Collège LaSalle
Montréal

INSTALLATION ET ADMINISTRATION DES RÉSEAUX (LEA.99)

Rapport de projet

DÉPLOIEMENT D'UN RÉSEAU D'ENTREPRISE MULTIPLATEFORMES

420-DR3-AS

Cezar Gurulea

2235092

27 novembre 2023

Sommaire

1. Introduction
    - Remerciements ---------- 2
    - Introduction ---------- 3
2. Installation et configuration de base des machines virtuelles
    - Topologie réseau et adressage IP ---------- 4
    - Hyperviseur - Hyper-V ---------- 5
    - Identification des noms d'hôtes, leur configuration et rôle ---------- 6
3. Installation et configuration des services d'infrastructure – première partie
    - Configuration d'Active Directory (ADDS) ---------- 10
    - RRAS, RIP, DHCP ---------- 11
    - Agent de relais DHCP ---------- 15
    - DNS Windows Server (primaire et secondaire) ---------- 17
    - GPO, Active Directory Users and Computers (ADUC), FGPP ---------- 21
    - Gestion des quotas ---------- 31
    - Restriction du type de fichier ---------- 32
4. Installation et configuration des services d'infrastructure – deuxième partie
    - NAT ---------- 35
    - Configuration Apache - **www.site3.com** ---------- 36
    - BIND DNS sur Linux Server ---------- 37
    - Configuration IIS – **www.site1.com** et **www.site2.com** ---------- 40
    - NFS, Samba, Script ---------- 45
    - Print Server (CUPS) ---------- 52
    - VPN et RADIUS ---------- 54
    - Terminal Server ---------- 61
    - WDS Server ---------- 64
    - Exchange Server ---------- 66
5. Problèmes rencontrés, méthodes de dépannage et recommandations. ---------- 70
6. Glossaire de termes techniques. ---------- 71
7. Conclusion ---------- 73

Remerciements

Chers Professeurs, du Collège LaSalle

A l'approche de la fin de notre parcours au collège, je tiens à exprimer ma profonde gratitude envers chacun d'entre vous. Votre dévouement, votre passion pour l'enseignement et votre engagement envers notre éducation ont laissé une empreinte indélébile dans nos vies.

Tout au long de la formation, vous avez été bien plus que des enseignants pour nous. Vous avez été des guides, des mentors et des modèles inspirants. Vos encouragements ont été les bouées de sauvetage dans les moments difficiles, et vos leçons vont bien au-delà des manuels scolaires. Vous nous avez enseigné la valeur du travail acharné, de la persévérance et de l'intégrité.

Votre passion pour vos matières respectives a allumé en nous la flamme de la curiosité et a nourri notre soif de connaissances. Chaque leçon était une aventure, chaque défi était une opportunité de grandir, grâce à vous.

Au-delà de l'enseignement académique, vous avez contribué à notre développement personnel. Vos conseils éclairés, votre soutien constant et vos encouragements ont renforcé notre confiance en nous et ont façonné notre vision du monde.

Alors que nous nous apprêtons à franchir cette étape importante de nos vies, nous emportons avec nous bien plus que des connaissances académiques. Nous emportons les leçons de vie précieuses que vous nous avez enseignées.

Merci du fond du cœur pour votre dévouement inlassable et votre impact positif sur notre éducation. Nous ne vous oublierons jamais et porterons vos enseignements avec nous tout au long de notre parcours.

Avec respect et reconnaissance,
Cezar Gurulea.

Introduction

Le but de ce projet est de configurer et d'optimiser les ressources informatiques du futur réseau de l'organisation Contoso. Le réseau est basé sur l'adresse IP 192.168.1.0/24, subdivisée en trois segments avec un masque /26.

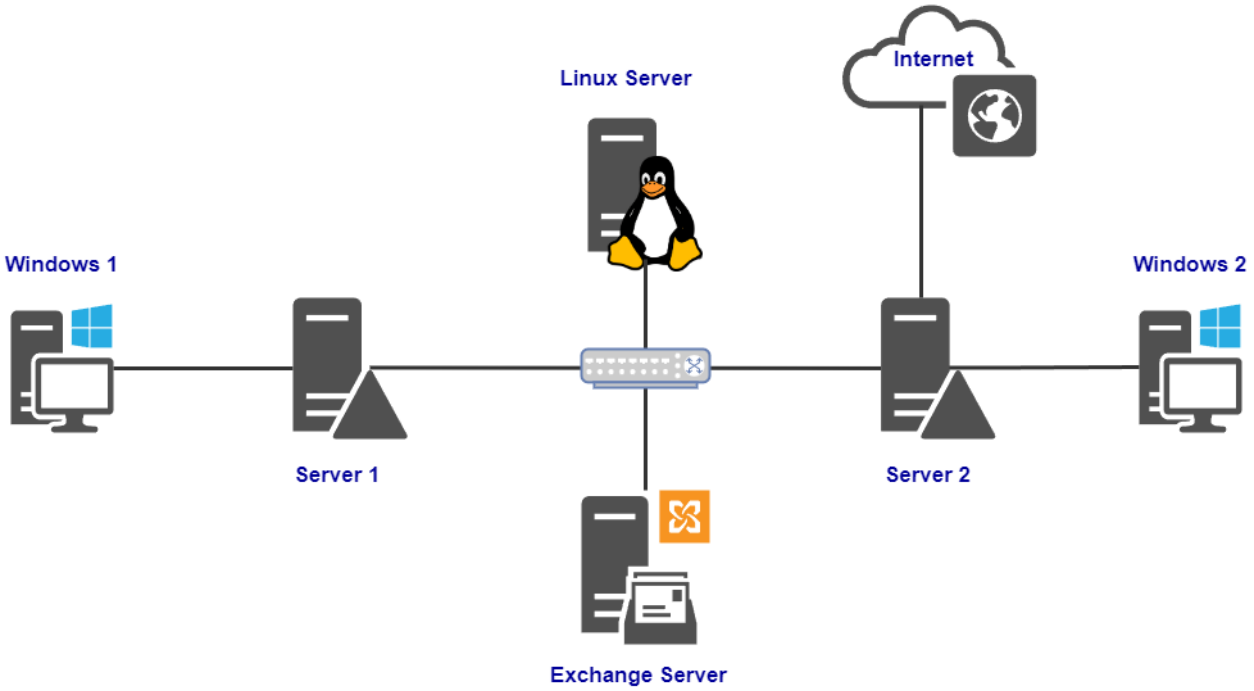
Il y a quatre serveurs dans le réseau, trois basés sur Windows Server 2022, dont l'un est un contrôleur de domaine, un autre est un sous-domaine, le troisième est un serveur Exchange, et un sur Alma Linux 9 (compatible binaire avec RHEL 9 / CentOS 9).

Le réseau est protégé par le NAT (Network Address Translation) et dispose d'un serveur VPN pour un accès distant. Différentes techniques de sécurité basées sur les GPO (Group Policy Objects) sont mises en œuvre dans le domaine. L'ensemble du réseau est routé à l'aide de RIPv2.

Même le DNS est basé sur trois serveurs pour assurer la redondance en cas de problèmes dans le réseau.

L'organisation gère trois sites web dirigés par IIS et Apache, la messagerie d'entreprise est gérée par Exchange Server, avec un accès vers l'extérieur vers Internet.

Topologie réseau et adressage IP



Réseaux :

Segment 1 – 192.168.1.0 / 26

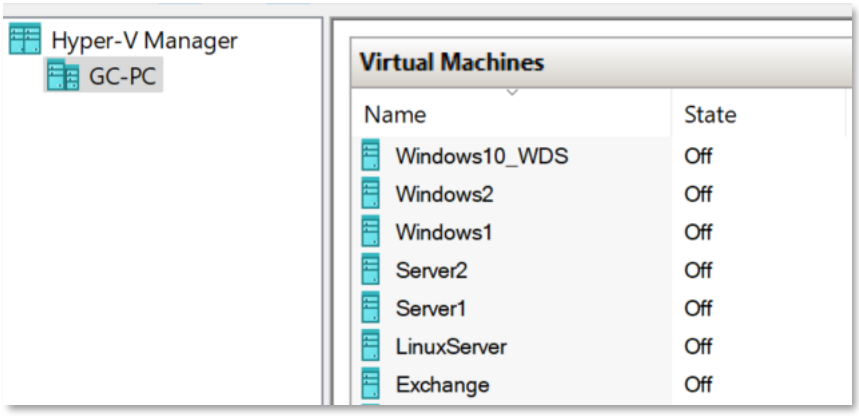
Segment 2 – 192.168.1.64 / 26

Segment 3 – 192.168.1.128 / 26

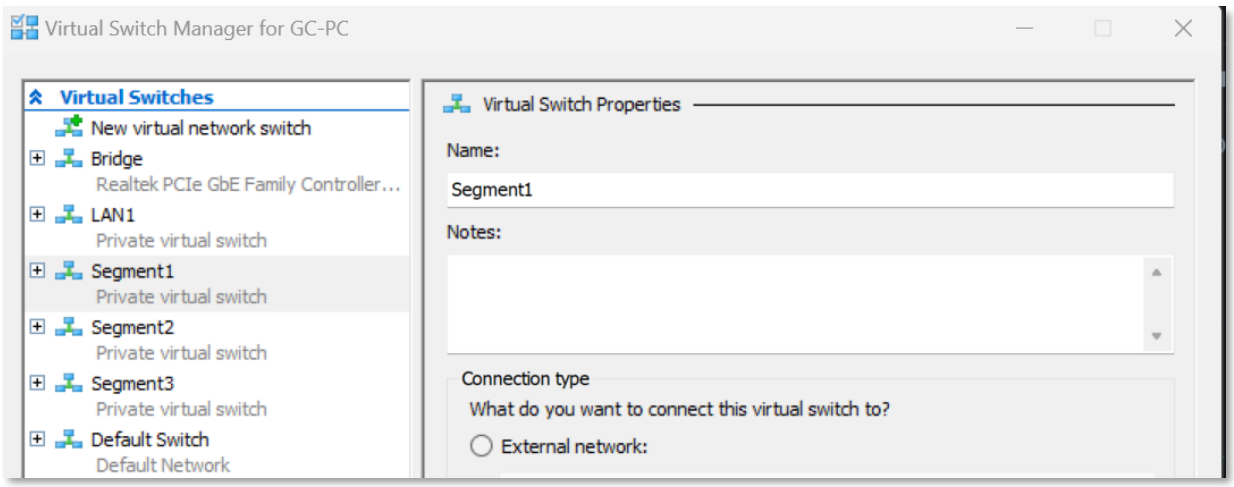
	Segment 1	Segment2	Segment3
Server1	192.168.1.10 / 26	192.168.1.70 / 26	-
Server2	-	192.168.1.80 / 26	192.168.1.130 / 26
LinuxServer	-	192.168.1.75 / 26	-
Exchange	-	192.168.1.85 / 26	-
Windows1	DHCP	-	-
Windows2	-	-	DHCP
Windows10_WDS	DHCP	-	-

Hyperviseur - Hyper-V

On a sept machines virtuelles. Quatre servers et trois clients.

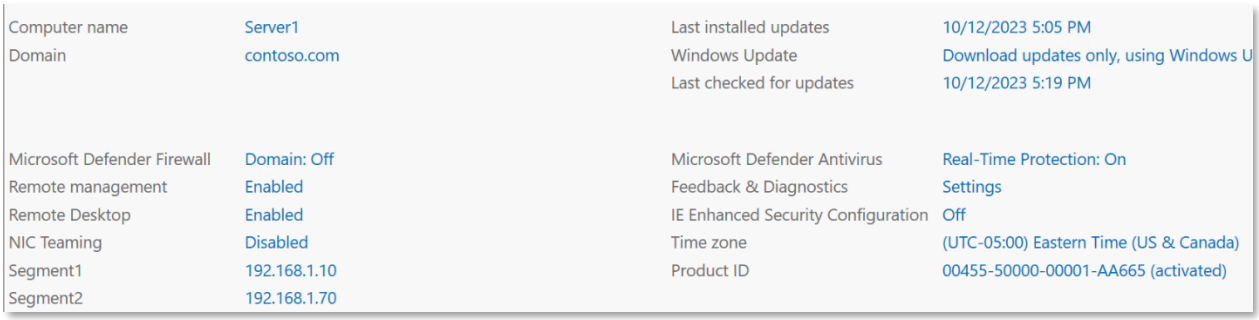


Le réseau est divisé en trois segments représentés par trois commutateurs virtuels, auxquels s'ajoute un commutateur Default Switch pour la connexion du réseau à Internet.



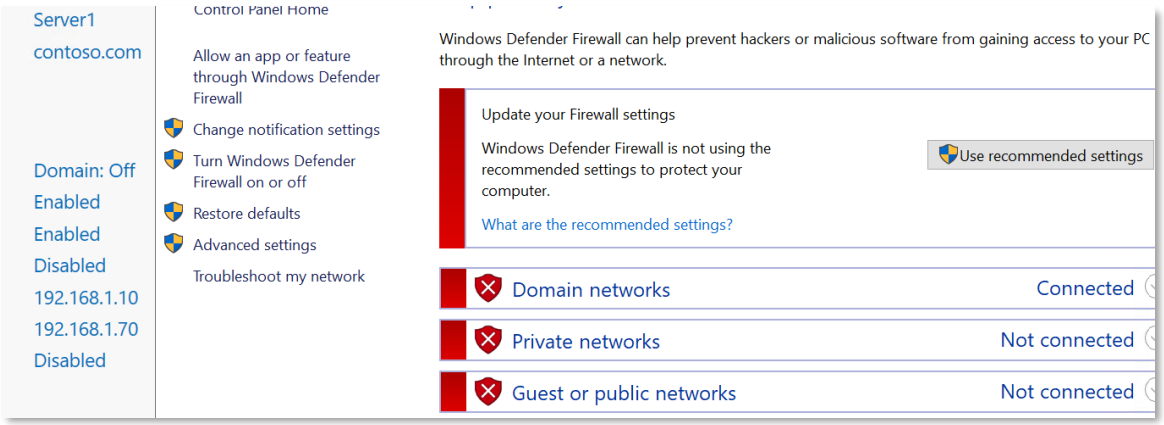
Identification des noms d'hôtes, leur configuration et rôles

Server1

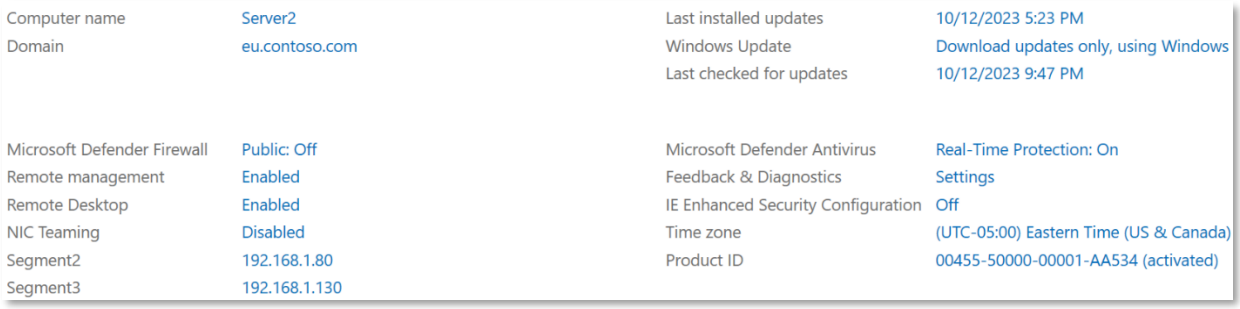


Computer name	Server1	Last installed updates	10/12/2023 5:05 PM
Domain	contoso.com	Windows Update	Download updates only, using Windows U
		Last checked for updates	10/12/2023 5:19 PM
Microsoft Defender Firewall	Domain: Off	Microsoft Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC-05:00) Eastern Time (US & Canada)
Segment1	192.168.1.10	Product ID	00455-50000-00001-AA665 (activated)
Segment2	192.168.1.70		

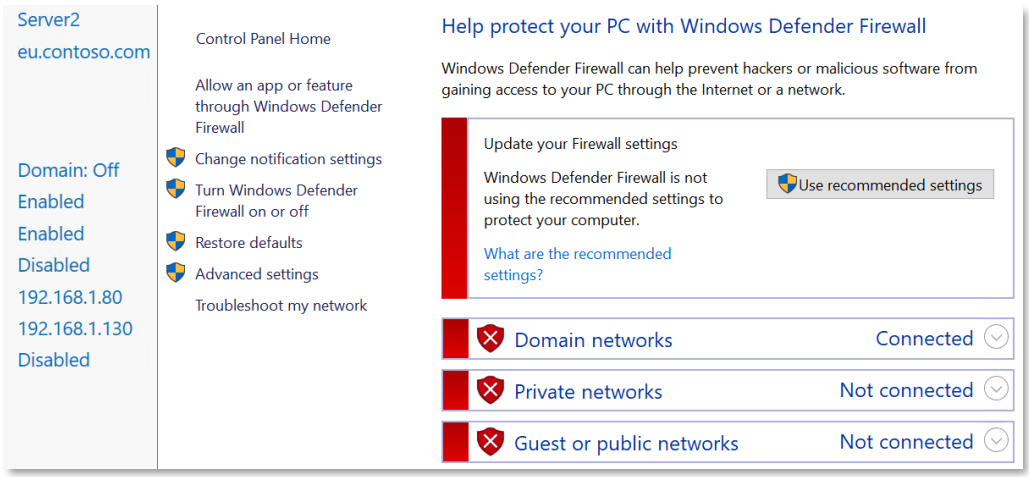
Nom d'hôte	Server1
Domaine	Contoso.com
Rôle	Contrôleur de domaine, NPS (Radius) server, DHCP server, Terminal server, IIS server, DNS
Système d'exploitation	Windows Server 2022
RAM	4 GB
CPU	1
HDD1	80 GB
HDD2	10 GB
Vidéo	MS remote display adapter
NIC1	Segment 1 – 192.168.1.10 / 26
NIC2	Segment 2 – 192.168.1.70 / 26



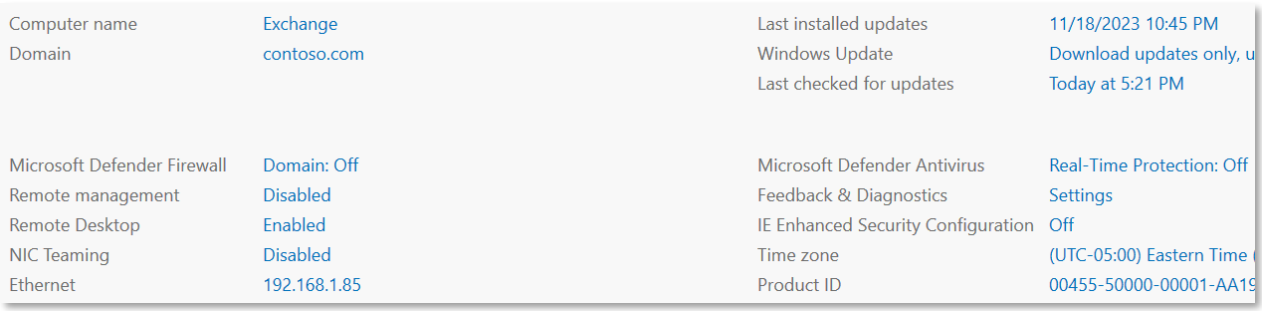
Server 2



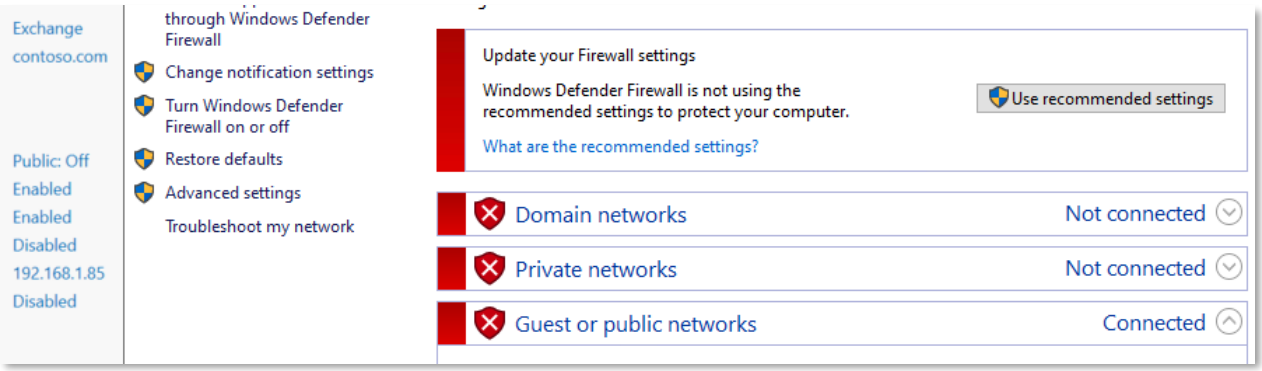
Nom d'hôte	Server2
Domaine	eu.contoso.com (part 1), contoso.com (part 2)
Rôle	Client de domaine, VPN server, NAT, Secondary DNS, DHCP relay agent
Système d'exploitation	Windows Server 2022
RAM	4 GB
CPU	1
HDD1	80 GB
Vidéo	MS remote display adapter
NIC1	Segment 2 – 192.168.1.80 / 26
NIC2	Segment 3 – 192.168.1.130 / 26
NIC3	NAT



Exchange Server



Nom d'hôte	Exchange
Domaine	contoso.com
Rôle	Client de domaine, Exchange server
Système d'exploitation	Windows Server 2022
RAM	16 GB
CPU	2
HDD1	80 GB
Video	MS remote display adapter
NIC1	Segment 2 – 192.168.1.85 / 26

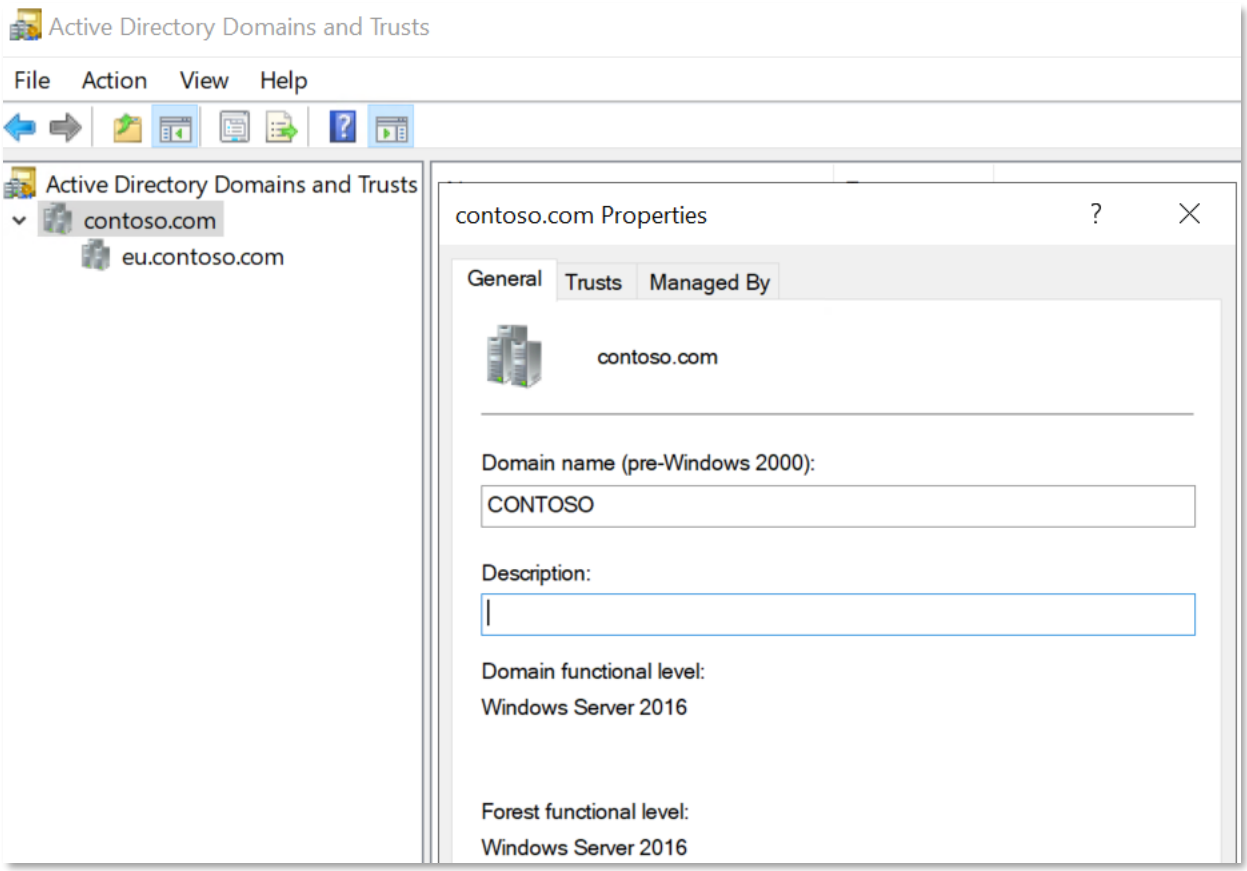


Linux Server

Nom d'hôte	linuxserver
Domaine	contoso.com
Rôle	Client de domaine, Web server, Slave DNS, Samba server, NFS server, Print server
RAM	4 GB
CPU	1
HDD1	40 GB
Video	MS Hyper-V virtual adapter
NIC1	Segment 2 – 192.168.1.75 / 26

Installation et configuration des services d'infrastructure – première partie

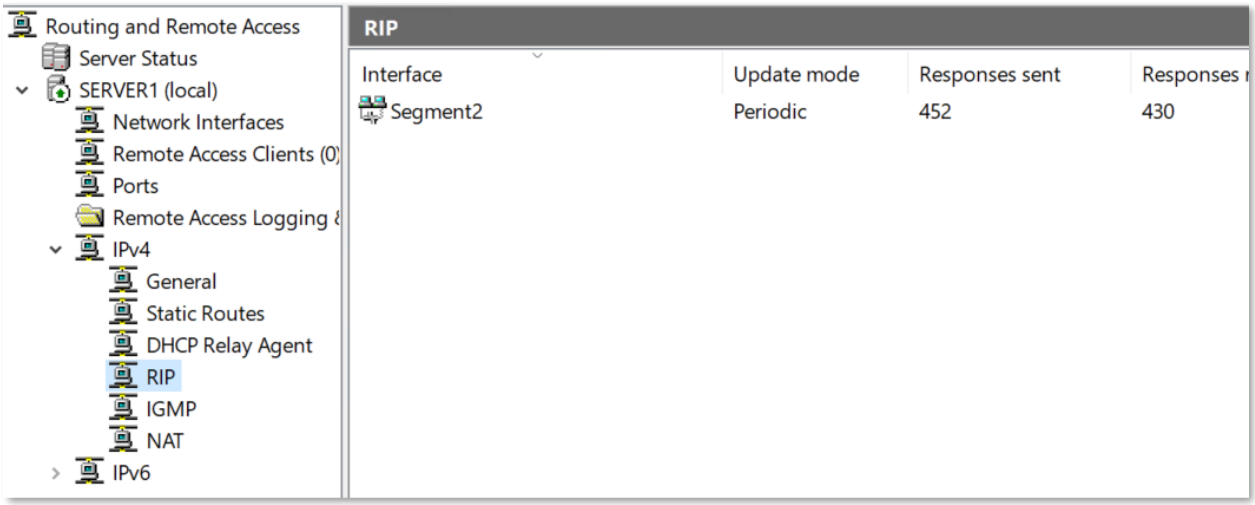
- Configuration de rôle Active Directory (ADDS) sur Server1 et child domaine sur Server2

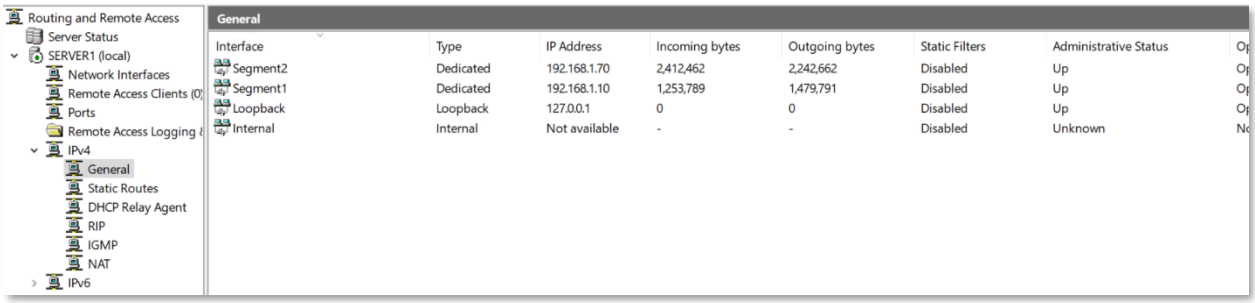


- RRAS, RIP, DHCP

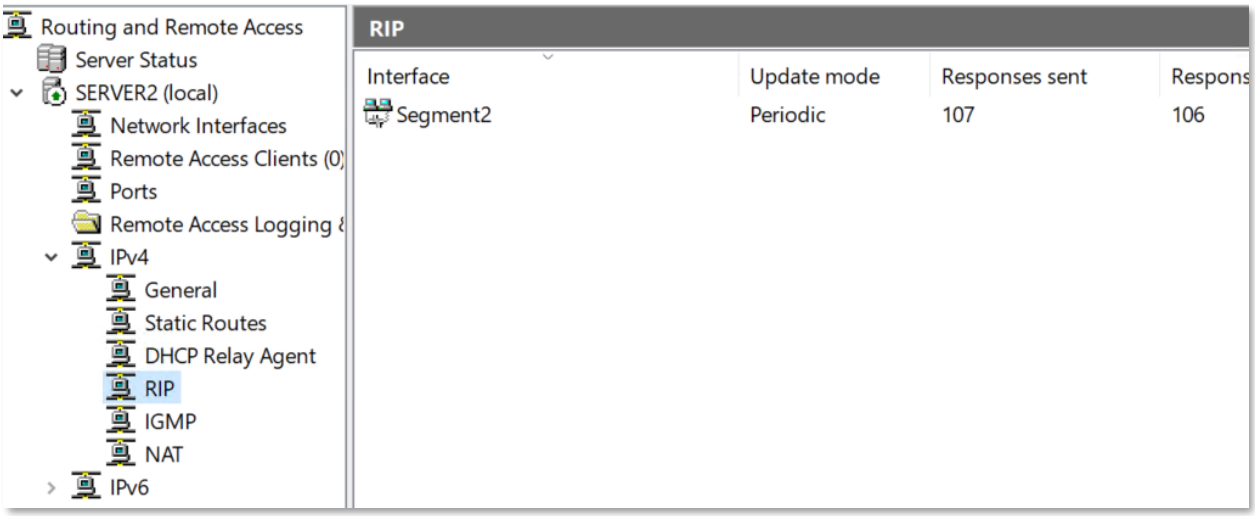
Entre les segments, le routage est assuré par le protocole RIPv2. Le rôle RRAS est installé sur Server1 et Server2. Server1 connecte les segments 1 et 2, tandis que Server2 connecte les segments 2 et 3. Dans la deuxième partie, il semble que Server2 sera également responsable de la liaison avec le NAT.

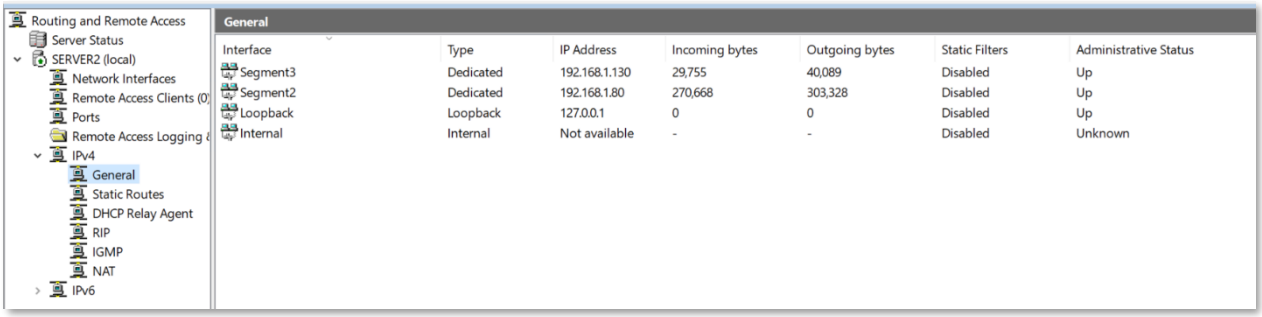
RIPv2 sur Server1





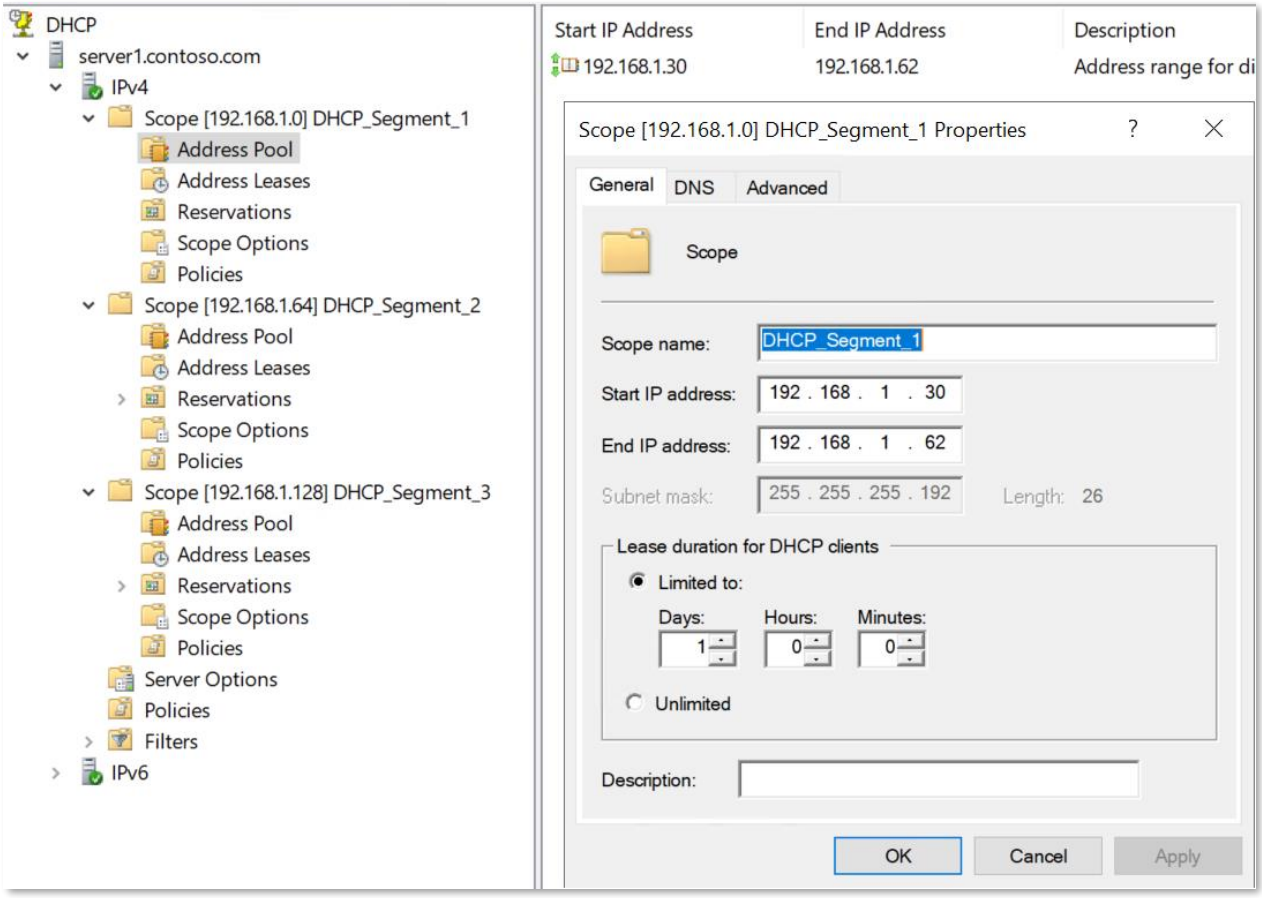
RIPv2 sur Server2

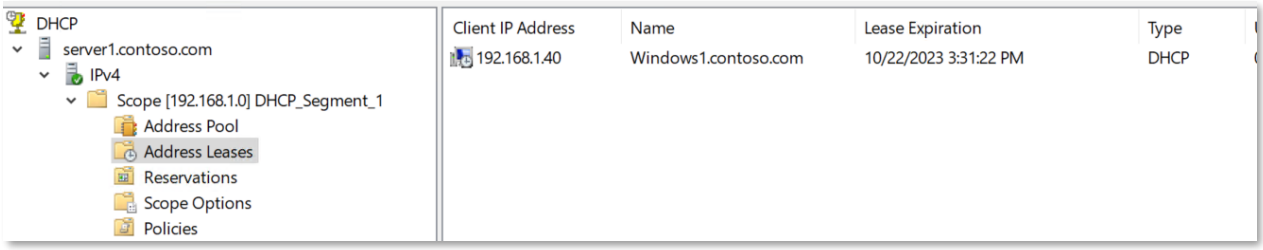


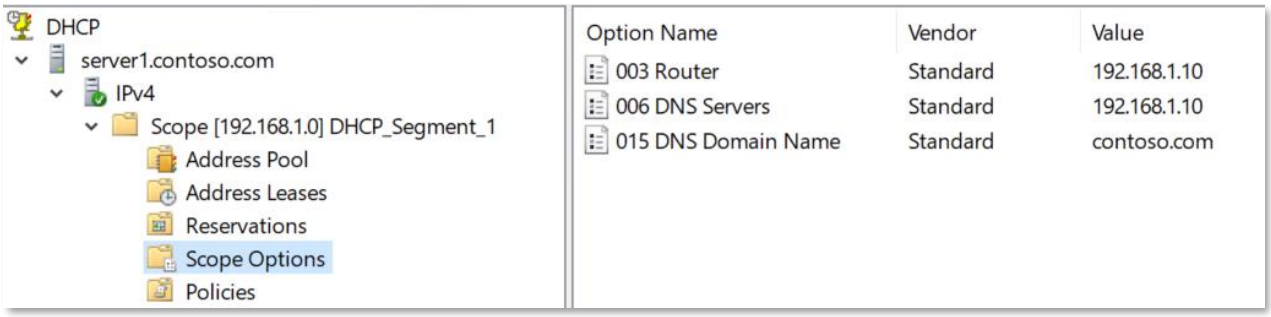


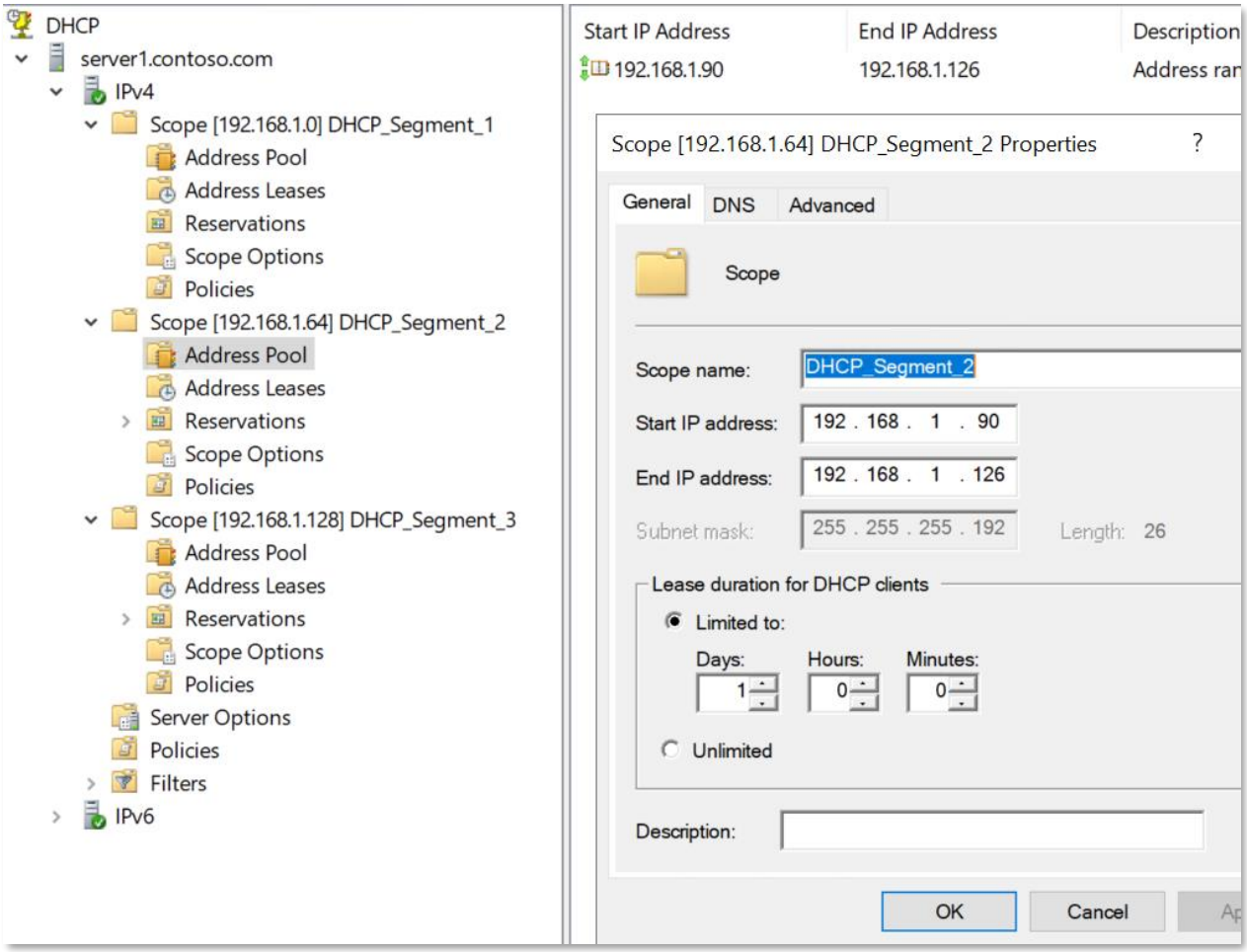
- DHCP server:

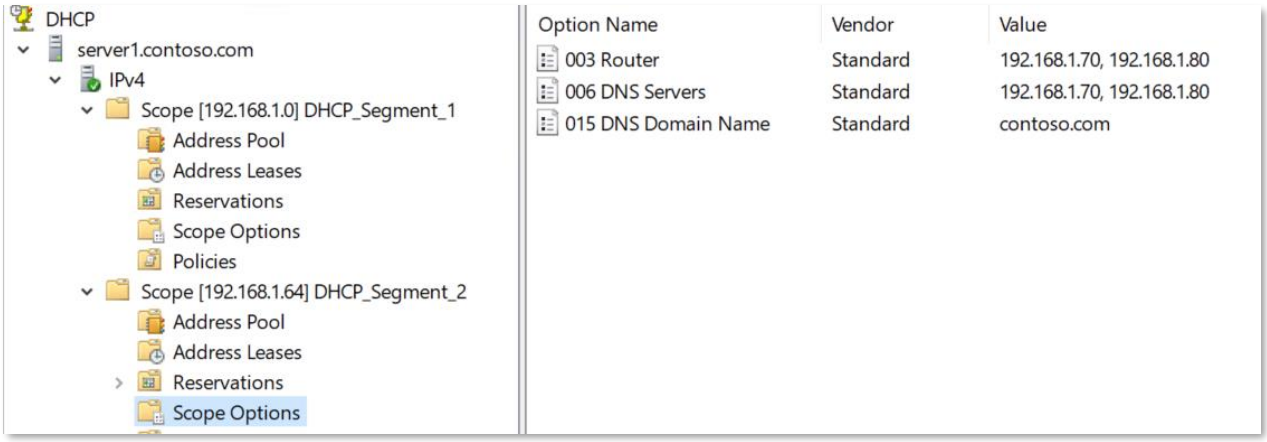
  Server1 remplit le rôle de serveur DHCP. Trois étendues DHCP distinctes sont configurées, chacune correspondant à l'un des trois segments du réseau. Cela permet à Server1 de distribuer automatiquement des adresses IP dans chacun de ces segments.

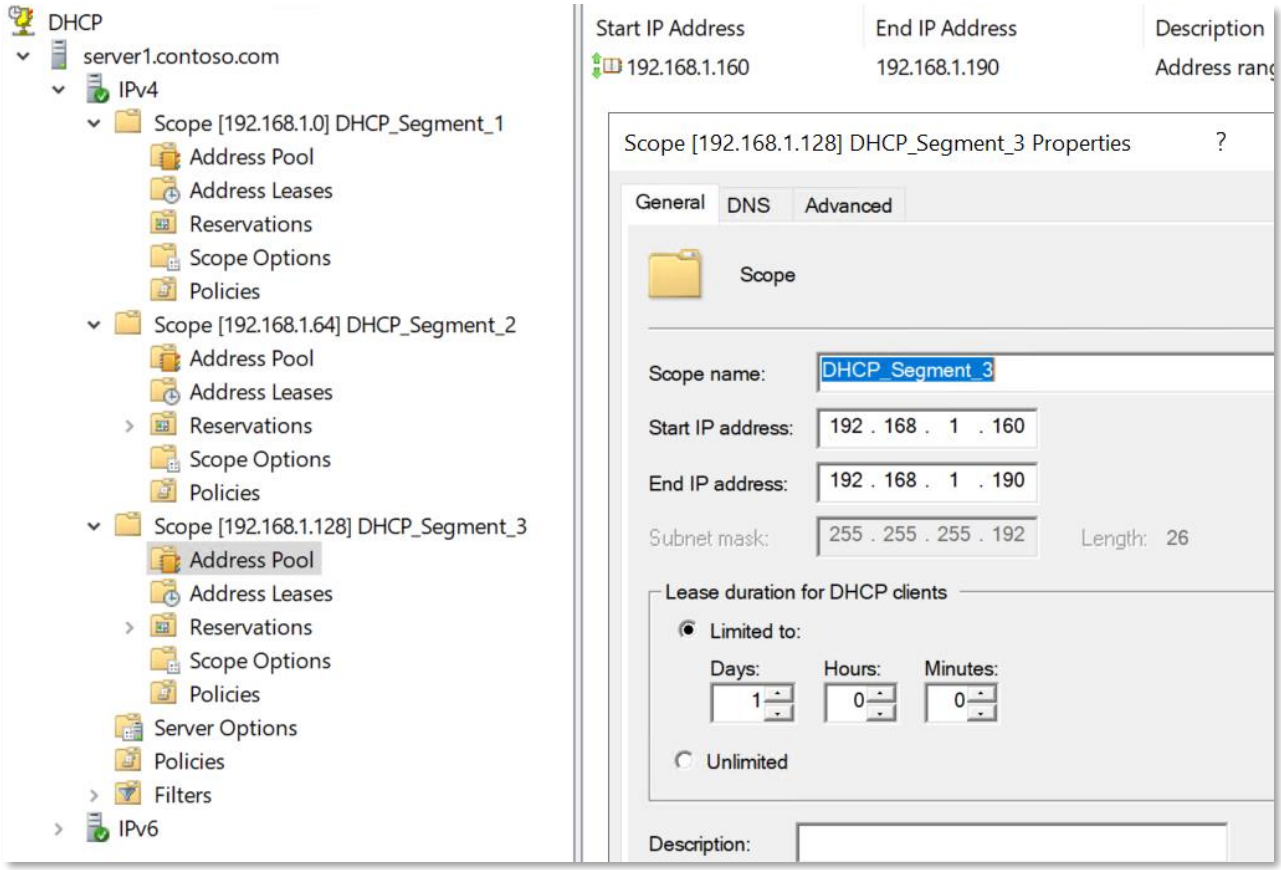



DHCP
server1.contoso.com
IPv4
Scope [192.168.1.0] DHCP_Segment_1
Address Pool
Address Leases
Reservations
Scope Options
Policies
Client IP Address
Name
Lease Expiration
Type
192.168.1.40
Windows1.contoso.com
10/22/2023 3:31:22 PM
DHCP

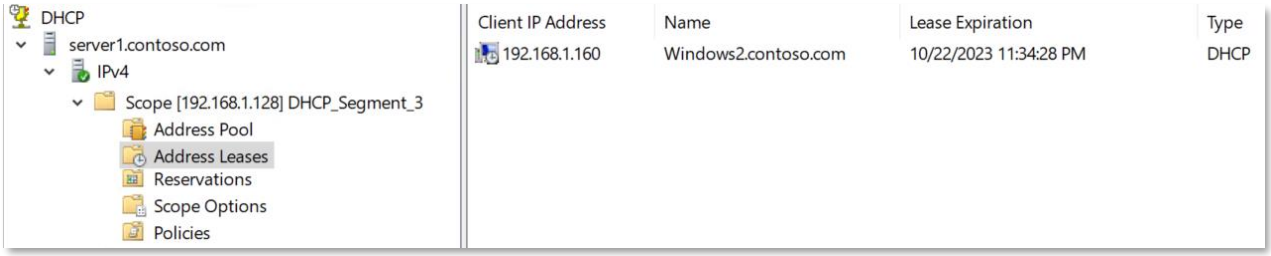

DHCP
server1.contoso.com
IPv4
Scope [192.168.1.0] DHCP_Segment_1
Address Pool
Address Leases
Reservations
Scope Options
Policies
Option Name
Vendor
Value
003 Router
Standard
192.168.1.10
006 DNS Servers
Standard
192.168.1.10
015 DNS Domain Name
Standard
contoso.com

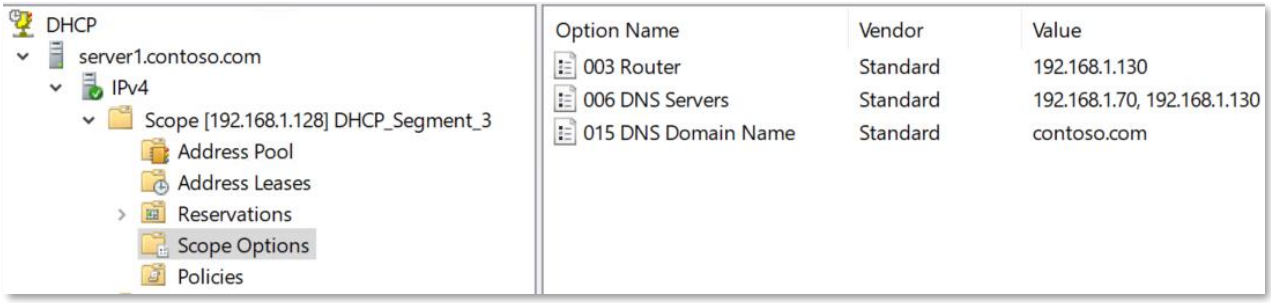

DHCP
server1.contoso.com
IPv4
Scope [192.168.1.0] DHCP_Segment_1
Address Pool
Address Leases
Reservations
Scope Options
Policies
Scope [192.168.1.64] DHCP_Segment_2
Address Pool
Address Leases
Reservations
Scope Options
Policies
Scope [192.168.1.128] DHCP_Segment_3
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
IPv6
Start IP Address
End IP Address
Description
192.168.1.90
192.168.1.126
Scope [192.168.1.64] DHCP_Segment_2 Properties
General
DNS
Advanced
Scope
Scope name:
DHCP_Segment_2
Start IP address:
192 . 168 . 1 . 90
End IP address:
192 . 168 . 1 . 126
Subnet mask:
255 . 255 . 255 . 192
Length: 26
Lease duration for DHCP clients
Limited to:
Days:
Hours:
Minutes:
1
0
0
Unlimited
Description:
OK
Cancel


DHCP
server1.contoso.com
IPv4
Scope [192.168.1.0] DHCP_Segment_1
Address Pool
Address Leases
Reservations
Scope Options
Policies
Scope [192.168.1.64] DHCP_Segment_2
Address Pool
Address Leases
Reservations
Scope Options
Option Name
Vendor
Value
003 Router
Standard
192.168.1.70, 192.168.1.80
006 DNS Servers
Standard
192.168.1.70, 192.168.1.80
015 DNS Domain Name
Standard
contoso.com


DHCP
server1.contoso.com
IPv4
Scope [192.168.1.0] DHCP_Segment_1
Address Pool
Address Leases
Reservations
Scope Options
Policies
Scope [192.168.1.64] DHCP_Segment_2
Address Pool
Address Leases
Reservations
Scope Options
Policies
Scope [192.168.1.128] DHCP_Segment_3
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
IPv6
Start IP Address
End IP Address
Description
192.168.1.160
192.168.1.190
Scope [192.168.1.128] DHCP_Segment_3 Properties
General
DNS
Advanced
Scope
Scope name:
DHCP_Segment_3
Start IP address:
192 . 168 . 1 . 160
End IP address:
192 . 168 . 1 . 190
Subnet mask:
255 . 255 . 255 . 192
Length: 26
Lease duration for DHCP clients
Limited to:
Days:
Hours:
Minutes:
1
0
0
Unlimited
Description:

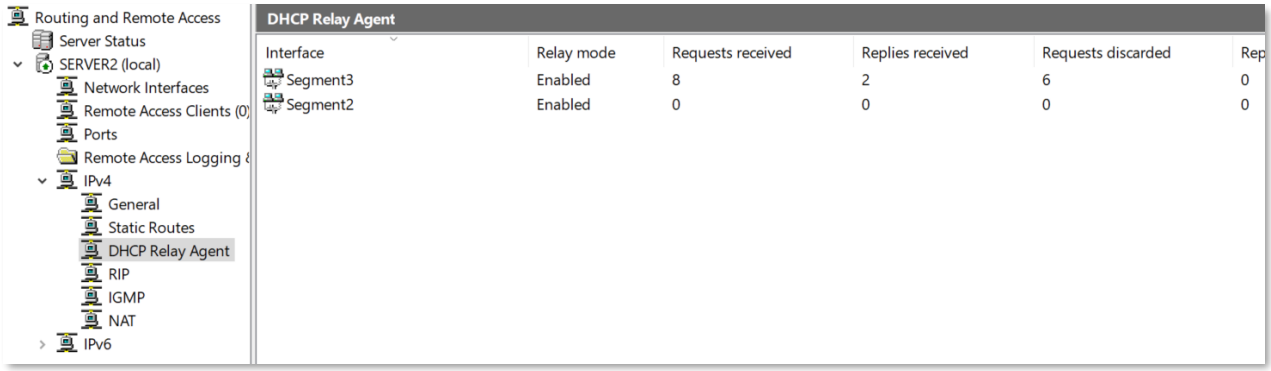
Si un relais DHCP est utilisé, cela signifie probablement que les clients DHCP, tels que Windows2 dans le Segment 3, envoient leurs demandes DHCP au serveur DHCP (Server1) à travers le relais DHCP situé sur le réseau. Ce relais DHCP agit comme un intermédiaire pour transmettre les demandes DHCP entre les clients et le serveur DHCP, facilitant ainsi la distribution d'adresses IP dans les différents segments du réseau.



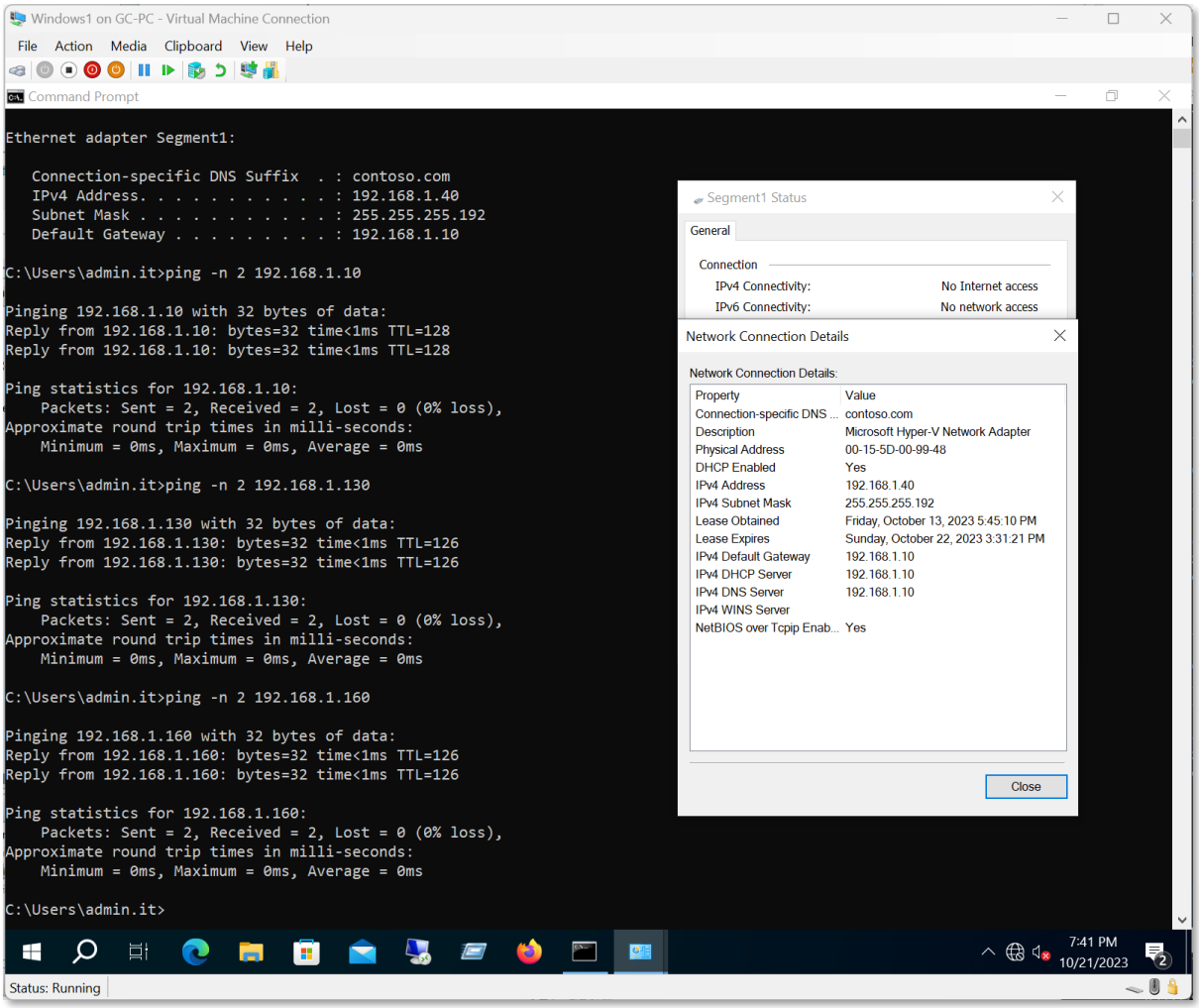


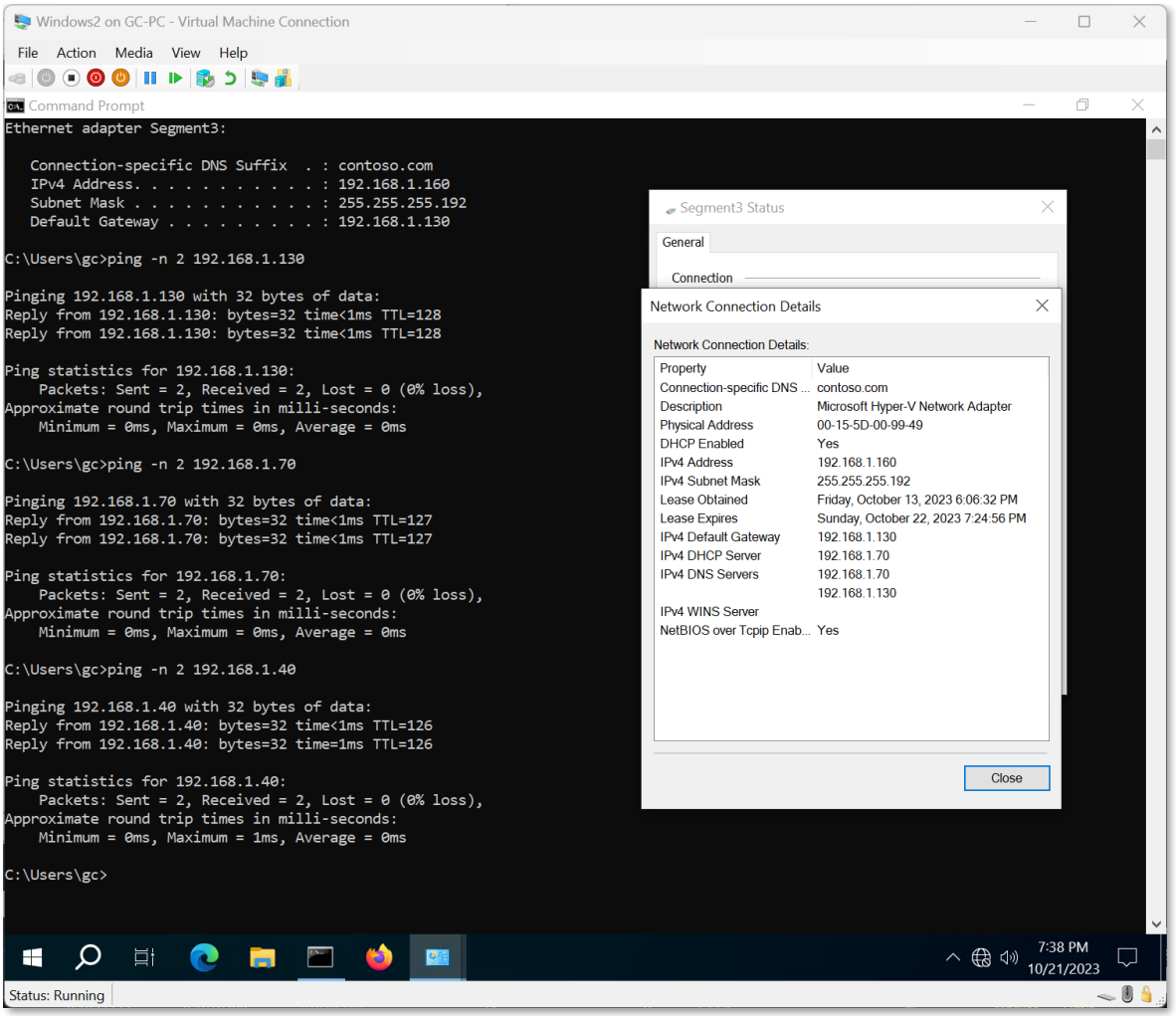
- Agent de relais DHCP

Server2 joue le rôle de relais DHCP agent pour distribuer les adresses DHCP dans le Segment 3. L'exemple mentionné précédemment montre que Server2 facilite la communication entre les clients DHCP du Segment 3 et le serveur DHCP (Server1), permettant ainsi la distribution d'adresses IP dans ce segment spécifique du réseau.



Si le ping réussit entre les clients des segments 1, 2 et 3, cela indique que le routage et la connectivité entre ces segments fonctionnent correctement. C'est un signe positif que la configuration du réseau et du routage, y compris les interactions DHCP, sont en ordre, et que les appareils des différents segments peuvent communiquer entre eux avec succès. Ceci est indispensable pour la configuration ultérieure des services réseau.

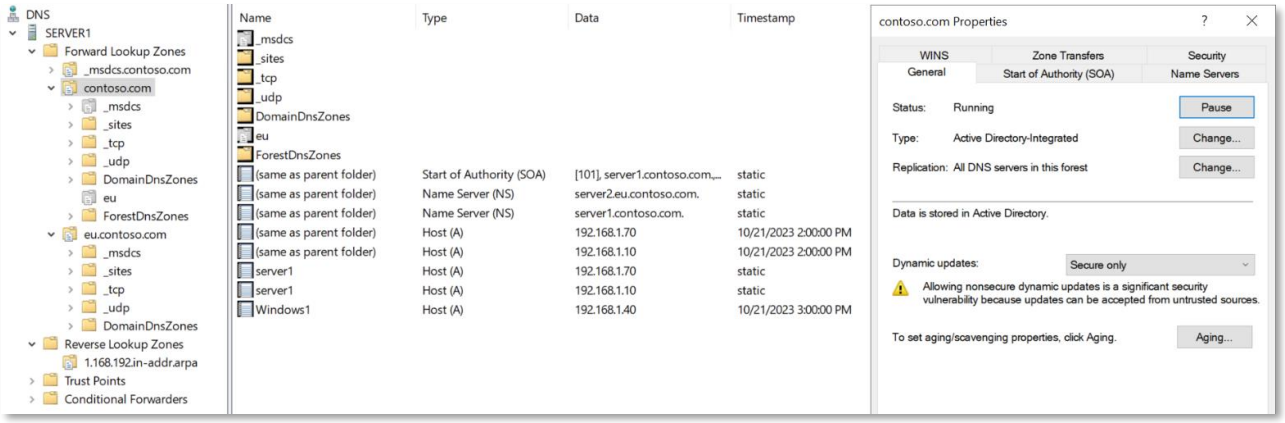


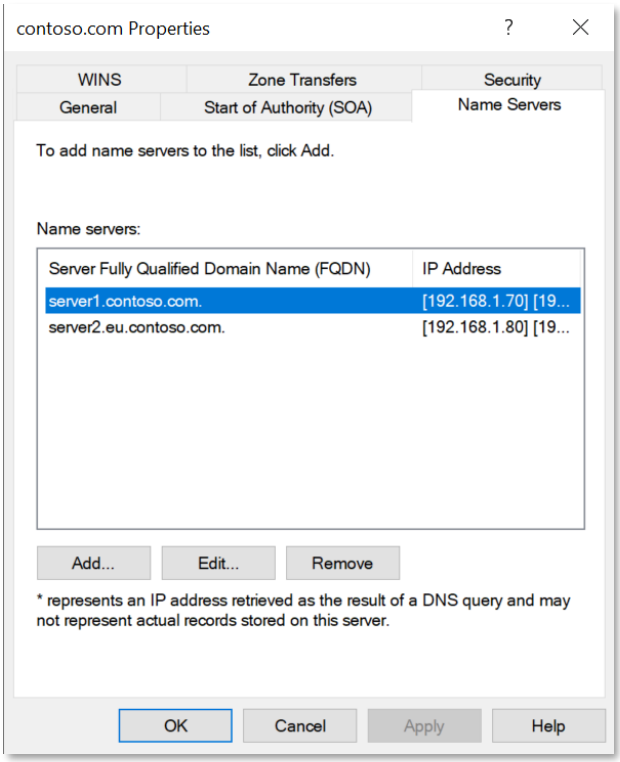


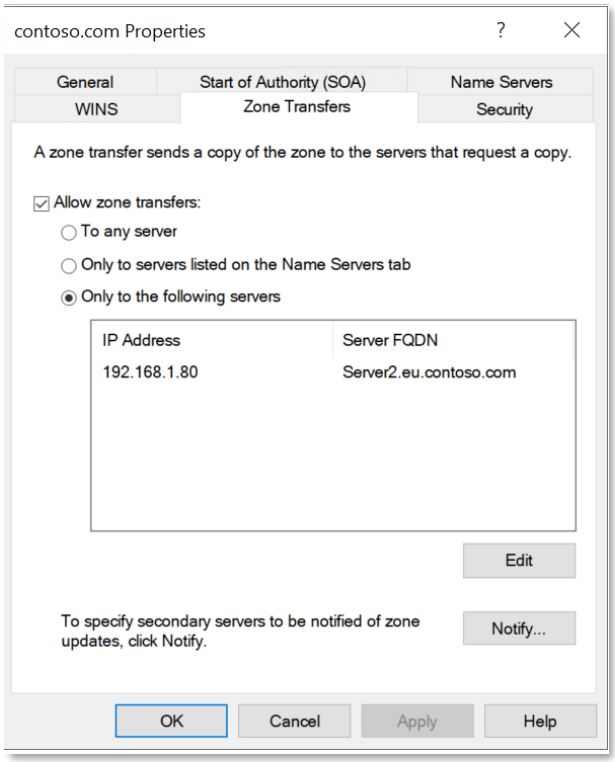
DNS Windows Server (primaire et secondaire)

À l'étape actuelle, la configuration DNS est effectuée sur deux serveurs, Server1 jouant le rôle de DNS principal et Server2 en tant que DNS secondaire. Cette configuration garantit une redondance DNS. De plus, Server1 prend en charge la zone contoso.com, tandis que Server2 gère la zone eu.contoso.com en tant que sous-domaine. Il y a également un transfert de zones entre les deux serveurs pour assurer la synchronisation des données.

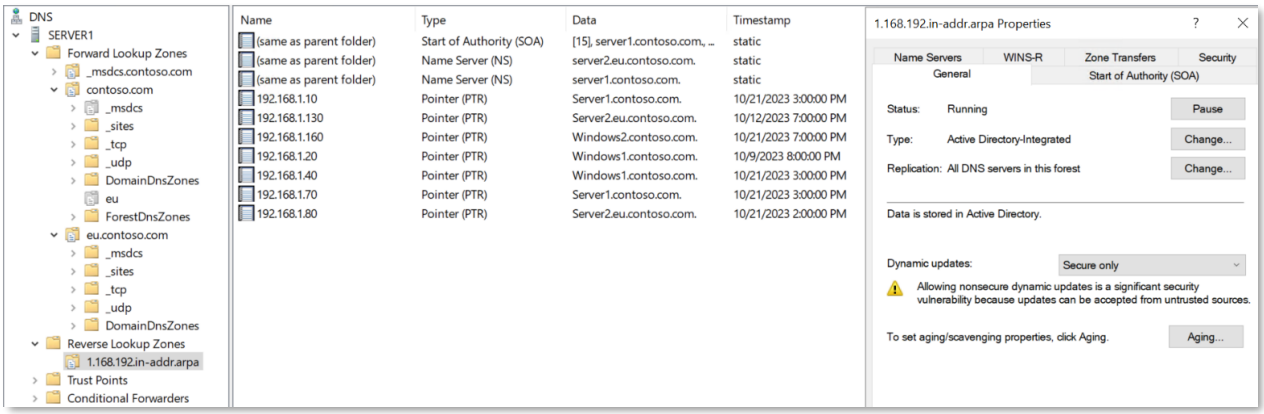
- Server1 – contoso.com zone



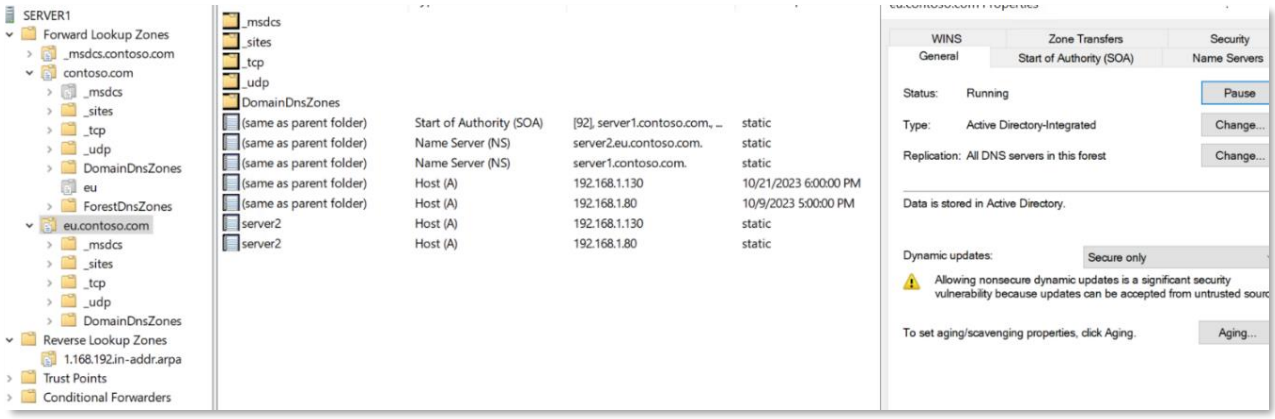




- Server1 – reverse zone

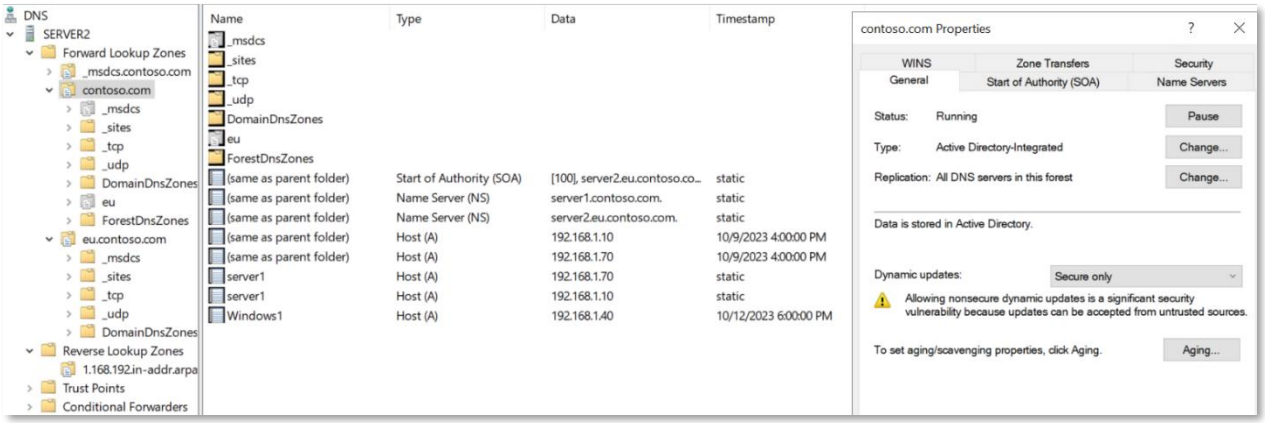


Ici, nous pouvons constater que la zone eu.contoso.com a été transférée vers Server1.

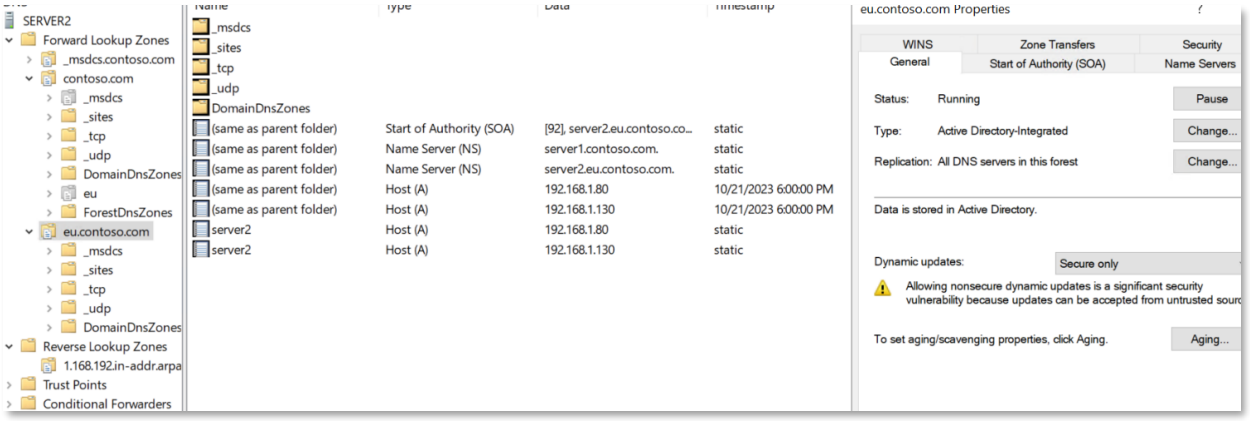


- Server2

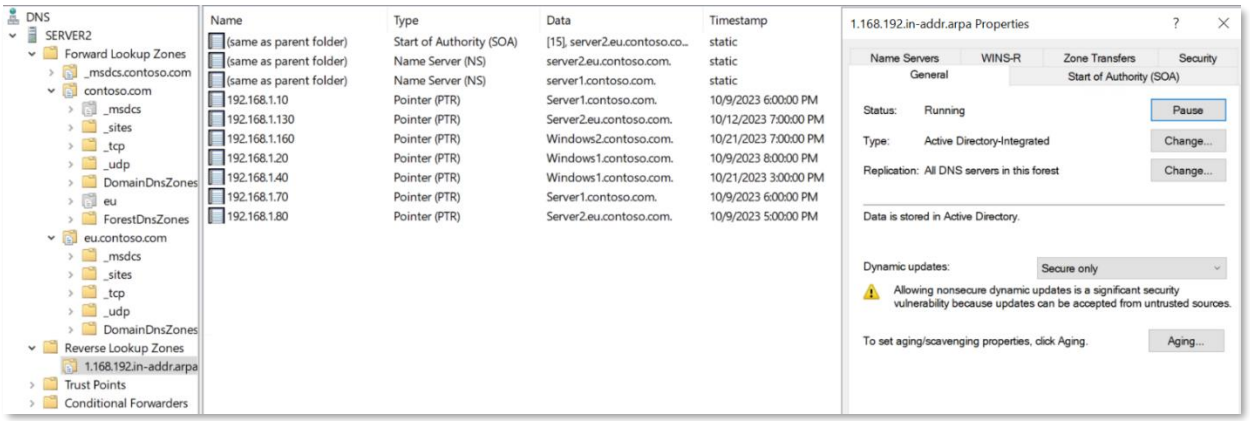
  La zone contoso.com a été transférée vers Server2.



Server2 – eu.contoso.com zone.



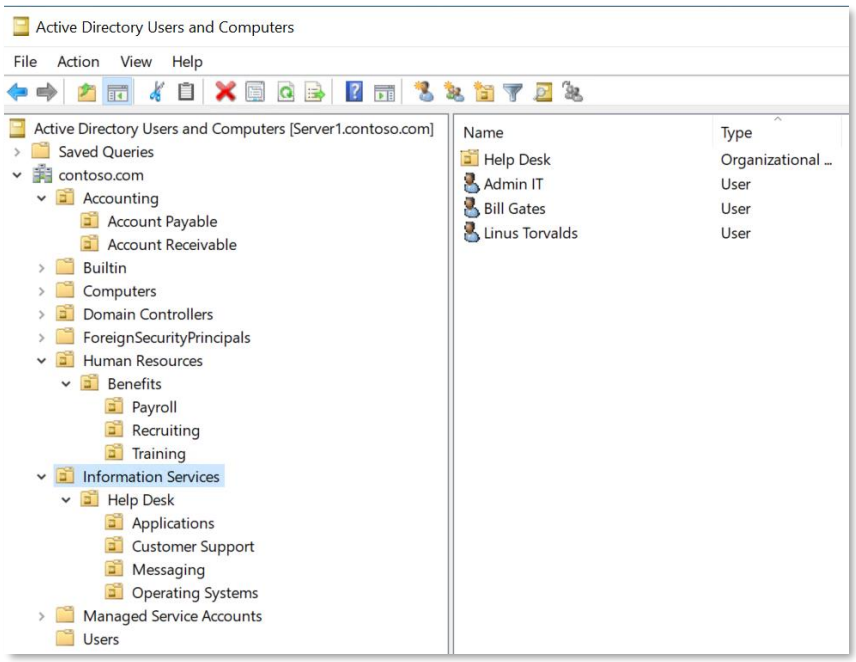
Server2 – reverse zone.



Dans la deuxième partie, on va ajouter trois zones secondaires supplémentaires sur Server1 pour site1.com, site2.com et site3.com.

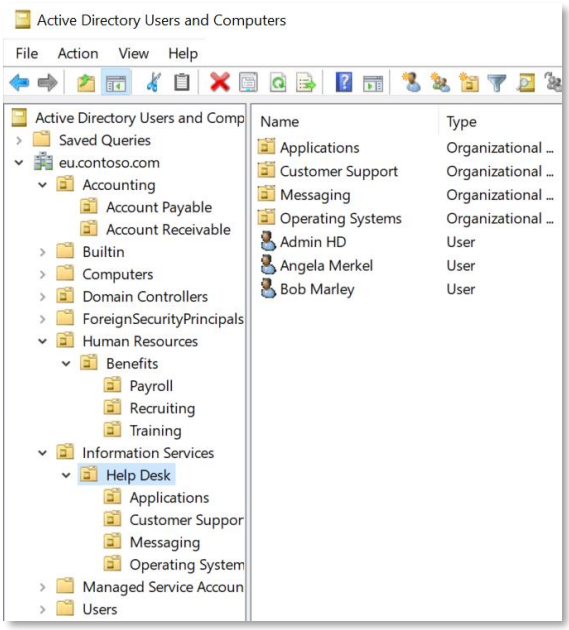
GPO, Active Directory Users and Computers (ADUC)

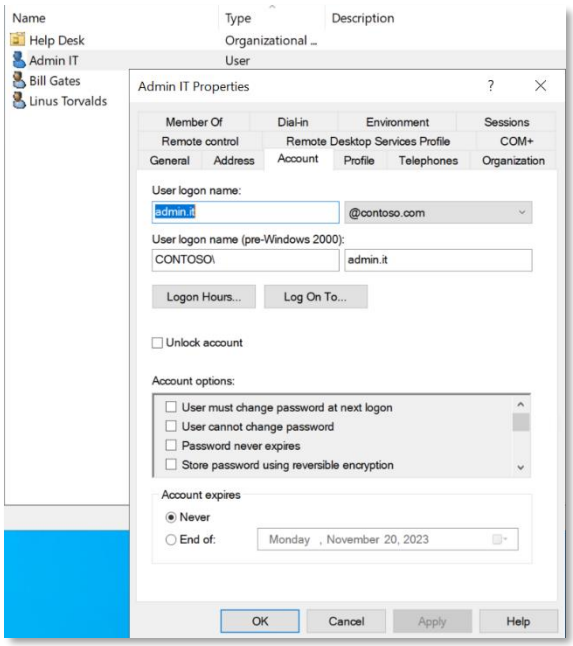
Dans l'organisation, il y a trois départements : Comptabilité (Accounting), Services Informatiques (Information Services) et Ressources Humaines (Human Resources). Pour chacun d'entre eux, une Unité Organisationnelle (OU) a été créée dans le domaine pour une gestion plus efficace et l'application de différentes politiques isolées. De plus, chaque OU contient plusieurs sous-OUs.

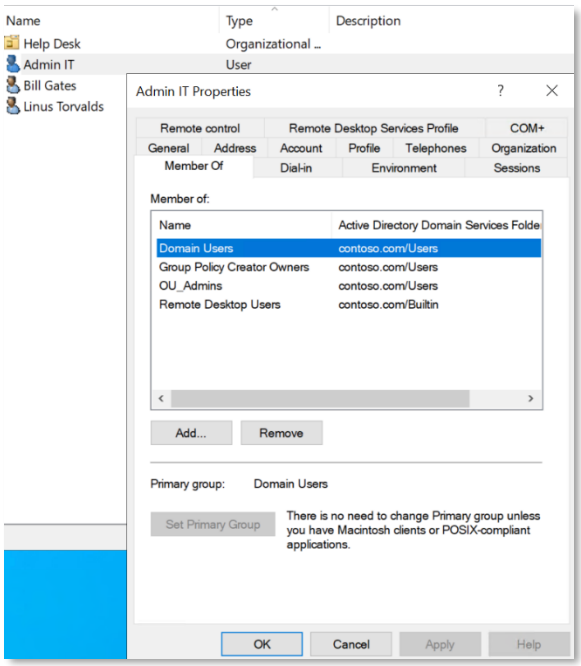


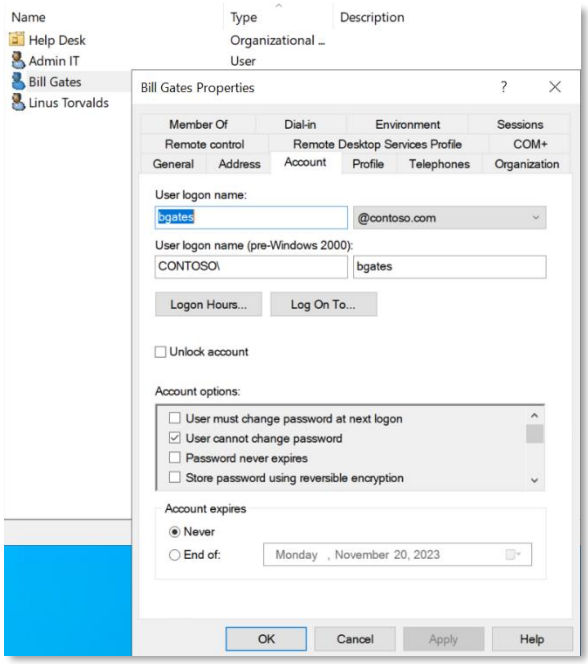
Chaque OU est gérée par un représentant du département, que nous appellerons administrateur de l'OU.

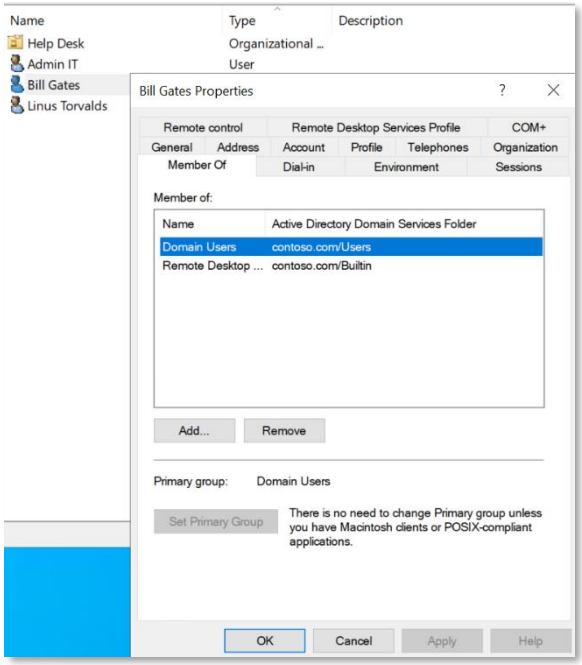
Par la suite, nous examinerons les politiques GPO créées et appliquées dans le domaine.



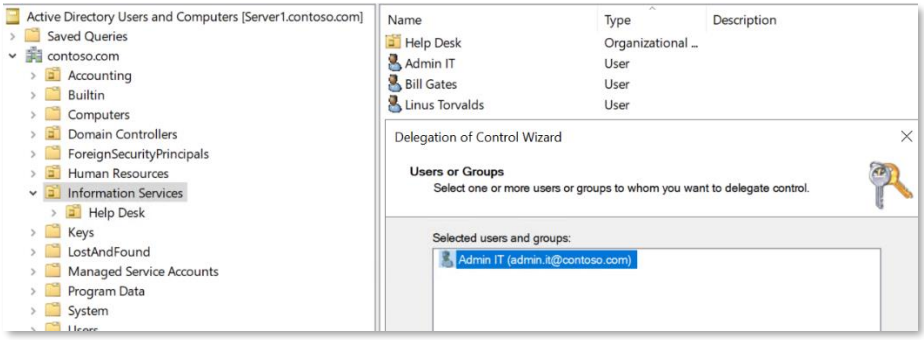

Name
Type
Description
Help Desk
Organizational ...
Admin IT
User
Bill Gates
Linus Torvalds
Admin IT Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
User logon name:
admin.it
@contoso.com
User logon name (pre-Windows 2000):
CONTOSO\
admin.it
Logon Hours...
Log On To...
Unlock account
Account options:
User must change password at next logon
User cannot change password
Password never expires
Store password using reversible encryption
Account expires
Never
End of:
Monday , November 20, 2023
OK
Cancel
Apply
Help

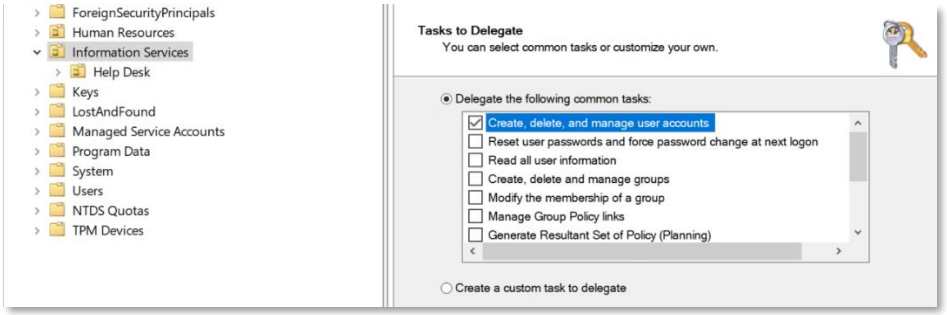

Name
Type
Description
Help Desk
Organizational ...
Admin IT
User
Bill Gates
Linus Torvalds
Admin IT Properties
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Domain Services Folde
Domain Users
contoso.com/Users
Group Policy Creator Owners
contoso.com/Users
OU_Admins
contoso.com/Users
Remote Desktop Users
contoso.com/Builtin
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help

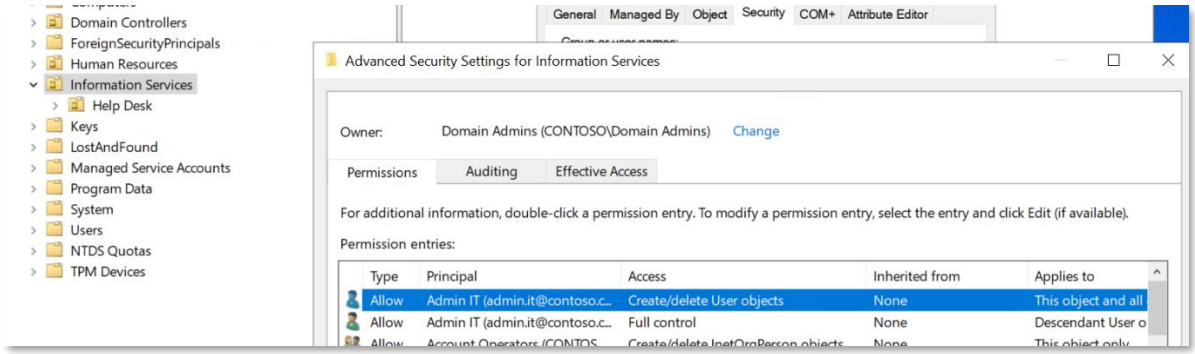

Name
Type
Description
Help Desk
Organizational ...
Admin IT
User
Bill Gates
Linus Torvalds
Bill Gates Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
User logon name:
bgates
@contoso.com
User logon name (pre-Windows 2000):
CONTOSO\
bgates
Logon Hours...
Log On To...
Unlock account
Account options:
User must change password at next logon
User cannot change password
Password never expires
Store password using reversible encryption
Account expires
Never
End of:
Monday , November 20, 2023
OK
Cancel
Apply
Help


Name
Type
Description
Help Desk
Organizational ...
Admin IT
User
Bill Gates
Linus Torvalds
Bill Gates Properties
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Domain Services Folder
Domain Users
contoso.com/Users
Remote Desktop ...
contoso.com/Builtin
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help

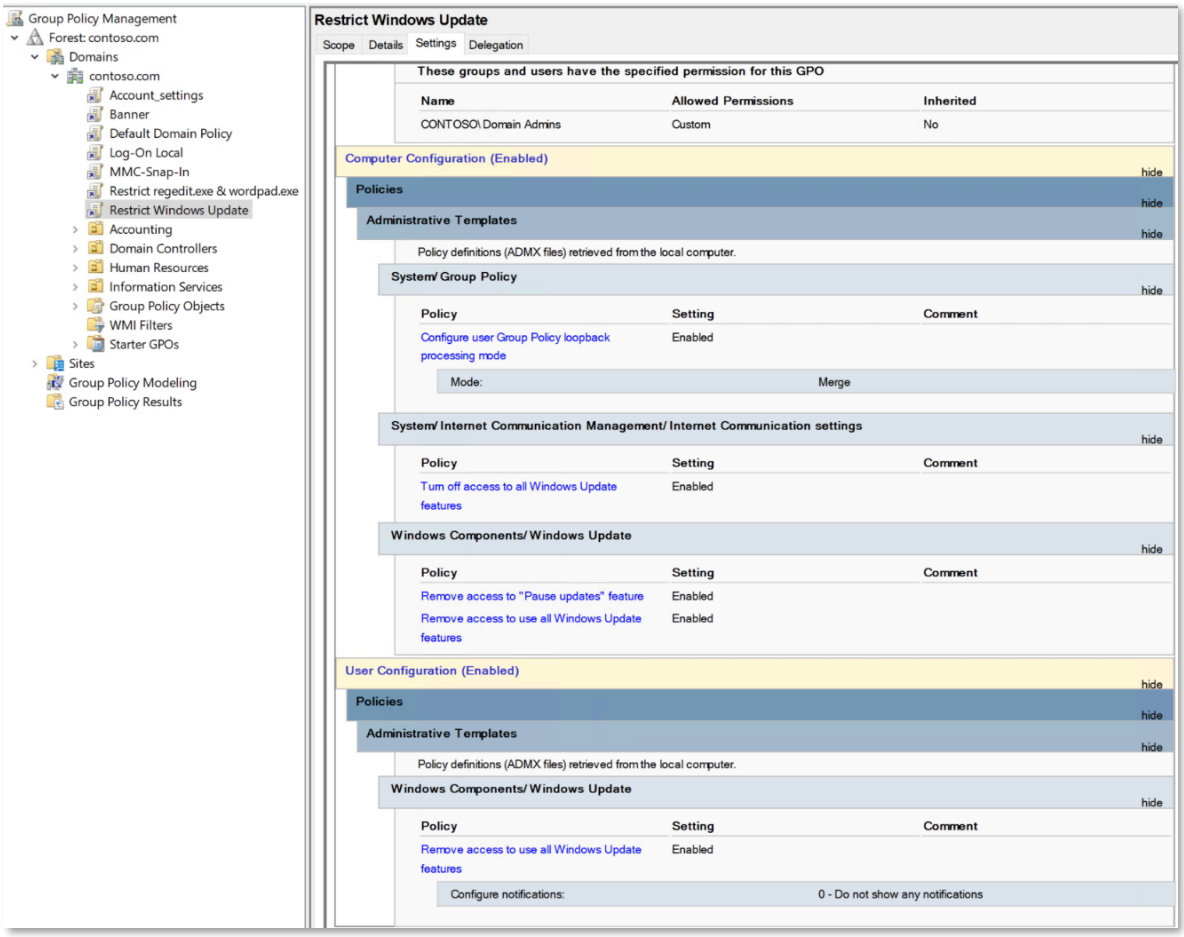
Dans l'organisation, chaque Unité Organisationnelle (OU) est dirigée par un représentant de l'OU qui détient une délégation pour créer, modifier et supprimer les utilisateurs de son OU respectif. Nous examinerons un exemple de délégation dans les illustrations suivantes.

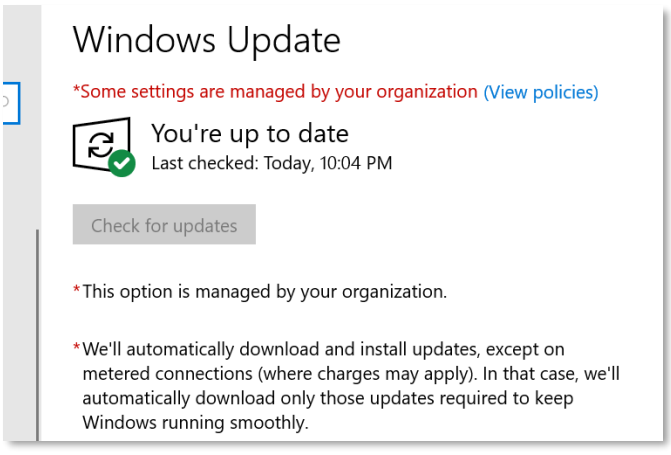


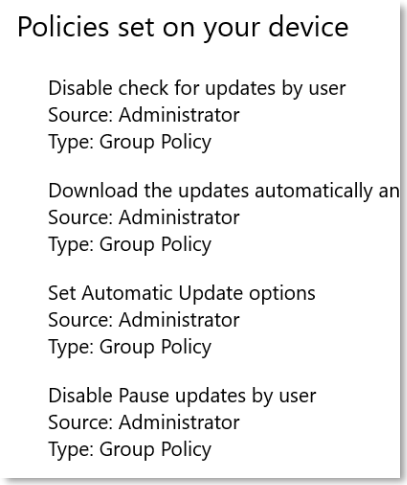




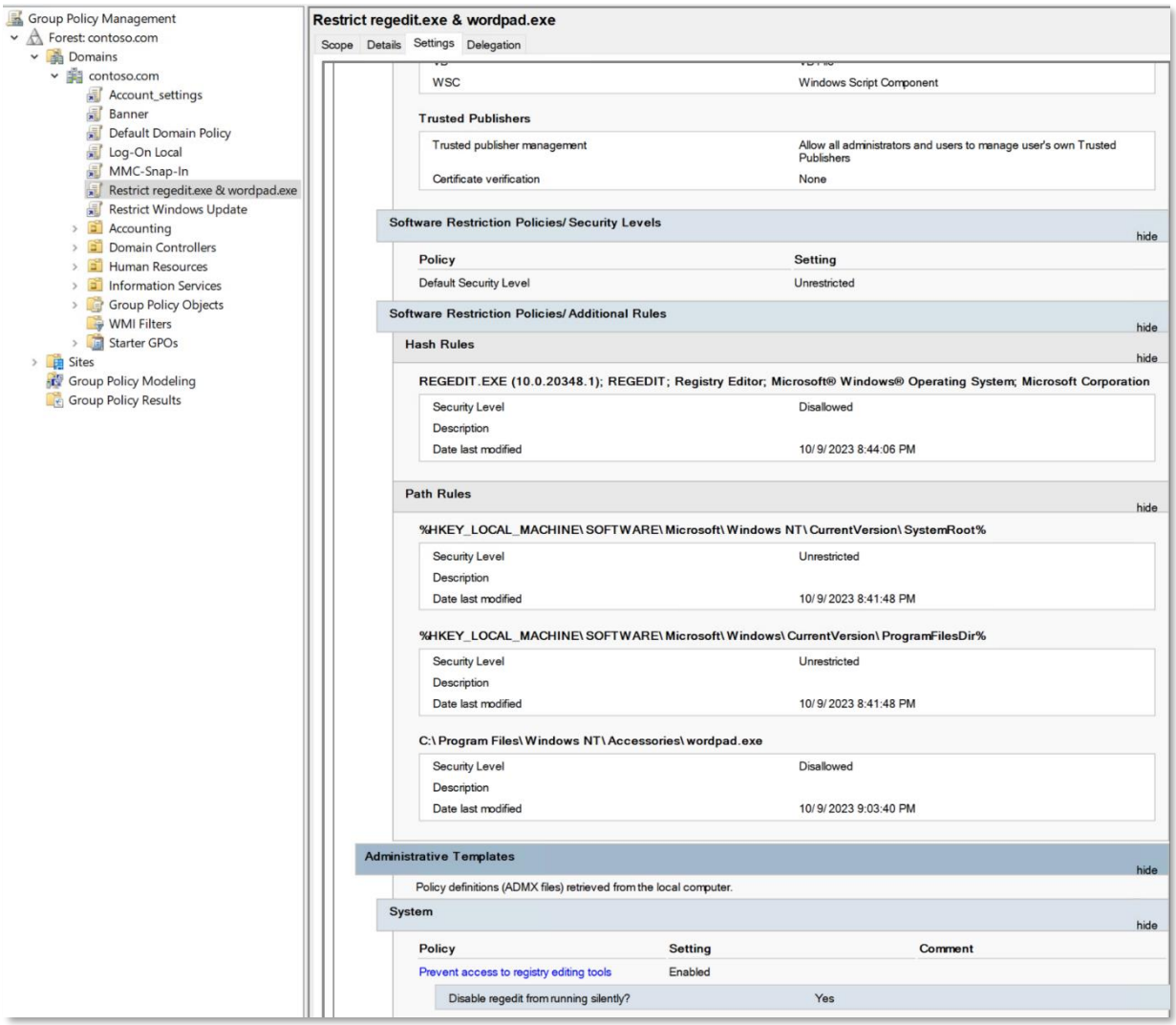
- La politique de **restriction des mises à jour Windows** est appliquée dans l'ensemble du domaine. Tous les utilisateurs sont restreints d'accéder au service de Windows Update pour des raisons de sécurité. Certains paquets de mises à jour peuvent causer des problèmes, et c'est la raison pour laquelle cette restriction est mise en place.

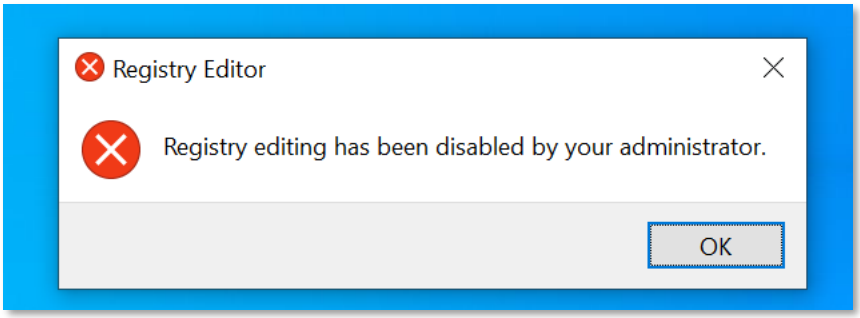


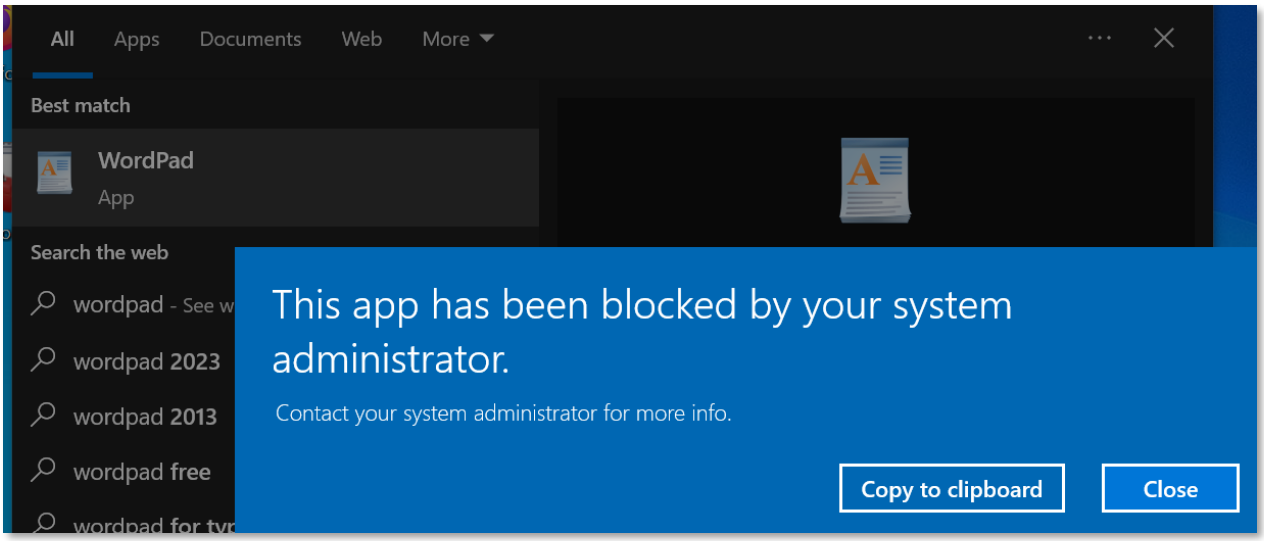




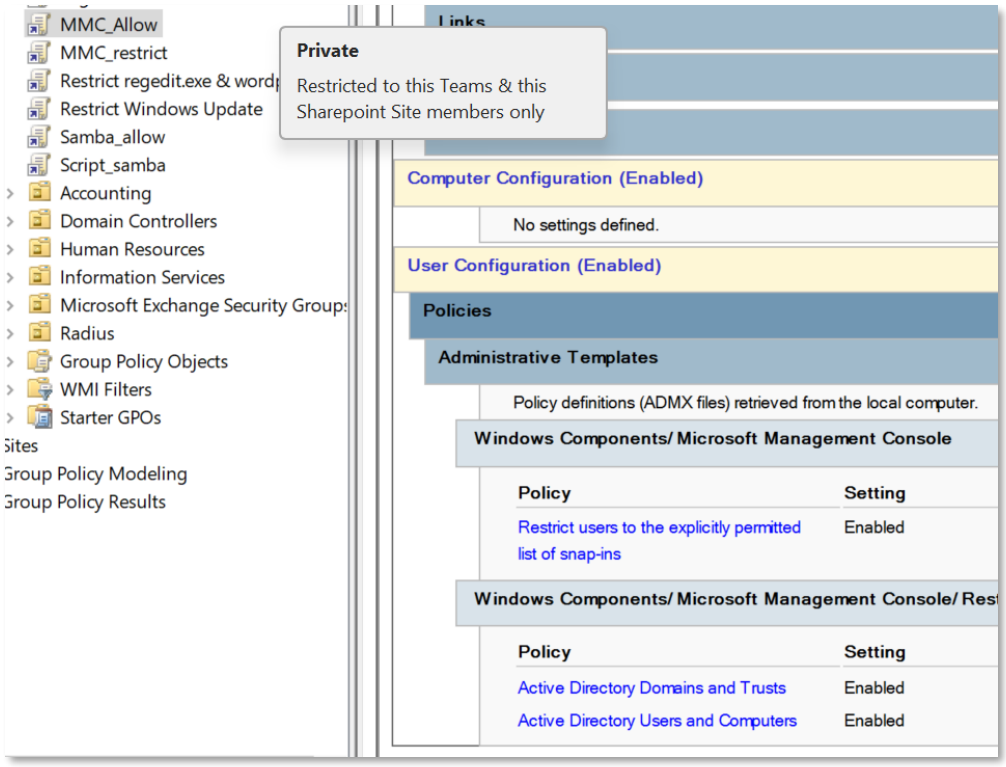
- Dans l'organisation, l'accès à l'Éditeur du Registre (**regedit.exe**) et au Bloc-notes (**wordpad.exe**) est restreint grâce à une stratégie de groupe (GPO). Cette restriction a été mise en place pour des raisons de sécurité afin de limiter l'accès à ces outils sensibles au sein de l'environnement organisationnel.

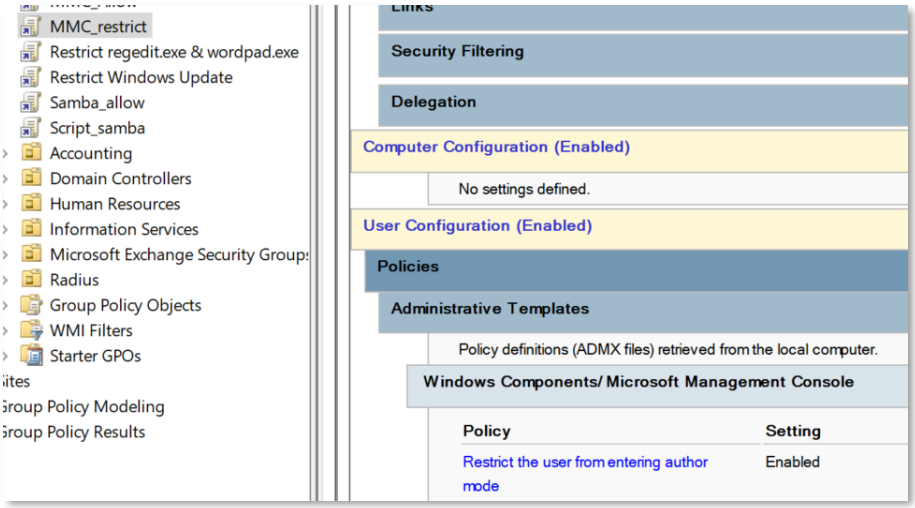


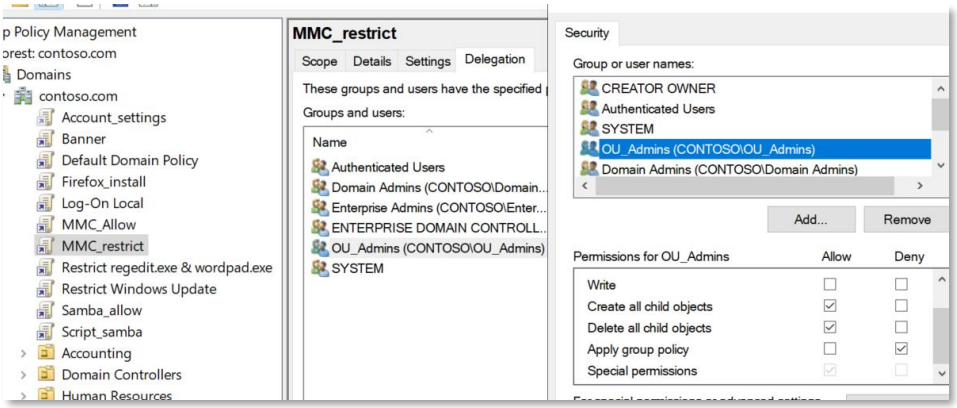


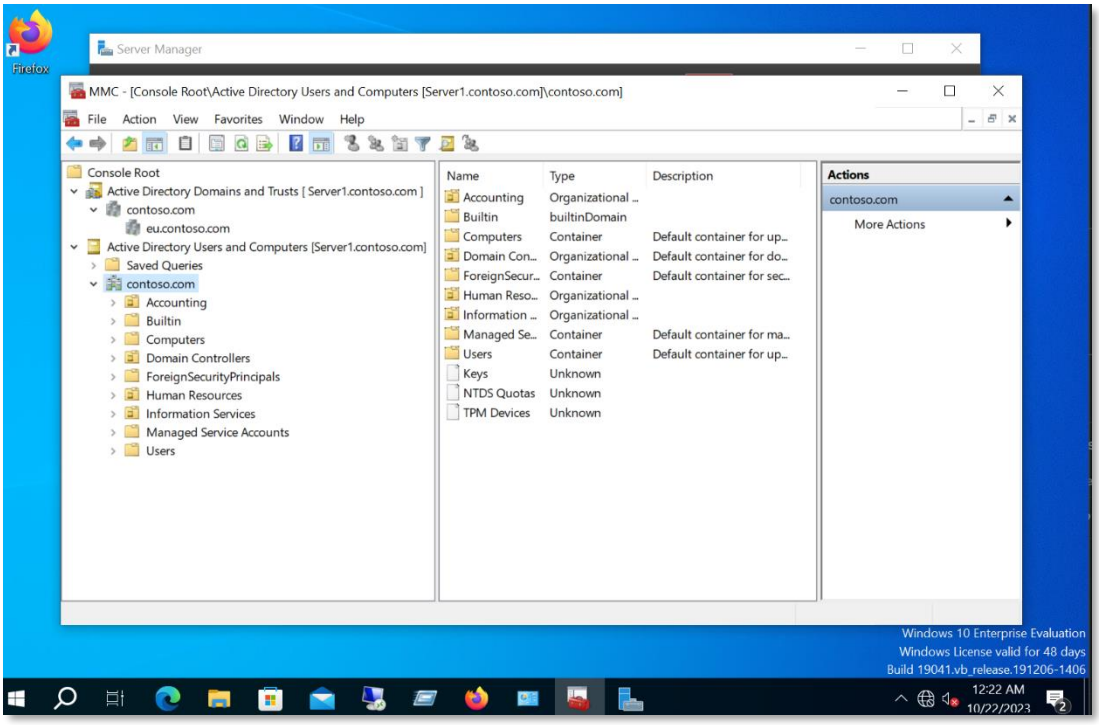


- Aux administrateurs des Unités d'Organisation (OU), le droit de gérer l'Active Directory Users and Computers (ADUC) ainsi que l'Active Directory Domains and Trusts (ADDT) a été accordé via la Console de Gestion Microsoft Management Console (MMC snap-in). Cela permet aux administrateurs de l'OU de prendre en charge efficacement les utilisateurs et les trusts de domaine au sein de l'Active Directory.

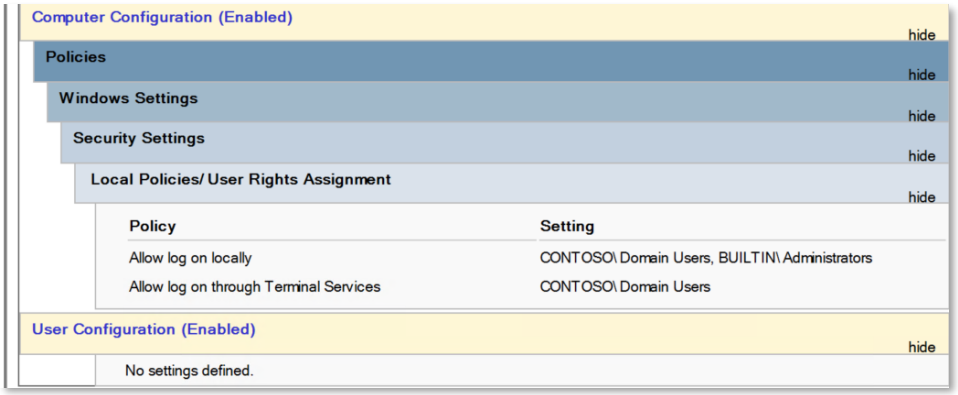



MMC_restrict
Restrict regedit.exe & wordpad.exe
Restrict Windows Update
Samba_allow
Script_samba
Accounting
Domain Controllers
Human Resources
Information Services
Microsoft Exchange Security Groups
Radius
Group Policy Objects
WMI Filters
Starter GPOs
Group Policy Modeling
Group Policy Results
Security Filtering
Delegation
Computer Configuration (Enabled)
No settings defined.
User Configuration (Enabled)
Policies
Administrative Templates
Policy definitions (ADMX files) retrieved from the local computer.
Windows Components/ Microsoft Management Console
Policy
Setting
Restrict the user from entering author mode
Enabled

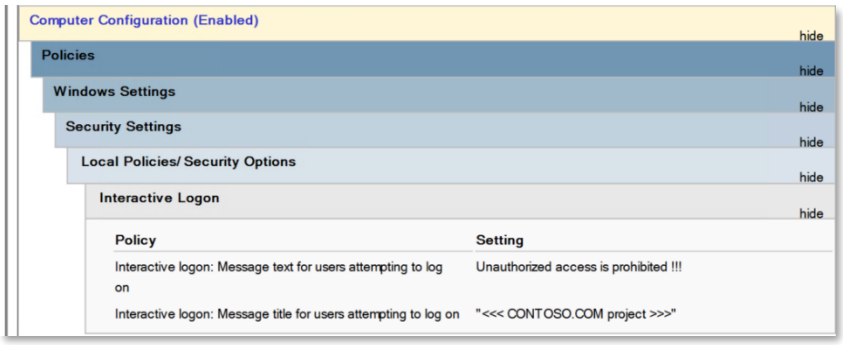

Policy Management
Domains
contoso.com
Account_settings
Banner
Default Domain Policy
Firefox_install
Log-On Local
MMC_Allow
MMC_restrict
Restrict regedit.exe & wordpad.exe
Restrict Windows Update
Samba_allow
Script_samba
Accounting
Domain Controllers
MMC_restrict
Scope
Details
Settings
Delegation
Groups and users:
Name
Authenticated Users
Domain Admins (CONTOSO\Domain...
Enterprise Admins (CONTOSO\Enter...
ENTERPRISE DOMAIN CONTROLL...
OU_Admins (CONTOSO\OU_Admins)
SYSTEM
Security
Group or user names:
CREATOR OWNER
Authenticated Users
SYSTEM
OU_Admins (CONTOSO\OU_Admins)
Domain Admins (CONTOSO\Domain Admins)
Add...
Remove
Permissions for OU_Admins
Allow
Deny
Write
Create all child objects
Delete all child objects
Apply group policy
Special permissions

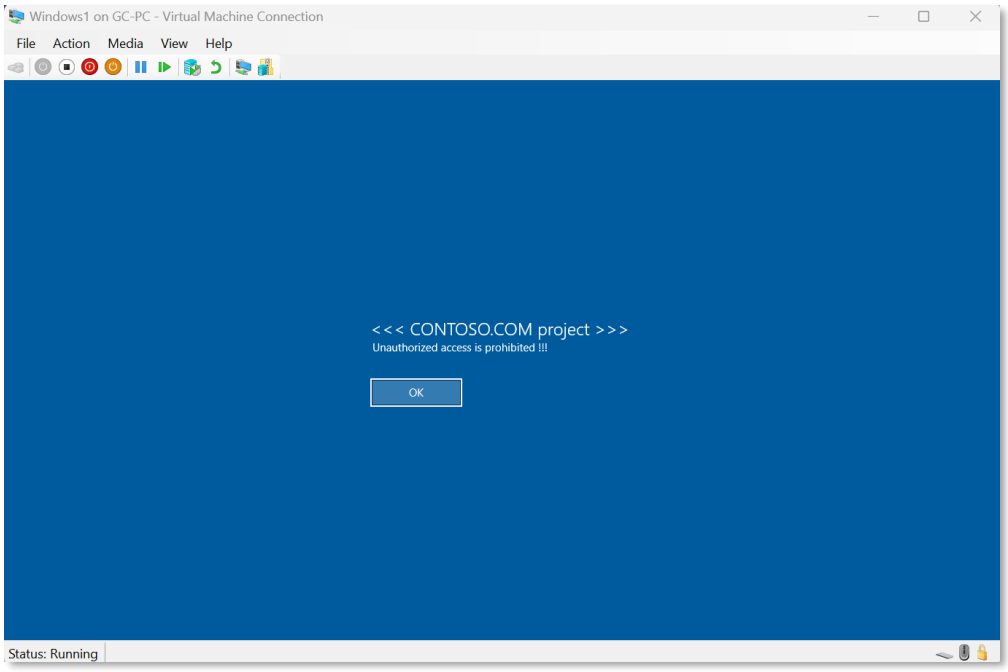

Firefox
Server Manager
MMC - [Console Root\Active Directory Users and Computers [Server1.contoso.com]\contoso.com]
File
Action
View
Favorites
Window
Help
Console Root
Active Directory Domains and Trusts [Server1.contoso.com]
contoso.com
eu.contoso.com
Active Directory Users and Computers [Server1.contoso.com]
Saved Queries
contoso.com
Accounting
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Human Resources
Information Services
Managed Service Accounts
Users
Name
Type
Description
Accounting
Organizational ...
Builtin
builtinDomain
Computers
Container
Default container for up...
Domain Con...
Organizational ...
Default container for do...
ForeignSecur...
Container
Default container for sec...
Human Reso...
Organizational ...
Information ...
Organizational ...
Managed Se...
Container
Default container for ma...
Users
Container
Default container for up...
Keys
Unknown
NTDS Quotas
Unknown
TPM Devices
Unknown
Actions
contoso.com
More Actions
Windows 10 Enterprise Evaluation
Windows License valid for 48 days
Build 19041.vb_release.191206-1406
12:22 AM
10/22/2023

- Aux utilisateurs, l'autorisation **de se connecter localement** a été accordée en appliquant une stratégie de groupe (GPO). Cela signifie que les utilisateurs ont la possibilité de se connecter directement à une machine locale dans le réseau, conformément aux paramètres définis dans la GPO. Cette autorisation peut être utile pour certains scénarios ou exigences spécifiques au sein de l'organisation. De même, l'accès à se connecter aux Terminal Services a été autorisé aux utilisateurs, comme cela sera démontré dans la deuxième partie du projet.



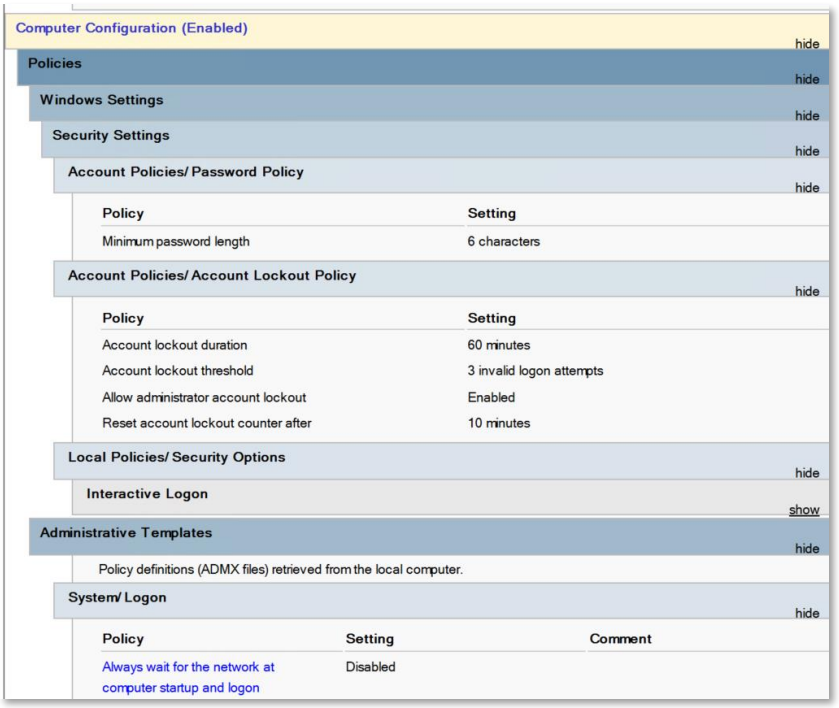
- Le démarrage des terminaux affichera une bannière avec un message déterminé par l'organisation. Cette mesure est souvent utilisée pour communiquer des informations importantes, des politiques ou des avertissements avant que les utilisateurs ne se connectent au terminal. Cela contribue à informer les utilisateurs des règles et des directives de l'organisation dès le début de la session.





- Password policy

Dans l'organisation, la politique de base pour les mots de passe des utilisateurs est appliquée via une stratégie de groupe (GPO). Selon cette politique le mot de passe doit avoir au moins 6 caractères, et après 3 tentatives de connexion infructueuses, le compte sera verrouillé pendant 60 minutes. Ces mesures de sécurité contribuent à renforcer la protection des comptes utilisateur et à minimiser les risques liés aux attaques par force brute.



Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/ Password Policy hide

Policy	Setting
Minimum password length	6 characters

Account Policies/ Account Lockout Policy hide

Policy	Setting
Account lockout duration	60 minutes
Account lockout threshold	3 invalid logon attempts
Allow administrator account lockout	Enabled
Reset account lockout counter after	10 minutes

Local Policies/ Security Options hide

Interactive Logon show

Administrative Templates hide

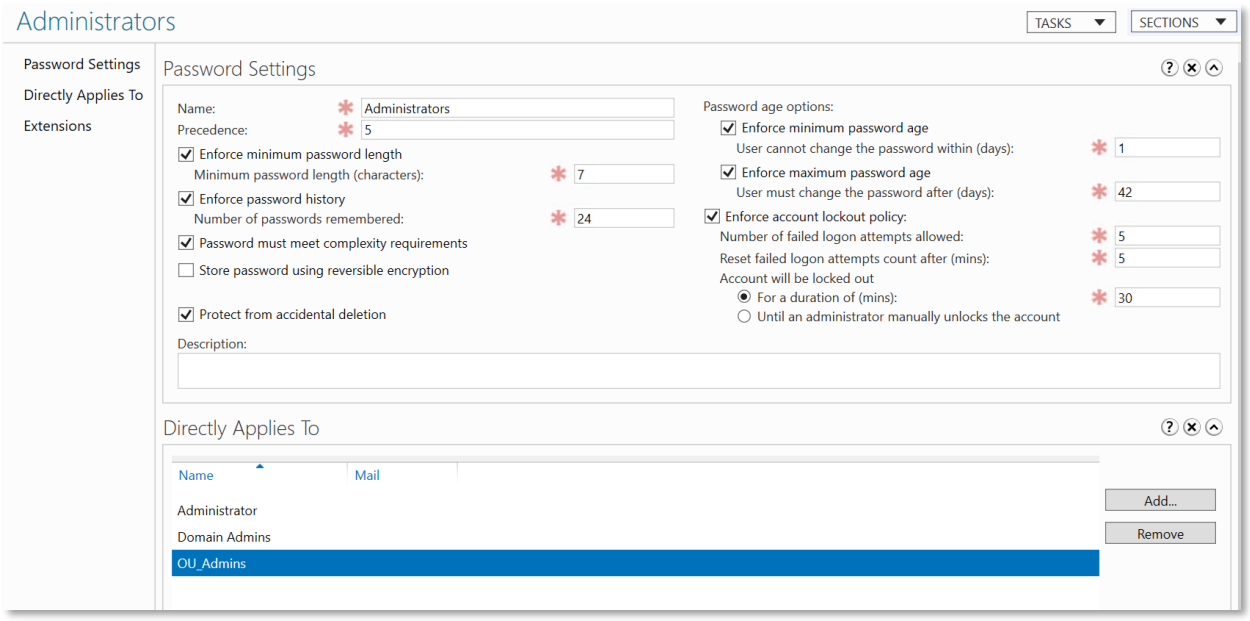
Policy definitions (ADMX files) retrieved from the local computer.

System/ Logon hide

Policy	Setting	Comment
Always wait for the network at computer startup and logon	Disabled	

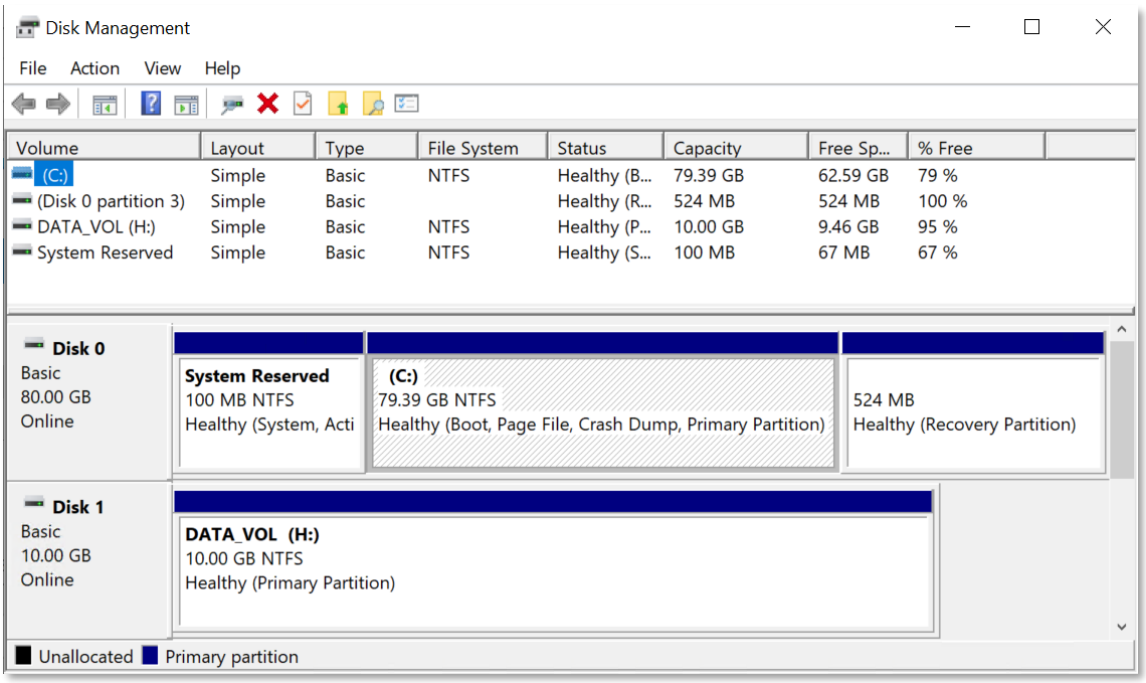
- Les administrateurs ont une autre politique pour les mots de passe, dirigée par FGPP (Fine-Grained Password Policies). Selon cette politique spécifique aux administrateurs. Le mot de passe doit avoir au moins 7 caractères.

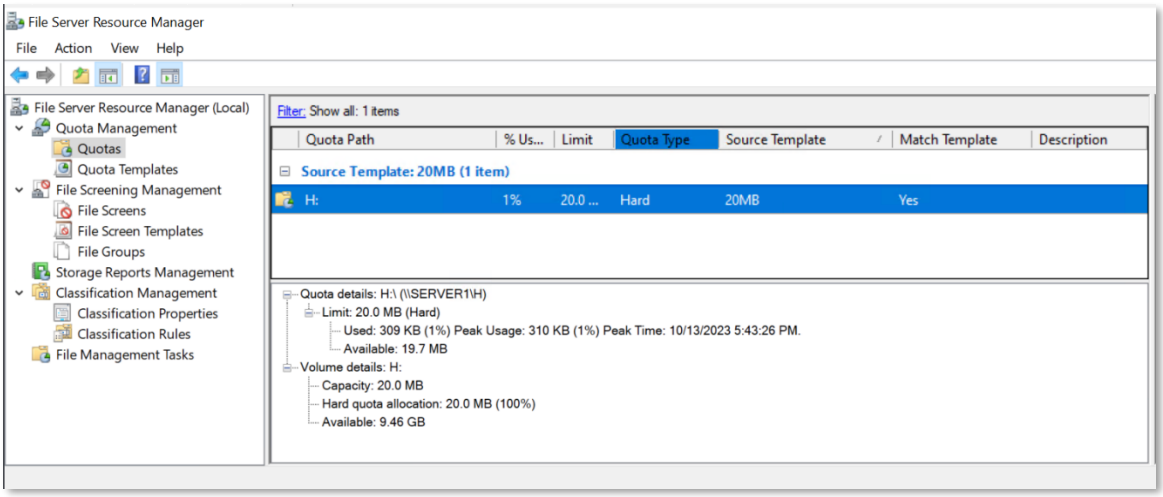
L'utilisation de FGPP permet d'appliquer des politiques de mot de passe plus spécifiques à certains groupes d'utilisateurs, dans ce cas, les administrateurs. Cela permet d'adapter les exigences de sécurité en fonction des besoins et des responsabilités des différents utilisateurs au sein de l'organisation.

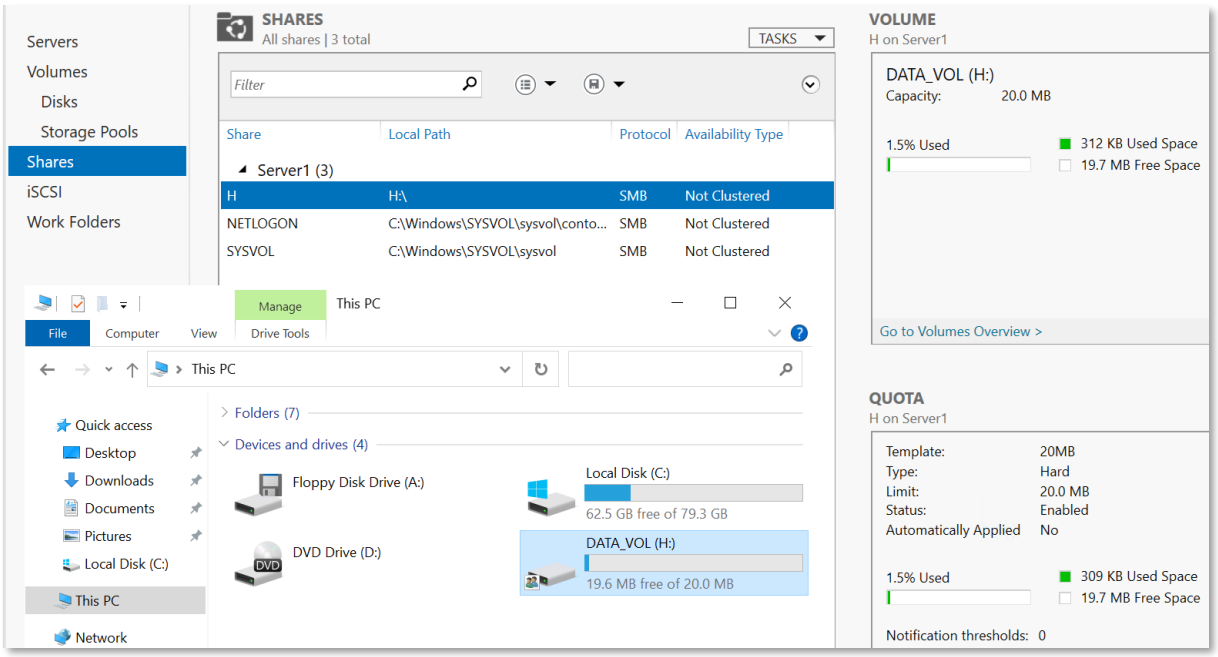


Gestion des quotas

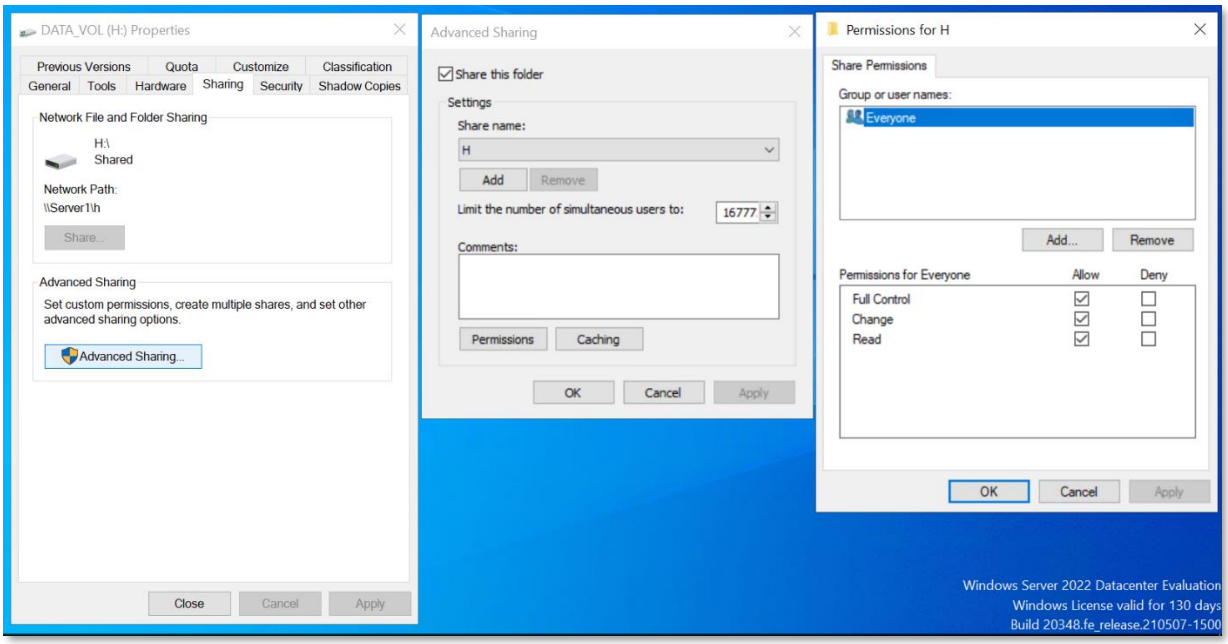
Pour économiser les ressources de stockage sur le serveur, une limite de quota a été appliquée pour tous les utilisateurs. Cette mesure vise à contrôler la quantité de stockage utilisée par chaque utilisateur, assurant ainsi une utilisation efficace des ressources et évitant une utilisation excessive de l'espace de stockage. Les quotas peuvent être définis pour les utilisateurs individuels ou pour des groupes spécifiques, en fonction des besoins de l'organisation.

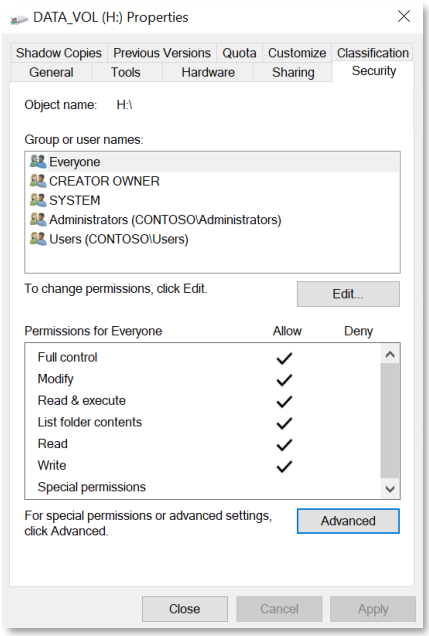




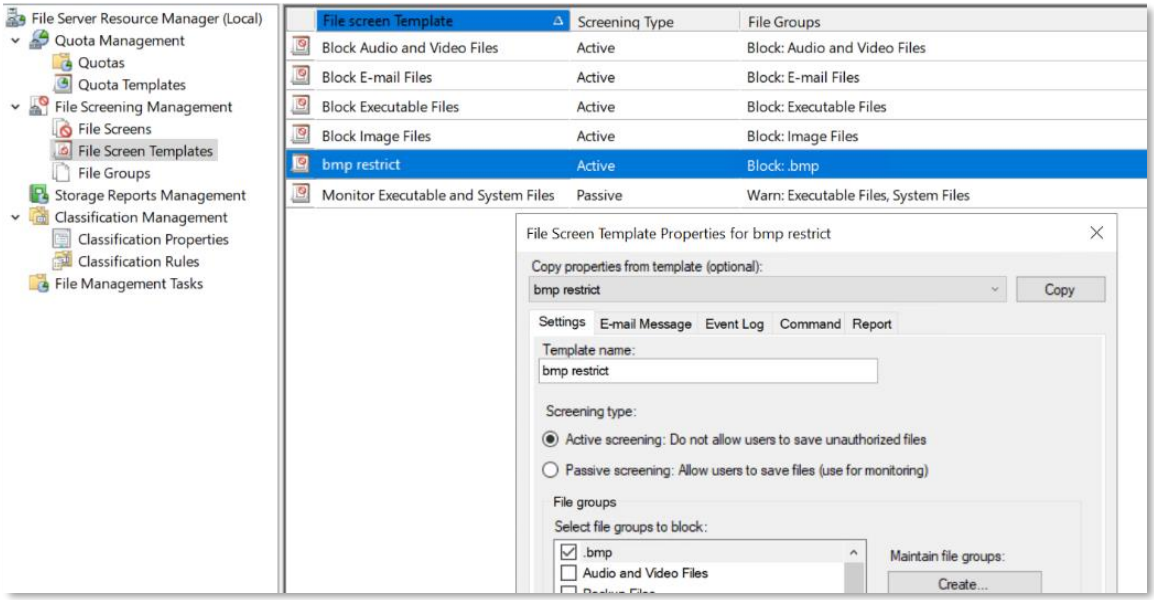


La partition DATA_VOL peut être accédée et gérée par n'importe quel utilisateur, y compris ceux qui ont des droits en écriture, lecture et suppression de fichiers. Les utilisateurs avec ces autorisations ont la liberté d'ajouter, lire ou supprimer des fichiers dans cette partition.

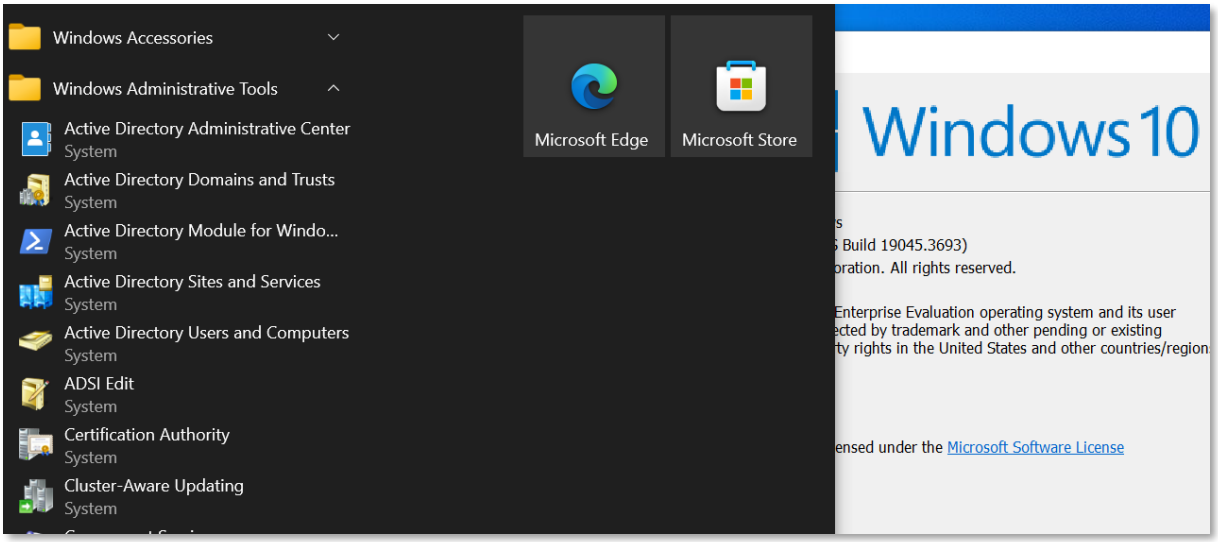


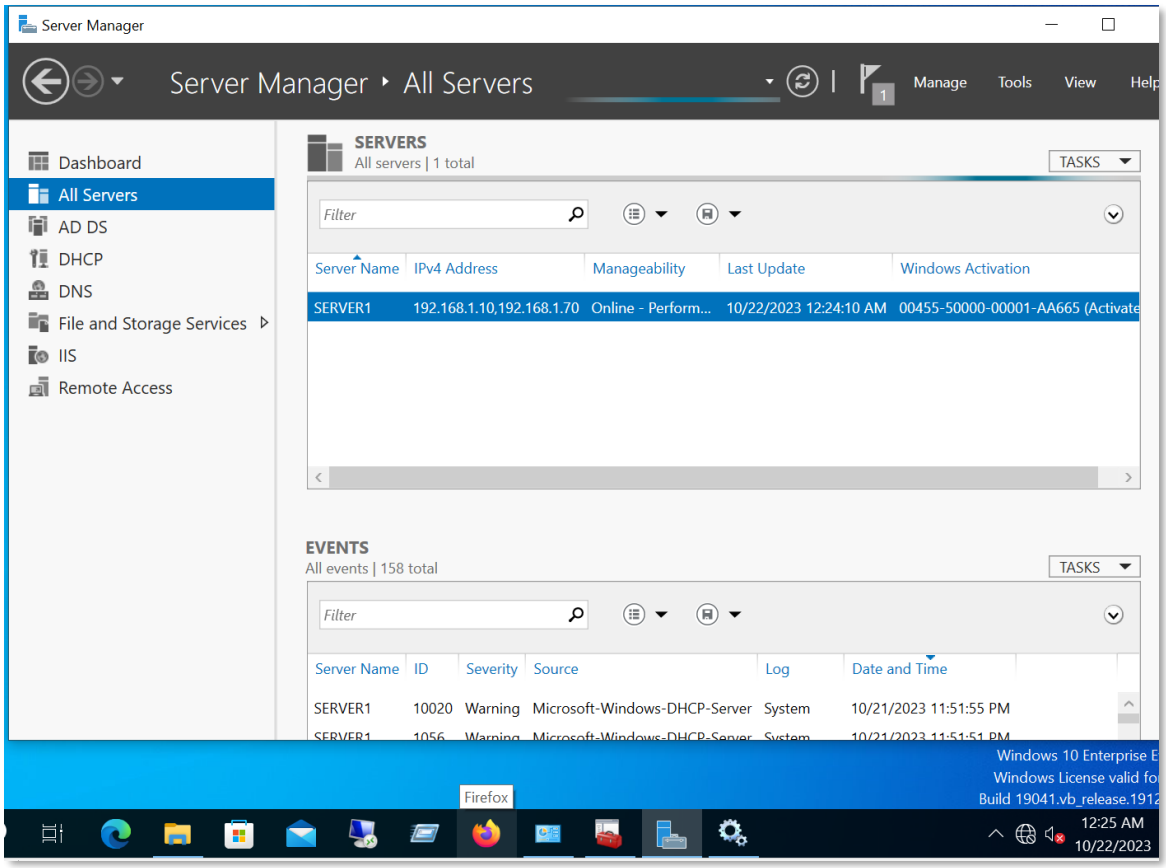


La restriction d'enregistrement du type de fichier .bmp dans le volume H a été mise en place à l'aide de la console Gestionnaire des ressources du serveur de fichiers sur Server1. Cette mesure garantit que les fichiers .bmp ne peuvent pas être sauvegardés dans le volume H, conformément à la politique établie.

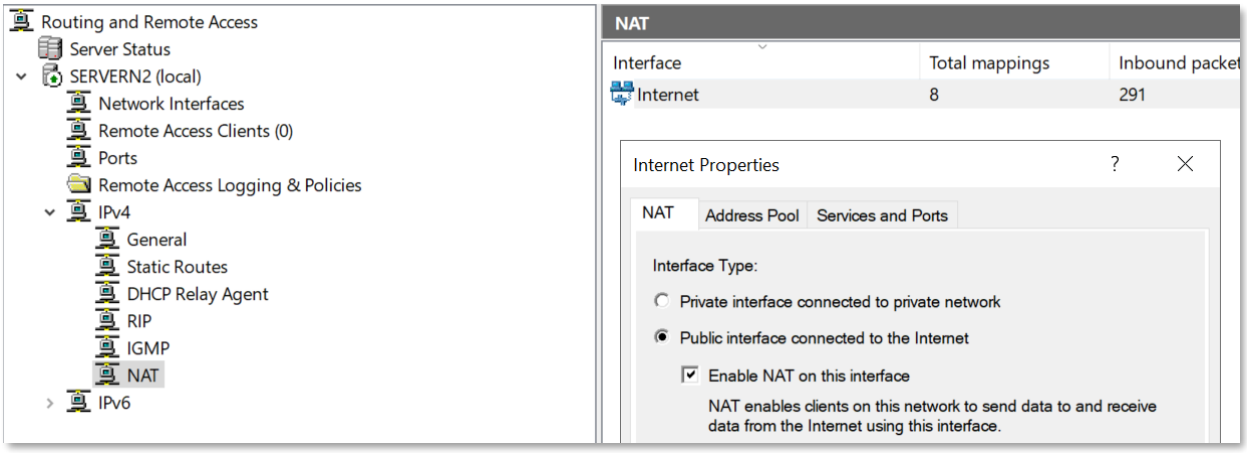


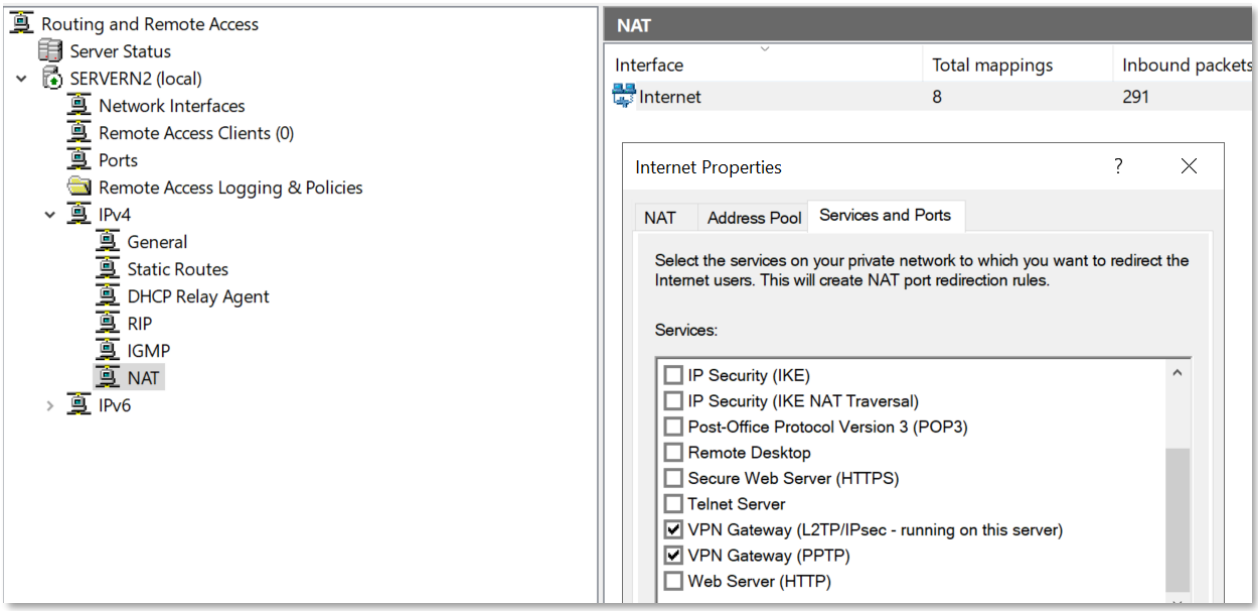
- Sur le client Windows 10 du domaine, les outils RSAT (Remote Server Administration Tools) ont été installés. Cela permet d'administrer à distance les serveurs dans le domaine.

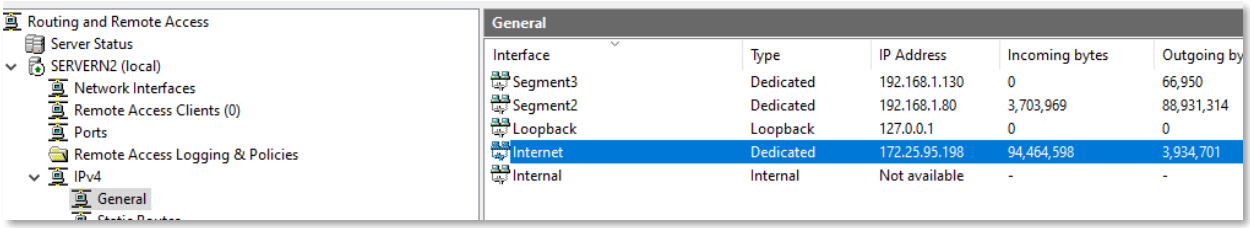




Sur le serveur2, est ajouté une carte réseau avec NAT pour permettre l'accès à Internet à l'ensemble du réseau de l'organisation.

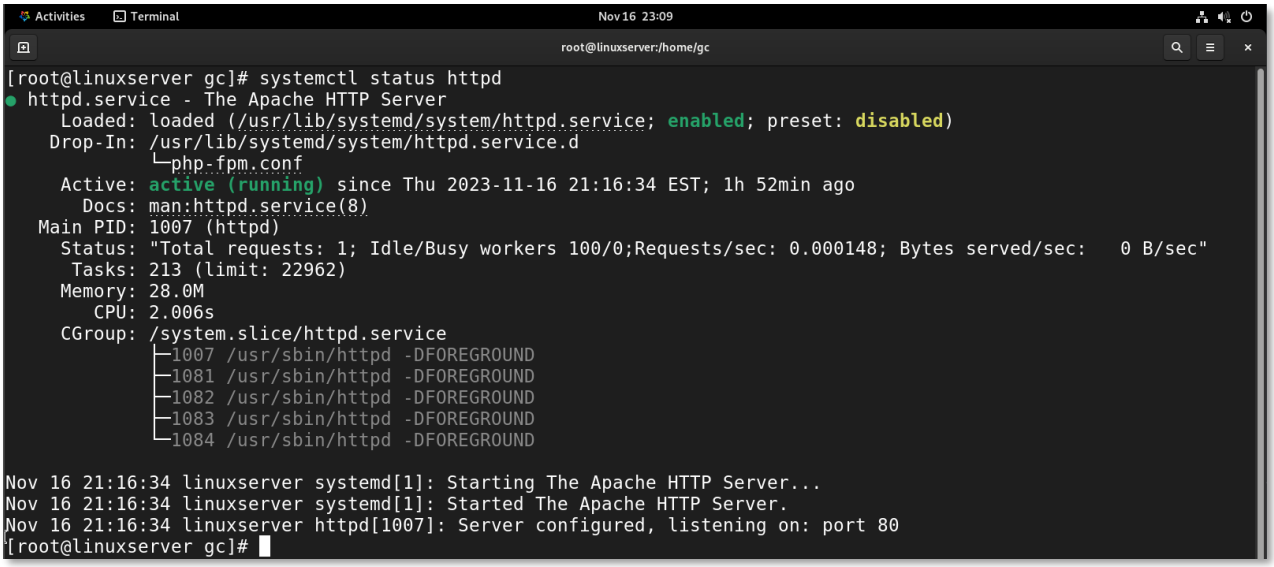




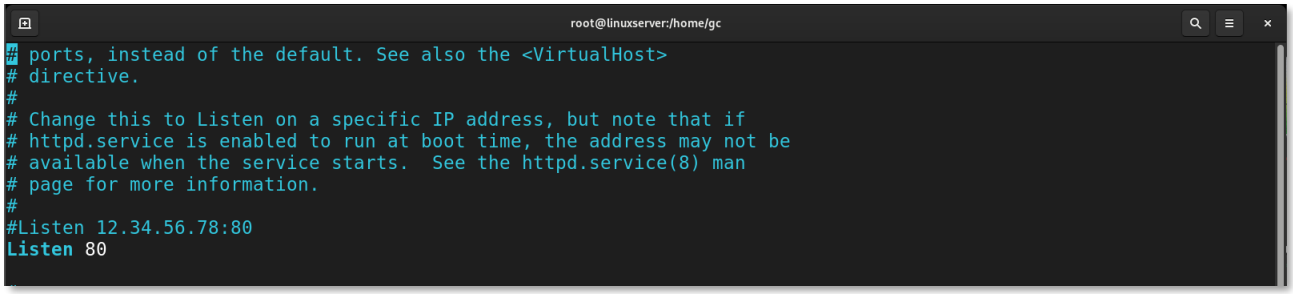


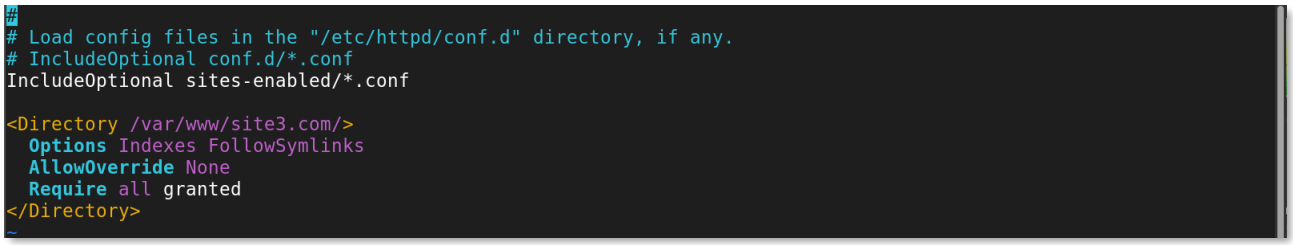
- Sur le réseau, est intégré un serveur Linux basé sur Alma Linux 9, qui se trouve dans le segment 2.

La première étape consiste à configurer Apache ainsi que le site3.com.



La configuration d'Apache /etc/httpd/conf/httpd.conf





Après cela, nous installons le service Bind DNS et procédons à la création des zones, une zone « slave » pour le domaine Contoso.com et trois zones « master » pour site1.com, site2.com et site3.com.

Le fichier de configuration du BIND DNS /etc/named.conf

```
options {
        listen-on port 53 { 127.0.0.1; 192.168.1.75; };   ##Slave Server IP
        listen-on-v6 port 53 { any; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost; 192.168.1.0/24; };
        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion no;

        dnssec-validation yes;

        managed-keys-directory "/var/named/dynamic";
        geoip-directory "/usr/share/GeoIP";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
```

```
root@linuxser
        /* https://fedoraproject.org/wiki/Changes/CryptoP
        include "/etc/crypto-policies/back-ends/bind.confi
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

## zones
zone "site1.com" {
        type master;
        file "site1.com.zone";
        allow-update { none; };
        allow-transfer { 192.168.1.70; };
};

zone "site2.com" {
        type master;
        file "site2.com.zone";
        allow-update { none; };
        allow-transfer { 192.168.1.70; };
};

zone "site3.com" {
        type master;
        file "site3.com.zone";
        allow-update { none; };
        allow-transfer { 192.168.1.70; };
};
/etc/named.conf
```

```
## zones
zone "site1.com" {
        type master;
        file "site1.com.zone";
        allow-update { none; };
        allow-transfer { 192.168.1.70; };
};

zone "site2.com" {
        type master;
        file "site2.com.zone";
        allow-update { none; };
        allow-transfer { 192.168.1.70; };
};


zone "site3.com" {
        type master;
        file "site3.com.zone";
        allow-update { none; };
        allow-transfer { 192.168.1.70; };
};

zone "contoso.com" IN {
        type slave;
        file "slaves/contoso.fwd.zone";
        masters { 192.168.1.70; };
};
zone "1.168.192.in-addr.arpa" IN {
        type slave;
        file "slaves/contoso.rev.zone";
        masters { 192.168.1.70; 192.168.1.75; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

~
/etc/named.conf
```

Il est nécessaire de créer des fichiers de configuration de la zone pour chaque site. La zone de domaine sera transférée automatiquement depuis le Server1.

Site1.com - /var/named/site1.com.zone

```
$TTL 1D
@       IN SOA  @ site1.com. (
                                        2023110402      ; serial
                                                1D      ; refresh
                                                1H      ; retry
                                                1W      ; expire
                                                3H )    ; minimum
;
@       IN NS    site1.com.
@       IN A     192.168.1.70
www     IN A     192.168.1.70
```

Site2.com - /var/named/site2.com.zone

```
$TTL 1D
@       IN SOA  @ site2.com. (
                                        2023110402      ; serial
                                                1D      ; refresh
                                                1H      ; retry
                                                1W      ; expire
                                                3H )    ; minimum
;
@       IN NS    site2.com.
@       IN A     192.168.1.70
www     IN A     192.168.1.70
```

Site3.com - /var/named/site3.com.zone

```
$TTL 1D
@       IN SOA  @ site3.com. (
                                        2023110205      ; serial
                                                1D      ; refresh
                                                1H      ; retry
                                                1W      ; expire
                                                3H )    ; minimum
;
@       IN NS    site3.com.
@       IN A     192.168.1.75
www     IN A     192.168.1.75
```

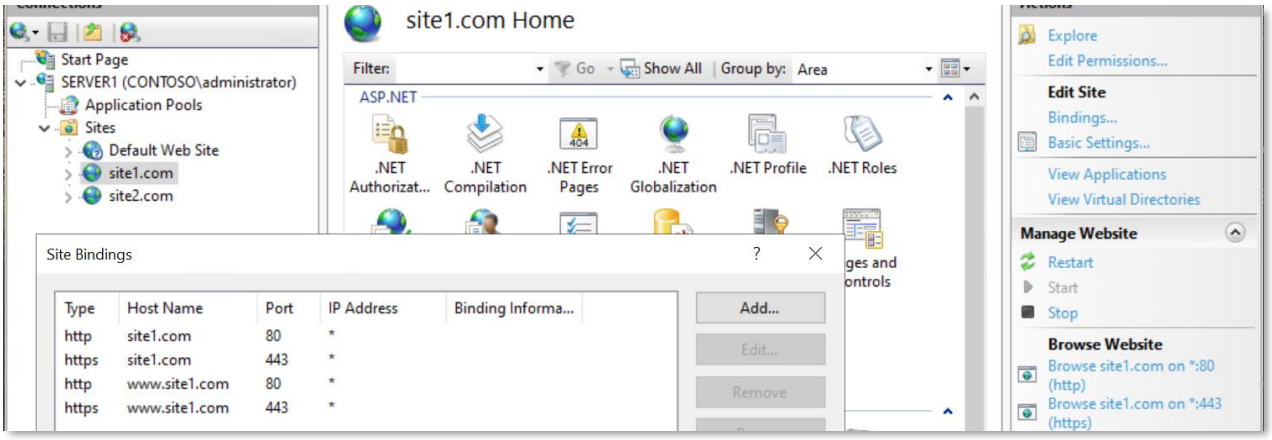
La vérification que BIND fonctionne correctement.

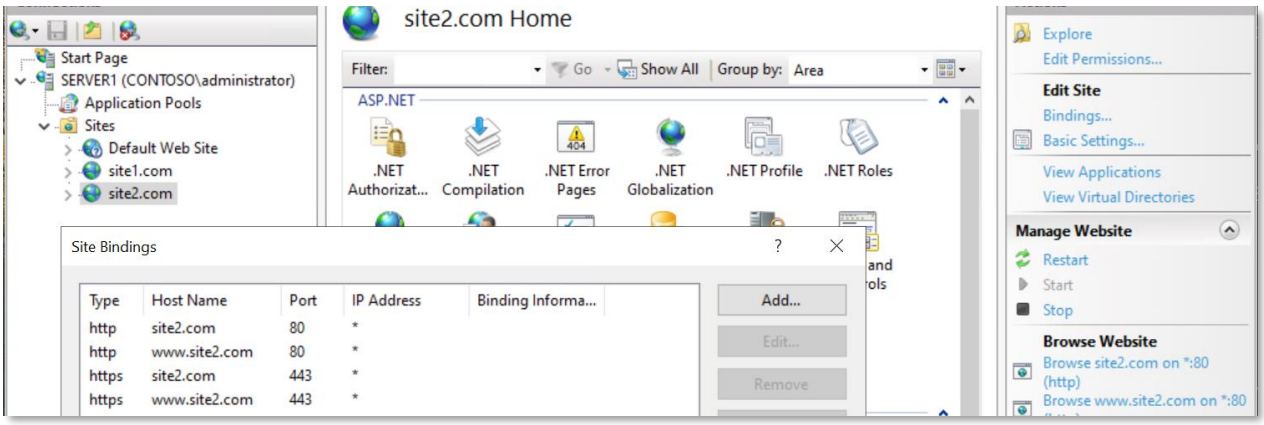
```
[root@linuxserver gc]# systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: disabled)
     Active: active (running) since Thu 2023-11-16 21:16:34 EST; 1h 2min ago
   Main PID: 933 (named)
      Tasks: 5 (limit: 22962)
     Memory: 20.9M
        CPU: 113ms
     CGroup: /system.slice/named.service
             └─933 /usr/sbin/named -u named -c /etc/named.conf
```

La réponse du DNS depuis le Server1 est correcte. BIND fonctionne correct et communique avec le serveur DNS Server1.

```
[root@linuxserver gc]# nslookup google.com
;; Got recursion not available from 192.168.1.75, trying next server
Server:         192.168.1.80
Address:        192.168.1.80#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.13.110
;; Got recursion not available from 192.168.1.75, trying next server
Name:   google.com
Address: 2607:f8b0:4020:804::200e

[root@linuxserver gc]# nslookup contoso.com
;; Got recursion not available from 192.168.1.75, trying next server
Server:         192.168.1.70
Address:        192.168.1.70#53

Name:   contoso.com
Address: 192.168.1.10
Name:   contoso.com
Address: 192.168.1.70
;; Got recursion not available from 192.168.1.75, trying next server

[root@linuxserver gc]#
```

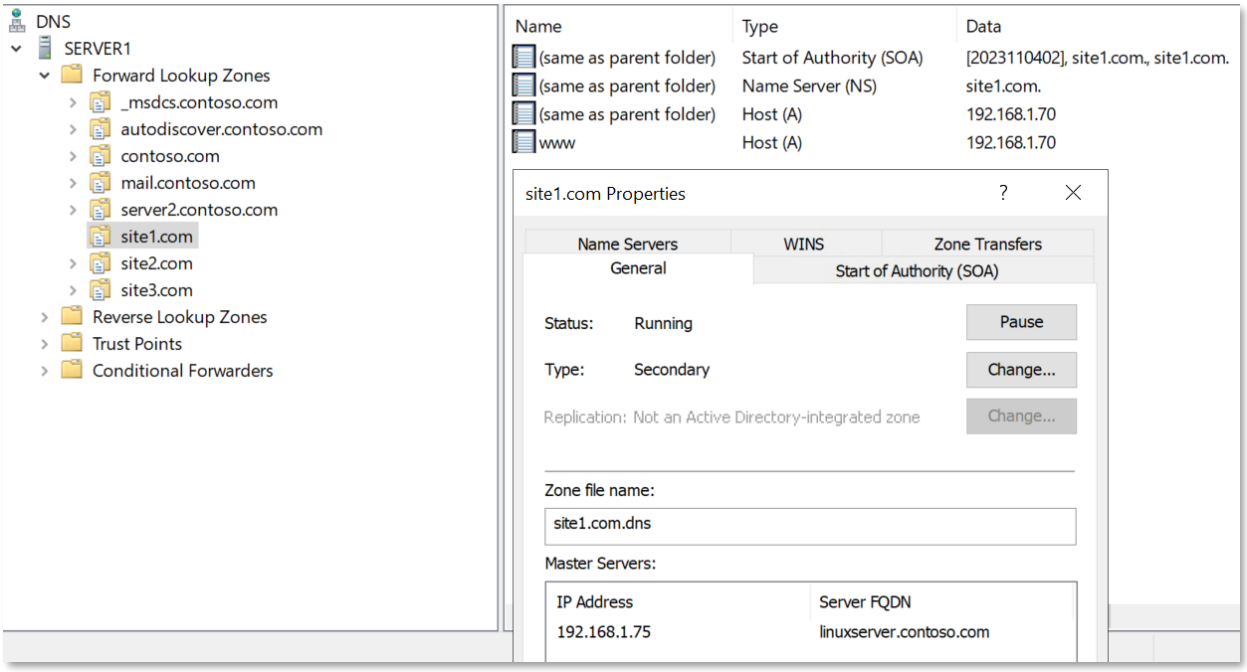
- Pour la prochaine étape, nous déployons le rôle IIS sur le Server1 et configurons les sites site1.com et site2.com. En parallèle, nous établissons les zones site1.com, site2.com et site3.com en tant que zones secondaires sur le serveur DNS Server1.

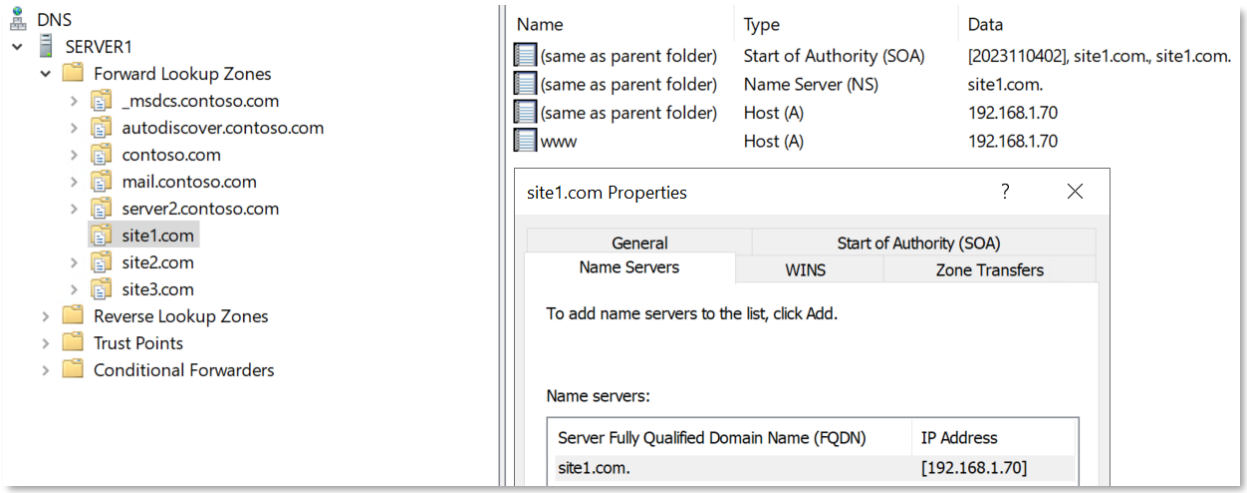




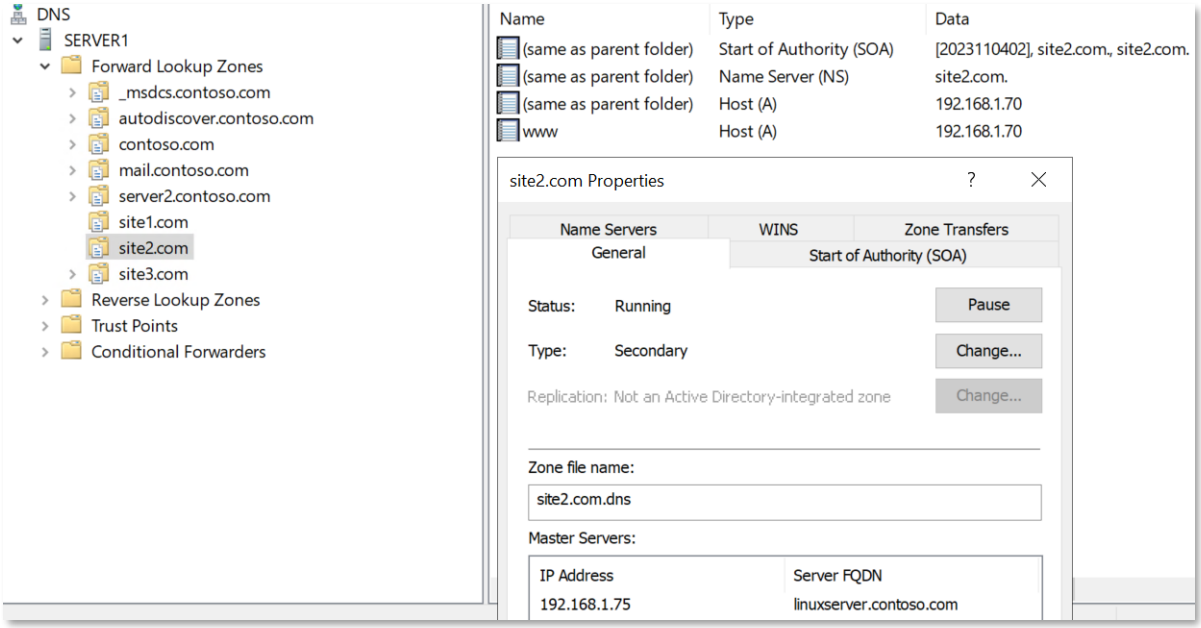
Les zones des tous les trois sites sont transférées sur le serveur DNS Server1.

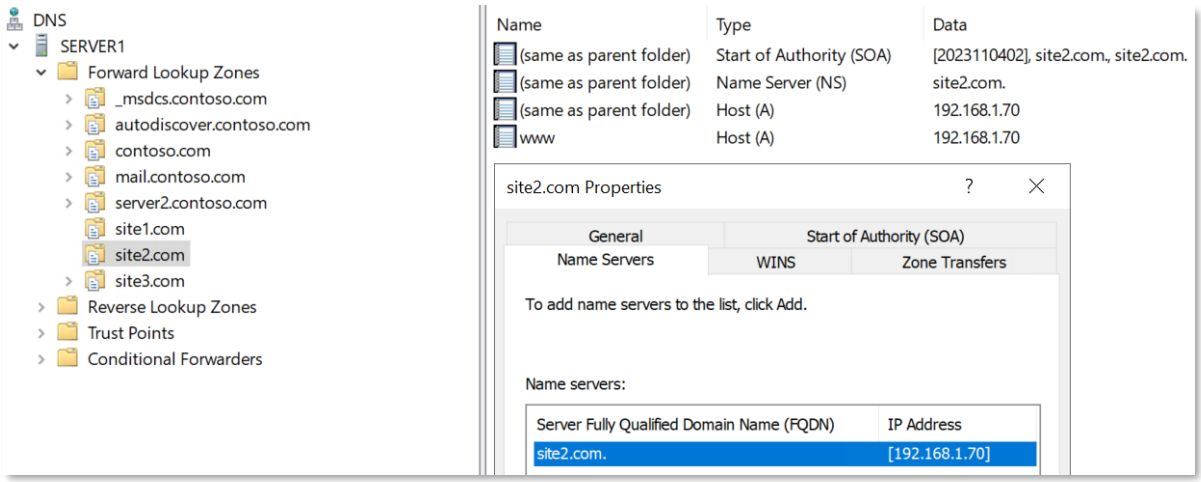
Site1.com - hébergé sur le Server1



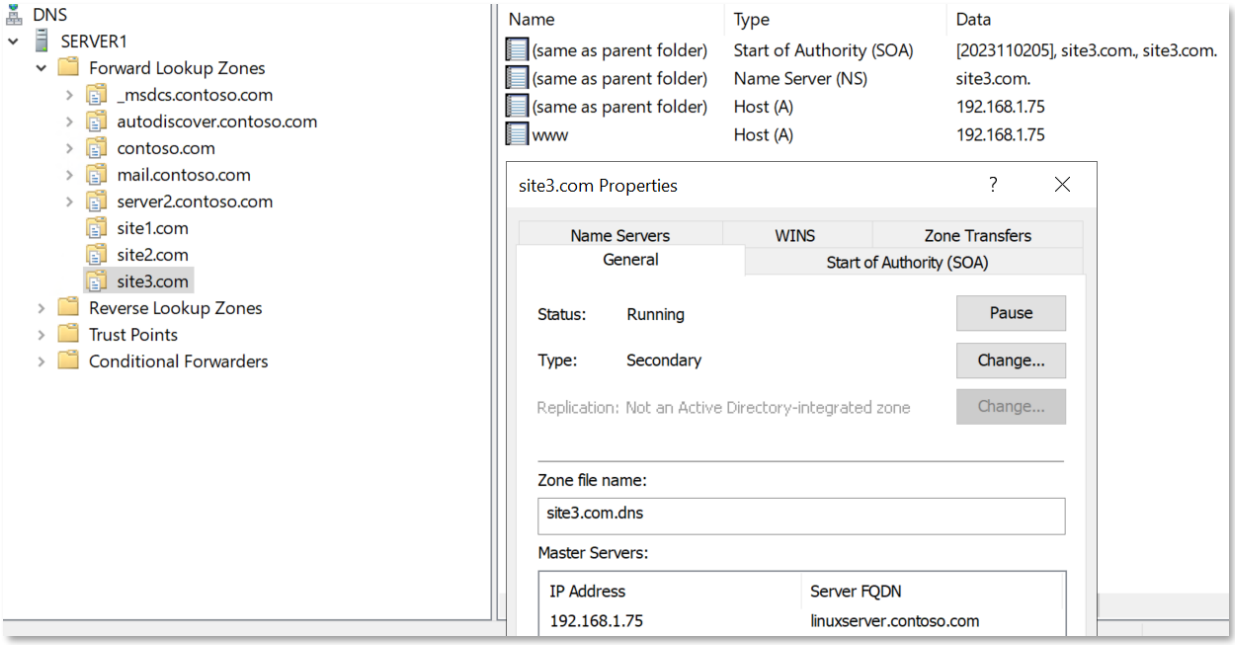


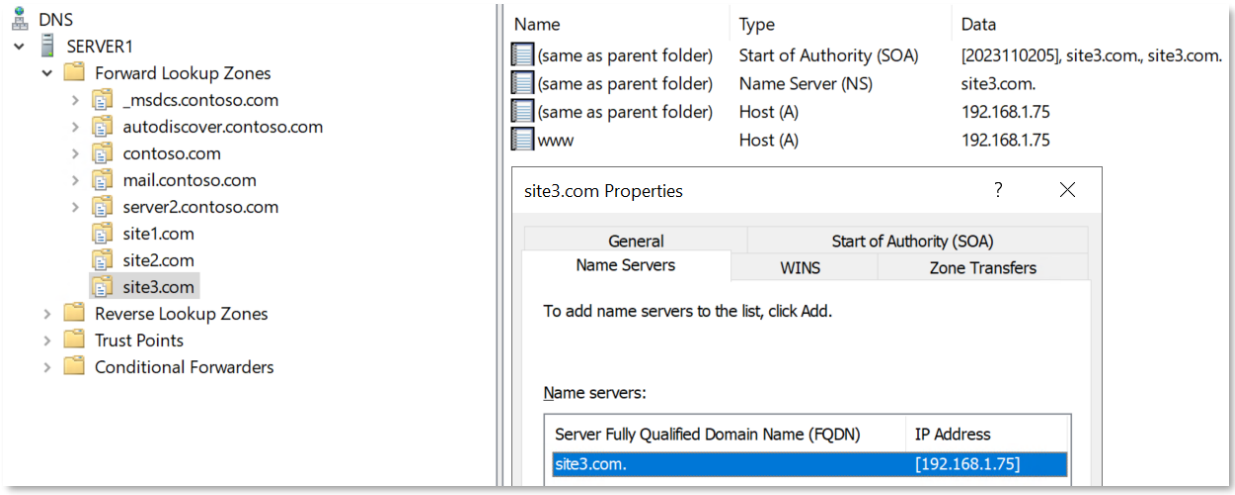
Site2.com - hébergé sur le Server1





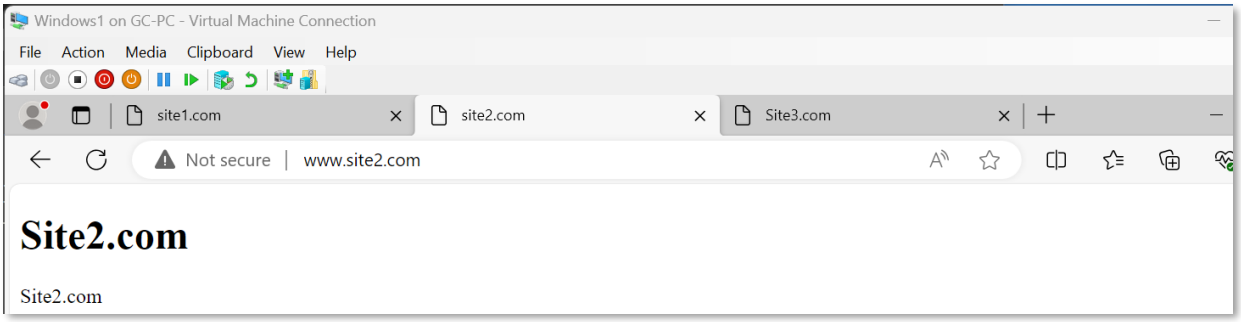
Site3.com - hébergé sur Linuxserver

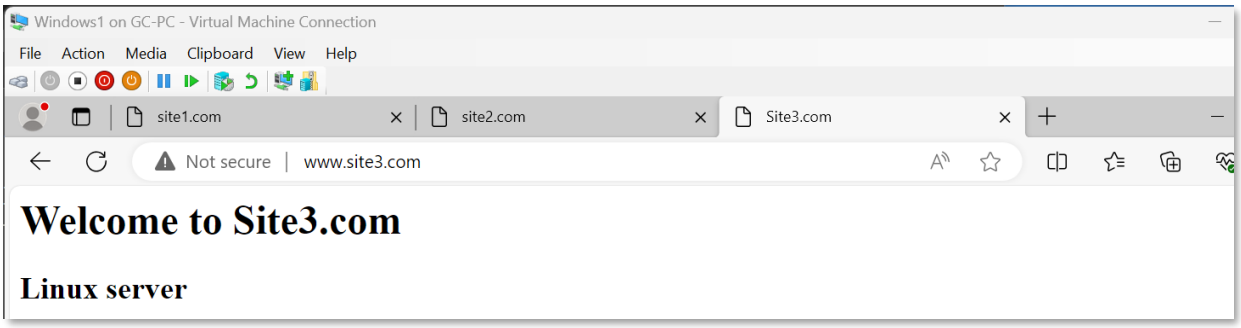




- La prochaine étape consiste à tester le bon fonctionnement des sites.

Les illustrations présenteront le test des sites sur le client Windows1





On constate que les sites s'ouvrent sans problème, que le DNS fonctionne correctement. Cependant, les sites publics portant les mêmes noms ne s'ouvrent pas, car le DNS est non récursif.

- Le serveur Linux est configuré en tant que serveur de stockage de données, tel que NFS et SAMBA. Voici une démonstration du serveur **NFS**.

```
[root@linuxserver gc]# systemctl status nfs-server
● nfs-server.service - NFS server and services
     Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; enabled; preset: d
    Drop-In: /run/systemd/generator/nfs-server.service.d
             └─order-with-mounts.conf
     Active: active (exited) since Thu 2023-11-16 21:16:35 EST; 1h 8min ago
   Main PID: 1545 (code=exited, status=0/SUCCESS)
        CPU: 9ms
```

- Le répertoire partage - /nfs_share

```
drwxr-xr-x.   2 root   root      6 Mar 25  2022 mnt
drwxrwxrwx.   2 nobody nobody    6 Oct 26 19:20 nfs_backup
drwxrwxrwx.   2 nobody nobody   51 Oct 26 21:51 nfs_share
drwxr-xr-x.   2 root   root      6 Mar 25  2022 opt
```

- Le fichier de configuration - /etc/exports

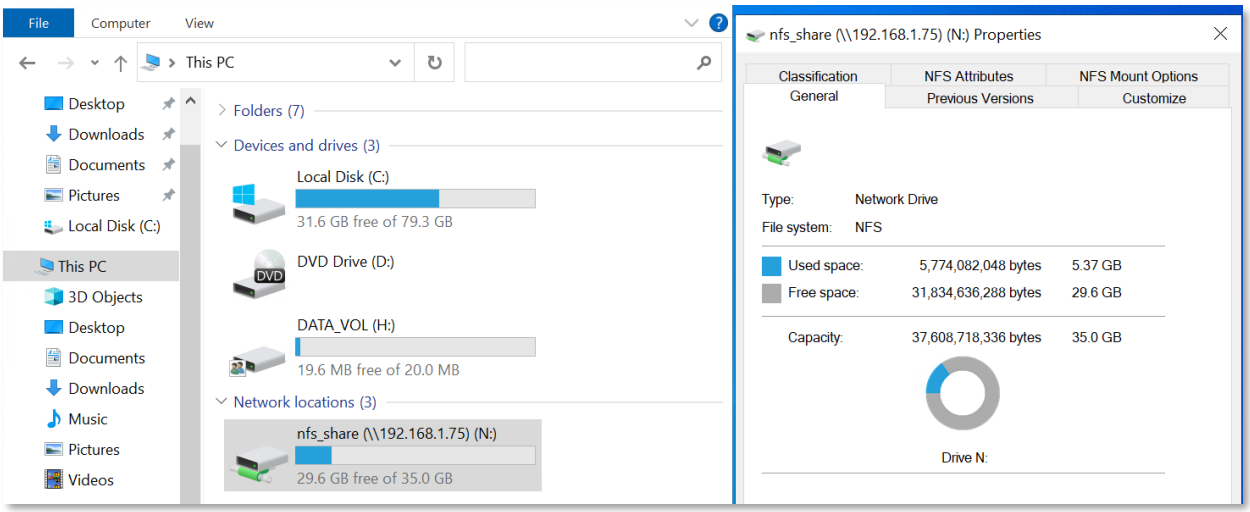
```
root@linuxserver:/home/gc
/nfs_share 192.168.1.0/24(rw,sync,no_subtree_check,no_root_squash)
```

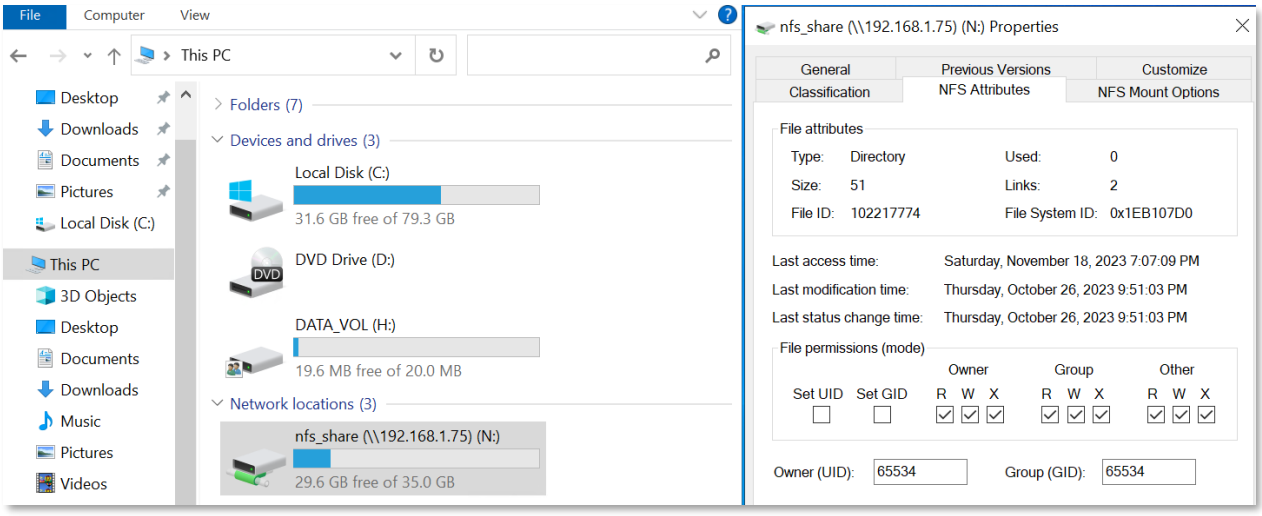
- rw - signifie "lecture-écriture" en français. Cela permet à la fois la lecture et l'écriture sur un volume NFS.
- sync - indique que le serveur répond aux requêtes seulement après que les modifications ont été confirmées et enregistrées de manière stable. C'est le comportement par défaut.
- no_subtree_check - désactive la vérification des sous-arborescences, ce qui a des implications de sécurité mineures mais peut améliorer la fiabilité dans certaines circonstances.
- no_root_squash - désactive l'écrasement du root. Cette option est principalement utile pour les clients sans disque.

- Le fichier - /etc/idmapd.conf, ou le domaine contoso.com est autorisé d'avoir accès au server NFS.

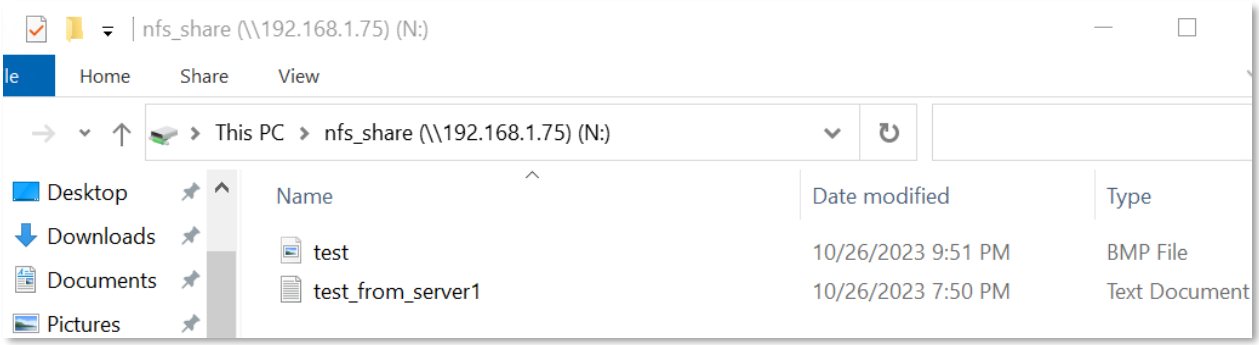
```
[General]
#Verbosity = 0
# The following should be set to the local NFSv4 domain name
# The default is the host's DNS domain name.
Domain = contoso.com
```

- La connexion du répertoire partagé nfs_share à Server1.





- Pour le test, j'ai créé deux fichiers directement depuis Server1.



Ils sont accessibles directement depuis Linux. Cela indique que le serveur NFS est fonctionnel à 100%. Les opérations de création et de lecture réussies confirment que les partages NFS sont configurés correctement et que les autorisations sont adéquates.

```
[root@linuxserver gc]# ls -l /nfs_share/
total 4
-rwxr-xr-x. 1 4294967294 4294967294 0 Oct 26 21:51 test.bmp
-rwxrwxrwx. 1 4294967294 4294967294 4 Oct 26 19:50 test_from_server1.txt
[root@linuxserver gc]#
```

- Samba

Le serveur Samba a été mis en place pour permettre le partage de fichiers via Samba et également pour partager les imprimantes de l'organisation. Pour réaliser cela, le serveur Samba est installé sur Linux, puis serveur Linux est ajouté au domaine Contoso.com.

```
[root@linuxserver gc]# realm list
contoso.com
  type: kerberos
  realm-name: CONTOSO.COM
  domain-name: contoso.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U@contoso.com
  login-policy: allow-realm-logins
[root@linuxserver gc]#
```

- Le serveur Samba est installé correctement et fonctionnel.

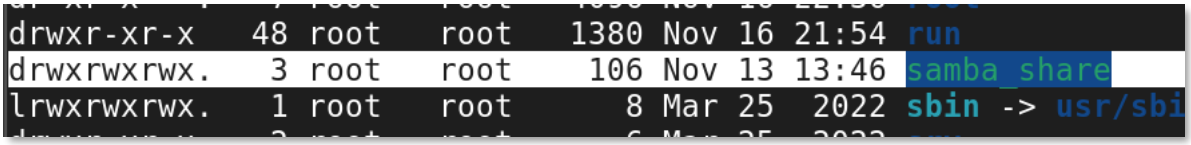
```
[root@linuxserver gc]# systemctl status smb
● smb.service - Samba SMB Daemon
     Loaded: loaded (/usr/lib/systemd/system/smb.service; enabled; preset: dis
     Active: active (running) since Thu 2023-11-16 21:16:34 EST; 1h 20min ago
       Docs: man:smbd(8)
             man:samba(7)
             man:smb.conf(5)
   Main PID: 1085 (smbd)
     Status: "smbd: ready to serve connections..."
      Tasks: 3 (limit: 22962)
     Memory: 13.1M
        CPU: 110ms
     CGroup: /system.slice/smb.service
             ├─1085 /usr/sbin/smbd --foreground --no-process-group
             ├─1363 /usr/sbin/smbd --foreground --no-process-group
             └─1364 /usr/sbin/smbd --foreground --no-process-group
```

- Le fichier de configuration Samba - /etc/samba/smb.conf

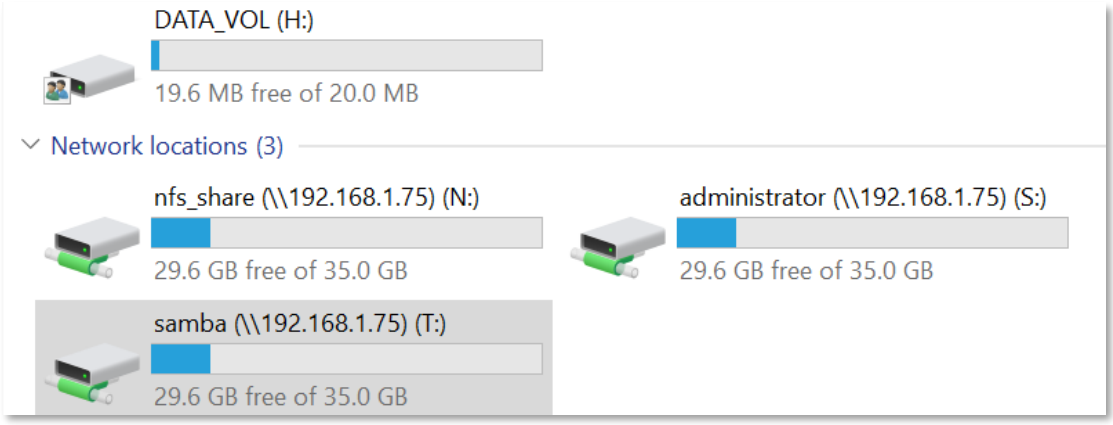
```
[global]
        workgroup = SAMBA
        security = user

        passdb backend = tdbsam
#       map to guest = Bad user

        printing = cups
        printcap name = cups
        load printers = yes
        cups options = raw

[homes]
        comment = Home Directories
        valid users = %S, %D%w%S
        browseable = No
        read only = No
        inherit acls = Yes


[printers]
        comment = All printers
        path = /var/tmp
        printable = yes
        create mask = 0700
        browseable = yes
        guest ok = yes
        writable = no
```

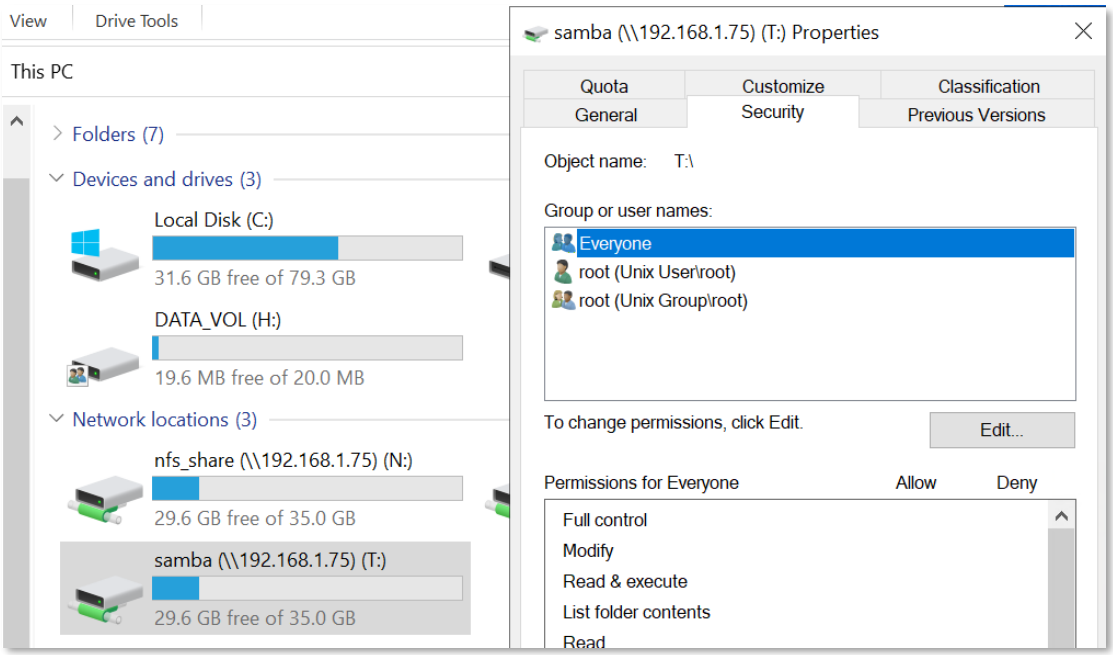
```
[print$]
        comment = Printer drivers
        path = /var/lib/samba/drivers
        write list = @printadmin root
        force group = @printadmin
        create mask = 0664
        directory mask = 0775

[samba]
        path = /samba_share
        browseable = yes
        writable = yes
        read only = no
        guest ok = yes
        public = yes
        valid users = administrator admin.it gc
        force create mode = 0777
        force directory mode = 0777

~
/etc/samba/smb.conf
```

- Le répertoire partagé samba_share

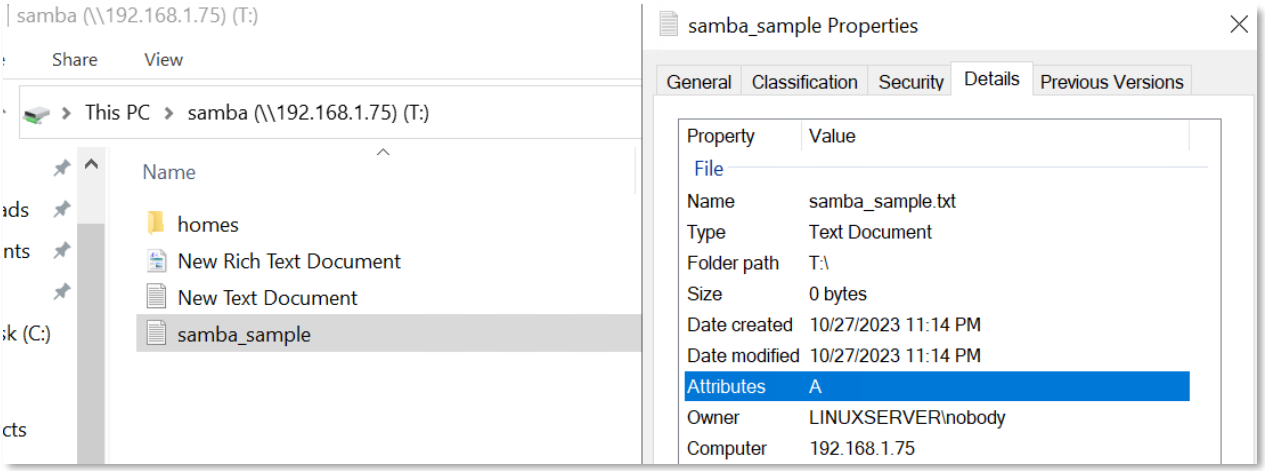


- La connexion du répertoire partagé Samba vers Server1 a réussi.





On teste le serveur en créant des différents fichiers. Ensuite, on vérifie directement sur le serveur Linux si les fichiers existent.

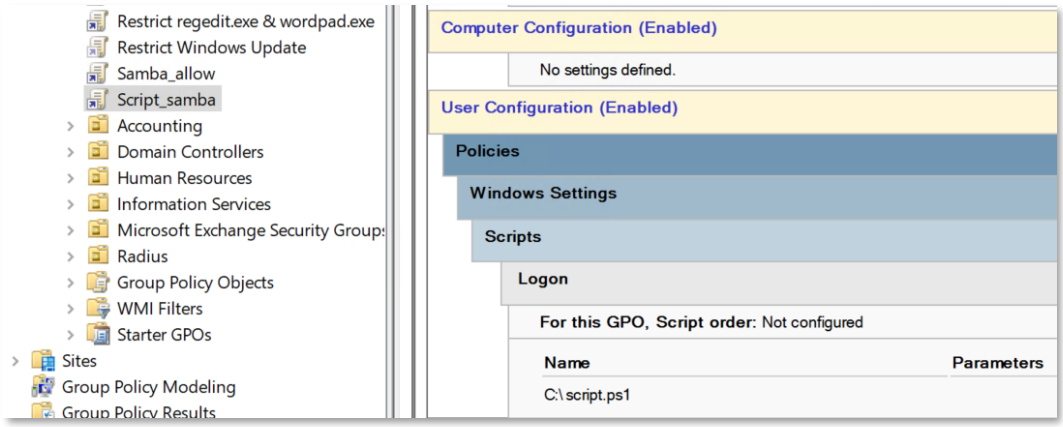



```
[root@linuxserver gc]# ls -l /samba_share/
total 4
drwxrwxrwx  2 administrator administrator 6 Nov 13 13:46  homes
-rwxrwxrwx  1 administrator administrator 7 Nov  2 19:35 'New Rich Text Document.rtf'
-rwxrwxr-x  1 nobody        nobody        0 Oct 30 18:24 'New Text Document.txt'
-rwxrwxr-x. 1 nobody        nobody        0 Oct 27 23:14  samba_sample.txt
[root@linuxserver gc]#
```

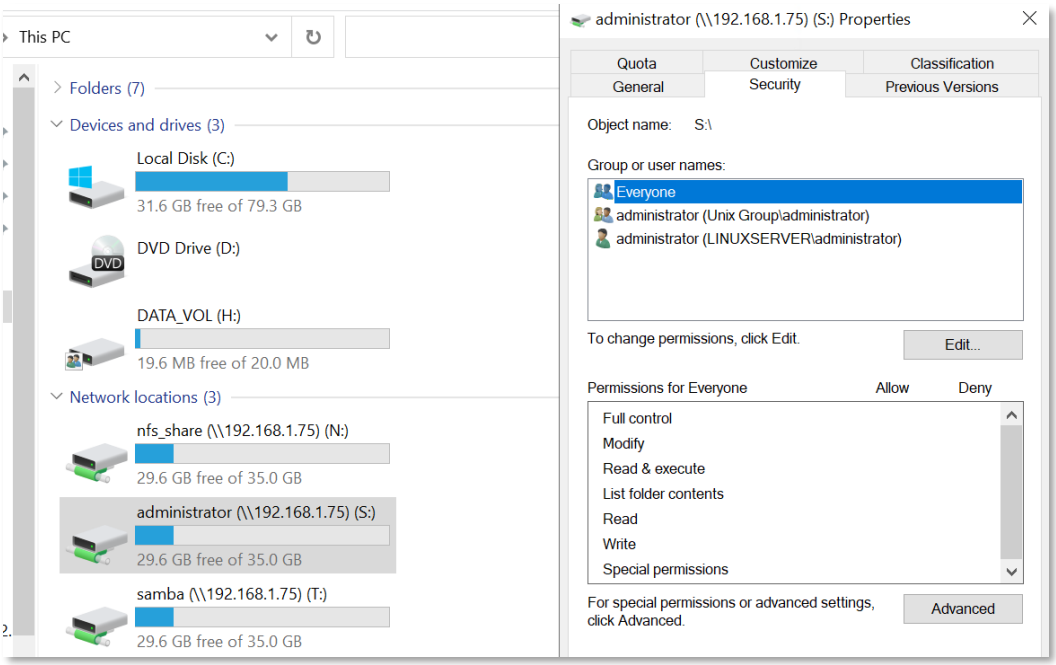
- L'organisation a décidé d'automatiser la connexion au répertoire Samba_share via le script suivant écrit en PowerShell, mais avec une différence: des répertoires seront créés pour les utilisateurs connectés. Le script est lancé à chaque démarrage de l'ordinateur ou du serveur via une stratégie de groupe (GPO).

script.ps1

```powershell
$SambaServer = "\\192.168.1.75"  ## Linux Server
$UserName = $env:USERNAME
$DriveLetter = "S"
$homeDirectory = Join-Path $SambaServer $UserName
if (Get-PSDrive -Name $DriveLetter -ErrorAction SilentlyContinue) {
    Remove-PSDrive -Name $DriveLetter -Force
}
New-PSDrive -Name $DriveLetter -PSProvider FileSystem -Root $homeDirectory -Persist
```



Nous observons la différence qu'un disque dur virtuel a été créé avec le nom de l'utilisateur, dans ce cas, celui de l'administrateur.




```
[root@linuxserver gc]# ls -l /home
total 12
drwx------   3 administrator            administrator                4096 Nov 13 21:24  administrator
drwx------   2 administrator@contoso.com domain users@contoso.com      160 Nov 13 21:22  administrator@co
m
drwx------   3 admin.it                 admin.it                     4096 Nov 13 14:40  admin.it
drwx------   2 exchange$@contoso.com    domain computers@contoso.com    6 Nov  2 19:36 'exchange$@contos
drwx------. 15 gc                       gc                           4096 Nov  2 19:56  gc
drwx------.  3 smbuser                  smbuser                        92 Oct 26 23:37  smbuser
[root@linuxserver gc]#
```

L'étape suivante consiste à configurer le serveur d'impression CUPS, qui fonctionnera également via le serveur Samba.

```
[root@linuxserver gc]# systemctl status cups
● cups.service - CUPS Scheduler
     Loaded: loaded (/usr/lib/systemd/system/cups.service; enabled; preset: enabled)
    Drop-In: /usr/lib/systemd/system/cups.service.d
             └─server.conf
     Active: active (running) since Thu 2023-11-16 21:16:34 EST; 1h 41min ago
TriggeredBy: ● cups.path
             ● cups.socket
       Docs: man:cupsd(8)
   Main PID: 901 (cupsd)
     Status: "Scheduler is running..."
      Tasks: 2 (limit: 22962)
     Memory: 7.4M
        CPU: 126ms
     CGroup: /system.slice/cups.service
             └─901 /usr/sbin/cupsd -l
```

- Le fichier de configuration du CUPS - /etc/cups/cupsd.conf

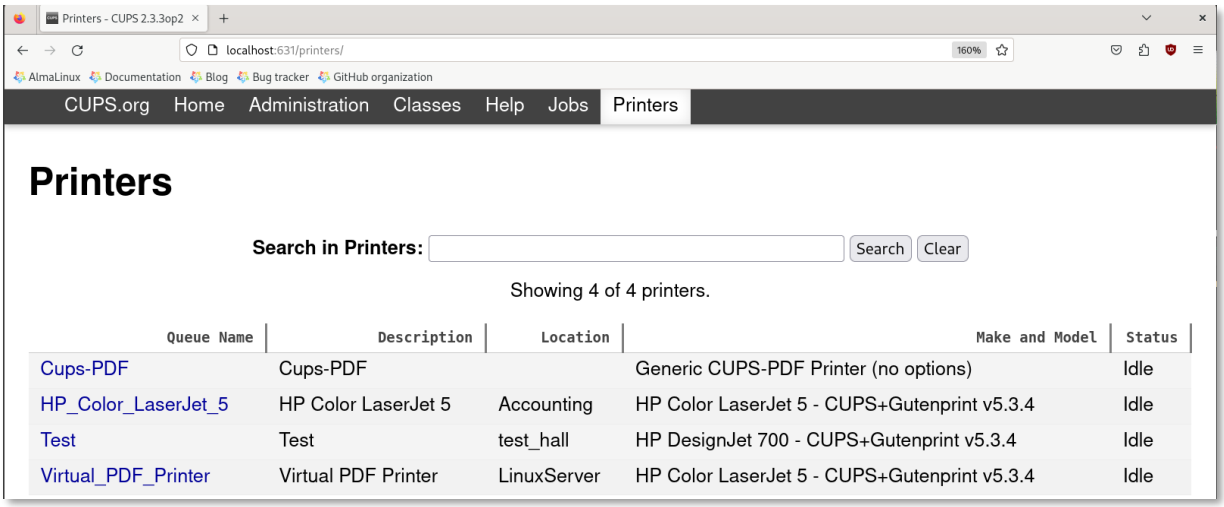
  L'accès est accordé uniquement au réseau local du Contoso.com.

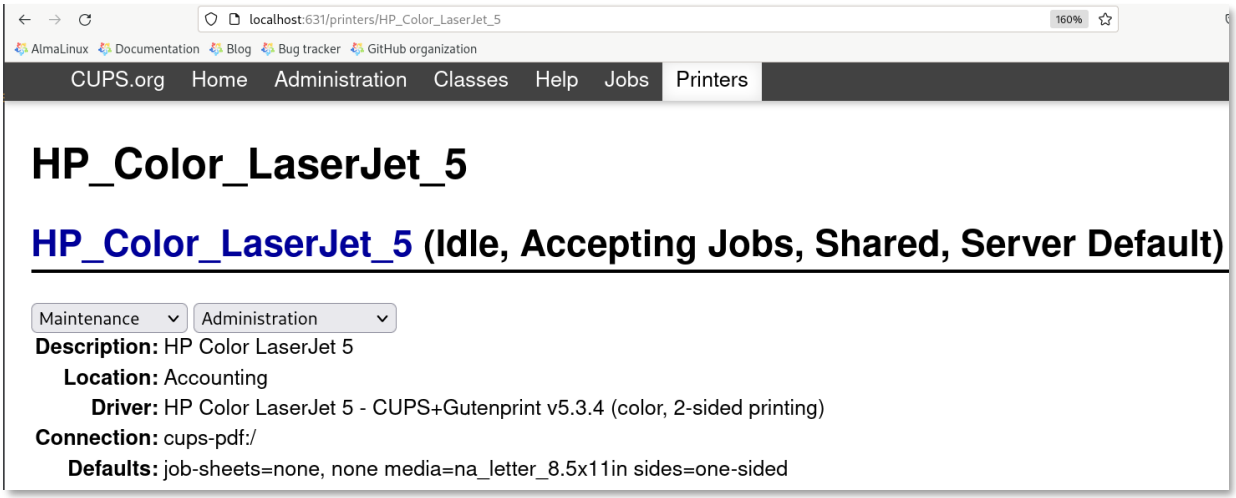
```
#Listen /run/cups/cups.sock
Port 631
# Show shared printers on the local network.
Browsing On
BrowseLocalProtocols dnssd

# Default authentication type, when authentication is required...
DefaultAuthType Basic

# Web interface setting...
WebInterface Yes

# Timeout after cupsd exits if idle (applied only if cupsd runs on-demand - with -l)
IdleExitTimeout 0
```

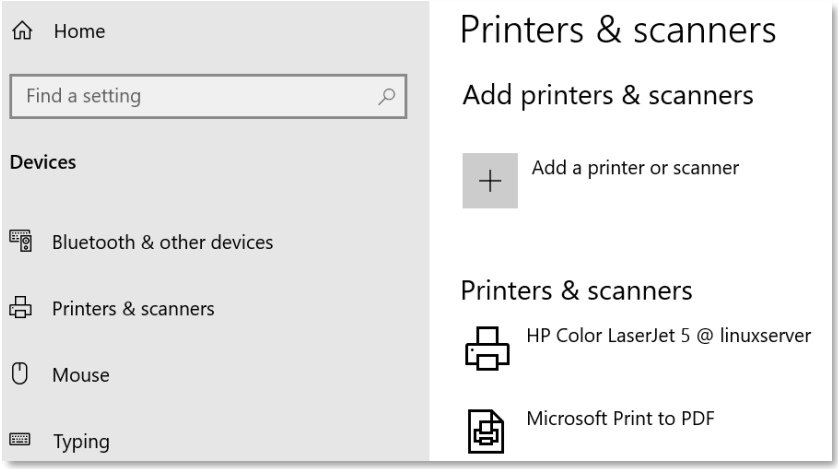
```
# Restrict access to the server...
<Location />
  Allow from 192.168.1.0/24
  Allow from 192.168.1.0/26
  Allow from 192.168.1.64/26
  Allow from 192.168.1.128/26
  Allow from localhost
  Order allow,deny
</Location>

# Restrict access to the admin pages...
<Location /admin>
  Allow from 192.168.1.70
  Allow from 192.168.1.75
  Allow localhost
  Order allow,deny
</Location>
```

```
# Restrict access to configuration files...
<Location /admin/conf>
  Allow from 192.168.1.70
  Allow from 192.168.1.75
  Allow from 192.168.1.0/24
  Allow localhost
  AuthType Default
  Require user @SYSTEM
  Order allow,deny
</Location>

# Restrict access to log files..
<Location /admin/log>
  Allow from 192.168.1.70
  Allow from 192.168.1.75
  Allow localhost
  AuthType Default
  Require user @SYSTEM
  Order allow,deny
</Location>
/etc/cups/cupsd.conf
```

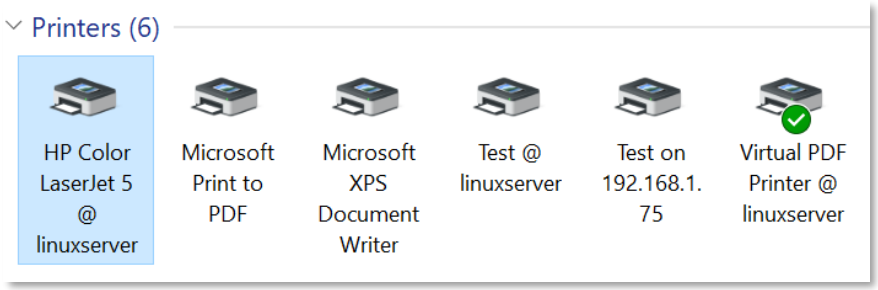
- On configure les imprimantes via l'interface Web du serveur CUPS.







On procède à l'installation d'une imprimante sur un système d'exploitation Windows, par exemple une imprimante HP LaserJet 5. Et on envoie un document à l'imprimante pour test.



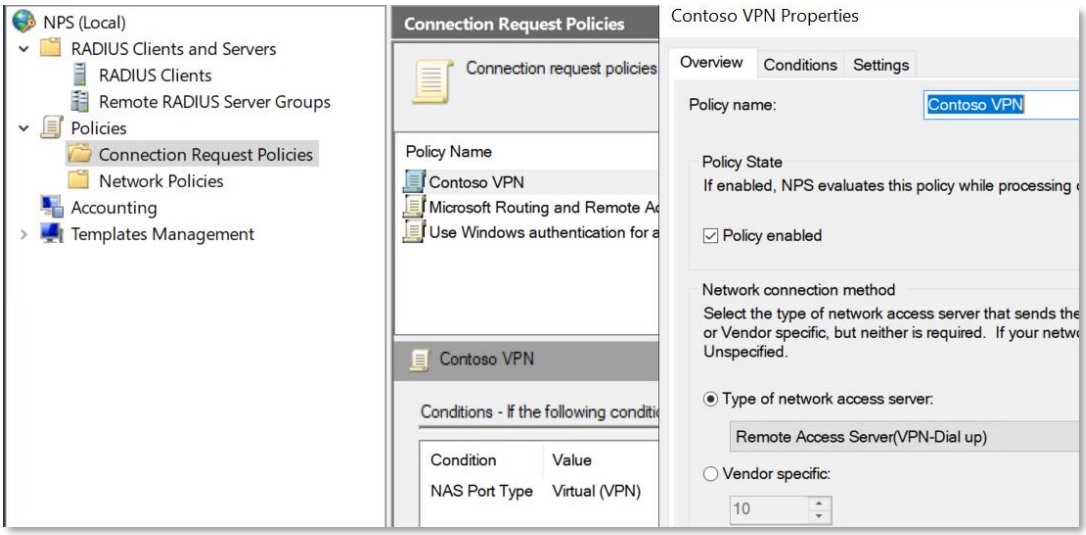
Dans l'interface Web d'administration du serveur CUPS, nous pouvons voir que l'impression a réussi

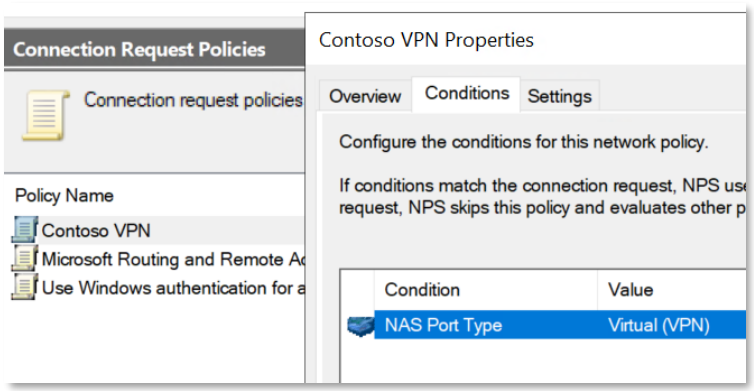
Jobs listed in descending order.

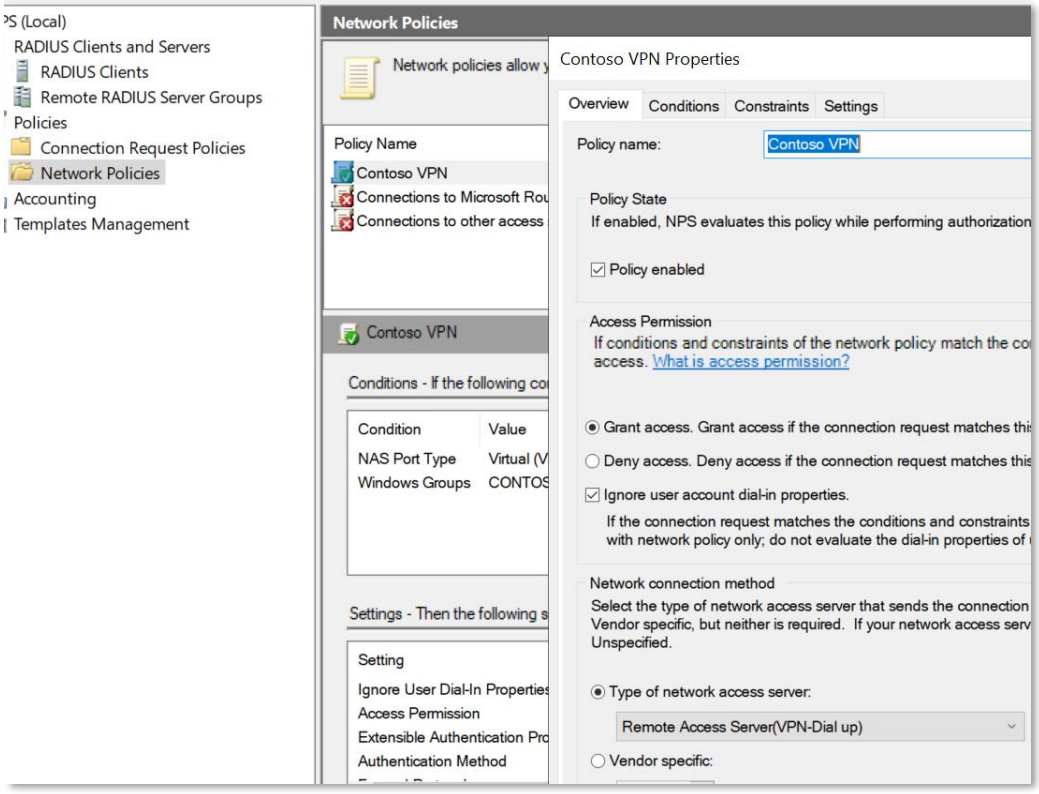
ID	Name	User	Size	Pages	State
HP_Color_LaserJet_5-7	Unknown	Withheld	2k	Unknown	completed at Thu 02 Nov 2023 07:52:26 PM
HP_Color_LaserJet_5-8	Unknown	Withheld	243k	1	completed at Thu 02 Nov 2023 08:35:27 PM
Test-13	Unknown	Withheld	243k	1	completed at Mon 13 Nov 2023 09:22:57 PM

- VPN et RADIUS

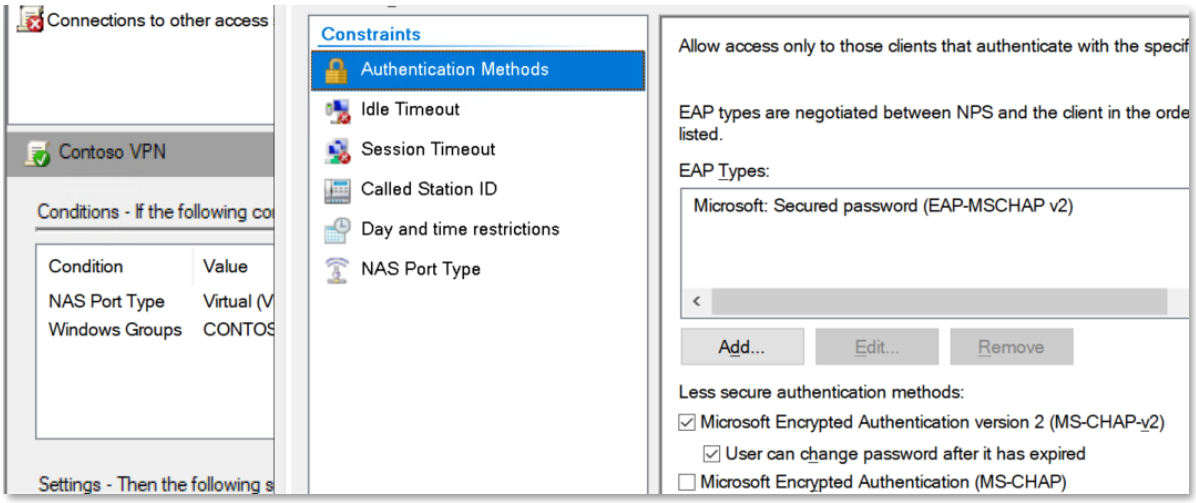
  L'organisation a besoin de mobilité, c'est pourquoi un serveur VPN avec une authentification Radius a été intégré. Les employés peuvent se connecter à distance depuis n'importe quel endroit du monde via le VPN et peuvent être gérés grâce aux politiques de domaine. Le rôle de serveur NPS (Radius) est installé sur Server1, tandis que le rôle de serveur VPN est installé sur Server2.



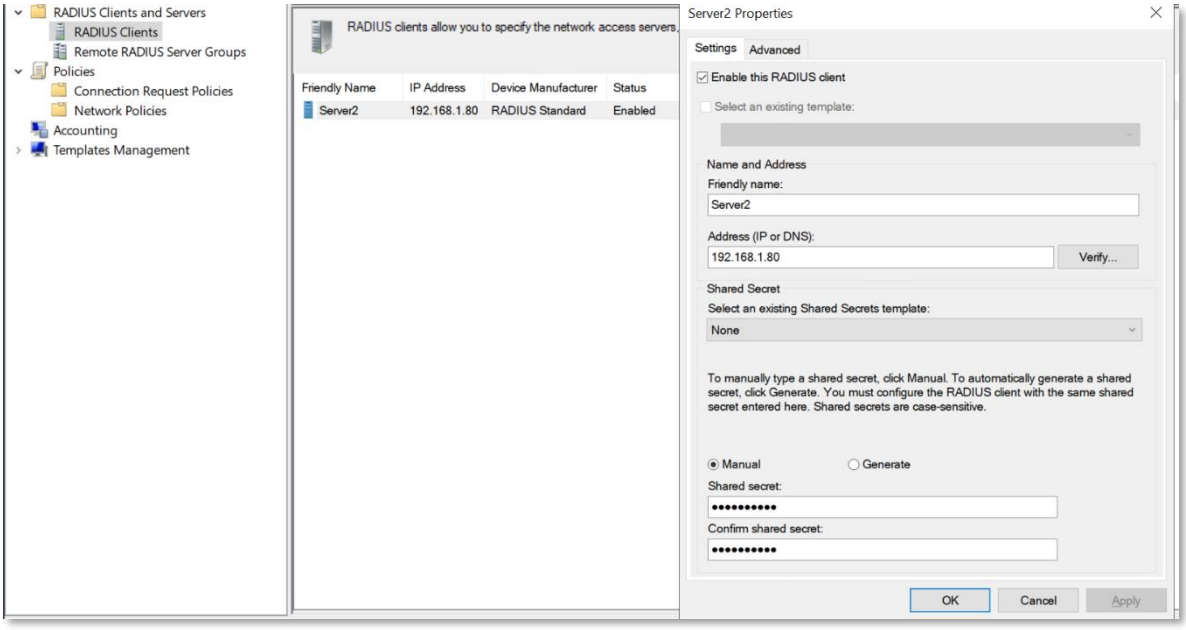

Connection Request Policies
Connection request policies
Policy Name
Contoso VPN
Microsoft Routing and Remote Ac
Use Windows authentication for a
Contoso VPN Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS us
request, NPS skips this policy and evaluates other p
Condition
Value
NAS Port Type
Virtual (VPN)


S (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Accounting
Templates Management
Network Policies
Network policies allow
Policy Name
Contoso VPN
Connections to Microsoft Rou
Connections to other access
Contoso VPN
Conditions - If the following co
Condition
Value
NAS Port Type
Virtual (V
Windows Groups
CONTOS
Settings - Then the following s
Setting
Ignore User Dial-In Properties
Access Permission
Extensible Authentication Pro
Authentication Method
Contoso VPN Properties
Overview
Conditions
Constraints
Settings
Policy name:
Contoso VPN
Policy State
If enabled, NPS evaluates this policy while performing authorization
Policy enabled
Access Permission
If conditions and constraints of the network policy match the co
access. What is access permission?
Grant access. Grant access if the connection request matches thi
Deny access. Deny access if the connection request matches this
Ignore user account dial-in properties.
If the connection request matches the conditions and constraints
with network policy only; do not evaluate the dial-in properties of
Network connection method
Select the type of network access server that sends the connection
Vendor specific, but neither is required. If your network access serv
Unspecified.
Type of network access server:
Remote Access Server(VPN-Dial up)
Vendor specific:

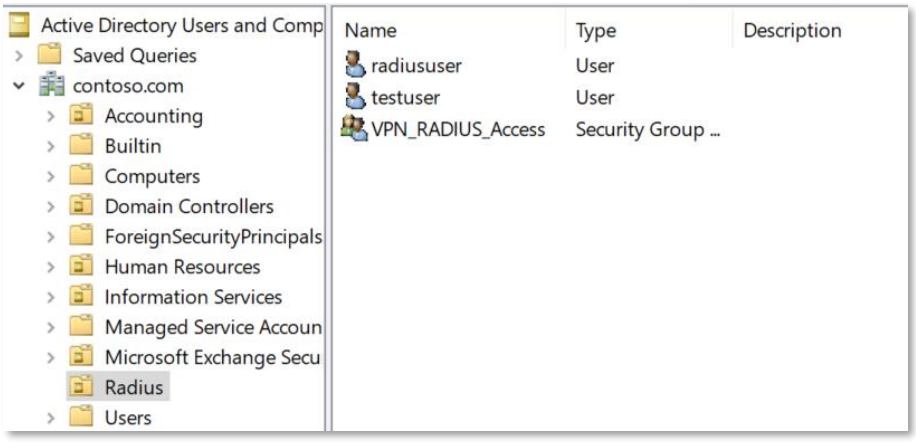
L'authentification a lieu à travers le protocole MS-CHAP2, ce qui indique que le processus d'authentification utilise le Microsoft Challenge Handshake Authentication Protocol version 2. Ce protocole est couramment utilisé pour sécuriser les connexions VPN

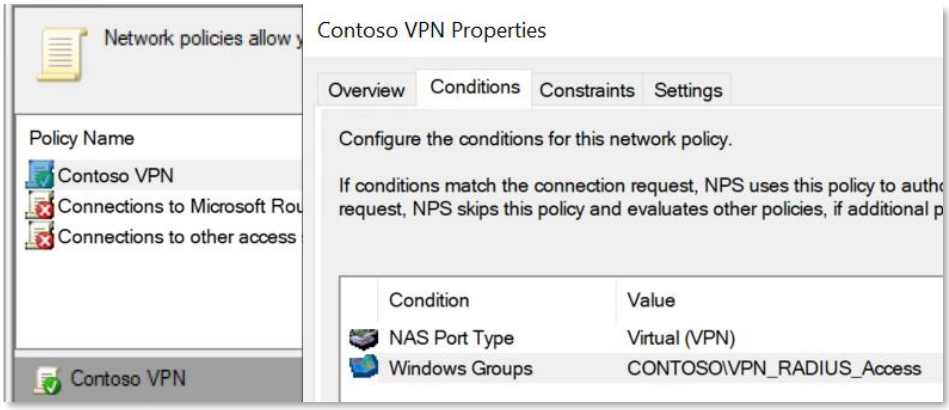


Le serveur2, avec le VPN installé, fait office de client Radius en se connectant à un serveur d'authentification Radius (comme Server1) pour vérifier les informations d'identification des utilisateurs VPN, assurant ainsi une gestion centralisée des accès.

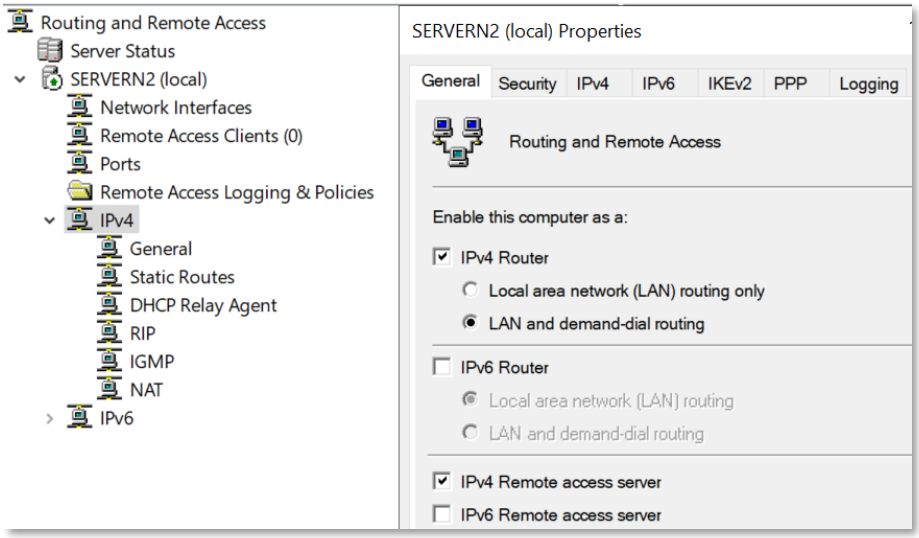


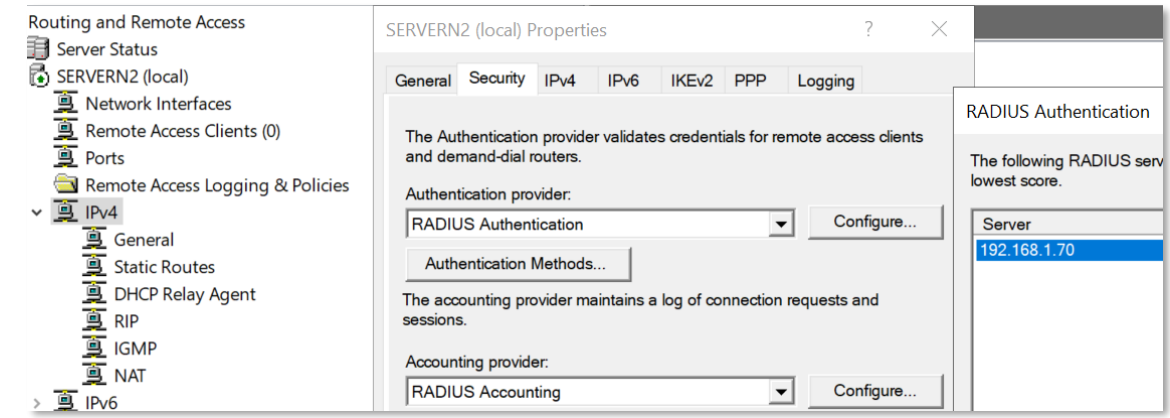
Pour l'authentification, il est nécessaire d'avoir un utilisateur ou un groupe dédié autorisé dans le serveur Radius, par exemple l'utilisateur **radiususer** et le groupe **VPN_Radius_Access.**

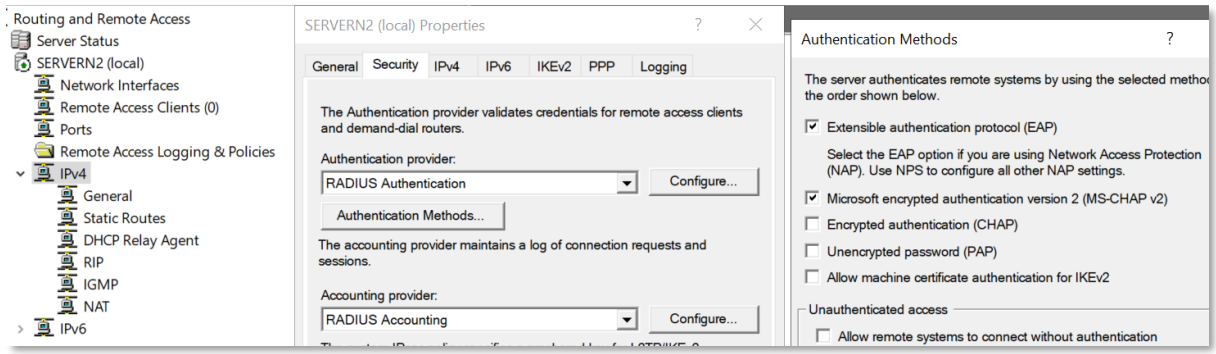


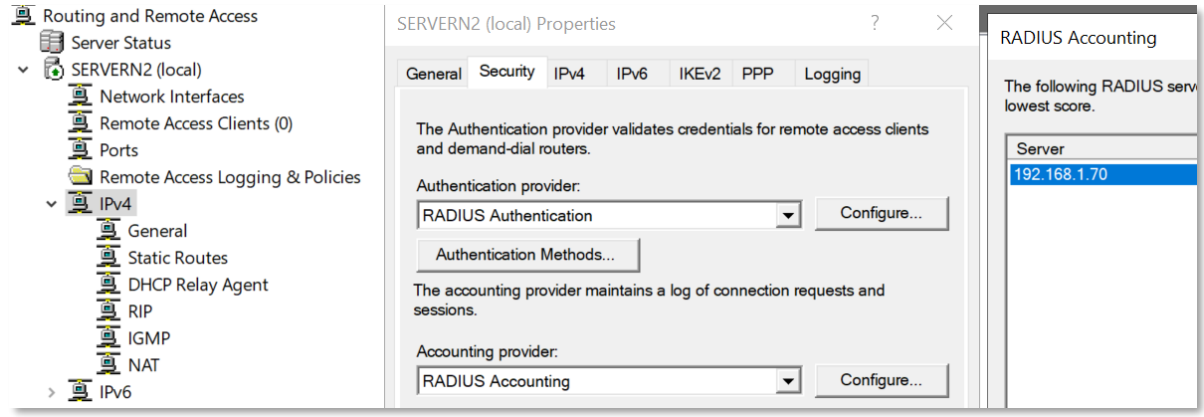


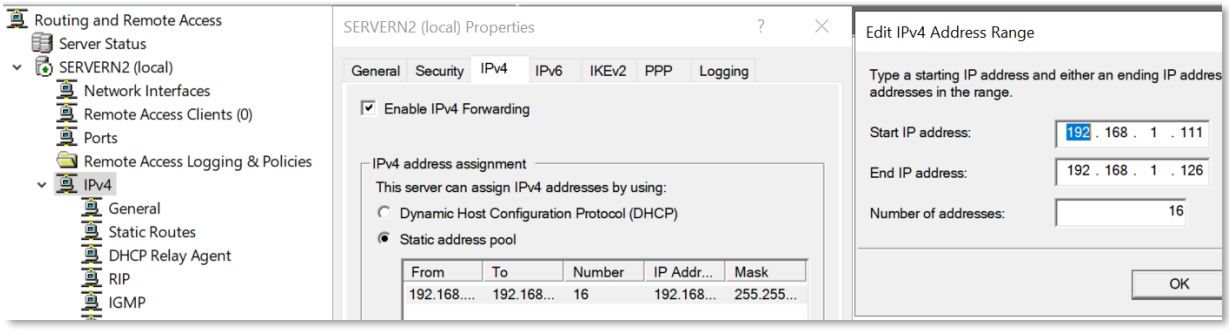
Lors de la configuration du serveur VPN, nous précisons l'utilisation de la méthode d'authentification MS-CHAP2 et indiquons le serveur Radius, qui est Server1 dans notre contexte.



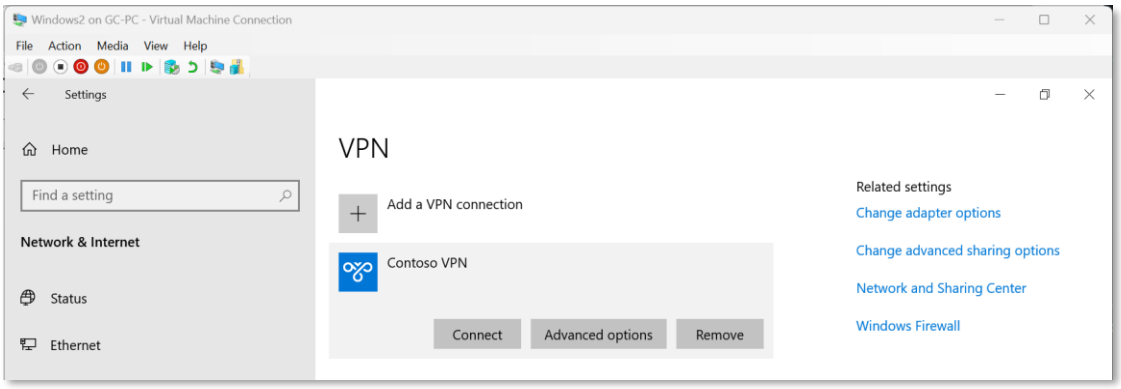

Routing and Remote Access
Server Status
SERVERN2 (local)
Network Interfaces
Remote Access Clients (0)
Ports
Remote Access Logging & Policies
IPv4
General
Static Routes
DHCP Relay Agent
RIP
IGMP
NAT
IPv6
SERVERN2 (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
The Authentication provider validates credentials for remote access clients and demand-dial routers.
Authentication provider:
RADIUS Authentication
Configure...
Authentication Methods...
The accounting provider maintains a log of connection requests and sessions.
Accounting provider:
RADIUS Accounting
Configure...
RADIUS Authentication
The following RADIUS serv
lowest score.
Server
192.168.1.70

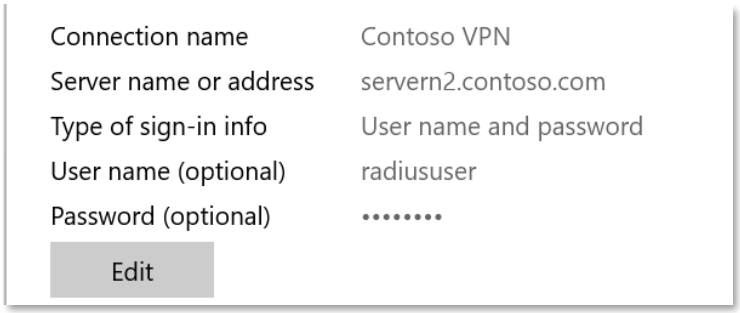

Routing and Remote Access
Server Status
SERVERN2 (local)
Network Interfaces
Remote Access Clients (0)
Ports
Remote Access Logging & Policies
IPv4
General
Static Routes
DHCP Relay Agent
RIP
IGMP
NAT
IPv6
SERVERN2 (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
The Authentication provider validates credentials for remote access clients and demand-dial routers.
Authentication provider:
RADIUS Authentication
Configure...
Authentication Methods...
The accounting provider maintains a log of connection requests and sessions.
Accounting provider:
RADIUS Accounting
Configure...
Authentication Methods
The server authenticates remote systems by using the selected metho
the order shown below.
Extensible authentication protocol (EAP)
Select the EAP option if you are using Network Access Protection (NAP). Use NPS to configure all other NAP settings.
Microsoft encrypted authentication version 2 (MS-CHAP v2)
Encrypted authentication (CHAP)
Unencrypted password (PAP)
Allow machine certificate authentication for IKEv2
Unauthenticated access
Allow remote systems to connect without authentication

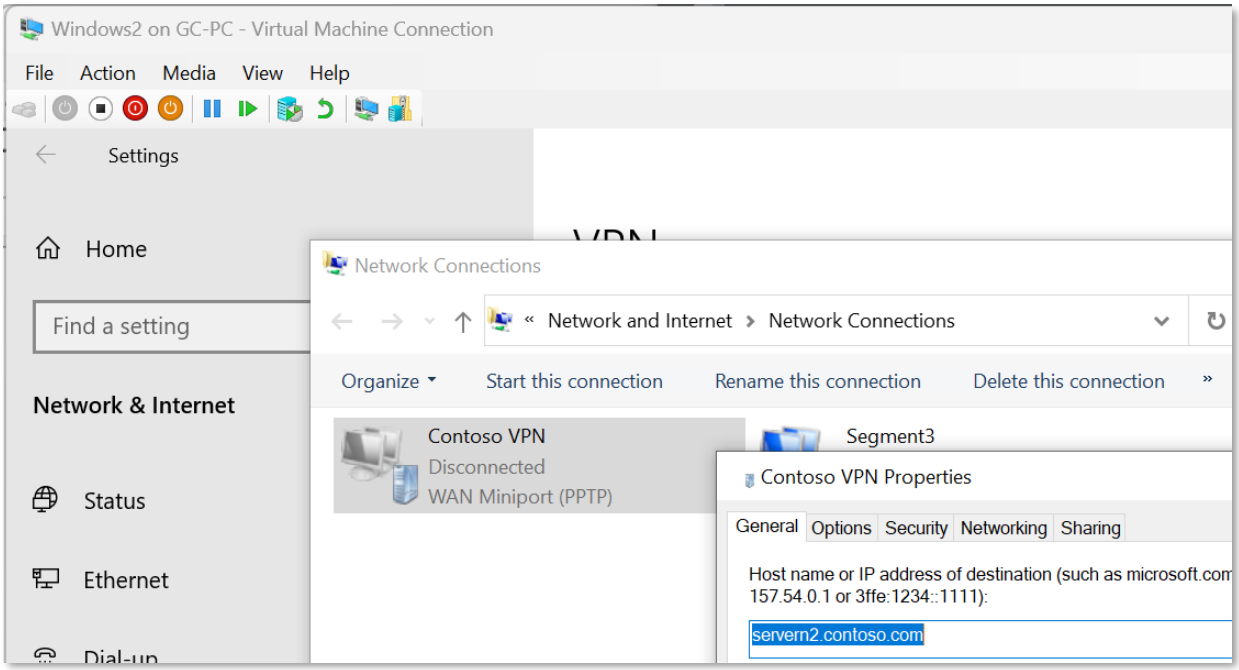

Routing and Remote Access
Server Status
SERVERN2 (local)
Network Interfaces
Remote Access Clients (0)
Ports
Remote Access Logging & Policies
IPv4
General
Static Routes
DHCP Relay Agent
RIP
IGMP
NAT
IPv6
SERVERN2 (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
The Authentication provider validates credentials for remote access clients and demand-dial routers.
Authentication provider:
RADIUS Authentication
Configure...
Authentication Methods...
The accounting provider maintains a log of connection requests and sessions.
Accounting provider:
RADIUS Accounting
Configure...
RADIUS Accounting
The following RADIUS serv
lowest score.
Server
192.168.1.70

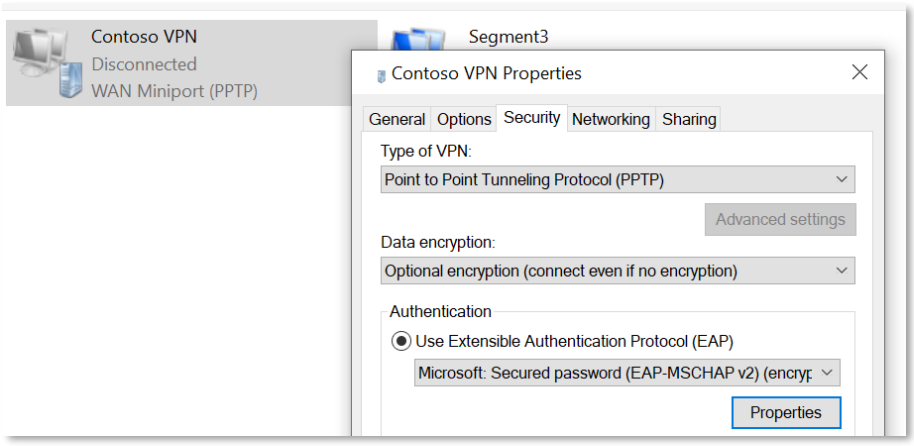

Routing and Remote Access
Server Status
SERVERN2 (local)
Network Interfaces
Remote Access Clients (0)
Ports
Remote Access Logging & Policies
IPv4
General
Static Routes
DHCP Relay Agent
RIP
IGMP
SERVERN2 (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
Enable IPv4 Forwarding
IPv4 address assignment
This server can assign IPv4 addresses by using:
Dynamic Host Configuration Protocol (DHCP)
Static address pool
From
To
Number
IP Addr...
Mask
192.168....
192.168...
16
192.168...
255.255...
Edit IPv4 Address Range
Type a starting IP address and either an ending IP addres
addresses in the range.
Start IP address:
192 . 168 . 1 . 111
End IP address:
192 . 168 . 1 . 126
Number of addresses:
16
OK

- Ensuite, on configure le client VPN dans le troisième segment du réseau, par exemple.



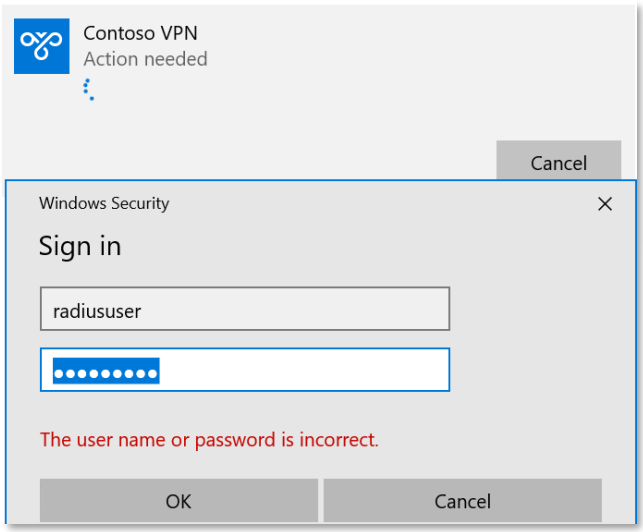


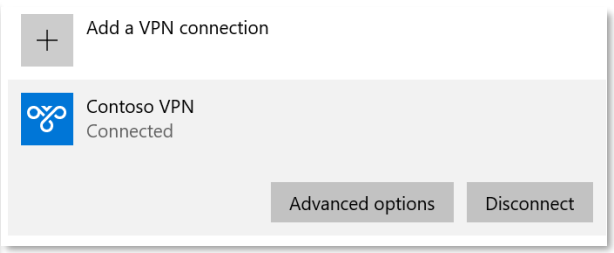




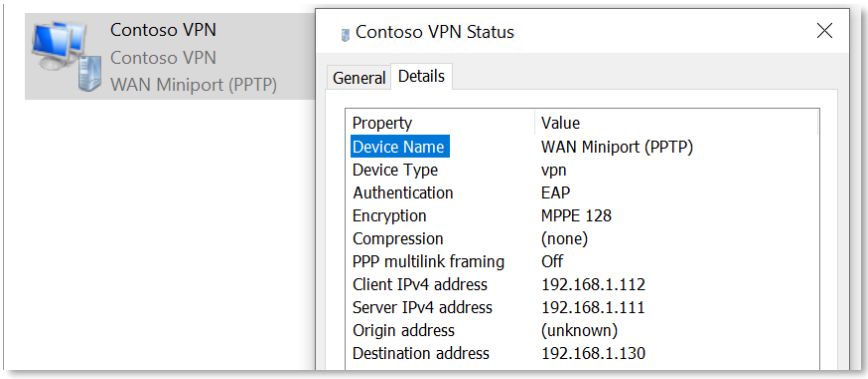
La configuration est en PPTP (Point-to-Point Tunneling Protocol) avec MS-CHAP2 comme méthode d'authentification.

Ensuite, on teste la connexion VPN en utilisant l'authentification avec l'utilisateur "radiususer".

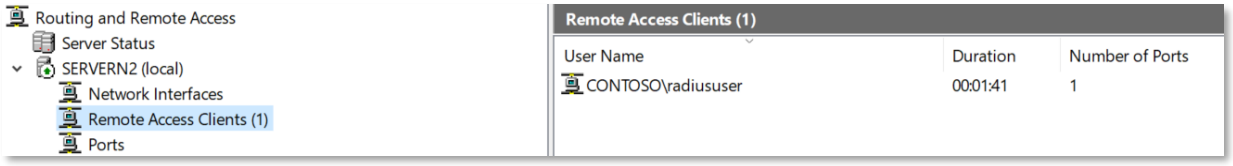




La connexion a réussi, et nous vérifions les paramètres du réseau de la connexion, tels que l'adresse IP et l'utilisateur connecté au serveur Radius. L'adresse IP est correcte.

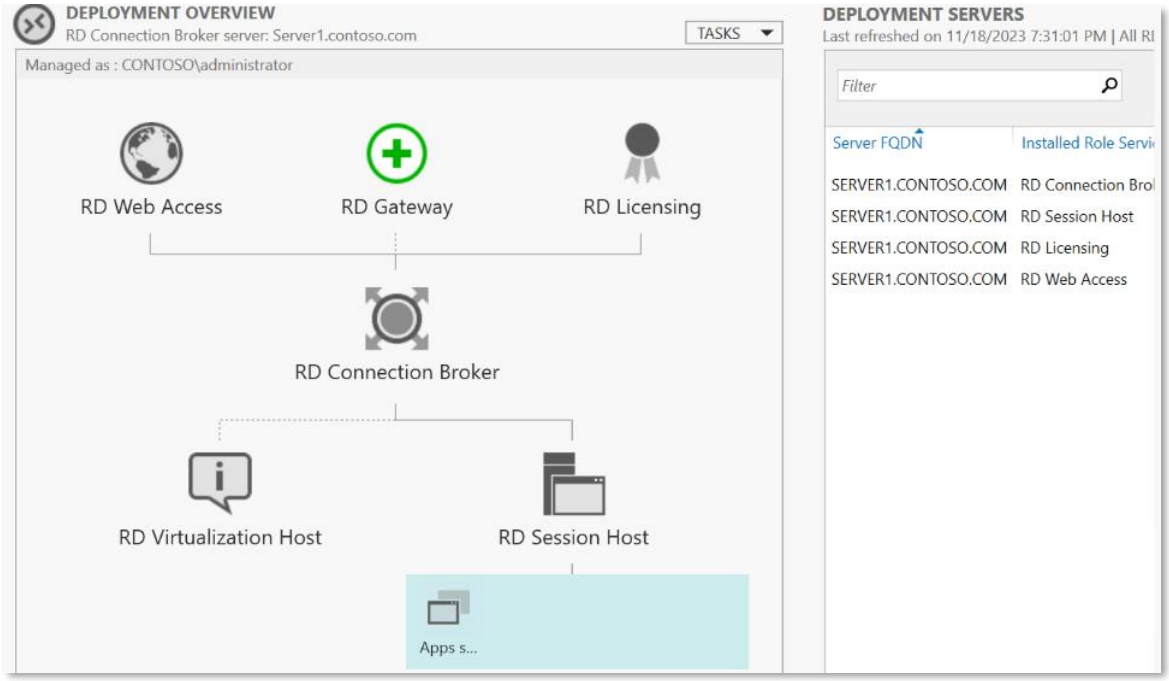


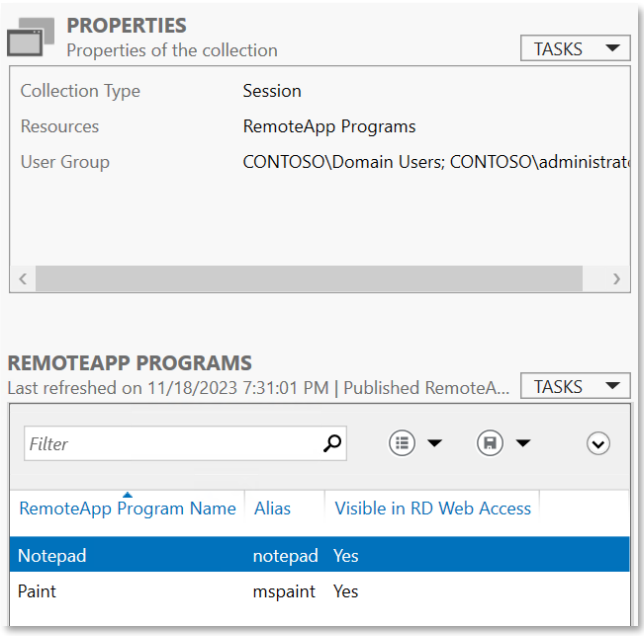
De plus, l'utilisateur connecté est "radiususer". Nous pouvons conclure que la configuration du serveur Radius et du serveur VPN est correcte.



Terminal Server

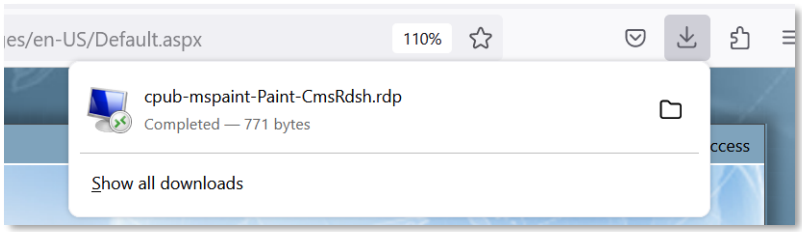
L'entreprise a l'intention de partager certaines applications, telles que Paint et Notepad, en utilisant les services Terminal Server sur Server1. Ensuite, nous procédons à la configuration de Server1 et effectuons des tests. On aj0oute les rôles RD Virtualization Host, RD Session Host, RD Connection Broker, RD Web Access et RD Licensing.



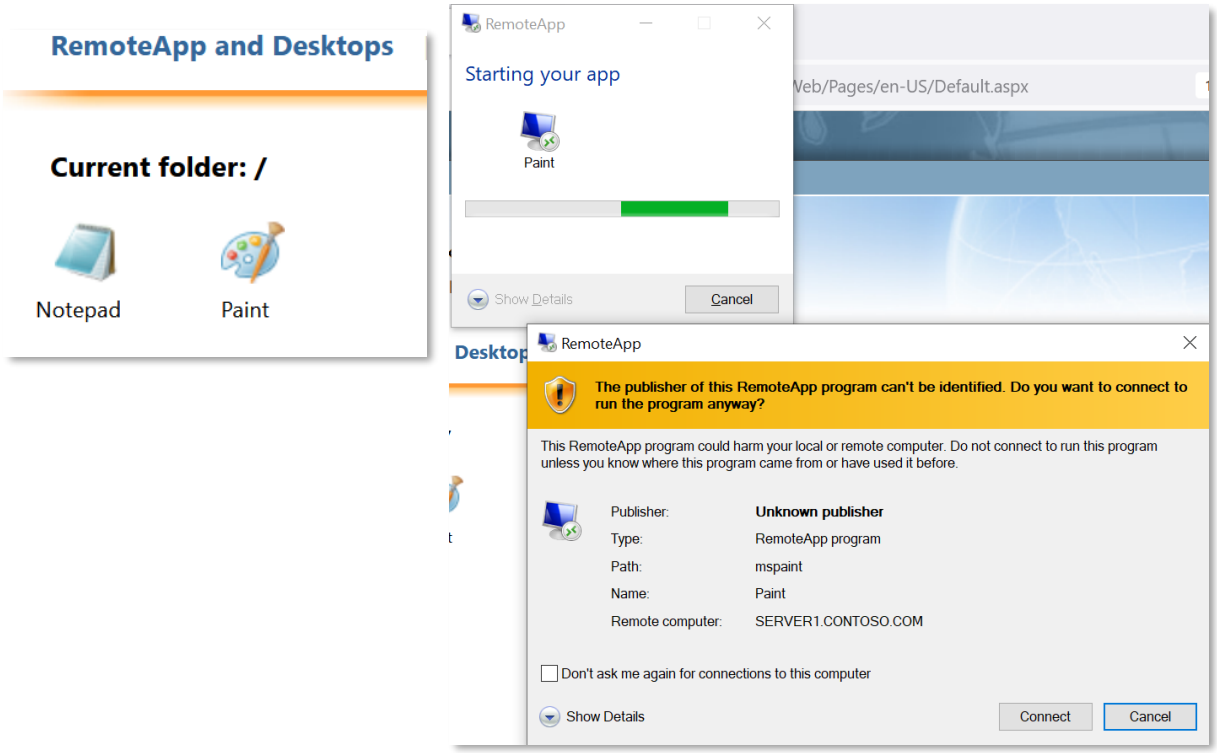


La configuration du serveur pour partager à distance les applications Paint et Notepad.

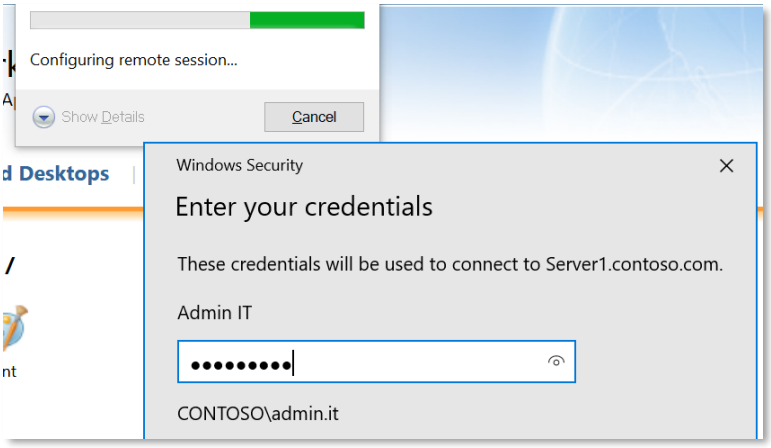
Sur un client Windows 10, nous accédons à la page web **server1.contoso.com/rdweb** pour tester le service Terminal Server. On se connecte avec le nom d'utilisateur du domaine.



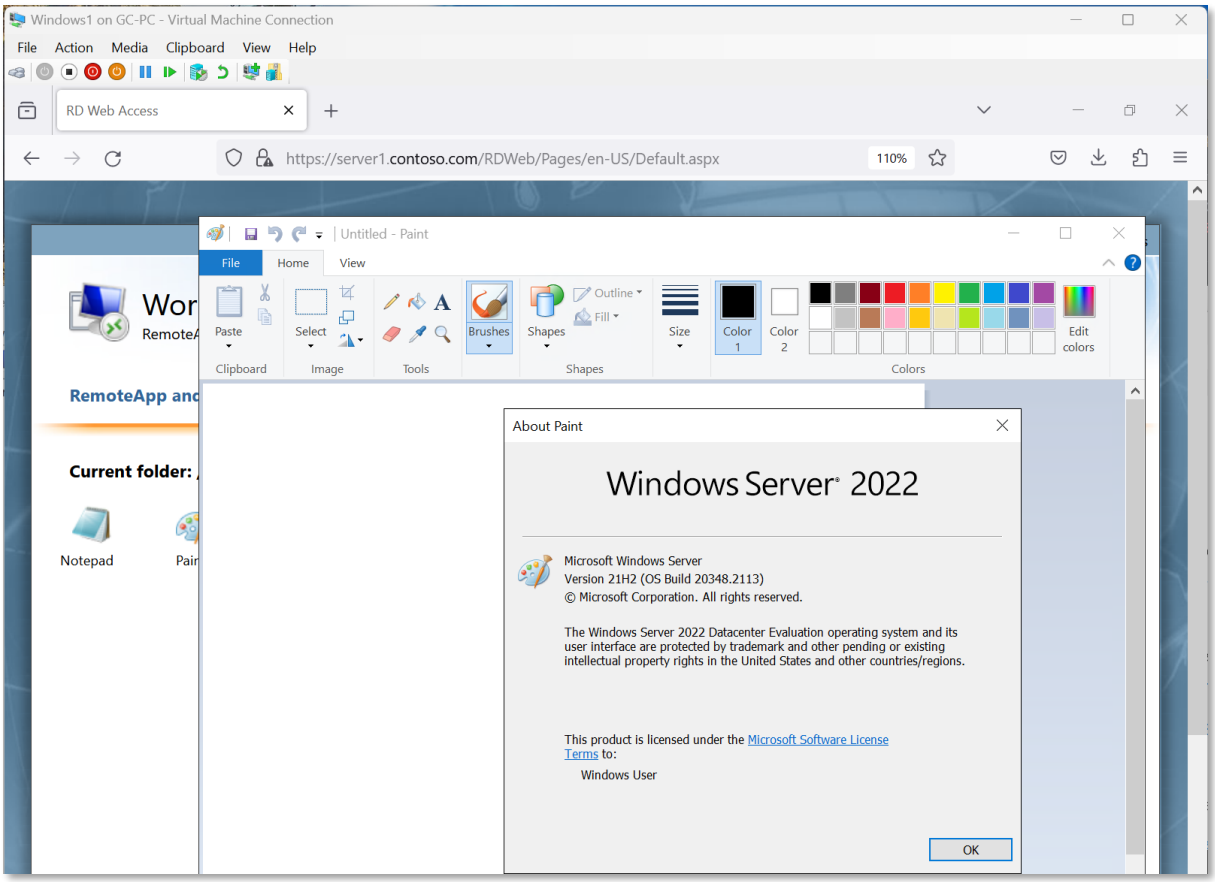
On trouve les applications partagées et on essaie d'ouvrir une application, par exemple Paint.



On saisit notre mot de passe utilisateur.

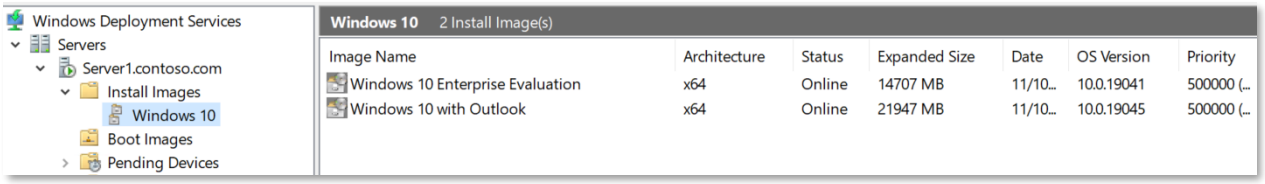


Voilà, l'application est démarrée avec succès.



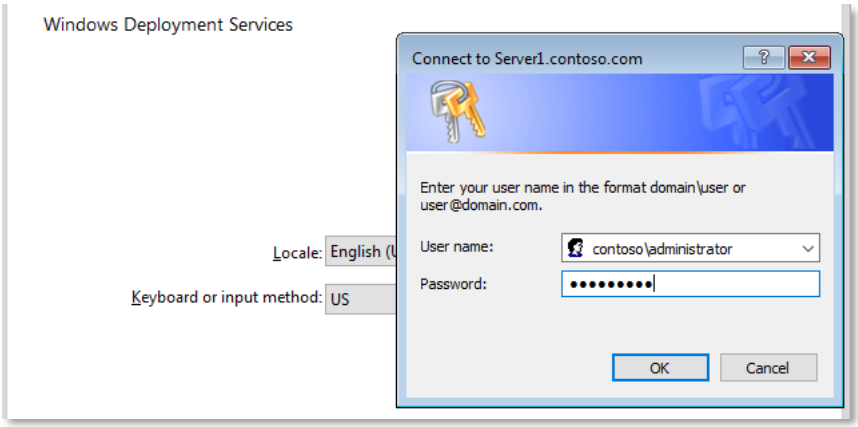
WDS Server

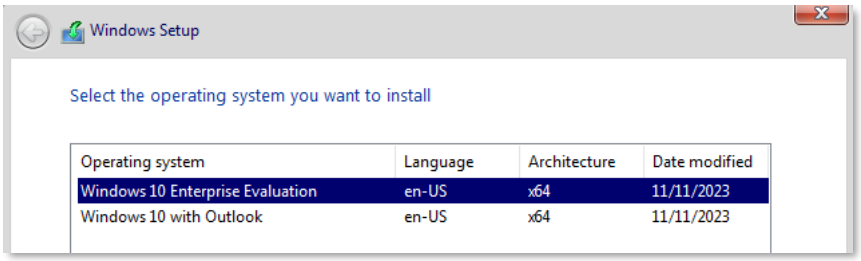
La prochaine étape consiste à configurer le rôle de serveur WDS (Windows Deployment Services) sur Server1. Nous allons configurer le serveur avec l'image d'installation de Windows 10 Enterprise. La configuration est simple et implique principalement l'autorisation de l'accès au serveur ainsi que l'installation des images boot.wim (image de démarrage de Windows) et install.wim (image d'installation réelle de Windows).

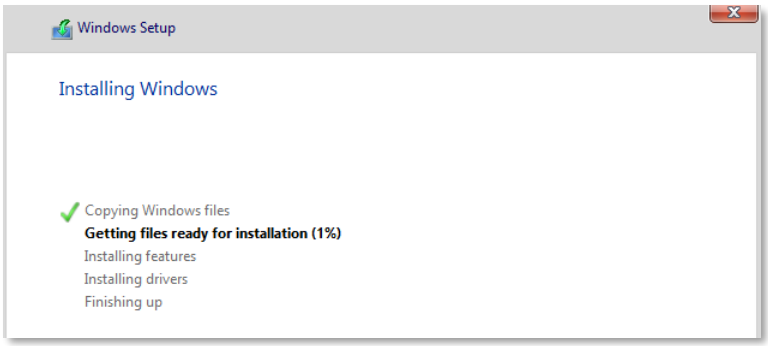


Pour le test, nous démarrons une machine virtuelle sans système d'exploitation. Nous observons que la machine se connecte au serveur TFTP, qui est en réalité le serveur WDS.

Nous saisissons le mot de passe de l'administrateur, puis nous pouvons commencer le processus d'installation proprement dit de Windows 10.



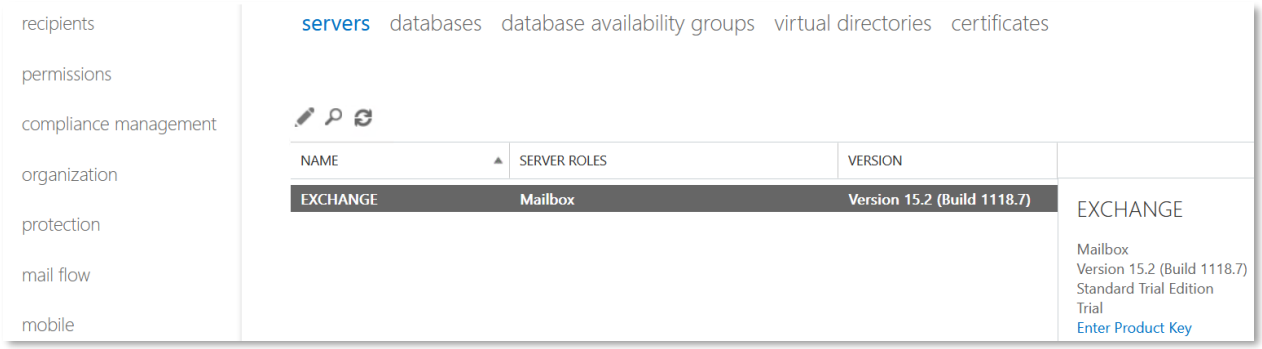




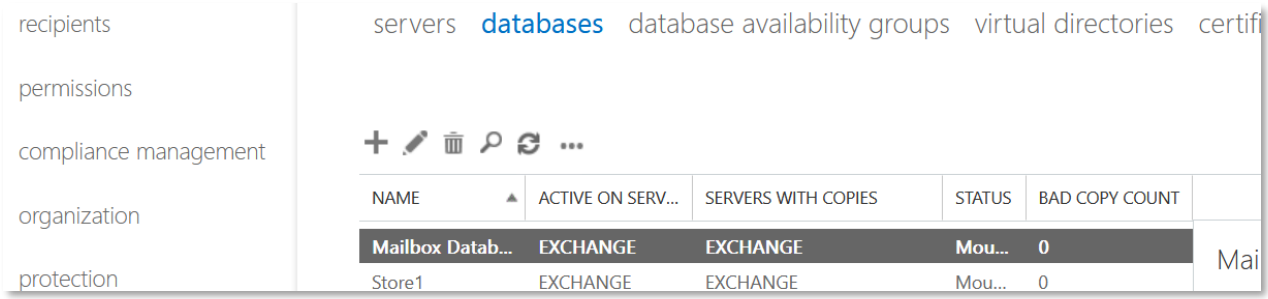
L'installation se déroule comme prévu, on peut conclure que le Terminal Server fonctionne correctement.

Exchange Server

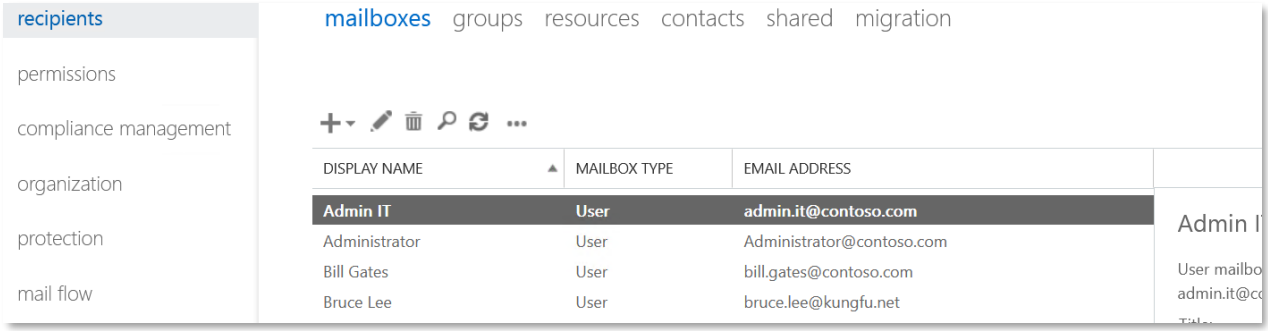
Contoso.com requiert la mise en place d'un serveur de messagerie électronique, avec le choix porté sur Exchange Server. Les détails de la configuration et des tests seront abordés plus bas.



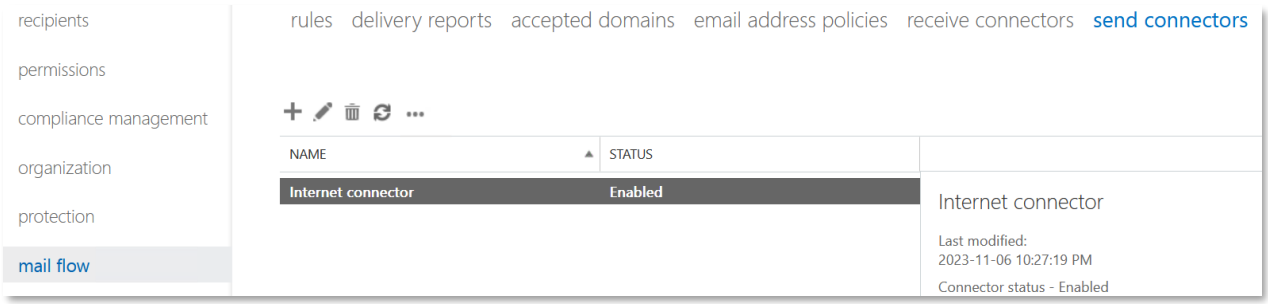
Pour commencer, on va créer une base de données nommée "store1".

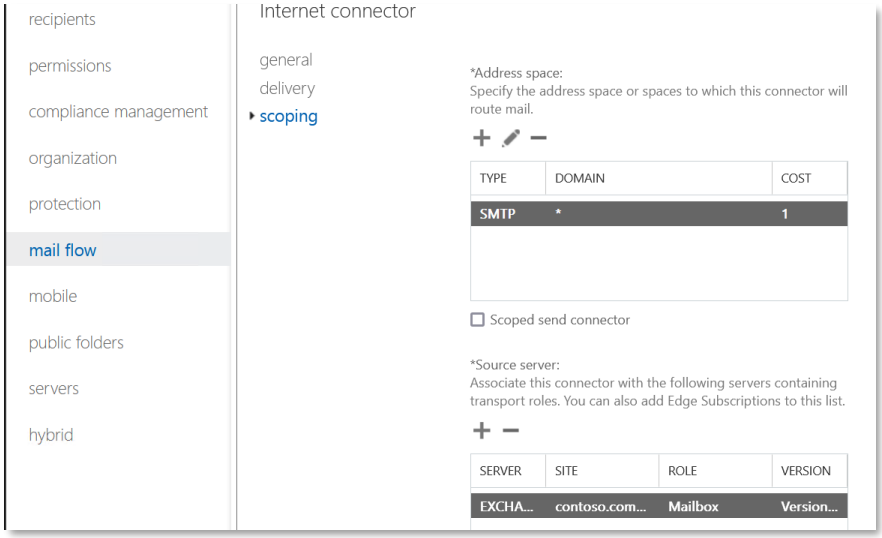


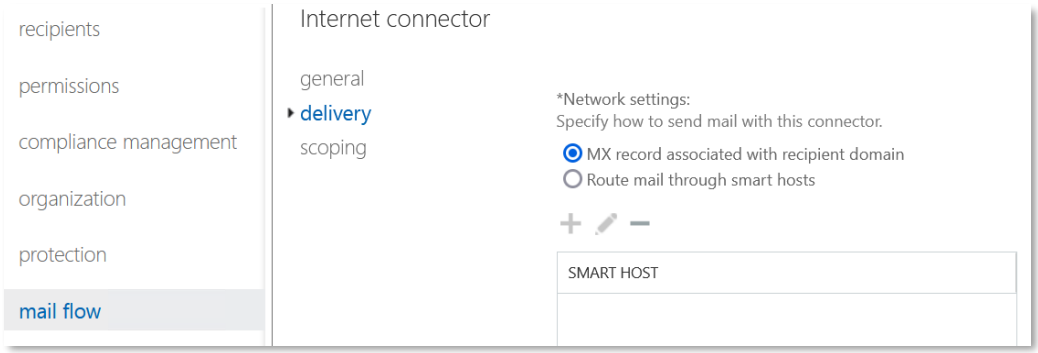
Ensuite, on ajoutera quelques utilisateurs actuels de l'organisation dans cette base de données, créant ainsi des boîtes aux lettres pour chacun d'eux.



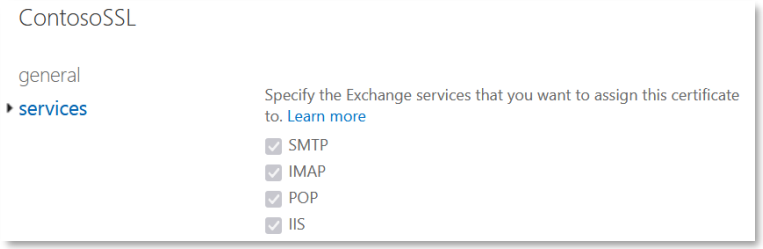
Pour pouvoir envoyer des e-mails vers des adresses Internet, il est nécessaire de configurer la connexion Internet avec **Send Connector.**

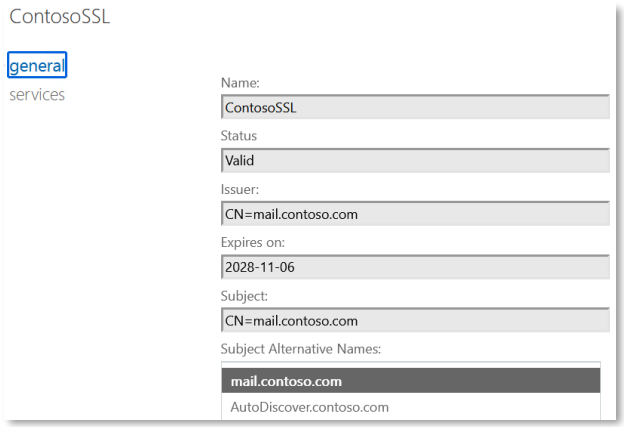




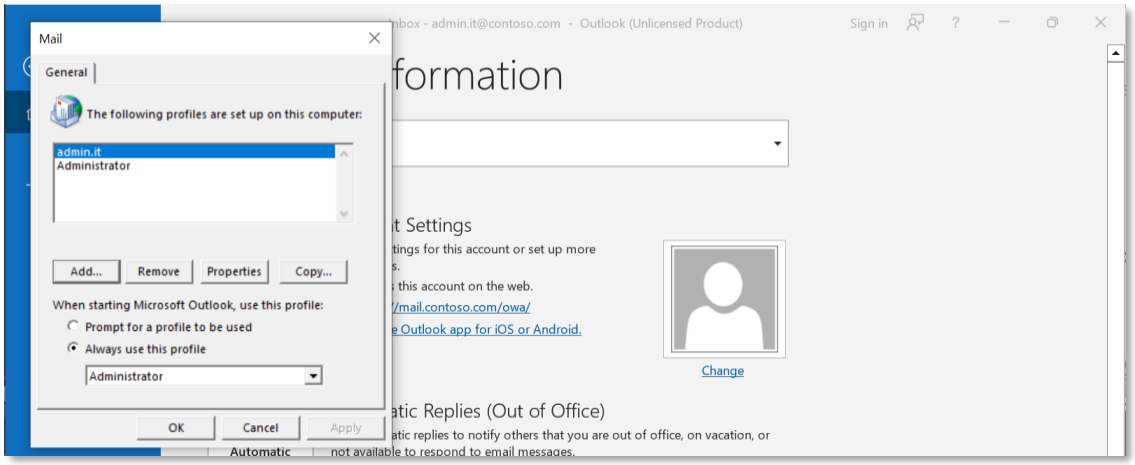


De même, la configuration d'un certificat SSL est également nécessaire.

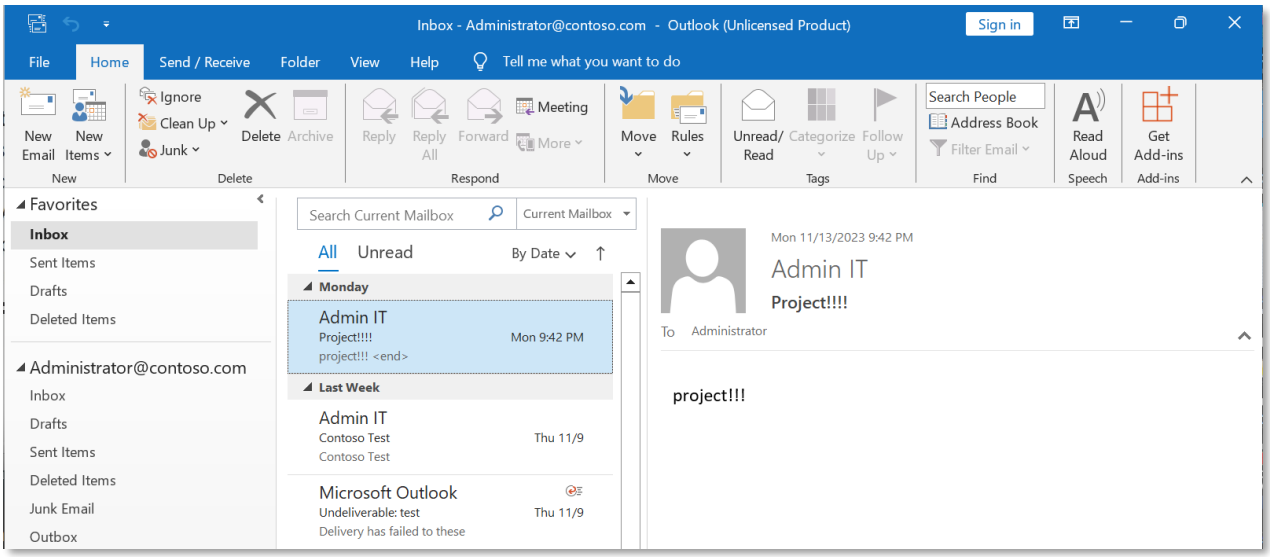




Pour le test, nous allons créer deux profils dans Outlook et envoyer des courriels entre les utilisateurs du domaine, puis à l'extérieur vers gmail.com, yahoo.com et lcieducation.net.



Les courriers soient envoyés et reçus avec succès à l'intérieur du domaine.



Les courriels sont bien envoyés vers Gmail, mais ils sont rejetés en raison de problèmes de sécurité liés à l'enregistrement SPF. Le domaine contoso.com est géré par Microsoft, et notre adresse IP n'est pas autorisée par le DNS public à utiliser le domaine contoso.com. Cela se produit également avec d'autres domaines de destinataires tels que Yahoo ou lcieducation.net.

Problèmes rencontrés, méthodes de dépannage et recommandations.

La principale difficulté survenue a été après la suppression du sous-domaine enfant eu.contoso.com, lorsque j'ai tenté d'installer le serveur Exchange. Des traces cachées du sous-domaine sont demeurées dans la forêt contoso.com, entraînant des erreurs lors du déploiement d'Exchange sur le serveur Server1. La solution a consisté à éliminer toutes les traces du sous-domaine trouvées, en utilisant les commandes cmd et PowerShell.

Une problématique additionnelle était liée au serveur Exchange, plus précisément aux envois vers les boîtes aux lettres sur Internet. Du fait que le domaine contoso.com est sous la gestion de Microsoft et doit être enregistré avec le SPF (Sender Policy Framework) sur un DNS public, cela implique que tout serveur non explicitement autorisé doit traiter le message comme suspect.

En conséquence, les courriers ont été rejetés. Cependant, cela démontre que le serveur Exchange fonctionne correctement.

La solution consiste à utiliser un domaine non utilisé par personne et à l'enregistrer auprès d'un DNS public.

Glossaire de termes techniques.

- ADDT - Active Directory Domains and Trusts, permet de gérer les relations de confiance entre les domaines dans une forêt Active Directory.
- ADUC - Active Directory Users and Computers, console d'administration pour gérer les utilisateurs, les groupes et les ordinateurs dans un environnement Active Directory.
- BIND (Berkeley Internet Name Domain) - serveur DNS (Domain Name System) le plus utilisé sur Internet.
- CUPS - acronyme de "Common Unix Printing System", est une plateforme d'impression open source conçue pour les systèmes d'exploitation Unix, notamment Linux.
- DNS - Domain Name System, convertit les noms de domaine en adresses IP, facilitant la navigation sur Internet.
- FGPP - Fine-Grained Password Policies, permet de définir des règles de mot de passe spécifiques pour des groupes d'utilisateurs dans un environnement Active Directory.
- GPO - Group Policy Object, moyen de définir des paramètres et des politiques pour les utilisateurs et les ordinateurs dans un réseau Windows.
- Microsoft Exchange - plateforme de messagerie et de collaboration. permet la gestion des e-mails, des calendriers, des contacts et d'autres fonctionnalités de communication au sein d'une organisation.
- MMC - Microsoft Management Console, interface centralisée pour administrer divers outils système sur Windows.
- MS-CHAP2 - Microsoft Challenge Handshake Authentication Protocol version 2, protocole d'authentification utilisé pour sécuriser les connexions réseau, souvent utilisé dans les réseaux VPN (Virtual Private Network) et d'autres systèmes d'accès sécurisé.
- NFS - Network File System, protocole qui permet à un ordinateur de partager des fichiers et des répertoires avec d'autres ordinateurs via un réseau. NFS est couramment utilisé dans les environnements Unix et Linux.
- NPS - Network Policy Server, service de rôle dans Windows Server qui effectue l'authentification et l'autorisation des connexions réseau, souvent utilisé avec des protocoles comme RADIUS.

- Quota - limitation de l'utilisation des ressources, généralement appliquée à l'espace disque attribué à un utilisateur ou à un groupe.
- RADIUS - Remote Authentication Dial-In User Service, protocole de gestion d'accès réseau utilisé pour l'authentification, l'autorisation et la gestion des comptes d'utilisateurs.
- Samba - logiciel open source qui permet le partage de fichiers et d'imprimantes entre les systèmes Linux/Unix et Windows. Il favorise l'interopérabilité entre ces environnements.
- Server - un ordinateur ou un logiciel fournissant des services à d'autres ordinateurs dans un réseau.
- SPF - "Sender Policy Framework", et un enregistrement SPF est un type d'enregistrement DNS utilisé pour spécifier quels serveurs sont autorisés à envoyer des courriels au nom d'un domaine particulier.
- Terminal Server, permet à plusieurs utilisateurs d'accéder à des applications ou à un bureau Windows à partir d'un emplacement distant.
- VPN - Virtual Private Network, réseau privé virtuel qui permet à des utilisateurs de se connecter à un réseau sécurisé à partir d'un emplacement distant via Internet.
- WDS - Windows Deployment Services, service de déploiement de Windows qui permet l'installation automatisée du système d'exploitation sur des ordinateurs via le réseau.

Conclusion

À travers ce projet, j'ai appliqué l'ensemble de mes connaissances en administration de serveurs Windows et Linux, réussissant à intégrer différents services essentiels tels qu'Exchange Server, un serveur web basé sur IIS et Apache, ainsi que des serveurs DNS utilisant à la fois la plateforme Windows et BIND sur Linux, etc. Le succès dans la combinaison de l'interconnexion de services sur des plates-formes différentes a été remarquable.

L'infrastructure IT de l'organisation Contoso est riche en technologies et services, offrant une base solide pour une mise en œuvre dans une entreprise de taille petite ou moyenne sans aucun doute.

Cette expérience a été l'occasion d'appliquer mes connaissances dans un environnement pratique, malgré les difficultés rencontrées. J'ai pris conscience que ces défis ont joué un rôle significatif dans mon développement professionnel. Il est essentiel de ne pas ignorer les obstacles, mais de les considérer comme des opportunités de croissance et d'amélioration.

Je crois fermement que l'infrastructure IT réalisée peut être mise en œuvre en toute confiance dans une entreprise réelle de petite ou moyenne taille, voire dans un environnement domestique (SOHO). La poursuite d'une approche proactive et l'apprentissage des difficultés contribueront à l'évolution constante de mes compétences dans le domaine de l'administration de serveurs.

Cette expérience n'a pas seulement été une démonstration de mes compétences, mais aussi une source d'apprentissage continu et de développement personnel. Je suis déterminé à appliquer ces leçons dans des projets futurs et à partager les connaissances acquises pour soutenir la communauté professionnelle dans sa croissance.

27 novembre 2023