# Sourcefire ユーザ エージェントが使用する Active Directory ユーザ アカウントに最小限の権 限を付与する

### 内容

<u>既要</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>設定</u>
<u>確認</u>
トラブルシュート

### 概要

このドキュメントでは、ADドメインコントローラーのクエリに必要な最小限のアクセス許可を Active Directory (AD)ユーザーに与える方法について説明します。Sourcefire User Agentは、ADド メインコントローラーのクエリにADユーザーを使用します。クエリーを実行するには、AD ユー ザに追加の権限は必要ありません。

## 前提条件

#### 要件

Microsoft Windows システムに Sourcefire ユーザ エージェントをインストールし、AD ドメイン コントローラへのアクセスを提供する必要があります。

#### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの ではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

# 設定

最初に、管理者がユーザ エージェント アクセス専用の新しい AD ユーザを作成する必要がありま す。この新しいユーザがドメイン管理者グループのメンバでない場合(およびメンバであっては ならない場合)、Windows Management Instrumentation(WMI)セキュリティ ログへのアクセ ス権限をユーザに明示的に与える必要が生じることがあります。権限を付与するには、次の手順 を完了します。

1. 次のように WMI コントロール コンソールを開きます。

AD サーバで [Start] メニューを選択します。

[Run] をクリックして wmimgmt.msc と入力します。

[OK] をクリックします。WMI コントロール コンソールが表示されます。



- 2. WMI コンソール ツリーで [WMI Control] を右クリックして、[Properties] をクリックします。
- 3. [Security] タブをクリックします。
- 4. ユーザまたはグループにアクセスを与える対象の名前空間を選択して(Root\CIMV2)、 [Security] をクリックします。

WMI Control (Local) Properties	9	23
General Backup/Restore Security Advanced		
Namespace navigation allows you to set namespace specific sec	curity.	
Root   Image: SecurityCenter   Image: SecurityCenter <tr< th=""><th></th><th></th></tr<>		
Sec	urity	
OK Cancel	App	ply

5. [Security] ダイアログボックスで [Add] をクリックします。

county			
Group or user names:			
🍇 Authenticated Users			
Service Local Service			
METWORK SERVICE			
Machinistrators (TS-WIN)	∕\Administrators)		
	Add	Remove	
	huu	Hellove	
Permissions	Allow	Deny	
Execute Methods		· ·	
Full Write		=	
Partial Write			
Provider Write			
Enable Account		-	
For special permissions or adv	vanced settings,	Advanced	
click Advanced.	-	Auvanceu	
l earn about access control and permissions			

- 6. [Select Users, Computers, or Groups] ダイアログボックスでは、追加するオブジェクト(ユーザまたはグループ)の名前を入力します。入力内容を検証するために [Check Names] を クリックして、[OK] をクリックします。オブジェクトをクエリーするために、場所を変更 するか [Advanced] をクリックする必要が生じることもあります。詳しくは、状況依存ヘル プ(?)を参照してください。
- [Security] ダイアログボックスの [Permissions] セクションで、新しいユーザまたはグループ に権限を与えるために [Allow] または [Deny] を選択します(すべての権限を与えるのが最も 簡単です)。 少なくとも [Remote Enable] 権限をユーザに与える必要があります。
- 8. 変更を保存するには [Apply] をクリックします。ウィンドウを閉じます。

### 確認

現在、この設定に使用できる確認手順はありません。

# トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

設定を変更した後に引き続き問題が発生する場合は、リモート アクセスを許可するために分散 COM(DCOM)設定を更新してください。

- 1. [Start] メニューを選択します。
- 2. [Run] をクリックして DCOMCNFG と入力します。
- 3. [OK] をクリックします。[Component Services] ダイアログボックスが表示されます。

Omponent Services			- • ×		
Eile Action View Window Help					
♦ 2 □ × □ 4 ≥					
Console Root Component Services Computers File My Computer Event Viewer (Local) Console Root Services (Local)	lame COM+ Applications DCOM Config Running Processes Distributed Transaction Coordi	Actions My Comput More Ad	er 🔺		
		])			

- 4. [Component Services] ダイアログボックスで、[Component Services] および [Computers] の 順に展開し、[My Computer] **を右クリックして [Properties] を選択します。**
- 5. [My Computer Properties] ダイアログボックスで、[COM Security] タブをクリックします。

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 l	edit who is allo imits on applica	wed default acco ations that determ	ess to applic ine their ow	cations. You m n permissions.	lay
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 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	Ap	ply

- 6. [Launch and Activation Permissions] の下で、[Edit Limits] をクリックします。
- 7. [Launch and Activation Permission] ダイアログボックスで、グループまたはユーザ名のリストに名前やグループが表示されない場合には次の手順を完了します。

[Launch and Activation Permission] ダイアログボックスで [Add] をクリックします。

[Select Users, Computers, or Groups] ダイアログボックスで、[Enter the object names to select] フィールドに名前とグループを入力して、[OK] をクリックします。

8. [Launch and Activation Permission] ダイアログボックスの [Group or user names] セクショ

ンでユーザとグループを選択します。

aunch and Activation Permission	1	ନ	23	
Security Limits				
Group or user names:				
& Everyone				
Administrators (TS-WIN7\Ad	lministrators)			
Reformance Log Users (TS	-WIN7\Performance	e Log Use	rs)	
COM Users (15-		UNI Users		
	Add	Remov	/e	
Permissions for Everyone	Allow	Deny		
Local Launch				
Remote Launch	<b>v</b>			
Local Activation				
Remote Activation				
Learn about access control and permissions				
	1 1 1			

- [Permissions for User] の下の [Allow] カラムで、[Remote Launch] および [Remote Activation] チェックボックスをオンにして [OK] をクリックします。注:ユーザ名には、AD サーバでユーザ ログイン データをクエリーする権限が必要です。プロキシを介してユーザ を認証するには、完全修飾ユーザ名を入力します。デフォルトでは、エージェントのインストール場所のコンピュータへのログインで使用したアカウントのドメインが [Domain] フィールドに自動的に入力されます。異なるドメインのメンバーをユーザとして指定する場合、提供するユーザ クレデンシャルのドメインを更新してください。
- 10. 問題が引き続き発生する場合、ドメイン コントローラで、[Manage auditing and security log] ポリシーにユーザを追加してみてください。ユーザを追加するには、次の手順を完了 します。

[Group Policy Management Editor]を選択します。

[Computer Configuration] > [Windows Settings] > [Security Settings] > [Local Policies] > [User Rights Assignment] を選択します。

[Manage auditing and security log] を選択します。

ユーザを追加します。

If Group Policy Management Editor			_ <b>_</b> X		
File Action View Help	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>Windows Settings</li> <li>Name Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> <li>Security Settings</li> <li>Local Policies</li> <li>Local Policies</li> <li>Audit Policy</li> <li>User Rights Assignment</li> <li>Security Options</li> </ul>	< III	Policy         Image: Porce shutdown from a remote system         Image: Porce shutdown from a remote system         Image: Porcess security audits         Image: Porcess security provide the porcess security porcess         Image: Porcess security porcess         Image: Porcess porcess         Image: Porcess porcess         Image: Porcess porcess         Image: Porcess         Imag	Policy Setting Server Operato IIS APPPOOL\C Not Defined Administrators Print Operators Not Defined Performance Lo Not Defined Administrators Not Defined		
Event Log     Event Log     Event Log     Action Services     System Services     Services	<	Modify firmware environment values Perform volume maintenance tasks Profile single process Profile system performance Remove computer from docking station Replace a process level token Restore files and directories Shut down the system Synchronize directory service data Take ownershin of files or other objects	Administrators Not Defined Administrators NT SERVICE\W Administrators IIS APPPOOL\D Server Operato Print Operators Not Defined Administrators >		