Integración de Active Directory con VA o CSC

Contenido

Introducción

Este documento describe dos métodos para integrar Active Directory (AD) con Umbrella: Virtual Appliance (VA) o Cisco Secure Client (CSC).

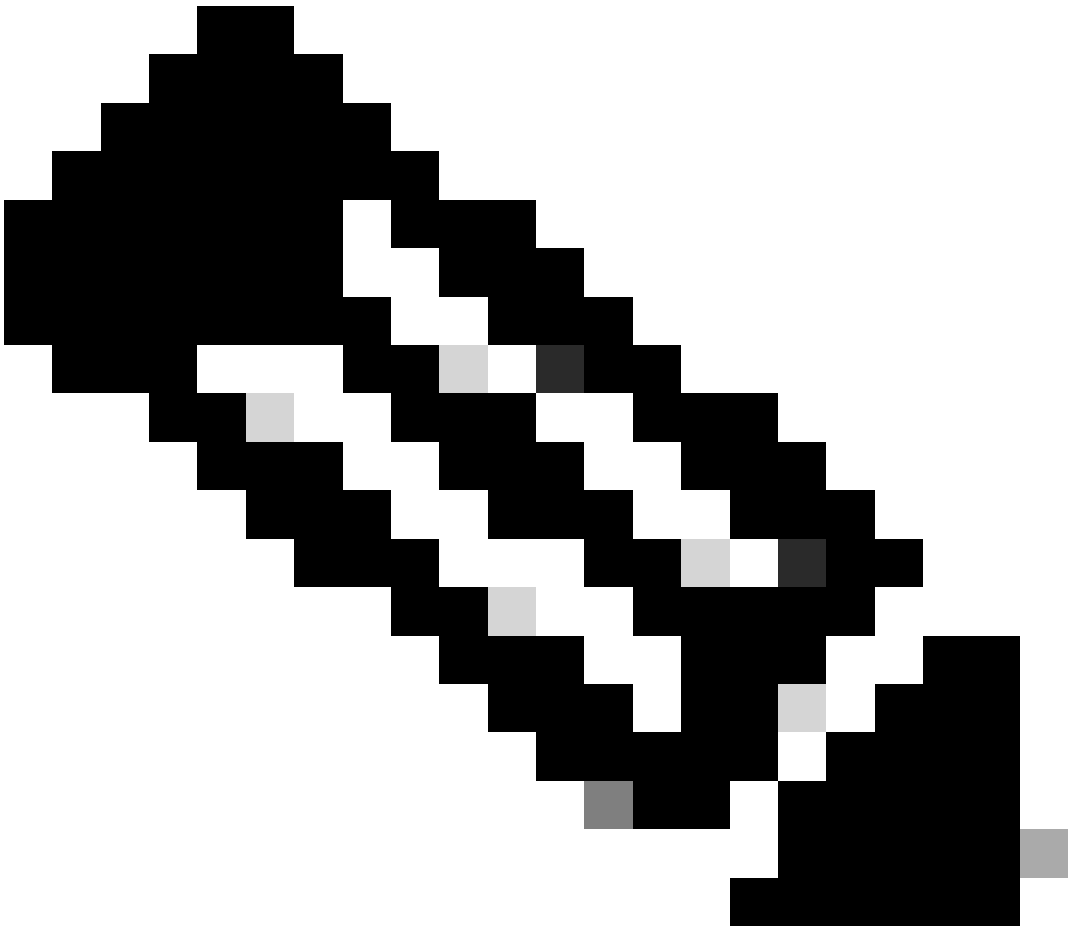
Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conector AD: Sincroniza el árbol de AD de un único dominio de Active Directory con el panel. Para la implementación de VA, también sincroniza activamente los eventos de inicio de sesión de los DC del mismo sitio de Umbrella con los VA. El árbol AD de la organización se sincroniza con la nube de Umbrella mediante el conector AD, obteniendo estos datos del DC registrado. Se detectan actualizaciones de árbol y la nube de Umbrella se actualiza en varias horas.
- Controlador de dominio (servidor AD): Los DC se registran en el panel a través del script .wsf de configuración de registro que se descarga del panel. Esto agrega su nombre, dominio e IP interna al panel para informar al conector con qué IP se intenta sincronizar. Si no puede ejecutar el script, también es posible el registro manual. Póngase en contacto con Umbrella Support para obtener más información y asistencia.
- Dispositivo virtual: El reenviador DNS Umbrella en las instalaciones. Aplica la identidad de AD (opcional) en la red, así como las IP internas en los informes. Esto activa todos los

clientes de roaming detrás de él para inhabilitar la protección DNS y diferir al modo "Detrás de la protección VA".
- Cisco Secure Client: El servicio de software Umbrella in situ que proporciona cifrado DNS, así como identificación de usuario para Windows y macOS. También viene como un módulo de AnyConnect.



Nota: Los requisitos previos difieren significativamente entre las dos implementaciones. Consulte la implementación específica para conocer todos los requisitos previos.

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.

Overview

Este artículo aclara y explora los dos métodos diferentes de integración de Active Directory con el Panel de Umbrella. En la actualidad, los usuarios de AD pueden aplicarse a las políticas y los informes a través de los dispositivos virtuales Umbrella o Cisco Secure Client.

Implementación de clientes seguros

Requirements

- Un conector AD
- Un DC en el panel
- El usuario de OpenDNS_Connector debe tener permiso de controlador de dominio de sólo lectura.
- Versiones mínimas de Secure Client para el cliente independiente (módulo AnyConnect):
    - Windows: 2.1.0 (4.5.01044)
    - OSX: 2.0.39 (4.5.02033).

Cómo funciona

- El cliente móvil que lee el Registro local determina directamente en el equipo local el usuario de AD que ha iniciado sesión actualmente.
- Admite un máximo de un usuario conectado simultáneamente en la estación de trabajo.
- Dos usuarios simultáneos pueden hacer que no se aplique ningún usuario de AD.
- El GUID de usuario de AD y la IP interna se adjuntan a través de EDNS0 dentro del proxy DNS del cliente de roaming a la consulta DNS enviada a los resolvers de Umbrella, identificando de manera única al usuario de AD.
- Todas las políticas se aplican en el lado de la resolución.
- No se necesita ningún conector activo. Sin embargo, la aplicación de directiva de grupo y usuario de AD puede reflejar la sincronización del árbol de AD correcta más reciente.

Dónde funciona

- Cualquier red globalmente.
- No funciona detrás de un dispositivo virtual Umbrella, ya que la capa DNS está desactivada para diferir a los VA locales.

Limitaciones

- Requiere un agente de terminal activo y activado en la estación de trabajo.
- No admite SO de servidor.
- No se puede aplicar la política basada en IP de red interna.
- No se pueden aplicar directivas o informes para el equipo AD (use el nombre de host móvil en su lugar).

El conector aún puede intentar extraer los eventos de inicio de sesión de AD del DC registrado. Esto puede dar lugar a un error de panel que no es relevante para la integración de AD basada en cliente de roaming. Para eliminar los errores con permisos relacionados con la extracción de eventos de inicio de sesión sin extraer ningún evento, desactive la auditoría de eventos de inicio de sesión (si no se utiliza de otra forma) siguiendo las instrucciones inversas de auditoría que aparecen aquí.

Implementación de dispositivo virtual

Requirements

- Dos AV por emplazamiento de Umbrella
- Un conector AD (redundante, segundo, opcional) por sitio de Umbrella
- Cada DC (que no es un DC de solo lectura) debe estar registrado en el Panel.
- El usuario de OpenDNS_Connector debe tener el conjunto completo de permisos necesarios.
- Los eventos de inicio de sesión deben estar habilitados para registrar los registros de eventos de seguridad 4624 en todos los DC. Consulte las sugerencias completas para solucionar problemas.

Cómo funciona

- Los VA reciben asignaciones de usuario de AD basadas en los registros de eventos de inicio de sesión de seguridad de los DC de Windows.
- Cada inicio de sesión de la estación de trabajo se registra en el registro de eventos de seguridad del DC del servidor de inicio de sesión como un evento de inicio de sesión único, con el nombre de usuario de AD o el nombre del equipo de AD y la IP interna de la estación de trabajo.
- El conector analiza estos eventos en tiempo real mediante una suscripción WMI y los sincroniza con cada VA del sitio Umbrella mediante TCP 443.
- El dispositivo virtual crea una asignación de usuarios activos entre la dirección IP interna de un usuario/equipo AD y el nombre de usuario/equipo AD.
- El VA solo tiene visibilidad en la IP de origen interna de una consulta DNS y utiliza el archivo de asignación mencionado anteriormente creado por los eventos sincronizados por el conector. El dispositivo virtual no tiene visibilidad directa de quién está conectado actualmente a una máquina. Esto adjunta el GUID de usuario de AD y la IP interna a través de EDNS0 a la consulta DNS enviada a los resolvers de Umbrella por el VA, identificando de manera única al usuario de AD.
- El hash del equipo de AD se aplica de la misma manera.
- Todas las políticas se aplican en el lado de la resolución.
- Para recibir un usuario de AD, un conector debe ser funcional y activo en la organización, y los eventos de inicio de sesión deben ser actuales.
- El usuario debe ser el último usuario de AD en autenticarse en este equipo tal como se ve en los registros de eventos.

Dónde funciona

En la red corporativa local, donde todos los DNS apuntan a un dispositivo virtual Umbrella que pertenece al mismo sitio Umbrella que el DC con el que el usuario se ha autenticado.

Limitaciones

- El equipo no puede señalar a un VA que pertenece a un dominio AD o sitio de Umbrella diferente (las implementaciones grandes en varios dominios no pueden ver la aplicación AD fuera de su red base).
- Las implementaciones de gran tamaño pueden requerir la subdivisión en ubicaciones de Umbrella con AV independientes.
- Las excepciones de usuario de AD pueden ser necesarias para los usuarios de AD de servicio.
- Existe un rendimiento máximo de eventos de inicio de sesión por segundo para el conector mencionado anteriormente que puede retrasar la aplicación del usuario. Se trata de un factor de latencia de red y del número de dispositivos virtuales.

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).