



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.

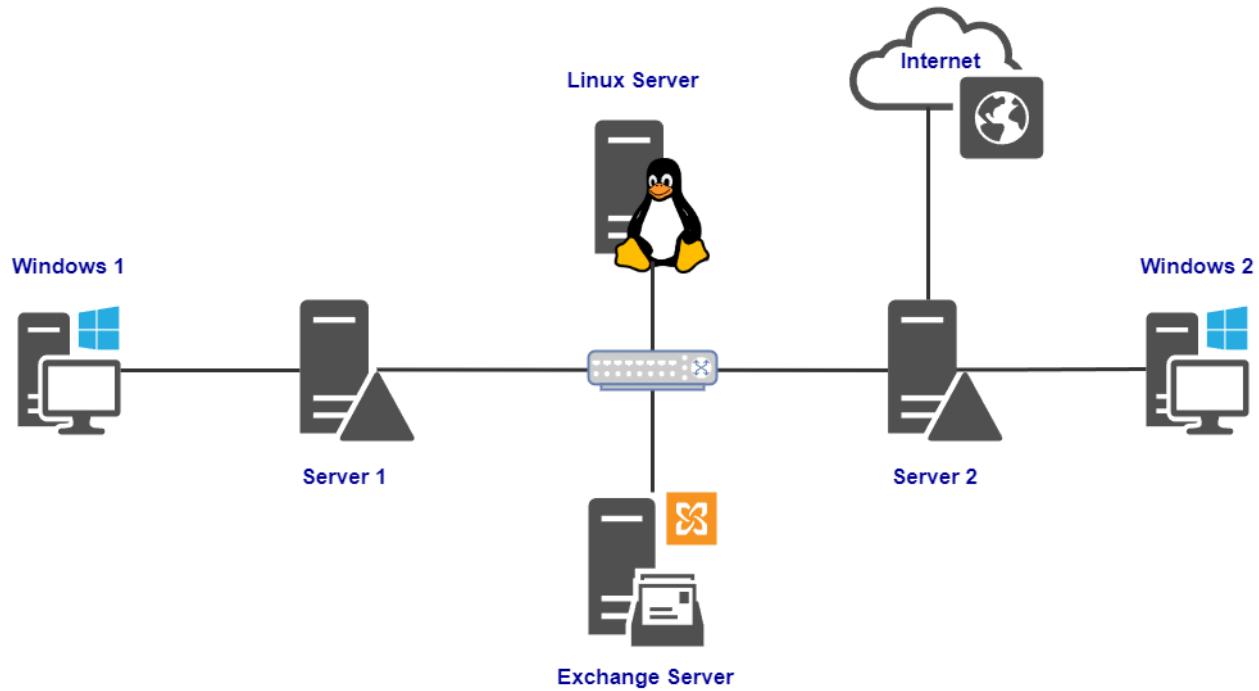
Il y a quatre serveurs dans le réseau, trois basés sur Windows Server 2022, dont l'un est un contrôleur de domaine, un autre est un sous-domaine, le troisième est un serveur Exchange, et un sur Alma Linux 9 (compatible binaire avec RHEL 9 / CentOS 9).

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.

The screenshot shows the 'Hyper-V Manager' window with the title bar 'Hyper-V Manager' and a node 'GC-PC'. On the left, there's a tree view with 'Virtual Machines'. On the right, a table titled 'Virtual Machines' lists seven virtual machines with their names and states:

Name	State
Windows10_WDS	Off
Windows2	Off
Windows1	Off
Server2	Off
Server1	Off
LinuxServer	Off
Exchange	Off

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.

The screenshot shows the 'Virtual Switch Manager for GC-PC' window. On the left, a tree view under 'Virtual Switches' shows several switches: 'New virtual network switch', 'Bridge' (selected), 'LAN1', 'Segment1', 'Segment2', 'Segment3', and 'Default Switch'. On the right, a 'Virtual Switch Properties' dialog is open for 'Segment1'. It has fields for 'Name' (set to 'Segment1') and 'Notes'. Under 'Connection type', it asks 'What do you want to connect this virtual switch to?' with an option 'External network:'.

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 Update
		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

<p>Server1 contoso.com</p> <p>Domain: Off Enabled Enabled Disabled 192.168.1.10 192.168.1.70 Disabled</p>	<p>Control Panel Home</p> <p>Allow an app or feature through Windows Defender Firewall</p> <ul style="list-style-type: none"> 🛡️ Change notification settings 🛡️ Turn Windows Defender Firewall on or off 🛡️ Restore defaults 🛡️ Advanced settings <p>Troubleshoot my network</p>	<p>Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.</p> <p>Update your Firewall settings</p> <p>Windows Defender Firewall is not using the recommended settings to protect your computer.</p> <p>What are the recommended settings?</p> <p>🛡️ Domain networks Connected</p> <p>🛡️ Private networks Not connected</p> <p>🛡️ Guest or public networks Not connected</p>
---	---	---

Server 2

Computer name	Server2	Last installed updates	10/12/2023 5:23 PM
Domain	eu.contoso.com	Windows Update	Download updates only, using Windows
		Last checked for updates	10/12/2023 9:47 PM
Microsoft Defender Firewall	Public: 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)
Segment2	192.168.1.80	Product ID	00455-50000-00001-AA534 (activated)
Segment3	192.168.1.130		

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

Server2
eu.contoso.com

Domain: Off
Enabled
Enabled
Disabled
192.168.1.80
192.168.1.130
Disabled

Control Panel Home

Allow an app or feature through Windows Defender Firewall

- 🛡️ Change notification settings
- 🛡️ Turn Windows Defender Firewall on or off
- 🛡️ Restore defaults
- 🛡️ Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

█ Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

[Use recommended settings](#)

[What are the recommended settings?](#)

█	✖️ Domain networks	Connected (✓)
█	✖️ Private networks	Not connected (✗)
█	✖️ Guest or public networks	Not connected (✗)

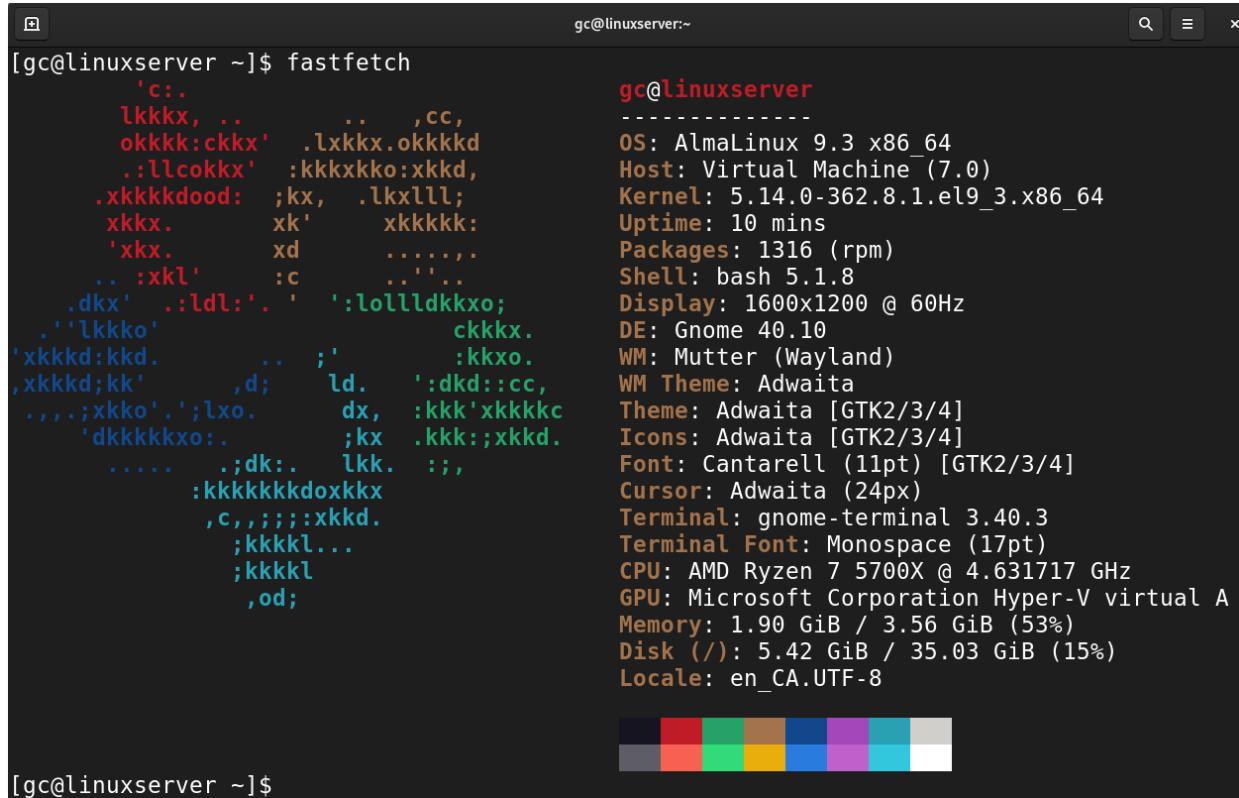
Exchange Server

Computer name	Exchange	Last installed updates	11/18/2023 10:45 PM
Domain	contoso.com	Windows Update	Download updates only, u
		Last checked for updates	Today at 5:21 PM
Microsoft Defender Firewall	Domain: Off	Microsoft Defender Antivirus	Real-Time Protection: Off
Remote management	Disabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC-05:00) Eastern Time (
Ethernet	192.168.1.85	Product ID	00455-50000-00001-AA19

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

Exchange contoso.com Public: Off Enabled Enabled Disabled 192.168.1.85 Disabled	<p>through Windows Defender Firewall</p> <ul style="list-style-type: none"> 🛡️ Change notification settings 🛡️ Turn Windows Defender Firewall on or off 🛡️ Restore defaults 🛡️ Advanced settings Troubleshoot my network 	<p>Update your Firewall settings</p> <p>Windows Defender Firewall is not using the recommended settings to protect your computer.</p> <p>What are the recommended settings?</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">🛡️ X Domain networks</td> <td style="padding: 5px;">Not connected ⓘ</td> </tr> <tr> <td style="padding: 5px;">🛡️ X Private networks</td> <td style="padding: 5px;">Not connected ⓘ</td> </tr> <tr> <td style="padding: 5px;">🛡️ X Guest or public networks</td> <td style="padding: 5px;">Connected ⓘ</td> </tr> </table>	🛡️ X Domain networks	Not connected ⓘ	🛡️ X Private networks	Not connected ⓘ	🛡️ X Guest or public networks	Connected ⓘ
🛡️ X Domain networks	Not connected ⓘ							
🛡️ X Private networks	Not connected ⓘ							
🛡️ X Guest or public networks	Connected ⓘ							

Linux Server



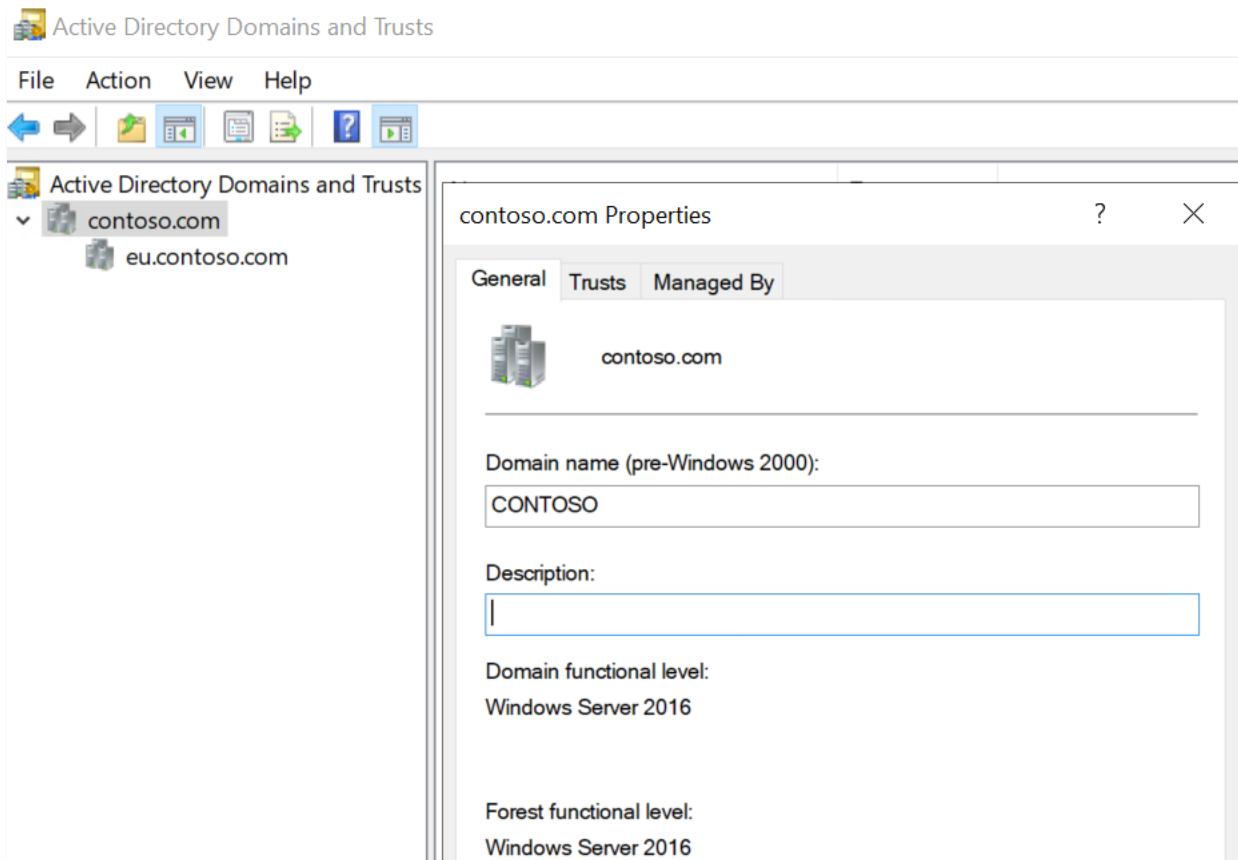
```
[gc@linuxserver ~]$ fastfetch
[c...]
lkxx, .. . ,cc,
okkk:ckkx' .lxkx. okkkd
.:llcokkx' :kkkxkko:xkx
.xkkkdoood: ;kx, .lkxlll;
xkx. xk' xkkkk:
'xkx. xd ..... .
.. :xkl' :c ..... .
.dkx' .:ldl:' . ':lollldkkxo;
.' 'lkkko' ckkx.
'xkkkd:kkd. .; :kxo.
,xkkkd;kk' ,d; ld. ':dkd::cc,
.,.;xkko';'lxo. dx, :kkk'xkkkkc
'dkkkkkxo:. ;kx .kkk:;xkxd.
..... .;dk:. lkk. :;;
:kkkkkkdoxkkx
,c,;:;:xkxd.
;kkkkl...
;kkkl
,od;

[gc@linuxserver ~]$
```

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

The screenshot shows the Windows Server 2012 Routing and Remote Access Management Console. The left pane displays the navigation tree under SERVER1 (local), including Network Interfaces, Ports, Remote Access Logging, IPv4 (with RIP selected), and IPv6. The right pane is titled 'RIP' and contains a table with one row for Segment2. The table columns are Interface, Update mode, Responses sent, and Responses received. The data is as follows:

Interface	Update mode	Responses sent	Responses received
Segment2	Periodic	452	430

The screenshot shows the Windows Server 2012 Routing and Remote Access Management Console. The left pane displays the navigation tree under SERVER1 (local). The right pane is titled 'General' and contains a table with four rows of network interface information. The table columns are Interface, Type, IP Address, Incoming bytes, Outgoing bytes, Static Filters, and Administrative Status. The data is as follows:

Interface	Type	IP Address	Incoming bytes	Outgoing bytes	Static Filters	Administrative Status
Segment2	Dedicated	192.168.1.70	2,412,462	2,242,662	Disabled	Up
Segment1	Dedicated	192.168.1.10	1,253,789	1,479,791	Disabled	Up
Loopback	Loopback	127.0.0.1	0	0	Disabled	Up
Internal	Internal	Not available	-	-	Disabled	Unknown

RIPv2 sur Server2

The screenshot shows the Windows Server 2012 Routing and Remote Access Management Console. The left pane displays the navigation tree under SERVER2 (local), including Network Interfaces, Ports, Remote Access Logging, IPv4 (with RIP selected), and IPv6. The right pane is titled 'RIP' and contains a table with one row for Segment2. The table columns are Interface, Update mode, Responses sent, and Responses received. The data is as follows:

Interface	Update mode	Responses sent	Responses received
Segment2	Periodic	107	106

General						
Interface	Type	IP Address	Incoming bytes	Outgoing bytes	Static Filters	Administrative Status
Segment3	Dedicated	192.168.1.130	29,755	40,089	Disabled	Up
Segment2	Dedicated	192.168.1.80	270,668	303,328	Disabled	Up
Loopback	Loopback	127.0.0.1	0	0	Disabled	Up
Internal	Internal	Not available	-	-	Disabled	Unknown

- 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.

The screenshot shows the Windows Server 2012 DHCP Management Console. On the left, the tree view shows the root node 'DHCP' expanded, followed by 'server1.contoso.com', 'IPv4', and three scopes: 'Scope [192.168.1.0] DHCP_Segment_1', 'Scope [192.168.1.64] DHCP_Segment_2', and 'Scope [192.168.1.128] DHCP_Segment_3'. Each scope node has sub-items for 'Address Pool', 'Address Leases', 'Reservations', 'Scope Options', and 'Policies'. Below the scopes, there are nodes for 'Server Options', 'Policies', and 'Filters'. On the right, a detailed configuration window for 'Scope [192.168.1.0] DHCP_Segment_1 Properties' is open. The 'General' tab is selected, showing the following settings:

Start IP Address	192.168.1.30	End IP Address	192.168.1.62	Description	Address range for di
Scope name:	DHCP_Segment_1				
Start IP address:	192 . 168 . 1 . 30				
End IP address:	192 . 168 . 1 . 62				
Subnet mask:	255 . 255 . 255 . 192		Length: 26		
Lease duration for DHCP clients					
<input checked="" type="radio"/> Limited to: Days: <input type="button" value="1"/> Hours: <input type="button" value="0"/> Minutes: <input type="button" value="0"/>					
<input type="radio"/> Unlimited					
Description: <input type="text"/>					

At the bottom of the window are buttons for 'OK', 'Cancel', and 'Apply'.

Detailed description: This screenshot shows the Windows Server 2012 DHCP console. On the left, the navigation pane shows a tree structure under 'server1.contoso.com' with 'IPv4' selected. Under 'IPv4', 'Scope [192.168.1.0] DHCP_Segment_1' is expanded, showing 'Address Pool', 'Address Leases', 'Reservations', 'Scope Options', and 'Policies'. On the right, a table displays information for a client lease:

Client IP Address	Name	Lease Expiration	Type
192.168.1.40	Windows1.contoso.com	10/22/2023 3:31:22 PM	DHCP

Detailed description: This screenshot shows the Windows Server 2012 DHCP console. On the left, the navigation pane shows a tree structure under 'server1.contoso.com' with 'IPv4' selected. Under 'IPv4', 'Scope [192.168.1.0] DHCP_Segment_1' is expanded, showing 'Address Pool', 'Address Leases', 'Reservations', 'Scope Options', and 'Policies'. On the right, a table displays configuration options for the scope:

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

Detailed description: This screenshot shows the Windows Server 2012 DHCP console. On the left, the navigation pane shows a tree structure under 'server1.contoso.com' with 'IPv4' selected. Under 'IPv4', three scopes are listed: 'Scope [192.168.1.0] DHCP_Segment_1', 'Scope [192.168.1.64] DHCP_Segment_2', and 'Scope [192.168.1.128] DHCP_Segment_3'. Each scope has its own sub-section for 'Address Pool', 'Address Leases', 'Reservations', 'Scope Options', and 'Policies'. On the right, a dialog box titled 'Scope [192.168.1.64] DHCP_Segment_2 Properties' is open, showing the following details:

Start IP Address	End IP Address	Description
192.168.1.90	192.168.1.126	Address range

The dialog also includes tabs for 'General', 'DNS', and 'Advanced'. In the 'General' tab, the 'Scope name:' field is set to 'DHCP_Segment_2'. The 'Start IP address:' is 192.168.1.90 and the 'End IP address:' is 192.168.1.126. The 'Subnet mask:' is 255.255.255.192. The 'Lease duration for DHCP clients' section shows 'Limited to:' with 'Days' set to 1, 'Hours' to 0, and 'Minutes' to 0. There is also an 'Unlimited' option. A 'Description:' field is present at the bottom, and buttons for 'OK', 'Cancel', and 'Apply' are at the bottom right.

Detailed description: This screenshot shows the Windows Server 2012 DHCP management console. On the left, the tree view shows a server named 'server1.contoso.com' under the 'IPv4' node, which contains two scopes: 'DHCP_Segment_1' and 'DHCP_Segment_2'. On the right, a table displays global options for the server:

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

Detailed description: This screenshot shows the Windows Server 2012 DHCP management console. On the left, the tree view shows a server named 'server1.contoso.com' under the 'IPv4' node, which contains three scopes: 'DHCP_Segment_1', 'DHCP_Segment_2', and 'DHCP_Segment_3'. On the right, the properties for 'Scope [192.168.1.128] DHCP_Segment_3' are displayed:

Start IP Address	End IP Address	Description
192.168.1.160	192.168.1.190	Address range

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: **1** Hours: **0** Minutes: **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.

The top screenshot shows the DHCP console for server1.contoso.com. It displays a tree view of scopes, including 'Scope [192.168.1.128] DHCP_Segment_3'. A details pane on the right shows a lease for 'Windows2.contoso.com' with an IP of 192.168.1.160, an expiration date of 10/22/2023 11:34:28 PM, and a type of DHCP.

The bottom screenshot also shows the DHCP console for server1.contoso.com. It highlights the 'Reservations' node under a scope. A details pane on the right lists DNS-related reservations:

Option Name	Vendor	Value
003 Router	Standard	192.168.1.130
006 DNS Servers	Standard	192.168.1.70, 192.168.1.130
015 DNS Domain Name	Standard	contoso.com

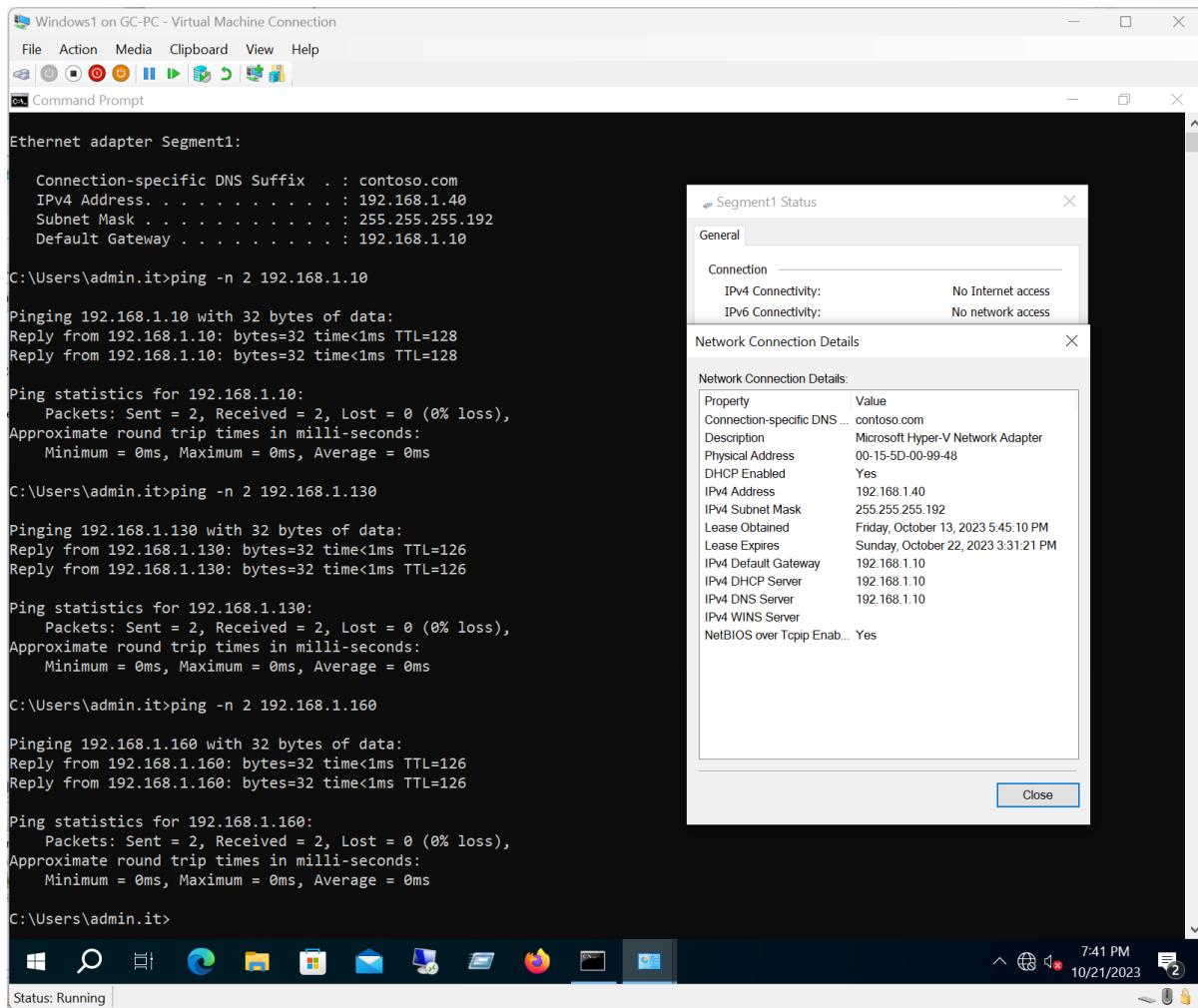
- Agent de relais DHCP

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.

The screenshot shows the 'Routing and Remote Access' management console on SERVER2. Under 'IPv4', the 'DHCP Relay Agent' option is selected. The interface table shows two interfaces: 'Segment3' and 'Segment2', both in 'Enabled' relay mode. The 'DHCP Relay Agent' section of the left navigation pane is highlighted.

Interface	Relay mode	Requests received	Replies received	Requests discarded	Rep
Segment3	Enabled	8	2	6	0
Segment2	Enabled	0	0	0	0

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.



The screenshot shows a Windows Command Prompt window titled "Windows1 on GC-PC - Virtual Machine Connection". The window contains the following text:

```

File Action Media Clipboard View Help
File Open Save Print Copy Paste Find Replace
Command Prompt

Ethernet adapter Segment1:

Connection-specific DNS Suffix . : contoso.com
IPv4 Address . . . . . : 192.168.1.40
Subnet Mask . . . . . : 255.255.255.192
Default Gateway . . . . . : 192.168.1.10

C:\Users\admin.it>ping -n 2 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\admin.it>ping -n 2 192.168.1.130
Pinging 192.168.1.130 with 32 bytes of data:
Reply from 192.168.1.130: bytes=32 time<1ms TTL=126
Reply from 192.168.1.130: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.130:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\admin.it>ping -n 2 192.168.1.160
Pinging 192.168.1.160 with 32 bytes of data:
Reply from 192.168.1.160: bytes=32 time<1ms TTL=126
Reply from 192.168.1.160: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.160:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\admin.it>

```

On the right side of the window, there are two overlapping status windows:

- Segment1 Status** (General tab):

Connection	
IPv4 Connectivity:	No Internet access
IPv6 Connectivity:	No network access
- Network Connection Details** (Network Connection Details tab):

Property	Value
Connection-specific DNS ...	contoso.com
Description	Microsoft Hyper-V Network Adapter
Physical Address	00-15-5D-00-99-48
DHCP Enabled	Yes
IPv4 Address	192.168.1.40
IPv4 Subnet Mask	255.255.255.192
Lease Obtained	Friday, October 13, 2023 5:45:10 PM
Lease Expires	Sunday, October 22, 2023 3:31:21 PM
IPv4 Default Gateway	192.168.1.10
IPv4 DHCP Server	192.168.1.10
IPv4 DNS Server	192.168.1.10
IPv4 WINS Server	
NetBIOS over Tcpip Enab...	Yes

The taskbar at the bottom shows several pinned icons and the system tray indicates the date and time as 7:41 PM on 10/21/2023.

```

Windows2 on GC-PC - Virtual Machine Connection
File Action Media View Help
Command Prompt
Ethernet adapter Segment3:

Connection-specific DNS Suffix . : contoso.com
IPv4 Address . . . . . : 192.168.1.160
Subnet Mask . . . . . : 255.255.255.192
Default Gateway . . . . . : 192.168.1.130

C:\Users\gc>ping -n 2 192.168.1.130

Pinging 192.168.1.130 with 32 bytes of data:
Reply from 192.168.1.130: bytes=32 time<1ms TTL=128
Reply from 192.168.1.130: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.130:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\gc>ping -n 2 192.168.1.70

Pinging 192.168.1.70 with 32 bytes of data:
Reply from 192.168.1.70: bytes=32 time<1ms TTL=127
Reply from 192.168.1.70: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.70:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\gc>ping -n 2 192.168.1.40

Pinging 192.168.1.40 with 32 bytes of data:
Reply from 192.168.1.40: bytes=32 time<1ms TTL=126
Reply from 192.168.1.40: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.40:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\gc>

```

Segment3 Status

Property	Value
Connection-specific DNS ...	contoso.com
Description	Microsoft Hyper-V Network Adapter
Physical Address	00-15-5D-00-99-49
DHCP Enabled	Yes
IPv4 Address	192.168.1.160
IPv4 Subnet Mask	255.255.255.192
Lease Obtained	Friday, October 13, 2023 6:06:32 PM
Lease Expires	Sunday, October 22, 2023 7:24:56 PM
IPv4 Default Gateway	192.168.1.130
IPv4 DHCP Server	192.168.1.70
IPv4 DNS Servers	192.168.1.70 192.168.1.130
IPv4 WINS Server	NetBIOS over Tcpip Enab... Yes

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

The screenshot shows the Windows DNS Management console. On the left, the tree view shows SERVER1 under DNS, with branches for Forward Lookup Zones, Reverse Lookup Zones, Trust Points, and Conditional Forwarders. Under Forward Lookup Zones, there are entries for _msdcs.contoso.com, contoso.com, eucontoso.com, and 1.168.192.in-addrarpa. The contoso.com zone is expanded, showing subzones like _msdcs, _sites, _tcp, _udp, DomainDnsZones, and ForestDnsZones. The properties window for contoso.com is open, showing the General tab with Status: Running, Type: Active Directory-Integrated, and Replication: All DNS servers in this forest. The Zone Transfers tab is selected, showing the Start of Authority (SOA) information: Name Server (NS) server1.contoso.com, Name Server (NS) server2.eu.contoso.com, and Name Server (NS) server1.contoso.com. The Security tab shows Dynamic updates: Secure only.

The left screenshot shows the 'Name Servers' tab of the 'contoso.com Properties' dialog. It lists two servers: server1.contoso.com (IP 192.168.1.70) and server2.eu.contoso.com (IP 192.168.1.80). Buttons for Add..., Edit..., and Remove are at the bottom. A note at the bottom states: "* represents an IP address retrieved as the result of a DNS query and may not represent actual records stored on this server."

The right screenshot shows the 'Zone Transfers' tab of the 'contoso.com Properties' dialog. It has an 'Allow zone transfers:' checkbox checked. Below it are three radio button options: 'To any server', 'Only to servers listed on the Name Servers tab', and 'Only to the following servers'. Under 'Only to the following servers', there is a table with one entry: IP Address 192.168.1.80 and Server FQDN Server2.eu.contoso.com. Buttons for Edit and Notify... are at the bottom.

- Server1 – reverse zone

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[15], server1.contoso.com, ...	static
(same as parent folder)	Name Server (NS)	server2.eu.contoso.com.	static
(same as parent folder)	Name Server (NS)	server1.contoso.com.	static
192.168.1.10	Pointer (PTR)	Server1.contoso.com.	10/21/2023 3:00:00 PM
192.168.1.130	Pointer (PTR)	Server2.eu.contoso.com.	10/12/2023 7:00:00 PM
192.168.1.160	Pointer (PTR)	Windows2.contoso.com.	10/21/2023 7:00:00 PM
192.168.1.120	Pointer (PTR)	Windows1.contoso.com.	10/9/2023 8:00:00 PM
192.168.1.40	Pointer (PTR)	Windows1.contoso.com.	10/21/2023 3:00:00 PM
192.168.1.70	Pointer (PTR)	Server1.contoso.com.	10/21/2023 3:00:00 PM
192.168.1.80	Pointer (PTR)	Server2.eu.contoso.com.	10/21/2023 2:00:00 PM

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

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[92], server1.contoso.com, ...	static
(same as parent folder)	Name Server (NS)	server2.eu.contoso.com.	static
(same as parent folder)	Name Server (NS)	server1.contoso.com.	static
(same as parent folder)	Host (A)	192.168.1.130	10/21/2023 6:00:00 PM
(same as parent folder)	Host (A)	192.168.1.80	10/9/2023 5:00:00 PM
server2	Host (A)	192.168.1.130	static
server2	Host (A)	192.168.1.80	static

- Server2

La zone contoso.com a été transférée vers Server2.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[100], server2.eu.contoso.co...	static
(same as parent folder)	Name Server (NS)	server1.contoso.com.	static
(same as parent folder)	Name Server (NS)	server2.eu.contoso.com.	static
(same as parent folder)	Host (A)	192.168.1.10	10/9/2023 4:00:00 PM
(same as parent folder)	Host (A)	192.168.1.70	10/9/2023 4:00:00 PM
server1	Host (A)	192.168.1.70	static
server1	Host (A)	192.168.1.10	static
Windows1	Host (A)	192.168.1.40	10/12/2023 6:00:00 PM

Server2 – eu.contoso.com zone.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[92] server2.eu.contoso.co...	static
(same as parent folder)	Name Server (NS)	server1.contoso.com.	static
(same as parent folder)	Name Server (NS)	server2.eu.contoso.com.	static
(same as parent folder)	Host (A)	192.168.1.80	10/21/2023 6:00:00 PM
(same as parent folder)	Host (A)	192.168.1.130	10/21/2023 6:00:00 PM
server2	Host (A)	192.168.1.80	static
server2	Host (A)	192.168.1.130	static

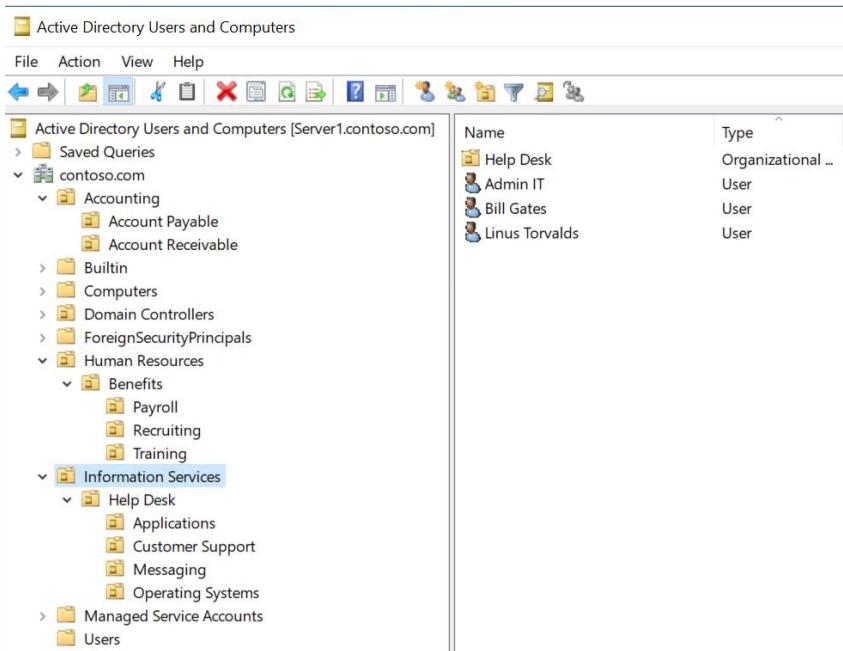
Server2 – reverse zone.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[15] server2.eu.contoso.co...	static
(same as parent folder)	Name Server (NS)	server2.eu.contoso.com.	static
(same as parent folder)	Name Server (NS)	server1.contoso.com.	static
192.168.1.10	Pointer (PTR)	Server1.contoso.com.	10/9/2023 6:00:00 PM
192.168.1.130	Pointer (PTR)	Server2.eu.contoso.com.	10/12/2023 7:00:00 PM
192.168.1.160	Pointer (PTR)	Windows2.contoso.com.	10/21/2023 7:00:00 PM
192.168.1.20	Pointer (PTR)	Windows1.contoso.com.	10/9/2023 8:00:00 PM
192.168.1.40	Pointer (PTR)	Windows1.contoso.com.	10/21/2023 3:00:00 PM
192.168.1.70	Pointer (PTR)	Server1.contoso.com.	10/9/2023 6:00:00 PM
192.168.1.80	Pointer (PTR)	Server2.eu.contoso.com.	10/9/2023 5:00:00 PM

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

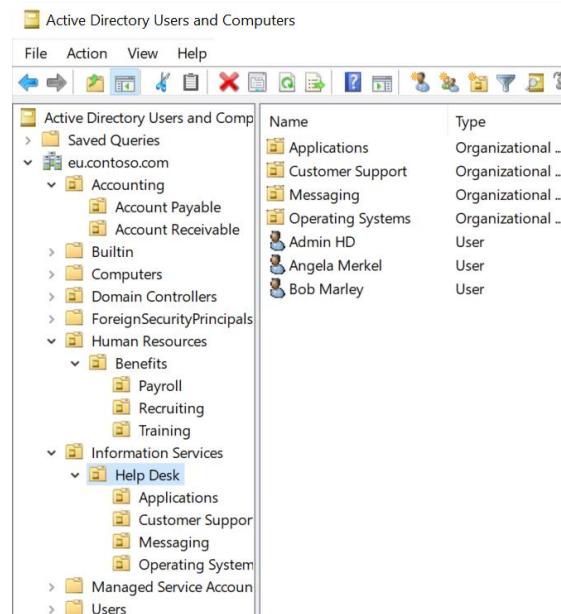
GPO, Active Directory Users and Computers (ADUC)

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:
 @contoso.com

User logon name (pre-Windows 2000):
 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	Description
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:
 @contoso.com

User logon name (pre-Windows 2000):
 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	Description
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.

The image consists of three screenshots from the Active Directory Users and Computers snap-in:

- Screenshot 1: Delegation of Control Wizard - Step 1: Select Users or Groups**
Shows the left pane with the navigation tree and the right pane titled "Delegation of Control Wizard". It lists users under "Selected users and groups": "Admin IT (admin.it@contoso.com)".
- Screenshot 2: Tasks to Delegate**
Shows the left pane with the navigation tree and the right pane titled "Tasks to Delegate". It lists common tasks with checkboxes:
 Create, delete, and manage user accounts
 Reset user passwords and force password change at next logon
 Read all user information
 Create, delete and manage groups
 Modify the membership of a group
 Manage Group Policy links
 Generate Resultant Set of Policy (Planning)
- Screenshot 3: Advanced Security Settings for Information Services**
Shows the left pane with the navigation tree and the right pane titled "Advanced Security Settings for Information Services". It displays permission entries for the "Information Services" object:

Type	Principal	Access	Inherited from	Applies to
Allow	Admin IT (admin.it@contoso.c...)	Create/delete User objects	None	This object and all descendants
Allow	Admin IT (admin.it@contoso.c...)	Full control	None	Descendant User objects
Allow	Account Operators (CONTOSO\...)	Create/delete InetOrgPerson objects	None	This object only

- 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.

Restrict Windows Update

Computer Configuration (Enabled)

Name	Allowed Permissions	Inherited
CONTOSO\Domain Admins	Custom	No

Policies

Administrative Templates

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

System\Group Policy

Policy	Setting	Comment
Configure user Group Policy loopback processing mode	Enabled	Merge

System\Internet Communication Management/ Internet Communication settings

Policy	Setting	Comment
Turn off access to all Windows Update features	Enabled	

Windows Components/Windows Update

Policy	Setting	Comment
Remove access to "Pause updates" feature	Enabled	
Remove access to use all Windows Update features	Enabled	

User Configuration (Enabled)

Policies

Administrative Templates

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

Windows Components/Windows Update

Policy	Setting	Comment
Remove access to use all Windows Update features	Enabled	

Configure notifications: 0 - Do not show any notifications

Windows Update

*Some settings are managed by your organization [\(View policies\)](#)



You're up to date

Last checked: Today, 10:04 PM

[Check for updates](#)

*This option is managed by your organization.

*We'll automatically download and install updates, except on metered connections (where charges may apply). In that case, we'll automatically download only those updates required to keep Windows running smoothly.

Policies set on your device

Disable check for updates by user

Source: Administrator

Type: Group Policy

Download the updates automatically an

Source: Administrator

Type: Group Policy

Set Automatic Update options

Source: Administrator

Type: Group Policy

Disable Pause updates by user

Source: Administrator

Type: Group Policy

- 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.

The screenshot shows the Group Policy Management console. On the left, the navigation pane shows a tree structure under 'Forest: contoso.com' with 'Domains' expanded, showing 'contoso.com' and its subfolders like 'Account_settings', 'Banner', 'Default Domain Policy', etc. A GPO named 'Restrict regedit.exe & wordpad.exe' is selected under 'contoso.com\Default Domain Policy'.

The main pane displays the 'Restrict regedit.exe & wordpad.exe' policy details. It includes sections for 'Trusted Publishers', 'Software Restriction Policies/Security Levels', 'Software Restriction Policies/Additional Rules', 'Hash Rules', 'Path Rules', and 'Administrative Templates'.

Software Restriction Policies/Security Levels:

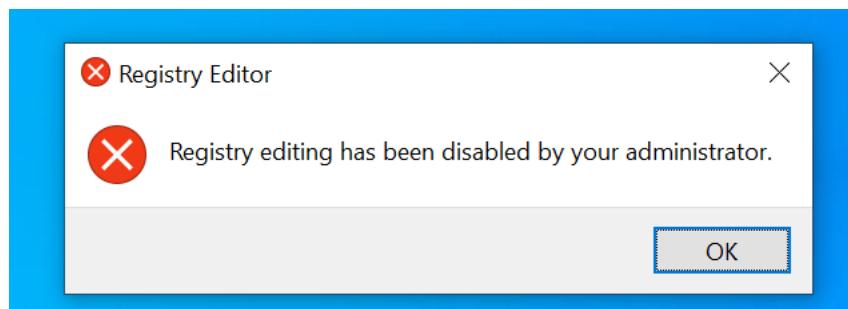
Policy	Setting
Default Security Level	Unrestricted

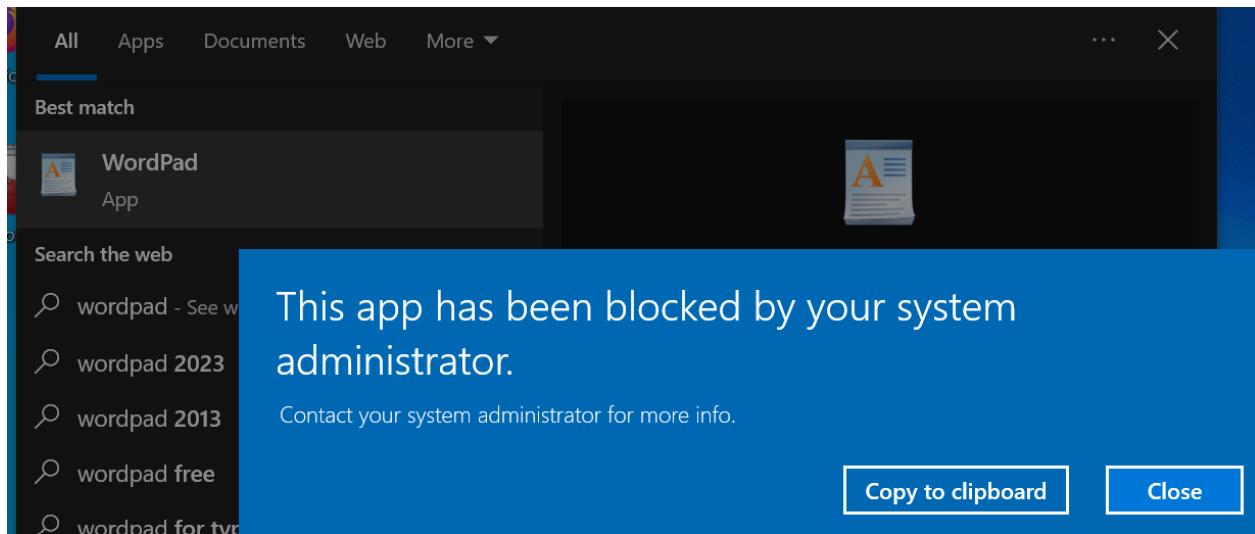
Software Restriction Policies/Additional Rules:

Rule	Description	Date last modified
REGEDIT.EXE (10.0.20348.1); REGEDIT; Registry Editor; Microsoft® Windows® Operating System; Microsoft Corporation	Disallow	10/9/2023 8:44:06 PM
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	Unrestricted	10/9/2023 8:41:48 PM
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	Unrestricted	10/9/2023 8:41:48 PM
C:\Program Files\Windows NT\Accessories\wordpad.exe	Disallow	10/9/2023 9:03:40 PM

Administrative Templates:

Policy	Setting	Comment
Prevent access to registry editing tools	Enabled	Disable regedit from running silently? Yes





- 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.

Policy	Setting
Restrict users to the explicitly permitted list of snap-ins	Enabled

Policy	Setting
Active Directory Domains and Trusts	Enabled
Active Directory Users and Computers	Enabled

MMC_restrict

- Restrict regedit.exe & wordpad.exe
- Restrict Windows Update
- Samba_allow
- Script_samba
- Accounting
- Domain Controllers
- Human Resources
- Information Services
- Microsoft Exchange Security Group
- Radius
- Group Policy Objects
- WMI Filters
- Starter GPOs
- sites
- Group Policy Modeling
- Group Policy Results

LINKS

- Security Filtering
- Delegation
- Computer Configuration (Enabled)
- User Configuration (Enabled)
- Policies
- Administrative Templates
- Windows Components/ Microsoft Management Console

Policy	Setting
Restrict the user from entering author mode	Enabled

Policy Management

contoso.com

- 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
 - Human Resources

MMC_restrict

Scope Details Settings Delegation

These groups and users have the specified permissions:

Groups and users:

Name	Allow	Deny
Authenticated Users	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Domain Admins (CONTOSO\Domain Admins)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enterprise Admins (CONTOSO\Enterprise Admins)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ENTERPRISE DOMAIN CONTROLLERS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
OU_Admins (CONTOSO\OU_Admins)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SYSTEM	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Security

Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- OU_Admins (CONTOSO\OU_Admins)
- Domain Admins (CONTOSO\Domain Admins)

Add... Remove

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]
 - 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 Cont...	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

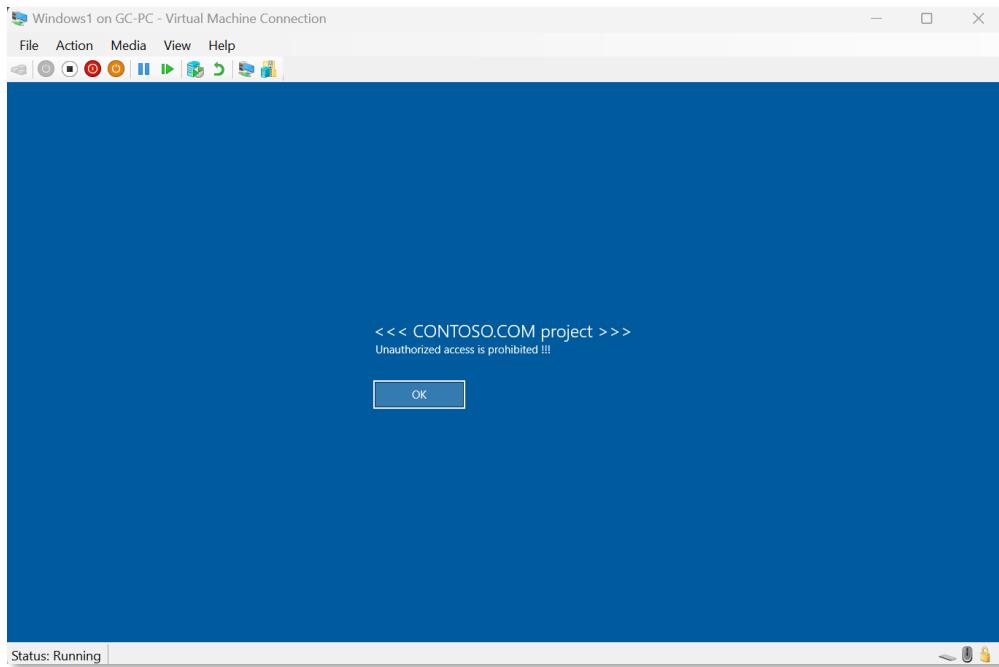
12:22 AM 10/22/2023

- 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.

Policy	Setting
Allow log on locally	CONTOSO\Domain Users, BUILTIN\Administrators
Allow log on through Terminal Services	CONTOSO\Domain Users

- 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.

Policy	Setting
Interactive logon: Message text for users attempting to log on	Unauthorized access is prohibited !!!
Interactive logon: Message title for users attempting to log on	<<< CONTOSO.COM project >>>



- 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)

Policies		
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.

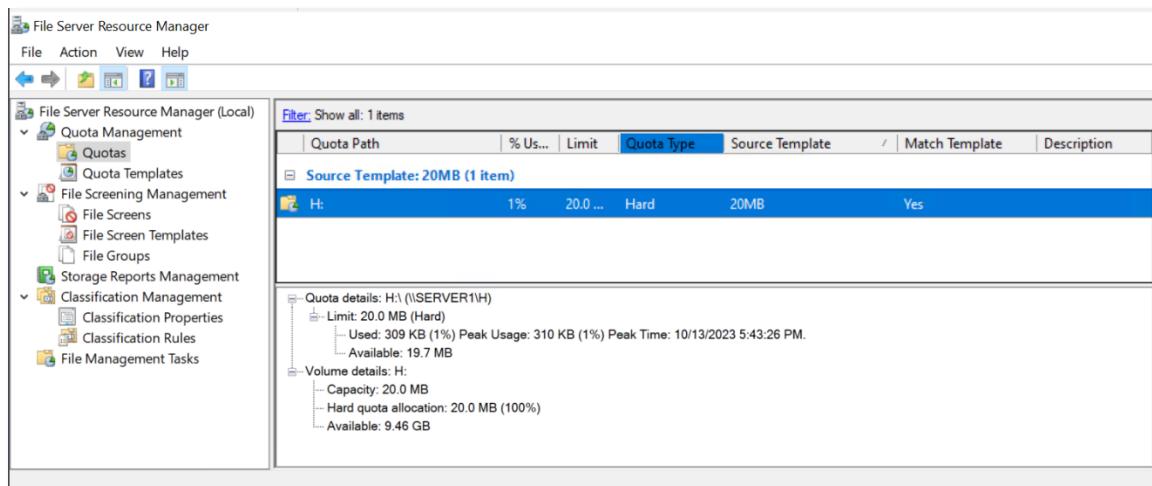
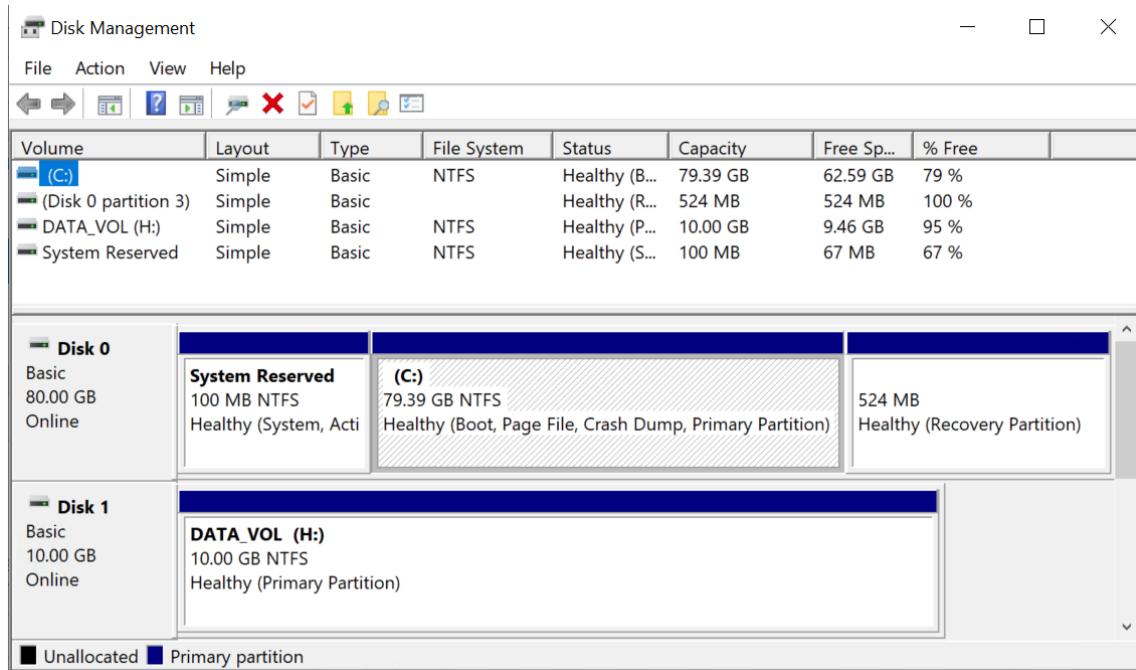
The screenshot shows the 'Administrators' password policy configuration in the Active Directory Administrative Center. The 'Password Settings' tab is selected. Key settings include:

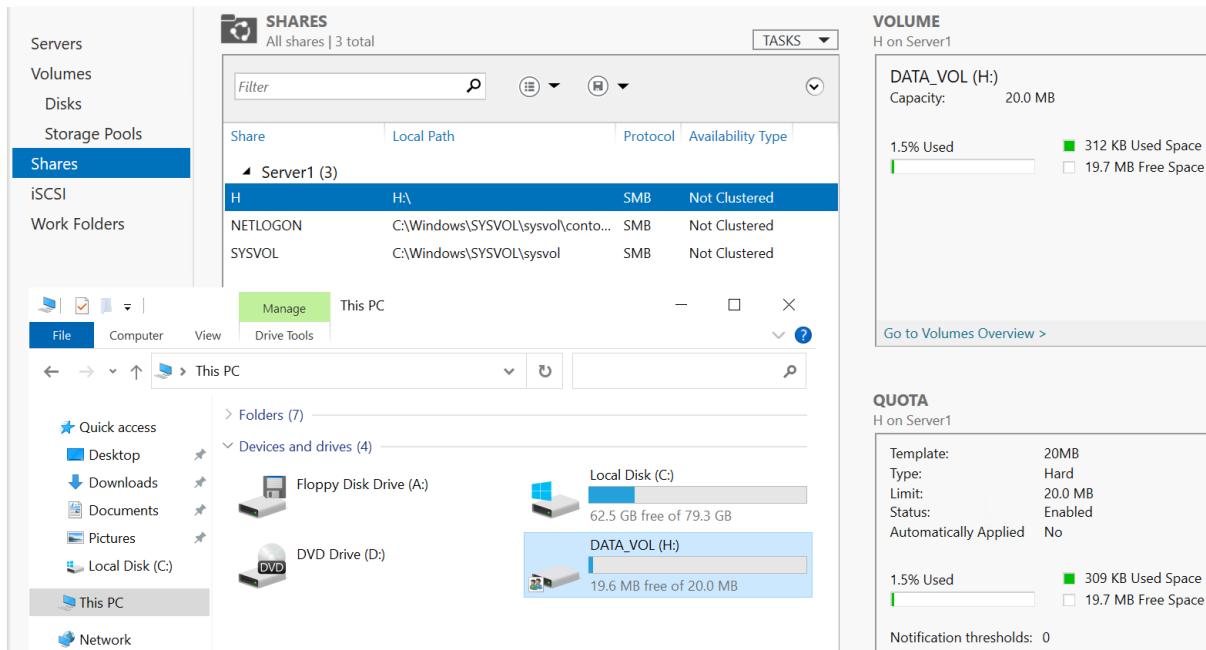
- Name:** Administrators
- Precedence:** 5
- Enforce minimum password length:** Minimum password length (characters): 7
- Enforce password history:** Number of passwords remembered: 24
- Protect from accidental deletion:** Checked
- Password age options:**
 - Enforce minimum password age: User cannot change the password within (days): 1
 - Enforce maximum password age: User must change the password after (days): 42
 - Enforce account lockout policy:
 - Number of failed logon attempts allowed: 5
 - Reset failed logon attempts count after (mins): 5
 - Account will be locked out:
 - For a duration of (mins): 30
 - Until an administrator manually unlocks the account
- Description:** (Empty)

The 'Directly Applies To' section shows the users and groups to which this policy applies, including 'Administrator', 'Domain Admins', and 'OU_Admins'.

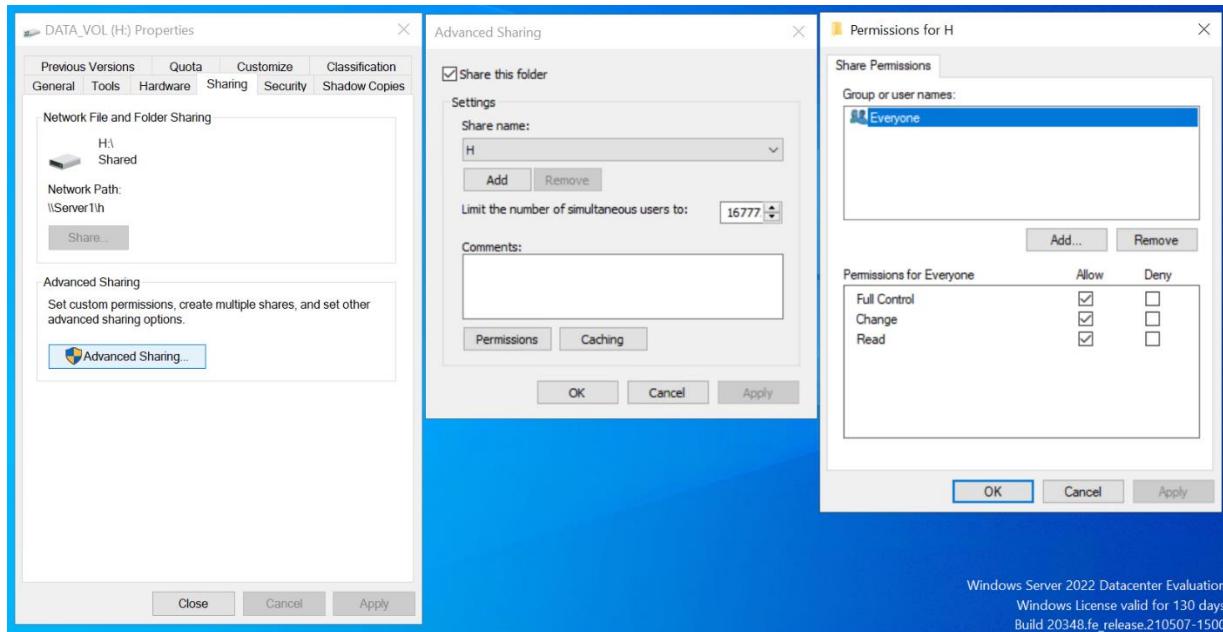
Gestion des quotas

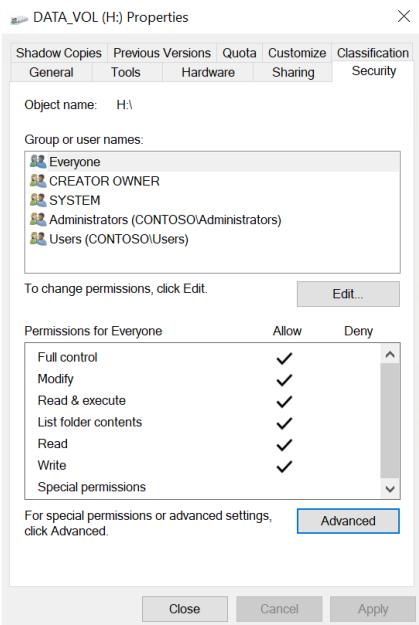
Pour économiser les ressources de stockage sur le serveur, une limite de quota a été appliquée pour tous les utilisateurs. Cette mesure vise à contrôler la quantité de stockage utilisée par chaque utilisateur, assurant ainsi une utilisation efficace des ressources et évitant une utilisation excessive 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.





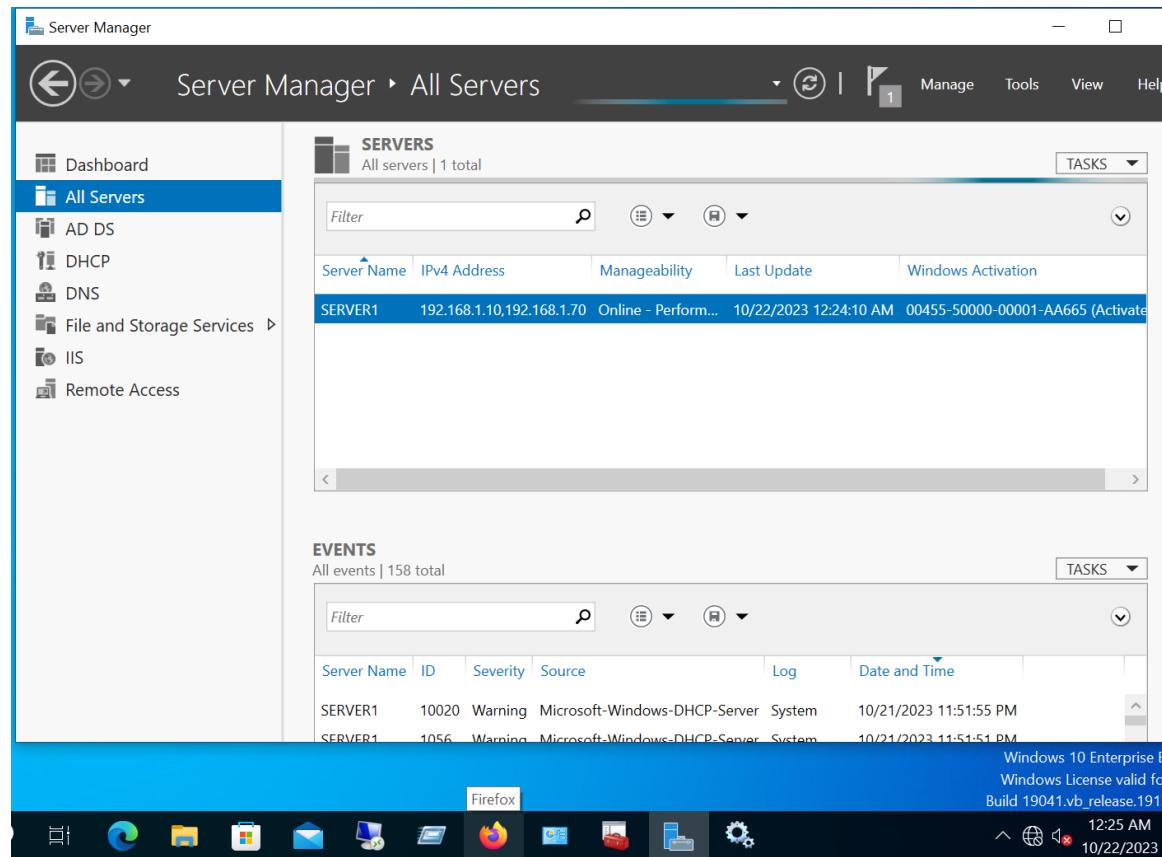
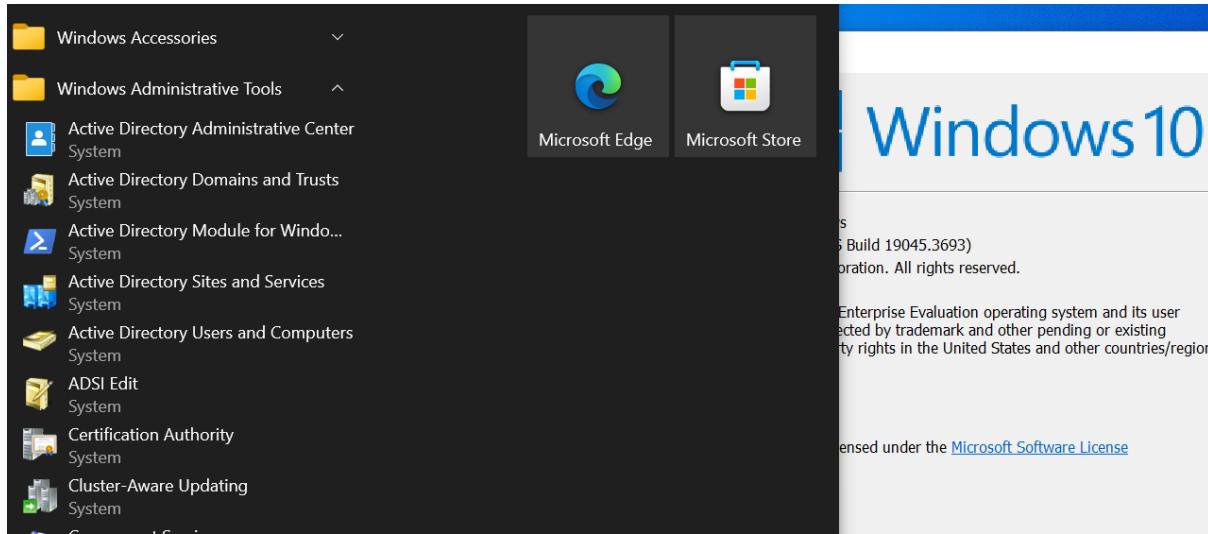
La restriction d'enregistrement du type de fichier .bmp dans le volume H a été mise en place à l'aide de la console Gestionnaire des ressources du serveur de fichiers sur Server1. Cette mesure garantit que les fichiers .bmp ne peuvent pas être sauvegardés dans le volume H, conformément à la politique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

The screenshot shows the 'File Server Resource Manager (Local)' interface. On the left, under 'File Screening Management', there is a tree view with 'File Screens', 'File Screen Templates', and 'File Groups'. A 'File Screen Template' table is displayed on the right:

File screen Template	Screening Type	File Groups
Block Audio and Video Files	Active	Block: Audio and Video Files
Block E-mail Files	Active	Block: E-mail Files
Block Executable Files	Active	Block: Executable Files
Block Image Files	Active	Block: Image Files
bmp restrict	Active	Block:.bmp
Monitor Executable and System Files	Passive	Warn: Executable Files, System Files

A detailed 'File Screen Template Properties for bmp restrict' dialog is open in the foreground. It shows the template name 'bmp restrict' and the screening type 'Active screening: Do not allow users to save unauthorized files'. Under 'File groups', it lists '.bmp' and 'Audio and Video Files' with checkboxes. A 'Create...' button is visible for maintaining file groups.

- 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.



Installation et configuration des services d'infrastructure – deuxième partie

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

The screenshot shows the Windows Server 2012 Routing and Remote Access Management Console. On the left, under 'SERVERN2 (local) > IPv4 > NAT', the 'NAT' icon is selected. On the right, the 'NAT' properties window is open, showing the 'Internet Properties' dialog. Under 'Interface Type', the 'Public interface connected to the Internet' radio button is selected. A checked checkbox 'Enable NAT on this interface' is present, with a note below stating: 'NAT enables clients on this network to send data to and receive data from the Internet using this interface.'

The screenshot shows the same management console. The 'NAT' properties window is open, showing the 'Services and Ports' tab. It displays a list of services to be redirected to the private network: IP Security (IKE), IP Security (IKE NAT Traversal), Post-Office Protocol Version 3 (POP3), Remote Desktop, Secure Web Server (HTTPS), Telnet Server, VPN Gateway (L2TP/IPsec - running on this server), VPN Gateway (PPTP), and Web Server (HTTP). The 'VPN Gateway (L2TP/IPsec - running on this server)' and 'VPN Gateway (PPTP)' checkboxes are checked.

The screenshot shows the 'General' properties table for the Internet interface. The table lists the following interfaces and their details:

Interface	Type	IP Address	Incoming bytes	Outgoing bytes
Segment3	Dedicated	192.168.1.130	0	66,950
Segment2	Dedicated	192.168.1.80	3,703,969	88,931,314
Loopback	Loopback	127.0.0.1	0	0
Internet	Dedicated	172.25.95.198	94,464,598	3,934,701
Internal	Internal	Not available	-	-

- 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.

```
[root@linuxserver gc]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Drop-In: /usr/lib/systemd/system/httpd.service.d
             └─php-fpm.conf
     Active: active (running) since Thu 2023-11-16 21:16:34 EST; 1h 52min ago
       Docs: man:httpd.service(8)
   Main PID: 1007 (httpd)
      Status: "Total requests: 1; Idle/Busy workers 100/0;Requests/sec: 0.000148; Bytes served/sec: 0 B/sec"
         Tasks: 213 (limit: 22962)
        Memory: 28.0M
        CPU: 2.006s
      CGroup: /system.slice/httpd.service
              ├─1007 /usr/sbin/httpd -DFOREGROUND
              ├─1081 /usr/sbin/httpd -DFOREGROUND
              ├─1082 /usr/sbin/httpd -DFOREGROUND
              ├─1083 /usr/sbin/httpd -DFOREGROUND
              └─1084 /usr/sbin/httpd -DFOREGROUND

Nov 16 21:16:34 linuxserver systemd[1]: Starting The Apache HTTP Server...
Nov 16 21:16:34 linuxserver systemd[1]: Started The Apache HTTP Server.
Nov 16 21:16:34 linuxserver httpd[1007]: Server configured, listening on: port 80
[root@linuxserver gc]#
```

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

```
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 80
```



```
# Load config files in the "/etc/httpd/conf.d" directory, if any.
# IncludeOptional conf.d/*.conf
IncludeOptional sites-enabled/*.conf

<Directory /var/www/site3.com/>
  Options Indexes FollowSymlinks
  AllowOverride None
  Require all granted
</Directory>
```

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.recurising";
    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@linuxserver:~# cat /etc/named.conf
/*
 * https://fedoraproject.org/wiki/Changes/CryptoPolicy
 * include "/etc/crypto-policies/back-ends/bind.conf";
};

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; };
};

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";

```

```

## 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";

```

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 -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

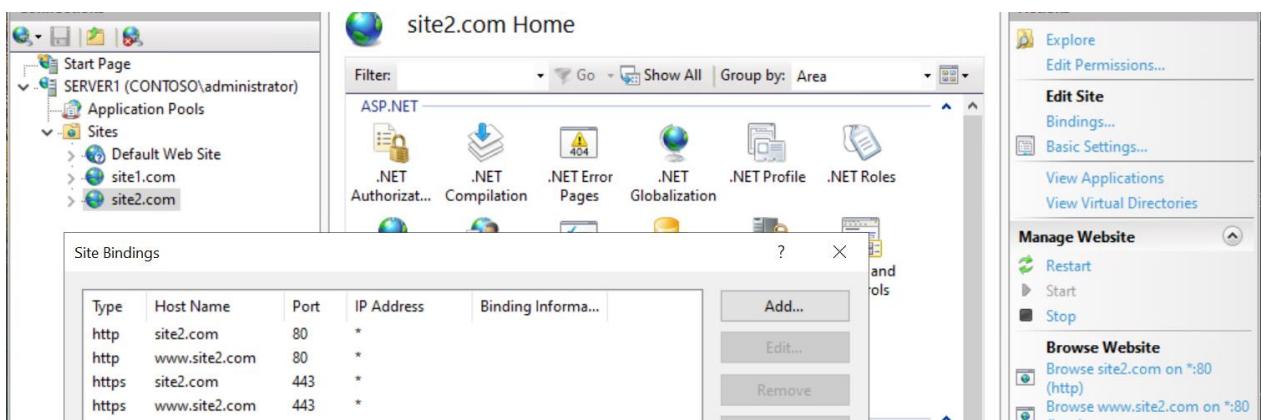
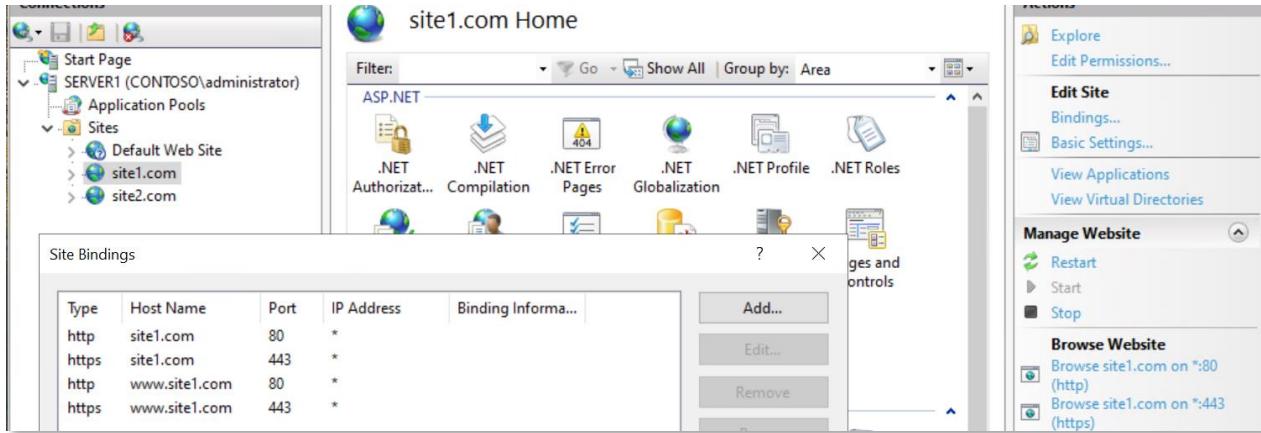
Non-authoritative answer:
Name:   google.com
Address: 172.217.13.110
;; Got recursion not available from 192.168.1.75, trying next server
Name:   google.com
Address: 2607:f8b0:4020:804::200e

[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

The screenshot shows the Windows Server DNS Management console. On the left, the navigation pane displays the DNS tree with SERVER1 selected. Under SERVER1, the Forward Lookup Zones section is expanded, showing zones for _msdcs.contoso.com, autodiscover.contoso.com, contoso.com, mail.contoso.com, server2.contoso.com, site1.com, site2.com, and site3.com. The Reverse Lookup Zones, Trust Points, and Conditional Forwarders sections are also visible. On the right, the details pane shows the properties for the site1.com zone. The General tab is selected, displaying the following information:

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[2023110402], site1.com, site1.com.
(same as parent folder)	Name Server (NS)	site1.com.
(same as parent folder)	Host (A)	192.168.1.70
www	Host (A)	192.168.1.70

The Zone Transfers tab is also visible, showing the zone is a Secondary type. The Master Servers table lists the IP address 192.168.1.75 and the Server FQDN linuxserver.contoso.com.

This screenshot shows the same DNS Management console interface, but the configuration has been changed. The General tab in the site1.com Properties dialog now displays the following information:

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[2023110402], site1.com, site1.com.
(same as parent folder)	Name Server (NS)	site1.com.
(same as parent folder)	Host (A)	192.168.1.70
www	Host (A)	192.168.1.70

The Zone Transfers tab is still present, showing the zone is a Secondary type. The Master Servers table is empty, indicating no master servers have been added yet. A message at the bottom of the General tab states: "To add name servers to the list, click Add."

Site2.com - hébergé sur le Server1

Screenshot of the Windows Server DNS Manager showing the configuration for the site2.com zone.

Forward Lookup Zones:

- _msdcs.contoso.com
- autodiscover.contoso.com
- contoso.com
- mail.contoso.com
- server2.contoso.com
- site1.com
- site2.com** (selected)
- site3.com

Zone Table:

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[2023110402], site2.com., site2.com.
(same as parent folder)	Name Server (NS)	site2.com.
(same as parent folder)	Host (A)	192.168.1.70
www	Host (A)	192.168.1.70

site2.com Properties:

- General Tab:** Status: Running, Type: Secondary, Replication: Not an Active Directory-integrated zone.
- Start of Authority (SOA) Tab:** Zone file name: site2.com.dns, Master Servers: IP Address 192.168.1.75, Server FQDN linuxserver.contoso.com.

Screenshot of the Windows Server DNS Manager showing the configuration for the site2.com zone.

Forward Lookup Zones:

- _msdcs.contoso.com
- autodiscover.contoso.com
- contoso.com
- mail.contoso.com
- server2.contoso.com
- site1.com
- site2.com** (selected)
- site3.com

Zone Table:

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[2023110402], site2.com., site2.com.
(same as parent folder)	Name Server (NS)	site2.com.
(same as parent folder)	Host (A)	192.168.1.70
www	Host (A)	192.168.1.70

site2.com Properties:

- General Tab:** To add name servers to the list, click Add.
- Name servers:** Server Fully Qualified Domain Name (FQDN): site2.com., IP Address: [192.168.1.70].

Site3.com - hébergé sur Linuxserver

Screenshot of the Windows Server DNS Manager showing the configuration for the site3.com zone.

Left pane (DNS View):

- SERVER1
 - Forward Lookup Zones
 - _msdcs.contoso.com
 - autodiscover.contoso.com
 - contoso.com
 - mail.contoso.com
 - server2.contoso.com
 - site1.com
 - site2.com
 - site3.com
 - Reverse Lookup Zones
 - Trust Points
 - Conditional Forwarders

Right pane (site3.com Properties):

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[2023110205], site3.com., site3.com.
(same as parent folder)	Name Server (NS)	site3.com.
(same as parent folder)	Host (A)	192.168.1.75
www	Host (A)	192.168.1.75

General Tab:

- Status: Running
- Type: Secondary
- Replication: Not an Active Directory-integrated zone

Start of Authority (SOA) Tab:

- Zone file name: site3.com.dns
- Master Servers:

IP Address	Server FQDN
192.168.1.75	linuxserver.contoso.com

Screenshot of the Windows Server DNS Manager showing the configuration for the site3.com zone.

Left pane (DNS View):

- SERVER1
 - Forward Lookup Zones
 - _msdcs.contoso.com
 - autodiscover.contoso.com
 - contoso.com
 - mail.contoso.com
 - server2.contoso.com
 - site1.com
 - site2.com
 - site3.com
 - Reverse Lookup Zones
 - Trust Points
 - Conditional Forwarders

Right pane (site3.com Properties):

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[2023110205], site3.com., site3.com.
(same as parent folder)	Name Server (NS)	site3.com.
(same as parent folder)	Host (A)	192.168.1.75
www	Host (A)	192.168.1.75

General Tab:

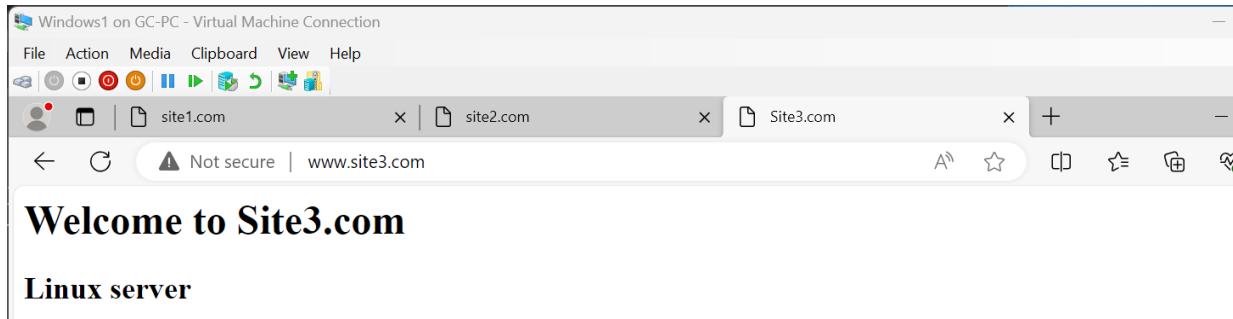
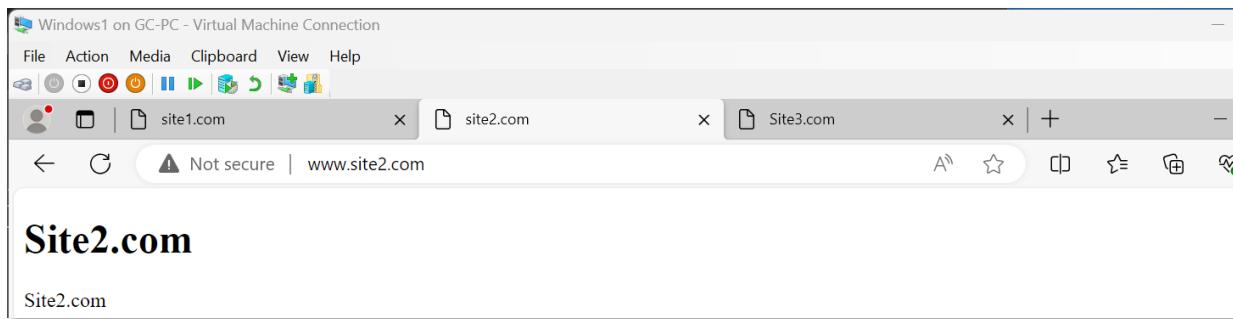
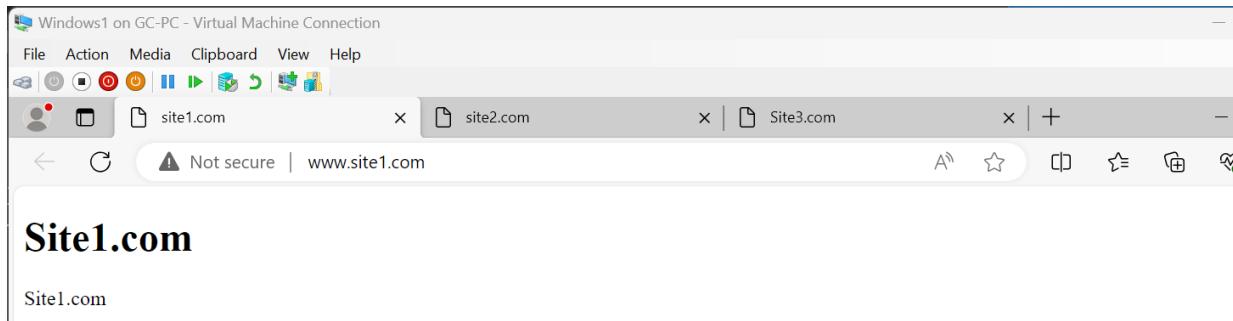
To add name servers to the list, click Add.

Name servers:

Server Fully Qualified Domain Name (FQDN)	IP Address
site3.com.	[192.168.1.75]

- 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: on)
  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		
drwxr-xr-x.	203	root	root	9 Nov 16 21:16		proc		

- Le fichier de configuration - /etc/exports

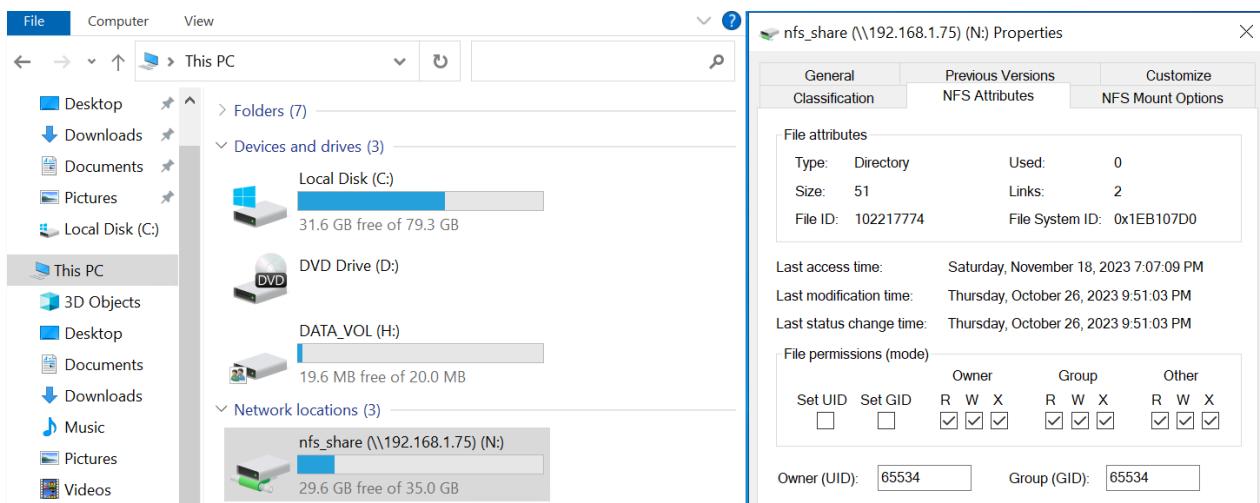
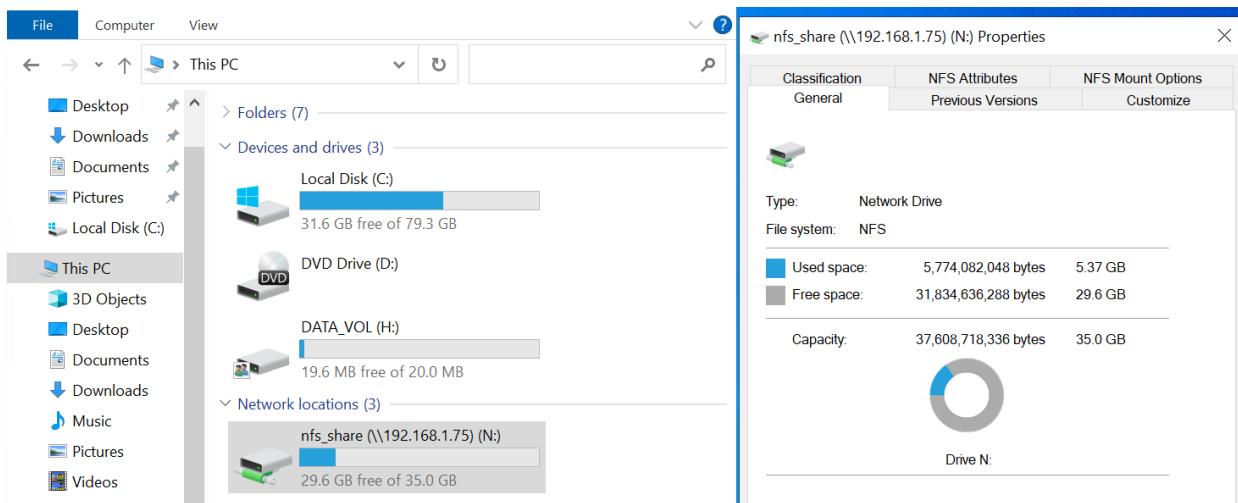
```
root@linuxserver:/home/gc
/nfs_share 192.168.1.0/24(rw, sync, no_subtree_check, no_root_squash)
```

- 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.

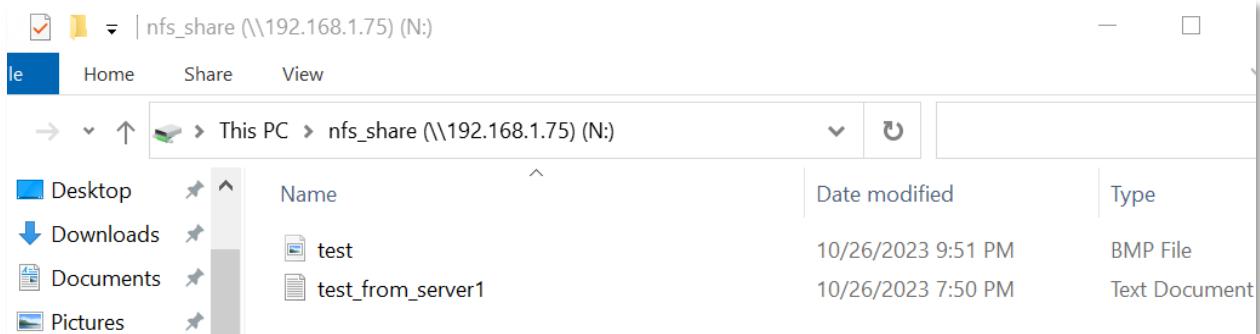
- Le fichier - /etc/idmapd.conf, ou le domaine contoso.com est autorisé d'avoir accès au serveur NFS.

```
[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: disabled)
  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 = tdbSAMBA
  #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
  browsable = No
  read only = No
  inherit acls = Yes

[printers]
  comment = All printers
  path = /var/tmp
  printable = yes
  create mask = 0700
  browsable = 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
  browsable = 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

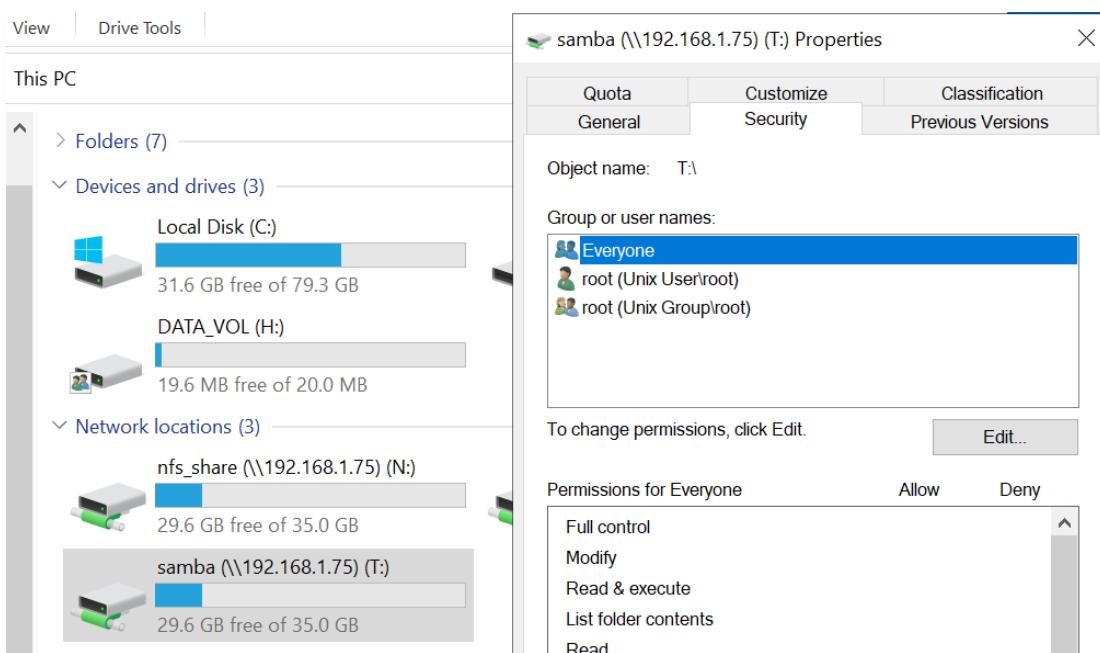
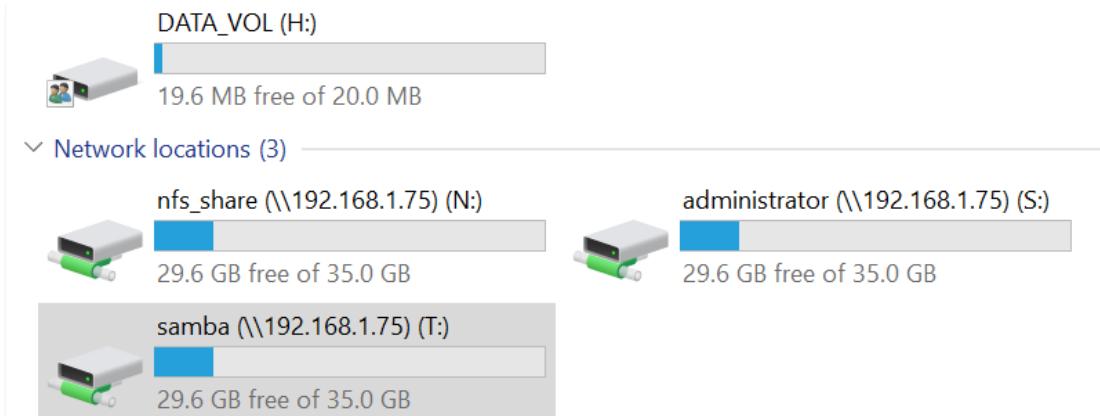
~
```

/etc/samba/smb.conf

- Le répertoire partagé samba_share

```
drwxr-xr-x 48 root root 1380 Nov 16 21:54 run
drwxrwxrwx. 3 root root 106 Nov 13 13:46 samba_share
lrwxrwxrwx. 1 root root 8 Mar 25 2022 sbin -> /usr/sbin
```

- 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.

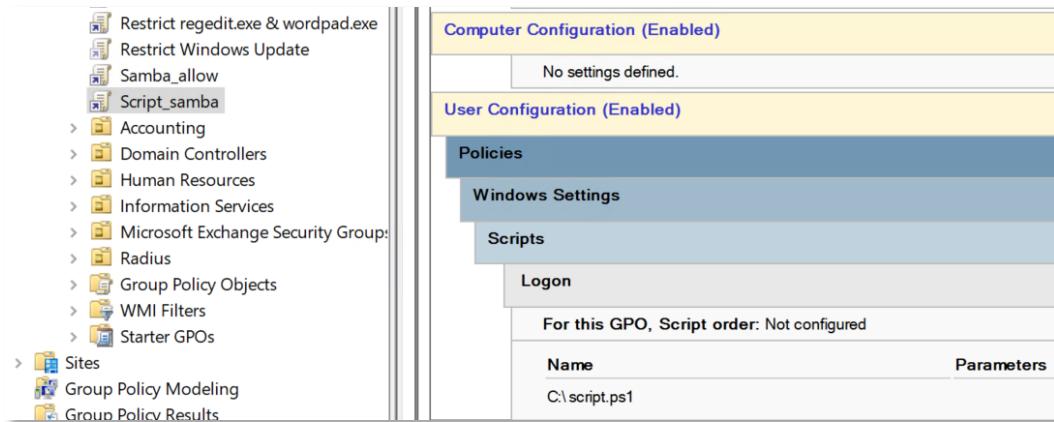
The screenshot shows a Windows File Explorer window with the path 'samba (\\"192.168.1.75) (T:)'. Inside, there's a folder 'homes' and three files: 'New Rich Text Document.rtf', 'New Text Document.txt', and 'samba_sample'. A context menu is open over 'samba_sample', and a properties dialog box is displayed for it. The properties show:

Property	Value
Name	samba_sample.txt
Type	Text Document
Folder path	T:\
Size	0 bytes
Date created	10/27/2023 11:14 PM
Date modified	10/27/2023 11:14 PM
Attributes	A
Owner	LINUXSERVER\nobody
Computer	192.168.1.75

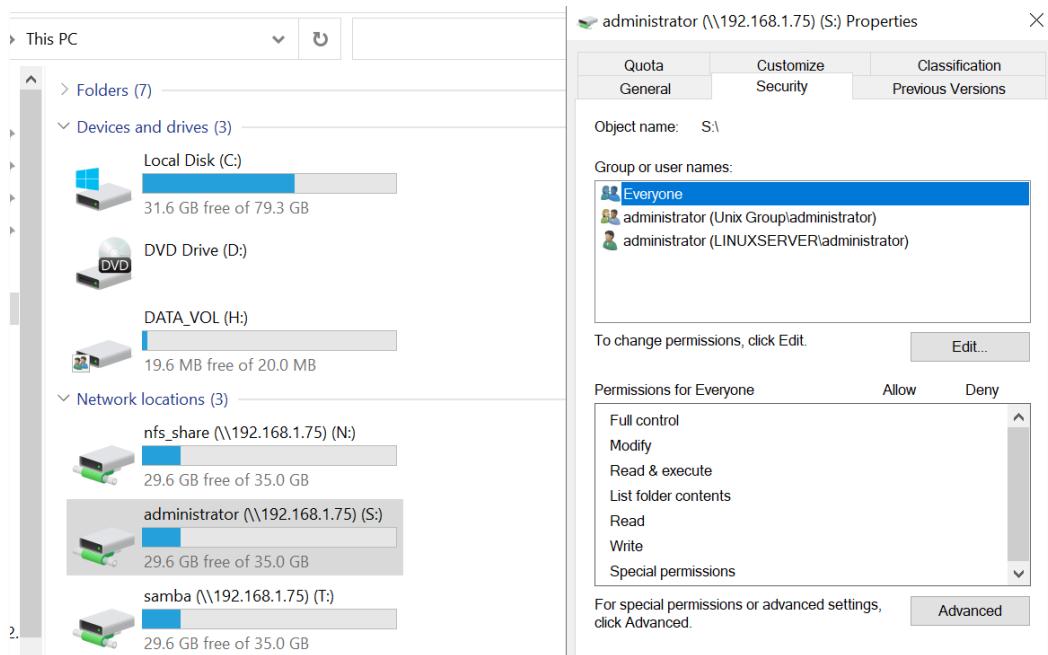

```
[root@linuxserver gc]# ls -l /samba_share/
total 4
drwxrwxrwx  2 administrator administrator 6 Nov 13 13:46 homes
-rwxrwxrwx  1 administrator administrator 7 Nov  2 19:35 'New Rich Text Document.rtf'
-rwxrwxr-x  1 nobody      nobody          0 Oct 30 18:24 'New Text Document.txt'
-rwxrwxr-x  1 nobody      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
1 $SambaServer = "\\"192.168.1.75" ## Linux Server
2 $UserName = $env:USERNAME
3 $DriveLetter = "S"
4 $homeDirectory = Join-Path $SambaServer $UserName
5 if (Get-PSDrive -Name $DriveLetter -ErrorAction SilentlyContinue) {
6     Remove-PSDrive -Name $DriveLetter -Force
7 }
8 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.

The screenshot shows a web browser window titled "Printers - CUPS 2.3.0p2". The URL is "localhost:631/printers/". The page has a header with links to "CUPS.org", "Home", "Administration", "Classes", "Help", "Jobs", and "Printers". Below the header, there is a search bar with the placeholder "Search in Printers:" and buttons for "Search" and "Clear". A message says "Showing 4 of 4 printers." A table lists four printers:

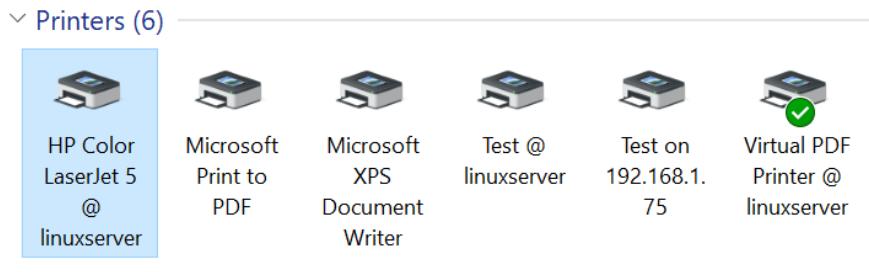
Queue Name	Description	Location	Make and Model	Status
Cups-PDF	Cups-PDF		Generic CUPS-PDF Printer (no options)	Idle
HP_Color_LaserJet_5	HP Color LaserJet 5	Accounting	HP Color LaserJet 5 - CUPS+Gutenprint v5.3.4	Idle
Test	Test	test_hall	HP DesignJet 700 - CUPS+Gutenprint v5.3.4	Idle
Virtual_PDF_Printer	Virtual PDF Printer	LinuxServer	HP Color LaserJet 5 - CUPS+Gutenprint v5.3.4	Idle

The screenshot shows a web browser window titled "localhost:631/printers/HP_Color_LaserJet_5". The URL is "localhost:631/printers/HP_Color_LaserJet_5". The page has a header with links to "CUPS.org", "Home", "Administration", "Classes", "Help", "Jobs", and "Printers". Below the header, the title is "HP_Color_LaserJet_5" and the subtitle is "HP_Color_LaserJet_5 (Idle, Accepting Jobs, Shared, Server Default)". There are dropdown menus for "Maintenance" and "Administration". The printer details are listed:

- Description:** HP Color LaserJet 5
- Location:** Accounting
- Driver:** HP Color LaserJet 5 - CUPS+Gutenprint v5.3.4 (color, 2-sided printing)
- Connection:** cups-pdf:/
- Defaults:** job-sheets=none, none media=na_letter_8.5x11in sides=one-sided

The screenshot shows the AlmaLinux desktop environment. On the left, there is a sidebar with "Home", a search bar, "Devices", "Bluetooth & other devices", "Printers & scanners", "Mouse", and "Typing". On the right, under "Printers & scanners", there is a section titled "Printers & scanners" with a plus icon and the text "Add a printer or scanner". Below it is another section titled "Printers & scanners" with icons for "HP Color LaserJet 5 @ linuxserver" and "Microsoft Print to PDF".

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.

NPS (Local)

- RADIUS Clients and Servers
 - RADIUS Clients
 - Remote RADIUS Server Groups
- Policies
 - Connection Request Policies
 - Network Policies
- Accounting
- Templates Management

Connection Request Policies

Connection request policies	
Policy Name	
Contoso VPN	<input checked="" type="checkbox"/> Use Windows authentication for a...

Conditions - If the following condition is met:

Condition	Value
NAS Port Type	Virtual (VPN)

Contoso VPN Properties

Overview Conditions Settings

Policy name: **Contoso VPN**

Policy State

If enabled, NPS evaluates this policy while processing connection requests.

Policy enabled

Network connection method

Select the type of network access server that sends the connection request. If your network access server is either Vendor specific, or neither is required. If your network access server is either Vendor specific, or neither is required.

Type of network access server:
Remote Access Server(VPN-Dial up)

Vendor specific:
10

Connection Request Policies

- Connection request policies

Policy Name

- Contoso VPN
- Microsoft Routing and Remote Access
- 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 uses this policy. If conditions do not match the connection request, NPS skips this policy and evaluates other policies.

Condition	Value
NAS Port Type	Virtual (VPN)

NPS (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 Router
- Connections to other access...

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 connection request, NPS grants or denies access. [What is access permission?](#)

Grant access. Grant access if the connection request matches this condition.

Deny access. Deny access if the connection request matches this condition.

Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network policy only, do not evaluate the dial-in properties of the user account.

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Virtual (VPN)
Windows Groups	CONTOSO\VPN

Settings - Then the following settings are applied:

Setting
Ignore User Dial-In Properties
Access Permission
Extensible Authentication Protocol
Authentication Method

Network connection method

Select the type of network access server that sends the connection request. If neither is selected, the connection request is rejected.

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

Condition	Value
NAS Port Type	Virtual (V)
Windows Groups	CONTOSO

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**.

Name	Type	Description
radiususer	User	
testuser	User	
VPN_RADIUS_Access	Security Group ...	

Contoso VPN Properties

Overview Conditions Constraints Settings

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authenticate the request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
NAS Port Type	Virtual (VPN)
Windows Groups	CONTOSO\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

ROUTING AND REMOTE ACCESS

Enable this computer as a:

IPv4 Router
 Local area network (LAN) routing only
 LAN and demand-dial routing

IPv6 Router
 Local area network (LAN) routing
 LAN and demand-dial routing

IPv4 Remote access server
 IPv6 Remote access server

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 servers have been configured. The server with the lowest score is selected.

Server
192.168.1.70

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 methods in 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

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 servers have been configured. The server with the lowest score is selected.

Server
192.168.1.70

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...

Edit IPv4 Address Range

Type a starting IP address and either an ending IP address or a number of addresses in the range.

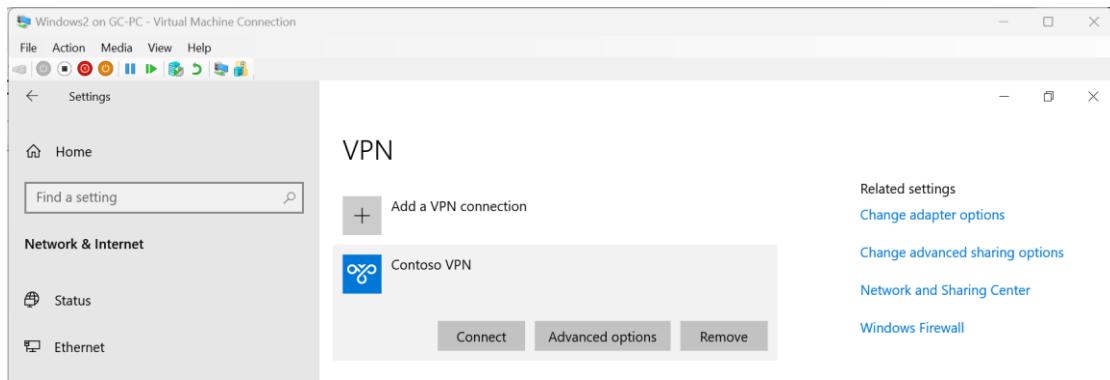
Start IP address: 192.168.1.111

End IP address: 192.168.1.126

Number of addresses: 16

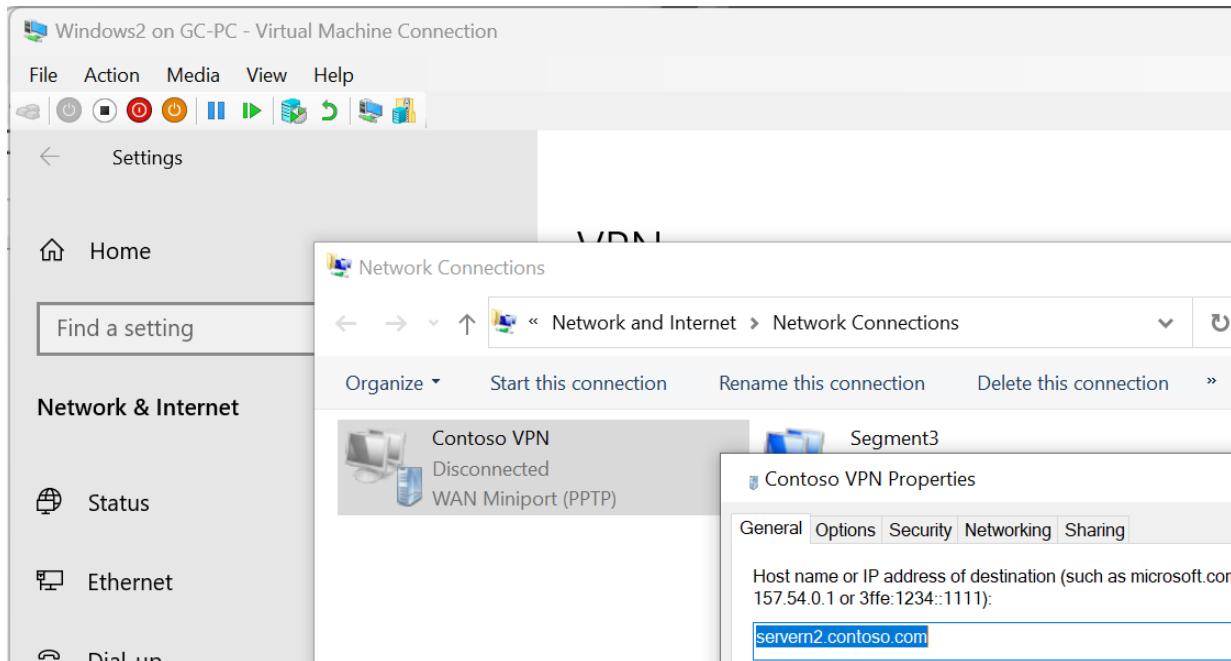
OK

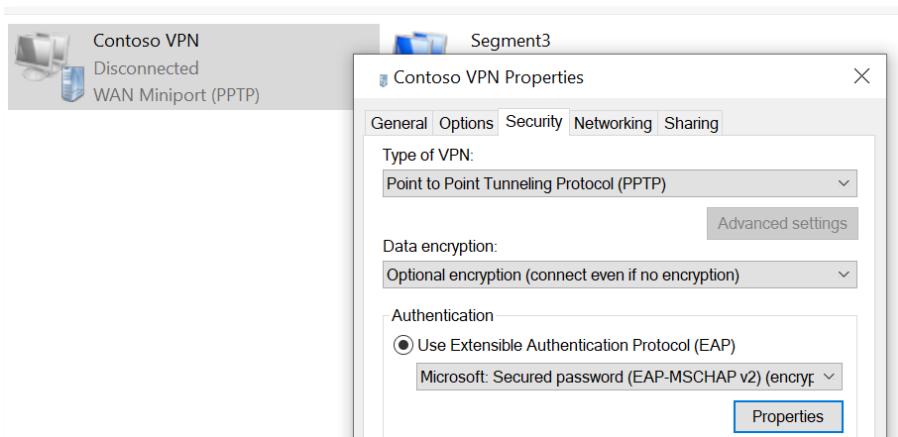
- Ensuite, on configure le client VPN dans le troisième segment du réseau, par exemple.



Connection name	Contoso VPN
Server name or address	servern2.contoso.com
Type of sign-in info	User name and password
User name (optional)	radiususer
Password (optional)	*****

Edit



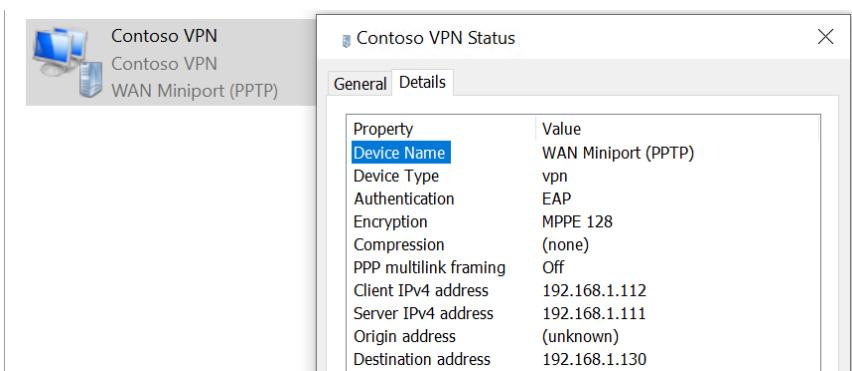


La configuration est en PPTP (Point-to-Point Tunneling Protocol) avec MS-CHAP2 comme méthode d'authentification.

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

Property	Value
Device Name	WAN Miniport (PPTP)
Device Type	vpn
Authentication	EAP
Encryption	MPPE 128
Compression	(none)
PPP multilink framing	Off
Client IPv4 address	192.168.1.112
Server IPv4 address	192.168.1.111
Origin address	(unknown)
Destination address	192.168.1.130

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.

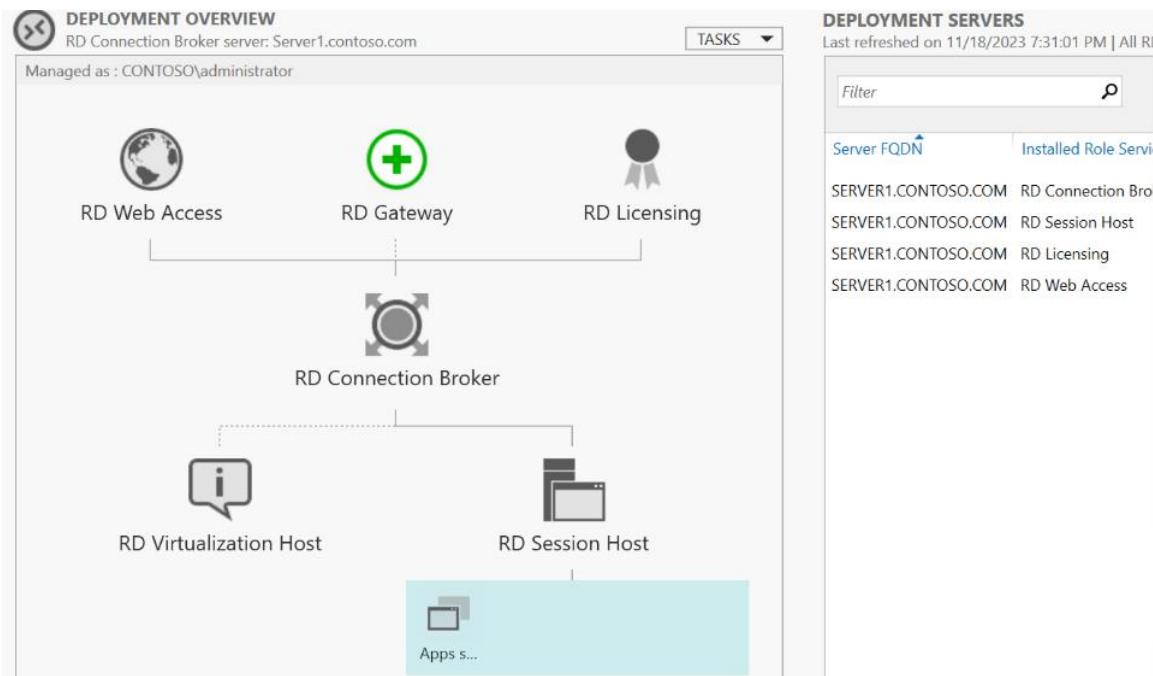


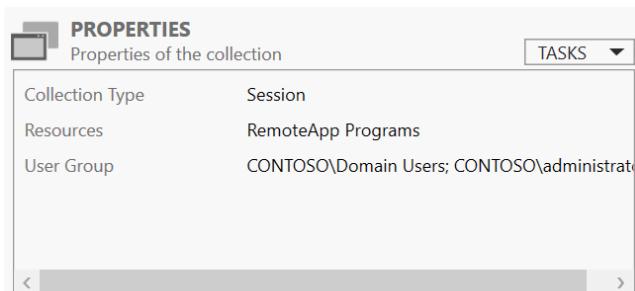
De plus, l'utilisateur connecté est "radiususer". Nous pouvons conclure que la configuration du serveur Radius et du serveur VPN est correcte.

Remote Access Clients (1)			
User Name	Duration	Number of Ports	
CONTOSO\radiususer	00:01:41	1	

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 ajoute les rôles RD Virtualization Host, RD Session Host, RD Connection Broker, RD Web Access et RD Licensing.



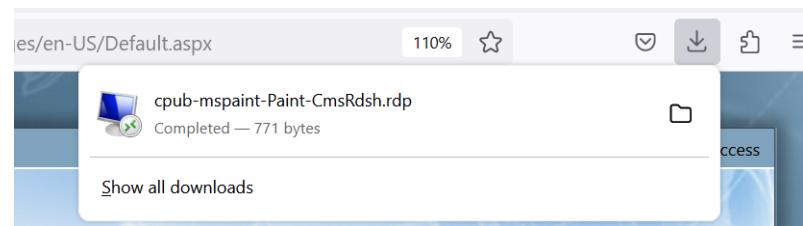


La configuration du serveur pour partager à distance les applications Paint et Notepad.

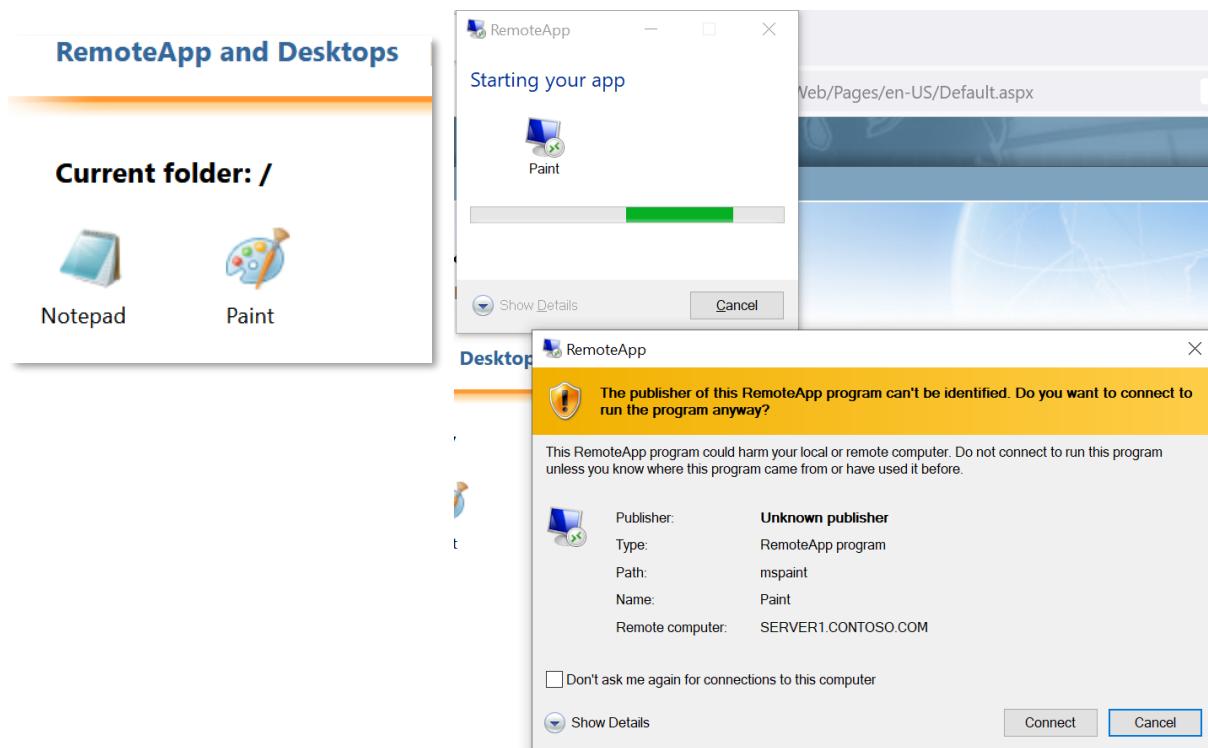
The screenshot shows the 'REMOTEAPP PROGRAMS' section of the properties dialog. It lists two programs: 'Notepad' and 'Paint'. Both are configured with an alias and marked as visible in RD Web Access.

RemoteApp Program Name	Alias	Visible in RD Web Access
Notepad	notepad	Yes
Paint	mspaint	Yes

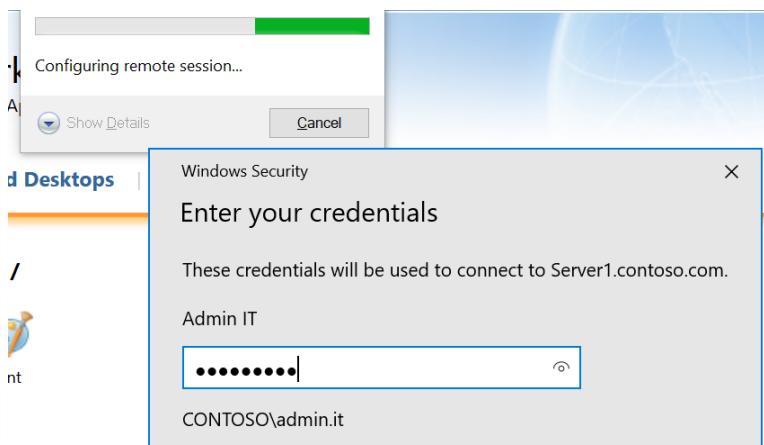
Sur un client Windows 10, nous accédons à la page web **server1.contoso.com/rdweb** pour tester le service Terminal Server. On se connecte avec le nom d'utilisateur du domaine.



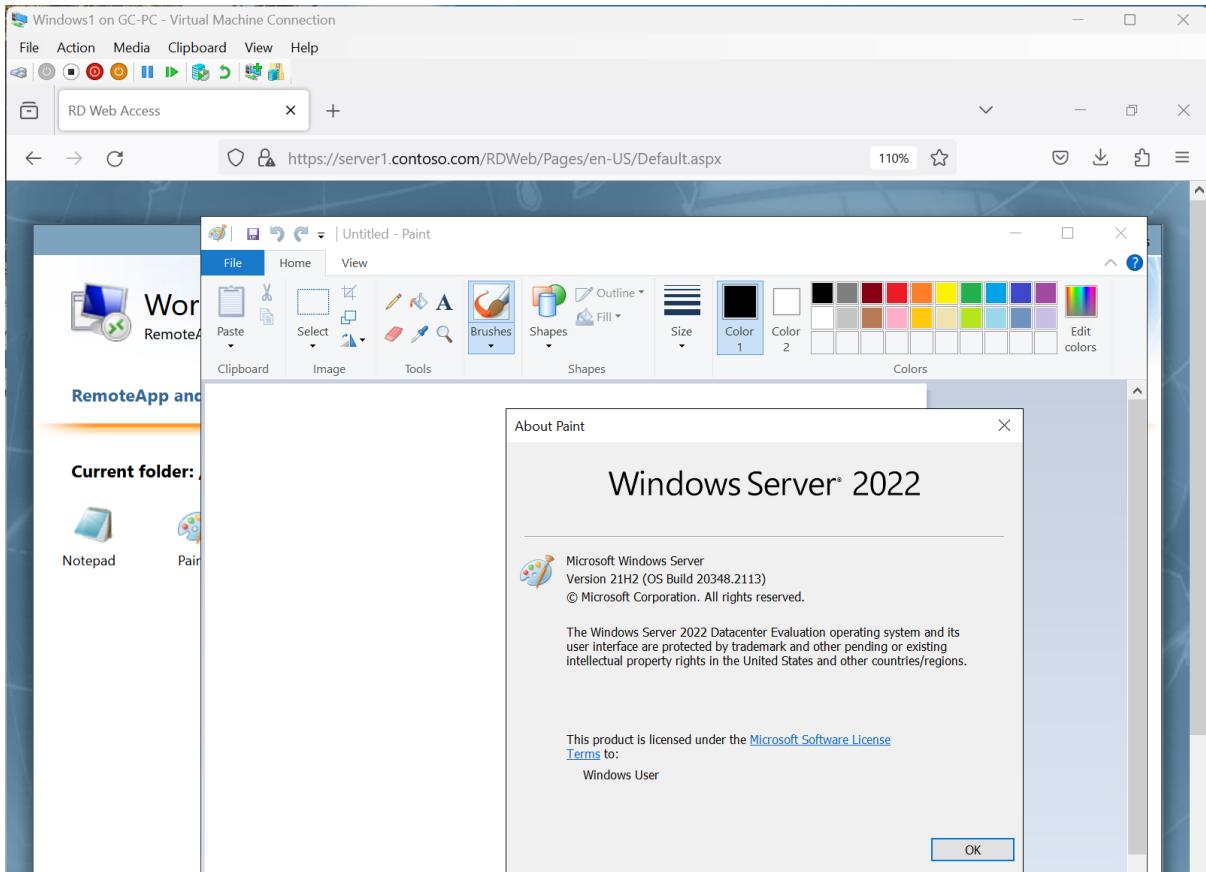
On trouve les applications partagées et on essaie d'ouvrir une application, par exemple Paint.



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).

A screenshot of the Windows Deployment Services (WDS) console. On the left, there is a navigation tree under "Windows Deployment Services" with "Servers" expanded, showing "Server1.contoso.com" and its sub-folders: "Install Images" (with "Windows 10" selected), "Boot Images", and "Pending Devices". On the right, a table titled "Windows 10 2 Install Image(s)" lists two images: "Windows 10 Enterprise Evaluation" and "Windows 10 with Outlook". The table columns are: Image Name, Architecture, Status, Expanded Size, Date, OS Version, and Priority. The details for "Windows 10 Enterprise Evaluation" are: x64, Online, 14707 MB, 11/10/2022, 10.0.19041, and Priority 500000. The details for "Windows 10 with Outlook" are: x64, Online, 21947 MB, 11/10/2022, 10.0.19045, and Priority 500000.

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.



Operating system	Language	Architecture	Date modified
Windows 10 Enterprise Evaluation	en-US	x64	11/11/2023
Windows 10 with Outlook	en-US	x64	11/11/2023



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.

The screenshot shows the Exchange Admin Center interface. On the left, a navigation pane lists: recipients, servers, databases, database availability groups, virtual directories, certificates, permissions, compliance management, organization, protection, mail flow, and mobile. The 'servers' link is highlighted. The main content area displays server details for 'EXCHANGE'. It includes a toolbar with edit, search, and copy icons, and a table with columns: NAME, SERVER ROLES, and VERSION. A single row is shown for 'EXCHANGE' with 'Mailbox' under SERVER ROLES and 'Version 15.2 (Build 1118.7)' under VERSION. To the right of the table, a summary box provides more details: Mailbox, Version 15.2 (Build 1118.7), Standard Trial Edition, Trial, and a link to 'Enter Product Key'.

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

The screenshot shows the Exchange Admin Center interface. The left navigation pane is identical to the previous one. The main content area shows the 'databases' section. It includes a toolbar with add, edit, delete, search, and copy icons, and a table with columns: NAME, ACTIVE ON SERV..., SERVERS WITH COPIES, STATUS, and BAD COPY COUNT. A new row is being added, with 'Mailbox Database...' under NAME, 'EXCHANGE' under ACTIVE ON SERV..., 'EXCHANGE' under SERVERS WITH COPIES, 'Mou...' under STATUS, and '0' under BAD COPY COUNT. The row for 'Store1' is also visible, showing it is active on both servers and has 0 bad copy counts.

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

The screenshot shows the Exchange Admin Center interface. The left navigation pane is identical to the previous ones. The main content area shows the 'mailboxes' section. It includes a toolbar with add, edit, delete, search, and copy icons, and a table with columns: DISPLAY NAME, MAILBOX TYPE, and EMAIL ADDRESS. A new row is being added, with 'Admin IT' under DISPLAY NAME, 'User' under MAILBOX TYPE, and 'admin.it@contoso.com' under EMAIL ADDRESS. The row for 'Admin IT' is highlighted. Other users listed are 'Administrator', 'Bill Gates', and 'Bruce Lee', each with their respective details. To the right, a summary box indicates 'User mailboxes' and 'admin.it@contoso.com'.

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

The screenshot shows the Microsoft 365 Admin Center interface. On the left, a sidebar menu under 'mail flow' includes options like recipients, permissions, compliance management, organization, protection, and 'Internet connector'. The 'Internet connector' option is selected. The main pane displays a table titled 'Internet connector' with one row: 'Internet connector' (Status: Enabled). Below the table, it says 'Last modified: 2023-11-06 10:27:19 PM' and 'Connector status - Enabled'. At the top of the main pane, there are navigation links: rules, delivery reports, accepted domains, email address policies, receive connectors, and send connectors (which is highlighted in blue).

This screenshot shows the 'general' tab of the 'Internet connector' configuration. It includes fields for 'Address space' (specifying address spaces to route mail) and 'Source server' (associating the connector with servers containing transport roles). A checkbox for 'Scoped send connector' is also present. Below these sections, there are 'scoping' and 'delivery' tabs.

TYPE	DOMAIN	COST
SMTP	*	1

SERVER	SITE	ROLE	VERSION
EXCHA...	contoso.com...	Mailbox	Version...

This screenshot shows the 'delivery' tab of the 'Internet connector' configuration. It includes sections for 'Network settings' (specifying how to send mail with this connector), with options for 'MX record associated with recipient domain' (selected) and 'Route mail through smart hosts'. Below these, there is a 'SMART HOST' section.

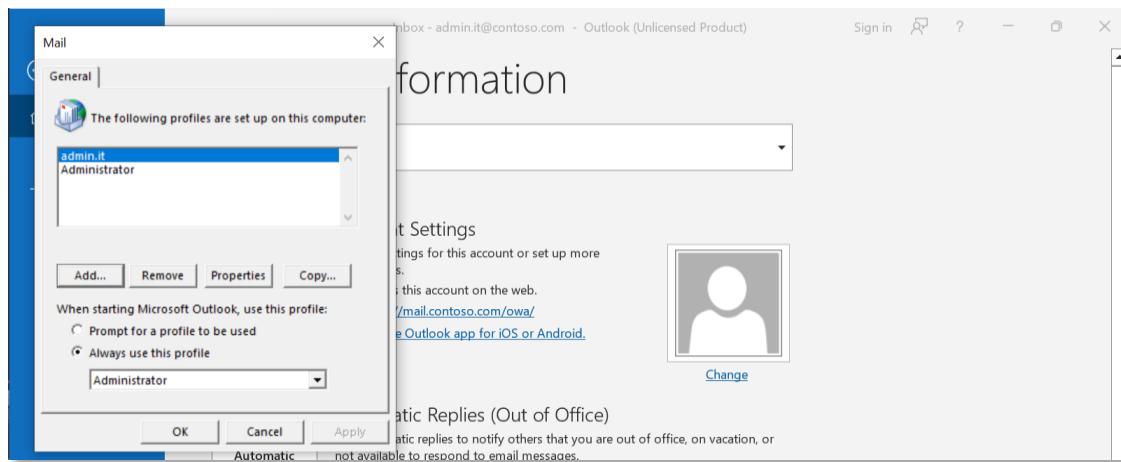
SMART HOST	

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

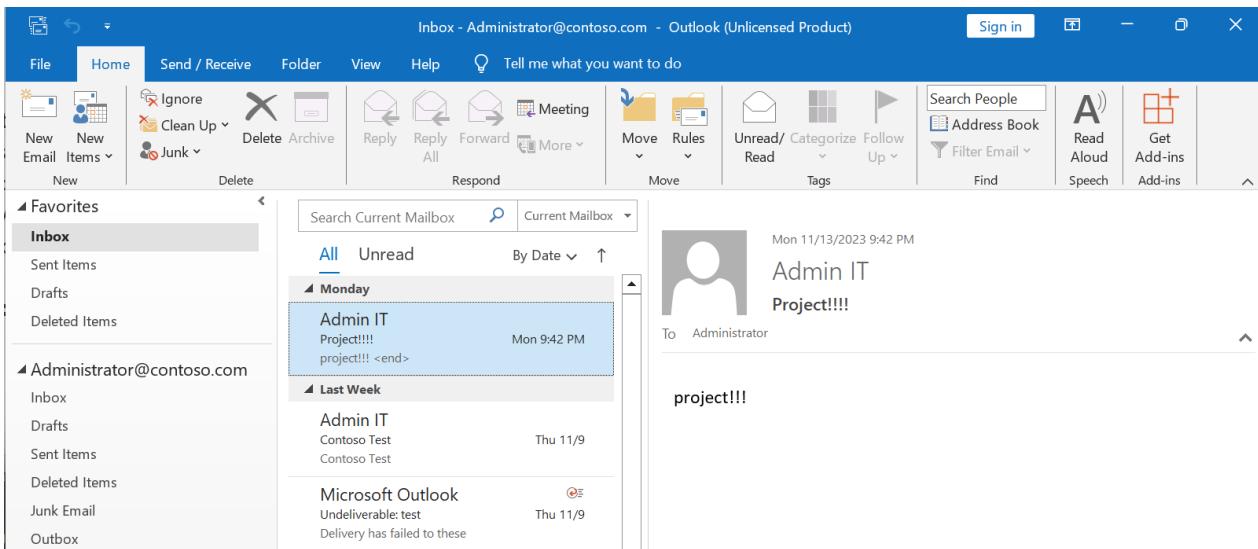
The image contains two screenshots of the Microsoft Exchange Admin Center interface. The top screenshot shows the 'services' section for a certificate named 'ContosoSSL'. It lists four services that can be assigned the certificate: SMTP, IMAP, POP, and IIS. All four checkboxes are checked. The bottom screenshot shows the 'general' details for the same certificate. It displays the following information:

Setting	Value
Name:	ContosoSSL
Status:	Valid
Issuer:	CN=mail.contoso.com
Expires on:	2028-11-06
Subject:	CN=mail.contoso.com
Subject Alternative Names:	mail.contoso.com
AutoDiscover.contoso.com	

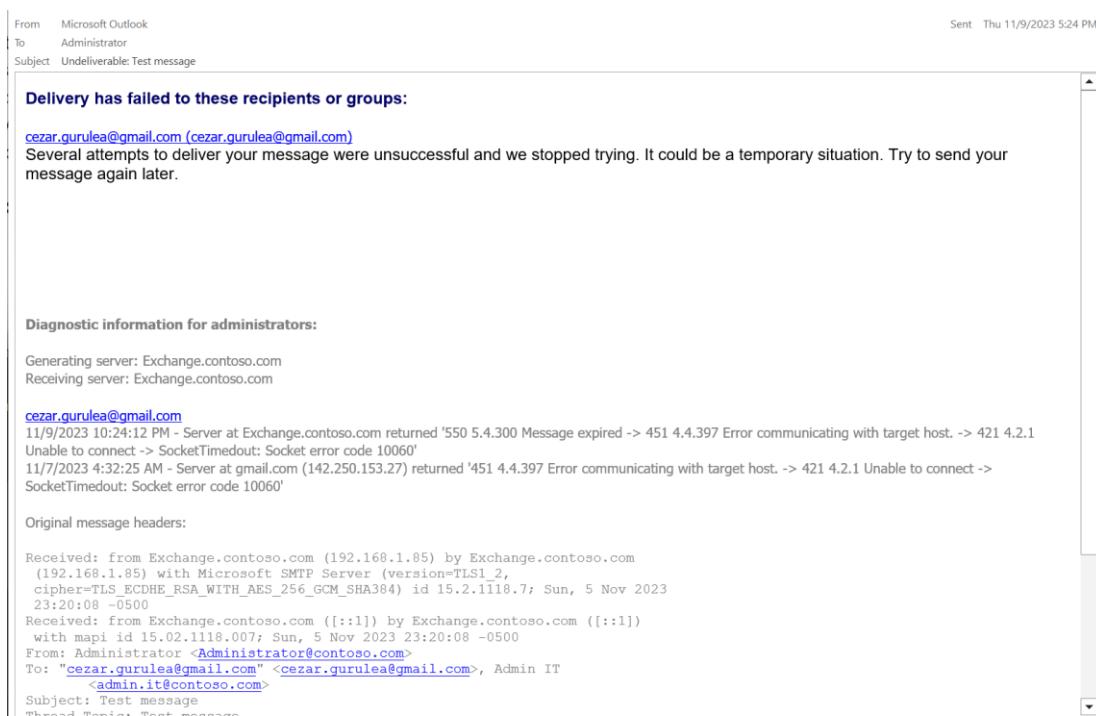
Pour le test, nous allons créer deux profils dans Outlook et envoyer des courriels entre les utilisateurs du domaine, puis à l'extérieur vers gmail.com, yahoo.com et lcieducation.net.

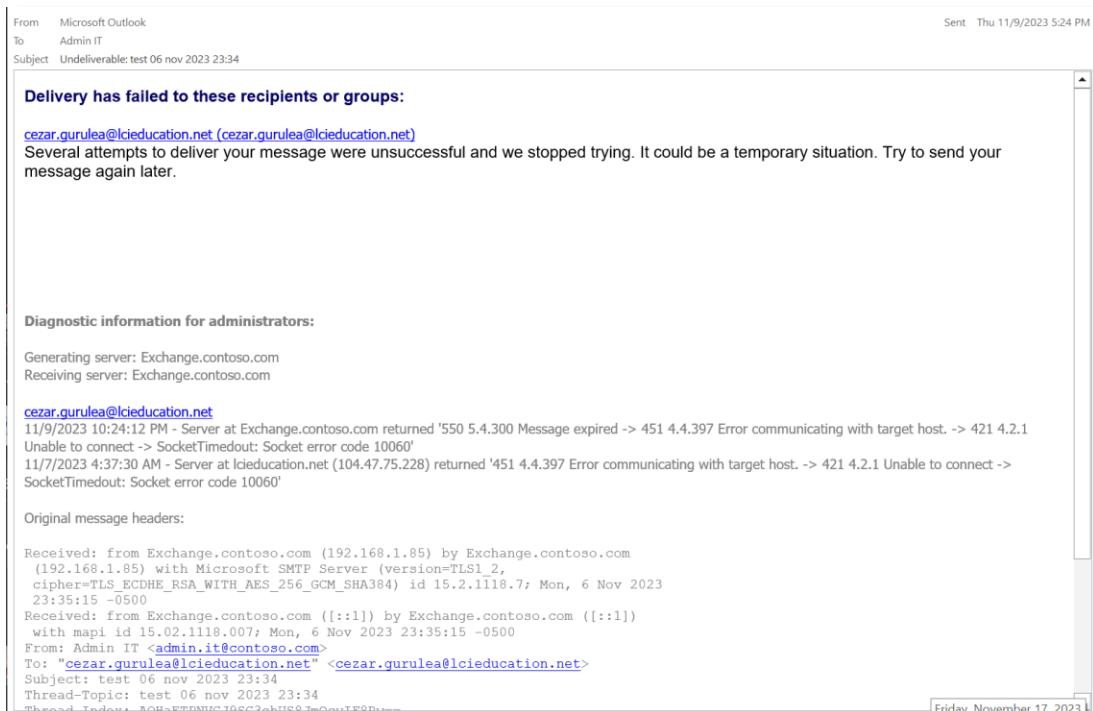


Les courriers soient envoyés et reçus avec succès à l'intérieur du domaine.



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.