

# Comprendre l'intégration de Terminal Services, Citrix et Umbrella avec Active Directory

## Table des matières

---

[Introduction](#)

[Aperçu](#)

[Stratégie Web : Applicable aux services RDS et VDI](#)

[Stratégie DNS : RDS avec intégration AD](#)

[Stratégie DNS:Solution - RDS avec intégration AD](#)

[Stratégie DNS:utilisation de VDI avec intégration AD](#)

---

## Introduction

Ce document décrit l'intégration de Terminal Services, Citrix et Umbrella avec Active Directory.

## Aperçu

S'applique à : Services Terminal Server et Bureau à distance Windows, Windows 10 Entreprise multisession, Citrix XenApp et XenDesktop

Les services Terminal Server et les serveurs Citrix permettent d'héberger plusieurs sessions client simultanées sur un seul serveur. Il existe deux configurations distinctes :

- Service Bureau à distance (RDS). Plusieurs utilisateurs exécutent une session sur une seule machine virtuelle sur le même serveur. Ces sessions partagent toutes le même système d'exploitation et la même adresse IP. Il s'agit généralement des services Terminal Server.
- Infrastructure de poste de travail virtuel (VDI). Le serveur exécute un pool de machines virtuelles et chaque utilisateur se connecte à une machine virtuelle unique, avec son propre système d'exploitation et sa propre adresse IP

## Stratégie Web : Applicable aux services RDS et VDI

Secure Web Gateway avec authentification basée sur les cookies SAML via un fichier PAC, un tunnel CDFW et une chaîne proxy prennent en charge plusieurs utilisateurs à une adresse IP unique. Cela signifie que les postes de travail virtuels (Citrix/TS) sont pris en charge par l'application de la stratégie Web par utilisateur.

## Stratégie DNS : RDS avec intégration AD

Nous ne prenons pas en charge les serveurs RDS / Hôte de session Bureau à distance / Terminal

Server pour l'identification par utilisateur. Cela inclut le système d'exploitation multissession Windows 10 Entreprise Azure uniquement.

Les sessions client hébergées sur ces serveurs partagent une adresse IP unique : Celui qui appartient à l'ordinateur hôte. L'intégration d'Umbrella Active Directory (AD) avec les appareils virtuels (VA) repose sur des mappages d'adresse IP à utilisateur unique afin de fonctionner correctement. En bref, cela signifie que l'identification par utilisateur n'est pas possible dans les situations où les utilisateurs partagent la même adresse IP source.

Lorsque plusieurs utilisateurs connectés partagent la même adresse IP, cela affecte négativement l'application de la stratégie et le reporting. Tous les utilisateurs reçoivent la même stratégie et l'utilisateur identifié peut changer continuellement en fonction du dernier utilisateur connecté.

## Politique DNS : solution - RDS avec intégration AD

La meilleure façon de résoudre ce problème est de configurer une stratégie unique pour l'adresse IP de votre serveur Terminal Server ou Citrix. Cela signifie que tous les utilisateurs du serveur Terminal Server reçoivent la même stratégie cohérente.

1. Créez un réseau interne dans « Déploiements > Réseaux internes ». Cette section couvre l'adresse IP /32 de votre serveur Terminal Server. Attribuez le réseau au même site Umbrella que le ou les appareils virtuels concernés.
2. Accédez à l'Assistant Stratégie et créez une nouvelle stratégie.
3. Dans la section Select Identities, sélectionnez cliquez sur « Sites », puis ouvrez le site Umbrella approprié.
4. Sélectionnez l'identité réseau interne que vous avez créée précédemment
5. Configurez la stratégie comme vous le feriez normalement
6. Une fois que vous avez créé la stratégie pour votre serveur Terminal Server, veillez à classer cette stratégie en haut de la liste des stratégies afin qu'elle soit prioritaire sur toutes les stratégies basées sur l'utilisateur.

Il est également possible de créer une stratégie pour le serveur Terminal Server basée sur l'identité de l'ordinateur AD. Cette méthode fonctionne de la même manière ; tous les utilisateurs du serveur sont identifiés comme le nom de l'ordinateur Terminal Server. Cependant, pour que cela fonctionne de manière cohérente, la VA doit être configurée de manière à optimiser les mappages hôte-IP. Pour plus d'informations, consultez les instructions relatives au délai d'expiration du GUID d'hôte AD ou contactez le support Umbrella pour obtenir de l'aide.

## Stratégie DNS : utilisation de VDI avec intégration AD

Les déploiements de type VDI, où une machine virtuelle unique est exécutée pour chaque utilisateur, peuvent toujours recevoir des identités par utilisateur. Les exigences sont les suivantes :

- Appareil virtuel - Chaque utilisateur doit disposer d'une adresse IP source unique visible par l'appareil virtuel. L'adresse IP source ne doit pas faire l'objet d'un « NAT source » avant d'atteindre l'appliance.

- Client d'itinérance - L'intégration d'Active Directory dans le client d'itinérance est possible lorsque le client d'itinérance est installé sur chaque ordinateur virtuel. Le déploiement de cette manière est plus facile lorsque chaque utilisateur a une connexion persistante (par ex. personnel) machine virtuelle.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.