Terminal Services, Citrix en Umbrella Integration met Active Directory begrijpen

Inhoud

Inleiding

Dit document beschrijft de integratie van Terminal Services, Citrix en Umbrella met Active Directory.

Overzicht

Van toepassing op: Windows Terminal Services en Remote Desktop Services, Windows 10 Enterprise met meerdere sessies, Citrix XenApp en XenDesktop

Terminal Services en Citrix-servers bieden de mogelijkheid om meerdere, gelijktijdige cliensessies op één server te hosten. Er zijn twee verschillende configuraties:

- Remote Desktop Service (RDS). Meerdere gebruikers voeren een sessie uit op één virtuele machine op dezelfde server. Deze sessies delen allemaal hetzelfde besturingssysteem en IP-adres. Dit wordt vaak aangeduid als terminalservices.
- Virtual Desktop Infrastructure (VDI). De server draait een pool van virtuele machines en elke gebruiker maakt verbinding met een unieke VM, met een eigen besturingssysteem en IP-adres

Webbeleid: van toepassing op RDS en VDI

Secure Web Gateway met SAML-cookies op basis van verificatie via PAC-bestand, CDFW Tunnel en Proxy Chain ondersteunen meerdere gebruikers naar één IP-adres. Dit betekent dat virtuele desktops (Citrix/TS) worden ondersteund volgens het webbeleid van de gebruiker.

DNS-beleid: RDS met AD-integratie

Wij ondersteunen geen RDS-/Remote Desktop Session Host-/Terminal-servers voor identificatie per gebruiker. Dit omvat het Azure Windows 10 Enterprise-besturingssysteem met meerdere

sessies.

De cliensessies die op deze servers worden gehost, delen één IP-adres: dat van het hostsysteem. Integratie van overkoepelende Active Directory (AD) met virtuele apparaten (VA's) is afhankelijk van unieke toewijzing van gebruikers aan IP-adressen om correct te werken. Kortom, dit betekent dat identificatie per gebruiker niet mogelijk is in elke situatie waarin gebruikers hetzelfde bron-IP-adres delen.

Wanneer meerdere ingelogde gebruikers hetzelfde IP-adres delen, heeft dit een negatief effect op de beleidstoepassing en rapportage. Alle gebruikers ontvangen hetzelfde beleid en de geïdentificeerde gebruiker kan voortdurend wijzigen op basis van de laatst ingelogde gebruiker.

DNS-beleid: oplossing - RDS met AD-integratie

De beste manier om dit probleem aan te pakken, is door een uniek beleid te configureren voor het IP-adres van uw Terminal Server of Citrix-server. Dit betekent dat alle gebruikers van de Terminal Server hetzelfde, consistente beleid ontvangen.

1. Maak een intern netwerk in 'Implementaties > Interne netwerken'. Dit omvat het IP-adres /32 van uw Terminal Server. Wijs het netwerk toe aan dezelfde overkoepelende site als het (de) toepasselijke virtuele apparaat(apparaten).
2. Navigeer naar de wizard Beleid en maak een nieuw beleid.
3. Selecteer in de sectie Identiteiten selecteren de optie 'Sites' en open vervolgens de betreffende overkoepelende site.
4. Selecteer de identiteit van het interne netwerk die u eerder hebt gemaakt
5. Configureer het beleid zoals u normaal zou doen
6. Nadat u het beleid voor uw Terminal-server hebt gemaakt, moet u dit beleid bovenaan de lijst met beleidsregels bestellen, zodat het voorrang heeft op gebruikersbeleid.

U kunt ook een beleid maken voor de terminalserver op basis van de identiteit van de AD-computer. Deze methode werkt op dezelfde manier; alle gebruikers van de server worden geïdentificeerd als de naam van de Terminal Server-computer. Om dit consistent te laten werken, moet de VA echter zo worden geconfigureerd dat de toewijzing van host naar IP wordt geoptimaliseerd. Raadpleeg de instructies voor de time-out van de AD Host GUID voor meer informatie of neem contact op met Umbrella Support voor hulp.

DNS-beleid: VDI gebruiken met AD-integratie

Implementaties van het VDI-type - waarbij voor elke gebruiker een unieke virtuele machine wordt uitgevoerd - kunnen nog steeds identiteiten per gebruiker ontvangen. De vereisten zijn als volgt:

- Virtuele toestellen - Elke gebruiker moet een unieke bron-IP hebben die zichtbaar is voor de virtuele toestellen. De bron-IP mag niet worden onderworpen aan "Source NATing" voordat deze het toestel bereikt.
- Zwervende client - integratie van AD in de zwervende client is mogelijk wanneer de zwervende client op elke virtuele machine is geïnstalleerd. Implementatie op deze manier is meer haalbaar wanneer elke gebruiker een permanente (bijv. persoonlijke) virtuele machine

heeft.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.