Controllo CRL su HTTP su un concentratore Cisco VPN 3000

Sommario

Introduzione

In questo documento viene descritto come abilitare il controllo CRL (Certificate Revocation List) per i certificati CA (Certification Authority) installati in Cisco VPN 3000 Concentrator utilizzando la modalità HTTP.

Un certificato in genere è valido per l'intero periodo di validità. Tuttavia, se un certificato non è più valido a causa di modifiche del nome, modifiche dell'associazione tra il soggetto e la CA e compromessi sulla sicurezza, la CA revoca il certificato. In X.509, le CA revocano i certificati rilasciando periodicamente un CRL firmato, in cui ogni certificato revocato è identificato dal relativo numero di serie. Se si attiva il controllo CRL, ogni volta che il concentratore VPN utilizza il certificato per l'autenticazione, controlla anche il CRL per verificare che il certificato da verificare non sia stato revocato.

Le CA utilizzano database LDAP (Lightweight Directory Access Protocol)/HTTP per archiviare e distribuire le CRL. Possono anche utilizzare altri mezzi, ma VPN Concentrator si basa sull'accesso LDAP/HTTP.

La verifica CRL HTTP è introdotta in VPN Concentrator versione 3.6 o successive. Tuttavia, la verifica della CRL basata su LDAP è stata introdotta nelle release precedenti della versione 3.x. In questo documento viene descritto solo il controllo CRL tramite HTTP.

Nota: le dimensioni della cache CRL dei concentratori VPN serie 3000 dipendono dalla piattaforma e non possono essere configurate secondo le richieste dell'amministratore.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Il tunnel IPsec è stato stabilito correttamente dai client hardware VPN 3.x utilizzando i certificati per l'autenticazione IKE (Internet Key Exchange) (senza controllo CRL abilitato).
- Il tuo VPN Concentrator è sempre connesso al server CA.
- Se il server CA è connesso all'interfaccia pubblica, le regole necessarie sono state aperte nel filtro pubblico (predefinito).

Componenti usati

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

- VPN 3000 Concentrator versione 4.0.1 C
- Client hardware VPN 3.x
- Server CA Microsoft per la generazione di certificati e la verifica CRL in esecuzione su un server Windows 2000.

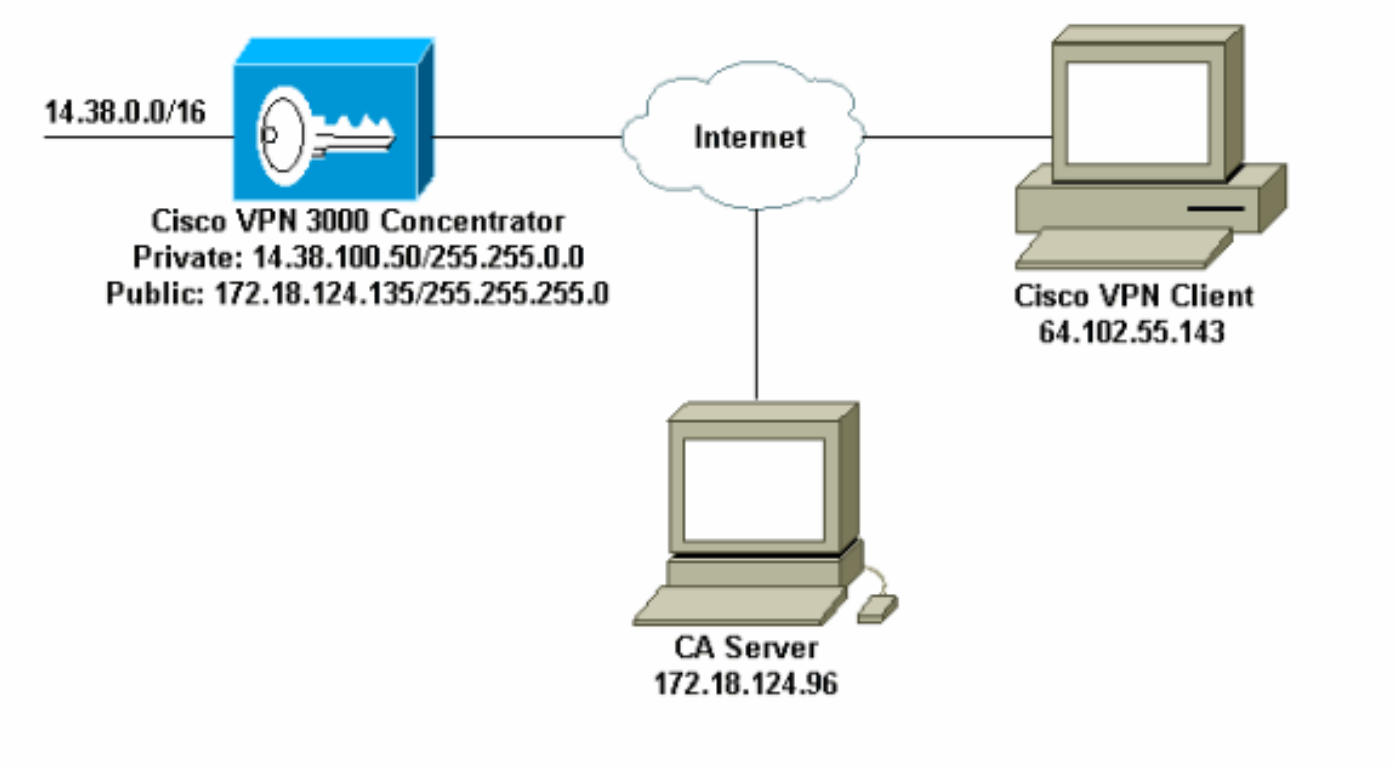
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Esempio di rete

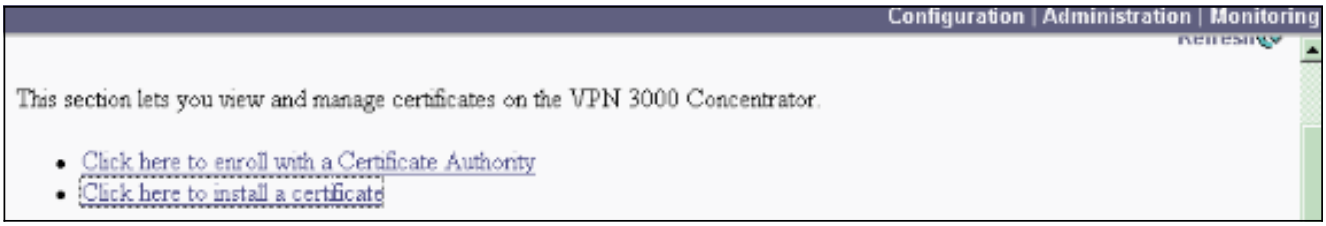
Nel documento viene usata questa impostazione di rete:



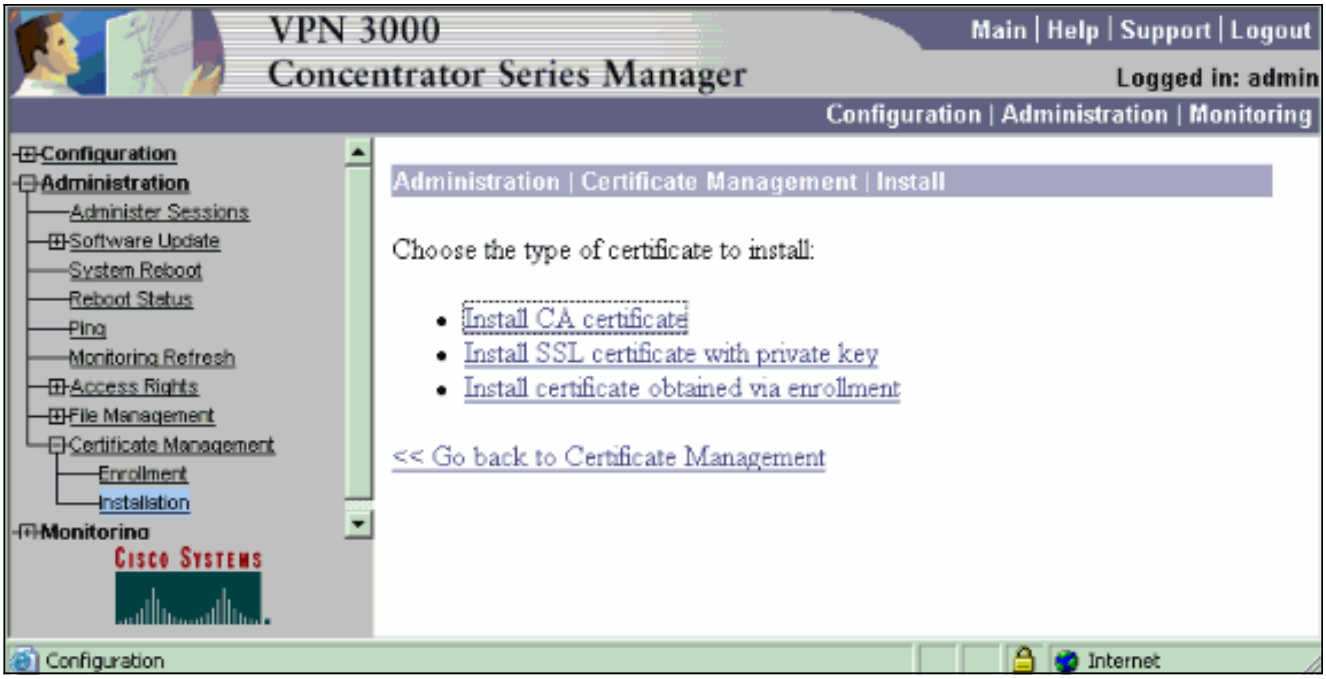
Configurazione di VPN 3000 Concentrator

Istruzioni dettagliate

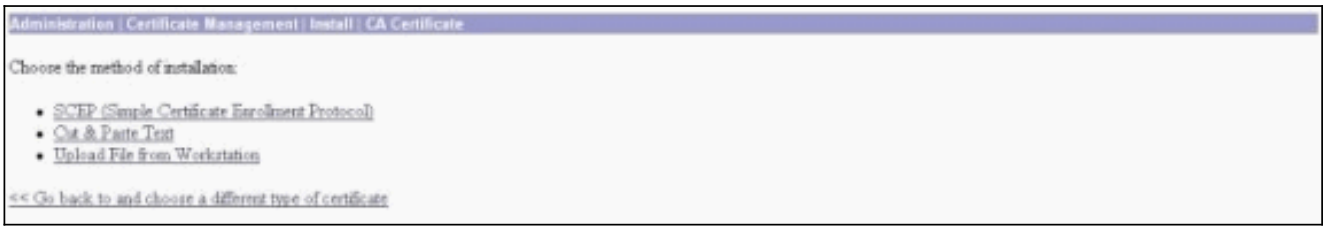
Completare questa procedura per configurare VPN 3000 Concentrator:

1. Selezionare **Amministrazione > Gestione certificati** per richiedere un certificato se non si dispone di un certificato.Selezionare **Fare clic qui per installare un certificato** per installare il certificato radice nel concentratore
   VPN.
   

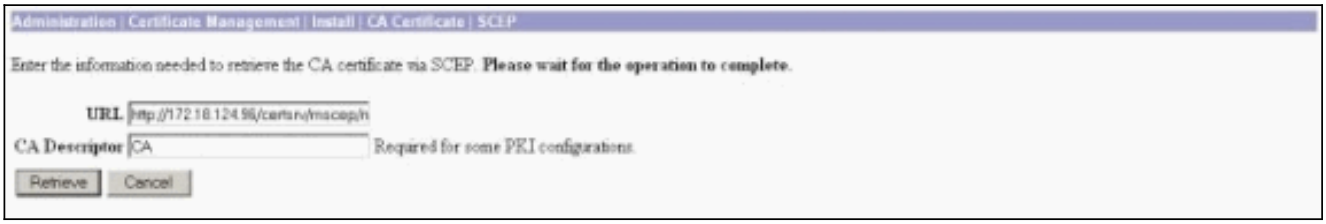
2. Selezionare **Installa certificato**
   CA.



3. Selezionare **SCEP (Simple Certificate Enrollment Protocol)** per recuperare i certificati CA.

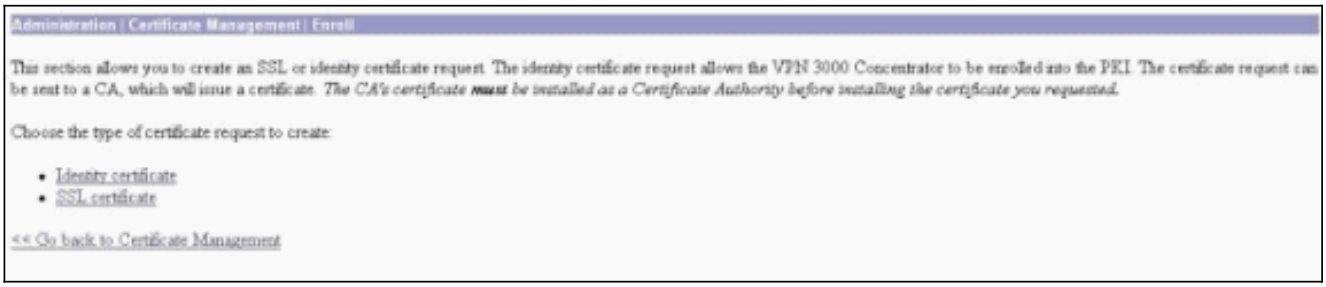


4. Nella finestra SCEP immettere l'URL completo del server CA nella finestra di dialogo URL.In questo esempio, l'indirizzo IP del server CA è 172.18.124.96. Poiché in questo esempio viene utilizzato il server CA di Microsoft, l'URL completo è http://172.18.124.96/certsrv/mscep/mscep.dll. Immettere quindi un descrittore di una parola nella finestra di dialogo Descrittore CA. In questo esempio viene utilizzato CA.

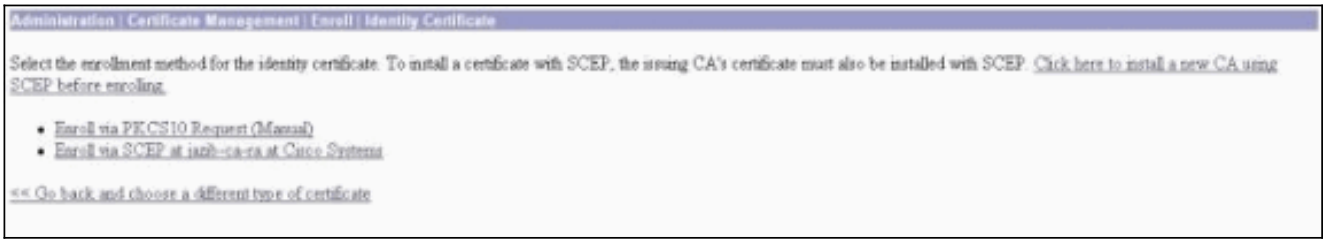


5. Fare clic su **Recupera**.Il certificato CA verrà visualizzato nella finestra Amministrazione > Gestione certificati. Se il certificato non è visibile, tornare al passaggio 1 e seguire nuovamente la procedura.

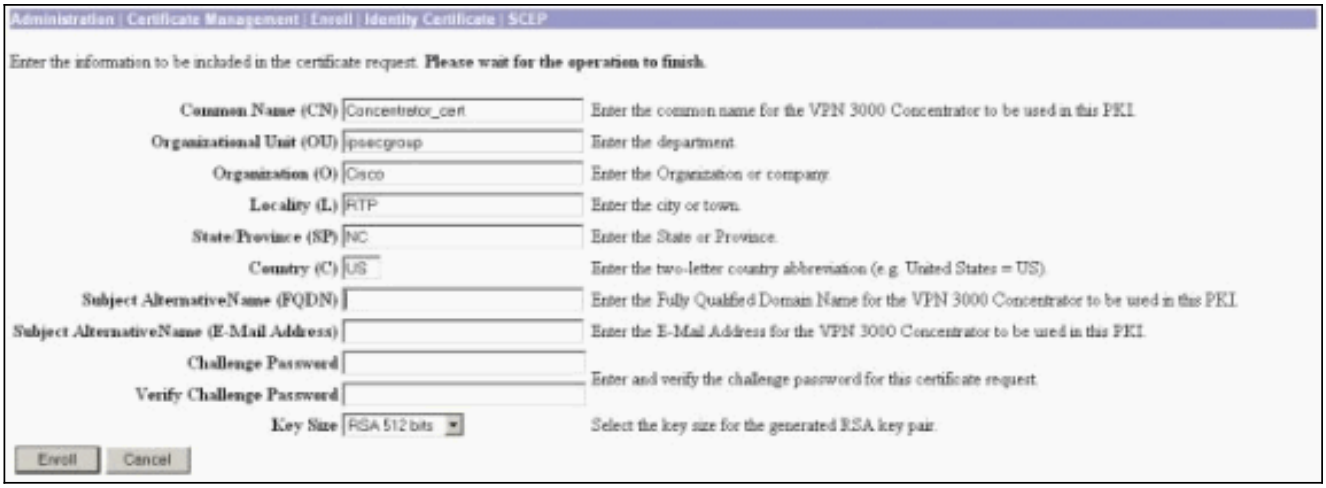
6. Una volta ottenuto il certificato CA, selezionare **Amministrazione > Gestione certificati > Registra** e fare clic su **Certificato di identità**.



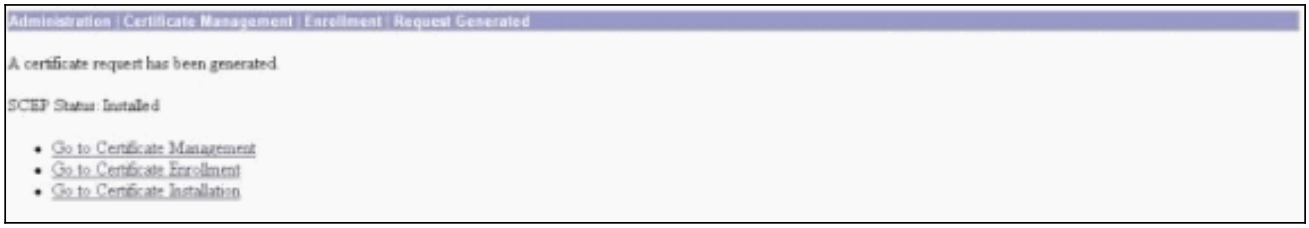
7. Fare clic su **Registra tramite SCEP all'indirizzo ...** per richiedere il certificato di identità.



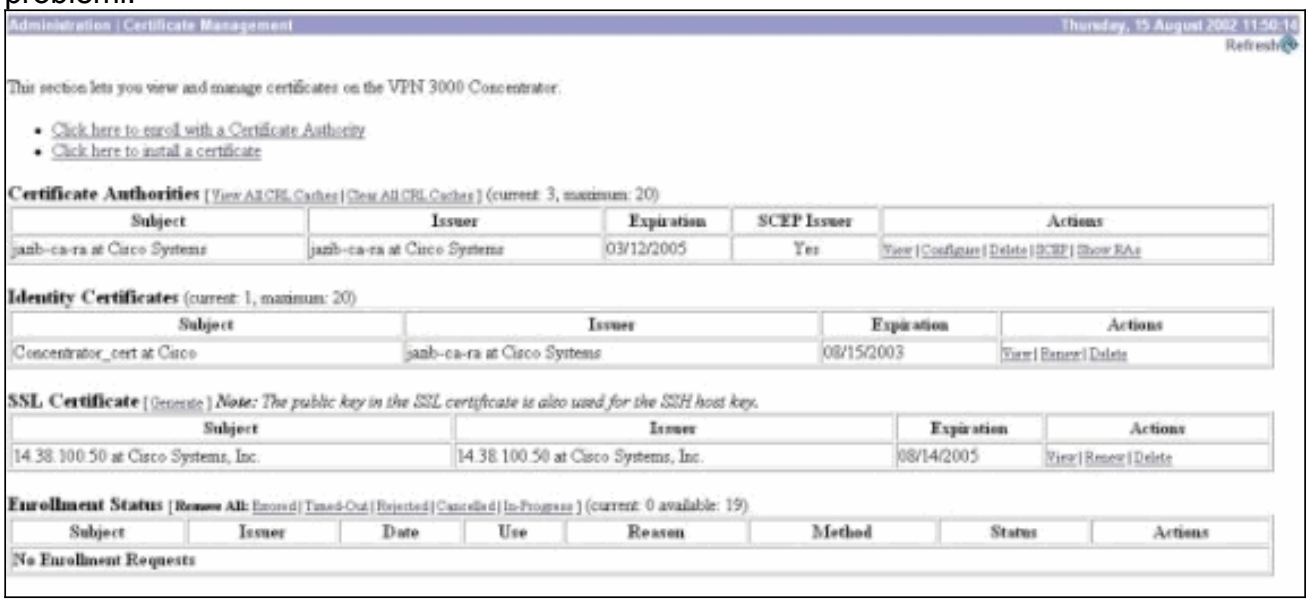
8. Completare i seguenti passaggi per compilare il modulo Iscrizione:Immettere il nome comune del concentratore VPN da utilizzare nell'infrastruttura a chiave pubblica (PKI) nel campo Nome comune (CN).Inserire il reparto nel campo Unità organizzativa. L'unità organizzativa deve corrispondere al nome del gruppo IPSec configurato.Inserire l'organizzazione o la società nel campo Organizzazione (O).Immettere la città nel campo Località (L).Immettere la provincia nel campo Stato/Provincia (SP).Inserire il paese nel campo Paese (C).Immettere il nome di dominio completo (FQDN) per il concentratore VPN da utilizzare nella PKI nel campo Nome di dominio completo (FQDN).Immettere l'indirizzo di posta elettronica per il concentratore VPN da utilizzare nella PKI nel campo Nome alternativo oggetto (indirizzo di posta elettronica).Immettere la password di verifica per la richiesta di certificato nel campo Password di verifica.Immettere nuovamente la password di verifica nel campo Verifica password di verifica.Selezionare le dimensioni della chiave per la coppia di chiavi RSA generata dall'elenco a discesa Dimensione chiave.



9. Selezionare **Enroll** e visualizzare lo stato SCEP nello stato di polling.
10. Passare al server CA per approvare il certificato di identità. Una volta approvato sul server CA, lo stato di SCEP deve essere
    Installato.



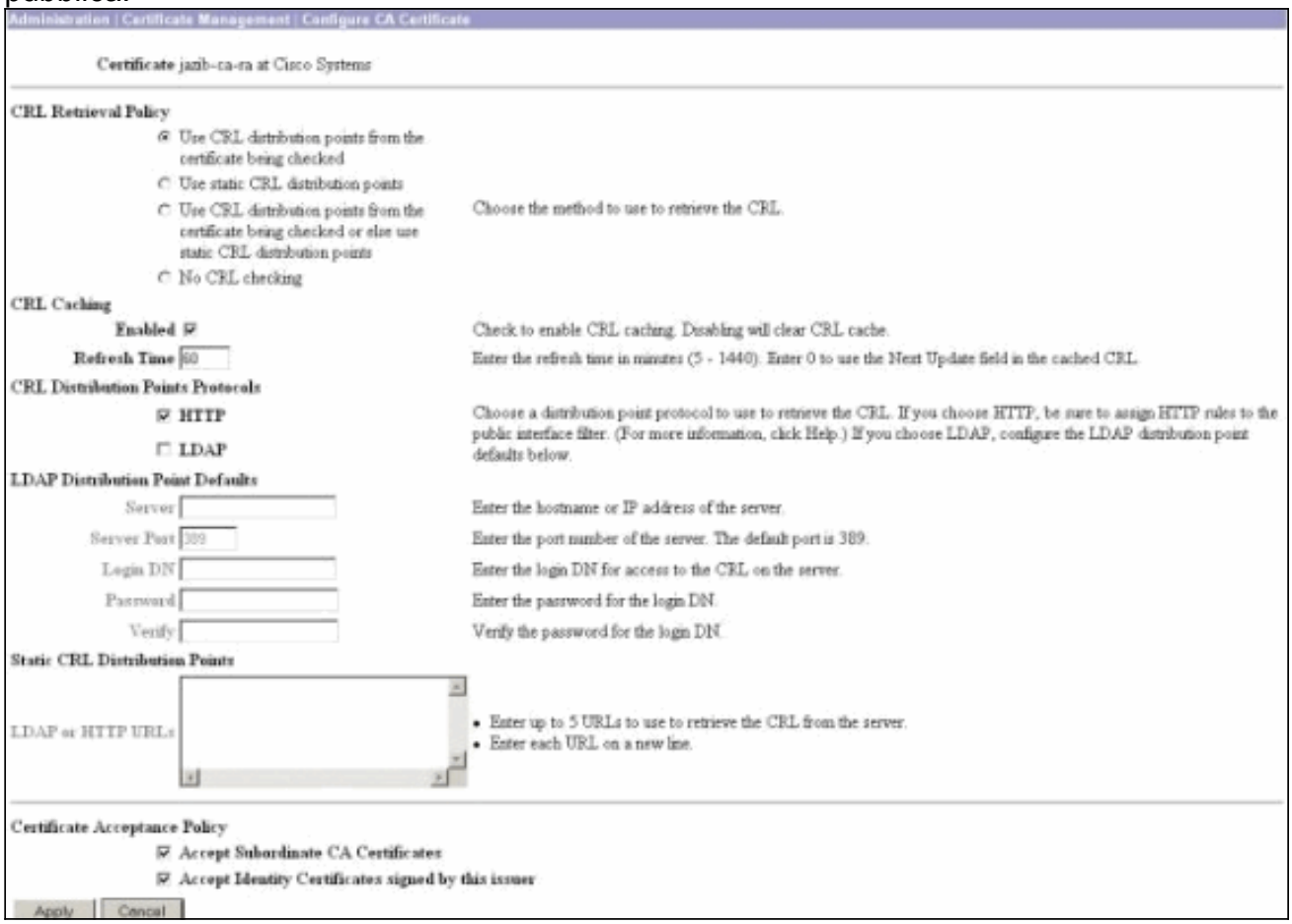
11. In Gestione certificati dovrebbe essere visualizzato il certificato di identità.In caso contrario, controllare i registri sul server CA per ulteriori informazioni sulla risoluzione dei problemi.



12. Selezionare **Visualizza** sul certificato ricevuto per verificare se il certificato dispone di un punto di distribuzione CRL (CDP).Il CDP elenca tutti i punti di distribuzione CRL dell'autorità emittente del certificato. Se il certificato include CDP e si utilizza un nome DNS per inviare una query al server CA, verificare che nel concentratore VPN siano definiti server DNS per risolvere il nome host con un indirizzo IP. In questo caso, il nome host del server CA di esempio è jazib-pc che viene risolto in un indirizzo IP di 172.18.124.96 sul server DNS.

13. Fare clic su **Configura** nel certificato CA per abilitare il controllo CRL sui certificati ricevuti.Se il certificato ricevuto contiene CDP e si desidera utilizzarlo, selezionare **Usa punti di distribuzione CRL dal certificato da controllare**.Poiché il sistema deve recuperare ed esaminare il CRL da un punto di distribuzione di rete, l'attivazione del controllo CRL potrebbe rallentare i tempi di risposta del sistema. Inoltre, se la rete è lenta o congestionata, il controllo CRL potrebbe non riuscire. Abilitare la memorizzazione nella cache CRL per ridurre questi potenziali problemi. In questo modo i CRL recuperati vengono archiviati nella memoria volatile locale e pertanto il concentratore VPN può verificare più rapidamente lo stato di revoca dei certificati.Se la memorizzazione nella cache CRL è abilitata, il concentratore VPN controlla innanzitutto se il CRL richiesto è presente nella cache e controlla il numero di serie del certificato confrontandolo con l'elenco dei numeri di serie del CRL quando è necessario controllare lo stato di revoca di un certificato. Il certificato è considerato revocato se viene trovato il relativo numero di serie. VPN Concentrator recupera un CRL da un server esterno quando non trova il CRL richiesto nella cache, quando il periodo di validità del CRL memorizzato nella cache è scaduto o quando è trascorso il tempo di aggiornamento configurato. Quando VPN Concentrator riceve un nuovo CRL da un server esterno, aggiorna la cache con il nuovo CRL. La cache può contenere fino a 64 CRL.**Nota:** la cache CRL è presente in memoria. Il riavvio di VPN Concentrator comporta la cancellazione della cache CRL. VPN Concentrator ripopola la cache CRL con CRL aggiornati durante l'elaborazione delle nuove richieste di autenticazione peer.Se si seleziona **Utilizza punti di distribuzione CRL statici**, è possibile utilizzare fino a cinque punti di distribuzione CRL statici, come specificato in questa finestra. Se si sceglie questa opzione, è necessario immettere almeno un URL.Èinoltre possibile selezionare **Utilizza punti di distribuzione CRL dal certificato controllato** oppure **Utilizza punti di distribuzione CRL statici**. Se VPN Concentrator non è in grado di trovare cinque punti di distribuzione CRL nel certificato, aggiunge punti di distribuzione CRL statici, fino a un massimo di cinque. Se si sceglie questa opzione, abilitare almeno un protocollo del punto di distribuzione CRL. È inoltre necessario immettere almeno un punto di distribuzione CRL statico e non più di cinque.Selezionare **Nessun controllo CRL** se si desidera disattivare il controllo CRL.In Cache CRL selezionare la casella **Abilitato** per consentire a Concentrator VPN di memorizzare nella cache i CRL recuperati. Per impostazione predefinita, la memorizzazione nella cache CRL non è attivata. Quando si disattiva la memorizzazione nella cache CRL (deselezionare la casella), la cache CRL viene cancellata.Se sono stati configurati criteri di recupero CRL che utilizzano i punti di distribuzione CRL del certificato controllato, scegliere un protocollo del punto di distribuzione da utilizzare per recuperare il CRL. In questo caso, scegliere **HTTP** per recuperare il CRL. Assegnare le regole HTTP al

filtro dell'interfaccia pubblica se il server CA è diretto all'interfaccia pubblica.



Monitoraggio

Selezionare **Amministrazione > Gestione certificati** e fare clic su **Visualizza tutte le cache CRL** per verificare se il concentratore VPN ha memorizzato nella cache qualsiasi CRL del server CA.

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Log da Concentrator

Abilitare questi eventi su VPN Concentrator per essere certi che il controllo CRL funzioni.

1. Selezionare **Configurazione > Sistema > Eventi > Classi** per impostare i livelli di log.
2. In Nome classe selezionare IKE, **IKEDBG**, **IPSEC**, **IPSECDBG** o **CERT**.
3. Fare clic su **Aggiungi** o **Modifica** e scegliere l'opzione **Gravità da registrare 1-13**.
4. Fare clic su **Applica** se si desidera modificare o su **Aggiungi** se si desidera aggiungere una nuova voce.

Registri concentratore riusciti

Se il controllo CRL ha esito positivo, questi messaggi vengono visualizzati nei registri eventi

filtrabili.

```
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)
```

Per l'output completo di un log del concentratore corretto, fare riferimento a Log del concentratore riusciti.

Log non riusciti

Se l'archiviazione del CRL non ha esito positivo, questi messaggi vengono visualizzati nei registri eventi filtrabili.

```
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.
```

Per l'output completo di un log del concentratore fallito, fare riferimento ai log del concentratore revocati.

Per l'output completo di un log client corretto, fare riferimento a Log client riusciti.

Per l'output completo di un log client non riuscito, fare riferimento a Log client revocati.

Risoluzione dei problemi

Per ulteriori informazioni sulla risoluzione dei problemi, fare riferimento a Risoluzione dei problemi di connessione su VPN 3000 Concentrator.

Informazioni correlate

- Pagina di supporto per Cisco VPN serie 3000 concentrator
- Pagina di supporto per i client Cisco VPN 3000
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems