Solucionar problemas de acceso denegado " Alerta en el conector de Umbrella AD

Contenido

Introducción

Este documento describe la solución de problemas de "Acceso denegado" cuando el conector de Active Directory (AD) de Cisco Umbrella se encuentra en estados de alerta o error.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

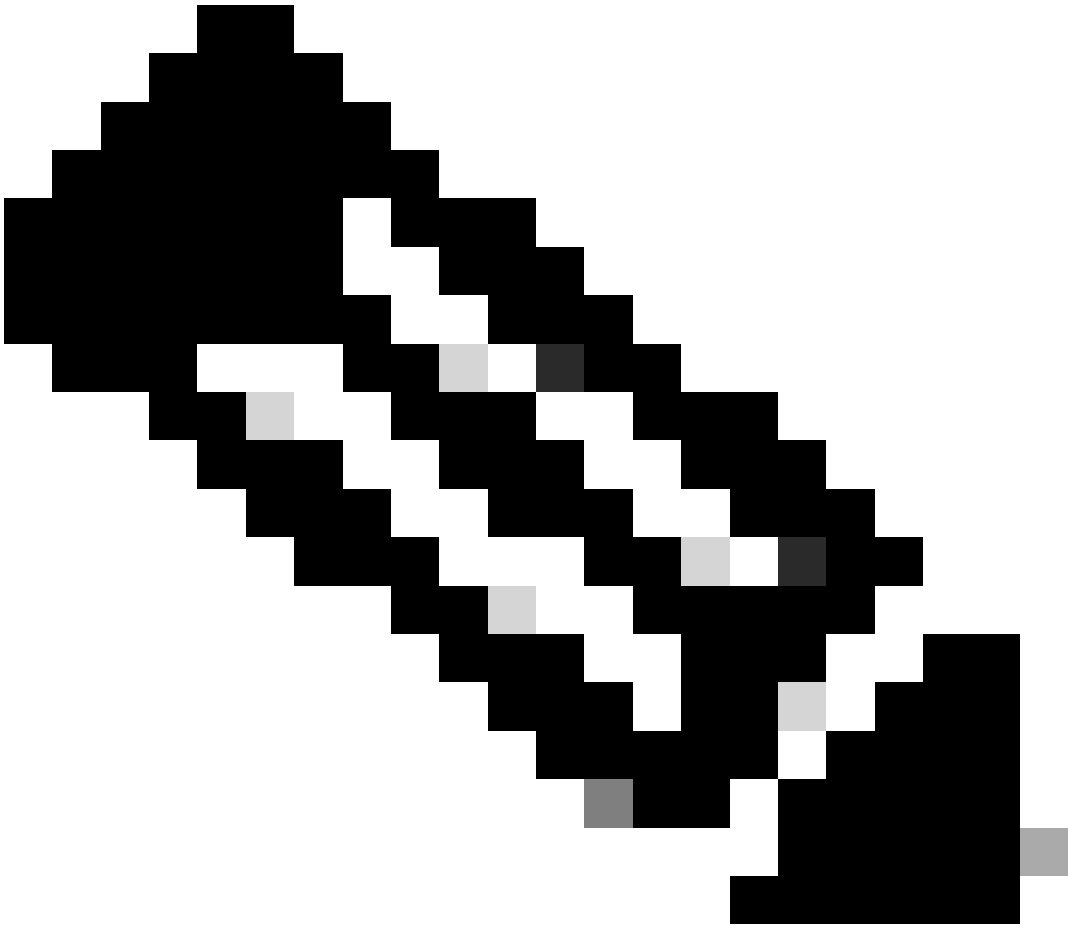
Se da cuenta de que un conector de AD muestra el estado de alerta o error, y el mensaje que aparece cuando se coloca sobre la alerta incluye "Acceso denegado" a uno de los servidores de AD registrados.

Solución

Asegúrese de que el usuario de OpenDNS_Connector sea miembro de estos grupos AD:

- Lectores del registro de eventos
- Usuarios COM distribuidos
- Controladores de dominio de solo lectura empresariales

La solución consiste en asegurarse de que DCOM, WMI y Manage Audit and Security Log estén correctamente configurados en el servidor AD en cuestión.



> Nota: De forma predeterminada, no se admiten varios dominios o bosques. Consulte el anuncio de Multi-AD Domain Support in Umbrella. También puede ponerse en contacto con Umbrella Support para obtener ayuda sobre su configuración si se encuentra con estos problemas.

Para comprobar los permisos WMI:

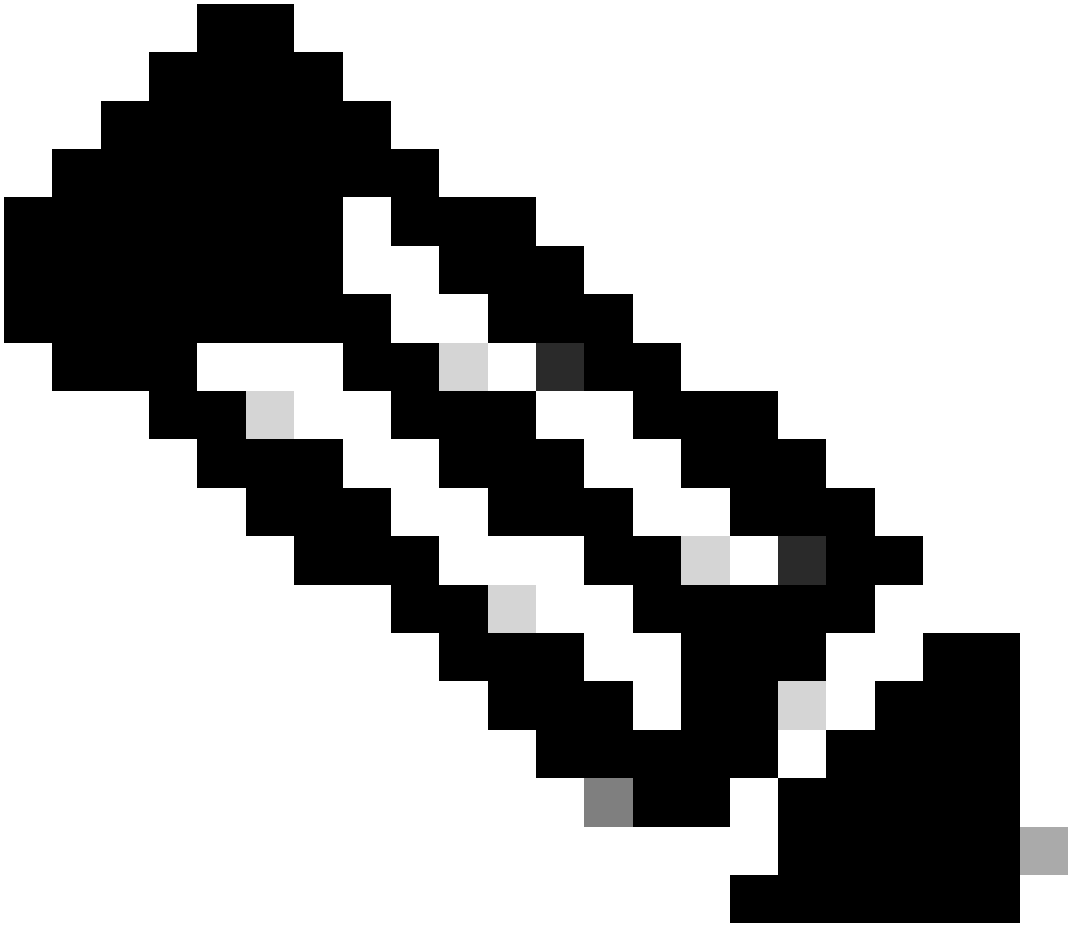
1. Seleccione Inicio > Ejecutar > wmimgmt.msc para acceder a la consola de Control de la

infraestructura de administración de Windows.
2. Haga clic con el botón derecho en Control WMI > Propiedades > ficha Seguridad.
3. Seleccione Root > CIMV2 namespace y seleccione el botón Security.
4. Agregue el usuario OpenDNS_Connector y Permita estos permisos:

- Habilitar cuenta
- Activar remoto
- Leer seguridad

Para comprobar los permisos DCOM:

1. Desde una línea de comandos, ejecute dcomcnfg.
2. Vaya a Raíz de Consola > Servicios de Componentes > Equipos.
3. Haga clic con el botón derecho del ratón en Mi PC y seleccione Propiedades.
4. En Propiedades de Mi PC, seleccione la pestaña Seguridad COM.
5. En la sección Permisos de Inicio y Activación, seleccione Editar Límites.
6. Agregue el usuario OpenDNS_Connector y permita los permisos Inicio remoto y Activación remota.
7. Seleccione Aceptar para confirmar y cerrar Propiedades de Mi PC.



Nota: En la mayoría de los casos, si se realizan cambios en DCOM, es necesario reiniciar el DC para que los cambios surtan efecto.

Para comprobar "Administrar registros de auditoría y seguridad" en servidores con Windows 2003:

1. En un controlador de dominio, abra un símbolo del sistema y escriba este comando (si ejecuta Windows 2003, reemplace /r por /v):

```
gpresult /scope computer /r
```

2. Busque la línea Objetos de política de grupo aplicados. Debajo hay una lista de directivas aplicadas a ese controlador de dominio. Anote uno que se pueda aplicar a todos los controladores de dominio.
(como "Directiva predeterminada de controladores de dominio"). Si no existe ninguno, debe crear

uno y aplicarlo.

Para editar la política adecuada:

3. Abra el panel Administración de directivas de grupo (a través de Inicio/Herramientas administrativas). Seleccione la política que desee. Algo en la carpeta "Controladores de dominio" es un candidato probable.

4. Haga clic con el botón derecho en esa directiva y seleccione Editar para que aparezca el Editor de administración de directivas de grupo.

5. Vaya a la carpeta Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Directivas locales\Asignación de derechos de usuario y seleccione Administrar registro de auditoría y seguridad para ver sus propiedades.

6. Seleccione Definir esta configuración de directiva >Agregar usuario o grupo. Busque y seleccione el usuario OpenDNS_Connector.

7. Ejecute el comando "gpupdate /force" en el controlador de dominio para asegurarse de que se aplica la directiva.

Causa

Este error generalmente indica que el usuario de OpenDNS_Connector no tiene permisos suficientes para operar.

El script Conector de Windows normalmente establece los permisos necesarios para el usuario OpenDNS_Connector. Sin embargo, en entornos AD estrictos, algunos administradores no pueden ejecutar scripts VB en sus controladores de dominio y, por lo tanto, deben replicar manualmente las acciones del script Configuración de Windows.

Additional Information

Para obtener más información sobre cómo resolver este problema, visite Temas completos para resolución de acceso denegado.

Si después de confirmar o cambiar la configuración mencionada, sigue viendo mensajes de "Acceso denegado" en el panel, envíe Asistencia para los registros del conector como se describe en este artículo: Asistencia con los registros del conector de AD.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).