向Sourcefire使用者代理使用的Active Directory使用者帳戶授予最低許可權

目錄

<u>簡介</u> <u>必要條件</u> <u>需求用元件</u> 設設 設 難 排解

簡介

本文檔介紹如何為Active Directory(AD)使用者提供查詢AD域控制器所需的最低許可權。 Sourcefire使用者代理使用AD使用者來查詢AD域控制器。為了執行查詢,AD使用者不需要任何其 他許可權。

必要條件

需求

思科要求您在Microsoft Windows系統上安裝Sourcefire使用者代理並提供對AD域控制器的訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

首先,管理員必須專門為使用者代理訪問建立新的AD使用者。如果此新使用者不是域管理員組的成員(他們不應是),則可能需要明確授予該使用者訪問Windows Management Instrumentation(WMI)安全日誌的許可權。若要授予許可權,請完成以下步驟: 1. 開啟WMI控制控制檯:

在AD伺服器上,選擇Start選單。

按一下「Run」,然後輸入wmimgmt.msc。

按一下「OK」(確定)。出現WMI控制控制檯。



2. 在WMI控制檯樹上,按一下右鍵WMI Control,然後按一下Properties。

3. 按一下Security頁籤。

4. 選擇要授予使用者或組訪問許可權的名稱空間(Root \CIMV2),然後按一下Security。

WMI Control (Local) Properties	9	23			
General Backup/Restore Security Advanced					
Namespace navigation allows you to set namespace specific set	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. 在「安全」對話方塊中,按一下**新增**。

Group or user names:			
& Authenticated Users			
Service Local Service			
Service			
Machinistrators (TS-WIN7)	Administrators)		
	Add	Remove	
Permissions	Allow	Deny	
Execute Methods		· · ·	
Full Write		=	
Partial Write			
Provider Write			
Enable Account		-	
For special permissions or adva	anced settings.	Adversed	
click Advanced.		Advanced	
Learn about access control and normissions			

- 6. 在選擇使用者、電腦或組對話方塊中,輸入要新增的對象(使用者或組)的名稱。按一下「 Check Names」以驗證您的輸入,然後按一下「OK」。您可能必須更改位置或按一下高級才 能查詢對象。有關詳細資訊,請參閱上下文相關幫助(?)。
- 7. 在「安全」對話方塊的「許可權」部分中,選擇**允許**或**拒絕**以向新使用者或組授予許可權(最 容易授予所有許可權)。 必須至少為使用者提供遠端啟**用許可權**許可權。

8. 按一下「Apply」以儲存變更。關閉視窗。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

如果在配置更改後問題仍然存在,請更新分散式元件對象模型(DCOM)設定以允許遠端訪問:

- 1. 選擇Start選單。
- 2. 按一下Run並輸入DCOMCNFG。
- 3. 按一下「OK」(確定)。此時將出現「元件服務」對話方塊。

Component Services				
🍋 File Action View Window Help				
Console Root Component Services Computers My Computer Event Viewer (Local) Services (Local)	Name COM+ Applications COM+ Applications COM+ Config Running Processes Distributed Transaction Coordi	Actions My Computer More Actions		

- 4. 在「元件服務」對話方塊中,展開**元件服務**,展開**電腦**,然後按一下右鍵**我的電腦**,然後選擇 **屬性**。
- 5. 在「My Computer Properties(我的電腦屬性)」對話方塊中,按一下「**COM Security(COM安全)」**頁籤。

My Computer Prop	perties		-	8	X
General		Options	Defa	ault Properties	
Default Prot	ocols	COM Sec	urity	MSDT	С
Access Permis	sions				
You may ed also set limit	it who is allo s on applica	wed default acce tions that determ	ess to applic ine their ow	ations. You m n permissions	iay
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 A	ctivation Pe	missions			
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 <u>setting these properties</u> .					
		ОК	Cance	Ap	ply

- 6. 在「啟動和啟用許可權」下,按一下「編輯限制」。
- 7. 如果您的姓名或您的組未顯示在「組或使用者名稱」清單中,請在「啟動和啟用許可權」對話 方塊中完成以下步驟:

在「啟動和啟用許可權」對話方塊中,按一下新增。

在「選擇使用者、電腦或組」對話方塊的「輸入要選擇的對象名稱」欄位中輸入您的姓名和組 ,然後按一下**確定**。

8. 在「啟動和啟用許可權」對話方塊中,在「組或使用者名稱」部分選擇您的使用者和組。

Launch and Activation Permission				
Security Limits				
Group or user names:				
& Everyone				
Administrators (TS-WIN7\Administrators)	ministrators)			
Performance Log Users (TS-	VIN7\Performance Lo VIN7\Distributed CON	og Users)		
	Add	Remove		
Permissions for Everyone	Allow	Deny		
Local Launch				
Remote Launch				
Local Activation				
Remote Activation	V			
Learn about access control and permissions				
OK Cancel				

- 9. 在「使用者許可權」下的「允許」列中,選中Remote Launch和Remote Activation覈取方塊 ,然後按一下OK。附註:使用者名稱必須具有在AD伺服器上查詢使用者登入資料的許可權。 若要透過代理與使用者進行驗證,請輸入完全限定使用者名稱。預設情況下,用於登入到安裝 代理的電腦中的帳戶的域會自動填充「域」欄位。如果您提供的使用者是其他域的成員,請為 提供的使用者憑據更新域。
- 10. 如果問題仍然存在,請在域控制器上嘗試在「管理稽核和安全日誌」策略中新增使用者。要 新增使用者,請完成以下步驟:

選擇**組策略管理編輯器**。

選擇Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment。

選擇管理稽核和安全日誌。

新增使用者。

J Gro	up	Policy Management Editor	_ _ ×			
File Action View Help						
Default Domain Controllers Policy Computer Configuration Policies Software Settings Software Settings Scripts (Startup/Shutdown) Scripts (Startup/Shutdown) Security Settings Account Policies Account Policies Account Policies Account Policies Account Policies Security Options Security Options Security Options System Services System Services System Services Windows Firewall with Advanced Security Check and Security Intervent (IEEE 802.3) Policies Vindows Firewall with Advanced Security Check and Security Check and Security Policies Windows Firewall with Advanced Security Check and Security Check		Policy Policy Force shutdown from a remote system 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 Take ownershin of files or other objects.	Policy Setting Server Operato IIS APPPOOL\D Not Defined Administrators Print Operators Not Defined Administrators Not Defined Administrators Not Defined Administrators Not Defined Administrators IIS APPPOOL\D Server Operato Print Operators Not Defined Administrators IIS APPPOOL\D Server Operato Print Operators Not Defined Administrators			
	_					