Aplicación de políticas para cuentas locales en Umbrella Active Directory

Contenido

Introducción

Este documento describe el comportamiento esperado de la política al sincronizar los productos de Umbrella en las instalaciones con Active Directory y las cuentas de usuario locales.

Identificación de cuenta local y dispositivo virtual de Umbrella

El dispositivo virtual Umbrella recibe información de inicio de sesión de Active Directory de los controladores de dominio de Windows. Almacena en caché e identifica a los usuarios de Active Directory en función de su dirección IP de origen.

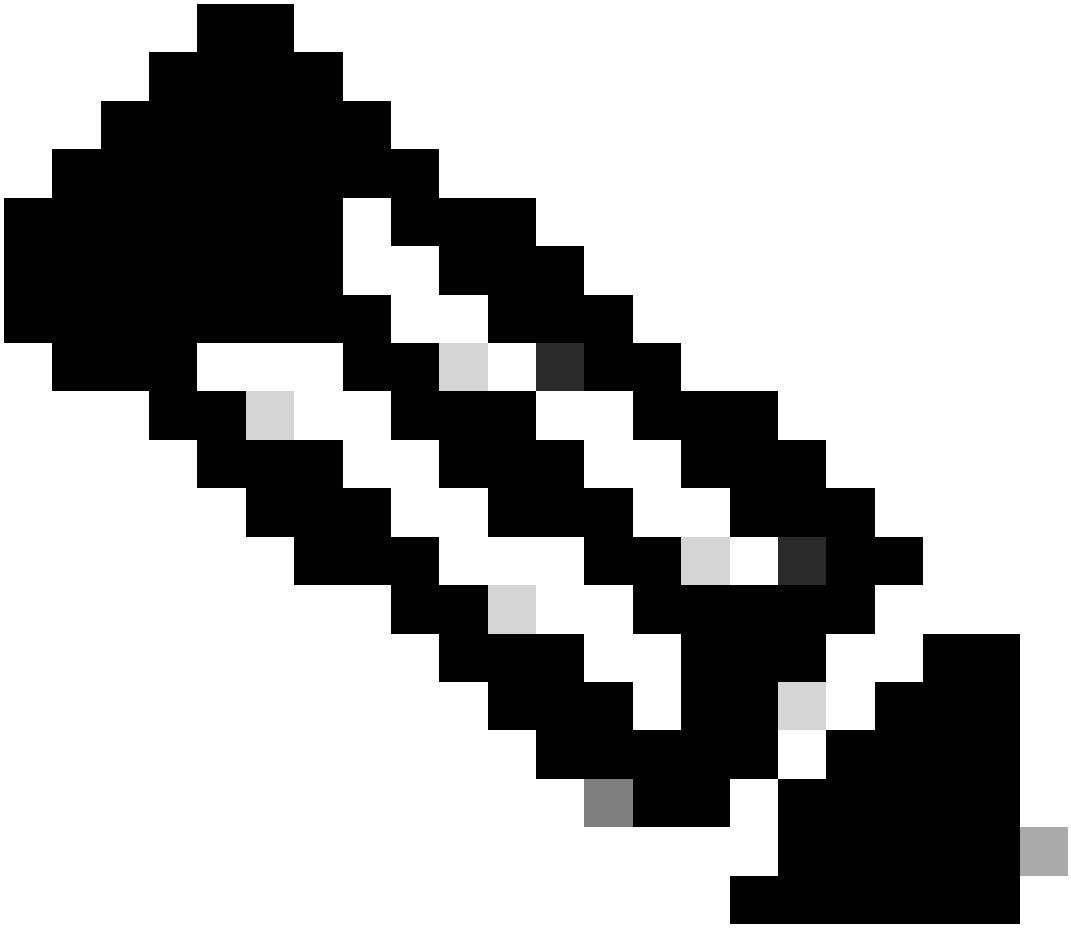
- El controlador de dominio no realiza un seguimiento de los inicios de sesión de los usuarios locales, por lo que el dispositivo virtual no puede identificar directamente a estos usuarios.
- Si un usuario de Active Directory ha iniciado sesión recientemente desde una dirección IP, la identidad almacenada en caché se puede seguir utilizando según nuestra caché. El dispositivo virtual no tiene forma de saber que el usuario de AD se ha sustituido por una cuenta local.
- Si no hay ningún usuario en caché, el dispositivo virtual utiliza una identidad predeterminada (no AD). La identidad desencadenada puede ser:
  - Nombre del sitio de paraguas (por ejemplo, Sitio predeterminado)
  - Red interna (dirección IP interna)
  - Red (dirección IP externa)

Recomendaciones para el appliance virtual Umbrella

- Restrinja el acceso a cuentas y contraseñas locales.
- Cree una directiva independiente para el nombre del sitio de Umbrella (por ejemplo, Sitio predeterminado). Asigne a esta directiva una prioridad inferior a la directiva de usuario estándar de Active Directory. Esta política más restrictiva se aplica cuando no se detecta ningún usuario de AD.

- Si necesita políticas diferentes para las cuentas de usuario locales, considere la posibilidad de implementar Umbrella Roaming Client.

Cliente de roaming de Umbrella y política de cuenta local



Nota: Para utilizar la integración de Active Directory con el cliente de roaming, navegue hasta Identidades > Equipos de roaming y habilite la configuración Habilitar la aplicación de directivas de grupo y usuario de Active Directory.

El cliente de roaming detecta los usuarios que han iniciado sesión en el Registro de Windows, lo que permite identificar a los usuarios de Active Directory por su GUID de AD único.

- El cliente de roaming no puede identificar nombres de usuario locales para fines de políticas.
- Cuando se detecta un usuario de AD, la identidad del usuario de AD se aplica a la

aplicación de políticas, incluidos los usuarios de AD que han iniciado sesión con credenciales en caché mientras no están en la red.
- Si no se detecta ningún usuario de AD (por ejemplo, cuando un usuario local ha iniciado sesión), la identidad del equipo móvil se utiliza para la aplicación de políticas.

Recomendaciones para Umbrella Roaming Client

- Restrinja el acceso a cuentas y contraseñas locales.
- Cree una política independiente para los equipos en roaming con una prioridad inferior a la política de usuario de AD estándar. Esta directiva se aplica a los equipos móviles que no están unidos al dominio o que utilizan los usuarios locales.

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).