

Préparation à l'examen **MCSA**

Windows Server 2012 R2

Configuration des services avancés

EXAMEN N° 70-412

150 Questions-réponses
75 Travaux pratiques

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



Avant-propos**À propos de ce livre**

A. Avant-propos	16
1. À propos du livre	16
B. Conditions requises	17
1. Niveau/connaissances	17
2. Certifications précédentes	17
3. Matériel nécessaire pour les travaux pratiques	17
C. Le cursus de certification Microsoft	18
1. Détails du cursus MCSA	19
2. Détails du cursus MCSE	19

Chapitre 1**Présentation de Windows Server 2012 R2**

A. Windows Server 2012 R2	22
B. Nouvelle interface graphique	23
1. Menu Démarrer	24
2. Panneau de configuration	25
3. Les programmes	26
4. Les raccourcis-clavier utiles	27
C. Déploiement de Windows Server 2012 R2	28
1. Installation complète	28
2. Installation minimale (Server Core)	29
D. L'adressage IP	31
1. Adressage IP dynamique	31
2. Adressage IP statique	31
E. Les protocoles réseau	31
1. Modèle TCP/IP	31
2. Protocole IP	32
a. Adressage IPv4	32
b. Adressage IPv6	32
F. L'administration de Windows Server 2012 R2	33
1. La console Gestion de l'ordinateur	33
2. La console Gestionnaire de serveur	35
3. Les outils d'administration	35

G. Travaux pratiques	36
1. Installer Windows Server 2012 R2 en mode graphique	37
2. Installer Windows Server 2012 R2 en mode Server Core	44
3. Configurer l'interface réseau	47
4. Renommer un serveur avec sconfig	52
5. Configurer l'adressage IP avec sconfig	55
H. Résumé du chapitre	62
I. Validation des acquis : questions/réponses	63

Chapitre 2

Les services de domaine Active Directory

A. Présentation d'Active Directory	68
1. Service d'annuaire	68
2. Gestion du service d'annuaire	69
a. Administrer Active Directory	70
b. Partitions Active Directory	74
3. Gestion des identités et des accès	75
4. Gestion des unités d'organisation	76
a. Ajouter une OU via l'interface graphique	77
b. Ajouter une OU via les commandes DOS	81
c. Ajouter une OU avec PowerShell	81
5. Stratégies de groupe	82
a. Gestion des stratégies de groupe	82
b. Dépannage des stratégies de groupe	84
c. Nouveauté des stratégies de groupe	86
B. Forêts et domaines Active Directory	89
1. Forêts	89
2. Domaines	90
3. Arbres de domaines	90
C. Niveaux fonctionnels	91
1. Niveaux fonctionnels de forêt	91
2. Niveaux fonctionnels de domaine	92
3. Augmenter le niveau fonctionnel	93
D. Contrôleurs de domaine	94
1. Rôles FSMO	95
2. Catalogue global	98

E. Gestion des comptes d'utilisateurs	101
1. Administration des comptes d'utilisateurs	102
2. Création des comptes d'utilisateurs	102
a. Par lignes de commandes DOS	102
b. Par lignes de commandes PowerShell	103
F. Gestion des groupes de sécurité	104
1. Groupes globaux	105
2. Groupes de domaine locaux	106
3. Groupes universels	106
G. Travaux pratiques	107
1. Installer le rôle AD DS via l'interface graphique	108
2. Installer le rôle AD DS sur une installation minimale	112
3. Créer des stratégies de sécurité	116
H. Résumé du chapitre	119
I. Validation des acquis : questions/réponses	120

Chapitre 3

Les services réseau avancés

A. Service DNS	124
1. Présentation du service DNS	125
2. Fonctionnement du service DNS	126
a. Outils en lignes de commandes DOS	127
b. Principe de résolution de noms DNS	128
3. Gestion du service DNS	129
a. Implémentation des logs détaillés	131
b. Enregistrements DNS	133
c. Nettoyage des enregistrements DNS	137
d. Redirecteurs du service DNS	140
e. Sauvegarder la configuration DNS	142
4. Zones DNS	143
a. Zone principale	144
b. Zone secondaire	144
c. Zone de recherche inversée	144
d. Zone de stub	145
e. Zone GlobalNames	145
5. DNS et Active Directory	152

6.	Sécurité du service DNS	153
a.	Sécuriser le cache DNS	153
b.	Configurer le pool de sockets DNS	154
c.	Implémenter DNSSEC	156
7.	Gestion du service DNS via Windows PowerShell	158
B.	Service DHCP	159
1.	Présentation du service DHCP	159
2.	Gestion du serveur DHCP	160
3.	Fonctionnement du service DHCP	161
a.	Principe d'attribution d'une adresse IP en IPv4	162
b.	Principe d'attribution d'une adresse IP sous IPv6	163
4.	Options de configuration du service DHCP	164
5.	Gestion du service DHCP via Windows PowerShell	169
6.	Haute disponibilité du service DHCP	169
7.	Sauvegarde et restauration du service DHCP	170
a.	Sauvegarde automatique	170
b.	Sauvegarde manuelle	171
c.	Restauration	171
C.	IPAM	172
1.	Présentation du serveur IPAM	172
2.	Gestion du serveur IPAM	173
3.	Installer et configurer la gestion d'adresses IPAM	175
4.	Gestion de l'espace d'adressage IP	182
a.	Plages d'adresses IP	183
b.	Adresses IP	185
c.	Blocs d'adresses IP	186
5.	Surveiller et gérer IPAM	187
a.	Serveurs DNS et DHCP	187
b.	Étendues DHCP	188
c.	Analyse des zones DNS	188
d.	Groupes de serveurs	188
6.	Catalogue des événements	189
D.	Travaux pratiques	190
1.	Installer et configurer le service DNS	191
2.	Configurer le service DNS avec DNSSEC	213
3.	Installer et configurer le service DHCP	226
4.	Installer et configurer la haute disponibilité du service DHCP	239
E.	Résumé du chapitre	247

F. Validation des acquis : questions/réponses	247
---	-----

Chapitre 4

Les services de fichiers avancés

A. Présentation des services de fichiers	252
1. Fonctionnement des services de fichiers	252
2. Gestion des services de fichiers	253
a. Administrer les services de fichiers	254
b. Rôles et services de stockage	259
B. Stockage réseau	260
1. Stockage SAN iSCSI	260
a. Fonctionnement du stockage iSCSI	261
b. Gestion du stockage iSCSI	263
2. Stockage SAN FCoE	264
3. Stockage NFS	265
4. Stockage DAS	265
5. Stockage NAS	265
C. Optimiser l'usage du stockage	265
1. Gestionnaire de ressources	265
a. Fonctionnement FSRM	265
b. Gestion FSRM	267
2. Gestion de quota	267
a. Création d'un quota	268
b. Création d'un modèle de quota	273
3. Gestion du filtrage de fichiers	275
a. Création d'un filtre de fichiers	276
b. Création d'un modèle de filtre	278
4. Gestion de la classification	281
a. Création d'une propriété de classification	282
b. Création d'une règle de classification	283
5. Gestion des rapports de stockage	286
6. Déduplication des données	287
a. Installer la déduplication des données	288
b. Activer la déduplication des données	289
c. Vérifier la déduplication	291

D. BranchCache	291
1. Présentation de BranchCache	291
a. Fonctionnement de BranchCache	292
b. Gestion de BranchCache.	293
2. Mode de cache.	295
a. Mode de cache hébergé	295
b. Mode de cache distribué.	296
3. Déployer BranchCache	297
E. Travaux pratiques	298
1. Créer une infrastructure iSCSI	299
2. Implémenter BranchCache	307
F. Résumé du chapitre	324
G. Validation des acquis : questions/réponses	325

Chapitre 5

Contrôle d'accès dynamique

A. Contrôle d'accès dynamique.	330
1. Présentation du DAC.	330
2. Fonctionnement du DAC	330
a. Revendications.	332
b. Stratégie d'accès central	332
c. Règle d'accès central	333
3. Gestion du DAC	333
4. Implémentation du DAC	335
B. Travaux pratiques	336
1. Configurer Kerberos	338
2. Créer les revendications	339
3. Configurer les propriétés.	342
4. Configurer la classification	344
5. Configurer une règle d'accès central.	350
6. Créer une stratégie d'accès central.	353
7. Publier une stratégie d'accès	356
8. Tester l'accès aux ressources	359
C. Résumé du chapitre	360
D. Validation des acquis : questions/réponses	360

Chapitre 6	Déploiement distribué AD DS
A. Présentation du déploiement distribué AD DS	362
1. Gestion de forêts Active Directory	362
a. Gestion administrative	362
b. Partitions	363
2. Gestion de domaines Active Directory	363
a. Gestion administrative	363
b. Partitions	363
3. Déploiement distribué AD DS	363
a. Domaines ou forêts multiples	364
b. Mise à jour vers Windows Server 2012 R2	365
c. Migration vers Windows Server 2012 R2	366
d. Relations d'approbation	367
e. Routage des suffixes de noms	371
B. Travaux pratiques	374
1. Ajouter un domaine dans la forêt	374
2. Configurer une approbation AD DS	379
C. Résumé du chapitre	383
D. Validation des acquis : questions/réponses	384

Chapitre 7	Sites et services Active Directory
A. Présentation des sites Active Directory	388
1. Objectif des sites	388
a. Gestion des sites	389
b. Location des services	390
2. Les sites	390
3. Les sous-réseaux	390
4. Les serveurs de catalogue global	391
5. Les partitions Active Directory	392
6. Les liens de sites	392
a. Fonctionnement des liens de sites	393
b. Gestion des liens de sites	394
7. Les ponts de sites	396
B. Travaux pratiques	396
1. Renommer le site par défaut	397
2. Créer des sites	397
3. Affecter des serveurs à un site	399

4. Créer des sous-réseaux	400
5. Configurer le catalogue global	403
6. Configurer la mise en cache	403
C. Résumé du chapitre	405
D. Validation des acquis : questions/réponses	405

Chapitre 8**Répliquions Active Directory**

A. Présentation de la réplication Active Directory	408
1. Répliquions Active Directory	408
a. Planification des répliquions	409
b. Topologie de réplication	410
c. Objets de connexion	412
d. Réplication vers des RODC	416
e. Réplication des mots de passe (RODC)	417
f. Les conflits de répliquions	419
2. Réplication SYSVOL	420
a. Présentation du répertoire SYSVOL	420
b. Réplication du répertoire SYSVOL	422
3. Surveiller et dépanner	423
B. Travaux pratiques	424
1. Configurer la réplication	425
2. Configurer la stratégie RODC	429
3. Surveiller la réplication	435
C. Résumé du chapitre	439
D. Validation des acquis : questions/réponses	440

Chapitre 9**Services de certificats AD CS**

A. Infrastructures à clés publiques	444
1. Présentation des PKI	444
2. Composants d'une PKI	445
3. Chiffrement	447
B. Présentation d'AD CS	447
1. Services de certificats AD CS	447
a. CA autonome	448
b. CA d'entreprise	448
c. Gestion d'AD CS	448

2.	Hiérarchie de CA	450
a.	Infrastructure à deux couches	450
b.	Infrastructure à trois couches	451
c.	CA racine	453
d.	CA intermédiaire.	454
e.	CA émettrice	454
3.	Services de rôles AD CS	454
a.	Autorité de certification	454
b.	Demande de certificats via le web	455
c.	Répondeur en ligne	455
d.	Inscription de composants réseau	455
e.	Inscription des certificats.	455
f.	Stratégie des certificats	456
4.	Certificats	456
a.	Modèles de certificats	457
b.	Demande de certificat.	459
C.	Travaux pratiques	459
1.	Installer une CA autonome	460
2.	Installer une CA d'entreprise	471
3.	Activer une CA émettrice	476
4.	Publier un certificat via des GPO.	480
5.	Configurer l'interface Web	480
6.	Demander un certificat	488
D.	Résumé du chapitre	490
E.	Validation des acquis : questions/réponses	491

Chapitre 10**Services de gestion des droits**

A.	Services de gestion des droits	496
1.	Présentation d'AD RMS	496
a.	Fonctionnement d'AD RMS	497
b.	Gestion d'AD RMS	498
c.	Composants d'AD RMS.	504
2.	Installer et configurer AD RMS	504
a.	Schématiser l'infrastructure	504
b.	Pré-requis d'installation	505
3.	Protéger le contenu des fichiers	505

B. Travaux pratiques	507
1. Préparer le déploiement AD RMS	508
2. Installer AD RMS.	512
3. Post-installation AD RMS	514
4. Configurer la console AD RMS	519
5. Configurer les super utilisateurs.	521
6. Configurer un modèle de stratégies.	522
7. Créer une stratégie d'exclusion	527
8. Protéger du contenu	528
C. Résumé du chapitre	535
D. Validation des acquis : questions/réponses	535

Chapitre 11**Services de fédération AD FS**

A. Services de fédération	538
1. Présentation d'AD FS	539
a. Fonctionnement d'AD FS	539
b. Gestion d'AD FS.	540
2. Revendications.	541
3. Infrastructure AD FS	542
a. Infrastructure.	542
b. Composants.	543
4. Installer et configurer AD FS.	544
B. Travaux pratiques	545
1. Préparer le déploiement d'AD FS	546
2. Installer les serveurs AD FS.	550
3. Configurer la signature de jetons	553
4. Configurer les revendications	553
5. Installer les proxy AD FS	554
C. Résumé du chapitre	555
D. Validation des acquis : questions/réponses	555

Chapitre 12	La répartition de charge
A. Répartition de charge	558
1. Présentation de la répartition	558
a. Technologies existantes	559
b. Avantages et inconvénients	559
B. Répartition de charge réseau	561
1. Network Load Balancing	561
2. Différents modes de répartition	562
a. Prioritaire	562
b. Mode égal	563
c. Mode manuel	563
3. Modes de transmission	564
a. Unicast - Monodiffusion	564
b. Multicast - Multidiffusion	565
c. Multidiffusion IGMP	565
4. Affinité de répartition de charge	565
5. Convergence et haute disponibilité	566
C. Travaux pratiques	567
1. Installer et configurer le NLB	568
2. Gérer un cluster NLB	575
3. Gérer un cluster via PowerShell	583
4. Simuler la répartition de charge	586
D. Résumé du chapitre	588
E. Validation des acquis : questions/réponses	588
Chapitre 13	Cluster et haute disponibilité
A. Haute disponibilité	592
1. Présentation de la haute disponibilité	592
2. Solutions de haute disponibilité	593
B. Clusters de basculement	593
1. Présentation des clusters	593
2. Fonctionnement d'un cluster	593
a. Réseaux	594
b. Basculement	595
c. Volumes partagés	597
d. Console de gestion du cluster	598
e. Administration d'un cluster de basculement	599

f. Quorum	603
g. Installer et configurer un cluster	604
h. Les rôles	606
i. Optimisation des CSV	607
C. Travaux pratiques	607
1. Installer IIS sur chaque nœud	609
2. Connecter les nœuds au disque iSCSI	609
3. Créer un cluster de serveurs	610
4. Créer un volume partagé de cluster	615
5. Configurer un rôle de serveur	615
6. Simuler une panne dans le cluster	617
D. Résumé du chapitre	618
E. Validation des acquis : questions/réponses	618

Chapitre 14

Cluster de basculement Hyper-V

A. Virtualisation avec Hyper-V	622
1. Présentation d'Hyper-V	622
a. Installation du rôle Hyper-V	624
b. Gestion d'Hyper-V	625
c. Gestion d'Hyper-V via SCVMM	626
B. Haute disponibilité avec Hyper-V	626
1. Réplication	626
2. Clusters de basculement	626
3. Migration des machines virtuelles	627
C. Travaux pratiques	628
1. Préparer le stockage Hyper-V	628
2. Installer le rôle Hyper-V	632
3. Importer des machines virtuelles	635
4. Configurer la réplication Hyper-V	635
5. Configurer la réplication d'une VM	637
6. Configurer le basculement de cluster	639
7. Migrer une machine virtuelle	640
8. Migrer le stockage d'une VM	641
9. Redimensionner un VHDX à chaud	641
D. Résumé du chapitre	643
E. Validation des acquis : questions/réponses	643

Chapitre 15**Sauvegarde et restauration**

A. Présentation de la récupération d'urgence	646
1. Récupération d'urgence	646
2. Présentation de la sauvegarde.	648
3. Sauvegarde Windows Server.	649
a. Gestion de la sauvegarde Windows Server.	650
b. Planifier la sauvegarde Windows.	651
c. Configurer la sauvegarde Windows	652
d. Configurer la restauration des données	654
B. Récupération des données	655
1. Clichés instantanés.	655
2. Corbeille Active Directory	659
C. Travaux pratiques	660
1. Installer un outil de sauvegarde	661
2. Configurer la sauvegarde Windows	661
3. Restaurer des données.	670
4. Windows Azure Backup	672
D. Résumé du chapitre	686
E. Validation des acquis : questions/réponses	686
Tableau des objectifs	689
Index.	691

Chapitre 15

A. Présentation de la récupération d'urgence	646
B. Récupération des données	655
C. Travaux pratiques	660
D. Résumé du chapitre	686
E. Validation des acquis : questions/réponses	686

Pré-requis

- Connaître les principes d'une sauvegarde de données.
- Connaître les principes d'une restauration de données.
- Connaître les bases d'un plan de reprise d'activité.

Objectifs

- Savoir implémenter un plan de reprise d'activité en cas de sinistre.
- Savoir définir une stratégie de sauvegarde.
- Savoir implémenter la sauvegarde sous Windows Server 2012 R2.
- Savoir restaurer des données effacées d'un serveur de fichiers.
- Savoir récupérer des objets supprimés accidentellement d'un annuaire.

A. Présentation de la récupération d'urgence

De nos jours, de plus en plus de sociétés fonctionnent en utilisant au quotidien l'outil informatique (serveurs, postes de travail, terminaux fixes ou mobiles, e-mails, etc.). Les données manipulées sont multiples présentes sous différents supports, accessibles à un ou plusieurs utilisateurs et sont plus ou moins confidentielles. Pour beaucoup d'entreprises, l'essentiel de l'activité est basée sur des données numériques (contrats, factures, commandes, gestion de stocks, produits, services en ligne, sites web, projets, etc.). C'est pourquoi la perte de données informatiques lors d'un sinistre peut s'avérer vitale pour une entreprise (incendie, suppression accidentelle, crash, piratage, vol, etc.). D'après les statistiques, une entreprise qui perd l'essentiel de ses données informatique suite à un crash ou une mauvaise manipulation a un pourcentage de chance plus élevé de cesser toute activité dans les semaines suivant le sinistre, si aucun plan de récupération d'urgence n'a été mis en place au préalable. C'est pourquoi la sauvegarde est un point crucial, commun à presque toutes les entreprises. Mettre en place une infrastructure informatique, signifie également de planifier et mettre en place des solutions pour la restaurer en cas de sinistre.

1. Récupération d'urgence

La récupération d'urgence consiste à restaurer le service qui a été détérioré suite à un sinistre. Pour cela, une entreprise peut, par exemple, mettre en place un Plan de Reprise d'Activité (PRA) qui consiste à définir les tâches et actions à réaliser pour restaurer, en un temps record, le service offert aux utilisateurs. Un PRA comprend notamment un plan de sauvegarde qui consiste à définir une stratégie visant à sauvegarder l'ensemble des données de la société afin de pouvoir les restaurer si besoin. Avant de mettre en place une stratégie de sauvegarde, une entreprise doit d'abord faire une étude préliminaire qui aidera à mieux cibler les besoins et ainsi, orienter la bonne implémentation du plan de sauvegarde. Afin de répondre au mieux aux exigences requises par un système informatique, il convient de respecter et suivre les bonnes pratiques définies dans les normes ITIL (*Information Technology Infrastructure Library*).

Les bonnes pratiques figurant dans les ouvrages ITIL préconisent de répondre aux questions suivantes avant de mettre en place un plan de récupération d'urgence :

- **Définir les éléments à sécuriser et/ou sauvegarder** : sécuriser ou sauvegarder l'ensemble du périmètre informatique occasionne des coûts (logiciels, matériels, espace de stockage disque ou sur bande, redondance des équipements, etc.). C'est pourquoi il convient d'évaluer à l'avance la volumétrie à sauvegarder en faisant la sélection des éléments à conserver.
- **Évaluer les coûts de la sauvegarde** : plus il y a de données à sauvegarder, plus le coût du plan de sauvegarde est élevé (équipement de sauvegarde, espace disque, etc.). Pour maîtriser son budget, il est important de ne pas négliger l'évaluation des coûts liés à la sauvegarde. Tous les éléments de l'infrastructure de sauvegarde doivent être évalués, comme le matériel, les logiciels, la volumétrie, les coûts de rétention, les coûts de stockage ainsi que les coûts humains (administrateur, technicien, etc.).
- **Définir les clauses du contrat de niveau de service** : les ouvrages décrivant les bonnes pratiques informatiques mentionnent le fait qu'il est important de définir à l'avance le niveau de service apporté aux utilisateurs. Ces clauses doivent être recensées dans un document exposant clairement la qualité de service attendue (ce contrat client-fournisseur est également appelé SLA : *Service Level Agreement*), ainsi que les délais d'interruption de service maximum en cas de panne ou sinistre. La durée maximale d'interruption du service pouvant être tolérée avant la reprise de l'activité, est également appelé RTO (*Recovery Time Objective*) d'après les ouvrages ITIL.
- **Définir les pertes de données acceptables en cas de sinistre** : lors d'un sinistre, il est possible de restaurer les données perdues ou corrompues d'un serveur à un instant T, si la politique de sauvegarde mise en place est opérationnelle. Cependant, les données saisies quelques minutes avant le sinistre par les utilisateurs peuvent ne pas avoir été sauvegardées. Ce qui, implicitement, veut dire qu'il n'est plus possible de restaurer ces éléments non sauvegardés. C'est pourquoi il est important de définir la tolérance de perte de données en cas de sinistre dans un document spécifique, également appelé RPO (*Recovery Point Objective*) dans les ouvrages ITIL.
- **Définir la stratégie de rétention des sauvegardes** : lorsque les sauvegardes sont réalisées sur bande, online, ou sur disque, de l'espace de stockage est consommé. La politique de rétention des sauvegardes définit le temps que ces archives sauvegardées doivent être conservées avant écrasement par une nouvelle sauvegarde ou simple destruction. Plus la stratégie de rétention impose un délai de conservation des sauvegardes élevé, et plus il est facile pour un administrateur de restaurer des données supprimées depuis quelques jours. Le cas se présente surtout pour les situations de suppression accidentelle de données. Par exemple, si un utilisateur supprime accidentellement un dossier important et qu'aucun utilisateur ne s'en rend compte pendant deux semaines... Il sera alors impossible pour un administrateur de restaurer les données supprimées si la politique de rétention des sauvegardes impose une rotation par écrasement des archives plus vieille d'une semaine. Afin de pouvoir restaurer dans différentes situations, il est possible de mettre deux plans de sauvegarde simultanément. Par exemple, un plan de sauvegarde hebdomadaire sur disque peut réaliser des archives avec un délai de rétention sur quatre semaines, tandis qu'un autre plan de sauvegarde mensuel sur bande peut réaliser des archives avec un délai de rétention sur un an.

- **Définir une stratégie de restauration des données** : il existe différentes méthodes pour restaurer des données en fonction des méthodes de sauvegarde ou récupération mises en place pour sécuriser l'infrastructure informatique. Lors d'un sinistre, il convient de déterminer à l'avance les méthodes de récupération des données en fonction de telle ou telle situation. Une stratégie de restauration doit être définie en accord avec les clauses définies dans les contrats de qualité de service. Par exemple, si un utilisateur perd un fichier, il sera plus rapide de tenter une restauration des données en jetant un œil dans le cache des clichés instantanés plutôt que de rapatrier une bande du centre de stockage des archives sauvegardées. Plus vite les données sont restaurées et plus grand est le pourcentage pour les administrateurs de respecter les clauses de qualité de service, ainsi que le temps d'interruption maximale admissible pour les utilisateurs. Tout plan de sauvegarde mis en place doit être validé et testé régulièrement afin de s'assurer que la stratégie de restauration est opérationnelle et que les données sauvegardées sont exploitables. Il arrive bien trop souvent qu'une entreprise sauvegarde des données sur bande et que le jour où une restauration s'impose, les administrateurs se retrouvent impuissants face à une bande vierge ou contenant des données inexploitable. Il faut donc systématiquement tester que le processus de restauration fonctionne et que les fichiers restaurés sont accessibles par les utilisateurs. Cela garantit ainsi l'intégrité des données restaurées ainsi que la qualité de service apporté.

2. Présentation de la sauvegarde

Il existe plusieurs technologies de sauvegarde des données, plusieurs supports de destination, plusieurs éditeurs tiers ; que les solutions utilisent des composants matériels ou logicielles.

On retrouve notamment des sauvegardes de données sur les supports suivants :

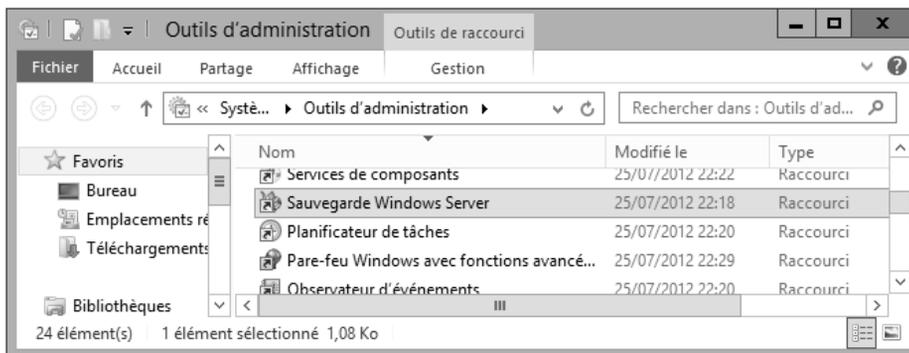
- **Cloud**
- **Disques durs internes/externes**
- **Supports amovibles**
- **CD/DVD ROM**
- **Emplacements réseau**
- **Réplication des données (sur un équipement redondé ou un emplacement géographique différent)**
- **Bandes de sauvegarde**
- **Clichés instantanés**
- **RAID**
- **Snapshots (sauvegarde de l'état du système à un instant précis)**

La plupart des solutions logicielles existantes issues d'éditeurs tiers utilisent des composants qui nécessitent un serveur sur lequel installer la solution de sauvegarde et des agents installés sur chaque serveur pour assurer la communication et le transfert des données à sauvegarder. Ce manuel ne couvre que la solution de sauvegarde intégrée au système d'exploitation Windows Server 2012 R2 (fonctionnalité **Sauvegarde Windows Server**), les clichés instantanés (**Shadow Copy**), ainsi que le système de sauvegarde de type Cloud proposé par Microsoft et nommé **Windows Azure Online Backup**.

3. Sauvegarde Windows Server

Le système d'exploitation Microsoft Windows Server 2012 R2 intègre nativement la fonctionnalité de serveur nommée **Sauvegarde Windows Server**.

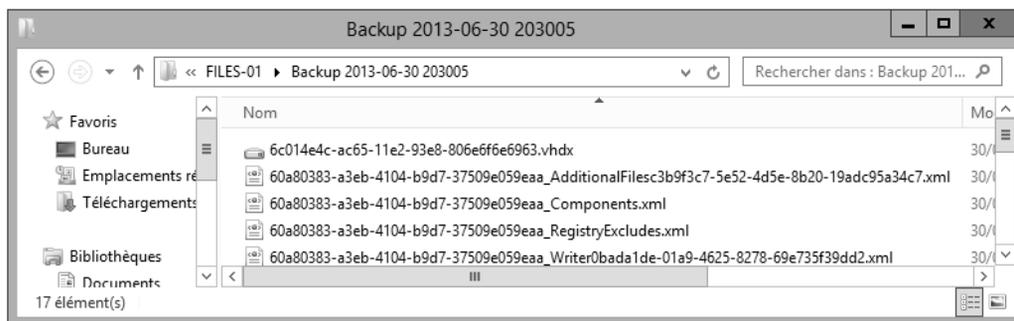
Une fois installé, cet utilitaire se présente sous la forme d'un composant logiciel enfichable accessible depuis le répertoire système `%Windir%\system32\wbadmin.msc`, les outils d'administration du système d'exploitation ou via le Gestionnaire de serveur.



Cet utilitaire permet notamment de gérer les sauvegardes locales (emplacement réseau, volume disque) ou en ligne (**Windows Azure Online Backup**).

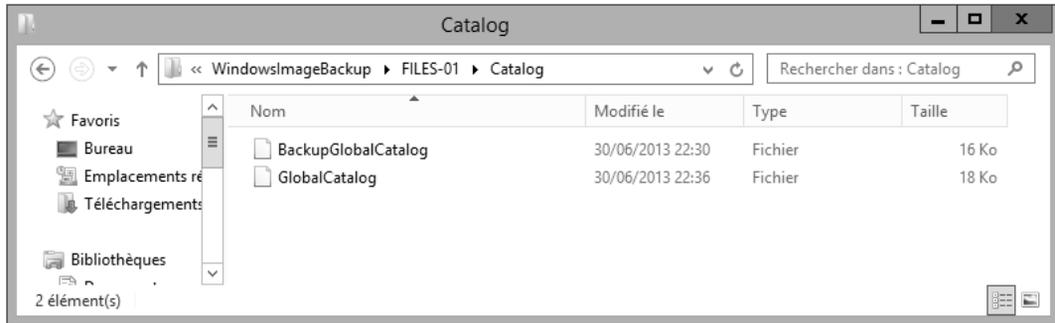
Lorsqu'une sauvegarde est exécutée via cet outil, le composant logiciel enfichable *Sauvegarde Windows Server*, crée un disque virtuel du volume à archiver. Ce disque virtuel est un fichier image au format *.vhdx, qui est le nouveau format de stockage des machines virtuelles sous Microsoft Hyper-V3. Les disques virtuels VHDX peuvent supporter 64 To de données. Le disque virtuel dédié à la sauvegarde des données est créé à l'emplacement suivant :

[Lecteur:]\WindowsImageBackup\[Nom du serveur]\Backup [Date de la sauvegarde]



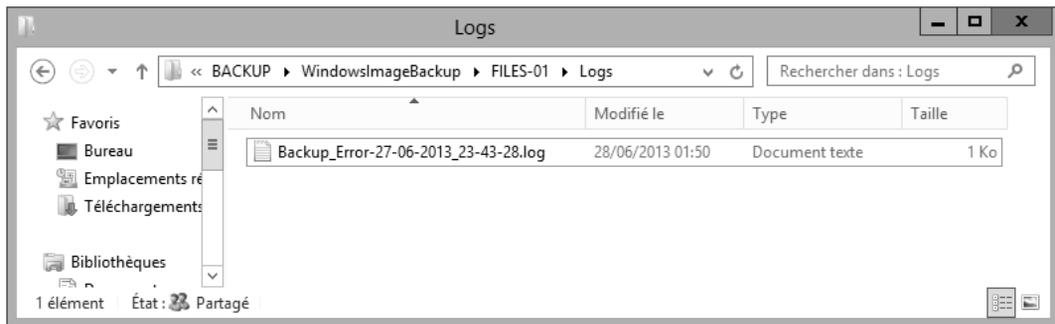
Il est possible de naviguer à tout moment dans ces fichiers image de disque dur au travers du composant logiciel enfichable. L'utilitaire crée les fichiers *BackupGlobalCatalog* et *GlobalCatalog* qui enregistrent la configuration des volumes sauvegardés dans l'arborescence suivante :

[Lecteur:]\WindowsImageBackup\[Nom du serveur]\Catalog



Chaque sauvegarde réalisée doit être vérifiée afin de s'assurer que les données sont accessibles en cas de demande de restauration en urgence. Si un incident survient pendant le processus de sauvegarde, l'utilitaire enregistre des logs d'erreurs à l'emplacement suivant :

[Lecteur:]\\WindowsImageBackup[Nom du serveur]Logs



L'utilitaire de sauvegarde permet l'archivage de l'ensemble des données des systèmes d'exploitation Windows Server, ainsi que des machines virtuelles fonctionnant sous Hyper-V.

a. Gestion de la sauvegarde Windows Server

La console de gestion **Sauvegarde Windows Server** permet de gérer les types **Sauvegarde locale** ou **Sauvegarde en ligne**. Le menu **Actions** de la **Sauvegarde locale** permet de gérer les éléments suivants :

