Entender a integração de serviços de terminal, Citrix e Umbrella com o Ative Diretory

Contents

[Introdução](#)

[Overview](#)

[Política da Web: Aplicável ao RDS e ao VDI](#)

[Política DNS: RDS com integração ao AD](#)

[Política DNS:Solução - RDS com integração ao AD](#)

[Política DNS:usando VDI com integração ao AD](#)

Introdução

Este documento descreve os Serviços de Terminal, Citrix e integração do Umbrella com o Ative Diretory.

Overview

Aplicável a: Serviços de Terminal e Serviços de Área de Trabalho Remota do Windows, multisessão do Windows 10 Enterprise, Citrix XenApp e XenDesktop

Os Terminal Services e os servidores Citrix oferecem a capacidade de várias sessões simultâneas do cliente serem hospedadas em um único servidor. Há duas configurações distintas:

- Serviço de Área de Trabalho Remota (RDS). Vários usuários executam uma sessão em uma única máquina virtual no mesmo servidor. Todas essas sessões compartilham o mesmo SO e endereço IP. Isso é comumente chamado de Serviços de Terminal.
- Virtual Desktop Infrastructure (VDI). O servidor executa um pool de máquinas virtuais e cada usuário se conecta a uma VM exclusiva, com seu próprio sistema operacional e endereço IP

Política da Web: Aplicável ao RDS e ao VDI

O Secure Web Gateway com autenticação baseada em cookies SAML via arquivo PAC, túnel CDFW e cadeia de proxy suportam vários usuários para um único endereço IP. Isso significa que os desktops virtuais (Citrix/TS) são compatíveis com a aplicação da política da Web por usuário.

Política DNS: RDS com integração ao AD

Não oferecemos suporte a servidores RDS/Host da Sessão da Área de Trabalho

Remota/Terminal para identificação por usuário. Isso inclui o SO de várias sessões do Windows 10 Enterprise somente do Azure.

As sessões de cliente hospedadas nesses servidores compartilham um único endereço IP: o que pertence ao computador host. A integração do Ative Diretory (AD) do Umbrella com os Virtual Appliances (VAs) depende de mapeamentos exclusivos de usuário para endereço IP para funcionar corretamente. Em resumo, isso significa que a identificação por usuário não é possível em nenhuma situação em que os usuários compartilhem o mesmo endereço IP origem.

Quando vários usuários conectados compartilham o mesmo IP, isso afeta negativamente a aplicação de políticas e a geração de relatórios. Todos os usuários recebem a mesma política e o usuário identificado pode mudar continuamente com base no último usuário conectado.

Política DNS: Solução - RDS com integração ao AD

A melhor maneira de lidar com esse problema é configurar uma política exclusiva para o endereço IP do servidor de terminal ou do servidor Citrix. Isso significa que todos os usuários do Terminal Server recebem a mesma política consistente.

1. Crie uma Rede Interna em 'Implantações > Redes Internas'. Isso abrange o endereço IP /32 do seu Terminal Server. Atribua a rede ao mesmo local de guarda-chuva que o(s) dispositivo(s) virtual(is) aplicável(is).
2. Navegue até o Assistente de política e crie uma nova política.
3. Na seção Selecionar identidades, clique em 'Sites' e abra o site relevante do Umbrella.
4. Selecione a identidade da rede interna que você criou anteriormente
5. Configure a política como faria normalmente
6. Depois de criar a política para o seu Terminal Server, certifique-se de ordenar essa política no topo da lista de políticas para que ela tenha precedência sobre qualquer política baseada em usuário.

Como alternativa, é possível criar uma política para o Terminal Server com base na identidade do computador do AD. Este método funciona da mesma forma; todos os usuários do servidor são identificados como o nome do computador do Terminal Server. No entanto, para que isso funcione de forma consistente, o VA deve ser configurado de forma a otimizar os mapeamentos de host para IP. Consulte as instruções de Tempo Limite de GUID de Host do AD para obter mais detalhes ou entre em contato com o suporte do Umbrella para obter assistência.

Política DNS: usando VDI com integração ao AD

As implantações do tipo VDI - em que há uma máquina virtual exclusiva em execução para cada usuário - ainda podem receber identidades por usuário. Os requisitos são os seguintes:

- Virtual Appliance - Cada usuário deve ter um IP de origem exclusivo que seja visível para o Virtual Appliance. O IP de origem não deve estar sujeito ao "NAT de origem" antes de alcançar o dispositivo.
- Cliente de roaming - A integração do AD no cliente de roaming é possível quando o cliente de roaming está instalado em cada máquina virtual. A implantação dessa maneira é mais

viável quando cada usuário tem uma persistente (por exemplo, pessoal).

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.