# 向Sourcefire用户代理使用的Active Directory用户 帐户授予最低权限

### 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 配置 验证 故障排除

# 简介

本文档介绍如何向Active Directory(AD)用户提供查询AD域控制器所需的最小权限。Sourcefire用户 代理使用AD用户来查询AD域控制器。要执行查询,AD用户不需要任何附加权限。

# 先决条件

#### 要求

思科要求您在Microsoft Windows系统上安装Sourcefire用户代理,并提供对AD域控制器的访问。

#### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

### 配置

首先,管理员必须专门为用户代理访问创建新的AD用户。如果此新用户不是域管理员组的成员(而 且不应是),则可能必须明确授予该用户访问Windows Management Instrumentation(WMI)安全日 志的权限。要授予权限,请完成以下步骤:

1. 打开WMI控制台:

在AD服务器上,选择"开始"菜单。

单击Run,然后输入wmimgmt.msc。

Click OK.系统将显示WMI控制台。



2. 在WMI控制台树上,右键单击WMI控件,然后单击属性。

3. 单击"Security"选项卡。

4. 选择要为其授予用户或组访问权限的命名空(Root\CIMV2),然后单击Security。

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. 在"安全"对话框中,单击"**添加"**。

Group or user names:		
& Authenticated Users		
Service Local Service		
Service		
Administrators (TS-WIN7\Administrators)		
	Add	Remove
Permissions	Allow	Deny
Execute Methods		<b>^</b>
Full Write		=
Partial Write		
Provider Write		
Enable Account		-
For special permissions or advar	ced settings	
click Advanced.		Advanced

- 6. 在选择用户、计算机或组对话框中,输入要添加的对象(用户或组)的名称。单击Check Names(检查名称)以验证您的条目,然后单击OK(确定)。您可能必须更改位置或单击"高级"以查询对象。有关详细信息,请参阅上下文相关帮助(?)。
- 7. 在"安全"对话框的"权限"部分,选择**允许**或**拒绝**,以便向新用户或组授予权限(最容易授予所 有权限)。 必须至少为用户授予"远程启**用"**权限。

8. 单击Apply以保存更改。关闭窗口。

### 验证

当前没有可用于此配置的验证过程。

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

如果配置更改后问题仍然存在,请更新分布式组件对象模型(DCOM)设置以允许远程访问:

- 1. 选择"开**始"**菜单。
- 2. 单击Run并输入DCOMCNFG。
- 3. Click OK.系统将显示"组件服务"对话框。



4. 在"组件服务"对话框中,展开**组件服务**,展开**计算机**,然后右键单击**我的计算机**并选择**属性**。

5. 在"我的计算机属性"对话框中,单击"COM安全"选项卡。

My Computer P	properties		-	8	X
General		Options	Defa	ault Properties	
Default F	rotocols	COM Sec	urity	MSDT	
- Access Per	missions				— II
You may also set l	edit who is allo limits on applica	wed default acco ations that determ	ess to applic ine their ow	cations. 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	d Activation 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	E	dit Default	
Learn more about setting these properties.					
		ОК	Cance		ply

- 6. 在"启动和激活权限"下,单击编辑限制。
- 7. 在"启动和激活权限"对话框中,如果您的姓名或组未出现在"组"或"用户名"列表中,请完成以下 步骤:

在启动和激活权限对话框中,单击添加。

在"选择用户、计算机或组"对话框中,在"输入要选择的对象名称"字段中输入您的名称和组 ,然后单击"确**定"**。

8. 在"启动和激活权限"对话框中,在"组"或"用户名"部**分中选择您的用户**和组。

Launch and Activation Permission				
Security Limits				
Group or user names:				
& Everyone				
Administrators (TS-WIN7\Administrators (TS-WIN7\Administrators)	ninistrators) MINZ Performance Lo			
Performance Log Users (TS-WIN/\Performance Log Users)				
		-		
	Add	Remove		
Permissions for Everyone	Allow	Deny		
Local Launch				
Remote Launch				
Local Activation Remote Activation				
Learn about access control and permissions				
OK Cancel				

- 9. 在"用户权限"下的"允许"列中,选中"远程启动"和"远程激活"复选框,然后单击确定。注意:用 户名必须具有在AD服务器上查询用户登录数据的权限。要通过代理向用户进行身份验证,请 输入完全限定的用户名。默认情况下,用于登录安装代理的计算机的帐户的域会自动填充"域 "字段。如果您提供的用户是不同域的成员,请更新提供的用户凭据的域。
- 10. 如果问题仍然存在,请在域控制器上尝试在管理审核和安全日志策略中添加用户。要添加用 户,请完成以下步骤:

#### 选择组策**略管理编辑器**。

选择"计算机配置">"Windows设置">"安全设置">"本地策略">"用户权限分配"。

选择Manage auditing and security log。

添加用户。

J Gro	up	Policy Management Editor	_ <b>_</b> ×
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
	_		