Concedere autorizzazioni minime a un account utente di Active Directory utilizzato dall'agente utente Sourcefire

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto come fornire a un utente di Active Directory (AD) le autorizzazioni minime necessarie per eseguire query sul controller di dominio AD. L'agente utente Sourcefire utilizza un utente AD per eseguire query sul controller di dominio AD. Per eseguire una query, un utente AD non richiede autorizzazioni aggiuntive.

Prerequisiti

Requisiti

Cisco richiede l'installazione dell'agente utente Sourcefire in un sistema Microsoft Windows e l'accesso al controller di dominio Active Directory.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In primo luogo, un amministratore deve creare un nuovo utente AD specifico per l'accesso Agente utente. Se il nuovo utente non è membro del gruppo degli amministratori di dominio e non dovrebbe esserlo, potrebbe essere necessario concedere in modo esplicito all'utente l'autorizzazione ad accedere ai registri di protezione di Strumentazione gestione Windows (WMI). Per concedere l'autorizzazione, attenersi alla seguente procedura:

1. Aprire la console di controllo WMI:

Sul server AD, scegliere il menu Start.

Fare clic su Esegui e immettere wmimgmt.msc.

Fare clic su OK. Verrà visualizzata la console di controllo WMI.



- 2. Nell'albero della console WMI fare clic con il pulsante destro del mouse su **Controllo WMI** e quindi scegliere **Proprietà**.
- 3. Fare clic sulla scheda Protezione.
- 4. Selezionare lo spazio dei nomi per il quale si desidera concedere a un utente o a un gruppo l'accesso (Root\CIMV2), quindi fare clic su **Protezione**.

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

5. Nella finestra di dialogo Protezione fare clic su Aggiungi.

-			
Group or user names:			
& Authenticated Users			
& LOCAL SERVICE			
METWORK SERVICE			
Machinistrators (TS-WIN/\Administrators)			
	Add	Remove	
		nemove	
Permissions	Allow	Deny	
Execute Methods		^	
Full Write		=	
Partial Write			
Provider Write			
Enable Account		-	
For special permissions or advanced settings.			
click Advanced.		Auvanced	
Learn about access control and normissions			

- 6. Nella finestra di dialogo Seleziona utenti, computer o gruppi immettere il nome dell'oggetto (utente o gruppo) che si desidera aggiungere. Fare clic su Controlla nomi per verificare la voce immessa, quindi fare clic su OK. Per eseguire una query sugli oggetti, potrebbe essere necessario modificare il percorso o fare clic su Avanzate. Vedere la Guida sensibile al contesto (?) per ulteriori informazioni.
- Nella sezione Autorizzazioni della finestra di dialogo Protezione scegliere Consenti o Nega per concedere le autorizzazioni al nuovo utente o gruppo (operazione più semplice). All'utente deve essere concessa almeno l'autorizzazione Abilitazione remota.
- 8. Per salvare le modifiche, fare clic su **Apply** (Applica). Chiudete la finestra.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Se il problema persiste dopo la modifica della configurazione, aggiornare le impostazioni DCOM (Distributed Component Object Model) per consentire l'accesso remoto:

- 1. Scegliere il menu Start.
- 2. Fare clic su Esegui e immettere DCOMCNFG.
- 3. Fare clic su OK. Verrà visualizzata la finestra di dialogo Servizi componenti.



- 4. Nella finestra di dialogo Servizi componenti espandere **Servizi componenti**, **Computer**, fare clic con il pulsante destro del mouse su **Risorse del computer** e scegliere **Proprietà**.
- 5. Nella finestra di dialogo Proprietà Risorse del computer fare clic sulla scheda **Protezione COM**.

My Computer P	roperties			8	X
General		Options	Defa	ault Properties	
Default P	rotocols	COM Sec	urity	MSDT	
Access Per	missions				— II
You may also set li	edit who is allo imits on applica	owed default acco ations that determ	ess to applic ine their ow	cations. You m n permissions.	ay
Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.					
		Edit Limits	E	dit Default	
-Launch and	Launch and Activation Permissions				
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	E	dit Default	
Learn more about <u>setting these properties</u> .					
		ОК	Cance	I Ap	ply

- 6. In Autorizzazioni di avvio e attivazione fare clic su Modifica limiti.
- 7. Nella finestra di dialogo Autorizzazioni di avvio e attivazione eseguire la procedura seguente se il proprio nome o il proprio gruppo non è visualizzato nell'elenco Gruppi o nomi utente:

Nella finestra di dialogo Autorizzazioni di avvio e attivazione fare clic su Aggiungi.

Nella finestra di dialogo Seleziona utenti, computer o gruppi immettere il proprio nome e il gruppo nel campo Immettere i nomi degli oggetti da selezionare e quindi fare clic su **OK**.

8. Nella finestra di dialogo Autorizzazione di avvio e attivazione selezionare l'utente e il gruppo

nella sezione Utenti e gruppi.

Security Limits Group or user names:	Launch and Activation Permission		8 23			
Group or user names:	Security Limits					
Image: Severyone Image: Administrators (TS-WIN7\Administrators) Image: Performance Log Users (TS-WIN7\Performance Log Users) Image: Distributed COM Users (TS-WIN7\Distributed COM Users) Image: Add Remove Add Remove Image: Performance Log Users (TS-WIN7\Distributed COM Users) Image: Add Remove Image: Permissions for Everyone Allow Deny Local Launch Image: Remote Launch Image: Local Activation Remote Activation Image: Remote Activation Image: Learn about access control and permissions	Group or user names:					
Administrators (TS-WIN7\Administrators) Performance Log Users (TS-WIN7\Performance Log Users) Distributed COM Users (TS-WIN7\Distributed COM Users) Add Remove Permissions for Everyone Allow Deny Local Launch Remote Launch Local Activation Remote Activation Local Activation Leam about access control and permissions	& Everyone					
Performance Log Users (TS-WIN7/Performance Log Users) Distributed COM Users (TS-WIN7/Distributed COM Users) Add Remove Permissions for Everyone Allow Deny Local Launch Remote Launch Local Activation Remote Activation Leam about access control and permissions	Administrators (TS-WIN7\Ad	ministrators)				
Add Remove Permissions for Everyone Allow Deny Local Launch Remote Launch Local Activation Remote Activation	Performance Log Users (15- Reformance Log Users (15-	Performance Log Users (TS-WIN7\Performance Log Users)				
Add Remove Permissions for Everyone Allow Deny Local Launch Image: Control and permissions Remote Activation Image: Control and permissions						
Add Remove Permissions for Everyone Allow Deny Local Launch Image: Control and permissions Image: Control and permissions						
Permissions for Everyone Allow Deny Local Launch Image: Control and permissions Remote Launch Image: Control and permissions		Add	Remove			
Local Launch Remote Launch Local Activation Remote Activation Remote Activation Leam about access control and permissions	Permissions for Everyone	Allow	Deny			
Remote Launch Local Activation Remote Activation Image: Control and permissions	Local Launch					
Local Activation Remote Activation Remote Activation Image: Control and permissions	Remote Launch	\checkmark				
Remote Activation Leam about access control and permissions	Local Activation					
Leam about access control and permissions	Remote Activation	\checkmark				
Leam about access control and permissions						
Leam about access control and permissions						
Learn about access control and permissions						
	Leam about access control and permissions					
OK Cancel		ОК	Cancel			

- 9. Nella colonna Consenti in Autorizzazioni per l'utente selezionare le caselle di controllo Avvio remoto e Attivazione remota e quindi fare clic su OK.Nota: Un nome utente deve disporre dei diritti per eseguire query sui dati di accesso utente in un server AD. Per eseguire l'autenticazione con un utente tramite proxy, immettere un nome utente completo. Per impostazione predefinita, il campo Dominio viene compilato automaticamente dal dominio dell'account utilizzato per accedere al computer in cui è stato installato l'agente. Se l'utente specificato è membro di un dominio diverso, aggiornare il dominio per le credenziali utente fornite.
- 10. Se il problema persiste, nel controller di dominio provare ad aggiungere l'utente nel criterio Gestione registro di controllo e di protezione. Per aggiungere l'utente, attenersi alla seguente procedura:

Scegliere l'Editor Gestione Criteri di gruppo.

Scegliere Configurazione computer > Impostazioni di Windows > Impostazioni protezione > Criteri locali > Assegnazione diritti utente.

Scegliere Gestisci registro di controllo e di protezione.

Aggiungere l'utente.

🧉 Group Policy Management Editor 📃 🗖 💌						
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 Policies Local Policies Security Options Event Log Restricted Groups System Services System Services Wired Network (IEEE 802.3) Policies Windows Firewall with Advanced Set 	=	Policy Import of the system Import of the system performance Import of the system performance Import of the system Import of the system	Policy Setting Server Operato IIS APPPOOL\C Not Defined Administrators Print Operators Not Defined Performance L Not Defined Administrators Not Defined Administrators Not Defined Administrators Not Defined Administrators Not Defined Administrators IIS APPPOOL\C Server Operato			
 Wireless Network (IEEE 802.11) Polic Public Key Policies 	~	Synchronize directory service data	Not Defined			
< III >		< 111	>			