Integración de Cisco ACS 5.X con el servidor Token del SecurID RSA

Contenido

Introducción

Este documento describe cómo integrar una versión 5.x del Sistema de control de acceso de Cisco (ACS) con la tecnología de la autenticación de SecurID RSA.

Antecedentes

El Cisco Secure ACS soporta el servidor del SecurID RSA como base de datos externa.

La autenticación bifactorial del SecurID RSA consiste en el número de identificación personal del usuario (PIN) y un token individualmente registrado del SecurID RSA que genere los códigos de Token no reutilizables basados en un algoritmo del código del tiempo.

Un diverso código de Token se genera en los intervalos fijos, generalmente cada 30 o 60 segundos. El servidor del SecurID RSA valida este código dinámico de la autenticación. Cada token del SecurID RSA es único, y no es posible predecir el valor futuro encendido de los últimos tokens basados un token.

Así, cuando un código de Token correcto se suministra así como un PIN, hay un nivel alto de

certeza que la persona es usuario válido. Por lo tanto, los servidores del SecurID RSA proporcionan un mecanismo de autenticación más confiable que las contraseñas reutilizables convencionales.

Usted puede integrar Cisco ACS 5.x con la tecnología de la autenticación de SecurID RSA de estas maneras:

- Autentican a los usuarios agentes del SecurID RSA con el nombre de usuario y la contraseña con el protocolo nativo RSA.
- Protocolo RADIUS - Autentican a los usuarios con el nombre de usuario y la contraseña con el protocolo RADIUS.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 5.x del Cisco Secure Access Control System (ACS)
- Servidor Token del SecurID RSA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configuraciones

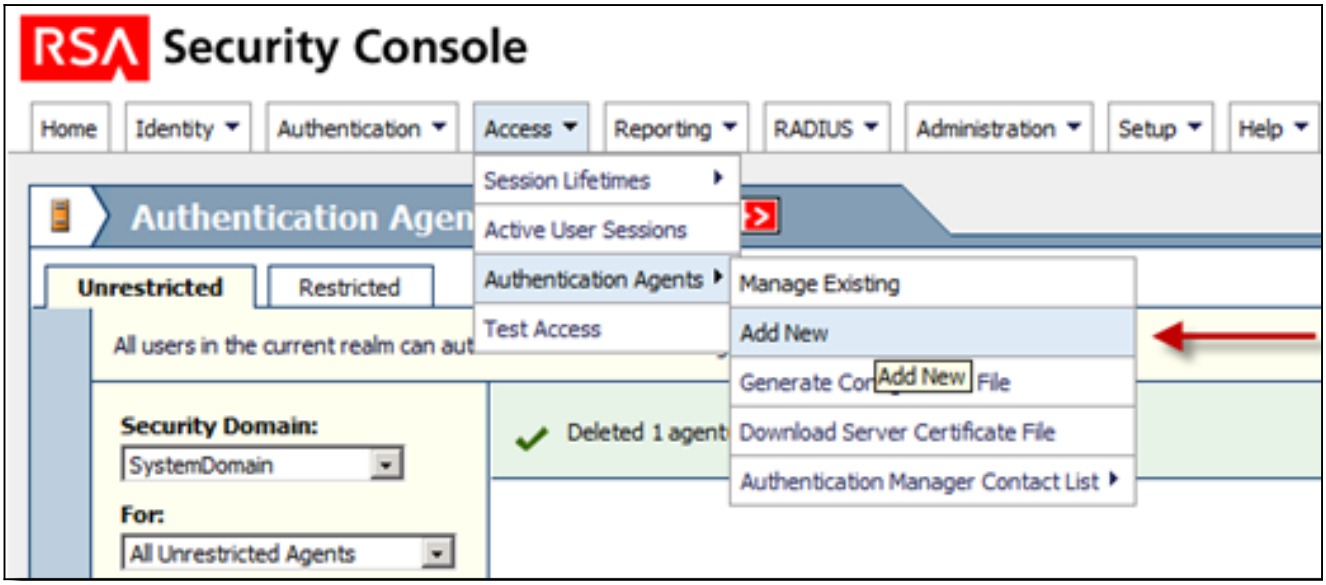
Servidor RSA

Este procedimiento describe cómo el Administrador del servidor del SecurID RSA crea los agentes de autenticación y un archivo de configuración. Un agente de autenticación es básicamente un nombre del Domain Name Server (DNS) y una dirección IP de un dispositivo, de un software, o de un servicio que tenga derechos de acceder la base de datos RSA. El archivo de configuración describe básicamente la topología y la comunicación RSA.

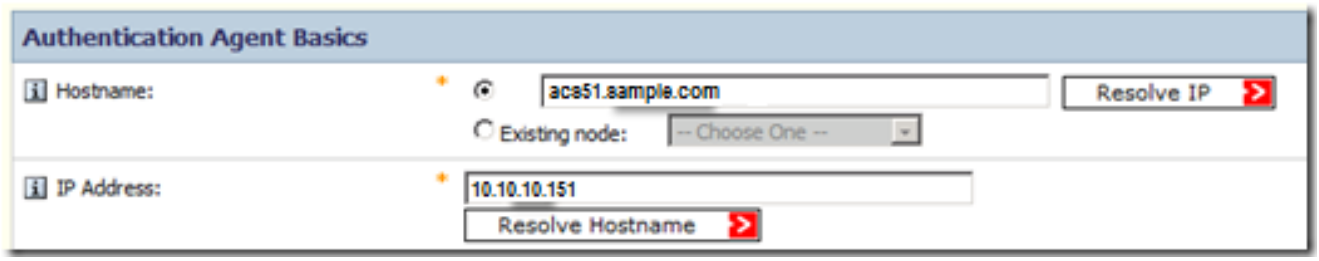
En este ejemplo, el administrador RSA debe crear dos agentes para los dos casos ACS.

1. En la consola de la Seguridad RSA, navegue **para acceder >** los **agentes de autenticación >**

Add **nuevos**:

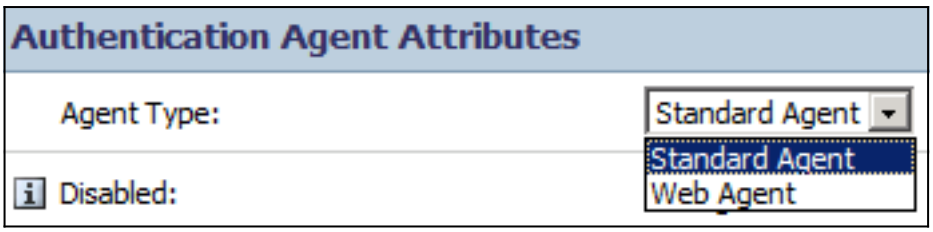


2. En la nueva ventana del agente de autenticación del agregar, defina un nombre de host y una dirección IP para cada uno de los dos agentes:

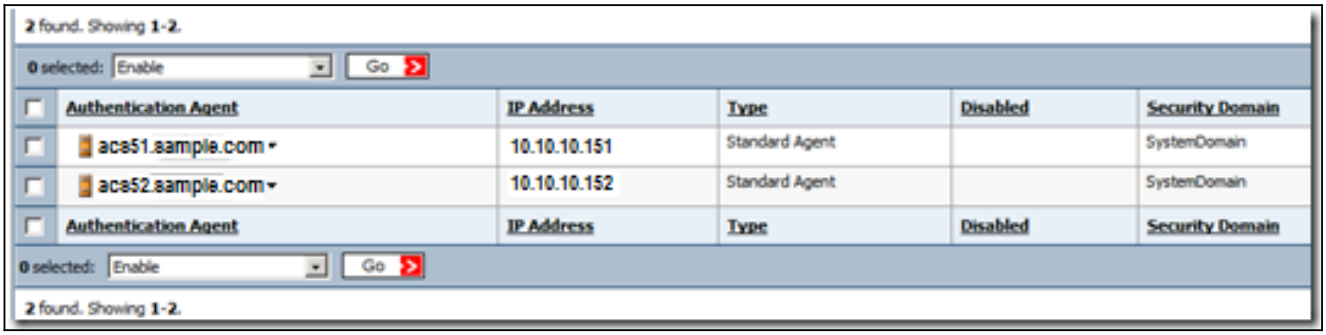


El DNS delantero y las búsquedas inversas para los agentes ACS deben trabajar.

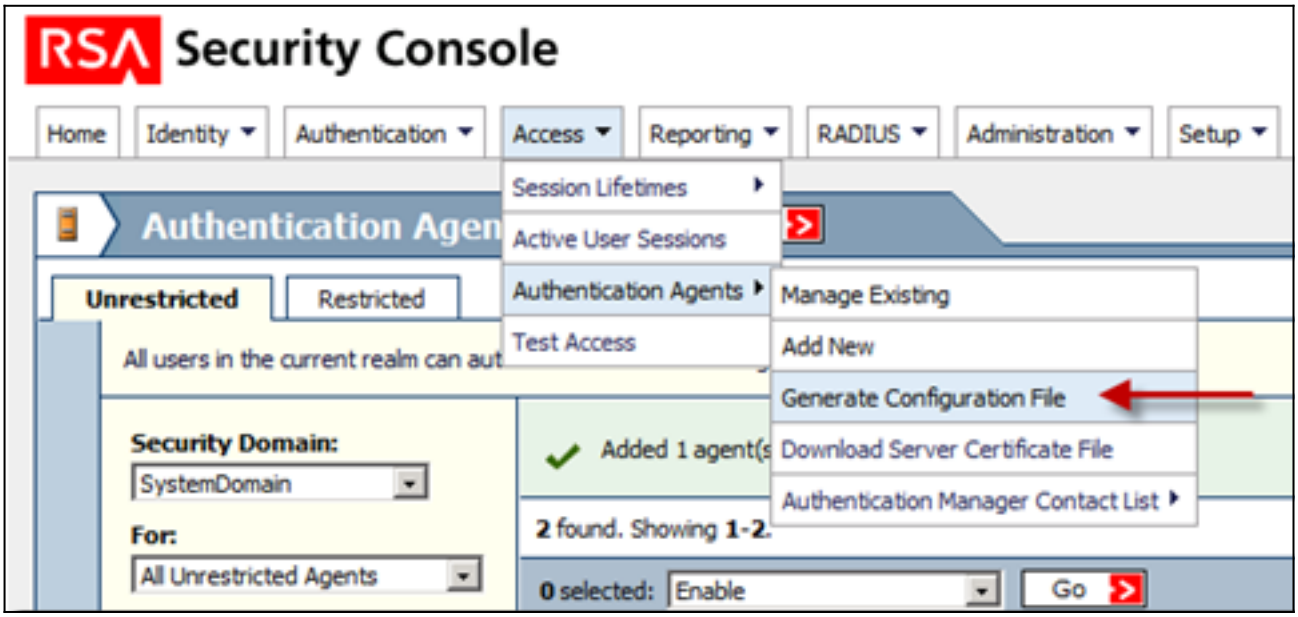
3. Defina el tipo del agente como agente estándar:



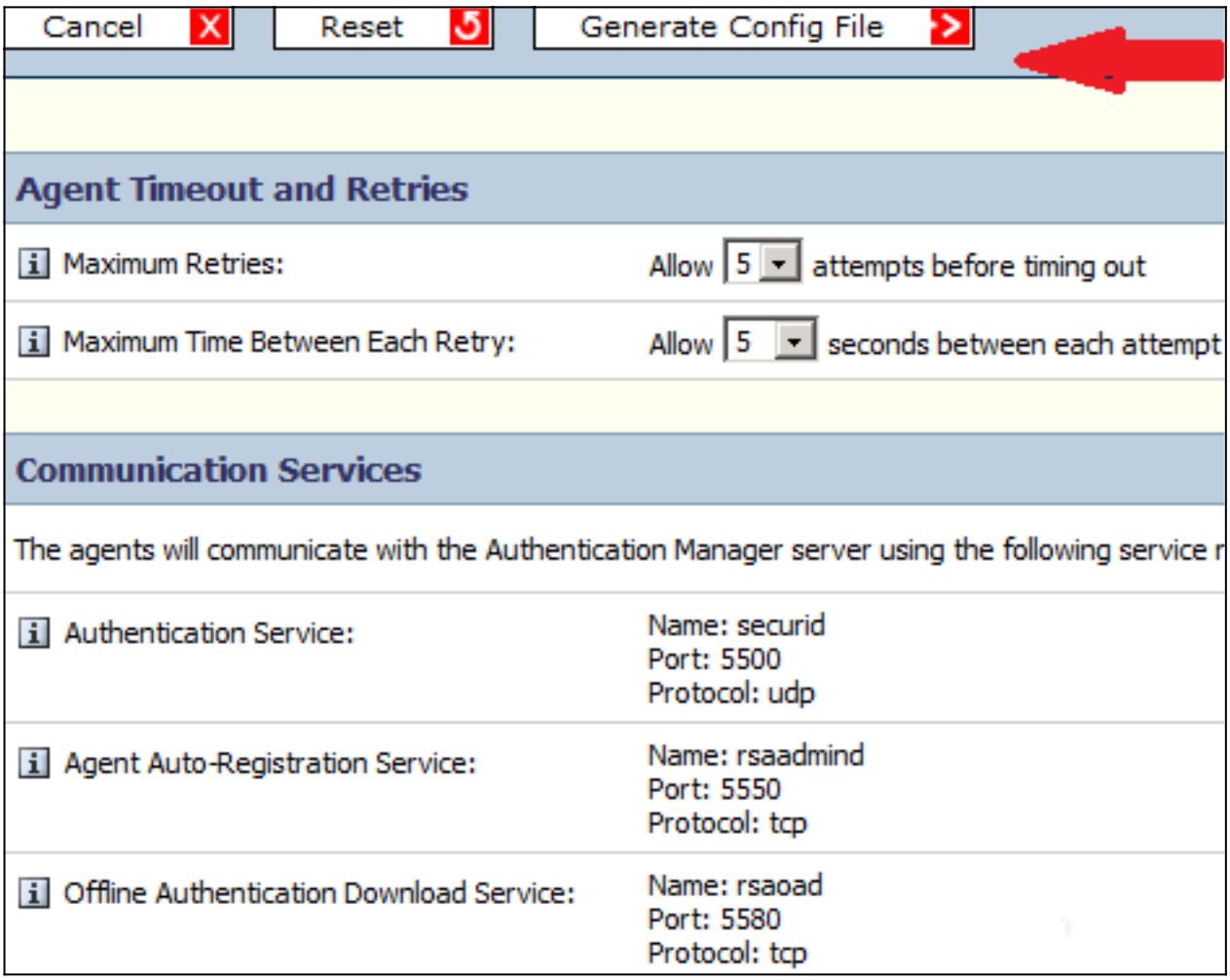
Éste es un ejemplo de la información que usted ve una vez que se agregan los agentes:



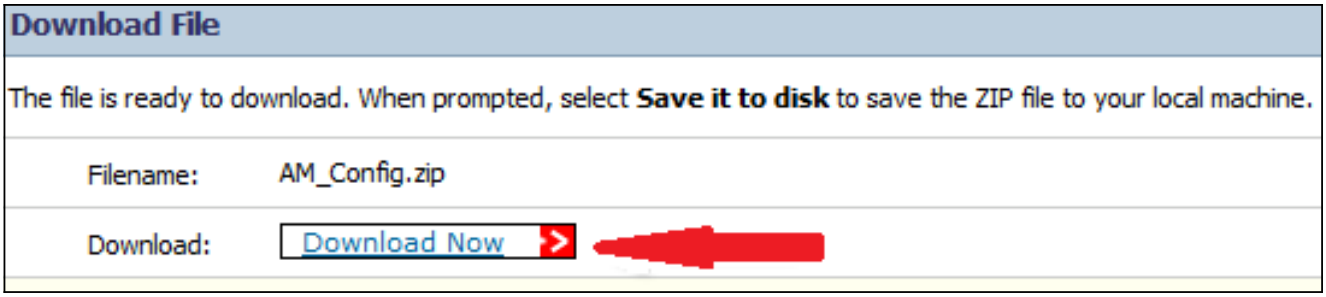
4. En la consola de la Seguridad RSA, navegue **para acceder** > los **agentes de autenticación** > **generan el archivo de configuración** para generar el archivo de configuración sdconf.rec:



5. Utilice los valores predeterminados para las cantidades de intentos máximas y el tiempo máximo entre cada recomprobación:



6. Descargue el archivo de configuración:

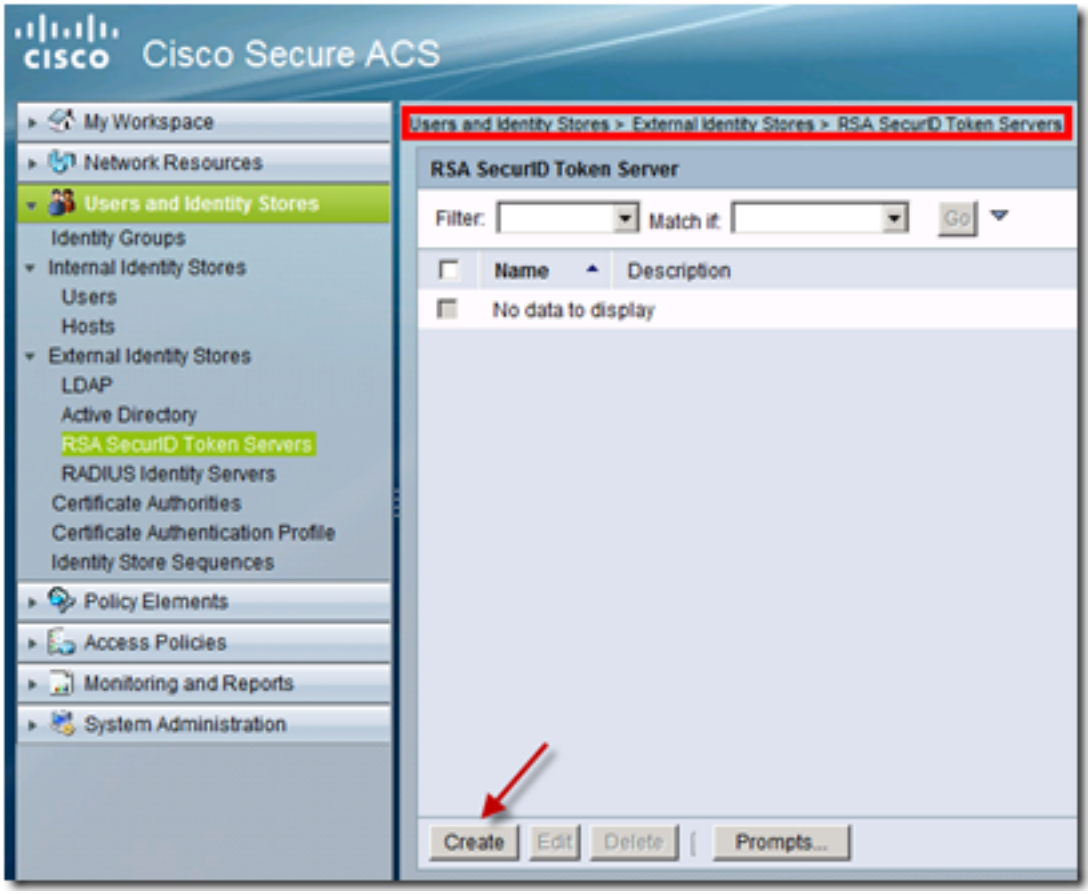


El archivo del .zip contiene el archivo de la configuración real sdconf.rec, que el administrador ACS necesita para completar las tareas de configuración.

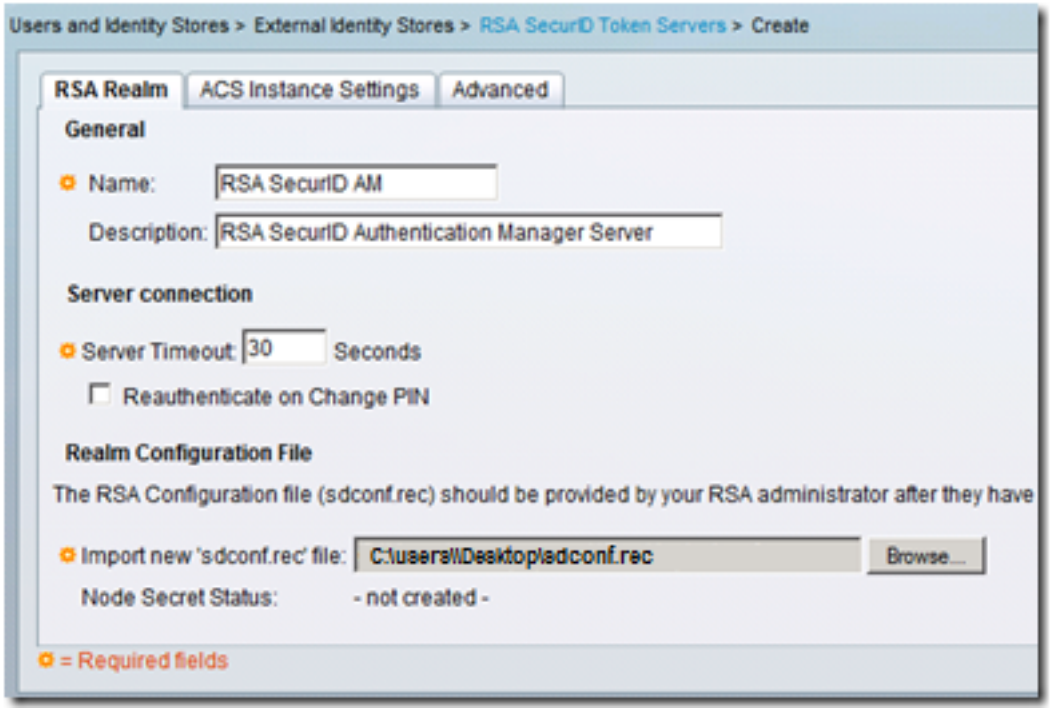
Servidor del ACS versión 5.X

Este procedimiento describe cómo el administrador ACS extrae y presenta el archivo de configuración.

1. En la consola de la versión 5.x del Cisco Secure ACS, navegue a los **usuarios y la identidad salva > identidad externa salva >** los **servidores Token del SecurID RSA**, y el tecleo **crea**:



2. Ingrese el nombre del servidor RSA, y hojee al archivo sdconf.rec que fue descargado del servidor RSA:



3. Seleccione el archivo, y el tecleo **somete**.

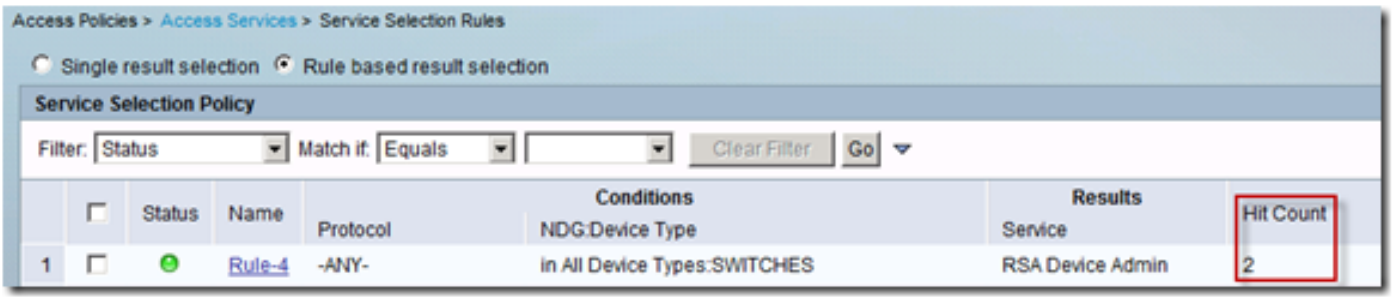
   Nota: La primera vez que el ACS entra en contacto al servidor Token, otro archivo, llamado el archivo node secret, se crea para el agente ACS en el administrador de la Autenticación RSA y se descarga al ACS. Este archivo se utiliza para la comunicación encriptada.

Verificación

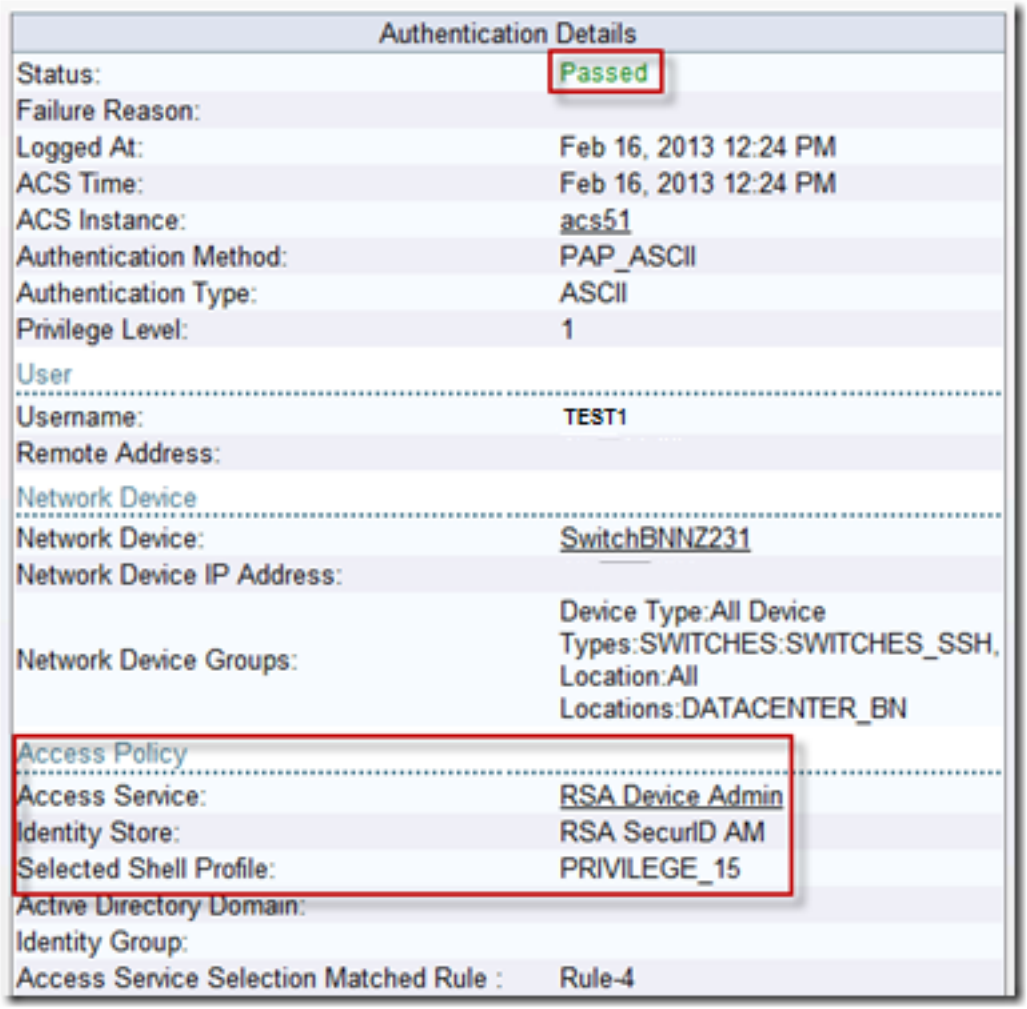
Utilize esta sección para confirmar que su configuración funcione correctamente.

Servidor del ACS versión 5.X

Para verificar una registración satisfactoria, vaya a la consola ACS, y revise la cuenta del golpe:



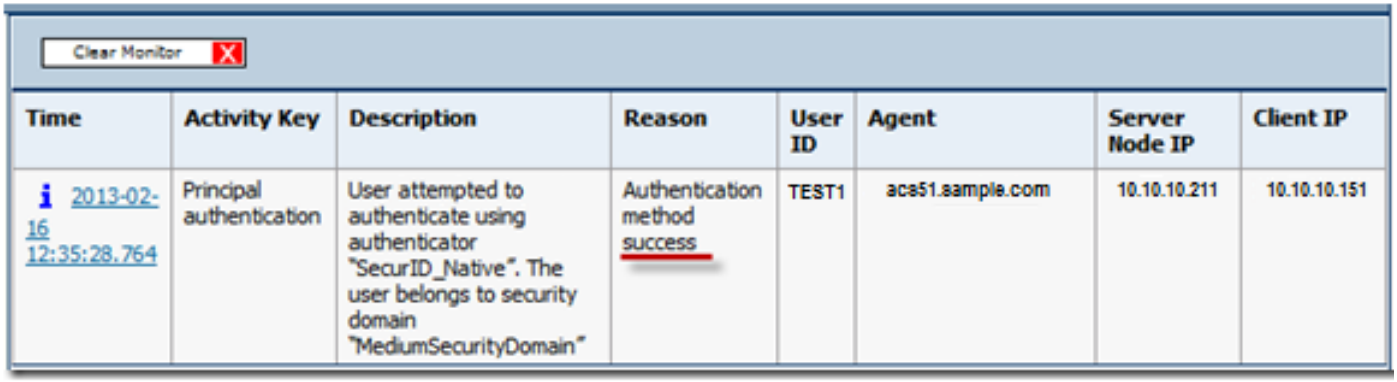
Usted puede también revisar los detalles de la autenticación de los registros ACS:



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

Servidor RSA

Para verificar la autenticación satisfactoria, vaya a la consola RSA, y revise los registros:



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 sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Cree un expediente del agente (sdconf.rec)

Para configurar a un servidor Token del SecurID RSA en el ACS versión 5.3, el administrador ACS debe tener el archivo sdconf.rec. El archivo sdconf.rec es un archivo de registro de configuración que especifica cómo el agente RSA comunica con el reino del servidor del SecurID RSA.

Para crear el archivo sdconf.rec, el administrador RSA debe agregar el host ACS como host agente en el servidor del SecurID RSA y generar un archivo de configuración para este host agente.

Reajuste el secreto de nodo (el securid)

Después de que el agente comunique inicialmente con el servidor del SecurID RSA, el servidor proporciona el agente con un archivo node secret llamado securid. La comunicación subsiguiente entre el servidor y el agente confía en el intercambio del secreto de nodo para verificar el otro autenticidad.

A veces, los administradores pudieron tener que reajustar el secreto de nodo:

1. El administrador RSA debe desmarcar la casilla de verificación creada secreto de nodo en el expediente del host agente en el servidor del SecurID RSA.
2. El administrador ACS debe quitar el archivo SECURID del ACS.

Equilibrio de carga automático de la invalidación

El agente del SecurID RSA equilibra automáticamente las cargas pedidas en los servidores del SecurID RSA en el reino. Sin embargo, usted tiene la opción para equilibrar manualmente la carga. Usted puede especificar el servidor usado por cada uno de los host agente. Usted puede asignar una prioridad a cada servidor de modo que el host agente dirija los pedidos de autenticación a algunos servidores más con frecuencia que otros.

Usted debe especificar las Configuraciones de prioridad en un archivo de texto, salvarlas como sdopts.rec, y cargarlas al ACS.

Intervenga manualmente para quitar un servidor del SecurID del plumón RSA

Cuando un servidor del SecurID RSA está abajo, el mecanismo automático de la exclusión no trabaja siempre rápidamente. Quite el archivo sdstatus.12 del ACS para acelerar este proceso.