



12/11/2017

# Documentation Mission Déploi

[Sous-titre du document]



Fabien MAUHOURLAT  
[NOM DE LA SOCIETE]

## Mise en place de dl'infrastructure de l'hotel BORA

### Contexte :

"Le Bora Bora" dispose actuellement :

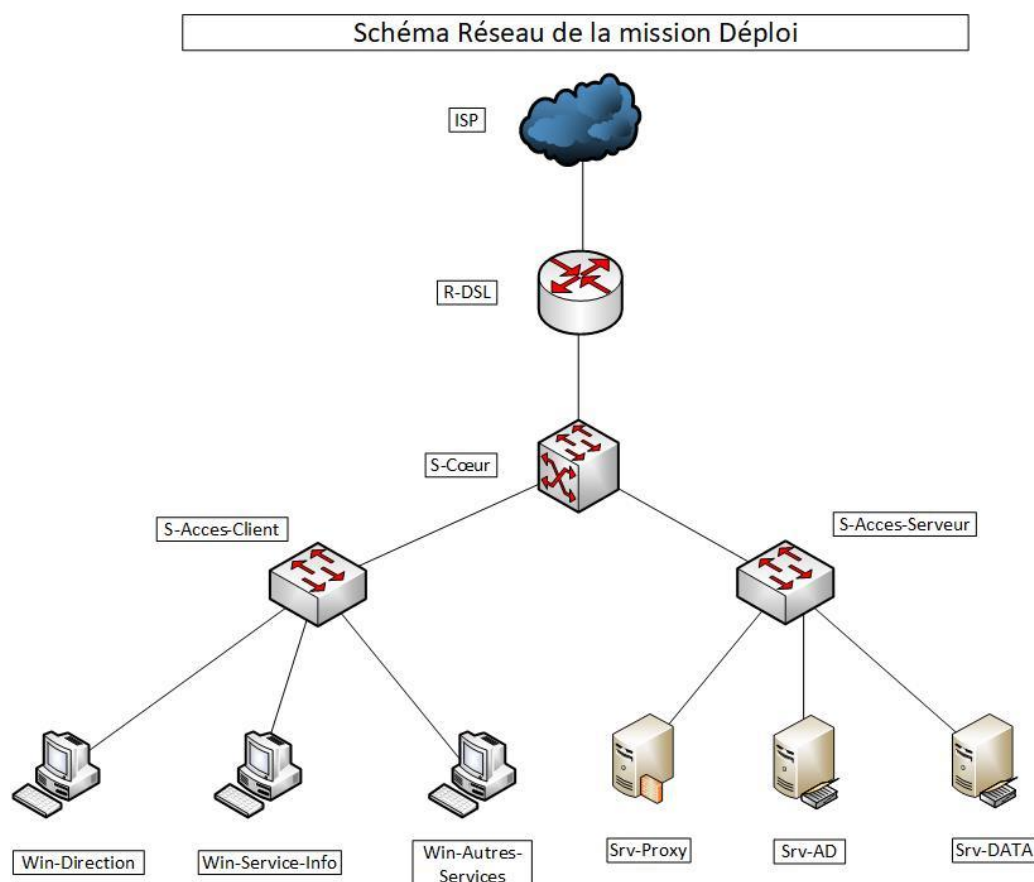
- D'un serveur Windows Active Directory srvad, d'un serveur de fichiers et de base de données sous Windows srvdata et d'un serveur linux qui gérera la sécurité (firewall, proxy) srvlinux.
- Il existe 163 utilisateurs répartis en 3 groupes, la direction, le service informatique et les reste du personnel.

Chaque groupe a un espace de travail sur srvdata.

Les différents ordinateurs n'ont pas de restriction d'accès hormis les PC de la direction et du service informatique qui ne doivent être accessibles qu'aux groupes concernés. Le service informatique doit avoir un accès à tous les ordinateurs du parc informatique (soit 3 configurations clientes différentes).

Chaque ordinateur doit être équipé d'un open office et d'un antivirus gratuit.

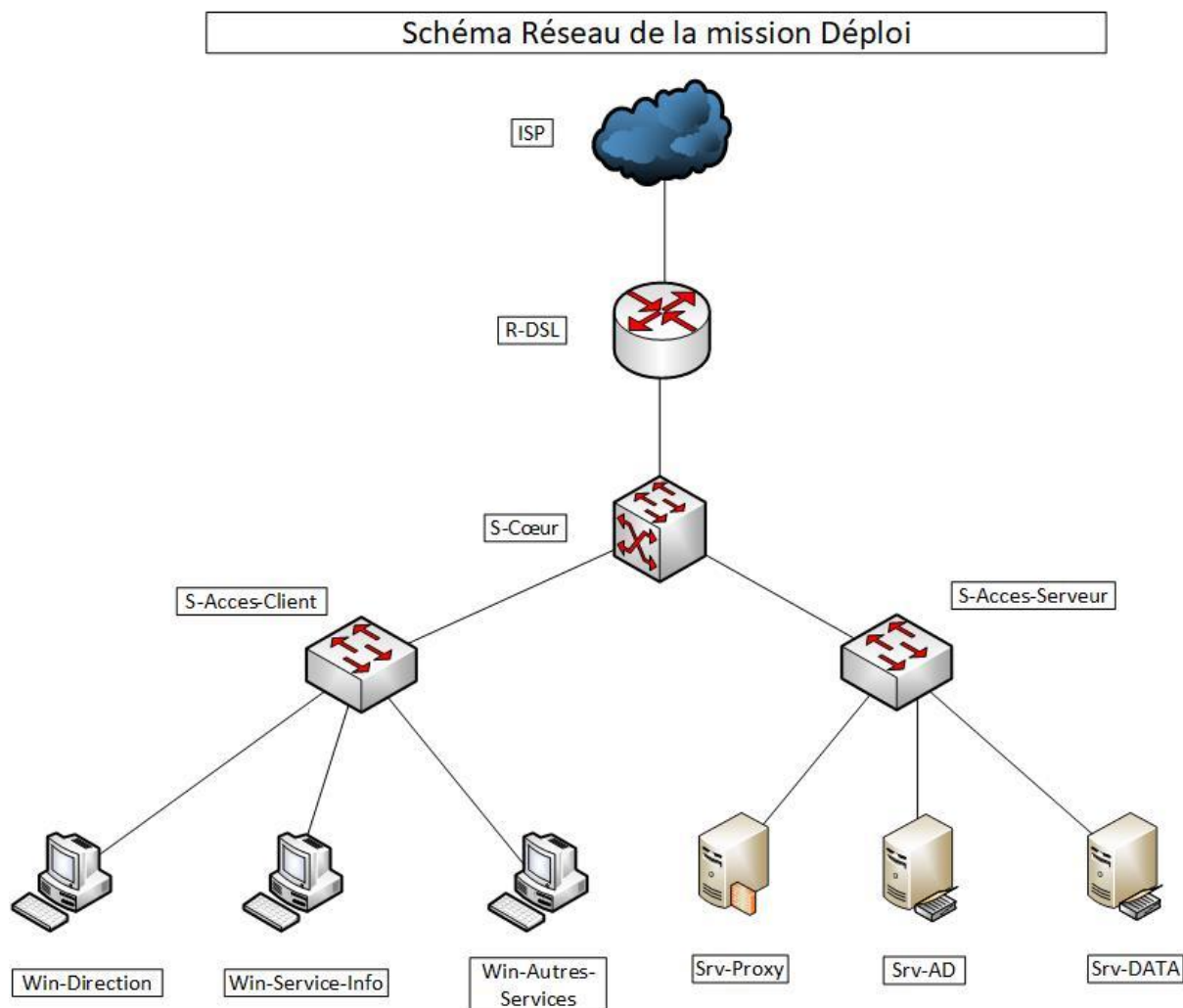
### Voici l'architecture mise en place :



## Sommaire

- I. [Schéma réseau et plan d'adressage](#)
- II. [Choix de l'infrastructure](#)
- III. [Configuration des serveurs Windows sous 2012 r2](#)
- IV. [Configuration du domaine sur SrvAD avec Powershell](#)
  - a. [Configuration du domaine sur SrvAD avec Powershell](#)
  - b. [Arborescence Domaine Bora](#)
- V. [Configuration des partages sur SrvDATA et SrvAD](#)
- VI. [Configuration des GPO](#)
  - a. [GPO qui permet de monter les lecteurs réseau à l'ouverture de session](#)
  - b. [GPO qui restreint l'accès au poste du domaine aux groupes concernés](#)
  - c. [GPO qui déploie les logiciels Avast et open office sur les machines](#)
  - d. [GPO qui paramètre le proxy automatiquement](#)
- VII. [Configuration de serveur linux Proxy](#)
  - a. [Configuration du SSH pour l'accès à distance](#)
  - b. [Configuration du proxy pour filtrer les requêtes](#)
  - c. [Configuration de la sauvegarde des logs du proxy](#)
  - d. [Configuration du pare feu avec IP tables sur le serveur Proxy](#)

## I. Schéma réseau et plan d'adressage



### 1. Table d'adressage des équipements client et serveurs

Equipement	Interface	Vlan	Adresse IP	Passerelle	DNS
Srv_AD	Ethernet 0	130	192.168.130.250/24	192.168.130.254	192.168.130.250
Srv_DATA	Ethernet 0	130	192.168.130.251/24	192.168.130.254	192.168.130.250
Srv_Squid	Ethernet 0	130	192.168.130.240/24	192.168.130.254	192.168.130.250
Win_Direction	Ethernet 0	150	192.168.150.1/24	192.168.150.254	192.168.130.250
Win_Services_Info	Ethernet 0	140	192.168.140.1/24	192.168.140.254	192.168.130.250
Win_Autres_Services	Ethernet 0	160	192.168.160.1/24	192.168.160.254	192.168.130.250

## 2. Plan d'adressage et vlan de l'infrastructure BORA

Service	Vlan	Adresses Sous-réseaux	Passerelle
Serveurs	130	192.168.130.0/24	192.168.130.254
Direction	150	192.168.150.0/24	192.168.150.254
Services-Info	140	192.168.140.0/24	192.168.140.254
Autres-services	160	192.168.160.0/24	192.168.160.254

## II. Choix de l'infrastructure

Présentation du fonctionnement des différentes branches de Windows 10 :

Avec l'arrivée de Windows 10 Microsoft utilise comme modèle le service.

Microsoft va améliorer les fonctionnalités du système avec des mises à jour de fonctionnalité 2 à 3 fois par an plutôt que de proposer un nouveau système d'exploitation tous les trois ans.

### CB : Current Branch ou phase pilote

Current Branch est la branche recevant la nouvelle build en premier. Elle aura été en amont validée par les betas testeurs grâce au programme « Windows Insider ».

### CBB : Current Branch for Business ou phase production

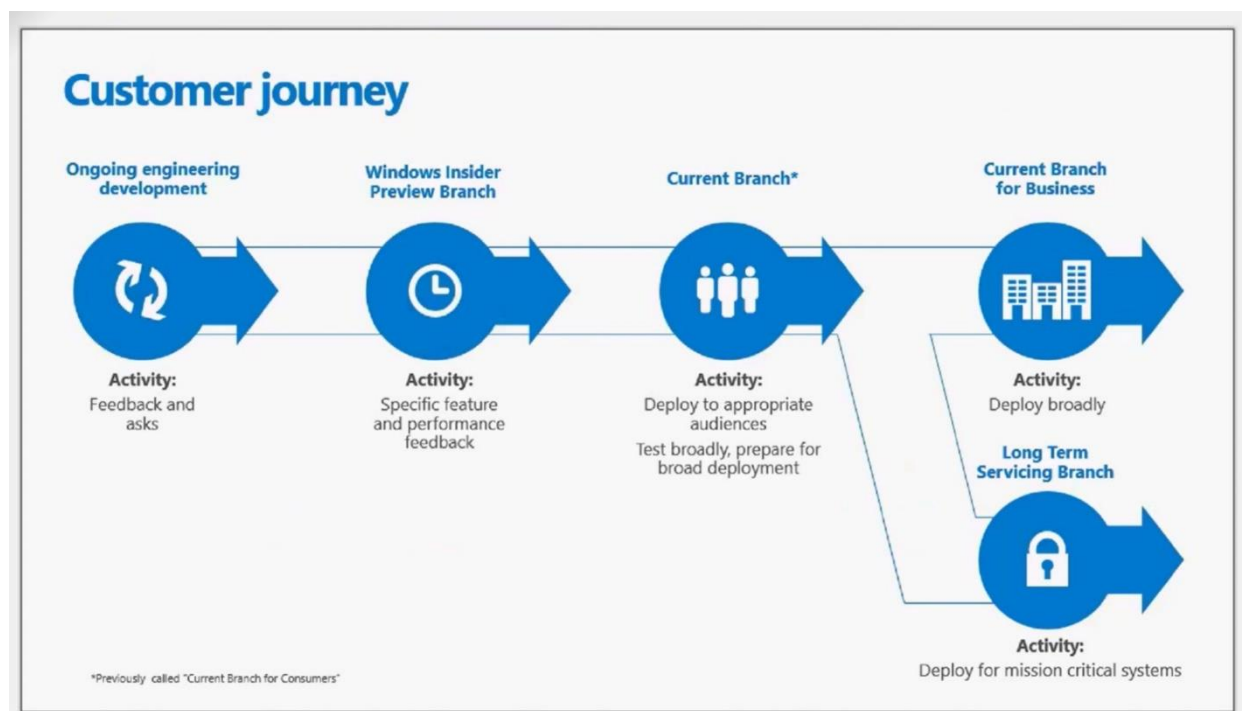
Après environ 4 mois, Microsoft annonce que la build a atteint la maturité attendue pour être déployer en entreprise. Nous recommandons nos clients d'effectuer les tests avec leurs environnements avant tout déploiement.

### LTSB : Long Term Service Branch

Enfin pour les postes critiques, la branche « Long Term service Branch » aura quant à elle un support de 10 ans. (5 ans en support standard et 5 en support étendu).

Cette version n'inclut pas le Windows Store, les Windows Universal Apps installés par défaut ainsi que Microsoft Edge.

C'est cette version qui a été choisie pour l'infrastructure grâce notamment à une meilleure stabilité du système.



Du côté des serveurs la version standard de 2012 r2 a été choisie dans la configuration de l'infrastructure du fait principalement qu'elle dispose de toutes les fonctionnalités de Windows server. La version Datacenter permet de faire de la virtualisation plus avancée mais pas nécessaire ici.

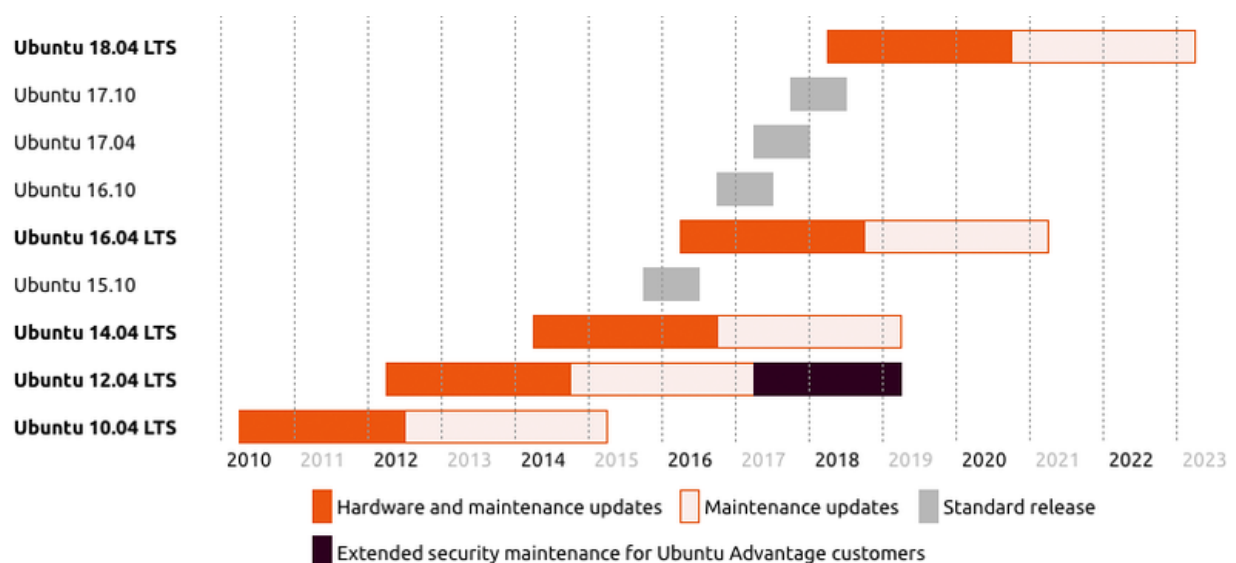


Du côté du serveur linux le choix s'est porté sur la version LTS de la version 16.04 qui est la dernière version en date.

Une version stable d'Ubuntu est publiée tous les six mois, pour les postes de travail et les serveurs.

Passés les 9 mois après la sortie de la version, une version d'Ubuntu devient alors en fin de vie (*end of life, EOL*) et ne profite plus de mises à jour de sécurité.

Une version LTS est publiée tous les deux ans au mois d'avril, sont soutenues pour une durée prolongée de 60 mois (5 ans) pour les postes de travail et les serveurs.



### III. Configuration des serveurs Windows sous 2012 r2

- Configuration de base des deux serveurs Windows

- Renommer le serveur : `Rename-Computer -NewName "nom" (shutdown /R)`
- Configurer l'autorisation du Ping dans le pare-feu : `netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol="icmpv4:8,any" dir=in action=allow`
- Configurer Windows Update pour interdire les mises à jour (sconfig) :

```
Entrez un nombre pour sélectionner une option : 5
Windows Update actuellement défini sur : Manuel
Sélectionner les mises à jour (a)utomatiques ou (m)anuelles : m
Désactivation des mises à jour automatiques...
```

- Activer le Bureau à distance pour les connexions sécurisées (scconfig) :

```
Entrez un nombre pour sélectionner une option : 7
(A)ctiver ou (D)ésactiver le Bureau à distance ? (Vide=Annuler) A
1) Autoriser seulement les clients exécutant le Bureau à distance avec authentification NLA (plus sécurisé)
2) Autoriser les clients exécutant n'importe quelle version du Bureau à distance (moins sécurisé)
Entrez la sélection : 1
Activation du Bureau à distance...
```

- Voici la configuration finale :

```
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. Tous droits réservés.

Inspection en cours du système...

=====
Configuration du serveur
=====

1) Domaine ou groupe de travail :          Domaine:  bora.nc
2) Nom d'ordinateur :                      SRVAD
3) Ajouter l'administrateur local
4) Configurer l'administration à distance  Activé
5) Paramètres de Windows Update :          Manuel
6) Télécharger et installer les mises à jour
7) Bureau à distance :                     Activé (clients plus sécurisés seulement)
```



## Configuration de SrvAD

Propriétés de : Protocole Internet version 4 (TCP/IPv4) [X]

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 0 . 253

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 192 . 168 . 0 . 254

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 127 . 0 . 0 . 1

Serveur DNS auxiliaire : 192 . 168 . 0 . 252

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

## Configuration de SrvDATA

Propriétés de : Protocole Internet version 4 (TCP/IPv4) [X]

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 0 . 252

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 192 . 168 . 0 . 254

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 192 . 168 . 0 . 253

Serveur DNS auxiliaire : 127 . 0 . 0 . 1

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

- Voici la configuration finale des deux serveurs SrvAD et SrvDATA

Tableau de bord

Serveur local

Tous les serveurs

AD DS

DNS

Services de fichiers et d... ▶

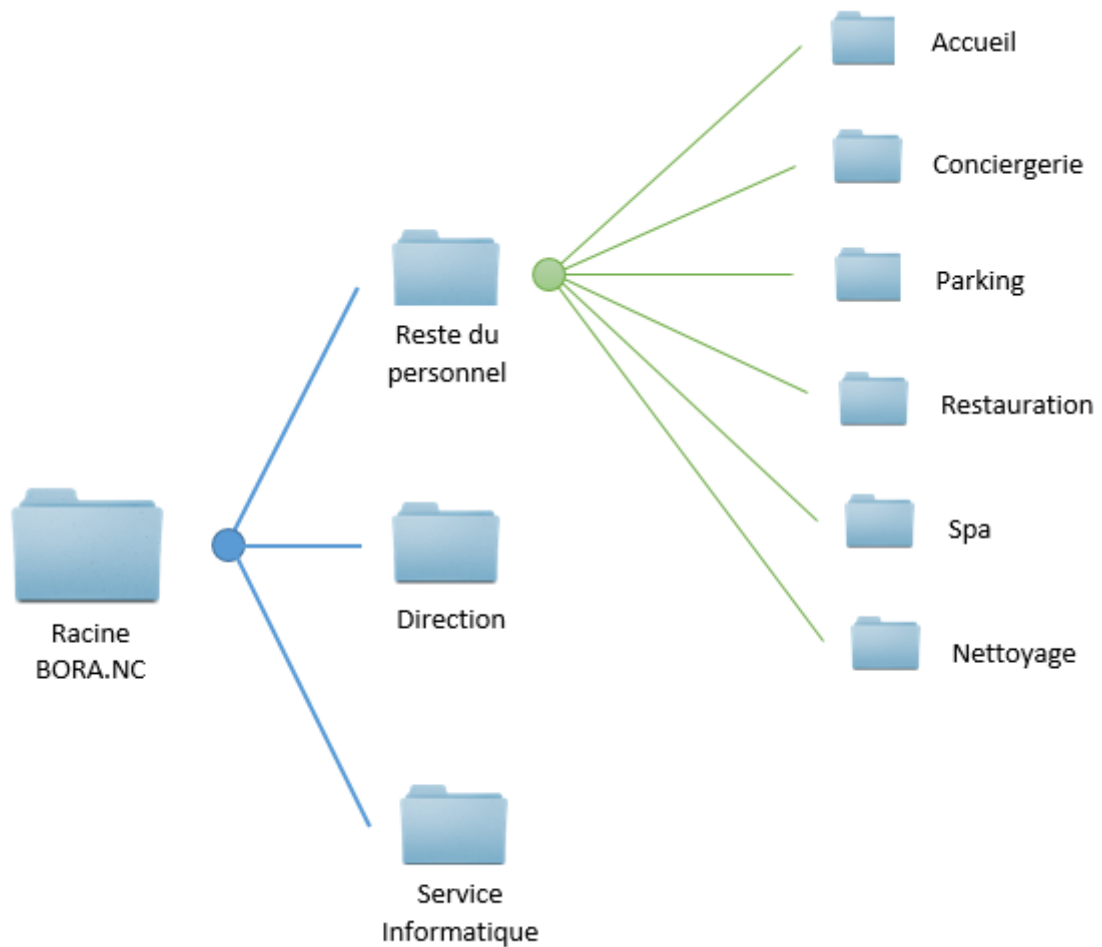
PROPRIÉTÉS

Pour SrvAD

TÂCHES ▼

Nom de l'ordinateur	SrvAD	Dernières mises à jour installées	Jamais
Domaine	bora.nc	Windows Update	Ne jamais rechercher de mises à jour
		Dernière recherche de mises à jour :	Jamais
Pare-feu Windows	Public : Actif	Rapport d'erreurs Windows	Inactif
Gestion à distance	Activé	Programme d'amélioration de l'expérience utilisateur	Non participant
Bureau à distance	Activé	Configuration de sécurité renforcée d'Internet Explorer	Actif
Association de cartes réseau	Activé	Fuseau horaire	(UTC+11:00) Îles Salomon, Nouvelle-Calédonie
SrvAD	192.168.0.253, Compatible IPv6	ID de produit (Product ID)	Non activé
Version du système d'exploitation	Microsoft Windows Server 2012 R2 Standard	Processeurs	Intel(R) Core(TM) i7-5700HQ CPU @ 2.70GHz
Informations sur le matériel	VMware, Inc. VMware Virtual Platform	Mémoire installée (RAM)	2 Go
		Espace disque total	60 Go

## Arborescence Domaine Bora



## IV. Configuration du domaine sur SrvAD avec Powershell

- Ajout du rôle ADDS avec la console PowerShell :
  - `Add-WindowsFeature AD-Domain-Services -IncludeAllSubFeature -Restart`
- Ajout des outils d'administration à distance RSAT :
  - `Add-WindowsFeature RSAT-AD-Tools -IncludeAllSubFeature -Restart`

```

Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. Tous droits réservés.

PS C:\Windows\system32> Add-WindowsFeature AD-Domain-Services -IncludeAllSubFeature -Restart

Success Restart Needed Exit Code      Feature Result
-----
True      No      Success      {Services AD DS, Outils d'administration d...
AVERTISSEMENT : La fonctionnalité Mises à jour automatiques de Windows n'est pas activée. Pour garantir que votre rôle
ou fonction récemment installé est automatiquement mis à jour, activez Windows Update.

PS C:\Windows\system32> Add-WindowsFeature RSAT-AD-Tools -IncludeAllSubFeature -Restart

Success Restart Needed Exit Code      Feature Result
-----
True      No      Success      {Centre d'administration Active Directory,...
AVERTISSEMENT : La fonctionnalité Mises à jour automatiques de Windows n'est pas activée. Pour garantir que votre rôle
ou fonction récemment installé est automatiquement mis à jour, activez Windows Update.

PS C:\Windows\system32>

```

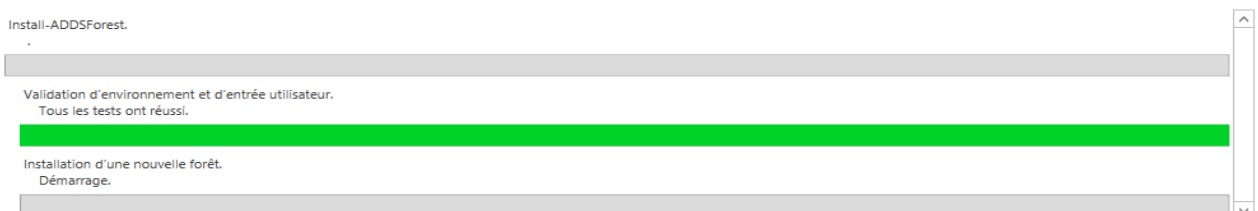
- Ensuite il faut promouvoir le contrôleur de domaine en créant le domaine bora.nc à l'aide d'un script PowerShell

```

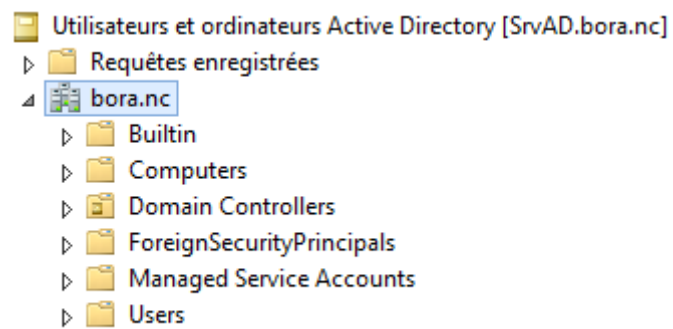
PowerShell création Domaine AD - Copie.ps1 X
1  #
2  # script windows PowerShell pour le déploiement d'AD DS
3  #
4
5  Import-Module ADDSDeployment
6  Install-ADDSForest `
7  -CreateDnsDelegation:$false `
8  -DatabasePath "C:\windows\NTDS" `
9  -DomainMode "win2012R2" `
10 -DomainName "bora.nc" `
11 -DomainNetbiosName "BORA" `
12 -ForestMode "win2012R2" `
13 -InstallDns:$true `
14 -LogPath "C:\windows\NTDS" `
15 -NoRebootOnCompletion:$false `
16 -SysvolPath "C:\windows\SYSVOL" `
17 -Force:$true
18
19

```

- L'installation s'effectue automatiquement :



- Pour vérifier que Le domaine a bien été créé il suffit de se rendre dans la console Utilisateur et ordinateur Active Directory



## Création des utilisateurs sur le domaine BORA avec Powershell

- La création des utilisateurs se fait grâce à un script qui importe des fichiers csv.  
Pour créer ces fichiers nous allons utiliser Excel avec plusieurs Feuille de calcul qui répartit les utilisateurs des différents groupes.

	A	B	C	D	E	F	G	H
1	Name	Surname	GivenName	SAMAccountName				
2	BOUCHETIERE Bastien	Bastien	BOUCHETIER	bbouchetiere				
3	BERNARD Dilhan	Dilhan	BERNARD	dbernard				
4	ENOKA Stecy	Stecy	ENOKA	senoka				
5	FANDOUX Louis	Louis	FANDOUX	lfandoux				
6	JACQUEMET Delphine	Delphine	JACQUEMET	djacquemet				
7	LAFARGUE Jerome	Jerome	LAFARGUE	jlafargue				
8	LEONARD Clement	Clement	LEONARD	cleonard				
9	LEPEU Paule-Emmanuelle	Paule-Emma	LEPEU	plepeu				
10	MONEFARA Brenda	Brenda	MONEFARA	bmonefara				
11	NGUYEN Ductam	Ductam	NGUYEN	dnguyen				
12	NGUYEN Steven	Steven	NGUYEN	snguyen				
13	OBRY Ilona	Ilona	OBRY	iobry				
14	POIRCUITTE Dephny	Dephny	POIRCUITTE	dpoircuitte				
15	POITCHILI Leopold	Leopold	POITCHILI	lpoitchili				
16	VIVANCOS Thomas	Thomas	VIVANCOS	tvivancos				
17	WETE Isaac	Isaac	WETE	iwete				
18	Abitong Jonas	Jonas	Abitong	jabitong				
19	Abke Jonathan	Jonathan	Abke	jabke				
20	Abkemeier Jonathon	Jonathon	Abkemeier	jabkemeier				
21	Ablang Jone	Jone	Ablang	jablang				
22								
23								
<div> <div> <div></div> <div></div> </div> <div> <div>Accueil</div> <div>Conciergerie</div> <div>Parkings</div> <div>Restauration</div> <div>Spa</div> <div>Direction</div> <div>Nettoyage</div> <div>Informaticiens</div> </div> </div>								

- Une macro va permettre après avoir entré le nom dans la colonne A de remplir automatiquement les autres colonnes puis d'exporter les feuilles de calcul en fichier csv différents.

```

Utilisateur.xlsm - Module1 (Code)
(Général) Splitfunc

Sub Splitfunc()

    Dim nbLignes As Integer
    Dim Current As Worksheet
    For Each Current In Worksheets
        Sheets(Current.Name).Select
        Range("A2").Select
        nbLignes = Range("A2", Selection.End(xlDown)).Cells.Count
        For i = 1 To nbLignes
            cell = Sheets(Current.Name).Cells(i + 1, 1).Value
            coupe = Split(cell, " ")
            coupesam = Left(coupe(1), 1)
            Worksheets(Current.Name).Cells(i + 1, 2) = coupe(1)
            Worksheets(Current.Name).Cells(i + 1, 3) = coupe(0)
            Worksheets(Current.Name).Cells(i + 1, 4) = LCase(coupesam) & LCase(coupe(0))
        Next
    Next
    Dim Plage As Object, oL As Object, oC As Object, Tmp As String
    Dim NomEtCheminFichier As String
    For Each Current In Worksheets
        Sheets(Current.Name).Select
        NomEtCheminFichier = Current.Name & ".csv"
        Plage1 = ActiveSheet.Range("A" & Rows.Count).End(xlUp).Row
        Set Plage2 = ActiveSheet.Range("A1:D" & Plage1)
        Plage2.Copy
        Workbooks.Add
        ActiveSheet.Paste
        Application.CutCopyMode = False
        Application.DisplayAlerts = False
        ActiveWorkbook.SaveAs Filename:=NomEtCheminFichier, FileFormat:=xlCSV, CreateBackup:=False
        ActiveWindow.Close
        Application.DisplayAlerts = True
    Next
End Sub








```

- Remplissage automatique des autres colonnes :

	A	B	C	D
1	Name	Surname	GivenName	SAMAccountName
2	MAUHOURAT Fabien			
3	DESAINTGILLES Remi			
4	FRETAY Vetea			
5	LEGER Roderik			
6				

	A	B	C	D
1	Name	Surname	GivenName	SAMAccountName
2	MAUHOURLAT Fabien	Fabien	MAUHOURLAT	fmauhourat
3	DESAINTGILLES Remi	Remi	DESAINTGILLES	rdesaintgilles
4	FRETAY Vetea	Vetea	FRETAY	vfretay
5	LEGER Roderik	Roderik	LEGER	rleger
6				

- Les feuilles de calcul sont exportées dans différents fichiers au format csv

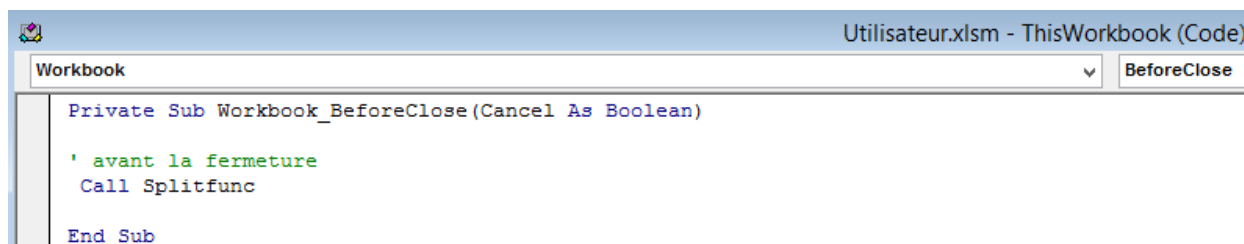
 Accueil.csv	05/04/2017 09:32	Fichier CSV Micro...	1 Ko
 AD PPE Deploi.ps1	05/04/2017 10:47	Fichier PS1	6 Ko
 Conciergerie.csv	05/04/2017 09:32	Fichier CSV Micro...	1 Ko
 Direction.csv	05/04/2017 09:32	Fichier CSV Micro...	1 Ko
 Informaticiens.csv	05/04/2017 09:32	Fichier CSV Micro...	1 Ko
 Nettoyage.csv	05/04/2017 09:32	Fichier CSV Micro...	3 Ko
 Parkings.csv	05/04/2017 09:32	Fichier CSV Micro...	1 Ko
 Restauration.csv	05/04/2017 09:32	Fichier CSV Micro...	2 Ko
 Spa.csv	05/04/2017 09:32	Fichier CSV Micro...	1 Ko
 Utilisateur.xlsm	05/04/2017 14:14	Feuille de calcul ...	36 Ko

- Le fichier csv sépare les colonnes du fichier Excel avec des virgules

1	Name,Surname,GivenName,SAMAccountName
2	BOUCHETIERE Bastien ,Bastien,BOUCHETIERE,bbouchetiere
3	BERNARD Dilhan,Dilhan,BERNARD,dbernard
4	ENOKA Stecy,Stecy,ENOKA,senoka
5	FANDOUX Louis,Louis,FANDOUX,lfandoux
6	JACQUEMET Delphine,Delphine,JACQUEMET,djacquemet
7	LAFARGUE Jerome,Jerome,LAFARGUE,jlafargue
8	LEONARD Clement,Clement,LEONARD,cleonard
9	LEPEU Paule-Emmanuelle,Paule-Emmanuelle,LEPEU,plepeu
10	MONEFARA Brenda,Brenda,MONEFARA,bmonefara
11	NGUYEN Ductam,Ductam,NGUYEN,dnguyen
12	NGUYEN Steven,Steven,NGUYEN,snguyen
13	OBRY Ilona,Ilona,OBRY,iobry
14	POIRCUITTE Dephny,Dephny,POIRCUITTE,dpoircuitte
15	POITCHILI Leopold,Leopold,POITCHILI,lpoitchili
16	VIVANCOS Thomas,Thomas,VIVANCOS,tvivancos
17	WETE Isaac,Isaac,WETE,iwete
18	Abitong Jonas,Jonas,Abitong,jabitong
19	Abke Jonathan,Jonathan,Abke,jabke
20	Abkemeier Jonathon,Jonathon,Abkemeier,jabkemeier
21	Ablang Jone,Jone,Ablang,jablang
22	



- Pour que la macro s'exécute à la fermeture du fichier Excel il faut ajouter cette ligne dans le workbook :
  - Call suivi du nom de la fonction

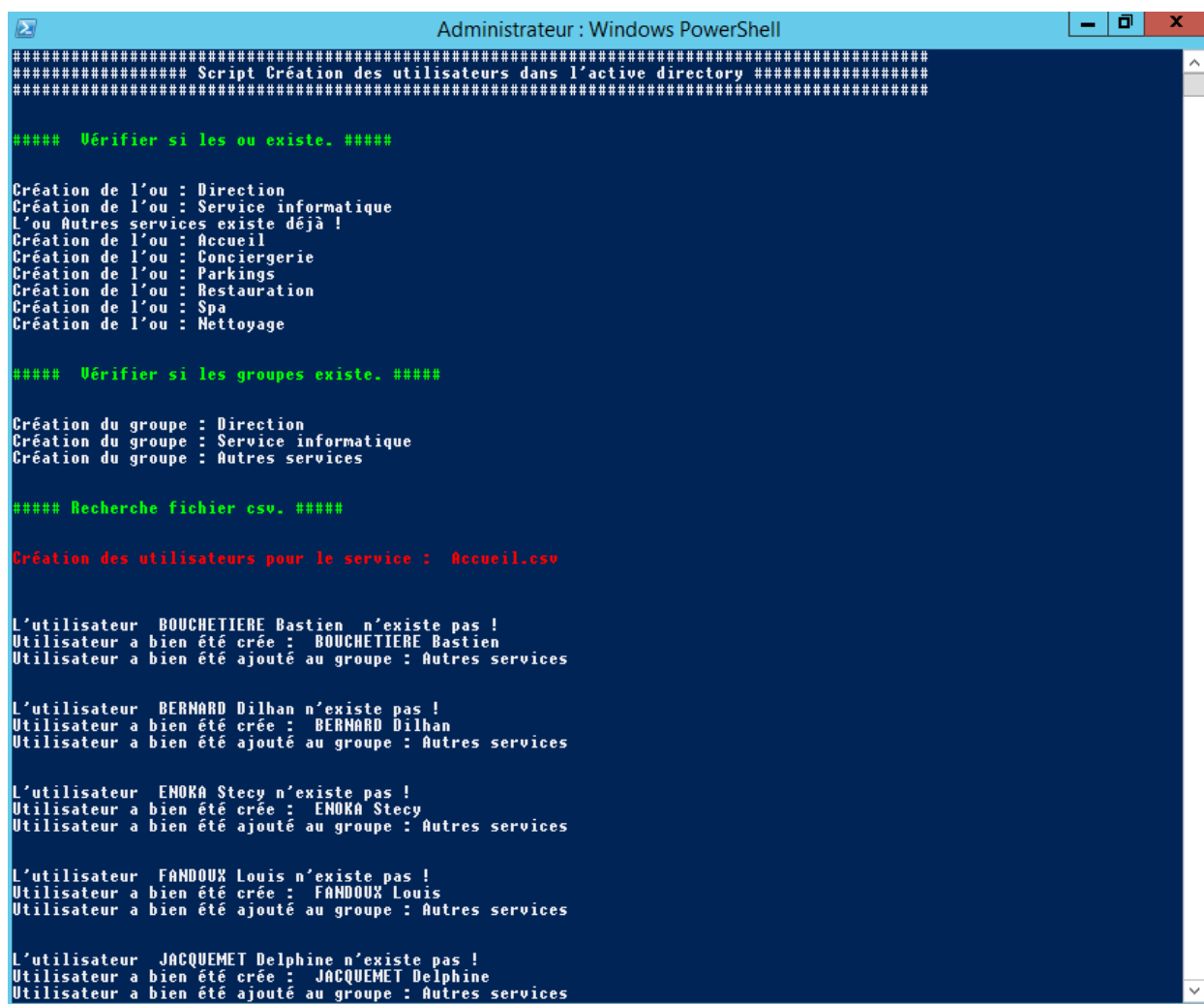


The screenshot shows the VBA editor for 'Utilisateur.xlsm - ThisWorkbook (Code)'. The 'Workbook' dropdown is selected, and the 'BeforeClose' event is chosen. The code is as follows:

```
Private Sub Workbook_BeforeClose(Cancel As Boolean)

    ' avant la fermeture
    Call Splitfunc

End Sub
```



The screenshot shows a Windows PowerShell window titled 'Administrateur : Windows PowerShell'. It displays the output of a script for creating users and groups in Active Directory. The script includes sections for verifying the existence of users, groups, and files, and then creating them if they do not exist.

```
##### Script Création des utilisateurs dans l'active directory #####

#### Vérifier si les ou existe. ####

Création de l'ou : Direction
Création de l'ou : Service informatique
L'ou Autres services existe déjà !
Création de l'ou : Accueil
Création de l'ou : Conciergerie
Création de l'ou : Parkings
Création de l'ou : Restauration
Création de l'ou : Spa
Création de l'ou : Nettoyage

#### Vérifier si les groupes existe. ####

Création du groupe : Direction
Création du groupe : Service informatique
Création du groupe : Autres services

#### Recherche fichier csv. ####

Création des utilisateurs pour le service : Accueil.csv

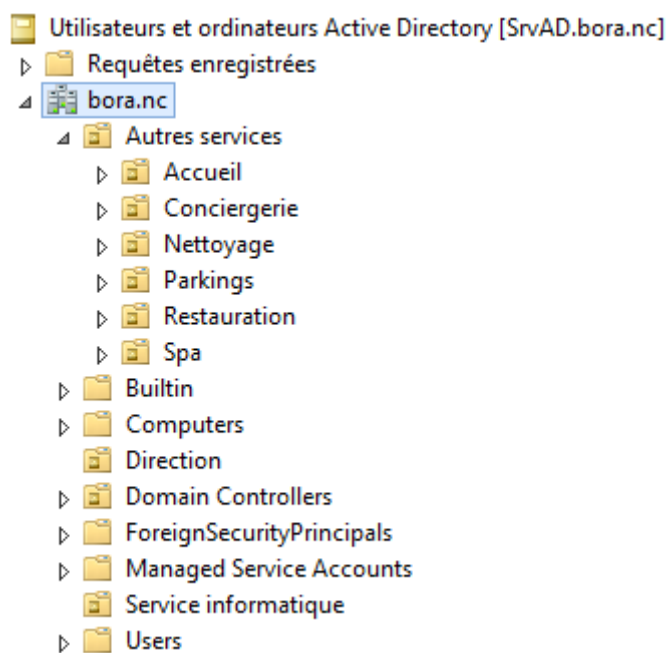
L'utilisateur BOUCHETIERE Bastien n'existe pas !
Utilisateur a bien été crée : BOUCHETIERE Bastien
Utilisateur a bien été ajouté au groupe : Autres services

L'utilisateur BERNARD Dilhan n'existe pas !
Utilisateur a bien été crée : BERNARD Dilhan
Utilisateur a bien été ajouté au groupe : Autres services

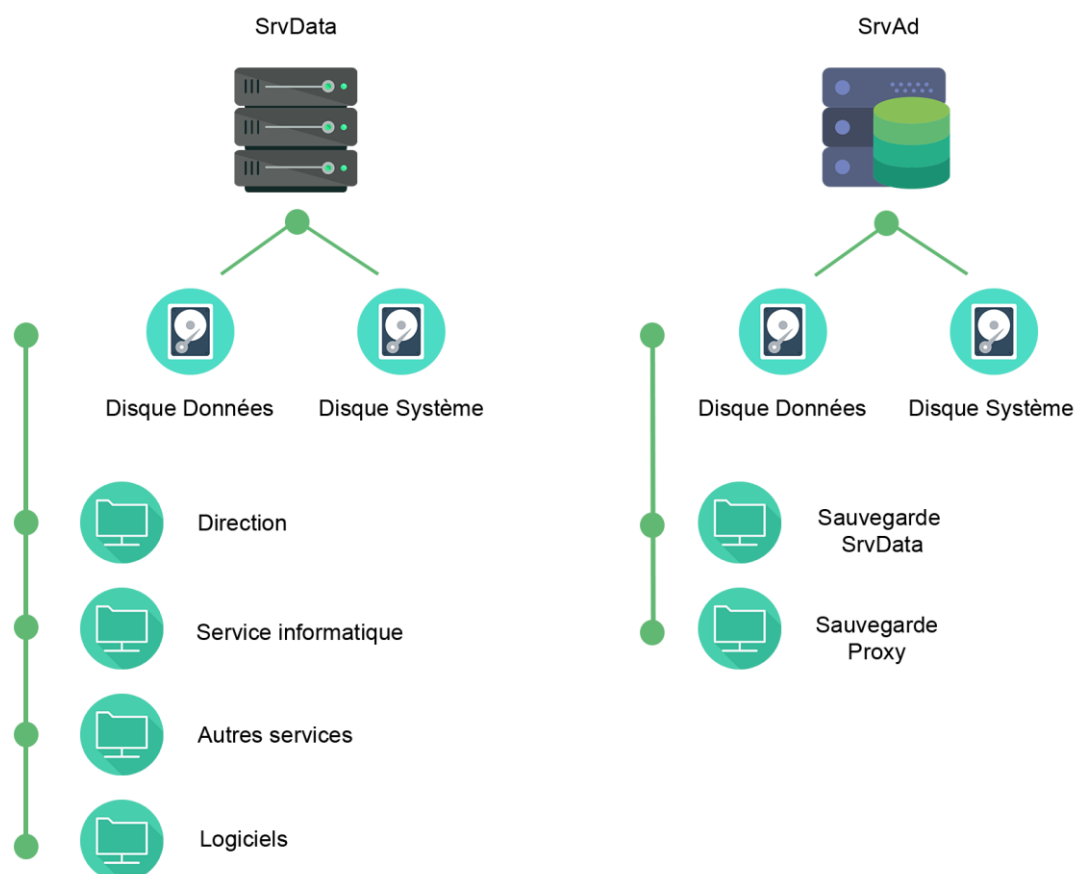
L'utilisateur ENOKA Stecy n'existe pas !
Utilisateur a bien été crée : ENOKA Stecy
Utilisateur a bien été ajouté au groupe : Autres services

L'utilisateur FANDOUX Louis n'existe pas !
Utilisateur a bien été crée : FANDOUX Louis
Utilisateur a bien été ajouté au groupe : Autres services

L'utilisateur JACQUEMET Delphine n'existe pas !
Utilisateur a bien été crée : JACQUEMET Delphine
Utilisateur a bien été ajouté au groupe : Autres services
```

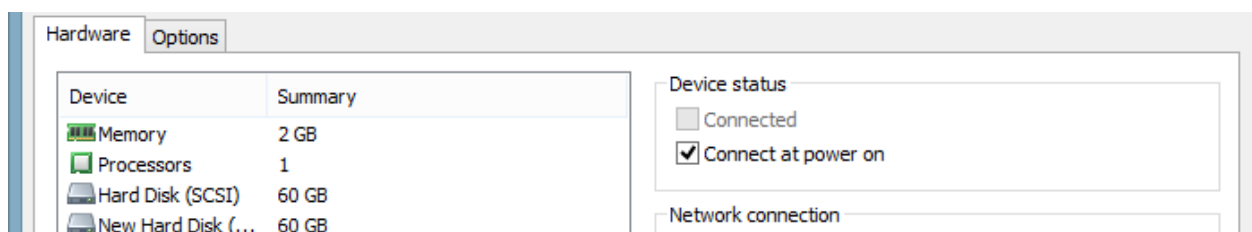


## V. Configuration des partages sur SrvDATA et SrvAD

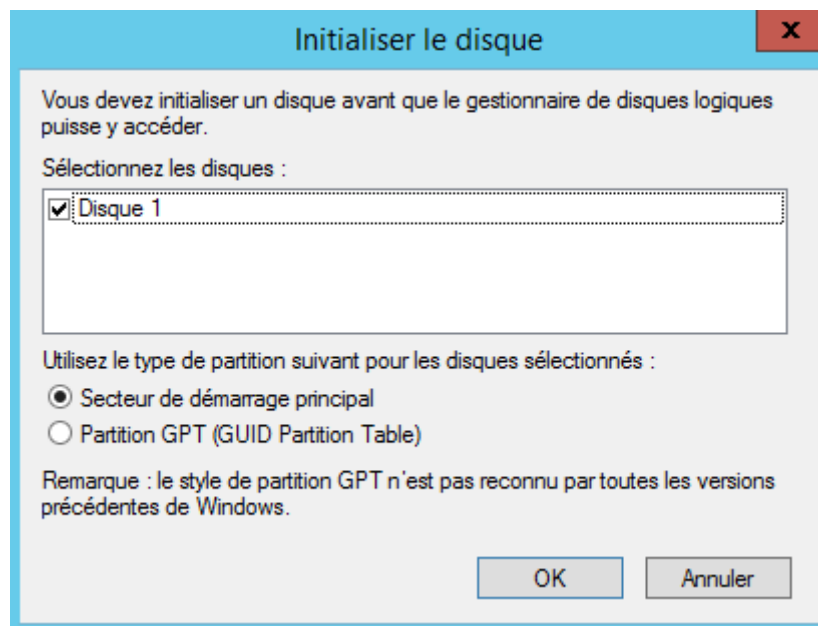


### Arborescence des partages

- Il est nécessaire d'avoir au préalable ajouter un disque dur en plus sur chaque serveur



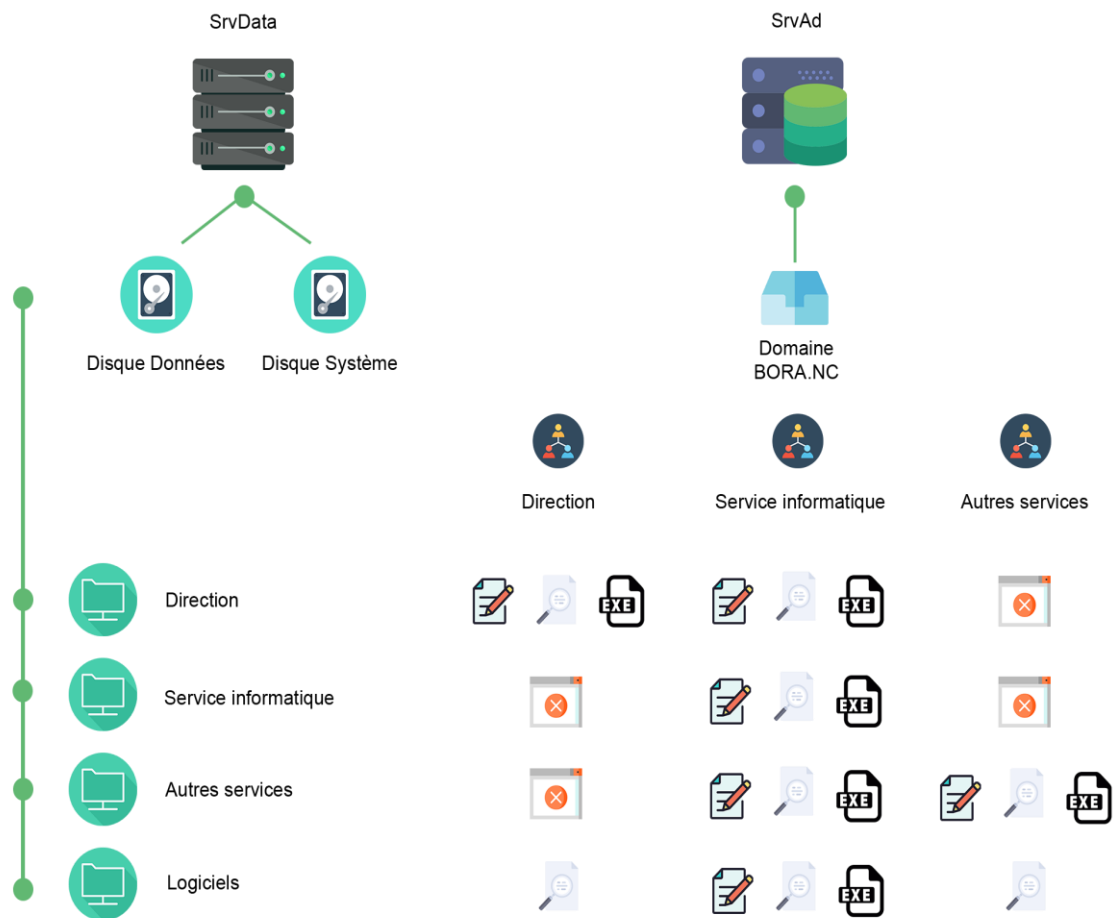
- Il faut initialiser le disque puis le formater à l'aide de l'utilitaire Gestion des disques sous Windows



- Ensuite notre deuxième disque apparait dans l'explorateur

#### ⚡ Périphériques et lecteurs (3)





- L'arborescence ainsi que les permissions sont créés à l'aide d'un script PowerShell
  - Le script va d'abord vérifier si les dossiers existent et si ce n'est pas le cas il va les créer
  - Ensuite il va ajouter les permissions pour chaque groupe sur tous les dossiers de la racine du lecteur E :

Administrateur : Windows PowerShell

```
Création des Dossier

Répertoire : E:\

Mode                LastWriteTime         Length Name
----                -
d-----          05/04/2017    22:57         Direction
Direction a été partagé.
d-----          05/04/2017    22:57      Service Informatique
Service-Informatique a été partagé.
d-----          05/04/2017    22:57      Autres services
Autres-services a été partagé.
d-----          05/04/2017    22:57         Logiciel
Logiciel a été partagé.

Application des permissions

Autres services
Application des droits sur le dossier Autres services

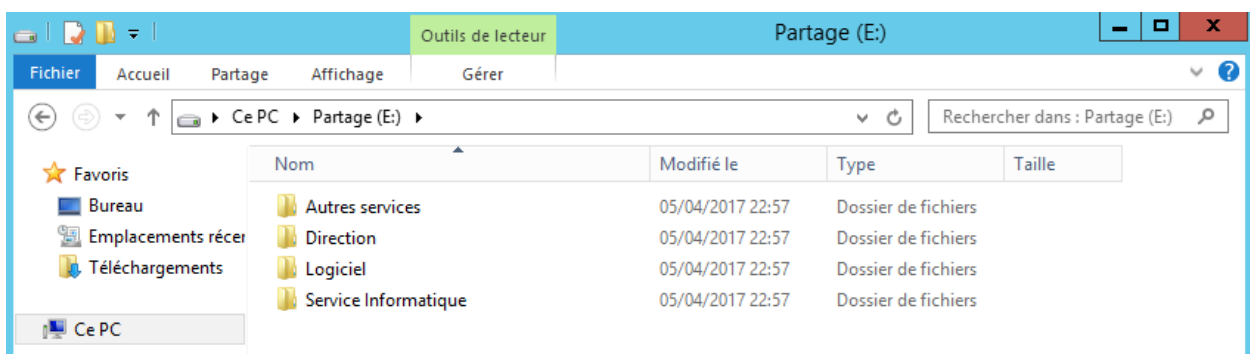
Direction
Application des droits sur le dossier Direction

Logiciel
Application des droits sur le dossier Logiciel

Service Informatique
Application des droits sur le dossier Service Informatique

Cliquez sur Entrée pour continuer....: _
```

- L'arborescence des dossiers à la racine du lecteur E :



- Vérification des droits sur les dossiers Partagés avec la commande :

```
Get-Acl | Select path -expand Access | Format-Table -Wrap -AutoSize -Property
IdentityReference,FileSystemRights,AccessControlType,Path
```

```
PS E:\> Get-Acl -Path '.\Autres services' | Select Path -expand
Reference,FileSystemRights,AccessControlType
```

IdentityReference	FileSystemRights	AccessControlType
BORA\Direction	FullControl	Deny
BUILTIN\Administrateurs	FullControl	Allow
BORA\Service informatique	FullControl	Allow
BORA\Autres services	FullControl	Allow

```
PS E:\> Get-Acl -Path .\Direction | Select Path -expand Access
e,FileSystemRights,AccessControlType
```

IdentityReference	FileSystemRights	AccessControlType
BORA\Autres services	FullControl	Deny
BUILTIN\Administrateurs	FullControl	Allow
BORA\Direction	FullControl	Allow
BORA\Service informatique	FullControl	Allow

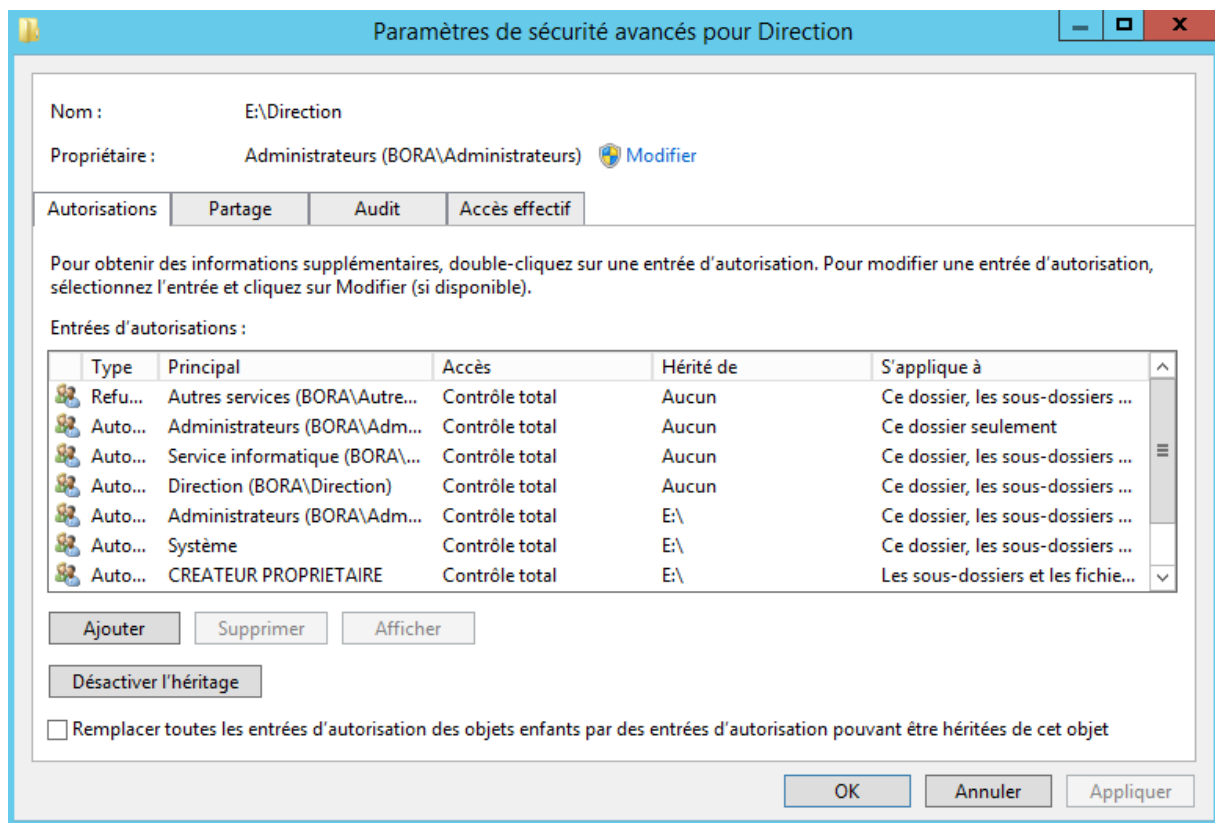
```
PS E:\> Get-Acl -Path '.\Service Informatique' | Select Path -ex
ntityReference,FileSystemRights,AccessControlType
```

IdentityReference	FileSystemRights	AccessControlType
BORA\Direction	FullControl	Deny
BORA\Autres services	FullControl	Deny
BUILTIN\Administrateurs	FullControl	Allow
BORA\Service informatique	FullControl	Allow

```
PS E:\> Get-Acl -Path .\Logiciels | Select Path -expand Access
e,FileSystemRights,AccessControlType
```

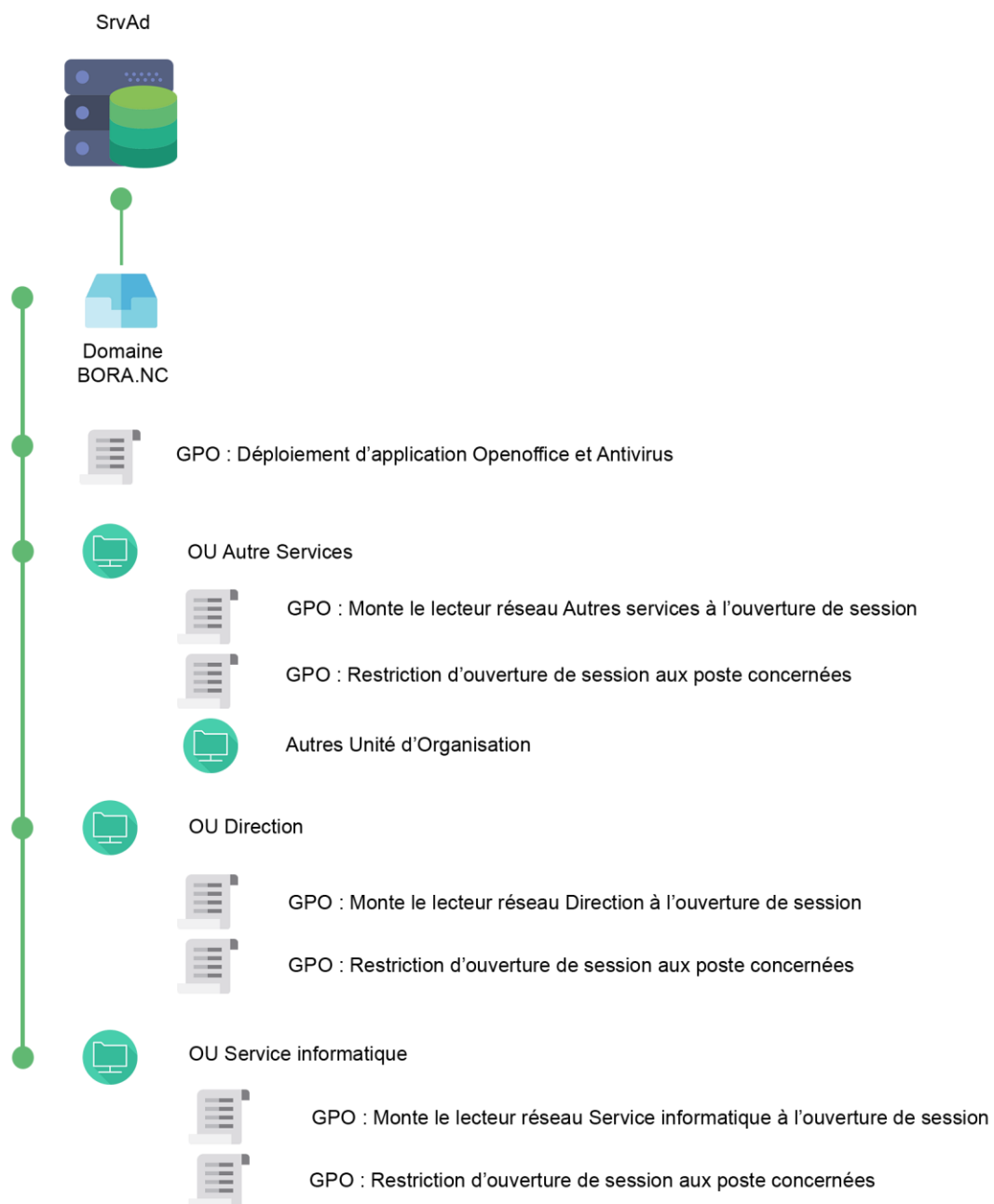
IdentityReference	FileSystemRights	AccessControlType
BUILTIN\Administrateurs	FullControl	Allow
BORA\Direction	Read, Synchronize	Allow
BORA\Service informatique	FullControl	Allow
BORA\Autres services	Read, Synchronize	Allow

- Désactivation de l'héritage des dossiers



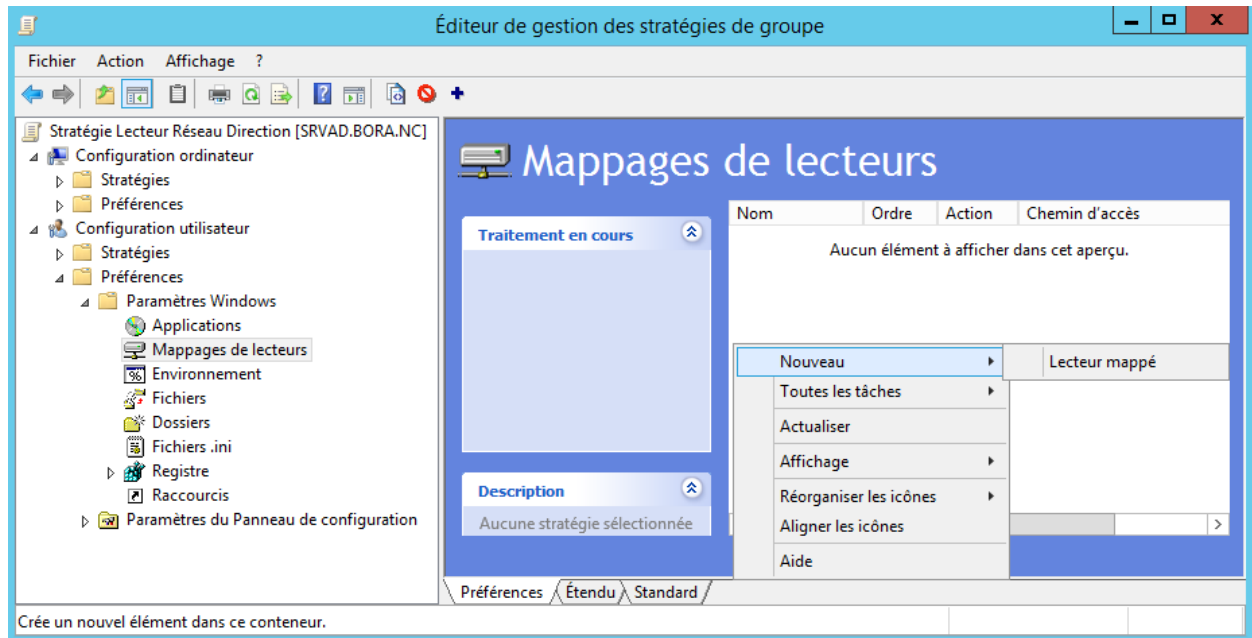


## VI. Configuration des GPO



## GPO qui va permettre de monter les lecteurs réseau à l'ouverture de session

- Il faut créer une GPO pour chaque groupe du domaine BORA (Direction, Autres Services et le service info)



- Créer le lecteur réseau
  - Spécifier l'emplacement et le libellé et la lettre de lecteur à utiliser
  - Ne pas oublier d'afficher ce lecteur

**Action :** Créer

**Emplacement :** \\SrvDATA\Direction

**Reconnecter :** ☒ **Libeller en tant que :** Direction

**Lettre de lecteur**

☐ Utiliser le premier disponible, en commençant à : ☐ Utiliser : Z

**Se connecter en tant que (facultatif)**

Nom d'utilisateur :

Mot de passe :  Confirmer le mot de passe :

**Masquer/Afficher ce lecteur**

☐ Aucune modification  
☐ Masquer ce lecteur  
☒ Afficher ce lecteur

**Masquer/Afficher tous les lecteurs**

☒ Aucune modification  
☐ Masquer tous les lecteurs  
☐ Afficher tous les lecteurs

## GPO qui va restreindre l'accès au poste du domaine aux groupes concernés

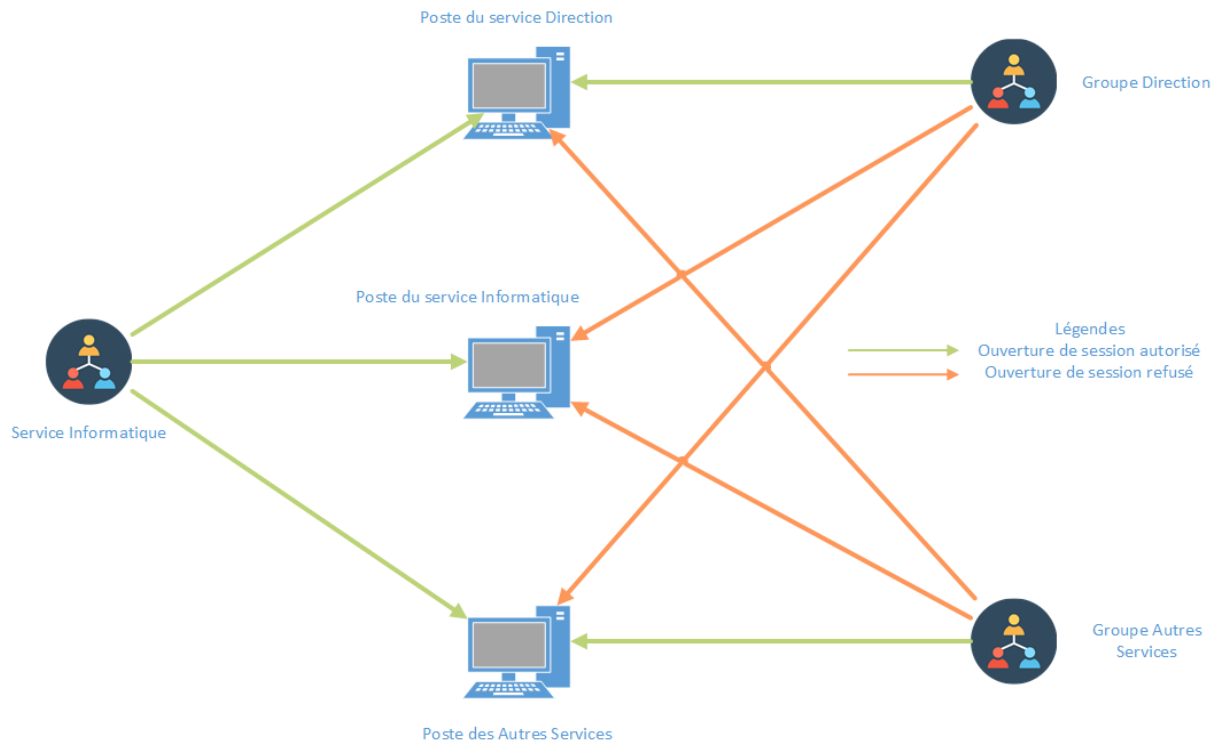
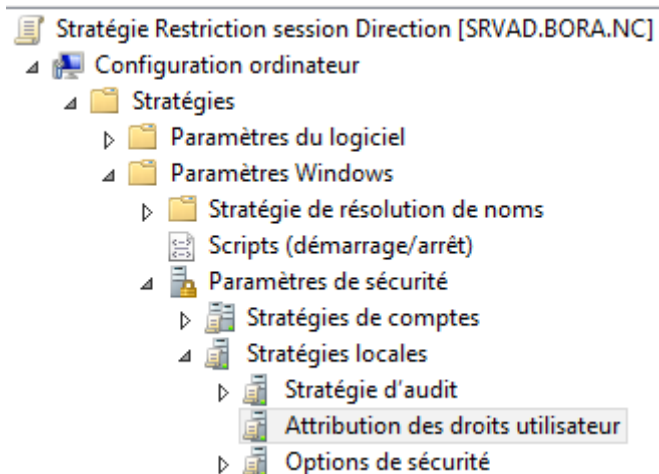
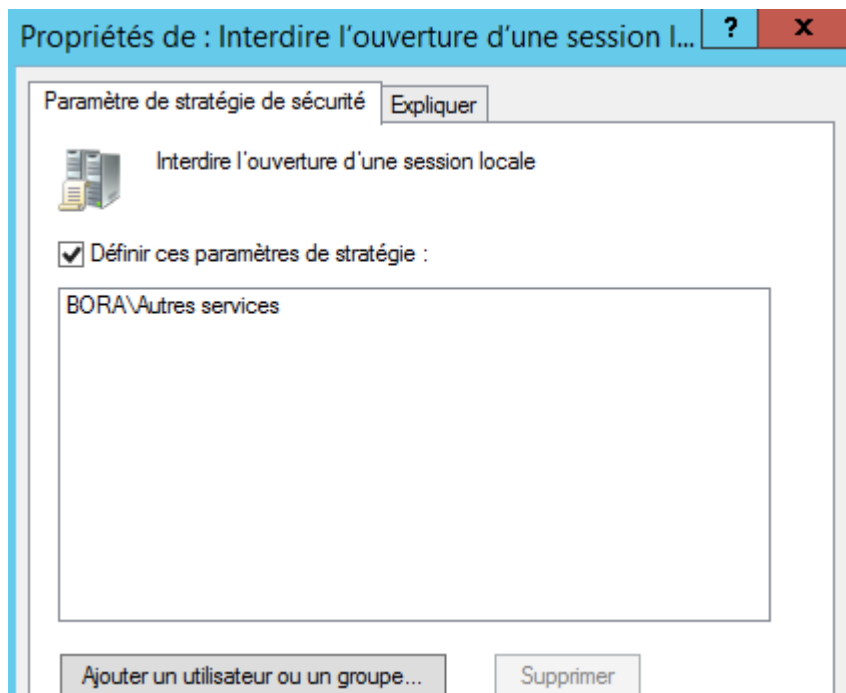


Schéma des restrictions d'ouverture de session

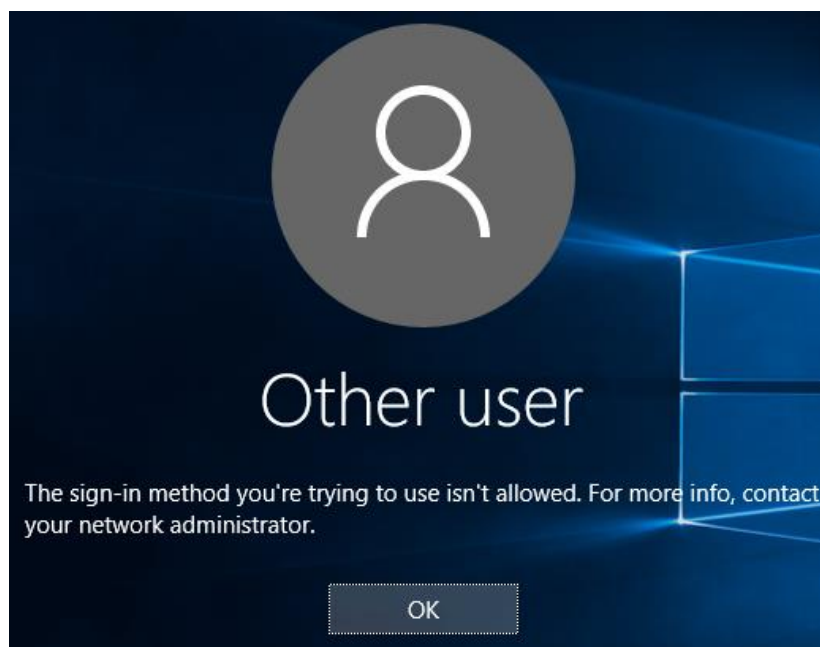
- Le paramètre de restriction d'ouverture de session local se situe dans :
  - Configuration d'ordinateur puis Paramètre Windows puis Paramètre de sécurité et ensuite Attribution des droits utilisateurs



- Ensuite il suffit d'ajouter les compte autorisé a ouvrir une session sur l'ordianteur local. Tous les autres utilisateur qui ne font pas partie du group ne pourront pas ouvrir de session sur l'ordinateur.

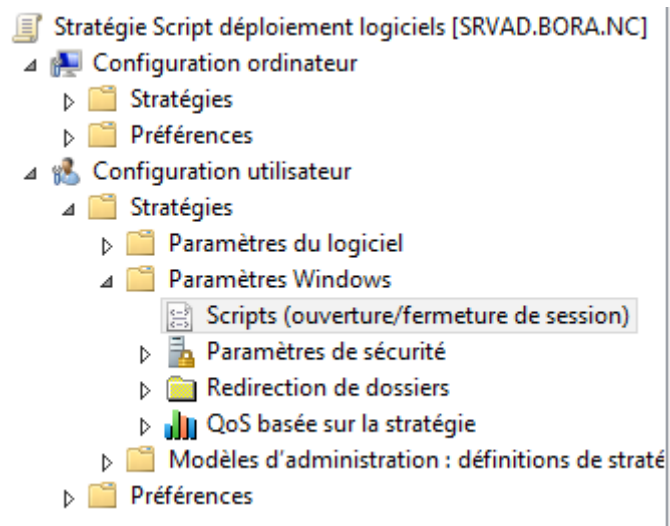


- Exemple de message lorsqu'un utilisateur n'est pas autorisé à ouvrir une session sur l'ordinateur en question.

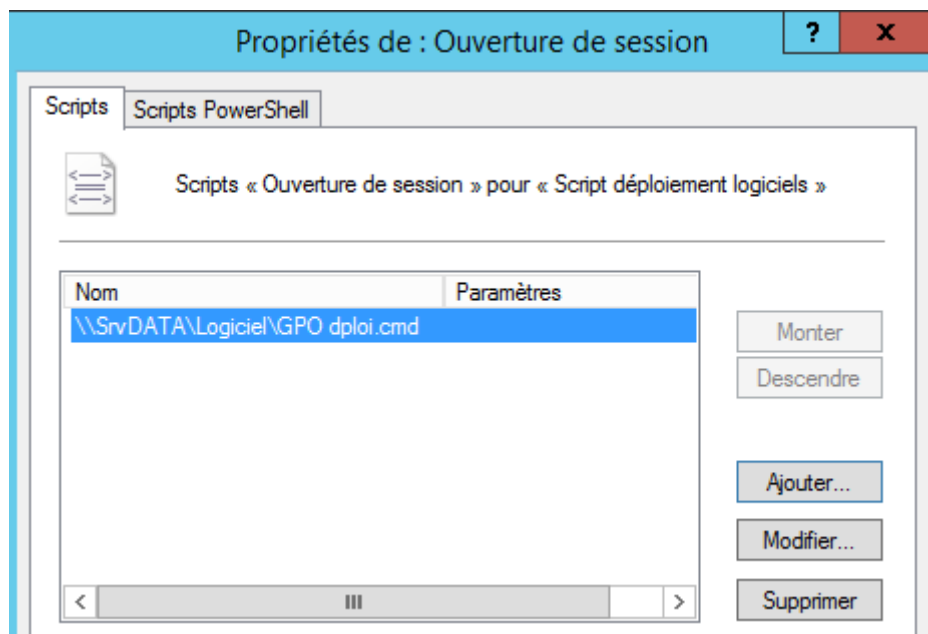


## GPO qui va déployer les logiciels Avast et open office sur les machines

- Le déploiement va s'effectuer grâce à un script d'ouverture de session qui se configure dans la configuration de l'utilisateur puis dans les paramètres Windows puis l'onglet script apparaît :






- Il suffit de placer le script à exécuter à l'ouverture de session de l'utilisateur
  - Le script se situe dans le partage Logiciel du serveur SrvDATA






- Il ne reste plus qu'à restreindre l'application de la GPO aux trois groupes du domaine :
  - Autres services
  - Direction
  - Et Service Informatique

#### Filtrage de sécurité

Les paramètres de cet objet GPO ne s'appliquent qu'à ces groupes, utilisateurs et ordinateurs :

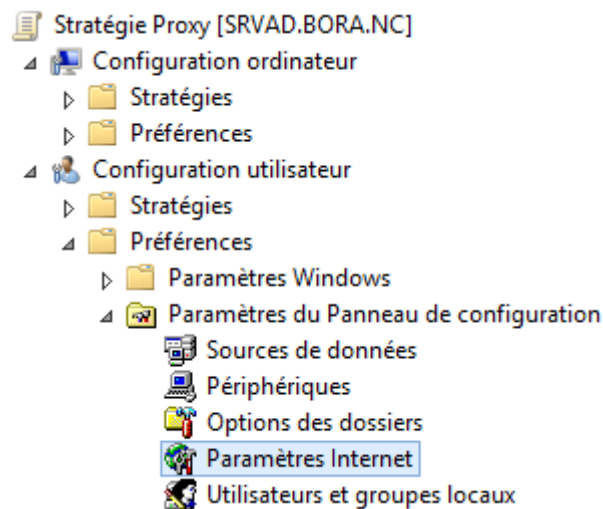
Nom
 Autres services (BORA\Autres services)
 Direction (BORA\Direction)
 Service informatique (BORA\Service informatique)

- Voici le contenu du dossier Logiciels du serveur SrvDATA
- Les Utilisateurs des groupes Autres Services et Direction y ont accès en lecture seule et le service informatique a un accès total

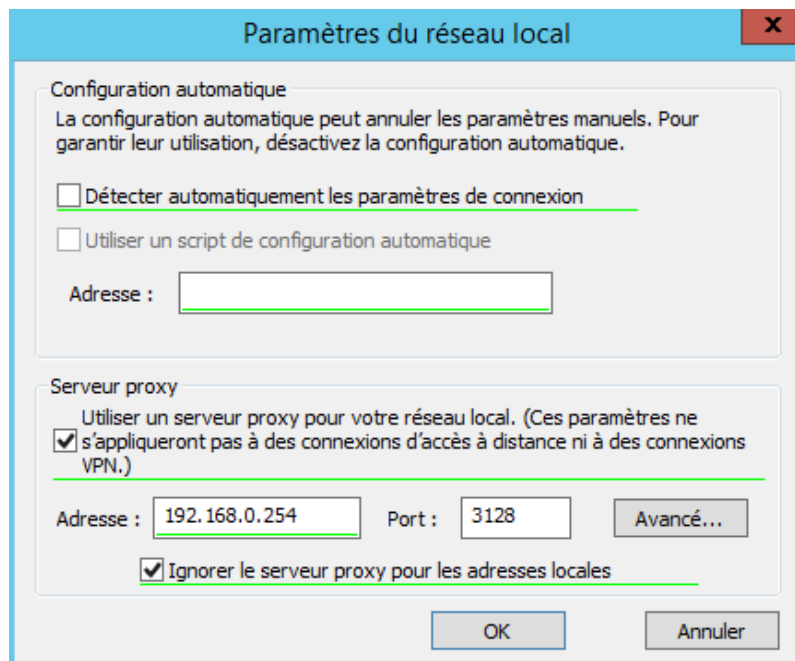
Ce PC > Données (E:) > Logiciels			
Nom	Modifié le	Type	Taille
 OpenOffice	07/04/2017 12:08	Dossier de fichiers	
 avast	27/03/2017 14:27	Application	281 935 Ko
 GPO dploi	07/04/2017 16:22	Script de comman...	1 Ko

## GPO qui va paramétrer le proxy automatiquement

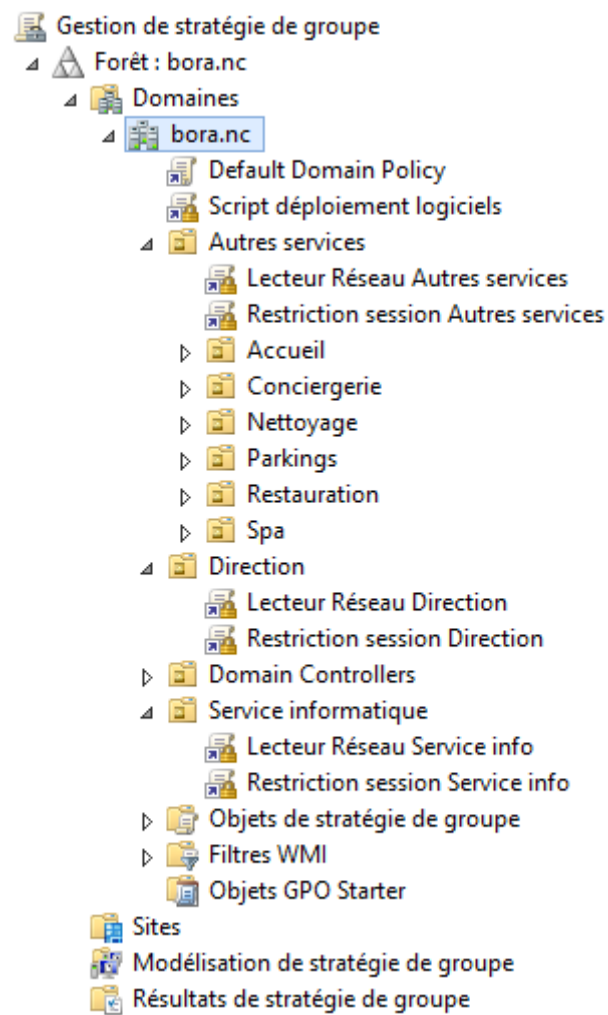
- Pour configurer le proxy automatiquement il faut se rendre dans configuration d'utilisateur puis dans Paramètre Windows et dans paramètre Internet



- Ensuite il suffit de renseigner les informations voulu puis d'appuyer sur la touche Alt + f5 pour enregistrer les paramètres
  - Adresse : 192.168.0.254
  - Port : 3128
  - Ignorer le proxy pour les adresses locales



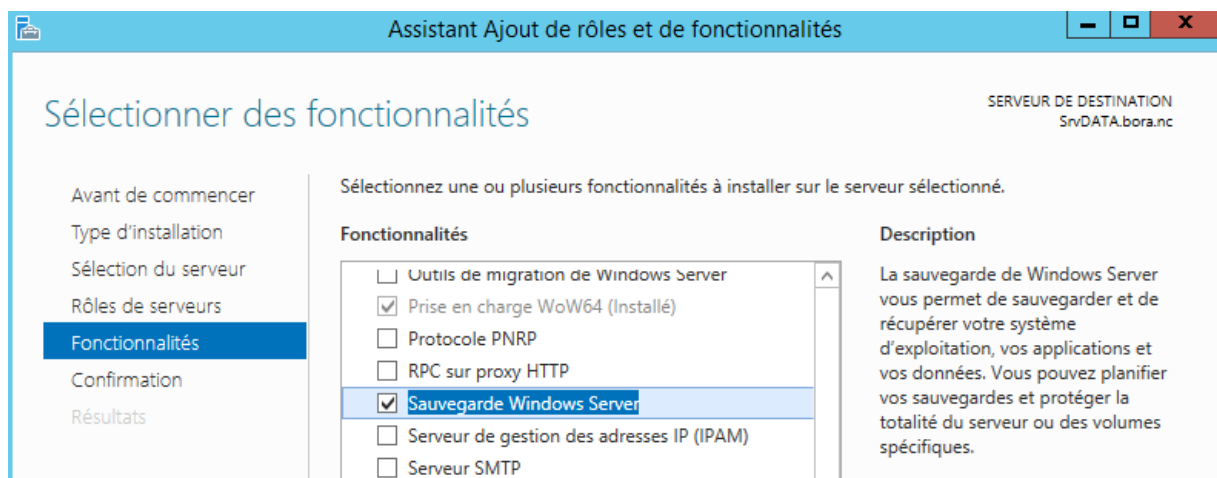
- Vérification de la création des GPO dans la console d'administration des stratégies de groupes :



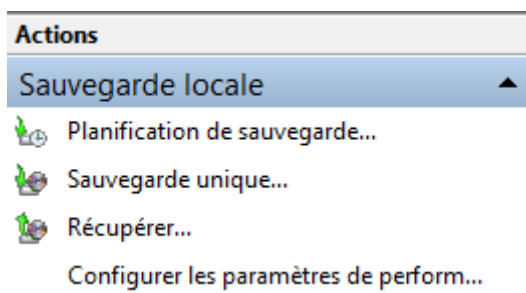


## Configuration de la sauvegarde de SrvDATA sur SrvAD

- Ajout du rôle Sauvegarde Windows serveur sur SrvDATA



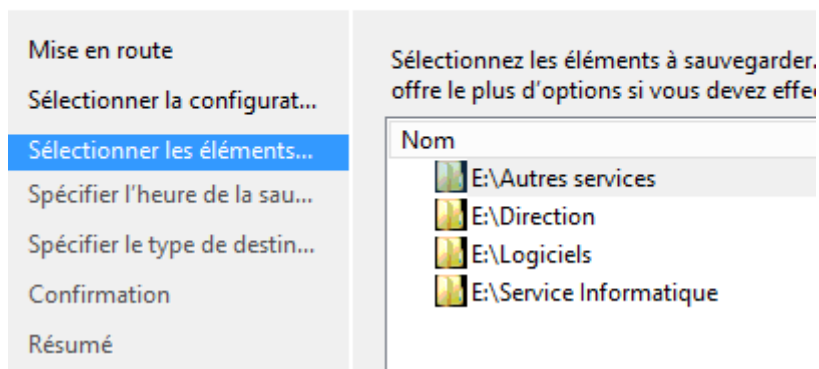
- Ensuite il suffit depuis le panneau Sauvegarde Windows serveur de planifier une nouvelle sauvegarde



- Il faut spécifier les éléments à sauvegarder à savoir tous les partages du lecteur E :



### Sélectionner les éléments à sauvegarder



- Il faut spécifier l'heure de la sauvegarde et la fréquence des sauvegardes :
  - Tous les jours à 21h



## Spécifier l'heure de la sauvegarde

Mise en route	À quelle fréquence et à quel moment voulez-vous exécuter les sauvegardes ?
Sélectionner la configurat...	<input checked="" type="radio"/> Tous les jours
Sélectionner les éléments...	Sélectionnez une heure : <input type="text" value="21:00"/>
<b>Spécifier l'heure de la sau...</b>	<input type="radio"/> Plusieurs fois par jour


- Ensuite il faut spécifier le lieu de la sauvegarde
  - Sélectionner partage distant puis spécifier le l'emplacement de la sauvegarde



## Spécifier le dossier partagé distant

Mise en route	Emplacement :
Sélectionner la configurat...	<input type="text" value="\\SrvAD\le\$\Sauvegarde SrvDATA"/>
Sélectionner les éléments...	Exemple : \\Mon_serveur_fichiers\Nom_dossier_partagé
Spécifier l'heure de la sau...	Cet Assistant crée un dossier d'après le nom du serveur sauvegardé, comme par exemple Mon_serveur-Fichiers_de_sauvegarde.
Spécifier le type de destin...	Contrôle d'accès
<b>Spécifier le dossier partag...</b>	<input type="radio"/> Ne pas hériter
Confirmation	Cette option donne accès à la sauvegarde uniquement à l'utilisateur dont les informations d'identification sont fournies à l'étape suivante.
Résumé	<input checked="" type="radio"/> Hériter
	Cette option permet à tous les utilisateurs ayant accès au dossier partagé distant spécifié d'accéder à la sauvegarde.


**Statut****Dernière sauvegarde**

État : -  
Durée : -  
 [Afficher les détails](#)

**Prochaine sauvegarde**

État : Planifiée  
Durée : 07/04/2017 21:00  
 [Afficher les détails](#)

**Toutes les sauvegardes**

Total des sauvegardes : 0 copies  
Copie la plus récente : -  
Copie la plus ancienne : -  
 [Afficher les détails](#)

**Sauvegarde planifiée**

Une sauvegarde planifiée à intervalles réguliers est configurée pour ce serveur.

**Paramètres**

Éléments de sauvegarde : Fichiers sélectionnés (Données (E:))  
Fichier exclus : Aucun  
Option avancée : Sauvegarde de copie VSS  
Destination : \\SrvAD\efs\Sauvegarde SrvDATA (Partage réseau distant)  
Heure de la sauvegarde : Tous les jours 21:00

**Utilisation de la destination**

Nom : \\SrvAD\efs\Sauvegarde SrvDATA  
Capacité : Aucun détail n'est disponible pour le dossier partagé di...  
Espace utilisé : Aucun détail n'est disponible pour le dossier partagé di...  
Sauvegardes disponibles : Aucun détail n'est disponible pour le dossier partagé di...

 [Afficher les détails](#)

 [Actualiser les informations](#)

## Récupération de sauvegarde de SrvAD sur SrvDATA

- Pour restaurer une sauvegarde il faut lancer l'utilitaire Récupérer du panneau de sauvegarde de Windows serveur
  - Pui il suffit de spécifier l'endroit où ont été sauvegardés les fichiers dans ce cas c'est « [\\SrvAD\Sauvegarde SrvDATA](#) »



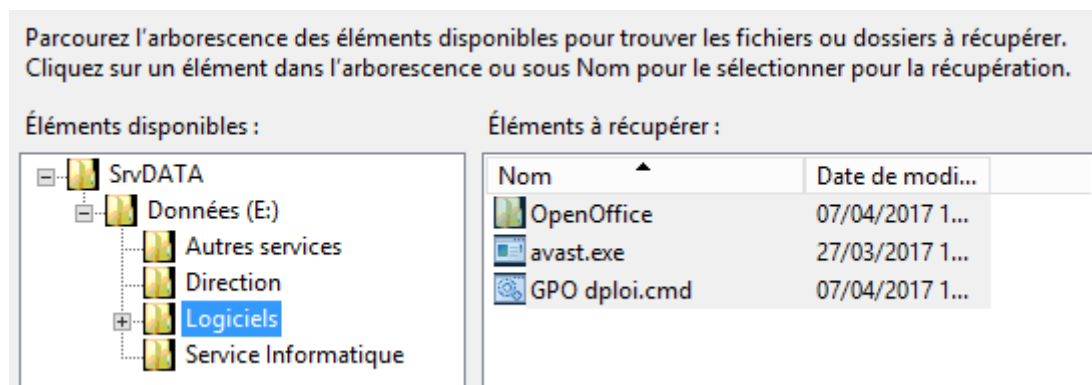
### Spécifier un dossier distant

Mise en route	Tapez le chemin UNC (Universal Naming Convention) d'accès contient la sauvegarde à utiliser. <input type="text" value="\\SrvAD\Sauvegarde SrvDATA"/> Exemple : \\Mon_serveur_fichiers\Nom_dossier_partagé
Spécifier un type d'empla...	
<b>Spécifier un dossier distant</b>	
Sélectionner une date de ...	

- Ensuite il faut choisir la date de la sauvegarde que l'on veut récupérer
  - Dans ce cas il n'y a qu'une sauvegarde qui a été effectuée le 10/04/2017 à 15h01

Sauvegarde la plus ancienne : 10/04/2017 15:01																																																		
Sauvegarde la plus récente : 10/04/2017 15:01																																																		
Sauvegardes disponibles																																																		
Sélectionnez la date d'une sauvegarde à utiliser pour la récupération. Des sauvegardes sont disponibles pour les dates affichées en gras.																																																		
<table border="1"> <thead> <tr> <th colspan="7">avril 2017</th> </tr> <tr> <th>lun.</th> <th>mar.</th> <th>mer.</th> <th>jeu.</th> <th>ven.</th> <th>sam.</th> <th>dim.</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td>1</td> <td>2</td> </tr> <tr> <td>3</td> <td>4</td> <td>5</td> <td>6</td> <td>7</td> <td>8</td> <td>9</td> </tr> <tr> <td><b>10</b></td> <td>11</td> <td>12</td> <td>13</td> <td>14</td> <td>15</td> <td>16</td> </tr> <tr> <td>17</td> <td>18</td> <td>19</td> <td>20</td> <td>21</td> <td>22</td> <td>23</td> </tr> <tr> <td>24</td> <td>25</td> <td>26</td> <td>27</td> <td>28</td> <td>29</td> <td>30</td> </tr> </tbody> </table>	avril 2017							lun.	mar.	mer.	jeu.	ven.	sam.	dim.						1	2	3	4	5	6	7	8	9	<b>10</b>	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	Date de sauvegarde : 10/04/2017 Durée : <input type="text" value="15:01"/> Éléments récupérables : <a href="#">Données (E:)(Fichiers sélectionnés)</a>
avril 2017																																																		
lun.	mar.	mer.	jeu.	ven.	sam.	dim.																																												
					1	2																																												
3	4	5	6	7	8	9																																												
<b>10</b>	11	12	13	14	15	16																																												
17	18	19	20	21	22	23																																												
24	25	26	27	28	29	30																																												

- Ensuite il faut choisir les éléments à récupérer :
  - Dans ce cas seul des logiciels ont été sauvegardés



- Pour finaliser la restauration il faut choisir la destination :
  - E:\Logiciels
  - Il faut aussi choisir parmi les options de récupération
  - Il faut restaurer la liste de contrôle d'accès des fichiers et dossiers

**Destination de la récupération**

☐ Emplacement d'origine  
☒ Autre emplacement

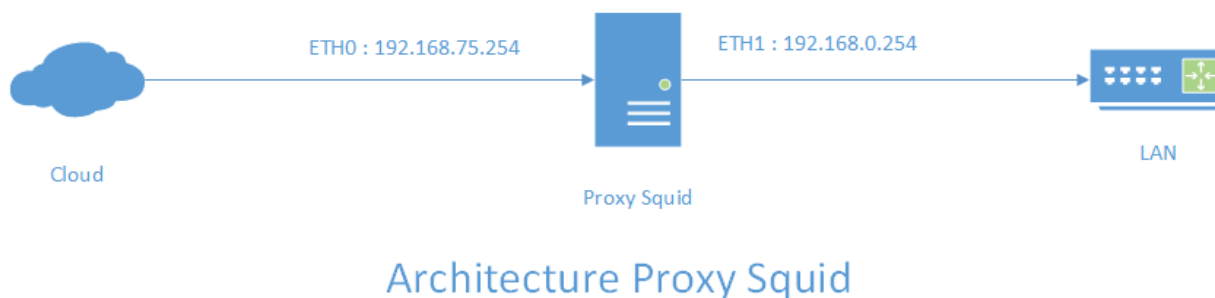
**Quand l'Assist. trouve dans la sauvegarde des éléments déjà dans dest. de la récup**

☒ Créer des copies pour avoir les deux versions  
☐ Remplacer les versions existantes par les versions récupérées  
☐ Ne pas récupérer les éléments existant déjà sur la destination de récupération

**Paramètres de sécurité**

☒ Restaurer les autorisations de la liste contrôle d'accès au fichier ou dossier à récupérer

## VII. Configuration de serveur linux Proxy



### Configuration du serveur SSH pour l'accès à distance

- **Installation du serveur SSH :**
  - apt-get update
  - apt-get install openssh-server
- **Modifier le fichier de configuration d'SSH /etc/ssh/sshd\_config :**
  - Protocol 2
  - Port 47111
  - ListenAddress 192.168.0.254 (Interface LAN)
  - # PermitRootLogin yes (commenter cette ligne pour interdire la connexion de l'utilisateur root)
  - PasswordAuthentication yes (Supprimer le commentaire cette ligne pour désactiver l'authentification par mot de passe)
  - AllowUsers sio (Seulement l'utilisateur sio sera autorisé à se connecter en SSH)
  - PrintLastLog yes (affiche la dernière connexion SSH lors de la connexion)

```
root@Sisr:/home/sio# netstat -ntpl
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat PID/Program name
tcp 0 0 192.168.0.254:22 0.0.0.0:* LISTEN 1977/sshd
tcp6 0 0 :::3128 :::* LISTEN 1600/squid3
```

```
Port 47111
ListenAddress 192.168.0.254 (Décommenter cette ligne)
Protocol 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
UsePrivilegeSeparation yes

KeyRegenerationInterval 3600
ServerKeyBits 1024

SyslogFacility AUTH
LogLevel INFO

LoginGraceTime 120
PermitRootLogin without-password (Commenter cette ligne)
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes

IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no

PermitEmptyPasswords no

ChallengeResponseAuthentication no

PasswordAuthentication yes (Décommenter cette ligne)

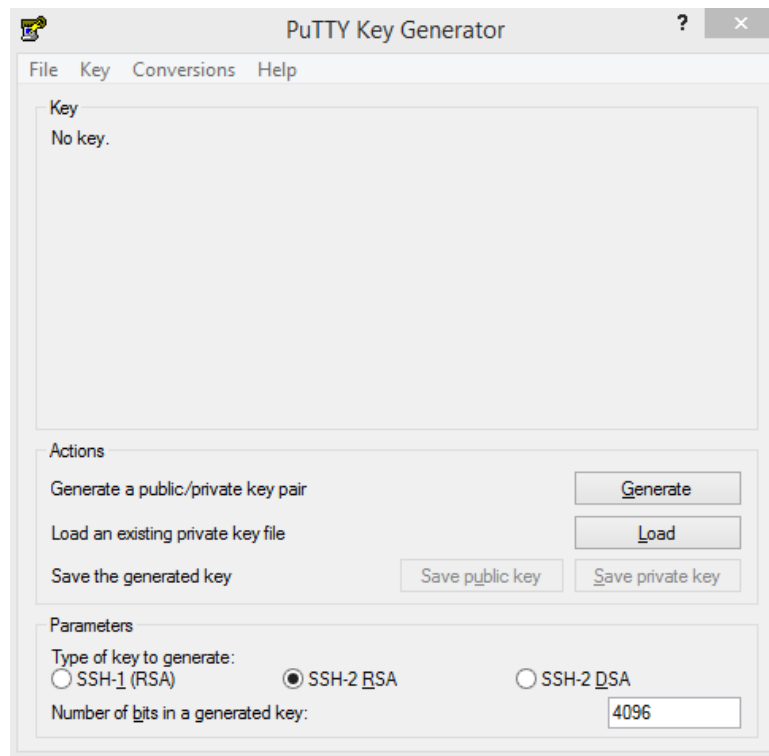
X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes

AcceptEnv LANG LC_*

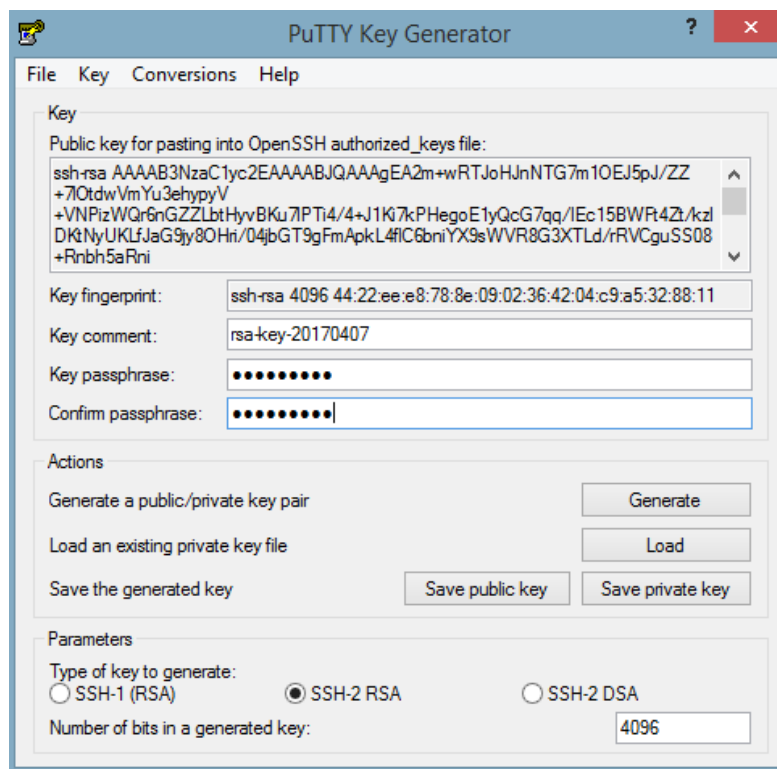
Subsystem sftp /usr/lib/openssh/sftp-server

UsePAM yes
```

- **Mise en place de l'authentification par clé :**
  - Création de la paire de clé avec puttygen :



- Ajout de la PassPhrase :





- Mise en place de la clé sur le serveur pour l'utilisateur Sio

```
mkdir .ssh
```

```
vi ~/.ssh/authorized_key
```

```
chmod 700 .ssh -Rf
```

```
comment: "rsa-key-20170407"
AAAAB3NzaC1yc2EAAAABJQAAAQEApA0GtKrf8odKOV3JaV3Eb5s8F2/TGKjrPDf6
sumVMX6DSYAv3qUv4nx5tppe/dZuxb3oQO0ihy4VwzaXLP9G7FwrRisM/hKTnRhB
xHtMG1jkJk2hgOogr6zubxJZXunEsN1Aom+DsnFY8M1dZ4dUD0m/7Q/MwuKpgR18
ZwVCQ/4Dl5CkN/tRnKhZR10jQ7Irvltosrw0HBcBExBqQxLCsAqTbq/v/3PVaRrp
iUO/tqzSBfemeNZEZw/V+q7ly86kuhscPLFRRE/911kwP0YmMfbqQBrRxQM/dI97
n7X2UgVuq82kt4TqS0gqK84czNLIKwWQ2WQM+uEfQVeykT9oim+bWglQ/nRv5fld
E3AgmBAdWjxWW764LnGPr8w1f6BLBJLuTJvfAQOaZMG+8MZW6vODg0bMNE3NQFlP
9yHhwQkoFXuZTxorJ5PI9gd7SvlvDelGCREvbk5h1WhY1NUuSEcimjhggqzU1opa
+HKuLw1GM2iwU4sB9/zoiVn3NuNrdCrkMbFL2VYe4GMsEtbwouFvRJ+Qp6uywpmx
shg+04dapo+GZSoMeTix1Enbpq05TsTWiGgp5bd2DLN4rr+hFrRsQ4E/c/+jxWkn
6X/+zj4MM81RpF9KGvyHNud2E5hc9ViIPrNq3SHZgDZ1++TWTc96LUDVFzI9IhWG
X+rkCJs=
```

## Configuration du serveur Proxy pour filtrer les requêtes

- **Configurer le proxy Squid :**
  - Création des interfaces WAN ETH0 et LAN ETH1

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.75.254
    netmask 255.255.255.0
    network 192.168.75.0
    gateway 192.168.75.2
    dns-nameservers 192.168.75.2

auto eth1
iface eth1 inet static
    address 192.168.0.254
    netmask 255.255.255.0
    network 192.168.0.0
    broadcast 192.168.0.255
    dns-nameservers 192.168.75.2
```

- Installation de Squid
- apt-get install squid3
- cp /etc/squid3/squid.conf /etc/squid3/squid.conf.original
- chmod a-w /etc/squid3/squid.conf.original

```
root@Sisr:/home/sio# netstat -ntpl
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat PID/Program name
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 1047/sshd
tcp6 0 0 :::22 :::* LISTEN 1047/sshd
tcp6 0 0 :::3128 :::* LISTEN 1123/squid3
```

- Configuration de Squid
- /etc/squid3/squid.conf:
- forwarded\_for off (Ne pas inclure l'adresse IP dans les requêtes HTTP)
- cache\_dir ufs /var/spool/squid 500 16 256
- positive\_dns\_ttl 8 hours
- acl localnet src 192.168.0.0/24
- acl localnet-hours time M T W T F 9:00-17:00
- http\_access allow localnet localnet-hours
- service squid3 restart

```
##### Acl #####

acl localnet src 192.168.0.0/24
acl local_hours time M T W T F 9:00-17:00

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

##### Autorisations #####
http_access deny !Safe_ports
http_access allow localnet local_hours
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
http_access deny all

http_port 3128

coredump_dir /var/spool/squid

refresh_pattern ^ftp:          1440    20%    10080
refresh_pattern ^gopher:       1440    0%     1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%     0
refresh_pattern (Release|Packages (.gz)*)$ 0    20%    2880
refresh_pattern .              0       20%    4320

forwarded_for off

# Mise en tampon de page web
cache_dir ufs /var/spool/squid 500 16 256
cache_mem 16 MB
maximum_object_size 15 MB

# Temps de tampon pour la résolution de nom
positive_dns_ttl 8 hours
negative_ttl 4 minutes
```

- Analyse des logs pour vérifier si les connexions fonctionnent

```
root@Sisr:/home/sio# tail -f /var/log/squid3/access.log
1491535701.801 7614 192.168.0.50 TCP_MISS/200 5139 CONNECT googleads.g.doubleclick.net:443 - HIER_DIRECT/216.58.220.130 -
1491535701.801 9877 192.168.0.50 TCP_MISS/200 978942 CONNECT www.youtube.com:443 - HIER_DIRECT/61.5.222.176 -
1491535711.798 4973 192.168.0.50 TCP_MISS/200 6985 CONNECT www.gstatic.com:443 - HIER_DIRECT/61.5.222.144 -
1491535711.799 5810 192.168.0.50 TCP_MISS/200 5864 CONNECT youtubei.youtube.com:443 - HIER_DIRECT/61.5.222.159 -
1491535711.799 6490 192.168.0.50 TCP_MISS/200 5063 CONNECT youtubei.youtube.com:443 - HIER_DIRECT/61.5.222.159 -
```

- **Configurer l'analyse des logs du proxy avec Calamaris:**

- Installation de Calamaris
  - apt-get update && apt-get install calamaris
- Analyse basique avec calamaris
  - cat /var/log/squid/access.log | calamaris

```
# Summary
Calamaris statistics
-----
lines parsed:                                lines      3682
invalid lines:                               lines        7
parse time:                                  sec          1
parse speed:                                lines/sec    3689
-----
Proxy statistics
-----
Total amount:                                requests     3682
Total Bandwidth:                             Byte    21484943
Proxy efficiency (HIT [kB/sec] / DIRECT [kB/sec]): factor    4323.62
Average speed increase:                      %          0.00
-----
Cache statistics
-----
Total amount cached:                         requests        1
Request hit rate:                            %          0.03
Bandwidth savings:                           Byte          838
Bandwidth savings in Percent (Byte hit rate): %          0.00
-----
```

- Analyse basique avec Calamaris au format html
  - `cat /var/log/squid3/access.log | Calamaris --output-format html > calamaris.html`

## Proxy Report

**Report period:** 26.Apr 17 14:31:14 - 01.May 17 14:24:57

**Generated at:** 01.May 17 14:28:35

Table of Content / Overview			
<a href="#">Summary</a>	-	-	-
<a href="#">Incoming requests by method</a>	most requested method	GET	1531 Requests
<a href="#">Incoming UDP-requests by status</a>	-	-	no requests found
<a href="#">Incoming TCP-requests by status</a>	most incoming request by status to	MISS	2042 Requests
<a href="#">Outgoing requests by status</a>	most outgoing request to	DIRECT Fetch from Source	2042 Requests
<a href="#">Outgoing requests by destination</a>	most requested destination	DIRECT	2042 Requests

## Configuration de la sauvegarde des logs du proxy

- Installation du service smb

apt-get install smbclient cifs-utils

- Monter le partage réseau pour la sauvegarde du proxy au démarrage dans fstab

```
//ipdu serveur/Partage /media/partage cifs auto,credential=pathcredentials 0 0
```

```
/root/.smbcredentials
```

```
username=IDENTIFIANT
```

```
password=MOTDEPASSE
```

```
chmod 600 ~/.smbcredentials
```

```
mount -a pour verifier integriter fstab
```

```
mount pour afficher les points de montage
```

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=41544036-cb90-4ffd-861a-afc3224e2214 / ext4 errors=remount-ro 0 1
# swap was on /dev/sda5 during installation
UUID=ae271c95-4e81-4aa9-9a8e-37b27dc75ee7 none swap sw 0 0
//192.168.0.253/SauvegardeProxy /Sauvegarde cifs auto,credentials=/root/.smbcredentials 0 0
```

- Configuration de la sauvegarde avec rsync

apt-get install rsync

```
touch /usr/bin/backup.sh
```

```
#!/bin/bash
```

```
rsync -rv /var/www/ /media/partage
```

```
chmod u+x /usr/bin/backup.sh
```

```
#!/bin/bash
rsync -rv /var/log/squid3 /Sauvegarde
```

- Création de la tâche planifiée tous les jours à 20h

crontab -e

00 20 \* \* \* /usr/bin/backup.sh

service cron restart

```
# m h dom mon dow   command
00 21 * * * /usr/bin/backup.sh
```

## Configuration du pare feu avec IP tables sur le serveur Proxy

- Mise en place d'une politique d'hardening sur le serveur proxy :

```
# Routage entre les interfaces
net.ipv4.ip_forward = 1
net.ipv4.conf.all.forwarding = 1

# Disable ipv6
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1

# IP Spoofing protection
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

# Ignore ICMP broadcast requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Ignore Directed pings
net.ipv4.icmp_echo_ignore_all = 1

# Disable source packet routing (tracert etc)
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0

# Ignore send redirects
# Ne pas envoyer de redirections ICMP
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Block SYN attacks
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 5

# Loguer les paquets ayant des IPs anormales
# (adresse source falsifiée ou non routable)
net.ipv4.conf.all.log_martians = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Ignore ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
```



- Configuration du routeur Ubuntu

Activation du routage des paquets dans le fichier /etc/sysctl.conf

Puis sysctl -p pour prendre en compte la configuration

```
# Routage entre les interfaces
net.ipv4.ip_forward = 1
net.ipv4.conf.all.forwarding = 1
```

Mise en place du Nat sur l'interface de sortie Wan (interface ens33):

Configuration d'une règle de post routage :

iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE

```
Chain POSTROUTING (policy ACCEPT 6 packets, 442 bytes)
  pkts bytes target    prot opt in     out     source    destination
   608 40415 MASQUERADE all  --  any    ens33    anywhere   anywhere
root@ProxyDeploi:/home/sio#
```

- Sauvegarde des règles du pare-feu :
  - Sauvegarde des règles dans un fichier : iptables-save > /etc/iptables\_rules.save
  - Puis importation des règles au démarrage des interfaces (/etc/network/interfaces) :
    - post-up iptables-restore < /etc/iptables\_rules.save

```
auto ens38
iface ens38 inet static
    address 192.168.0.254
    netmask 255.255.255.0
    dns-nameservers 8.8.8.8
    post-up iptables-restore < /etc/iptables_rules.save
```

```

root@ProxyDeploi:/home/sio# iptables -L -v
Chain INPUT (policy DROP 15 packets, 3447 bytes)
  pkts bytes target     prot opt in     out     source               destination           LOG level debug
 44756 7909K LOG         all  --  any    any    anywhere             anywhere              LOG level debug
  1737 1878K ACCEPT     tcp  --  ens33 any    anywhere             192.168.75.254        tcp spt:http
  3097 3291K ACCEPT     tcp  --  ens33 any    anywhere             192.168.75.254        tcp spt:https
    0    0 ACCEPT     tcp  --  ens33 any    anywhere             192.168.75.254        tcp spt:ftp
35985 2447K ACCEPT     tcp  --  ens38 any    192.168.0.0/24       anywhere              tcp dpt:3128
    0    0 ACCEPT     tcp  --  ens38 any    192.168.0.0/24       anywhere              tcp dpt:ssh
   671 49752 ACCEPT     tcp  --  any    anywhere             anywhere              tcp dpt:ssh
   138 18161 ACCEPT     udp  --  ens33 any    anywhere             192.168.75.254        udp spt:domain
    16 1344 ACCEPT     all  --  lo     any    anywhere             anywhere              LOG level debug

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination           tcp spt:ssh
    0    0 ACCEPT     tcp  --  ens33 ens38  anywhere             192.168.0.0/24        tcp dpt:ssh
    0    0 ACCEPT     tcp  --  ens38 ens33  192.168.0.0/24       anywhere
   92 5520 ACCEPT     icmp --  any    any    anywhere             anywhere
  131 19722 ACCEPT     udp  --  ens33 ens38  anywhere             192.168.0.0/24        udp spt:domain
  144 10698 ACCEPT     udp  --  ens38 ens33  192.168.0.0/24       anywhere              udp dpt:domain
  502 25464 LOG         all  --  any    any    anywhere             anywhere              LOG level debug

Chain OUTPUT (policy DROP 853 packets, 51228 bytes)
  pkts bytes target     prot opt in     out     source               destination           LOG level debug
 304K 283M LOG         all  --  any    any    anywhere             anywhere              LOG level debug
 1573 131K ACCEPT     tcp  --  any    ens33  192.168.75.254       anywhere              tcp dpt:http
 2516 233K ACCEPT     tcp  --  any    ens33  192.168.75.254       anywhere              tcp dpt:https
    0    0 ACCEPT     tcp  --  any    ens33  192.168.75.254       anywhere              tcp dpt:ftp
35432 24M ACCEPT     tcp  --  any    ens38  anywhere             192.168.0.0/24        tcp spt:3128
    0    0 ACCEPT     tcp  --  any    ens38  anywhere             192.168.0.0/24        tcp spt:ssh
   503 82133 ACCEPT     tcp  --  any    any    anywhere             anywhere              tcp spt:ssh
   161 10603 ACCEPT     udp  --  any    ens33  192.168.75.254       anywhere              udp dpt:domain
    16 1344 ACCEPT     all  --  any    lo     anywhere             anywhere

```

- Vérification du bon fonctionnement des règles avec une requête Ping des Dns de Google

```

PS C:\Users\Administrator.BORA> whoami
boraladministrator
PS C:\Users\Administrator.BORA> hostname
SrvDATA
PS C:\Users\Administrator.BORA> ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=88 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=79 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=79 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=88 ms TTL=127

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 79ms, Maximum = 88ms, Moyenne = 83ms
PS C:\Users\Administrator.BORA>

```

## VIII. Annexes

<https://blogs.technet.microsoft.com/windowsfr/2016/06/29/explication-des-branches-cbcbb-et-ltsb/>

<https://www.it-connect.fr/cours-tutoriels/administration-systemes/windows-server/dfs-dfsr/>

<https://www.it-connect.fr/cours/notions-de-base-de-lactive-directory/>

<https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/>

<https://www.ssi.gouv.fr/administration/guide/recommandations-pour-un-usage-securise-dopenssh/>