

Collection
Certifications

Préparation à la certification **MCSA**

Windows Server 2012 R2 Administration

EXAMEN N° 70-411

49 Ateliers
171 Questions-réponses

OFFERT :
UN EXAMEN BLANC en ligne
avec réponses commentées et détaillées



Téléchargement
www.editions-eni.fr



Nicolas BONNET

Les éléments à télécharger sont disponibles à l'adresse suivante :

<http://www.editions-eni.fr>

Saisissez la référence ENI de l'ouvrage **CE12R2WINA** dans la zone de recherche et validez.

Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Descriptif

Chapitre 1	Introduction
A. Organisation des certifications	12
B. Comment est organisé ce livre	12
C. Compétences testées lors de l'examen 70-411	14
1. L'examen de certification	14
2. Préparation de l'examen	14
D. Les machines virtuelles utilisées.	14
E. Le gestionnaire de serveur	15
1. Création d'un groupe de serveurs	21
2. Installation d'un rôle à distance	24
3. Suppression d'un groupe de serveurs	24
F. Serveur en mode installation minimale.	25
1. Installation de rôles avec une installation en mode Core.	28
2. Ajouter/supprimer l'interface graphique	30
3. Configuration avec sconfig	31
G. Hyper-V	34
1. Pré-requis matériels.	34
2. Les machines virtuelles sous Hyper-V	34
3. La mémoire dynamique avec Hyper-V	36
4. Le disque dur des machines virtuelles	37
5. Les captures instantanées dans Hyper-V	39
6. Gestion des réseaux virtuels	39
 Chapitre 2	 Installation du bac à sable
A. Le bac à sable	42
1. Configuration nécessaire	42
2. Installation de Windows Server 2012 R2	42

B. Création des machines virtuelles	43
1. Schéma de la maquette	48
2. Machine virtuelle AD1	50
a. Création et paramétrage de la VM	50
b. Installation du système d'exploitation	54
c. Configuration post-installation	56
3. Machine virtuelle AD2	60
4. Machine virtuelle SV1	60
5. Machine virtuelle SV2	60
6. Machine virtuelle CL8-01	61
7. Machine virtuelle SRV-RT	61
8. Machine virtuelle CL8-02	61
9. Les captures instantanées	61

Chapitre 3

Gestion d'un annuaire AD DS

A. Introduction	64
B. Présentation d'Active Directory Domain Services	64
1. Les différents composants d'AD DS	64
2. Vue d'ensemble des notions de schéma et de forêt Active Directory	65
3. La structure de l'annuaire Active Directory	68
C. Implémentation de contrôleurs de domaine virtualisés	69
1. Déploiement de contrôleurs de domaine virtualisés	69
2. Gestion des contrôleurs de domaine virtualisés	70
D. Implémentation d'un RODC	70
1. Gestion de la mise en cache sur un RODC	71
2. Administration locale sur les contrôleurs de domaine en lecture seule	71
E. Administration d'Active Directory	72
1. Présentation des différentes consoles AD	72
2. Les modules Active Directory pour PowerShell	72
3. Gestion des rôles FSMO	73
4. Utilisation d'un compte de service	74
5. Restauration d'un compte à l'aide de la corbeille AD	74
6. Sauvegarde et restauration d'Active Directory	75
F. Gestion de la base de données	75
1. La base de données Active Directory	75
2. Utilisation de la commande NTDSUtil	76
3. Redémarrage du service Active Directory	76

4. Création d'un snapshot AD	77
5. Restauration d'un objet du domaine	77
G. Ateliers : Gestion d'Active Directory	78
1. Installation et configuration d'Active Directory	78
2. Mise en place d'un RODC	83
3. Clonage d'un contrôleur de domaine virtuel	103
4. Création d'un snapshot AD	111
5. Manipulation de la corbeille AD	114
6. Défragmentation de la base de données	117
H. Validation des acquis : questions/réponses	120

Chapitre 4**Gestion de l'environnement**

A. Introduction	126
B. Automatisation de la gestion des comptes utilisateurs	126
1. Configuration de la politique de sécurité	128
2. Gestion de la stratégie de mots de passe affinée	131
3. Configuration des comptes de services	133
C. Stratégies de groupe	135
1. Gestion de la configuration	135
2. Vue d'ensemble des stratégies de groupe	135
3. Extensions côté client	136
4. Stratégies de groupe par défaut	136
5. Stockage des stratégies de groupe	137
6. GPO Starter	137
7. Sauvegarde et restauration d'une stratégie de groupe	139
8. Délégation de l'administration	139
9. PowerShell avec les GPO	140
D. Mise en place et administration des stratégies de groupe	141
1. Liens d'une GPO	141
2. Ordre d'application	141
3. Héritage et option d'application	142
4. Mise en place des filtres pour gérer l'étendue	144
5. Fonctionnement d'une stratégie de groupe avec les liaisons lentes	145
6. Récupération des stratégies par les postes clients	146
E. Maintenance d'une stratégie de groupe	147
1. Stratégie de groupe résultante	149
2. Rapport RSOP	149

3. Utilisation des journaux d'événements	150
4. Liaison lente et mise en cache des stratégies de groupe	151
5. Configuration d'une politique de sécurité Kerberos	151
F. Ateliers : Gestion de l'environnement utilisateur	152
1. Importation de comptes utilisateurs à l'aide de cmdlets PowerShell	152
2. Création d'un PSO	154
3. Création d'un compte de service	161
4. Création et configuration d'une stratégie de groupe	163
5. Création d'un rapport RSOP	167
G. Validation des acquis : questions/réponses	168

Chapitre 5

Mise en place des stratégies de groupe

A. Introduction	172
B. Modèles d'administration	172
1. Les fichiers ADMX et ADML	172
2. Mise en place du magasin central	173
3. Utilisation des filtres sur les modèles d'administration	173
C. Configuration de la redirection de dossiers et des scripts	174
1. Présentation de la redirection de dossiers	174
2. Configuration de la redirection	174
3. Utilisation de scripts dans les stratégies de groupe	175
D. Configuration des préférences de stratégie de groupe	176
1. Vue d'ensemble des préférences	176
2. Comparaison entre les stratégies et les préférences	177
E. Gestion des logiciels à l'aide des GPO	177
F. Ateliers : Gestion des postes utilisateurs	178
1. Implémentation des préférences	178
2. Configuration de la redirection de dossiers	183
3. Exécution de scripts à l'aide de GPO	186
4. Déploiement de logiciels à l'aide d'une stratégie de groupe	188
G. Validation des acquis : questions/réponses	191

Chapitre 6	Implémentation d'un serveur DHCP
A. Introduction	194
B. Rôle du service DHCP	194
1. Fonctionnement de l'allocation d'une adresse IP	194
2. Utilisation d'un relais DHCP	195
C. Installation et configuration du rôle DHCP	196
1. Ajout d'une nouvelle étendue	197
2. Configuration des options dans le DHCP	199
3. Réserve de bail DHCP	203
4. Mise en place des filtres	204
D. Base de données DHCP	208
1. Présentation de la base de données DHCP	208
2. Sauvegarde et restauration de la base de données	209
3. Réconciliation et déplacement de la base de données	210
E. Haute disponibilité du service DHCP	214
F. IPAM	214
1. Les spécifications d'IPAM	215
2. Les fonctionnalités d'IPAM	215
G. Ateliers : Installation et configuration du rôle DHCP	216
1. Ajout et configuration du rôle DHCP	216
2. Mise en place d'IPAM	223
3. Haute disponibilité au niveau du DHCP	240
H. Validation des acquis : questions/réponses	248

Chapitre 7	Configuration et maintenance de DNS
A. Introduction	252
B. Installation de DNS	252
1. Vue d'ensemble de l'espace de noms DNS	252
2. Séparation entre DNS privé/public	253
3. Déploiement du DNS	253
C. Configuration du rôle	254
1. Composants du serveur	254
2. Requêtes effectuées par le DNS	254
3. Enregistrement de ressources du serveur DNS	256
4. Fonctionnement du serveur de cache	257

D. Configuration des zones DNS	258
1. Vue d'ensemble des zones DNS	258
2. Zones de recherche directes et zones de recherche inversée	259
3. Délégation de zone DNS	259
E. Configuration du transfert de zone	259
1. Présentation du transfert de zone	259
2. Sécurisation du transfert de zone	260
F. Gestion et dépannage du serveur DNS	261
G. Ateliers : Installation et configuration du rôle DNS	261
1. Configuration des enregistrements de ressources	261
2. Vieillessement et nettoyage des enregistrements	263
3. Configuration d'un redirecteur conditionnel	265
H. Validation des acquis : questions/réponses	270

Chapitre 8

Déploiement et support de WDS

A. Introduction	274
B. Les services de déploiement Windows	274
1. Les composants de WDS	275
2. Pourquoi utiliser WDS ?	276
C. Implémentation du rôle WDS	276
1. Installation et configuration du serveur	276
2. Gestion des déploiements	279
D. Administration du service WDS	280
E. Automatisation du déploiement	281
F. Ateliers : Déploiement avec WDS	282
1. Installation et configuration des services de déploiement Windows	282
2. Importation des images utilisées pour le déploiement	284
3. Configuration du serveur de déploiement	286
4. Ajout et configuration d'un groupe de pilotes	287
5. Déploiement d'images sur les postes clients	292
6. Capture d'un poste de référence	296
7. Automatisation du déploiement	300
G. Validation des acquis : questions/réponses	309

Chapitre 9	Configuration de l'accès distant
A. Introduction	312
B. Composants d'une infrastructure de service d'accès réseau	312
1. Présentation du rôle Services de stratégie et accès réseau	312
2. Authentification et autorisation réseau	313
3. Méthodes d'authentification	313
4. Vue d'ensemble de la PKI	314
5. Intégration du DHCP avec routage et accès distant	314
C. Configuration de l'accès VPN	314
1. Les connexions VPN	314
2. Protocoles utilisés pour le tunnel VPN	315
3. Présentation de la fonctionnalité VPN Reconnect	315
4. Configuration du serveur	315
5. Présentation du kit CMAK	316
D. Vue d'ensemble des politiques de sécurité	316
E. Présentation du Web Application Proxy et du proxy RADIUS	317
F. Support du routage et accès distant	318
1. Configuration des logs d'accès distant	318
2. Résolution des problèmes du VPN	318
G. Configuration de DirectAccess	319
1. Présentation de DirectAccess	319
2. Composants de DirectAccess	319
3. La table de stratégie de résolution de noms	320
4. Pré-requis pour l'implémentation de DirectAccess	320
H. Présentation du rôle Network Policy Server	320
I. Configuration du serveur RADIUS	321
1. Notions sur le client RADIUS	321
2. Stratégie de demande de connexion	321
J. Méthode d'authentification NPS	321
1. Configurer les templates NPS	321
2. L'authentification	322
K. Surveillance et maintenance du rôle NPS	322
L. Ateliers : Configuration de l'accès distant	323
1. Configuration d'un serveur VPN	323
2. Configuration du client VPN	341
3. Configuration de DirectAccess	346

4. Configuration du client DirectAccess	364
M. Validation des acquis : questions/réponses	367

Chapitre 10**Implémentation de la solution NAP**

A. Introduction	372
B. Vue d'ensemble de la solution NAP	372
1. Méthode d'application de NAP	372
2. Architecture de la plateforme NAP	373
C. Processus d'application NAP	374
1. Mise en place d'IPsec avec NAP	374
2. Le 802.1x avec NAP	375
3. Mise en place de NAP avec un serveur VPN	375
4. Utilisation de NAP pour DHCP	375
D. Validation de l'état de santé	375
E. Surveillance et support du serveur NAP	376
F. Ateliers : Implémentation de la solution NAP	376
1. Configuration des composants NAP	376
G. Validation des acquis : questions/réponses	388

Chapitre 11**Optimisation des services de fichiers**

A. Introduction	392
B. Vue d'ensemble du rôle FSRM	392
C. Gestion du serveur de fichiers à l'aide de FSRM	393
1. Gestion des quotas	393
2. Gestion du filtrage de fichiers	396
3. Les rapports de stockage	397
D. Implémentation de la classification de fichiers	398
1. Présentation des règles de classification	398
2. Les tâches de gestion des fichiers	399
E. Le système DFS	399
1. Présentation de l'espace de noms DFS	400
2. La réplication DFS	400
3. Fonctionnement de l'espace de noms	401
4. La déduplication de données	401
5. Scénarios DFS	404

F. Configuration de l'espace de noms	406
1. Mise en place du service DFS.	406
2. Optimisation d'un espace de noms	406
G. Configuration et support de DFS-R	407
1. Fonctionnement de la réplication	407
2. Processus de réplication initial	407
3. Support du système de réplication.	407
4. Opérations sur la base de données	408
H. Ateliers : Gestion du serveur de fichiers	409
1. Installation du rôle FSRM et mise en place des quotas.	409
2. Mise en place d'une politique de filtrage par extension.	417
3. Utilisation des rapports de stockage	421
4. Configuration de la classification	425
5. Installation et configuration du serveur DFS.	431
6. Configuration de la réplication.	437
I. Validation des acquis : questions/réponses	442

Chapitre 12**Encryption de données et audit**

A. Introduction	448
B. Présentation d'EFS	448
1. Fonctionnement d'EFS	448
2. Récupération d'un fichier crypté	450
C. Configuration de l'audit	451
1. Vue d'ensemble de la politique d'audit	451
2. Spécification des paramètres d'audit sur un fichier ou un dossier	452
3. Activation de la politique d'audit	455
4. Politique d'audit avancée.	457
D. Ateliers : Configuration de l'audit	458
1. Configuration d'une politique d'audit avancée	458
2. Audit des modifications dans Active Directory	461
3. Audit des accès à un répertoire	463
E. Validation des acquis : questions/réponses	468

Chapitre 13	Implémentation du serveur WSUS
A. Introduction	472
B. Présentation du rôle WSUS	472
C. Pré-requis nécessaires pour le rôle	474
D. Déploiement de mises à jour avec WSUS	474
1. Configuration du client de mise à jour	474
2. Administration de WSUS	475
3. Présentation des groupes d'ordinateurs	476
4. Approbation des mises à jour	476
E. Ateliers : Implémentation du serveur WSUS	477
1. Installation et configuration du rôle WSUS	477
2. Approbation et déploiement des mises à jour	491
3. Création de rapports	495
F. Validation des acquis : questions/réponses	497
Chapitre 14	Surveillance des serveurs
A. Le Gestionnaire des tâches	500
B. Le Moniteur de ressources	510
C. L'Analyseur de performances	515
D. Les journaux d'événements	521
1. Création d'une vue personnalisée	524
2. Abonnement	525
E. Ateliers : Mise en place des outils d'analyse	526
1. Utilisation de l'Analyseur de performances	526
2. Création d'une vue personnalisée	534
3. Associer une tâche à un événement	536
4. Mise en place et utilisation d'un abonnement	541
F. Validation des acquis : questions/réponses	548
Tableaux des objectifs	551
Index	555

Chapitre 4

A. Introduction	126
B. Automatisation de la gestion des comptes utilisateurs	126
C. Stratégies de groupe	135
D. Mise en place et administration des stratégies de groupe	141
E. Maintenance d'une stratégie de groupe	147
F. Ateliers : Gestion de l'environnement utilisateur	152
G. Validation des acquis : questions/réponses	168

Pré-requis

- Connaître les différents types d'objets utilisateur.
- Avoir des notions sur les stratégies de groupe.
- Avoir des notions sur les paramètres de stratégies de groupe permettant la mise en place d'une politique de sécurité.

Objectifs

- Automatisation de la gestion des comptes.
- Mise en place d'une politique de sécurité.
- Gestion d'une stratégie de groupe.
- Maintenance de stratégie de groupe.

A. Introduction

La gestion des utilisateurs est une tâche quotidienne pour un administrateur système et réseau. Les comptes utilisateurs permettent l'authentification de personnes physiques souhaitant accéder à une ressource du domaine.

B. Automatisation de la gestion des comptes utilisateurs

En plus des consoles Active Directory, il est possible de procéder à la gestion des objets à l'aide d'outils en ligne de commande.

CSVDE (*Comma-Separated Values Data Exchange*) est un outil permettant l'export et l'import d'objets dans un annuaire Active Directory. Des fichiers au format CSV (*Comma-Separated Value*) sont utilisés pour les différentes opérations. Ce type de fichier peut être modifié à l'aide du bloc-notes (notepad) présent dans les systèmes d'exploitation Windows ou avec Microsoft Excel.

Syntaxe de la commande

```
csvde -f NomFichier.csv
```

Le commutateur *-f* est utilisé afin d'indiquer le fichier à utiliser. La commande permet par défaut d'effectuer une exportation.

Différents commutateurs peuvent être utilisés :

-d RootDN : permet de définir le conteneur où débute l'exportation. Par défaut, le conteneur sélectionné est la racine du domaine.

-p ÉtendueRecherche : détermine l'étendue de la recherche (Base, OneLevel, Subtree).

-r Filtre : permet la mise en place d'un filtre LDAP.

-l ListeAttributs : fournit la liste des attributs sur lesquels il est nécessaire d'effectuer une recherche. Chacun de ces attributs est séparé des autres par une virgule.

☞ Exemples d'attributs : *givenName*, *userPrincipalName*,...

-i : informe la commande qu'il est nécessaire d'effectuer une importation. Pour rappel, une exportation est effectuée par défaut.

-k : le commutateur -k permet d'ignorer les erreurs lors de l'importation. Ainsi, l'exécution de la commande se poursuit même si une erreur de type non-respect de contrainte ou objet existant est rencontrée.

```

Administrateur : Invite de commandes

Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>csvde /?
Option inconnue

Échange d'annuaires CSU

Paramètres généraux
=====
-i Active l'importation (l'exportation est activée par défaut)
-f NomFichier Nom de fichier d'entrée ou de sortie
-s NomServeur Serveur avec lequel effectuer la liaison (par défaut, le
  contrôleur de domaine du domaine de l'ordinateur)
-v Affiche les commentaires
-c NDsrc NDcib Remplace les occurrences de NDsrc par NDcib
-j Chemin Emplacement du fichier journal
-t Port Numéro de port (par défaut = 389)
-u Utilise le format Unicode
-h Activer la signature et le chiffrement de couche SASL
-? Affiche l'aide

Exportation
=====
  
```

Une deuxième commande peut être utilisée, *ldifde*. Cette instruction DOS permet comme pour *csvde* d'effectuer des opérations d'importation ou d'exportation, de plus il est possible d'effectuer des modifications sur un objet (contrairement à *csvde*).

Pour effectuer ces opérations des fichiers portant l'extension LDIF (*LDAP Data Interchange Format*) sont nécessaires. Ces fichiers contiennent des blocs de lignes qui constituent chacun une opération. Il est évident qu'un fichier peut contenir plusieurs actions, dans ce cas chaque bloc est séparé des autres par une ligne blanche.

Chaque opération nécessite de posséder l'attribut DN (*Distinguished Name*) ainsi que l'opération à effectuer (Add, Modify, Delete).

Syntaxe de la commande

```
ldifde -f NomFichier.ldif
```

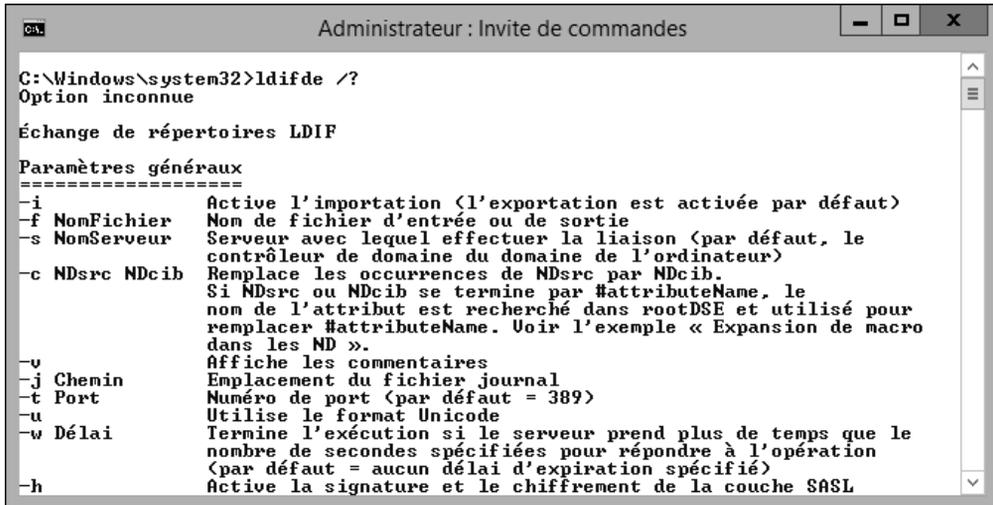
Le commutateur -f est utilisé afin d'indiquer le fichier à utiliser. La commande permet par défaut d'effectuer une exportation.

Comme pour la commande *csvde*, plusieurs commutateurs peuvent être utilisés :

-i : permet d'effectuer une importation. Par défaut, une exportation est effectuée.

-k : le commutateur -k permet d'ignorer les erreurs lors de l'importation. Ainsi l'exécution de la commande se poursuit même si une erreur de type non-respect de contrainte ou objet existant est rencontrée.

- s *NomServeur* : indique le serveur sur lequel il est nécessaire de se connecter.
- t *Port* : indique le port à utiliser (port par défaut : 389).
- d *NDRacine* : permet de situer la racine de la recherche.
- r *Filtre* : permet la mise en place d'un filtre LDAP.



```

C:\Windows\system32>ldifde /?
Option inconnue

Échange de répertoires LDIF

Paramètres généraux
=====
-i Active l'importation (l'exportation est activée par défaut)
-f NonFichier Nom de fichier d'entrée ou de sortie
-s NonServeur Serveur avec lequel effectuer la liaison (par défaut, le
contrôleur de domaine du domaine de l'ordinateur)
-c NDsrc NDcib Remplace les occurrences de NDsrc par NDcib.
Si NDsrc ou NDcib se termine par #attributeName, le
nom de l'attribut est recherché dans rootDSE et utilisé pour
remplacer #attributeName. Voir l'exemple « Expansion de macro
dans les ND ».
-v Affiche les commentaires
-j Chemin Emplacement du fichier journal
-t Port Numéro de port (par défaut = 389)
-u Utilise le format Unicode
-w Délai Termine l'exécution si le serveur prend plus de temps que le
nombre de secondes spécifiées pour répondre à l'opération
(par défaut = aucun délai d'expiration spécifié)
-h Active la signature et le chiffrement de la couche SASL

```

1. Configuration de la politique de sécurité

La politique de sécurité permet de définir un ensemble de paramètres qui s'appliquent à plusieurs objets. On retrouve dans cette politique deux types de paramètres différents :

- Paramètre de sécurité
- Paramètre de verrouillage

Les deux peuvent évidemment être configurés pour une machine spécifique (stratégie de groupe locale) ou l'ensemble des objets d'un domaine AD (généralement configuré dans la Default Domain Policy).

Paramètres de sécurité

Plusieurs types de paramètres peuvent être configurés dans la politique.

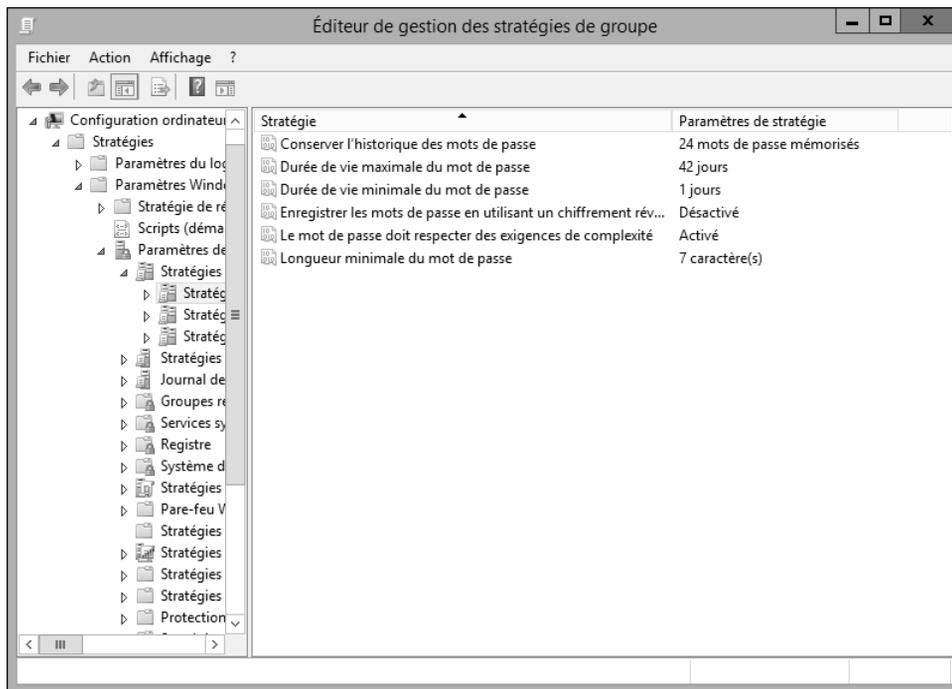
L'âge minimal du mot de passe permet d'indiquer le temps minimum avant qu'un utilisateur puisse de nouveau changer son mot de passe. L'âge maximal indique lui le nombre de jours pendant lequel le mot de passe reste valide. Une fois ce délai passé, l'utilisateur doit changer son mot de passe pour pouvoir ouvrir une session sur le domaine. L'historique de mot de passe est également à prendre en compte, il permet d'interdire les x derniers mots de passe utilisés. Attention à ne pas mettre une trop grosse valeur au niveau de ce paramètre, sans quoi les utilisateurs risquent fortement d'être mécontents.

Lors de la création du domaine Active Directory, la complexité des mots de passe est activée, ce paramètre implique la nécessité de respecter des critères spécifiques dans le mot de passe. En effet, le mot de passe est considéré comme complexe dès lors :

- Qu'il respecte trois des quatre critères suivants :
 - Majuscules
 - Minuscules
 - Caractères alphanumériques
 - Caractères spéciaux
- Qu'il ne contient pas le prénom ou le nom de l'utilisateur.

Cela complique la recherche du mot de passe par un éventuel pirate mais peut (très souvent d'ailleurs) être difficilement accepté par les utilisateurs. Il est préférable de baisser les exigences en termes de sécurité plutôt que de voir les mots de passe marqués en clair sur l'écran ou sous le clavier.

Un autre paramètre important dans une politique de mot de passe est la longueur minimale. En effet, il permet d'indiquer le nombre de caractères que le mot de passe doit contenir.



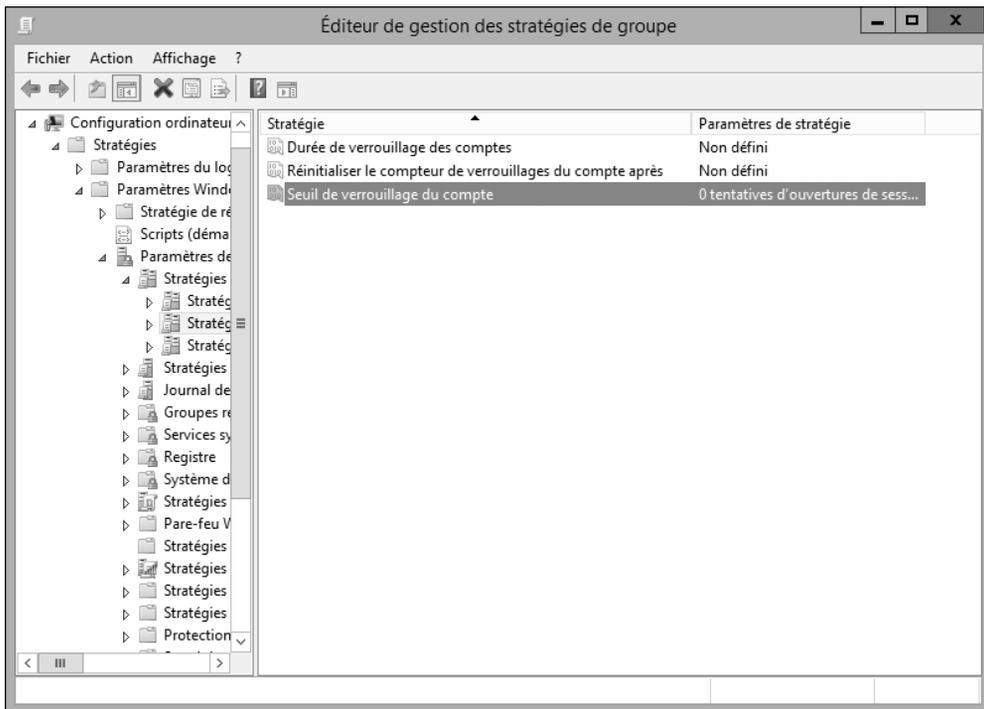
Paramètres de verrouillage

Ces paramètres permettent la configuration du verrouillage.

La durée de verrouillage est celle pendant laquelle le compte utilisateur ne peut ouvrir de session. Pour un déverrouillage manuel effectué par l'administrateur, il est nécessaire de configurer le paramètre à 0.

Le nombre de tentatives infructueuses limite le nombre d'essais en échec. Ainsi le compte concerné est verrouillé une fois ce nombre de tentatives atteint. La valeur 0 implique des tentatives infructueuses illimitées car le compte n'est alors jamais verrouillé.

Il est nécessaire de remettre à zéro le compteur du nombre de tentatives infructueuses sans quoi la politique de verrouillage n'a plus de sens. Ainsi un autre paramètre entre en compte dans la politique de verrouillage, il s'agit cette fois de la mise à jour du compteur (du nombre de tentatives en échec) après un certain nombre de minutes.



Enfin, un troisième type de paramètres (politique Kerberos) peut être également configuré. Il est donc possible d'avoir accès à des paramètres du protocole Kerberos v5.

La configuration peut, comme nous l'avons vu plus haut dans ce chapitre, être paramétrée depuis une stratégie locale ou une stratégie du domaine (console **Éditeur de gestion des stratégies de groupe**). Attention néanmoins, en cas de conflit entre une stratégie de groupe locale et une stratégie du domaine, celle du domaine l'emporte.

Les paramètres de sécurité sont généralement configurés dans la stratégie de groupe Default Domain Policy.