Integração de Cisco ACS 5.X com o servidor de tokens do SecurID RSA

Índice

Introdução
Informações de Apoio
Pré-requisitos
Requisitos
Componentes Utilizados
Configurações
Server RSA
Server da versão de ACS 5.X
Verificar
Server da versão de ACS 5.X
Server RSA
Troubleshooting
Crie um registro do agente (sdconf.rec)
Restaure o segredo de nó (o SecurID)
Cancele o Balanceamento de carga automático
Intervenha manualmente para remover um server do SecurID da pena RSA

Introdução

Este documento descreve como integrar uma versão 5.x do sistema de controle de acesso (ACS) de Cisco com tecnologia da autenticação securid RSA.

Informações de Apoio

O Cisco Secure ACS apoia o server do SecurID RSA como um base de dados externo.

A autenticação de dois fatores do SecurID RSA consiste no número de identificação pessoal do usuário (PIN) e em um token individualmente registrado do SecurID RSA que gerencia os códigos de token do único-uso baseados em um algoritmo do código do tempo.

Um código de token diferente é gerado em intervalos fixos, geralmente cada 30 ou 60 segundos. O server do SecurID RSA valida este código dinâmico da autenticação. Cada token do SecurID RSA é original, e não é possível prever o valor futuro de tokens passados sobre baseados um token.

Assim, quando um código de token correto estiver fornecido junto com um PIN, há um grau

elevado de certeza que a pessoa seja um usuário válido. Consequentemente, os server do SecurID RSA fornecem um mecanismo da autenticação mais seguro do que senhas reutilizável convencionais.

Você pode integrar Cisco ACS 5.x com tecnologia da autenticação securid RSA nestas maneiras:

- Agente do SecurID RSA - Os usuários são autenticados com username e senha com o protocolo nativo RSA.
- Protocolo de raio - Os usuários são autenticados com username e senha com o protocolo de raio.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Segurança de RSA
- Cisco Secure Access Control System (ACS)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 5.x do Cisco Secure Access Control System (ACS)
- Servidor de tokens do SecurID RSA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

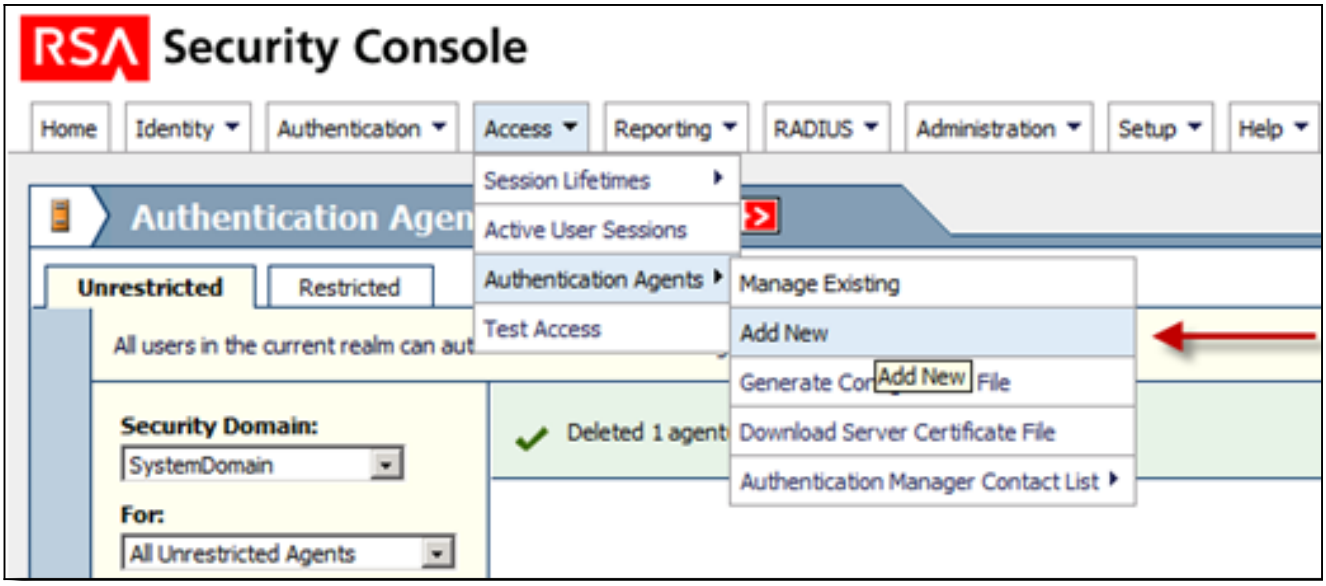
Configurações

Server RSA

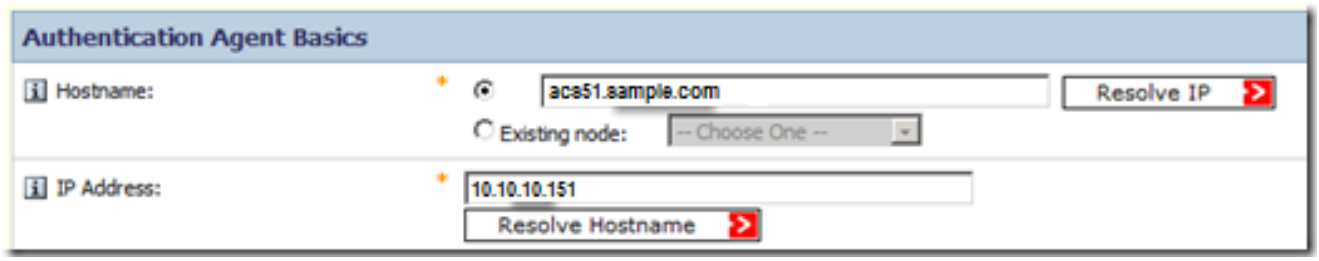
Este procedimento descreve como o administrador do servidor do SecurID RSA cria Agentes de Autenticação e um arquivo de configuração. Um Agente de Autenticação é basicamente um nome do Domain Name Server (DNS) e um endereço IP de Um ou Mais Servidores Cisco ICM NT de um dispositivo, de um software, ou de um serviço que tenha direitos de alcançar o base de dados RSA. O arquivo de configuração descreve basicamente a topologia e a comunicação RSA.

Neste exemplo, o administrador RSA deve criar dois agentes para os dois exemplos ACS.

1. No console da Segurança de RSA, navegue **para alcançar** > > Add dos **Agentes de Autenticação novo**:

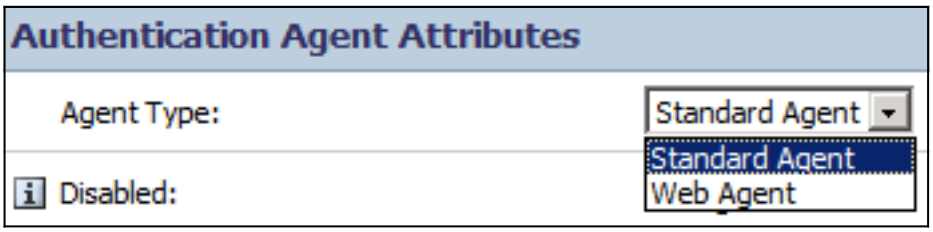


2. No indicador novo do Agente de Autenticação adicionar, defina um hostname e um endereço IP de Um ou Mais Servidores Cisco ICM NT para cada um dos dois agentes:

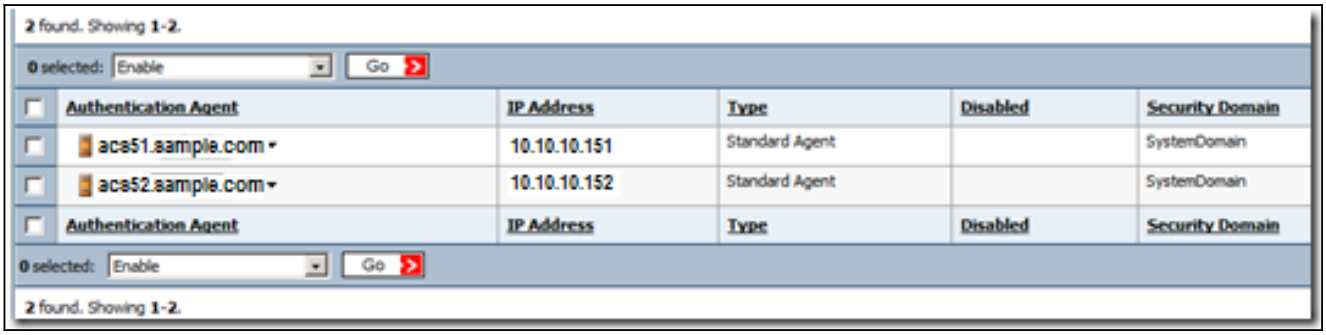


o DNS dianteiro e as consultas reversas para agentes ACS devem trabalhar.

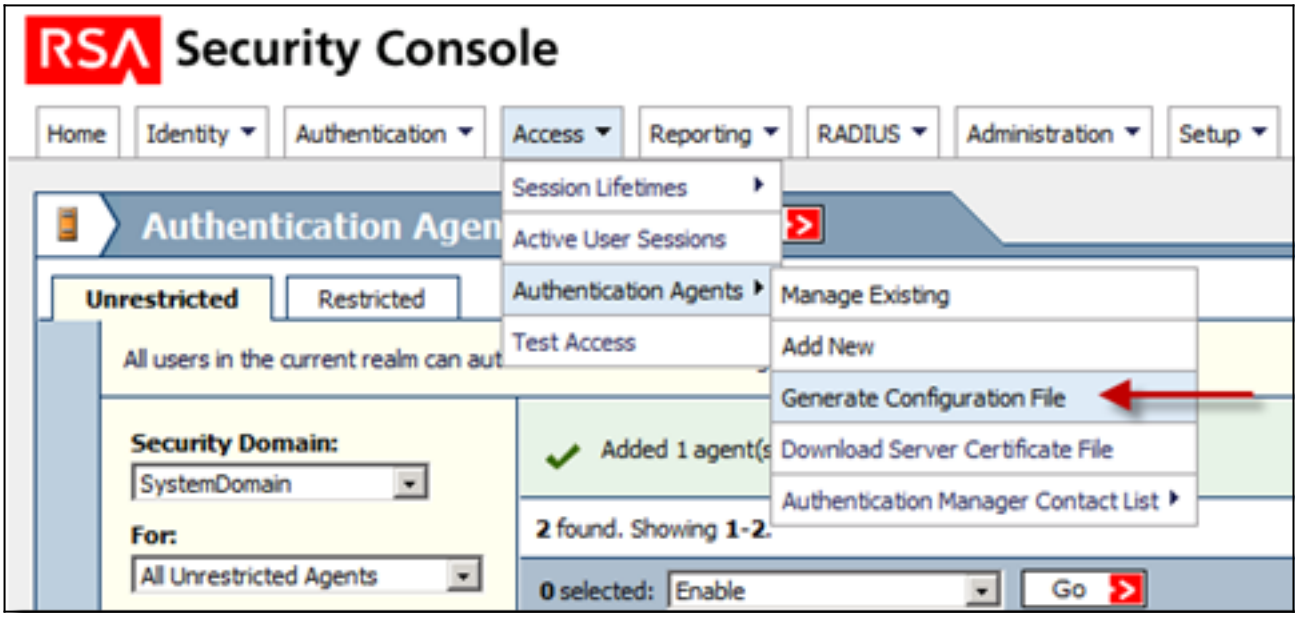
3. Defina o tipo do agente como o agente padrão:



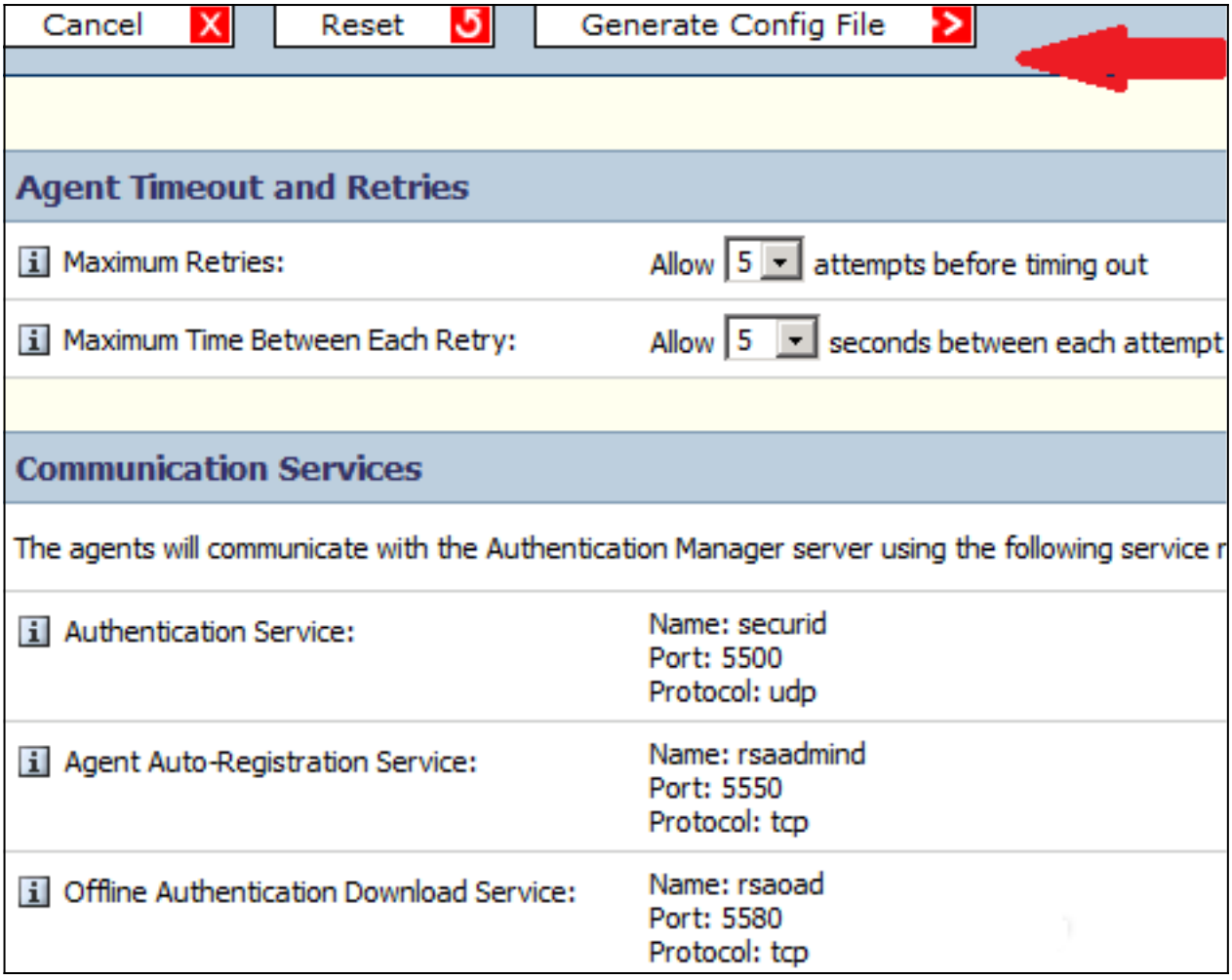
Este é um exemplo da informação que você vê uma vez que os agentes são adicionados:



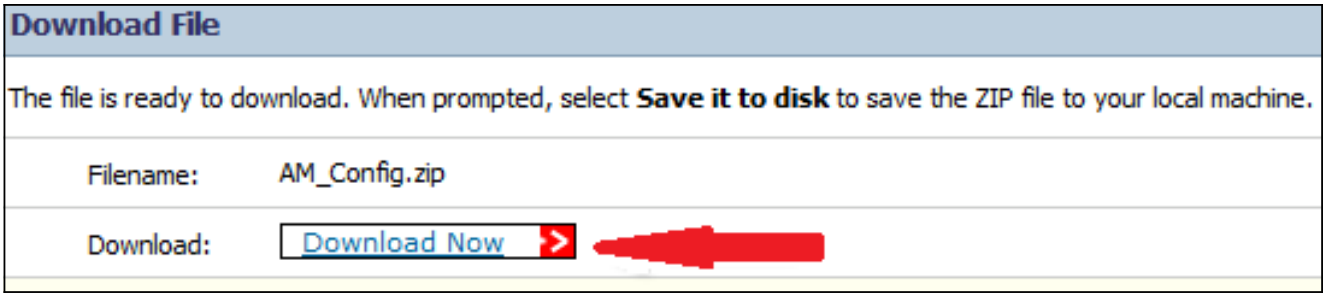
4. No console da Segurança de RSA, navegue **para alcançar > Agentes de Autenticação > gerenciem o arquivo de configuração** a fim gerar o arquivo de configuração sdconf.rec:



5. Use os valores padrão para novas tentativas máxima e o tempo máximo entre cada nova tentativa:



6. Transfira o arquivo de configuração:

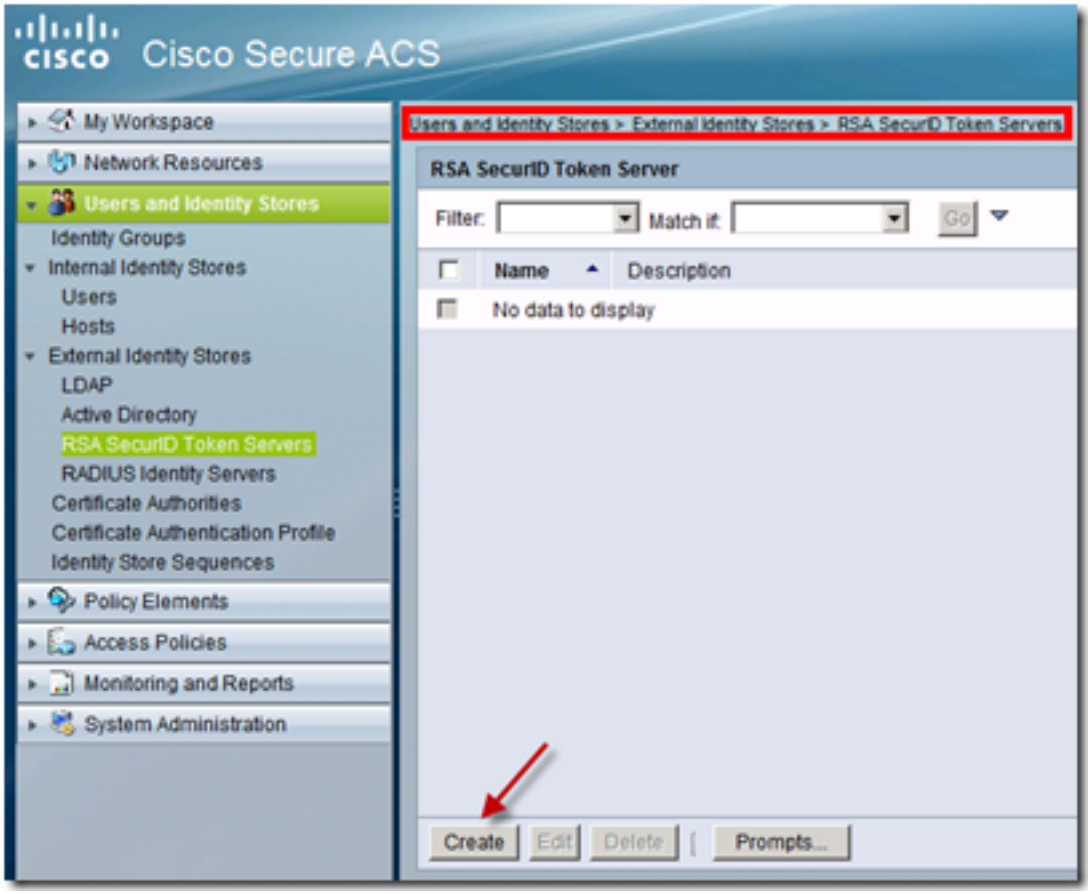


O arquivo do .zip contém o arquivo da configuração real sdconf.rec, que o administrador ACS precisa a fim terminar tarefas de configuração.

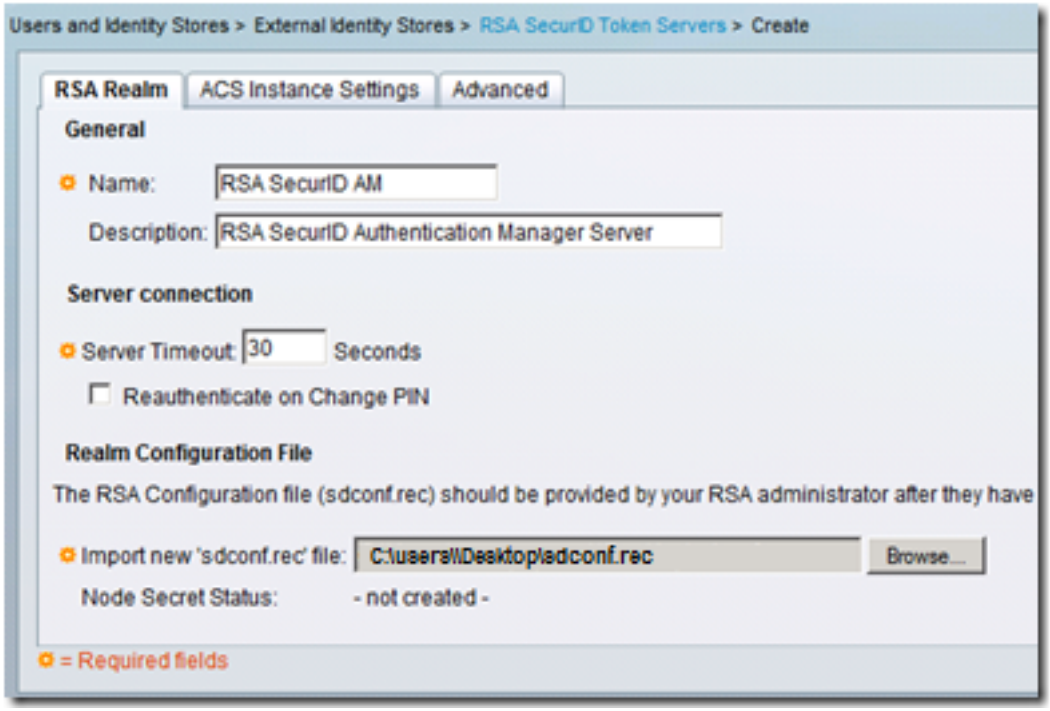
Server da versão de ACS 5.X

Este procedimento descreve como o administrador ACS recupera e submete o arquivo de configuração.

1. No console da versão 5.x do Cisco Secure ACS, navegue aos **usuários e a identidade armazena > identidade externo armazena > servidores de tokens do SecurID RSA**, e o clique **cria**:



2. Dê entrada com o nome do server RSA, e consulte ao arquivo sdconf.rec que foi transferido do server RSA:



3. Selecione o arquivo, e o clique **submete-se**.

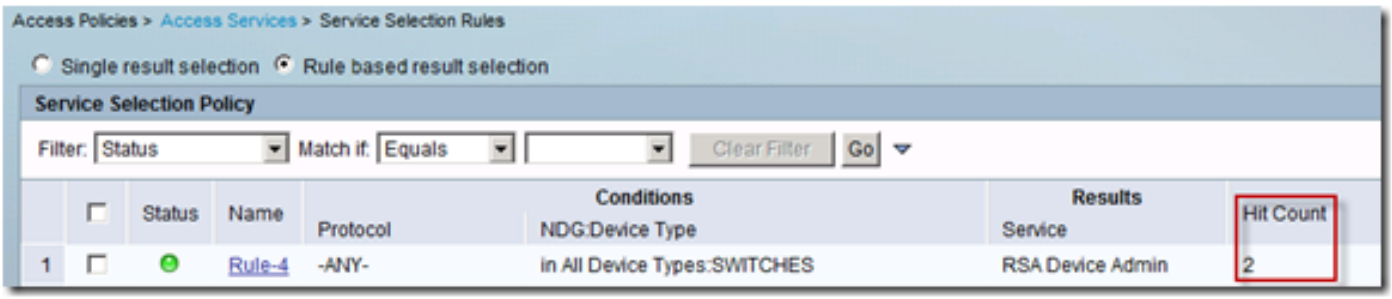
   Nota: A primeira vez que o ACS contacta o servidor de tokens, outro arquivo, chamado o arquivo do segredo de nó, está criado para o agente ACS no gerente da autenticação de RSA e transferido ao ACS. Este arquivo é usado para uma comunicação codificada.

Verificar

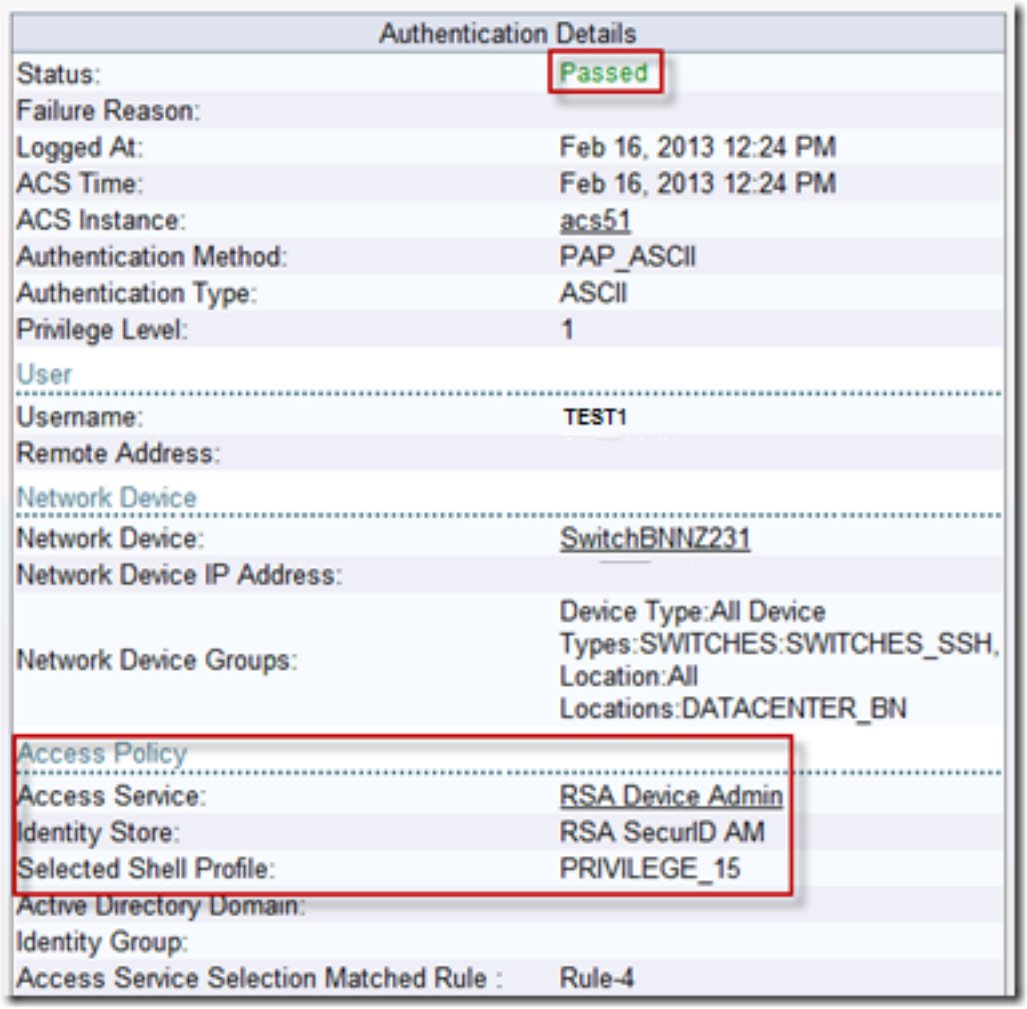
Use esta seção para confirmar se a sua configuração funciona corretamente.

Server da versão de ACS 5.X

A fim verificar um login bem-sucedido, vá ao console ACS, e reveja a contagem da batida:



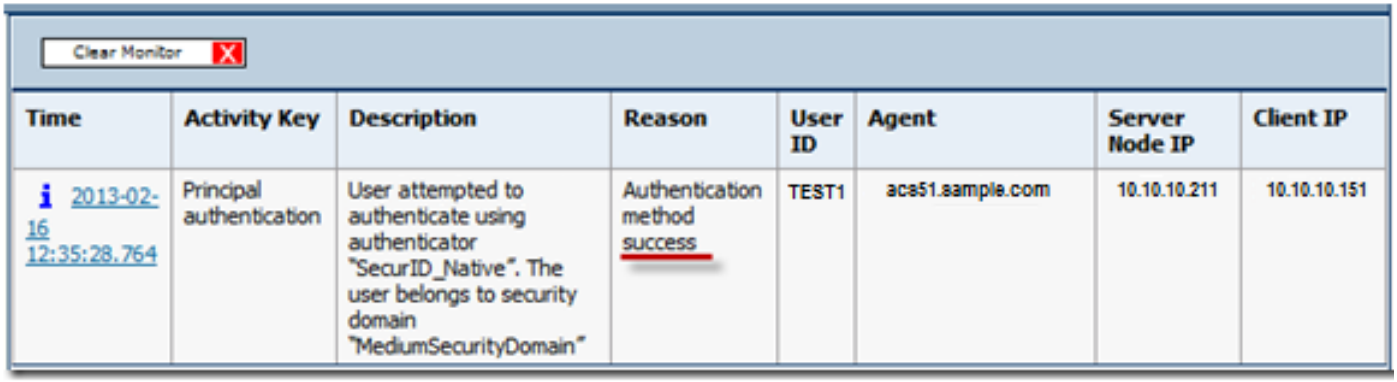
Você pode igualmente rever os detalhes da autenticação dos logs ACS:



Authentication Details	
Status:	Passed
Failure Reason:	
Logged At:	Feb 16, 2013 12:24 PM
ACS Time:	Feb 16, 2013 12:24 PM
ACS Instance:	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

Server RSA

A fim verificar a autenticação bem sucedida, vá ao console RSA, e reveja os logs:



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

Troubleshooting

Esta seção fornece informações que você pode usar na solução de problemas de sua configuração.

Crie um registro do agente (sdconf.rec)

A fim configurar um servidor de tokens do SecurID RSA na versão de ACS 5.3, o administrador ACS deve ter o arquivo sdconf.rec. O arquivo sdconf.rec é um arquivo de registro de configuração que especifique como o agente RSA se comunica com o reino do server do SecurID RSA.

A fim criar o arquivo sdconf.rec, o administrador RSA deve adicionar o host ACS como um host do agente no server do SecurID RSA e gerar um arquivo de configuração para este host do agente.

Restaure o segredo de nó (o SecurID)

Depois que o agente se comunica inicialmente com o server do SecurID RSA, o server fornece o agente um arquivo do segredo de nó chamado SecurID. Uma comunicação subsequente entre o server e o agente confia na troca do segredo de nó a fim verificar o outro autenticidade.

Às vezes, os administradores puderam ter que restaurar o segredo de nó:

1. O administrador RSA deve desmarcar a caixa de verificação criada segredo de nó no registro do host do agente no server do SecurID RSA.
2. O administrador ACS deve remover o arquivo SECURID do ACS.

Balanceamento de carga automático da ultrapassagem

O agente do SecurID RSA equilibra automaticamente as cargas pedidas nos server do SecurID RSA no reino. Contudo, você tem a opção para equilibrar manualmente a carga. Você pode especificar o server usado por cada um dos host do agente. Você pode atribuir uma prioridade a cada server de modo que o host do agente dirija pedidos de autenticação a alguns server mais frequentemente do que outro.

Você deve especificar as configurações de prioridade em um arquivo de texto, salvar as como sdopts.rec, e transferi-las arquivos pela rede ao ACS.

Intervenha manualmente para remover um server do SecurID da pena RSA

Quando um server do SecurID RSA está para baixo, o mecanismo automático da exclusão não trabalha sempre rapidamente. Remova o arquivo sdstatus.12 do ACS a fim acelerar este processo.