Conceder permissão mínima para uma conta de usuário do Ative Diretory usada pelo agente de usuário da Sourcefire

Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Verificar Troubleshoot

Introduction

Este documento descreve como fornecer a um usuário do Ative Diretory (AD) as permissões mínimas necessárias para consultar o controlador de domínio do AD. O agente de usuário Sourcefire usa um usuário do AD para consultar o controlador de domínio do AD. Para realizar uma consulta, um usuário do AD não exige nenhuma permissão adicional.

Prerequisites

Requirements

A Cisco exige que você instale o Sourcefire User Agent em um sistema Microsoft Windows e forneça acesso ao controlador de domínio do AD.

Componentes Utilizados

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

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.

Configurar

Primeiro, um administrador deve criar um novo usuário do AD especificamente para acesso ao Agente de usuário. Se esse novo usuário não for membro do grupo de administradores de domínio (e eles não devem ser), talvez seja necessário conceder explicitamente ao usuário permissão para acessar os logs de segurança da Instrumentação de Gerenciamento do Windows (WMI). Para conceder permissão, faça o seguinte:

1. Abra o Console de controle WMI:

No servidor AD, escolha o menu Iniciar.

Clique em Executar e digite wmimgmt.msc.

Click OK. O Console de controle WMI é exibido.



- 2. Na árvore do console WMI, clique com o botão direito do mouse em **Controle WMI** e clique em **Propriedades**.
- 3. Clique na guia Security.
- 4. Selecione o espaço de nomes para o qual pretende conceder a um utilizador ou grupo acesso (Raiz\cimv2) e, em seguida, clique em **Segurança**.

WMI Control (Local) Properties	ବ	23				
General Backup/Restore Security Advanced						
Namespace navigation allows you to set namespace specific security.						
Root Image: SecurityCenter Image: SecurityCenter <tr< th=""><th></th><th></th></tr<>						
Sec	urity					
OK Cancel	Ap	ply				

5. Na caixa de diálogo Segurança, clique em Adicionar.

Group or user names:		
& Authenticated Users		
& LOCAL SERVICE		
& NETWORK SERVICE		
Administrators (TS-WIN7\A	dministrators)	
	Add	Remove
	Add	Nelliove
Permissions	Allow	Deny
Execute Methods		· ·
Full Write		=
Partial Write		
Provider Write		
Enable Account		-
For special permissions or advan click Advanced.	ced settings,	Advanced

- 6. Na caixa de diálogo Selecionar usuários, computadores ou grupos, digite o nome do objeto (usuário ou grupo) que deseja adicionar. Clique em Verificar nomes para verificar sua entrada e clique em OK. Talvez seja necessário alterar o local ou clicar em Avançado para procurar objetos. Consulte a Ajuda sensível ao contexto (?) para obter mais detalhes.
- 7. Na caixa de diálogo Segurança, na seção Permissões, escolha **Permitir** ou **Negar** para conceder permissões ao novo usuário ou grupo (mais fácil de conceder todas as permissões). O usuário deve receber pelo menos a permissão **Remote Enable**.
- 8. Clique em Apply para salvar as alterações. Feche a janela.

Verificar

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

Troubleshoot

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

Se um problema persistir após as alterações de configuração, atualize as configurações do Distributed Component Object Model (DCOM) para permitir acesso remoto:

- 1. Escolha o menu Iniciar.
- 2. Clique em Executar e digite DCOMCNFG.
- 3. Click OK. A caixa de diálogo Serviços de Componentes é exibida.



- Na caixa de diálogo Serviços de componente, expanda Serviços de componente, expanda Computadores e clique com o botão direito do mouse em Meu computador e escolha Propriedades.
- 5. Na caixa de diálogo Propriedades do meu computador, clique na guia Segurança COM.

My Computer Properties	8	X		
General Options Defa	ault Properties			
Default Protocols COM Security	MSDTC			
Access Permissions				
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.				
Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.				
Edit Limits	dit Default			
Launch and Activation Permissions		51		
You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.				
Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.				
Edit Limits	dit Default			
Learn more about <u>setting these properties</u> .				
OK Cance	Appl	y		

- 6. Em Permissões de inicialização e ativação, clique em Editar limites.
- 7. Na caixa de diálogo Iniciar e permissão de ativação, faça o seguinte caso seu nome ou seu grupo não apareça na lista Grupos ou nomes de usuário:

Na caixa de diálogo Iniciar e permissão de ativação, clique em Adicionar.

Na caixa de diálogo Selecionar usuários, computadores ou grupos, digite seu nome e o grupo no campo Inserir os nomes dos objetos a serem selecionados e clique em **OK**.

8. Na caixa de diálogo Iniciar e permissão de ativação, selecione seu usuário e grupo na seção

Grupo ou nomes de usuário.

Launch and Activation Permission		_	8	23
Security Limits				
Group or user names:				
& Everyone				
& Administrators (TS-WIN7\Adr	ninistrators)			.
Reformance Log Users (TS-WIN7\Performance Log Users) Bistributed COM Users (TS-WIN7\Distributed COM Users)				
	Add	F	Remov	/e
Permissions for Everyone	Allow		Deny	
Local Launch				
Remote Launch	v			
Local Activation				
Remote Activation				
Learn about access control and permissions				
	ОК		Са	ncel

- 9. Na coluna Allow (Permitir) em Permissions for User (Permissões para usuário), marque as caixas de seleção Remote Launch (Inicialização remota) e Remote Ativation (Ativação remota) e clique em OK.Note: Um nome de utilizador tem de ter direitos para consultar dados de início de sessão de utilizador num servidor AD. Para autenticar com um usuário via proxy, insira um nome de usuário totalmente qualificado. Por padrão, o domínio da conta que você usou para fazer logon no computador em que o agente instalou preenche automaticamente o campo Domínio. Se um usuário fornecido for membro de um domínio diferente, atualize o domínio para as credenciais de usuário fornecidas.
- 10. Se o problema persistir, no Controlador de Domínio tente adicionar o usuário na política Gerenciar auditoria e log de segurança. Para adicionar o usuário, faça o seguinte:

Escolha o Editor de Gerenciamento de Política de Grupo.

Escolha Configuração do computador > **Configurações do Windows > Configurações de segurança > Políticas locais > Atribuição de direitos de usuário**.

Escolha Gerenciar auditoria e registro de segurança.

Adicione o usuário.

If Group Policy Management Editor			_ D X			
File Action View Help						
 Default Domain Controllers Policy Computer Configuration Policies Software Settings Windows Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Security Settings Local Policies Local Policies Local Policy Security Options Event Log Event Log System Services System Services File System 		Policy Impersonate a client after authentication Impersonate a client after authentication Increase a process working set Increase a process working set Increase scheduling priority Load and unload device drivers Lock pages in memory Log on as a batch job Log on as a service Manage auditing and security log Modify an object label Modify firmware environment values Perform volume maintenance tasks Profile single process Profile system performance Remove computer from docking station	Policy Setting ^ Server Operato IIS APPPOOL\D Not Defined Not Defined Administrators Print Operators Not Defined Performance Lo Not Defined Administrators NOT SERVICE\W Administrators			
Windows Firewall with Advanced Se		Restore files and directories	Server Operato			
Network List Manager Policies		Shut down the system	Print Operators			
Wireless Network (IEEE 802.11) Polic		Synchronize directory service data	Not Defined			
Public Key Policies	~	Take ownership of files or other objects	Administrators ×			