ACS 5.x e posterior - Configurar integração com o Microsoft AD

Contents

Introduction

Este documento fornece uma configuração de exemplo para integrar o Microsoft Active Directory com o Cisco Secure Access Control System (ACS) 5.x ou posterior. O ACS usa o Microsoft Active Directory (AD) como um armazenamento de identidade externa para armazenar recursos, como usuários, máquinas, grupos e atributos. O ACS autentica esses recursos em relação ao AD.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O Domínio do Windows Ative Diretory a ser usado precisa estar totalmente configurado e operacional.
- Use o Domínio do Microsoft Windows Server 2003, o Domínio do Microsoft Windows Server 2008 ou o Domínio do Microsoft Windows Server 2008 R2, pois eles são suportados pelo ACS 5.x.**Observação:** a integração do domínio do Microsoft Windows Server 2008 R2 com ACS é suportada do ACS 5.2 e posterior.

Componentes Utilizados

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

- Cisco Secure ACS 5.3
- Domínio do Microsoft Windows Server 2003

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O Windows Ative Diretory fornece muitos recursos usados no uso diário da rede. A integração do ACS 5.x com o AD permite o uso de usuários, máquinas e mapeamento de grupo existentes do AD.

O ACS 5.x integrado ao AD oferece os seguintes recursos:

1. Autenticação de máquina
2. Recuperação de atributo para autorização
3. Recuperação de certificado para autenticação EAP-TLS
4. Restrição de conta de usuário e máquina
5. Restrições de acesso à máquina
6. Verificação de Permissões de Discagem
7. Opções de retorno de chamada para usuários de discagem
8. Atributos de suporte de discagem

Configuração

Configurar o ADE-OS (Application Deployment Engine, mecanismo de implantação de aplicativo) ACS 5.x

Antes de integrar o ACS 5.x ao AD, verifique se o **TimeZone, Date & Time** no ACS corresponde ao que está no controlador de domínio primário do AD. Além disso, defina o servidor DNS no ACS para poder resolver o nome de domínio do ACS 5.x. Conclua estes passos para configurar o ADE-OS (Application Deployment Engine, mecanismo de implantação de aplicativo) ACS 5.x:

1. SSH para o dispositivo ACS e insira as credenciais CLI.
2. Emita o comando **clock timezone** no modo de configuração como mostrado para configurar o **TIMEZONE** no ACS a fim de corresponder ao que está no controlador de domínio.

   ```
   clock timezone Asia/Kolkata
   ```

   Observação: Ásia/Calcutá é o fuso horário usado neste documento. Você pode encontrar o seu fuso horário específico pelo comando **show timezone do** modo exec.

3. Caso seu controlador de domínio do AD esteja sincronizado com um servidor NTP que reside em sua rede, é altamente recomendável usar o mesmo servidor NTP no ACS. Se você não tiver um servidor NTP, vá para a **etapa 4**. Estas são as etapas para configurar o servidor NTP:O servidor NTP pode ser configurado com o **comando ntp server <ip address of the NTP server>** no modo de configuração como mostrado.

```
ntp server 192.168.26.55
The NTP server was modified.
If this action resulted in a clock modification, you must restart ACS.
```

   Consulte o ACS 5.x: Exemplo de Sincronização do Cisco ACS com o Servidor NTP para obter mais informações sobre a configuração do NTP.
4. Para configurar a data e a hora manualmente, use o comando **clock set** no **modo exec**. Um exemplo é mostrado abaixo:

```
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. Agora, verifique o **fuso horário, a data** e a **hora** com o comando **show clock**. A saída do comando show clock é mostrada aqui:

```
acs51/admin# show clock
Fri Jun  8 10:36:05 IST 2012
```

6. Configure o DNS no ACS com o **<ip name-server <ip address of the DNS>** comando no **modo de configuração** conforme mostrado aqui:

```
ip name-server 192.168.26.55
```

   Observação: o endereço IP DNS é fornecido pelo administrador do domínio do Windows.
7. Execute o **comando nslookup <domain name>** para verificar se o nome de domínio está acessível como mostrado.

```
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
```

   Observação: se a **SEÇÃO RESPOSTA** estiver vazia, entre em contato com o administrador do domínio do Windows para descobrir o servidor DNS correto para o domínio.
8. Execute o comando **ip domain-name <nome de domínio>** para configurar **DOMAIN-NAME** no ACS conforme mostrado aqui:

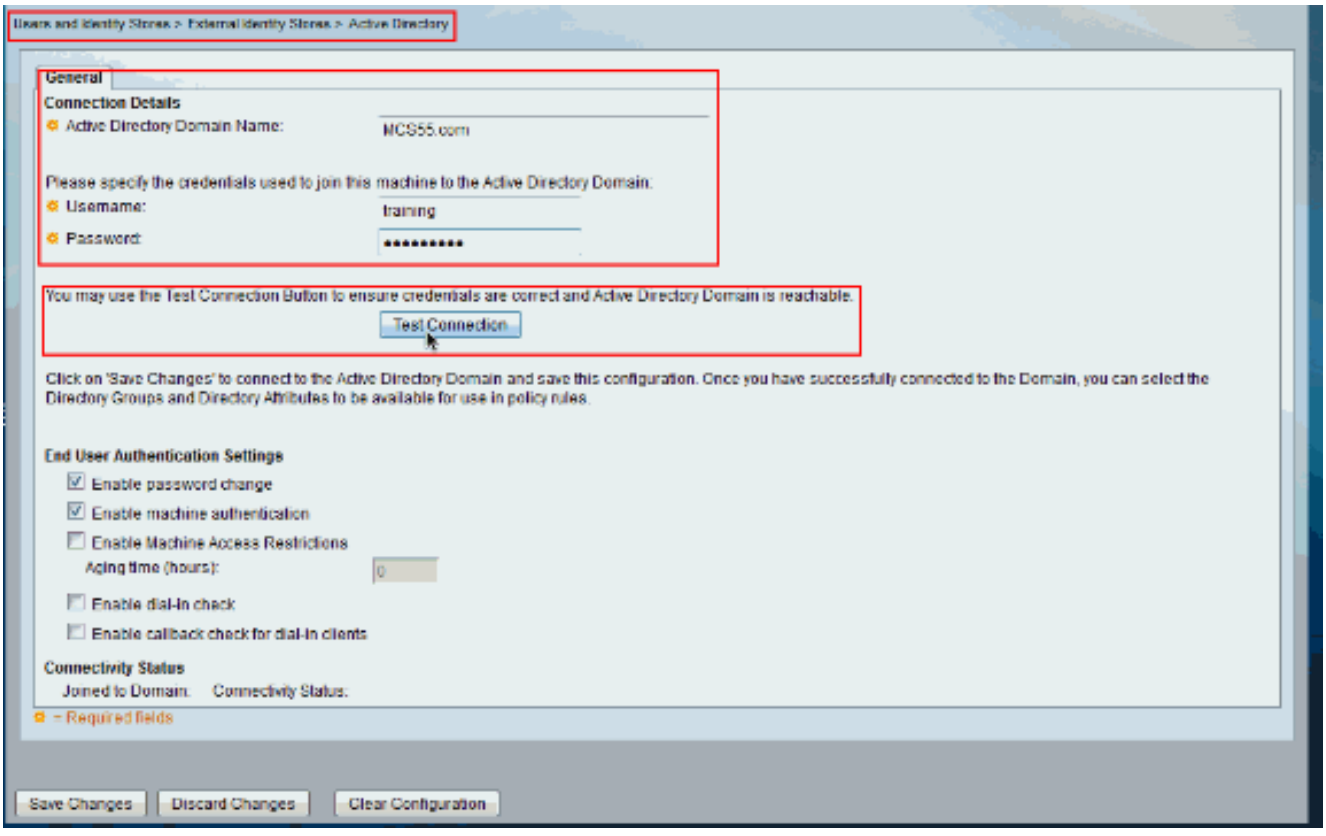
```
ip domain-name MCS55.com
```

9. Emita o **comando hostname <hostname>** para configurar **HOSTNAME** no ACS conforme mostrado aqui:
   ```
   hostname acs51
   ```
   Observação: devido às limitações do NETBIOS, os nomes de host ACS devem conter menos ou igual a 15 caracteres.
10. Execute o comando **Write memory** para salvar a configuração no ACS.

Participe do ACS 5.x para o AD

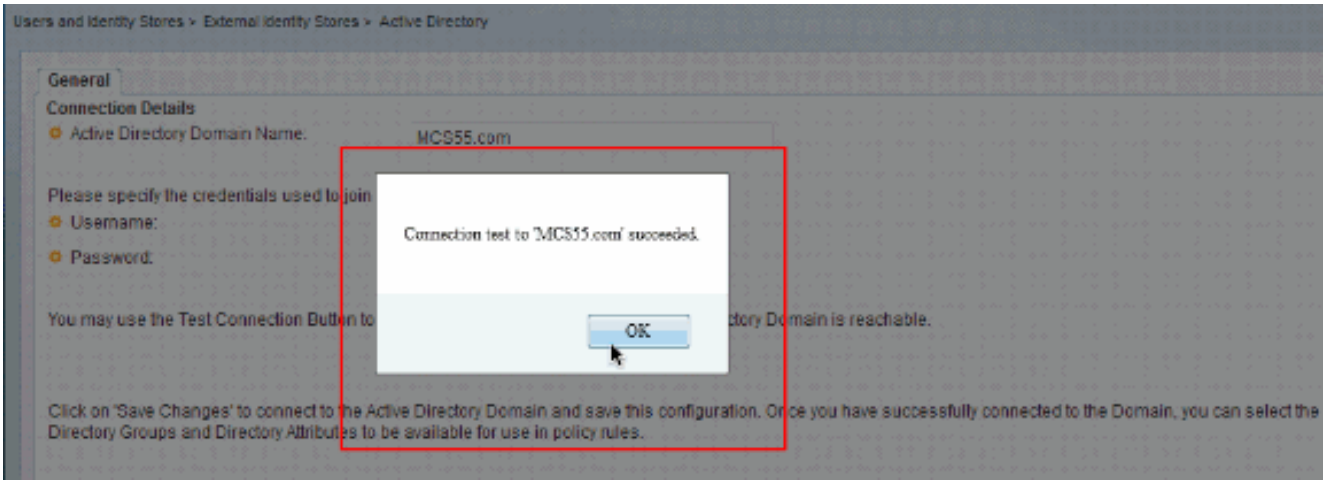
Conclua estes passos para participar do ACS5.x para o AD:

1. Escolha **Users and Identity Stores > External Identity Stores > Ative Diretory** e forneça o nome do domínio, a conta do AD (nome do usuário) e sua senha e clique em **Test Connection**.**Observação:** a conta do AD necessária para acesso ao domínio no ACS deve ter um destes:Adicione estações de trabalho ao domínio direito do usuário no domínio correspondente.A permissão Criar Objetos de Computador ou Excluir Objetos de Computador no contêiner de computadores correspondente onde a conta da máquina ACS é criada antes de ingressar na máquina ACS no domínio.**Observação:** a Cisco recomenda que você desative a política de bloqueio da conta ACS e configure a infraestrutura do AD para enviar alertas ao administrador se uma senha incorreta for usada para essa conta. Isso ocorre porque se você digitar uma senha incorreta, o ACS não cria ou modifica sua conta de máquina quando ela é necessária e, portanto, possivelmente nega todas as autenticações.**Observação:** a conta do Windows AD, que une o ACS ao domínio do AD, pode ser colocada em sua própria unidade organizacional (OU). Ela reside em sua própria OU quando a conta é criada ou posteriormente com uma restrição de que o nome do dispositivo deve corresponder ao nome da conta do AD.



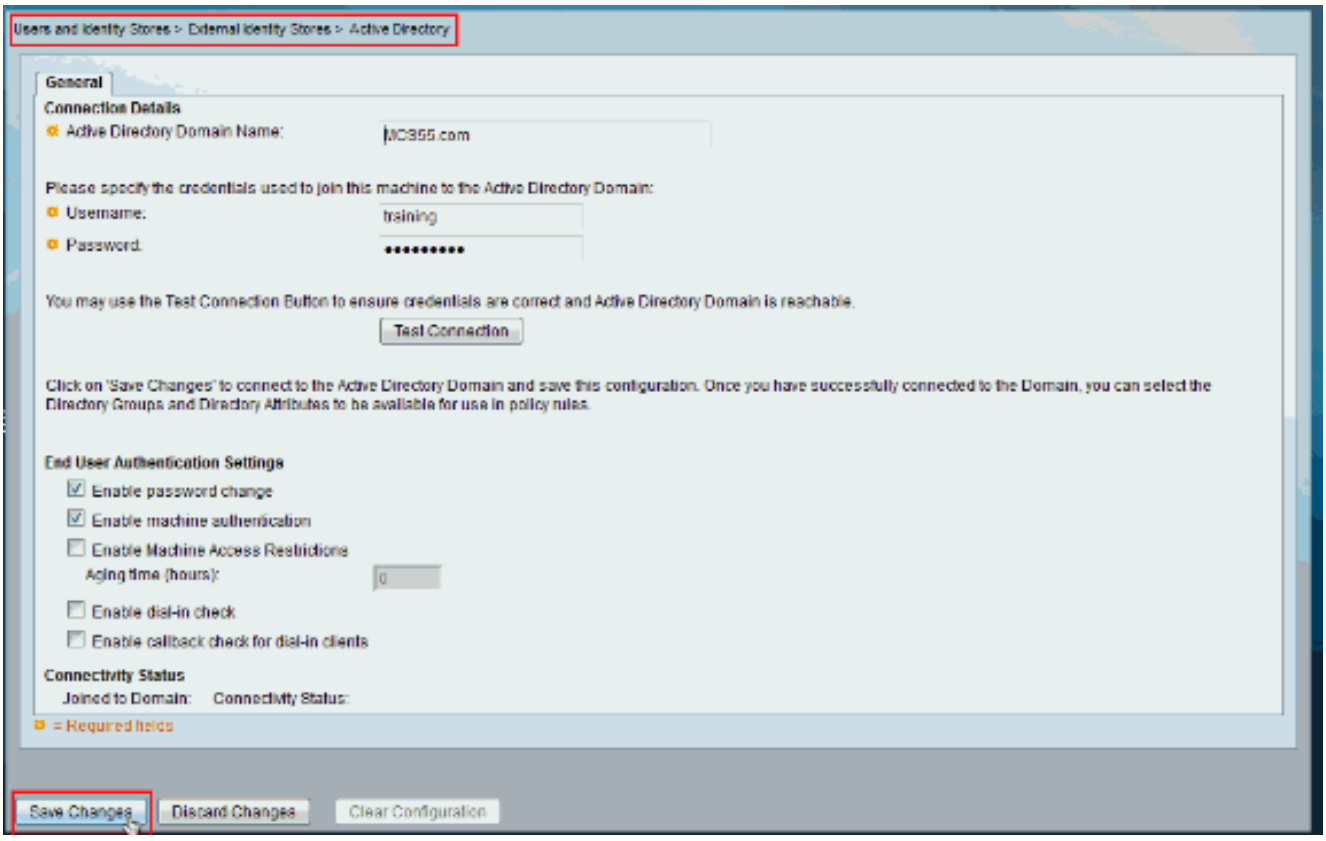
2. Esta captura de tela mostra que a conexão de teste com o AD foi bem-sucedida. Em seguida, clique em

"OK".



Observação: a configuração da centralização é afetada e às vezes é desconectada quando há uma resposta lenta do servidor enquanto você testa a conexão do ACS com o domínio do AD. No entanto, funciona bem com os outros aplicativos.

3. Clique em **Save Changes (Salvar alterações)** para o ACS ingressar no AD.



4. Depois que o ACS ingressou no domínio do AD com êxito, ele aparece no status da conectividade.

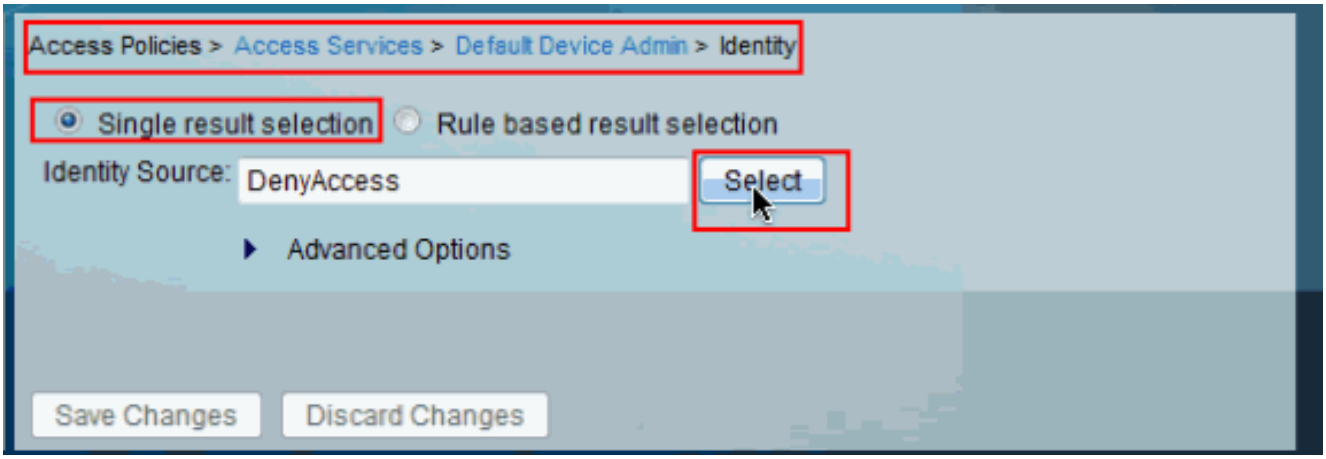
Observação: quando você configura um repositório de identidade do AD, o ACS também cria:Um novo dicionário para esse repositório com dois atributos: ExternalGroups e outro atributo para qualquer atributo recuperado da página Diretory Attributes.Um novo atributo, IdentityAccessRestricted. Você pode criar manualmente uma condição personalizada para este atributo.Uma condição personalizada para o mapeamento de grupo a partir do atributo

ExternalGroup; o nome da condição personalizada é AD1:ExternalGroups e outra condição personalizada para cada atributo selecionado na página Diretory Attributes, por exemplo, AD1:cn.

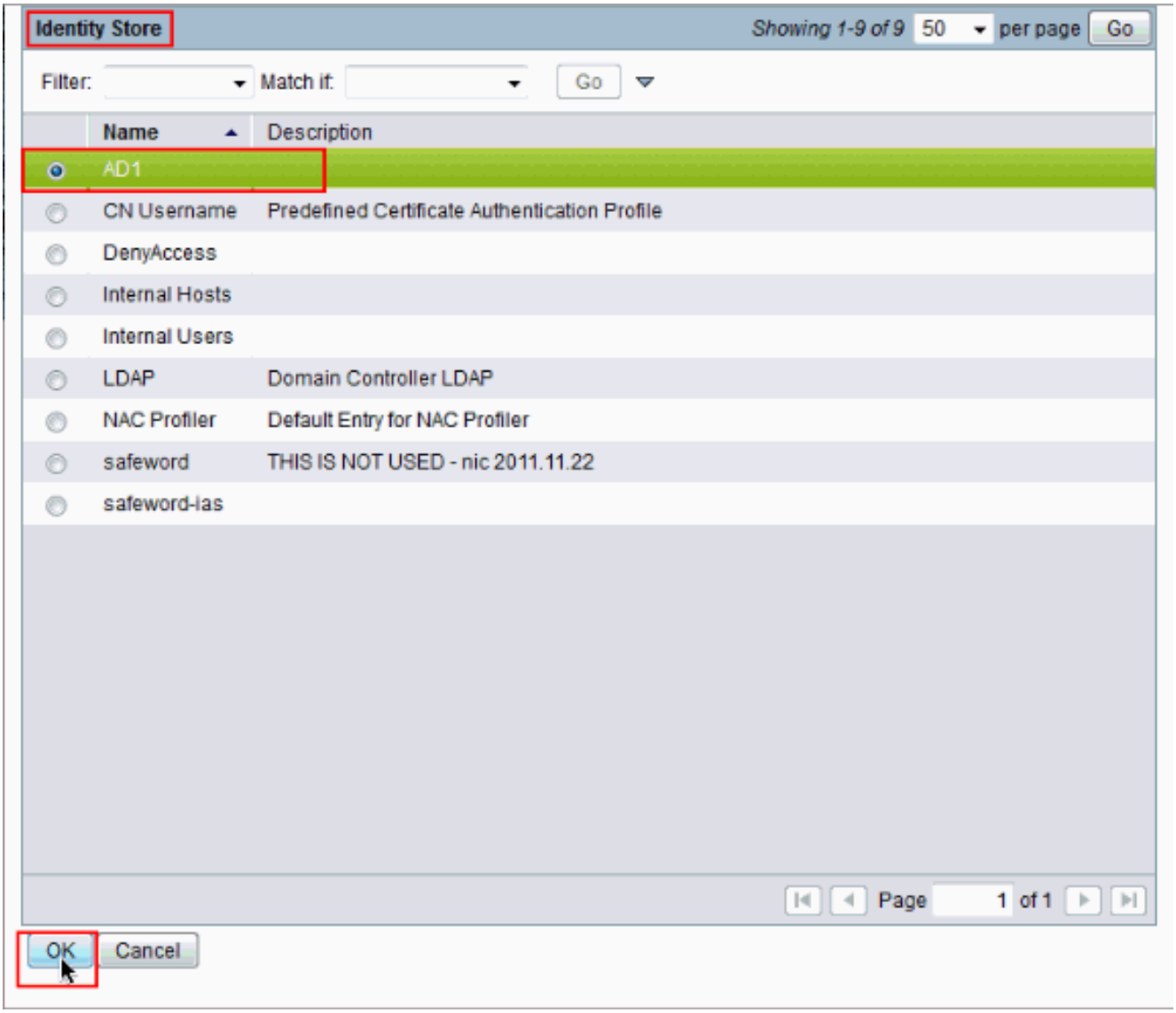
Configurar o serviço de acesso

Conclua estes passos para concluir a configuração do Serviço de Acesso de modo que o ACS possa usar a integração do AD recém-configurada.

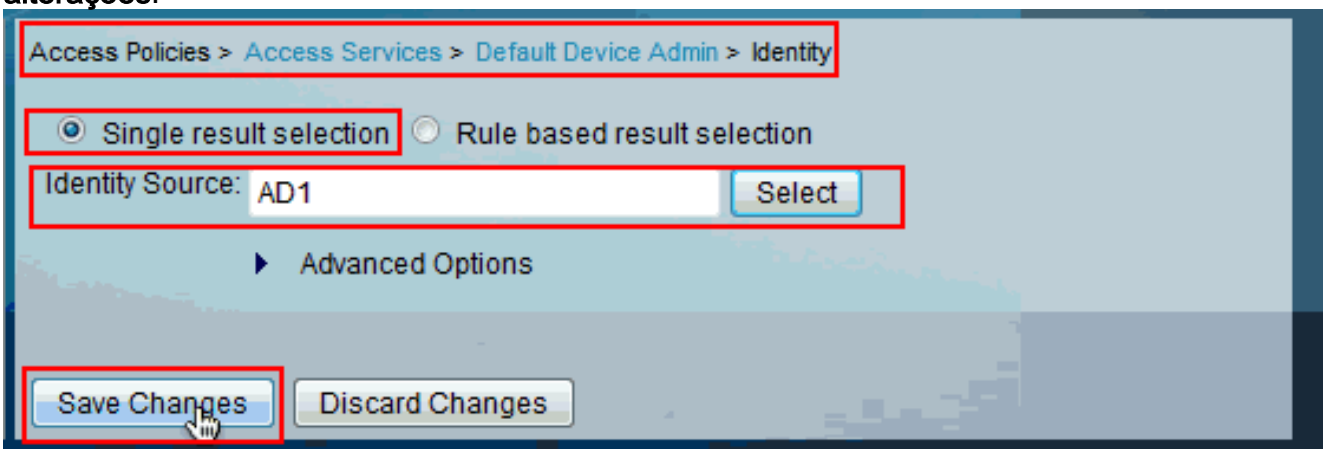
1. Escolha o serviço de onde deseja que os usuários sejam autenticados no AD e clique em **Identidade**. Agora, clique em **Selecionar** ao lado do campo Origem da identidade.



2. Escolha **AD1** e clique em **OK**.



3. Clique em **Salvar alterações**.

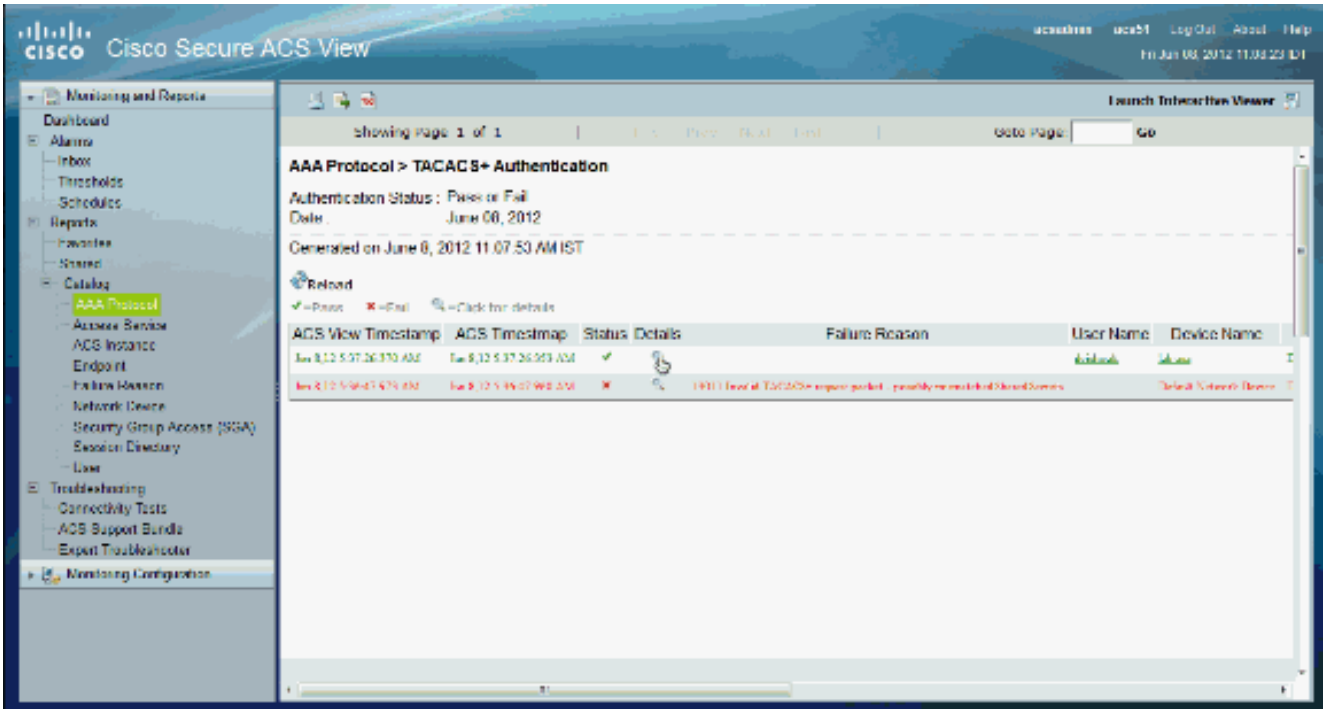


Verificar

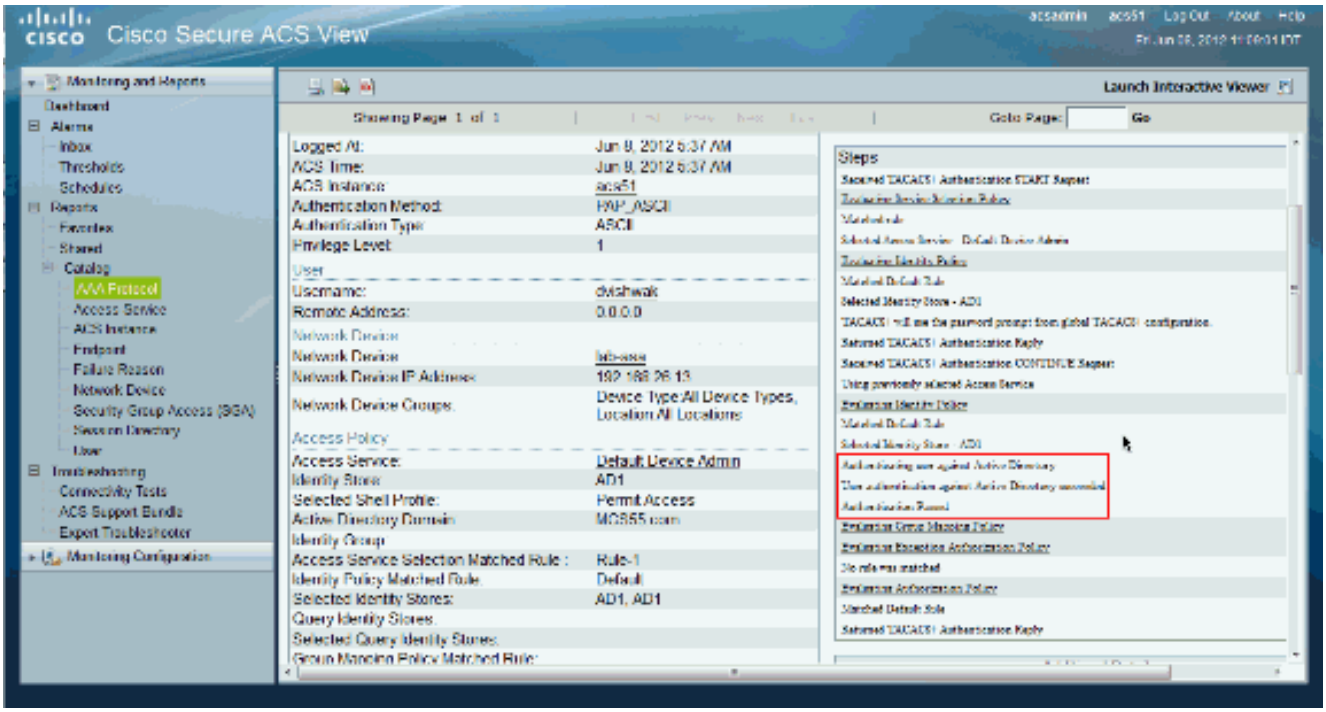
Para verificar a autenticação do AD, envie uma solicitação de autenticação de um NAS com credenciais do AD. Certifique-se de que o NAS esteja configurado no ACS e que a solicitação seja processada pelo serviço de acesso configurado na seção anterior.

1. Após a autenticação bem-sucedida do NAS, faça login na GUI do ACS e escolha **Monitoring and Reports > AAA Protocol > TACACS+Authentication**. Identifique a autenticação aprovada

na lista e clique no símbolo **de lupa** como mostrado.



2. Você pode verificar nas etapas que o ACS enviou a solicitação de autenticação ao AD.



Informações Relacionadas

- Cisco Secure Access Control System
- Suporte Técnico e Documentação - Cisco Systems