Diplôme technicien spécialisé
En
Infrastructure digital option système et réseau

Rapport

Installation et configuration de l'accés a distance sous Windows Server 2019

Nom et prénom : Ouahman youssef
Filiére : infrastructur digitale

1

Sommaire

introduction 3

partie 1 4

concepts généraux sur VPN/MPS 5

VPN (Virtual Private Network) 5

Rôle du VPN (Virtual Private Network) 5

NPS (Network Policy Server) 6

RRôle de NPS (Network Policy Server) 6

partie 2 8

les étapes de configuration du VPN/NPS installation de la plate forme de test 9

étapes de configuration du VPN installation de la plate forme de test 3

étapes de configuration du NPS installation de la plate forme de test 11

instalation la plate forme de test protocole 13

PPTP (Point-to-Point Tunneling Protocol) 13

L2TP (Layer 2 Tunneling Protocol 13

STP (Spanning Tree Protocol) 13

Configuration spécifique pour différents protocoles 16

Configuration du protocole Sur la platforme de text 18

Intégration avec d'autres services 20

Base de données 20

Services tiers 20

Sécurité et confidentialité 20

Test et validation 20

conclusion 21

Remerciement 22

Introduction géneral

LL'accès à distance est une fonctionnalité essentielle pour les administrateurs système qui doivent gérer efficacement les serveurs à partir de différents emplacements. Sous Windows Server 2019, l'installation et la configuration de l'accès à distance sont des processus relativement simples, mais ils exigent une compréhension claire des étapes impliquées pour garantir la sécurité et la fiabilité du système.

Une fois que ces deux étapes sont effectuées, vous pouvez utiliser un autre ordinateur pour vous connecter à distance à votre serveur. Il vous suffit d'ouvrir l'application "Connexion Bureau à distance" sur votre ordinateur distant, de saisir l'adresse IP ou le nom de votre serveur, puis de vous connecter en utilisant vos informations d'identification.

L'accès à distance peut vous faire gagner beaucoup de temps et vous permettre de gérer votre serveur de manière pratique, où que vous soyez. Assurez-vous simplement de suivre les bonnes pratiques de sécurité pour protéger votre serveur contre tout accès non autorisé.

Partie 1:

4

concepts généraux sur VPN/MPS

VPN (Virtual Private Network) :

Un VPN est un réseau privé virtuel qui permet à un utilisateur de se connecter à un réseau sécurisé à partir d'un emplacement distant via Internet ou un réseau public. Il crée un tunnel crypté entre l'appareil de l'utilisateur et le serveur VPN, assurant ainsi la confidentialité et la sécurité des données échangées. Les VPN sont utilisés pour sécuriser les connexions à distance, contourner les restrictions géographiques et protéger la confidentialité en ligne.

Rôle du VPN (Virtual Private Network) :

Connexion sécurisée : Le principal rôle d'un VPN est de fournir une connexion sécurisée entre un utilisateur distant et un réseau privé, souvent à travers Internet. Il crée un tunnel crypté qui protège les données contre les interceptions et les atteintes à la confidentialité.

Accès distant : Les VPN permettent aux utilisateurs distants d'accéder aux ressources internes d'un réseau d'entreprise comme s'ils étaient physiquement présents sur site. Cela est crucial pour les employés travaillant à distance ou en déplacement, leur permettant d'accéder aux fichiers, aux applications et aux services internes en toute sécurité.

Contournement des restrictions géographiques : Les VPN sont souvent utilisés pour contourner les restrictions géographiques en masquant l'adresse IP de l'utilisateur et en lui permettant d'accéder à du contenu en ligne qui pourrait être restreint dans sa région géographique.

Sécurisation des connexions publiques : Lors de l'utilisation de réseaux Wi-Fi publics ou autres réseaux non sécurisés, un VPN assure la sécurité des données en cryptant le trafic, protégeant ainsi les utilisateurs contre les cyberattaques potentielles.

NPS (Network Policy Server) :

NPS est un service de serveur de rôle dans les systèmes d'exploitation Windows Server. Il fournit une plate-forme pour configurer et gérer l'authentification, l'autorisation et la comptabilité des connexions réseau. NPS est souvent utilisé pour définir des politiques réseau, authentifier les utilisateurs ou les appareils qui tentent de se connecter au réseau, autoriser l'accès en fonction des règles définies et enregistrer des informations de journalisation pour l'audit et la conformité..

RRôle de NPS (Network Policy Server) :

1. Authentification des utilisateurs et des appareils : NPS joue un rôle central dans l'authentification des utilisateurs et des appareils qui tentent de se connecter au réseau. Il vérifie les informations d'identification fournies par les utilisateurs et les appareils pour s'assurer de leur légitimité avant de leur accorder l'accès au réseau.

6

Autorisation d'accès : Une fois qu'un utilisateur ou un appareil est authentifié, NPS détermine les droits d'accès appropriés en fonction des politiques réseau définies. Cela peut inclure l'autorisation d'accéder à certaines ressources réseau ou de se connecter à certains services en fonction des paramètres configurés.
Comptabilité et journalisation : NPS enregistre des informations de comptabilité et de journalisation sur les activités des utilisateurs et des appareils connectés au réseau. Cela permet aux administrateurs réseau de surveiller l'utilisation du réseau, de générer des rapports d'audit et de garantir la conformité aux politiques de sécurité et de conformité.

Partie 2:

les étapes de configuration du VPN/NPS installation de la plate forme de test

- **étapes de configuration du VPN installation de la plate forme de test**

Préparation de l'environnement de test :
Sélectionnez un environnement de test isolé qui ne perturbera pas la production.
Configurez au moins deux machines virtuelles ou physiques pour représenter le serveur VPN et le client VPN.
Assurez-vous que chaque machine dispose des ressources nécessaires, notamment CPU, mémoire et stockage.
Installation du serveur VPN :
Choisissez le logiciel VPN approprié pour votre environnement de test (OpenVPN, IPSec, etc.).
Installez et configurez le serveur VPN selon les instructions du fournisseur.
Configurez les paramètres de sécurité, y compris le chiffrement et les méthodes d'authentification.
Configuration du serveur VPN :
Créez les certificats et les clés nécessaires pour le serveur VPN.
Configurez les règles de pare-feu pour permettre le trafic VPN entrant et sortant.
Définissez les adresses IP attribuées aux clients VPN et configurez les plages d'adresses IP disponibles.
Configuration du client VPN :
Installez le logiciel client VPN sur la machine désignée comme client.
Configurez les paramètres du client VPN pour se connecter au serveur VPN.
Testez la connexion VPN depuis le client pour vérifier la connectivité.
Tests de connectivité et de performances :
Vérifiez que le client peut se connecter au serveur VPN avec succès.
Testez les performances du VPN en transférant des fichiers de différentes tailles à travers la connexion.
Effectuez des tests de connectivité en simulant des scénarios réels d'utilisation du VPN.

Tests de sécurité :
Effectuez des tests de sécurité pour vérifier la robustesse de la configuration du VPN.
Vérifiez l'efficacité du chiffrement et de l'authentification en utilisant des outils appropriés.
Analysez les journaux du serveur VPN pour détecter les éventuelles tentatives d'attaque ou d'intrusion.
Documentation et rapport :
Documentez toutes les étapes de configuration et les résultats des tests.
Créez un rapport détaillé sur la configuration du VPN, les tests effectués et les résultats obtenus.
Proposez des recommandations pour améliorer la sécurité et les performances du VPN si nécessaire.

10

étapes de configuration du NPS installation de la plate forme de test

1. Préparation de l'environnement de test :
   - Sélectionnez un environnement de test isolé, idéalement une machine virtuelle dédiée.
   - Assurez-vous que cette machine a accès au réseau pour communiquer avec les périphériques que vous souhaitez tester.
2. Installation du service NPS :
   - Sur votre machine de test, installez le service NPS à partir des fonctionnalités de Windows Server.
   - Suivez l'assistant d'installation pour configurer les paramètres de base.
3. Configuration du NPS pour l'authentification :
   - Ouvrez l'outil de gestion NPS à partir du Panneau de configuration.
   - Configurez les stratégies d'accès réseau pour spécifier les conditions d'accès au réseau.
   - Définissez les méthodes d'authentification (par exemple, Active Directory, certificats, etc.) selon les besoins de votre environnement.
4. Configuration des clients :
   - Ajoutez les clients qui seront autorisés à se connecter au réseau via NPS.
   - Configurez les paramètres de connexion sur les clients pour qu'ils puissent utiliser NPS comme serveur d'authentification.
5. Tests de connexion :
   - Testez la connexion en utilisant un client configuré pour se connecter à NPS.
   - Vérifiez que les utilisateurs autorisés peuvent se connecter avec succès et que les utilisateurs non autorisés sont refusés.
6. Configuration des stratégies réseau :
   - Définissez les politiques d'accès pour contrôler qui peut accéder au réseau, à quel moment et dans quelles conditions.
   - Configurez des règles pour autoriser ou refuser l'accès en fonction de différents critères (utilisateur, groupe, heure, etc.).
7. Tests de politique :
   - Testez les politiques définies en vérifiant qu'elles sont appliquées comme prévu.

11

Vérifiez que les utilisateurs sont autorisés ou refusés en fonction des conditions définies dans les stratégies.
8. Surveillance et débogage :
Surveillez les journaux du NPS pour détecter les éventuels problèmes de connexion ou d'authentification.
Effectuez des tests de débogage pour résoudre les problèmes éventuels et ajustez la configuration en conséquence.
9. Documentation et rapport :
Documentez la configuration du NPS, y compris les stratégies mises en place et les paramètres de sécurité.
Créez un rapport détaillé sur les tests effectués, les résultats obtenus et les éventuelles recommandations pour améliorer la configuration.

12

instalation la plate forme de test: protocole

- PPTP (Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol°
- STP (Spanning Tree Protocol)

13

PPTP (Point-to-Point Tunneling Protocol) :

PPTP est un protocole de tunneling utilisé pour créer des connexions VPN sécurisées sur des réseaux publics comme Internet.
Il permet à des utilisateurs distants de se connecter en toute sécurité à un réseau privé à travers un tunnel chiffré.
PPTP est généralement intégré aux systèmes d'exploitation Windows et est largement pris en charge par de nombreux routeurs et périphériques réseau.

L2TP (Layer 2 Tunneling Protocol) :

L2TP est un protocole de tunneling utilisé pour établir des connexions VPN, souvent en combinaison avec des protocoles de chiffrement comme IPsec (Internet Protocol Security).
Il permet la création de tunnels de communication sécurisés entre deux points sur un réseau, typiquement entre un client et un serveur VPN.
L2TP est utilisé pour transporter des données encapsulées sur le réseau, offrant ainsi une confidentialité et une intégrité des données.

STP (Spanning Tree Protocol) :

STP est un protocole de réseau utilisé pour empêcher les boucles de commutation dans les réseaux Ethernet en détectant et en éliminant les chemins redondants.
Il permet de créer un graphe de connectivité sans boucle pour les commutateurs Ethernet, garantissant ainsi la fiabilité et la stabilité des réseaux locaux.
STP fonctionne en désactivant sélectivement certains liens dans le réseau pour créer un seul chemin logique entre tous les appareils.

15

configuration du protocole Sur la platforme de text

Accès à l'interface de configuration :

Connectez-vous à l'interface d'administration ou de configuration de votre plateforme de test de texte. Cela peut être un tableau de bord en ligne, une interface de ligne de commande ou un panneau de contrôle.
Identification des options de configuration :

Recherchez les paramètres de configuration liés au protocole que vous souhaitez configurer. Par exemple, si vous utilisez une application de messagerie, vous devrez peut-être configurer les paramètres SMTP, POP3 ou IMAP.
Configuration du protocole :

Sélectionnez le protocole que vous souhaitez configurer (par exemple, SMTP pour l'envoi de courriels).
Entrez les informations requises telles que les serveurs de messagerie, les ports, les options d'authentification, etc.
Pour d'autres plateformes de test, telles que des chatbots, vous devrez peut-être configurer des protocoles de communication tels que HTTP, WebSocket, etc.
Validation et tests :

16

Une fois la configuration terminée, effectuez des tests pour vous assurer que le protocole fonctionne correctement.
Par exemple, envoyez un courriel de test pour vérifier la fonctionnalité SMTP, ou envoyez des requêtes HTTP pour tester une API.
Sécurité :

Assurez-vous que la configuration du protocole respecte les meilleures pratiques de sécurité. Cela peut inclure l'utilisation de connexions chiffrées (HTTPS), l'authentification sécurisée, etc.
Documentation et suivi :

Documentez la configuration du protocole pour référence future. Incluez les détails des paramètres configurés ainsi que toute information importante.
Maintenance et support :

Mettez en place des procédures de maintenance régulières pour surveiller les performances du protocole et effectuer des ajustements si nécessaire.
Fournissez un support technique aux utilisateurs en cas de problèmes ou de questions liés à la configuration du protocole.

Configuration spécifique pour différents protocoles

SMTP (Simple Mail Transfer Protocol) :
Pour configurer l'envoi de courriels, vous devrez fournir les paramètres du serveur SMTP, tels que l'adresse du serveur SMTP, le numéro de port (généralement 25, 465 ou 587), les informations d'authentification (nom d'utilisateur, mot de passe), etc.
Assurez-vous que les adresses d'expéditeur et de destinataire sont correctement définies pour les tests.
POP3 (Post Office Protocol version 3) et IMAP (Internet Message Access Protocol) :

Si vous souhaitez tester la réception de courriels, vous devrez configurer les paramètres POP3 ou IMAP. Cela inclut généralement les informations du serveur (adresse du serveur POP3/IMAP, numéro de port), les informations d'authentification, etc.
Assurez-vous que les boîtes aux lettres de test sont correctement configurées sur le serveur de messagerie pour recevoir les courriels.

18

HTTP (Hypertext Transfer Protocol) et HTTPS (HTTP Secure) :
Si votre plateforme de test implique des interactions HTTP, configurez les paramètres de connexion HTTP ou HTTPS en fonction de vos besoins. Cela peut inclure les URL des endpoints, les méthodes HTTP (GET, POST, etc.), les en-têtes de requête, les données de formulaire, etc.
WebSocket :

Si vous utilisez des connexions WebSocket pour des communications en temps réel, configurez les paramètres WebSocket. Cela comprend généralement les URL des endpoints WebSocket, les en-têtes WebSocket, les messages à envoyer, etc.

Intégration avec d'autres services

Base de données :
Si votre plateforme de test doit interagir avec une base de données, configurez les paramètres de connexion à la base de données. Cela peut inclure les informations de connexion (hôte, port, nom d'utilisateur, mot de passe), le type de base de données, etc.
Services tiers :
Si votre plateforme de test utilise des services tiers tels que des API externes, des services cloud, etc., configurez les paramètres de connexion et d'authentification nécessaires pour ces services.
Sécurité et confidentialité :
Pour tous les protocoles, assurez-vous de prendre en compte les mesures de sécurité appropriées. Cela peut inclure l'utilisation de connexions chiffrées (SSL/TLS), l'authentification sécurisée, la gestion des jetons d'authentification, etc.
Test et validation :
Après la configuration, effectuez des tests approfondis pour vous assurer que les fonctionnalités fonctionnent comme prévu. Cela peut inclure l'envoi de courriels de test, l'accès à des ressources HTTP/HTTPS, etc.

20

Conclusion

la configuration de l'accès à distance sous Windows Server 2019 en utilisant VPN et NPS est une étape cruciale pour permettre aux utilisateurs distants de se connecter de manière sécurisée au réseau de votre organisation. En suivant les étapes mentionnées, vous pouvez établir un environnement d'accès à distance robuste qui répond aux besoins de sécurité et de performance de votre organisation.

Il est essentiel de comprendre les concepts de base du VPN et du NPS pour configurer efficacement ces services. De plus, une planification minutieuse de l'architecture réseau et des paramètres de sécurité est nécessaire pour garantir une configuration fiable et sécurisée.

Une fois la configuration terminée, il est important de tester la connexion à distance, de surveiller régulièrement les performances du serveur et de maintenir la sécurité en appliquant les mises à jour et correctifs appropriés.

En suivant ces bonnes pratiques et en restant attentif aux évolutions de la technologie et aux menaces potentielles, vous pouvez offrir à vos utilisateurs un accès à distance sûr et fiable aux ressources de votre organisation.

Remerciement

Nous tenons à exprimer notre sincère gratitude à tous ceux qui ont contribué à la réalisation de ce rapport sur l'installation et la configuration de l'accès à distance sous Windows Server 2019.

Nous remercions tout particulièrement [insérer les noms ici], pour leur expertise technique et leurs précieux conseils tout au long du processus. Leur soutien a été indispensable pour comprendre les concepts fondamentaux du VPN, du NPS et pour surmonter les défis rencontrés lors de la configuration.

Nous souhaitons également exprimer notre reconnaissance envers [insérer les noms ici] pour leur assistance lors des tests et du débogage, ainsi que pour leur engagement à garantir que la solution mise en place réponde aux normes de sécurité et de performance les plus élevées.

Enfin, un grand merci à toute l'équipe pour sa collaboration et son dévouement à mener à bien ce projet. Chacun a apporté sa contribution unique, ce qui a permis d'aboutir à un résultat final réussi.

Nous sommes reconnaissants envers tous ceux qui ont soutenu ce projet et nous sommes impatients de continuer à travailler ensemble sur des initiatives futures.

22