Erteilen von Mindestberechtigungen für ein Active Directory-Benutzerkonto, das vom Sourcefire Benutzer-Agent verwendet wird

### Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Überprüfen Fehlerbehebung

## Einführung

In diesem Dokument wird beschrieben, wie einem Active Directory-Benutzer (AD) die minimalen Berechtigungen für die Abfrage des AD-Domänencontrollers bereitgestellt werden. Der Sourcefire User Agent verwendet einen AD-Benutzer, um den AD-Domänen-Controller abzufragen. Zum Durchführen einer Abfrage sind für einen AD-Benutzer keine zusätzlichen Berechtigungen erforderlich.

### Voraussetzungen

### Anforderungen

Cisco verlangt, dass Sie den Sourcefire User Agent auf einem Microsoft Windows-System installieren und Zugriff auf den AD-Domänen-Controller gewähren.

#### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

### Konfigurieren

Zunächst muss ein Administrator einen neuen AD-Benutzer speziell für den Benutzeragentenzugriff erstellen. Wenn dieser neue Benutzer kein Mitglied der Gruppe der Domänenadministratoren ist (und dies sollte auch nicht sein), muss dem Benutzer möglicherweise explizit die Berechtigung für den Zugriff auf die WMI-Sicherheitsprotokolle (Windows Management Instrumentation) erteilt werden. Gehen Sie wie folgt vor, um die Berechtigung zu erteilen:

1. Öffnen Sie die WMI-Steuerungskonsole:

Wählen Sie auf dem AD-Server das Start-Menü aus.

Klicken Sie auf Ausführen und geben Sie wmimgmt.msc ein.

Klicken Sie auf OK. Die WMI-Steuerungskonsole wird angezeigt.



- 2. Klicken Sie in der WMI-Konsolenstruktur mit der rechten Maustaste auf **WMI-Steuerung** und klicken Sie dann auf **Eigenschaften**.
- 3. Klicken Sie auf die Registerkarte Sicherheit.
- 4. Wählen Sie den Namespace aus, für den Sie einem Benutzer oder einer Gruppe Zugriff gewähren möchten (Root\CIMV2), und klicken Sie dann auf **Sicherheit**.

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. Klicken Sie im Dialogfeld "Sicherheit" auf Hinzufügen.

Group or user names:		
Authenticated Users		
Service		
METWORK SERVICE		
Machinistrators (TS-WIN/	'\Administrators)	
		D
	Add	Remove
Permissions	Allow	Deny
Execute Methods		· · ·
Full Write		=
Partial Write		
Provider Write		
Enable Account		-
For special permissions or adv	vanced settings	
click Advanced.		Advanced

- 6. Geben Sie im Dialogfeld Benutzer, Computer oder Gruppen auswählen den Namen des Objekts (Benutzer oder Gruppe) ein, das Sie hinzufügen möchten. Klicken Sie auf Namen überprüfen, um Ihren Eintrag zu überprüfen, und klicken Sie dann auf OK. Möglicherweise müssen Sie den Speicherort ändern oder auf Erweitert klicken, um Objekte abzufragen. Weitere Informationen finden Sie in der kontextsensitiven Hilfe (?).
- 7. Wählen Sie im Dialogfeld "Sicherheit" im Abschnitt "Berechtigungen" die Option Zulassen oder Verweigern, um Berechtigungen für den neuen Benutzer oder die neue Gruppe zu erteilen (am einfachsten alle Berechtigungen). Dem Benutzer muss mindestens die Berechtigung Remote Enable (Fernzugriff aktivieren) erteilt werden.
- 8. Klicken Sie auf Apply, um die Änderungen zu speichern. Schließen Sie das Fenster.

# Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Wenn nach den Konfigurationsänderungen ein Problem weiter besteht, aktualisieren Sie die DCOM-Einstellungen (Distributed Component Object Model), um den Remotezugriff zu ermöglichen:

- 1. Wählen Sie das Menü Start aus.
- 2. Klicken Sie auf Ausführen und geben Sie DCOMCNFG ein.
- 3. Klicken Sie auf OK. Das Dialogfeld Komponentendienste wird angezeigt.



- 4. Erweitern Sie im Dialogfeld Komponentendienste die **Komponentendienste**, erweitern Sie **Computer**, und klicken Sie dann mit der rechten Maustaste auf **Arbeitsplatz**, und wählen Sie **Eigenschaften aus**.
- 5. Klicken Sie im Dialogfeld Eigenschaften von Arbeitsplatz auf die Registerkarte **COM**-**Sicherheit**.

My Computer Properties 2					
General         Options         Default 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 Edit Default					
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 Edit Default					
Learn more about setting these properties.					
OK Cancel Apply					

- 6. Klicken Sie unter "Berechtigungen für Starten und Aktivierung" auf Grenzen bearbeiten.
- 7. Führen Sie im Dialogfeld "Genehmigung für das Starten und die Aktivierung" die folgenden Schritte aus, wenn Ihr Name oder Ihre Gruppe nicht in der Liste "Gruppen" oder "Benutzernamen" angezeigt wird:

Klicken Sie im Dialogfeld "Berechtigungen für Starten und Aktivierung" auf Hinzufügen.

Geben Sie im Dialogfeld Benutzer, Computer oder Gruppen auswählen im Feld Geben Sie die zu verwendenden Objektnamen ein Ihren Namen und die Gruppe ein, und klicken Sie dann auf **OK**.

8. Wählen Sie im Dialogfeld "Launch and Activation Permission" (Genehmigung für Starten und Aktivierung) im Abschnitt **Gruppen- oder Benutzernamen** Ihren Benutzer und Ihre Gruppe aus.

aunch and Activation Permissio	n	8 23		
Security Limits				
Group or user names:				
& Everyone				
Administrators (TS-WIN7\A	dministrators)			
Performance Log Users (TS-WIN7\Performance Log Users)				
Distributed COM Users (13-WIN7 (Distributed COM Users)				
	Add	Remove		
Permissions for Everyone	Allow	Deny		
Local Launch				
Remote Launch	<b>v</b>			
Local Activation				
Remote Activation	<b>v</b>			
Learn about access control and	Learn about access control and permissions			
	OK	Canaal		

- 9. Aktivieren Sie in der Spalte Zulassen unter Berechtigungen für Benutzer die Kontrollkästchen Remote Launch and Remote Activation (Remote-Start und Remote-Aktivierung), und klicken Sie dann auf OK.Hinweis: Ein Benutzername muss über Rechte zum Abfragen von Benutzeranmeldeinformationen auf einem AD-Server verfügen. Um sich bei einem Benutzer über Proxy zu authentifizieren, geben Sie einen vollqualifizierten Benutzernamen ein. Standardmäßig füllt die Domäne für das Konto, mit dem Sie sich bei dem Computer anmelden, auf dem der Agent installiert ist, automatisch das Feld Domäne ein. Wenn ein von Ihnen bereitgestellter Benutzer Mitglied einer anderen Domäne ist, aktualisieren Sie die Domäne für die angegebenen Benutzeranmeldeinformationen.
- 10. Wenn das Problem weiterhin besteht, versuchen Sie auf dem Domänen-Controller, den Benutzer in der Richtlinie für Überwachungs- und Sicherheitsprotokolle verwalten hinzuzufügen. Gehen Sie wie folgt vor, um den Benutzer hinzuzufügen:

Wählen Sie den Gruppenrichtlinienverwaltungs-Editor aus.

Wählen Sie Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment (Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Benutzerrechtszuweisung) aus.

Wählen Sie Audit- und Sicherheitsprotokoll verwalten aus.

Fügen Sie den Benutzer hinzu.

🧾 Grou	up	Policy Management Editor			x
File Action View Help					
🗢 🔿 📶 🗙 🖾 📑 🔟 🖬					
<ul> <li>Default Domain Controllers Policy</li> <li>Computer Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Name Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> <li>Security Settings</li> <li>Account Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Security Options</li> <li>Security Options</li> <li>System Services</li> <li>Registry</li> <li>Registry</li> <li>File System</li> <li>Wired Network (IEEE 802.3) Policies</li> <li>Windows Firewall with Advanced Sc</li> <li>Network List Manager Policies</li> </ul>		Policy         Policy         Generate security audits         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         Restore files and directories         Shut down the system         Synchronize directory service data	Policy S Server ( IIS APPI Not Del Admini Print O Not Del Perform Not Del Admini Not Del Admini	Setting Operato POOL\ fined fined strators perator fined strators fined istrators fined istrators fined operator POOL\ Operator fined	
< III >	~	C Take ownership of files or other objects	Admini	istrator >	s ~