Solución de problemas de Umbrella Connector que bloquea una cuenta de servicio de Active Directory

Contenido

[Introducción](#)

[Overview](#)

[Lista de cuentas bloqueadas](#)

[Más información](#)

Introducción

Este documento describe cómo resolver problemas por qué una cuenta de servicio de Active Directory es bloqueada por Umbrella Connector.

Overview

El servicio Umbrella Connector realiza conexiones WMI a los registros de eventos de cualquier controlador de dominio (DC) registrado que forme parte del mismo [sitio Umbrella](#), para leer la información de eventos de inicio de sesión. Estos eventos de inicio de sesión se analizan y se cargan en todos los dispositivos virtuales (VA) en el mismo sitio de Umbrella. A continuación, el AV crea una asignación temporal de usuario a IP para ese nombre de usuario/dirección IP de origen. Hay un par de puntos que vale la pena destacar:

- Umbrella Insights solo admite un usuario conectado por IP a la vez
- El evento de inicio de sesión procesado más recientemente desde una IP de origen "gana"

Como todos los eventos de inicio de sesión son iguales, el conector tiene una lista codificada de cuentas de servicio de AD comunes cuyos eventos se omiten. Puede ver los sucesos de inicio de sesión de estas cuentas recogidos en el archivo de registro del conector. Por ejemplo:

Evento del usuario de la lista negra ignorado: OpenDNS_Connector

Esto se hace para evitar que las cuentas de servicio (que al igual que los usuarios estándar generan eventos de inicio de sesión en los registros de eventos de seguridad del DC) anulen la asignación de usuario a IP del usuario real que ha iniciado sesión.

En entornos de gran tamaño, dependiendo del proceso o aplicación para el que se utilice una cuenta de servicio, también pueden generar miles de eventos de inicio de sesión cada minuto. Esta es también una carga adicional para el conector, que se puede manifestar como un retraso entre el inicio de sesión del usuario y la directiva correcta que se aplica, o una directiva correcta que se pierde más tarde.

Lista de cuentas bloqueadas

- _vmware_user_
- Administrador
- ANÓNIMO
- Inicio de sesión anónimo
- ASPNET
- Servicio local
- McAfeeMVSUser
- MHControl
- Servicio de red
- netwrix
- OpenDNS_Connector
- peersyncsvc
- s-pcadmin
- SophosUpdateMgr
- SophosUpdMgr
- svc-altiris
- svc.iCreate

Más información

También puede excluir cualquier otro evento de inicio de sesión de la cuenta de AD para que no lo procese el conector. Consulte este artículo para obtener instrucciones:

<https://support.umbrella.com/hc/en-us/articles/231266088>

Además, hay grupos de AD que se pueden excluir de la sincronización de AD del conector, que se realiza para rellenar el área de directivas del panel con una lista de usuarios, equipos y grupos de AD. Esto se puede encontrar aquí:

<https://support.umbrella.com/hc/en-us/articles/115005206526>

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).