Conceder permiso mínimo a una cuenta de usuario de Active Directory utilizada por el agente de usuario de Sourcefire

### Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Verificación Troubleshoot

## Introducción

Este documento describe cómo proporcionar a un usuario de Active Directory (AD) los permisos mínimos necesarios para consultar el controlador de dominio AD. El agente de usuario de Sourcefire utiliza un usuario AD para consultar el controlador de dominio AD. Para realizar una consulta, un usuario de AD no requiere permisos adicionales.

### Prerequisites

#### Requirements

Cisco requiere que instale el agente de usuario de Sourcefire en un sistema Microsoft Windows y proporcione acceso al controlador de dominio AD.

#### **Componentes Utilizados**

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configurar

En primer lugar, un administrador debe crear un nuevo usuario AD específicamente para el acceso de agente de usuario. Si este nuevo usuario no es miembro del grupo de administradores de dominio (y no debería serlo), es posible que se deba conceder explícitamente al usuario permiso para acceder a los registros de seguridad de Windows Management Instrumentation (WMI). Para conceder permiso, complete estos pasos:

1. Abra la consola de control WMI:

En el servidor AD, elija el menú Inicio.

Haga clic en Ejecutar e ingrese wmimgmt.msc.

Click OK. Aparece la consola de control WMI.



- 2. En el árbol de la consola WMI, haga clic con el botón secundario del mouse en **Control WMI** y, a continuación, haga clic en **Propiedades**.
- 3. Haga clic en la ficha Security (Seguridad).
- 4. Seleccione el espacio de nombres para el que desea otorgar acceso a un usuario o grupo (ROOL\CIMV2) y, a continuación, haga clic en **Security**.

WMI Control (Local) Properties	ବ	23				
General Backup/Restore Security Advanced						
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. En el cuadro de diálogo Seguridad, haga clic en Agregar.

-		
Group or user names:		
& Authenticated Users		
& LOCAL SERVICE		
METWORK SERVICE		
Administrators (TS-WIN/\Administrators)		
	Add	Remove
		nemove
Permissions	Allow	Deny
Execute Methods		<b>^</b>
Full Write		=
Partial Write		
Provider Write		
Enable Account		-
For special permissions or a	dvanced settings.	٨
click Advanced.		Auvanced

- 6. En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, introduzca el nombre del objeto (usuario o grupo) que desea agregar. Haga clic en Verificar nombres para verificar su entrada y luego haga clic en Aceptar. Puede que tenga que cambiar la ubicación o hacer clic en Avanzadas para consultar los objetos. Consulte la ayuda contextual (?) para obtener más información.
- 7. En el cuadro de diálogo Seguridad, en la sección Permisos, elija **Permitir** o **Denegar** para conceder permisos al nuevo usuario o grupo (lo más fácil es otorgar todos los permisos). Se debe dar al usuario al menos el permiso **Remote Enable**.
- 8. Haga clic en Aplicar para guardar los cambios. Cerrar ventana

# Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

### Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Si un problema persiste después de los cambios de configuración, actualice la configuración del Modelo de objetos componentes distribuidos (DCOM) para permitir el acceso remoto:

- 1. Elija el menú Inicio.
- 2. Haga clic en Ejecutar e introduzca DCOMCNFG.
- 3. Click OK. Aparecerá el cuadro de diálogo Servicios de componentes.



- 4. En el cuadro de diálogo Servicios de componentes, expanda **Servicios de componentes**, expanda **Equipos** y, a continuación, haga clic con el botón derecho en **Mi PC** y elija **Propiedades**.
- 5. En el cuadro de diálogo Propiedades de mi equipo, haga clic en la ficha Seguridad COM.

My Computer Properties	8	X			
General Options Defaul	t Properties				
Default Protocols COM Security	MSDTC	;			
Access Permissions					
You may edit who is allowed default access to applicat also set limits on applications that determine their own p	ions. You ma permissions.	ay			
Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.					
Edit Limits	: 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 <u>setting these properties</u> .					
OK Cancel	App	ply			

- 6. En Permisos de inicio y activación, haga clic en Editar límites.
- 7. En el cuadro de diálogo Permiso de inicio y activación, complete estos pasos si su nombre o grupo no aparece en la lista Grupos o nombres de usuario:

En el cuadro de diálogo Permiso de inicio y activación, haga clic en Agregar.

En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, introduzca su nombre y el grupo en el campo Introducir los nombres de objeto para seleccionar y, a continuación, haga clic en **Aceptar**.

8. En el cuadro de diálogo Permiso de inicio y activación, seleccione su usuario y grupo en la sección **Nombres de grupo o de usuario**.

Launch and Activation Permission		8 23			
Security Limits					
Group or user names:					
& Everyone					
Administrators (TS-WIN7\Adm	ninistrators)				
Performance Log Users (TS-WIN/\Performance Log Users)     Reformance Log Users (TS-WIN/\Performance Log Users)					
	Add	Remove			
Permissions for Everyone	Allow	Deny			
Local Launch					
Remote Launch					
Local Activation					
Nemole Activation					
Learn about access control and permissions					
	ОК	Cancel			

- 9. En la columna Permitir en Permisos para usuario, active las casillas de verificación Inicio remoto y Activación remota y, a continuación, haga clic en Aceptar.Nota: Un nombre de usuario debe tener derechos para consultar los datos de inicio de sesión del usuario en un servidor AD. Para autenticarse con un usuario a través de proxy, ingrese un nombre de usuario completamente calificado. De forma predeterminada, el dominio de la cuenta que utilizó para iniciar sesión en el equipo donde instaló el agente rellena automáticamente el campo Dominio. Si un usuario proporcionado es miembro de un dominio diferente, actualice el dominio para las credenciales de usuario proporcionadas.
- 10. Si el problema persiste, en el controlador de dominio intente agregar el usuario en la política Administrar auditoría y registro de seguridad. Para agregar el usuario, complete estos pasos:

Elija el Editor de administración de directivas de grupo.

Elija Computer Configuration > Windows Settings > Security Settings > Local Policies >

User Rights Assignment.

Elija Administrar auditoría y registro de seguridad.

Agregue el usuario.

Group Policy Management Editor			_ 🗆 X					
File Action View Help								
Default Domain Controllers Policy Computer Configuration Policies Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Script	=	Policy Force shutdown from a remote system Generate security audits Impersonate a client after authentication 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	Policy Setting Server Operato IIS APPPOOL\D Not Defined Not Defined Administrators Print Operators Not Defined Performance Lo Not Defined					
	*	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 Replace a process level token Restore files and directories Shut down the system Shut down the system Take ownership of files or other objects	Administrators Not Defined Administrators Not Defined Administrators NT SERVICE\W Administrators IIS APPPOOL\D Server Operato Print Operators Not Defined Administrators >					