Solución de problemas de Umbrella Insights La integración de AD no detecta el tráfico de usuarios

Contenido

Introducción

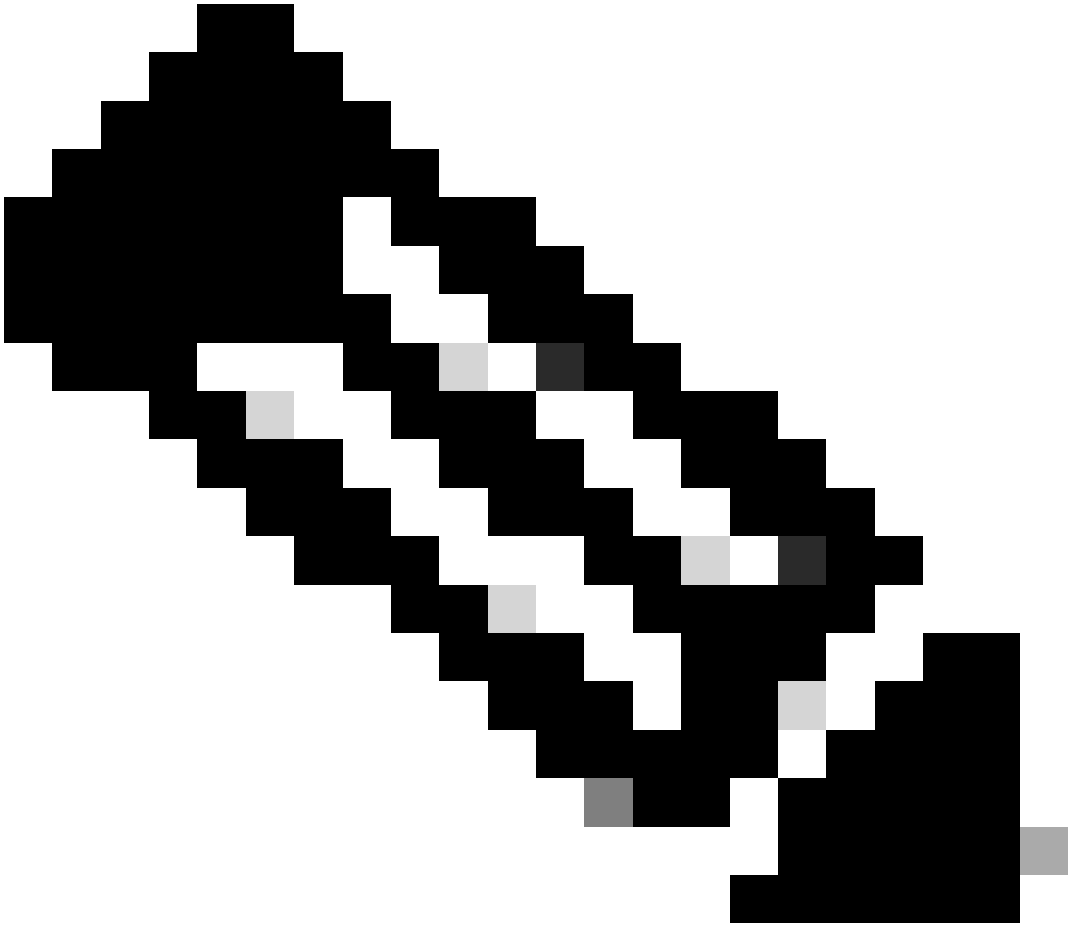
Este documento describe cómo resolver problemas de integración de Umbrella Insights AD sin detectar el tráfico de usuarios.

Overview

Ha instalado Umbrella Insights, ha configurado un conector y dispositivos virtuales y ha registrado sus controladores de dominio. Todos los componentes se muestran en verde y funcionan en el panel en `implementaciones -> Sitios y Active Directory`; sin embargo, tiene una directiva configurada para usar usuarios de AD u objetos de grupo, pero sigue sin ver cómo se informa de la actividad del usuario en el panel o si la directiva se aplica correctamente.

También puede observar en esta entrada repeticiones en el archivo OpenDNSuditClient.log

`Último evento recibido en 1970-01-01 00:00:00`



Nota: El archivo de registro se encuentra en C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\
VERSIÓN = la versión instalada real del servicio Conector, como v1.1.22

Explicación

La razón principal por la que esto sucede es que los eventos de inicio de sesión de auditoría podrían no estar configurados en el dominio de Active Directory. El mensaje de registro indica que el conector no ha visto un solo evento de usuario desde que se instaló. Actualmente, esto no es algo que genere un error en el panel.

Resolución

Lo principal que debe comprobar es la directiva de grupo de AD para la configuración de directiva de auditoría correcta:

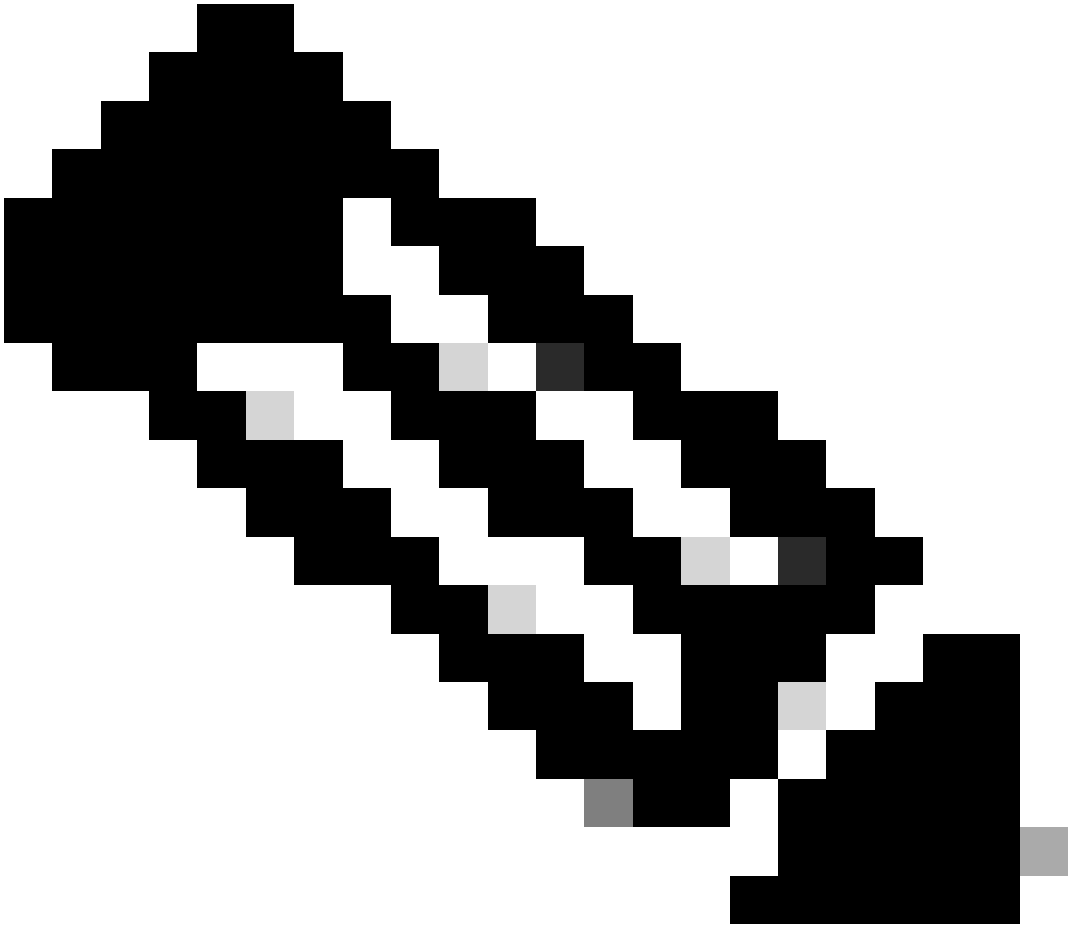
1. En el controlador de dominio, abra el panel Administración de directivas de grupo ubicado en *Herramientas administrativas* y seleccione una directiva que se aplique a los controladores de dominio (la directiva predeterminada del controlador de dominio sería la candidata más probable).

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

3. Vaya a la carpeta "Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Directivas locales\Directiva de auditoría" y seleccione Auditar sucesos de inicio de sesión para ver sus propiedades.

4. Esta directiva debe utilizarse para auditar los intentos de éxito.

5. Ejecute el comando gpupdate para aplicar la política.



Nota: Hay casos en los que es posible que tanto los "Controladores de dominio

---

predeterminados como la Directiva de dominio predeterminada" necesiten tener esa configuración configurada.

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).