ACS 5.x y posterior: Integración con el ejemplo de configuración del Microsoft Active Directory

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Antecedentes](#)
[Configuración](#)
[Motor del despliegue de la aplicación de la configuración ACS 5.x (ADE-OS)](#)
[Únase a ACS 5.x al AD](#)
[Configure el servicio del acceso](#)
[Verificación](#)
[Información Relacionada](#)

Introducción

Este documento proporciona una configuración de ejemplo para integrar Microsoft Active Directory con Cisco Secure Access Control System (ACS) 5.x y posteriores. ACS utiliza Microsoft Active Directory (AD) como almacén de identidades externo para guardar recursos como usuarios, equipos, grupos y atributos. ACS autentica estos recursos respecto a AD.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Dominio de Active Directory de Windows a ser necesidades usadas de ser de configuración completa y operativo.
- Utilice el dominio 2003 del Microsoft Windows server, el dominio 2008 del Microsoft Windows server o el dominio 2008 del r2 del Microsoft Windows server como éstos son soportados por ACS 5.x.**Nota:** La integración del dominio 2008 del r2 del Microsoft Windows server con el ACS se soporta de ACS 5.2 y posterior.

Componentes Utilizados

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

hardware.

- Cisco Secure ACS 5.3
- Dominio 2003 del Microsoft Windows server

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El Active Directory de Windows proporciona muchas características que se utilicen en el USO de la red diario. La integración de ACS 5.x con el AD permite el uso de los usuarios existentes AD, de las máquinas y de su asignación del grupo.

El ACS 5.x integrado con el AD proporciona estas características:

1. Autenticación de la máquina
2. Extracción del atributo para la autorización
3. Recuperación de certificados para autenticación EAP-TLS
4. Restricción del usuario y de la cuenta de equipo
5. Restricciones de acceso de la máquina
6. Control de los permisos de dial in
7. Opciones de devolución de llamada para los usuarios de dial in
8. Atributos del soporte del dial-in

Configuración

Motor del despliegue de la aplicación de la configuración ACS 5.x (ADE-OS)

Antes de que usted integre ACS 5.x al AD, asegúrese de que el **timezone, la fecha y la hora** en el ACS haga juego con ése en el Primary Domain Controller AD. También, defina al servidor DNS en el ACS para poder resolver el Domain Name del ACS 5.x. Complete estos pasos para configurar el motor del despliegue de la aplicación ACS 5.x (ADE-OS):

1. El SSH al dispositivo ACS y ingresa las credenciales CLI.
2. Publique el **comando clock timezone** en el modo de configuración tal y como se muestra en de la orden de configurar el **TIMEZONE** en el ACS para hacer juego con eso en el controlador de dominio.
   `clock timezone Asia/Kolkata` **Nota:** Asia/Kolkata es el timezone usado en este documento. Usted puede encontrar su timezone específico por el comando de los **timezones de la demostración del** modo EXEC.
3. En caso de que su controlador de dominio AD se sincronice con un servidor NTP que resida

en su red, se recomienda altamente para utilizar al mismo servidor NTP en el ACS. Si usted no tiene el servidor NTP, después salte al **paso 4.** Éstos son los pasos para configurar al servidor NTP:El servidor NTP puede ser configurado con el **servidor NTP < el IP Address del** comando del **server> NTP** en el modo de configuración como se muestra.`ntp server 192.168.26.55`
`The NTP server was modified.`
`If this action resulted in a clock modification, you must restart ACS.`Refiera a [ACS 5.x: Sincronización de Cisco ACS con el ejemplo de configuración del servidor NTP] para más información sobre la configuración del NTP.

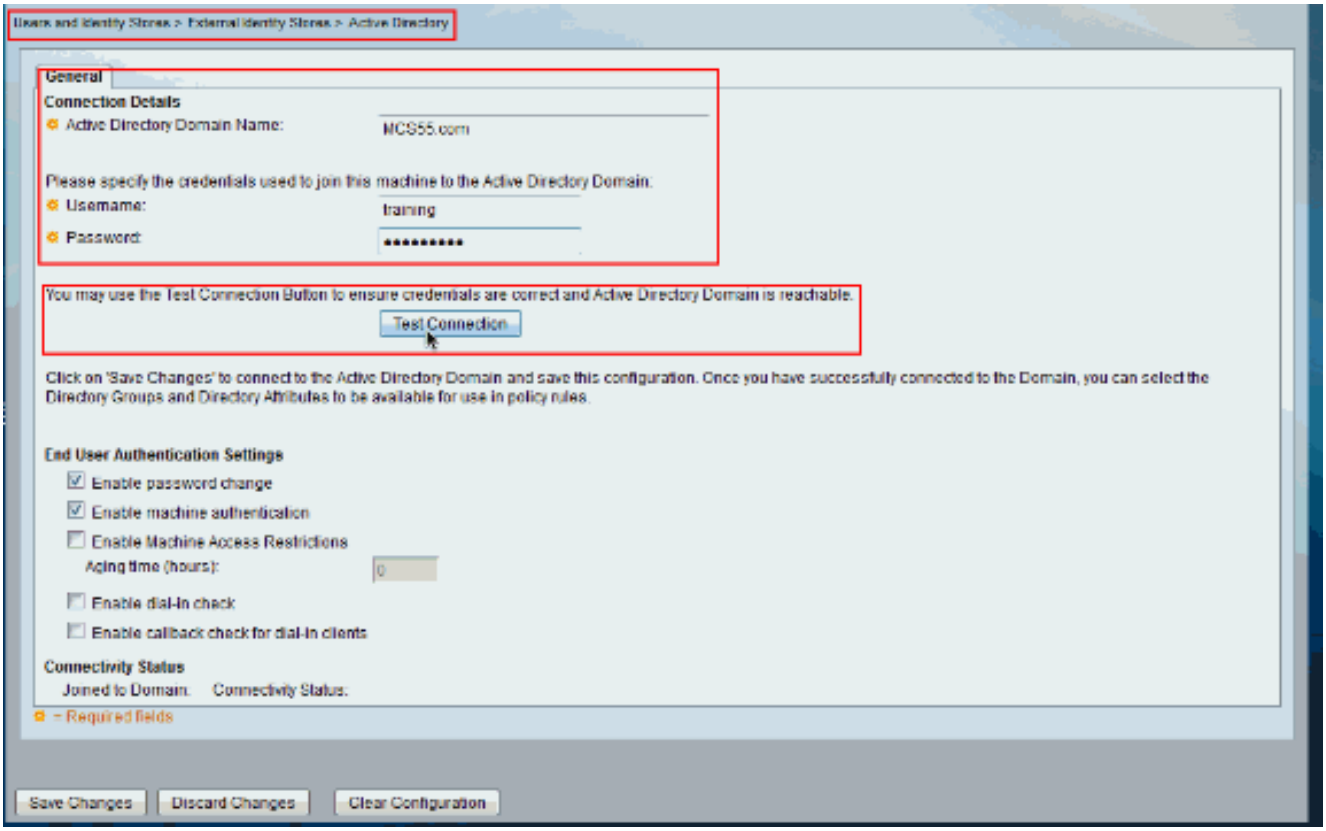
4. Para configurar la fecha y hora utilice manualmente el **comando clock set** en el **modo EXEC**. Un ejemplo se muestra aquí:
```
clock set Jun 8 10:36:00 2012
Clock was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS.
Stopping Management and View.....................
Stopping Runtime......
Stopping Database....
Cleanup.....
Starting ACS ....

To verify that ACS processes are running, use the
'show application status acs' command.
```
5. Ahora verifique el **timezone, fecha y hora** con el **comando show clock**. La salida del comando show clock se muestra aquí:`acs51/admin# **show clock** Fri Jun 8 10:36:05 IST 2012`
6. Configure el DNS en el ACS con el **Servidor de nombres del <ip < el IP Address del** comando **DNS>** en el **modo de configuración** como se muestra aquí:`ip name-server 192.168.26.55`**Nota:** La dirección IP DNS es proporcionada por su administrador del Dominio de Windows.
7. Publique el comando del **< Domain Name > del nslookup** para verificar el accesibilidad del Domain Name como se muestra.`acs51/admin#**nslookup MCS55.com** Trying "MCS55.com" ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60485 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1 ;; QUESTION SECTION: ;MCS55.com. IN ANY ;; ANSWER SECTION: MCS55.com. 600 IN A 192.168.26.55 MCS55.com. 3600 IN NS admin-zq2ttn9ux.MCS55.com. MCS55.com. 3600 IN SOA admin-zq2ttn9ux.MCS55.com. hostmaster.MCS55.com. 635 900 600 86400 3600 ;; ADDITIONAL SECTION: admin-zq2ttn9ux.MCS55.com. 3600 IN A 192.168.26.55 Received 136 bytes from 192.168.26.55#53 in 0 ms` **Nota:** Si la **SECCIÓN de la RESPUESTA** está vacía, después entre en contacto a su administrador del Dominio de Windows para descubrir al servidor DNS correcto para el dominio.
8. Publique el comando del **< Domain Name > del Domain Name del IP** para configurar el **DOMAIN NAME** en el ACS como se muestra aquí:`ip domain-name MCS55.com`
9. Publique el comando del **<hostname> del nombre de host** para configurar el **NOMBRE DE HOST** en el ACS como se muestra aquí:`hostname acs51`**Nota:** Debido a las limitaciones NETBIOS, los nombres de host ACS deben contener inferior o igual 15 caracteres.
10. Publique el **comando write memory** para salvar la configuración al ACS.

Únase a ACS 5.x al AD

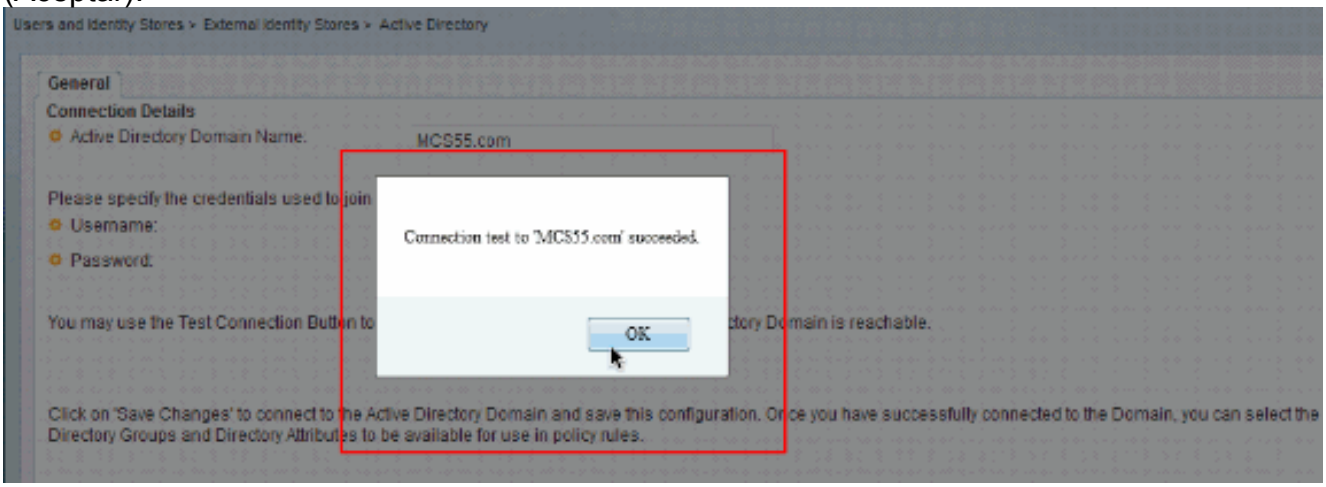
Complete estos pasos para unirse a ACS5.x al AD:

1. Elija a los **usuarios y la identidad salva > identidad externa salva > Active Directory** y proporciona el Domain Name, la cuenta AD (nombre de usuario) y su contraseña y hace clic en la **conexión de prueba**.**Nota:** La cuenta AD requerida para el acceso del dominio en el

ACS debe tener cualquiera de éstos:Agregue los puestos de trabajo a la derecha de Domain User en el dominio correspondiente.Cree los objetos de la Computadora o borre el permiso de los objetos de la Computadora en el envase correspondiente de los ordenadores donde la cuenta de máquina ACS se crea antes de unirse a la máquina ACS al dominio.**Nota:** Cisco recomienda que usted inhabilita la directiva del cierre para la cuenta ACS y configura la infraestructura AD para enviar las alertas al admin si una contraseña incorrecta se utiliza para esa cuenta. Esto es porque si usted ingresa una contraseña incorrecta, el ACS no crea ni modifica su cuenta de máquina cuando es necesario y por lo tanto para negar posiblemente todas las autenticaciones.**Nota:** La cuenta de Windows AD, que se une al ACS al dominio AD, se puede poner en su propia unidad organizativa (OU). Reside en su propio OU cualquiera cuando la cuenta se crea o después con una restricción que el nombre del dispositivo debe hacer juego el nombre de la cuenta
AD.



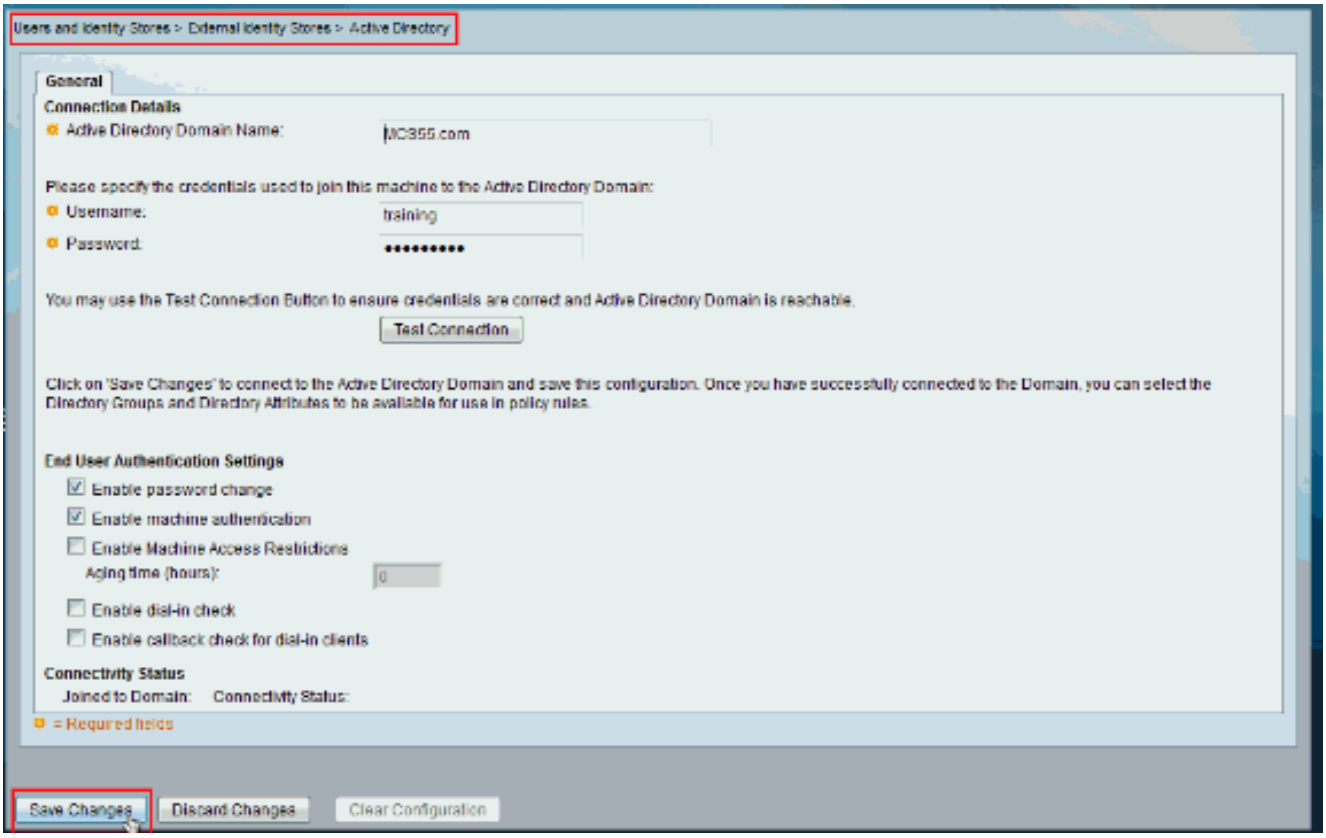
2. Esta captura de pantalla muestra que la conexión de prueba al AD es acertada. Luego haga clic en OK
(Aceptar).



Nota: La configuración de Centrify consigue afectada y consigue a veces disconnected

cuando hay una respuesta lenta del servidor mientras que usted prueba la conexión ACS con el dominio AD. Sin embargo, trabaja muy bien con las otras aplicaciones.

3. **La salvaguardia del** tecleo **cambia** para que el ACS se una al AD.



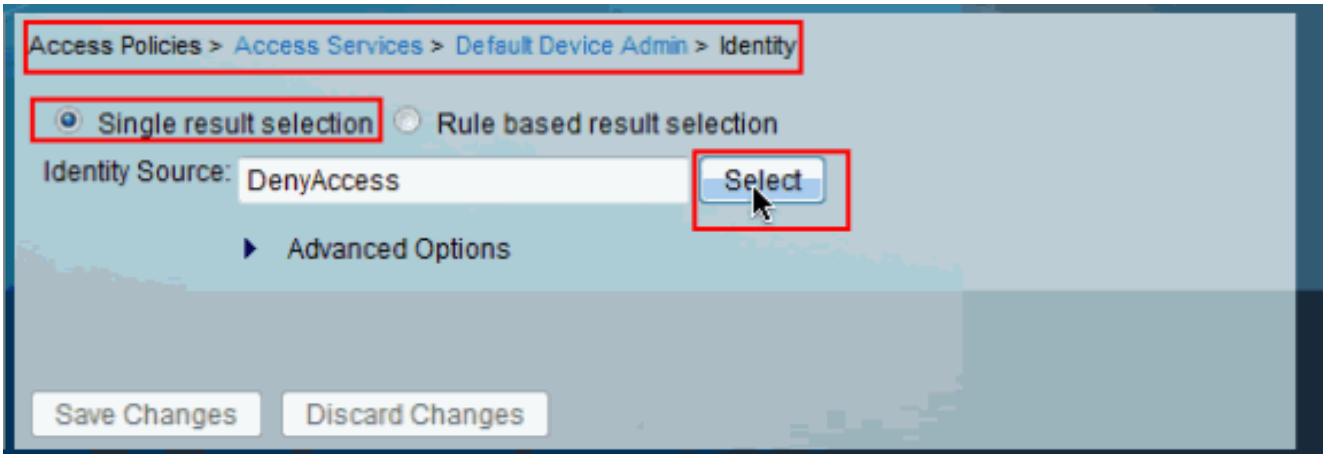
4. Una vez que el ACS se ha unido a con éxito el dominio AD, muestra en el estatus de la Conectividad.

Nota: Cuando usted configura un almacén de la identidad AD, el ACS también crea:Un nuevo diccionario para ese almacén con dos atributos: ExternalGroups y otro atributo para cualquier atributo extraído de la página de los atributos del directorio.Un nuevo atributo, IdentityAccessRestricted. Usted puede crear manualmente una condición de encargo para este atributo.Una condición de encargo para la asignación del grupo del atributo de ExternalGroup; el nombre de condición de encargo es AD1:ExternalGroups y otra condición de encargo para cada atributo seleccionado en la página de los atributos del directorio, por ejemplo, AD1:cn.

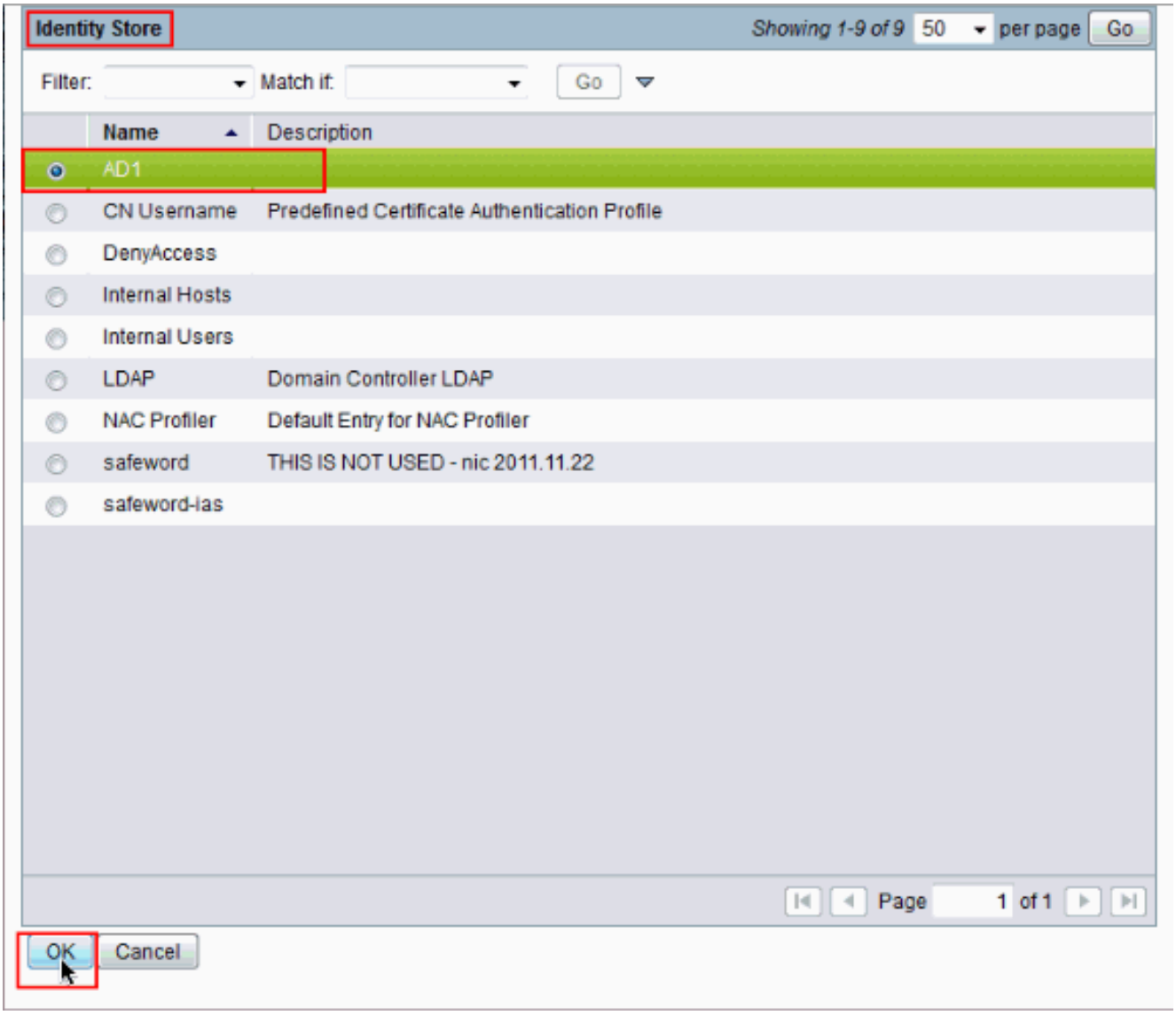
Servicio del acceso de la configuración

Complete estos pasos para completar la configuración de servicio del acceso de modo que el ACS pueda utilizar la integración nuevamente configurada AD.

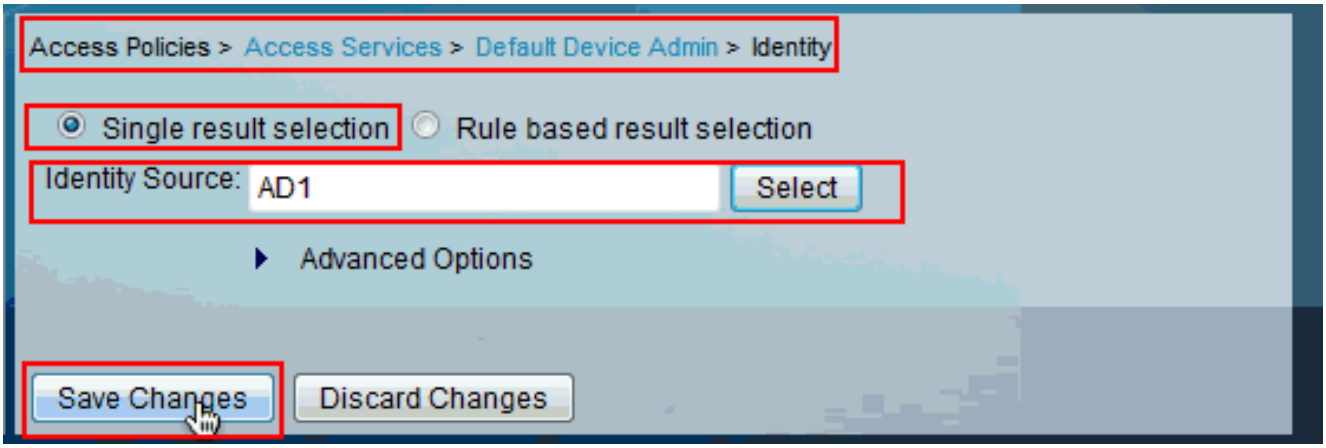
1. Elija el servicio de donde le como los usuarios autenticarían del AD y hacer clic en la **identidad**. Ahora haga clic **selecto** al lado del campo de fuente de la identidad.



2. Elija **AD1** y haga clic la **AUTORIZACIÓN**.



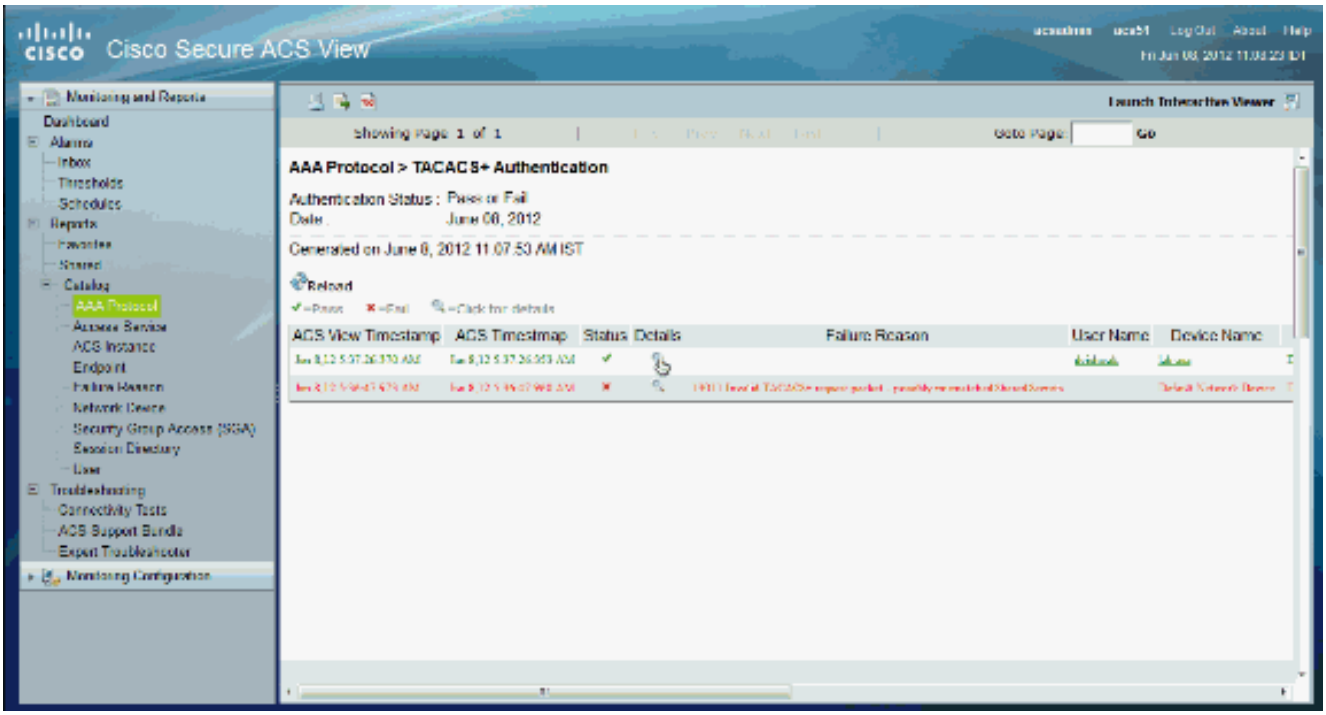
3. Haga clic los **cambios de la salvaguardia**.



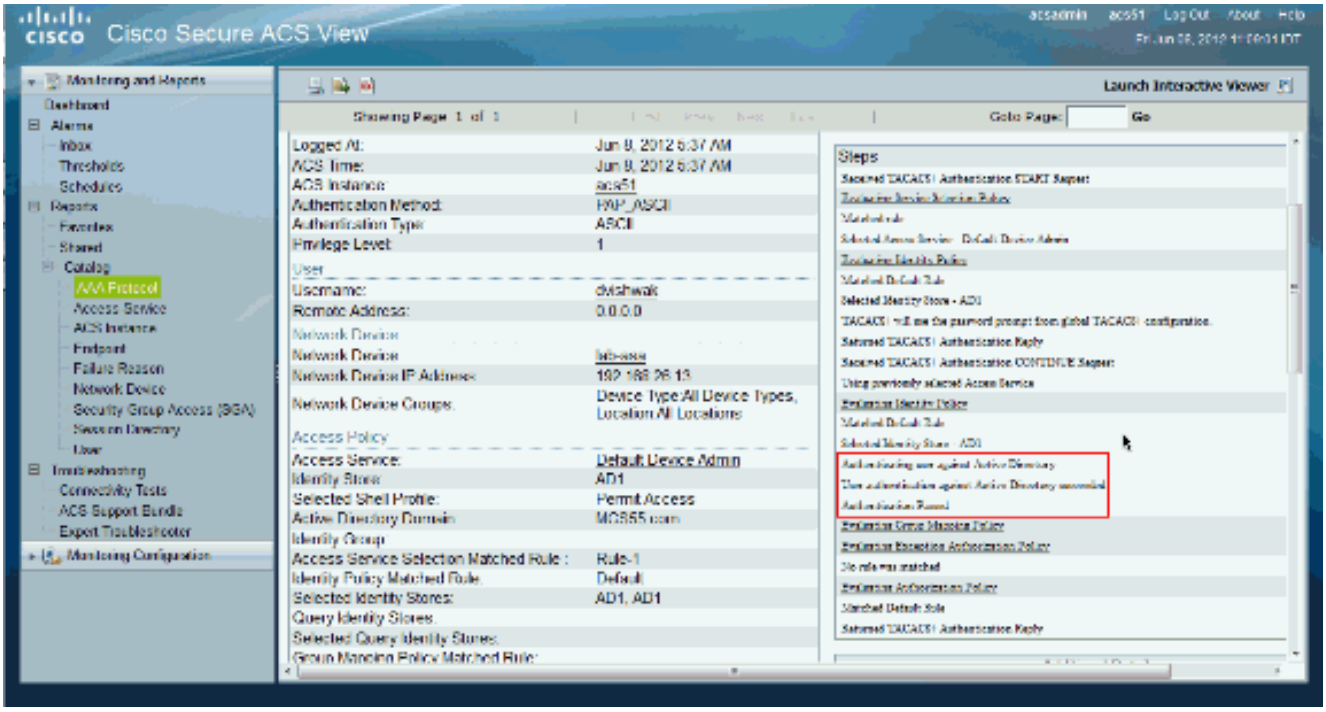
Verificación

Para verificar la autenticación AD, envíe un pedido de autenticación de un NAS con las credenciales AD. Asegúrese de que el NAS esté configurado en el ACS y la petición sería procesada por el servicio del acceso configurado en la sección anterior.

1. Después de la autenticación satisfactoria del NAS registre en el ACS GUI y elija el **protocolo de la supervisión y de los informes >AAA > TACACS+Authentication**. Identifique la autenticación pasajera de la lista y haga clic en el símbolo de la **lupa** como se muestra.



2. Usted puede verificar de los pasos que el ACS ha enviado pedido de autenticación al AD.



Información Relacionada

- Cisco Secure Access Control System
- Soporte Técnico y Documentación - Cisco Systems