www.tri.0fees.net

PROJET DE FIN DE FORMATION

MICROSOFT WINDOWS SERVER® 2008

EST UNE NOUVELLE GÉNÉRATION DU SYSTÈME D'EXPLOITATION WINDOWS SERVER CONÇUE POUR AIDER LES ADMINISTRATEURS SYSTÈME À RATIONALISER LEURS INFRASTRUCTURES.

Réalisé par : Mr AL ECHCHEIKH EL ALAOUI ADNANE
Filière : Techniques de Réseaux Informatiques
ISTA ERRACHIDIA
2008/2009

SOMMAIRE

1. INTRUDUCTION 3
2. Présentation de Windows Server 2008 4
3. Ensemble des rôles Active Directory 7
4. Virtualisation Windows Server 22
5. Accès centralisé aux applications 24
6. Application de la stratégie et de la sécurité 30
7. Plate-forme Web et d'applications 45
8. Gestion des serveurs 53
9. Conclusion 70

INTRUDUCTION

Windows Server 2008 tire pleinement parti des grandes innovations qui sont intervenues depuis la mise à disposition de ses prédécesseurs : l'évolution des processeurs vers le 64bit et les architectures multi-coeurs, généralisation de la virtualisation, pilotage fin des bilans énergétiques, nouvelles méthodes de développement et de test sécurisées (TWC).
Windows Server 2008 est une solution conçue pour répondre aux problématiques de montée en charge, de haute disponibilité et d'agilité requises dans les centres de traitement et habituellement résolues avec des mainframes ou des Unix historiques.
En même temps, il conserve l'ergonomie de ses prédécesseurs et met à la disposition des organisations de toute taille les technologies de virtualisation, de sécurité et de haute disponibilité qui leur étaient inaccessibles.
Pour cela, Windows Server 2008 innove sur 4 axes majeurs :

Aider à gérer la complexité

De nouveaux outils de gestion des serveurs permettent d'automatiser
les tâches récurrentes (Windows PowerShell™) en vous offrant la possibilité d'installer, de configurer et d'administrer vos serveurs locaux et distants depuis une interface unique et centralisée (la console Server Manager). La fonction de clusters dans Windows Server 2008 a été améliorée pour offrir une solution de haute disponibilité qui protège les applications critiques, les services et les informations des utilisateurs. Les services de déploiement Windows (WDS) réduisent le coût et la complexité des déploiements des systèmes d'exploitation sur les postes clients et les serveurs. Enfin l'installation de Windows Server 2008 en mode minimaliste (Server Core) permet de ne pas s'encombrer des composants inutiles. Cela réduit les interventions de mises à jour et les interruptions de services qui peuvent en découler.

Ouvrir le réseau et protéger les données

NAP (Network Access Protection) est une fonctionnalité clé de Windows Server 2008 qui permet de contrôler l'accès au réseau des ordinateurs en vérifiant la bonne santé de leur système et leur conformité aux politiques de sécurité de l'entreprise. Citons également le renforcement des services Windows pour
un système d'exploitation plus résistant contre les attaques, la nouvelle option d'installation Server Core qui diminue la surface exposée aux risques informatiques, ainsi que le contrôleur de domaine en lecture seule (RODC) qui permet de renforcer la sécurité dans les sites distants. Enfin, Windows Server 2008 contient le serveur Active Directory Right Management Server qui permet de contrôler et de restreindre la diffusion et l'accès aux informations de l'entreprise.

Rationaliser les infrastructures avec la virtualisation

Windows Serveur 2008 permet de consolider les serveurs X86 (virtualisation de serveurs) et de centraliser les applications (virtualisation de présentation). Hyper-V, l'hyperviseur de Windows Server 2008, est une architecture moderne de para-virtualisation conçue pour héberger des machines virtuelles multi-processeurs et 64 bits et permettre ainsi de rationaliser les investissements matériels. Cette technologie est intégrée directement dans le système d'exploitation et ne requiert

donc aucun investissement complémentaire. La génération 2008 de cette technologie est parfaitement compatible avec les précédentes et utilise les mêmes outils de supervision (System Center Virtual Machine Manager). Pour les entreprises qui ont une stratégie de centralisation des applications, les nouveaux services Terminal Services intégrés à Windows Server 2008 proposent 3 innovations très significatives, notamment pour les populations nomades : une fonction de passerelle d'accès aux applications qui permet d'y accéder à partir de n'importe quelle connexion internet, l'amélioration de l'ergonomie d'accès aux applications et la fonction « EasyPrint » qui permet d'exploiter plus simplement les imprimantes.

Faciliter l'évolution du Web

Internet Information Server 7.0 (IIS 7), le nouveau serveur Web de Windows Server 2008, permet une montée en puissance des infrastructures Web pour internet ou pour les intranets. Il permet aussi de reprendre l'existant – ASP, ASP.NET et PHP – avec un minimum de modifications. Fortement intégré à Windows Server 2008, il tire pleinement parti des fonctions de celui-ci pour la sécurité, l'administration, la haute disponibilité et la montée en charge. Windows® Sharepoint Services 3.0 (WSS 3.0) est un service téléchargeable pour Windows Server 2008 qui permet de créer des sites web spécialisés pour le partage d'informations et de documents dans l'entreprise. WSS 3.0 permet de déployer rapidement des démarches collaboratives et sa mise en œuvre est couverte par les licences de Windows Server 2008.

PRÉSENTATION DE WINDOWS SERVER 2008

Microsoft Windows Server® 2008 est une nouvelle génération du système d'exploitation Windows Server conçue pour aider les administrateurs système à rationaliser leurs infrastructures.
Windows Server 2008 innove sur 4 axes majeurs :

Virtualisation

Terminal Services est une fonction de Windows Server 2008 qui permet de faire fonctionner une ou plusieurs applications sur un serveur centralisé en déportant uniquement les interfaces utilisateurs vers le poste de travail de l'utilisateur.
Terminal Services Gateway est une extension à Terminal Services qui permet d'accéder à Terminal Services sans être connecté directement au réseau de l'entreprise. C'est une fonction très intéressante pour les populations nomades.
Terminal Services Easy Print permet d'utiliser des imprimantes locales au poste de travail sans avoir à monter des pilotes d'impression sur le serveur.
Terminal Services Remote App est une extension de Terminal Services qui permet d'améliorer l'expérience de l'utilisateur Grâce à cette nouvelle fonction, l'utilisateur ne fait plus du tout la différence entre une application locale et une application qui est exécutée à distance. Cela améliore leur productivité et diminue les coûts de support et de formation aux utilisateurs.
Hyper-V, l'hyperviseur de Windows Server 2008, est une très fine couche de logiciel qui s'intercale entre le matériel et les systèmes d'exploitation (les serveurs virtualisés) pour que ceux-ci se partagent les ressources mémoire et processeurs de la machine. Les serveurs virtualisés n'opèrent pas nécessairement sous les mêmes environnements. Cela permet de faire passer le taux d'utilisation des serveurs x86 d'une tranche de 8-15% à une tranche de 30-40% et donc de rationaliser les investissements en terme de matériel.

Sécurité

Windows Right Management Server est un service inclus dans Windows Server 2008 et qui permet de gérer ce que chacun a le droit de faire d'un document donné. Ainsi l'auteur d'un document va pouvoir en restreindre la lecture, la modification, l'impression ou le transfert par mail à un nombre limité de personnes.
Network Access Protection (NAP) est une technologie Microsoft permettant de contrôler l'accès au réseau d'un ordinateur en se basant sur la santé de son système. NAP est utilisée pour faire respecter la stratégie de sécurité de l'entreprise : lorsqu'un ordinateur, qu'il appartienne à un utilisateur interne, à un utilisateur mobile ou à un visiteur, tente de se connecter au réseau de l'entreprise, NAP vérifie sa conformité à la stratégie de sécurité de l'entreprise. Si cet ordinateur s'avère infecté ou non conforme, NAP lui refuse l'accès au réseau et tente de mettre à jour le système avant qu'il puisse se connecter au réseau.
Windows BitLocker™ Drive Encryption, ou chiffrement complet de l'espace de stockage, est une fonctionnalité clé de Windows Server 2008 améliorant la protection des serveurs, des postes de travail, ordinateurs portables et autres équipements mobiles. Il encode le contenu du disque dur afin que les données soient protégées, même si elles tombent dans de mauvaises mains.
Read-Only Domain Controller (RODC), ou contrôleur de domaine en lecture seule, permet de sauvegarder des comptes utilisateurs là où la sécurité physique ne peut être garantie. RODC fournit une authentification locale pour les utilisateurs des succursales et des agences sans copier entièrement la base de données Active Directory, ce qui réduit les risques.
Active Directory Federation Services (ADFS) est un composant de Windows Server 2008 qui offre à l'utilisateur une expérience d'authentification unique. Avec ADFS, l'utilisateur peut donc accéder à des applications distinctes dans des entreprises indépendantes sans avoir à présenter des informations d'identification à chaque application.

Web

Internet Information Server 7.0 (IIS 7) est le serveur Web livré avec Windows Server 2008. C'est le composant fondateur d'une infrastructure de site Web pour Internet, de site intranet, ou bien encore pour déployer ou intégrer des services Web. Fortement intégré à Windows Server 2008 il tire pleinement parti des fonctions de celui-ci pour la sécurité, l'administration, la haute disponibilité et la montée en puissance.
Windows SharePoint Services (WSS) 3.0 est un service téléchargeable pour Windows Server 2008 qui permet de créer des sites Web spécialisés pour le partage d'informations et de documents. Il permet de déployer rapidement des démarches collaboratives. La mise en oeuvre de WSS 3.0 est couverte par les licences de Windows Server.

Fondations du système

Windows PowerShell est un langage de script en mode ligne de commande qui permet aux administrateurs d'automatiser et de personnaliser les tâches d'administration en toute sécurité.
Server Manager est un nouvel outil permettant d'installer, de configurer et d'administrer les serveurs depuis une seule et unique console.
La fonction de clusters (failover clustering) dans Windows Server 2008 a été améliorée en vue de simplifier sa mise en oeuvre et d'améliorer la stabilité des clusters. Cette fonctionnalité permet d'offrir aux organisations une solution de « haute disponibilité » afin que les applications critiques, les services et les informations restent à la disposition de tous les utilisateurs, y compris en cas de catastrophe.
Server Core est une nouvelle option d'installation pour certains scénarios d'usage qui permet de n'installer un serveur qu'avec les éléments strictement nécessaires à son fonctionnement. Avec cette option, vous diminuez la charge de mises à jour du serveur et les interruptions éventuelles liées à la maintenance. En n'installant que les composants nécessaires pour un rôle, vous réduisez également la surface d'exposition aux risques informatiques.

Windows Deployment Services, ou services de déploiement Windows (WDS), est une version repensée des ser vices d'installation à distance, qui accélère le déploiement rapide et massif des systèmes d'exploitation Windows à partir d'une image. Avec WDS, vous pouvez effectuer une installation réseau de Windows Server 2008 (ainsi que de Windows Vista®) sur des ordinateurs nus (qui ne disposent pas de système d'exploitation). Ainsi, les services de déploiement Windows offrent une solution complète pour le déploiement des systèmes d'exploitation Windows sur les postes clients et les serveurs, et réduit le coût total de possession et la complexité des déploiements Windows Server 2008 et Windows Vista.

Task scheduler est un ordonnanceur de tâche.

Windows Remote Shell permet d'exécuter des commandes primitives du système d'exploitation à distance.

Editions et fonctionnalités disponibles de Windows Server 2008

● Inclus ❍ Disponible partiellement

Fonctionnalités	Enterprise	Datacenter	Standard	Itanium	Web
Web Services (IIS)	●	●	●	●	●
Application Server	●	●	●	●	
Print Services	●	●	●		
Windows SharePoint Services[1]	●	●	●		
Hyper-V[2]	●	●	●		
Active Directory Domain Services	●	●	●		
Active Directory Lightweight Directory Services	●	●	●		
Active Directory Rights Management Services	●	●	●		
DHCP Server	●	●	●		
DNS Server	●	●	●		
Fax Server	●	●	●		
UDDI Services	●	●	●		
Windows Deployment Services	●	●	●		
Active Directory Certificate Services	●	●	❍[3]		
File Services	●	●	❍[4]		
Network Policy and Access Services	●	●	❍[5]		
Terminal Services	●	●	❍[6]		
Active Directory Federation Services	●	●			

Mode d'installation Server Core

La nouvelle option d'installation Server Core permet de supporter les fonctionnalités suivantes :

Fonctionnalités	Enterprise	Datacenter	Standard	Itanium	Web
Web Services (IIS)	●	●	●		●
Print Services	●	●	●		
Hyper-V[1]	●	●	●		
Active Directory Domain Services	●	●	●		
Active Directory Lightweight Directory Services	●	●	●		
DHCP Server	●	●	●		
DNS Server	●	●	●		
File Services	●	●	❍[2]		

Configuration requise

Processeur	**Minimum :** 1GHz pour ordinateurs x86 et 1.4GHz pour ordinateurs x64 **Recommandé :** 2 GHz **Optimal :** 3 GHz ou supérieur
Espace disque requis	**Minimum :** 10 Go **Recommandé :** 40 Go (installation complète) ou 10 Go (installation Server Core) **Optimal :** 80 Go (installation complète) ou 40 Go (installation Server Core) ou plus **Remarque : Les ordinateurs avec plus de 16 Go de RAM nécessiteront davantage d'espace disque pour les fichiers de pagination, de mise en veille prolongée et de vidage**
Mémoire	**Minimum :** 512 Mo de RAM **Recommandé :** 2 Go de RAM ou plus **Maximum (systèmes 32 bits) :** 4 Go (Standard) ou 64 Go (Enterprise et Datacenter) **Maximum (systèmes 64 bits) :** 32 Go (Standard) ou 2 To (Enterprise, Datacenter et pour système Itanium)
Lecteur	Lecteur de DVD-ROM
Autres périphériques requis	Moniteur Super VGA (800 × 600) ou résolution supérieure Clavier et souris Microsoft ou dispositif de pointage compatible

ENSEMBLE DES RÔLES ACTIVE DIRECTORY

Services de certificats Active Directory

Les services de certificats Active Directory (AD CS) fournissent des services personnalisables pour l'émission et la gestion de certificats qui sont utilisés dans les systèmes de sécurité logiciels employant des technologies de clé publique.

Dans les sections suivantes, découvrez les services AD CS, les fonctionnalités requises et facultatives dans les services AD CS, ainsi que les logiciels et le matériel utilisés pour l'exécution des services AD CS. À la fin de cette rubrique, apprenez à ouvrir l'interface des services AD CS et à découvrir plus d'informations sur les services AD CS.

Fonctionnalités des services AD CS

À l'aide du Gestionnaire de serveur, vous pouvez configurer les composants suivants des services AD CS :

- Autorités de certification. Des autorités de certification racine et secondaires sont utilisés pour émettre des certificats aux utilisateurs, aux ordinateurs et aux services, et pour gérer la validité des certificats.
- Inscription via le Web. L'inscription via le Web permet aux utilisateurs de se connecter à une autorité de certification au moyen d'un navigateur Web afin de demander des certificats et de récupérer des listes de révocation de certificats.
- Répondeur en ligne. Le service Répondeur en ligne décode les demandes d'état de révocation pour des certificats spécifiques, évalue l'état de ces certificats et renvoie une réponse signée contenant les informations demandées sur l'état des certificats.
- Service d'inscription de périphériques réseau. Le Service d'inscription de périphériques réseau permet aux routeurs et à d'autres périphériques réseaux ne possédant pas de comptes de domaine d'obtenir des certificats.

Avantages des services AD CS

Les organisations peuvent utiliser les services AD CS pour améliorer la sécurité en liant l'identité d'une personne, d'un périphérique d'un service à une clé privé correspondante. Les services AD CS

offrent une solution rentable, efficace et sécurisée pour gérer la distribution et l'utilisation des certificats.

Les applications prises en charge par les services AD CS incluent les extensions S/MIME (Secure/Multipurpose Internet Mail Extensions), les réseaux sans fil sécurisés, les réseaux privés virtuels (VPN), la sécurité du protocole Internet (IPsec), le système de fichiers EFS, l'ouverture de session par carte à puce, SSL/TLS (Secure Socket Layer/Transport Layer Security) et les signatures numériques.

Dans Windows Server® 2008, les services AD CS présentent les nouvelles fonctionnalités suivantes :

- Des capacités d'inscription améliorée qui permettent l'attribution d'agents d'inscription délégués en fonction des modèles.
- Des services d'inscription SCEP (Simple Certificate Enrollment Protocol) intégrés qui permettent d'émettre des certificats à des périphériques réseau tels que des routeurs.
- Des services de réponse d'état de révocation évolutifs et rapides combinant à la fois les listes de révocation de certificats et les services Répondeur en ligne intégrés.

Considérations logicielles et matérielles

Les services AD CS nécessitent Windows Server 2008 et les services de domaine Active Directory (AD DS). Bien que les services AD CS puissent être déployés sur un serveur unique, de nombreux déploiements impliquent plusieurs serveurs configurés en tant qu'autorités de certification, d'autres serveurs configurés en tant que répondeurs en ligne et d'autres serveurs servant de portails d'inscription via le Web. Vous pouvez configurer des autorités de certification sur des serveurs exécutant divers systèmes d'exploitation, y compris Windows Server 2008, Windows Server 2003 et Windows 2000 Server. Toutefois, tous les systèmes d'exploitation ne prennent pas en charge l'ensemble des fonctionnalités ou des conditions de conception. Ainsi, pour créer une conception optimale, vous devrez planifier et tester minutieusement les services AD CS avant de les déployer dans un environnement de production.

Installation des services AD CS

Au terme de l'installation du système d'exploitation, vous pouvez configurer une autorité de certification et d'autres composants facultatifs à l'aide du Gestionnaire de serveur.

Pour qu'une autorité de certification ou un répondeur en ligne soit fonctionnel, vous devez effectuer d'autres étapes de configuration à l'aide des composants logiciels enfichables appropriés. Pour plus d'informations, voir les rubriques d'aide associées pour les composants logiciels enfichables Autorité de certification et Répondeur en ligne.

Gestion des services AD CS

Les services de rôle AD CS sont gérés à l'aide de composants logiciels enfichables MMC (Microsoft Management Console).

- Pour gérer une autorité de certification, utilisez le composant logiciel enfichable Autorité de certification. Pour ouvrir le composant logiciel enfichable Autorité de certification, cliquez sur Démarrer, sur Exécuter, tapez mmc, cliquez sur Fichier, sur Ajouter/Supprimer un composant logiciel enfichable, sur Autorité de certification, sur Ajouter, sur OK, puis double-cliquez sur Autorité de certification.
- Pour gérer des certificats, utilisez le composant logiciel enfichable Certificats. Pour ouvrir le composant logiciel enfichable Certificats, cliquez sur Démarrer, sur Exécuter, tapez mmc,

cliquez sur Fichier, sur Ajouter/Supprimer un composant logiciel enfichable, sur Certificats, sur Ajouter, sur OK, puis double-cliquez sur Certificats.

- Pour gérer des modèles de certificats, utilisez le composant logiciel enfichable Modèles de certificats. Pour ouvrir le composant logiciel enfichable Modèles de certificats, cliquez sur Démarrer, sur Exécuter, tapez mmc, cliquez sur Fichier, sur Ajouter/Supprimer un composant logiciel enfichable, sur Modèles de certificats, sur Ajouter, sur OK, puis double-cliquez sur Modèles de certificats.
- Pour gérer un répondeur en ligne, utilisez le composant logiciel enfichable Répondeur en ligne. Pour ouvrir le composant logiciel enfichable Répondeur en ligne, cliquez sur Démarrer, sur Exécuter, tapez mmc, cliquez sur Fichier, sur Ajouter/Supprimer un composant logiciel enfichable, sur Répondeur en ligne, sur Ajouter, sur OK, puis double-cliquez sur Répondeur en ligne.

Si vous utilisez Windows Server 2008, mais que vous n'avez pas encore installé l'un des services de rôle AD CS, seul le composant logiciel enfichable Certificats est installé par défaut. Vous pouvez installer les composants logiciels enfichables restants sans installer les services de rôle AD CS à l'aide du Gestionnaire de serveur en sélectionnant les outils des services de certificats Active Directory sous Outils d'administration de serveur distant Si l'ordinateur à partir duquel vous voulez effectuer des tâches d'administration à distance exécute Windows Vista.

Services de domaine Active Directory

En utilisant le rôle de serveur Services de domaine Active Directory® (AD DS) sous le système d'exploitation Windows Server® 2008, vous pouvez créer une infrastructure évolutive, sécurisée et gérable pour la gestion des utilisateurs et des ressources et vous pouvez assurer la prise en charge des applications utilisant un annuaire, telles que Microsoft® Exchange Server.

Dans les sections suivantes, vous obtiendrez plus d'informations sur AD DS, les fonctionnalités proposées dans AD DS, ainsi que sur les considérations d'ordre logiciel et matériel. Pour plus d'informations sur la planification, le déploiement et l'utilisation du rôle de serveur AD DS, et pour obtenir une référence technique qui explique comment AD DS fonctionne et les différents outils et paramètres que ces services utilisent.

Qu'est-ce que le rôle de serveur AD DS ?

AD DS fournit une base de données distribuée qui stocke et gère des informations sur les ressources réseau et les données spécifiques à des applications provenant d'applications utilisant un annuaire. Les administrateurs peuvent utiliser AD DS pour organiser les éléments d'un réseau, tels que les utilisateurs, les ordinateurs et les autres périphériques, en une structure hiérarchique de type contenant-contenu. La structure hiérarchique de type contenant-contenu inclut la forêt Active Directory, les domaines inclus dans la forêt et les unités d'organisation (OU) de chaque domaine. Un serveur qui exécute AD DS est nommé contrôleur de domaine.

L'organisation des éléments d'un réseau en une structure hiérarchique de type contenant-contenu offre les avantages suivants :

- La forêt agit comme une limite de sécurité pour une organisation et définit l'étendue de l'autorité des administrateurs. Par défaut, une forêt contient un domaine unique, appelé également domaine racine de la forêt.
- Des domaines supplémentaires peuvent être créés dans la forêt pour assurer le partitionnement des données AD DS, ce qui permet aux organisations de répliquer des données uniquement là où cela est nécessaire. Cela permet le dimensionnement global des services AD DS sur un réseau disposant d'une bande passante limitée. Un domaine Active Directory prend en charge

également plusieurs autres fonctions principales liées à l'administration, dont notamment l'identité des utilisateurs, l'authentification et les relations d'approbation à l'échelle du réseau.

- Les unités d'organisations simplifient la délégation de l'autorité pour faciliter la gestion d'un grand nombre d'objets. Par le biais de la délégation, des propriétaires peuvent transférer une autorité complète ou limitée sur des objets à d'autres utilisateurs ou groupes. La délégation est importante car elle aide à distribuer la gestion d'un grand nombre d'objets à plusieurs personnes chargées d'effectuer des tâches de gestion.

Fonctionnalités proposées dans AD DS

La sécurité est intégrée dans AD DS par le biais de l'authentification d'ouverture de session et le contrôle d'accès aux ressources de l'annuaire. À l'aide d'une ouverture de session réseau unique, les administrateurs peuvent gérer les données et l'organisation de l'annuaire par le biais de leur réseau. Les utilisateurs réseau autorisés peuvent également utiliser une ouverture de session réseau unique pour accéder à des ressources à tout emplacement sur le réseau. L'administration basée sur des stratégies facilite même la gestion des réseaux les plus complexes.

Autres fonctionnalités des services AD DS :

- Un ensemble de règles, le schéma, qui définit les classes d'objets et les attributs contenus dans l'annuaire, les contraintes et les limites qui s'appliquent aux instances de ces objets, ainsi que le format de leurs noms.
- Un catalogue global qui contient des informations sur chaque objet de l'annuaire. Les utilisateurs et les administrateurs peuvent utiliser le catalogue global pour rechercher des informations dans l'annuaire, quel que soit le domaine de l'annuaire qui contient les données.
- Un mécanisme de requête et d'index, de sorte que les objets et leurs propriétés puissent être publiés et recherchés par les utilisateurs du réseau ou des applications.
- Un service de réplication qui distribue les données d'annuaire sur l'ensemble du réseau. Tous les contrôleurs de domaine accessibles en écriture dans un domaine participent à la réplication et contiennent une copie complète de toutes les informations d'annuaire liées à leur domaine. Toute modification des données d'annuaire est répliquée sur tous les contrôleurs de domaine inclus dans le domaine.
- Les rôles de maître d'opérations (également appelés opérations à maître unique flottant ou FSMO). Les contrôleurs de domaine qui détiennent des rôles de maître d'opérations sont désignés pour effectuer des tâches spécifiques pour assurer la cohérence et éliminer les entrées en conflit dans l'annuaire.

Gestion des identités pour UNIX

La gestion des identités pour UNIX est un service de rôle AD DS qui peut être installé uniquement sur des contrôleurs de domaine. Deux technologies de gestion des identités pour UNIX, Serveur pour NIS et Synchronisation de mot de passe, facilitent l'intégration des ordinateurs exécutant Windows® dans votre entreprise UNIX existante. Les administrateurs des services d'annuaire Active Directory peuvent utiliser Serveur pour NIS afin de gérer les domaines NIS (Network Information Service). La synchronisation de mot de passe synchronise automatiquement les mots de passe entre les systèmes d'exploitation Windows et UNIX.

Nouvelles fonctionnalités incluses dans les services d'annuaire Active Directory de Windows Server 2008

Windows Server 2008 inclut les nouvelles fonctionnalités AD DS répertoriées dans le tableau ci-dessous.

Fonctionnalité	Description

Contrôleur de domaine en lecture seule (RODC)	Un RODC correspond à un nouveau type de contrôleur de domaine qui héberge des partitions en lecture seule de la base de données Active Directory. Un RODC est particulièrement utile dans les cas suivants : • La sécurité physique d'un contrôleur de domaine ne peut pas être garantie ou son emplacement n'inclut pas d'administrateur doté de l'autorité à l'échelle du domaine requise pour administrer un contrôleur de domaine accessible en écriture. • Les utilisateurs situés dans une succursale peuvent bénéficier d'un processus d'ouverture de session plus efficace qui est fourni par un contrôleur de domaine local dans la succursale.
Installation intermédiaire d'un RODC	Cette fonctionnalité permet l'installation en deux phases d'un contrôleur de domaine en lecture seule. Au cours de la première phase, un membre du groupe Admins du domaine crée un compte pour le RODC. Au cours de la seconde phase, un utilisateur délégué joint un serveur au compte RODC.
Jeu d'attributs filtrés du RODC	Un jeu d'attributs de type secret qui n'est pas répliqué sur un RODC. Cela empêche que les valeurs des attributs soient révélées si un RODC est volé. Le jeu d'attributs filtrés du RODC peut être configuré dynamiquement pour une application.
Séparation des rôles d'administrateur	Cette fonctionnalité permet aux administrateurs de domaine de déléguer l'installation et l'administration d'un RODC à des utilisateurs n'ayant pas le statut d'administrateur.
Assistant Installation amélioré	L'Assistant Installation des services de domaine Active Directory (dcpromo.exe) propose une prise en charge améliorée des installations sans assistance, de la sélection de site et de l'installation intermédiaire des RODC, ainsi que d'autres options avancées.
Générer un support d'installation sécurisé	Cette fonctionnalité vous permet d'utiliser Ntdsutil.exe sous Windows Server 2008 pour créer un support d'installation sécurisé pour les installations ultérieures des services AD DS et ADLDS (Active Directory Lightweight Directory Services). Dans les versions antérieures de Windows Server, les administrateurs étaient incités à utiliser Ntbackup.exe pour créer un support d'installation de contrôleur de domaine. Dans Windows Server 2008, les administrateurs sont encouragés à utiliser Ntdsutil.exe pour créer le support d'installation. Vous pouvez créer un support ne contenant pas de secrets mis en cache (tels que des mots de passe) pour l'utiliser pour l'installation d'un RODC. Lorsque vous supprimez des secrets mis en cache du support d'installation, un utilisateur malveillant accédant au support d'installation ne peut pas en extraire de secrets.
Redémarrage des services AD DS	Vous pouvez utiliser cette fonctionnalité pour arrêter et redémarrer AD DS sans redémarrer le contrôleur de domaine lui-même. Les opérations hors connexion, telles que la défragmentation hors connexion, peuvent être exécutées plus rapidement car il n'est pas nécessaire de redémarrer le contrôleur de domaine en mode restauration des services d'annuaire.
Audit des modifications apportées à AD DS	Cette fonctionnalité configure l'audit AD DS avec une nouvelle sous-catégorie d'audit pour enregistrer dans le journal les valeurs anciennes et nouvelles lorsque des modifications sont apportées à des objets et à leurs attributs.
Stratégie de mots de passe stricte	Cette fonctionnalité permet de spécifier des stratégies de mots de passe et de verrouillage de compte pour certains utilisateurs et groupes de sécurité globaux dans un domaine. Elle utilise de nouveaux objets de paramétrage de

	mot de passe et des règles de priorité pour supprimer la restriction d'une stratégie unique pour chaque domaine.
Prise en charge des identificateurs MAPI dynamiques	Cette fonctionnalité permet l'affectation dynamique des identificateurs (ID) MAPI (Messaging API) (c'est-à-dire leur génération aléatoire à partir d'un pool réservé d'ID MAPI), outre leur affectation statique. Grâce aux ID MAPI dynamiques, vous pouvez étendre votre schéma Active Directory et ajouter des attributs personnalisés pour Exchange Server.
Outil d'exploration de données	Cette fonctionnalité vous permet de visualiser les données AD DS et ADLDS stockées dans des captures instantanées ou des sauvegardes en ligne. Bien que cette fonctionnalité ne vous permette pas de restaurer des objets ou des conteneurs supprimés, vous pouvez l'utiliser pour comparer des données dans des captures instantanées ou des sauvegardes qui sont prises à des moments différents pour décider des données à restaurer, sans avoir à redémarrer le contrôleur de domaine ou le serveur ADLDS.

Considérations matérielles et logicielles

Vous pouvez utiliser des compteurs de performance, des tests en laboratoire, des données provenant du matériel existant dans un environnement de production et des déploiements pilotes pour déterminer la capacité requise pour votre serveur. Les serveurs exécutant Windows Server 2008 ont besoin d'au moins 512 mégaoctets (Mo) de RAM et de 20 gigaoctets (Go) d'espace sur le disque dur.

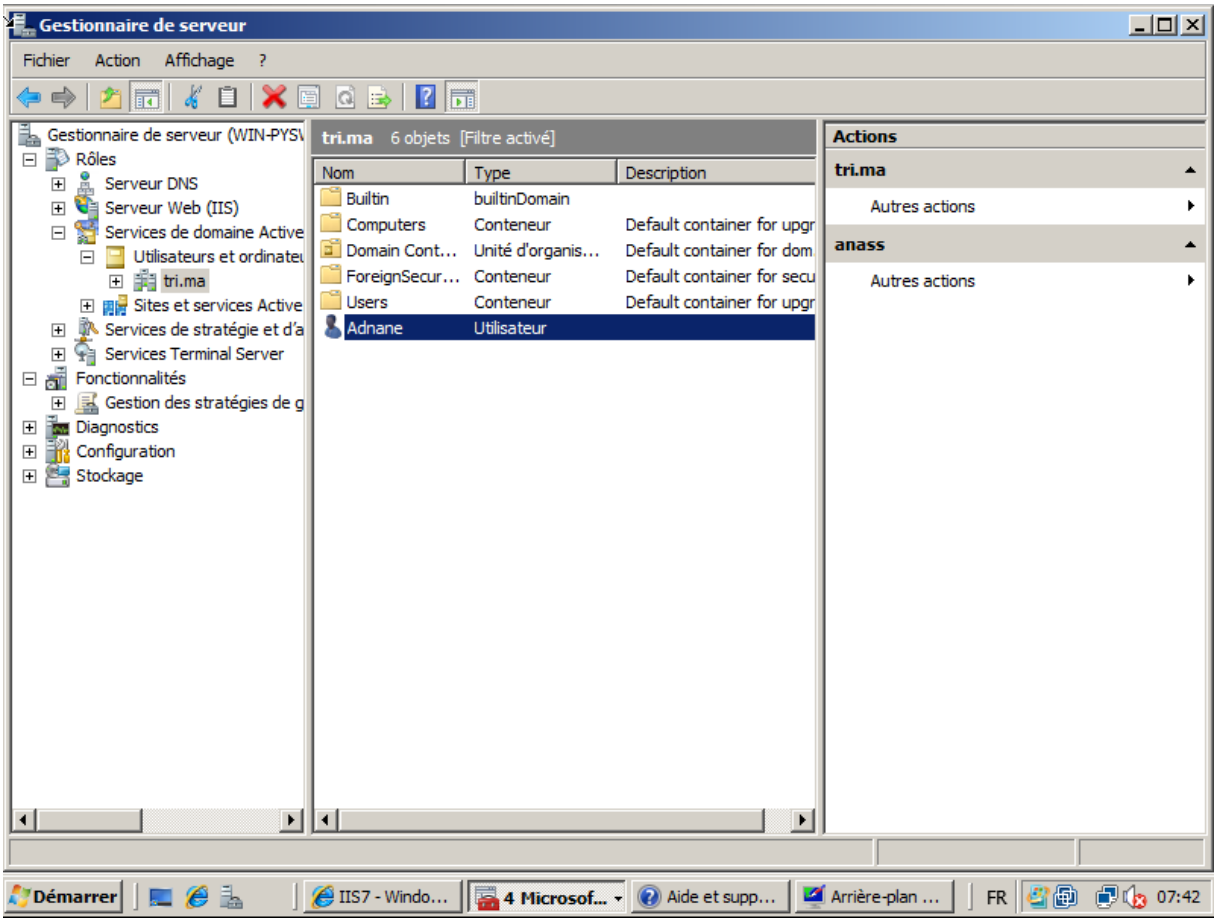
Important

- Outre l'espace disque minimal requis sur le disque dur, la mise à niveau des contrôleurs de domaine exécutant Microsoft Windows Server 2003 vers Windows Server 2008 requiert également deux fois plus d'espace que celui alloué actuellement pour la base de données Active Directory, les fichiers journaux et SYSVOL sur leurs volumes respectifs. Ces conditions doivent être respectées pour la restauration d'une mise à niveau. L'espace est recyclé automatiquement à la fin du processus de mise à niveau.

Le rôle de serveur AD DS requiert les services DNS (Domain Name System) pour localiser les ordinateurs, les contrôleurs de domaine, les serveurs membres et les services réseau par leur nom. Le rôle Serveur DNS fournit des services de résolution de noms DNS pour les réseaux TCP/IP en mappant les noms à des adresses IP, ce qui permet aux ordinateurs de localiser les ressources réseau dans un environnement AD DS.

En outre, les services AD DS doivent être installés sur le réseau pour implémenter d'autres technologies importantes Windows Server, telles que la stratégie de groupe et les services de certificats Active Directory (AD CS).

Installation du rôle de serveur AD DS



Une fois l'installation du système d'exploitation terminée, vous pouvez utiliser Tâches de configuration initiales ou Gestionnaire de serveur pour installer des rôles de serveur. Pour installer le rôle de serveur AD DS, cliquez sur Ajouter des rôles pour démarrer l'Assistant Ajout de rôles, puis cliquez sur Services de domaine Active Directory. Parcourez l'Assistant Ajout de rôles pour installer les fichiers pour le rôle de serveur AD DS. Une fois l'exécution de l'Assistant Ajout de rôles terminée, cliquez sur le lien permettant de démarrer l'Assistant Installation des services de domaine Active Directory.

Parcourez l'Assistant Installation des services de domaine Active Directory pour effectuer l'installation et la configuration de votre contrôleur de domaine. La plupart des pages de l'Assistant présentent un lien Aide pour plus d'informations sur les paramètres que vous pouvez configurer.

Pour automatiser les installations de contrôleurs de domaine, vous pouvez utiliser un fichier de réponses ou spécifier des paramètres d'installation sans assistance à la ligne de commande. Pour plus d'informations sur l'installation des services AD DS.

Gestion du rôle de serveur AD DS

Vous pouvez gérer les rôles de serveur à l'aide des composants logiciels enfichables MMC (Microsoft Management Console). Pour gérer un contrôleur de domaine (c'est-à-dire un serveur exécutant AD DS), cliquez sur Démarrer, sur Panneau de configuration, sur Outils d'administration, puis double-cliquez sur le composant logiciel enfichable approprié :

- Pour gérer les comptes d'utilisateurs et d'ordinateurs, cliquez sur Utilisateurs et ordinateurs Active Directory.

- Pour gérer les approbations Active Directory, les niveaux fonctionnels et les rôles de maître d'opérations à l'échelle de la forêt, cliquez sur Domaines et approbations Active Directory.
- Pour gérer les sites et les liens des sites Active Directory, cliquez sur Sites et services Active Directory.

Vous pouvez également double-cliquer sur le composant logiciel enfichable approprié dans la page Services de domaine Active Directory dans le Gestionnaire de serveur.

Les programmeurs et les administrateurs système expérimentés peuvent gérer le schéma Active Directory, mais le composant logiciel enfichable Schéma Active Directory n'est pas installé par défaut. De plus, le fichier schmmgmt.dll doit être enregistré avant que le composant logiciel enfichable puisse être installé.

Pour installer le composant logiciel enfichable Schéma Active Directory

1. Cliquez sur Démarrer, cliquez avec le bouton droit sur Invite de commandes, puis cliquez sur Exécuter en tant qu'administrateur.
2. Si la boîte de dialogue Contrôle de compte d'utilisateur apparaît, confirmez que l'action affichée est celle que vous souhaitez, puis cliquez sur Continuer.
3. Tapez la commande suivante et appuyez sur Entrée :

   regsvr32 schmmgmt.dll

4. Cliquez sur OK pour fermer la boîte de dialogue qui confirme que l'opération a réussi.
5. Cliquez sur Démarrer, sur Exécuter, tapez mmc, puis cliquez sur OK.
6. Si la boîte de dialogue Contrôle de compte d'utilisateur apparaît, confirmez que l'action affichée est celle que vous souhaitez, puis cliquez sur Continuer.
7. Dans le menu Fichier, cliquez sur Ajouter/Supprimer un composant logiciel enfichable.
8. Sous Composants logiciels enfichables disponibles, cliquez sur Schéma Active Directory, sur Ajouter, puis sur OK.
9. Pour enregistrer cette console, cliquez sur Enregistrer dans le menu Fichier.
10. Dans la boîte de dialogue Enregistrer sous, effectuez l'une des opérations suivantes :
    - Pour placer le composant logiciel enfichable dans le menu Outils d'administration, dans Nom de fichier, tapez un nom pour le composant logiciel enfichable, puis cliquez sur Enregistrer.
    - Pour enregistrer le composant logiciel enfichable dans un emplacement autre que le dossier Outils d'administration, dans Enregistrer dans, accédez à l'emplacement de votre choix. Dans Nom de fichier, tapez un nom pour le composant logiciel enfichable, puis cliquez sur Enregistrer.

Services ADFS (Active Directory Federation Services)

Vous pouvez utiliser le rôle de serveur AD FS (Active Directory® Federation Services) du système d'exploitation Microsoft® Windows Server® 2008 pour créer une solution d'accès aux identités sécurisée, hautement évolutive et pouvant être étendue à Internet, qui peut fonctionner sur plusieurs plateformes à la fois, qu'il s'agisse d'environnements Windows ou non-Windows.

Consultez les sections suivantes pour en savoir plus sur le rôle AD FS, avec entre autres une vue d'ensemble de la technologie ainsi que des consignes d'installation et de gestion.

Qu'est-ce qu'AD FS ?

AD FS est une solution d'accès aux identités qui offre aux clients de navigateur (appartenant ou non à votre réseau) un accès transparent en une seule étape à une ou plusieurs applications protégées qui sont

tournées vers Internet, même lorsque les comptes d'utilisateurs et les applications ne se trouvent pas du tout sur le même réseau ou dans la même organisation.

Lorsqu'une application se trouve sur un réseau et les comptes d'utilisateurs sur un autre, il est habituellement demandé aux utilisateurs de fournir des informations d'identification secondaires lorsqu'ils tentent d'accéder à l'application. Ces informations d'identification secondaires représentent l'identité des utilisateurs dans le domaine où réside l'application. Le serveur Web qui héberge l'application a généralement besoin de ces informations d'identification pour pouvoir prendre la décision d'autorisation la plus appropriée.

AD FS rend les comptes secondaires et leurs informations d'identification inutiles en fournissant des relations d'approbation que vous pouvez utiliser pour transmettre l'identité numérique et les droits d'accès d'un utilisateur aux partenaires approuvés. Dans un environnement fédéré, chaque organisation continue à gérer ses propres identités, mais peut aussi, en toute sécurité, transmettre et accepter des identités provenant d'autres organisations.

En outre, vous pouvez déployer des serveurs de fédération dans plusieurs organisations pour faciliter les transactions inter-entreprises (B2B) entre des organisations partenaires approuvées. Dans un partenariat inter-entreprises fédéré, chaque partenaire commercial est identifié selon les types d'organisation suivants :

- Organisation de ressource : les organisations qui possèdent et gèrent des ressources accessibles à partir d'Internet peuvent déployer des serveurs de fédération AD FS et des serveurs Web prenant en charge AD FS pour gérer l'accès aux ressources protégées pour les partenaires approuvés. Ces partenaires approuvés peuvent inclure des tiers externes ou d'autres services ou filiales de la même organisation.
- Organisation de compte : les organisations qui possèdent et gèrent des comptes d'utilisateurs peuvent déployer des serveurs de fédération AD FS qui authentifient les utilisateurs locaux et créent des jetons de sécurité que les serveurs de fédération de l'organisation de ressource utilisent ensuite pour prendre des décisions d'autorisation.

On appelle authentification unique (SSO) le processus consistant à s'authentifier sur un réseau tout en accédant à des ressources se trouvant sur un autre réseau, sans avoir à s'identifier plusieurs fois. AD FS fournit une solution SSO basée sur le Web qui authentifie les utilisateurs dans plusieurs applications Web au cours d'une même session de navigateur.

Services du rôle AD FS

Le rôle de serveur AD FS inclut des services de fédération, des services de proxy et des services d'agent Web que vous configurez pour activer l'authentification Web SSO, pour fédérer les ressources Web, pour personnaliser le processus d'accès et pour gérer la manière dont les utilisateurs sont autorisés à accéder aux applications.

En fonction des impératifs de votre organisation, vous pouvez déployer des serveurs exécutant n'importe lequel des services du rôle AD FS ci-dessous :

- Service de fédération : le service de fédération comprend un ou plusieurs serveurs de fédération qui partagent une stratégie d'approbation commune. Vous utilisez les serveurs de fédération pour acheminer les demandes d'authentification émises par les comptes d'utilisateurs d'autres organisations ou par des clients se trouvant n'importe où sur Internet.
- Proxy du service de fédération : le proxy du service de fédération fait office de proxy pour le service de fédération dans le réseau de périmètre (également appelé zone démilitarisée et sous-réseau filtré). Le proxy du service de fédération utilise les protocoles WS-F PRP (WS-Federation Passive Requestor Profile) pour collecter les informations d'identification des

utilisateurs auprès des clients de navigateur, puis envoie de leur part les informations d'identification au service de fédération.

- Agent prenant en charge les revendications : l'agent prenant en charge les revendications peut être utilisé sur un serveur Web hébergeant une application prenant en charge les revendications pour permettre l'interrogation des revendications des jetons de sécurité AD FS. Une application prenant en charge les revendications est une application Microsoft ASP.NET qui utilise les revendications présentes dans un jeton de sécurité AD FS pour prendre des décisions d'autorisation et personnaliser des applications.
- Agent basé sur les jetons Windows : l'agent basé sur les jetons Windows peut être utilisé sur un serveur Web hébergeant une application basée sur une autorisation de jeton Windows NT pour prendre en charge la conversion d'un jeton de sécurité AD FS en jeton d'accès Windows NT d'emprunt d'identité. Une application basée sur une autorisation de jeton Windows NT est une application qui utilise des mécanismes d'autorisation basés sur Windows.

Installation du rôle AD FS

Une fois que vous avez fini d'installer le système d'exploitation, une liste de tâches de configuration initiales s'affiche. Pour installer AD FS, dans la liste des tâches, cliquez sur Ajouter des rôles, puis sur Services ADFS (Active Directory Federation Services).

Gestion du rôle AD FS

Vous pouvez gérer les rôles de serveur à l'aide de composants logiciels enfichables MMC (Microsoft Management Console). Après avoir installé AD FS, vous pouvez utiliser le composant logiciel enfichable Services ADFS (Active Directory Federation Services) pour gérer le service de fédération et le proxy du service de fédération. Pour ouvrir ce composant logiciel enfichable, cliquez sur Démarrer, sur Outils d'administration, puis sur Services ADFS (Active Directory Federation Services).

Pour gérer l'agent basé sur les jetons Windows, cliquez successivement sur Démarrer, Outils d'administration et Gestionnaire des services Internet (IIS), puis cliquez sur Connexion à localhost.

Services AD LDS (Active Directory Lightweight Directory Services)

À l'aide du rôle Windows Server 2008 AD LDS (Active Directory® Lightweight Directory Services), anciennement appelé Active Directory Application Mode (ADAM), vous pouvez fournir des services d'annuaire aux applications utilisant un annuaire sans être soumis à la surcharge représentée par les domaines et les forêts, ou à l'obligation de disposer d'un schéma unique dans l'ensemble d'une forêt.

Consultez les sections suivantes pour en savoir plus sur le rôle de serveur AD LDS, ses fonctionnalités et les considérations logicielles et matérielles relatives à son installation.

Qu'est-ce que le rôle de serveur AD LDS ?

AD LDS est un service d'annuaire LDAP (Lightweight Directory Access Protocol) qui fournit une prise en charge flexible des applications compatibles avec l'annuaire, sans les dépendances requises pour les services de domaine Active Directory (AD DS, Active Directory Domain Services). Les services AD LDS (Active Directory Lightweight Directory Services) fournissent quasiment les mêmes fonctionnalités que les services de domaine Active Directory, mais sans imposer le déploiement de domaines ni de contrôleurs de domaines. Vous pouvez exécuter simultanément plusieurs instances AD LDS sur un même ordinateur, avec un schéma géré indépendamment pour chaque instance AD LDS.

Les services de domaine Active Directory fournissent des services d'annuaire aussi bien pour le système d'exploitation serveur Microsoft® Windows Server® que pour les applications utilisant un annuaire. Pour le système d'exploitation serveur, AD DS stocke des informations critiques sur l'infrastructure du réseau, les utilisateurs et les groupes, les services réseau, etc. Dans ce rôle, les services de domaine Active Directory doivent adhérer à un schéma unique dans l'ensemble d'une forêt.

Par contre, le rôle de serveur AD LDS fournit des services d'annuaire spécifiquement pour les applications utilisant un annuaire. Les services AD LDS (Active Directory Lightweight Directory Services) ne nécessitent ni domaines ni forêts Active Directory. Cependant, dans les environnements où les services de domaine Active Directory existent, les services AD LDS (Active Directory Lightweight Directory Services) peuvent utiliser les services de domaine Active Directory pour l'authentification d'entités de sécurité Windows.

Fonctionnalités du rôle de serveur AD LDS

Vous pouvez utiliser le rôle de serveur AD LDS pour créer plusieurs instances AD LDS sur un même ordinateur. Chaque instance s'exécute en tant que service distinct dans son propre contexte d'exécution. Le rôle de serveur AD LDS offre les fonctionnalités suivantes pour faciliter la création, la configuration et la gestion des instances AD LDS :

- un Assistant qui vous guide tout au long du processus de création d'une instance AD LDS ;
- des outils en ligne de commande pour effectuer une installation ou une suppression sans assistance d'instances AD LDS ;
- des composants logiciels enfichables MMC (Microsoft Management Console) pour configurer et gérer les instances AD LDS, y compris le schéma de chaque instance ;
- des outils en ligne de commande spécifiques à AD LDS pour gérer, peupler et synchroniser les instances AD LDS.

Outre ces outils, vous pouvez également utiliser de nombreux outils Active Directory pour administrer les instances AD LDS.

Le ystème d'exploitation Windows Server® 2008 propose les fonctionnalités AD LDS supplémentaires répertoriées dans le tableau suivant.

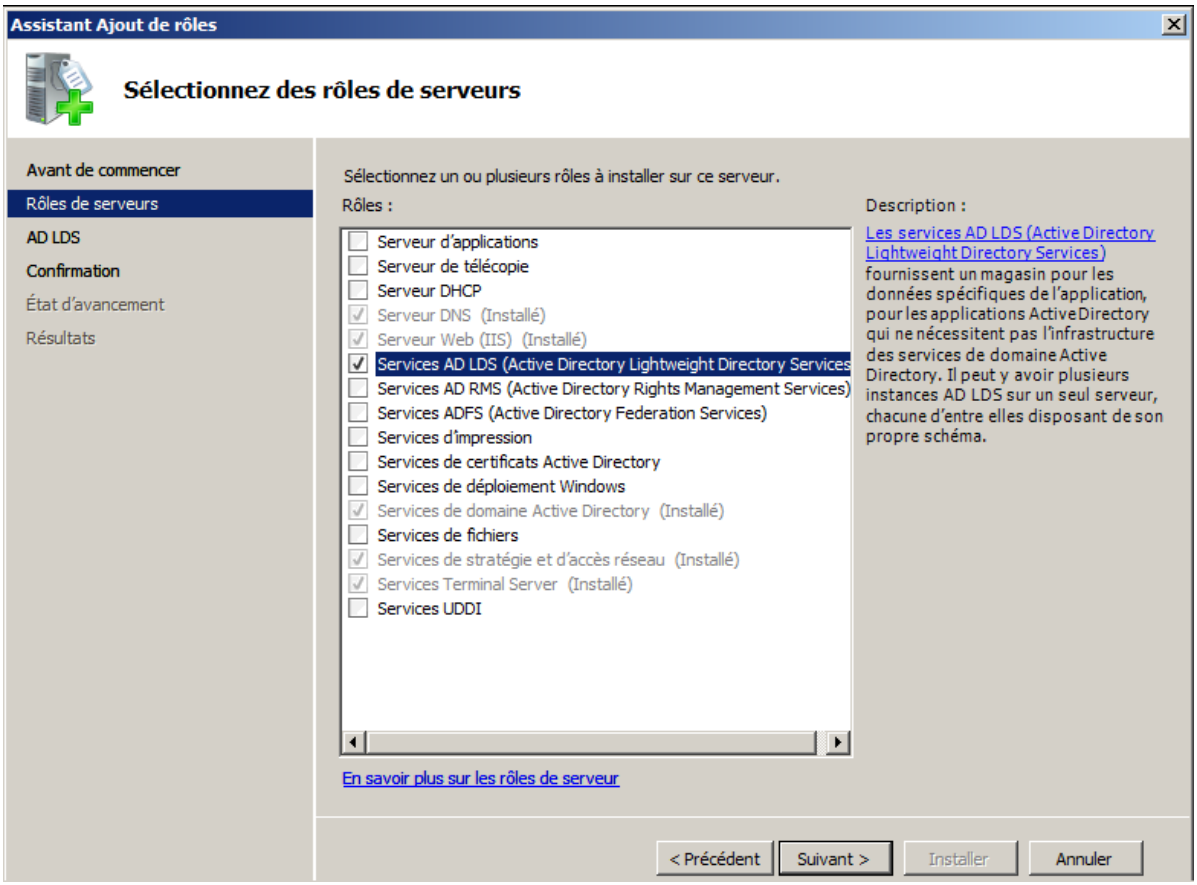
Fonctionnalité	Description
Génération d'Installation à partir du support	Avec cette fonctionnalité, vous pouvez utiliser un processus Ntdsutil.exe ou Dsdbutil.exe en une étape pour créer un support d'installation pour des installations AD LDS ultérieures.
Auditer les modifications des services AD LDS (Active Directory Lightweight Directory Services)	Avec cette fonctionnalité, vous pouvez configurer l'audit des services AD LDS avec une nouvelle sous-catégorie d'audit pour journaliser les anciennes et nouvelles valeurs lorsque des modifications sont apportées aux objets et à leurs attributs. **Remarques** • Cette fonctionnalité s'applique également aux services AD DS. Pour plus d'informations, voir la page concernant l'audit dans les services AD DS
Outil d'exploration de données	Avec cette fonctionnalité, vous pouvez afficher des données d'annuaire stockées en ligne dans des captures instantanées effectuées à différents points dans le temps, afin de prendre des décisions

	informées quant aux données à restaurer, sans avoir à redémarrer le serveur.
Prise en charge des sites et services Active Directory	Avec cette fonctionnalité, vous pouvez utiliser le composant logiciel enfichable Sites et services Active Directory pour gérer la réplication entre les instances AD LDS. Pour pouvoir utiliser cet outil, vous devez importer les classes dans MS-ADLDS-DisplaySpecifiers.LDF afin d'étendre le schéma d'un jeu de configuration que vous gérez. Pour vous connecter à une instance AD LDS qui héberge votre jeu de configuration, spécifiez le nom d'ordinateur et le numéro de port d'un serveur qui héberge cette instance AD LDS.
Liste dynamique de fichiers LDIF (LDAP Data Interchange Format) pendant l'installation d'une instance	Avec cette fonctionnalité, vous pouvez rendre des fichiers LDIF personnalisés disponibles pendant l'installation d'une instance AD LDS (en plus des fichiers LDIF par défaut fournis avec AD LDS) en ajoutant ces fichiers au répertoire %systemroot%\ADAM.
Requêtes récursives basées sur des attributs liés :	Avec cette fonctionnalité, vous pouvez créer une requête LDAP unique qui peut suivre des liens d'attributs imbriqués. Cela peut se révéler très utile pour déterminer l'appartenance aux groupes et l'ascendance. Pour plus d'informations, voir l'article 914825 de la Base de connaissances Microsoft

Considérations matérielles et logicielles

Utilisez des compteurs de performance, des tests en laboratoire, des données provenant du matériel existant dans un environnement de production et des déploiements pilotes pour déterminer la capacité requise pour votre serveur.

Installation des services AD LDS (Active Directory Lightweight Directory Services)



Une fois que vous avez fini d'installer le système d'exploitation, une liste de tâches de configuration initiales s'affiche. Pour installer les services AD LDS (Active Directory Lightweight Directory Services), dans la liste des tâches, cliquez sur Ajouter des rôles, puis sur Services AD LDS (Active Directory Lightweight Directory Services).

Après avoir ajouté le rôle de serveur AD LDS à votre serveur, vous pouvez créer une instance AD LDS. Pour créer une instance AD LDS, cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Assistant Installation des services AD LDS.

Gestion d'une instance AD LDS

Vous pouvez gérer les instances AD LDS à l'aide du composant logiciel enfichable MMC Éditeur ADSI. Pour gérer une instance AD LDS, cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Éditeur ADSI.

Services AD RMS (Active Directory Rights Management Services)

Active Directory Rights Management Services (AD RMS) et le client AD RMS permettent de renforcer la stratégie de sécurité d'une organisation en protégeant les informations en appliquant en permanence des stratégies d'utilisation aux informations, même si ces dernières sont déplacées. Vous pouvez utiliser AD RMS pour renforcer la protection des informations sensibles, telles que les rapports financiers, les spécifications de produits, les données des clients et les messages électroniques confidentiels, afin d'empêcher des personnes non autorisées d'avoir accès à ces informations accidentellement ou non.

Dans les sections suivantes, vous découvrirez AD RMS, les fonctionnalités requises et facultatives d'AD RMS ainsi que les logiciels et le matériel utilisés pour l'exécution d'AD RMS. À la fin de cette

rubrique, vous apprendrez à ouvrir la console d'AD RMS et découvrirez où trouver des informations supplémentaires sur AD RMS.

En quoi consistent les services AD RMS (Active Directory Rights Management Services) ?

Un système AD RMS se compose d'un serveur Windows Server® 2008 sur lequel est exécuté le rôle serveur Active Directory Rights Management Services (AD RMS) qui gère les certificats et les licences, d'un serveur de base de données et du client AD RMS. La version la plus récente du client AD RMS est intégrée au système d'exploitation Windows Vista®. Le déploiement d'un système AD RMS offre aux organisations les avantages suivants :

- Protection des informations sensibles. Les applications telles que les traitements de texte, les clients de messagerie électronique et les applications cœur de métier peuvent être activées pour AD RMS en vue de protéger les informations sensibles. Les utilisateurs peuvent choisir les personnes autorisées à ouvrir, modifier, imprimer ou transférer les informations, ou à entreprendre d'autres actions liées à ces informations. Les organisations peuvent créer des modèles personnalisés de stratégies d'utilisation, tels que « Confidentiel - Lecture seule », pouvant être appliqués directement aux informations.
- Protection permanente. AD RMS vient renforcer les solutions de sécurité existantes, telles que les pare-feu et les listes de contrôle d'accès, fonctionnant sur la base de périmètres de sécurité, afin de mieux protéger les informations en verrouillant les droits d'utilisation dans le document lui-même et en contrôlant la manière dont les informations sont utilisées, même après leur ouverture par un destinataire prévu.
- Technologie souple et personnalisable. Les éditeurs de logiciels indépendants et les développeurs peuvent activer n'importe quelle application pour AD RMS et permettre à d'autres serveurs, tels que les systèmes de gestion de contenu ou les serveurs de portail fonctionnant sous Windows ou sous d'autres systèmes d'exploitation, de fonctionner avec AD RMS et de contribuer ainsi à la protection des informations sensibles. Les éditeurs de logiciels indépendants peuvent intégrer des fonctions de protection des informations à leurs solutions serveur, qu'il s'agisse de solutions de gestion des documents et des enregistrements, de systèmes de passerelle de messagerie électronique et d'archivage, de solutions de workflows automatisés ou de systèmes d'inspection de contenu, par exemple.

AD RMS regroupe les fonctions des services RMS (Rights Management Services) de Windows Server 2003, des outils destinés aux développeurs, ainsi que des technologies de sécurité standard (chiffrement, certificats et authentification, entre autres), afin d'aider les organisations à créer des solutions fiables de protection des informations. Pour permettre le développement de solutions AD RMS personnalisées, un kit de développement logiciel (SDK) AD RMS est disponible.

Fonctions des services AD RMS

Vous pouvez configurer les composants suivants d'AD RMS à l'aide du Gestionnaire de serveur :

- Services AD RMS (Active Directory Rights Management Services). Le service de rôle Active Directory Rights Management Services (AD RMS) est un service de rôle obligatoire qui installe les composants AD RMS permettant de publier du contenu protégé par des droits et d'y accéder.
- Prise en charge de la fédération des identités. Le service de rôle de prise en charge de la fédération des identités est un service de rôle facultatif permettant aux identités fédérées d'accéder à du contenu protégé par des droits à l'aide des services de fédération Active Directory (ADFS, Active Directory Federation Services).

Considérations logicielles et matérielles

AD RMS fonctionne sur un ordinateur exécutant le système d'exploitation Windows Server 2008. Lorsque le rôle serveur AD RMS est installé, les services requis le sont aussi, y compris Internet Information Services (IIS). AD RMS nécessite également une base de données, telle que Microsoft SQL Server, qui peut être exécutée sur le même serveur qu'AD RMS ou sur un serveur distant, ainsi qu'une forêt des services de domaine Active Directory.

Le tableau suivant indique la configuration matérielle minimale requise et la configuration matérielle recommandée pour l'exécution de serveurs Windows Server 2008 avec le rôle serveur AD RMS.

Configuration requise	Configuration recommandée
Un processeur Pentium 4, 3 GHz ou supérieur	Deux processeurs Pentium 4, 3 GHz ou supérieur
512 Mo de RAM	1024 Mo de RAM
40 Go d'espace libre de disque dur	80 Go d'espace libre de disque dur

Pour faciliter le choix du matériel, effectuez des tests en laboratoire, utilisez des données provenant d'équipements existants issus d'un environnement de production et procédez à des déploiements pilotes afin de déterminer la capacité requise par votre serveur.

Le tableau suivant indique la configuration logicielle requise pour l'exécution de serveurs Windows Server 2008 avec le rôle serveur AD RMS. L'installation du rôle serveur AD RMS permet d'activer des fonctionnalités requises sur le système d'exploitation et de les configurer comme il convient si ce n'est pas déjà fait.

Logiciel	Configuration requise
Système d'exploitation	Windows Server 2008, sauf pour Windows® Web Server 2008
Système de fichiers	Le système de fichiers NTFS est recommandé
Messagerie	Message Queuing
Services Web	Internet Information Services (IIS). ASP.NET doit être activé.
Active Directory ou services de domaine Active Directory	AD RMS doit être installé dans un domaine Active Directory dans lequel les contrôleurs de domaine exécutent Windows Server 2000 avec Service Pack 3 (SP3), Windows Server 2003 ou Windows Server 2008. Tous les utilisateurs et groupes qui utilisent AD RMS pour acquérir des licences et publier des contenus doivent disposer d'une adresse de messagerie configurée dans Active Directory.
Serveur de base de données	AD RMS requiert un serveur de base de données, tel que Microsoft SQL Server 2005, ainsi que des procédures stockées pour effectuer certaines opérations.

Le client activé pour AD RMS doit disposer d'un navigateur ou d'une application activée pour AD RMS, telle que les versions de Microsoft Word, Outlook ou PowerPoint de Microsoft Office 2007. Pour créer du contenu protégé par des droits, Microsoft Office 2007 Entreprise, Professionnel Plus ou Intégrale est requis. Pour une sécurité renforcée, il est possible d'intégrer AD RMS à d'autres technologies telles que les cartes à puce.

Par défaut, Windows Vista intègre le client AD RMS. Le client RMS doit en revanche être installé sur les autres systèmes d'exploitations clients. Le client RMS avec Service Pack 2 (SP2) peut être téléchargé sur le Centre de téléchargement Microsoft. Il fonctionne sur les versions du système d'exploitation client antérieures à Windows Vista et Windows Server 2008.

Installation d'AD RMS

Une fois l'installation du système d'exploitation terminée, vous pouvez utiliser les Tâches de configuration initiales ou le Gestionnaire de serveur pour installer des rôles de serveur. Pour installer AD RMS, cliquez sur Ajouter des rôles dans la liste des tâches, puis activez la case à cocher Services AD RMS (Active Directory Rights Management Services).

Gestion d'AD RMS

Les rôles de serveur sont gérés à l'aide d'un composant logiciel enfichable MMC (Microsoft Management Console). Utilisez la console AD RMS (Active Directory Rights Management Services) pour gérer AD RMS. Pour ouvrir la console AD RMS (Active Directory Rights Management), cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Services AD RMS (Active Directory Rights Management Services.

VIRTUALISATION WINDOWS SERVER

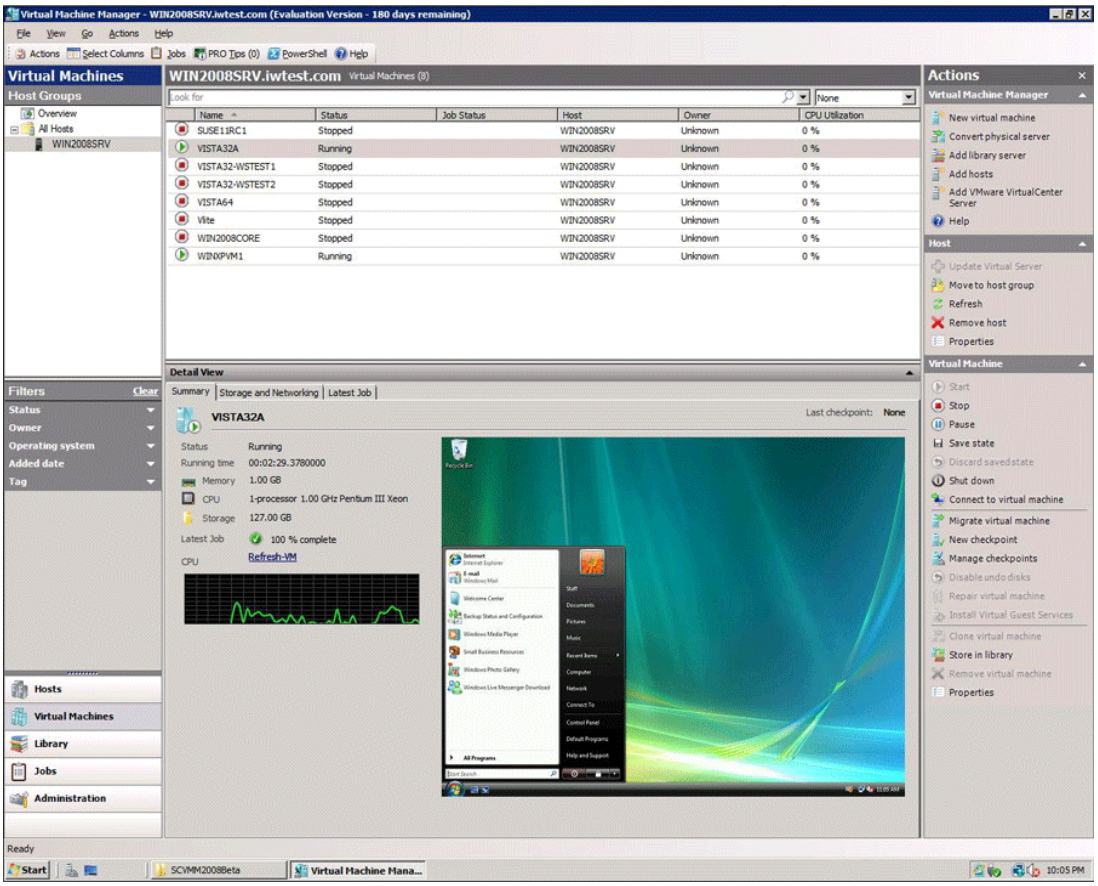
Présentation d'Hyper-V

Hyper-V™ vous permet de créer un environnement informatique de serveur virtualisé à l'aide d'une technologie faisant partie de Windows Server® 2008. Vous pouvez utiliser un environnement informatique virtualisé afin d'améliorer l'efficacité de vos ressources informatiques en utilisant une plus grande partie de vos ressources matérielles.

Quelle est la fonction d'Hyper-V ?

Hyper-V fournit une infrastructure logicielle et des outils de gestion de base dans Windows Server 2008 que vous pouvez utiliser pour créer et gérer un environnement informatique de serveur virtualisé. Cet environnement virtualisé peut être utilisé afin de réaliser différents objectifs professionnels liés à l'amélioration de l'efficacité et à la réduction des coûts. Un environnement de serveur virtualisé peut par exemple vous aider à :

- réduire les coûts liés à l'exploitation et à la maintenance de serveurs physiques en augmentant l'utilisation de votre matériel. Vous pouvez réduire la quantité de matériel nécessaire pour exécuter vos charges de travail de serveur ;
- augmenter l'efficacité du développement et des tests en réduisant la durée nécessaire à la configuration du matériel et des logiciels et à la reproduction des environnements de test ;
- améliorer la disponibilité des serveurs sans utiliser autant d'ordinateurs physiques que dans une configuration de basculement qui utilise uniquement des ordinateurs physiques ;
- augmenter ou réduire les ressources de serveur suite à une évolution de la demande.



Qui ce rôle peut-il intéresser ?

Hyper-V peut vous être utile si vous êtes l'une des personnes suivantes :

- un administrateur, un planificateur ou un concepteur informatique ;
- un architecte informatique responsable de la gestion informatique et de la sécurité de l'organisation ;
- un responsable des opérations informatiques qui recherche un moyen de réduire le coût total de propriété de son infrastructure de serveurs, à la fois en termes de coûts de puissance et de coûts de gestion ;
- un développeur ou testeur de logiciels qui recherche un moyen d'augmenter la productivité en réduisant la durée nécessaire à la création et la configuration d'un serveur destiné au développement ou à des tests.

Existe-t-il des considérations particulières ?

Hyper-V requiert du matériel spécifique. Vous devrez disposer des éléments suivants :

- Un processeur x64. Hyper-V sera disponible uniquement dans les versions à base de processeur x64 de Windows Server 2008 — plus particulièrement les versions à base de processeur x64 de Windows Server 2008, Standard Edition, Windows Server 2008, Édition Entreprise et Windows Server 2008, Datacenter Edition.
- Virtualisation d'assistance matérielle. Cette virtualisation est disponible avec les processeurs qui incluent une option de virtualisation ; plus spécifiquement, Intel VT ou AMD Virtualization (AMD-V, ancien nom de code « Pacifica »).

- La protection matérielle de l'exécution des données doit être disponible et activée. Plus spécifiquement, vous devez activer le bit Intel XD (bit de désactivation d'exécution) ou le bit AMD NX (bit de non-exécution).

Quelles sont les principales fonctionnalités d'Hyper-V ?

Les principales fonctionnalités de Hyper-V sont les suivantes :

- virtualisation hyperviseur native 64 bits ;
- capacité à exécuter simultanément des machines virtuelles 32 bits et 64 bits ;
- machines virtuelles monoprocesseurs et multiprocesseurs ;
- captures instantanées de machines virtuelles, qui capturent l'état d'une machine virtuelle en cours d'exécution. Les captures instantanées indiquent l'état du système, ce qui vous permet de restaurer la machine virtuelle à un état précédent ;
- prise en charge de grande mémoire de machine virtuelle ;
- prise en charge de réseau local virtuel ;
- outil de gestion Microsoft Management Console (MMC) 3.0 ;
- interfaces WMI (Windows Management Instrumentation) documentées pour l'écriture de scripts et la gestion.

ACCÈS CENTRALISÉ AUX APPLICATIONS

Services Terminal Server

Que sont les services Terminal Server ?

Le rôle de serveur Services Terminal Server dans Windows Server® 2008 fournit des technologies qui permettent aux utilisateurs d'accéder aux programmes Windows installés sur un serveur Terminal Server ou d'accéder au Bureau Windows. Grâce aux services Terminal Server, les utilisateurs peuvent accéder à un serveur Terminal Server à partir d'un réseau d'entreprise ou d'Internet.

Les services Terminal Server vous permettent de déployer et gérer efficacement des logiciels dans un environnement d'entreprise. Vous pouvez facilement déployer des programmes à partir d'un emplacement centralisé. Du fait qu'ils sont installés sur le serveur Terminal Server et non pas sur l'ordinateur client, les programmes sont plus faciles à mettre à niveau et à gérer.

Lorsqu'un utilisateur accède à un programme sur un serveur Terminal Server, l'exécution de ce programme s'effectue sur le serveur. Seules les informations du clavier, de la souris et de l'affichage sont transmises sur le réseau. Chaque utilisateur ne voit que sa propre session. La session est gérée de manière transparente par le système d'exploitation du serveur, indépendamment des sessions des autres clients.

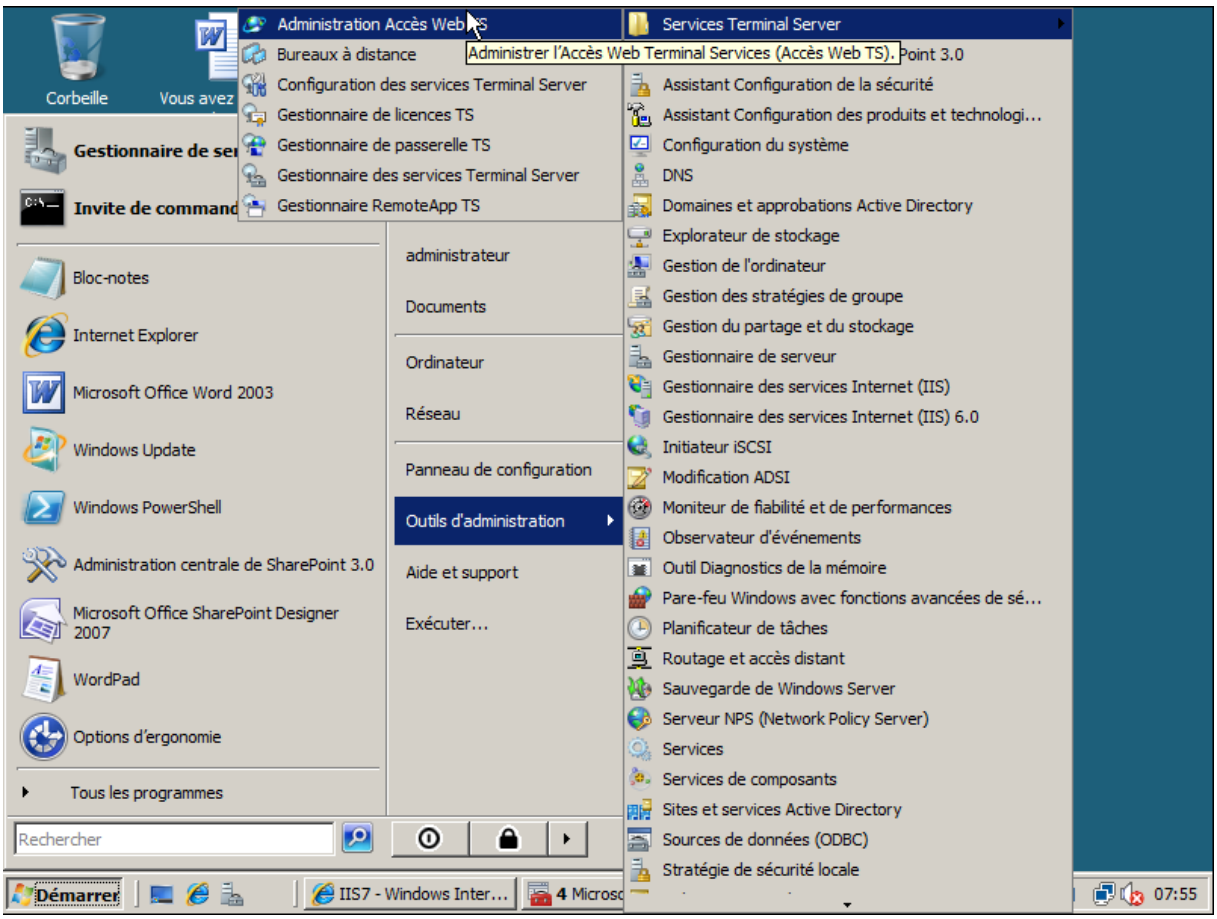
Pourquoi utiliser des services Terminal Server ?

Le fait de déployer un programme sur un serveur Terminal Server au lieu de le déployer sur chaque périphérique offre de nombreux avantages, notamment :

- Vous pouvez déployer rapidement des programmes Windows sur les périphériques informatiques d'une entreprise. Les services Terminal Server sont très utiles lorsque des programmes sont mis à jour régulièrement, peu utilisés ou difficiles à gérer.
- Ils peuvent considérablement réduire la quantité de bande passante réseau requise pour accéder à des applications distantes.

- Les services Terminal Server contribuent à améliorer la productivité des utilisateurs. Les utilisateurs peuvent accéder à des programmes exécutés sur un serveur Terminal Server à partir de périphériques, tels que des ordinateurs personnels, des bornes, du matériel de faible puissance et des systèmes d'exploitation autres que Windows.
- Les services Terminal Server améliorent les performances des programmes pour les employés de succursales qui ont besoin d'accéder à des magasins de données centralisés. Les programmes utilisant énormément de données n'ont parfois pas de protocoles client-serveur optimisés pour les connexions à basse vitesse. Les programmes de ce type fonctionnent généralement mieux sur une connexion des services Terminal Server que sur un réseau étendu (WAN) classique.

Services de rôle des services Terminal Server



Services Terminal Server est un rôle de serveur qui comprend plusieurs sous-composants, appelés « services de rôle ». Dans Windows Server 2008, les services Terminal Server intègrent les services de rôle suivants :

- Terminal Server : Le service de rôle Terminal Server permet à un serveur d'héberger des programmes Windows ou le Bureau Windows. Les utilisateurs peuvent se connecter à un serveur Terminal Server pour exécuter des programmes, enregistrer des fichiers et utiliser des ressources réseau sur ce serveur.
- TS Web Access : L'Accès au Web pour les services Terminal Server permet aux utilisateurs d'accéder à des programmes de l'Application distante™ et à une connexion Bureau à distance vers le serveur Terminal Server via un site Web.
- Gestionnaire de licences des services Terminal Server : Le Gestionnaire de licences des services Terminal Server gère les licences d'accès client des services Terminal Server nécessaires à chaque périphérique ou utilisateur pour se connecter à un serveur Terminal

Server. La Gestion de licences Terminal Server permet d'installer et d'octroyer des licences d'accès client TS et de surveiller leur disponibilité sur un serveur de licences des services Terminal Server.

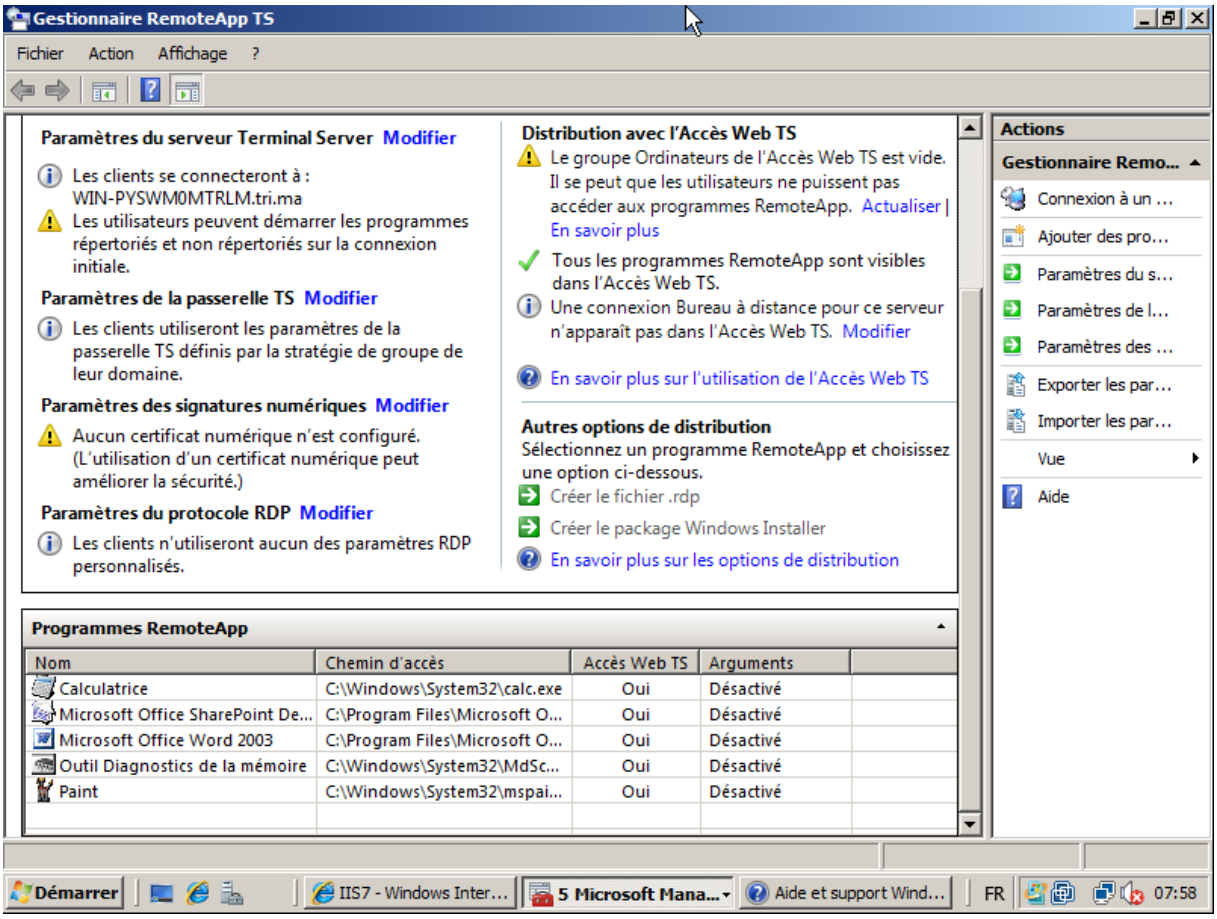
- Passerelle des services Terminal Server : La Passerelle des services Terminal Server permet aux utilisateurs distants autorisés de se connecter à des ressources sur un réseau d'entreprise interne, à partir de tout périphérique relié à Internet.
- Session Broker TS : Terminal Services Session Broker (TS Session Broker) prend en charge l'équilibrage de la charge des sessions entre les serveurs Terminal Server d'une batterie, et les reconnexions à une session existante dans une batterie de serveurs Terminal Server à charge équilibrée.

Qu'est-ce qu'un serveur Terminal Server ?

Un serveur Terminal Server est le serveur qui héberge les programmes Windows ou le Bureau Windows pour les clients des services Terminal Server. Les utilisateurs peuvent se connecter à un serveur Terminal Server pour exécuter des programmes, enregistrer des fichiers et utiliser des ressources réseau sur ce serveur. Ils peuvent accéder à un serveur Terminal Server par le biais d'une connexion Bureau à distance ou à l'aide des programmes de l'Application distante.

RemoteApp des services Terminal Server (TS RemoteApp)

Les programmes de l'Application distante sont des programmes accessibles à distance par le biais des services Terminal Server et qui se comportent comme s'ils étaient exécutés sur l'ordinateur local de l'utilisateur final. Les utilisateurs peuvent exécuter côte à côte des programmes de l'Application distante et leurs programmes locaux. Si un utilisateur exécute plusieurs programmes de l'Application distante à partir du même serveur Terminal Server, ces programmes partagent la même session des services Terminal Server. Cette fonctionnalité conserve les sessions utilisateur et permet d'établir une connexion plus rapide vers chaque programme supplémentaire de l'Application distante situé sur le même serveur.



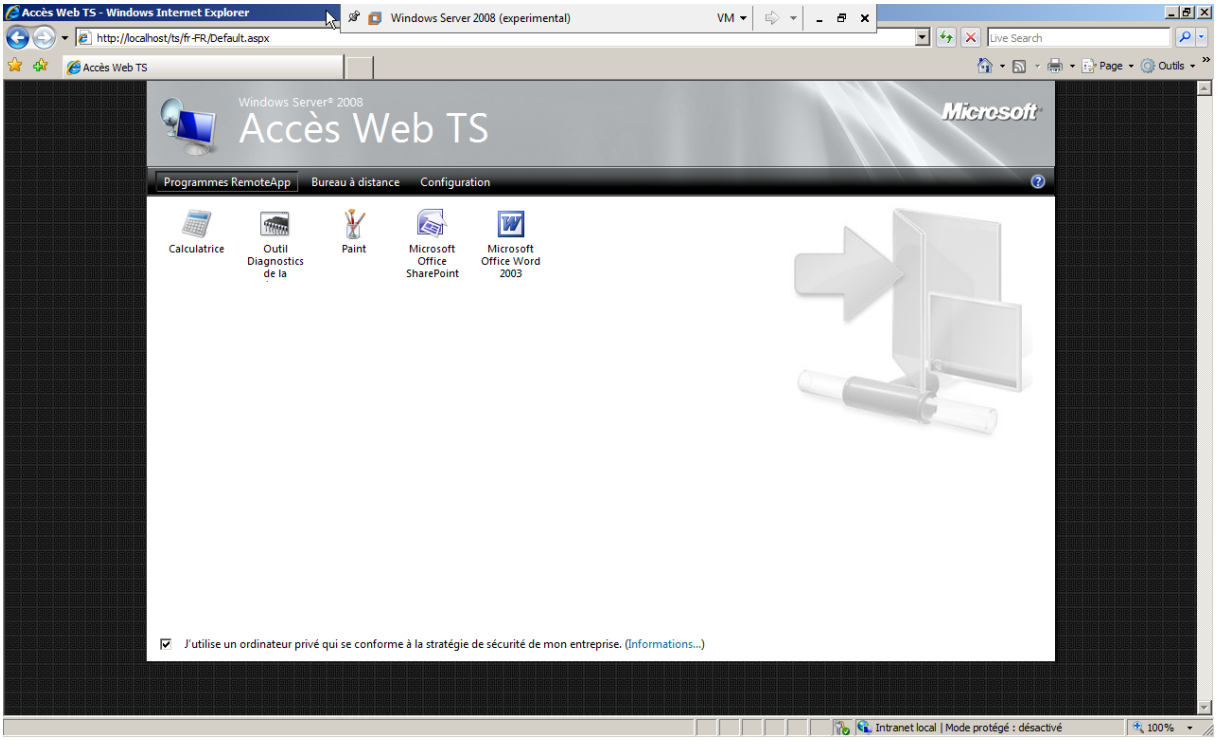
Le Gestionnaire d'application distante TS vous permet de créer des packages Windows Installer (packages .msi) ou des fichiers .rdp, puis de distribuer ces packages dans votre organisation. Ou, si vous souhaitez que les utilisateurs accèdent à des programmes de l'Application distante sur le Web, vous pouvez les déployer sur un site Web à l'aide de TS Web Access.

Pourquoi utiliser l'Application distante des services TS ?

L'Application distante des services TS peut réduire la complexité des procédures et limiter la charge administrative dans un grand nombre de situations, notamment :

- lorsque des succursales sont limitées au niveau du support informatique local et de la bande passante réseau ;
- lorsque des utilisateurs ont besoin d'accéder à des applications à distance ;
- lors du déploiement d'applications métier, en particulier les applications métier personnalisées ;
- dans certains environnements, tels que les espaces de travail de type bureaux partagés ou bureaux à la carte ;
- lors du déploiement de plusieurs versions d'une application, notamment si l'installation de plusieurs versions localement est susceptible de provoquer des conflits.

Qu’est-ce que TS Web Access ?



TS Web Access vous permet de rendre disponibles des programmes de l’Application distante et une connexion Bureau à distance vers le serveur Terminal Server aux utilisateurs à partir d’un navigateur Web. À l’aide de TS Web Access, les utilisateurs peuvent visiter un site Web (sur Internet ou un intranet) pour accéder à une liste des programmes de l’Application distante disponibles. Lorsque vous démarrez un programme de l’Application distante, une session des services Terminal Server démarre sur le serveur Terminal Server qui héberge le programme de l’Application distante.

Lorsque vous déployez TS Web Access, vous pouvez spécifier le serveur Terminal Server à utiliser en tant que source de données pour renseigner la liste des programmes de l’Application distante qui s’affiche dans la page Web.

Qu’est-ce que la Gestion de licences Terminal Server ?

La Gestion de licences Terminal Server gère les licences d’accès client des services Terminal Server nécessaires à chaque périphérique ou utilisateur pour se connecter à un serveur Terminal Server. La Gestion de licences Terminal Server permet d’installer et d’octroyer des licences d’accès client TS et de surveiller leur disponibilité sur un serveur de licences des services Terminal Server.

Pour utiliser les services Terminal Server, vous devez disposer d’au moins un serveur de licences. Pour les déploiements de petite taille, vous pouvez installer le service de rôle Terminal Server et le service de rôle Gestion de licences Terminal Server sur le même ordinateur. Pour les déploiements plus importants, il est recommandé d’installer le service de rôle Gestion de licences Terminal Server sur un ordinateur différent de celui hébergeant le service de rôle Terminal Server.

Vous devez correctement configurer la Gestion de licences Terminal Server pour que votre serveur Terminal Server continue d’accepter les connexions des clients.

Qu'est-ce que la Passerelle des services Terminal Server ?

La Passerelle des services Terminal Server permet aux utilisateurs distants autorisés de se connecter à des ressources sur un réseau d'entreprise interne, à partir de tout périphérique relié à Internet. Ces ressources réseau peuvent être des serveurs Terminal Server exécutant des applications distantes [hébergeant des programmes métier] ou des ordinateurs avec le Bureau à distance activé. La Passerelle des services Terminal Server encapsule le protocole RDP via HTTPS pour établir une connexion sécurisée et chiffrée entre les utilisateurs sur Internet et les ressources réseau internes sur lesquelles s'exécutent leurs applications de productivité.

Pourquoi utiliser la Passerelle des services Terminal Server ?

La Passerelle des services Terminal Server présente les avantages suivants :

- La Passerelle des services Terminal Server permet à des utilisateurs distants de se connecter à des ressources réseau internes sur Internet à l'aide d'une connexion chiffrée, sans avoir besoin de configurer de connexion de réseau privé virtuel (VPN, Virtual Private Network).
- La Passerelle des services Terminal Server fournit un modèle complet de configuration de la sécurité qui vous permet de contrôler l'accès à des ressources réseau internes spécifiques. La Passerelle des services Terminal Server fournit une connexion RDP point-à-point, au lieu d'autoriser des utilisateurs distants à accéder à l'ensemble des ressources réseau internes.
- La Passerelle des services Terminal Server permet à des utilisateurs distants de se connecter à des ressources réseau internes hébergées derrière des pare-feu sur des réseaux privés et des traducteurs d'adresses réseau (NAT, Network Address Translator). Grâce à la Passerelle des services Terminal Server, vous n'avez pas besoin, dans ce cas, d'effectuer des procédures de configuration supplémentaires pour le serveur ou les clients de la passerelle.

  Avant la parution de cette version de Windows Server, des mesures de sécurité empêchaient les utilisateurs distants de se connecter à des ressources réseau internes via des pare-feu et des traducteurs NAT. Cela est dû au fait que le port 3389, utilisé pour les connexions RDP, est généralement bloqué à des fins de sécurisation du réseau. La Passerelle des services Terminal Server transmet quant à elle le trafic RDP vers le port 443, en utilisant un tunnel HTTP TLS/SSL (Transport Layer Security/Secure Sockets Layer). Comme la plupart des entreprises ouvrent le port 443 pour activer la connectivité Internet, la Passerelle des services Terminal Server tire avantage de cette conception de réseau pour fournir des connexions d'accès distant à travers plusieurs pare-feu.

- Le Gestionnaire des passerelles TS vous permet de configurer des stratégies d'autorisation pour définir les conditions que les utilisateurs doivent remplir pour se connecter à des ressources réseau internes. Par exemple, vous pouvez spécifier les éléments suivants :
  - Les personnes autorisées à se connecter à des ressources internes (autrement dit, les groupes d'utilisateurs autorisés à se connecter).
  - Les ressources réseau internes (groupe d'ordinateurs) auxquelles les utilisateurs peuvent se connecter.
  - L'obligation ou non pour les ordinateurs clients d'appartenir à des groupes de sécurité Active Directory spécifiques.
  - Le choix d'autoriser ou non la redirection de périphérique et de disque.
  - L'obligation pour les clients d'utiliser exclusivement l'authentification par carte à puce ou l'authentification par mot de passe, ou l'une des deux méthodes indifféremment.
- Vous pouvez configurer des serveurs de Passerelle des services Terminal Server et des clients des services Terminal Server pour qu'ils utilisent la protection d'accès réseau (NAP, Network Access Protection) pour optimiser la sécurité. La protection NAP est une technologie de création de stratégie d'intégrité, d'application de l'intégrité et de rétablissement de l'intégrité

fournie dans Windows XP Service Pack 2, Windows Vista™ et Windows Server 2008. La protection NAP permet aux administrateurs système d'imposer des spécificités d'intégrité, qui peuvent inclure des impératifs logiciels, des impératifs de mise à jour de sécurité, des configurations d'ordinateur requises et d'autres paramètres.

Pour plus d'informations sur la façon de configurer la Passerelle des services Terminal Server pour qu'elle utilise la protection NAP à des fins d'application de stratégies d'intégrité pour des clients des services Terminal Server qui se connectent à des serveurs de la Passerelle des services Terminal Server.

- Vous pouvez utiliser un serveur de la Passerelle des services Terminal Server avec Microsoft ISA (Internet Security and Acceleration) Server pour améliorer la sécurité. Dans ce cas, vous pouvez héberger des serveurs de la Passerelle des services Terminal Server sur un réseau privé plutôt que sur un réseau de périmètre (également appelé zone démilitarisée et sous-réseau filtré), ainsi qu'ISA Server sur le réseau de périmètre. La connexion SSL (Secure Sockets Layer) entre le client des services Terminal Server et ISA Server peut être interrompue au niveau d'ISA Server, connecté à Internet.

  Pour plus d'informations sur la façon de configurer ISA Server en tant que périphérique d'interruption de connexion SSL dans le cas de serveurs de Passerelle des services Terminal Server,

  Le Gestionnaire des passerelles TS fournit des outils pour vous aider à surveiller l'état de connexion, l'intégrité et les événements de la Passerelle des services Terminal Server. Le Gestionnaire des passerelles TS vous permet de spécifier des événements (par exemple, les échecs de connexion au serveur de Passerelle des services Terminal Server) que vous souhaitez surveiller à des fins d'audit.

Qu'est-ce que Session Broker TS ?

TS Session Broker effectue le suivi des sessions utilisateur dans une batterie de serveurs Terminal Server à charge équilibrée. La base de données TS Session Broker stocke des informations d'état qui incluent les ID de session, les noms d'utilisateur associés et le nom du serveur hébergeant chaque session. Lorsqu'un utilisateur avec une session existante se connecte à un serveur Terminal Server dans la batterie à charge équilibrée, TS Session Broker le redirige vers le serveur Terminal Server hébergeant sa session. Cela évite à l'utilisateur d'être connecté à un autre serveur de la batterie et de démarrer une nouvelle session.

Si la fonctionnalité d'équilibrage de charge de TS Session Broker est activée, TS Session Broker suit également le nombre de sessions utilisateur sur chaque serveur Terminal Server dans la batterie, et redirige les utilisateurs qui n'ont pas de session existante vers le serveur hébergeant le plus petit nombre de sessions. Cette fonctionnalité vous permet de répartir équitablement la charge des sessions entre les serveurs d'une batterie de serveurs Terminal Server à charge équilibrée.

APPLICATION DE LA STRATÉGIE ET DE LA SÉCURITÉ

La sécurité

Les fonctionnalités de sécurité disponibles dans Windows Server® 2008 permettent d'implémenter et de gérer des éléments de sécurité essentiels dans votre infrastructure informatique.

Consultez les sections suivantes pour en savoir plus sur les fonctionnalités de sécurité mises à votre disposition, sur le mode d'accès à ces dernières et leur utilisation pour gérer des aspects spécifiques liés à la sécurité globale.

Cette rubrique contient les sections suivantes :

Chaque rôle serveur nécessite des configurations de sécurité spécifiques, en fonction de votre scénario de déploiement et des exigences en matière d'infrastructure. La documentation de prise en charge de chacun des rôles serveur contient des informations sur la configuration de la sécurité et d'autres considérations relatives à la sécurité. Vous pouvez afficher la liste complète des rôles serveur disponibles dans le Gestionnaire de serveur. Pour ouvrir le Gestionnaire de serveur, cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Gestionnaire de serveur.

Technologies de réduction des menaces et des vulnérabilités

Ces technologies fournissent des défenses en couche contre les menaces des logiciels malveillants et les intrusions par le biais d'une stratégie de prévention, d'isolation et de récupération. Cet ensemble de technologies propose de la documentation et des ressources pour les produits et les technologies qui aident à protéger les clients, les serveurs d'applications et le périmètre du réseau contre les programmes malveillants, tels que les logiciels espions, les rootkits et les virus.

Technologies d'évaluation et de gestion d'une configuration sécurisée

Ces technologies sont disponibles pour Windows Server 2008 et permettent d'administrer la sécurité sur le système local ou dans le cadre d'une défense en couche et de gérer les menaces en cours. Pour plus d'informations sur l'évaluation des risques, l'analyse de la configuration de la sécurité et d'autres technologies d'évaluation et de gestion d'une configuration sécurisée

Gestionnaire d'autorisations

Le Gestionnaire d'autorisations est un outil de gestion basé sur les rôles qui permet de contrôler l'accès aux ressources en attribuant des rôles aux utilisateurs. Il fournit un emplacement central pour gérer et assurer le suivi des autorisations qui ont été octroyées à chacun des rôles, et par conséquent pour gérer et assurer le suivi de chacun des utilisateurs inclus dans ce rôle.

Le tableau suivant contient des informations supplémentaires sur le Gestionnaire d'autorisations.

Rubriques	Descriptions
Considérations matérielles et logicielles pour le Gestionnaire d'autorisations	Aucune
Installation du Gestionnaire d'autorisations	Le Gestionnaire d'autorisations est installé par défaut sur Windows Server 2008.
Gestion de la sécurité avec le Gestionnaire d'autorisations	Ajoutez le composant logiciel enfichable Gestionnaire d'autorisations à la console MMC.

Audit de sécurité

L'audit de sécurité permet d'assurer le suivi des événements de sécurité sur un ordinateur ou système informatique en consignant des événements spécifiques. L'audit de sécurité dans Windows Server 2008 permet de suivre la création ou la modification d'objets, vous donne le moyen de dépister des problèmes potentiels de sécurité, vous aide à gérer les comptes des utilisateurs et apporte des preuves en cas de violation de la sécurité.

Le tableau suivant contient des informations supplémentaires sur l'audit de sécurité.

Rubriques	Descriptions
Considérations matérielles et logicielles pour l'audit de sécurité	La prise en charge de l'audit est disponible sur les ordinateurs fonctionnant sous Windows Server 2008, Windows Server 2003, Windows 2000 Server, Windows Vista, Windows XP Professionnel et Windows 2000 Professionnel. Vous avez la possibilité de spécifier des stratégies d'audit détaillées uniquement sur les ordinateurs fonctionnant sous Windows Server 2008 et Windows Vista.
Installation de l'audit de sécurité	L'audit de sécurité est une fonctionnalité intégrée de Windows Server 2008, mais vous devez la configurer.
Gestion de l'audit des événements de sécurité	Dans un environnement composé de plusieurs systèmes d'exploitation Windows, les stratégies d'audit détaillées sont gérées à l'aide de différents outils, notamment Auditpol.exe, des scripts, les services de domaine Active Directory (AD DS) et la Stratégie de groupe. Pour plus d'informations sur l'audit de sécurité et les stratégies d'audit détaillées, Vous pouvez gérer les tâches suivantes à l'aide de l'éditeur de contrôle d'accès : • Définir ou modifier les paramètres de la stratégie d'audit pour une catégorie d'événement • Appliquer ou modifier les paramètres de la stratégie d'audit pour un fichier ou un dossier local Pour définir des stratégies d'audit sur un ordinateur local et du domaine, cliquez avec le bouton droit sur l'objet, cliquez sur Propriétés, cliquez sur l'onglet Sécurité, puis cliquez sur l'onglet Audit.

Assistant Configuration de la sécurité

L'Assistant Configuration de la sécurité détermine les fonctionnalités minimales nécessaires pour un ou plusieurs rôles serveur et désactive celles qui ne sont pas utiles.

Vous pouvez exécuter l'Assistant Configuration de sécurité indépendamment ou à partir de Gestionnaire de serveur. Cet Assistant vous guide à travers les différentes étapes de création, de modification, d'application ou d'annulation d'une stratégie de sécurité basée sur les rôles sélectionnés du serveur. Les stratégies de sécurité créées avec l'Assistant Configuration de sécurité sont des fichiers .xml qui, lorsqu'ils sont appliqués, configurent les services, la sécurité du réseau, des valeurs de Registre spécifiques et la stratégie d'audit.

Le tableau suivant contient des informations supplémentaires sur l'Assistant Configuration de sécurité.

Rubriques	Descriptions
Considérations matérielles et logicielles pour l'Assistant Configuration de sécurité	Cet Assistant permet de configurer la sécurité du serveur. Toutes les applications qui utilisent le protocole et des ports IP doivent être en cours d'exécution sur le serveur sur lequel vous exécutez l'Assistant Configuration de sécurité. Cet Assistant désactive les services inutiles et fournit le Pare-feu

	Windows avec fonctions avancées de sécurité. Cet Assistant n'installe pas (ou ne désinstalle pas) les composants nécessaires au serveur pour jouer un rôle. Le Gestionnaire de serveur permet d'installer des composants spécifiques à un rôle. Pour ouvrir le Gestionnaire de serveur, cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Gestionnaire de serveur.
Installation de l'Assistant Configuration de sécurité	L'Assistant Configuration de sécurité est une fonctionnalité intégrée de Windows Server 2008.
Gestion de l'Assistant Configuration de sécurité	Pour exécuter l'Assistant Configuration de sécurité, cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Assistant Configuration de sécurité. En outre, vous pouvez utiliser l'outil de ligne de commande Scwcmd.
Références supplémentaires pour l'Assistant Configuration de sécurité	• Pour accéder à l'Aide (scwhelp.chm) lorsque vous exécutez l'Assistant Configuration de sécurité, appuyez sur F1. • L'Aide sur la ligne de commande (/?) est disponible pour l'outil Scwcmd.

Stratégies de restriction logicielle

Les stratégies de restriction logicielle permettent d'identifier les logiciels et de contrôler leur capacité à s'exécuter sur l'ordinateur local, l'unité d'organisation, le domaine ou le site.

Le tableau suivant contient des informations supplémentaires sur les stratégies de restriction logicielle.

Rubriques	Descriptions
Considérations matérielles et logicielles lors de l'utilisation de stratégies de restriction logicielle	Aucune
Installation de stratégies de restriction logicielle	Vous pouvez créer et gérer des stratégies de restriction logicielle par défaut dans Windows Server 2008. Cependant, pour administrer un domaine, un site ou une unité d'organisation, vous devez installer la Console de gestion des stratégies de groupe.
Gestion des stratégies de restriction logicielle	Sur l'ordinateur local, cliquez sur Démarrer, pointez sur Outils d'administration et cliquez sur Stratégie de sécurité locale. Dans l'arborescence de la console, cliquez sur Stratégies de restriction logicielle. Pour un domaine, un site ou une unité d'organisation, lorsque vous êtes sur un serveur membre ou une station de travail jointe à un domaine, cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Gestion des stratégies de groupe. Sélectionnez un objet de stratégie de groupe dans le domaine, le site ou l'unité d'organisation correspondant. Dans l'arborescence de la console, cliquez sur Stratégies de restriction logicielle.

Configuration et analyse de la sécurité

Le composant logiciel enfichable Configuration et analyse de la sécurité permet d'analyser et de configurer la sécurité de l'ordinateur local. Il affiche des recommandations ainsi que les paramètres actuels du système et utilise des indicateurs visuels ou des remarques pour indiquer les zones dans lesquelles les paramètres actuels ne correspondent pas au niveau de sécurité proposé. Il permet de résoudre les incohérences révélées par une analyse et de configurer directement la sécurité du système local en important des modèles de sécurité.

Le tableau suivant contient des informations supplémentaires sur le composant logiciel enfichable Configuration et analyse de la sécurité.

Rubriques	Descriptions
Considérations matérielles et logicielles pour le composant logiciel enfichable Configuration et analyse de la sécurité	Ce composant logiciel enfichable utilise le modèle de sécurité actuel comme base de l'analyse. Par conséquent, vous devez installer le modèle de sécurité approprié.
Installation du composant logiciel enfichable Configuration et analyse de la sécurité	Ce composant logiciel enfichable est installé par défaut sur Windows Server 2008.
Gestion de la sécurité locale avec le composant logiciel enfichable Configuration et analyse de la sécurité	Ajoutez le composant logiciel enfichable Configuration et analyse de la sécurité à la console MMC. Vous pouvez aussi utiliser l'outil de ligne de commande Secedit pour effectuer certaines tâches de gestion.

Technologies de contrôle d'identité et d'accès

Ces technologies fournissent une méthode centrale de gestion des informations d'identification visant à autoriser uniquement les utilisateurs légitimes à accéder aux périphériques, aux applications et aux données.

Pour obtenir des informations sur la configuration des protocoles d'authentification (Negotiate, Kerberos, NTLM, Digest, TLS et SSL), l'ouverture de session Windows, les scripts d'ouverture de session et les fournisseurs d'informations d'identification,

Cartes à puce

Les cartes à puce représentent un moyen résistant aux falsifications et portable permettant d'offrir des solutions de sécurité pour des tâches telles que l'authentification des clients, la connexion aux domaines, la signature du code et la sécurisation des messages électroniques.

Le tableau suivant contient des informations supplémentaires sur les cartes à puce.

Rubriques	Descriptions
Considérations matérielles et logicielles pour les cartes à puce	Les cartes à puce et les lecteurs de carte à puce nécessitent des achats, une installation et une administration supplémentaires.
Installation de la technologie des cartes à puce sur Windows	La possibilité de configurer Windows Server 2008 en utilisant une carte à puce est intégrée par le fournisseur d'informations d'identification. L'installation du lecteur de carte à puce doit être effectuée conformément aux instructions du fabricant. L'émission d'un certificat est nécessaire.
Gestion des cartes à	La gestion s'effectue via l'inscription des certificats, la stratégie de groupe

puce	et les outils de gestion fournis par le fabricant du matériel.

Autorisations et contrôle d'accès

Le contrôle d'accès est le processus autorisant des utilisateurs, des groupes et des ordinateurs à accéder à des objets pour lesquels vous pouvez définir des autorisations sur l'ordinateur ou sur le réseau.

Le tableau suivant contient des informations supplémentaires sur les autorisations et le contrôle d'accès.

Rubriques	Descriptions
Considérations matérielles et logicielles pour l'utilisation du contrôle d'accès	Pour administrer les autorisations et le contrôle d'accès dans le domaine, vous devez être un administrateur de domaine. Pour administrer le contrôle d'accès sur l'ordinateur local, vous devez être un administrateur sur cet ordinateur ou disposer des droits appropriés sur l'objet.
Installation du contrôle d'accès	Autorisations et contrôle d'accès sont des composants intégrés à Windows Server 2008 ; cependant, pour les gérer dans le domaine, vous devez installer et configurer le rôle serveur AD DS et la Console de gestion des stratégies de groupe.
Gestion du contrôle d'accès	Pour gérer les autorisations et le contrôle d'accès dans un domaine, vous pouvez utiliser les outils d'Active Directory et la stratégie de groupe. Pour gérer les autorisations et le contrôle d'accès sur l'ordinateur local, vous pouvez utiliser Utilisateurs et groupes locaux et l'Éditeur de stratégie de groupes local.

Chiffrement des lecteurs BitLocker

Le chiffrement des lecteurs BitLocker Windows est une fonctionnalité de protection des données disponible dans Windows Vista Entreprise et Windows Vista Édition Intégrale pour les ordinateurs clients et dans Windows Server 2008. BitLocker améliore la protection des données en associant le chiffrement intégral des lecteurs au contrôle d'intégrité des composants de démarrage.

Le tableau suivant contient des informations supplémentaires sur BitLocker.

Rubriques	Descriptions
Considérations matérielles et logicielles pour BitLocker	Configuration requise pour BitLocker : • Un ordinateur fonctionnant sous Windows Vista Entreprise, Windows Vista Édition Intégrale ou Windows Server 2008 • Un microprocesseur de module de plateforme sécurisée (TPM), version 2.2 ou un périphérique USB amovible et sécurisé • Un BIOS TCG (Trusted Computing Group) • Deux partitions de lecteur NTFS, une pour le volume du système et une pour le volume hébergeant le système d'exploitation • Un paramètre de BIOS qui démarre tout d'abord l'ordinateur à partir du lecteur de disque dur et non pas des lecteurs USB ou de CD
Installation de BitLocker	Pour installer BitLocker, exécutez l'Assistant Ajout de composant dans le Gestionnaire de serveur. Pour ouvrir le Gestionnaire de serveur, cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Gestionnaire

	de serveur. Un redémarrage est nécessaire pour terminer l'installation.
Gestion de BitLocker	Avec le module de plateforme sécurisée, ajoutez le composant logiciel enfichable Gestion du module de plateforme sécurisée à la console MMC. Sans le module de plateforme sécurisée, une clé de démarrage USB amovible est nécessaire.

Gestion du module de plateforme sécurisée

Les services de module de plateforme sécurisée constituent un nouvel ensemble de fonctionnalités dans Windows Vista et Windows Server 2008, utilisé pour administrer les composants matériels dédiés à la sécurité du module de plateforme sécurisée de votre ordinateur. L'architecture des services de module de plateforme sécurisée fournit l'infrastructure pour la sécurité matérielle, en permettant l'accès au module de plateforme sécurisée ainsi que le partage au niveau applicatif. La console Gestion du module de plateforme sécurisée est un composant logiciel enfichable MMC (Microsoft Management Console) qui permet aux administrateurs d'interagir avec les services du module de plateforme sécurisée.

Le tableau suivant contient des informations supplémentaires sur la gestion du module de plateforme sécurisée.

Rubriques	Descriptions
Considérations matérielles et logicielles pour le module de plateforme sécurisée	Configuration requise pour le module de plateforme sécurisée : • Un microprocesseur de module de plateforme sécurisée fonctionnel, version 1.2 • Un BIOS TCG (Trusted Computing Group) fonctionnel
Installation du composant logiciel enfichable Gestion du module de plateforme sécurisée	Si votre ordinateur est doté d'un microprocesseur de module de plateforme sécurisée, aucune installation supplémentaire n'est nécessaire.
Gestion du module de plateforme sécurisée	Ajoutez le composant logiciel enfichable Gestion du module de plateforme sécurisée à la console MMC.

Système de fichiers EFS

Le système de fichiers EFS est une technologie de chiffrement de fichier importante utilisée pour stocker des fichiers chiffrés sur des volumes du système de fichiers NTFS. Intégré au système de fichiers, il est simple à gérer, difficile à attaquer et transparent pour l'utilisateur. Il est particulièrement utile pour protéger les données sur des ordinateurs qui peuvent être vulnérables à l'accès par d'autres utilisateurs. Une fois qu'un fichier ou dossier est chiffré, vous l'utilisez de la même façon que les autres fichiers et dossiers.

Le tableau suivant contient des informations supplémentaires sur le système de fichiers EFS.

Rubriques	Descriptions
Considérations matérielles et logicielles pour l'utilisation du système de fichiers EFS	Vous pouvez uniquement chiffrer des fichiers et des dossiers sur les volumes du système de fichiers EFS. Des fichiers ou des dossiers compressés ne peuvent pas non plus être chiffrés. Si vous chiffrez un fichier ou un dossier compressé, celui-ci sera

	décompressé. Il n'est pas possible de chiffrer des fichiers portant l'attribut Système ou des fichiers placés dans le dossier systemroot. Vous pouvez utiliser des cartes à puce pour conserver les clés EFS qui doivent être appliquées via la Stratégie de groupe.
Installation du système de fichiers EFS	Le système de fichiers EFS est installé par défaut avec Windows Server 2008.
Gestion du système de fichiers EFS	Vous pouvez gérer le système de fichiers EFS via la Stratégie de groupe ou à l'aide de l'Assistant Système de fichiers EFS. • Pour afficher les stratégies EFS définies, ouvrez Stratégies de sécurité locales (secpol.msc) et accédez à Paramètres de sécurité\Stratégies de clé publique\Système de fichiers EFS\Propriétés. • Pour démarrer l'Assistant Système de fichiers EFS : Dans le Panneau de configuration, double-cliquez sur Comptes d'utilisateurs. Sous Tâches, cliquez sur Gérer vos certificats de chiffrement de fichier. Pour utiliser le système de fichiers EFS, ouvrez l'Explorateur Windows et cliquez avec le bouton droit sur le fichier ou le dossier à chiffrer. Cliquez sur Propriétés. Dans l'onglet Général, cliquez sur Avancé. Activez la case à cocher Chiffrer le contenu pour sécuriser les données, puis cliquez sur OK. Des options de chiffrement supplémentaires sont disponibles. Vous pouvez aussi utiliser l'outil de ligne de commande Cipher pour afficher ou modifier le chiffrement des dossiers et des fichiers sur les partitions NTFS.

Services de stratégie et d'accès réseau

Les services de stratégie et d'accès réseau fournissent les solutions de connectivité réseau suivantes :

- Protection d'accès réseau (NAP). La protection d'accès réseau (NAP, Network Access Protection) est une technologie de création de stratégie de contrôle d'intégrité, d'application de l'intégrité et de rétablissement de l'intégrité du client fournie avec le système d'exploitation client Windows Vista® et le système d'exploitation Windows Server® 2008. La protection d'accès réseau (NAP) permet aux administrateurs d'établir et d'appliquer automatiquement des stratégies de contrôle d'intégrité, qui peuvent inclure des impératifs logiciels, des impératifs de mise à jour de sécurité, des configurations d'ordinateur requises et d'autres paramètres. Les ordinateurs clients qui ne sont pas conformes à la stratégie de contrôle d'intégrité peuvent recevoir un accès réseau limité jusqu'à ce que leur configuration soit mise à jour ou mise en conformité avec la stratégie. Selon la manière dont vous choisissez de déployer la protection d'accès réseau, les clients non conformes peuvent être mis à jour automatiquement de sorte que les utilisateurs puissent obtenir de nouveau un accès complet au réseau sans avoir à mettre à jour ou à reconfigurer manuellement leur ordinateur.
- Accès sécurisé câblé et sans fil. Lorsque vous déployez des points d'accès sans fil 802.1X, l'accès sans fil sécurisé fournit aux utilisateurs sans fil une méthode d'authentification par mot de passe sécurisé facile à déployer. Lorsque vous déployez des commutateurs d'authentification 802.1X, l'accès câblé vous permet de sécuriser votre réseau en veillant à ce

que les utilisateurs intranet soient authentifiés avant qu'ils ne puissent se connecter au réseau ou obtenir une adresse IP à l'aide du protocole DHCP.

- Solutions d'accès à distance. Les solutions d'accès à distance vous permettent de fournir aux utilisateurs un réseau privé virtuel (VPN) et un accès à distance classique au réseau de votre organisation. Vous pouvez également connecter des succursales à votre réseau à l'aide de solutions VPN, déployer des routeurs logiciels complets sur votre réseau et partager des connexions Internet sur l'intranet.
- Gestion de stratégie de réseau centralisée à l'aide d'un serveur et d'un proxy RADIUS. Au lieu de configurer une stratégie d'accès réseau au niveau de chaque serveur d'accès réseau, tel que des points d'accès sans fil, des commutateurs d'authentification 802.1X, des serveurs VPN et des serveurs d'accès à distance, vous pouvez utiliser un même emplacement pour créer des stratégies qui spécifient tous les aspects des demandes de connexion réseau, y compris l'identité des utilisateurs autorisés à se connecter, le moment où ils peuvent se connecter et le niveau de sécurité requis pour se connecter à votre réseau.

Services de rôle pour les services de stratégie et d'accès réseau

Lorsque vous installez des services de stratégie et d'accès réseau, les services de rôle suivants sont disponibles :

- Serveur de stratégie réseau (NPS). Le serveur NPS (Network Policy Server) est l'implémentation Microsoft d'un serveur et d'un proxy RADIUS. Le serveur NPS vous permet de gérer de manière centralisée les accès au réseau à l'aide de différents serveurs d'accès réseau, y compris des points d'accès sans fil, des serveurs VPN, des serveurs d'accès à distance et des commutateurs d'authentification 802.1X. Par ailleurs, le serveur NPS permet de déployer l'authentification par mot de passe sécurisé à l'aide du protocole PEAP (Protected Extensible Authentication Protocol)-MS-CHAP v2 pour les connexions sans fil. Le serveur NPS contient des éléments clés pour déployer la protection d'accès réseau (NAP) sur votre réseau.

  Les technologies suivantes peuvent être déployées après l'installation du service de rôle NPS :

  - Serveur de stratégie de contrôle d'intégrité NAP. Lorsque vous configurez le serveur NPS en tant que serveur de stratégie de contrôle d'intégrité NAP, il évalue les déclarations d'intégrité (SoH) envoyées par les ordinateurs clients compatibles avec la protection d'accès réseau (NAP) qui souhaitent communiquer sur le réseau. Vous pouvez configurer des stratégies NAP sur le serveur NPS qui permettent à des ordinateurs clients de mettre à jour leur configuration pour devenir compatibles avec la stratégie réseau de votre organisation.
  - Connexion sans fil IEEE 802.11. Le composant logiciel enfichable MMC NPS vous permet de configurer des stratégies de demande de connexion 802.1X pour l'accès au réseau client sans fil IEEE 802.11. Vous pouvez également configurer des points d'accès sans fil en tant que clients RADIUS (Remote Authentication Dial-In User Service) dans NPS, et utiliser NPS en tant que serveur RADIUS pour traiter les demandes de connexion, ainsi que pour effectuer les processus d'authentification, d'autorisation et de gestion des comptes pour les connexions sans fil 802.11. Vous pouvez entièrement intégrer l'accès sans fil IEEE 802.11 à la protection d'accès réseau (NAP) lorsque vous déployez une infrastructure d'authentification 802.1X sans fil afin que l'état d'intégrité des clients sans fil soit vérifié par rapport à la stratégie de contrôle d'intégrité avant que les clients ne soient autorisés à se connecter au réseau.
  - Connexion câblée IEEE 802.3. Le composant logiciel enfichable MMC NPS vous permet de configurer des stratégies de demande de connexion 802.1X pour l'accès au réseau Ethernet client câblé IEEE 802.3. Vous pouvez également configurer des commutateurs compatibles 802.1X en tant que clients RADIUS dans NPS, et utiliser

NPS en tant que serveur RADIUS pour traiter les demandes de connexion, ainsi que pour effectuer les processus d'authentification, d'autorisation et de gestion des comptes pour les connexions Ethernet 802.3. Vous pouvez entièrement intégrer l'accès client câblé IEEE 802.3 à la protection d'accès réseau (NAP) lorsque vous déployez une infrastructure d'authentification câblée 802.1X.

- Serveur RADIUS. Le serveur NPS effectue de façon centralisée les processus d'authentification, d'autorisation et de gestion des comptes pour les connexions sans fil, par commutateur d'authentification, par accès à distance et VPN. Lorsque vous utilisez NPS en tant que serveur RADIUS, vous configurez des serveurs d'accès réseau, tels que des points d'accès sans fil et des serveurs VPN, en tant que clients RADIUS dans NPS. Vous configurez également des stratégies réseau que NPS utilise pour autoriser les demandes de connexion, et vous pouvez configurer la gestion de comptes RADIUS de manière à ce que NPS enregistre les informations de gestion dans des fichiers journaux sur le disque dur local ou dans une base de données Microsoft® SQL Server™.
- Proxy RADIUS. Lorsque vous utilisez NPS en tant que proxy RADIUS, vous configurez des stratégies de demande de connexion qui indiquent au serveur NPS les demandes de connexion à transmettre et les serveurs RADIUS auxquels vous souhaitez transmettre ces demandes. Vous pouvez également configurer le serveur NPS pour qu'il transfère les données de gestion qui doivent être enregistrées par un ou plusieurs ordinateurs dans un groupe de serveurs RADIUS distants.

- Routage et accès à distance. Le service Routage et accès à distance vous permet de déployer des services VPN et d'accès réseau à distance et le multi-protocole LAN-to-LAN, LAN-to-WAN, les réseaux privés virtuels (VPN) et les services de routage de traduction d'adresse réseau (NAT).

  Les technologies suivantes peuvent être déployées lors de l'installation du service de rôle Routage et accès à distance :

  - Service d'accès à distance. Le service Routage et accès à distance vous permet de déployer des connexions VPN PPTP (Point-to-Point Tunneling Protocol), SSTP (Secure Socket Tunneling Protocol) ou L2TP (Layer Two Tunneling Protocol) avec IPsec (Internet Protocol security) pour fournir à l'utilisateur final un accès à distance au réseau de votre organisation. Vous pouvez également créer une connexion VPN de site à site entre deux serveurs situés à différents emplacements. Chaque serveur est configuré à l'aide du service Routage et accès à distance pour envoyer des données privées de manière sécurisée. La connexion entre les deux serveurs peut être permanente (toujours activée) ou sur demande (connexion à la demande).

    L'accès à distance fournit également l'accès à distance classique pour prendre en charge les utilisateurs distants ou à domicile qui se connectent aux intranets des organisations. L'équipement d'accès à distance installé sur le serveur exécutant le service Routage et accès à distance répond aux demandes de connexion entrantes des clients d'accès réseau à distance. Le serveur d'accès à distance répond à l'appel, authentifie et autorise l'appelant et transfère les données entre le client d'accès réseau à distance et l'intranet de l'organisation.

  - Routage. Le routage fournit un routeur logiciel complet et une plateforme ouverte pour le routage et l'interconnexion. Il offre des services de routage aux entreprises situées dans des environnements de réseau local (LAN, Local Area Network) et de réseau étendu (WAN, Wide Area Network).

    Lorsque vous déployez le traducteur d'adresses réseau (NAT), le serveur Routage et accès à distance est configuré de façon à partager une connexion Internet avec des

ordinateurs sur le réseau privé et à traduire le trafic entre son adresse publique et le réseau privé. La traduction d'adresses réseau procure aux ordinateurs du réseau privé une mesure de protection car le routeur configuré avec NAT ne transfère pas le trafic Internet vers le réseau privé à moins qu'un client du réseau privé ne l'ait demandé ou que le trafic n'ait fait l'objet d'une autorisation explicite.

Si vous déployez VPN et NAT, le serveur Routage et accès à distance est configuré de façon à fournir la traduction NAT au réseau privé et à accepter les connexions VPN. Les ordinateurs sur Internet ne seront pas en mesure de déterminer les adresses IP des ordinateurs sur le réseau privé. Toutefois, les clients VPN pourront se connecter aux ordinateurs du réseau privé comme s'ils étaient connectés physiquement au même réseau.

- Autorité HRA (Health Registration Authority). L'Autorité HRA (Health Registration Authority) est un composant NAP qui émet des certificats d'intégrité aux clients qui passent la vérification de stratégie de contrôle d'intégrité exécutée par le serveur NPS à l'aide des déclarations d'intégrité (SoH) des clients. L'Autorité HRA (Health Registration Authority) s'utilise uniquement avec la méthode d'application IPsec NAP.
- HCAP (Host Credential Authorization Protocol). Le protocole HCAP vous permet d'intégrer votre solution de protection d'accès réseau (NAP) Microsoft au serveur de contrôle d'accès réseau Cisco. Lorsque vous déployez le protocole HCAP avec le serveur NPS et la protection d'accès réseau (NAP), le serveur NPS peut prendre en charge l'évaluation de l'intégrité des clients et l'autorisation des clients d'accès 802.1X Cisco.

Gestion du rôle de serveur Services de stratégie et d'accès réseau

Les outils suivants sont fournis pour gérer le rôle de serveur Services de stratégie et d'accès réseau :

- Composant logiciel enfichable MMC NPS. Le composant logiciel enfichable MMC NPS permet de configurer un serveur RADIUS, un proxy RADIUS ou la technologie NAP.
- Commandes Netsh pour NPS. Les commandes Netsh pour NPS fournissent un jeu de commandes en tout point équivalent aux paramètres de configuration disponibles via le composant logiciel enfichable MMC NPS. Les commandes Netsh peuvent être exécutées manuellement à l'invite Netsh ou dans des scripts d'administrateur.
- Composant logiciel enfichable MMC HRA. Le composant logiciel enfichable MMC HRA permet de désigner l'autorité de certification utilisée par l'autorité HRA pour obtenir des certificats d'intégrité pour les ordinateurs clients et définir le serveur NPS auquel l'autorité HRA envoie les déclarations d'intégrité (SoH) des clients afin qu'elles soient vérifiées par rapport à la stratégie de contrôle d'intégrité.
- Commandes Netsh pour HRA. Les commandes Netsh pour HRA fournissent un jeu de commandes en tout point équivalent aux paramètres de configuration disponibles via le composant logiciel enfichable MMC HRA. Les commandes Netsh peuvent être exécutées manuellement à l'invite Netsh ou dans des scripts créés par les administrateurs.
- Composant logiciel enfichable MMC Gestion des clients NAP. Le composant logiciel enfichable MMC Gestion des clients NAP permet de configurer des paramètres de sécurité et des paramètres d'interface utilisateur sur des ordinateurs clients qui prennent en charge l'architecture NAP.
- Commandes Netsh pour la configuration des paramètres du client NAP. Les commandes Netsh pour les paramètres du client NAP fournissent un jeu de commandes en tout point équivalent aux paramètres de configuration disponibles via le composant logiciel enfichable Gestion des clients NAP. Les commandes Netsh peuvent être exécutées manuellement à l'invite Netsh ou dans des scripts créés par les administrateurs.
- Composant logiciel enfichable MMC Routage et accès à distance. Ce composant logiciel enfichable MMC permet de configurer un serveur VPN, une serveur d'accès réseau à distance,

un routeur, la traduction d'adresses réseau (NAT), des réseaux privés virtuels (VPN) et la traduction d'adresses réseau (NAT) ou une connexion de site à site VPN.

- Commandes Netsh pour l'accès à distance. Les commandes Netsh pour l'accès à distance fournissent un jeu de commandes en tout point équivalent aux paramètres de configuration d'accès à distance disponibles via le composant logiciel enfichable MMC Routage et accès à distance. Les commandes Netsh peuvent être exécutées manuellement à l'invite Netsh ou dans des scripts d'administrateur.
- Commandes Netsh pour le routage. Les commandes Netsh pour le routage fournissent un jeu de commandes en tout point équivalent aux paramètres de configuration de routage disponibles via le composant logiciel enfichable MMC Routage et accès à distance. Les commandes Netsh peuvent être exécutées manuellement à l'invite Netsh ou dans des scripts d'administrateur.
- Stratégies de réseau sans fil (IEEE 802.11) - Console de gestion des stratégies de groupe (GPMC). L'extension Stratégies de réseau sans fil (IEEE 802.11) automatise la configuration des paramètres réseau sans fil sur les ordinateurs dotés de pilotes de carte réseau sans fil qui prennent en charge le service de configuration automatique LAN sans fil (service de configuration automatique WLAN). Vous pouvez utiliser l'extension Stratégies de réseau sans fil (IEEE 802.11) dans la console de gestion des stratégies de groupe pour spécifier les paramètres de configuration des clients sans fil Windows XP et/ou Windows Vista. Les extensions de stratégie de groupe Stratégies de réseau sans fil (IEEE 802.11) incluent des paramètres sans fil globaux, la liste des réseaux favoris, des paramètres WPA (Wi-Fi Protected Access) et des paramètres IEEE 802.1X.

  Une fois configurés, les paramètres sont téléchargés sur les clients sans fil Windows membres du domaine. Les paramètres sans fil configurés par cette stratégie font partie de la stratégie de groupe Configuration de l'ordinateur. Par défaut, les stratégies de réseau sans fil (IEEE 802.11) ne sont pas configurées ni activées.

- Commandes Netsh pour le réseau local sans fil (WLAN). Vous pouvez utiliser la commandes Netsh WLAN au lieu de la stratégie de groupe pour configurer des paramètres de connectivité et de sécurité sans fil Windows Vista. Les commandes Netsh wlan vous permettent de configurer l'ordinateur local ou plusieurs ordinateurs à l'aide d'un script d'ouverture de session. Vous pouvez également utiliser les commandes Netsh wlan pour afficher les paramètres de stratégie de groupe sans fil et administrer les paramètres WISP (Wireless Internet Service Provider) et les paramètres utilisateur sans fil.

  L'interface Netsh sans fil offre les avantages suivants :

  - Prise en charge du mode mixte : Permet aux administrateurs de configurer des clients pour qu'ils prennent en charge plusieurs options de sécurité. Par exemple, un client peut être configuré pour prendre en charge les standards d'authentification WPA2 et WPA. Le client peut ainsi utiliser WPA2 pour se connecter à des réseaux qui prennent en charge le standard WPA2 et WPA pour se connecter à des réseaux qui prennent uniquement en charge le standard WPA.
  - Blocage des réseaux indésirables : Les administrateurs peuvent bloquer des réseaux sans fil n'appartenant pas à l'entreprise et masquer leur accès en ajoutant des réseaux ou des types de réseaux à la liste des réseaux refusés. De la même manière, les administrateurs peuvent autoriser l'accès à des réseaux sans fil d'entreprise.
- Stratégies de réseau câblé (IEEE 802.3) - Console de gestion des stratégies de groupe (GPMC). Les stratégies de réseau câblé (IEEE 802.3) permettent de spécifier et de modifier les paramètres de configuration des clients Windows Vista équipés de cartes et de pilotes réseau qui prennent en charge le service de configuration automatique de réseau câblé. Les extensions de stratégie de groupe Stratégies de réseau sans fil (IEEE 802.11) incluent des

paramètres de réseau câblé globaux et IEEE 802.1X. Ces paramètres incluent l'ensemble des éléments de configuration câblés associés aux onglets Général et Sécurité.

Une fois configurés, les paramètres sont téléchargés sur les clients sans fil Windows membres du domaine. Les paramètres sans fil configurés par cette stratégie font partie de la stratégie de groupe Configuration de l'ordinateur. Par défaut, les stratégies de réseau câblé (IEEE 802.3) ne sont pas configurées ni activées.

- Commandes Netsh pour le réseau local (LAN) câblé. Vous pouvez utiliser l'interface Netsh LAN au lieu de la stratégie de groupe dans Windows Server 2008 pour configurer des paramètres de connectivité et de sécurité de réseau câblé Windows Vista. Vous pouvez utiliser la commande Netsh LAN pour configurer l'ordinateur local, ou les commandes dans des scripts d'ouverture de session pour configurer plusieurs ordinateurs. Les commandes Netsh lan permettent également d'afficher les stratégies de réseau câblé (IEEE 802.3) et d'administrer les paramètres de réseau câblé 1x client.

Les technologies réseaux

Microsoft Windows Server® 2008 offre une large gamme de technologies en réponse aux besoins complexes des environnements de connexion actuels. Les technologies réseau de Windows Server 2008 sont conçues pour prendre en charge tous les types d'entreprises, des petites configurations réseau entre agences aux solutions pour grandes entreprises.

Cette rubrique contient les vues d'ensemble suivantes :

- TCP/IP
- Routage
- Accès à distance
- Surveillance réseau
- Accès et sécurité du réseau

Le protocole TCP/IP

Le protocole TCP/IP est une suite de protocoles normalisés prenant en charge les communications sur les réseaux d'entreprise et Internet. Deux versions du protocole TCP/IP sont prises en charge par Windows Server 2008 :

IPv4

IPv4 est une suite de protocoles et de normes basée sur la spécification IP d'origine décrite dans le document RFC 791, au sein de la base de données RFC de l'IETF ; l'utilisation de cette suite est largement répandue aujourd'hui sur Internet et sur les réseaux privés. IPv4 dispose d'un espace d'adresses dont la taille s'amenuise progressivement avec l'extension d'Internet. L'augmentation du nombre d'adresses IP et la prise en charge des nouvelles technologies réseau sont des facteurs qui encouragent l'adoption de la suite de protocoles et de normes IPv6.

IPv6

IPv6 est une suite de protocoles et de normes qui prend en charge un espace d'adresses beaucoup plus important que la suite IPv4. IPv6 fournit des adresses IP sources et de destination codées sur 128 bits (16 octets). En revanche, IPv4 fournit des adresses IP sources et de destination codées sur 32 bits (4 octets). IPv6 bénéficie de nombreuses autres améliorations en matière de sécurité et d'efficacité.

Routage

Les technologies de routage gèrent le flux de données entre les segments de réseau, également appelés sous-réseaux. Ces technologies de routage sont les suivantes :

- Routage monodiffusion
- Routage multidiffusion

Routage monodiffusion

Ce type de routage transmet le trafic destiné à un emplacement unique sur un réseau, entre un hôte source et un hôte de destination, à l'aide de routeurs. De nos jours, la majorité du trafic réseau mondial s'effectue sur des réseaux IPv4 (Internet Protocol version 4), et la plus grande partie du trafic généré par les utilisateurs sur les réseaux IPv4 est de type monodiffusion. Le routage IP monodiffusion s'effectue sur tous les réseaux IP connectés par des routeurs.

Routage multidiffusion

La multidiffusion (ou émission multiple) est l'envoi du trafic réseau à un groupe de points de terminaison. Seuls les membres du groupe de points de terminaison à l'écoute du trafic de multidiffusion (groupe de multidiffusion) traitent le trafic de multidiffusion. Tous les autres nœuds ignorent le trafic de multidiffusion.

Le concept d'appartenance aux groupes est essentiel dans l'émission multiple en protocole Internet. Des datagrammes de multidiffusion IP sont envoyés à un groupe ; seuls les membres du groupe peuvent recevoir ces datagrammes. Un groupe est identifié par une adresse de multidiffusion IP unique, qui est une adresse IP de classe D, dont la plage est comprise entre 224.0.0.0 et 239.255.255.255 (représentée sous la forme 224.0.0.0/4 dans la notation CIDR (Classless Interdomain Routing)). Ces adresses de classe D sont appelées adresses de groupes. Un hôte source envoie des datagrammes de multidiffusion à une adresse de groupe. Les hôtes de destination informent un routeur local qu'ils doivent joindre le groupe.

Vue d'ensemble de l'accès à distance

La fonctionnalité d'accès à distance contient des informations sur la prise en charge par Windows Server 2008 des solutions d'accès à distance, notamment :

- Réseau privé virtuel (VPN)
- Accès à distance
- Telnet

Réseaux privés virtuels (VPN)

Les réseaux privés virtuels (VPN) sont des connexions point à point sur un réseau privé ou public, par exemple Internet. Un client VPN utilise des protocoles TCP/IP spéciaux, appelés protocoles de tunneling, pour envoyer un appel virtuel vers un port virtuel sur un serveur VPN. Dans un déploiement VPN classique, un client entame une connexion point à point virtuelle avec un serveur d'accès à distance via Internet. Le serveur d'accès à distance répond à l'appel, authentifie l'appelant, puis transfère les données entre le client VPN et le réseau privé de l'organisation.

Pour émuler une liaison point à point, les données sont encapsulées avec un en-tête. L'en-tête fournit des informations de routage qui permettent aux données de traverser le réseau public ou partagé pour atteindre leur point de terminaison. Pour émuler une liaison privée, les données envoyées sont

chiffrées par souci de confidentialité. Les paquets interceptés sur le réseau public ou partagé ne sont pas déchiffrables sans les clés de chiffrement. La liaison dans laquelle les données privées sont encapsulées et chiffrées se nomme une connexion VPN.

Accès à distance

L'accès à distance permet à des clients d'accès à distance de se connecter à un réseau. Les clients d'accès à distance utilisent l'infrastructure disponible en matière de télécommunications pour créer un circuit physique ou virtuel temporaire vers un port situé sur un serveur d'accès à distance connecté à un réseau. Une fois la connexion établie entre le client d'accès à distance et le serveur d'accès à distance, le serveur d'accès à distance transfère les paquets entre le client d'accès à distance et le réseau.

Telnet

Telnet est un protocole qui permet les connexions à distance entre un client d'accès à distance et un hôte. Vous pouvez utiliser une invite de commandes locale sur un client d'accès à distance pour exécuter des programmes de ligne de commande, des commandes d'interpréteur de commandes, ainsi que des scripts, dans une session de console de commandes à distance.

la surveillance réseau

La fonctionnalité de surveillance réseau contient des informations sur les services de surveillance réseau pris en charge par Windows Server 2008. Ces services sont les suivants :

- Protocole SNMP (Simple Network Management Protocol)
- QoS (Qualité de service) basée sur la stratégie

Protocole SNMP (Simple Network Management Protocol)

Le protocole SNMP (Simple Network Management Protocol) représente une infrastructure et un protocole de gestion réseau largement utilisés dans les réseaux TCP/IP pour effectuer des tâches à distance telles que la surveillance, la configuration et le dépannage des ressources réseau à partir d'un système de gestion SNMP situé à un emplacement central.

Qualité de service (QoS) basée sur la stratégie

La qualité de service (QoS) est un ensemble d'exigences en matière de service auxquelles un réseau doit répondre pour garantir un niveau de service adéquat lors d'une transmission de données. QoS permet aux programmes en temps réel de tirer le meilleur parti de l'utilisation de la bande passante réseau.

l'accès et de la sécurité du réseau

La fonctionnalité d'accès réseau prend en charge les solutions sécurisées d'accès au réseau, notamment :

- Connexions authentifiées câblées ou sans fil 802.1X
- Connection Manager
- Pare-feu Windows avec sécurité avancée

Connexions câblées ou sans fil basées sur l'authentification 802.1X

La norme IEEE (Institute of Electrical and Electronics Engineers) 802.1X, définit l'accès authentifié pour les connexions Ethernet câblées (IEEE 802.3) et sans fil (IEEE 802.11). Pour les connexions sans fil, l'ensemble de normes IEEE 802.11 permet à l'extension d'un réseau local câblé d'inclure des clients mobiles, sans fil. L'authentification 802.1X des connexions Ethernet câblées (802.3) et sans fil (802.11) empêche les utilisateurs et ordinateurs non authentifiés et non autorisés de se connecter à votre réseau. L'accès basé sur l'authentification 802.1X repose sur des commutateurs Ethernet compatibles 802.1X et des points d'accès sans fil compatibles 802.1X pour fournir un contrôle d'accès réseau basé sur les ports afin d'empêcher les utilisateurs et ordinateurs non authentifiés et non autorisés d'accéder aux ressources réseau et d'envoyer des paquets sur le réseau. En matière de sécurité des connexions sans fil, les réseaux sans fil 802.11 utilisent la norme d'authentification IEEE 802.1X, ainsi que la norme WPA2 (Wi-Fi Protected Access version 2) ou WPA pour le chiffrement.

Windows Server 2008 fournit les fonctionnalités utilisables avec les commutateurs Ethernet et les points d'accès sans fil compatibles 802.1X pour assurer la prise en charge complète du déploiement et de la gestion des infrastructures réseau basées sur l'authentification 802.1X. Vous pouvez utiliser les fonctionnalités de Windows Server 2008 avec des commutateurs compatibles 802.1X afin de fournir et de gérer un accès Ethernet câblé basé sur l'authentification 802.1X pour des ordinateurs exécutant Windows Vista® et Windows Server 2008. Vous pouvez utiliser conjointement les fonctionnalités de Windows Server 2008 et des points d'accès sans fil compatibles 802.1X afin de fournir et de gérer un accès sans fil IEEE 802.11 basé sur l'authentification 802.1X pour des ordinateurs exécutant Windows® XP, Windows Server 2003, Windows Vista et Windows Server 2008.

Connection Manager

Permet aux administrateurs de créer des connexions ayant une interface utilisateur cohérente sur tous les systèmes d'exploitation Windows, d'utiliser des protocoles d'authentification spécifiques, de contrôler les programmes requis, de vérifier les paramètres de Registre, de mettre à jour les fichiers et les annuaires téléphoniques, ou d'effectuer plusieurs combinaisons possibles de ces tâches. Le Kit d'administration de Microsoft Connection Manager disponible dans Windows Vista et Windows Server 2008 offre de nombreux avantages par rapport à la création manuelle de connexions.

Pare-feu Windows avec sécurité avancée

Le Pare-feu Windows avec sécurité avancée associe un pare-feu hôte à la sécurité du protocole Internet (IPsec). À la différence d'un pare-feu de périmètre, le Pare-feu Windows avec sécurité avancée s'exécute sur chaque ordinateur équipé de Microsoft Windows Vista ou Windows Server 2008, et fournit une protection locale contre les attaques réseau susceptibles de franchir le réseau de périmètre ou de se déclencher au sein de votre organisation. Il fournit également une sécurité de connexion d'ordinateur à ordinateur qui vous permet d'imposer l'authentification et la protection des données pour toutes les communications.

PLATE-FORME WEB ET D'APPLICATIONS

Serveurs Web

Le rôle de serveur Web dans Windows Server® 2008 vous permet de partager des informations avec des utilisateurs sur Internet, sur un intranet ou un extranet. Windows Server 2008 met à votre disposition IIS 7.0, qui est une plateforme Web unifiée intégrant IIS, ASP.NET et Windows Communication Foundation. Les principales fonctionnalités et améliorations d'IIS 7.0 sont les suivantes :

- Plateforme Web unifiée qui propose une solution Web uniforme unique aux administrateurs et développeurs.
- Sécurité améliorée et possibilité de personnaliser le serveur pour réduire la zone exposée aux attaques.
- Fonctionnalités de diagnostics et de dépannage simplifiées pour aider à la résolution de problèmes.
- Configuration améliorée et prise en charge des batteries de serveurs.
- Administration déléguée pour l'hébergement et les charges de travail des entreprises.

Les sections suivantes contiennent des informations supplémentaires sur le rôle de serveur Web, les fonctionnalités requises et facultatives d'un serveur Web ainsi que les éléments matériels et logiciels nécessaires à l'exécution d'un serveur Web. À la fin de cette rubrique, vous apprendrez à ouvrir l'interface du serveur Web et à rechercher des informations supplémentaires sur les serveurs Web.

Qu'est-ce qu'un serveur Web ?

Un serveur Web est un ordinateur disposant d'un logiciel spécifique qui lui permet d'accepter des demandes d'ordinateurs clients et de renvoyer des réponses à ces demandes. Un serveur Web permet de partager des informations via Internet ou via des réseaux intranet et extranet.

Avec un serveur Web, vous pouvez effectuer les opérations suivantes :

- fournir des informations à des utilisateurs sur Internet ;
- permettre aux utilisateurs de télécharger du contenu avec FTP ou WebDAV (World Wide Web Distributed Versioning and Authoring) ;
- héberger des services Web contenant de la logique métier pour des applications à trois niveaux ;
- distribuer des applications aux utilisateurs via Internet plutôt que par l'intermédiaire d'un média physique, tel que des disquettes ou des CD-ROM.

Les serveurs Web peuvent être utiles pour différents clients et besoins. Par exemple :

- Les petites entreprises peuvent fournir des informations sur les services qu'elles proposent par le biais d'un site Web simple.
- Les entreprises de taille moyenne peuvent proposer leurs produits et services via un système de commande en ligne constitué de différentes applications dans un site.
- Les grandes entreprises peuvent développer et fournir des applications de gestion à leurs employés via des intranets d'entreprise.
- Les sociétés d'hébergement peuvent offrir à chacun de leurs clients de l'espace serveur et des services permettant d'héberger différents contenus et applications en ligne.
- Les entreprises commerciales peuvent fournir des applications et des informations pertinentes à leurs partenaires commerciaux via des extranets.

Fonctionnalités du rôle de serveur Web IIS 7.0

Les sections suivantes décrivent les fonctionnalités et améliorations d'IIS 7.0, la plateforme Web dans Windows Server 2008.

Nouveaux outils d'administration

IIS 7.0 propose une nouvelle interface utilisateur basée sur les tâches et un nouvel outil de ligne de commande performant. Ces nouveaux outils d'administration vous permettent :

- de gérer IIS et ASP.NET dans un seul outil ;
- d'afficher des informations d'intégrité et de diagnostic, ce qui inclut la possibilité de voir les demandes en cours d'exécution en temps réel ;
- de configurer les autorisations de rôle et d'utilisateur pour les sites et les applications ;
- de déléguer la configuration de site et d'application à des utilisateurs qui ne sont pas administrateurs.

Configuration

IIS 7.0 propose un nouveau magasin de configuration qui intègre les paramètres de configuration d'IIS et d'ASP.NET pour l'intégralité de la plateforme Web. Ce nouveau magasin de configuration vous permet :

- de configurer les paramètres d'IIS et d'ASP.NET dans un seul magasin de configuration qui utilise un format cohérent et est accessible à partir d'un ensemble d'API commun ;
- de déléguer la configuration de manière précise et sûre aux fichiers de configuration distribués se trouvant dans les répertoires de contenu ;
- de copier la configuration et le contenu d'une application ou d'un site particulier sur un autre ordinateur ;
- de créer un script de configuration pour IIS et ASP.NET à l'aide d'un nouveau fournisseur WMI.

Diagnostic et dépannage

Le serveur Web IIS 7.0 permet de diagnostiquer et de dépanner plus facilement les problèmes survenant sur le serveur Web. Les nouvelles fonctionnalités de diagnostic et de dépannage vous permettent :

- de voir les informations d'état en temps réel sur les pools d'applications, les processus de travail, les sites, les domaines d'application et les demandes en cours ;
- d'enregistrer des informations de suivi détaillé sur une demande lors de son parcours dans le processus IIS de traitement des demandes ;
- de configurer IIS de façon à enregistrer automatiquement les informations de suivi détaillé en fonction du temps écoulé ou des codes de réponse d'erreur.

Architecture modulaire

Dans IIS 7.0, le serveur Web se compose de modules que vous pouvez ajouter ou supprimer du serveur selon vos besoins. Cette nouvelle architecture vous permet :

- de personnaliser votre serveur en ajoutant uniquement les fonctionnalités dont vous avez besoin, ce qui minimise la sécurité et l'encombrement mémoire du serveur Web ;
- de configurer les fonctionnalités (telles que l'authentification, l'autorisation et les erreurs personnalisées) précédemment en double dans IIS et ASP.NET à un seul emplacement ;
- d'appliquer les fonctionnalités ASP.NET existantes, telles que l'authentification par formulaire ou l'autorisation d'URL, à tous les types de demandes.

Compatibilité

Le serveur Web IIS 7.0 garantit une compatibilité maximale avec les applications existantes. IIS 7.0 permet de continuer à :

- utiliser les scripts d'interfaces ADSI (Active Directory Service Interfaces) et WMI existants ;
- exécuter les applications ASP (Active Server Pages) sans modification de code ;
- exécuter les applications ASP.NET 1.1 et ASP.NET 2.0 existantes sans modification de code (lorsqu'elles sont exécutées dans un pool d'applications en mode ISAPI dans IIS 7.0) ;
- utiliser les extensions ISAPI existantes sans effectuer de modifications ;
- utiliser les filtres ISAPI existants à l'exception de ceux qui reposent sur des notifications READ RAW.

Considérations matérielles et logicielles

La configuration matérielle et logicielle requise pour le rôle de serveur Web est identique à celle de Windows Server 2008. Utilisez les compteurs de performance, les résultats des tests d'atelier, les données existantes des environnements de production et les déploiements pilotes pour déterminer la capacité dont le serveur a besoin et procédez à des ajustements si nécessaire.

Installation d'un serveur Web

Une fois le système d'exploitation installé, vous pouvez utiliser Tâches de configuration initiales ou Gestionnaire de serveur pour installer les rôles du serveur. Pour installer le rôle de serveur Web, dans la liste des tâches, cliquez sur Ajouter un rôle, puis dans la liste des rôles de serveur figurant dans l'Assistant, cliquez sur Serveur Web (IIS).

Gestion d'un serveur Web

Les rôles de serveur sont gérés à l'aide des composants logiciels enfichables MMC (Microsoft Management Console). Utilisez le Gestionnaire des services Internet (IIS) pour gérer un serveur Web. Pour ouvrir le Gestionnaire des services Internet (IIS), cliquez sur Démarrer, Tous les programmes, Outils d'administration, puis cliquez sur Gestionnaire des services Internet (IIS).

Serveur d'applications

Le serveur d'applications fournit un environnement intégré pour le déploiement et l'exécution des applications d'entreprise personnalisées conçues à l'aide de Microsoft® .NET Framework version 3.0. Lorsque vous installez le rôle de serveur d'applications, vous pouvez sélectionner les services qui prennent en charge les applications conçues pour utiliser COM+, Message Queuing, les services Web et les transactions distribuées.

Le serveur d'applications fournit aux professionnels de l'informatique et aux développeurs les avantages suivants :

- Une exécution centrale qui prend en charge la gestion et le déploiement des applications d'entreprise aux performances élevées.
- L'environnement de développement .NET Framework qui propose un modèle de programmation simplifié et un modèle d'exécution haute performance destiné aux applications serveur.

  Le .NET Framework active les services Web et intègre les nouvelles applications aux applications et à l'infrastructure existantes.

- Un Assistant d'installation convivial qui offre des choix pour les différents services et fonctionnalités de rôles nécessaires à l'exécution d'applications dans votre organisation.
- Une fonctionnalité d'installation qui installe automatiquement les fonctionnalités pour un service de rôle donné.

Dans les sections suivantes, découvrez mieux le rôle de serveur d'applications, les fonctionnalités requises et facultatives du rôle de serveur d'applications, les logiciels et le matériel utilisés pour son exécution. Au terme de cette rubrique, vous apprendrez à ouvrir les interfaces du rôle de serveur d'applications et comment accéder à d'autres informations sur le rôle de serveur d'applications.

Qu'est-ce que le rôle de serveur d'applications ?

Le serveur d'applications est un rôle de serveur élargi au sein du système d'exploitation Windows Server® 2008. La nouvelle version du serveur d'applications offre un environnement intégré pour le déploiement et l'exécution des applications d'entreprise serveur personnalisées. Cet environnement simplifie le processus de déploiement des applications qui répondent aux demandes émises sur le réseau par les ordinateurs clients distants ou d'autres applications. Généralement, les applications déployées sur le serveur d'applications bénéficient d'une ou de plusieurs des technologies suivantes :

- Les services Internet (IIS), le serveur HTTP (Hypertext Transfer Protocol) intégré à Windows Server
- Microsoft .NET Framework version 3.0 et 2.0
- ASP.NET
- COM+
- Microsoft DTC (Microsoft Distributed Transaction Coordinator)
- Message Queuing

- Services Web conçus à l'aide de Windows Communication Foundation (WCF)

Le rôle de serveur d'applications est utile lorsque Windows Server 2008 exécute des applications qui dépendent des services ou des fonctionnalités qui font partie du rôle intégré du serveur d'applications. Sélectionnez les services ou les fonctionnalités appropriés lorsque vous installez le rôle du serveur d'applications. Par exemple, vous pouvez installer une configuration spécifique de Microsoft BizTalk® Server qui fait appel à un ou plusieurs services ou fonctionnalités de l'environnement du serveur d'applications.

Généralement, le rôle du serveur d'applications est essentiel lors du déploiement d'une application d'entreprise qui nécessite des services de rôle spécifiques qui sont définis par le développeur de l'application. Par exemple, votre organisation utilise peut-être une application de traitement des commandes qui accède aux enregistrements clients stockés dans une base de données. L'application accède aux enregistrements clients via un jeu de services Web WCF. Dans ce cas, comme WCF fait partie du .NET Framework 3.0, une fonctionnalité du serveur d'applications, vous pouvez utiliser le serveur d'applications pour déployer et configurer WCF sur des ordinateurs sur lesquels s'exécutent votre application de traitement des commandes, et vous pouvez installer la base de données sur le même ordinateur ou sur un autre ordinateur.

Les applications de serveur ne nécessitent pas toutes l'installation du rôle du serveur d'applications pour fonctionner correctement. Par exemple, le rôle du serveur d'applications n'est pas nécessaire pour prendre en charge Microsoft Exchange Server ou Microsoft SQL Server™ dans Windows Server 2008.

Pour déterminer si le rôle du serveur d'applications est nécessaire aux applications de votre organisation, faites collaborer étroitement vos administrateurs avec les développeurs de l'application afin de connaître les besoins de l'application, notamment, si celle-ci doit faire appel aux composants COM+ ou .NET Framework 3.0.

Fonctionnalités du rôle de serveur d'applications

Les fonctionnalités suivantes font partie du rôle du serveur d'applications et, à l'exception des fonctionnalités par défaut, elles sont sélectionnées par l'administrateur au cours de l'installation du rôle.

Application Server Foundation

Application Server Foundation est le groupe des technologies installées par défaut lorsque vous installez le rôle du serveur d'applications. En fait, Application Server Foundation correspond au .NET Framework 3.0.

Windows Server 2008 inclut le .NET Framework 2.0, indépendamment du rôle de serveur qui est installé. Le .NET Framework 2.0 contient le langage CLR (Common Language Runtime) qui fournit un environnement d'exécution du code qui promeut une exécution sécurisée du code, un déploiement simplifié du code et une prise en charge de l'interopérabilité des langages ainsi que des bibliothèques complètes destinées à la création d'applications.

À un niveau supérieur, le .NET Framework 3.0 est composé des trois composants de base suivants :

Le .NET Framework

WCF

Windows Presentation Foundation (WPF)

Windows Workflow Foundation (WF)

Serveur Web

La sélection de cette option au cours de l'installation du serveur d'applications ajoute IIS version 7.0, le serveur Web intégré à Windows Server 2008. Bien que disponible dans Windows Server depuis plusieurs années, IIS a cependant fait l'objet d'une révision en profondeur pour Windows Server 2008 afin de bénéficier d'améliorations de performance, de sécurité, de gestion, de prise en charge, de fiabilité et de modularité.

IIS présente les avantages suivants :

- IIS permet au serveur d'applications d'héberger des sites Web internes ou externes ou des services avec un contenu statique ou dynamique.
- IIS offre une prise en charge pour les applications ASP.NET accessibles à partir d'un navigateur Web.
- IIS fournit une prise en charge des services Web intégrés à WCF ou à ASP.NET.

Accès réseau COM+

La sélection de cette option au cours de l'installation du serveur d'applications ajoute l'accès réseau COM+ pour l'invocation distante des composants d'application qui sont créés et hébergés dans COM+. Certains composants d'applications sont aussi parfois appelés des composants de services d'entreprise.

L'accès réseau COM+ est une fonction d'invocation distante prise en charge dans Windows Server depuis Windows 2000 Server, et qui continue d'être prise en charge dans Windows Server 2008. Les applications plus récentes utilisent généralement WCF pour prendre en charge des invocations distantes étant donné que WCF offre un couplage souple qui réduit l'interdépendances des systèmes intégrés, ainsi qu'une interopérabilité multi-plateforme.

Service d'activation de processus Windows

La sélection de cette option au cours de l'installation du rôle de serveur d'applications ajoute le service d'activation de processus Windows (WAS, Windows Process Activation Service). Le service WAS est le nouveau mécanisme d'activation de processus pour les systèmes d'exploitation Windows Vista® et Windows Server 2008. Le service WAS conserve le modèle de traitement IIS 6.0 familier (pools d'applications et activation de processus basée sur des messages) et les fonctionnalités d'hébergement (par exemple, la protection rapide contre les pannes, le contrôle de santé et le recyclage), mais il supprime de l'architecture d'activation la dépendance vis à vis de HTTP. IIS 7.0 fait appel au service WAS pour accomplir l'activation basée sur des messages sur HTTP. Le service WCF peut aussi utiliser les protocoles non HTTP pris en charge par WAS, tels que TCP, Message Queuing, et les canaux nommés, en plus de HTTP, pour fournir une activation basée sur des messages. De cette manière, les applications qui font appel aux protocoles de communication peuvent exploiter les fonctionnalités IIS, telles que le recyclage de processus, la protection rapide contre les pannes et le système de configuration courant, qui étaient réservées auparavant aux applications HTTP.

Partage de port Net.TCP

Le service Partage de port Net.TCP est un nouveau service dans Windows Server 2008. La sélection de cette option au cours de l'installation du serveur d'applications permet d'ajouter ce service. Grâce à ce service de rôle, plusieurs applications peuvent utiliser le port TCP unique pour les communications

entrantes. Par exemple, plusieurs applications dans une architecture SOA (Service-Oriented Architecture) créée à l'aide de WCF peuvent partager le même port. Le partage des ports fait souvent partie des configurations de pare-feu ou des restrictions réseau qui n'autorisent qu'un nombre limité de ports ouverts ou si plusieurs instances distinctes d'une application WCF doivent s'exécuter et être disponibles simultanément.

Pour permettre aux applications WCF de partager des ports (également connu sous le nom de multiplexage), le service Partage de port Net.TCP effectue le multiplexage. Le service accepte les demandes de connexions entrantes à l'aide de TCP. Le service transmet ensuit les demandes entrantes automatiquement aux divers services WCF en fonction des adresses cibles des demandes. Le partage des ports ne fonctionne que lorsque les applications WCF utilisent le protocole Net.TCP pour des communications entrantes.

Transactions distribuées

La prise en charge des transactions distribuées dans Windows Server remonte à Microsoft Windows NT® Server 4.0, cette fonctionnalité continue d'être prise en charge dans Windows Server 2008. Les applications qui se connectent à plusieurs bases de données ou d'autres ressources transactionnelles pour effectuer des mises à jour peuvent nécessiter l'utilisation des sémantiques transactionnelles de type « tout ou rien », technologie qui vérifie que chaque portion d'une transaction est complète sans quoi toute la transaction est restaurée à son état d'origine. Ces ressources et bases de données transactionnelles peuvent se trouver sur un seul ordinateur ou être distribuées sur un réseau. Le service MS DTC dans Windows Server 2008 fournit ces sémantiques transactionnelles.

Considérations logicielles et matérielles

Le rôle du serveur d'applications ne contient aucune autre configuration matérielle ou logicielle que celle nécessaire à l'exécution de Windows Server 2008. Cependant, votre application qui exécute l'environnement du serveur d'applications peut nécessiter ses propres critères en matière de capacité de traitement, de mémoire ou d'espace disque. Il vous appartient d'identifier ces critères en collaborant avec les développeurs chargés de fournir ces applications.

Installation du rôle de serveur d'applications

Au terme de l'installation du système d'exploitation, une liste des tâches de configuration initiales s'affiche. Procédez comme suit pour installer le rôle du serveur d'applications à l'aide de l'Assistant Ajout de rôles.

Pour installer le rôle de serveur d'applications

1. Cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Gestionnaire de serveur.
2. Si la boîte de dialogue Contrôle de compte d'utilisateur apparaît, confirmez que l'action affichée est celle que vous souhaitez, puis cliquez sur Continuer.
3. Dans le menu Action, cliquez sur Ajouter des rôles.
4. L'Assistant Ajout de rôles apparaît. Cliquez sur Suivant.
5. Dans la page Sélectionner des rôles de serveurs, activez la case à cocher Serveur d'applications.
6. Dans la boîte de dialogue Ajouter les fonctionnalités requises pour Serveur d'applications ?, cliquez sur Ajouter les fonctionnalités requises, puis cliquez sur Suivant.
7. Les informations relatives au rôle du serveur d'applications s'affichent. Prenez connaissance des informations, puis cliquez sur Suivant.
8. Dans la page Sélectionner les services de rôle, sélectionnez les services de rôles qui sont nécessaires à l'exécution de vos applications (par exemple, Prise en charge du serveur Web

(IIS) pour héberger les sites Web ou Transactions distribuées si vos applications nécessitent des fonctions de transactions distantes), puis cliquez sur Suivant. Application Server Foundation, le service de rôle par défaut, est toujours installé comme composant du rôle du serveur d'applications.

9. Si l'installation d'une fonctionnalité de prise en charge ou d'un service de rôle provenant d'un autre rôle est requise, la page suivante fournit des informations importantes sur la fonctionnalité ou l'ensembles des fonctionnalités. Cliquez sur Suivant pour passer à la page Confirmer les options d'installation.
10. Cliquez sur Installer pour commencer l'installation du rôle du serveur d'applications avec les options qui s'affichent sur la page. Le processus d'installation peut être long selon les services de rôle que vous choisissez. Après le démarrage du processus d'installation, aucune saisie de l'opérateur n'est nécessaire. Au terme du processus d'installation, le statut de l'installation s'affiche sur la page Résultats de l'installation.

Gestion du rôle de serveur d'applications

L'installation du rôle du serveur d'applications n'installe pas un composant logiciel enfichable MMC (Microsoft Management Console). Vous pouvez gérer le rôle du serveur d'applications via le Gestionnaire de serveur.

GESTION DES SERVEURS

Gestionnaire de serveur

Windows Server® 2008 facilite la gestion et la sécurisation de plusieurs rôles de serveur dans une entreprise avec la console Gestionnaire de serveur. Gestionnaire de serveur dans Windows Server 2008 fournit une source unique de gestion de l'identité d'un serveur et des informations système, en affichant l'état du serveur, en identifiant les problèmes de configuration de rôle de serveur et en gérant tous les rôles installés sur le serveur.

Comment le Gestionnaire de serveur rationalise l'Administration serveur

Gestionnaire de serveur permet une administration serveur plus efficace en autorisant les administrateurs à effectuer les tâches suivantes à l'aide d'un seul outil :

- Afficher et apporter des modifications aux rôles et fonctionnalités de serveur installés sur le serveur.
- Effectuer des tâches de gestion associées au cycle de vie opérationnel du serveur, tel que le démarrage ou l'arrêt de services et la gestion de comptes d'utilisateur local.
- Réaliser des tâches de gestion associées au cycle de vie opérationnel des rôles installés sur le serveur.
- Déterminer l'état d'un serveur, identifier des événements critiques, analyser et dépanner des problèmes ou des échecs de configuration.

1 Rôles, services de rôle et fonctionnalités

Gestionnaire de serveur dans Windows Server® 2008 remplace les consoles de gestion antérieures telles que Configurer votre serveur et Gérer votre serveur. Avec Gestionnaire de serveur, vous préparez votre serveur pour un déploiement en installant des packages logiciels logiques identifiés comme rôles, services de rôle et fonctionnalités.

Cette rubrique définit les rôles, services de rôle et fonctionnalités et traite leur intégration dans votre entreprise.

Que sont les rôles de serveur, les services de rôle et les fonctionnalités ?

Cette section définit les termes **rôle**, **service de rôle** et **fonctionnalité** tels qu'ils s'appliquent à Windows Server 2008.

Rôles

Un rôle de serveur est un ensemble de programmes logiciels qui, une fois installés et correctement configurés, permettent à un ordinateur de remplir une fonction spécifique pour plusieurs utilisateurs ou d'autres ordinateurs dans un réseau. En règle générale, les rôles partagent les caractéristiques suivantes :

- Ils décrivent la fonction, l'utilisation ou le but principal d'un ordinateur. Un ordinateur spécifique peut être consacré à un rôle unique très utilisé dans l'entreprise, ou bien remplir plusieurs rôles si chaque rôle est uniquement peu utilisé dans l'entreprise.

- Ils fournissent aux utilisateurs d'une organisation un accès à des ressources gérées par d'autres ordinateurs, tels que des sites Web, des imprimantes ou des fichiers stockés sur différents ordinateurs.

- Ils incluent généralement leurs propres bases de données, qui peuvent placer des demandes d'utilisateur ou d'ordinateur en file d'attente ou enregistrer des informations sur des utilisateurs ou des ordinateurs réseau associés au rôle. Par exemple, Services de domaine Active Directory inclut une base de données pour le stockage des noms et des relations hiérarchiques de tous les ordinateurs d'un réseau.

- Une fois correctement installés et configurés, les rôles ont été conçus de manière à fonctionner automatiquement, ce qui permet aux ordinateurs sur lesquels ils sont installés d'effectuer des tâches prescrites avec des commandes ou une supervision d'utilisateur limitée.

Services de rôle

Les services de rôle sont des programmes logiciels qui fournissent la fonctionnalité d'un rôle. Lorsque vous installez un rôle, vous pouvez choisir les services de rôle que le rôle doit fournir pour d'autres utilisateurs et ordinateurs dans votre entreprise. Certains rôles, tels que Serveur DNS, possèdent une seule fonction et ne disposent donc pas de services de rôle disponibles. D'autres rôles, tels que Services Terminal Server, possèdent plusieurs services de rôle qui peuvent être installés, en fonction des besoins informatiques distants de votre entreprise.

Vous pouvez considérer un rôle en tant qu'un groupement de services de rôle étroitement associés et complémentaires pour lesquels, dans la majorité des cas, l'installation du rôle signifie celle d'un ou de plusieurs de ses services de rôle.

Fonctionnalités

Les fonctionnalités sont des programmes logiciels qui, bien qu'elles ne fassent pas directement partie des rôles, peuvent prendre en charge ou augmenter la fonctionnalité d'un ou de plusieurs rôles, ou encore améliorer la fonctionnalité de la totalité du serveur, quels que soient les rôles installés. Par exemple, la fonctionnalité Clustering avec basculement augmente la fonctionnalité des autres rôles, tels que Services de fichiers et Serveur DHCP, en leur permettant de rejoindre des clusters de serveurs, afin d'augmenter la redondance et d'améliorer les performances. Une autre fonctionnalité, Client Telnet, vous permet de communiquer à distance avec un serveur telnet via une connexion réseau, ce qui améliore les options de communication du serveur dans sa globalité.

Dépendances dans le Gestionnaire de serveur

Lorsque vous installez des rôles et préparez le déploiement de votre serveur, Gestionnaire de serveur vous demande d'installer tout autre rôle, service de rôle ou fonctionnalité requis par un rôle à installer. Par exemple, de nombreux rôles, tels que les Services UDDI, nécessitent l'exécution du Serveur Web (IIS).

De manière identique, pour supprimer des rôles, des services de rôle ou des fonctionnalités de votre ordinateur, des messages de Gestionnaire de serveur vous indiquent si d'autres programmes nécessitent le logiciel que vous êtes en train de supprimer. Si, par exemple, vous voulez supprimer le Serveur Web (IIS), Gestionnaire de serveur vous avertit s'il reste d'autres rôles qui dépendent du Serveur Web (IIS) sur l'ordinateur. Cet arrangement complexe de dépendances logicielles est gérée par Gestionnaire de serveur et empêche toute suppression accidentelle de logiciel dont le serveur a besoin pour effectuer les tâches qui lui sont affectées. Les utilisateurs n'ont pas besoin de savoir de quels logiciels dépendent les rôles qu'ils veulent installer.

2 Ajout de rôles et de fonctionnalités de serveur

Windows Server® 2008 facilite la gestion et la sécurisation de plusieurs rôles de serveur dans une entreprise avec la nouvelle console Gestionnaire de serveur. Gestionnaire de serveur dans Windows Server 2008 fournit une source unique de gestion de l'identité d'un serveur et des informations système, en affichant l'état du serveur, en identifiant les problèmes de configuration de rôle de serveur et en gérant tous les rôles installés sur le serveur.

Comment le Gestionnaire de serveur rationalise l'Administration serveur

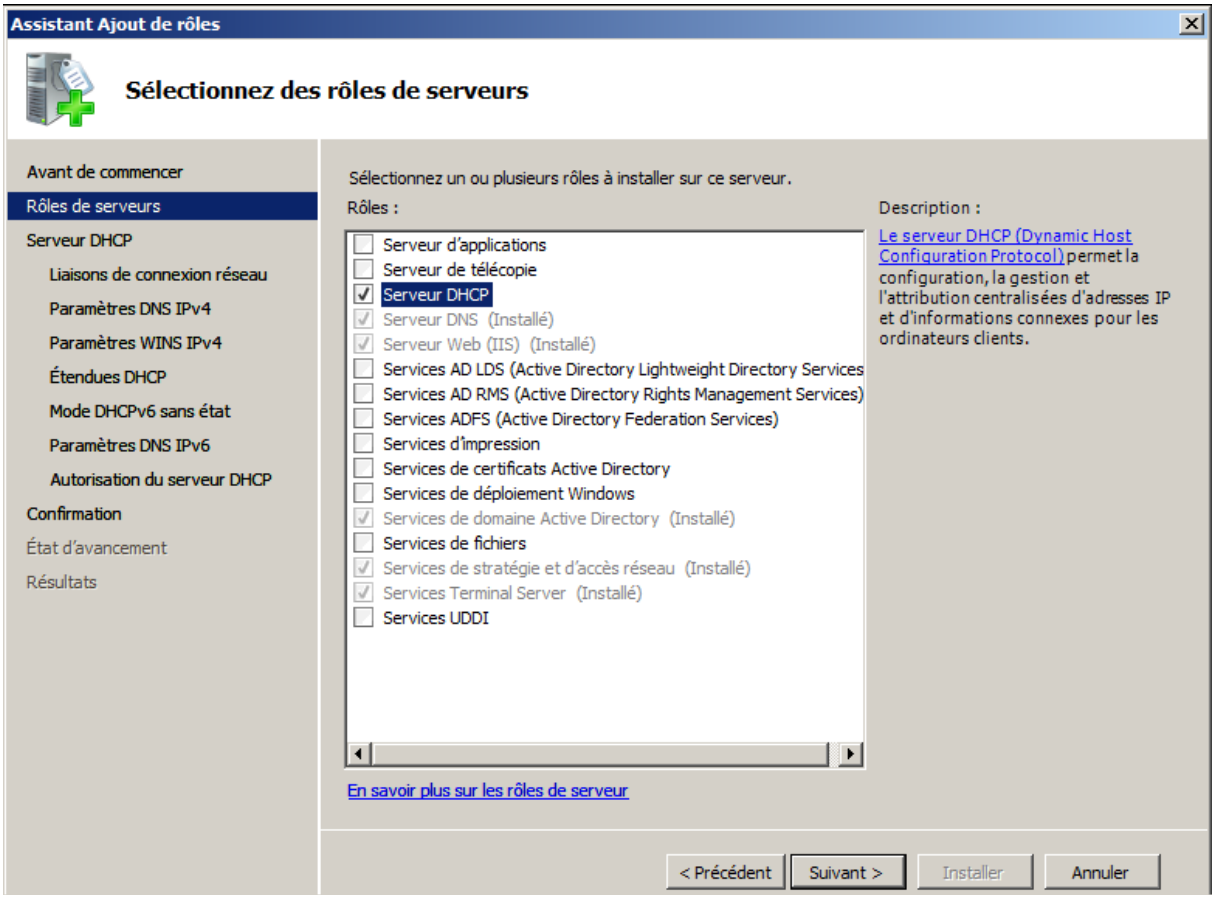
Gestionnaire de serveur permet une administration serveur plus efficace en autorisant les administrateurs à effectuer les tâches suivantes à l'aide d'un seul outil :

- Afficher et apporter des modifications aux rôles et fonctionnalités de serveur installés sur le serveur.
- Effectuer des tâches de gestion associées au cycle de vie opérationnel du serveur, tel que le démarrage ou l'arrêt de services et la gestion de comptes d'utilisateur local.
- Réaliser des tâches de gestion associées au cycle de vie opérationnel des rôles installés sur le serveur.
- Déterminer l'état d'un serveur, identifier des événements critiques, analyser et dépanner des problèmes ou des échecs de configuration.

Comment ajouter des rôles à votre serveur

Dans Windows Server 2008, vous pouvez ajouter des rôles à votre serveur à 'laide de l'Assistant Ajout de rôles. Vous pouvez démarrer l'Assistant Ajout de rôles depuis la fenêtre **Tâches de configuration initiales** ou depuis Gestionnaire de serveur.

Rôles disponibles pour l'installation dans cette version



Les rôles suivants sont disponibles pour l'installation en ouvrant l'Assistant Ajout de rôles, depuis la fenêtre **Tâches de configuration initiales** ou depuis Gestionnaire de serveur.

Nom de rôle	Description
services de certificats Active Directory®	Les services de certificats Active Directory® fournissent des services personnalisables pour la création et la gestion de certificats qui sont utilisés dans les systèmes de sécurité logiciels employant des technologies de clé publique. Les organisations peuvent utiliser des services de certificats Active Directory pour améliorer la sécurité en liant l'identité d'une personne, d'un périphérique ou d'un service à une clé privé correspondante. Les services de certificats Active Directory contiennent aussi des fonctions qui vous permettent de gérer l'inscription et la révocation de certificats dans une variété d'environnements évolutifs. Les applications prises en charge par les services de certificats Active Directory incluent les extensions S/MIME (Secure/Multipurpose Internet Mail Extensions), les réseaux sans fil sécurisés, les réseaux privés virtuels (VPN), la sécurité du protocole Internet (IPsec), le système de fichiers EFS, l'ouverture de session par carte à puce, SSL/TLS (Secure Socket Layer/Transport Layer Security) et les signatures numériques.
Services de domaine Active Directory	Services de domaine Active Directory (AD DS) stocke des informations sur les utilisateurs, les ordinateurs et d'autres périphériques sur le réseau. AD DS permet aux administrateurs de gérer en toute sécurité ces informations et facilitent le partage des ressources et la collaboration entre les utilisateurs. AD DS doit aussi être installé sur le réseau afin d'installer des applications compatibles avec l'annuaire, telles que Microsoft

	Exchange Server, et d'autres technologies Windows Server, telles que la stratégie de groupe.
Services ADFS (Active Directory Federation Services)	Les services ADFS (Active Directory Federation Services) fournissent des technologies d'ouverture de session Web unique (SSO) pour authentifier un utilisateur dans plusieurs applications Web, à l'aide d'un compte d'utilisateur unique. AD FS réalise cela grâce à la fédération ou au partage sécurisé des identités utilisateur et des droits d'accès sous la forme de demandes numériques entre les organisations partenaires.
Services AD LDS (Active Directory Lightweight Directory Services)	Les organisations dont les applications nécessitent un annuaire pour le stockage des données d'application peuvent utiliser les services AD LDS (Active Directory Lightweight Directory Services) comme magasin de données. Les services AD LDS ne sont pas exécutés en tant que service du système d'exploitation et, en tant que tel, ne demande pas à être déployé sur un contrôleur de domaine. Cela permet d'exécuter plusieurs instances AD LDS simultanément sur un même serveur. Chaque instance peut être configurée indépendamment pour gérer plusieurs applications.
Active Directory Rights Management Services (AD RMS)	Active Directory Rights Management Services (AD RMS) (AD RMS) est une technologie de protection des informations qui fonctionne avec des applications activées pour AD RMS et dont l'objectif est de protéger les informations numériques contre les utilisations non autorisées. Les propriétaires du contenu peuvent définir exactement comment un destinataire peut utiliser les informations, par exemple qui peut ouvrir, modifier, imprimer, transférer et/ou effectuer d'autres manipulations des informations. Les organisations peuvent créer des modèles de droits d'utilisation personnalisés, tels que « Confidentiel - Lecture seule », qui peuvent être appliqués directement à des informations telles que des rapports financiers, des spécifications de produit, des données clients et des messages électroniques.
Serveur d'application	Application Server permet la gestion centralisée et l'hébergement d'applications métier distribuées de haute performance. Les services intégrés, tels que .NET Framework, la prise en charge du serveur Web, Message Queuing, COM+, Windows Communication Foundation et le Clustering avec basculement augmentent la productivité à travers le cycle de vie de l'application, depuis la conception jusqu'au développement, via le déploiement et les opérations.
Serveur DHCP (Dynamic Host Configuration Protocol)	Le protocole DHCP (Dynamic Host Configuration Protocol) permet aux serveurs d'affecter (ou de louer) des adresses IP aux ordinateurs et autres périphériques reconnus comme clients DHCP. Le déploiement de serveurs DHCP sur le réseau fournit automatiquement aux ordinateurs et autres périphériques réseau TCP/IP des adresses IP valides, ainsi que les paramètres de configuration supplémentaires nécessaires, appelés options DHCP, qui leur permettent de se connecter à d'autres ressources réseau, telles que des serveurs DNS, des serveurs WINS et des routeurs.
Serveur DNS	Le système DNS (Domain Name System) fournit une méthode standard d'association de noms à des adresses Internet numériques. Cela permet aux utilisateurs de référencer les ordinateurs réseau en utilisant des noms faciles à retenir au lieu d'une longue série de chiffres. Les services DNS Windows peuvent être intégrés aux services DHCP (Dynamic Host Configuration Protocol) sous Windows. Il n'est ainsi plus nécessaire d'ajouter les enregistrements DNS car les ordinateurs sont ajoutés au

	réseau.
Serveur de télécopie	Serveur de télécopie envoie et reçoit des télécopies et vous permet de gérer les ressources de télécopie, tels que les tâches, les paramètres, les rapports et les périphériques de télécopie sur cet ordinateur ou sur le réseau.
Services de fichiers	Services de fichiers fournit les technologies pour la gestion du stockage, la réplication des fichiers, la gestion des espaces de noms distribuée, la recherche rapide de fichiers et l'accès client aux fichiers simplifié.
Services de stratégie et d'accès réseau	Les services de stratégie et d'accès réseau offrent plusieurs méthodes pour fournir aux utilisateurs une connectivité réseau locale et à distance, pour connecter des segments réseau et pour permettre aux administrateurs réseau de gérer de façon centralisée les accès au réseau et les stratégies de contrôle d'intégrité des clients. Avec les services de stratégie et d'accès réseau, vous pouvez déployer des serveurs VPN, des serveurs d'accès à distance, des routeurs et des accès sans fil protégés 802.11. Vous pouvez aussi déployer des serveurs et des proxys RADIUS, et utiliser le Kit d'administration de Connection Manager pour créer des profils d'accès à distance qui permettent aux ordinateurs clients de se connecter à votre réseau.
Services d'impression	Services d'impression permettent la gestion des serveurs d'impression et des imprimantes. Un serveur d'impression réduit la charge de travail d'administration et de gestion en centralisant les tâches de gestion des imprimantes.
Services Terminal Server	Services Terminal Server fournit des technologies qui permettent aux utilisateurs d'accéder aux programmes Windows installés sur un serveur Terminal Server ou d'accéder au Bureau même, à partir de pratiquement n'importe quel périphérique informatique. Les utilisateurs peuvent se connecter à un serveur Terminal Server pour exécuter des programmes et utiliser des ressources réseau sur ce serveur.
Services UDDI (Universal Description Discovery and Integration)	Les services UDDI fournissent des fonctionnalités destinées au partage d'informations relatives aux services Web sur l'intranet d'une organisation, entre des partenaires commerciaux sur un extranet ou sur Internet. Les services UDDI peuvent aider à améliorer la productivité de développeurs et de professionnels de l'informatique avec des applications plus fiables et faciles à gérer. Avec les services UDDI, vous pouvez supprimer tout effort de duplication en effectuant la promotion de la réutilisation du travail de développement existant.
Serveur Web (IIS)	Serveur Web (IIS) permet le partage d'informations sur Internet, un intranet ou un extranet. Il s'agit d'une plateforme Web unifiée qui intègre IIS 7.0, ASP.NET et Windows Communication Foundation. IIS 7.0 permet aussi de renforcer la sécurité, simplifier les diagnostics et déléguer l'administration
Services de déploiement Windows	Vous pouvez utiliser Windows Deployment Services pour installer et configurer des systèmes d'exploitation Microsoft® Windows à distance sur des ordinateurs avec une mémoire morte (ROM) de démarrage d'environnement d'exécution de prédémarrage (PXE). La surcharge d'administration est réduite via l'implémentation du composant logiciel enfichable de la console MMC (Microsoft Management Console) WdsMgmt, qui gère tous les aspects des services de déploiement Windows. Les services de déploiement Windows fournissent aussi aux

	utilisateurs finaux une expérience cohérente avec l'installation de Windows.
Hyper-V™	Hyper-V fournit les services que vous pouvez utiliser pour créer et gérer des machines virtuelles et leurs ressources. Chaque machine virtuelle est un système informatique virtualisé qui fonctionne dans un environnement d'exécution isolé. Cela vous permet d'exécuter plusieurs systèmes d'exploitation simultanément.

L'Assistant Ajout de rôles

L'Assistant Ajout de rôles simplifie le processus d'installation de rôles sur votre serveur et vous permet d'installer plusieurs rôles à la fois. Avec les versions antérieures du système d'exploitation Windows, les administrateurs devaient exécuter Ajouter ou supprimer des composants Windows à plusieurs reprises pour installer tous les rôles, les services de rôle et les fonctionnalités requis sur un serveur. Gestionnaire de serveur remplace Ajouter ou supprimer des composants Windows et une seule session de l'Assistant Ajout de rôles peut effectuer la configuration de votre serveur.

L'Assistant Ajout de rôles vérifie que tous les composants logiciels requis par un rôle s'installent pour n'importe quel rôle sélectionné dans l'Assistant. Le cas échéant, l'Assistant vous demande d'approuver l'installation d'autres rôles, services de rôle ou composants logiciels requis par les rôles que vous sélectionnez.

La plupart des rôles et services de rôle disponibles pour l'installation exigent que vous preniez des décisions lors du processus d'installation qui déterminent le fonctionnement du rôle dans votre entreprise. Les exemples incluent les services ADFS (Active Directory Federation Services), qui nécessitent l'installation d'un certificat ; ou DNS (Domain Name System) qui vous oblige à fournir un nom de domaine pleinement qualifié (FQDN).

Pour démarrer l'Assistant Ajout de rôles

- Dans la zone **Résumé des rôles** de la fenêtre principale Gestionnaire de serveur, cliquez sur **Ajouter des rôles**.

  -- ou --

  Dans la zone **Personnaliser ce serveur** de la fenêtre **Tâches de configuration initiales**, cliquez sur **Ajouter des rôles**.

  Remarque

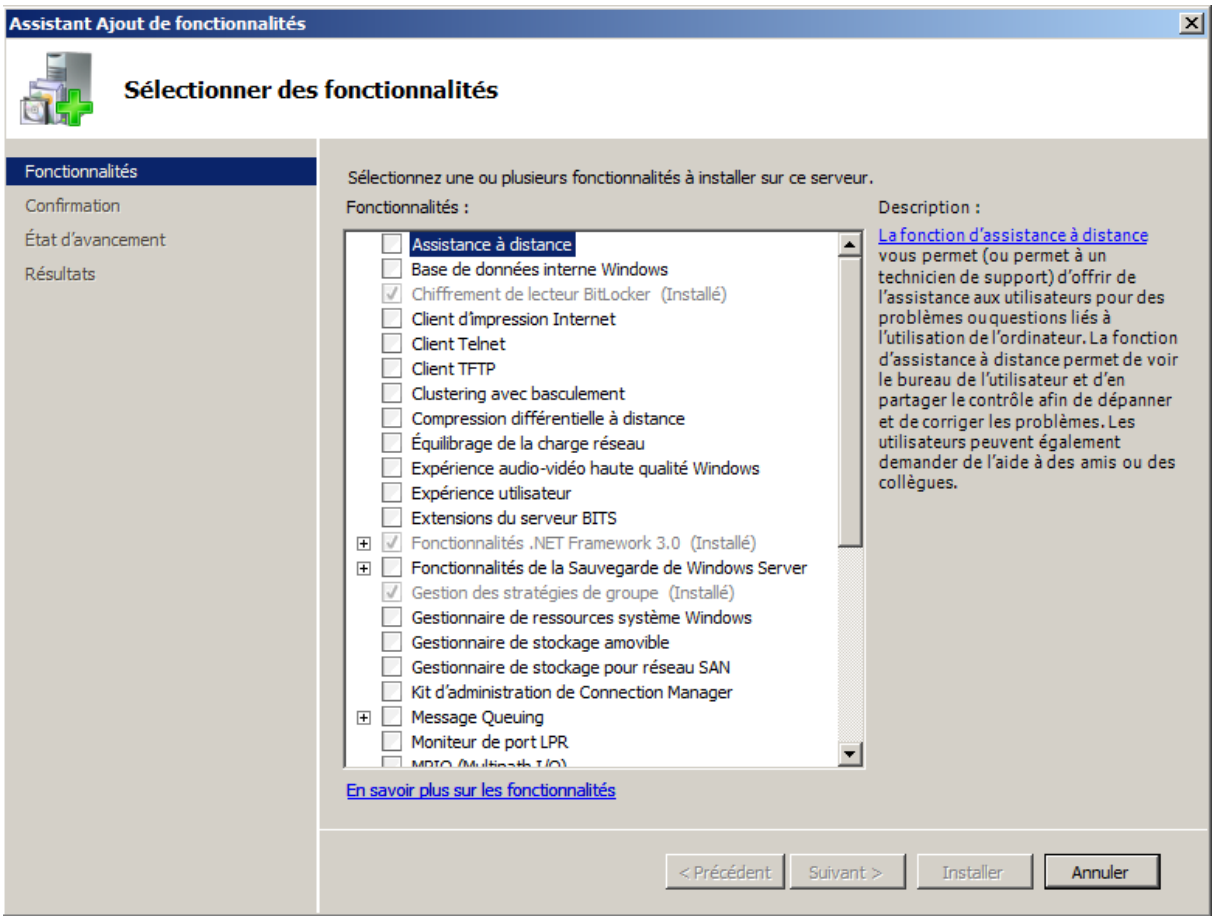
  - La fenêtre **Tâches de configuration initiales** s'ouvre par défaut lorsqu'un membre du groupe Administrateurs ouvre une session sur l'ordinateur.
  - Gestionnaire de serveur s'ouvre lors de la fermeture de la fenêtre **Tâches de configuration initiales**. Vous pouvez également ouvrir Gestionnaire de serveur à l'aide de raccourcis dans le menu **Démarrer** ou dans les Outils d'administration.

Comment ajouter des fonctionnalités à votre serveur

Dans Windows Server 2008, vous pouvez ajouter des fonctionnalités disponibles à votre serveur à l'aide de l'Assistant Ajout de fonctionnalités.

Ajout de fonctionnalités à votre serveur à l'aide de l'Assistant Ajout de fonctionnalités

Vous pouvez ajouter les fonctionnalités suivantes à l'aide de l'Assistant Ajout de fonctionnalités.



Fonctionnalité	Description
.NET Framework 3,0	Microsoft .NET Framework 3.0 combine la puissance des API du .NET Framework 2.0 aux nouvelles technologies pour construire des applications offrant des interfaces utilisateur efficaces, protéger les informations d'identité personnelle de vos clients, permettre une communication transparente et sécurisée et fournir la possibilité de modéliser une large gamme de processus d'entreprise.
Chiffrement de lecteur BitLocker	Le Chiffrement de lecteur BitLocker aide à protéger les données sur des ordinateurs égarés, dérobés ou retirés de manière inappropriée en chiffrant la totalité du volume et en vérifiant l'intégrité des composants de la séquence de démarrage. Les données sont déchiffrées uniquement si ces composants ont été vérifiés avec succès et si le lecteur chiffré se trouve dans l'ordinateur d'origine. La vérification de l'intégrité nécessite un module de plateforme sécurisée (TPM) compatible.
Extensions du serveur BITS	Les extensions serveur du service de transfert intelligent en arrière-plan (BITS) permettent à un serveur de recevoir des fichiers chargés par des clients à l'aide de BITS. BITS permet à des ordinateurs clients de transférer des fichiers au premier plan ou en arrière-plan de manière asynchrone, de préserver la réactivité d'autres applications réseau et de reprendre des transferts de fichier après des pannes de réseau et des redémarrages d'ordinateur.
Kit d'administration de Connection Manager	Kit d'administration de Connection Manager (CMAK) génère des profils Connection Manager.
Expérience utilisateur	L'expérience utilisateur inclut des fonctionnalités de Windows Vista®, telles que le Lecteur Windows Media, des thèmes du bureau et une galerie de

	photos. L'expérience utilisateur n'active aucune des fonctionnalités de Windows Vista par défaut ; vous devez les activer manuellement.
Gestion des stratégies de groupe	La gestion des stratégies de groupe facilite la compréhension, le déploiement, la gestion et le dépannage d'implémentations d'une stratégie de groupe. L'outil standard est la console de gestion des stratégies de groupe (GPMC, Group Policy Management Console), un composant logiciel enfichable MMC (Microsoft Management Console) scriptable, qui permet de gérer la stratégie de groupe sur l'ensemble de l'entreprise de façon centralisée.
Client d'impression Internet	Le client d'impression Internet vous permet d'utiliser HTTP pour se connecter à des imprimantes qui se trouvent sur des serveurs d'impression Web et les utiliser. L'impression Internet autorise des connexions entre utilisateurs et imprimantes qui ne se trouvent pas sur le même domaine ou réseau. Parmi les exemples d'utilisation, citons celui d'un employé en déplacement dans une succursale ou dans un bar équipé d'un accès Wi-Fi.
Serveur iSNS (Internet Storage Name Server)	Le serveur iSNS fournit des services de découverte pour les réseaux de zone de stockage iSCSI (Internet Small Computer System Interface). Le serveur iSNS traite des demandes d'inscription, d'annulation d'enregistrement et de clients iSNS.
Moniteur de port LPR	Le moniteur de port LPR (Line Printer Remote) permet aux utilisateurs disposant d'un accès à des ordinateurs UNIX d'imprimer sur des périphériques reliés à ceux-ci.
Message Queuing	Message Queuing fournit une livraison des messages garantie, un routage efficace, une sécurité et une messagerie basée sur la priorité entre les applications. Message Queuing permet aussi la livraison de messages entre des applications qui s'exécutent sur différents systèmes d'exploitation, utilisent des infrastructures réseau distinctes, sont temporairement hors connexion ou s'exécutent à des heures différentes.
MPIO (Multipath I/O)	MPIO (Multipath I/O), associé au DSM (Microsoft Device Specific Module) ou à un DSM tiers, fournit une prise en charge pour l'utilisation de plusieurs chemins d'accès aux données à un périphérique de stockage sous Microsoft Windows.
Protocole PNRP (Peer Name Resolution Protocol)	Le protocole PNRP (Peer Name Resolution Protocol) permet aux applications de s'inscrire et de résoudre des noms à partir de votre ordinateur, afin que d'autres ordinateurs puissent communiquer avec ces applications.
Expérience audio-vidéo haute qualité Windows (qWave)	L'expérience audio-vidéo haute qualité Windows (qWave) est une plateforme réseau destinée aux applications de flux AV (audio vidéo) sur des réseaux domestiques IP. qWave améliore les performances et la fiabilité des flux AV en assurant la qualité de service (QoS) sur le réseau des applications AV. Cette plateforme fournit des mécanismes concernant le contrôle d'admission, l'analyse et la mise en œuvre des principes de protection des informations personnelles à l'exécution, la rétroaction des applications et la définition des priorités du trafic. Sur des plateformes Windows Server, qWave fournit uniquement des services de taux de flux et de définition de priorités.
Assistance à distance	L'assistance à distance (ou une personne chargée du support) vous permet de fournir une assistance aux utilisateurs qui ont des problèmes ou des questions concernant leur ordinateur. Elle vous permet d'afficher et de partager le contrôle du Bureau de l'utilisateur afin de dépanner et de

	résoudre les problèmes. Les utilisateurs peuvent aussi demander de l'aide auprès d'amis ou de collègues.
Compression différentielle à distance	La fonctionnalité de compression différentielle à distance est un ensemble d'interfaces de programmation d'application que les applications peuvent utiliser pour déterminer si un ensemble de fichiers a changé et, si c'est le cas, pour détecter les parties des fichiers qui contiennent des modifications.
Outils d'administration de serveur distant	Outils d'administration de serveur distant permet une gestion à distance de Windows Server 2003 et de Windows Server 2008 à partir d'un ordinateur exécutant Windows Server 2008, en vous permettant d'exécuter certains des outils de gestion pour rôles, services de rôle et fonctionnalités sur un ordinateur distant.
Gestionnaire de stockage amovible	Le Gestionnaire de stockage amovible (RSM) gère et catalogue les médias amovibles et fait fonctionner les médias amovibles automatisés.
Proxy RPC sur HTTP	Le Proxy RPC sur HTTP est un proxy utilisé par des objets qui reçoit des appels de procédure distant (RPC) via HTTP (Hypertext Transfer Protocol). Ce proxy permet aux clients de découvrir ces objets même s'ils sont déplacés entre des serveurs ou s'ils existent à des emplacements spécifiques du réseau, généralement pour des raisons de sécurité.
Services pour NFS	Services pour NFS (Network File System) est un protocole qui agit comme un système de fichiers DFS, permettant à un ordinateur d'accéder à des fichiers à travers un réseau aussi aisément que s'ils se trouvaient sur ses disques locaux. Cette fonctionnalité est disponible pour l'installation dans Windows Server 2008 pour les systèmes Itanium uniquement ; dans les autres versions de Windows Server 2008, Services pour NFS est disponible sous forme d'un service de rôle du rôle Services de fichiers.
Serveur SMTP	Un serveur SMTP prend en charge le transfert des messages électroniques entre les systèmes de messagerie.
Gestionnaire de stockage SAN	Le gestionnaire de stockage SAN (Storage Area Networks) vous aide à créer et à gérer les numéros d'unités logiques dans des sous-systèmes de disque Fibre Channel et iSCSI prenant en charge le service de disque virtuel (VDS) dans votre réseau de stockage SAN.
Services TCP/IP simples	Les services TCP/IP simples prennent en charge les services TCP/IP suivants : Générateur de caractères, Heure du jour, Ignorer, Écho et Citation du jour. Les services TCP/IP simples sont fournis pour une compatibilité descendante et ne doivent pas être installés sauf s'ils sont requis.
Services SNMP	Les services SNMP (Simple Network Management Protocol) représentent le protocole standard Internet pour l'échange d'informations de gestion entre applications de console de gestion, telles que HP Openview, Novell NMS, IBM NetView ou Sun Net Manager et entités gérées. Les entités gérées peuvent inclure des hôtes, des routeurs, des passerelles et des concentrateurs.
Sous-système pour les applications UNIX	Les sous-systèmes pour les applications UNIX, associés à un package d'utilitaires de support disponible sous forme de téléchargement sur le site Web de Microsoft, vous permettent d'exécuter, de compiler et d'exécuter des applications UNIX personnalisées dans l'environnement Windows.
Client Telnet	Le client Telnet utilise le protocole Telnet pour se connecter à un serveur Telnet distant et exécuter des applications sur ce serveur.
Serveur Telnet	Le serveur Telnet permet aux utilisateurs distants, y compris à ceux qui exécutent des systèmes d'exploitation UNIX, d'effectuer des tâches

	d'administration de ligne de commande et d'exécuter des programmes à l'aide d'un client Telnet.
Client TFTP (Trivial File Transfer Protocol)	Le client TFTP (Trivial File Transfer Protocol) sert à lire des fichiers depuis un serveur TFTP ou à écrire des fichiers sur celui-ci. TFTP est principalement utilisé par des périphériques ou des systèmes incorporés, qui récupèrent des informations de configuration de microprogramme, ou par une image de système au cours du processus de démarrage à partir d'un serveur TFTP.
Clustering avec basculement	La fonction Clustering avec basculement permet à plusieurs serveurs de collaborer pour fournir une haute disponibilité de services et d'applications. Cette fonction est souvent utilisée pour des services de fichiers et d'impression, ainsi que pour des applications de base de données et de messagerie.
Équilibrage de la charge réseau	L'équilibrage de la charge réseau répartit le trafic sur plusieurs serveurs, à l'aide du protocole réseau TCP/IP. Il se révèle particulièrement utile pour garantir que les applications sans état, telles qu'un serveur Web complet exécutant les services Internet (IIS), sont évolutives en ajoutant des serveurs supplémentaires lors d'une augmentation de la charge.
Sauvegarde de Windows Server	La Sauvegarde de Windows Server vous permet de sauvegarder et de récupérer votre système d'exploitation, des applications et des données. Vous pouvez planifier des sauvegardes quotidiennes ou plus fréquentes et protéger la totalité du serveur ou des volumes spécifiques.
Gestionnaire de ressources système Windows	Le Gestionnaire de ressources système Windows est un outil d'administration du système d'exploitation Windows Server, qui peut gérer l'allocation des ressources d'unité centrale et de mémoire. La gestion d'allocation de ressources améliore les performances du système et réduit les risques d'interférence entre applications, services ou processus susceptibles de porter atteinte à l'efficacité du serveur et au temps de réponse du système.
Serveur WINS (Windows Internet Name Service)	Le serveur WINS (Windows Internet Name Service) fournit une base de données distribuée pour l'inscription et l'interrogation de mappages dynamiques de noms NetBIOS pour les ordinateurs et les groupes utilisés sur votre réseau. Le service WINS mappe des noms NetBIOS à des adresses IP et résout les problèmes liés à la résolution de noms NetBIOS dans des environnements routés.
Service de réseau local sans fil	Le service de réseau local sans fil configure et démarre le service de configuration automatique WLAN, que l'ordinateur dispose d'adaptateurs sans fil ou pas. Le service de configuration automatique WLAN énumère les adaptateurs sans fil et gère les connexions sans fil, ainsi que les profils sans fil contenant les paramètres requis pour configurer un client sans fil en vue d'une connexion à un réseau sans fil.
Base de données interne Windows	La base de données interne Windows est un magasin de données relationnelles utilisable uniquement par des rôles et des fonctionnalités Windows, tels que les services UDDI, Active Directory Rights Management Services (AD RMS), Windows Server Update Services et le Gestionnaire de ressources système Windows.
Windows PowerShell	Windows PowerShell est un interpréteur de ligne de commande et un langage de script qui améliore la productivité des professionnels de l'informatique. Il fournit un nouveau langage de script orienté administration et plus de 130 outils en ligne de commande standard permettant une

	administration système simplifiée et une automatisation accélérée.
Service d'activation des processus Windows	Le service d'activation des processus Windows généralise le modèle de processus IIS, en éliminant la dépendance sur HTTP. Toutes les fonctionnalités d'IIS qui étaient précédemment disponibles uniquement pour les applications HTTP sont maintenant disponibles pour les applications hébergeant des services WCF (Windows Communication Foundation), utilisant des protocoles non-HTTP. IIS 7.0 utilise également le service d'activation des processus Windows pour l'activation basée sur des messages sur HTTP.

Ouvrez l'Assistant Ajout de fonctionnalités de l'une des manières suivantes :

Pour démarrer l'Assistant Ajout de fonctionnalités

- Dans la zone **Résumé des fonctionnalités** de la fenêtre principale Gestionnaire de serveur, cliquez sur **Ajouter des fonctionnalités**.

  -- ou --

  Dans la zone **Personnaliser ce serveur** de la fenêtre **Tâches de configuration initiales**, cliquez sur **Ajouter des fonctionnalités**.

  Remarque

  - La fenêtre **Tâches de configuration initiales** s'ouvre par défaut lorsqu'un membre du groupe Administrateurs ouvre une session sur l'ordinateur.
  - Gestionnaire de serveur s'ouvre lors de la fermeture de la fenêtre **Tâches de configuration initiales**. Vous pouvez également ouvrir Gestionnaire de serveur à l'aide de raccourcis dans le menu **Démarrer** ou dans les Outils d'administration.

Suppression de rôles et de fonctionnalités de serveur

Les outils contenus dans Windows Server® 2008 vous permettent de supprimer aisément des rôles et des fonctionnalités de serveur. Vous pouvez supprimer des rôles à l'aide de l'Assistant Suppression de rôle et supprimer des fonctionnalités via l'Assistant Suppression de fonctionnalités.

Comment supprimer des rôles de votre serveur

Dans Windows Server 2008, vous pouvez supprimer des rôles de votre serveur à l'aide de l'Assistant Suppression de rôle. Vous pouvez démarrer l'Assistant Suppression de rôle depuis la fenêtre **Tâches de configuration initiales** ou depuis Gestionnaire de serveur.

Assistant Suppression de rôle

L'Assistant Suppression de rôle simplifie le processus de suppression de rôles depuis votre serveur et vous permet de supprimer plusieurs rôles à la fois. Vous n'avez plus besoin d'ouvrir **Ajouter ou supprimer des composants Windows** à plusieurs reprises pour supprimer plus d'un rôle, un service de rôle ou une fonctionnalité installé sur votre serveur. Une session unique dans l'Assistant Suppression de rôle permet d'effectuer la configuration de votre serveur.

Avant de supprimer un rôle, l'Assistant Suppression de rôle vérifie qu'aucun composant logiciel requis par l'un des rôles restants n'a été supprimé accidentellement. Le cas échéant, l'Assistant vous demande d'approuver la suppression d'autres rôles, services de rôle ou composants logiciels requis par

les rôles qui demeurent installés. Le risque de suppression de logiciels dont dépendent d'autres rôles est pratiquement supprimé.

Pour démarrer l'Assistant Suppression de rôle

- Dans la zone **Résumé des rôles** de la fenêtre principale Gestionnaire de serveur, cliquez sur **Supprimer des rôles**.

Remarque

- Gestionnaire de serveur s'ouvre pas défaut lorsqu'un membre du groupe Administrateurs ouvre une session sur l'ordinateur.
- Gestionnaire de serveur s'ouvre également lors de la fermeture de la fenêtre **Tâches de configuration initiales**. Vous pouvez également ouvrir Gestionnaire de serveur à l'aide de raccourcis dans le menu **Démarrer** ou dans les Outils d'administration.

3 Comment supprimer des fonctionnalités de votre serveur

Dans Windows Server 2008, vous pouvez supprimer des fonctionnalités installées sur votre serveur à l'aide de l'Assistant Suppression de fonctionnalités.

Suppression de fonctionnalités de votre serveur à l'aide de l'Assistant Suppression de fonctionnalités

Vous pouvez supprimer des fonctionnalités à l'aide de l'Assistant Suppression de fonctionnalités.

Pour démarrer l'Assistant Suppression de fonctionnalités

- Dans la zone **Résumé des fonctionnalités** de la fenêtre principale Gestionnaire de serveur, cliquez sur **Supprimer des fonctionnalités**.

Remarque

- Gestionnaire de serveur s'ouvre pas défaut lorsqu'un membre du groupe Administrateurs ouvre une session sur l'ordinateur.
- Gestionnaire de serveur s'ouvre également par défaut lors de la fermeture de la fenêtre **Tâches de configuration initiales**. Vous pouvez également ouvrir Gestionnaire de serveur à l'aide de raccourcis dans le menu **Démarrer** ou dans les Outils d'administration.

4 Fenêtre principale du Gestionnaire de serveur

La fenêtre principale Gestionnaire de serveur vous permet d'afficher un instantané détaillé des informations d'identité de votre serveur, des options de configuration de sécurité sélectionnées, ainsi que des rôles et fonctionnalités installés.

La zone Ressources et support de la fenêtre principale Gestionnaire de serveur contient des liens qui vous aident à rester connecté aux dernières documentations et téléchargements. Elle vous permet aussi de participer à des programmes de commentaires qui aident à améliorer les versions ultérieures de Windows Server® 2008.

Zone Résumé serveur

La zone Résumé serveur affiche des détails sur votre serveur qui se révèlent particulièrement utiles lors du dépannage, tels que le nom d'ordinateur et les adresses réseau, ainsi que l'ID de produit du système d'exploitation exécuté sur l'ordinateur.

À partir de la zone Résumé serveur, vous pouvez afficher et modifier des connexions réseau, modifier des propriétés du système et activer et configurer le Bureau à distance.

La zone Résumé serveur contient les sous-sections réductibles suivantes :

Informations sur l'ordinateur

Le tableau suivant décrit les informations qui apparaissent dans la section **Informations sur l'ordinateur**.

Texte du champ	Description des données
Nom complet de l'ordinateur :	Nom de domaine pleinement qualifié (FQDN) du serveur cible.
Domaine (ou groupe de travail si l'ordinateur n'est pas joint au domaine.	Suffixe DNS principal
<nom de connexion réseau 1>:	Adresse IP :
<nom de connexion réseau 2>:	Adresse IP :
<nom de connexion réseau 3>:	Adresse IP :
État d'activation de produit Windows :	Nombre de jours restant pour activer le système d'exploitation Windows du serveur
ID de produit (si active) :	ID de produit (pas la clé produit Windows)

Informations sur la sécurité

Le tableau suivant décrit les informations qui apparaissent dans la section Informations sur la sécurité.

Texte du champ	Description des données
État du Pare-feu Windows	Indique si le Pare-feu Windows est activé sur le serveur.
État de Windows Update	Affiche si le serveur est configuré pour télécharger et installer des mises à jour logicielles Windows automatiquement
Dernière recherche de mises à jour	Affiche le jour et l'heure de la dernière vérification par le serveur de la présence de mises à jour logicielles.
Dernières mises à jour installées	Affiche le jour et l'heure de la dernière vérification par le serveur de la présence de mises à jour logicielles.
Configuration de sécurité renforcée d'Internet Explorer	Indique si la configuration de sécurité avancée d'Internet Explorer est activée pour les membres du groupe Administrateurs et les autres utilisateurs.

À partir de la zone Informations sur la sécurité, vous pouvez aussi démarrer l'Assistant Configuration de la sécurité, qui vous aide à créer une stratégie de sécurité pouvant être appliquée à n'importe quel serveur sur votre réseau.

Zone Résumé des rôles

La zone Résumé des rôles de la fenêtre principale Gestionnaire de serveur affiche une liste de tous les rôles installés sur l'ordinateur. Les noms des rôles installés sur l'ordinateur s'affiche au format hypertexte ; lorsque vous cliquez sur un nom de rôle, la page d'accueil Gestionnaire de serveur pour gérer ce rôle s'ouvre.

Pour installer des rôles supplémentaires ou supprimer des rôles existants, cliquez sur la commande appropriée dans la marge de droite de la zone Résumé des rôles.

La commande **Accéder à la page Gérer les rôles** de cette section ouvre la page d'accueil Rôles, à partir de laquelle vous pouvez trouver plus de détails sur les rôles installés, et connaître, par exemple les services de rôles qui sont installés pour le rôle, l'état opérationnel du rôle et savoir si des messages d'événements sont disponibles à la lecture pour le rôle.

Zone Résumé des fonctionnalités

La zone Résumé des fonctionnalités de l'en-tête de la page d'accueil Gestionnaire de serveur affiche une liste de toutes les fonctionnalités installées sur l'ordinateur.

Pour installer des fonctionnalités supplémentaires ou supprimer des fonctionnalités existantes, cliquez sur la commande appropriée dans la marge de droite de la zone Résumé des fonctionnalités.

Windows PowerShell

Windows PowerShell est un nouveau langage de script et un nouvel interpréteur de ligne de commande à base de tâches, conçu pour l'administration système. Créé à partir du .NET Framework, Windows PowerShell aide les professionnels de l'informatique et les utilisateurs chevronnés à contrôler et automatiser l'administration du système d'exploitation Windows, ainsi que des applications s'exécutant dans Windows.

Les commandes Windows PowerShell intégrées, appelées cmdlets, vous permettent de gérer les ordinateurs de votre entreprise à partir de la ligne de commande. Les fournisseurs Windows PowerShell vous permettent d'accéder à des magasins de données, par exemple le Registre et le magasin de certificats, aussi facilement que si vous accédiez au système de fichiers. En outre, Windows PowerShell dispose d'un puissant analyseur d'expressions et d'un langage de script très complet.

Windows PowerShell 1.0 comprend les fonctionnalités suivantes :

- 129 cmdlets standard pour l'exécution de tâches d'administration système usuelles, par exemple la gestion du Registre, des services, des processus et des journaux d'événements, ainsi que l'utilisation de l'infrastructure WMI (Windows Management Instrumentation).
- Langage de script à base de tâches prenant en charge les scripts et outils de ligne de commande existants.
- Conception cohérente. Dans la mesure où les magasins de données système et les cmdlets Windows PowerShell utilisent une syntaxe et des conventions de dénomination communes, les données peuvent être partagées facilement ; en outre, la sortie d'une cmdlet peut servir d'entrée pour une autre cmdlet sans nouvelle mise en forme ou manipulation.
- Navigation simplifiée au sein du système d'exploitation à l'aide de commandes, ce qui permet aux utilisateurs de naviguer dans le Registre et autres magasins de données de la même façon que dans le système de fichiers.
- Puissantes fonctionnalités de manipulation d'objets. Les objets peuvent être manipulés directement ou envoyés vers d'autres outils ou bases de données.
- Interface extensible. Les éditeurs de logiciels indépendants et les développeurs professionnels peuvent créer des outils et utilitaires personnalisés afin d'administrer leurs logiciels.

Utilisation de Windows PowerShell

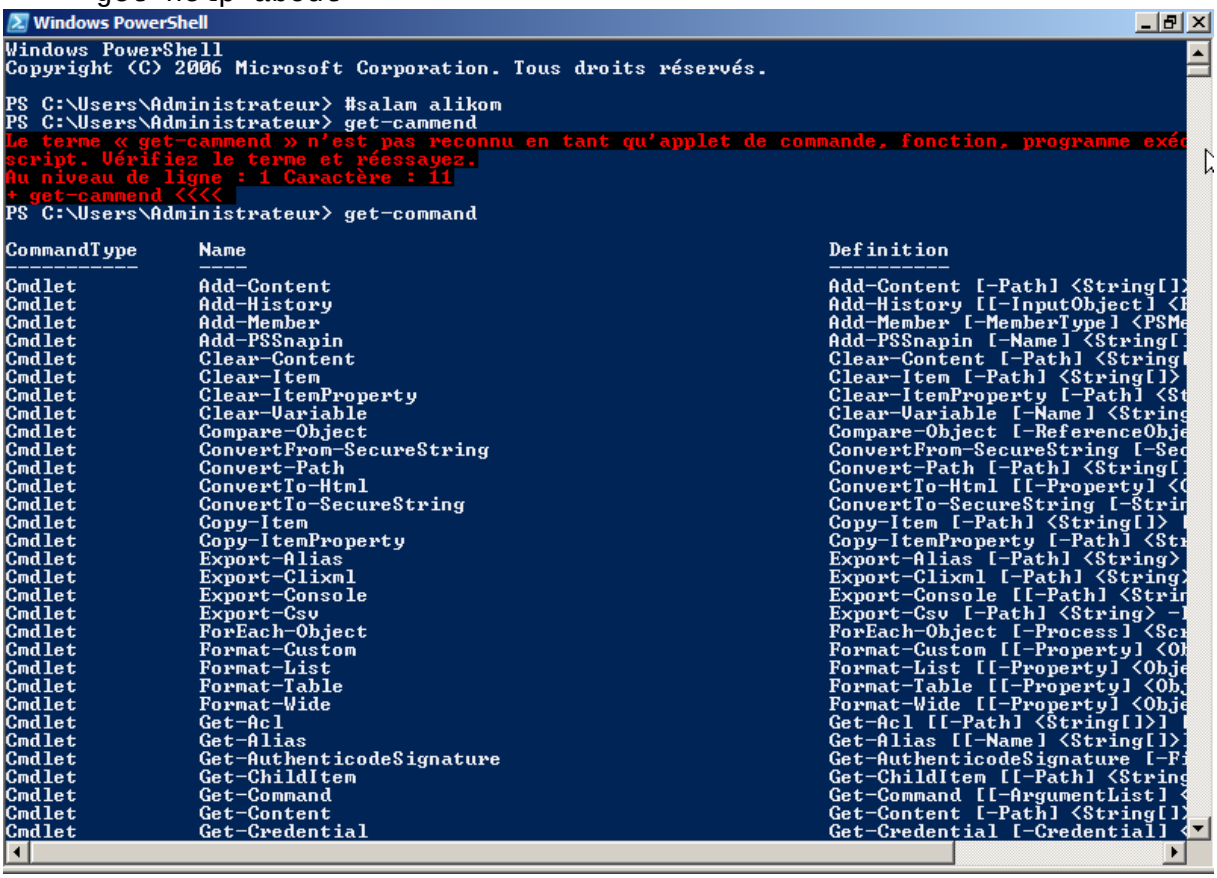
Pour apprendre à utiliser Windows PowerShell, commencez par consulter les ressources suivantes, qui sont incluses dans l'outil :

- Mise en route (éventuellement en anglais). Brève introduction et didacticiel. Pour l'ouvrir, cliquez sur Démarrer, sur Tous les programmes, sur Windows PowerShell 1.0, puis sur Mise en route.
- Guide de l'utilisateur (éventuellement en anglais). Introduction détaillée comprenant des scripts et des scénarios concrets pour vous aider à débuter.
- Cmdlet Get-Help. Cmdlet Windows PowerShell qui vous permet d'obtenir rapidement des informations sur les cmdlets et les fournisseurs de votre système. Pour commencer, démarrez Windows PowerShell, puis tapez la ligne ci-après à l'invite de commandes :

  ```
  get-help
  ```

  Pour en savoir plus sur le langage de script Windows PowerShell et d'autres concepts, lisez les rubriques « about ». Pour afficher une liste de rubriques « about », tapez :

  ```
  get-help about
  ```



Server Core

Server Core est une nouvelle option d'installation du système d'exploitation Microsoft Windows Server 2008. Elle permet d'installer un environnement minimal pour exécuter des rôles de serveurs spécifiques. Cette option permet de diminuer le taux de mises à jour et les interruptions éventuelles liées à la maintenance. En outre, Elle réduit la surface d'exposition aux risques informatiques. Une installation en mode Core prend en charge les rôles suivants :

KEY: ◯ = Non disponible ◍ = Fonction partielle/limitée ✔ = Fonction complète

Rôle de serveur	Enterprise	Datacenter	Standard	Web	Itanium
Services Web (IIS)	✔	✔	✔	✔	
Services d'impression	✔	✔	✔	◯	
Hyper-V [1]	✔	✔	✔	◯	
Services de domaine Active Directory	✔	✔	✔	◯	
Active Directory Lightweight Directory Services	✔	✔	✔	◯	
Serveur DHCP	✔	✔	✔	◯	
Serveur DNS	✔	✔	✔	◯	
Services de fichiers	✔	✔	◍ [2]	◯	

CONCLUSION

WINDOWS SERVER 2008 A PLUSIEURS AVANTAGES :

Offrez-vous une sécurité optimale. Windows Server 2008 propose de nouvelles technologies comme l'audit optimisé, le chiffrement de lecteur, le transfert d'événements et les services RMS (Rights Management Services) pour empêcher les connexions non autorisées à vos serveurs, réseau, données et comptes utilisateur.

- **Simplifiez-vous l'installation et la gestion.** Le tout nouveau Gestionnaire de serveur de Windows Server 2008 fournit une console de gestion unifiée qui facilite l'installation, la configuration et la gestion au quotidien des serveurs.
- **Optimisez votre infrastructure.** La fonction de virtualisation intégrée vous permet d'utiliser plusieurs systèmes d'exploitation sur un même serveur, ce qui améliore l'utilisation de votre matériel et la disponibilité du serveur pour les opérations de consolidation des serveurs de production, de récupération d'urgence, de test et de développement.
- **Contrôlez les accès à votre réseau.** La protection d'accès réseau (NAP) de Windows Server 2008 vous permet de vérifier que les ordinateurs qui tentent d'accéder à votre réseau sont conformes aux stratégies de sécurité que vous avez définies.
- **Dopez les performances de votre réseau.** Windows Server 2008 propose des technologies comme le réglage automatique de la fenêtre de réception, la mise à l'échelle côté réception et la qualité de service (QOS) qui permettent à l'entreprise de tirer pleinement parti des réseaux de plusieurs gigabits qui sont utilisés
- **Identifiez et résolvez efficacement les problèmes.** De puissants outils de diagnostic vous donnent une visibilité en temps réel sur votre environnement de serveurs, qu'ils soient physiques ou virtuels.
- **Offrez une expérience utilisateur complète sur le Web.** Les outils de développement et outils applicatifs de Windows Server 2008 créent une plate-forme sécurisée et facile à gérer pour développer et héberger de manière fiable des applications et services fournis par le biais des serveurs ou via le Web.
- **Automatisez les tâches courantes.** De nouvelles technologies comme Windows PowerShell, un interpréteur de ligne de commande et un langage de script, permettent aux services Informatique de contrôler plus facilement l'administration des systèmes et d'accélérer l'automatisation.
- **Simplifiez l'administration des serveurs dans les agences.** Les améliorations apportées à Active Directory et les technologies de chiffrement comme BitLocker renforcent la sécurité et répondent aux besoins spécifiques des agences.