveur de Microsoft CA pour la génération de certificat et CRL vérifiant s'exécuter sur un serveur de Windows 2000.

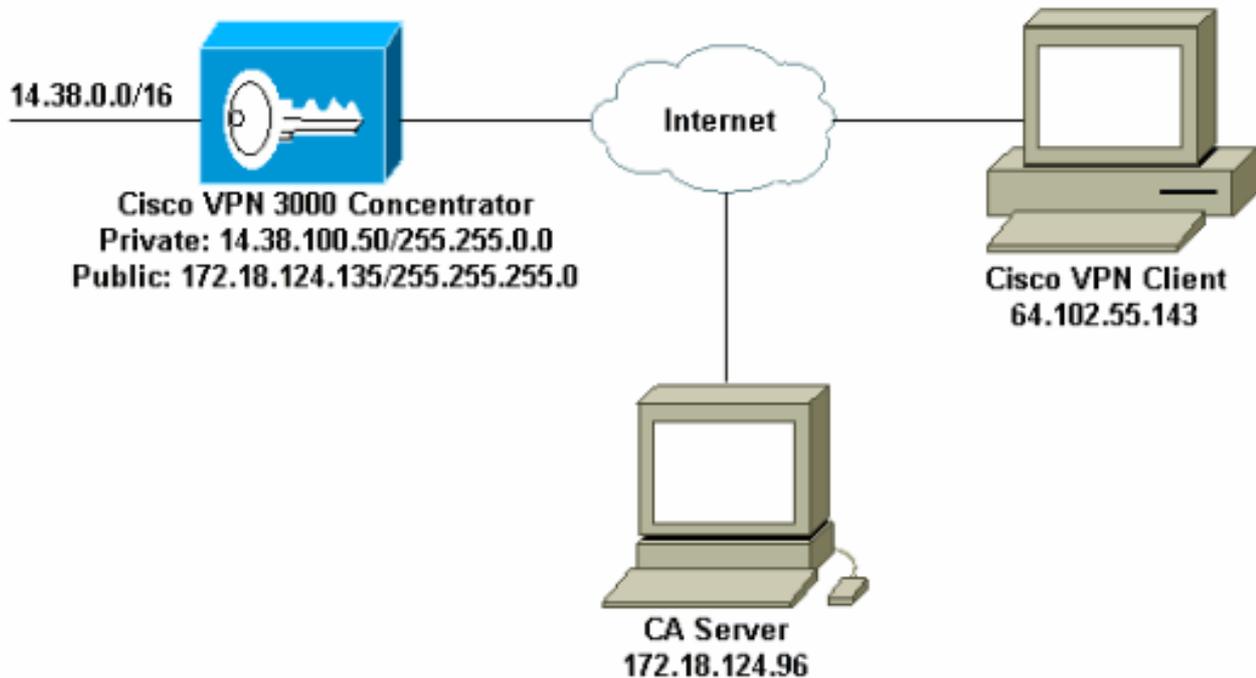
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurez le concentrateur VPN 3000

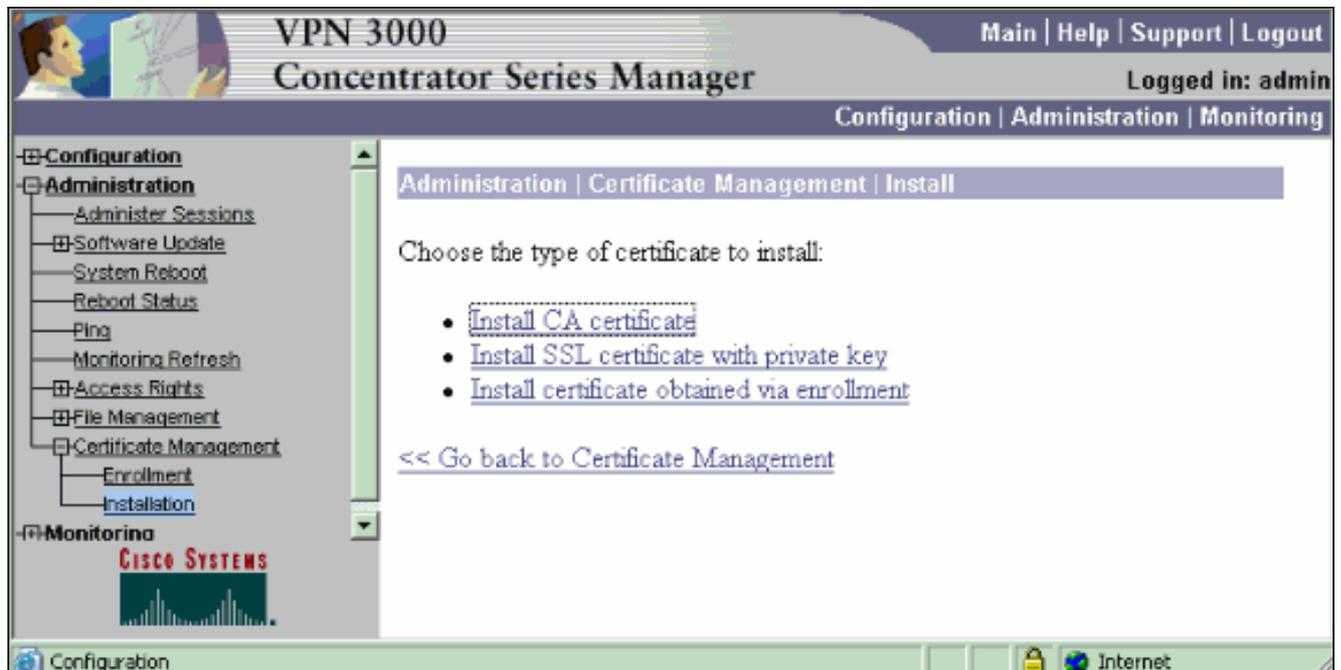
Instructions pas à pas

Terminez-vous ces étapes pour configurer le concentrateur VPN 3000 :

1. **Administration > Certificate Management** choisi pour demander un certificat si vous n'avez pas un certificat. Choisi **a cliquez ici pour installer un certificat** pour installer le certificat racine sur le concentrateur VPN.



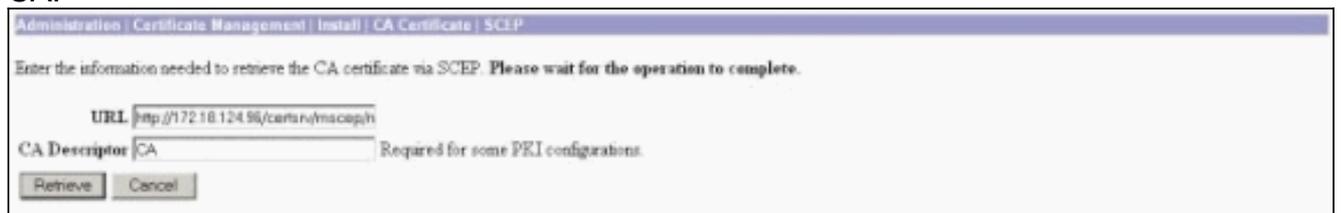
2. Choisi **installez le certificat de CA.**



3. SCEP choisi (inscription de certificat simple Protocol) pour récupérer les Certificats CA.



4. De la fenêtre SCEP, écrivez l'URL complet du serveur CA dans la boîte de dialogue URL. Dans cet exemple, l'adresse IP du serveur CA est 172.18.124.96. Puisque cet exemple utilise le serveur CA de Microsoft, l'URL complet est `http://172.18.124.96/certsrv/mscep/mscep.dll`. Ensuite, écrivez un descripteur sur un mot dans la boîte de dialogue de descripteur CA. Cet exemple utilise le CA.



5. Cliquez sur **Retrieve**. Votre certificat de CA devrait apparaître sous la fenêtre d'Administration > Certificate Management. Si vous ne voyez pas un certificat, passez de retour à l'étape 1 et suivez la procédure de nouveau.

Administration | Certificate Management Thursday, 13 August 2003 11:45:41
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CAs](#)] [[Clear All CAs](#)] (current: 3, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
janb-ca-ra at Cisco Systems	janb-ca-ra at Cisco Systems	03/12/2005	Yes	View Configure Delete SCEP Show RSA

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificate [[Generate](#)] *Note: The public key in the SSL certificate is also used for the SSH host key.*

Subject	Issuer	Expiration	Actions
14.38.100.50 at Cisco Systems, Inc.	14.38.100.50 at Cisco Systems, Inc.	08/14/2005	View Renew Delete

Enrollment Status [[Remove All Errors](#)] [[Timed Out](#)] [[Rejected](#)] [[Cancelled](#)] [[In Progress](#)] (current: 0 available: 20)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

6. Une fois que vous avez le certificat de CA, l'**Administration > Certificate Management** choisi > **s'inscrivent**, et cliquent sur le **certificat d'identité**.

Administration | Certificate Management | Enroll

This section allows you to create an SSL or identity certificate request. The identity certificate request allows the VPN 3000 Concentrator to be enrolled into the PKI. The certificate request can be sent to a CA, which will issue a certificate. *The CA's certificate must be installed as a Certificate Authority before installing the certificate you requested.*

Choose the type of certificate request to create:

- [Identity certificate](#)
- [SSL certificate](#)

[<< Go back to Certificate Management](#)

7. Le clic **s'inscrivent** par l'intermédiaire de SCEP à... pour s'appliquer pour le certificat d'identité.

Administration | Certificate Management | Enroll | Identity Certificate

Select the enrollment method for the identity certificate. To install a certificate with SCEP, the issuing CA's certificate must also be installed with SCEP. [Click here to install a new CA using SCEP before enrolling.](#)

- [Enroll via PKCS10 Request \(Manual\)](#)
- [Enroll via SCEP at janb-ca-ra at Cisco Systems](#)

[<< Go back and choose a different type of certificate](#)

8. Terminez-vous ces étapes pour compléter la forme d'inscription :Écrivez le nom commun pour que le concentrateur VPN soit utilisé dans l'Infrastructure à clés publiques (PKI) dans le domaine commun du nom (NC).Écrivez votre service dans le domaine de l'unité organisationnelle (OU). L'OU devrait apparier le nom de groupe configuré d'IPsec.Entrez dans votre organisation ou société dans le domaine de l'organisation (o).Entrez dans votre ville ou ville dans le domaine de la localité (l).Entrez dans votre état ou province dans le domaine d'état/province (fournisseur de services).Entrez dans votre pays dans le domaine du pays (c).Écrivez le nom de domaine complet (FQDN) pour que le concentrateur VPN soit utilisé dans le PKI dans le domaine du nom de domaine complet (FQDN).Écrivez l'adresse e-mail pour que le concentrateur VPN soit utilisé dans le PKI dans le domaine alternatif soumis de nom (adresse e-mail).Entrez le mot de passe de défi pour la demande de certificat dans le domaine de mot de passe de défi.Ressaisissez le mot de passe de défi dans le domaine de mot de passe de défi de vérifier.Sélectionnez la taille de clé pour la paire de clés RSA générée de la liste déroulante de taille de clé.

Administration | Certificate Management | Enroll | Identity Certificate | SCEP

Enter the information to be included in the certificate request. Please wait for the operation to finish.

Common Name (CN) Enter the common name for the VPN 3000 Concentrator to be used in this PKI.

Organizational Unit (OU) Enter the department.

Organization (O) Enter the Organization or company.

Locality (L) Enter the city or town.

State/Province (SP) Enter the State or Province.

Country (C) Enter the two-letter country abbreviation (e.g. United States = US).

Subject AlternativeName (FQDN) Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.

Subject AlternativeName (E-Mail Address) Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.

Challenge Password

Verify Challenge Password Enter and verify the challenge password for this certificate request.

Key Size Select the key size for the generated RSA key pair.

9. Choisissez **inscrivez-vous** et visualisez l'état SCEP dans l'état de sondage.

10. Allez à votre serveur CA approuver le certificat d'identité. Une fois qu'il est approuvé sur le serveur CA, votre état SCEP devrait être installé.

Administration | Certificate Management | Enrollment | Request Generated

A certificate request has been generated.

SCEP Status: Installed

- [Go to Certificate Management](#)
- [Go to Certificate Enrollment](#)
- [Go to Certificate Installation](#)

11. Sous la Gestion de certificat, vous devriez voir votre certificat d'identité. Si vous ne faites pas, vérifiez les logins de votre serveur CA pour plus de débogage.

Administration | Certificate Management Thursday, 15 August 2002 11:50:10
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [View All CRL Caches | Clear All CRL Caches] (current: 3, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
janb-ca-ra at Cisco Systems	janb-ca-ra at Cisco Systems	03/12/2005	Yes	View Configure Delete SCEP Show EAs

Identity Certificates (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
Concentrator_cert at Cisco	janb-ca-ra at Cisco Systems	08/15/2003	View Renew Delete

SSL Certificate [[Generate](#)] *Note: The public key in the SSL certificate is also used for the SSH host key.*

Subject	Issuer	Expiration	Actions
14.38.100.50 at Cisco Systems, Inc.	14.38.100.50 at Cisco Systems, Inc.	08/14/2005	View Renew Delete

Enrollment Status [[Remove All](#) | [Expired](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In-Progress](#)] (current: 0 available: 19)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

12. **Vue** choisie sur votre certificat reçu pour voir si votre certificat a un point de distribution CRL (CDP). Le CDP répertorie tous les points de distribution CRL de l'émetteur de ce certificat. Si vous avez le CDP sur votre certificat, et vous employez un nom DNS pour envoyer une requête au serveur CA, assurez-vous que vous faites définir des serveurs DNS dans votre concentrateur VPN pour résoudre l'adresse Internet avec une adresse IP. Dans ce cas, le nom d'hôte du serveur de l'exemple CA est le jazib-PC qui le résout à une adresse IP de 172.18.124.96 sur le serveur DNS.



13. Cliquez sur Configurer sur votre certificat de CA pour activer CRL vérifiant sur les Certificats reçus. Si vous avez le CDP sur votre certificat reçu et vous voudriez l'utiliser, alors sélectionnez les **points de distribution de l'utilisation CRL du certificat étant vérifié**. Puisque le système doit récupérer et examiner le CRL d'un point de la distribution du réseau, l'activation de vérifier CRL pourrait ralentir des temps de réponse de système. En outre, si le réseau est lent ou congestionné, vérifier CRL pourrait échouer. Permettez à la mise en cache CRL d'atténuer ces problèmes potentiels. Ceci enregistre le CRLs récupéré dans la mémoire volatile locale et permet donc au concentrateur VPN pour vérifier l'état de révocation des Certificats plus rapidement. La mise en cache CRL étant activé, le concentrateur VPN d'abord vérifie si le CRL exigé existe dans le cache et vérifie le numéro de série du certificat contre la liste de numéros de série dans le CRL quand il doit vérifier l'état de révocation d'un certificat. Le certificat est considéré retiré si son numéro de série est trouvé. Le concentrateur VPN récupère un CRL d'un serveur externe l'un ou l'autre quand il ne trouve pas le CRL exigé dans le cache, quand la période de validité du CRL caché a expiré, ou quand configurés régénèrent temps se sont écoulés. Quand le concentrateur VPN reçoit un nouveau CRL d'un serveur externe, il met à jour le cache avec le nouveau CRL. Le cache peut contenir jusqu'à 64 CRLs. **Note:** Le cache CRL existe dans la mémoire. Par conséquent, la réinitialisation du concentrateur VPN efface le cache CRL. Les repopulates de concentrateur VPN le cache CRL avec CRLs mis à jour en tant que lui traite de nouvelles demandes d'authentification de pair. Si vous sélectionnez les **points de distribution statiques de l'utilisation CRL**, alors vous pouvez utiliser jusqu'à cinq points de distribution statiques CRL, comme spécifié sur cette fenêtre. Si vous choisissez cette option, vous devez écrire au moins un URL. Vous pouvez également sélectionner des **points de distribution de l'utilisation CRL du certificat étant vérifié**, ou sélectionner les **points de distribution statiques de l'utilisation CRL**. Si le concentrateur VPN ne peut pas trouver cinq points de distribution CRL dans le certificat, il ajoute les points de distribution statiques CRL, jusqu'à une limite de cinq. Si vous choisissez cette option, activez au moins un point de distribution Protocol CRL. Vous devez également entrer dans au moins les points de distribution statiques un (et pas plus de cinq) CRL. Ne sélectionnez **aucun CRL vérifiant** si vous voulez désactiver vérifier CRL. Sous la mise en cache CRL, sélectionnez la case **activée** pour permettre au concentrateur VPN pour cacher CRLs récupéré. Le par défaut n'est pas d'activer la mise en cache CRL. Quand vous désactivez la mise en cache CRL (unselect la case), le cache CRL est effacé. Si vous configurez une stratégie de récupération CRL qui utilise des points de distribution CRL du certificat étant vérifié, choisissez un protocole de point de distribution pour l'utiliser pour récupérer le CRL. Choisissez le **HTTP** dans ce cas pour récupérer le CRL. Assignez les règles de HTTP au

filtre d'interface publique si votre serveur CA est vers l'interface publique.

Administration | Certificate Management | Configure CA Certificate

Certificate janz-ca-ca at Cisco Systems

CRL Retrieval Policy

Use CRL distribution points from the certificate being checked

Use static CRL distribution points

Use CRL distribution points from the certificate being checked or else use static CRL distribution points

No CRL checking

Choose the method to use to retrieve the CRL.

CRL Caching

Enabled

Refresh Time

Check to enable CRL caching. Disabling will clear CRL cache.

Enter the refresh time in minutes (5 - 1440). Enter 0 to use the Next Update field in the cached CRL.

CRL Distribution Points Protocols

HTTP

LDAP

Choose a distribution point protocol to use to retrieve the CRL. If you choose HTTP, be sure to assign HTTP rules to the public interface filter. (For more information, click Help.) If you choose LDAP, configure the LDAP distribution point defaults below.

LDAP Distribution Point Defaults

Server

Server Port

Login DN

Password

Verify

Enter the hostname or IP address of the server.

Enter the port number of the server. The default port is 389.

Enter the login DN for access to the CRL on the server.

Enter the password for the login DN.

Verify the password for the login DN.

Static CRL Distribution Points

LDAP or HTTP URLs

- Enter up to 5 URLs to use to retrieve the CRL from the server.
- Enter each URL on a new line.

Certificate Acceptance Policy

Accept Subordinate CA Certificates

Accept Identity Certificates signed by this issuer

Apply Cancel

[Surveillance](#)

L'Administration > Certificate Management choisi et cliquent sur en fonction la **vue tous les caches CRL** pour voir si votre concentrateur VPN a caché n'importe quel CRLs du serveur CA.

[Vérifiez](#)

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

[Logs de concentrateur](#)

Permettez à ces événements sur le concentrateur VPN afin de s'assurer que CRL vérifiant des travaux.

1. **La configuration** > le **système** > les **événements** choisis > **classe** pour placer les niveaux se connectants.
2. Sous le nom de classe sélectionnez l'**IKE**, l'**IKEDBG**, l'**IPSEC**, l'**IPSECDBG**, ou le **CERT**.
3. Cliquez sur **ajoutent** ou **modifiant**, et choisissent la **sévérité pour se connecter l'option 1-13**.
4. Cliquez sur **Apply** si vous voulez modifier, ou **ajoutez** si vous voulez ajouter une nouvelle entrée.

[Logs réussis de concentrateur](#)

Si votre vérifier CRL est réussi, ces messages sont vus dans les journaux d'événements filtrables.

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl
```

```
1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)
```

```
1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1
Certificate has not been revoked: session = 2
```

```
1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1
CERT_Callback(62f56e8, 0, 0)
```

```
1320 08/15/2002 13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53
Group [ipsecgroup]
Validation of certificate successful
(CN=client_cert, SN=61521511000000000086)
```

Référez-vous aux [logs réussis de concentrateur](#) pour la sortie complète d'un log réussi de concentrateur.

[Logs défectueux](#)

Si vos CRL vérifiant dans non réussi, ces messages sont vus dans les journaux d'événements filtrables.

```
1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2
Failed to retrieve revocation list: session = 5
```

```
1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2
CRL retrieval over HTTP has failed. Please make sure that proper filter rules
have been configured.
```

```
1335 08/15/2002 18:00:36.730 SEV=7 CERT/8 RPT=2
Error processing revocation list: session = 5, reason = Failed to retrieve CRL
from the server.
```

Référez-vous aux [logs retirés de concentrateur](#) pour la sortie complète d'un log défectueux de concentrateur.

Référez-vous aux [logs réussis de client](#) pour la sortie complète d'un log réussi de client.

Référez-vous aux [logs retirés de client](#) pour la sortie complète d'un log défectueux de client.

[Dépannez](#)

Référez-vous aux [problèmes de connexion de dépannage sur le concentrateur VPN 3000](#) pour plus d'information de dépannage.

[Informations connexes](#)

- [Page de support pour Concentrateurs VPN Cisco 3000](#)
- [Page de support pour le Client Cisco VPN 3000](#)
- [Négociation IPSec/Protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)