Examine el flujo de integración de Umbrella Active Directory

Contenido

Introducción

Este documento describe el flujo de comunicación entre los componentes operativos en una integración de Active Directory (AD) de Cisco Umbrella.

Antecedentes

La comprensión del flujo de comunicación de Active Directory puede ayudar a solucionar problemas y garantizar un entorno correctamente configurado antes de la implementación.

Flujo de comunicación con la implementación de Umbrella Active Directory

Cuando el script del conector de AD se ejecuta en un controlador de dominio (DC)

El script de Windows realiza una conexión única desde el controlador de dominio (DC) a la nube en el puerto TCP/443 mediante HTTPS para registrar el DC en el panel. Este registro permite que el conector reconozca el DC. Se realiza una llamada a **https://api.opendns.com** con parámetros específicos. Una vez que la secuencia de comandos registra correctamente el DC, se muestra en el panel.

A veces, los problemas pueden estar relacionados con Actualizaciones de certificados raíz en Windows. Para determinarlo rápidamente, vaya a Internet Explorer y sitúe el explorador en: https://api.opendns.com/v2/OnPrem.Asset. Esta acción imprime un mensaje como **1005 Missing API key**. Si aparece algún error o advertencia de certificado en esa página, asegúrese de que esté instalada la última

actualización de certificados raíz de Microsoft.

Cómo se comunica el conector de AD

El conector AD se comunica con el servicio Umbrella Cloud o un dispositivo virtual de la siguiente manera:

- Conector a la nube

  El conector carga todos los datos de Active Directory (AD) cada cinco minutos si se producen cambios, mediante una conexión HTTPS en el puerto 443 TCP. Solo se carga la información de Grupos, Usuarios y Equipos. No se cargan contraseñas y toda la información del usuario se trocea localmente, lo que hace que los datos sean únicos.

- Conector a dispositivos virtuales

  El conector envía constantemente eventos AD a los dispositivos virtuales mediante el puerto 443 TCP (no cifrado). Se trata de una comunicación unidireccional; los dispositivos no se comunican con los conectores. Un requisito previo obligatorio es que el conector y el dispositivo virtual (VA) se comuniquen a través de una red de confianza.

- Conector a controladores de dominio

  El conector se comunica con todos los controladores de dominio ubicados en el mismo sitio mediante los puertos 389 TCP y 3268 TCP/UDP para la sincronización LDAP. El conector también se comunica con los controladores de dominio mediante WMI/RPC. El puerto 135 TCP es el puerto estándar para RPC y WMI. WMI también utiliza un puerto asignado aleatoriamente entre 1024 TCP y 65535 TCP para Windows 2003 y versiones anteriores, o entre 49152 TCP y 65535 TCP para Windows 2008 y versiones posteriores. A partir de la versión 1.1.24, el conector también se comunica con el controlador de dominio mediante LDAP (LDAP sobre SSL) a través de los puertos 636 TCP y 3269 TCP.

Si se observan problemas de comunicación, compruebe si hay algún proxy de aplicación de capa 7 que pueda estar bloqueando o descartando datos. Un caso común es la función de inspección en dispositivos Cisco que actúan en protocolos como DNS, HTTP o HTTPS. Para obtener más información, consulte nuestra documentación sobre Aplicación de la Inspección de Application Layer Protocol.

Dispositivos virtuales (VA) a la nube

Los dispositivos virtuales se comunican con frecuencia en el puerto 443 TCP a **api.opendns.com**, así como a 53 TCP/UDP para consultas o sondeos DNS y a 22, 25, 53, 80, 443 o 4766 TCP para establecer el túnel de soporte. Los dispositivos virtuales se comunican con la nube mediante los puertos 53 UDP/TCP, 443 TCP, 123 TCP y 80 TCP. Reciben datos de los conectores en el puerto 443 TCP (no una conexión HTTPS) pero no requieren comunicación con ellos.

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).