

Utilizar Umbrella Active Directory Connector para la autenticación

Contenido

[Introducción](#)

[Overview](#)

[Autenticación mediante 802.1x, RADIUS o ISE](#)

[Soluciones alternativas](#)

Introducción

Este documento describe cómo utilizar el conector de Umbrella Active Directory para la autenticación a través de 802.1x, Radius o ISE.

Overview

El [conector de Active Directory \(AD\) de Cisco Umbrella](#) funciona mediante la asignación de usuarios/equipos AD a direcciones IP internas. Para que la asignación sea correcta, los usuarios de AD deben autenticarse en un controlador de dominio configurado para comunicarse con un conector de AD de Cisco Umbrella.

Si los usuarios de AD se autentican por otros medios, es posible que no se genere ningún evento de inicio de sesión en el controlador de dominio o que haya una asignación inesperada que provoque la aplicación de una directiva incorrecta.

Autenticación mediante 802.1x, RADIUS o ISE

La autenticación a través de 802.1x, RADIUS o ISE no se admite debido a las limitaciones de cómo funcionan los inicios de sesión de Active Directory con estas soluciones. Los eventos de inicio de sesión que busca el conector de AD a menudo no se generan.

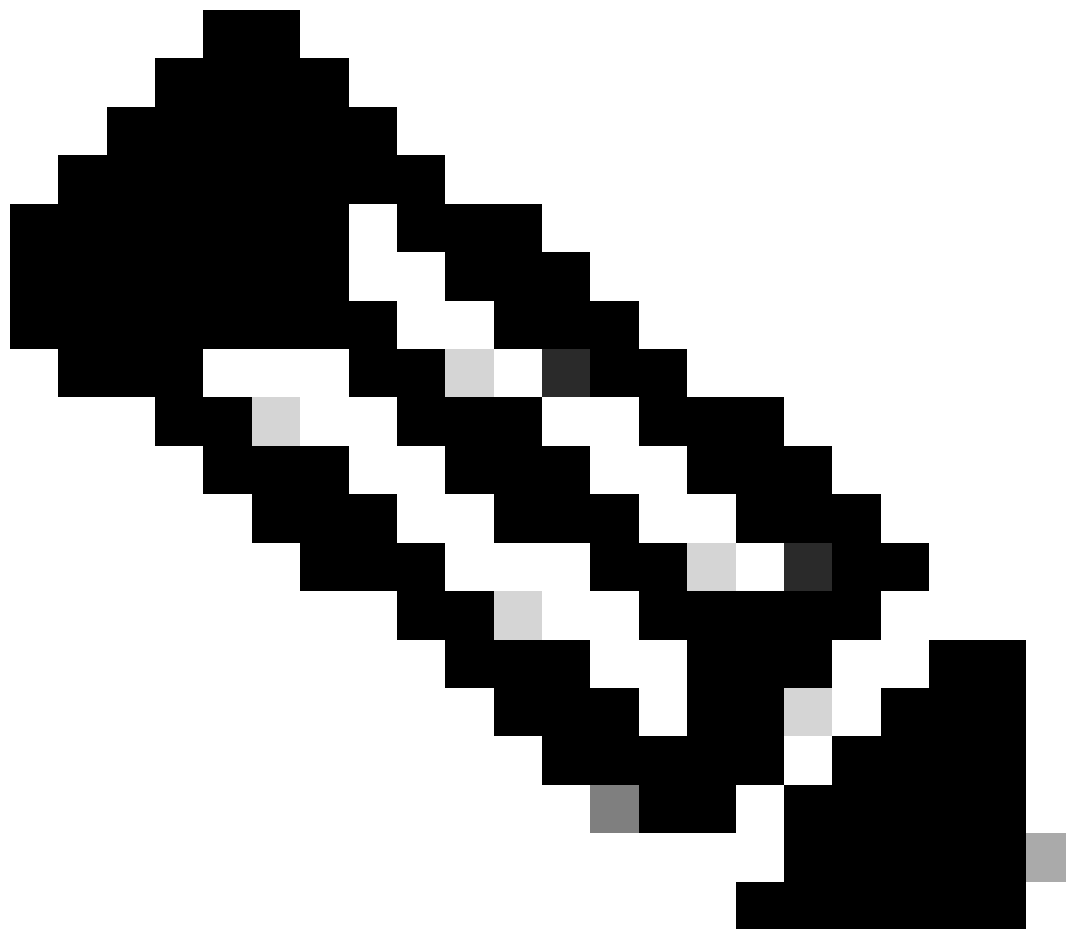
Obtenga más información sobre los ID de eventos que busca el conector de AD aquí: ¿Qué eventos de ventana/ID de evento busca el servicio de conector?

Normalmente, la dirección IP del servicio de autenticación se asigna al usuario de AD en lugar de a la dirección IP del equipo del usuario.

Soluciones alternativas

La integración de AD también se puede lograr mediante el uso del cliente de roaming con la función de compatibilidad de identidades habilitada. Puede encontrar más información sobre esta

función en nuestra [documentación de implementación](#).



Nota: Esta solución requiere que los appliances virtuales no estén presentes en la red, ya que esto provoca que el cliente de roaming pase a un estado de "detrás de VA" deshabilitado.

Si se utilizan dispositivos virtuales en la red, se pueden utilizar direcciones IP internas para la identificación. Por ejemplo, puede crear una identidad de "[red interna](#)" para el intervalo de direcciones de la red inalámbrica y, a continuación, aplicar una política a esta identidad. El único inconveniente de este método es que todos los dispositivos en este rango de direcciones reciben la misma política.

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).