COMPTE RENDU TECHNIQUE
AP17

Techniciens	Killian Goncalves & Cristopher Boni Fuentes
Groupe	8
Date	Mars 2026

SUJETS TRAITÉS
- Sécurisation HTTPS(GLPI/Nagios)
- Messagerie STARTTLS/TLS(Postfix)
- Pare-feu UFW
- Authentification LDAP/ActiveDirectory
- Administration et sécuritéActive Directory

0. Prérequis

- **Répartition des tâches :** Utilisation d'un diagramme de Gantt(lien Gantt) pour planifier les durées et la répartition entre les membres de l'équipe (Killian et Cristopher).

- **Mise à jour du schéma réseau :** Intégration des nouvelles machines virtuelles dans la topologie existante(lien shema).

1. Sécurisation du service Web (HTTPS)

L'objectif decettesection est derendreles services web (serveurNAGIOS ou GLPI) accessibles en HTTPS. Cela nécessite la création d'une autorité de certification (CA) interne et d'un certificat serveur auto-signé.

1.1 Création du répertoire PKI et de la clé CA

Création du répertoire de travail et génération de la clé privée de l'autorité de certification :

```
root@glpi:~/pki-glpi# openssl req -x509 -new -nodes -key maCA.key -sha256 -days 1825 -out maCA.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:fr
State or Province Name (full name) [Some-State]:seineetmarne
Locality Name (eg, city) []:melun
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
root@glpi:~/pki-glpi#
```

Création du répertoire /root/pki-glpi et génération de la clé CA (2048 bits)

```
root@glpi:~/pki-glpi# openssl req -new -newkey rsa:2048 -nodes -keyout glpi.key -out glpi.csr
..........+.....+....+...++++++++++++++++++++++++++++++++++++++++*..+..+....+..............+...
..+...+.+..+............+.........+......+..+....+.....+.........+.+.........+.....+.+...+..+..
+.....................+....+......+...........+......+.........++++++
...+...+....+...+..+.+...+..++++++++++++++++++++++++++++++++++++++++*...+...+..+...+...+.......+
.....+...+..+.........+.........+.....+...+.+...........+.........+...+..+....+..............
----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

Génération de la clé privée du serveur GLPI et de la CSR

1.2 Génération et signature du certificat serveur

Signature du certificat serveur par la CA interne (durée 825 jours) puis vérification :

```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:seineetmarne
Locality Name (eg, city) []:melun
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

Informations DN saisies pour le certificat serveur GLPI

```
root@glpi:~/pki-glpi# openssl x509 -req -in glpi.csr -CA maCA.pem -CAkey maCA.key -CAcreateserial -out glpi.crt -days 825 -sha256
Certificate request self-signature ok
subject=C=FR, ST=seineetmarne, L=melun, O=Internet Widgits Pty Ltd
root@glpi:~/pki-glpi#
```

Signature du certificat serveur par la CA – Certificate request self-signature ok

1.3 Déploiement des certificats et activation SSL Apache

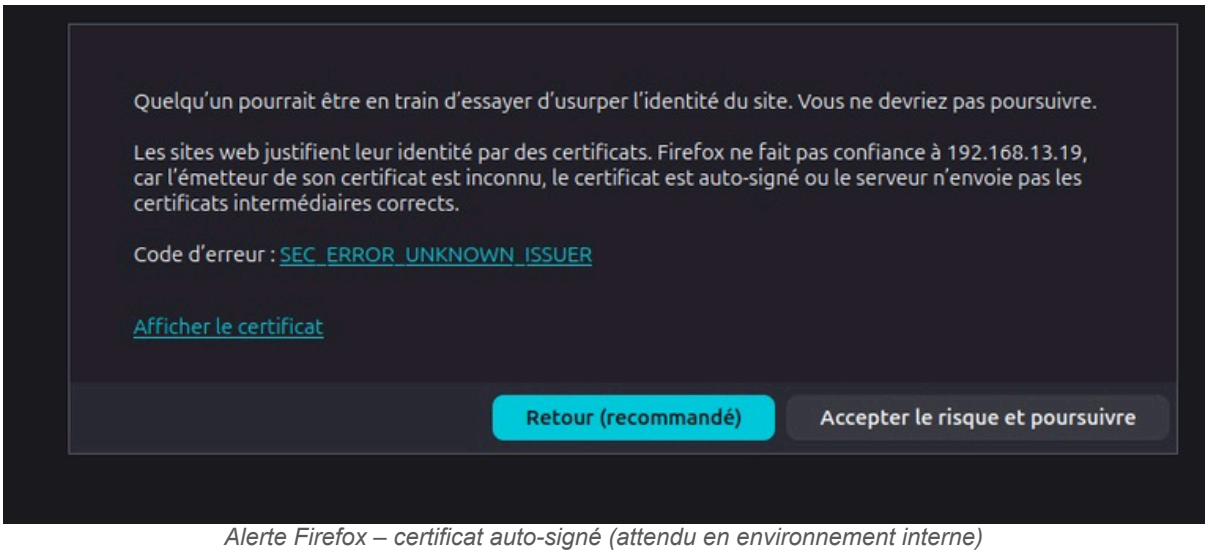
Copie desfichiersdecertificatetdeclédanslesrépertoiressystèmeApache, puis activation du module SSL :

```
root@glpi:~/pki-glpi# a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL
To activate the new configuration, you need to run:
  systemctl restart apache2
root@glpi:~/pki-glpi# systemctl restart apache2
root@glpi:~/pki-glpi# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
```

Activation du module SSL Apache2 (a2enmod ssl, a2ensite default-ssl)

1.4 Configuration du VirtualHost HTTPS

Éditiondufichier/etc/apache2/sites-available/default-ssl.conf pour référencer les certificats générés. Le navigateur affiche une alerte SEC_ERROR_UNKNOWN_ISSUER car le certificat est auto-signé :



Alerte Firefox – certificat auto-signé (attendu en environnement interne)

■■ Il suffit d'importer le certificat CA (maCA.pem) dans le magasin de confiance du navigateur ou d'accepter l'exception de sécurité pour les tests internes.

2. Amélioration des services de messagerie

2.a Sécurisation STARTTLS / TLS (Postfix)

Configuration de Postfix pour chiffrer lesfluxSMTPvia STARTTLS. Modification du fichier /etc/postfix/master.cf :

```
E..4.\@.@..     ..............@#G.....j.......
:.6.....
17:20:34.824121 ens18 In  IP 192.168.13.250.59070 > glpi.https: Flags [P.], seq 3239:3263, ack 6474, win 61
5741001 ecr 284663834], length 24
E..L.]@.@..................@#G.-...j.......
:.6..........[:...if........M..
17:20:34.824122 ens18 In  IP 192.168.13.250.59070 > glpi.https: Flags [F.], seq 3263, ack 6474, win 618, op
01 ecr 284663834], length 0
E..4.^@.@..................X#G.-...j.[.....
:.6.....
17:20:34.824155 ens18 Out IP glpi.https > 192.168.13.250.59070: Flags [.], ack 3264, win 485, options [nop,
41001], length 0
E..45.@.@.iT............#G.-...Y...........
....:.6.
^C
79 packets captured
89 packets received by filter
0 packets dropped by kernel
root@glpi:~#
```

master.cf – activation STARTTLS et authentification SASL sur le port 587

2.b Vérification du port 587

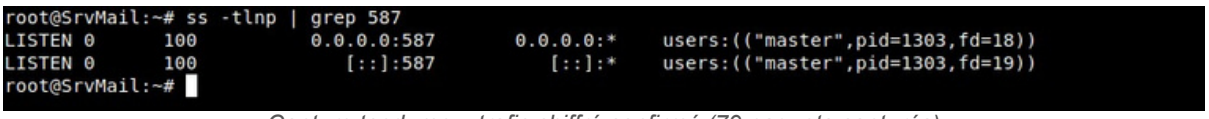
Après redémarrage de Postfix,vérification que le daemon écoute bien sur le port 587 (submission) avec la commande ss -tlnp :

```
# Choose one: enable submission for loopback clients only, or for any client.
#127.0.0.1:submission inet n -   y       -       -       smtpd
#submission inet n       -       y       -       -       smtpd
   -o syslog_name=postfix/submission
#  -o smtpd_forbid_unauth_pipelining=no
   -o smtpd_tls_security_level=encrypt
   -o smtpd_sasl_auth_enable=yes
   -o smtpd_tls_auth_only=yes
#  -o local_header_rewrite_clients=static:all
#  -o smtpd_hide_client_session=yes
#  -o smtpd_reject_unlisted_recipient=no
#     Instead of specifying complex smtpd_<xxx>_restrictions here,
#     specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
#     here, and specify mua_<xxx>_restrictions in main.cf (where
#     "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
#  -o smtpd_client_restrictions=
#  -o smtpd_helo_restrictions=
#  -o smtpd_sender_restrictions=
#  -o smtpd_relay_restrictions=
   -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
```

Port 587 en écoute – service "master" confirmé

2.c Capture de trafic chiffré (tcpdump)

Pourprouver le chiffrement, tcpdumpintercepteles trames sur le port 587. Après la commande STARTTLS, le contenu des échanges (identifiants, corps du mail) devient totalement illisible (caractères binaires) :



Capture tcpdump – trafic chiffré confirmé (79 paquets capturés)

✓ Le trafic post-STARTTLS est entièrement chiffré et illisible en clair – chiffrement opérationnel.

3. Firewall UFW

Mise enplace dupare-feuUFW (Uncomplicated Firewall) sur le routeur pour filtrer et journaliser le trafic réseau.

3.1 Installation et configuration initiale

Installation de UFW et rsyslog, puis mise en place des politiques par défaut (tout bloquer) :

```
root@routeur:~# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@routeur:~# ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
root@routeur:~# ufw default deny routed
Default routed policy changed to 'deny'
(be sure to update your rules accordingly)
root@routeur:~#
```

Installation de UFW – politiques deny incoming / deny outgoing / deny routed

3.2 Configuration avancée (sysctl & IPv6)

Activation du routage IP dans /etc/sysctl.conf (net.ipv4.ip_forward=1) et désactivation d'IPv6 dans /etc/default/ufw (IPV6=no) :

```
 GNU nano 8.4                                    /etc/default/ufw *
# /etc/default/ufw
#

# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=no
```

/etc/default/ufw – IPV6=no et /etc/sysctl.conf – net.ipv4.ip_forward=1

3.3 Activation des logs et démarrage du pare-feu

```
root@routeur:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

ufw logging on/medium – journalisation activée

```
root@routeur:~# ufw route allow from 192.168.14.0/24 to 192.168.12.0/24 port 80,443 proto tcp
Rule added
root@routeur:~# ufw route allow from 192.168.11.0/24 to 192.168.12.0/24 port 22 proto tcp
Rule added
root@routeur:~# ufw status numbered
```

ufw enable – Firewall actif et démarrage automatique au boot

3.4 Règles de routage et consultation des logs

Ajout desrèglesdeforwardHTTP/HTTPSetSSHentresous-réseaux, puis consultation des logs UFW :

```
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
53/udp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
8080/tcp                   ALLOW       Anywhere

192.168.12.0/24 80,443/tcp ALLOW FWD   192.168.14.0/24
192.168.12.0/24 22/tcp     ALLOW FWD   192.168.11.0/24
192.168.13.0/24 443/tcp    ALLOW FWD   192.168.11.0/24

root@routeur:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@routeur:~# ufw route allow from 192.168.11.0/24 to 192.168.13.0/24 port 443 proto tcp
Skipping adding existing rule
root@routeur:~# tail -f /var/log/ufw.log
2026-03-27T14:51:45.041878+01:00 routeur kernel: [UFW AUDIT] IN=eth2 OUT= MAC=bc:24:11:2e:41:6b:bc:24:11:bc:af:5b:08:00 SRC=192.168.11.
21 DST=10.177.94.2 LEN=78 TOS=0x00 PREC=0x00 TTL=64 ID=64182 DF PROTO=UDP SPT=41285 DPT=53 LEN=58
2026-03-27T14:51:45.043176+01:00 routeur kernel: [UFW AUDIT] IN=eth2 OUT= MAC=bc:24:11:2e:41:6b:bc:24:11:bc:af:5b:08:00 SRC=192.168.11.
21 DST=10.177.94.2 LEN=78 TOS=0x00 PREC=0x00 TTL=64 ID=63417 DF PROTO=UDP SPT=57742 DPT=53 LEN=58
2026-03-27T14:51:45.043297+01:00 routeur kernel: [UFW AUDIT] IN=eth2 OUT= MAC=bc:24:11:2e:41:6b:bc:24:11:bc:af:5b:08:00 SRC=192.168.11.
21 DST=10.177.94.2 LEN=78 TOS=0x00 PREC=0x00 TTL=64 ID=50563 DF PROTO=UDP SPT=46411 DPT=53 LEN=58
2026-03-27T14:51:50.045091+01:00 routeur kernel: [UFW AUDIT] IN=eth2 OUT= MAC=bc:24:11:2e:41:6b:bc:24:11:bc:af:5b:08:00 SRC=192.168.11.
21 DST=10.177.94.2 LEN=78 TOS=0x00 PREC=0x00 TTL=64 ID=22158 DF PROTO=UDP SPT=43728 DPT=53 LEN=58
2026-03-27T14:51:50.045501+01:00 routeur kernel: [UFW AUDIT] IN=eth2 OUT= MAC=bc:24:11:2e:41:6b:bc:24:11:bc:af:5b:08:00 SRC=192.168.11.
21 DST=10.177.94.2 LEN=78 TOS=0x00 PREC=0x00 TTL=64 ID=44581 DF PROTO=UDP SPT=48276 DPT=53 LEN=58
2026-03-27T14:51:50.048472+01:00 routeur kernel: [UFW AUDIT] IN=eth2 OUT= MAC=bc:24:11:2e:41:6b:bc:24:11:bc:af:5b:08:00 SRC=192.168.11.
21 DST=10.177.94.2 LEN=78 TOS=0x00 PREC=0x00 TTL=64 ID=22781 DF PROTO=UDP SPT=41699 DPT=53 LEN=58
2026-03-27T14:51:50.048500+01:00 routeur kernel: [UFW AUDIT] IN=eth2 OUT= MAC=bc:24:11:2e:41:6b:bc:24:11:bc:af:5b:08:00 SRC=192.168.11.
21 DST=10.177.94.2 LEN=78 TOS=0x00 PREC=0x00 TTL=64 ID=11486 DF PROTO=UDP SPT=36136 DPT=53 LEN=58
2026-03-27T14:52:03.616916+01:00 routeur kernel: [UFW AUDIT] IN=eth2 OUT=eth3 MAC=bc:24:11:2e:41:6b:bc:24:11:50:4c:eb:08:00 SRC=192.168
11.1 DST=192.168.12.1 LEN=67 TOS=0x00 PREC=0x00 TTL=63 ID=32454 DF PROTO=UDP SPT=49374 DPT=53 LEN=47
2026-03-27T14:52:03.616947+01:00 routeur kernel: [UFW BLOCK] IN=eth2 OUT=eth3 MAC=bc:24:11:2e:41:6b:bc:24:11:50:4c:eb:08:00 SRC=192.168
11.1 DST=192.168.12.1 LEN=67 TOS=0x00 PREC=0x00 TTL=63 ID=32454 DF PROTO=UDP SPT=49374 DPT=53 LEN=47
2026-03-27T14:52:05.065040+01:00 routeur kernel: [UFW AUDIT] IN=eth2 OUT= MAC=bc:24:11:2e:41:6b:bc:24:11:bc:af:5b:08:00 SRC=192.168.11.
21 DST=10.177.94.2 LEN=78 TOS=0x00 PREC=0x00 TTL=64 ID=61708 DF PROTO=UDP SPT=58655 DPT=53 LEN=58
```

Logs UFW (/var/log/ufw.log) et règles de routage entre sous-réseaux

```
root@routeur:~# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 192.168.12.0/24 80,443/tcp ALLOW FWD   192.168.14.0/24
[ 3] 192.168.12.0/24 22/tcp     ALLOW FWD   192.168.11.0/24
```

Statut UFW numéroté – 3 règles actives

#	Destination	Action	Source
1	22/tcp	ALLOW IN	Anywhere
2	192.168.12.0/24 80,443/tcp	ALLOW FWD	192.168.14.0/24
3	192.168.12.0/24 22/tcp	ALLOW FWD	192.168.11.0/24

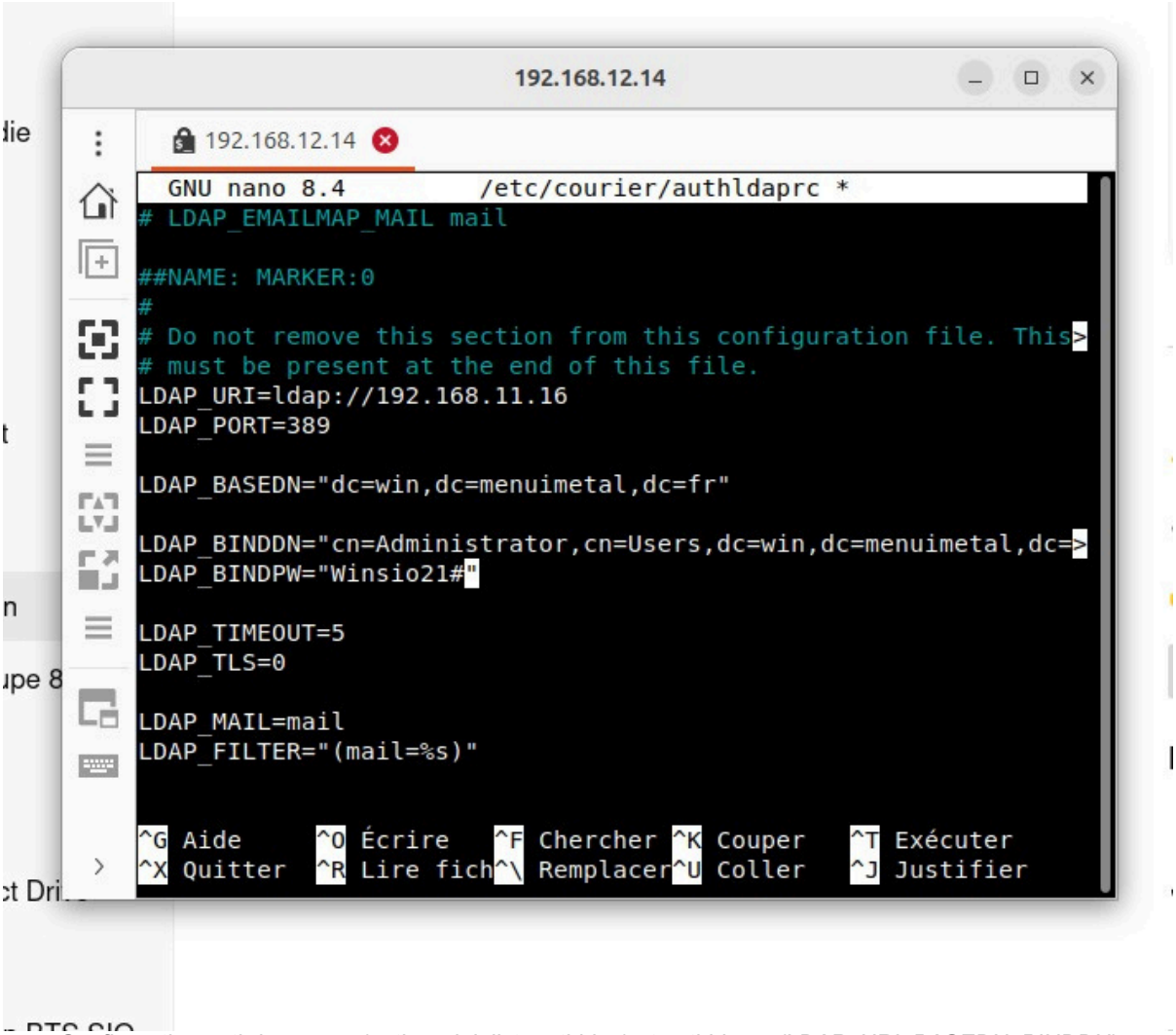
Récapitulatif des règles UFW actives

4. Authentification Centralisée LDAP (Active Directory)

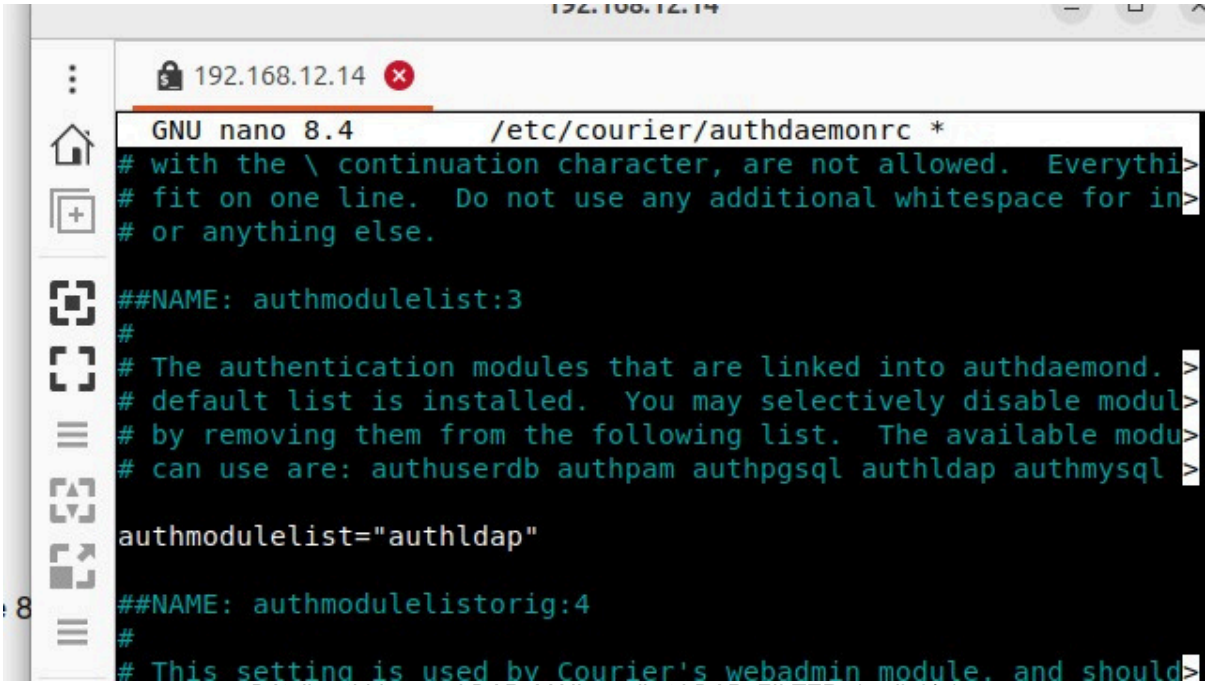
L'objectif étaitderemplacerlescompteslocauxduserveur Mail parlescomptesdel'ActiveDirectory (winsrv – 192.168.11.16).

4.1 Configuration de Courier-Authlib

Installation des paquets courier-authlib-ldap et ldap-utils, puis configuration des fichiers authdaemonrc et authldaprc :



Configuration authdaemonrc (authmodulelist=authldap) et authldaprc (LDAP_URI, BASEDN, BINDDN)



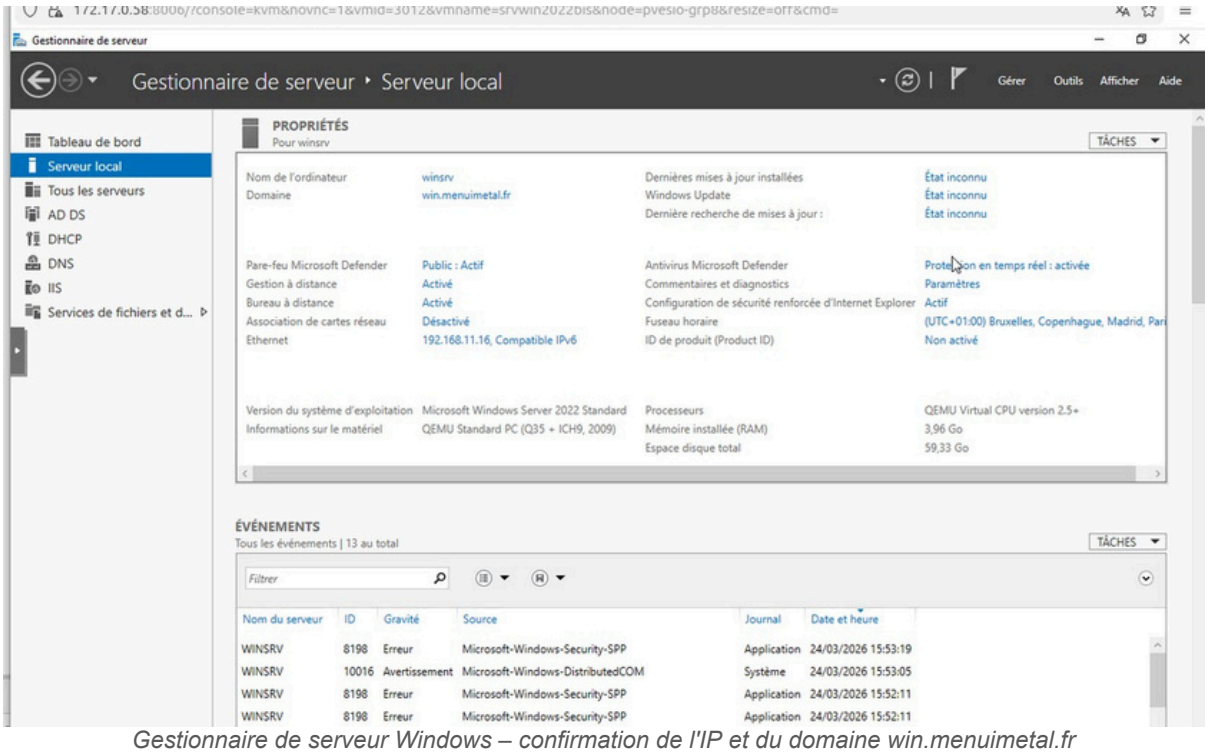
Détail authldaprc – LDAP_MAIL=mail et LDAP_FILTER=(mail=%s)

Fichier	Paramètre	Valeur
authdaemonrc	authmodulelist	`authldap`
authldaprc	LDAP_URI	`ldap://192.168.11.16`
authldaprc	LDAP_BASEDN	`dc=win,dc=menuimetal,dc=fr`
authldaprc	LDAP_BINDDN	`cn=Administrator,ou=Users,dc=win,...`
authldaprc	LDAP_MAIL	`mail`
authldaprc	LDAP_FILTER	`(mail=%s)`

Récapitulatif des paramètres LDAP configurés

4.2 Confirmation du serveur Windows (winsrv)

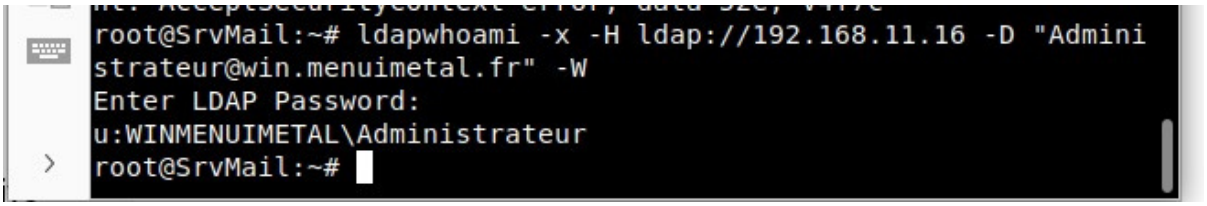
Vérificationdel'adresse IP etdunom dedomaineduserveurWindows Server (192.168.11.16 – win.menuimetal.fr) depuis la console de gestion :



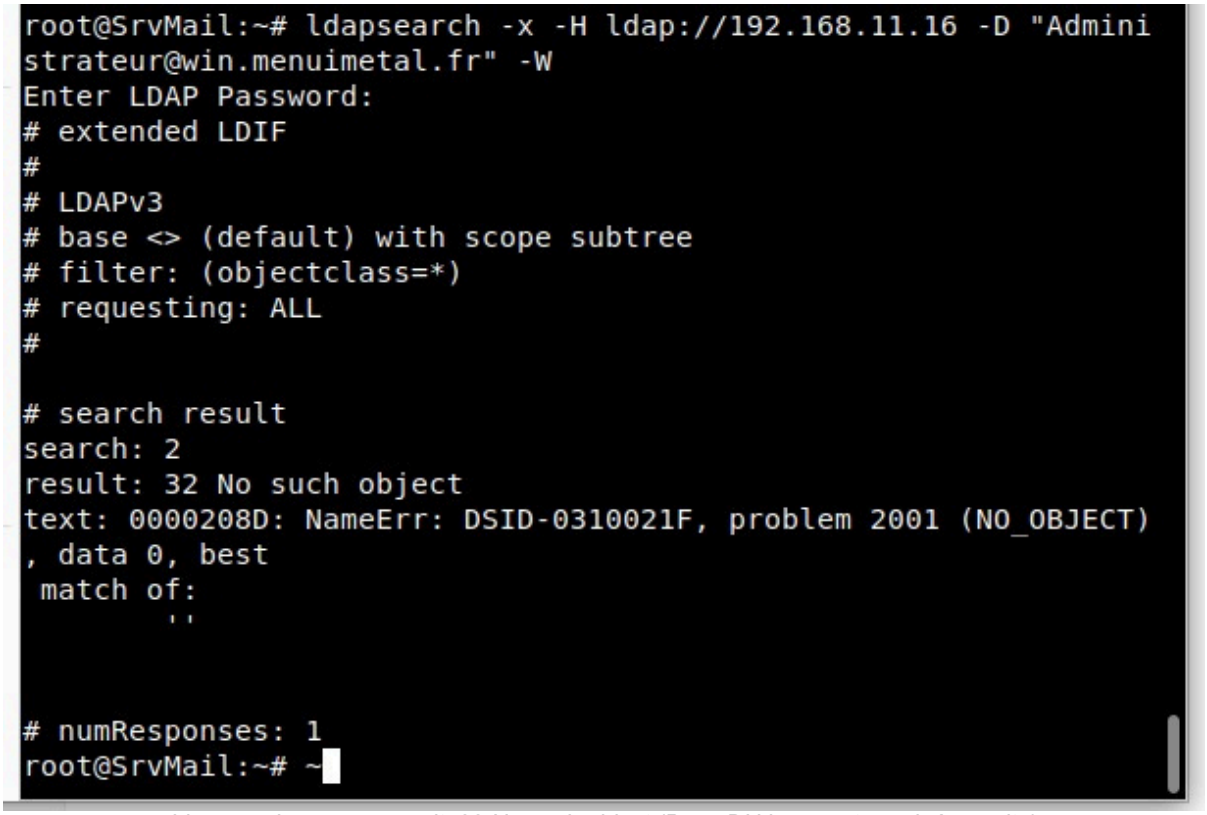
Gestionnaire de serveur Windows – confirmation de l'IP et du domaine win.menuimetal.fr

4.3 Tests de communication LDAP (ligne de commande)

Deuxtestssonteffectuéspourvaliderlacommunication Linux↔ActiveDirectory :



ldapwhoami – le serveur répond u:WINMENUIMETAL\Administrateur (authentification AD réussie)



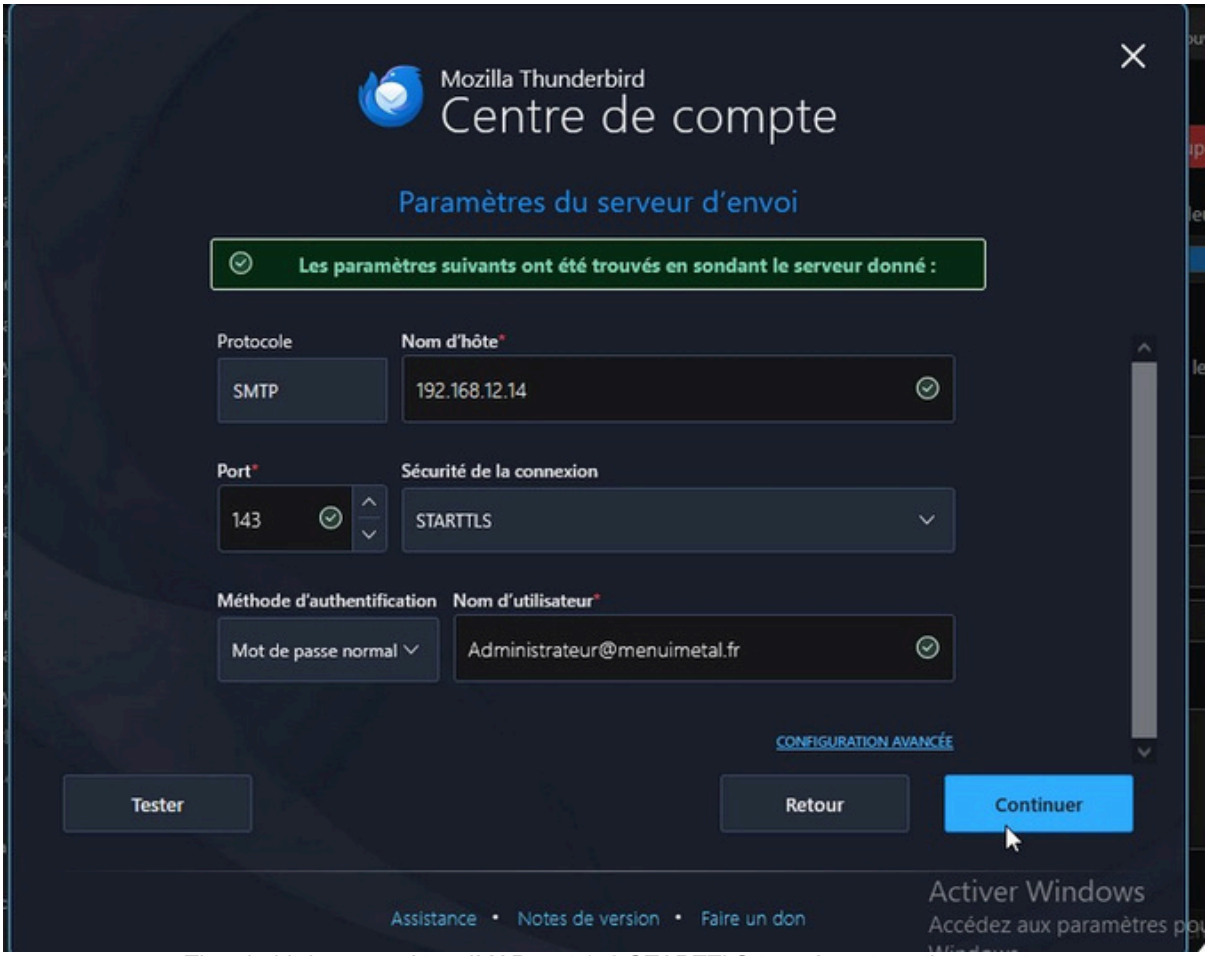
ldapsearch – erreur result: 32 No such object (Base DN incorrect, corrigé ensuite)

■■ ldapwhoami prouve que le serveur Linux s'authentifie correctement auprès de l'AD. L'erreur ldapsearch result: 32 indique que la connexion est établie mais que le Base DN était incorrect – ajustement de la configuration effectué.

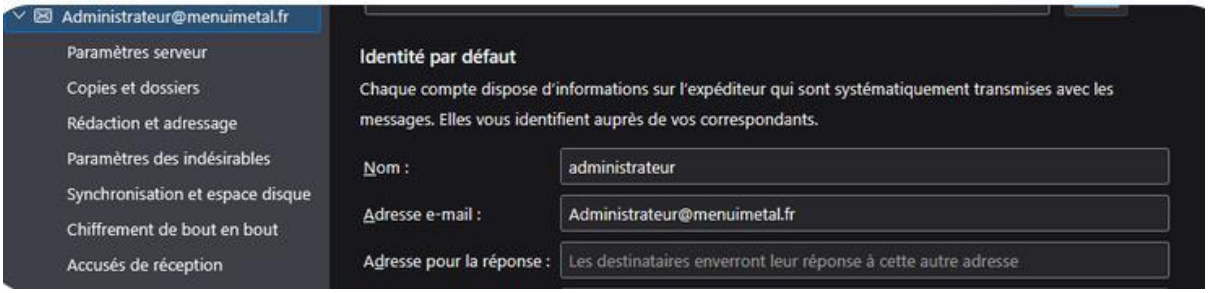
5. Administration et Sécurité Active Directory

5.1 Mise en œuvre et Troubleshooting sur Thunderbird

ConfigurationduclientThunderbird pourutiliserleserveur Mailavecauthentification AD. Le port 143 avec la sécurité STARTTLS est utilisé, conformément aux exigences de sécurité :



Thunderbird – paramètres IMAP port 143 STARTTLS trouvés automatiquement

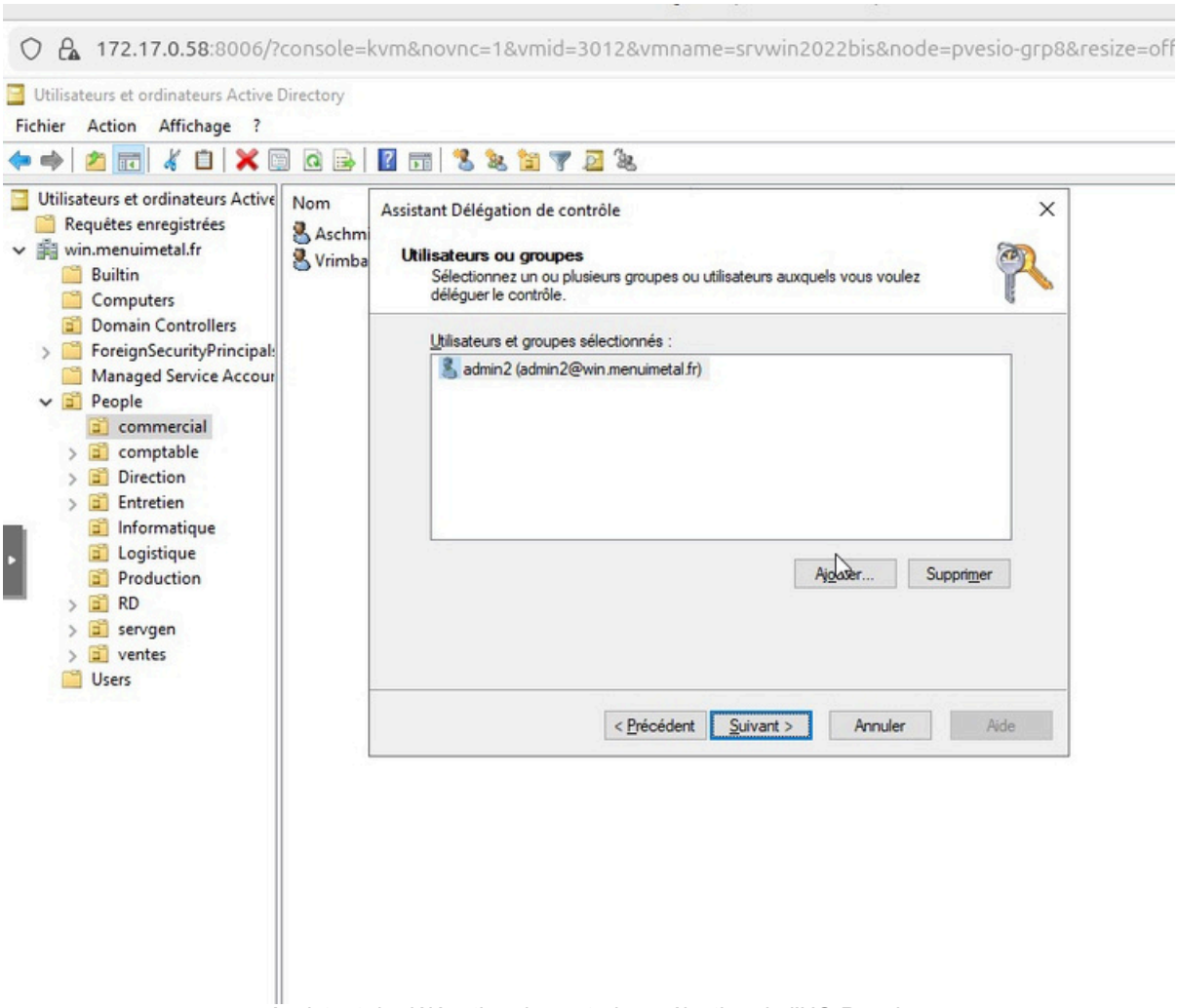


Identité Administrateur@menuimetal.fr configurée dans Thunderbird

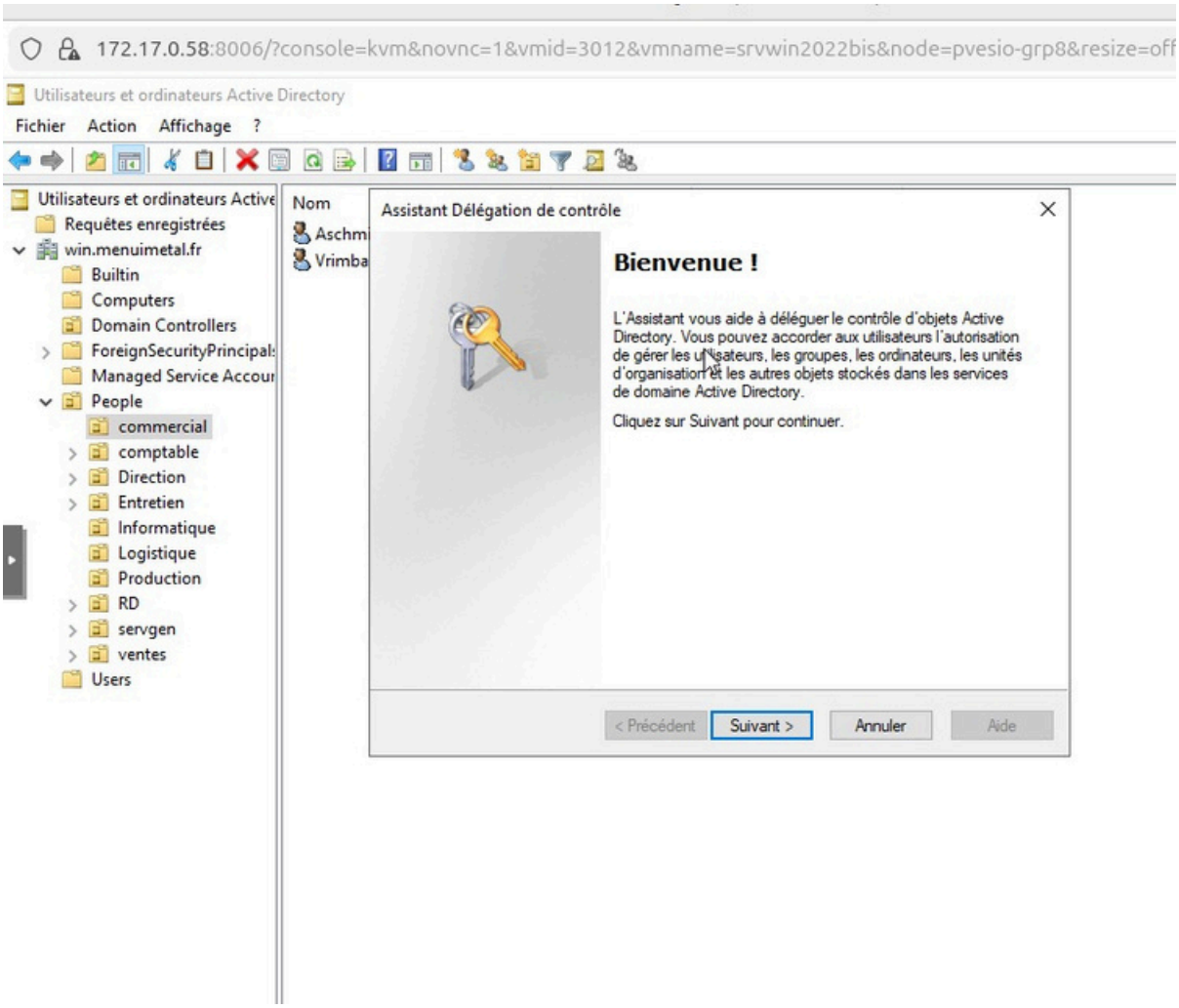
✓ Bandeau vert confirmé – paramètres IMAP trouvés. Port 143 avec STARTTLS opérationnel.

5.2 Délégation de contrôle (UO People → admin2)

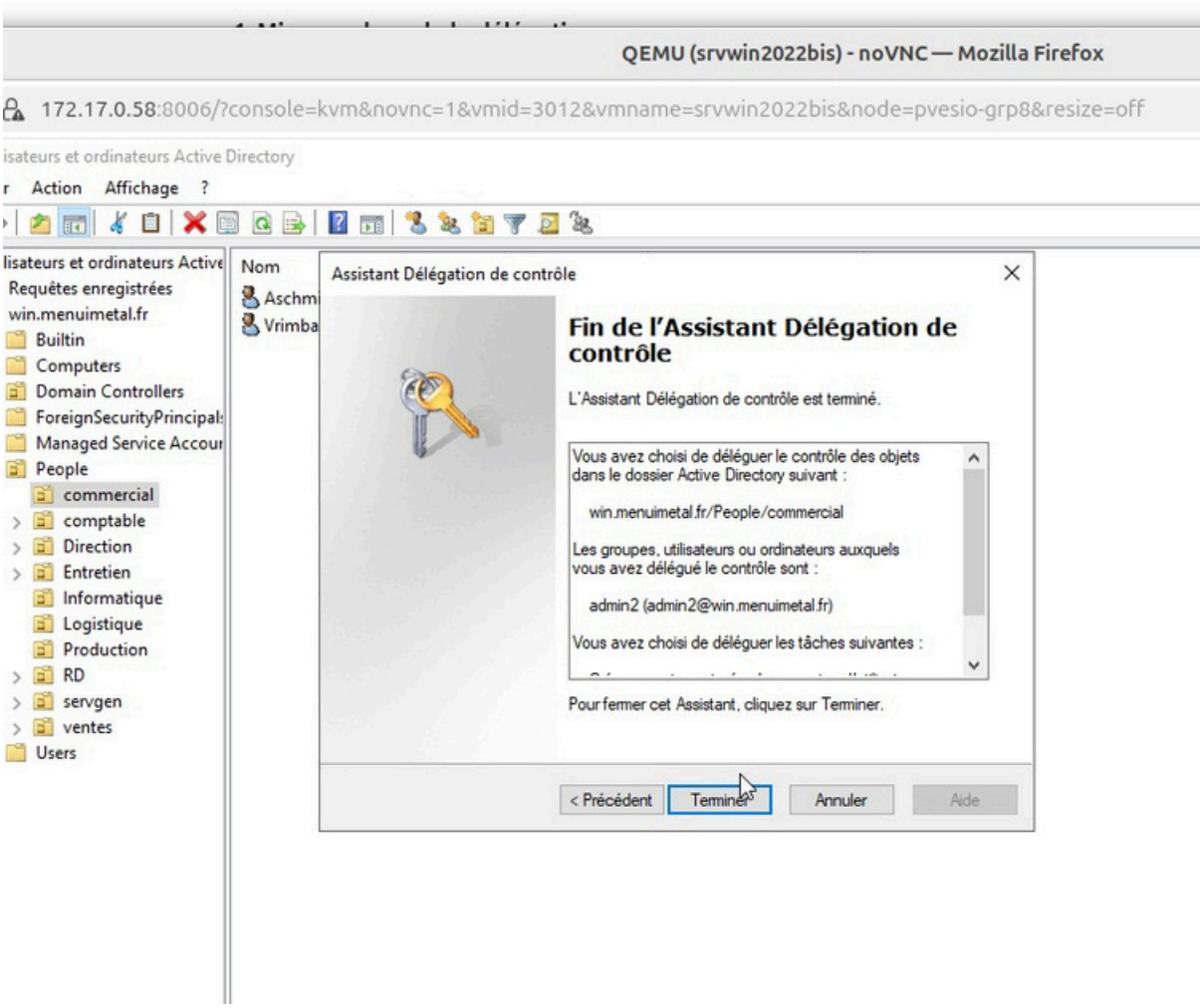
Pourrépondreaux exigencesdeM. Lepagesur la gestion desUnités d'Organisation (UO), une structure d'administration déléguée a été mise en place via l'Assistant de délégation de contrôle Windows Server :



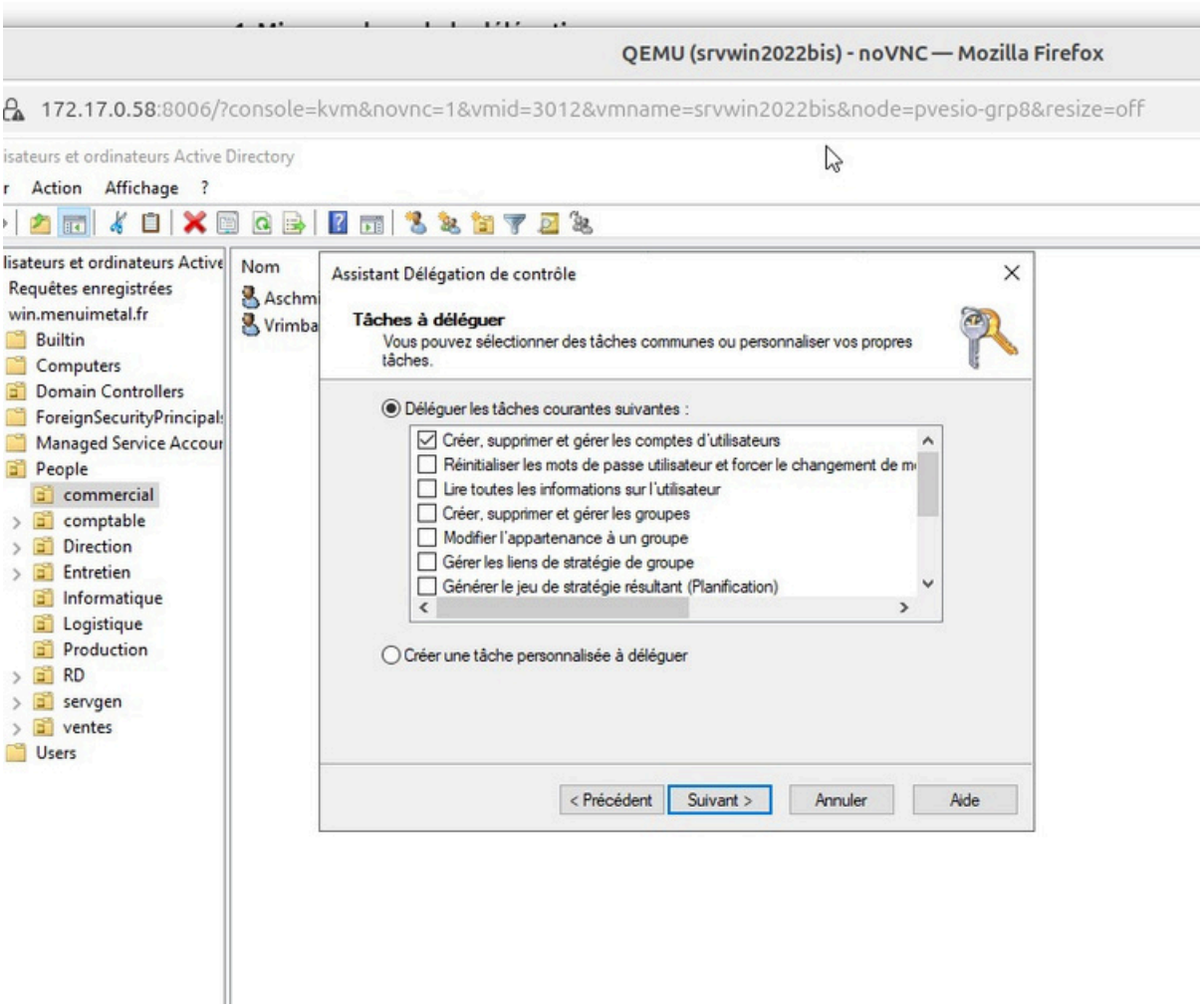
Assistant de délégation de contrôle – sélection de l'UO People



Ajout de l'utilisateur admin2 (admin2@win.menuimetal.fr) comme délégué



Tâches déléguées : créer/supprimer des utilisateurs, réinitialiser les mots de passe

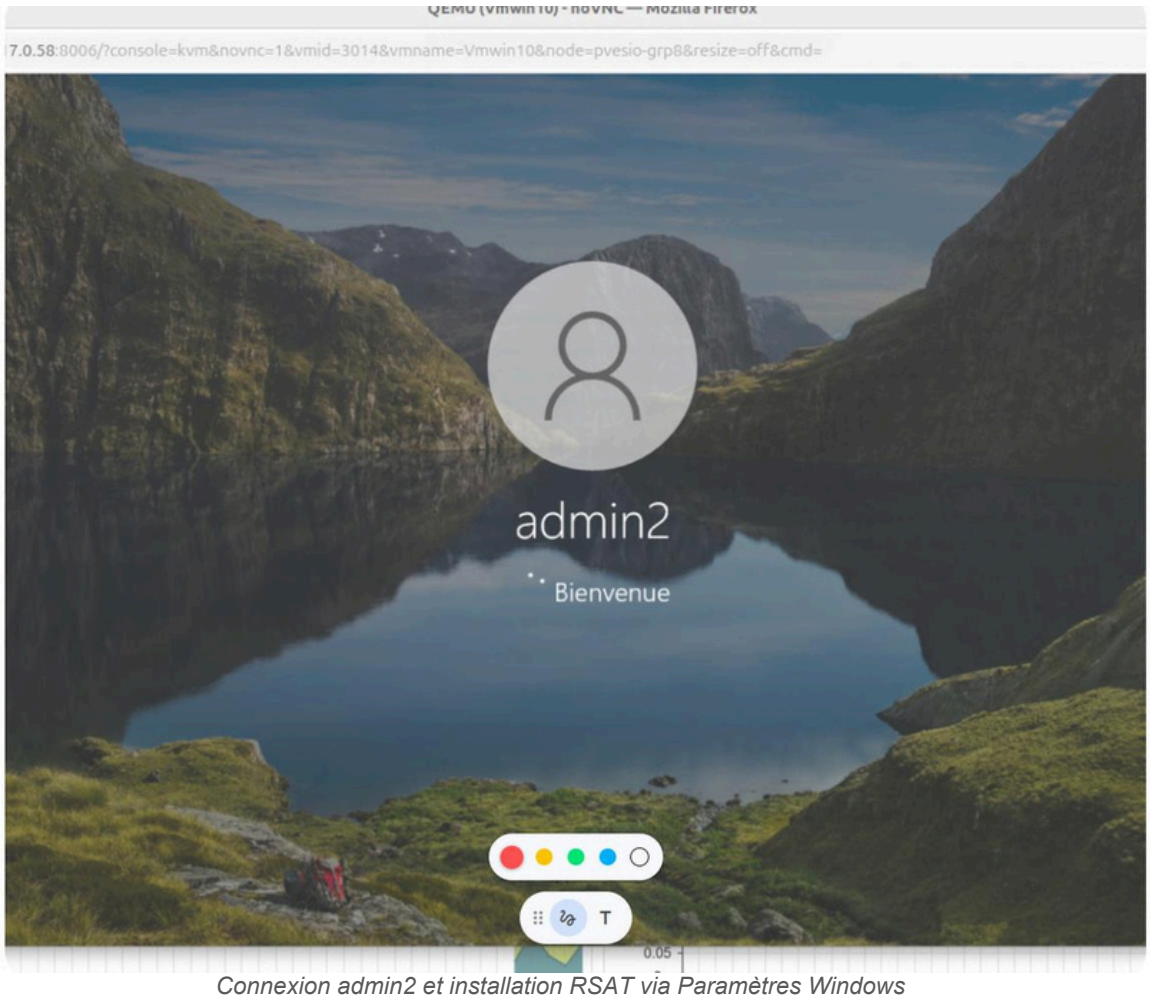


Fin de l'assistant – délégation confirmée sur win.menuimetal.fr/People/commercial

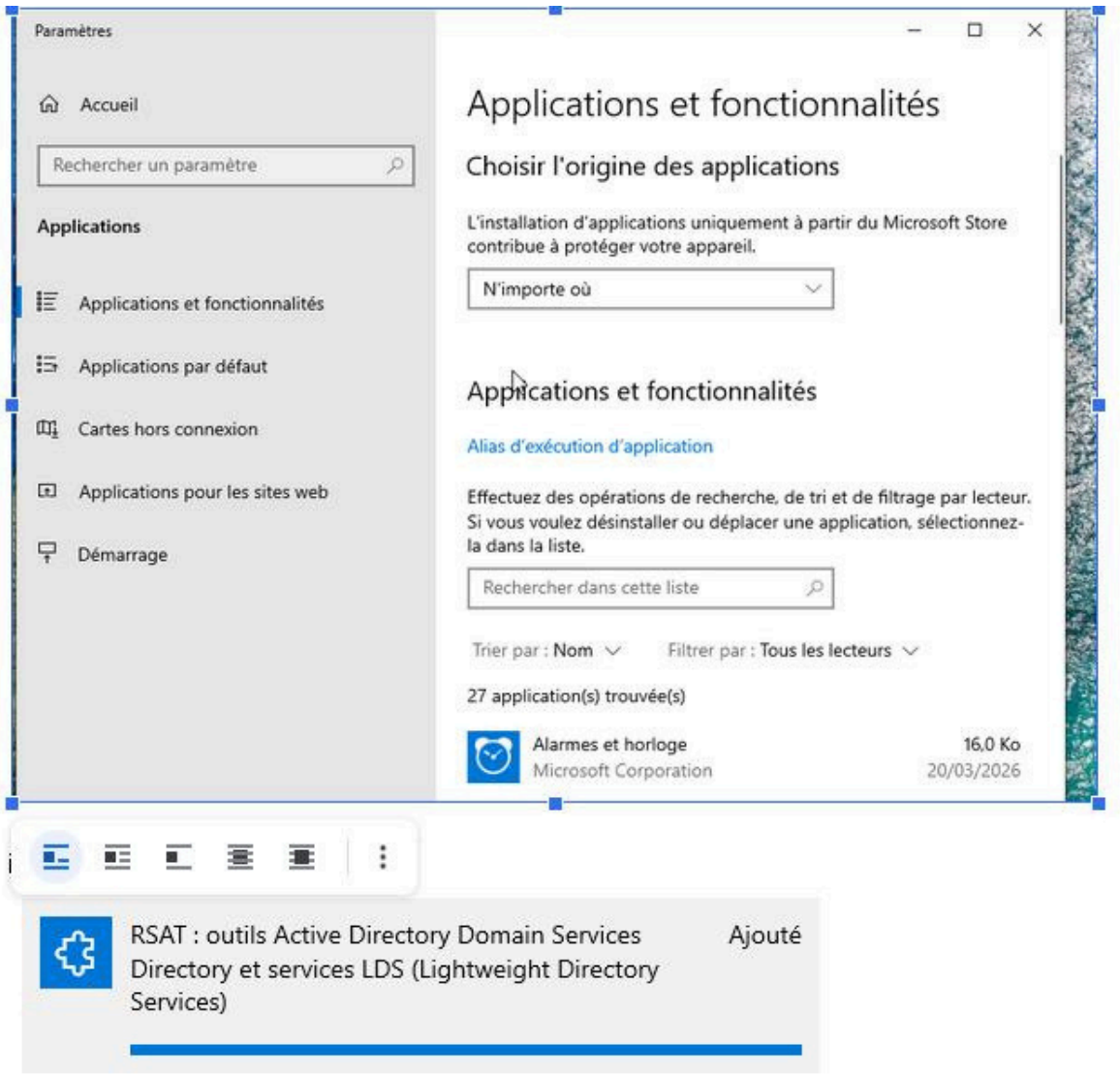
■■ Principe du moindre privilège respecté : admin2 peut gérer son service sans être administrateur du domaine complet.

5.3 Intervention sur le poste client (admin2)

Connexion sur le poste de travail (192.168.11.15) avec le compte admin2 puis installation des outils RSAT (Remote Server Administration Tools) via PowerShell :



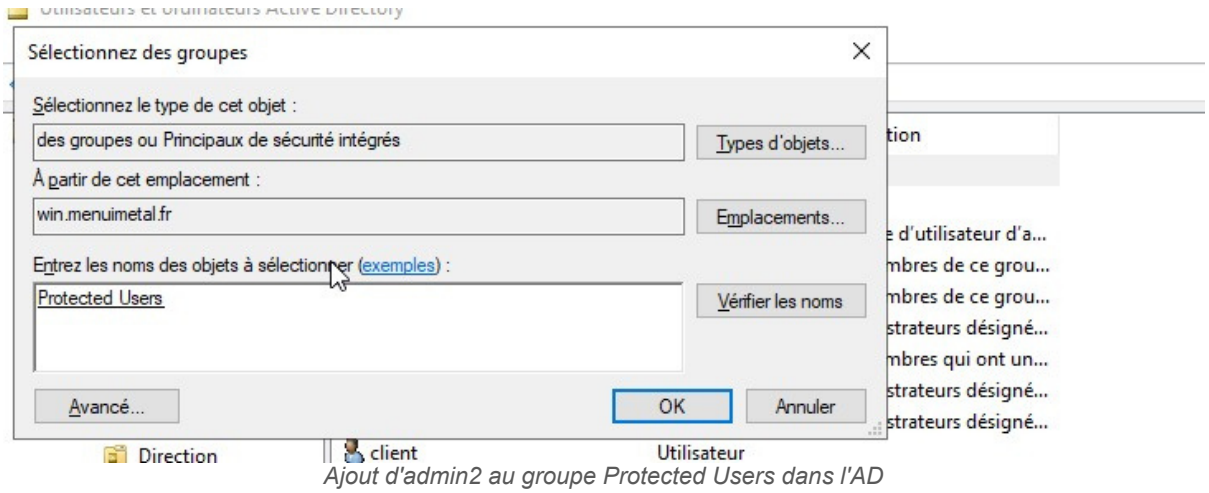
Connexion admin2 et installation RSAT via Paramètres Windows



RSAT : outils Active Directory Domain Services ajoutés avec succès

5.4 Sécurisation avec "Protected Users"

Le compte admin2, disposant désormaisdedroits sensibles (délégation de contrôle), a été intégré au groupe Protected Users de l'Active Directory pour renforcer sa sécurité (désactivation NTLM, Kerberos uniquement, pas de cache d'identifiants) :



Ajout d'admin2 au groupe Protected Users dans l'AD

✓ Sécurisation renforcée : NTLM désactivé, Kerberos uniquement, pas de cache d'identifiants sur les postes clients.

Conclusion

Cecompte rendudocumente la mise en sécurité complète de l'infrastructure réseau du projet. L'ensemble des tâches a été réalisé avec succès :

Domaine	Réalisation
Sécurisation HTTPS	Certificat auto-signé CA interne déployé sur Apache2 (GLPI/Nagios)
Messagerie sécurisée	STARTTLS/TLS activé sur Postfix (port 587) et IMAP (port 143)
Pare-feu UFW	Filtrage et routage inter-VLAN avec journalisation activée
LDAP / AD	Authentification centralisée Courier-IMAP ↔ Active Directory opérationnelle
Délégation AD	Administration déléguée avec principe du moindre privilège (Protected Users)

Cette activité professionnelle a permis de consolider les compétences en administration système Linux et Windows Server, en sécurité réseau (PKI, TLS, pare-feu) et en gestion centralisée des identités (LDAP/AD).