Éditez les listes des révocations de certificat pour ISE sur un exemple de configuration du serveur de Microsoft CA

Contenu

Introduction

Ce document décrit la configuration d'un serveur de Microsoft Certificate Authority (CA) qui dirige l'Internet Information Services (IIS) pour éditer des mises à jour de Liste des révocations de certificat (CRL). Il explique également comment configurer le Logiciel Cisco Identity Services Engine (ISE) (versions 1.1 et ultérieures) récupérer les mises à jour pour l'usage dans la validation de certificat. ISE peut être configuré pour récupérer CRLs pour les divers certificats racine CA qu'il l'utilise dans la validation de certificat.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

logiciel suivantes :

- Version 1.1.2.145 de Logiciel Cisco Identity Services Engine
- ® 2008 R2 de serveur de ® de Microsoft Windows

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.

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configurations

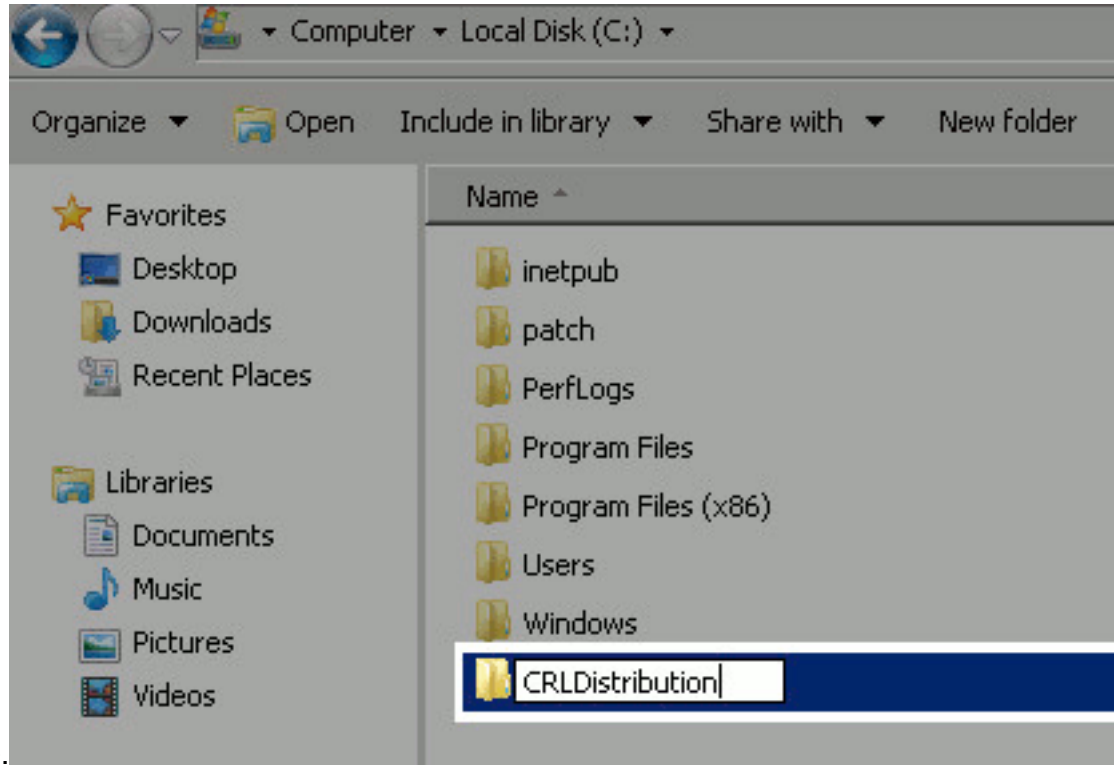
Ce document utilise les configurations suivantes :

- La section 1. créent et configurent un répertoire sur le CA pour loger les fichiers CRL
- La section 2. créent un site dans IIS pour exposer le nouveau point de distribution CRL
- La section 3. configurent le serveur de Microsoft CA pour éditer des fichiers CRL au point de distribution
- La section 4. vérifient le fichier CRL existe et est accessible par l'intermédiaire d'IIS
- La section 5. configurent ISE pour utiliser le nouveau point de distribution CRL

La section 1. créent et configurent un répertoire sur le CA pour loger les fichiers CRL

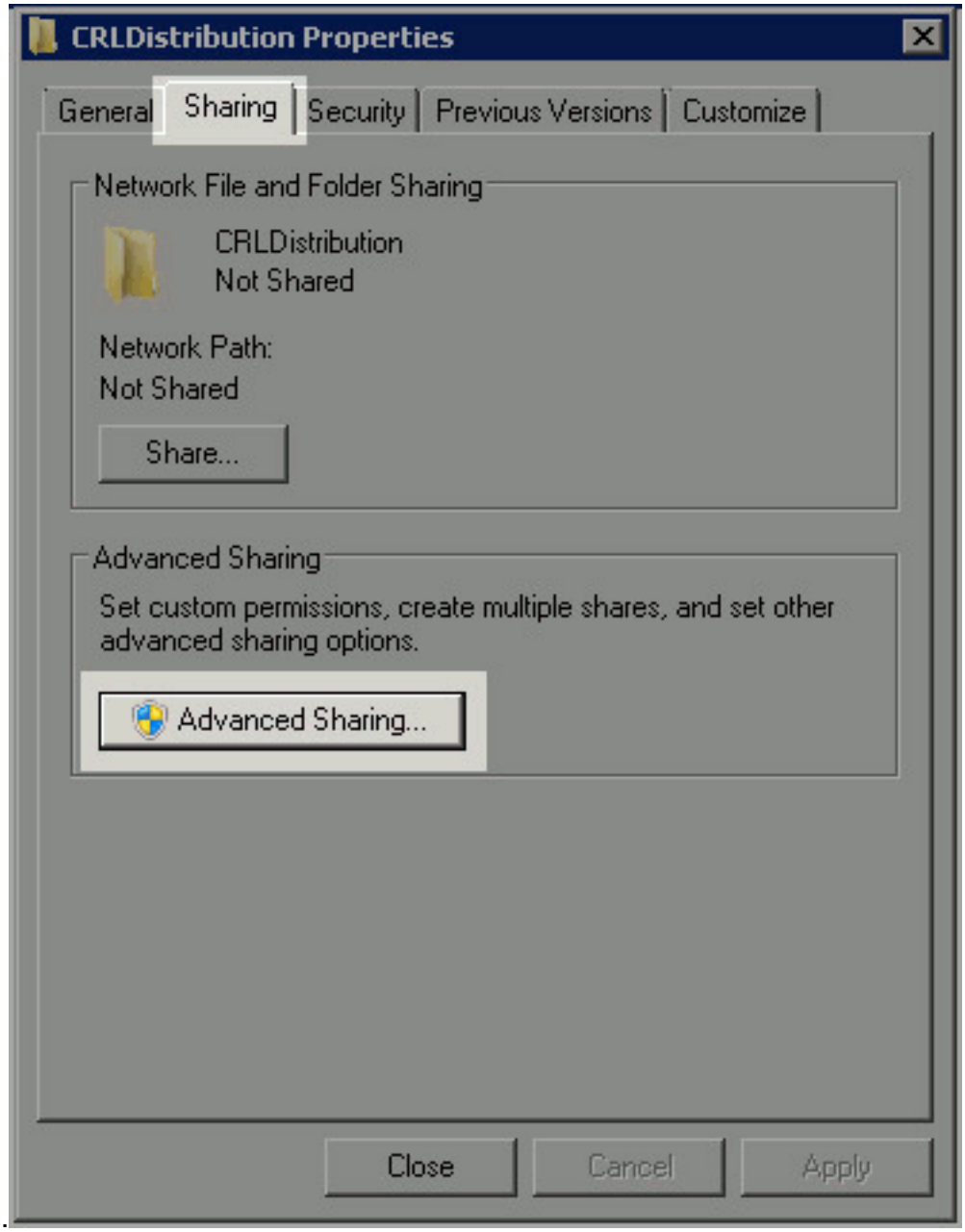
La première tâche est de configurer un emplacement sur le serveur CA pour enregistrer les fichiers CRL. Par défaut, le serveur de Microsoft CA édite les fichiers à C:\Windows\system32\CertSrv\CertEnroll\. Plutôt qu'utilisent ce dossier système, créent un nouveau répertoire pour les fichiers.

1. Sur le serveur IIS, choisissez un emplacement sur le système de fichiers et créez un nouveau répertoire. Dans cet exemple, le répertoire C:\CRLDistribution est



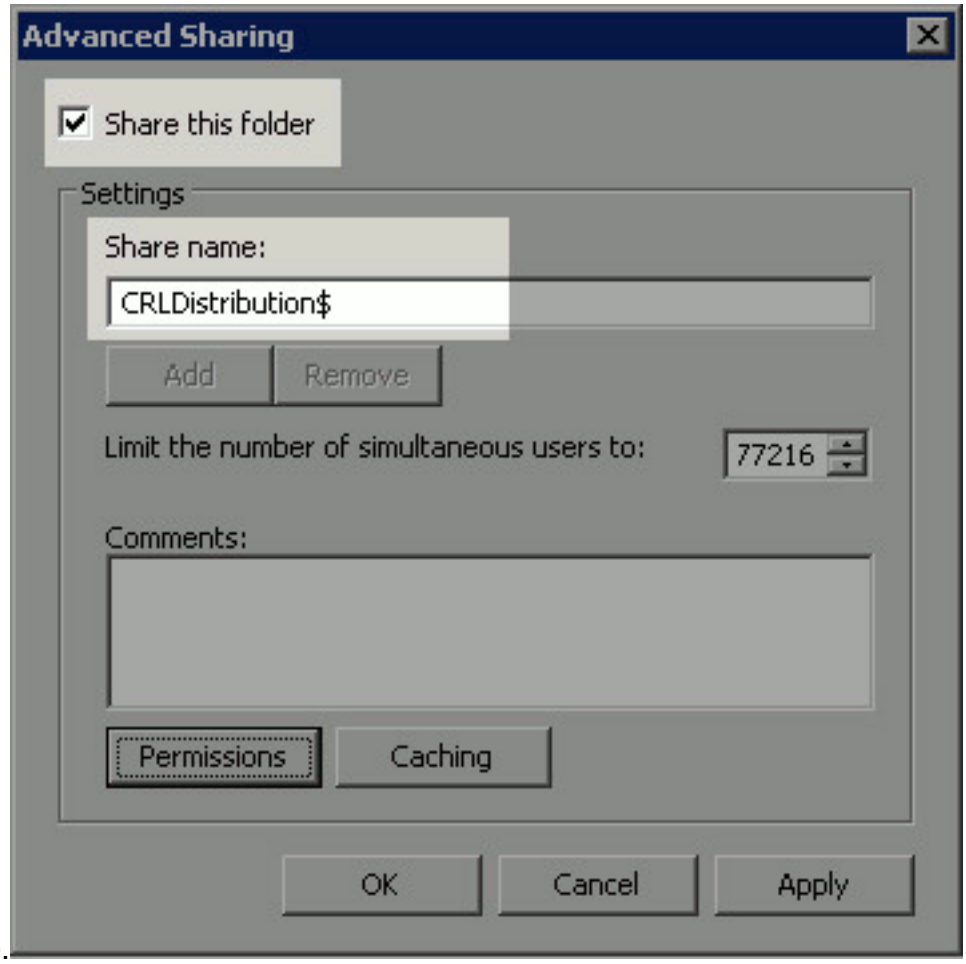
créé.

2. Pour que le CA écrive les fichiers CRL au nouveau répertoire, partageant doit être activé. Cliquez avec le bouton droit le nouveau répertoire, choisissez Properties, cliquez sur l'**onglet Partage**, et puis cliquez sur **partager**



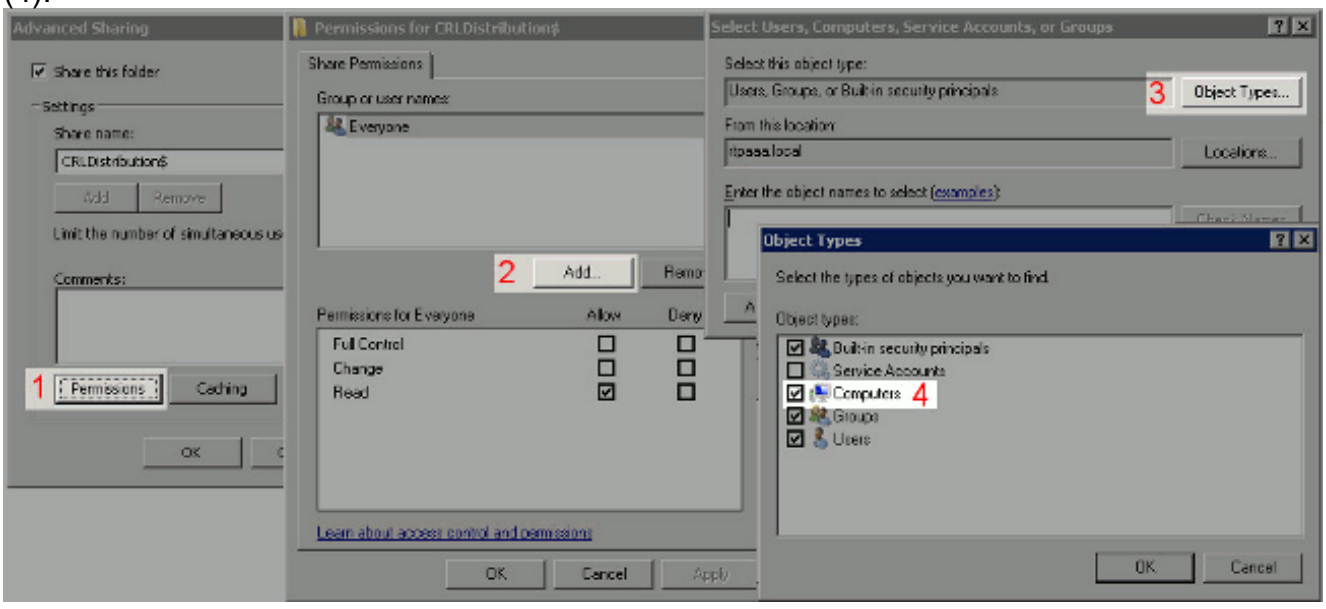
avancé.

3. Afin de partager le répertoire, cochez le **partage cette** case de **répertoire** et puis ajoutez un symbole dollar ($) à la fin du nom de partage dans le domaine de nom de partage de

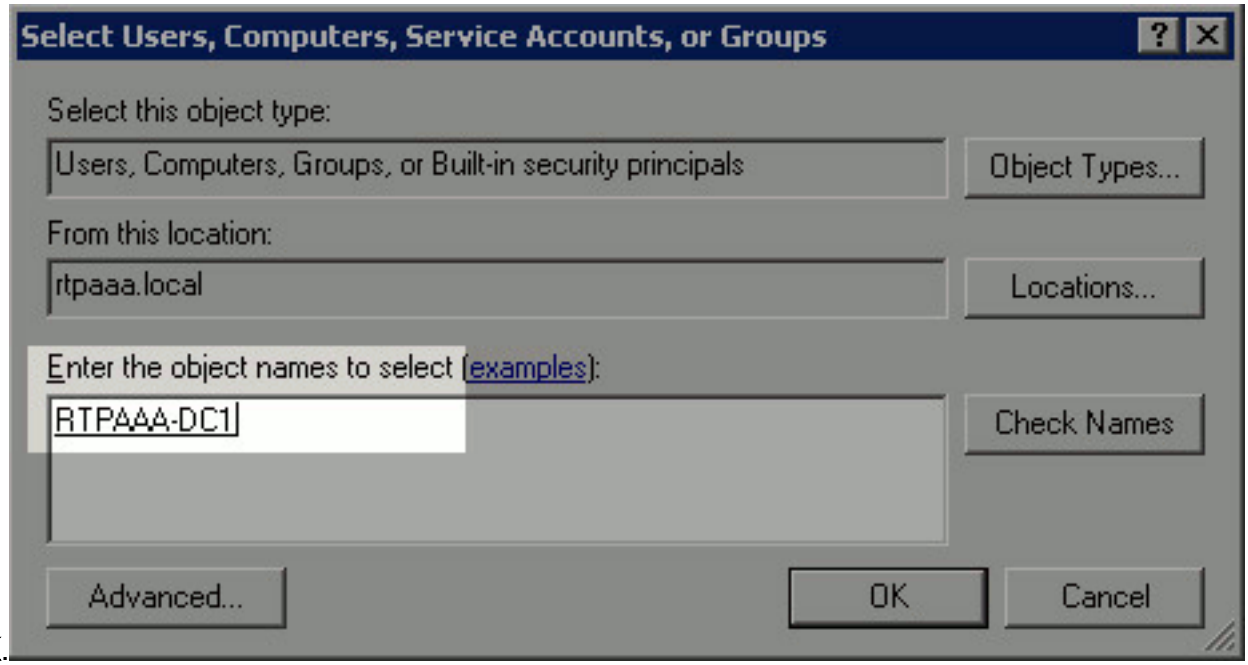


masquer le partage.

4. Cliquez sur les **autorisations** (1), cliquez sur Add (2), cliquez sur les **types d'objet** (3), et cochez la case d'**ordinateurs** (4).

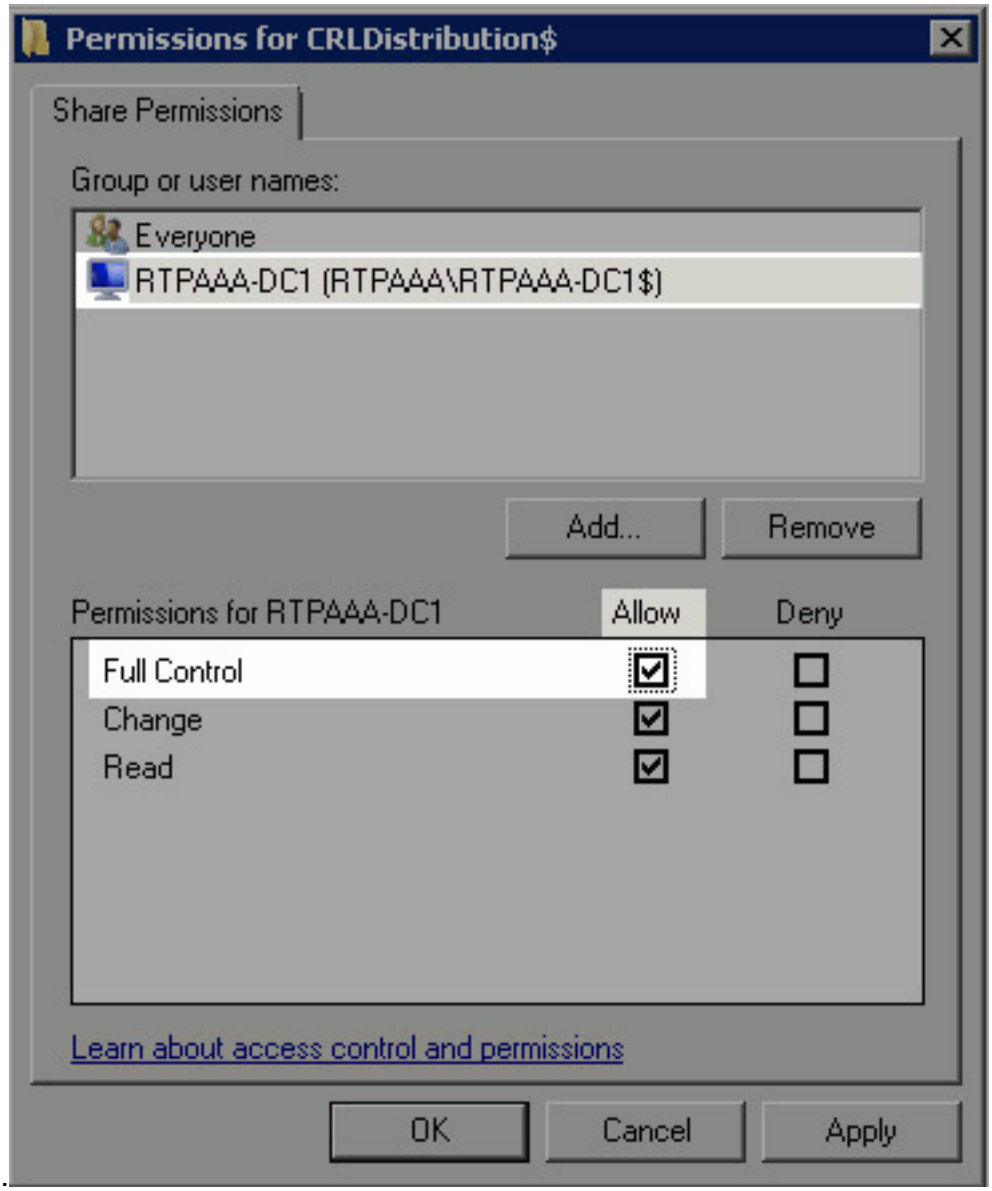


5. Afin de retourner aux utilisateurs choisis, les ordinateurs, fenêtre de comptes des services, ou de groupes, cliquent sur OK. Dans l'entrer les noms d'objet pour sélectionner le champ, écrire le nom de l'ordinateur du serveur CA et du **contrôle de** clic **nomme**. Si le nom écrit est valide, le nom régénère et semble souligné. Cliquez sur



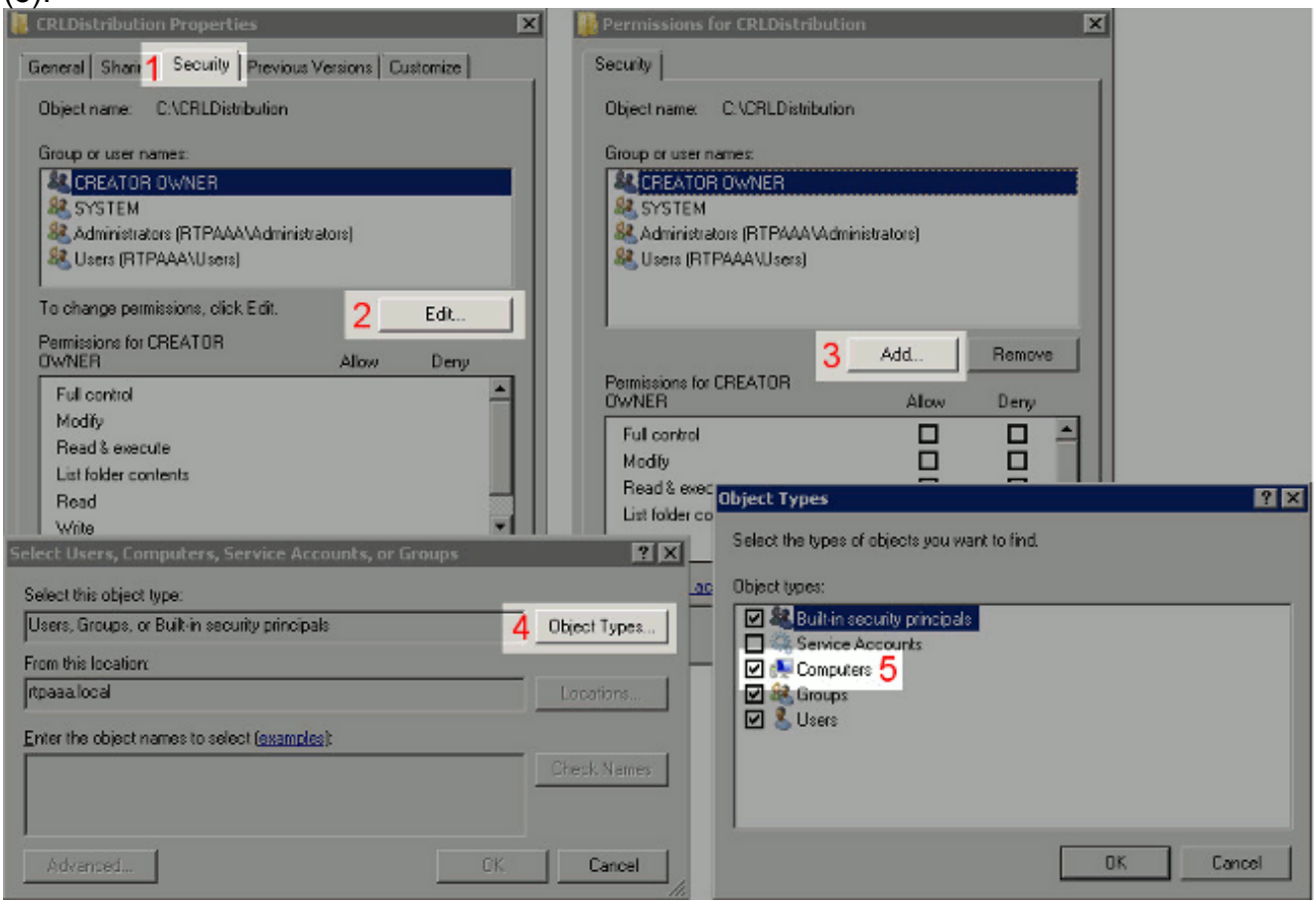
OK.

6. Dans le groupe ou les noms d'utilisateur mettez en place, choisissez l'ordinateur CA. Le contrôle **tiennent compte** pour que le plein contrôle accorde l'accès complet au CA cliquent sur OK. Cliquez sur OK de nouveau pour fermer la fenêtre partageante avancée et pour retourner à la fenêtre de

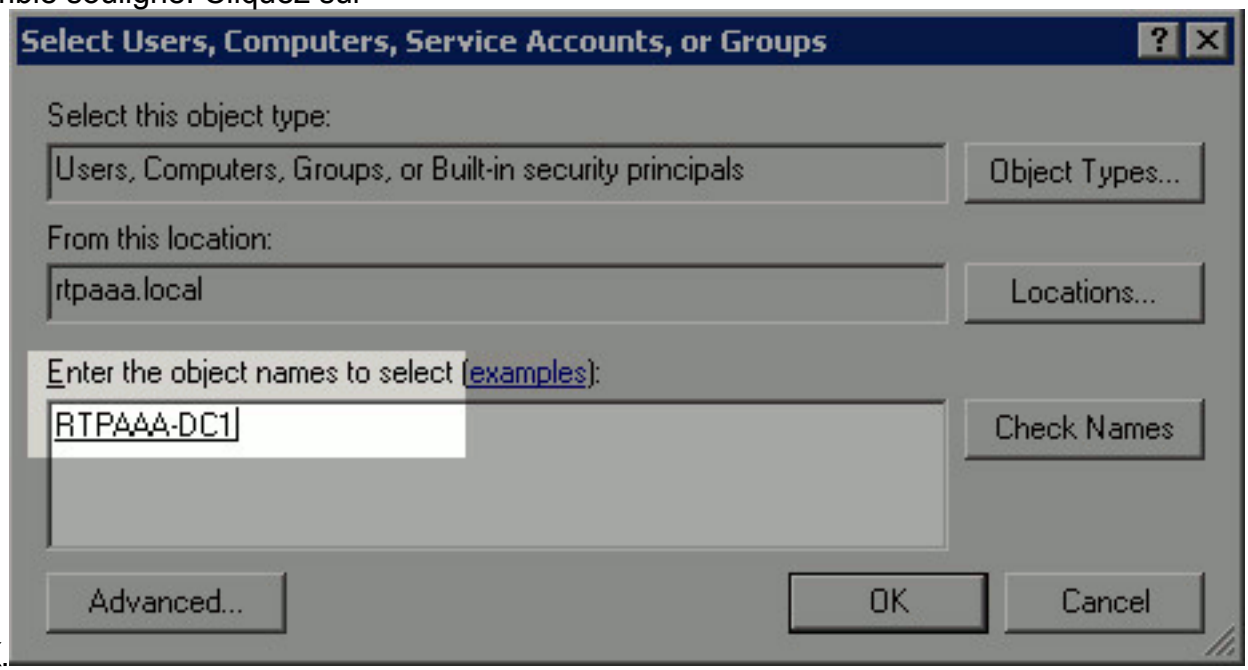


Properties.

7. Afin de permettre au CA pour écrire les fichiers CRL au nouveau répertoire, configurez les autorisations appropriées de Sécurité. Cliquez sur l'**onglet Sécurité** (1), cliquez sur Edit (2), cliquez sur Add (3), cliquez sur les **types d'objet** (4), et cochez la case d'**ordinateurs** (5).

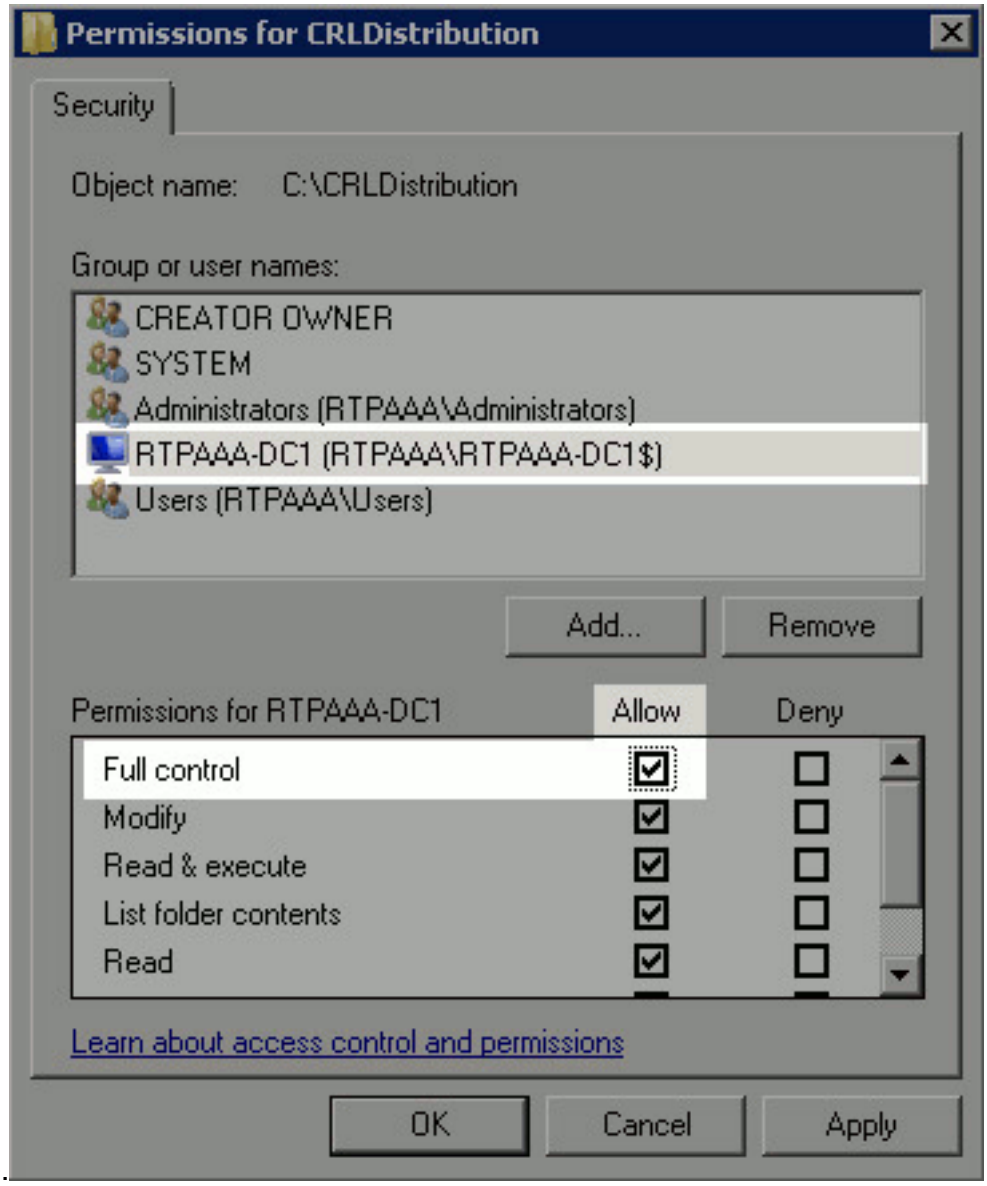


8. Dans l'entrer les noms d'objet pour sélectionner le champ, écrire le nom de l'ordinateur du serveur CA et du **contrôle de** clic **nomme**. Si le nom écrit est valide, le nom régénère et semble souligné. Cliquez sur **OK**.



9. Choisissez l'ordinateur CA dans le groupe ou les noms d'utilisateur mettent en place et puis vérifient **tiennent compte** pour que le plein contrôle accorde l'accès complet au CA cliquent sur OK et puis cliquent sur **près de** complet la

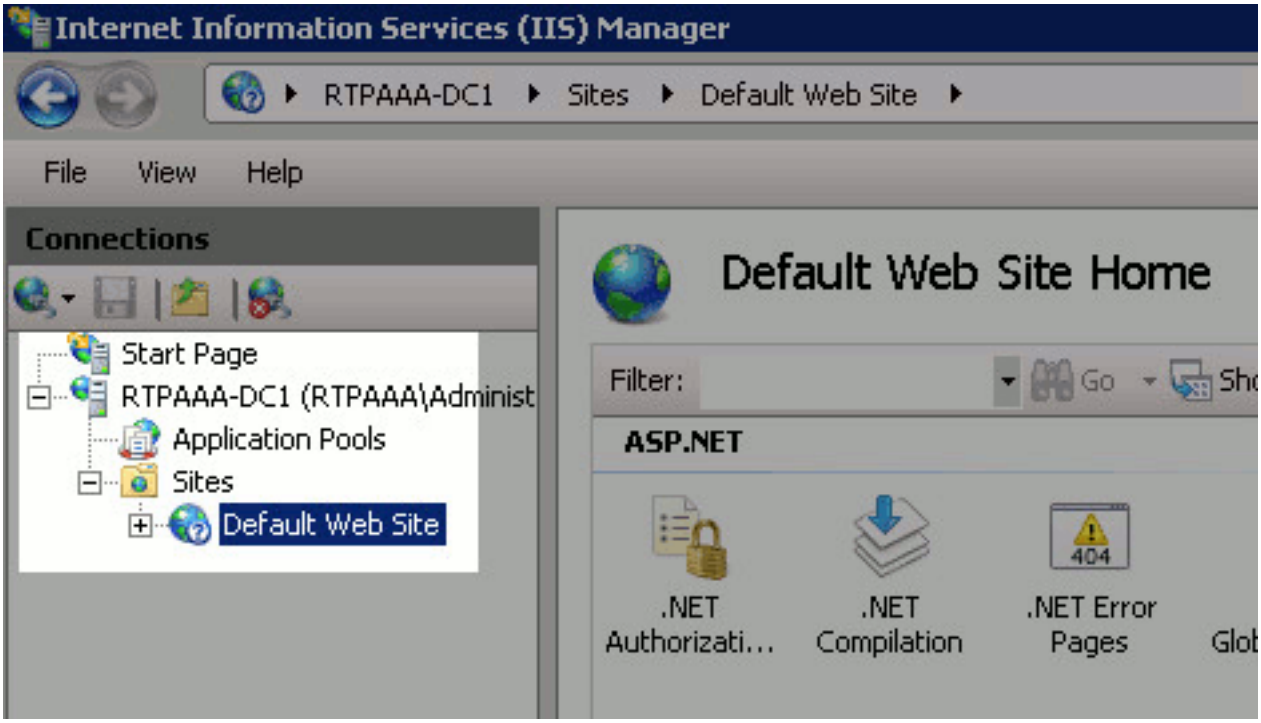
tâche.



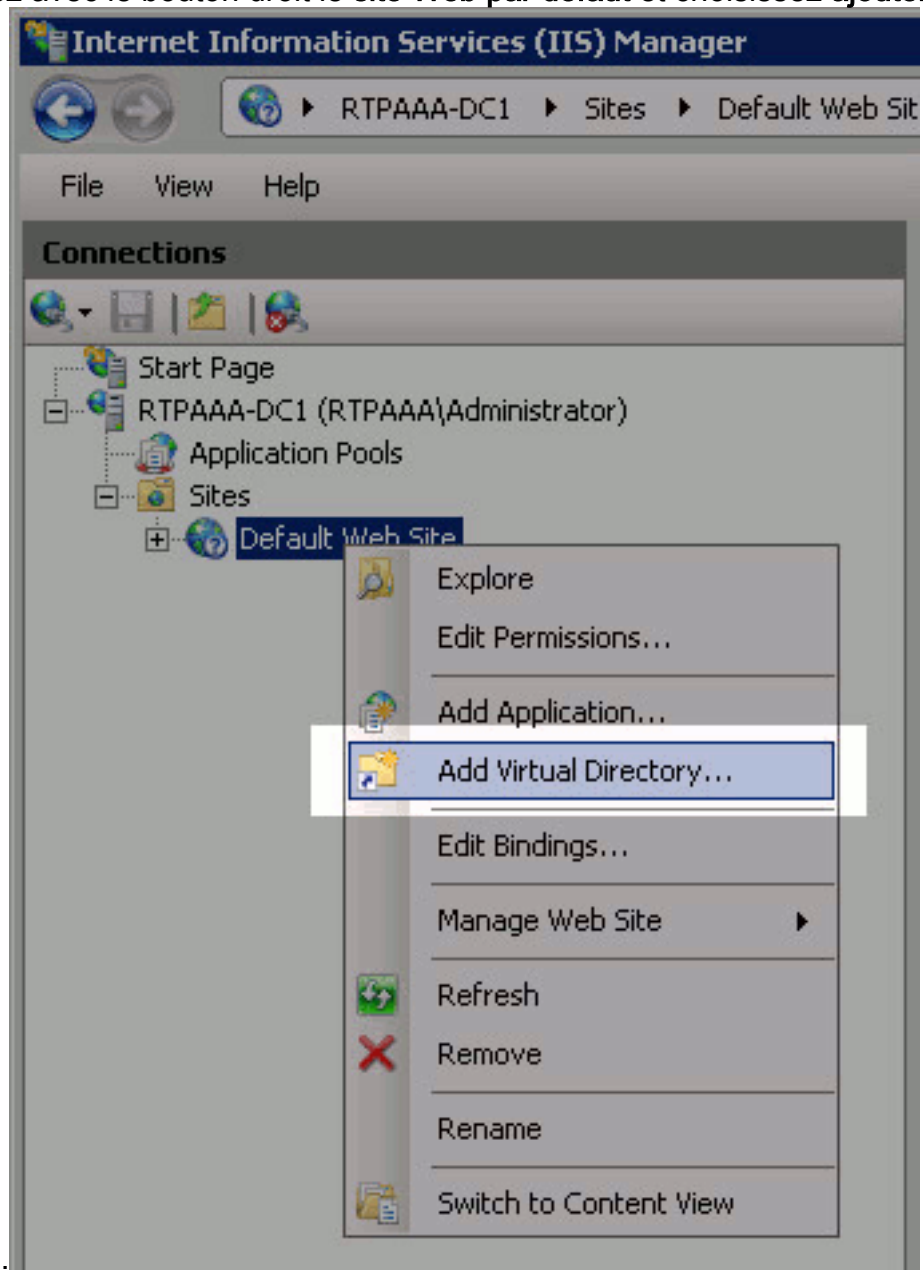
La section 2. créent un site dans IIS pour exposer le nouveau point de distribution CRL

Pour qu'ISE accède aux fichiers CRL, faites le répertoire qui loge les fichiers CRL accessibles par l'intermédiaire d'IIS.

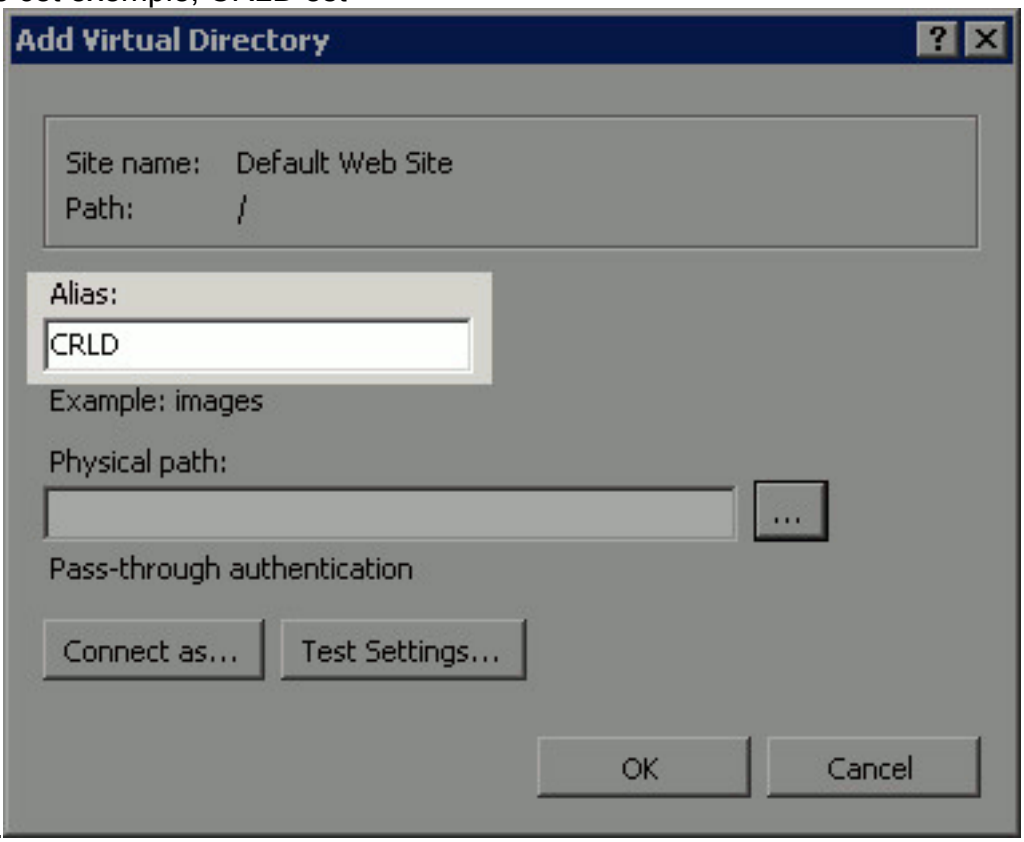
1. Sur la barre des tâches de serveur IIS, **début de** clic. Choisissez le **gestionnaire d'outils d'administration > d'Internet Information Services (IIS)**.
2. Dans le volet gauche (connu sous le nom d'arborescence de la console), développez le nom du serveur IIS et puis développez les
sites.



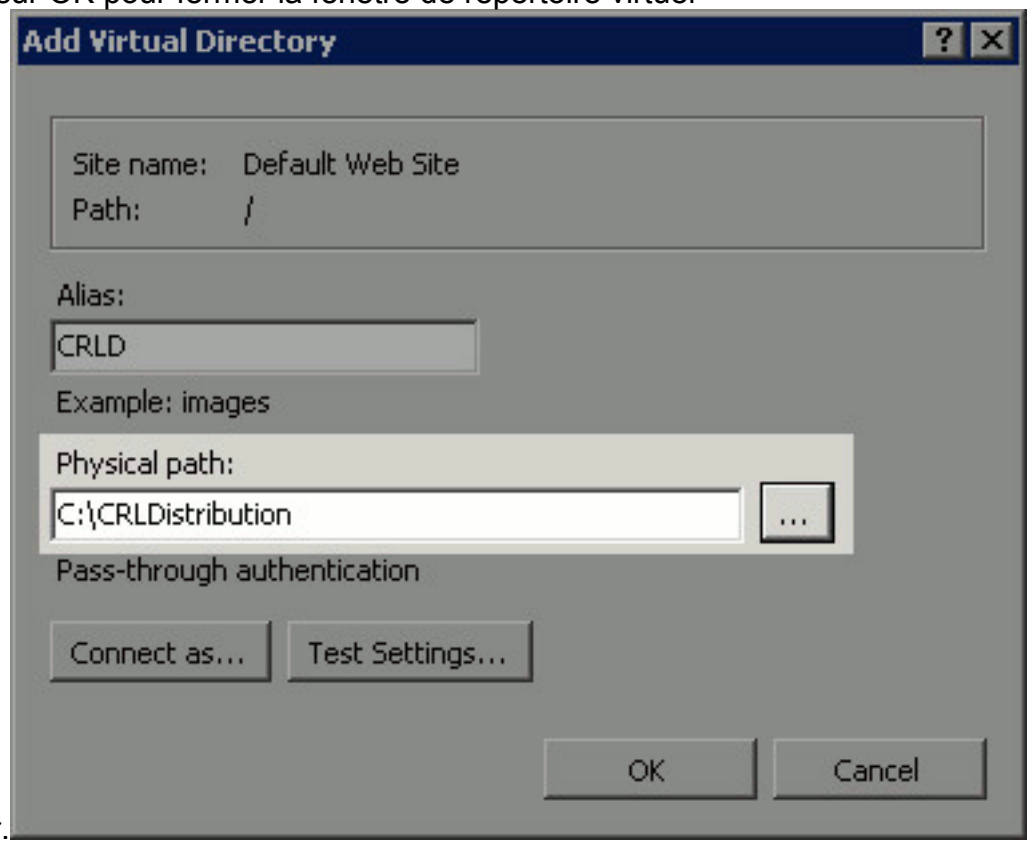
3. Cliquez avec le bouton droit le **site Web par défaut** et choisissez **ajoutent le répertoire virtuel**.



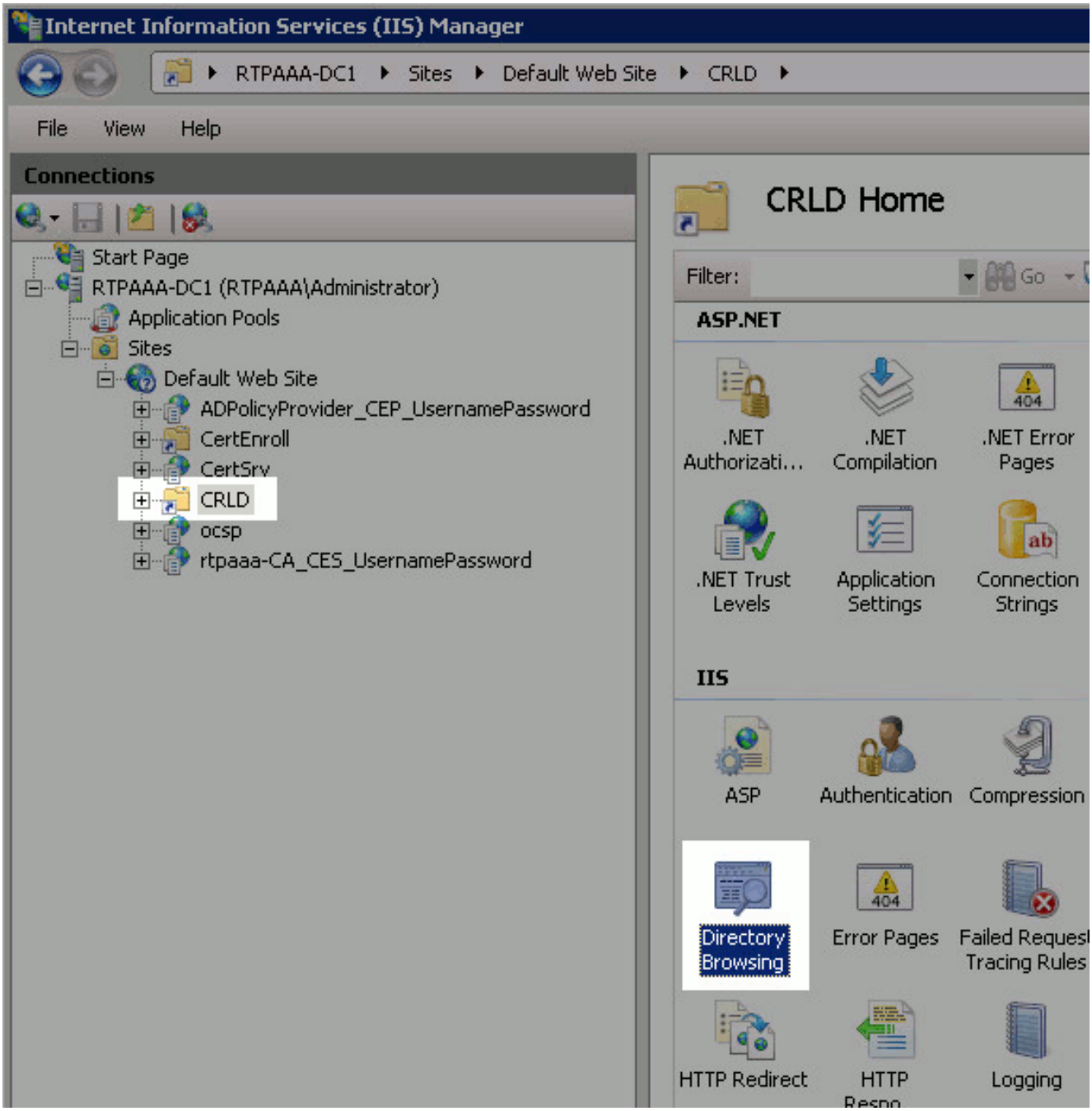
4. Dans le domaine de pseudonyme, écrivez un nom du site pour le point de distribution CRL. Dans cet exemple, CRLD est écrit.



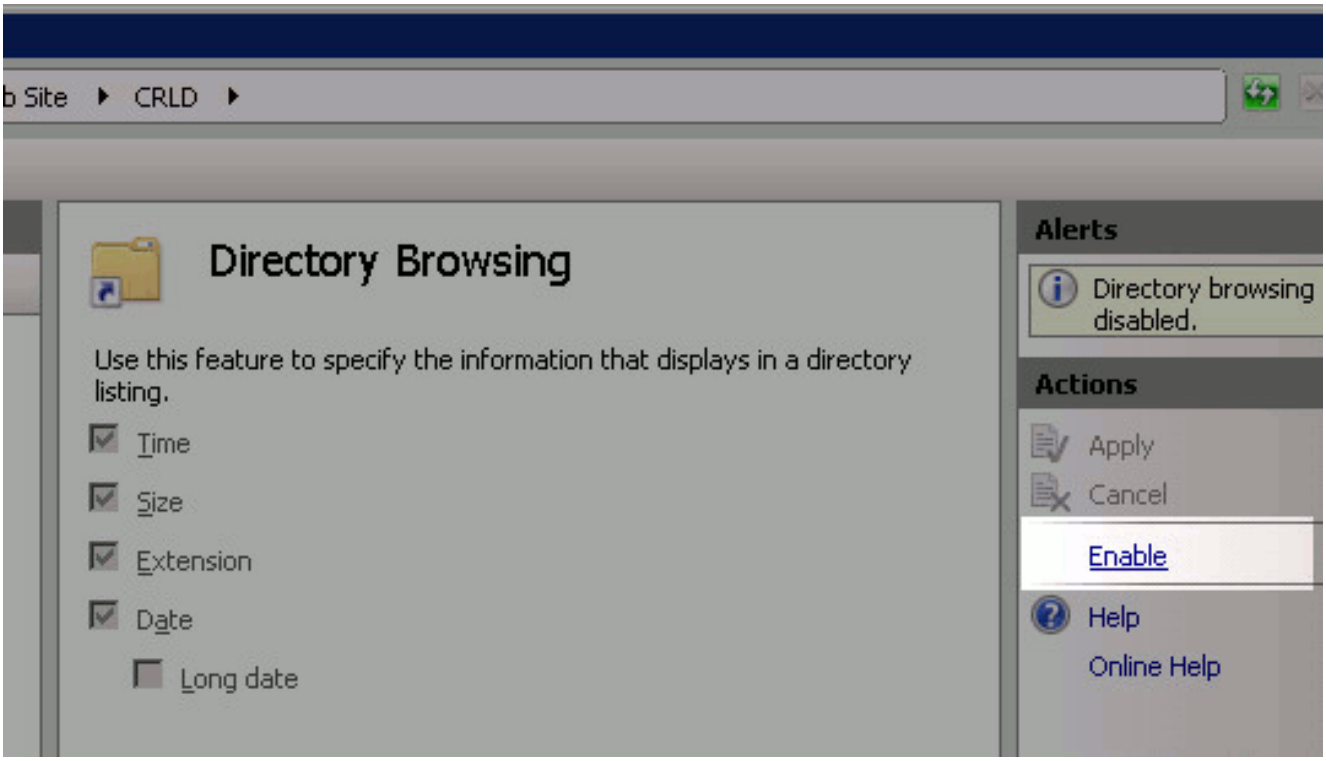
5. Cliquez sur les points de suspension (…) à la droite du gisement physique de chemin et parcourez au répertoire créé dans la section 1. choisie le répertoire et cliquez sur OK. Cliquez sur OK pour fermer la fenêtre de répertoire virtuel d'ajouter.



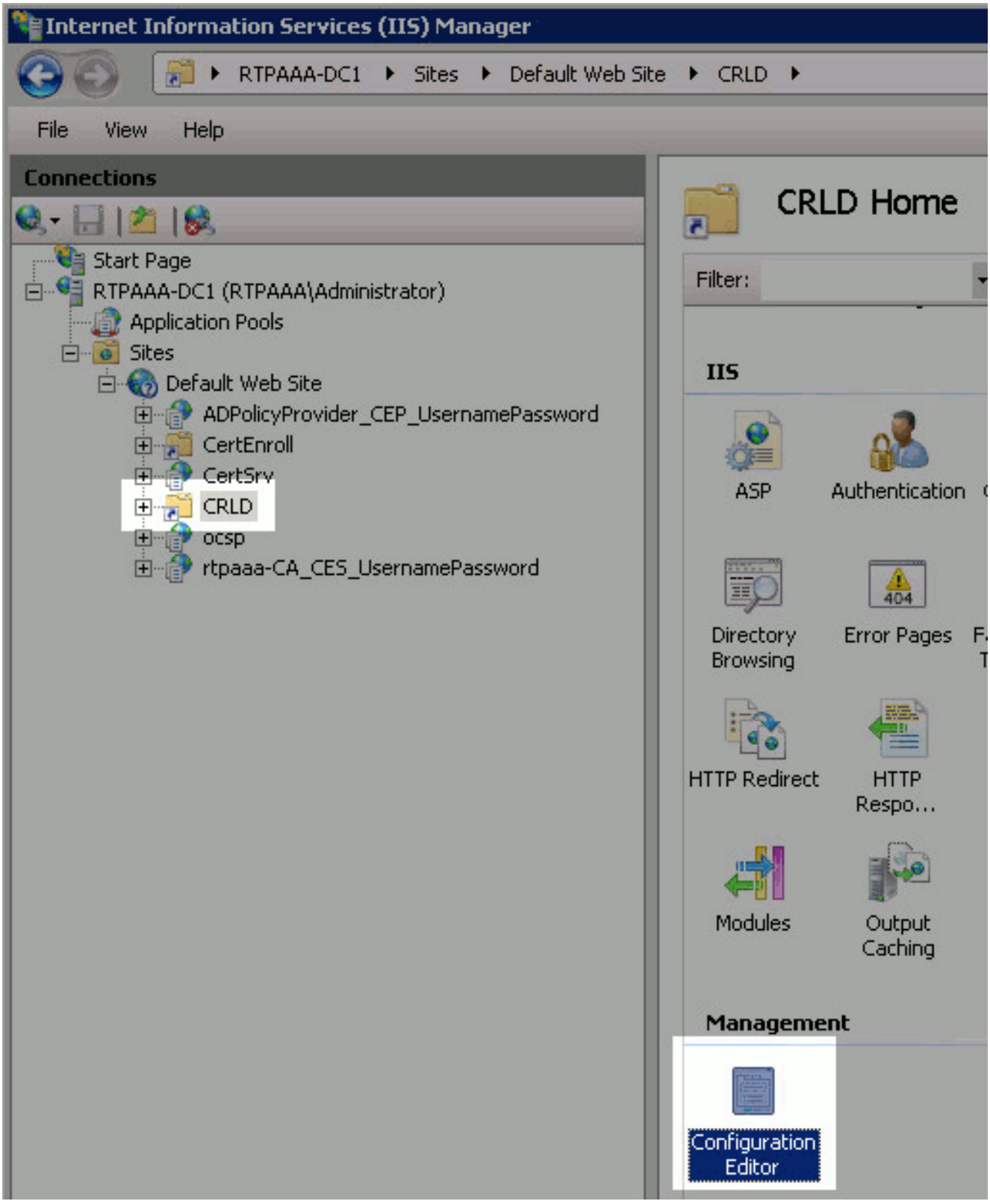
6. Le nom du site écrit dans l'étape 4 devrait être mis en valeur dans le volet gauche. Sinon, choisissez-le maintenant. Dans le volet central, **répertoire de** double clic **parcourant**.



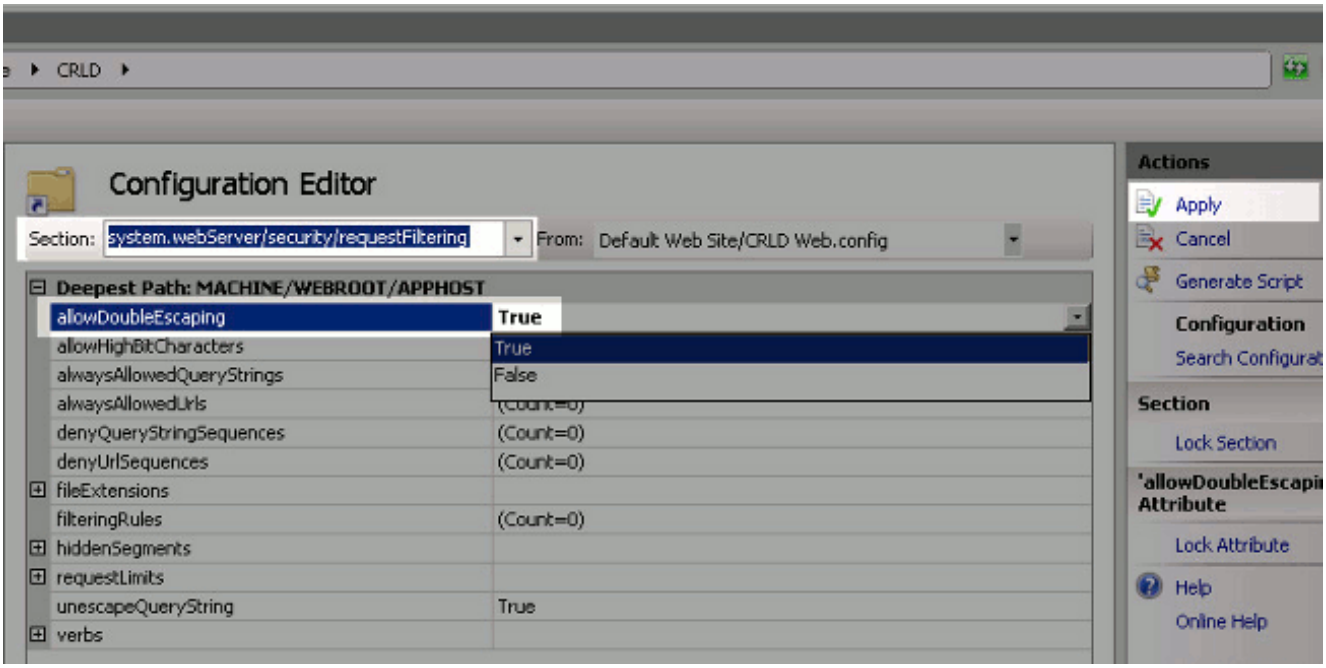
7. Dans le volet de droite, **enable de** clic pour activer le répertoire parcourant.



8. Dans le volet gauche, choisissez le nom du site de nouveau. Dans le volet central, **éditeur de configuration de** double
clic.



9. Dans la liste déroulante de section, choisissez **system.webServer/Sécurité/requestFiltering. Dans la** liste déroulante allowDoubleEscaping, choisissez vrai**. Dans le** volet de droite, cliquez sur
Apply**.**

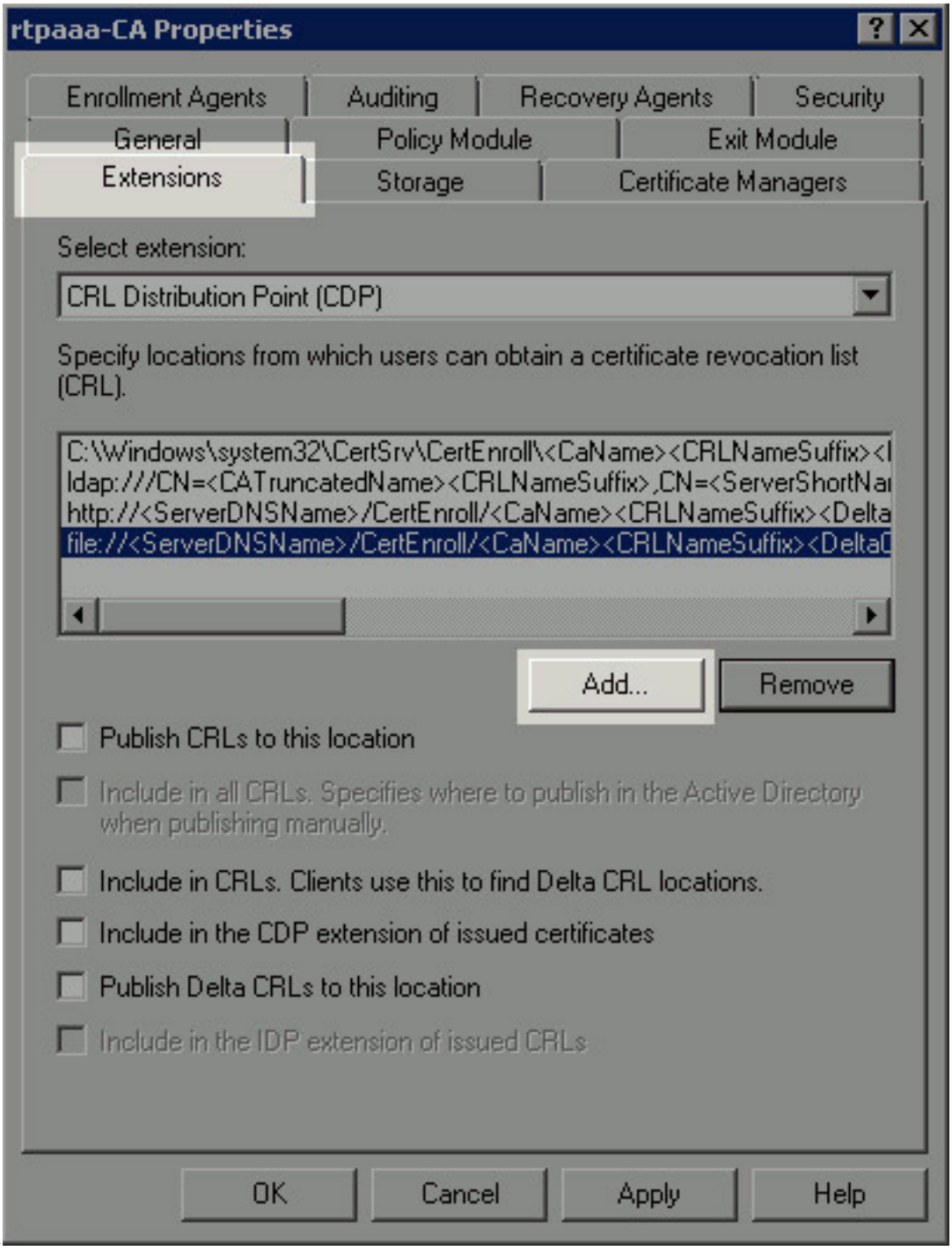


Le répertoire devrait maintenant être accessible par l'intermédiaire d'IIS.

La section 3. configurent le serveur de Microsoft CA pour éditer des fichiers CRL au point de distribution

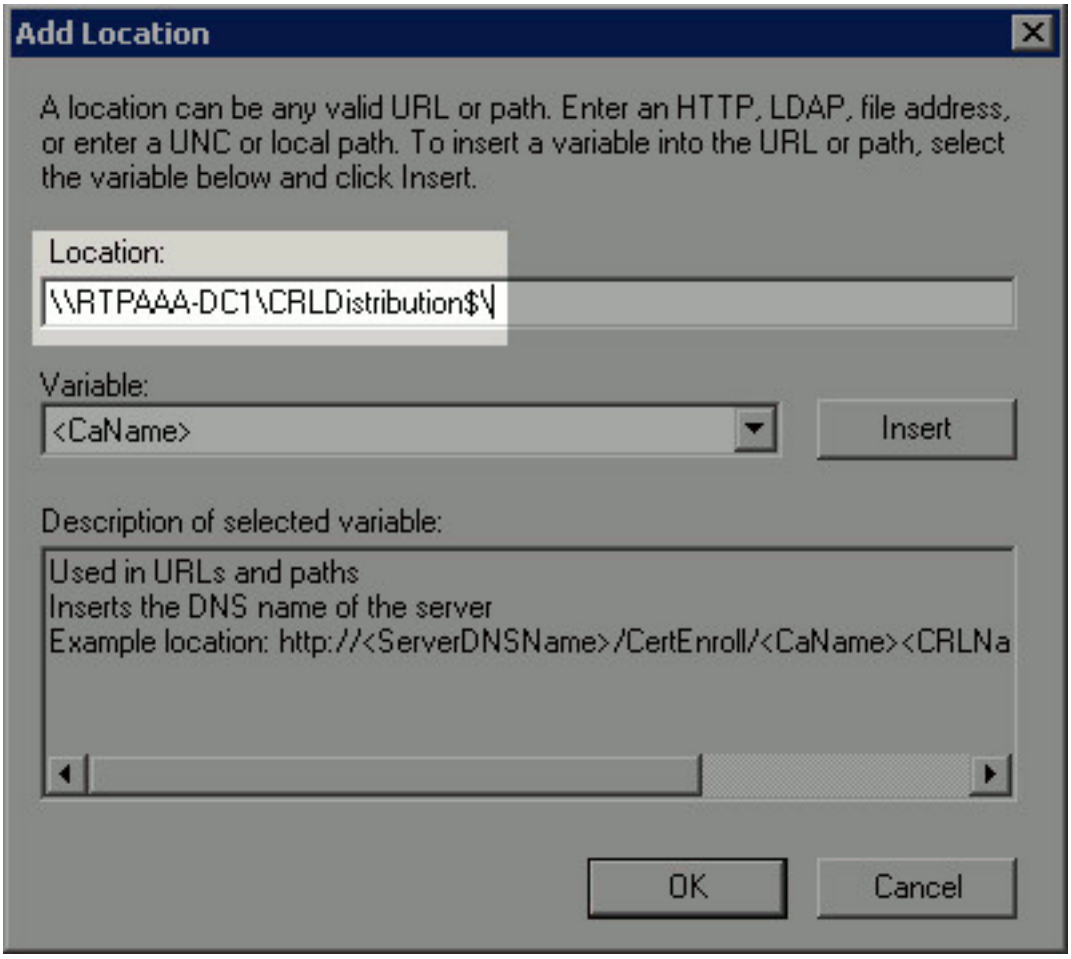
Maintenant qu'un nouveau répertoire a été configuré pour loger les fichiers CRL et le répertoire a été exposé dans IIS, configurez le serveur de Microsoft CA pour éditer les fichiers CRL au nouveau emplacement.

1. Sur la barre des tâches de serveur CA, **début de** clic. Choisissez les **outils d'administration > l'autorité de certification**.
2. Dans le volet gauche, cliquez avec le bouton droit le nom CA. Choisissez Properties et alors cliquez sur les **extensions** tableau afin d'ajouter un nouveau point de distribution CRL,

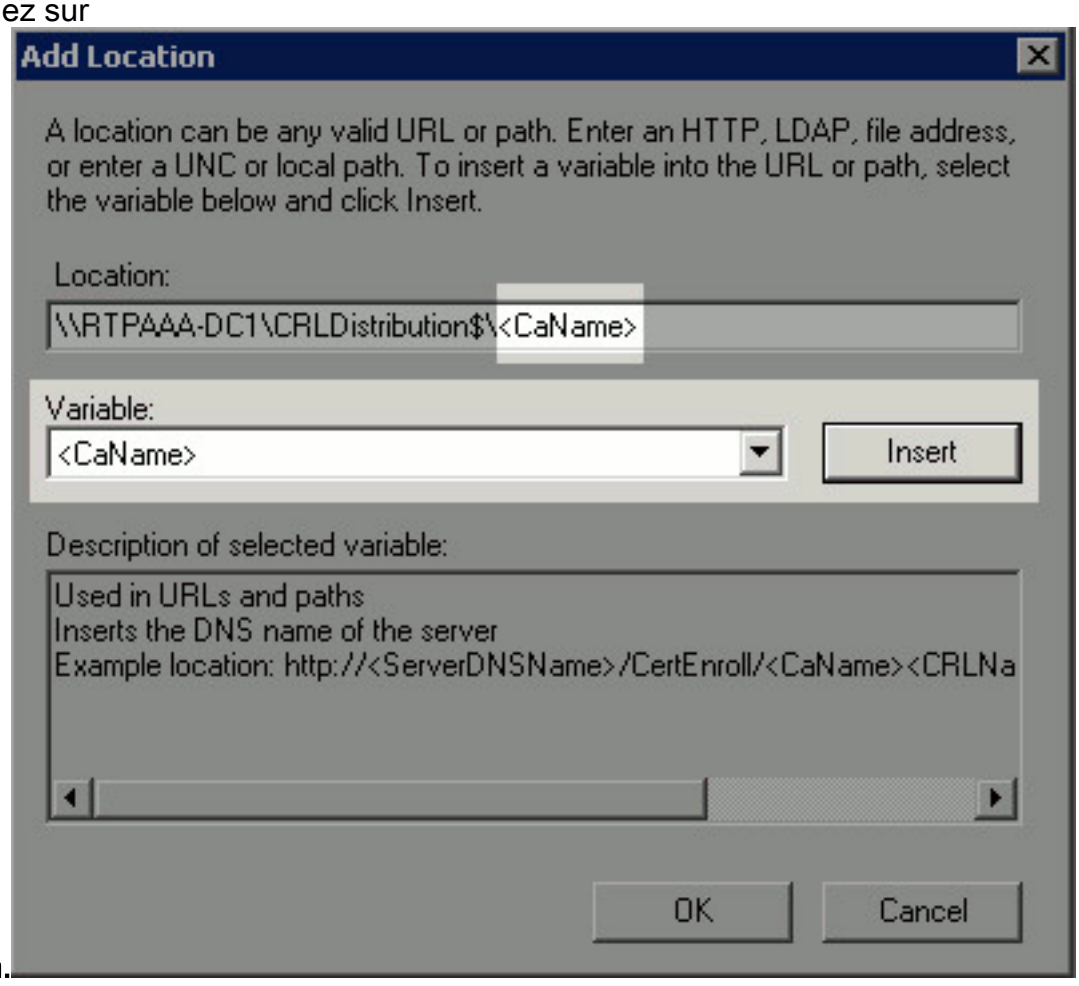


cliquez sur Add.

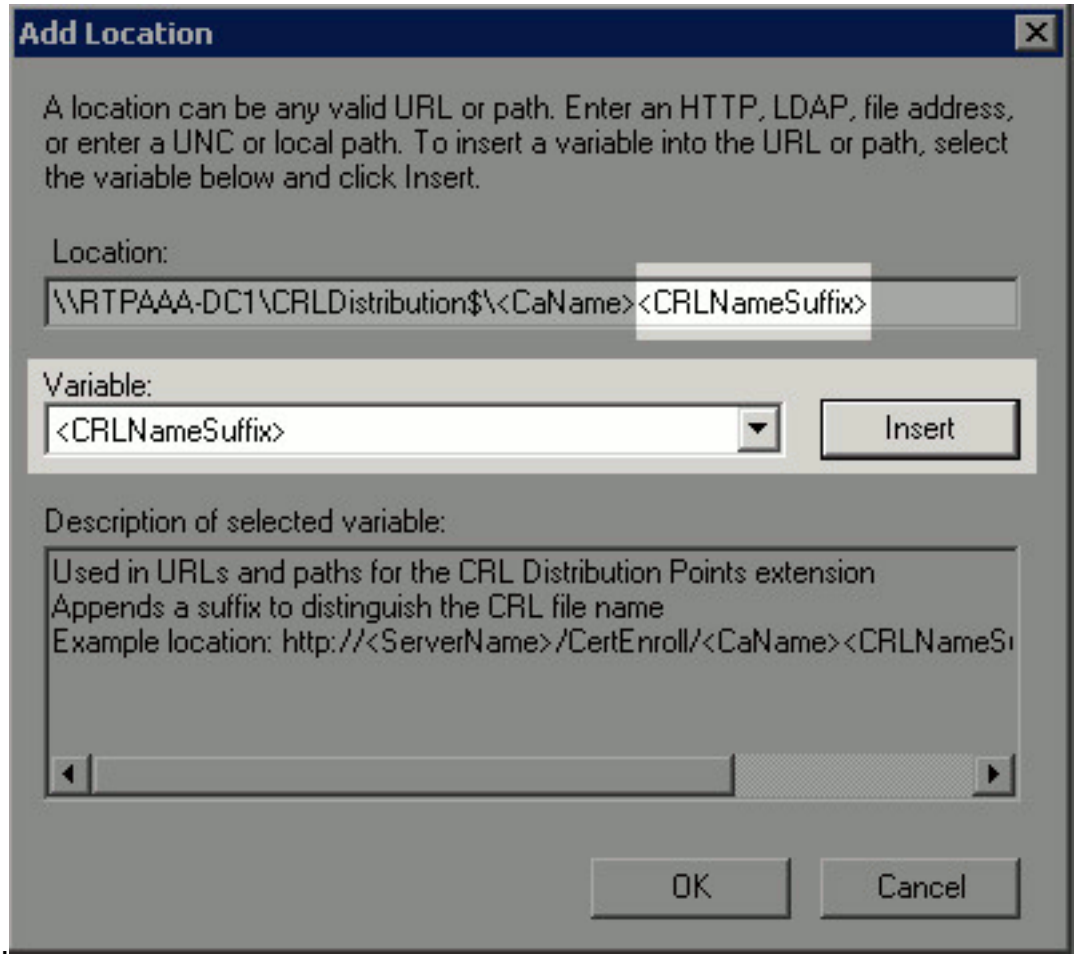
3. Dans le champ Location, entrez dans le chemin au répertoire créé et partagé dans la section 1. Dans l'exemple dans la section 1, le chemin est :
   `\\RTPAAA-DC1\CRLDistribution$\`



4. Le champ Location étant rempli, choisissez le **<CaName> de la** liste déroulante variable et puis cliquez sur l'**insertion.**

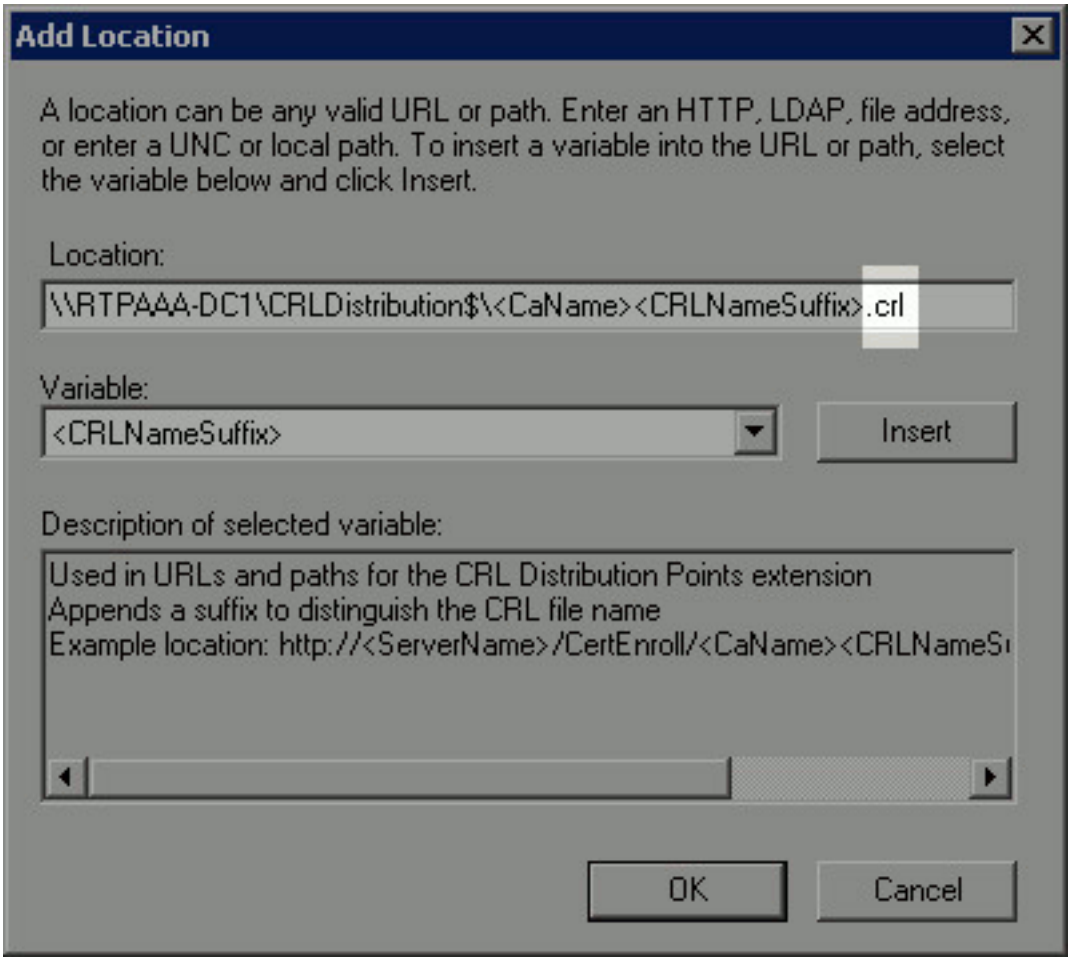


5. De la liste déroulante variable, choisissez le **<CRLNameSuffix>** et puis cliquez sur

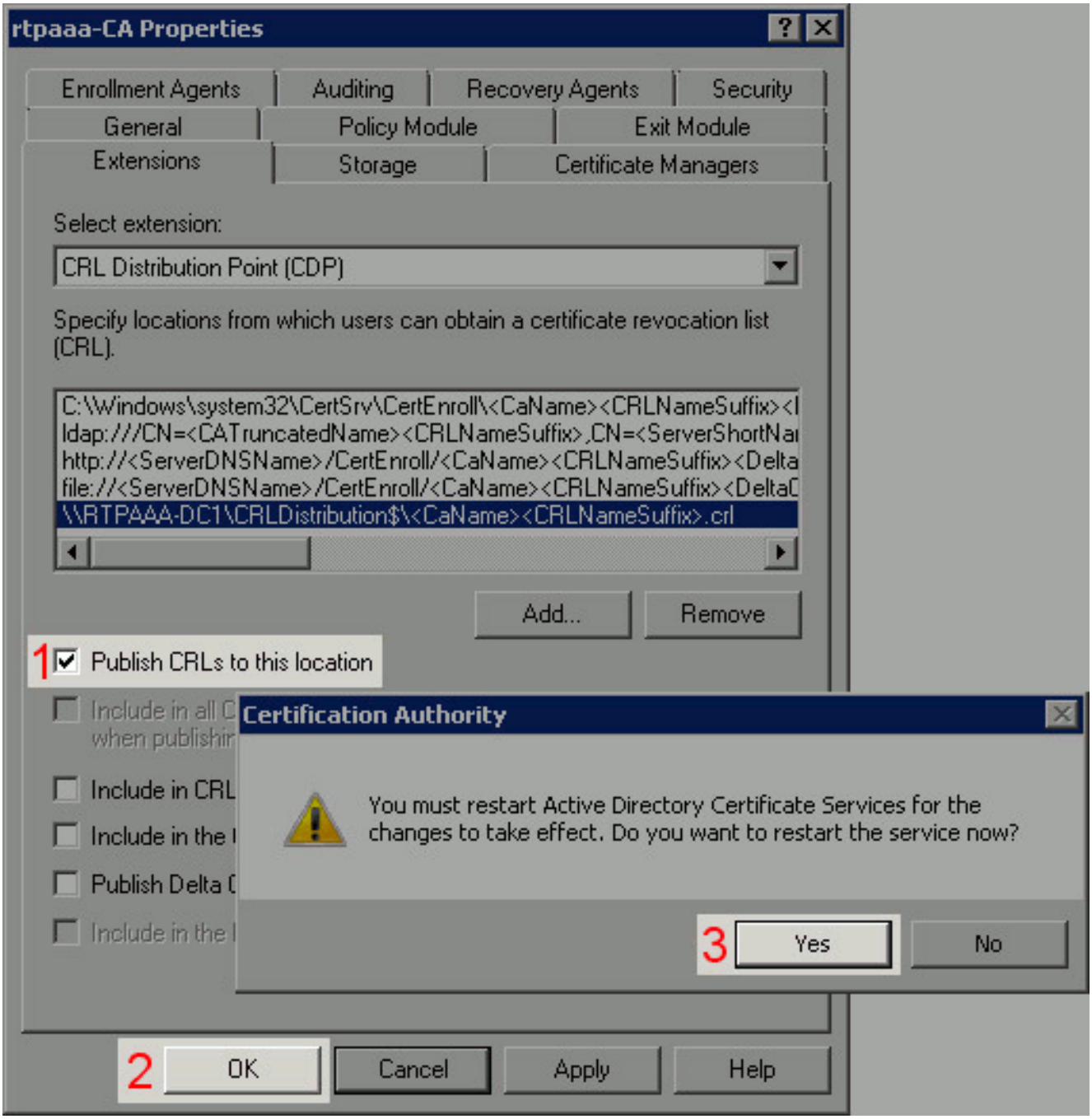


l'**insertion**.

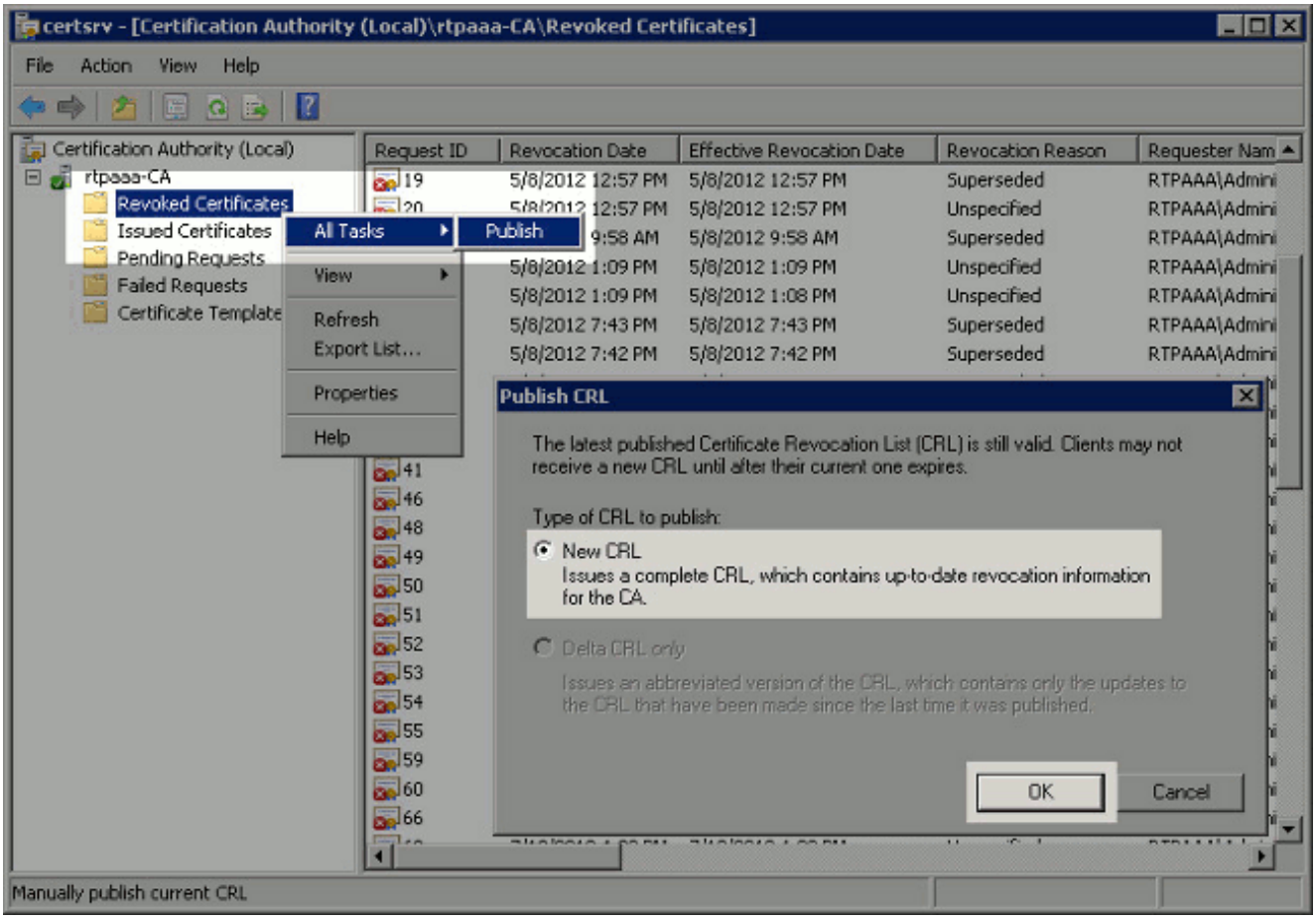
6. Dans le champ Location, ajoutez .crl à l'extrémité du chemin. Dans cet exemple, l'emplacement est :
   `\\RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl`



7. Cliquez sur OK pour retourner à l'onglet d'extensions. Cochez l'**édition CRLs dans cette** case d'**emplacement** (1) et puis cliquez sur OK (2) pour fermer la fenêtre de Properties. Une demande apparaît pour que l'autorisation redémarre des services de certificat de Répertoire actif. Clic **oui**
(3).



8. Dans le volet gauche, le clic droit **a retiré des Certificats**. Choisissez **toutes les tâches > éditent**. Assurez-vous que nouveau CRL est sélectionné et puis cliquez sur OK.

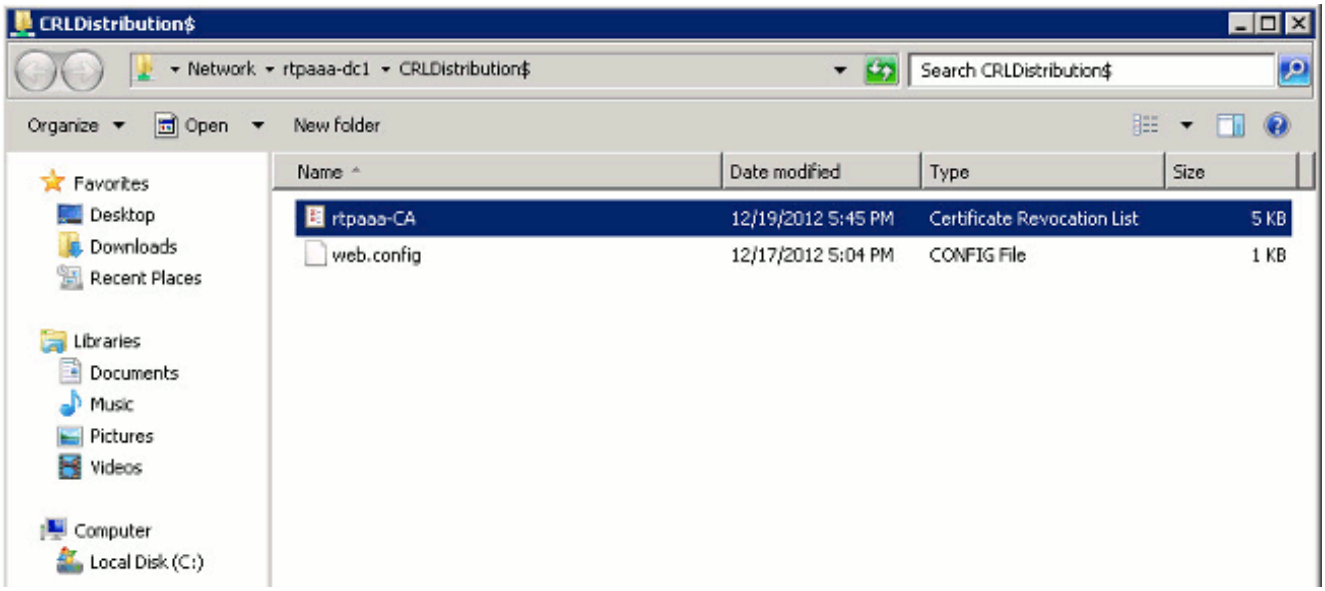


Le serveur de Microsoft CA devrait créer un nouveau fichier dans le dossier .crl créé dans la section 1. Si le nouveau fichier CRL est créé avec succès il n'y aura aucun dialogue après que CORRECT est cliqué sur. Si une erreur est retournée en vue de le nouveau répertoire de point de distribution, répétez soigneusement chaque étape dans cette section.

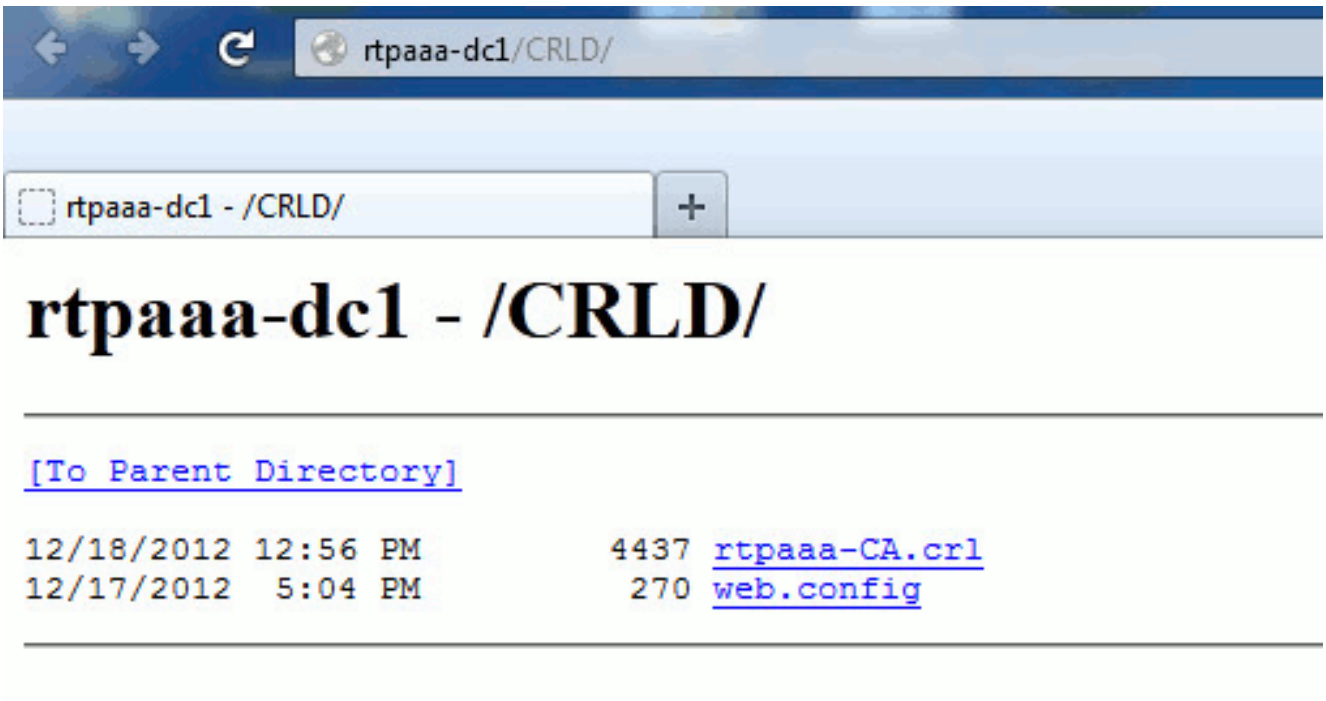
La section 4. vérifient le fichier CRL existe et est accessible par l'intermédiaire d'IIS

Vérifiez les nouveaux fichiers CRL existent et cela ils sont accessibles par l'intermédiaire d'IIS d'un autre poste de travail avant que vous commenciez cette section.

1. Sur le serveur IIS, ouvrez le répertoire créé dans la section 1. Il devrait y a un fichier simple .crl actuel avec la forme <CANAME>.crl où <CANAME> est le nom du serveur CA. Dans cet exemple, le nom du fichier est :
   `rtpaaa-CA.crl`



2. D'un poste de travail sur le réseau (idéalement sur le même réseau que le noeud primaire d'admin ISE), ouvrez un navigateur Web et parcourez à http:// <SERVER>/<CRLSITE> où <SERVER> est le nom du serveur du serveur IIS configuré dans la section 2 et <CRLSITE> est le nom du site choisi pour le point de distribution dans la section 2. Dans cet exemple, l'URL est :
`http://RTPAAA-DC1/CRLD`
Les affichages d'index de répertoire, qui inclut le fichier ont observé dans l'étape 1.



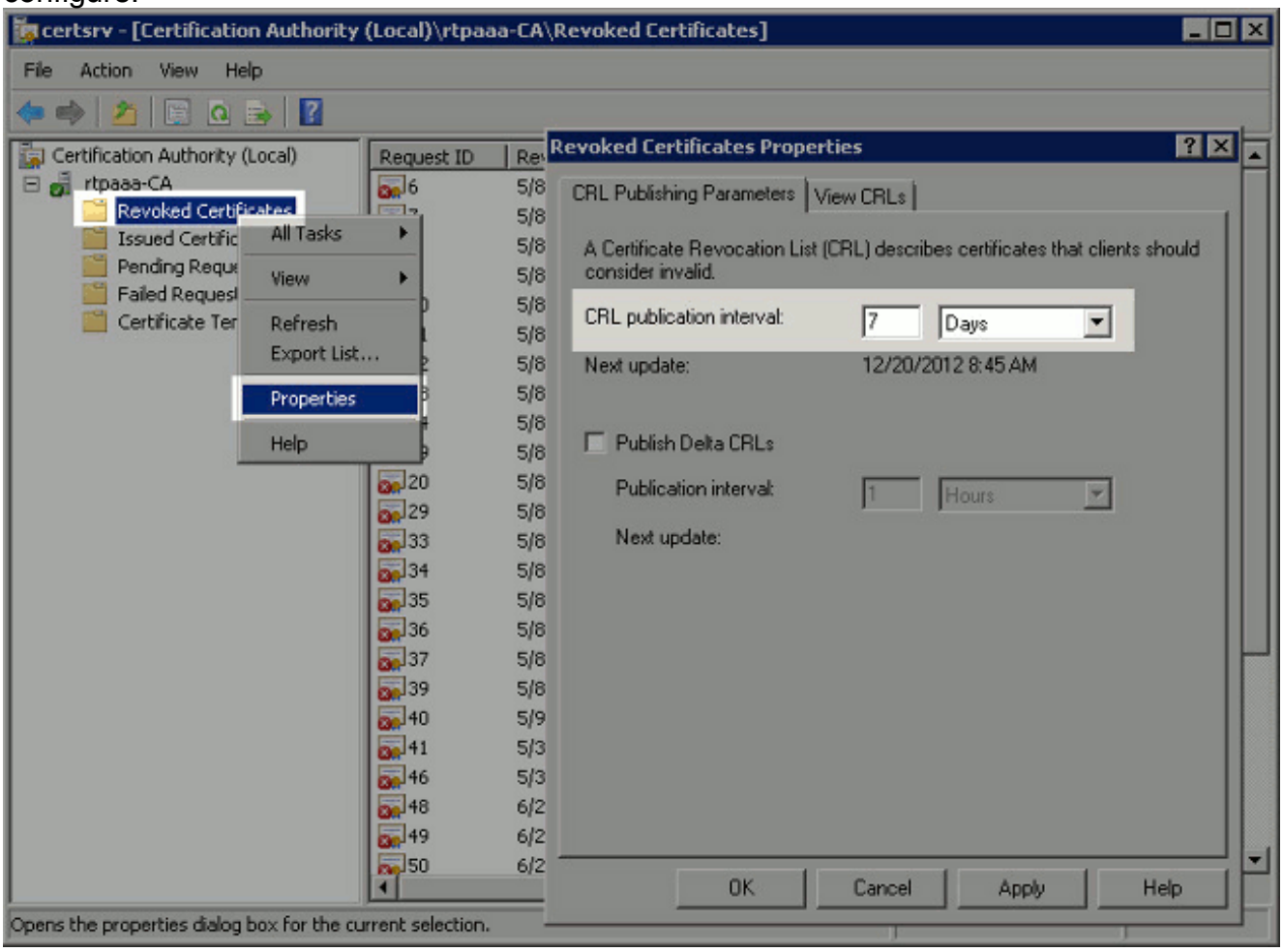
La section 5. configurent ISE pour utiliser le nouveau point de distribution CRL

Avant qu'ISE soit configuré pour récupérer le CRL, définissez l'intervalle pour éditer le CRL. La stratégie pour déterminer cet intervalle est hors de portée de ce document. Les valeurs potentielles (à Microsoft CA) sont de 1 heure à de 411 ans, d'incluses. La valeur par défaut est de 1 semaine. Une fois qu'un intervalle approprié pour votre environnement a été déterminé, placez l'intervalle avec ces instructions :

1. Sur la barre des tâches de serveur CA, **début de** clic. Choisissez les **outils d'administration >**

l'autorité de certification.

2. Dans le volet gauche, développez le clic droit CA le répertoire **retiré de Certificats** et choisissez Properties**.**
3. Dans les domaines d'intervalle de publication CRL, introduisez le nombre requis et choisissez le délai prévu. Cliquez sur OK pour fermer la fenêtre et pour appliquer la modification. Dans cet exemple, un intervalle de publication de 7 jours est configuré.



Vous devriez maintenant confirmer plusieurs valeurs de registre, qui aideront à déterminer les configurations de récupération CRL dans ISE.

4. Écrivez le **certutil - le getreg CA ** commande de **Clock*** de confirmer la valeur de ClockSkew. La valeur par défaut est de 10 minutes.Exemple de sortie :

```
Values:
    ClockSkewMinutes        REG_DWORS = a (10)
CertUtil: -getreg command completed successfully.
```

5. Écrivez le **certutil - le getreg CA ** commande de **CRLov*** de vérifier si le CRLOverlapPeriod a été manuellement placé. Par défaut la valeur de CRLOverlapUnit est 0, qui indique qu'aucune valeur manuelle n'a été placée. Si la valeur est une valeur autre que 0, enregistrez la valeur et les unités.Exemple de sortie :

```
Values:
    CRLOverlapPeriod      REG_SZ = Hours
    CRLOverlapUnits        REG_DWORD = 0
CertUtil: -getreg command completed successfully.
```

6. Écrivez le **certutil - le getreg CA ** commande de **CRLpe*** de vérifier le CRLPeriod, qui a été placé dans l'étape 3.Exemple de sortie :

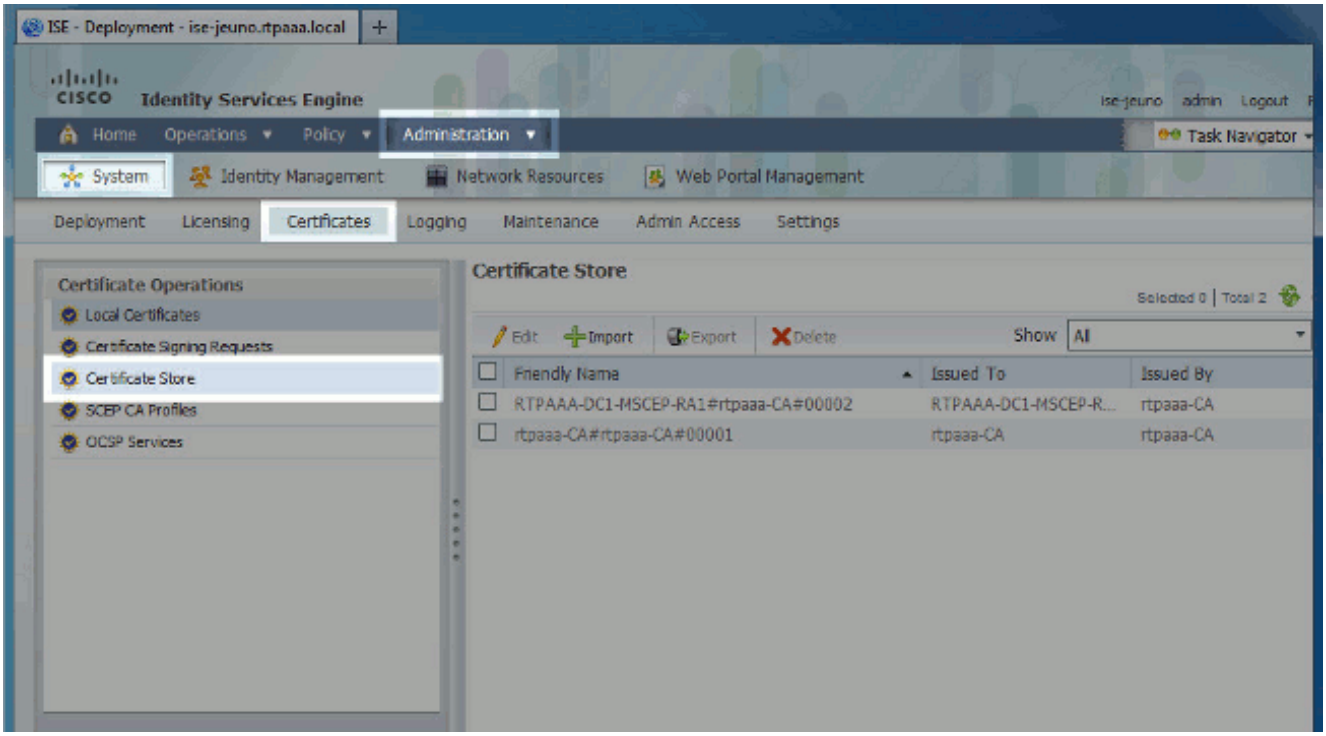
```
Values:
```

```
    CRLPeriod       REG_SZ = Days
    CRLUnits         REG_DWORD = 7
CertUtil: -getreg command completed successfully.
```

7. Calculez le délai de grâce CRL comme suit :Si CRLOverlapPeriod était placé dans l'étape 5 : SUPERPOSITION = CRLOverlapPeriod, en quelques minutes ;Autrement : SUPERPOSITION = (CRLPeriod/10), en quelques minutesSi SUPERPOSITION > puis SUPERPOSITION 720 = 720Si SUPERPOSITION < (1.5 * SUPERPOSITION de ClockSkewMinutes) puis = (1.5 * ClockSkewMinutes)Si SUPERPOSITION > CRLPeriod, dans la SUPERPOSITION de minutes puis = le CRLPeriod en quelques minutesDélai de grâce = 720 minutes + 10 minutes = 730 minutesExemple :
   ```
   As stated above, CRLPeriod was set to 7 days, or 10248 minutes and
   CRLOverlapPeriod was not set.

   a. OVERLAP = (10248 / 10) = 1024.8 minutes
   b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
   c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes
   d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
   e. Grace Period = 720 minutes + 10 minutes = 730 minutes
   ```

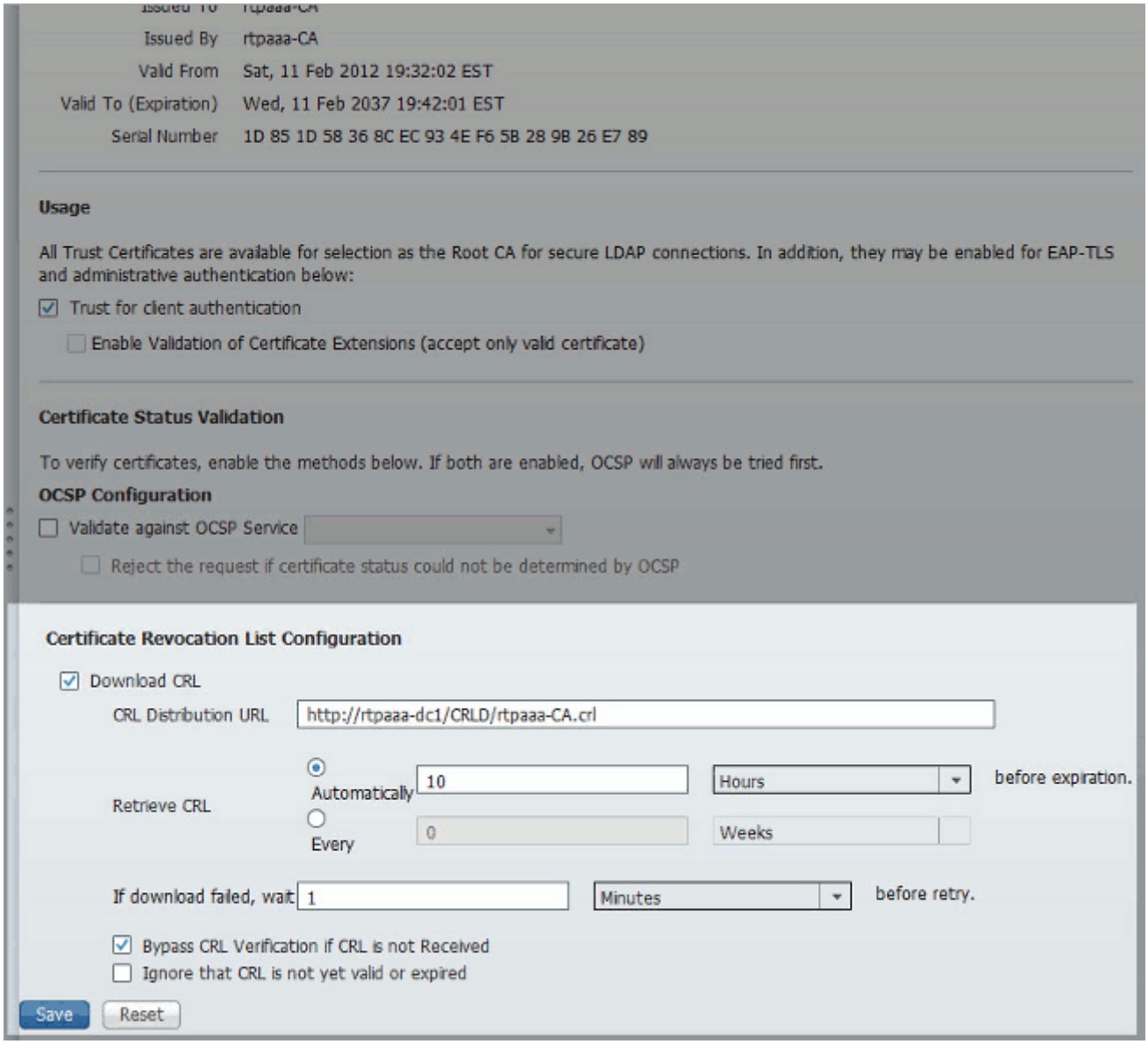
   Le délai de grâce calculé est la durée entre quand le CA édite le prochain CRL et quand le courant CRL expire. ISE doit être configuré pour récupérer le CRLs en conséquence.
8. Ouvrez une session au noeud primaire d'admin et choisissez la **gestion > le système > les Certificats**. Dans le volet gauche, **mémoire** choisie de **certificat**.



9. Cochez la case de mémoire de certificat à côté du certificat de CA pour lequel vous avez l'intention de configurer CRLs. Cliquez sur **Edit**.
10. Près du bas de la fenêtre, cochez la case du **téléchargement CRL**.
11. Dans le champ URL de distribution CRL, entrez dans le chemin au point de distribution CRL, qui inclut le fichier .crl, créé dans la section 2. Dans cet exemple, l'URL est :
    `http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl`
12. ISE peut être configuré pour récupérer le CRL à intervalles réguliers ou être basé sur l'expiration (qui, est généralement également un intervalle régulier). Quand les CRL éditent

l'intervalle est charge statique, des mises à jour plus opportunes CRL sont obtenus quand la dernière option est utilisée. Cliquez sur **automatiquement la** case d'option.

13. Placez la valeur pour la récupération à une valeur moins que le délai de grâce calculé dans l'étape 7. Si le positionnement de valeur est plus long que le délai de grâce, ISE vérifie le point de distribution CRL avant que le CA ait édité le prochain CRL. Dans cet exemple, le délai de grâce est calculé pour être de 730 minutes, ou de 12 heures et de 10 minutes. Une valeur de 10 heures sera utilisée pour la récupération.
14. Placez le retry interval comme approprié pour votre environnement. S'ISE ne peut pas récupérer le CRL à l'intervalle configuré dans l'étape précédente, il relancera à cet intervalle plus court.
15. Cochez la **vérification du contournement CRL si CRL n'est pas** case **reçue** pour permettre à l'authentification basée sur certificat pour poursuivre normalement (et sans contrôle CRL) s'ISE ne pouvait pas récupérer le CRL pour ce CA dans sa dernière tentative de téléchargement. Si cette case n'est pas cochée, toute l'authentification basée sur certificat avec des Certificats délivrés par ce CA échouera si le CRL ne peut pas être récupéré.
16. Cochez l'**ignorer que CRL n'est pas** case **encore valide ou expirée** pour permettre à ISE pour utiliser (ou pas encore valide) les fichiers expirés CRL comme s'ils étaient valides. Si cette case n'est pas cochée, ISE considère comme étant un CRL non valide avant leur date effective et après leurs minuteurs de mise à jour suivants. **Sauvegarde de** clic pour se terminer la
configuration.



Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support et documentation techniques - Cisco Systems