Permissão mínima de Grant a uma conta de usuário do diretório ativo usada pelo agente de usuário de Sourcefire

Índice

Introdução

Este documento descreve como fornecer um usuário do diretório ativo (AD) as permissões mínimas necessárias perguntar o controlador de domínio AD. O agente de usuário de Sourcefire usa um usuário AD a fim perguntar o controlador de domínio AD. A fim executar uma pergunta, um usuário AD não exige nenhumas permissões adicionais.

Pré-requisitos

Requisitos

Cisco exige que você instala o agente de usuário de Sourcefire em um sistema de Microsoft Windows e fornece o acesso ao controlador de domínio AD.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Configurar

Primeiramente, um administrador deve criar um usuário novo AD especificamente para o acesso do agente de usuário. Se este novo usuário não é um membro do grupo dos administradores de domínio (e eles não deve ser), o usuário pôde ter que ser concedido explicitamente a permissão alcançar os registros de segurança de Windows Management Instrumentation (WMI). A fim conceder a permissão, termine estas etapas:

1. Abra o console de controle WMI:

   No server AD, escolha o **menu de início**.

   Clique a **corrida** e incorpore **wmimgmt.msc.**

   Click **OK**. O console de controle WMI aparece.

2. Na árvore de console WMI, clicar com o botão direito o **controle WMI** e clique então **propriedades**.

3. Clique na guia Security.

4. Selecione o namespace para que você quer dar um acesso do usuário ou do grupo (`Root\CIMV2`), e clique então a **Segurança**.

5. Na caixa de diálogo da Segurança, o clique **adiciona**.

6. No selecionar Caixa de Diálogo de Usuários, Computadores ou Grupos, dão entrada com o nome do objeto (usuário ou grupo) esse você querem adicionar. Clique **nomes da verificação** a fim verificar sua entrada e clicar então a **APROVAÇÃO**. Você pôde ter que mudar o lugar ou clicá-lo **avançado** a fim perguntar para objetos. Veja a ajuda Contexto-sensível (`?`) para mais detalhe.

7. Na caixa de diálogo da Segurança, na seção das permissões, escolha **reservam** ou **negam** a fim conceder permissões ao novo usuário ou ao grupo (o mais fácil dar todas as permissões). O usuário deve ser dado pelo menos o **telecontrole permite a** permissão.

8. O clique **aplica-se** a fim salvar mudanças. Feche a janela.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Se uma edição persiste após as alterações de configuração, atualize os ajustes do modelo de objeto de componente distribuído (DCOM) a fim permitir o Acesso remoto:

1. Escolha o **menu de início**.

2. Clique a **corrida** e incorpore **DCOMCNFG**.

3. Click **OK**. A caixa de diálogo dos serviços de componente aparece.

4. Na caixa de diálogo dos serviços de componente, expanda **serviços de componente**, expanda **computadores**, e então clicar com o botão direito o **meu computador** e escolha **propriedades**.

5. Na caixa de diálogo das propriedades do meu computador, clique a **ABA de segurança COM**.

6. Sob permissões do lançamento e da ativação, o clique **edita limites**.

7. Na caixa de diálogo da permissão do lançamento e da ativação, termine estas etapas se seu nome ou seu grupo não aparecem nos grupos ou na lista de nomes de usuário:

   Na caixa de diálogo da permissão do lançamento e da ativação, o clique **adiciona**.

   No selecionar Caixa de Diálogo de Usuários, Computadores ou Grupos, inscrevem seu nome e o grupo na entrada os nomes de objeto para selecionar o campo, e clicam então a **APROVAÇÃO**.

8. Na caixa de diálogo da permissão do lançamento e da ativação, selecione seu usuário e agrupe-o no **grupo ou na** seção dos **nomes de usuário**.

9. Na coluna reservar sob permissões para o usuário, verifique o **lançamento remoto** e as caixas de seleção **remotas da ativação**, e clique então a **APROVAÇÃO**.**Note**: Um nome de usuário deve ter direitos de perguntar para dados do login de usuário em um server AD. A fim autenticar com um usuário através do proxy, dê entrada com um nome de usuário totalmente qualificado. À revelia, o domínio para a conta que você se usou para registrar no computador onde você instalou o agente auto-povoa o campo do domínio. Se um usuário

que você fornece é um membro de um domínio diferente, atualiza o domínio para as credenciais do usuário fornecidas.

10. Se o problema persiste, na tentativa do controlador de domínio para adicionar o usuário na política do exame e do registro de segurança Manage. A fim adicionar o usuário, termine estas etapas:

    Escolha o **editor do Gerenciamento de políticas do grupo**.

    Escolha o **Configuração de Computador > Configurações do Windows > Configurações de Segurança** > as **políticas local** > a **atribuição dos direitos do usuário**.

    Escolha o **exame e o registro de segurança Manage**.

    Adicionar o usuário.