Cisco ACS 5.X-integratie met RSA Secure Token Server

Inhoud

Inleiding

Dit document beschrijft hoe u een Cisco Access Control System (ACS) versie 5.x kunt integreren met RSA SecureID-verificatietechnologie.

Achtergrondinformatie

Cisco Secure ACS ondersteunt de RSA SecurityID server als een externe database.

RSA SecurID 2-factor authenticatie bestaat uit het persoonlijke identificatienummer van de gebruiker (PIN) en een individueel geregistreerd RSA SecurID-token dat token codes voor eenmalig gebruik genereert op basis van een tijdcode-algoritme.

Een andere token code wordt gegenereerd met vaste intervallen, gewoonlijk om de 30 of 60 seconden. De RSA SecurID server bevestigt deze dynamische authenticatie code. Elk RSA SecurID-token is uniek en het is niet mogelijk om de waarde van een toekomstig token te voorspellen op basis van eerdere tokens.

Wanneer een juiste symbolische code samen met een PIN wordt geleverd, is er dus een hoge

mate van zekerheid dat de persoon een geldige gebruiker is. Daarom bieden RSA SecurID-servers een betrouwbaarder authenticatiemechanisme dan conventionele herbruikbare wachtwoorden.

U kunt een Cisco ACS 5.x op deze manieren integreren met RSA SECurID-verificatietechnologie:

- RSA SecurID Agent - De gebruikers zijn geauthentiseerd met gebruikersnaam en wachtwoord door het autochtone RSA protocol.
- RADIUS-protocol - De gebruikers zijn gecertificeerd met de gebruikersnaam en het wachtwoord in het RADIUS-protocol.

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- RSA-beveiliging
- Cisco Secure Access Control System (ACS)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Access Control System (ACS) versie 5.x
- RSA SecureID Token Server

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

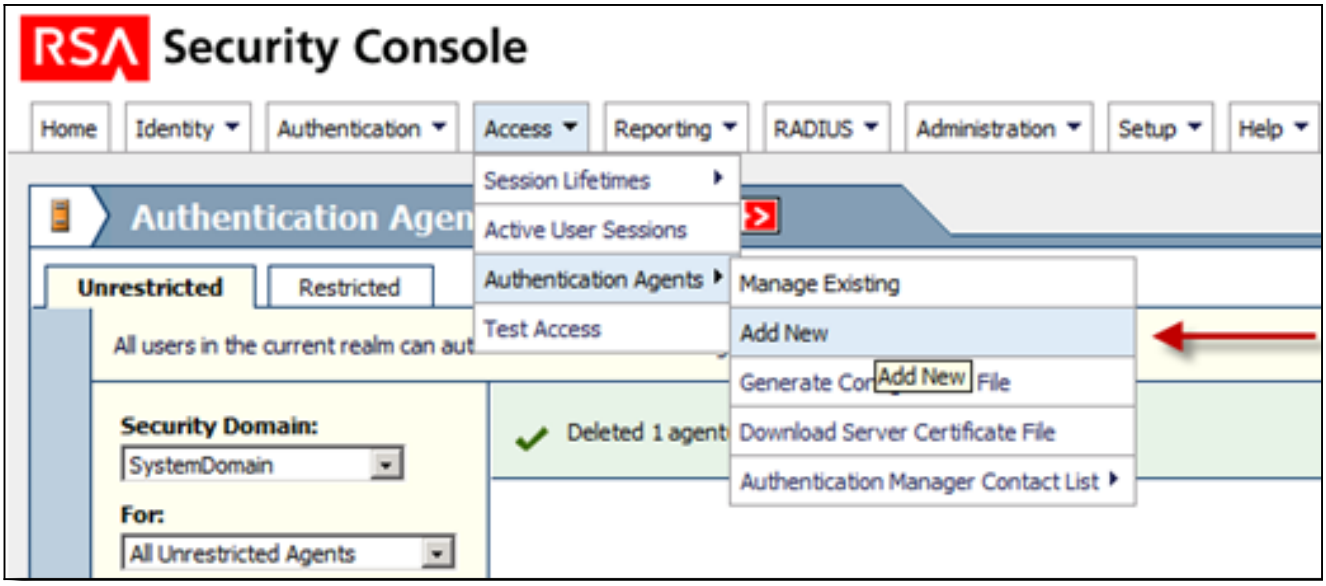
Configuraties

RSA-server

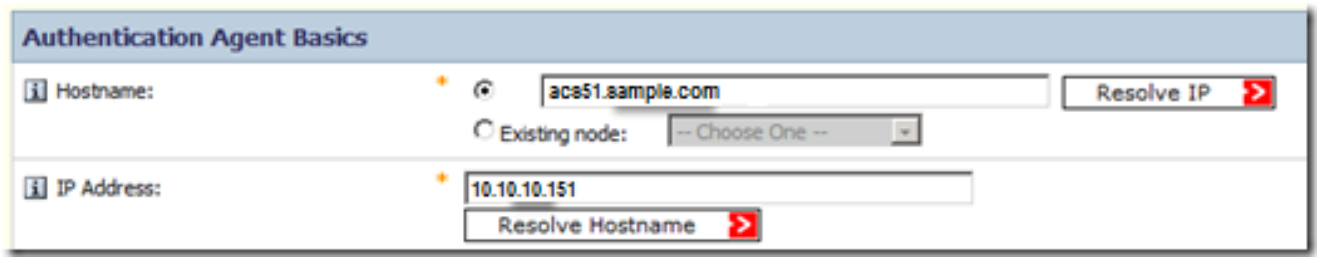
Deze procedure beschrijft hoe de RSA SecurID serverbeheerder authentificatieagenten en een configuratiebestand creëert. Een verificatie-agent is in wezen een DNS-naam (Domain Name Server) en een IP-adres van een apparaat, software of service die rechten heeft op toegang tot de RSA-database. Het configuratiebestand beschrijft in principe de topologie en de communicatie van RSA.

In dit voorbeeld, moet de RSA beheerder twee agenten voor de twee ACS instanties creëren.

1. In de RSA Security Console, navigeer naar **Access > Verificatieagenten > Voeg nieuw toe**:

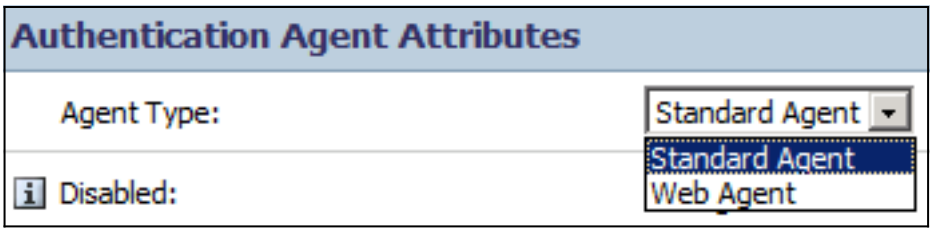


2. In het venster Add New Authentication Agent definieert een Hostname en IP-adres voor elk van de twee agents:

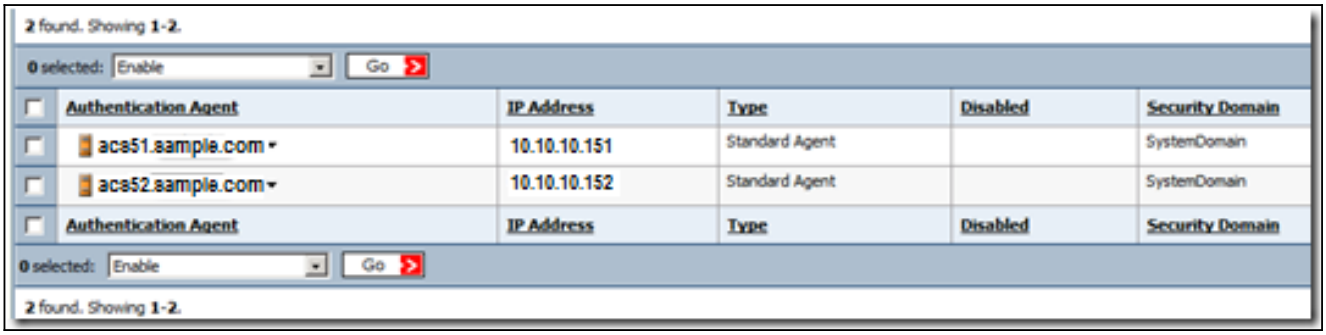


Zowel DNS voorwaartse als omgekeerde raadpleging voor ACS-agents moet werken.

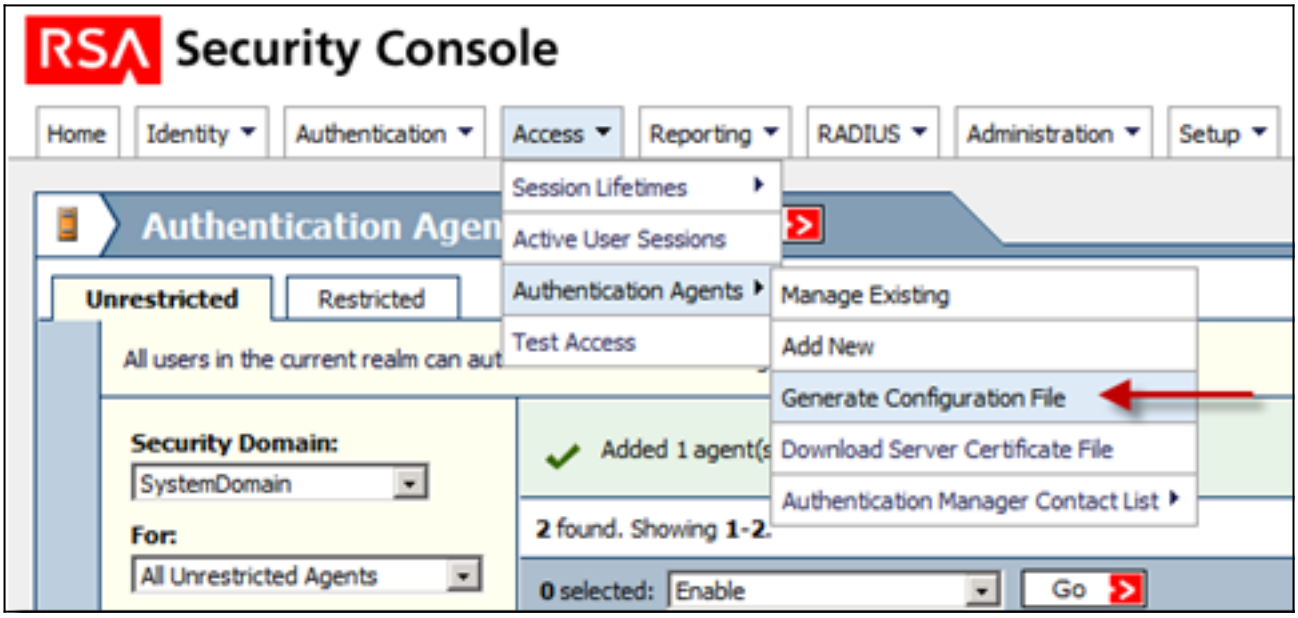
3. Bepaal het type Agent als standaardagent:



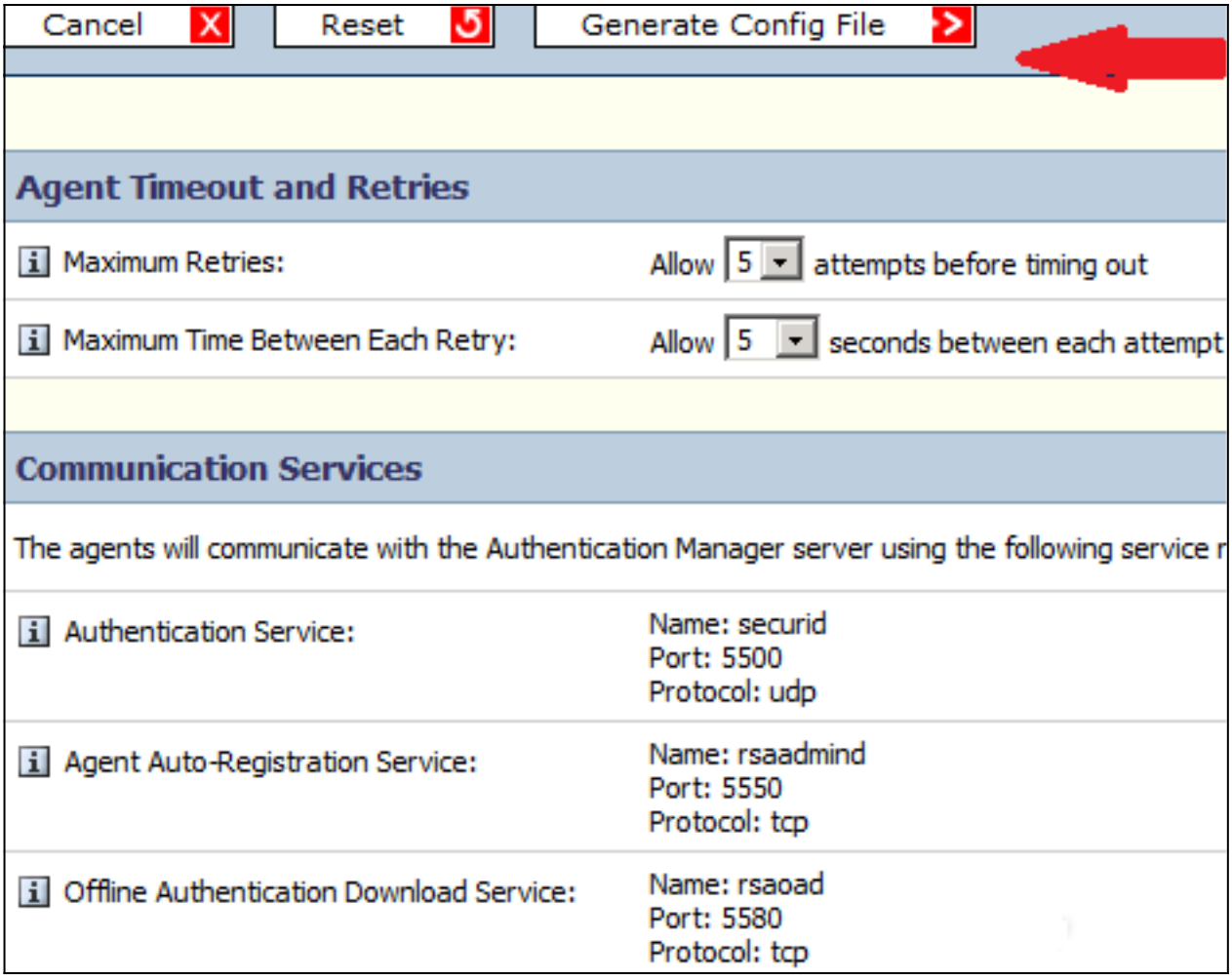
Dit is een voorbeeld van de informatie die u ziet wanneer de agents worden toegevoegd:



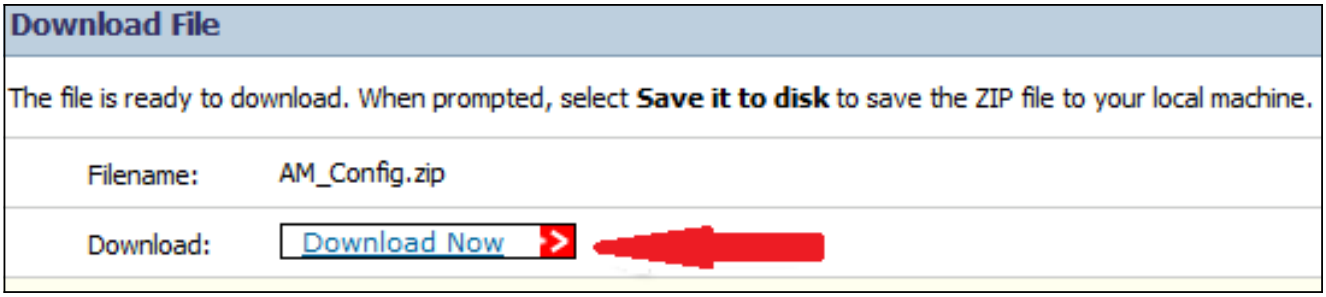
4. In de RSA Security Console, navigeer naar **Access** > **Verificatieagenten** > **Generate Configuration File** om het sdconf.rec-configuratiebestand te genereren:



5. Gebruik de standaardwaarden voor maximale herhalingen en maximale tijd tussen elk opnieuw proberen:



6. Download het configuratiebestand:

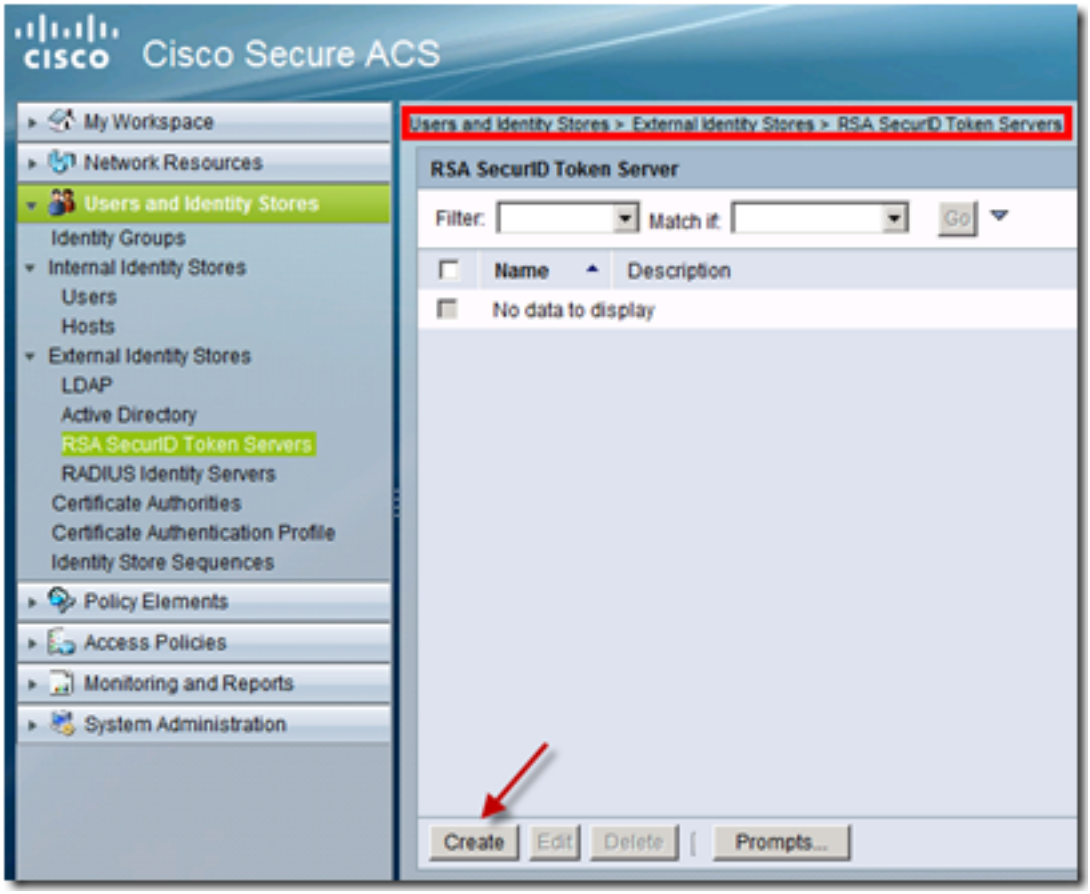


Het .zip-bestand bevat het eigenlijke configuratie sdconf.rec-bestand, dat de ACS-beheerder nodig heeft om de configuratietaken te voltooien.

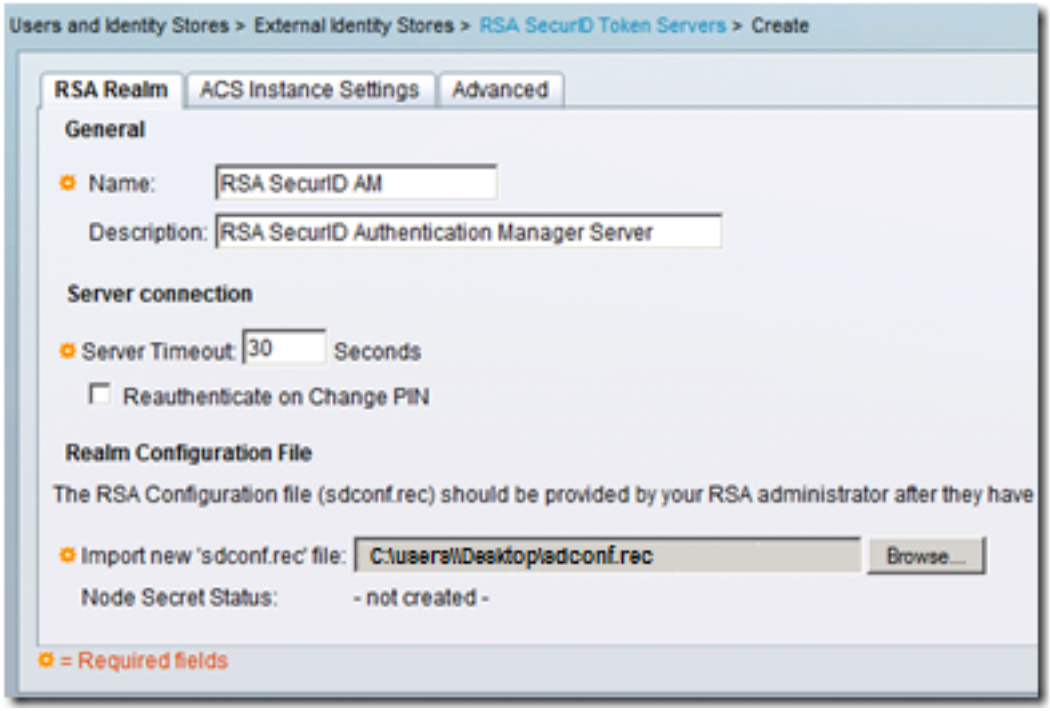
ACS versie 5.X-server

Deze procedure beschrijft hoe de ACS-beheerder het configuratiebestand terugwint en overlegt.

1. In de Cisco Secure ACS, versie 5.x-console, navigeer naar **gebruikers en identiteitsopslag > Externe identiteitsopslag > RSA SecureID Token Server** en klik op **Maken**:



2. Voer de naam van de RSA-server in en blader naar het sdconf.rec-bestand dat van de RSA-server is gedownload:



3. Selecteer het bestand en klik op **Indienen**.

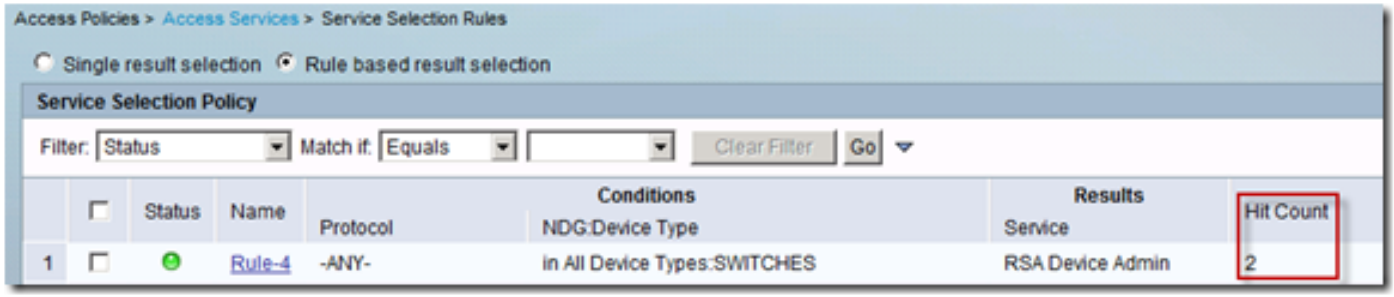
   Opmerking: De eerste keer dat ACS contact maakt met de token server, wordt er een ander bestand, het knooppunt-geheim bestand genoemd, voor de ACS-agent aangemaakt op de RSA-verificatiebeheer en wordt gedownload naar de ACS. Dit bestand wordt gebruikt voor versleutelde communicatie.

Verifiëren

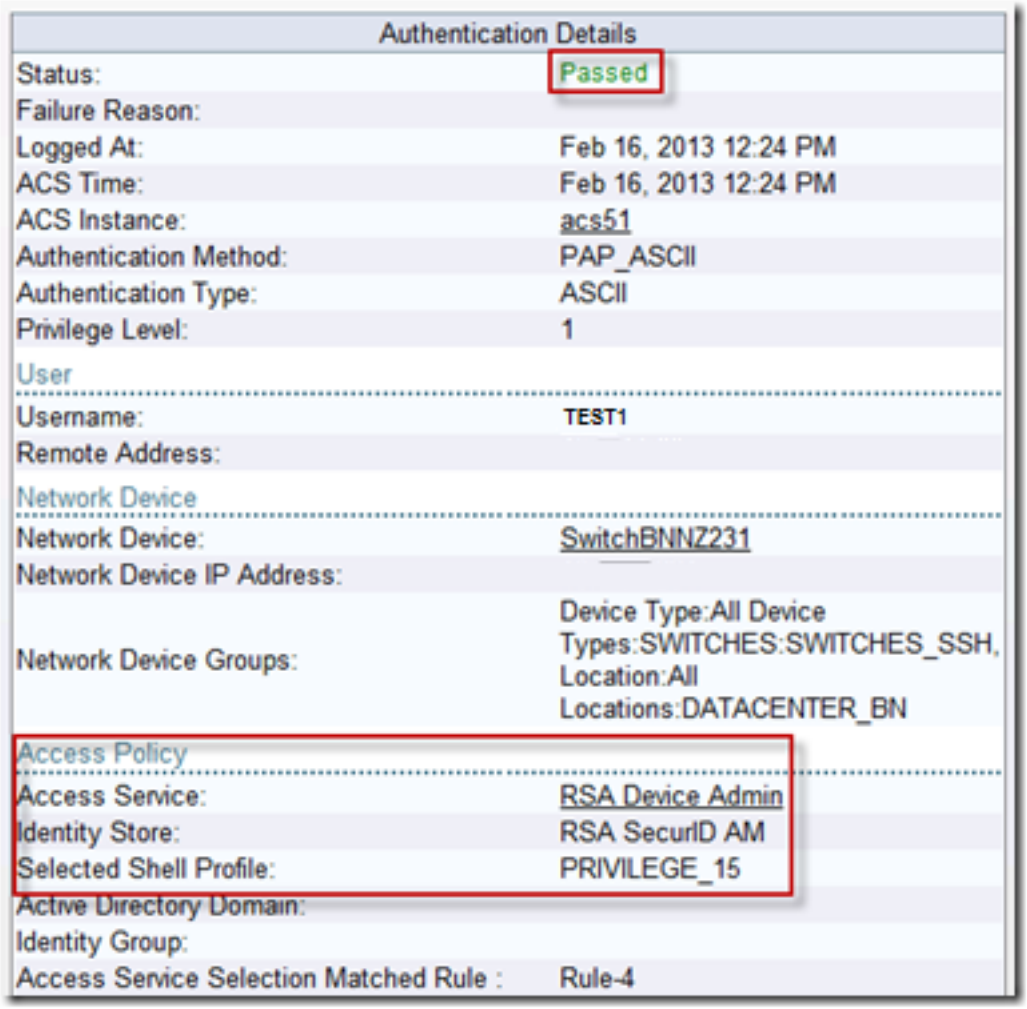
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

ACS versie 5.X-server

Ga naar de ACS-console om een succesvolle inlognaam te controleren en bekijk de Hit Count:



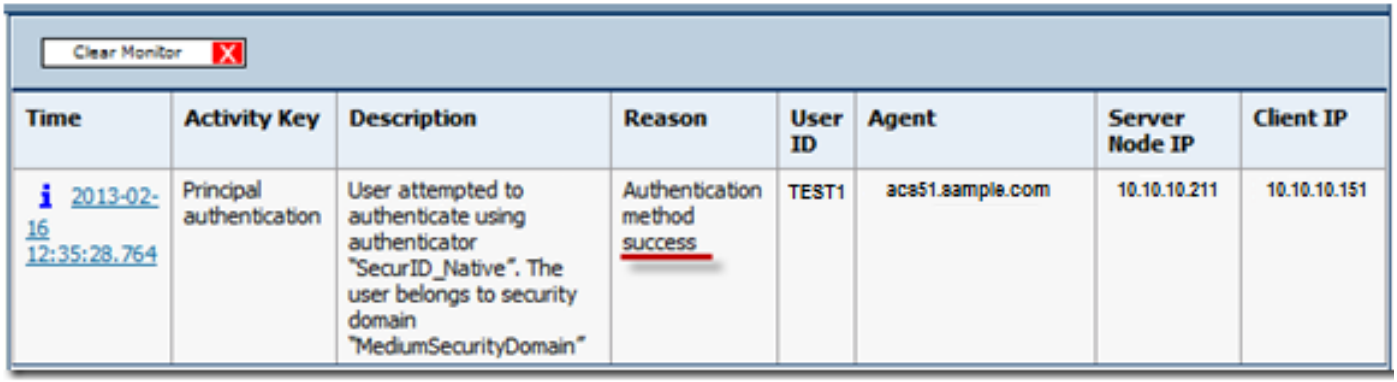
U kunt de verificatiedetails ook bekijken op de ACS-bestanden:



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

RSA-server

Ga naar de RSA-console om succesvolle authenticatie te controleren en bekijk de logbestanden:



Clear Monitor

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

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Een Agent Record maken (sdconf.rec)

Om een RSA SecureID-server in ACS versie 5.3 te configureren moet de ACS-beheerder het sdconf.rec-bestand hebben. Het sdconf.rec-bestand is een configuratierecord-bestand dat specificeert hoe de RSA-agent communiceert met het RSA SecureID-servergebied.

Om het sdconf.rec-bestand te maken, moet de RSA-beheerder de ACS-host als agent-host op de RSA SecureID-server toevoegen en een configuratiebestand voor deze agent-host genereren.

Het knooppunt opnieuw instellen (beveiligd)

Nadat de agent eerst met de RSA SecurID server communiceert, voorziet de server de agent van een knooppunt geheim bestand dat beveiligd wordt genoemd. De daaropvolgende communicatie tussen de server en de agent is afhankelijk van de uitwisseling van het knoopgeheim om de authenticiteit van de ander te controleren.

Soms moeten de beheerders het Nogegeheim wellicht opnieuw instellen:

1. De RSA-beheerder moet het van het Geheime van het Node Geheime van het Onderzoek van de Agent op het dossier van de Agent in de RSA SecurID server unchecken.
2. De ACS-beheerder moet het beveiligde bestand uit het ACS verwijderen.

Automatische taakverdeling negeren

De RSA SecurID agent plaatst de gevraagde ladingen automatisch op de RSA SecurID servers in het gebied. U hebt echter de optie om de lading handmatig in te stellen. U kunt de server specificeren die door elk van de agent hosts wordt gebruikt. U kunt een prioriteit aan elke server toewijzen zodat de agent host de verificatieverzoeken vaker naar bepaalde servers stuurt dan naar andere servers.

U moet de prioriteitsinstellingen in een tekstbestand specificeren, opslaan als sdopts.rec, en uploaden naar het ACS.

Handmatig ingrijpen om een RSA SecureID Server te verwijderen

Wanneer een RSA SecurID server omlaag is, werkt het automatische uitsluitingsmechanisme niet altijd snel. Verwijder het bestand sdstatus.12 uit het ACS om dit proces te versnellen.