Mode Opératoire

Diagnostic d'un échec de connexion Bureau à distance (RDP)

Code :	MO-AD-009
Version :	1.1
Date :	26 juin 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	07/05/2026	Création initiale — procédure validée suite à incident Protected Users + NLA (Sprint 3)
1.1	26/06/2026	Harmonisation de la présentation des étapes et des encadrés.

1 Objet

Ce mode opératoire décrit la procédure structurée de **diagnostic d'un échec de connexion Bureau à distance** (RDP) à un serveur du domaine BTS.SIO. Il couvre les causes les plus fréquentes : compte AD verrouillé, désactivé ou expiré, restrictions liées au groupe *Protected Users*, configuration GPO NLA/TLS, droits d'ouverture de session distante, et problèmes de résolution DNS empêchant l'authentification Kerberos.

Codes d'erreur

L'erreur affichée par le client RDP est souvent générique : « *Une restriction de compte d'utilisateur vous empêche de vous connecter* ». Seule l'analyse des journaux d'événements côté serveur permet d'identifier la cause exacte.

2 Champ d'application

Public concerné	Administrateurs de l'infrastructure BTS SIO
Systèmes ciblés	DC1 (Srv2022, 10.0.112.2), DC2 (Srv2022Phy, 10.0.112.3), tout serveur Windows du domaine
Outils	PowerShell (WinRM HTTPS 5986), `ldap3` (Python), `dig`/`nslookup`, Observateur d'événements
Durée	15 à 30 minutes selon la complexité

3 Prérequis

Prérequis

- **Accès WinRM HTTPS (port 5986) à au moins un contrôleur de domaine**
- **Identifiants du compte `Administrateur` du domaine (stockés dans Vaultwarden)**
- **Accès LDAP (port 389) ou LDAPS (port 636) aux DCs**
- **Poste d'administration avec `python3`, `pywinrm`, `ldap3` et `dig` installés**

Nom de compte

Le compte d'administration du domaine s'appelle `Administrateur` (avec un A majuscule, en français). Le compte `admin` n'existe pas dans l'AD : toute tentative d'authentification avec `BTS\admin` génère une erreur `0xC0000064` (*STATUS_NO_SUCH_USER*).

4 Procédure

4.1 Collecte d'informations initiales

1 Qualifier l'incident

Avant toute investigation technique, récolter auprès de l'utilisateur :

- **Serveur cible : adresse IP ou nom d'hôte utilisé dans le client RDP**
- **Compte domaine : login exact (format `BTS\login` ou `login@bts.sio`)**
- **Temporalité : depuis quand ? Fonctionnait-il avant ?**
- **Poste client : nom du poste, adresse IP, joint au domaine ou non**
- **Message d'erreur exact : demander une capture d'écran si possible**

> **Hostnames des DCs**
>
> **Le hostname réel de DC1 est `Srv2022` (pas « DC1 »). Le hostname de DC2 est `Srv2022Phy`. Les enregistrements DNS correspondants sont `Srv2022.bts.sio` et `Srv2022Phy.bts.sio`. Le nom `DC1.bts.sio` ne résout pas dans la zone DNS.**

4.2 Vérification de l'état du compte AD

2

Interroger l'annuaire LDAP

Requêter les propriétés du compte via LDAP ou PowerShell :

```
Get-ADUser -Identity <login> -Properties Enabled, LockedOut,
    AccountExpirationDate, PasswordExpired, PasswordLastSet,
    LastLogonDate, BadLogonCount, LastBadPasswordAttempt,
    MemberOf, userAccountControl | Format-List
```

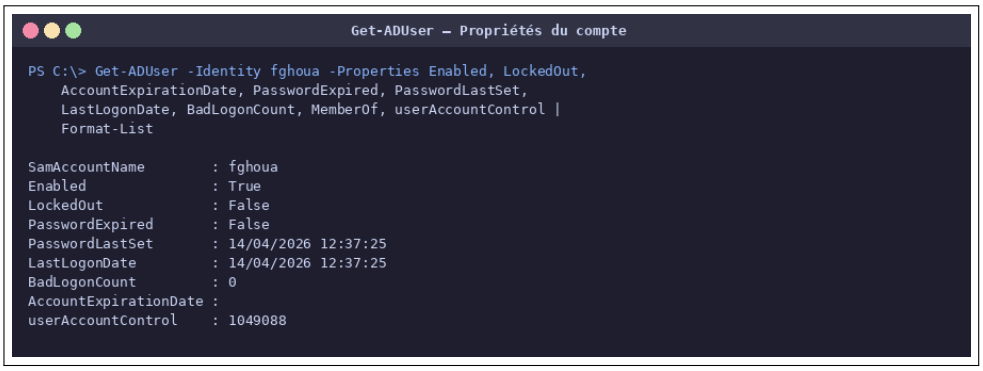

Figure 1 : Résultat de `Get-ADUser` pour le compte `fghoua` : compte actif, non verrouillé, `userAccountControl` à 1049088 (NORMAL + DONT_EXPIRE + NOT_DELEGATED).

Ou via Python `ldap3` :

```
from ldap3 import Server, Connection, NTLM, SUBTREE
import ssl
server = Server('10.0.112.2', port=389)
conn = Connection(server, user='BTS\\Administrateur',
    password='<MDP>', authentication=NTLM, auto_bind=True)
conn.search('DC=bts,DC=sio',
    '(sAMAccountName=<login>)', SUBTREE,
    attributes=['userAccountControl','lockoutTime',
    'badPwdCount','pwdLastSet','accountExpires','memberOf'])
```

3 Interpréter `userAccountControl`

Le champ `userAccountControl` est un masque binaire. Valeurs courantes :

Valeur	Signification	État
512	NORMAL_ACCOUNT	Actif
514	NORMAL_ACCOUNT + ACCOUNTDISABLE	Désactivé
66048	NORMAL + DONT_EXPIRE_PASSWD	Actif, MDP permanent
1049088	NORMAL + DONT_EXPIRE + NOT_DELEGATED	Actif, sécurisé

Si le bit `0x2` (ACCOUNTDISABLE) est présent, le compte est désactivé.

4 Vérifier le verrouillage

Si `LockedOut = True` ou `lockoutTime > 0` :

```
# Deverrouiller le compte
Unlock-ADAccount -Identity <login>
# Verifier
Get-ADUser -Identity <login> -Properties LockedOut | Select LockedOut
```

5 Vérifier l'appartenance au groupe Protected Users

C'est un point critique. Le groupe *Protected Users* interdit l'authentification NTLM :

```
Get-ADGroupMember -Identity "Protected Users" |
    Select Name, SamAccountName | Format-Table
```

Si l'utilisateur est membre de *Protected Users* et que son poste n'est pas joint au domaine, toute connexion RDP via NLA échouera systématiquement (voir MO-AD-010).

Protected Users + NLA

Lorsque NLA est activé (GPO « Securite - Restriction RDP »), le client RDP utilise CredSSP pour la pré-authentification. Si Kerberos n'est pas disponible (poste non joint au domaine, connexion par IP), CredSSP tombe en NTLM. Or *Protected Users* bloque NTLM : le DC retourne `STATUS_ACCOUNT_RESTRICTION` (`0xC000006E`). Le message affiché par le client est trompeur : « *Une restriction de compte d'utilisateur (ex. une restriction temporelle) vous empêche de vous connecter* ».

4.3 Analyse des journaux d'événements

6 **Rechercher les échecs d'authentification (Event 4625)**

Sur le DC cible, via WinRM :

```
Get-WinEvent -FilterHashtable @{
    LogName="Security"; ID=4625;
    StartTime=(Get-Date).AddHours(-2)
} -MaxEvents 20 | ForEach-Object {
    $msg = $_.Message
    $lines = $msg -split "`n"
    Write-Output "=== $($_.TimeCreated) ==="
    foreach ($l in $lines) {
        $t = $l.Trim()
        if ($t -match "^(Nom du compte|Domaine|Type
   d|Raison|Adresse|Station|Status)") {
            Write-Output "  $t"
        }
    }
```

```
}
```

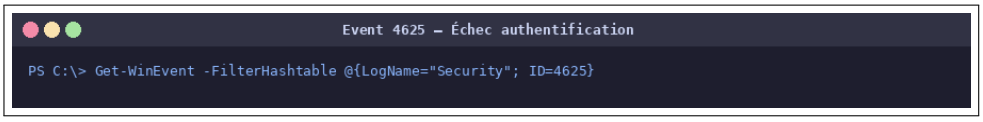

Figure 2 : Événement 4625 (échec d'authentification) remonté par le DC pour le compte `fghoua` suite à une tentative RDP bloquée.

7 Interpréter les codes NTSTATUS

Les champs `État` et `Sous-état` identifient la cause exacte :

Code	Nom	Signification
`0xC000006A`	**WRONG_PASSWORD**	**Mot de passe incorrect**
`0xC0000064`	**NO_SUCH_USER**	**Compte inexistant (`admin` au lieu de `Administrateur`)**
`0xC000006E`	**ACCOUNT_RESTRICTION**	**Protected Users bloque NTLM, ou horaires de connexion**
`0xC0000234`	**ACCOUNT_LOCKED**	**Compte verrouillé (trop de tentatives)**
`0xC0000072`	**ACCOUNT_DISABLED**	**Compte désactivé**
`0xC000006F`	**LOGON_HOURS**	**Horaires de connexion restreints**
`0xC000006D`	**LOGON_FAILURE**	**Échec générique (voir sous-état)**

8 Vérifier les événements NTLM et Kerberos

Compléter l'analyse avec les événements 4776 (validation NTLM) et 4768/4771 (Kerberos) :

```
# NTLM : event 4776
Get-WinEvent -FilterHashtable @{
    LogName="Security"; ID=4776;
    StartTime=(Get-Date).AddHours(-2)
} -MaxEvents 20 | ForEach-Object {
    Write-Output "$($_.TimeCreated) | $($_.Message.Substring(0,200))"
}

# Kerberos pre-auth failures : event 4771
Get-WinEvent -FilterHashtable @{
    LogName="Security"; ID=4771;
    StartTime=(Get-Date).AddHours(-2)
} -MaxEvents 10 -ErrorAction SilentlyContinue
```

Domaine MicrosoftAccount

Si le champ « Domaine du compte » affiche `MicrosoftAccount` au lieu de `BTS`, l'utilisateur n'a pas précisé le domaine dans sa connexion RDP. Windows 10/11 tente d'abord une authentification Microsoft Account avant le domaine AD.

4.4 Vérification des GPO et droits RDP

9 Vérifier les droits d'ouverture de session distante

La GPO « Securite - Restriction RDP » définit quels groupes sont autorisés en RDP :

```
secedit /export /cfg C:\Windows\Temp\secedit.inf /quiet
Get-Content C:\Windows\Temp\secedit.inf |
    Select-String "RemoteInteractiveLogon"
Remove-Item C:\Windows\Temp\secedit.inf
```

`SeRemoteInteractiveLogonRight = *S-1-5-32-544` signifie que seul le groupe *Administrators* (qui inclut *Domain Admins*) est autorisé. Un utilisateur non Domain Admin sera refusé même si son compte est valide.

Figure 3 : Sortie de `secedit` : le droit `SeRemoteInteractiveLogonRight` est restreint au SID `S-1-5-32-544` (groupe *Administrators*).

10 Vérifier la configuration NLA

```
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\
    Terminal Server\WinStations\RDP-Tcp" |
    Select UserAuthentication, SecurityLayer,
    MinEncryptionLevel | Format-List
```

Paramètre	Valeur	Signification
UserAuthentication	1	NLA activé (CredSSP obligatoire)
SecurityLayer	2	TLS requis
SecurityLayer	0	RDP Security (moins sécurisé, compatible Protected Users)
MinEncryptionLevel	2 ou 3	Chiffrement élevé

Figure 4 : Configuration NLA du DC : `UserAuthentication = 1` (NLA activé), `SecurityLayer = 2` (TLS), `MinEncryptionLevel = 2` (chiffrement élevé).

4.5 Vérification DNS et Kerberos

11 Tester la résolution DNS

Depuis le poste d'administration, interroger le serveur DNS utilisé par le client :

```
# Resolution du hostname du serveur cible
dig @10.0.112.2 Srv2022.bts.sio +short
# Doit repondre : 10.0.112.2

# SRV records Kerberos
dig @10.0.112.2 _kerberos._tcp.bts.sio SRV +short
# Doit repondre : srv2022.bts.sio:88 et srv2022phy.bts.sio:88

# Tester depuis le DNS du client (si different)
dig @10.0.112.20 Srv2022.bts.sio +short
```

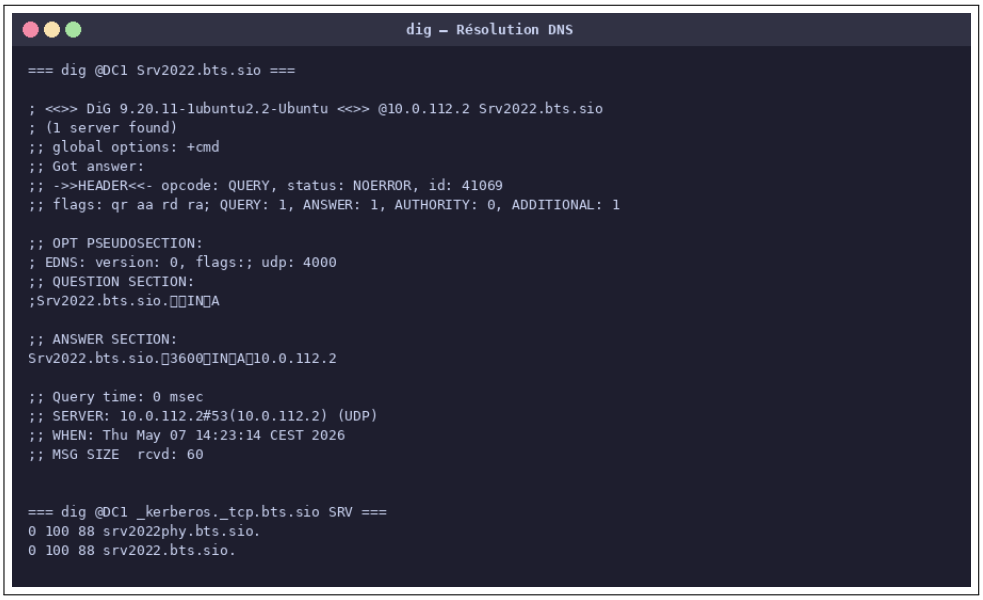

Figure 5 : Résolution DNS depuis le poste d'administration : `Srv2022.bts.sio` résout vers `10.0.112.2` et les enregistrements SRV Kerberos sont présents sur les deux DCs.

12 Vérifier si le poste client est joint au domaine

```
Get-ADComputer -Filter {Name -eq "<NOM_POSTE>"} `
    -Properties LastLogonDate, OperatingSystem |
    Format-List Name, LastLogonDate, OperatingSystem
```

Si le poste n'est pas trouvé dans l'AD, il n'est pas joint au domaine. Dans ce cas, l'authentification Kerberos est impossible et seul NTLM est disponible — ce qui est incompatible avec *Protected Users*.

Poste non joint + Protected Users

Si l'utilisateur est membre de *Protected Users* et son poste n'est pas joint au domaine, il y a deux solutions : retirer l'utilisateur du groupe *Protected Users* (voir MO-AD-010), ou joindre le poste au domaine (voir MO-AD-011).

La jonction au domaine est la solution recommandée car elle préserve le durcissement du compte.

4.6 Arbre de décision

Symptôme	Cause probable	Action
`0xC0000234`	Compte verrouillé	`Unlock-ADAccount`
`0xC0000072`	Compte désactivé	`Enable-ADAccount`
`0xC000006E` + Protected Users	NTLM bloqué par Protected Users	Retirer du groupe (MO-AD-010) ou joindre le PC au domaine (MO-AD-011)
`0xC000006E` + horaires	Horaires de connexion restreints	Vérifier `logonHours` dans l'AD
`0xC0000064`	Compte inexistant	Vérifier le login (`admin` ≠ `Administrateur`)
`0xC000006A`	Mauvais mot de passe	Réinitialiser via `Set-ADAccountPassword`
Domaine = `MicrosoftAccount`	L'utilisateur n'a pas spécifié le domaine	Utiliser `BTS\login` ou `login@bts.sio`

5 Vérification

Vérification

Après correction, valider les points suivants :

- ☐ **La connexion RDP de l'utilisateur fonctionne**
- ☐ **Le compte n'est pas reverrouillé après quelques minutes**
- ☐ **Les event logs montrent un événement 4624 (ouverture de session réussie) pour le compte concerné**

- ☐ **Si retrait de Protected Users : documenter la raison et planifier la remise en conformité**
- ☐ **La cause racine est identifiée et documentée (pas uniquement le symptôme)**

6 Rollback

Cette procédure est un **diagnostic**, elle ne modifie pas l'infrastructure de manière destructive. Les actions correctives éventuelles sont réversibles :

Action effectuée	**Retour arrière**
Déverrouillage de compte	Le compte se reverrouillera si le MDP est toujours mauvais
Retrait de Protected Users	`Add-ADGroupMember -Identity "Protected Users" -Members "<login>"`
Réinitialisation de mot de passe	L'ancien MDP n'est pas récupérable ; en informer l'utilisateur

7 Dépannage

Problème	Solution
WinRM 401 Unauthorized	Vérifier le nom de compte : utiliser `BTS\Administrateur`, pas `BTS\admin`. Le port HTTPS est 5986, pas 5985.
WinRM HTTPS timeout	Vérifier la connectivité : `Test-NetConnection 10.0.112.2 -Port 5986`. Le pare-feu du poste peut bloquer les connexions sortantes.
Event logs vides	Vérifier que l'audit est activé : GPO *Computer Configuration → Windows Settings → Security Settings → Advanced Audit Policy → Logon/Logoff → Audit Logon = Success, Failure.*
LDAP `invalidCredentials`	Le MDP `Administrateur` a peut-être été rotaté. Vérifier dans Vaultwarden (items DC1/DC2).
`DC1.bts.sio` ne résout pas	Normal : le hostname réel est `Srv2022.bts.sio`.

8 Voir aussi

— **MO-AD-001** : Administration distante des contrôleurs de domaine
— **MO-AD-005** : Santé Active Directory
— **MO-AD-010** : Gestion du groupe Protected Users
— **MO-AD-011** : Jonction d'un poste au domaine Active Directory

Références

— Microsoft — *Troubleshoot Remote Desktop connections* (documentation Windows Server)
— Microsoft — *Protected Users Security Group* (documentation Active Directory)
— Microsoft — *Network Level Authentication for Remote Desktop Services* (TechNet)
— ANSSI — *Recommandations de sécurité relatives à Active Directory*, R68 (2023)
— Audit BTS SIO — Sprint 3, incident Protected Users + NLA (mai 2026)