Terminaldienste, Citrix und Umbrella-Integration in Active Directory verstehen

Inhalt

Einleitung

In diesem Dokument werden die Terminaldienste, Citrix und Umbrella-Integration mit Active Directory beschrieben.

Überblick

Gilt für: Windows Terminal Services und Remotedesktopdienste, Windows 10 Enterprise Multi-Session, Citrix XenApp und XenDesktop

Terminaldienste und Citrix-Server bieten die Möglichkeit, mehrere Client-Sitzungen gleichzeitig auf einem einzigen Server zu hosten. Es gibt zwei verschiedene Konfigurationen:

- Remotedesktopdienst (RDS). Mehrere Benutzer führen eine Sitzung auf einem einzelnen virtuellen System auf demselben Server aus. Diese Sitzungen verwenden alle dasselbe Betriebssystem und dieselbe IP-Adresse. Dies wird allgemein als Terminaldienste bezeichnet.
- Virtual Desktop Infrastructure (VDI) Der Server führt einen Pool virtueller Systeme aus, und jeder Benutzer stellt eine Verbindung zu einem eindeutigen virtuellen System mit einem eigenen Betriebssystem und einer eigenen IP-Adresse her.

Webrichtlinie: Gilt für RDS und VDI

Secure Web Gateway mit SAML-Cookies-basierter Authentifizierung über PAC-Datei, CDFW Tunnel und Proxy Chain unterstützt mehrere Benutzer zu einer einzigen IP-Adresse. Das bedeutet, dass virtuelle Desktops (Citrix/TS) von den Benutzern für die Durchsetzung der Webrichtlinien unterstützt werden.

DNS-Richtlinie: RDS mit AD-Integration

Wir unterstützen keine RDS-/Remote Desktop Session Host-/Terminal-Server zur Identifizierung pro Benutzer. Dies umfasst das Azure Only-Betriebssystem Windows 10 Enterprise für mehrere Sitzungen.

Die auf diesen Servern gehosteten Client-Sitzungen haben eine gemeinsame IP-Adresse: Die Umbrella Active Directory (AD)-Integration mit virtuellen Appliances (VAs) basiert auf eindeutigen Benutzer-zu-IP-Adresszuordnungen, um ordnungsgemäß zu funktionieren. Kurz gesagt bedeutet dies, dass eine benutzerspezifische Identifikation in keiner Situation möglich ist, in der Benutzer dieselbe Quell-IP-Adresse verwenden.

Wenn mehrere angemeldete Benutzer dieselbe IP-Adresse verwenden, wirkt sich dies negativ auf die Richtlinienanwendung und die Berichterstellung aus. Alle Benutzer erhalten die gleiche Richtlinie, und der identifizierte Benutzer kann basierend auf dem zuletzt angemeldeten Benutzer kontinuierlich geändert werden.

DNS-Richtlinie: Lösung - RDS mit AD-Integration

Der beste Weg, dieses Problem zu beheben, ist die Konfiguration einer eindeutigen Richtlinie für die IP-Adresse Ihres Terminalservers oder Citrix Servers. Dies bedeutet, dass alle Benutzer des Terminalservers die gleiche, konsistente Richtlinie erhalten.

1. Erstellen Sie ein internes Netzwerk unter "Deployments > Internal Networks" (Bereitstellungen > Interne Netzwerke). Dies umfasst die IP-Adresse /32 Ihres Terminalservers. Weisen Sie das Netzwerk demselben Umbrella-Standort wie die entsprechenden virtuellen Appliances zu.
2. Navigieren Sie zum Richtlinien-Assistenten, und erstellen Sie eine neue Richtlinie.
3. Klicken Sie im Abschnitt "Identitäten auswählen" auf "Standorte", und öffnen Sie dann die entsprechende Umbrella-Site.
4. Wählen Sie die zuvor erstellte interne Netzwerkidentität aus.
5. Konfigurieren Sie die Richtlinie wie gewohnt.
6. Nachdem Sie die Richtlinie für den Terminalserver erstellt haben, müssen Sie diese Richtlinie ganz oben in der Liste der Richtlinien anordnen, damit sie Vorrang vor allen benutzerbasierten Richtlinien hat.

Alternativ ist es möglich, eine Richtlinie für den Terminalserver auf der Grundlage der AD-Computeridentität zu erstellen. Dieses Verfahren funktioniert auf die gleiche Weise; Alle Benutzer des Servers werden als Terminalserver-Computername identifiziert. Damit dies jedoch konsistent funktioniert, muss die VA so konfiguriert werden, dass die Host-zu-IP-Zuordnung optimiert wird. Weitere Informationen finden Sie in den Anweisungen zum AD-Host-GUID-Timeout oder wenden Sie sich an den Umbrella-Support.

DNS-Richtlinie: Verwendung von VDI mit AD-Integration

VDI-Bereitstellungen, bei denen für jeden Benutzer ein eindeutiges virtuelles System ausgeführt wird, können weiterhin Benutzeridentitäten empfangen. Die Anforderungen sind wie folgt:

- Virtuelle Appliance - Jeder Benutzer muss über eine eindeutige Quell-IP-Adresse verfügen,

die für die virtuelle Appliance sichtbar ist. Die Quell-IP darf nicht der Quell-NAT unterliegen, bevor sie die Appliance erreicht.

- Roaming-Client - Die AD-Integration in den Roaming-Client ist möglich, wenn der Roaming-Client auf jedem virtuellen System installiert ist. Eine solche Bereitstellung ist umsetzbarer, wenn jeder Benutzer über einen persistenten Port verfügt (z. B. Personal) virtuelles System.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.