ACS 5.x e mais tarde: Integração com exemplo de configuração do microsoft ative directory

Índice

Introdução

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.

Pré-requisitos

Requisitos

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

- Domínio do diretório ativo de Windows a ser necessidades usadas de ser configurado inteiramente e operacional.
- Use o domínio 2003 do Microsoft Windows server, o domínio 2008 do Microsoft Windows server ou o domínio R2 do Microsoft Windows server 2008 como estes são apoiados por ACS 5.x.**Nota:** A integração do domínio R2 do Microsoft Windows server 2008 com ACS é apoiada de ACS 5.2 e mais atrasado.

Componentes Utilizados

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

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

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.

Convenções

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

Informações de Apoio

O diretório ativo de Windows fornece muitas características que são usadas no USO de rede diário. A integração de ACS 5.x com AD permite o uso dos usuários existentes AD, de máquinas e de seu mapeamento do grupo.

O ACS 5.x integrado com AD fornece estas características:

1. Autenticação da máquina
2. Recuperação do atributo para a autorização
3. Recuperação de certificado para a autenticação EAP-TLS
4. Limitação da conta do usuário e de máquina
5. Restrições de acesso da máquina
6. Verificação das permissões de discagem de entrada
7. Opções de chamada de volta para usuários de discagem de entrada
8. Atributos do apoio do discado

Configuração

Configurar o motor do desenvolvimento de aplicativo ACS 5.x (ADE-OS)

Antes que você integre ACS 5.x ao AD, assegure-se de que aquele o **fuso horário, a data & a hora no** ACS combinem com o aquele no Primary Domain Controller AD. Também, defina o servidor DNS no ACS a fim poder resolver o Domain Name do ACS 5.x. Termine estas etapas a fim configurar o motor do desenvolvimento de aplicativo ACS 5.x (ADE-OS):

1. O SSH à ferramenta ACS e incorpora as credenciais CLI.
2. Emita o **comando clock timezone no** modo de configuração segundo as indicações da ordem configurar o **FUSO HORÁRIO no** ACS a fim combinar com o aquele no controlador de domínio.
   `clock timezone Asia/Kolkata` **Nota:** Ásia/Kolkata é o fuso horário usado neste documento. Você pode encontrar seu fuso horário específico pelo comando dos **fusos horários da mostra do** modo exec.
3. Caso que seu controlador de domínio AD é sincronizado com um servidor de NTP que resida em sua rede, é altamente recomendado usar o mesmo servidor de NTP no ACS. Se você não tem o servidor de NTP, a seguir salte a **etapa 4.** Estas são as etapas para

configurar o servidor de NTP:O servidor de NTP pode ser configurado com o **server NTP < endereço IP de Um ou Mais Servidores Cisco ICM NT do** comando do **server> NTP 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.`Refira ACS 5.x: Sincronização de Cisco ACS com exemplo de configuração do servidor de NTP para obter mais informações sobre da configuração de NTP.

4. A fim configurar a data e hora use manualmente o **comando clock set no modo exec**. Um exemplo é mostrado aqui:
```
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. Verifique agora o **fuso horário, data e 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. Configurar o DNS no ACS com o **Nome do servidor do <ip < endereço IP de Um ou Mais Servidores Cisco ICM NT do** comando **DNS> no modo de configuração** como mostrado aqui:`ip name-server 192.168.26.55`**Nota:** O endereço IP de Um ou Mais Servidores Cisco ICM NT DNS é fornecido por seu administrador do domínio do Windows.
7. Emita o comando **< do Domain Name > do nslookup** a fim verificar como mostrado a alcançabilidade do Domain Name.`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:** Se a **SEÇÃO da RESPOSTA** está vazia, a seguir contacte seu administrador do domínio do Windows para encontrar o servidor DNS correto para o domínio.
8. Emita o comando **< do Domain Name > do Domain Name IP** a fim configurar como mostrado o **DOMAIN NAME no** ACS aqui:`ip domain-name MCS55.com`
9. Emita o comando do **<hostname> do hostname** a fim configurar como mostrado o **HOSTNAME no** ACS aqui:`hostname acs51`**Nota:** Devido às limitações de NETBIOS, os nomes de host ACS devem conter inferior ou igual a 15 caráteres.
10. Emita o **comando write memory** a fim salvar a configuração ao ACS.

Junte-se a ACS 5.x ao AD

Termine estas etapas a fim juntar-se a ACS5.x ao AD:

1. Escolha **usuários e a identidade armazena > identidade externo armazena > diretório ativo** e fornece o Domain Name, a conta AD (username) e a sua senha e clica sobre a **conexão de teste**.**Nota:** A conta AD exigida para o acesso do domínio no ACS deve ter qualquer uma destes:Adicionar estações de trabalho à direita de usuário de domínio no domínio correspondente.Crie objetos do computador ou suprima da permissão dos objetos do

computador no recipiente correspondente dos computadores onde a conta de máquina ACS é criada antes de se juntar a máquina ACS ao domínio.**Nota:** Cisco recomenda que você desabilita a política do fechamento para a conta ACS e configura a infraestrutura AD para enviar alertas ao admin se uma senha errada é usada para essa conta. Isto é porque se você incorpora uma senha errada, o ACS não cria nem altera sua conta de máquina quando é necessário e consequentemente para negar possivelmente todas as autenticações.**Nota:** A conta de Windows AD, que se junta ao ACS ao domínio AD, pode ser colocada em sua própria unidade organizacional (OU). Reside em seu próprio OU qualquer um quando a conta é criada ou mais tarde com uma limitação que o nome do dispositivo deve combinar o nome da conta AD.
2. Este screen shot mostra que a conexão de teste ao AD é bem sucedida. Em seguida, clique em “OK”.**Nota:** A configuração de Centrify obtém afetada e obtém às vezes desligado quando há uma resposta lenta do server quando você testar a conexão ACS com o domínio AD. Contudo, trabalha muito bem com os outros aplicativos.
3. **A salvaguarda do** clique **muda** para que o ACS junte-se ao AD.
4. Uma vez que o ACS se juntou com sucesso ao domínio AD, mostra no estado da Conectividade.**Nota:** Quando você configura uma loja da identidade AD, o ACS igualmente cria:Um dicionário novo para essa loja com dois atributos: ExternalGroups e um outro atributo para algum atributo recuperado da página dos atributos do diretório.Um atributo novo, IdentityAccessRestricted. Você pode manualmente criar uma condição feita sob encomenda para este atributo.Uma condição feita sob encomenda para o mapeamento do grupo do atributo de ExternalGroup; o nome de circunstância feito sob encomenda é AD1:ExternalGroups e uma outra condição feita sob encomenda para cada atributo selecionado no diretório atribui a página, por exemplo, AD1:cn.

Configurar o serviço do acesso

Termine estas etapas a fim terminar a configuração de serviço do acesso de modo que o ACS possa usar a integração recentemente configurada AD.

1. Escolha o serviço de onde você como os usuários seria autenticado do AD e para clicar sobre a **identidade**. Clique agora **seleto** ao lado do campo de fonte da identidade.
2. Escolha **AD1** e clique a **APROVAÇÃO**.
3. Clique **mudanças da salvaguarda**.

Verificar

A fim verificar a autenticação AD, envie um pedido de autenticação de um NAS com credenciais AD. Assegure-se de que o NAS esteja configurado no ACS e o pedido esteja processado pelo serviço do acesso configurado na seção anterior.

1. Após a autenticação bem sucedida do NAS registre no ACS GUI e escolha a **monitoração e os relatórios > o protocolo de AAA > o TACACS+Authentication**. Identifique a autenticação passada da lista e clique sobre o símbolo da **lupa** como mostrado.
2. Você pode verificar das etapas que o ACS enviou o pedido de autenticação ao AD.

Informações Relacionadas

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