Comprender la integración de Terminal Services, Citrix y Umbrella con Active Directory

Contenido

Introducción

Este documento describe la integración de Terminal Services, Citrix y Umbrella con Active Directory.

Overview

Se aplica a: Servicios de terminal de Windows y servicios de escritorio remoto, multisesión de Windows 10 Enterprise, Citrix XenApp y XenDesktop

Los servicios de Terminal Server y los servidores Citrix permiten que varias sesiones de cliente simultáneas se alojen en un único servidor. Hay dos configuraciones distintas:

- Servicio de Escritorio remoto (RDS). Varios usuarios ejecutan una sesión en una única máquina virtual en el mismo servidor. Todas estas sesiones comparten el mismo sistema operativo y la misma dirección IP. Esto se conoce comúnmente como Servicios de Terminal Server.
- Infraestructura de escritorio virtual (VDI). El servidor ejecuta un conjunto de máquinas virtuales y cada usuario se conecta a una máquina virtual única, con su propio sistema operativo y dirección IP

Política web: Aplicable a RDS y VDI

El gateway web seguro con autenticación basada en cookies SAML a través del archivo PAC, el túnel CDFW y la cadena de proxy admiten varios usuarios en una única dirección IP. Esto significa que los escritorios virtuales (Citrix/TS) son compatibles con la aplicación de políticas web por usuario.

Política DNS: RDS con integración de AD

No admitimos servidores RDS / Host de sesión de Escritorio remoto / Terminal para la identificación por usuario. Esto incluye el sistema operativo multisesión solo de Azure Windows 10 Enterprise.

Las sesiones de cliente alojadas en estos servidores comparten una única dirección IP: el que pertenece a la máquina host. La integración de Umbrella Active Directory (AD) con dispositivos virtuales (VA) se basa en asignaciones de dirección IP a usuario únicas para funcionar correctamente. En resumen, esto significa que la identificación por usuario no es posible en ninguna situación en la que los usuarios compartan la misma dirección IP de origen.

Cuando varios usuarios que han iniciado sesión comparten la misma IP, esto afecta negativamente a la aplicación de políticas y a los informes. Todos los usuarios reciben la misma directiva y el usuario identificado puede cambiar continuamente en función del último usuario que inició sesión.

Política de DNS: Solución: RDS con integración de AD

La mejor manera de abordar este problema es configurar una política única para la dirección IP de su servidor Terminal Server o Citrix Server. Esto significa que todos los usuarios de Terminal Server reciben la misma directiva coherente.

1. Cree una red interna en 'Implementaciones > Redes internas'. Esto cubre la dirección IP /32 de su Terminal Server. Asigne la red al mismo sitio de Umbrella que el dispositivo o dispositivos virtuales aplicables.
2. Vaya al Asistente de directivas y cree una nueva directiva.
3. En la sección Seleccionar identidades, seleccione haga clic en 'Sitios' y abra el sitio de Umbrella correspondiente.
4. Seleccione la identidad de red interna que creó anteriormente
5. Configure la política como lo haría normalmente
6. Una vez creada la directiva para el servidor Terminal Server, asegúrese de que la ordena al principio de la lista de directivas para que tenga prioridad sobre las directivas basadas en el usuario.

Como alternativa, es posible crear una directiva para Terminal Server basada en la identidad del equipo AD. Este método funciona de la misma manera; todos los usuarios del servidor se identifican como el nombre del equipo de Terminal Server. Sin embargo, para que esto funcione consistentemente, el VA debe configurarse de manera que optimice los mapeos de host a IP. Consulte las instrucciones de tiempo de espera GUID de host de AD para obtener más detalles o póngase en contacto con el soporte técnico de Umbrella para obtener ayuda.

Política de DNS: uso de VDI con integración de AD

Las implementaciones de tipo VDI (en las que se ejecuta una máquina virtual exclusiva para cada usuario) pueden seguir recibiendo identidades por usuario. Los requisitos son los siguientes:

- Dispositivo virtual: cada usuario debe tener una IP de origen única que sea visible para el dispositivo virtual. La IP de origen no debe estar sujeta a la "NAT de origen" antes de llegar

al dispositivo.

- Cliente de roaming: la integración de AD en el cliente de roaming es posible cuando el cliente de roaming está instalado en cada máquina virtual. La implementación de esta manera es más factible cuando cada usuario tiene un persistente (por ejemplo, personal).

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).