

Intégration de Cisco ACS 5.X avec le serveur de jetons RSA SecurID

Contenu

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurations](#)

[Serveur RSA](#)

[Serveur de version 5.X ACS](#)

[Vérifier](#)

[Serveur de version 5.X ACS](#)

[Serveur RSA](#)

[Dépanner](#)

[Créez un enregistrement d'agent \(sdconf.rec\)](#)

[Remettez à l'état initial le secret de noeud \(le securid\)](#)

[Équilibrage de charge automatique de priorité](#)

[Intervenez manuellement pour retirer un serveur du bas RSA SecurID](#)

Introduction

Ce document décrit comment intégrer une version 5.x du système de contrôle d'accès de Cisco (ACS) avec la technologie d'authentification de la RSA SecurID.

Informations générales

Le Cisco Secure ACS prend en charge le serveur RSA SecurID comme base de données externe.

L'authentification à deux facteurs RSA SecurID comprend le numéro d'identification personnel de l'utilisateur (PIN) et un jeton individuellement enregistré RSA SecurID qui génère les codes de symboles à utiliser une seule fois basés sur un algorithme de code de temps.

Un code de symboles différent est généré à intervalles fixes, habituellement toutes les 30 ou 60 secondes. Le serveur RSA SecurID valide ce code dynamique d'authentification. Chaque jeton RSA SecurID est seul, et il n'est pas possible de prévoir la valeur des jetons passés en fonction basés un futur par jeton.

Ainsi, quand un code de symboles correct est fourni ainsi qu'un PIN, il y a un degré élevé de

certitude que la personne est un utilisateur valide. Par conséquent, les serveurs RSA SecurID fournissent un mécanisme d'authentification plus fiable que des mots de passe réutilisables conventionnels.

Vous pouvez intégrer Cisco ACS 5.x avec la technologie d'authentification RSA SecurID de ces manières :

- Agent RSA SecurID - Des utilisateurs sont authentifiés avec le nom d'utilisateur et le code de passage par le protocole indigène RSA.
- Protocole RADIUS - Des utilisateurs sont authentifiés avec le nom d'utilisateur et le code de passage par le protocole RADIUS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Sécurité RSA
- Système de contrôle d'accès sécurisé Cisco (ACS)

[Composants utilisés](#)

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

- Version 5.x du Système de contrôle d'accès sécurisé Cisco (ACS)
- Serveur de jetons RSA SecurID

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.

Configurations

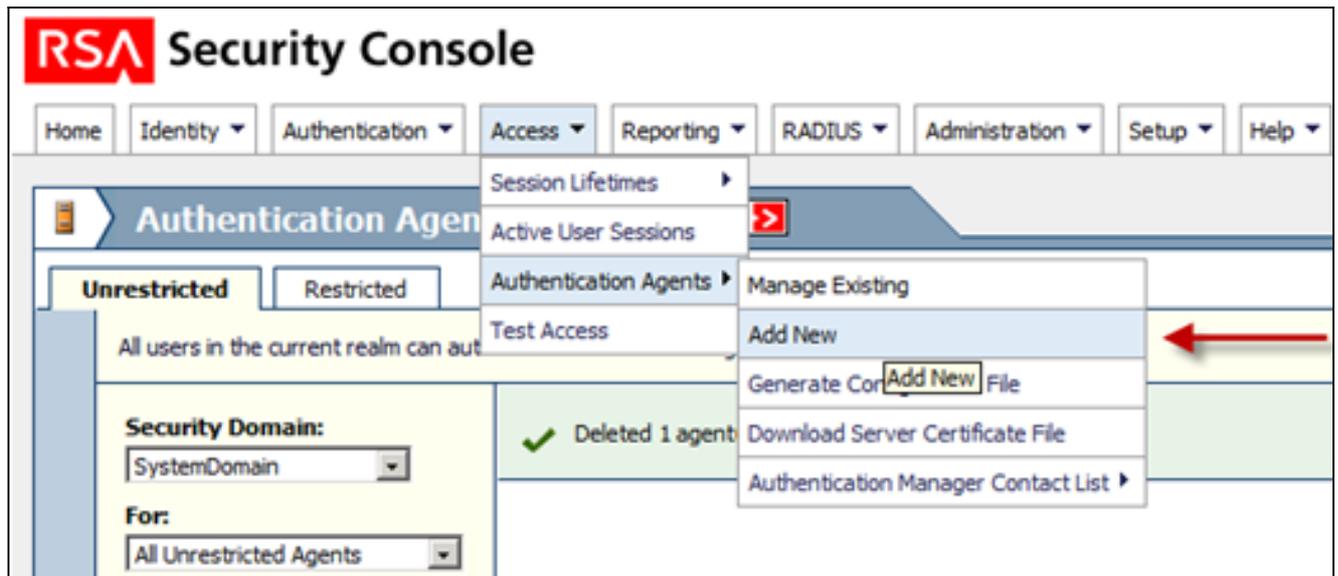
Serveur RSA

Cette procédure décrit comment l'administrateur du serveur RSA SecurID crée des agents d'authentification et un fichier de configuration. Un agent d'authentification est fondamentalement un nom de Domain Name Server (DN) et une adresse IP d'un périphérique, d'un logiciel, ou d'un service qui a des droits d'accéder à la base de données RSA. Le fichier de configuration décrit fondamentalement la topologie et la transmission RSA.

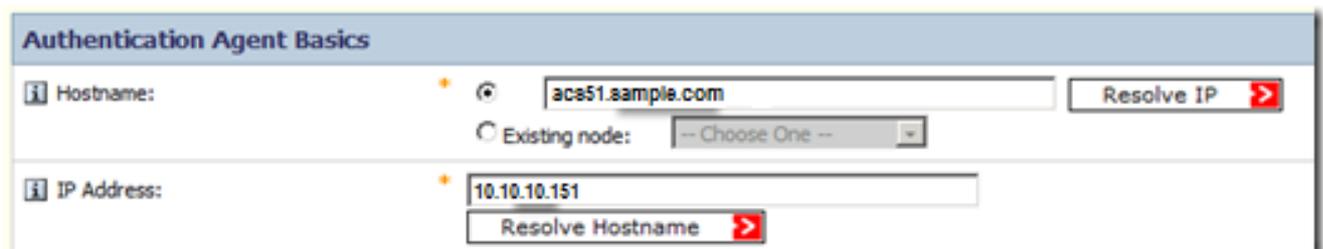
Dans cet exemple, l'administrateur RSA doit créer deux agents pour les deux exemples ACS.

1. Dans la console de RSA Security, naviguez **pour accéder à > des agents d'authentification >**

ajoutent nouveau :

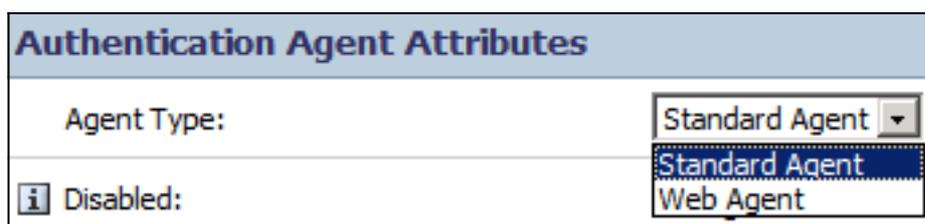


2. Dans la nouvelle fenêtre d'agent d'authentification d'ajouter, définissez une adresse Internet et une adresse IP pour chacun des deux agents :



Les DN expédient et les consultations d'inverse pour des agents ACS devraient fonctionner.

3. Définissez le type d'agent en tant qu'agent standard :

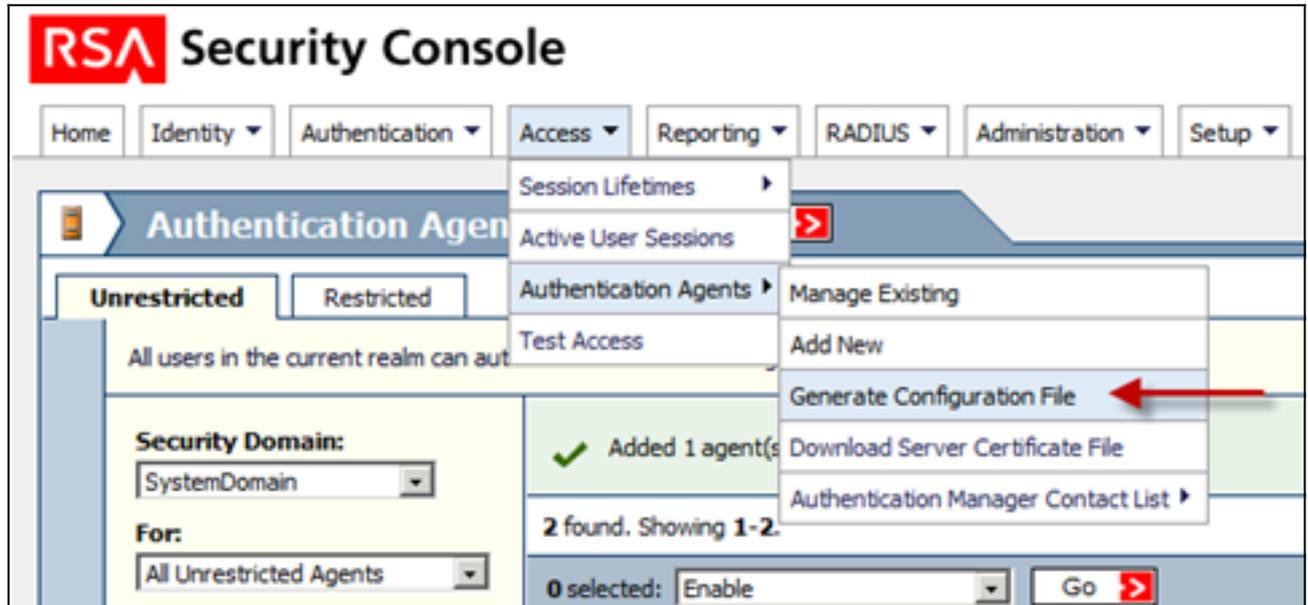


C'est un exemple des informations que vous voyez une fois que les agents sont ajoutés :

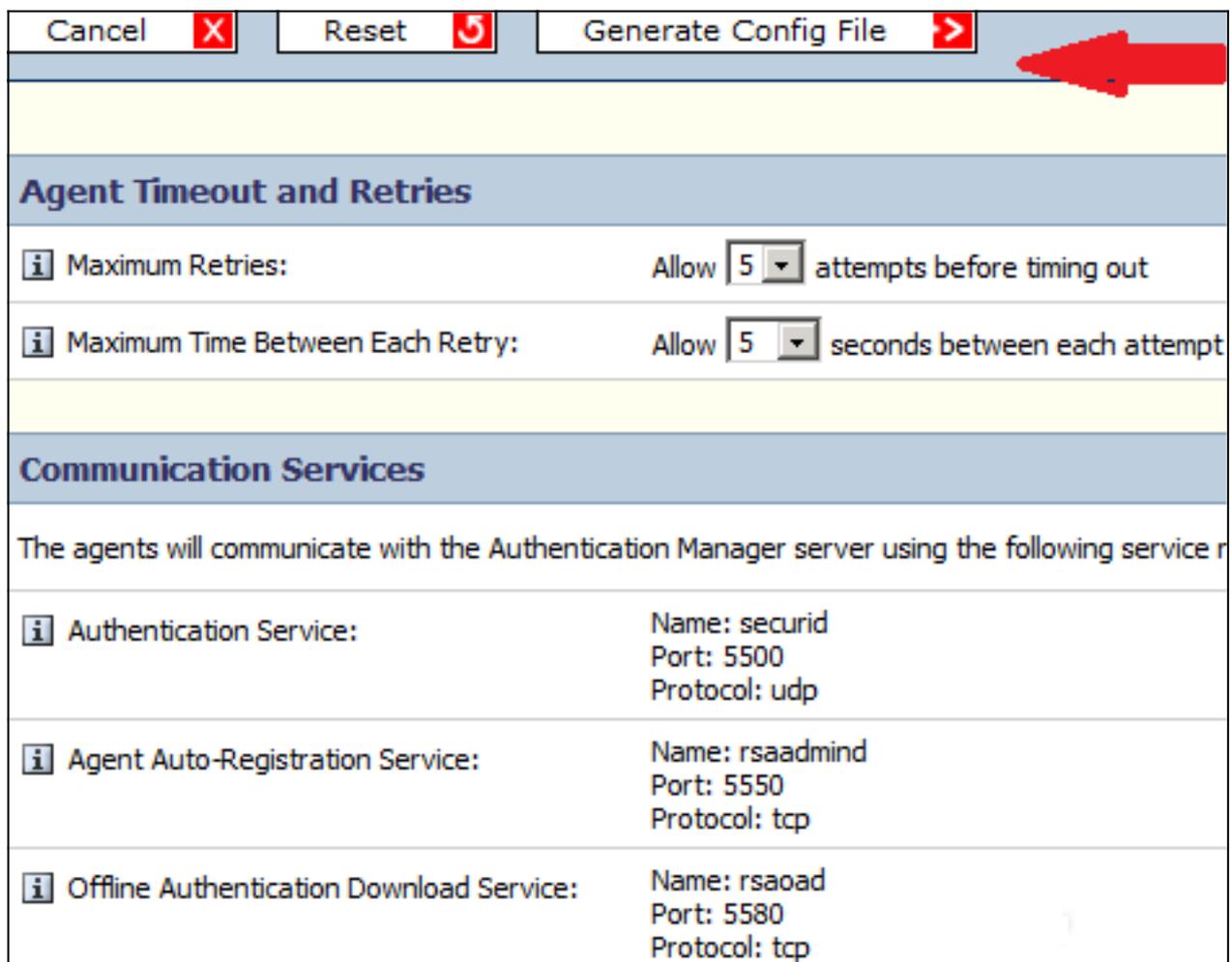
The screenshot shows a table listing the added authentication agents. The table has columns for 'Authentication Agent', 'IP Address', 'Type', 'Disabled', and 'Security Domain'. There are two agents listed: 'acs51.sample.com' and 'acs52.sample.com', both of type 'Standard Agent' and located in the 'SystemDomain' security domain. The table also shows a search bar at the top and bottom with '0 selected' and 'Enable' options.

Authentication Agent	IP Address	Type	Disabled	Security Domain
<input type="checkbox"/> acs51.sample.com	10.10.10.151	Standard Agent		SystemDomain
<input type="checkbox"/> acs52.sample.com	10.10.10.152	Standard Agent		SystemDomain

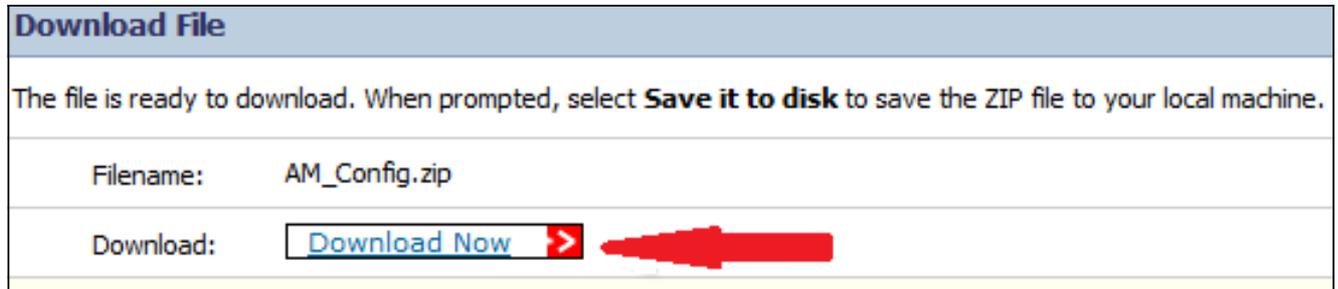
4. Dans la console de RSA Security, naviguez pour accéder à > des agents d'authentification > génèrent le fichier de configuration afin de générer le fichier de configuration sdconf.rec :



5. Utilisez les valeurs par défaut pour des relances maximum et le temps maximum entre chaque relance :



6. Téléchargez le fichier de configuration :

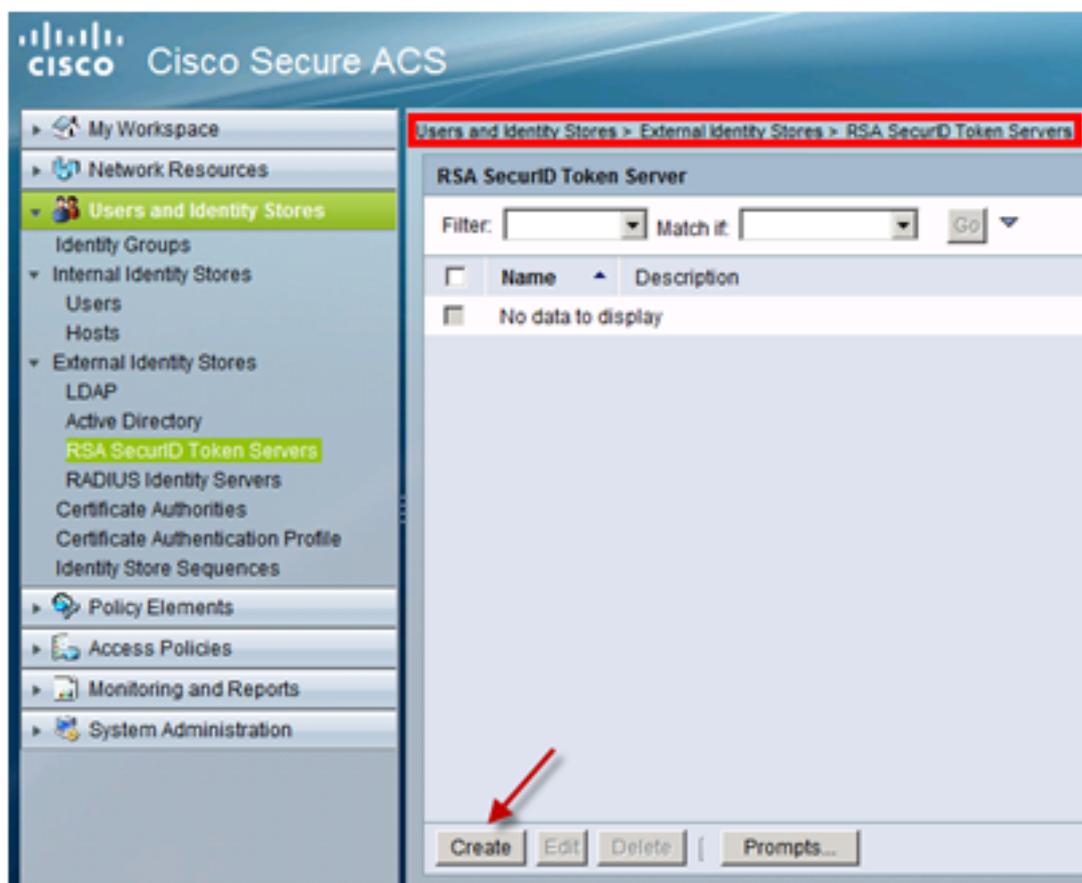


Le fichier .zip contient le fichier réel de la configuration sdconf.rec, dont l'administrateur ACS a besoin afin de se terminer des tâches de configuration.

Serveur de version 5.X ACS

Cette procédure décrit comment l'administrateur ACS récupère et soumet le fichier de configuration.

1. Dans la console de version 5.x de Cisco Secure ACS, naviguez vers des **utilisateurs et l'identité enregistrée** > **identité externe enregistrée** > des **serveurs de jetons de la RSA SecurID**, et le clic **créent** :



2. Écrivez le nom du serveur RSA, et parcourez au fichier sdconf.rec qui a été téléchargé du serveur RSA :

Users and Identity Stores > External Identity Stores > RSA SecurID Token Servers > Create

RSA Realm ACS Instance Settings Advanced

General

Name: RSA SecurID AM
 Description: RSA SecurID Authentication Manager Server

Server connection

Server Timeout: 30 Seconds
 Reauthenticate on Change PIN

Realm Configuration File

The RSA Configuration file (sdconf.rec) should be provided by your RSA administrator after they have

Import new 'sdconf.rec' file: C:\users\!\Desktop\sdconf.rec

Node Secret Status: - not created -

* = Required fields

3. Sélectionnez le fichier, et cliquez sur Submit.

Note: La première fois que l'ACS contacte le serveur de jetons, un autre fichier, appelé le fichier secret de noeud, est créé pour l'agent ACS sur le gestionnaire d'authentification RSA et est téléchargé à l'ACS. Ce fichier est utilisé pour la transmission chiffrée.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Serveur de version 5.X ACS

Afin de vérifier une procédure de connexion réussie, allez à la console ACS, et passez en revue le nombre de hits :

Access Policies > Access Services > Service Selection Rules

Single result selection Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals

	Status	Name	Protocol	Conditions	Results	Hit Count
				NDG:Device Type	Service	
1	<input type="checkbox"/>	Rule-4	-ANY-	In All Device Types:SWITCHES	RSA Device Admin	2

Vous pouvez également passer en revue les détails d'authentification des logs ACS :

Authentication Details	
Status:	Passed
Failure Reason:	
Logged At:	Feb 16, 2013 12:24 PM
ACS Time:	Feb 16, 2013 12:24 PM
ACS Instance:	<u>acs51</u>
Authentication Method:	PAP_ASCII
Authentication Type:	ASCII
Privilege Level:	1
User	
Username:	TEST1
Remote Address:	
Network Device	
Network Device:	<u>SwitchBNNZ231</u>
Network Device IP Address:	
Network Device Groups:	Device Type:All Device Types:SWITCHES:SWITCHES_SSH, Location:All Locations:DATACENTER_BN
Access Policy	
Access Service:	<u>RSA Device Admin</u>
Identity Store:	RSA SecurID AM
Selected Shell Profile:	PRIVILEGE_15
Active Directory Domain:	
Identity Group:	
Access Service Selection Matched Rule :	Rule-4

Serveur RSA

Afin de vérifier l'authentification réussie, aller à la console RSA, et passer en revue les logs :

Clear Monitor <input type="checkbox"/>							
Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP
i 2013-02-16 12:35:28.764	Principal authentication	User attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "MediumSecurityDomain"	<u>Authentication method success</u>	TEST1	acs51.sample.com	10.10.10.211	10.10.10.151

Dépanner

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Créez un enregistrement d'agent (sdconf.rec)

Afin de configurer un serveur de jetons de la RSA SecurID dans la version 5.3 ACS, l'administrateur ACS doit avoir le fichier `sdconf.rec`. Le fichier `sdconf.rec` est un fichier record de configuration qui spécifie comment l'agent RSA communique avec le royaume de serveur RSA SecurID.

Afin de créer le fichier `sdconf.rec`, l'administrateur RSA devrait ajouter l'hôte ACS comme hôte d'agent sur le serveur RSA SecurID et générer un fichier de configuration pour cet hôte d'agent.

Remettez à l'état initial le secret de noeud (le securid)

Après que l'agent communique au commencement avec le serveur RSA SecurID, le serveur fournit à l'agent un fichier secret de noeud appelé le `securid`. La transmission ultérieure entre le serveur et l'agent se fonde sur l'échange du secret de noeud afin de vérifier l'autre authenticité.

Parfois, les administrateurs pourraient devoir remettre à l'état initial le secret de noeud :

1. L'administrateur RSA doit décocher la case créée par secret de noeud sur l'enregistrement d'hôte d'agent dans le serveur RSA SecurID.
2. L'administrateur ACS doit retirer le fichier `SecureID` de l'ACS.

Équilibrage de charge automatique de priorité

L'agent RSA SecurID équilibre automatiquement les chargements demandés sur les serveurs RSA SecurID dans le royaume. Cependant, vous avez l'option d'équilibrer manuellement le chargement. Vous pouvez spécifier le serveur utilisé par chacun des hôtes d'agent. Vous pouvez assigner une priorité à chaque serveur de sorte que l'hôte d'agent dirige des demandes d'authentification vers quelques serveurs plus fréquemment que d'autres.

Vous devez spécifier les configurations de la priorité dans un fichier texte, les sauvegarder comme `sdopts.rec`, et les télécharger à l'ACS.

Intervenez manuellement pour retirer un serveur du bas RSA SecurID

Quand un serveur RSA SecurID est en panne, le mécanisme automatique d'exclusion ne fonctionne pas toujours rapidement. Retirez le fichier `sdstatus.12` de l'ACS afin d'accélérer ce processus.