Dell Wyse Device Manager 5.7.3

Guide d'installation

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

2018–04

Rév. A00

Table des matières

1

Introduction

Dell Wyse Device Manager (WDM) est un logiciel qui gère tous les clients légers et clients zéro de Dell Wyse. WDM permet aux administrateurs informatique d'utiliser les fonctions suivantes :

- Imagerie, mise à jour et configuration des appareils en client léger et client zéro par logiciels
- Suivi des éléments des périphériques
- Surveillance de l'intégrité des périphériques
- Gestion des politiques et paramètres réseau des périphériques
- Administration et duplication miroir à distance des périphériques

WDM utilise des protocoles de communication standard du secteur et une architecture orientée composant pour gérer efficacement les périphériques présents sur votre réseau. Ce guide fournit des informations sur les conditions requises pour installer WDM, ainsi que les étapes à suivre pour installer et configurer WDM dans votre environnement.

Sujets :

Tableau du programme d'installation

Le tableau suivant décrit les différentes combinaisons possibles de Microsoft SQL Server et de Microsoft Windows Server prises en charge par le programme d'installation.

Tableau 1. Matrice du programme d'installation

			Windows Server 2008 R2 SP1			
Authentification RapportDB		**SQL**			**Windows**	
	Enterprise	**Workgroup**	**Distribuée**	**Enterprise**	**Workgroup**	**Distribuée**
Windows 2008 R 2 SP1 + SQL Server 200 8 R2	Oui	Oui	Oui	Oui	Oui	Oui
Windows 2008 R 2 SP1 + SQL Server 200 8	Oui	Oui	Oui	Oui	Oui	Oui
Windows 2008 R 2 SP1 + SQL Server 2012	Oui	Oui	Oui	Oui	Oui	Oui

			Windows Server 2012			
Windows 2012 + SQL Express 2016 SP1	Oui	Oui	Oui	Oui	Oui	Oui
Windows 2012 + SQL Server 2008 R2	Oui	Oui	Oui	Oui	Oui	Oui
Windows 2012 + SQL Server 2008	Oui	Oui	Oui	Oui	Oui	Oui
Windows 2012 + SQL Server 2012	Oui	Oui	Oui	Oui	Oui	Oui
Windows 2012 + SQL Server 2014	Oui	Oui	Oui	Oui	Oui	Oui
Windows 2012 + SQL Server 2016	Oui	Oui	Oui	Oui	Oui	Oui
			Windows Server 2016			
Windows 2016 + SQL Express 2016 SP1	Oui	Oui	Oui	Oui	Oui	Oui
Windows 2016 + SQL Server 2012	Oui	Oui	Oui	Oui	Oui	Oui
Windows 2016 + SQL Server 2014	Oui	Oui	Oui	Oui	Oui	Oui
Windows 2016 + SQL Server 2016	Oui	Oui	Oui	Oui	Oui	Oui

Matrice de support

Tableau 2. Matrice de support

Systèmes d'exploitation pris en charge pour le serveur WDM	• Windows Server 2008 R2 Enterprise SP1 • Windows Server 2012 Standard • Windows Server 2012 R2 • Windows Server 2016 • Windows 7 Enterprise SP1—64 bits
Systèmes d'exploitation pris en charge pour la mise à niveau de tous les composants WDM	• Windows 2008 R2 SP1 Enterprise • Windows 2008 Service Pack 2 32 bits • Windows 7 Enterprise SP1—32 bits • Windows Server 2012 Standard • Windows Server 2012 R2
Bases de données prises en charge	• Microsoft SQL Server 2008 R2 – Anglais • Microsoft SQL Server 2008 Enterprise—32 bits) • Microsoft SQL Server 2012

	• Microsoft SQL Server 2014 • Microsoft SQL Server 2016 • Microsoft SQL Server 2012 Enterprise Edition pour la haute disponibilité • Microsoft SQL Server 2016 Express SP1
Thin Clients pris en charge	**Wyse ThinOS** • Client léger Wyse 3010 avec ThinOS • Client léger Wyse 3020 avec ThinOS • Client léger Wyse 3040 avec ThinOS • Client léger Wyse 5010 avec ThinOS • Client léger Wyse 5040 avec ThinOS • Client léger Wyse 3030 LT avec ThinOS • Client léger Wyse 5060 avec ThinOS • Client léger Wyse 7010 avec ThinOS **Wyse ThinOS PCoIP** • Client léger Wyse 5040 AIO avec PCoIP • Client léger Wyse 5010 avec PCoIP • Client léger Wyse 3030 LT avec PCoIP • Client léger Wyse 5060 avec PCoIP **Wyse Enhanced Microsoft Windows Embedded Standard 7— Build 818 ou version ultérieure** • Client léger Wyse 5010 avec WES7 • Client léger Wyse 5020 avec WES7 • Client léger Wyse 7010 avec WES7 • Client léger Wyse 7020 avec WES7 • Client léger Wyse 7010 à châssis étendu avec WES7 • Client léger Wyse 3030 avec WES7 **Wyse Enhanced Microsoft Windows Embedded Standard 7p— Build 850 ou version ultérieure** • Client léger Wyse 7010 avec WES7P • Client léger châssis étendu Wyse 7010 avec WES7P • Client léger Wyse 5020 avec WES7P • Client léger Wyse 7020 avec WES7P • Client léger Wyse 7040 avec WES7P • Client léger mobile Dell Latitude E7270 • Client léger Wyse 5060 avec WES7P • Client léger mobile Latitude 3460 **Wyse Enhanced Microsoft Windows Embedded 8 Standard— 64 bits** • Client léger Wyse 5010 avec WE8S • Client léger Wyse 5020 avec WE8S • Client léger Wyse 7010 avec WE8S • Client léger Wyse 7020 avec WE8S **Windows 10 IoT Enterprise, 64 bits**

	• Client léger Wyse 5020 avec Win10 IoT • Client léger Wyse 7020 avec Win10 IoT • Client léger Wyse 7040 avec Win10 IoT **Wyse Enhanced SUSE Linux Enterprise** • Client léger Wyse 5010 avec Linux • Client léger Wyse 5020 avec Linux • Client léger Wyse 7010 avec Linux • Client léger Wyse 7020 avec Linux **ThinOS Lite** • Client zéro Wyse 3010 avec Citrix • Client zéro Wyse 3020 avec Citrix • Client zéro Wyse 5010 avec Citrix **Client zéro ThreadX/View** • Client zéro Wyse 5030 • Client zéro Wyse 7030 • Client zéro Wyse 5050 AIO avec PCoIP **ThinLinux** • Client léger Wyse 3030 LT avec ThinLinux • Client léger Wyse 3040 avec ThinLinux • Client léger Wyse 7020 avec ThinLinux • Client léger Wyse 5020 avec ThinLinux • Client léger Wyse 5060 avec ThinLinux
Plates-formes client léger Dell Wyse EOL prises en charge	**Wyse Enhanced Microsoft Windows Embedded Standard 7—Build 818 ou version ultérieure** • C90LE7 • R90L7 • R90LE7 • X90c7 • X90m7 • Z90s7 **Wyse Enhanced Microsoft Windows Embedded Standard 7P** • X90m7P • Z90s7P **Wyse Enhanced Microsoft Windows Embedded 8 Standard—32 bits** • Client léger Wyse 5010 avec WE8S • Client léger Wyse 7010 avec WE8S • Z90D8E **Wyse Enhanced SUSE Linux Enterprise** • C50LE • R50L • R50LE

	• X50c • X50M • Z50S **ThinOS Lite** • C00X • R00X **Client zéro ThreadX/View** • P20 **Wyse ThinOS** • C10LE • R10L **Wyse Enhanced Microsoft Windows Embedded Standard 2009 —Build 641 ou version ultérieure** • C90LEW • 5010 • R90LW • R90LEW • V90LEW • X90CW • X90MW • 7010 • Z90SW

Prise en charge de la localisation

Pour le serveur WDM, la prise en charge de la localisation est fournie sous Windows 2008 R2 SP1 Enterprise Edition, Windows 2012 Standard R2 et Windows 2016 R2 Standard pour les langues suivantes :

- Français
- Allemand
- Espagnol
- Japonais
- Chinois simplifié

Support technique Dell Wyse

Pour accéder au portail des ressources techniques en libre-service, à la base de connaissances, aux téléchargements de logiciels, à l'inscription, aux extensions de garantie/autorisation de retour de matériel (RMA), aux manuels de référence et autres, consultez le site www.dell.com/wyse/support . Pour le service clientèle, rendez-vous sur www.dell.com/support/contents/us/en/19/article/Contact-Information/International-Support-Services/international-contact-center?ref=contactus. Les numéros de téléphone pour le support Basic et Pro sont disponibles sur le site www.dell.com/supportcontacts .

REMARQUE : avant de continuer, vérifiez que votre produit dispose d'un numéro de série Dell. Pour les produits dotés d'un numéro de service Dell, accédez à www.dell.com/support/contents/us/en/19/article/Product-Support/Dell-Subsidiaries/wyse pour obtenir plus d'informations.

Documentation et services connexes

Des fiches descriptives contenant les fonctionnalités des produits matériels sont disponibles sur le site Web Dell Wyse. Rendez-vous sur http://www.dell.com/wyse et sélectionnez votre produit matériel pour localiser et télécharger la fiche descriptive.

Pour obtenir de l'assistance au sujet de votre produit Wyse, vérifiez son Numéro de service ou numéro de série.

- Pour les produits Dell marqués comme services, vous trouverez les articles de la base de connaissances et les pilotes dans les pages des produits Dell Wyse.
- Pour les produits Dell non marqués comme services, vous trouverez toute l'assistance nécessaire en accédant au domaine d'assistance Wyse.

Communauté en ligne Dell Wyse

Dell Wyse entretient une communauté en ligne où les utilisateurs de nos produits peuvent rechercher et échanger des informations sur les forums d'utilisateurs. Visitez les forums de la communauté en ligne Dell Wyse à l'adresse : en.community.dell.com/techcenter/enterprise-client/wyse_general_forum/.

2

Prérequis

Cette section répertorie les prérequis, les configurations matérielles et logicielles requises pour la préparation de l'environnement accueillant l'installation et la configuration de WDM. Cette section comprend :

- La liste de pré-installation
- La configuration matérielle requise
- Configuration logicielle requise
- Les ports de communication requis
- Les mises à niveau requises
- Les conditions nécessaires à la gestion des périphériques PCoIP

Sujets :

Liste de pré-installation

Avant de démarrer l'installation de WDM, assurez-vous de répondre aux exigences suivantes :

- Le serveur sur lequel vous installez WDM doit être dédié aux services WDM et ne doit pas exécuter d'autres fonctions. Par exemple, le serveur ne doit pas fonctionner en tant que contrôleur de domaine, contrôleur de secours, serveur de messagerie, serveur Web de production, serveur DHCP, serveur MSMQ ou serveur d'applications.
- Installez un système d'exploitation pris en charge sur le serveur où vous installez WDM. Pour plus d'informations, voir Informations sur le support.
- Assurez-vous qu'aucune autre application nécessitant IIS pour fonctionner n'est en cours d'exécution sur le système accueillant WDM.
- Assurez-vous que tous les ports de communication nécessaires sont disponibles et prêts pour la communication entre les serveurs, routeurs et commutateurs. Pour plus d'informations, voir Ports de communication requis.
- Vérifiez que vous avez accès au CD-ROM de votre système d'exploitation et à votre système de fichiers Microsoft Windows pendant l'installation. Le programme d'installation WDM vérifie le système pour toutes les configurations logicielles requises. Si un logiciel n'est pas installé, le programme d'installation vous demande d'installer le logiciel requis. Par conséquent, vous devez avoir accès au CD-ROM de votre système d'exploitation ou à l'emplacement réseau pour accéder au système de fichiers Microsoft Windows.
- Installez Adobe Acrobat Reader pour lire le Contrat de licence d'utilisateur final (CLUF) et le Guide d'installation.
- Le serveur doit être installé avec les composants ThreadX 5x dans Windows 2012 ou une version ultérieure.

Configuration matérielle requise

Le système sur lequel WDM est installé doit répondre à la configuration matérielle minimale requise ou la dépasser et dépend du système d'exploitation installé. L'espace disque nécessaire dépend du nombre de progiciels que vous enregistrez et du nombre de périphériques que vous comptez gérer.

Tableau 3. Configuration matérielle requise pour un serveur équipé d'un système d'exploitation 32 bits

Catégorie	Configuration minimale requise	Configuration recommandée
Processeur	2,5 GHz double cœur Intel ou AMD	Quadruple cœur Intel ou AMD
Mémoire RAM	4 Go Pour une machine virtuelle, 2 Go doivent être initialement alloués	4 Go
Espace disque minimal disponible	40 Go	40 Go

Tableau 4. Configuration matérielle requise pour un serveur équipé d'un système d'exploitation 64 bits

Catégorie	Configuration minimale requise	Configuration recommandée
Processeur	2,5 GHz double cœur Intel ou AMD	Quadruple cœur Intel ou AMD
Mémoire RAM	6 Go	8 Go
Espace disque minimal disponible	40 Go	40 Go

Les ports de communication requis

Les composants logiciels WDM requièrent l'ouverture permanente de certains ports de communication sur vos serveurs, routeurs et commutateurs. Par exemple, WDM dépend des ports de communication HTTP/HTTPS pour les opérations initiées par WDM et transmises aux appareils.

Ces opérations push sont les suivantes :

- Émission de commandes comme Refresh Device Information, Reboot, Change Device or Network Information, Get Device Configuration, etc.
- Distribution de packages à une heure spécifique.

Généralement, le port 80 est le port HTTP par défaut, tandis que le port 443 est utilisé comme port HTTPS par défaut. Si l'un de ces ports est fermé, WDM ne peut pas transférer les mises à jour ou les commandes rapides vers les périphériques.

Tableau 5. Ports de communication

Composant WDM	Protocole et ports correspondants	Port	Fonction
Interface graphique utilisateur	HTTP	80 280	Communique avec le service Web et le service standard.
	FTP	21	Enregistre de nouveaux packages dans la logithèque maître.
	OLE DB	1433 (valeur par défaut) Peut être configuré au cours de l'installation.	Communique avec la base de données de WDM.
	VNC	5800 5900	Périphériques shadows distants.

Composant WDM	Protocole et ports correspondants	Port	Fonction
Service Web	HTTP	80 280	Communique avec l'agent Web, l'interface graphique utilisateur et le service standard.
	HTTPS	443 8443	Sécurise la communication avec l'agent Web, l'interface graphique utilisateur et le service standard.
	OLE DB	1433 (valeur par défaut) peut être configuré au cours de l'installation	Communique avec la base de données de WDM.
Agent Web	HTTP	80 280	Communique avec le service Web.
	FTP	21	Lecture et écriture de fichiers vers les logithèques maître et distantes.
Services DHCP Proxy et TFTP	OLE DB	1433 (valeur par défaut) peut être configuré au cours de l'installation	Communique avec la base de données de WDM.
	HTTP	8008	Communiquent avec l'interface utilisateur graphique et le service Web.
Services DHCP Proxy et TFTP et PXE	DHCP	67 68 4011	Traitent les demandes UDP envoyées au service standard par des périphériques activés pour PXE.
	TFTP	69	Téléchargent une image amorçable pour activer le traitement de la gestion.
	HTTP	80	Communiquent avec le service Web sur les actions et l'état de la tâche en cours.
	FTP	21	Téléchargent dans les deux sens des fichiers vers les logithèques maître et distantes.
Les services Proxy DHCP et TFTP sont là pour prendre en charge les anciens agents WDM	UDP	44956 44957	Détectent à l'aide de diffusions dirigées vers des sous-réseaux les périphériques sur lesquels sont installés des agents WDM anciens (5.0.0.x et antérieur).
	TCP	44955	Détectent les périphériques en parcourant les plages d'adresses IP et mettent à niveau les périphériques dotés d'une version ancienne de

Composant WDM	Protocole et ports correspondants	Port	Fonction
			l'agent WDM (5.0.0.x et antérieures).
Service de gestionnaire ThreadX 4.x	TCP	9880 50000	Communiquent avec les périphériques ThreadX 4.x.
Service de gestionnaire ThreadX 5.x	TCP	49159 5172	Communiquent avec les périphériques ThreadX 5.x. **REMARQUE : Les deux ports de communication doivent être ajoutés aux règles d'entrée du pare-feu. Le cas échéant, le numéro de port 49159 peut être personnalisé. Le port par défaut 49159 doit être ajouté manuellement lorsqu'il est personnalisé.**

Les conditions nécessaires à la gestion des périphériques PCoIP

Les périphériques PCoIP équipés du micrologiciel Thread X nécessitent l'enregistrement de ressource d'un emplacement de service (SRV) DNS afin de procéder aux actions suivantes :

- **Partial Check-In (heartbeat)** : (Mesure partielle (émissions de signaux)) : le périphérique vérifie les signaux émis par les nœuds (heartbeat) toutes les heures.
- **Firmware Download Completion Status** (État de progression du téléchargement du micrologiciel) : le téléchargement du micrologiciel est initié par le serveur tandis que l'achèvement du téléchargement est initié par le périphérique utilisant l'enregistrement SRV DNS.
- **ThreadX 4.x** : configurez le FTP si vous voulez utiliser la fonction de mise à niveau du micrologiciel pour les appareils PCoIP (ThreadX 4.x). Vous devez activer cette fonction dans la logithèque. Pour plus d'informations sur l'activation du protocole FTP dans la logithèque, reportez-vous au *Dell Wyse Device Manager Administrator's Guide (Guide de l'administrateur de Dell Wyse Device Manager)*.
- **ThreadX 5.x** : configurez le CIFS si vous voulez utiliser la fonction de mise à niveau du micrologiciel pour les appareils PCoIP (ThreadX 5.x). Vous devez activer cette fonction dans la logithèque. Pour plus d'informations sur l'activation CIFS dans le référentiel de logiciels, reportez-vous au *Dell Wyse Device Manager Administrator's Guide (Guide de l'administrateur de Dell Wyse Device Manager)*.

Liste de contrôle pour l'installation de l'édition Entreprise de WDM

Si vous installez l'édition Entreprise de WDM, faites en sorte que :

- Votre clé de vente Entreprise WDM ou la clé d'évaluation Entreprise WDM que vous avez utilisée lors de l'installation doit être accessible.
- Installez la version prise en charge de SQL Server. Le programme d'installation de WDM propose Microsoft SQL Express 2014 comme option par défaut, mais vous pouvez choisir une autre version prise en charge de SQL Server.
- Vous devez installer les services FTP et les activer pour utiliser le protocole FTP pour les périphériques Dell Wyse PCoIP (ThreadX 4.x).

- Vous devez installer les services CIFS et les activer pour utiliser le protocole CIFS pour les périphériques Dell Wyse PCoIP (ThreadX 5.x).

REMARQUE :

Si vous envisagez d'utiliser PCoIP (ThreadX), créez et configurez un enregistrement de ressource SRV d'emplacement de service DNS. Pour plus d'informations, reportez-vous à Configuring Load Balancing for ThreadX 4.x Devices (Configuration de l'équilibrage de charge pour les périphériques Thread X 4.x) et Configuring Load Balancing for ThreadX 5.x Devices (Configuration de l'équilibrage de charge pour les périphériques Thread X 5.x).

3

Installation de Wyse Device Manager

WDM inclut les composants suivants :

- Base de données
- Serveur de gestion
- Logithèque
- Autres services
- Interface utilisateur Web

Vous pouvez installer tous les composants sur le même système ou vous pouvez avoir une configuration distribuée où chaque composant est installé sur des systèmes différents.

WDM est disponible dans les éditions suivantes :

- **Édition Entreprise** : cette édition nécessite une clé de licence spécifique et est fournie avec toutes les fonctionnalités de WDM. Elle permet de gérer un très grand nombre de périphériques clients légers. Vous pouvez installer cette édition dans un environnement distribué et chaque composant sur des systèmes différents.
- **Édition Workgroup** : cette édition comprend une clé de licence gratuite et certaines fonctionnalités de WDM sont désactivées. De plus, vous pouvez gérer jusqu'à 10 000 clients légers. Cette édition requiert l'installation de la totalité des composants sur le même système et ne prend pas en charge les configurations distribuées.

REMARQUE : La licence Workgroup doit être activée.

REMARQUE :

- Pour exécuter le programme d'installation de WDM (Setup.exe), vous devez vous connecter au système en tant qu'administrateur.
- Vous ne pouvez pas installer WDM sur des serveurs exécutant d'autres services comme DNS ou DHCP, les services de domaines AD ou des services qui entreraient en conflit avec les fonctionnalités et les ressources WDM.
- Lorsque vous installez la base de données WDM en mode configuration autonome ou en mode configuration distribuée et que vous souhaitez utiliser une base de données SQL existante, assurez-vous qu'il s'agit d'une version complète de SQL Server et non de SQL Server Express.
- Pour WDM Workgroup, vous trouverez un support sur les forums de la communauté Dell.
- Le composant de gestion ThreadX 5x est pris en charge uniquement dans l'édition Enterprise.

Sujets :

Installation de WDM Workgroup Edition

Étapes

1 Décompressez le contenu du programme d'installation de WDM sur le système sur lequel vous souhaitez installer WDM.

2 Accédez au dossier dans lequel vous avez extrait le programme d'installation et exécutez **Setup.exe**.

L'écran **Welcome (Accueil)** s'affiche.

Figure 1. Écran Welcome (Accueil)

3 Cliquez sur **NEXT (SUIVANT)**.

4 Sous License type (Type de licence), sélectionnez **WORKGROUP**, puis cliquez sur **NEXT (SUIVANT)**.

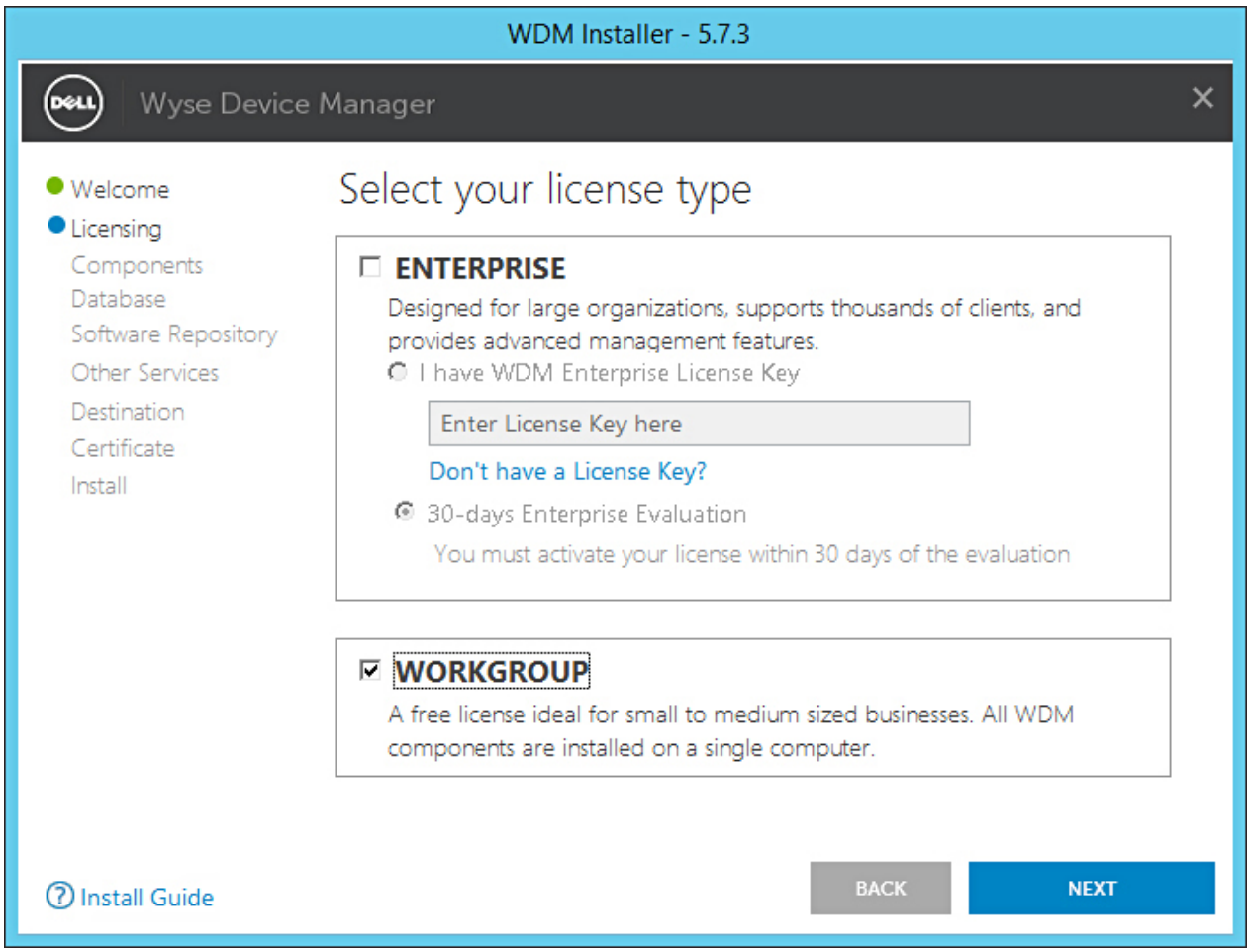


Figure 2. Type de licence Workgroup

REMARQUE : Pour Workgroup Edition, la clé de licence est fournie dans le programme d'installation et il n'est pas nécessaire d'entrer de détails.

L'écran **Components (Composants)** s'affiche.

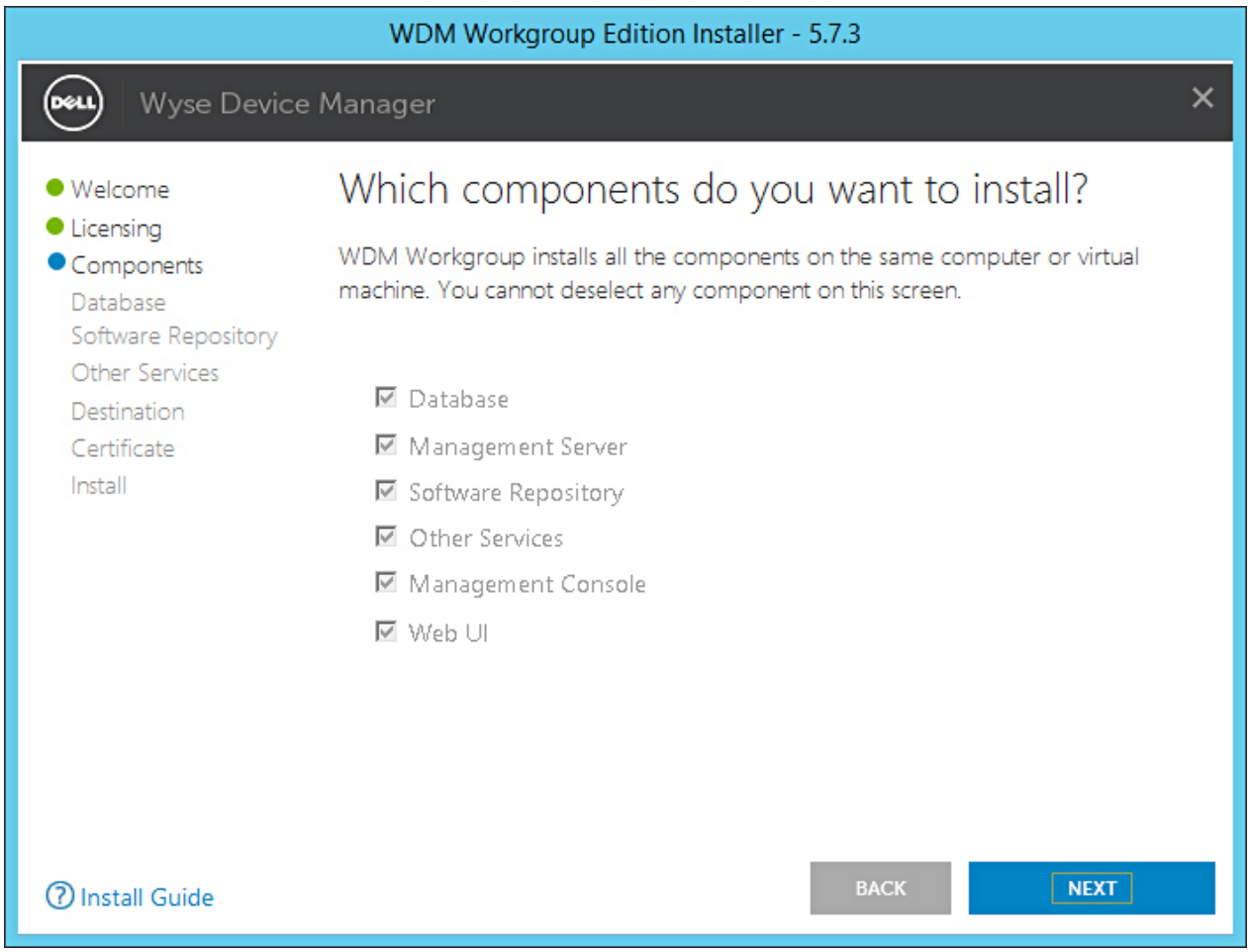


Figure 3. Écran Components (Composants)

5 Cliquez sur **NEXT (SUIVANT)**.

REMARQUE : Tous les composants sont sélectionnés par défaut et vous ne pouvez pas désélectionner de composants.

L'écran **Configure Database (Configurer la base de données)** s'affiche.

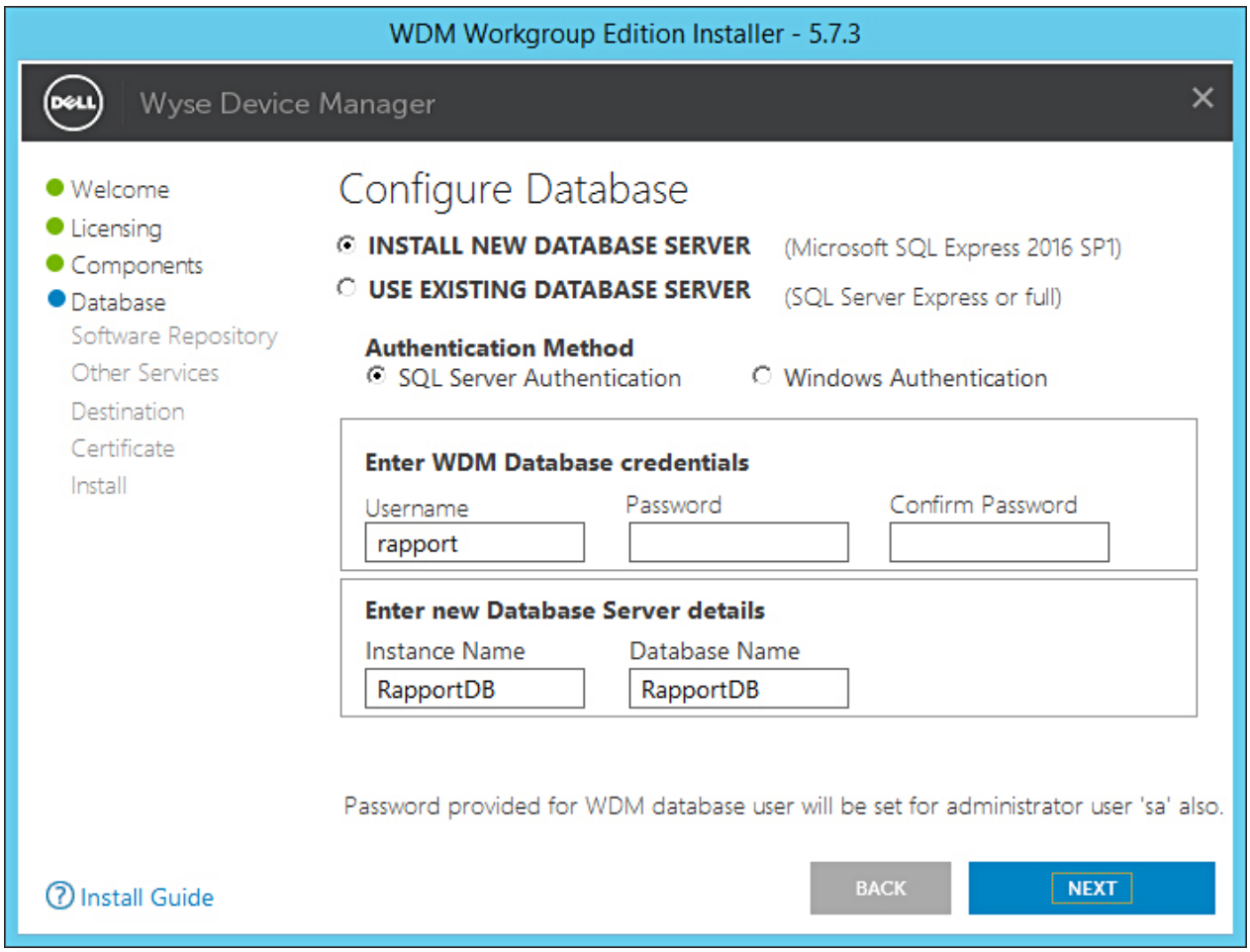


Figure 4. Configurer la base de données

6 Dans l'écran **Configure Database (Configurer la base de données)**, sélectionnez l'une des options suivantes :

- **Install New Database Server (Installer un nouveau serveur de base de données) (Microsoft SQL Express 2016 SP1)** : sélectionnez cette option si aucune version prise en charge de Microsoft SQL Server n'est installée sur le système. Passez à l'étape 8.
- **Use Existing Database Server (Utiliser le serveur de base de données existant) (SQL Server Express ou Full)** : sélectionnez cette option si une version prise en charge de Microsoft SQL Server est déjà installée sur le système. Si vous sélectionnez cette option, assurez-vous que le serveur de base de données se trouve sur le même système que celui sur lequel vous installez l'édition Workgroup de WDM, et passez à l'étape 9.

7 Si vous avez sélectionné la première option lors de l'étape 7, sélectionnez la méthode d'authentification.

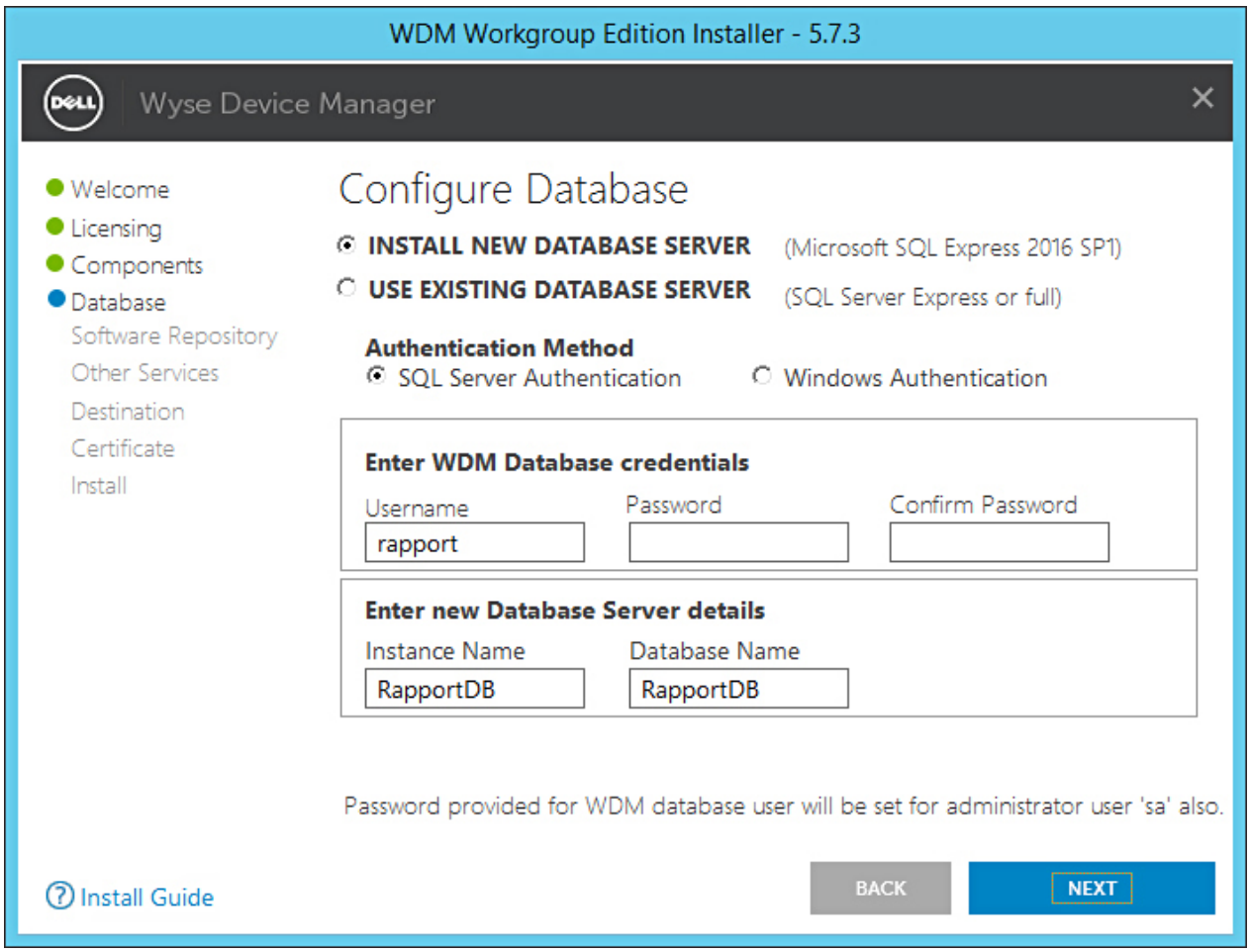


Figure 5. Option Install New Database Server (Installer un nouveau serveur de base de données)

- **SQL Server Authentication (Authentification du serveur SQL)** : cette option est sélectionnée par défaut. Pour configurer l'authentification du serveur SQL, procédez comme suit :
  1. Entrez les informations d'identification de la base de données WDM.
  2. Entrez les informations d'identification de la nouvelle base de données. Vous pouvez entrer le nom de l'instance et le nom de la base de données dans les détails du nouveau serveur de base de données. Le nom d'instance et le nom de la base de données par défaut sont RapportDB.
- **Windows Authentication (Authentification Windows)** : entrez les informations sur le nouveau serveur de base de données. Le nom d'instance et le nom de la base de données par défaut sont RapportDB.

REMARQUE :

- Sélectionnez **Windows Authentication (Authentification Windows)** si vous souhaitez vous connecter à la base de données WDM en utilisant vos informations de connexion Windows.
- Le mot de passe doit correspondre aux règles de complexité du système d'exploitation Windows.

8. Si vous avez sélectionné la seconde option lors de l'étape 7, sélectionnez la méthode d'authentification.

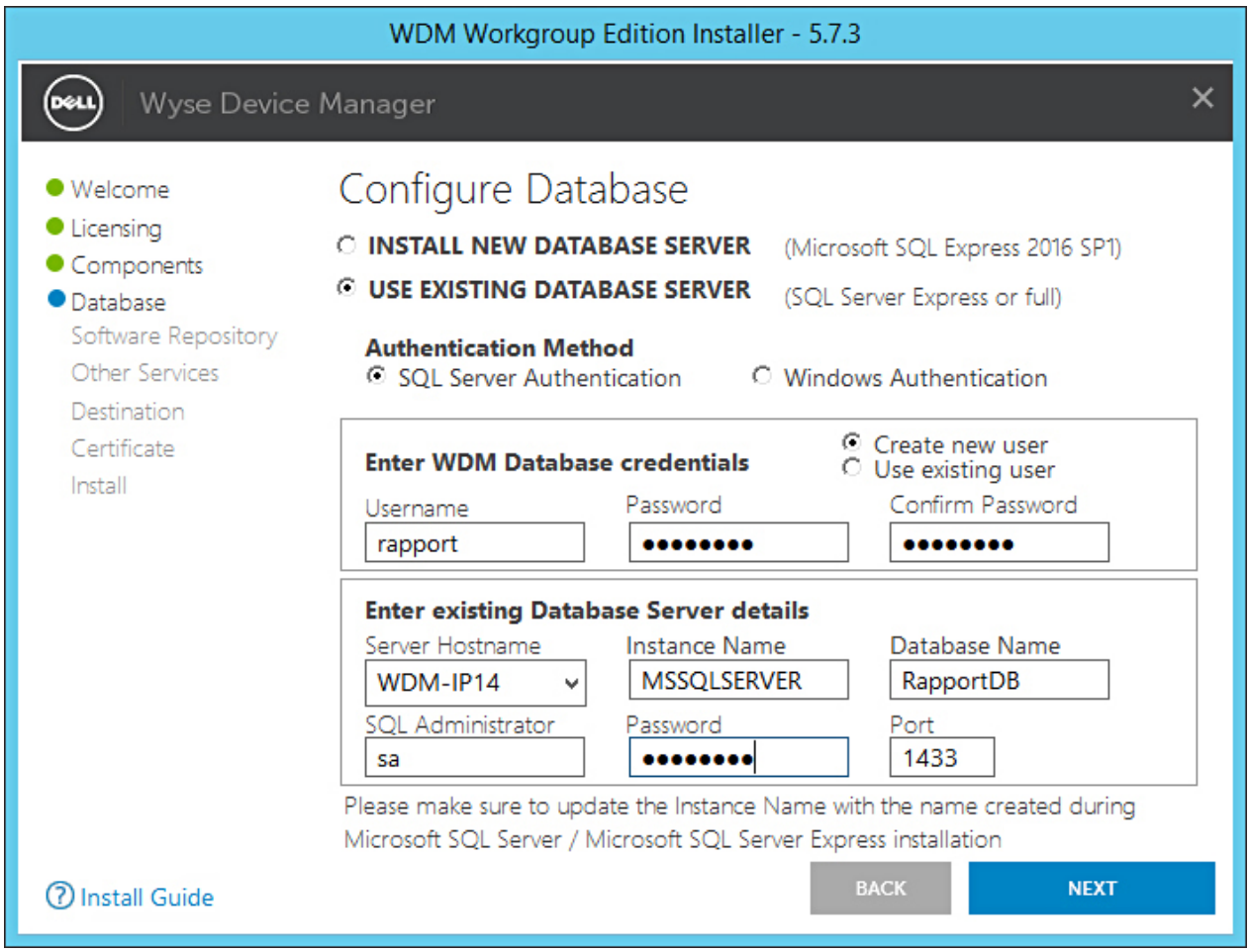


Figure 6. Option Use Existing Database Server (Utiliser le serveur de base de données existant)

- **SQL Server Authentication (Authentification du serveur SQL)** : cette option est sélectionnée par défaut. Pour configurer l'authentification du serveur SQL, procédez comme suit :
  1. Sélectionnez l'option Create new user (Créer un nouvel utilisateur) ou l'option Use the existing user (Utiliser l'utilisateur existant), puis entrez les informations d'identification de la base de données WDM.
  2. Entrez les informations sur le serveur de base de données existant, telles que le nom d'hôte du serveur, le nom de l'instance, le nom de la base de données, le numéro de port et le nom de l'administrateur et le mot de passe SQL. Le numéro de port par défaut est 1433.
- **Windows Authentication (Authentification Windows)** : entrez les informations sur le serveur de base de données existant, telles que le nom d'hôte du serveur, le nom de l'instance, le nom de la base de données, le numéro de port et le nom de l'administrateur et le mot de passe SQL.

9. Cliquez sur **NEXT (SUIVANT)**.

   L'écran **Configure Software Repository Server (Configurer le serveur pour la Logithèque)** s'affiche.

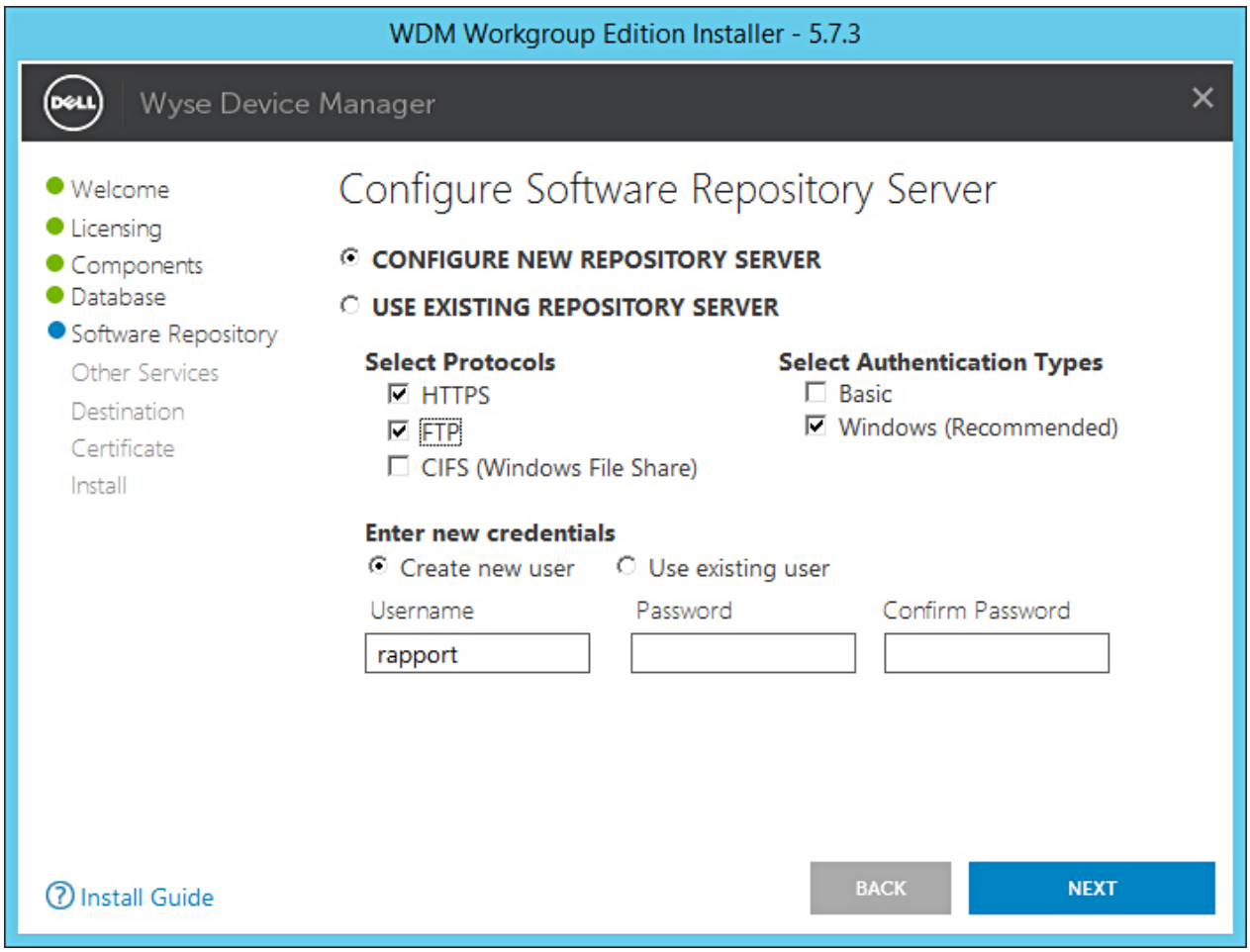


Figure 7. Écran Configure Software Repository Server (Configurer le serveur de référentiel de logiciels)

10 Dans l'écran **Configure Software Repository Server (Configurer le serveur de référentiel de logiciels)**, vous pouvez sélectionner l'une des options suivantes :

- **CONFIGURE NEW REPOSITORY SERVER (CONFIGURER UN NOUVEAU SERVEUR DE RÉFÉRENTIEL)** : sélectionnez cette option si vous souhaitez que le programme d'installation configure un nouveau serveur de référentiel. Pour configurer un nouveau serveur de référentiel :
  - Sélectionnez le protocole et les paramètres pour distribuer le logiciel vers les périphériques gérés. **HTTPS** est sélectionné par défaut. Vous pouvez également sélectionner **FTP** pour ThreadX 4.x et **CIFS** pour ThreadX 5.x.
  - Sélectionnez le type d'authentification. **Windows** est sélectionné par défaut.

    REMARQUE : L'authentification de base est requise pour les systèmes Linux.
  - Créez de nouvelles informations d'identification utilisateur ou utilisez des informations d'identification utilisateur existantes.
- **USE EXISTING REPOSITORY SERVER (UTLISER UN SERVEUR DE RÉFÉRENTIEL EXISTANT)** : sélectionnez cette option si vous souhaitez que le programme d'installation utilise un serveur de référentiel existant. Pour configurer le serveur de référentiel existant :
  - Sélectionnez le protocole et les paramètres pour distribuer le logiciel vers les périphériques gérés. **HTTPS** est sélectionné par défaut. Vous pouvez également sélectionner **FTP** pour ThreadX 4.x et **CIFS** pour ThreadX 5.x.
  - Sélectionnez le type d'authentification. **Windows** est sélectionné par défaut.
  - Saisissez les informations d'identification du serveur. L'option d'adresse IP du serveur est grisée et le nom d'utilisateur par défaut est « rapport ».

11 Cliquez sur **NEXT (SUIVANT)**.

12 Sélectionnez les services à installer, puis cliquez sur **NEXT (SUIVANT)**.

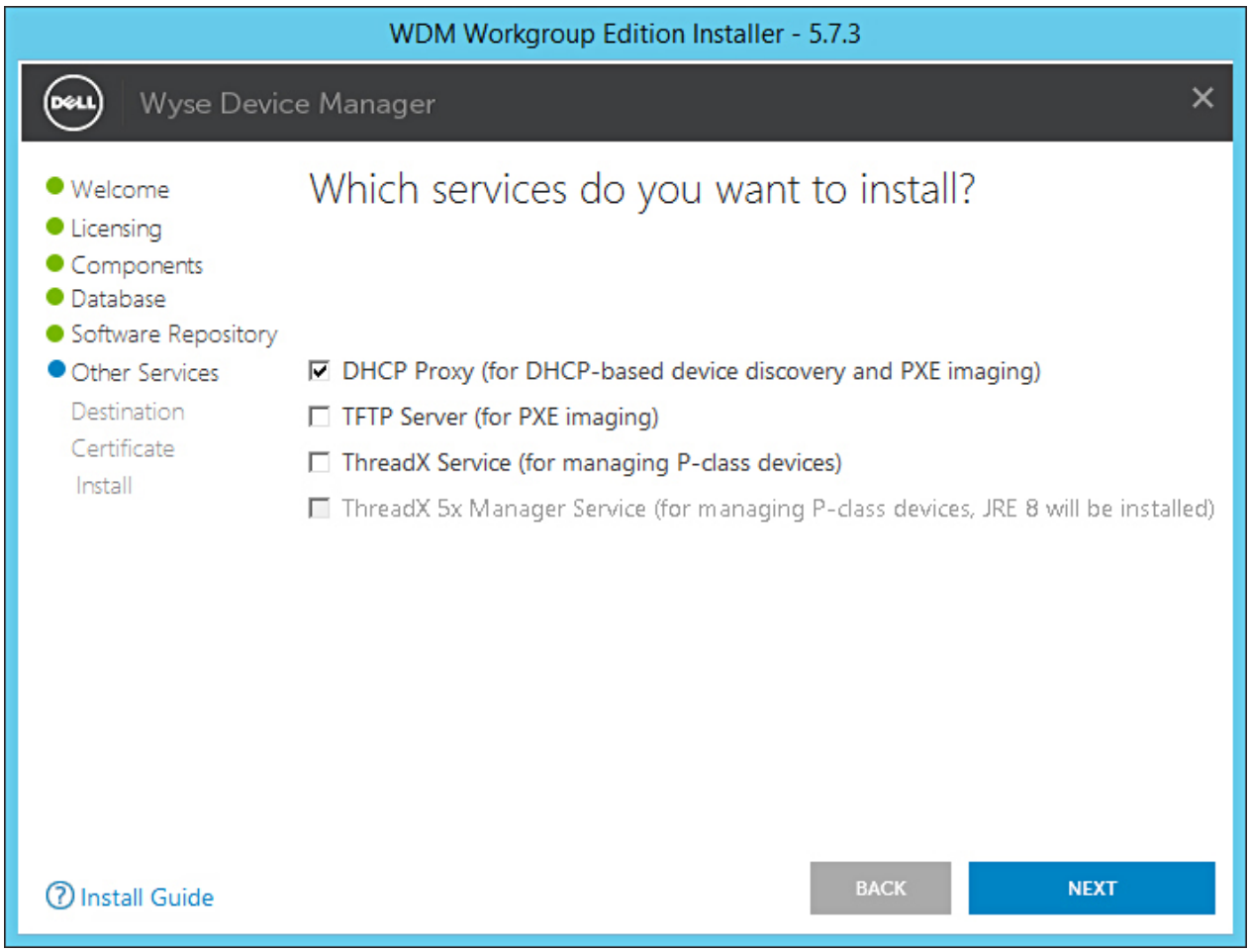


Figure 8. Écran Other Services (Autres services)

REMARQUE : DHCP Proxy (Proxy DHCP) est sélectionné par défaut.

13 Indiquez le chemin d'installation, puis cliquez sur **NEXT (SUIVANT)**.

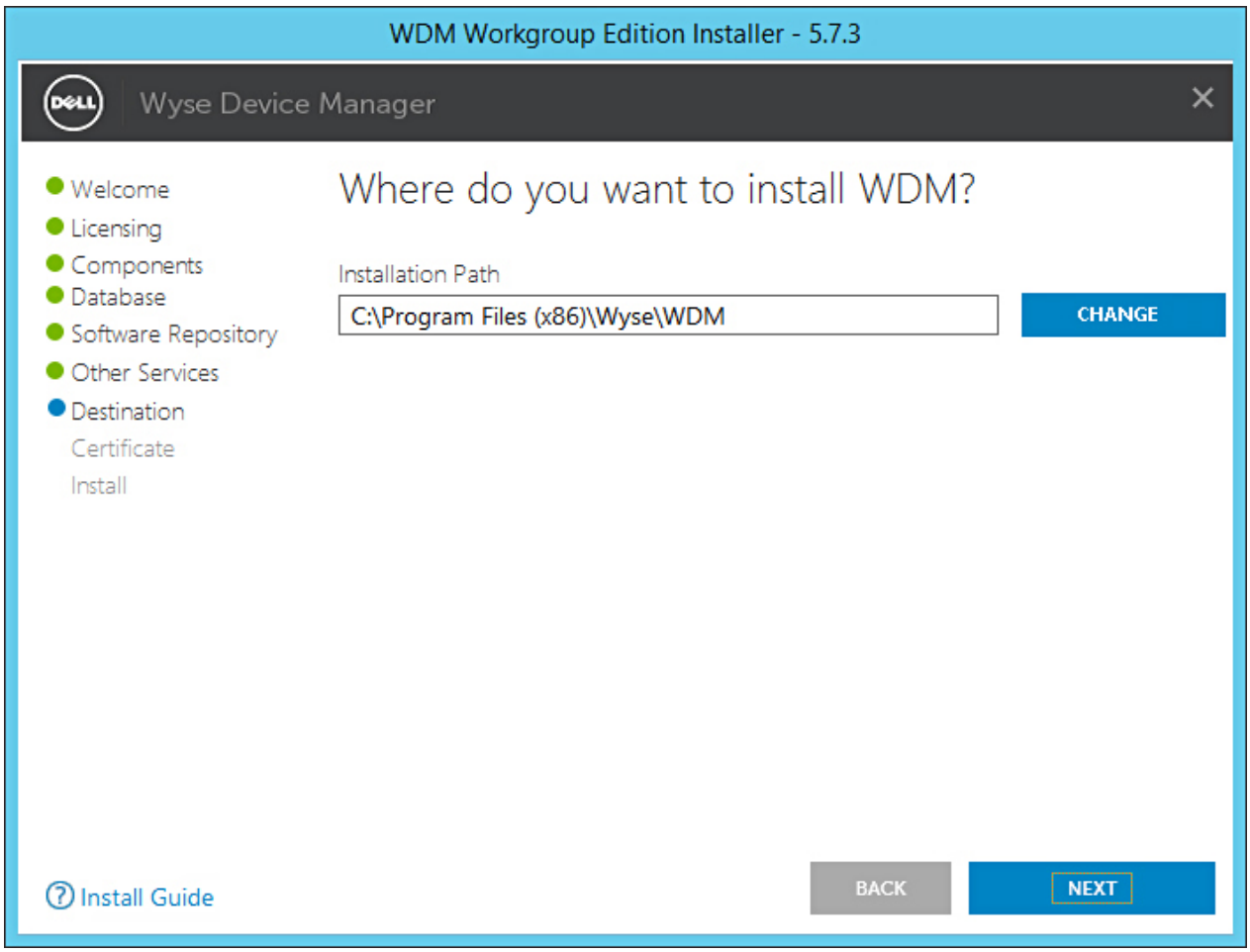


Figure 9. Écran de destination

14 Sélectionnez et importez le certificat pour démarrer l'installation.

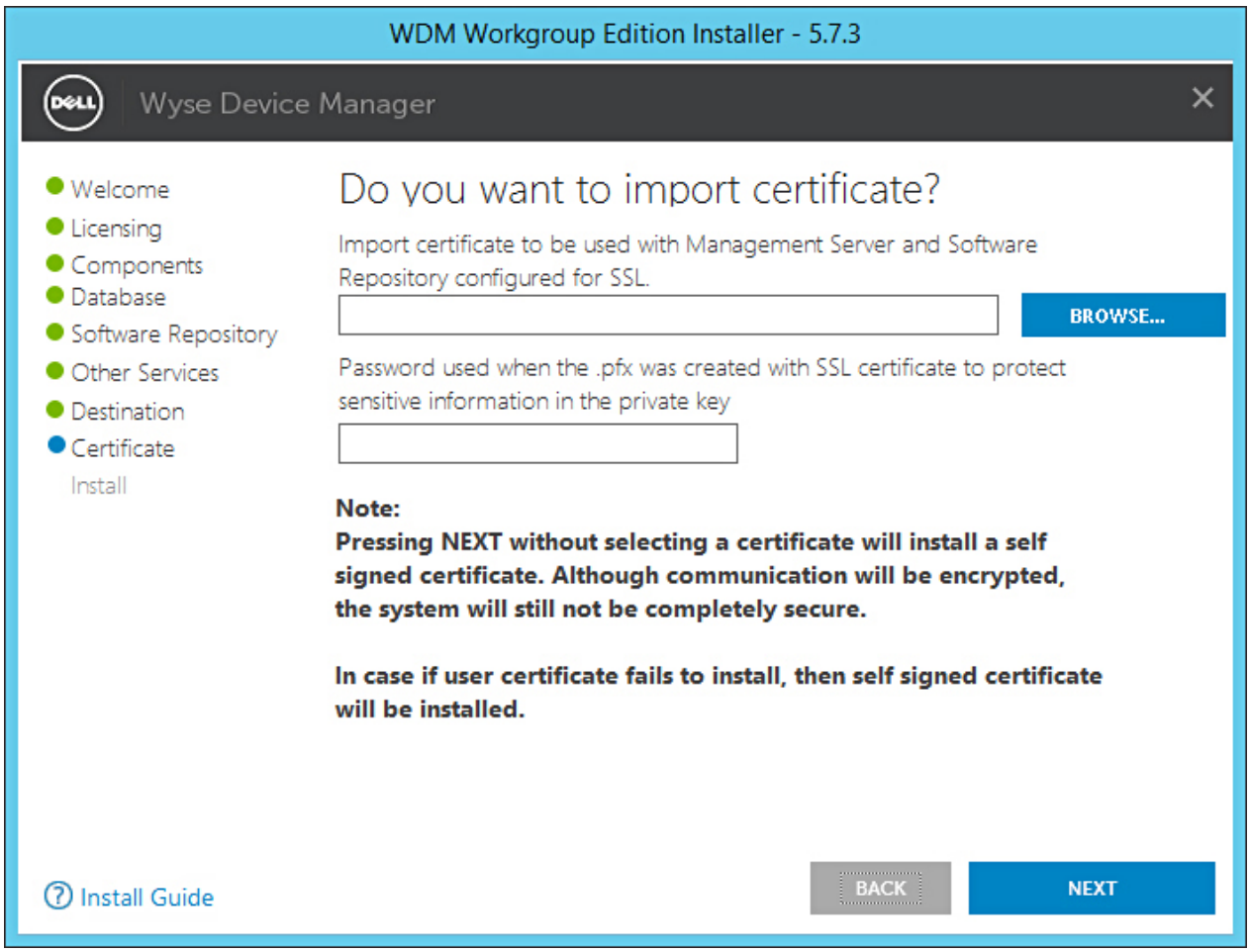


Figure 10. Écran Certificate (Certificat)

REMARQUE : Si vous cliquez sur NEXT (SUIVANT) sans avoir sélectionné de certificat, le programme d'installation installe un certificat auto-signé. Les communications sont chiffrées, mais le système n'est pas totalement sécurisé. Le certificat doit être au format .pfx.

La progression de l'installation s'affiche à l'écran. Une fois l'installation terminée, vous êtes invité à redémarrer votre système.

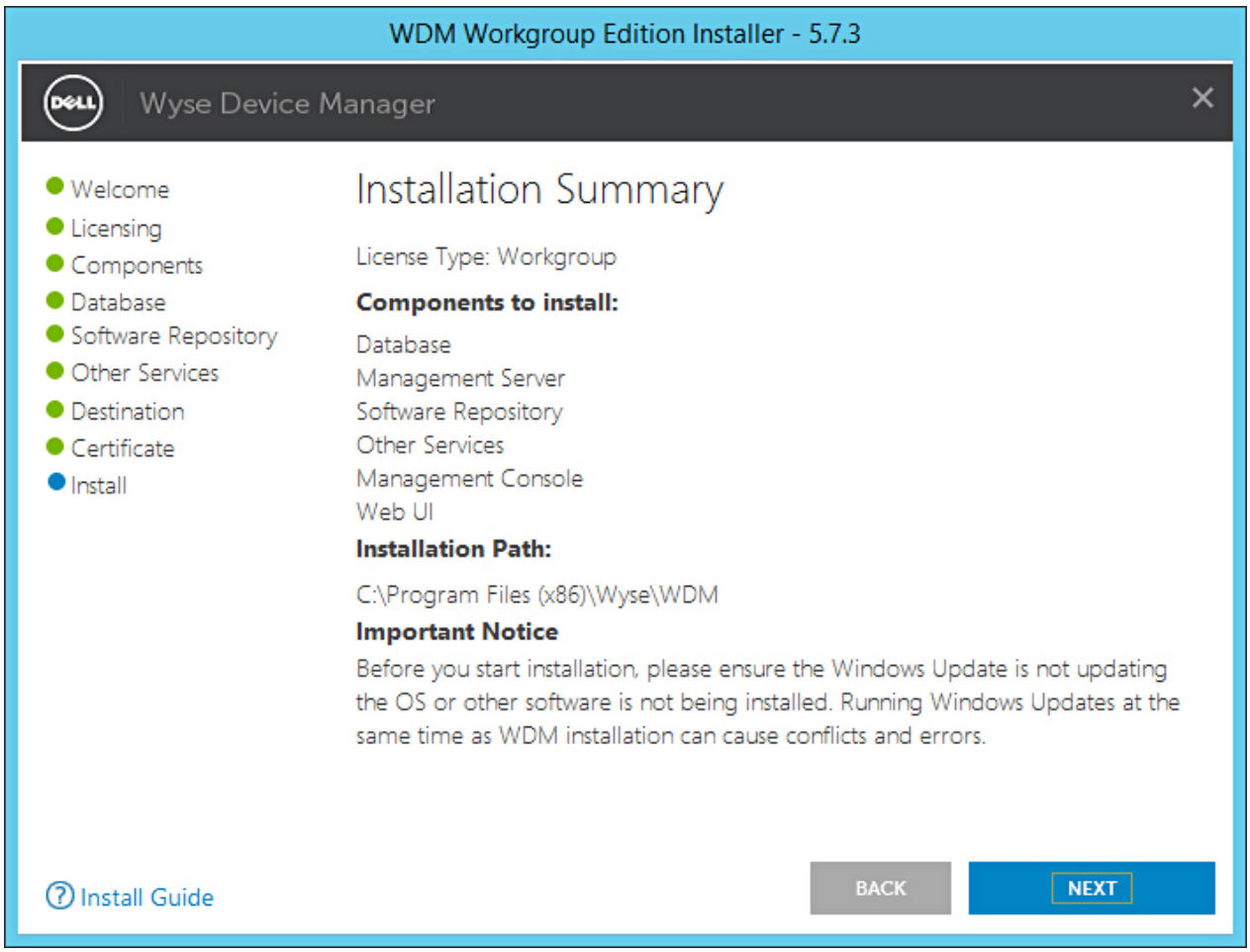


Figure 11. Écran Installation summary (Résumé de l'installation)

15 Redémarrez le système pour que les modifications prennent effet.

Étape suivante

Après l'installation, assurez-vous que les listes de contrôle suivantes sont respectées :

- WDM est installé dans **<drive C>\Inetpub\ftproot path** et le dossier Rapport est créé.
- L'icône WyseDeviceManager 5.7.3 WebUI est créée sur le Bureau.
- Dans IIS, l'application HApi est créée dans le dossier de serveur Rapport HTTP.
- Dans IIS, l'application MyWDM est créée dans le dossier de serveur Rapport HTTP.
- Dans IIS, l'application WebUI est créée dans le dossier de serveur Rapport HTTP.

REMARQUE : Après l'installation, assurez-vous que la base de données est créée avec l'instance fournie et le nom de la base de données.

Installation de WDM édition Entreprise

1 Décompressez le contenu du programme d'installation de WDM sur le système sur lequel vous souhaitez installer WDM.

2 Accédez au dossier dans lequel vous avez extrait le programme d'installation et exécutez **Setup.exe**.

Le cas échéant, le composant .NET Framework est installé automatiquement sur le serveur.

L'écran **Welcome** (Accueil) s'affiche.

Figure 12. Écran Welcome (Accueil)

3 Cliquez sur **NEXT** (SUIVANT).

4 Dans le type de licence, sélectionnez **ENTERPRISE** (ENTREPRISE).

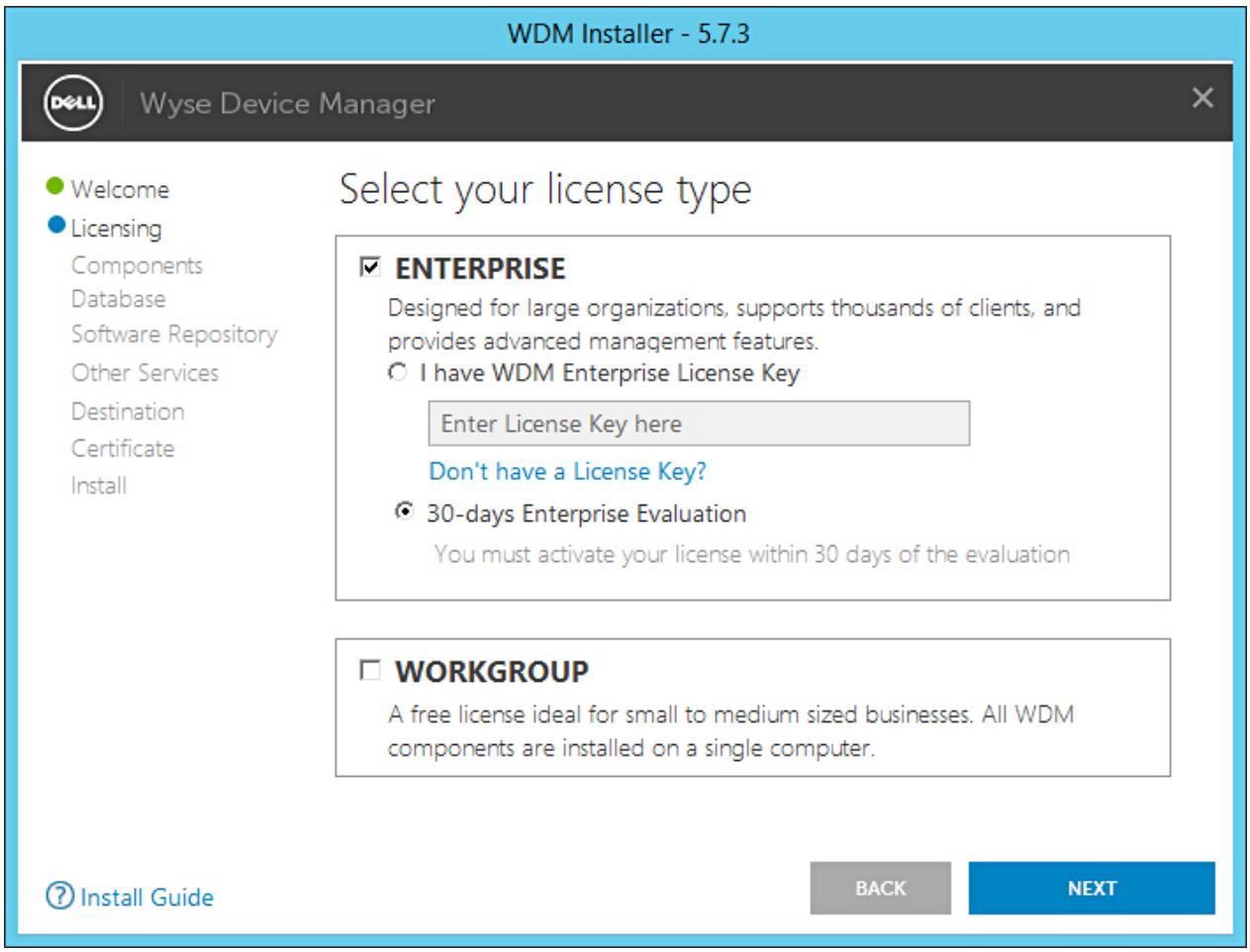


Figure 13. Type de licence Entreprise

a Si vous disposez de la clé de licence WDM, sélectionnez l'option **I have WDM Enterprise License Key** (J'ai une clé de licence Entreprise WDM), puis saisissez la clé de licence dans l'espace prévu à cet effet.

b Si vous ne disposez pas de la clé de licence, sélectionnez l'option **30–days Enterprise Evaluation** (30 jours d'essai de l'édition Entreprise).

La clé de licence est saisie par défaut. Cependant, après la période d'évaluation de 30 jours, vous devez obtenir la clé de licence et l'ajouter à WDM. Pour plus d'informations sur l'ajout de la clé de licence, consultez le *Dell Wyse Device Manager Administrator's Guide* (Guide de l'aministrateur de Dell Wyse Device Manager).

5 Cliquez sur **NEXT** (SUIVANT).

6 Sélectionnez les composants à installer, puis cliquez sur **NEXT** (SUIVANT).

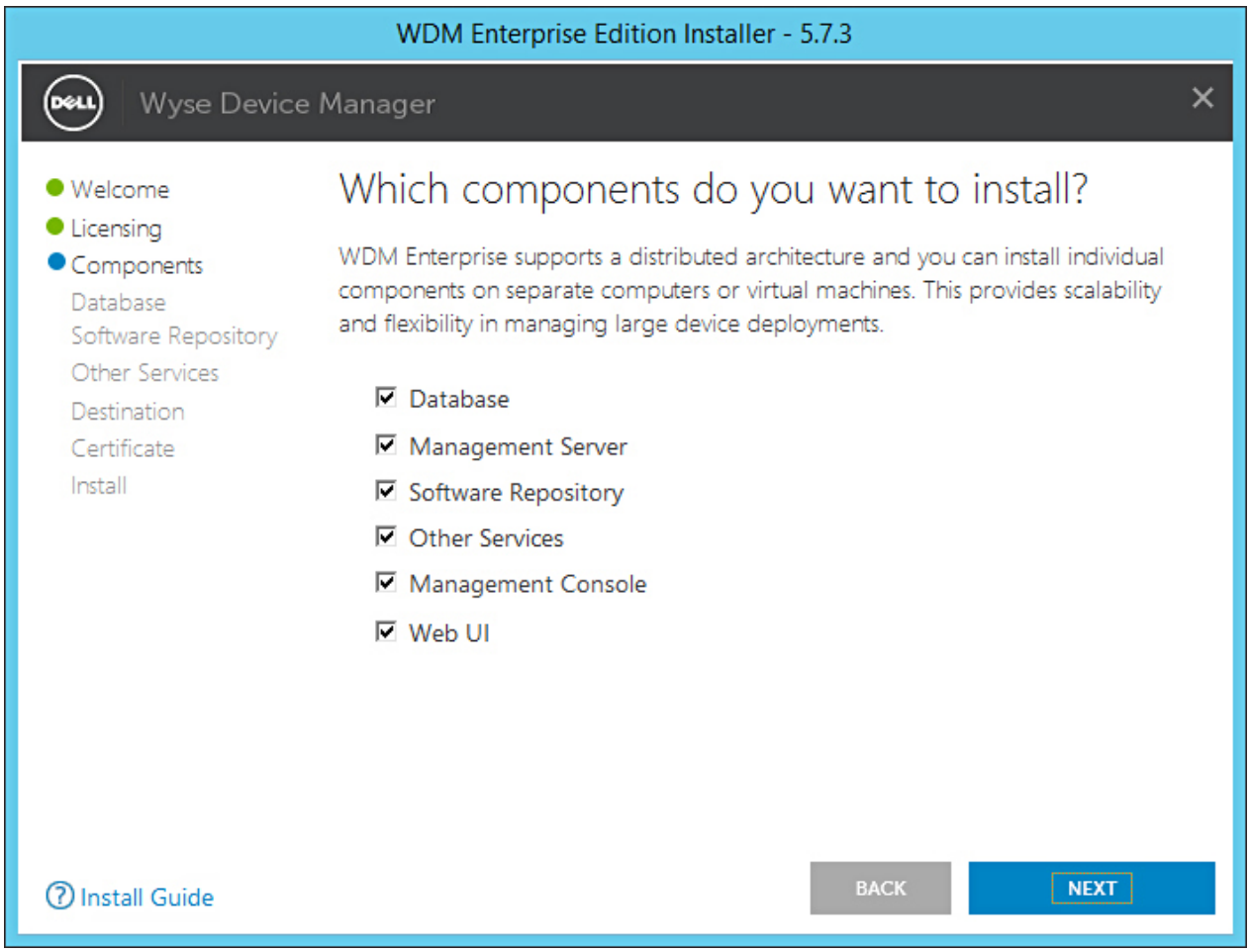


Figure 14. Écran Components (Composants)

Vous pouvez installer tous les composants sur le même système ou chaque composant sur un système différent.

REMARQUE : Si vous installez les composants séparément sur différents systèmes, assurez-vous d'installer la base de données en premier, sans quoi, vous ne pourrez pas installer les autres composants.

7 Dans l'écran **Configure Database** (Configurer la base de données), sélectionnez l'une des options suivantes :

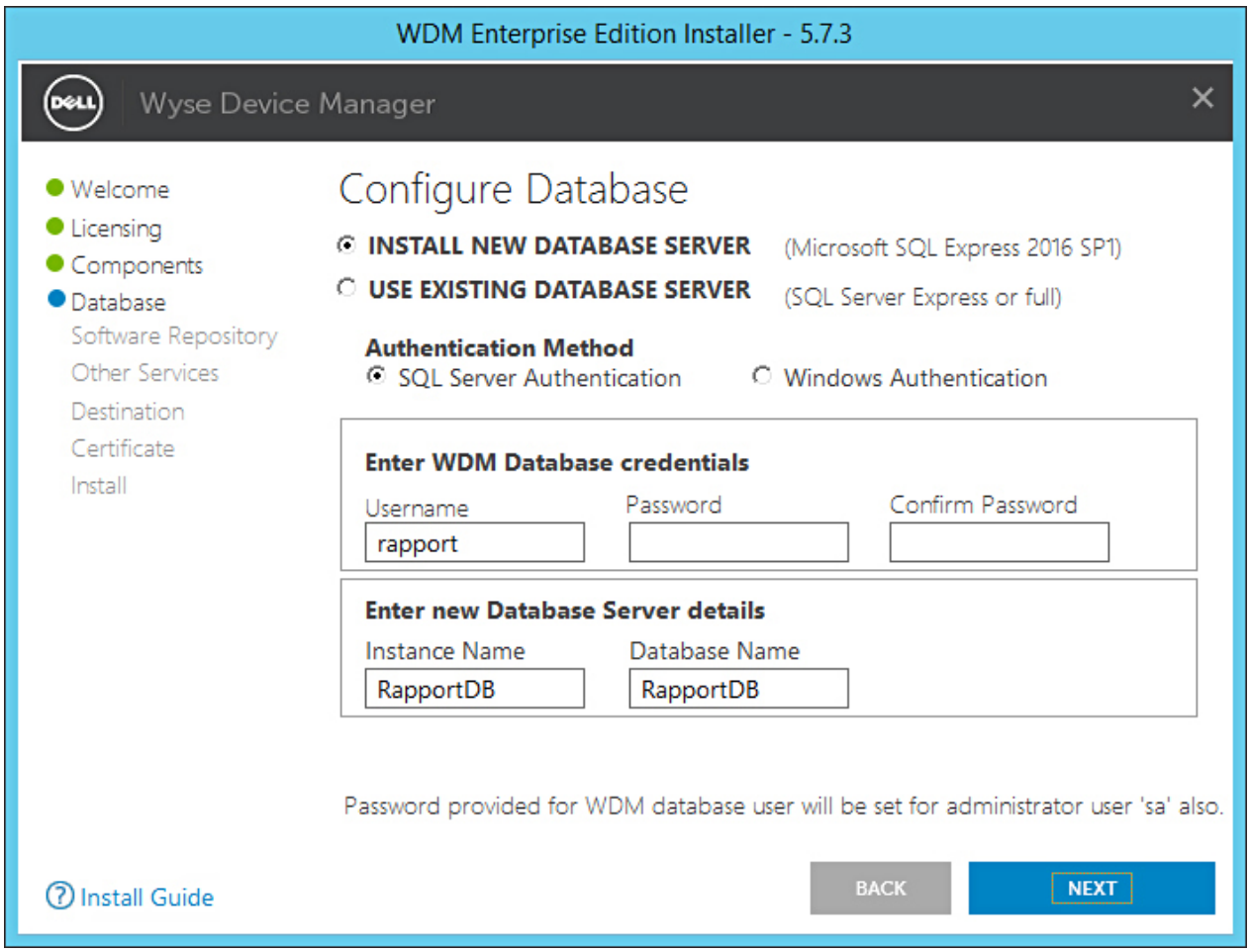


Figure 15. Configurer la base de données

- **Install New Database Server (Installer un nouveau serveur de base de données) (Microsoft SQL Express 2016 SP1)** : sélectionnez cette option si aucune version prise en charge de Microsoft SQL Server n'est installée sur le système. Passez à l'étape 8.
- **Use Existing Database Server (Utiliser le serveur de base de données existant) (SQL Server Express ou Full)** : sélectionnez cette option si une version prise en charge de Microsoft SQL Server est déjà installée sur le système. Si vous sélectionnez cette option, assurez-vous que le serveur de base de données se trouve sur le même système que celui sur lequel vous installez l'édition Workgroup de WDM, et passez à l'étape 9.

8 Si vous avez sélectionné la première option lors de l'étape 7, sélectionnez la méthode d'authentification.

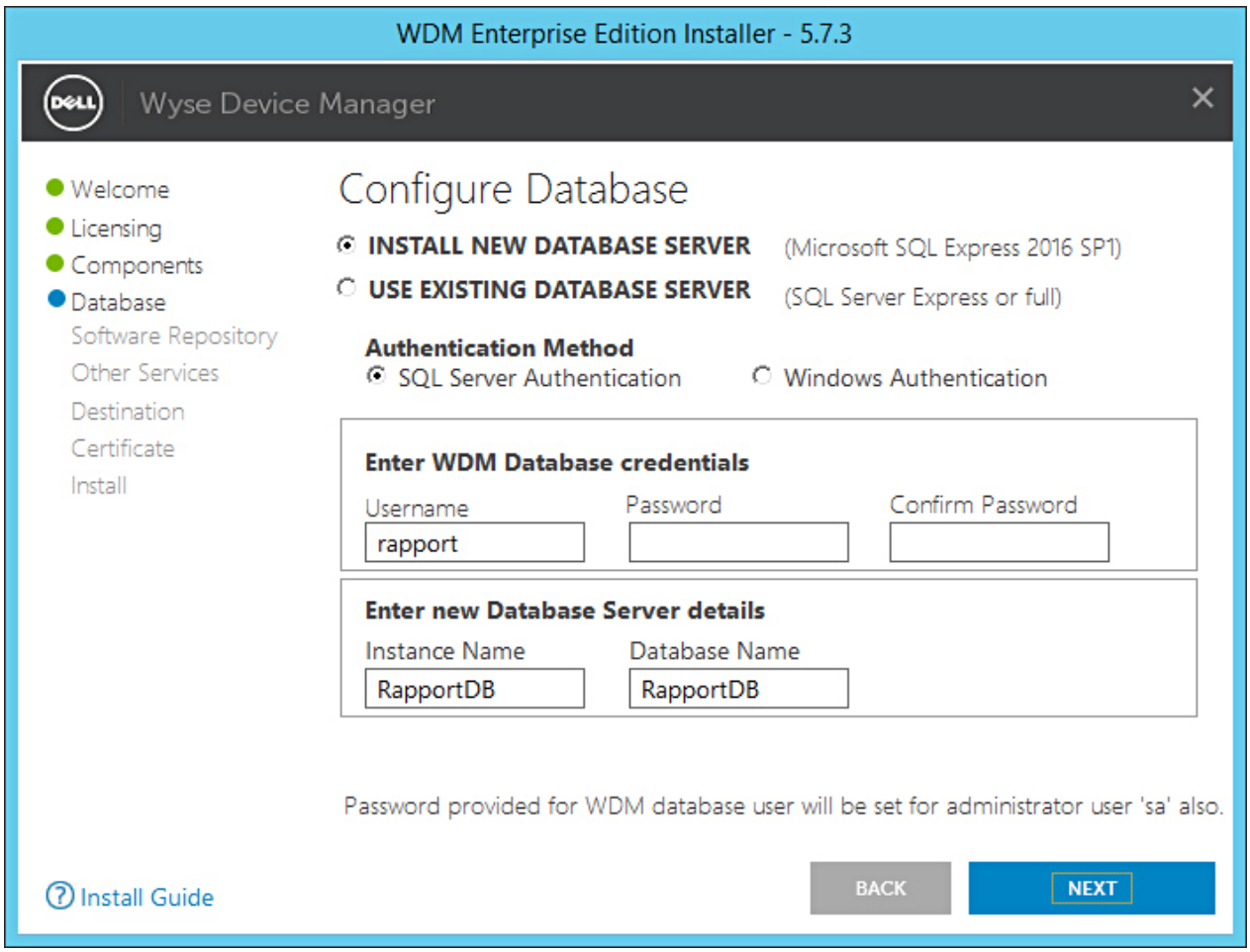


Figure 16. Option Install New Database Server (Installer un nouveau serveur de base de données)

- **SQL Server Authentication** (Authentification du serveur SQL) : cette option est sélectionnée par défaut. Pour configurer l'authentification du serveur SQL, procédez comme suit :
  1. Entrez les informations d'identification de la base de données WDM.
  2. Entrez les informations d'identification de la nouvelle base de données. Vous pouvez entrer le nom de l'instance et le nom de la base de données dans les détails du nouveau serveur de base de données. Le nom d'instance et le nom de la base de données par défaut sont RapportDB.

  REMARQUE : Même si vous choisissez l'authentification Windows, l'installation WDM nécessite l'authentification SQL pour accéder à la base de données SQL. Dans une installation autonome, après avoir terminé l'installation de la base de données WDM, le programme d'installation attribue l'utilisateur Active Directory à la base de données, et le même utilisateur est utilisé pour installer les services WDM.
- **Windows Authentication** (Authentification Windows) : entrez les informations sur le nouveau serveur de base de données. Le nom d'instance et le nom de la base de données par défaut sont RapportDB.

  REMARQUE :
  - Sélectionnez **Windows Authentication** (Authentification Windows) si vous souhaitez vous connecter à la base de données WDM en utilisant vos informations de connexion Windows.
  - Le mot de passe doit correspondre aux règles de complexité du système d'exploitation Windows.

9 Si vous avez sélectionné la seconde option lors de l'étape 7, sélectionnez la méthode d'authentification.

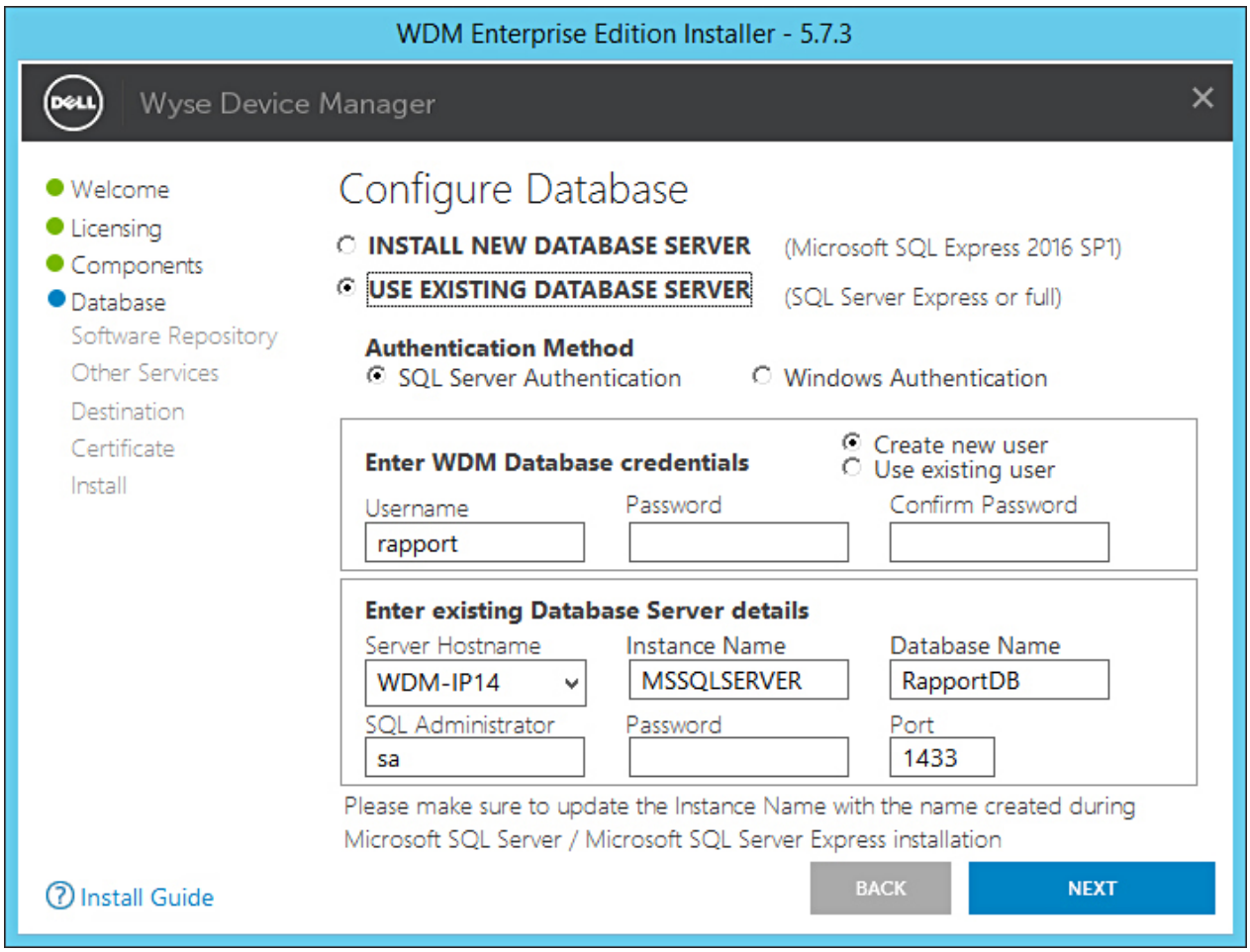


Figure 17. Option Use Existing Database Server (Utiliser le serveur de base de données existant)

- **SQL Server Authentication** (Authentification du serveur SQL) : cette option est sélectionnée par défaut. Pour configurer l'authentification du serveur SQL, procédez comme suit :
  1. Sélectionnez l'option Create new user (Créer un nouvel utilisateur) ou l'option Use the existing user (Utiliser l'utilisateur existant), puis entrez les informations d'identification de la base de données WDM.
  2. Entrez les informations sur le serveur de base de données existant, telles que le nom d'hôte du serveur, le nom de l'instance, le nom de la base de données, le numéro de port et le nom de l'administrateur et le mot de passe SQL.
- **Windows Authentication** (Authentification Windows) : entrez les informations sur le serveur de base de données existant, telles que le nom d'hôte du serveur, le nom de l'instance, le nom de la base de données, le numéro de port et le nom de l'administrateur et le mot de passe SQL.

REMARQUE : Le numéro de port par défaut est 1433. Dell vous recommande de saisir manuellement le numéro de port car il s'agit d'un numéro de port dynamique. Les numéros de port dynamique pour le protocole TCP/UDP vont de 49152 à 65535.

10 Cliquez sur **NEXT** (SUIVANT).

L'écran **Configure Software Repository Server** (Configurer le serveur pour la Logithèque) s'affiche.

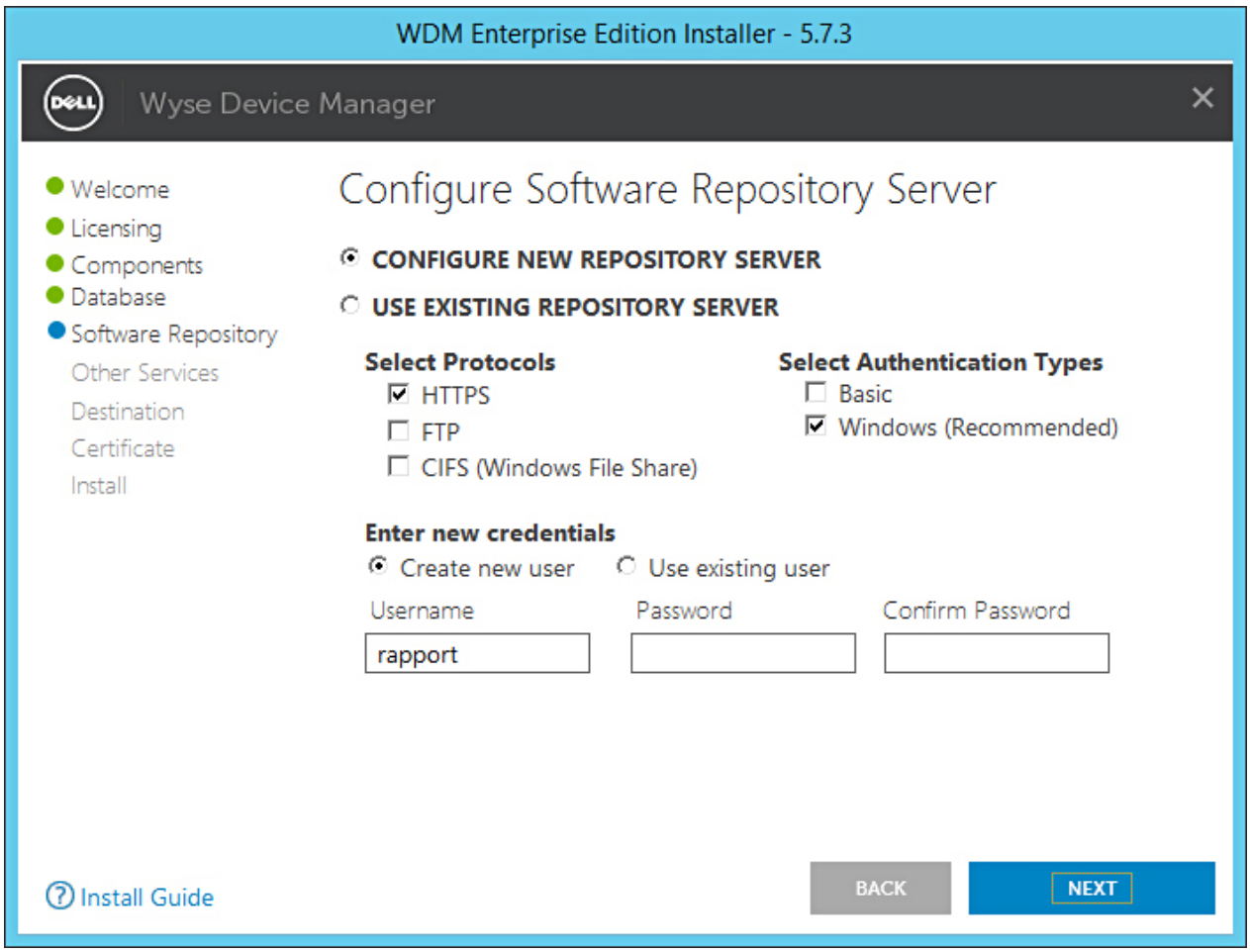


Figure 18. Écran Configure Software Repository Server (Configurer le serveur de référentiel de logiciels)

11 Dans l'écran **Configure Software Repository Server** (Configurer le serveur de référentiel de logiciels), vous pouvez sélectionner l'une des options suivantes :

- **CONFIGURE NEW REPOSITORY SERVER** (CONFIGURER UN NOUVEAU SERVEUR DE RÉFÉRENTIEL) : sélectionnez cette option si vous souhaitez que le programme d'installation configure un nouveau serveur de référentiel. Pour configurer un nouveau serveur de référentiel :
  - Sélectionnez le protocole et les paramètres pour distribuer le logiciel vers les périphériques gérés. **HTTPS** est sélectionné par défaut. Vous pouvez également sélectionner **FTP** pour ThreadX 4.x et **CIFS** pour ThreadX 5.x.
  - Sélectionnez le type d'authentification. **Windows** est sélectionné par défaut.

    REMARQUE : L'authentification de base est requise pour les systèmes Linux.
  - Créez de nouvelles informations d'identification utilisateur ou utilisez des informations d'identification utilisateur existantes.

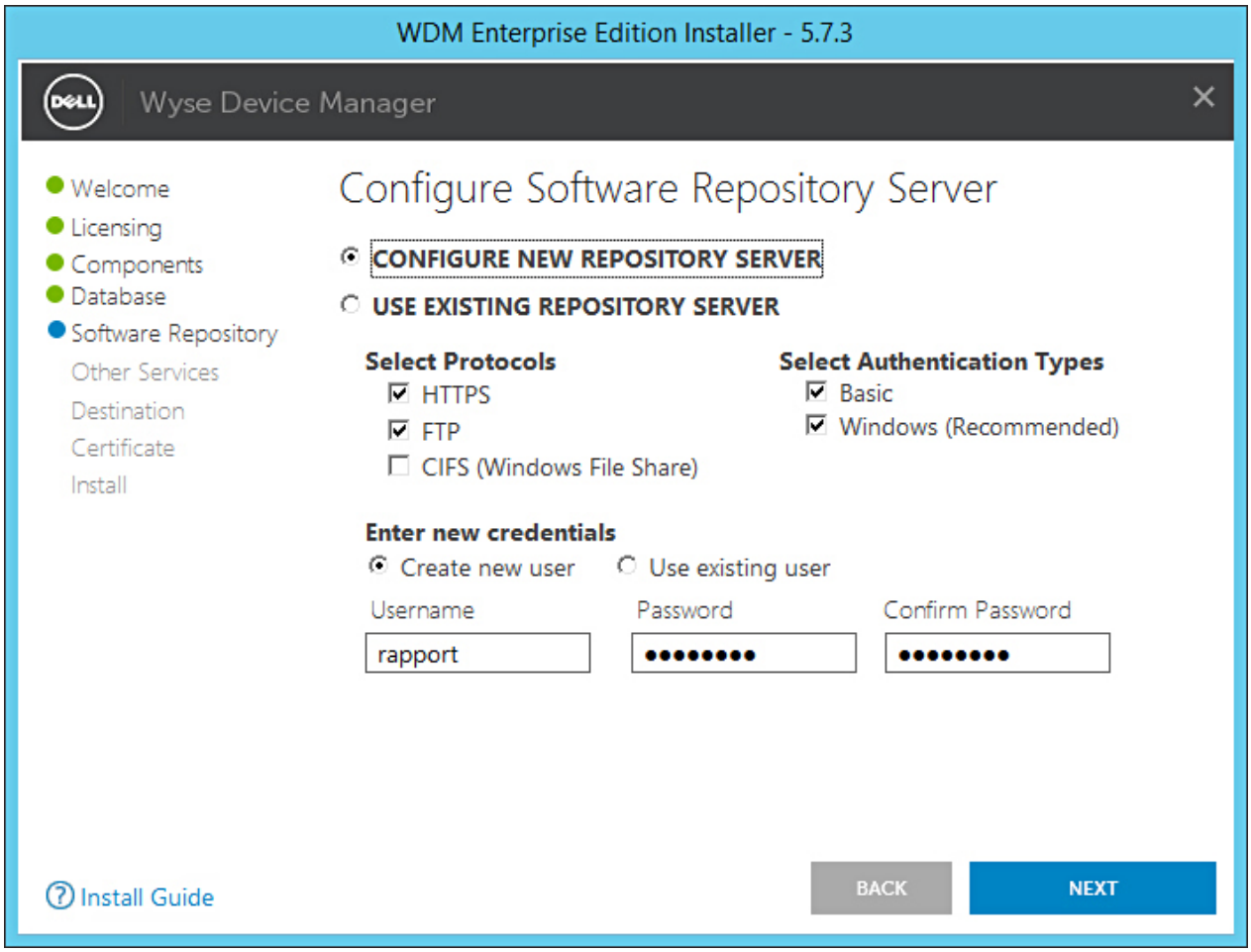


Figure 19. Option CONFIGURE NEW REPOSITORY SERVER (CONFIGURER UN NOUVEAU SERVEUR DE RÉFÉRENTIEL)

- **USE EXISTING REPOSITORY SERVER** (UTLISER UN SERVEUR DE RÉFÉRENTIEL EXISTANT) : sélectionnez cette option si vous souhaitez que le programme d'installation utilise un serveur de référentiel existant. Pour configurer le serveur de référentiel existant :
  - Sélectionnez le protocole et les paramètres pour distribuer le logiciel vers les périphériques gérés. **HTTPS** est sélectionné par défaut. Vous pouvez également sélectionner **FTP** pour ThreadX 4.x et **CIFS** pour ThreadX 5.x.
  - Sélectionnez le type d'authentification. **Windows** est sélectionné par défaut.
  - Saisissez les informations d'identification du serveur. L'option d'adresse IP du serveur est grisée et le nom d'utilisateur par défaut est « rapport ».

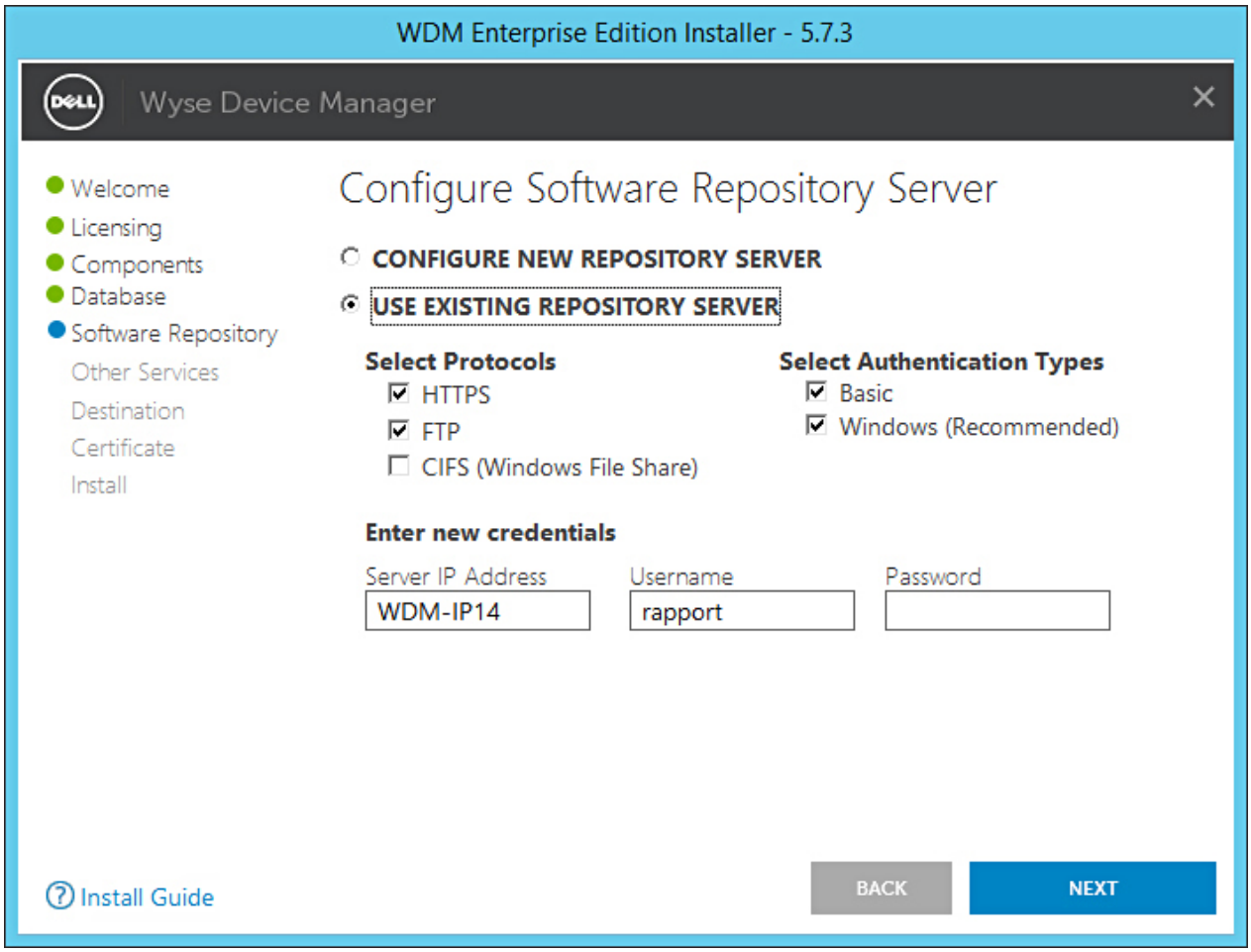


Figure 20. Option USE EXISTING REPOSITORY SERVER (UTILISER LE SERVEUR DE RÉFÉRENTIEL EXISTANT)

12 Cliquez sur **NEXT** (SUIVANT).

13 Sélectionnez les services à installer, puis cliquez sur **NEXT** (SUIVANT).

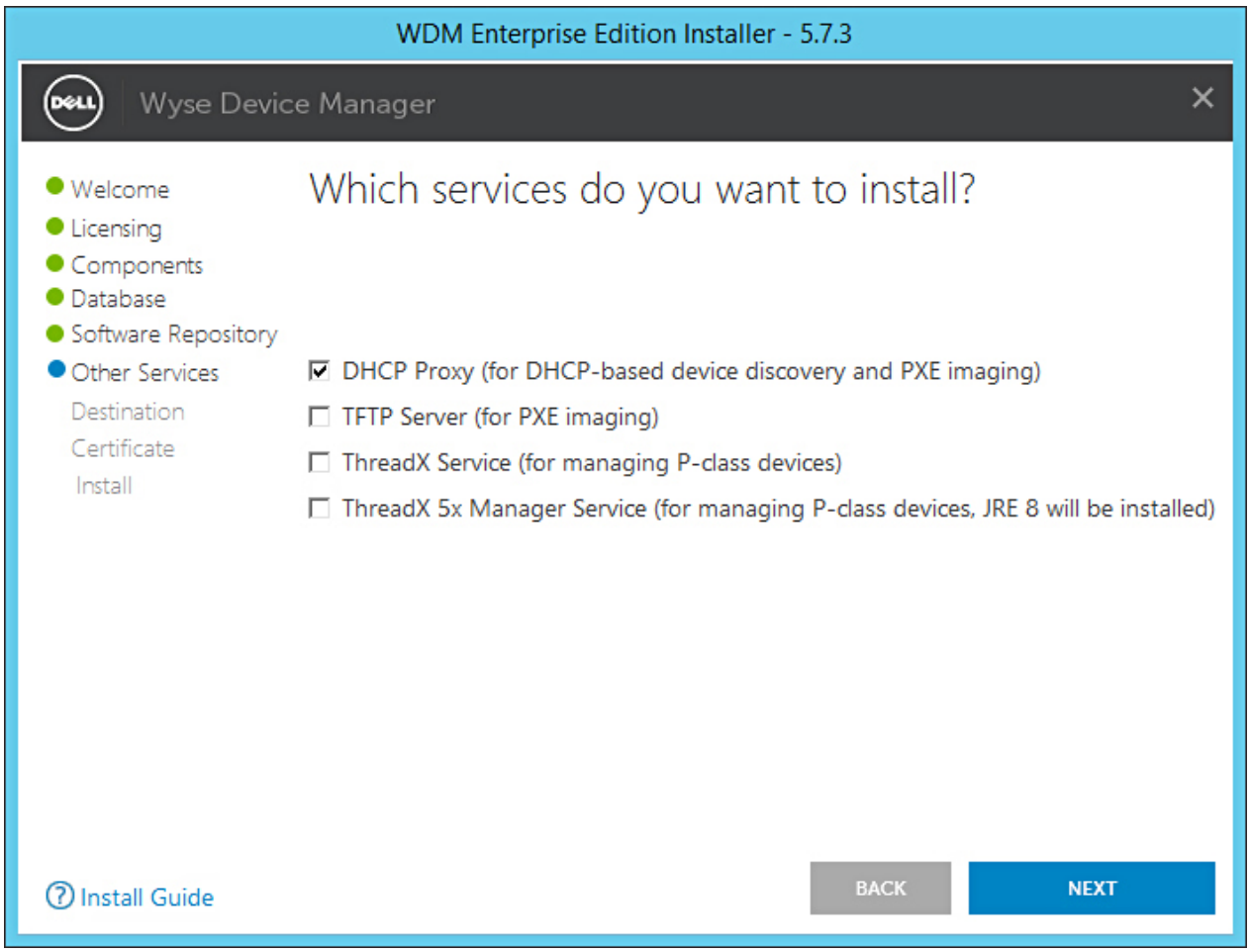


Figure 21. Écran Other Services (Autres services)

REMARQUE : DHCP Proxy (Proxy DHCP) est sélectionné par défaut.

14 Indiquez le chemin d'installation, puis cliquez sur **NEXT** (SUIVANT).

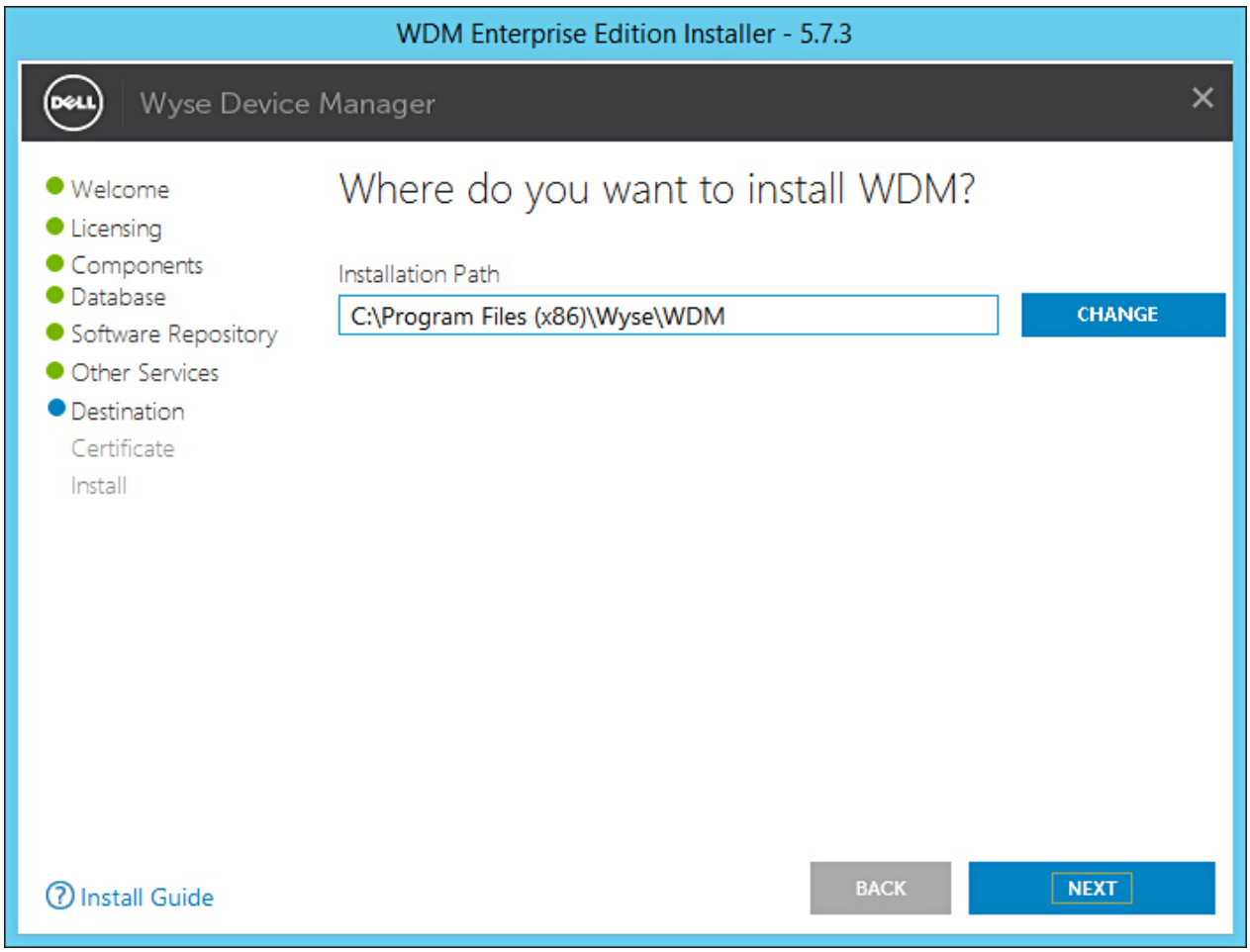


Figure 22. Écran de destination

15 Sélectionnez et importez le certificat pour démarrer l'installation.

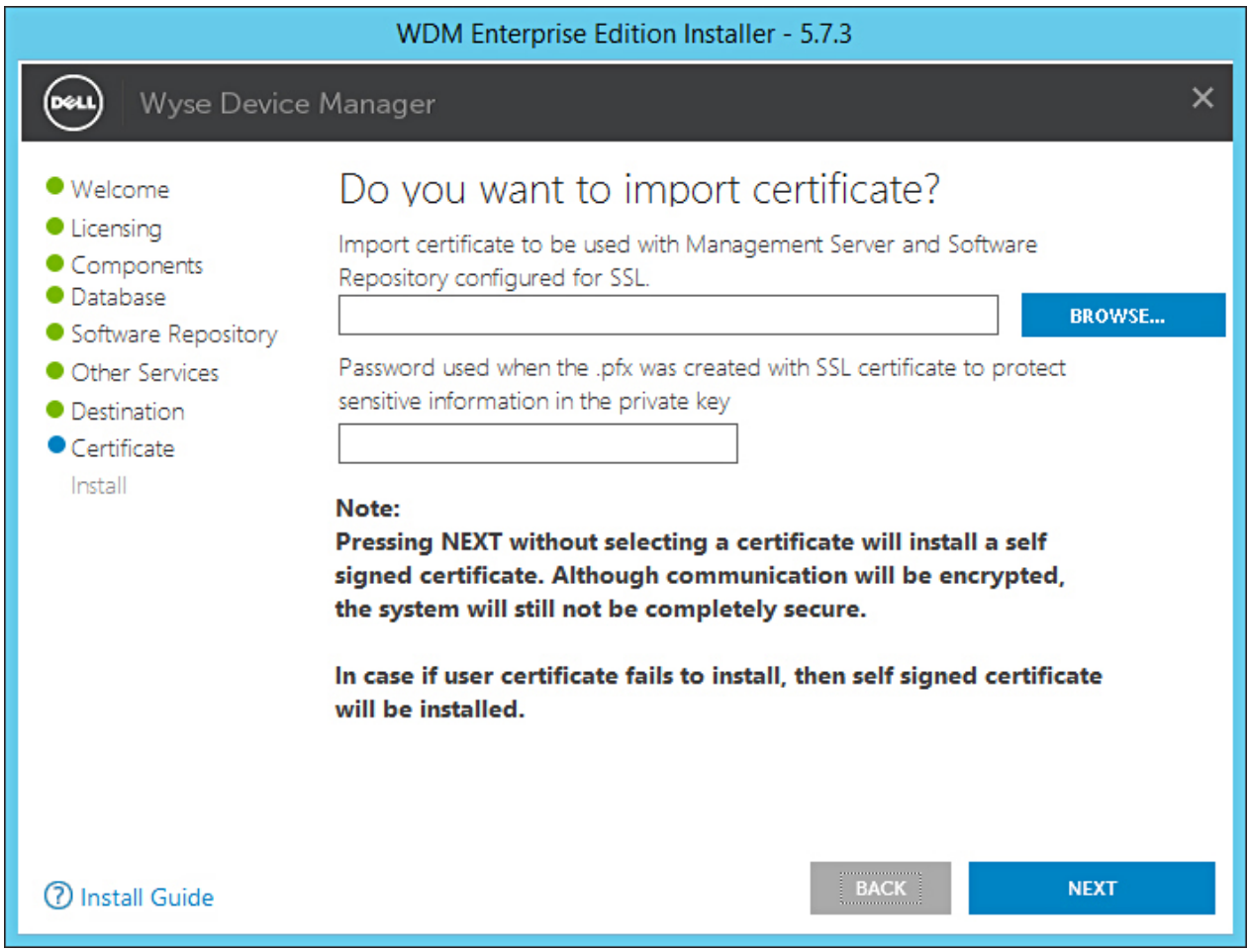


Figure 23. Écran Certificate (Certificat)

REMARQUE : Si vous cliquez sur NEXT (SUIVANT)sans avoir sélectionné de certificat, le programme d'installation installe un certificat auto-signé. Les communications sont chiffrées, mais le système n'est pas totalement sécurisé. Le certificat doit être au format .pfx.

La progression de l'installation s'affiche à l'écran. Une fois l'installation terminée, vous êtes invité à redémarrer votre système.

Figure 24. Écran Installation summary (Résumé de l'installation)

16 Redémarrez le système pour que les modifications prennent effet.

Installation de WDM dans un environnement Cloud

À propos de cette tâche

Pour installer WDM dans un environnement Cloud, vous devez installer l'édition d'entreprise.

Étapes

1 Décompressez le contenu du programme d'installation de WDM sur le système sur lequel vous souhaitez installer WDM.

2 Accédez au dossier dans lequel vous avez extrait le programme d'installation et exécutez Setup.exe.

Le cas échéant, le composant .NET Framework est installé automatiquement sur le serveur.

L'écran **Welcome** (Accueil) s'affiche.

Figure 25. Écran Welcome (Accueil)

3 Cliquez sur **NEXT** (SUIVANT).

4 Dans le type de licence, sélectionnez **ENTERPRISE** (ENTREPRISE).

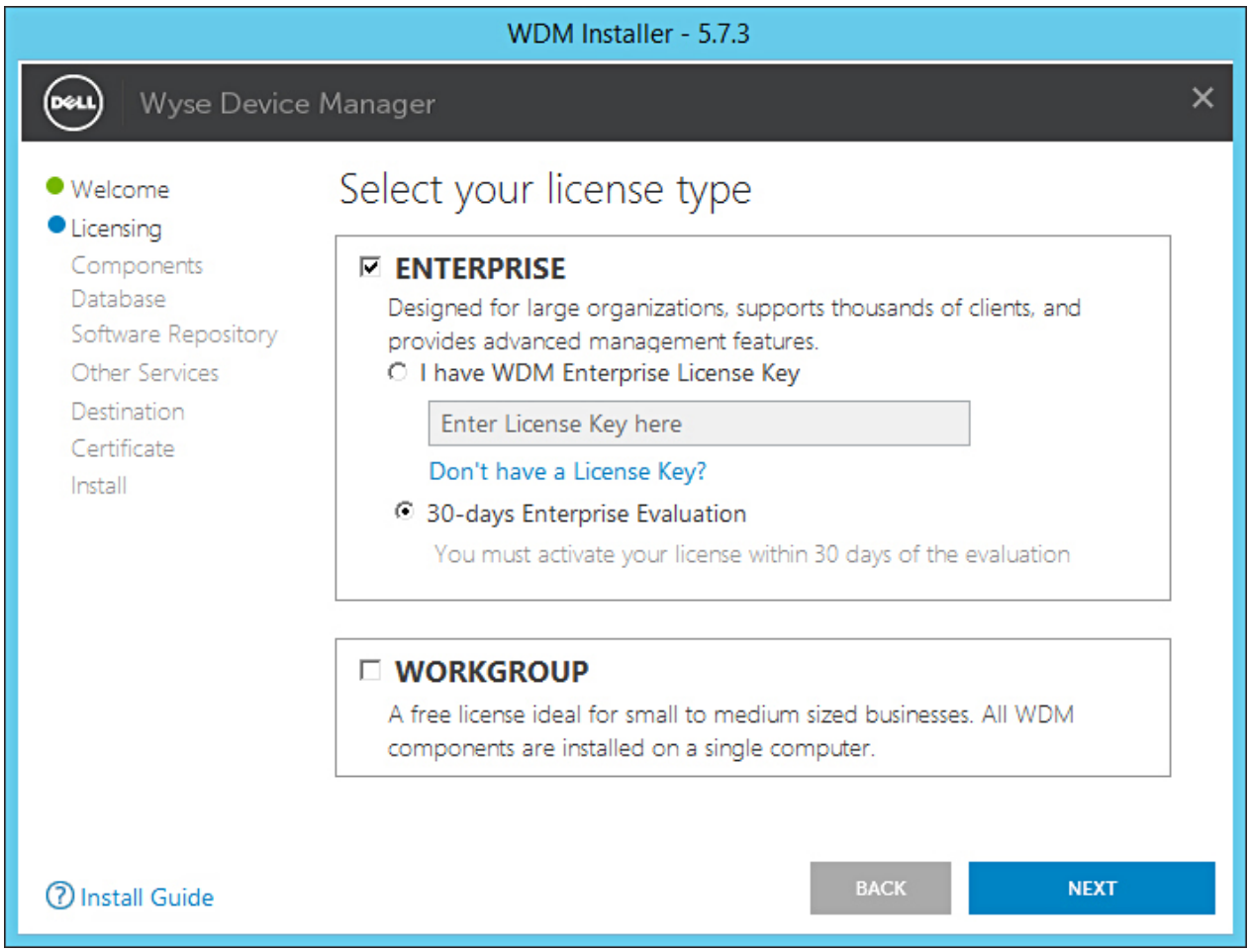


Figure 26. Type de licence Entreprise

a Si vous disposez de la clé de licence WDM, sélectionnez l'option **I have WDM Enterprise License Key** (J'ai une clé de licence Entreprise WDM), puis saisissez la clé de licence dans l'espace prévu à cet effet.

b Si vous ne disposez pas de la clé de licence, sélectionnez l'option **30–days Enterprise Evaluation** (30 jours d'essai de l'édition Entreprise).

La clé de licence est saisie par défaut. Cependant, après la période d'évaluation de 30 jours, vous devez obtenir la clé de licence et l'ajouter à WDM. Pour plus d'informations sur l'ajout de la clé de licence, consultez le *Dell Wyse Device Manager Administrator's Guide (Guide de l'aministrateur de Dell Wyse Device Manager)*.

5 Cliquez sur **NEXT** (SUIVANT).

6 Sélectionnez les composants à installer, puis cliquez sur **NEXT** (SUIVANT).

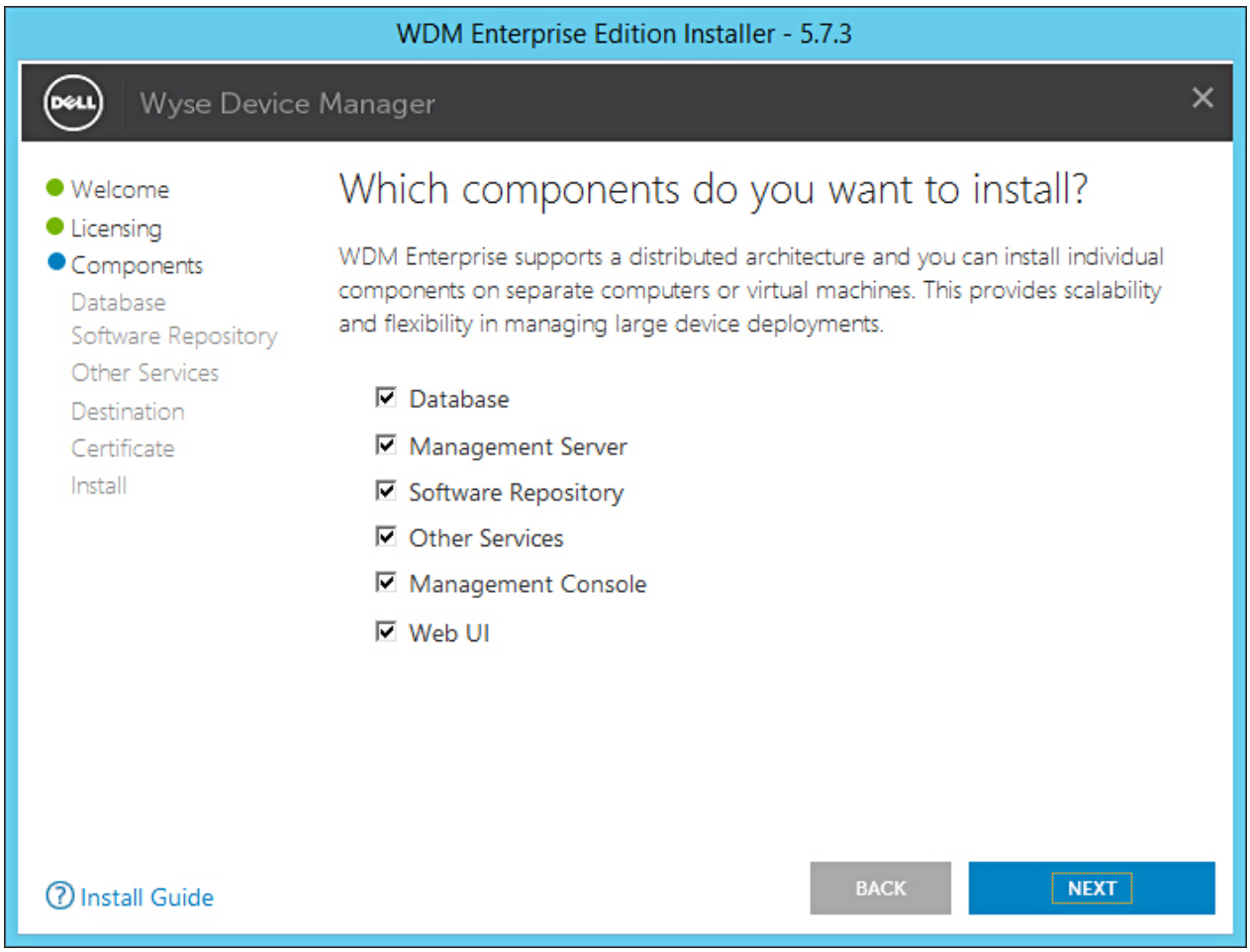


Figure 27. Écran Components (Composants)

Vous pouvez installer tous les composants sur le même système ou chaque composant sur un système différent.

REMARQUE : Si vous installez les composants séparément sur différents systèmes, assurez-vous d'installer la base de données en premier, sans quoi, vous ne pourrez pas installer les autres composants.

7 Dans l'écran **Configure Database** (Configurer la base de données), sélectionnez l'une des options suivantes :

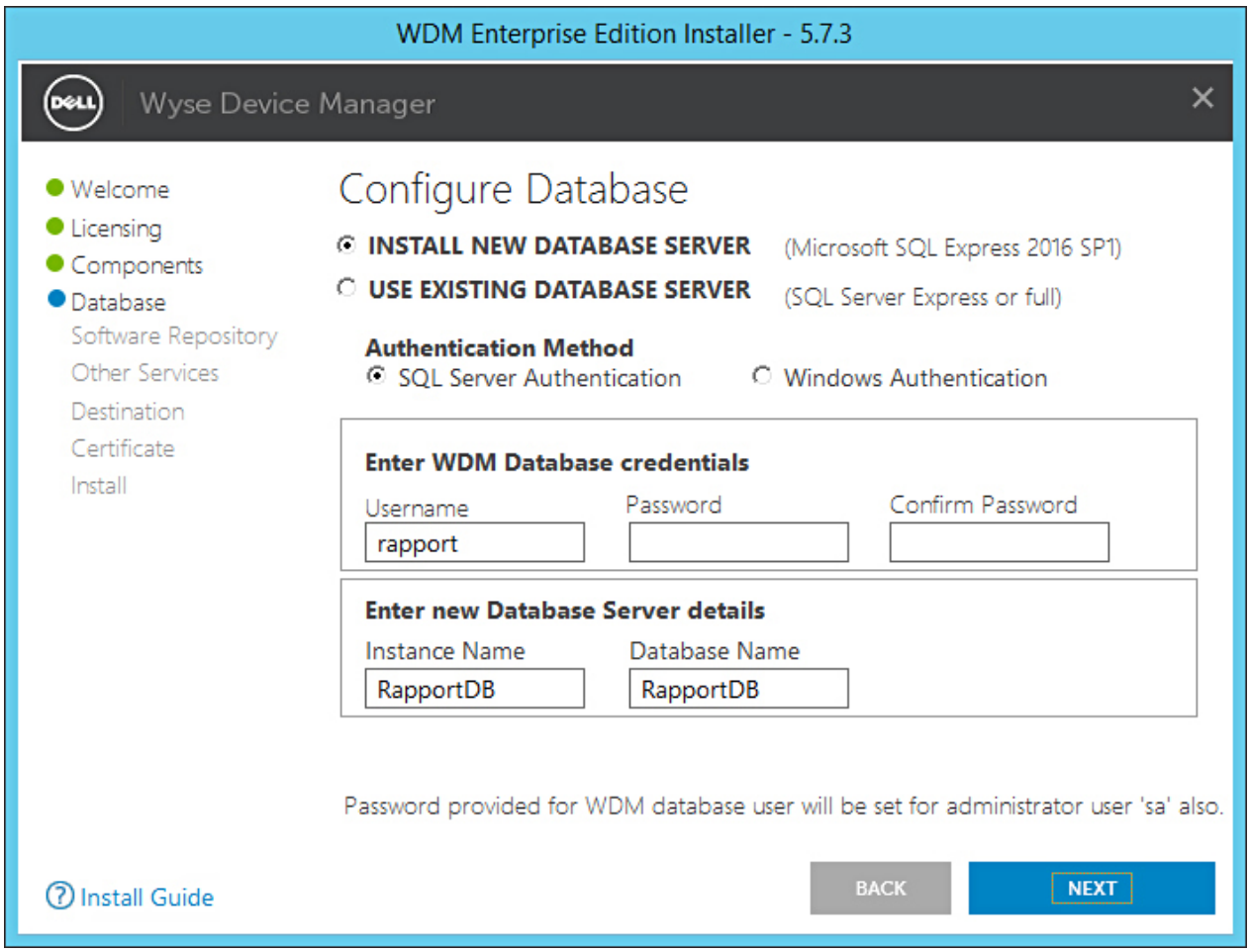


Figure 28. Configurer la base de données

- **Install New Database Server (Installer un nouveau serveur de base de données) (Microsoft SQL Express 2016 SP1)** : sélectionnez cette option si aucune version prise en charge de Microsoft SQL Server n'est installée sur le système. Passez à l'étape 8.
- **Use Existing Database Server (Utiliser le serveur de base de données existant) (SQL Server Express ou Full)** : sélectionnez cette option si une version prise en charge de Microsoft SQL Server est déjà installée sur le système. Si vous sélectionnez cette option, assurez-vous que le serveur de base de données se trouve sur le même système que celui sur lequel vous installez l'édition Workgroup de WDM, et passez à l'étape 9.

8 Si vous avez sélectionné la première option lors de l'étape 7, sélectionnez la méthode d'authentification.

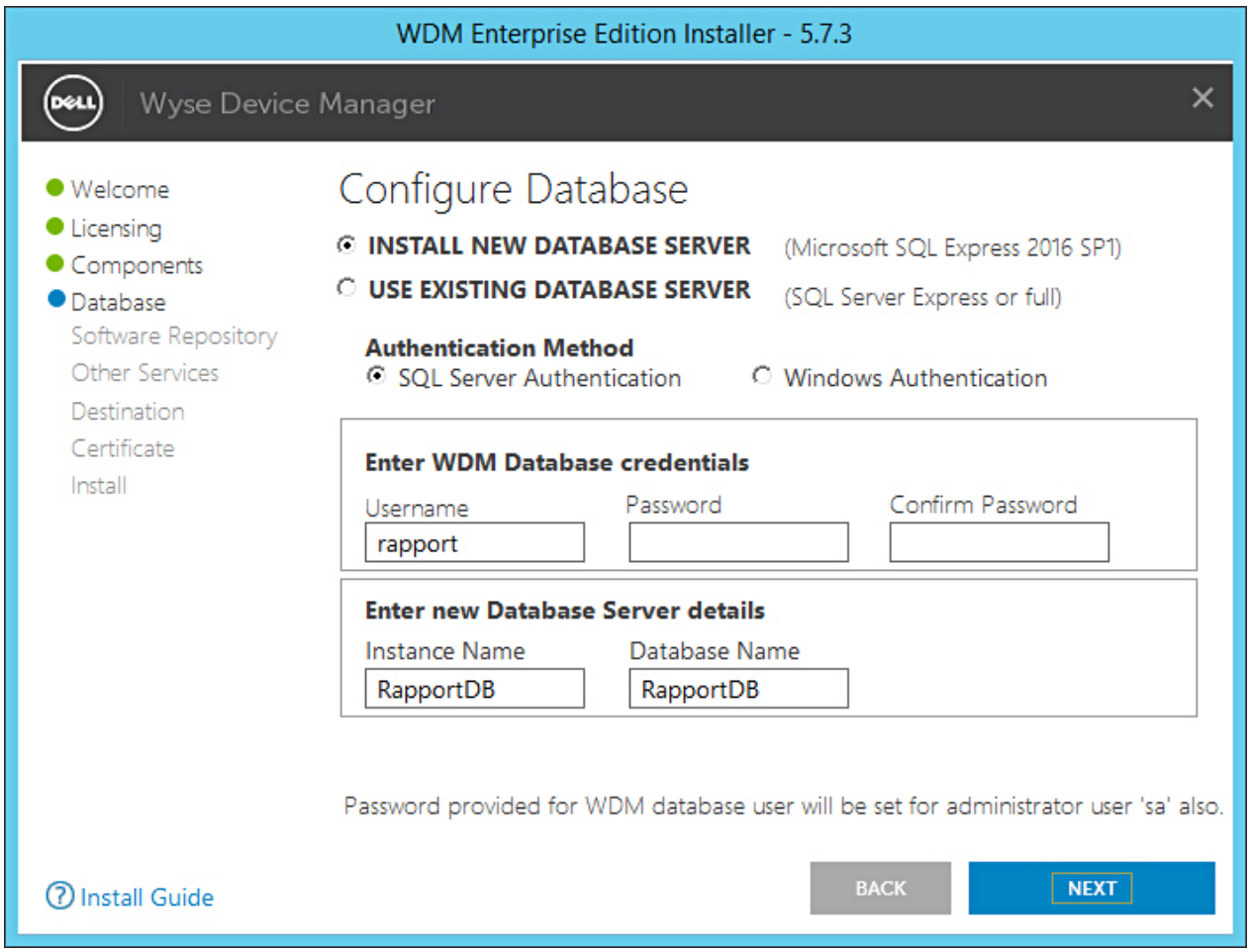


Figure 29. Option Install New Database Server (Installer un nouveau serveur de base de données)

- **SQL Server Authentication** (Authentification du serveur SQL) : cette option est sélectionnée par défaut. Pour configurer l'authentification du serveur SQL, procédez comme suit :
  1. Entrez les informations d'identification de la base de données WDM.
  2. Entrez les informations d'identification de la nouvelle base de données. Vous pouvez entrer le nom de l'instance et le nom de la base de données dans les détails du nouveau serveur de base de données. Le nom d'instance et le nom de la base de données par défaut sont RapportDB.

REMARQUE : Même si vous choisissez l'authentification Windows, l'installation WDM nécessite l'authentification SQL pour accéder à la base de données SQL. Dans une installation autonome, après avoir terminé l'installation de la base de données WDM, le programme d'installation attribue l'utilisateur Active Directory à la base de données, et le même utilisateur est utilisé pour installer les services WDM.

- **Windows Authentication** (Authentification Windows) : entrez les informations sur le nouveau serveur de base de données. Le nom d'instance et le nom de la base de données par défaut sont RapportDB.

REMARQUE :

- Sélectionnez **Windows Authentication** (Authentification Windows) si vous souhaitez vous connecter à la base de données WDM en utilisant vos informations de connexion Windows.
- Le mot de passe doit correspondre aux règles de complexité du système d'exploitation Windows.

9 Si vous avez sélectionné la seconde option lors de l'étape 7, sélectionnez la méthode d'authentification.

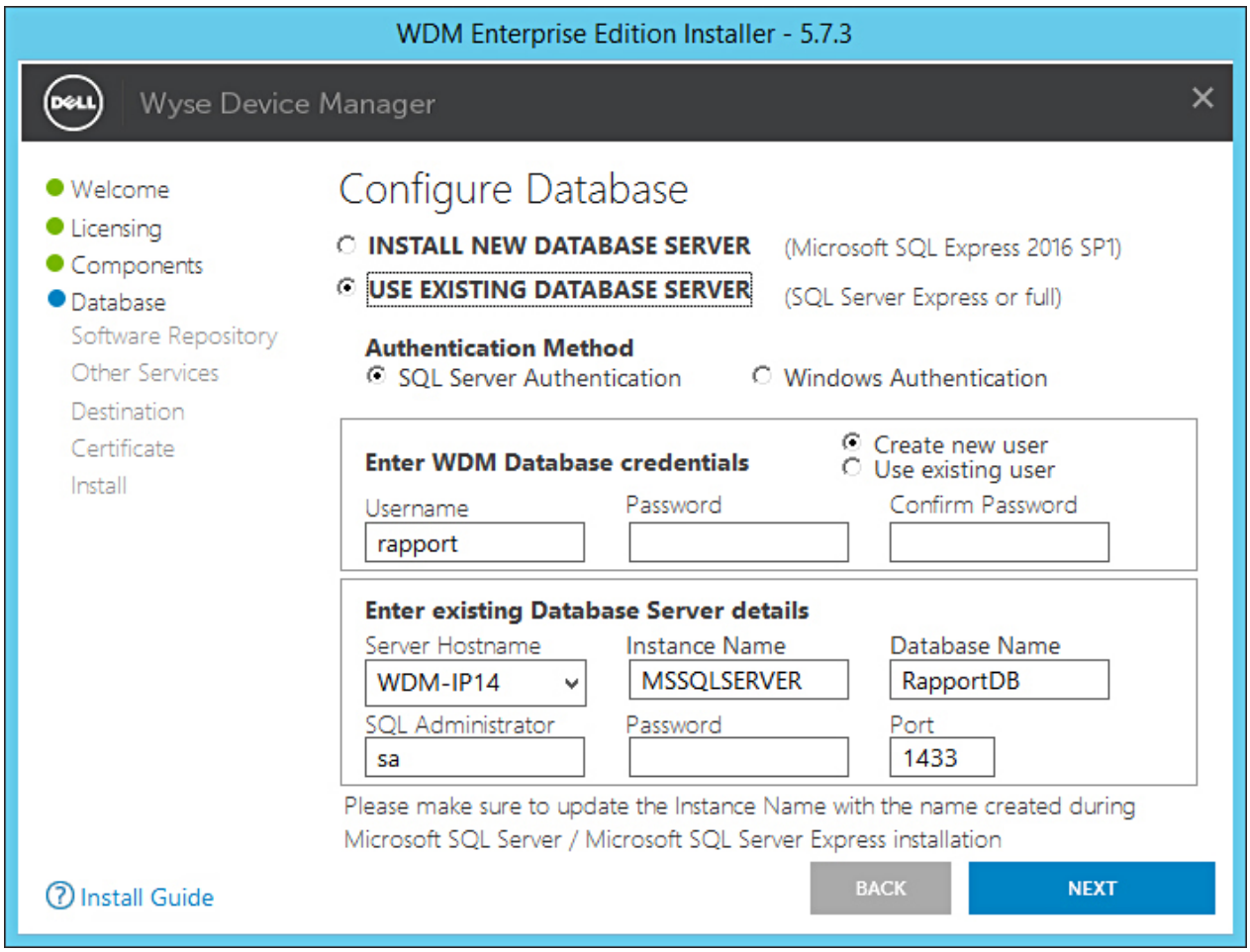


Figure 30. Option Use Existing Database Server (Utiliser le serveur de base de données existant)

- **SQL Server Authentication** (Authentification du serveur SQL) : cette option est sélectionnée par défaut. Pour configurer l'authentification du serveur SQL, procédez comme suit :
  1. Sélectionnez l'option Create new user (Créer un nouvel utilisateur) ou l'option Use the existing user (Utiliser l'utilisateur existant), puis entrez les informations d'identification de la base de données WDM.
  2. Entrez les informations sur le serveur de base de données existant, telles que le nom d'hôte du serveur, le nom de l'instance, le nom de la base de données, le numéro de port et le nom de l'administrateur et le mot de passe SQL.
- **Windows Authentication** (Authentification Windows) : entrez les informations sur le serveur de base de données existant, telles que le nom d'hôte du serveur, le nom de l'instance, le nom de la base de données, le numéro de port et le nom de l'administrateur et le mot de passe SQL.

REMARQUE : Le numéro de port par défaut est 1433. Dell vous recommande de saisir manuellement le numéro de port car il s'agit d'un numéro de port dynamique. Les numéros de port dynamique pour le protocole TCP/UDP vont de 49152 à 65535.

10 Cliquez sur **NEXT** (SUIVANT).

L'écran **Configure Software Repository Server** (Configurer le serveur pour la Logithèque) s'affiche.

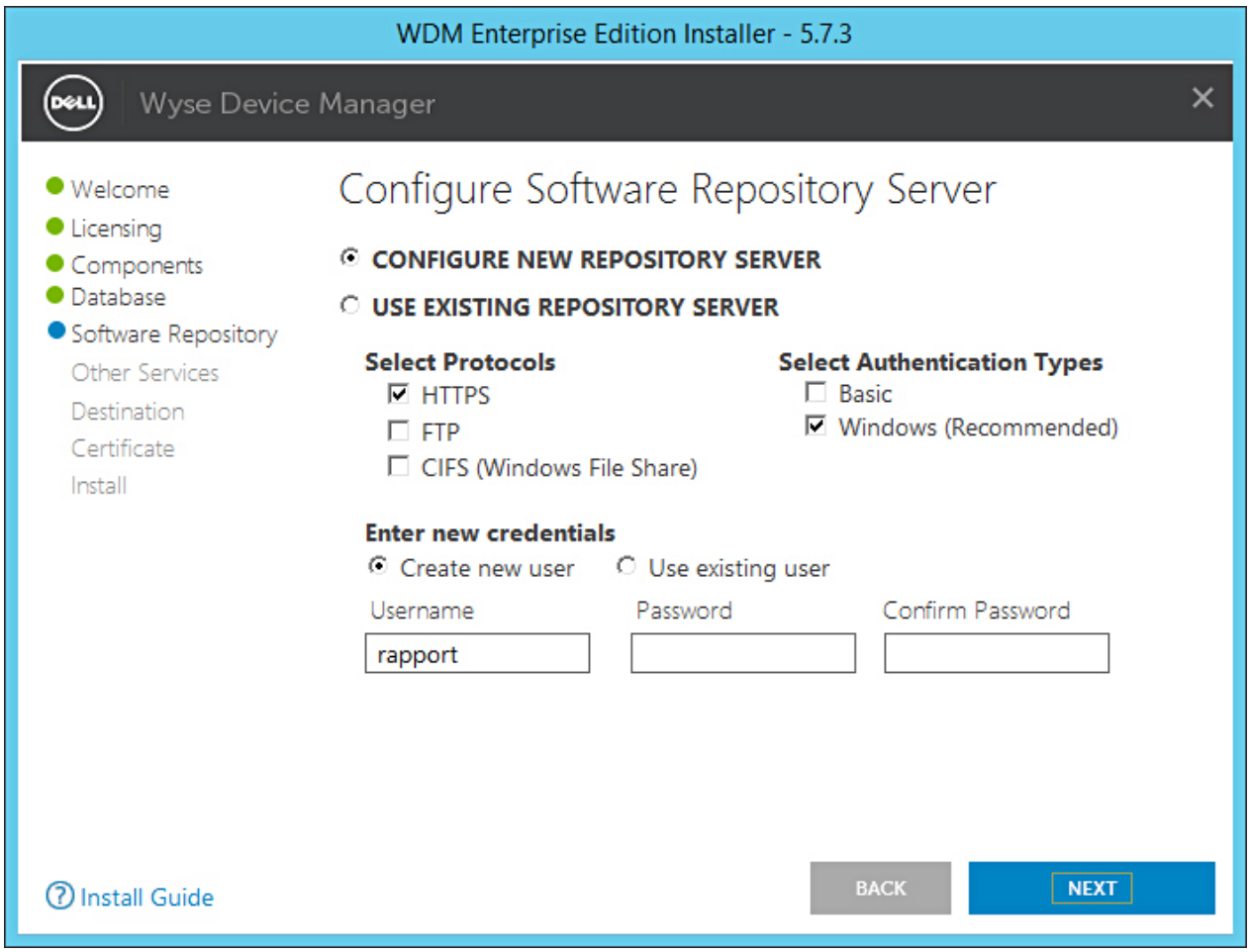


Figure 31. Écran Configure Software Repository Server (Configurer le serveur de référentiel de logiciels)

11 Dans l'écran **Configure Software Repository Server** (Configurer le serveur de référentiel de logiciels), vous pouvez sélectionner l'une des options suivantes :

- **CONFIGURE NEW REPOSITORY SERVER** (CONFIGURER UN NOUVEAU SERVEUR DE RÉFÉRENTIEL) : sélectionnez cette option si vous souhaitez que le programme d'installation configure un nouveau serveur de référentiel. Pour configurer un nouveau serveur de référentiel :
  - Sélectionnez le protocole et les paramètres pour distribuer le logiciel vers les périphériques gérés. **HTTPS** est sélectionné par défaut. Vous pouvez également sélectionner **FTP** pour ThreadX 4.x et **CIFS** pour ThreadX 5.x.
  - Sélectionnez le type d'authentification. **Windows** est sélectionné par défaut.

    REMARQUE : L'authentification de base est requise pour Linux.
  - Créez de nouvelles informations d'identification utilisateur ou utilisez des informations d'identification utilisateur existantes.

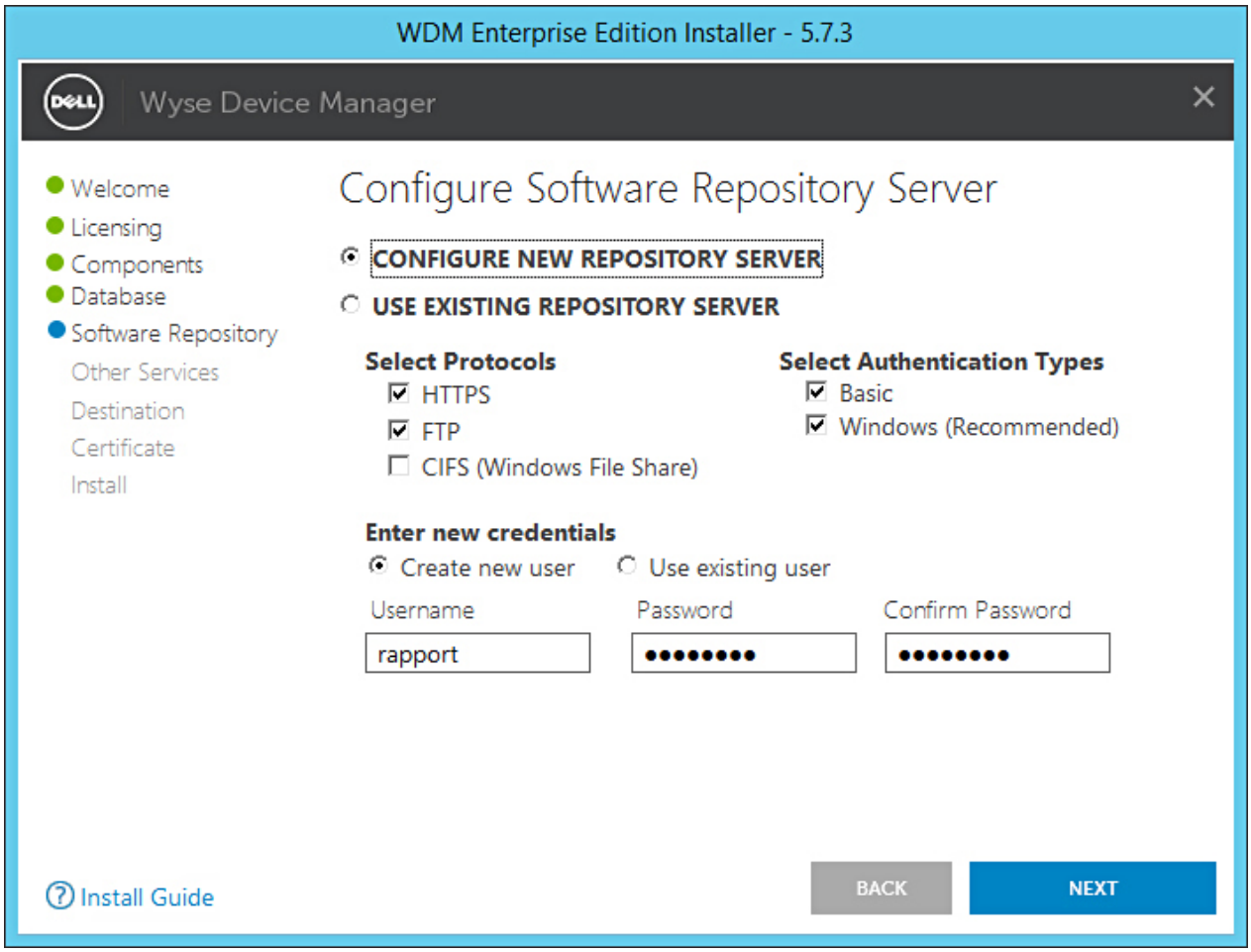


Figure 32. Option CONFIGURE NEW REPOSITORY SERVER (CONFIGURER UN NOUVEAU SERVEUR DE RÉFÉRENTIEL)

- **USE EXISTING REPOSITORY SERVER** (UTLISER UN SERVEUR DE RÉFÉRENTIEL EXISTANT) : sélectionnez cette option si vous souhaitez que le programme d'installation utilise un serveur de référentiel existant. Pour configurer le serveur de référentiel existant :
  - Sélectionnez le protocole et les paramètres pour distribuer le logiciel vers les périphériques gérés. **HTTPS** est sélectionné par défaut. Vous pouvez également sélectionner **FTP** pour ThreadX 4.x et **CIFS** pour ThreadX 5.x.
  - Sélectionnez le type d'authentification. **Windows** est sélectionné par défaut.
  - Saisissez les informations d'identification du serveur. L'option d'adresse IP du serveur est grisée et le nom d'utilisateur par défaut est « rapport ».

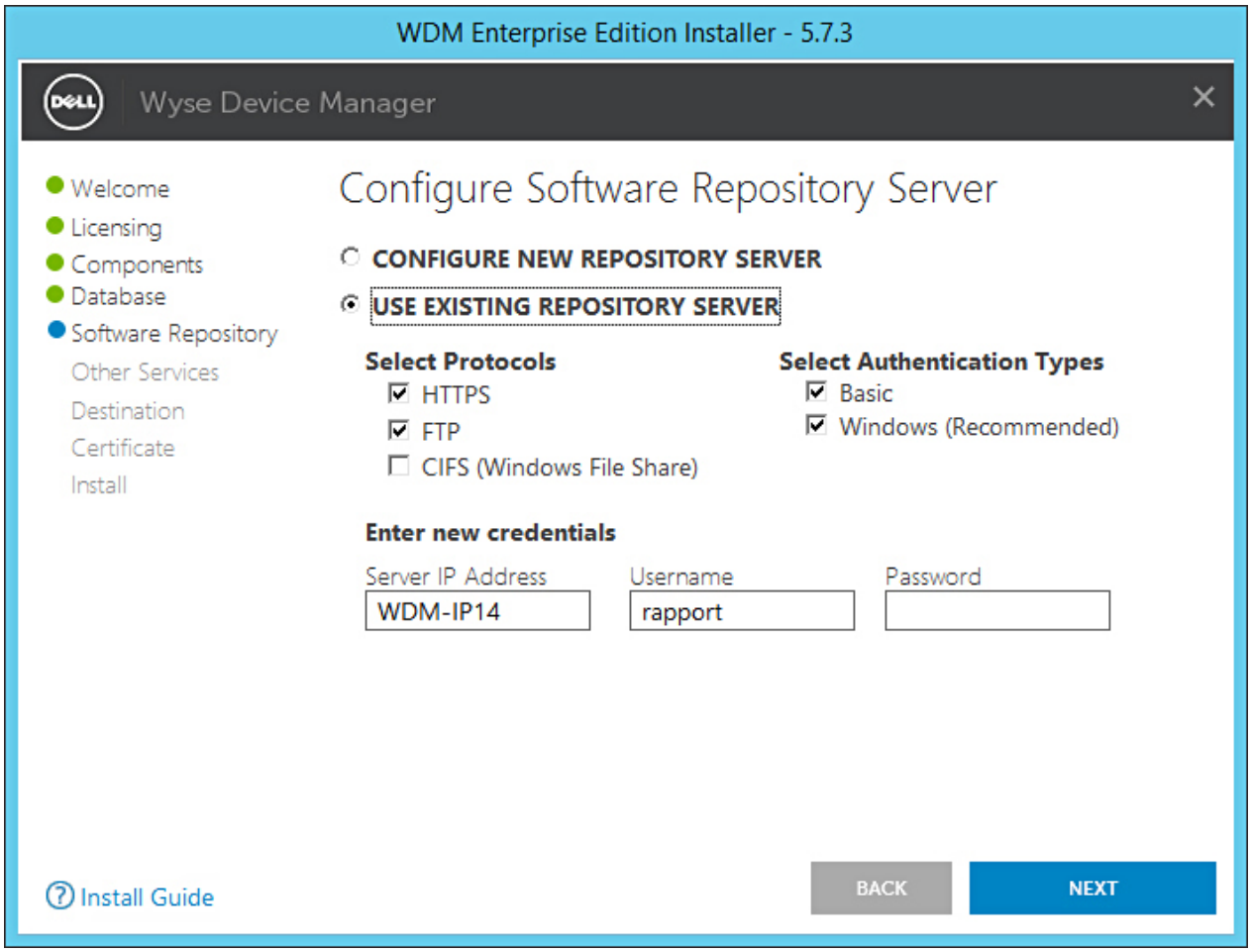


Figure 33. Option USE EXISTING REPOSITORY SERVER (UTILISER LE SERVEUR DE RÉFÉRENTIEL EXISTANT)

12 Cliquez sur **NEXT** (SUIVANT).

13 Sélectionnez les services à installer, puis cliquez sur **NEXT** (SUIVANT).

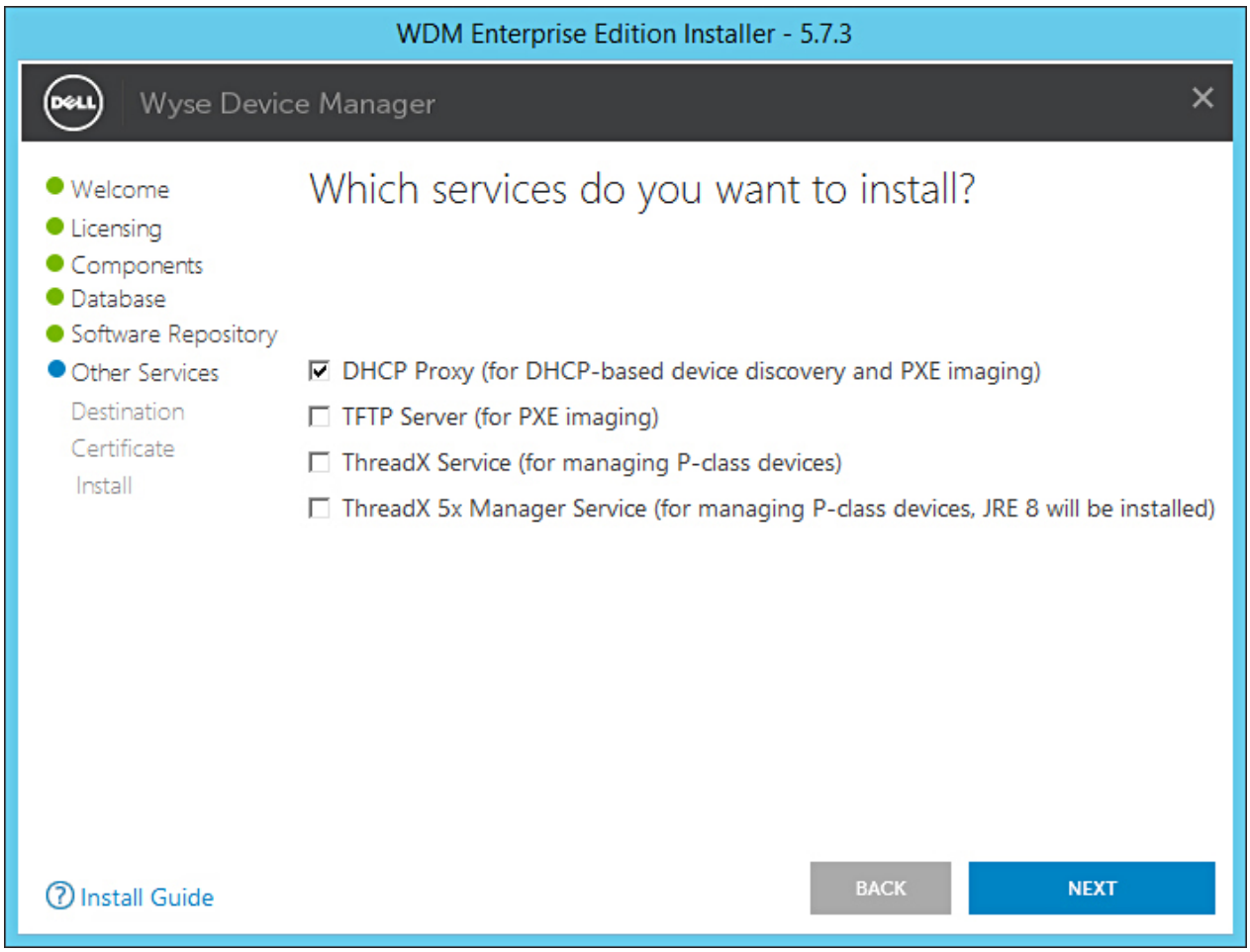


Figure 34. Écran Other Services (Autres services)

REMARQUE : DHCP Proxy (Proxy DHCP) est sélectionné par défaut.

14 Indiquez le chemin d'installation, puis cliquez sur **NEXT** (SUIVANT).

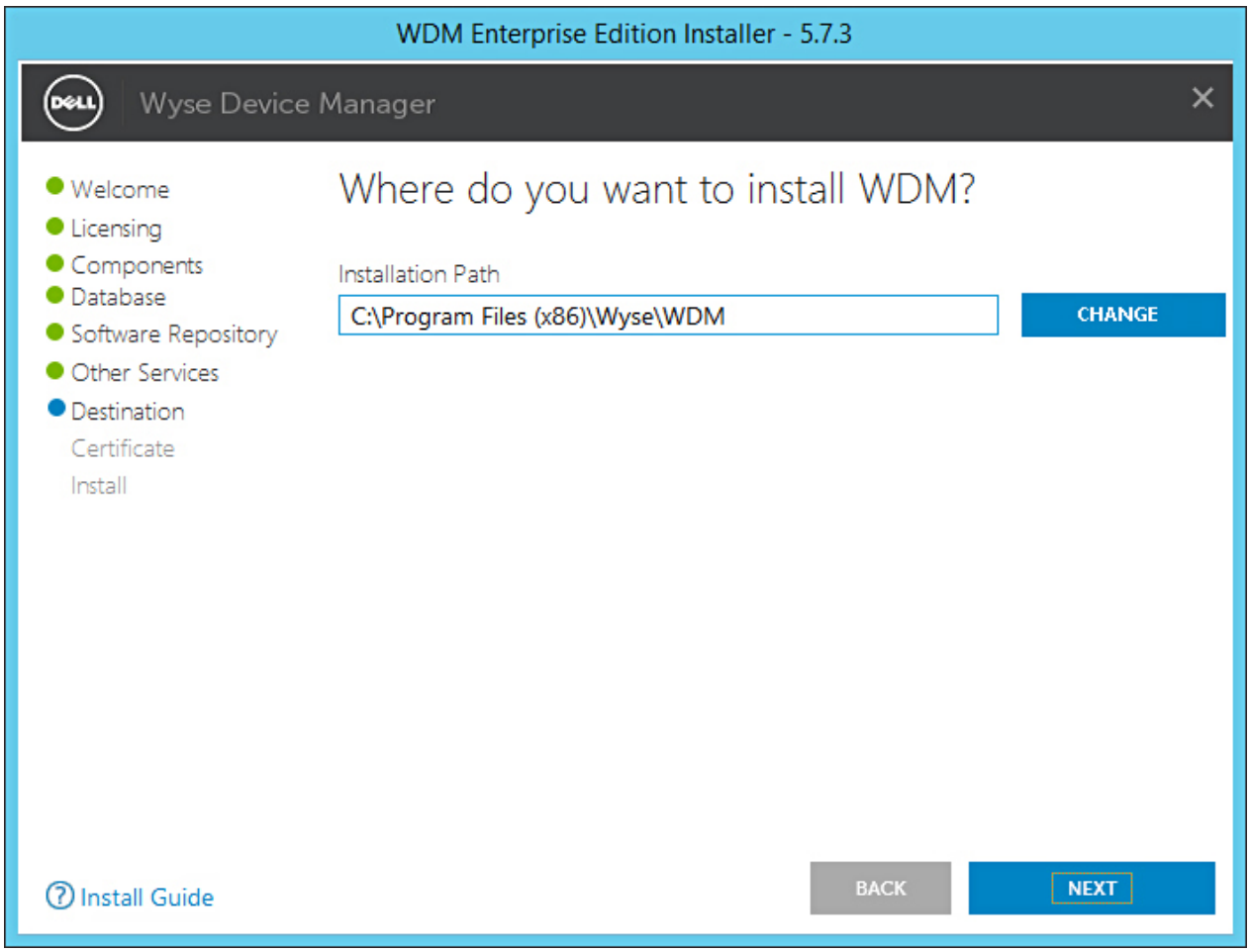


Figure 35. Écran de destination

15 Sélectionnez et importez le certificat pour démarrer l'installation.

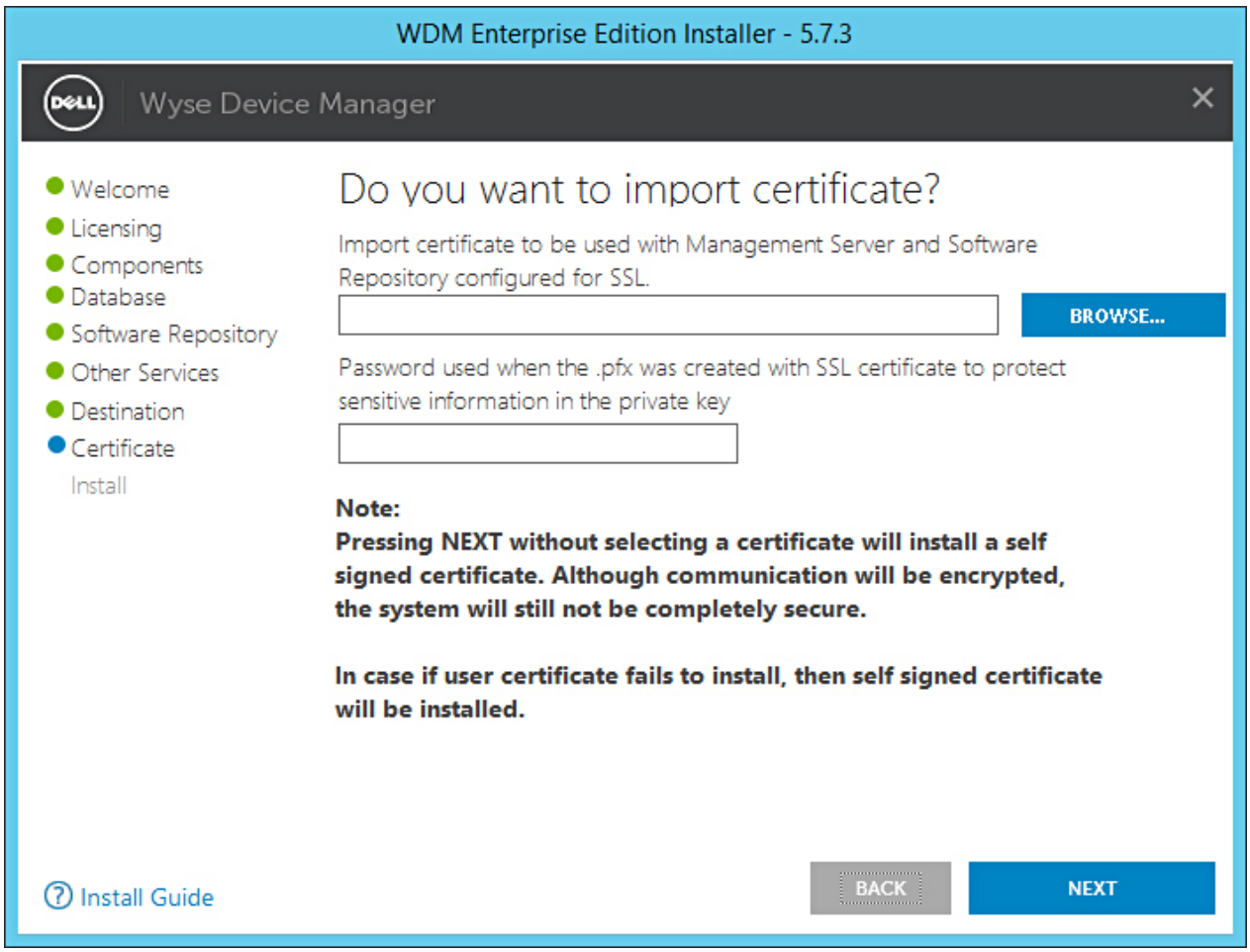


Figure 36. Écran Certificate (Certificat)

REMARQUE : Si vous cliquez sur NEXT (SUIVANT) sans avoir sélectionné de certificat, le programme d'installation installe un certificat auto-signé. Les communications sont chiffrées, mais le système n'est pas totalement sécurisé. Le certificat doit être au format de fichier .pfx.

La progression de l'installation s'affiche à l'écran. Une fois l'installation terminée, vous êtes invité à redémarrer votre système.

Figure 37. Écran Installation summary (Résumé de l'installation)

16 Redémarrez le système pour que les modifications prennent effet.

Installation de WDM dans une configuration distribuée

Vous pouvez diviser les composants WDM et les installer sur différents systèmes. Cette configuration est appelée une configuration distribuée de WDM. Il est préférable de fractionner les composants comme suit :

- Base de données WDM
- Serveur de gestion WDM, Console de gestion WDM et autres services
- Logithèque WDM
- Interface utilisateur Web

Vous pouvez également avoir plusieurs instances du serveur de gestion WDM et d'autres services installés sur différents systèmes pour permettre l'équilibrage de charge. Pour plus d'informations, voir Configuration de la fonction d'équilibrage de charge.

Installer WDM dans une configuration distribuée est particulièrement indiqué pour les grandes entreprises, où de très nombreux appareils doivent être gérés. Cette section décrit en détail les étapes suivantes :

- Installation de la base de données WDM.
- Installation du serveur de gestion et de l'interface utilisateur Web.
- Installation de la Logithèque.

Installation de la base de données WDM

Prérequis

Avant d'installer la base de données WDM sur un système ou une machine virtuelle (VM), assurez-vous que vous avez installé la version prise en charge de Microsoft SQL Server. Si vous ne disposez pas de SQL Server sur le système, vous pouvez choisir d'installer Microsoft SQL Express 2016 SP1, qui est fourni avec le programme d'installation de WDM.

REMARQUE :

Si vous installez la base de données de WDM sur une base de données SQL Server existante, assurez-vous que le port 1433 est disponible sur le système.

Pour installer la base de données de WDM, vous devez sélectionner **Database (Base de données)** dans l'écran **Components (Composants)** avant de poursuivre l'installation.

Étapes

1 Extrayez le contenu du programme d'installation WDM vers le système sur lequel vous souhaitez installer WDM.

2 Accédez au dossier dans lequel vous avez extrait le programme d'installation et exécutez **Setup.exe**.

Si le serveur ne dispose pas de .Net framework, celui-ci est installé automatiquement.

L'écran Welcome (Accueil) s'affiche.

3 Cliquez sur **NEXT (SUIVANT)**.

4 Dans Type de licence, sélectionnez **ENTERPRISE (ENTREPRISE)**.

a Si vous disposez de la clé de licence WDM, sélectionnez l'option **I have WDM Enterprise License Key (J'ai une clé de licence Entreprise WDM)**, puis saisissez la clé de licence dans l'espace prévu à cet effet.

b Si vous ne disposez pas de la clé de licence, sélectionnez l'option **30–days Enterprise Evaluation (30 jours d'essai de l'édition Entreprise)**.

La clé de licence est saisie par défaut. Cependant, après la période d'évaluation de 30 jours, vous devez obtenir la clé de licence et l'ajouter à WDM. Pour plus d'informations sur l'ajout d'une clé de licence, reportez-vous au *Dell Wyse Device Manager Administrator's Guide (Guide de l'administrateur de Dell Wyse Device Manager)*.

5 Cliquez sur **NEXT (SUIVANT)**.

6 Sélectionnez un composant **Database (Base de données)**.

7 Dans l'écran **Configure Database (Configurer la base de données)**, sélectionnez l'une des options suivantes :

- **Install New Database Server (Installer un nouveau serveur de base de données) (Microsoft SQL Express 2016 SP1)** : sélectionnez cette option si aucune version prise en charge de Microsoft SQL Server n'est installée sur le système. Passez à l'étape 8.
- **Use Existing Database Server (Utiliser le serveur de base de données existant) (SQL Server Express ou Full)** : sélectionnez cette option si une version prise en charge de Microsoft SQL Server est déjà installée sur le système. Si vous sélectionnez cette option, assurez-vous que le serveur de base de données se trouve sur le même système que celui sur lequel vous installez l'édition Workgroup de WDM, et passez à l'étape 9.

8 Si vous avez sélectionné la première option lors de l'étape 7, sélectionnez la méthode d'authentification.

- **SQL Server Authentication (Authentification du serveur SQL)** : cette option est sélectionnée par défaut. Pour configurer l'authentification du serveur SQL, procédez comme suit :
  1 Entrez les informations d'identification de la base de données WDM.
  2 Entrez les informations d'identification de la nouvelle base de données. Vous pouvez entrer le nom de l'instance et le nom de la base de données dans les détails du nouveau serveur de base de données. Le nom d'instance et le nom de la base de données par défaut sont RapportDB.

REMARQUE : Même si vous choisissez l'authentification Windows, l'installation WDM nécessite l'authentification SQL pour accéder à la base de données SQL. Dans une installation autonome, après avoir terminé l'installation de la base de données WDM, le programme d'installation attribue l'utilisateur Active Directory à la base de données, et le même utilisateur est utilisé pour installer les services WDM.

- **Windows Authentication (Authentification Windows)** : entrez les informations sur le nouveau serveur de base de données. Le nom d'instance et le nom de la base de données par défaut sont RapportDB.

REMARQUE :

- Sélectionnez **Windows Authentication (Authentification Windows)** si vous souhaitez vous connecter à la base de données WDM en utilisant vos informations de connexion Windows.
- Le mot de passe doit correspondre aux règles de complexité du système d'exploitation Windows.

9 Si vous avez sélectionné la seconde option lors de l'étape 7, sélectionnez la méthode d'authentification.

- **SQL Server Authentication (Authentification du serveur SQL)** : cette option est sélectionnée par défaut. Pour configurer l'authentification du serveur SQL, procédez comme suit :
  1. Sélectionnez l'option **Create New User (Créer un nouvel utilisateur)** ou l'option Use the existing user (Utiliser l'utilisateur existant), puis entrez les informations d'identification de la base de données WDM.
  2. Entrez les informations sur le serveur de base de données existant, telles que le nom d'hôte du serveur, le nom de l'instance, le nom de la base de données, le numéro de port et le nom de l'administrateur et le mot de passe SQL.
- **Windows Authentication (Authentification Windows)** : entrez les informations sur le serveur de base de données existant, telles que le nom d'hôte du serveur, le nom de l'instance, le nom de la base de données, le numéro de port et le nom de l'administrateur et le mot de passe SQL.

REMARQUE : Le numéro de port par défaut est 1433. Dell vous recommande de saisir manuellement le numéro de port car il s'agit d'un numéro de port dynamique. Vous pouvez ajouter un numéro de port personnalisé à cinq chiffres entre 49152 et 65535 pour le TCP/UDP.

10 Cliquez sur **NEXT (SUIVANT)**.

11 Indiquez le chemin d'installation, puis cliquez sur **NEXT (SUIVANT)**.

L'écran **Installation Summary (Résumé de l'installation)** s'affiche.

12 Cliquez sur **NEXT (SUIVANT)**.

La progression de l'installation s'affiche à l'écran. Une fois l'installation terminée, vous êtes invité à redémarrer votre système.

13 Redémarrez le système pour que les modifications prennent effet.

Pour l'installation manuelle de la base de données WDM à l'aide des scripts, reportez-vous à Manual installation of WDM database using scripts (Installation manuelle de la base de données WDM à l'aide de scripts).

Installation des services de gestion

À propos de cette tâche

Vous pouvez installer le serveur de gestion, la console de gestion et l'interface utilisateur Web sur le même système ou sur différents systèmes.

Étapes

1 Extrayez le contenu du programme d'installation WDM vers le système sur lequel vous souhaitez installer WDM.

2 Accédez au dossier dans lequel vous avez extrait le programme d'installation et exécutez **Setup.exe**.

Si le serveur ne dispose pas de .Net framework, celui-ci est installé automatiquement.

L'écran **Welcome (Accueil)** s'affiche.

3 Cliquez sur **NEXT (SUIVANT)**.

4 Dans Type de licence, sélectionnez **ENTERPRISE (ENTREPRISE)**.

a Si vous disposez de la clé de licence WDM, sélectionnez l'option **I have WDM Enterprise License Key (J'ai une clé de licence Entreprise WDM)**, puis saisissez la clé de licence dans l'espace prévu à cet effet.

b Si vous ne disposez pas de la clé de licence, sélectionnez l'option **30–days Enterprise Evaluation** (30 jours d'essai de l'édition Entreprise).

La clé de licence est saisie par défaut. Cependant, après la période d'évaluation de 30 jours, vous devez obtenir la clé de licence et l'ajouter à WDM. Pour plus d'informations sur l'ajout d'une clé de licence, reportez-vous au *Dell Wyse Device Manager Administrator's Guide (Guide de l'administrateur de Dell Wyse Device Manager)*.

5 Cliquez sur **NEXT (SUIVANT)**.

6 Installation de **Management Server (Serveur de gestion)**, **Other Services (Autres services)**, **Management Console (Console de gestion)** et **Web UI (Interface utilisateur Web)**

REMARQUE : Si vous installez chaque composant sur un système séparé, vous pouvez les sélectionner un par un en suivant les étapes 1 à 5.

7 Dans l'écran **Configure Database (Configurer la base de données)**, sélectionnez l'une des options suivantes :

- **SQL Server Authentication (Authentification du serveur SQL)** : cette option est sélectionnée par défaut. Pour configurer l'authentification du serveur SQL, entrez les informations d'identification du serveur de base de données WDM.
- **Windows Authentication (Authentification Windows)** : entrez les informations du serveur de base de données WDM, telles que le nom du serveur, le nom de l'instance, le nom de la base données, le mot de passe et le numéro de port. Le champ **Username (Nom d'utilisateur)** est grisé.

REMARQUE :

- Le numéro de port par défaut est 1433. Dell vous recommande de saisir manuellement le numéro de port car il s'agit d'un numéro de port dynamique. Vous pouvez ajouter un numéro de port personnalisé à cinq chiffres entre 49152 et 65535 pour le TCP/UDP.
- Sélectionnez **Windows Authentication (Authentification Windows)** si vous souhaitez vous connecter à la base de données WDM en utilisant vos informations de connexion Windows.

8 Cliquez sur **NEXT (SUIVANT)**.

9 Sélectionnez les services à installer, puis cliquez sur **NEXT (SUIVANT)**.

REMARQUE : DHCP Proxy (Proxy DHCP) est sélectionné par défaut.

10 Indiquez le chemin d'installation, puis cliquez sur **NEXT (SUIVANT)**.

11 Sélectionnez et importez le certificat pour démarrer l'installation.

REMARQUE : Si vous cliquez sur NEXT (SUIVANT) sans avoir sélectionné de certificat, le programme d'installation installe un certificat auto-signé. Les communications sont chiffrées, mais le système n'est pas sécurisé. Le certificat doit être au format de fichier .pfx.

La progression de l'installation s'affiche à l'écran. Une fois l'installation terminée, vous êtes invité à redémarrer votre système.

12 Redémarrez le système pour que les modifications prennent effet.

REMARQUE : Au sein d'un environnement distribué, l'interface utilisateur peut être installée sur une console multiple.

Installation de la logithèque

Prérequis

La logithèque est un autre composant important de WDM. En vue de leur déploiement sur les systèmes clients, les progiciels sont enregistrés et stockés dans la logithèque. Avant d'installer le référentiel de logiciels, assurez-vous que vous avez installé et configuré la base de données WDM.

Étapes

1 Décompressez le contenu du programme d'installation de WDM sur le système sur lequel vous souhaitez installer WDM.

2 Accédez au dossier dans lequel vous avez extrait le programme d'installation et exécutez Setup.exe.

Si le serveur ne dispose pas de .Net framework, celui-ci est installé automatiquement.

L'écran **Welcome (Accueil)** s'affiche.

3 Cliquez sur **NEXT (SUIVANT)**.

4 Dans Type de licence, sélectionnez **ENTERPRISE (ENTREPRISE)**.

a Si vous disposez de la clé de licence WDM, sélectionnez l'option **I have WDM Enterprise License Key (J'ai une clé de licence Entreprise WDM)**, puis saisissez la clé de licence dans l'espace prévu à cet effet.

b Si vous ne disposez pas de la clé de licence, sélectionnez l'option **30–days Enterprise Evaluation** (30 jours d'essai de l'édition Entreprise).

La clé de licence est saisie par défaut. Cependant, après la période d'évaluation de 30 jours, vous devez obtenir la clé de licence et l'ajouter à WDM. Pour plus d'informations sur l'ajout d'une clé de licence, reportez-vous au *Dell Wyse Device Manager Administrator's Guide (Guide de l'administrateur de Dell Wyse Device Manager)*.

5 Cliquez sur **NEXT (SUIVANT)**.

6 Sélectionnez le composant **Software Repository (Référentiel de logiciels)**.

7 Dans l'écran **Configure Database (Configurer la base de données)**, sélectionnez l'une des options suivantes :

- **SQL Server Authentication (Authentification du serveur SQL)** : cette option est sélectionnée par défaut. Pour configurer l'authentification du serveur SQL, entrez les informations d'identification du serveur de base de données WDM.
- **Windows Authentication (Authentification Windows)** : entrez les informations du serveur de base de données WDM, telles que le nom du serveur, le nom de l'instance, le nom de la base données, le mot de passe et le numéro de port. Le champ **Username (Nom d'utilisateur)** est grisé.

REMARQUE :

- Le numéro de port par défaut est 1433. Dell vous recommande de saisir manuellement le numéro de port car il s'agit d'un numéro de port dynamique. Vous pouvez ajouter un numéro de port personnalisé à cinq chiffres entre 49152 et 65535 pour le TCP/UDP.
- Sélectionnez **Windows Authentication (Authentification Windows)** si vous souhaitez vous connecter à la base de données WDM en utilisant vos informations de connexion Windows.

8 Cliquez sur **NEXT (SUIVANT)**.

9 Sélectionnez les services à installer, puis cliquez sur **NEXT (SUIVANT)**.

REMARQUE : DHCP Proxy (Proxy DHCP) est sélectionné par défaut.

10 Indiquez le chemin d'installation, puis cliquez sur **NEXT (SUIVANT)**.

11 Sélectionnez et importez le certificat pour démarrer l'installation.

REMARQUE : Si vous cliquez sur NEXT (SUIVANT) sans avoir sélectionné de certificat, le programme d'installation installe un certificat auto-signé. Les communications sont chiffrées, mais le système n'est pas sécurisé. Le certificat doit être au format de fichier .pfx.

La progression de l'installation s'affiche à l'écran. Une fois l'installation terminée, vous êtes invité à redémarrer votre système.

12 Redémarrez le système pour que les modifications prennent effet.

REMARQUE : Au sein d'un environnement distribué, l'interface utilisateur peut être installée sur une console multiple.

Mise à niveau de WDM

Conditions requises

La version actuelle de WDM prend en charge une mise à niveau depuis la version de correctif à chaud 5.7.2/5.7.2. La mise à niveau à partir d'une autre version n'est pas prise en charge. Si vous exécutez une ancienne version de WDM, vous devez d'abord effectuer une mise à niveau vers la version de correctif à chaud 5.7.2 /5.7.2, puis effectuer une mise à niveau vers la version la plus récente.

REMARQUE : Après la mise à niveau vers la version 5.7.3, vous devrez effectuer la mise à niveau de tous les périphériques avec les derniers packages Agents disponibles pour que vos périphériques puissent être gérés à l'aide de WDM. Pour plus d'informations, reportez-vous aux *Notes de mise à jour de WDM 5.7.3* à l'adresse support.dell.com.

Tâche

1 Extrayez le contenu du programme d'installation de WDM sur le système sur lequel vous avez installé la version de correctif à chaud 5.7.2/5.7.2 de WDM.

2 Accédez au dossier dans lequel vous avez décompressé le programme d'installation et exécutez **Setup.exe**.

L'écran **Welcome (Accueil)** s'affiche.

3 Cliquez sur **Next (Suivant)**.
L'écran **Upgrade Information (Informations de mise à niveau)** s'affiche.

4 Cliquez sur **Next (Suivant)**. L'écran **User Credentials** (Informations d'identification de l'utilisateur) s'affiche.

5 Entrez le mot de passe.

IMPORTANT: Le champ Password (Mot de passe) est désactivé pour l'authentification SQL. Le mot de passe est requis uniquement pour l'authentification Windows.

6 Cliquez sur **Next (Suivant)**.

L'écran **Important Information (Informations importantes)** s'affiche.

7 Prenez connaissance attentivement des **Important Information** (Informations importantes), puis cliquez sur **Next** (Suivant).

La mise à niveau commence.

8 Une fois la mise à niveau terminée, cliquez sur **Restart Now (Redémarrer maintenant)** pour que le système prenne en compte les modifications et que vous puissiez commencer à utiliser WDM.

REMARQUE : ThreadX 5.x est installé automatiquement lorsque ThreadX 4.x est déjà installé sur le système avec Windows 2012 et versions ultérieures.

Configuration de communications sécurisées

Configurations de communications sécurisées avec SSL :

Il existe différentes méthodes pour installer SSL dans IIS 6.0 et IIS 7.0. Les procédures de configuration de SSL dans IIS 6.0 et IIS 7.0 sont présentées ci-dessous.

Configuration du protocole SSL dans IIS 7.0 sous Windows Server 2008 R2

Pour configurer SSL dans IIS 7.0 :

1 Téléchargez l'utilitaire **SelfSSL7** depuis le lien SelfSSL.exe.

2 Exécutez l'utilitaire **SelfSSL7.exe** avec les paramètres mentionnés ci-dessous :

```
SelfSSL7.exe /Q /N cn=Certificate_Name /I /S Web_Site_Name. e.g. SelfSSL7.exe /Q /N
cn="TestCert.TestLab.com" /I /S "Default Web Site"
```

Configuration de communications sécurisées au moyen de l'autorité de certification racine

Installation de l'autorité de certification racine dans IIS 7.0 sous Windows Server 2008 R2

Suivez les consignes ci-dessous :

Afin d'installer le certificat, deux étapes doivent être respectées :

- Installer le certificat sur le serveur du **Domain Controller** (Contrôleur de domaine).
- Installer le certificat sur le serveur **WDM**.

Installation du certificat sur le serveur du contrôleur de domaine

Suivez les consignes ci-dessous :

1 Accédez au **Server Manager** (Gestionnaire de serveur).

2 Dans le volet arborescent, sélectionnez **Roles**->**Add Roles** (Rôles -> Ajouter des rôles).

3 Dans l'Assistant **Add Roles** (Ajouter des rôles), sélectionnez **Server Roles** (Rôles du serveur) depuis le volet arborescent.

4 Dans la fenêtre **Server Role** (Rôles du serveur) correspondante, sélectionnez **Active Directory Certificate Service** (Service de certificats Active Directory) depuis **Roles** (Rôles).

5 Cliquez sur **Next** (Suivant)->**Next** (Suivant). Puis dans **Role Services** (Services de rôle), sélectionnez les options **Certification Authority** (Autorité de certification) et **Certificate Authority Web Enrolment** (Enrôlement Web de l'autorité de certification).

6 Après avoir sélectionné l'option **Certificate Authority Web Enrolment** (Enrôlement Web de l'autorité de certification), et si IIS n'est pas installé sur le serveur, un nouvelle fenêtre **Add Required Role Services** (Ajouter les services de rôles requis) s'affichera.

7 Sur la fenêtre susmentionnée, cliquez sur le bouton **Add Required Role Services** (Ajouter les services de rôle requis), puis cliquez sur **Next** (Suivant) pour afficher la fenêtre **Specify Setup Type** (Sélectionner le type d'installation).

8 Dans la fenêtre sus-mentionnée, en fonction des exigences, sélectionnez soit le bouton radio **Enterprise** (Entreprise) ou bien **Standalone** (Autonome), puis cliquez sur **Next** (Suivant) pour ouvrir la fenêtre **Specify CA Type** (Spécifier le type d'autorité de certification).

9 Dans la fenêtre **Specify CA Type** (Spécifier le type d'autorité de certification), en fonction des exigences, sélectionnez soit le bouton radio **Root CA** (Autorité de certification racine) ou bien **Subordinate CA** (Autorité de certification secondaire), puis cliquez sur **Next** (Suivant) pour ouvrir la fenêtre **Setup Private Key** (Configuration de la clé privée).

10 Dans la fenêtre **Setup Private Key** (Configuration de la clé privée), en fonction des exigences, sélectionnez soit le bouton radio **Create a new private key** (Créer une nouvelle clé privée) ou bien **Use existing private key** (Utiliser une clé privée existante), puis cliquez sur **Next** (Suivant) pour ouvrir la fenêtre **Configure Cryptography for CA** (Configurer le chiffrement pour l'autorité de certification).

11 Dans la fenêtre **Configure Cryptography for CA** (Configurer le chiffrement pour l'autorité de certification), en fonction des exigences, sélectionnez la valeur pour le champ **Select a cryptography service provider (CSP)** (Sélectionner un fournisseur de services de chiffrement (CSP))dans la zone de liste déroulante, définissez la **Key character length** (Longueur de la clé en caractères) dans la zone de liste déroulante, sélectionnez la valeur pour le champ **Select the Hash algorithm for signing certificate issued by this CA** (Sélectionner l'algorithme de hashage pour la signature du certificat délivré par l'autorité de certification), puis sélectionnez ou désélectionnez **Allow administrator interaction when the private key is accessed by the CA** (Autoriser l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée) dans la case à cocher et cliquez sur le bouton **Next** (Suivant) pour ouvrir une nouvelle fenêtre **Configure CA Name** (Configurer le nom de l'autorité de certification).

REMARQUE : Le nom commun du certificat doit correspondre au nom de l'ordinateur du serveur WDM.

12 Dans la fenêtre **Configure CA Name** (Configurer le nom de l'autorité de certification), saisissez les valeurs pour les champs **Common name for this CA** (Nom commun de cette autorité de certification) et **Distinguished name suffix** (Suffixe du nom unique), puis cliquez sur **Next** (Suivant) pour ouvrir la fenêtre **Set Validity Period** (Période de validité du certificat).

13 Dans la fenêtre **Set Validity Period** (Période de validité du certificat), sélectionnez la période de validité pour le certificat généré pour cette autorité de certification, puis cliquez sur **Next** (Suivant) pour ouvrir la fenêtre **Configure Certificate Database** (Configurer la base de données de certificats).

14 Dans la fenêtre **Configure Certificate Database** (Configurer la base de données de certificats), sélectionnez le **Certificate database location** (Emplacement de la base de données de certificats) ainsi que le **Certificate database log location** (Emplacement du journal de la base de données de certificats), puis cliquez sur **Next** (Suivant) pour ouvrir la fenêtre **Add Roles Wizard** (Assistant Ajouter un rôle) pour IIS.

15 Sélectionnez les valeurs par défaut, puis cliquez sur **Next**-> **Installation** (Suivant -> Installation).

16 Les **Active Directory Certificate Services** (Services de certificats Active Directory), **Web Server (IIS)** (Serveur Web (IIS)) et **Remote Server Administration Tools** (Outils d'administration de serveur distant) seront installés.

17 Une fois l'installation de certificats terminée, accédez à **Internet Information Services Manager** (Gestionnaire des services IIS) du contrôleur de domaine.

18 Dans le volet d'arborescence du **Server Manager** (Gestionnaire de serveur), développez **Roles** (Rôles), puis cliquez sur **Web Server (IIS)**-> **Internet Information Services (IIS) Manager** (Serveur Web (IIS)-> Gestionnaire des services IIS) pour ouvrir la fenêtre **IIS Manager** (Gestionnaire des services IIS).

19 Dans le volet d'arborescence, sélectionnez **Server** (Serveur), puis double-cliquez sur **Server Certificates** (Certificats de serveur) dans le volet droit.

20 Dans le volet droit de **Server Certificates** (Certificats de serveur), double-cliquez sur **Create Domain Certificate...** (Créer un certificat de domaine...) pour débuter la création d'un certificat.

21 Remplissez les informations requises dans la fenêtre **Create Certificate** (Créer un certificat), puis cliquez sur **Next** (Suivant) pour ouvrir la fenêtre **Online Certification Authority** (Autorité de certification en ligne).

22 Dans **Online Certification Authority** (Autorité de certification en ligne), cliquez sur **Select** (Sélectionner) pour **Specify Online Certification Authority** (Indiquer une autorité de certification en ligne) et saisissez un **Friendly Name** (Nom convivial) pour cette dernière et cliquez enfin sur **Finish** (Terminer).

23 L'installation de certificats sur le serveur du contrôleur de domaine est maintenant accomplie, procédez ensuite à l'installation de certificats sur le serveur WDM.

Installation du certificat sur le serveur WDM

Suivez les consignes ci-dessous :

1 Dans la barre des tâches, cliquez sur **Start**->**Administrative Tools**->**Internet Information Services (IIS) Manager** (Démarrer -> Outils d'administration -> Gestionnaire des services IIS) pour ouvrir la fenêtre **IIS Manager** (Gestionnaire des services IIS).

2 Dans le volet d'arborescence, cliquez sur **Server** (Serveur) et, dans le volet droit, sur **Server Certificates** (Certificats de serveur) pour ouvrir la fenêtre **Server Certificates** (Certificats de serveur).

3 Remplissez les informations requises dans la fenêtre **Create Certificate** (Créer un certificat), puis cliquez sur **Next** (Suivant) pour ouvrir la fenêtre **Online Certification Authority** (Autorité de certification en ligne).

4 Dans **Online Certification Authority** (Autorité de certification en ligne), cliquez sur **Select** (Sélectionner) pour **Specify Online Certification Authority** (Indiquer une autorité de certification en ligne) et saisissez un **Friendly Name** (Nom convivial) pour cette dernière et cliquez enfin sur **Finish** (Terminer).

5 L'installation de certificats sur le serveur WDM est maintenant terminée.

6 Après l'installation du certificat, parcourez **Server** ->**Web Sites**->**Rapport HTTP Server** (Serveur ->Sites Web ->Relations du serveur HTTP), puis cliquez sur **Bindings...** (Liaisons...) dans le volet droit pour ouvrir la fenêtre **Site Bindings** (Liaisons de sites).

7 Dans la fenêtre **Site Bindings** (Liaisons de sites), cliquez sur **Add** (Ajouter) pour **Add Site Binding** (Ajouter une liaison de sites)

8 Dans **Add Site Binding** (Ajouter une liaison de sites), sélectionnez le certificat récemment créé dans la zone de liste déroulante **SSL Certificate** (Certificat SSL), puis cliquez sur le bouton **OK**.

9 Afin de ne lancer que la communication HTTPS, sélectionnez **SSL Settings** (Paramètres SSL) dans **Server**->**Web Sites**->**Rapport HTTP Server** (Serveur -> Sites Web -> Relations du serveur HTTP).

10 Dans **SSL Settings** (Paramètres SSL), cochez la case **Require SSL**, puis cliquez sur **Apply** (Appliquer).

Installation de l'autorité de certification racine dans IIS 7 sous Windows Server 2012 R2

Suivez les consignes ci-dessous :

- Afin d'installer le certificat, deux étapes doivent être respectées :
  - Installer le certificat sur le serveur du Contrôleur de domaine
  - Installer le certificat sur le serveur WDM

Installer le certificat sur le serveur du Contrôleur de domaine :

Suivez les consignes ci-dessous :

1 Accédez au Server Manager (Gestionnaire de serveur).

2 Dans **Dashboard** (Tableau de bord) >> sélectionnez l'option 2 **Add Roles and features** (Ajout de rôles et de fonctionnalités).

3 Dans l'assistant Add Roles and Features (Ajout de rôles et de fonctionnalités), sélectionnez le type d'installation basé sur le rôle ou basé sur la fonctionnalité.

4 Dans Server Selection (Sélection du serveur) >> sélectionnez un serveur dans le pool de serveurs (le serveur local est sélectionné par défaut).

5 Ensuite, dans la fenêtre Server Roles (Rôles du serveur), sélectionnez le rôle Active Directory Certificate Services (Services de certificats Active Directory).

6 La sélection du rôle Active Directory Certificate Services (Services de certificats Active Directory) lance l'assistant Add Roles and Features (Ajout de rôles et de fonctionnalités) qui se lance automatiquement avec les sous-fonctionnalités >> cliquez sur le bouton Add Features (Ajouter des fonctionnalités).

7 Cliquez sur Next->Next (Suivant->Suivant). Ensuite, dans la fenêtre Features (Fonctionnalités), laissez les valeurs par défaut et cliquez sur Next (Suivant).

8 Dans la fenêtre AD CS qui s'affiche ensuite, cliquez sur le bouton Next (Suivant).

9 Dans la fenêtre Role Services (Services de rôle), sélectionnez les options Certification Authority (Autorité de certification) et Certificate Authority Web Enrolment (Enrôlement Web de l'autorité de certification).

10 Après avoir sélectionné l'option Certificate Authority Web Enrolment (Enrôlement Web de l'autorité de certification), si IIS n'est pas installé sur le serveur, une nouvelle fenêtre Add Features (Ajouter des fonctionnalités) requises pour la sous-fenêtre Certification Authority Web Enrollment (Enrôlement Web de l'autorité de certification) s'affiche.

11 Dans la fenêtre ci-dessus, cliquez sur le bouton Add Feature (Ajouter une fonctionnalité) et cliquez sur Next (Suivant) dans la fenêtre de confirmation.

12 Cliquez ensuite sur le bouton « Install » (Installer) pour installer le rôle de certificat AD.

13 Dans la fenêtre Results (Résultats), la progression de l'installation de la fonctionnalité peut être consultée.

14 Une fois l'installation du rôle AD Certificate Authority (Autorité de certification AD) réussie, cliquez sur bouton « Close » (Fermer).

15 Ensuite, dans la console Server Manager >> Dashboard (Gestionnaire de serveur >> Tableau de bord), sous « Notifications », recherchez le message Post-deployment Configuration (Configuration après le déploiement).

16 Dans le message Post-deployment Configuration (Configuration après le déploiement), cliquez sur le lien « Configure Active Directory Certificate Services on the local server » (Configurer les services de certificats Active Directory sur le serveur local).

17 La fenêtre AD CS Configuration >> Credentials (Configuration AD CS >> Informations d'identification) s'ouvre ensuite ; indiquez les informations d'identification appropriées et cliquez sur le bouton « Next » (Suivant).

18 Ensuite, sous Role Services (Services de rôle) >> sélectionnez les options Certification Authority (Autorité de certification) et Certificate Authority Web Enrolment (Enrôlement Web de l'autorité de certification) et cliquez sur « Next » (Suivant).

19 Dans la fenêtre Setup Type (Type de configuration), en fonction des exigences, sélectionnez le bouton radio Enterprise (Entreprise) ou Standalone (Autonome), puis cliquez sur Next (Suivant) pour ouvrir la fenêtre CA Type (Type de CA).

20 Dans la fenêtre CA Type (Type de CA), en fonction des exigences, sélectionnez le bouton radio Root CA (Autorité de certification racine) ou Subordinate CA (Autorité de certification secondaire), puis cliquez sur Next (Suivant) pour ouvrir la fenêtre Private Key (Clé privée).

21 Dans la fenêtre Private Key (Clé privée), en fonction des exigences, sélectionnez le bouton radio Create a new private key (Créer une nouvelle clé privée) ou Use existing private key (Utiliser une clé privée existante), puis cliquez sur Next (Suivant) pour ouvrir la fenêtre Configure Cryptography for CA (Configurer le chiffrement pour l'autorité de certification).

22 Dans la fenêtre Configure Cryptography for CA (Configurer le chiffrement pour l'autorité de certification),

- en fonction des exigences, sélectionnez la valeur de champ Select a cryptographic service provider (CSP) (Sélectionner un fournisseur de services de chiffrement (CSP, Cryptography Service Provider)) depuis le menu déroulant.
- Indiquez la longueur de clé de la zone de liste déroulante suivante.
- Sélectionnez la valeur de champ Select the Hash algorithm for signing certificate issued by this CA (Sélectionner l'algorithme de hachage pour la signature du certificat délivré par l'autorité de certification)
- et cochez ou décochez ensuite la case « Allow administrator interaction when the private key is accessed by the CA » (Autoriser l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée).
- Cliquez ensuite sur le bouton Next (Suivant) pour ouvrir la fenêtre Configure CA Name (Configurer le nom de l'autorité de certification). REMARQUE : le nom commun du certificat doit correspondre au nom de l'ordinateur du serveur WDM.

23 Dans la fenêtre CA Name (Nom de l'autorité de certification), saisissez les valeurs pour les champs Common name for this CA (Nom commun de cette autorité de certification) et Distinguished name suffix (Suffixe du nom unique), puis cliquez sur Next (Suivant) pour ouvrir la fenêtre Validity Period (Période de validité).

24 Dans la fenêtre Specify Validity Period (Spécifier la période de validité), sélectionnez la période de validité pour le certificat généré pour cette autorité de certification, puis cliquez sur Next (Suivant) pour ouvrir la fenêtre Certificate Database (Base de données de certificats).

25 Dans la fenêtre Certificate Database (Base de données de certificats), sélectionnez l'emplacement de la base de données de certificats ainsi que l'emplacement du journal de la base de données de certificats, puis cliquez sur Next (Suivant) pour ouvrir la fenêtre Confirmation.

26 Dans la fenêtre Confirmation, cliquez sur le bouton Configure (Configurer) qui lancera la fenêtre de progression.

27 Ensuite, dans la fenêtre Results (Résultats), le message Certification Authority and Certification Authority Web Enrollment Configuration succeeded (L'autorité de certification et l'enrôlement Web de l'autorité de certification ont abouti) s'affiche.

28 Cliquez sur le bouton Close (Fermer) pour terminer la configuration d'AD CS.

29 L'installation de certificats sur le serveur du contrôleur de domaine est maintenant accomplie, procédez ensuite à l'installation de certificats sur le serveur WDM.

Installation du certificat sur le serveur WDM :

Suivez les consignes ci-dessous :

1 Dans la barre des tâches, cliquez sur Start->Administrative Tools->Internet Information Services (IIS) (Démarrer->Outils d'administration->Gestionnaire des services IIS) pour ouvrir la fenêtre IIS Server Manager (Gestionnaire des services IIS).

2 Dans le volet arborescent, cliquez sur Server (Serveur) et, dans le volet droit, sur Server Certificates (Certificats de serveur) pour ouvrir la fenêtre Server Certificates (Certificats de serveur).

3 Cliquez sur le lien Create Domain Certificate (Créer un certificat de domaine) dans le volet droit et renseignez les informations demandées dans la fenêtre Create Certificate (Créer un certificat). Cliquez sur Next (Suivant) pour ouvrir Online Certification Authority (Autorité de certification en ligne).

4 Dans Online Certification Authority (Autorité de certification en ligne), cliquez sur Select to Specify Online Certification Authority (Sélectionner pour Indiquer une autorité de certification en ligne) (Créé sur la machine de votre contrôleur AD ou dans votre configuration), saisissez un Friendly Name (Nom convivial) pour cette dernière et cliquez enfin sur Finish (Terminer).

5 L'installation de certificats sur le serveur WDM est maintenant terminée.

6 Après l'installation du certificat, parcourez Server -> Sites->Rapport HTTP Server (Serveur ->Sites ->Relations du serveur HTTP), puis cliquez sur Bindings... (Liaisons...) dans le volet droit pour ouvrir la fenêtre Site Bindings (Liaisons de sites).

7 Dans la fenêtre Site Bindings (Liaisons de sites), cliquez sur Add (Ajouter) pour ajouter une liaison de sites.

8 Dans Add Site Binding (Ajouter une liaison de sites), sélectionnez le type HTTPS, puis sélectionnez Certificate Authority (Autorité de certification) sous IP Address (Adresse IP), sélectionnez le certificat récemment créé dans la zone de liste déroulante SSL Certificate (Certificat SSL) et cliquez sur le bouton OK.

9 Afin de ne lancer que la communication HTTPS, sélectionnez SSL Settings (Paramètres SSL) dans Server->Web Sites->Rapport HTTP Server (Serveur->Sites Web->Relations du serveur HTTP).

10 Dans SSL Settings (Paramètres SSL), cochez la case Require SSL (SSL requis) et le bouton radio Client certificate (Certificat client) et appliquez les paramètres.

4

Désinstallation d'une installation autonome de WDM

À propos de cette tâche

Si vous avez une installation autonome de WDM, où tous les composants sont installés sur le même système, vous pouvez suivre la procédure décrite ci-dessous pour désinstaller WDM.

Étapes

1. Accédez à **Start (Démarrer)** > **Control Panel (Panneau de configuration)**.
2. Cliquez sur **Programs (Programmes)** > **Uninstall a program (Désinstaller un programme)**.
3. Sélectionnez **WDM 5.7.3** dans la liste des programmes et cliquez sur **Uninstall (Désinstaller)**.

   L'écran **Uninstallation (Désinstallation)** s'affiche.
4. Cliquez sur **Next (Suivant)** dans l'écran **Welcome (Accueil)**.
5. Entrez les informations d'identification permettant d'accéder à la base de données de WDM.

   Vous devez spécifier les informations de connexion SQL pour SQL Server et SQL Express selon l'emplacement où vous avez installé la base de données de WDM.

   Si les informations de connexion sont erronées, le message d'erreur **Unable to connect to database (Impossible de connecter la base de données)** s'affiche.
6. Cliquez sur **Next (Suivant)**.

   Une fois les composants désinstallés, vous êtes invité à redémarrer votre système.
7. Cliquez sur **Restart Now (Redémarrer maintenant)** pour terminer le processus de désinstallation.

Étape suivante

Après la désinstallation, vérifiez que vous respectez les listes de vérification suivantes :

- L'icône WyseDeviceManager 5.7.3 **WebUI** doit avoir disparu du Bureau.
- Dans IIS, l'application HApi doit être supprimée dans Rapport HTTP Server.
- Dans IIS, l'application MyWDM doit être supprimée dans Rapport HTTP Server.
- Dans IIS, l'application WebUI doit être supprimée dans Rapport HTTP Server.

Désinstallation de WDM dans une configuration distribuée

À propos de cette tâche

Si vous avez installé WDM dans une configuration distribuée, vous devez désinstaller les composants un par un sur les systèmes où vous les avez installés.

REMARQUE : Avant de désinstaller la base de données de WDM, vous devez avoir désinstallé tous les autres composants sur les systèmes où vous les avez installés.

Étapes

1. Ouvrez une session sur le ou les systèmes où vous avez installé le serveur de gestion, la console de gestion, d'autres services, la logithèque et l'interface utilisateur Web.
2. Accédez à **Start (Démarrer)** > **Control Panel (Panneau de configuration)**.
3. Cliquez sur **Programs (Programmes)** > **Uninstall a program (Désinstaller un programme)**.

4 Sélectionnez **WDM 5.7.3** dans la liste des programmes et cliquez sur **Uninstall (Désinstaller)**.
L'écran **Uninstallation (Désinstallation)** s'affiche.
5 Cliquez sur **Next (Suivant)** dans l'écran **Welcome (Accueil)**.
6 Cliquez sur **Next (Suivant)** pour lancer la désinstallation.
7 Connectez-vous au système sur lequel vous avez installé la base de données de WDM.
8 Répétez les étapes 2 à 5.
9 Entrez les informations d'identification permettant d'accéder à la base de données de WDM.
Vous devez spécifier l'ID de connexion SQL et le mot de passe pour SQL Server ou SQL Express selon l'emplacement où vous avez installé la base de données de WDM.

Si les informations d'identification que vous saisissez sont erronées, le programme affiche le message suivant : *Unable to connect to database (Impossible de se connecter à la base de données)*. Assurez-vous d'entrer des informations d'identification correctes.
10 Cliquez sur **Next (Suivant)** pour lancer la désinstallation.
11 Une fois la base de données désinstallée, redémarrez le système lorsque le programme vous y invite.

5

Configuration de la mise en cluster de la base de données haute disponibilité pour WDM

Les clusters à haute disponibilité (aussi appelés clusters HA ou clusters de basculement) sont des groupes d'ordinateurs qui prennent en charge les applications du serveur qui peuvent être utilisées de manière fiable avec des temps d'arrêt limités. Ils fonctionnent en exploitant les ordinateurs redondants dans les groupes ou clusters qui assurent la continuité du service lorsque les composants du système sont en panne.

Si un serveur exécutant une application particulière se bloque, alors, sans la mise en cluster, l'application est indisponible jusqu'à ce que le serveur en panne soit réparé. La mise en cluster HA corrige cette situation en détectant les erreurs de matériel/logiciel et en redémarrant immédiatement l'application sur un autre système sans nécessiter la moindre intervention de l'administrateur. Ce processus est nommé **failover** (basculement).

Les clusters HA utilisent généralement une connexion réseau privée d'émissions de signaux permettant de surveiller l'état et l'intégrité de chaque nœud du cluster.

Les clusters HA à deux nœuds sont les plus courants.

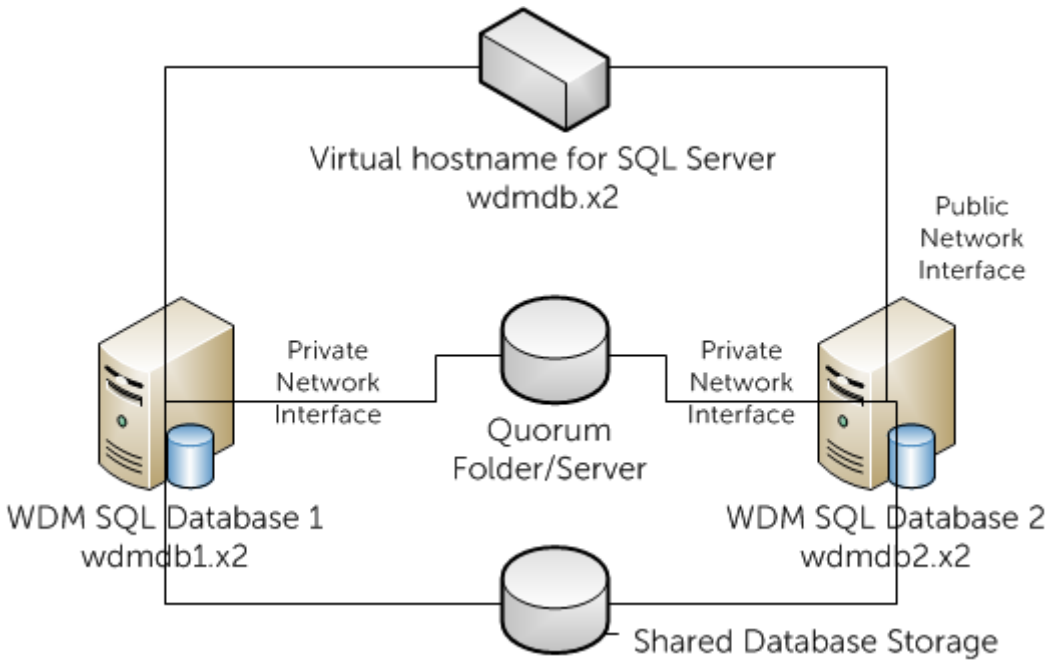


Figure 38. Mise en cluster de la base de données à haute disponibilité WDM

Cette section présente les étapes de la configuration pour la version 5.0 ou ultérieure de la mise en cluster de la base de données à haute disponibilité (HA) de Dell Wyse Device Manager (WDM).

Sujets :

- Composants nécessaires à la mise en cluster de la base de données

Composants nécessaires à la mise en cluster de la base de données

L'environnement à haute disponibilité pour WDM est constitué des éléments suivants :

- **Primary Server or Primary Node** (Serveur primaire ou nœud principal) : il s'agit de l'une des quatre machines virtuelles (VM) sur laquelle vous devez installer la base de données Microsoft SQL Server 2012. Il doit posséder deux cartes réseau, l'une configurée pour le réseau public et l'autre configurée pour le réseau privé.
- **Secondary Server or Secondary Node** (Serveur secondaire ou nœud secondaire) : il s'agit de la deuxième machine virtuelle ; elle garantit une haute disponibilité en cas de panne du serveur primaire. Il doit également posséder deux cartes réseau, l'une configurée pour le réseau public et l'autre configurée pour le réseau privé.
- **Server for the Quorum folder** (Serveur pour le dossier « Quorum ») : la troisième MV, elle est nécessaire à la création du dossier « Quorum ».
- **WDM Server** (Serveur WDM) : la quatrième et dernière MV sur laquelle WDM doit être installé.

Pré-requis pour la mise en cluster de la base de données

La mise en cluster de la base de données nécessite les éléments suivants :

- Quatre machines virtuelles VMware (MV), parmi lesquelles 2 d'entre elles doivent contenir deux adaptateurs réseau chacune.
- Version de Microsoft SQL Server Database (version autonome) prise en charge. Pour plus d'informations sur les bases de données prises en charge, voir Support Information (Informations de prise en charge).

  REMARQUE : les étapes de la mise en cluster de bases de données exposées dans ce guide sont effectuées sous Microsoft SQL Server 2012. Cependant, la mise en cluster de bases de données est possible sur d'autres versions de SQL Server prises en charge.

  Toutes les MV doivent être connectées à un domaine Active Directory (AD).
- Les quatre MV doivent être équipées de Windows Server 2008 R2 Enterprise.

REMARQUE : Vous ne pouvez pas utiliser SQL Server Express pour la mise en cluster de la base de données.

Configuration de la MV principale et de la MV secondaire

Une fois que vous avez créé les machines virtuelles sur le serveur, vous devez les configurer pour qu'elles prennent en charge la mise en cluster. Vous devez configurer les nœuds principal et secondaire en suivant la procédure décrite ci-dessous.

À propos de cette tâche

Pour configurer la MV principale et la MV secondaire

Étapes

1 Lancez le client vSphere sur n'importe quel système présent sur le réseau et sélectionnez la MV.

2 Cliquez avec le bouton droit et sélectionnez **Edit Settings** (Modifier les paramètres). Cliquez sur **Add** (Ajouter) pour ajouter une carte réseau supplémentaire (également appelée nœud).

3 Sur l'écran **Add Hardware** (Ajouter du matériel), sélectionnez **Ethernet Adapter** (Adaptateur Ethernet) et cliquez sur **Next** (Suivant).

4 Sélectionnez le sous-réseau dans la liste déroulante **Network label** (Étiquette réseau), puis cliquez sur **Next** (Suivant).

5 Cliquez sur **Finish** (Terminer).

6 Sur l'écran **VM Properties** (Propriétés des MV), vérifiez que deux nœuds sont présents.

7 Lancez l'écran **Network Connections** (Connexions réseau) dans **Control Panel** → **Réseau et Internet** (Panneau de configuration) → **Network Connections** (Connexions réseau), puis renommez les connexions réseau en **Private** (Privé) et **Public**.

REMARQUE : Il doit y avoir deux sous-réseaux pour deux cartes réseau, c'est-à-dire un sous-réseau pour le réseau Public (PDB) et un sous-réseau pour le réseau Privé (PDB). De même pour les deux cartes réseau sur le serveur SDB

8 Vérifiez que l'option **Public Network** (Réseau public) est en première position dans la fenêtre **Advanced Settings** (Paramètres avancés).

9 Pour ouvrir la fenêtre **Advanced Settings** (Paramètres avancés), appuyez sur le bouton « Alt » afin d'accéder au menu **Advanced** (Avancé) de l'écran **Network Connections** (Connexions réseau), puis sélectionnez l'option **Advanced Settings** (Paramètres avancés).

10 Sur l'écran **Network Connections** (Connexions réseau), sélectionnez **Public**, effectuez un clic droit et sélectionnez **Properties** (Propriétés).

11 Dans la fenêtre **Advanced Settings** (Paramètres avancés), sélectionnez **IPv4**, puis cliquez sur **Properties** (Propriétés).

12 Saisissez les valeurs **IP address** (Adresse IP), **Subnet mask** (Masque de sous-réseau), **Default gateway** (Passerelle par défaut) ainsi que **Preferred DNS server** (Serveur DNS souhaité). Cliquez sur OK.

13 Répétez les étapes 10 et 11 pour le réseau privé.

14 Vérifiez que le réseau privé contient uniquement l'adresse IP et le masque de sous-réseau. La passerelle par défaut ou les serveurs DNS ne doivent pas être définis.

15 Assurez-vous que les serveurs puissent communiquer à travers ce réseau afin que les nœuds puissent également communiquer entre eux en utilisant ce réseau.

16 Lancez Server Manager (Gestionnaire de serveur) depuis **Start** → **Administrative Tools** (Démarrer → Outils d'administration). Sélectionnez **Features** (Fonctionnalités).

17 Cliquez sur **Add Features** (Ajouter des fonctionnalités) pour lancer l'Assistant **Add Features** (Ajouter des fonctionnalités).

18 Sélectionnez **Failover Clustering** (Clustering de basculement), puis cliquez sur **Suivant** (Next).

19 Vérifiez que l'option **Failover Clustering** (Clustering de basculement) apparaît dans l'écran **Confirm Installation Selections** (Confirmer les sélections d'installation). Cliquez sur **Install** (Installer). La progression de l'installation s'affiche.

20 Une fois l'installation terminée, vérifiez les résultats de celle-ci puis cliquez sur **Close** (Fermer).

Étape suivante

Après l'installation de la Mise en cluster de basculement, redémarrez le serveur.

Validation d'une configuration

À propos de cette tâche

Après l'installation de la mise en cluster de basculement, vous devez valider la configuration sur le nœud principal. Pour valider la configuration :

Étapes

1 Lancez le Server Manager (Gestionnaire de serveur) du nœud principal depuis **Start** (Démarrer) → **Administrative Tools** (Outils d'administration).

2 Sélectionnez **Failover Cluster Manager** (Gestionnaire du cluster de basculement) dans **Features** (Fonctionnalités).

3 Cliquez sur **Validate a Configuration** (Valider une configuration) pour lancer l'Assistant.

4 Cliquez sur **Next** (Suivant) pour ajouter le nœud principal et le nœud secondaire.

5 Saisissez le nom d'hôte du nœud principal.

6 Cliquez sur **Add** (Ajouter) pour sélectionner les serveurs. L'écran affiche le message suivant lors de l'ajout des serveurs : *« The operation is taking longer than expected »* (L'opération prend plus longtemps que prévu). Vous devez attendre quelques minutes pour que les serveurs soient ajoutés.

7 Une fois les serveurs sélectionnés, ils sont affichés sous « Selected Servers » (Serveurs sélectionnés). Cliquez sur **Next** (Suivant).

8 Un cluster multisites n'a pas besoin de passer la validation du stockage. Pour ignorer le processus de validation du stockage, cliquez sur Run only the tests I select (Exécuter uniquement les tests que je sélectionne) et cliquez sur **Next** (Suivant).

9 Sur l'écran **Test Selection** (Sélection du test), décochez l'option **Storage** (Stockage) et cliquez sur **Next** (Suivant) pour continuer.

L'écran « Confirmation » s'affiche.

10 Cliquez sur **Next** (Suivant) pour commencer à exécuter les tests de validation sur les nœuds principal et secondaire (dans ce cas, cluster1 et cluster2). L'état des tests de validation s'affiche à l'écran.

11 Affichez le récapitulatif des validations et cliquez sur **Finish** (Terminer).

Création d'un cluster sur le nœud principal

À propos de cette tâche

Après avoir installé et validé la fonction **Failover Cluster Manager** (Gestionnaire du cluster de basculement) sur le nœud principal, vous pouvez créer un cluster.

Pour créer un cluster sur le nœud principal, procédez comme suit :

Étapes

1 Lancez le Server Manager (Gestionnaire de serveur) sur le nœud principal, sélectionnez **Failover Cluster Manager** (Gestionnaire du cluster de basculement) dans **Features** (Fonctionnalités), puis cliquez sur **Create a Cluster** (Créer un cluster).

2 Cliquez sur **Next** (Suivant) dans l'Assistant.

3 Cliquez sur **Next** (Suivant) pour continuer et, sur l'écran **Select Servers** (Sélectionner des serveurs), saisissez le nom d'hôte du nœud principal, puis cliquez sur **Add** (Ajouter) pour ajouter le serveur

4 Saisissez le nom du nœud secondaire et cliquez sur **Add** (Ajouter).

5 Une fois les serveurs ajoutés, cliquez sur **Next** (Suivant) pour continuer. Vous êtes invité à valider votre cluster. Sélectionnez **No** (Non) comme votre cluster est validé.

6 Sélectionnez la seconde option sur l'écran, puis cliquez sur **Next** (Suivant) pour continuer.

7 Indiquez un nom pour le cluster et une adresse IP pour administrer le cluster. Le nom que vous indiquez est prévu pour l'administration du cluster. Il ne doit pas être identique au nom de la ressource du cluster SQL que vous allez créer ultérieurement. Entrez **WINCLUSTER** comme nom de cluster et entrez l'adresse IP. Cliquez sur **Next (Suivant)** pour continuer.

> **REMARQUE : Il s'agit également du nom de l'ordinateur que vous devez autoriser pour le quorum de partage de fichiers majoritaires, qui est décrit plus loin dans ce document. Pour plus d'informations, voir Implémentation d'un quorum à nœud et partage de fichiers majoritaires.**

8 Confirmez et cliquez sur **Next** (Suivant).

La progression de la formation du cluster s'affiche à l'écran. Si vous avez effectué toutes les étapes correctement, la formation du cluster aboutit. Si vous voyez un symbole d'avertissement jaune à l'écran, il indique que la formation du cluster a abouti, mais avec des avertissements

9 Cliquez sur **View Report** (Affichage du rapport) pour consulter les avertissements pendant la formation du cluster. Le rapport s'affiche avec les messages d'avertissement surlignés en jaune.

10 Ignorez les messages d'avertissement et cliquez sur **Finish** (Terminer) pour achever le processus de mise en place du cluster.

Implémentation d'un quorum à nœud et partage de fichiers majoritaires

Un quorum est une conception permettant de traiter les problèmes de communication entre les ensembles de nœuds de cluster afin que deux serveurs ne tentent pas d'héberger simultanément un groupe de ressources et d'écrire sur le même disque en même temps. Avec ce concept de quorum, le cluster va forcer l'arrêt du service de cluster dans l'un des sous-ensembles de nœuds pour garantir qu'un groupe de ressources particulier n'est détenu que par un seul vrai propriétaire. La configuration du quorum Node and File Share Majority (Nœud et partage de fichiers majoritaires) est généralement utilisée par les clusters multisites. Cette configuration est utilisée lorsqu'il existe un même nombre de nœuds de cluster, afin qu'il puisse être utilisé indifféremment avec le mode de quorum Node and Disk Majority (Nœud et disques majoritaires). Dans cette configuration, chaque nœud obtient 1 voix et, en plus, 1 partage de fichiers à distance obtient 1 vote.

À propos de cette tâche

Pour configurer un quorum à nœud et partage de fichiers majoritaires :

Étapes

1 Sélectionnez la machine virtuelle (MV) désignée pour la création du dossier du quorum, puis créez un dossier intitulé **Quorum**, et partagez l'emplacement du dossier.

2 Effectuez un clic droit sur le dossier intitulé **Quorum** et sélectionnez **Share with (Partager avec) → Specific people** (Personnes spécifiques).

3 Dans la fenêtre **File Sharing** (Partage de fichiers), sélectionnez **Everyone** (Tout le monde). Sélectionnez **Read/Write permission** (Autorisation de lecture/écriture) et cliquez sur **Share** (Partager).

Le dossier est partagé en tant que **\\<Nom de la MV>\Quorum**.

4 Vous devez maintenant modifier votre type de quorum. Lancez le **Server Manager** (Gestionnaire de serveur) sur le nœud principal, et sélectionnez **Failover Cluster Manager** (Gestionnaire du cluster de basculement) sous **Features** (Fonctionnalités).

5 Effectuez un clic droit sur le cluster et sélectionnez **More Actions Plus d'options → Configure Cluster Quorum Settings** (Configurer les paramètres du quorum du cluster).

6 Sélectionnez l'option **Node and File Share Majority (for clusters with special configurations)** (Nœud et partage de fichiers majoritaires (pour les clusters disposant de configurations spéciales)), puis cliquez sur **Next** (Suivant).

7 Saisissez le chemin d'accès au dossier partagé que vous avez créé sur la troisième MV, puis cliquez sur **Next** (Suivant).

8 Confirmez l'emplacement du dossier partagé, puis cliquez sur **Next** (Suivant).

La configuration des paramètres du quorum pour le cluster est terminée.

9 Cliquez sur **Finish** (Terminer) pour achever le processus et afficher la configuration du quorum pour le cluster.

Installation de .NET Framework sur le nœud principal et le nœud secondaire

À propos de cette tâche

Microsoft .NET Framework est nécessaire à l'installation du logiciel indépendant SQL Server 2012 (ou toute autre version de SQL Server prise en charge) sur le nœud principal et le nœud secondaire.

Pour installer .NET Framework :

Étapes

1 Lancez **Server Manager** (Gestionnaire de serveur) sur les MV identifiées comme nœud principal et nœud secondaire.

2 Cliquez sur **Features** (Fonctionnalités) dans **Server Manager** (Gestionnaire de serveur) pour lancer l'Assistant **Add Features Wizard** (Assistant ajouter des fonctions) et sélectionnez **.NET Framework 3.5.1 Features** (Fonctionnalités .NET Framework 3.5.1).

3 Cliquez sur **Next** (Suivant), vous serez alors inviter à installer les services et fonctionnalités ROL nécessaires à l'installation des fonctionnalités de .NET Framework 3.5.1.

4 Cliquez sur **Add Required Role Services** (Ajouter les services de rôle requis). L'option .NET Extensibility (Extensibilité .NET) est sélectionnée par défaut. Cliquez sur **Next (Suivant)** pour continuer.

5 Confirmez les choix d'installation et cliquez sur **Install** (Installer).

6 Une fois l'installation des composants sélectionnés terminée, les résultats de l'installation sont affichés.

7 Cliquez sur **Close** (Fermer) pour terminer l'installation de .NET Framework.

Installation de SQL Server sur le nœud principal et le nœud secondaire

Installer SQL Server sur les deux nœuds et le configurer pour qu'il fonctionne en cluster est une étape clé dans la mise en place d'un cluster de base de données à haute disponibilité. Cette section présente les étapes nécessaires à l'installation et à la configuration de SQL Server 2012 en version autonome sur les deux nœuds. Si vous souhaitez installer une version de SQL Server prise en charge, consultez les instructions d'installation fournies par Microsoft.

Pour installer une version autonome de SQL Server 2012 sur les deux nœuds :

1 Lancez l'installation de SQL Server 2012.

2 Cliquez sur **Installation** et sélectionnez **New SQL Server stand-alone installation or add features to an existing installation (Nouvelle installation autonome SQL Server ou ajout de fonctionnalités à une installation existante)**.

3 Vérifiez que l'écran des règles de support du programme d'installation n'affiche aucun problème. Cliquez sur **Next (Suivant)** pour continuer.

4 Saisissez la clé produit, puis cliquez sur **Next (Suivant)**.

5 Vérifiez la mise à jour produit et cliquez sur **Next (Suivant).**

6 Acceptez le contrat de licence et cliquez sur **Next (Suivant)**.

7 Sélectionnez l'option **SQL Server Feature Installation (Installation de fonctionnalités SQL Server)**, puis cliquez sur Next (Suivant).

8 Sur l'écran **Feature Selection (Sélection de fonctionnalités)**, sélectionnez les fonctionnalités **Database Engine Services (Services Moteur de base de données)** ainsi que toutes les autres fonctionnalités présentes à l'intérieur de celle-ci.

9 Sélectionnez la fonctionnalité Management Tools – Basic (Outils de gestion – basique) ainsi que la fonctionnalité sous cette dernière. Cliquez sur **Next (Suivant)**.

10 Vérifiez que l'écran des règles d'installation n'affiche aucun problème. Cliquez sur **Next (Suivant)**.

11 Sur l'écran **Instance Configuration (Configuration de l'instance)**, vérifiez que l'option **Default instance (Instance par défaut)** est sélectionnée.

12 Cliquez sur **Next (Suivant)** pour afficher l'espace disque requis.

13 Cliquez sur **Next (Suivant)** pour afficher la Configuration du serveur.

14 Saisissez les informations d'identification du domaine pour la configuration du serveur, puis cliquez sur **Next (Suivant)**.

15 Sur l'écran de Configuration du moteur de base de données, sélectionnez **Mixed Mode (Mode mixte)**, saisissez le mot de passe d'administrateur SQL, puis cliquez sur **Add Current User (Ajouter l'utilisateur actuel)**.

16 Cliquez sur **Next (Suivant)** dans la fenêtre **Error Reporting (Rapport d'erreurs)**.

17 Cliquez sur **Next (Suivant)** et vérifiez que la configuration de l'installation n'affiche aucune panne.

18 Cliquez sur **Install (Installer)** pour lancer le processus d'installation.

19 Une fois l'installation terminée, son état est affiché. Affichez l'état et cliquez sur **Close (Fermer)** pour terminer l'installation.

REMARQUE : si un avertissement provenant du pare-feu Windows apparaît au cours de l'installation de SQL Server, vous pouvez l'ignorer et reprendre l'installation. Si nécessaire, vous pouvez ajouter le port 1433 aux exceptions du pare-feu SQL Server.

Installation du cluster de basculement SQL Server sur le nœud principal

Après l'installation de SQL Server 2012 sur le nœud principal et le nœud secondaire, vous devez configurer les deux nœuds afin qu'ils prennent en charge la mise en cluster de basculement.

Pour installer le cluster de basculement de SQL Server 2012 sur le nœud principal :

1 Lancez l'installation de SQL Server 2012.

2 Cliquez sur **Installation** et sélectionnez **New SQL Server failover cluster installation** (Nouvelle installation de cluster de basculement SQL Server).

3 Vérifiez que l'écran **Setup Support Rules** (Configurer les règles de prise en charge) n'affiche aucun problème. Cliquez sur **OK**.

4 Saisissez la clé produit, puis cliquez sur **Next** (Suivant).

5 Acceptez le contrat de licence et cliquez sur **Next** (Suivant).

6 Vérifiez les mises à jour produit et cliquez sur **Next** (Suivant).

7 Vérifiez que l'écran **Configurer les règles de prise en charge** n'affiche aucun problème ou erreur. Vous pouvez ignorer les avertissements et cliquer sur **Next** (Suivant).

8 Sélectionnez l'option **SQL Server Feature Installation** (Installation des fonctionnalités de SQL Server) sur l'écran **Setup Role** (Configurer rôle), puis cliquez sur **Next** (Suivant).

9 Sélectionnez toutes les options se trouvant dans **Instance Features → Database Engine Services** (Fonctionnalités d'instance → Services de moteur de base de données), et **Shared Features → Client Tools Connectivity** (Fonctionnalités partagées → Connectivité des outils client) sur l'écran **Feature Selection** (Sélection des fonctionnalités). Cliquez sur **Next** (Suivant).

10 Vérifiez que l'écran **Feature Rules** (Règles des fonctionnalités) n'affiche aucun problème. Cliquez sur Next (Suivant).

11 Sur l'écran **Instance Configuration** (Configuration d'instance), saisissez les informations suivantes :

- **SQL Server Network Name** (Nom de réseau SQL Server) – WDMCLUSTER
- **Named Instancex** (Named Instance) – WDMCLUST
- **Instance ID** (Identification d'instance) – WDMCLUST

Cliquez sur Next (Suivant).

12 Vérifiez l'**Espace disque requis** et cliquez sur **Next** (Suivant).

13 Laissez les paramètres par défaut de l'écran **Cluster Resource Group** (Groupe de ressources du cluster) et cliquez sur **Next** (Suivant).

14 Étant donné que vous avez configuré une mise en cluster **File Share Majority** (Partage de fichiers majoritaires), vous n'avez pas besoin de sélectionner un disque. Cliquez sur **Next** (Suivant) sur l'écran **Cluster Disk Selection** (Sélection de disque de cluster).

15 Sur l'écran **Cluster Network Configuration** (Configuration réseau du cluster), activez l'option **IP4** et saisissez l'adresse IP du cluster de basculement SQL, puis cliquez sur **Next** (Suivant) pour arriver à l'écran **Server Configuration** (Configuration du serveur).

16 Saisissez les informations de connexion de domaine pour l'agent SQL Server et le moteur de base de données SQL Server, puis cliquez sur **Next** (Suivant).

17 Sur l'écran **Database Engine Configuration** (Configuration du moteur de base de données), sélectionnez l'option **Mixed Mode** (Mode mixte) (authentification Windows et authentification SQL Server) et saisissez le mot de passe d'administrateur SQL.

18 Cliquez sur **Add Current User** (Ajouter un utilisateur actuel) pour ajouter l'utilisateur Administrateur, puis cliquez sur **Next** (Suivant).

19 Vous êtes invité à installer un cluster de basculement SQL. Cliquez sur **Yes** (Oui) à l'invite.

20 Cliquez sur l'onglet **Data Directories** (Répertoires de données) sur l'écran **Database Engine Configuration** (Configuration du moteur de base de données). Dans l'emplacement du répertoire racine des données, entrez **\\<*Nom de la machine virtuelle du quorum*> \quorum**. Cliquez sur Next (Suivant).

21 Vérifiez l'écran **Error Reporting** (Rapports d'erreur), puis cliquez sur **Next** (Suivant). Vous pouvez ignorer les avertissements.

22 Assurez-vous qu'aucune erreur ne soit présente sur l'écran **Cluster Installation Rules** (Règles d'installation du cluster). Cliquez sur Next (Suivant).

23 Cliquez sur **Install** (Installer) pour commencer l'installation.

24 L'écran **Installation Progress** (Progression de l'installation) affiche la progression de l'installation. Cliquez sur **Next** (Suivant) une fois l'installation terminée.

25 Cliquez sur **Close** (Fermer) pour terminer l'installation. Le **Failover Cluster Manager** (Gestionnaire du cluster de basculement) s'affiche sous **Server Manager** (Gestionnaire de serveur) sous **Features** (Fonctionnalités).

Procédure survenant après la mise en cluster

À propos de cette tâche

Cette section présente les différentes étapes que vous devez effectuer lorsque vous avez terminé la configuration du cluster. Ces étapes permettent à votre cluster de fonctionner sans aucun problème.

Suivez les étapes ci-dessous :

Étapes

1 Dans les deux nœuds du cluster, assurez-vous que les Services SQL Server sont exécutés avec les informations de connexion de domaine.

2 Lancez le **SQL Server Configuration Manager** (Gestionnaire de configuration SQL Server), puis sélectionnez **SQL Server Services** (Services SQL Server) → **SQL Server**. Cliquez avec le bouton droit et sélectionnez **Properties** (Propriétés).

3 Vérifiez les informations de connexion de domaine et cliquez sur **OK**.

4 Cliquez sur l'onglet **AlwaysOn High Availability** (Haute disponibilité AlwaysOn) sur les deux nœuds, puis sélectionnez **Enable AlwaysOn Availability Groups** (Activer les groupes de disponibilités AlwaysOn). Cliquez sur **OK**.

5 Installez la base de données WDM sur les MV identifiées comme nœud principal et nœud secondaire du cluster.

6 Exécutez le script suivant sur la base de données :

```
Use RapportDB
GO
Update Install set ServerName='NEWCLUSTER01' where Module='Rapport4DB'
```

7 Lorsque vous installez les composants WDM sans la base de données, assurez-vous d'indiquer le nom du cluster de la base de données SQL dans le champ « Server IP Address » (Adresse IP du serveur).

8 Créez la même structure de répertoires pointant vers l'emplacement de la base de données dans le nœud principal et le nœud secondaire. Par exemple, si la base de données est présente dans **C:\Program Files\WYSE\WDM\Database** dans le nœud principal, créez également la même structure dans le serveur secondaire.

9 Lancez SQL Server Management Studio sur le nœud principal. Ouvrez une session avec le nom d'utilisateur et le mot de passe SQL par défaut.

10 Effectuez un clic droit sur la base de données **RapportDB** et sélectionnez **Properties** (Propriétés).

11 Sur l'écran **Database Properties** (Propriétés de la base de données), changez le **Recovery Model** (Mode de récupération) en **Full** (Plein).

12 Effectuez un clic droit sur RapportDB et sélectionnez **Tasks→ Backup** (Tâches → Sauvegarde) pour réaliser une sauvegarde de RapportDB.

13 Laissez les paramètres par défaut sur l'écran **Backup Database** (Sauvegarde de la base de données), puis cliquez sur **OK**.

14 Effectuez un clic droit sur **AlwaysOn High Availability** (Haute disponibilité AlwaysOn) dans l'Explorateur d'objets et sélectionnez **New Availability Group Wizard** (Assistant Nouveau groupe de disponibilité).

15 Cliquez sur **Suivant** sur l'écran **Assistant Nouveau groupe de disponibilité**.

16 Donnez un nom au groupe de disponibilité, comme **Rapport_cluster** et cliquez sur **Next** (Suivant).

17 Sélectionnez la base de données et cliquez sur **Next** (Suivant).

18 Cliquez sur **Add Replica** (Ajouter réplica) et cochez les cases **Automatic Failover (up to 2)** (Basculement automatique (jusqu'à 2)) et **Synchronous commit (up to 3)** (Validation synchrone (jusqu'à 3).

Répétez l'étape pour le nœud secondaire.

19 Cliquez sur **Next** (Suivant).

20 Sélectionnez l'option **Full** (Plein) et précisez l'emplacement du dossier partagé ***<Nom de la machine quorum>*\quorum**. Cliquez sur **Next** (Suivant).

21 Vérifiez que l'écran **Validation** n'affiche aucune panne. Cliquez sur **Next** (Suivant).

22 Si un quelconque avertissement s'affiche à l'écran, vous pouvez l'ignorer et reprendre l'installation.

23 Cliquez sur **Finish** (Terminer) pour terminer l'installation du **Terminer** (Nouveau groupe de disponibilité).

24 La fenêtre de progression affiche la progression de l'installation. Cliquez sur **Next** (Suivant) une fois l'installation terminée.

25 Affichez les résultats, puis cliquez sur **Close** (Fermer).

26 Le nœud primaire et le nœud secondaire sont affichés sur le Studio de gestion de SQL Server.

27 Arrêtez le nœud secondaire et vérifiez que le nœud principal est en fonctionnement dans le cluster.

28 Lancez SQL Server Management Studio sur le nœud principal. Ouvrez une session avec le nom d'utilisateur et le mot de passe SQL par défaut.

29 Cliquez sur le nœud **Security** (Sécurité), sélectionnez **Login** (Connexion), cliquez avec le bouton droit et sélectionnez **New Login** (Nouvelle connexion) pour créer l'utilisateur de Rapport (Relation). Cette étape est importante pour que WDM fonctionne lorsque vous créez l'utilisateur pour l'authentification de SQL Server.

30 Sélectionnez **Server Roles** (Rôles du serveur), cochez la case **sysadmin**, puis cliquez sur **OK**.

31 Affichez l'utilisateur de **Relations** dans le **SQL Server Management Studio** (Studio de gestion de SQL Server).

32 Répétez les étapes 28 à 31 sur le nœud secondaire.

Étape suivante

REMARQUE : S'il y a un basculement de la base de données principale à la base de données secondaire, vous devrez redémarrer l'interface utilisateur WDM.

Exécution de l'utilitaire de configuration haute disponibilité (HA, High Availability)

À propos de cette tâche

WDM nécessite une connexion au cluster pour fonctionner à l'intérieur de ce dernier et s'assurer qu'aucune immobilisation ne survient.

L'utilitaire de configuration HA est disponible après avoir installé WDM sur un nœud distinct, autre que le nœud principal et le nœud secondaire.

Étapes

1 Connectez-vous au système sur lequel vous avez installé WDM.

2 Lancez **HAConfigureUtility** dans **Start** > **All Programs** > **Dell Wyse Device Manager** > **Utilities** (Démarrer > Tous les programmes > Gestionnaire de périphériques Wyse de Dell > Utilitaires).

3 Saisissez les informations suivantes :

- **Configure Setup As** (Configurer en tant que) : sélectionnez **Cluster** dans la liste déroulante.
- **Database Name** (Nom de base de données) : ceci est affiché par défaut et ne peut être modifié.
- **Database Server** (Serveur de base de données) : précisez le nom d'hôte du cluster de la base de données. Par exemple, **WDMCLUSTER**.
- **Database User Name** (Nom d'utilisateur de la base de données) : précisez **Relation** comme l'utilisateur de la base de données.
- **Database Password** (Mot de passe de la base de données : précisez le mot de passe de l'utilisateur de Relation.

4 Cliquez sur **Configure** (Configurer).

Les informations de connexion sont affichées sur le volet inférieur de l'utilitaire.

Ajout d'une licence WDM

À propos de cette tâche

WDM requiert une licence pour fonctionner. Le code de licence est généré en fonction de la base de données. WDM est normalement installé sur une base de données autonome, puis déplacé vers un cluster. Par conséquent, une fois la configuration du cluster terminée, vous devez générer à nouveau le code de licence pour le cluster.

Pour ajouter une licence au serveur WDM :

Étapes

1 Lancez Wyse Device Manager (WDM). Le message d'erreur suivant s'affiche : « *Application Function: ScopeItems_Expand: 13 Type mismatch* » (Fonction d'application : ScopeItems_Expand : incompatibilité de type 13).

2 Cliquez sur **OK** et ajouter la licence depuis la console WDM.

3 Pour initialiser un basculement, arrêtez la base de données du nœud principal, puis redémarrez la console WDM.

6

Configuration de l'équilibrage de charge

Si vous utilisez WDM pour gérer des périphériques clients légers dans un environnement d'entreprise de grande taille, un seul serveur de gestion WDM ne suffira pas pour assurer la gestion d'un si grand nombre de périphériques. Cela risquerait d'entraîner des problèmes ou des retards au niveau des archivages clients, des exécutions planifiées ou des exécutions en temps réel de commandes.

Toutefois, l'équilibrage de charge permet, dans une large mesure, de résoudre ces problèmes. Cette configuration permet en effet d'installer et d'exécuter plusieurs serveurs de gestion WDM sur divers systèmes et configurer la fonction d'équilibrage de charge entre eux. WDM utilise la fonctionnalité de Demande de routage d'applications (ARR, Application Request Routing) Microsoft pour IIS 7 afin d'équilibrer la charge entre les serveurs de gestion. Cette section explique comment installer et configurer l'équilibrage de charge.

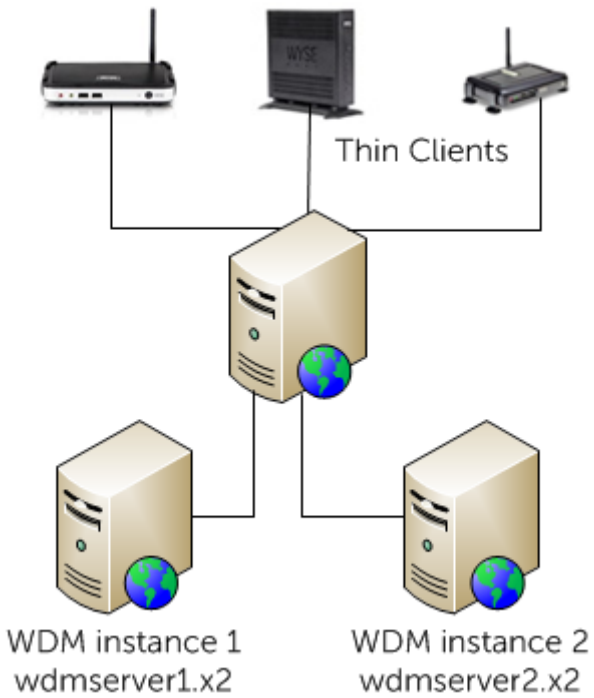


Figure 39. Configuration de l'équilibrage de charge WDM

Sujets :

- Configuration du serveur proxy ARR
- Installation de composants WDM
- Configuration de l'équilibrage de charge pour les périphériques Thread X 4.x
- Configuration de l'équilibrage de charge pour les appareils Thread X 5.x

Configuration du serveur proxy ARR

Le serveur proxy ARR (Application Routing Request) est le composant le plus important de l'équilibrage de charge. Ce serveur reçoit les requêtes provenant de systèmes clients légers et les achemine vers les différents serveurs de gestion WDM.

Prérequis

Avant de configurer le serveur proxy ARR, vous devez faire en sorte que :

- La configuration complète soit mise en place sur Windows 2008 Server R2 ou ultérieurs.
- Tous les composants de WDM soient installés sur un seul serveur.
- Seuls le serveur de gestion WDM et le service ThreadX 4.x soient installés sur un serveur différent.

REMARQUE : Vous pouvez configurer le serveur proxy ARR et les serveurs de gestion WDM sur plusieurs sous-réseaux appartenant au même domaine.

À propos de cette tâche

La configuration du serveur proxy ARR comprend les étapes suivantes :

Étapes

1. Installation d'IIS.
2. Installation du module ARR.
3. Configuration du processus de pool d'applications pour ARR.
4. Création d'une batterie de serveurs de gestion WDM.
5. Configuration de protocoles SSL
6. Configuration des propriétés de la batterie de serveurs pour ARR.
7. Configuration du filtrage des demandes
8. Configuration du FQDN du proxy dans les préférences WDM.

Installation des Services d'information Internet — IIS

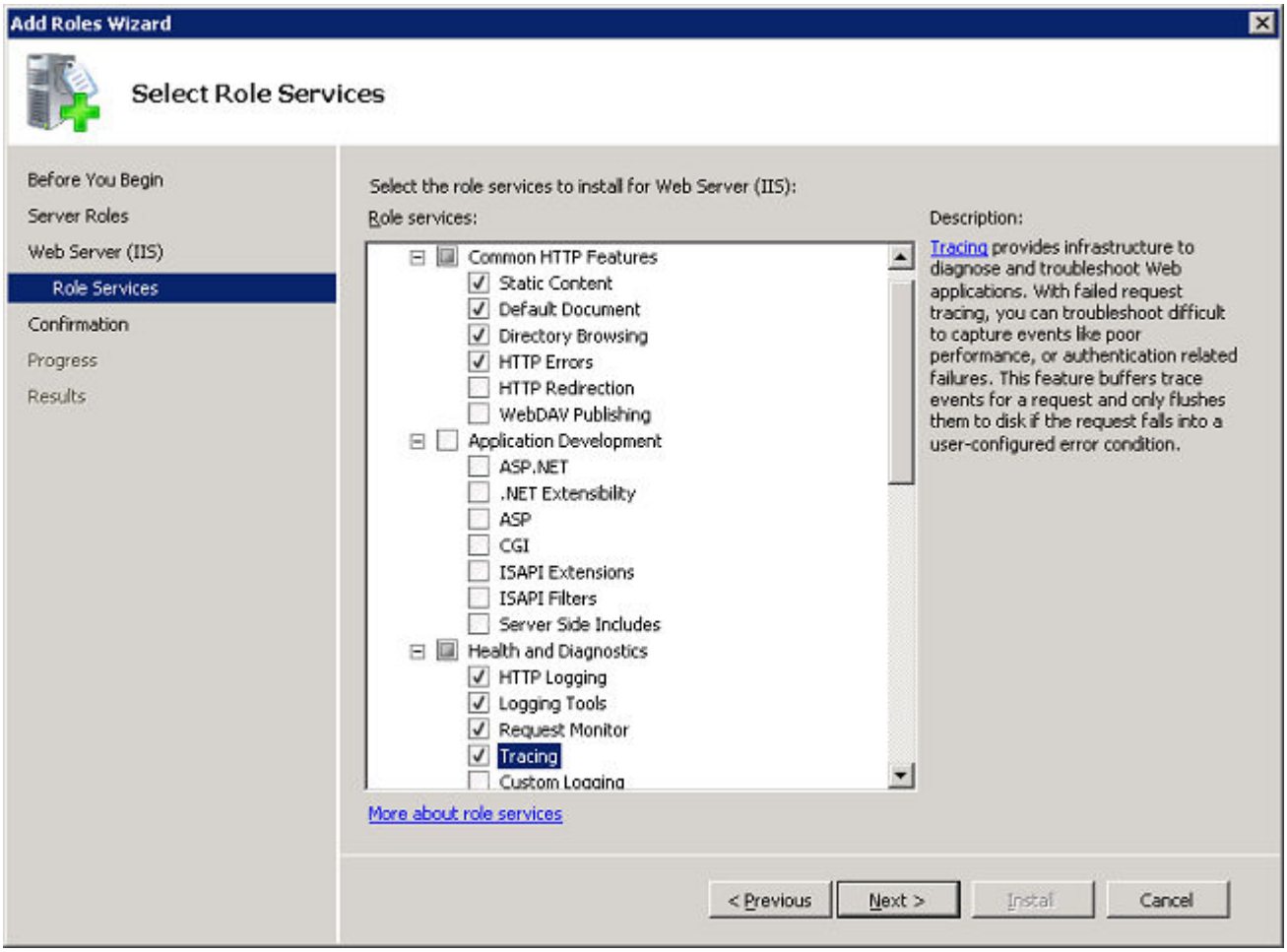
À propos de cette tâche

Installez Windows 2008 Server R2 sur le système identifié comme serveur proxy ARR.

Étapes

1. Connectez-vous au système en tant qu'administrateur et exécutez le **Server Manager (Gestionnaire de serveur)**.
2. Sélectionnez **Roles (Rôles)** dans le Server Manager (Gestionnaire de serveur) et cliquez sur **Add Roles (Ajouter des rôles)** dans le volet droit.

   L'Assistant **Add Roles Wizard (Ajout de rôles)** s'affiche.
3. Sélectionnez **Server Roles (Rôles du serveur)** et sélectionnez **Web Server (IIS) (Serveur Web (IIS))**, puis cliquez sur **Next (Suivant)**.



4 Sélectionnez les options suivantes :

Option	Sous-options
Common HTTP Features (Fonctions HTTP communes)	• Static Content (Contenu statique) • Default Document (Document par défaut) • HTTP Errors (Erreurs HTTP) • Directory Browsing (Recherche répertoire)
Health and Diagnostics (Intégrité et diagnostics)	• HTTP Logging (Connexion HTTP) • Request Monitor (Surveillance des requêtes) • Logging Tools (Outils de journalisation) • Tracing (Traçage)
Management Tools (Outils de gestion)	Sélectionnez toutes les sous-options.

5 Cliquez sur **Next (Suivant)** pour afficher le résumé.

6 Cliquez sur **Install (Installer)** pour installer IIS.

Installation du module ARR

Vous devez installer l'ARR (Application Request Routing) version 3.0 sur le système que vous avez identifié pour qu'il serve de serveur proxy ARR. Le programme d'installation est disponible sur le site de téléchargements Microsoft à l'adresse https://www.microsoft.com/en-us/download/details.aspx?id=47333. Téléchargez le fichier **ARRv3_0.exe** et installez-le.

Configuration du processus de pool d'applications pour ARR

Toutes les demandes et les réponses HTTP pour les sites à contenu passent nécessairement par la Demande de routage d'applications (ARR). Pour assurer son fonctionnement correct, vous devez faire en sorte que le processus de travail du site Web par défaut de l'ARR soit toujours en fonctionnement.

À propos de cette tâche

Pour configurer le processus de pool d'applications :

Étapes

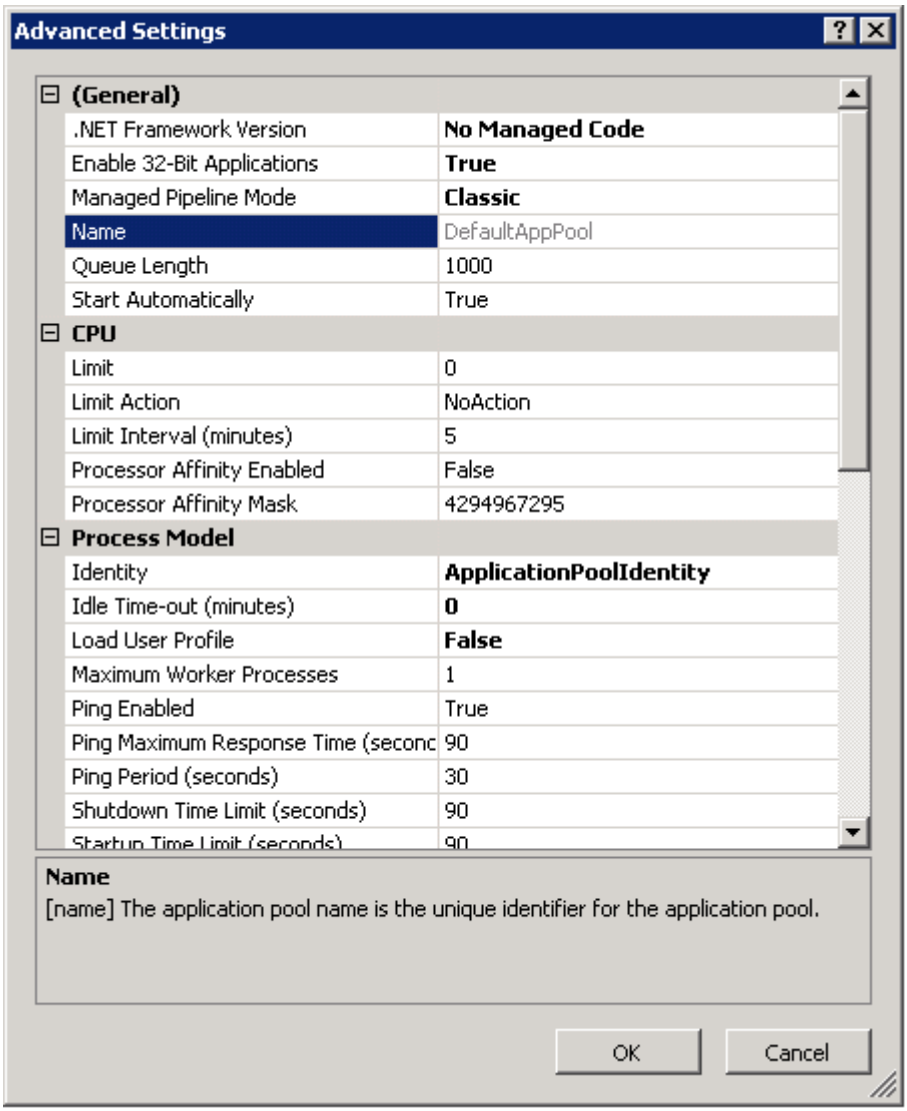
1 Connectez-vous au serveur proxy ARR et lancez IIS manager (Gestionnaire des services IIS).

2 Sélectionnez **Application Pools (Pools d'applications)** dans le nœud racine.

Le volet droit affiche **DefaultAppPool** en tant que pool d'applications pour le site Web par défaut.

3 Sélectionnez **DefaultAppPool**, puis cliquez sur **Edit Application Pool (Modifier le pool d'applications)** dans le volet **Action (Action)**.

4 Sélectionnez **Advanced Settings (Paramètres avancés)** pour afficher la fenêtre **Advanced Settings (Paramètres avancés)**.



5 Dans **Process Model (Modèle du processus)**, changez la valeur **Identity (Identité)** de **LocalSystem** en **ApplicationPoolIdentity**.

6 Faites passer **Idle Time-out (minutes) (Délai d'inactivité en minutes)** à 0 pour désactiver le paramètre. Cliquez sur **OK** pour enregistrer les modifications.

Création d'une batterie de serveurs de gestion WDM

À propos de cette tâche

Pour créer et définir une batterie de serveurs :

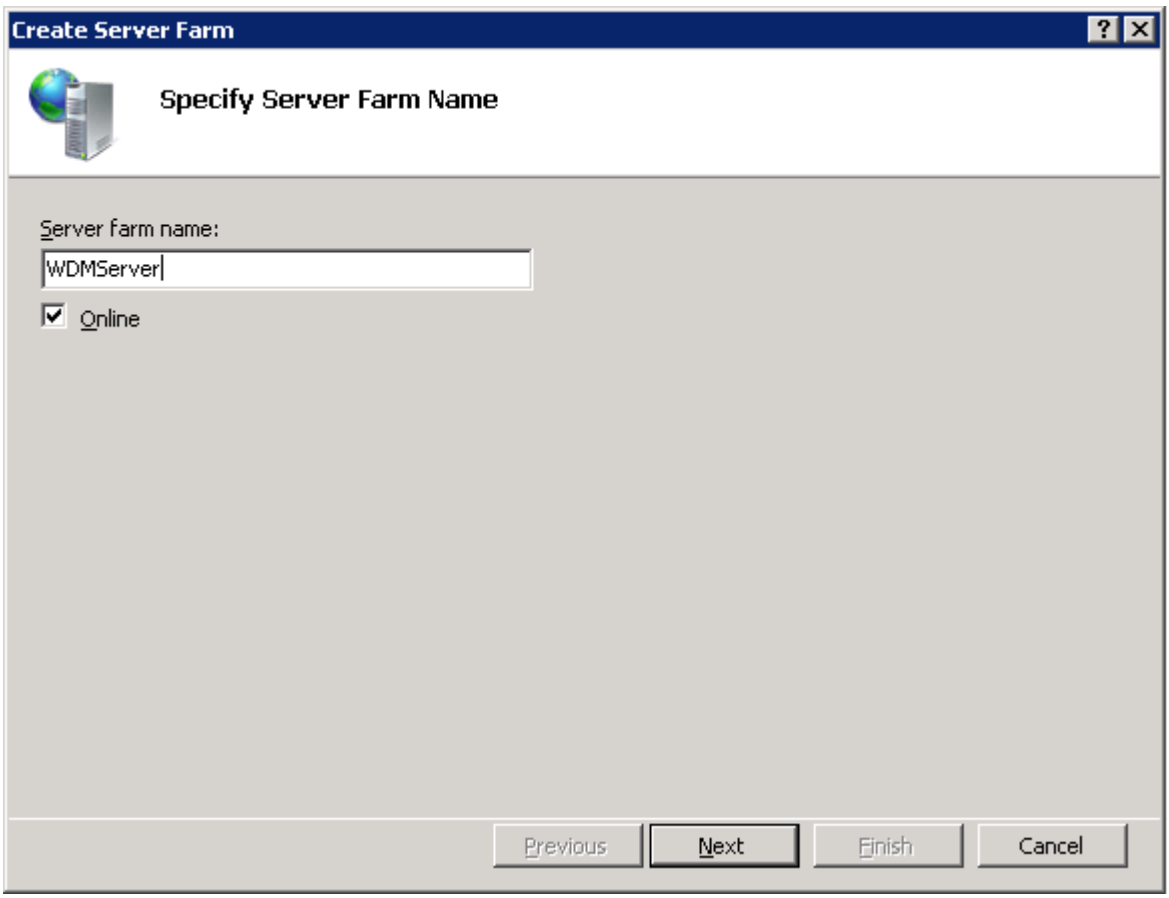
Étapes

1 Connectez-vous au système de serveur proxy ARR et lancez IIS manager (Gestionnaire des services IIS).

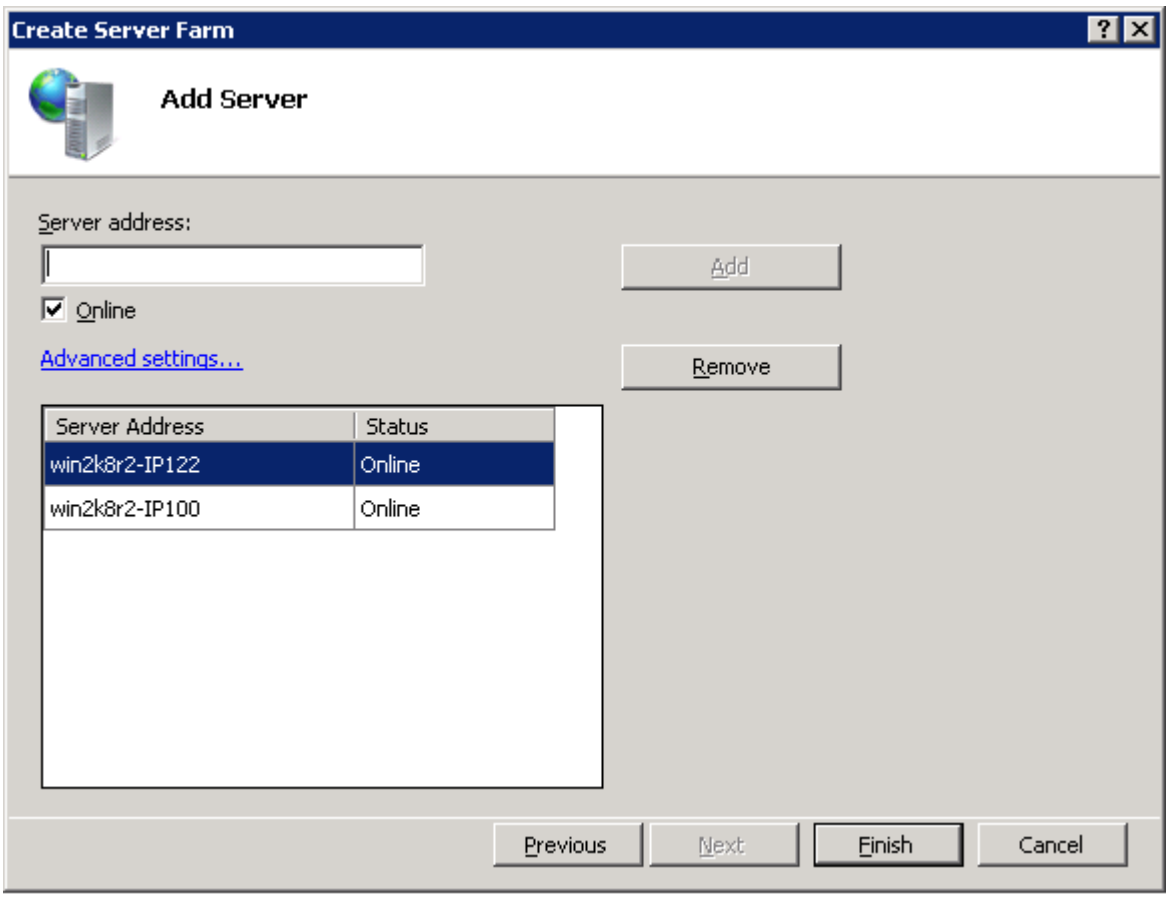
2 Sélectionnez **Server Farms (Batteries de serveurs)** sous le nœud racine. Cette option n'est disponible qu'après l'installation du module proxy ARR.

3 Cliquez avec le bouton droit, puis sélectionnez **Create Server Farm (Créer une batterie de serveurs)** dans le menu.

L'écran **Create Server Farm (Créer une batterie de serveur)** s'affiche alors.



4 Saisissez un nom pour la batterie de serveurs. Par exemple, **WDMServerFarm.** Cliquez sur **Next (Suivant)** pour ajouter les serveurs de gestion WDM.



5 Saisissez le nom d'hôte du serveur WDM et cliquez sur **Add (Ajouter)**. Vous pouvez ajouter tous les serveurs où vous avez installé le serveur de gestion WDM.

6 Cliquez sur **Finish (Terminer)** pour ajouter tous les serveurs à la batterie.

Après l'ajout des serveurs et la création de la batterie, un message apparaît vous invitant à redéfinir les règles de routage de toutes les demandes afin que celles-ci arrivent automatiquement à la batterie de serveurs.

7 Cliquez sur **Yes (Oui)** afin que IIS manager (Gestionnaire des services IIS) crée une règle de réécriture d'URL pour diriger toutes les demandes entrantes vers cette batterie de serveurs.

Configuration de protocoles SSL

L'une des fonctionnalités dans ARR est **SSL off-loading** (Déchargement SSL). Il s'agit d'une fonctionnalité dans laquelle les communications entre les clients et le serveur proxy ARR sont effectuées via SSL, et les communications entre le serveur proxy ARR et les serveurs de gestion WDM sont effectuées en texte clair. En activant cette fonctionnalité, vous pouvez optimiser les ressources du serveur sur les serveurs de gestion WDM.

Prérequis

Vous devez tout d'abord créer le certificat SSL sur le serveur proxy ARR.

À propos de cette tâche

Pour créer et configurer le certificat SSL :

Étapes

1 Connectez-vous au serveur proxy ARR et lancez IIS Manager (Gestionnaire des services IIS).

2 Sélectionnez le nœud racine et ouvrez la page **Server Certificates** (Certificats de serveur) située dans le volet droit.

3 Cliquez sur **Create Domain Certificate** (Créer un certificat de domaine) dans le volet Actions.

4 Indiquez le nom du serveur proxy ARR dans l'Assistant **Create Certificate** (Créer un certificat).

5 Cliquez sur **Next** (Suivant) pour achever la création du certificat.

6 Sélectionnez **Default Web Site** (Site Web par défaut) dans **Sites**, puis cliquez sur **Bindings** (Liaisons) dans le volet **Actions**.

7 Assignez le certificat à la liaison **HTTPS**.

8 Accédez à **Server Farm** (Batterie de serveurs) et double-cliquez sur **Created Farm** (Batterie créée).

9 Double-cliquez sur **Routing Rules** (Règles de routage) et sélectionnez l'option **Enable SSL offloading** (Activer le déchargement SSL) si vous souhaitez que la communication entre les serveurs proxy ARR et les serveurs de gestion WDM s'effectue en texte brut. Vous devrez également ajouter les ports HTTP et HTTPS aux liaisons de sites Web par défaut sur les systèmes de serveur de gestion WDM individuels.

REMARQUE :

Si vous souhaitez que la communication entre le serveur proxy ARR et les serveurs de gestion WDM s'effectue également sur le protocole HTTPS, vous devez désactiver la fonctionnalité **SSL off-loading** (Déchargement SSL) et configurer SSL sur les serveurs de gestion WDM. Si vous utilisez un certificat auto-signé pour configurer le SSL sur le serveur de gestion WDM, importez ce certificat vers **Trusted Root Certificate Authorities store** (Espace de stockage des Autorités de certification racine de confiance) de l'ordinateur local, associé au serveur proxy ARR, en suivant les étapes mentionnées sur le site web Microsoft : http://technet.microsoft.com/en-us/library/cc754841.aspx#BKMK_addlocal

Configuration des propriétés de la batterie de serveurs pour l'ARR

Une fois la batterie de serveurs créée et définie, vous devez déterminer des propriétés supplémentaires pour la gestion du comportement de l'ARR.

1 Connectez-vous au serveur proxy ARR et lancez IIS Server Manager (Gestionnaire des services IIS).

2 Sélectionnez la batterie de serveurs créée. Les options suivantes s'affichent sur le volet droit :

- Caching (Mise en cache)
- Health Test (Test d'intégrité)
- Load Balance (Équilibrage de charge)
- Monitoring and Management (Surveillance et gestion)
- Proxy
- Routing Rules (Règles de routage)
- Server Affinity (Affinité du serveur)

3 Sélectionnez **Caching (Mise en cache)**.

a Déselectionnez l'option **Enable disk cache (Activer le cache du disque)** pour désactiver la mise en cache.

b Réglez **Memory cache duration (Durée de la mise en cache mémoire)** sur 0.

4 Sélectionnez **Health Test (Test d'intégrité)**.

a Saisissez le nom de domaine complet (FQDN) du serveur proxy ARR dans le champ **URL**. La valeur doit correspondre à **http(s)/<ProxyFQDN>/hserver.dll?&V93**. Il s'agit de l'URL utilisée par l'ARR pour envoyer les demandes au serveur de gestion WDM dans le but de vérifier l'intégrité d'une batterie de serveurs en particulier.

b Définissez l'intervalle après lequel le Test d'intégrité ARR répète la vérification de l'intégrité. L'intervalle par défaut est de 30 secondes. Vous pouvez le régler sur 180 secondes.

c Définissez le délai d'attente pour l'URL en question. Ce délai correspond à la période de temps après laquelle un manque de réponse de la part du serveur entraîne son marquage comme **Unhealthy** (Défectueux).

d Définissez les **Acceptable Status codes (Codes d'état acceptables)** sur **200-399**. Si l'URL d'intégrité renvoie un code d'état qui ne correspond pas à la valeur indiquée dans **Acceptable Status Codes (Codes d'état acceptables)**, alors l'ARR marque le serveur comme défectueux.

e Définissez la valeur de texte **Server Healthy (Serveur sain)** dans le champ **Response Match (Correspondance des réponses)**. Le texte dans le champ **Response Match (Correspondance des réponses)** est comparé à l'entité de réponse de chaque serveur et, si la réponse d'un des serveurs ne contient pas la chaîne précisée dans la correspondance de réponse, alors ce serveur est indiqué comme étant défectueux.

f Cliquez sur **Verify URL (Vérifier URL)**. Cela devrait être effectué pour tous les serveurs de gestion WDM présents dans la batterie de serveurs.

5 Modifiez l'algorithme **Load Balance (Équilibrage de charge)**.

a Sélectionnez l'option **Weighted Round Robin (Permutation circulaire pondérée)** de la liste déroulante **Load balance algorithm (Algorithme d'équilibrage de charge)**.

b Sélectionnez l'option **Even distribution (Distribution uniforme)** de la liste déroulante **Load distribution (Distribution de charge)**.

c Cliquez sur **Apply (Appliquer)**.

6 Double-cliquez sur l'option **Monitoring and Management (Surveillance et gestion)** pour afficher l'état d'intégrité du serveur de gestion WDM, ainsi que d'autres options.

7 Double-cliquez sur **Proxy** pour configurer les paramètres du proxy :

a Réglez la valeur **Response buffer threshold (Seuil de mémoire tampon de réponse)** sur 0.

b Désélectionnez l'option **Keep Alive (Garder en vie)**.

c Modifiez la version **HTTP** sur **HTTP/1.1**.

d Sélectionnez l'option **Reverse rewrite host in response headers (Hôte de réécriture inverse dans les en-têtes de réponse)**.

8 Double-cliquez sur **Routing Rules (Règles de routage)**.

a Cliquez sur **URL Rewrite (Réécriture d'URL)** sur le volet **Actions**.

b Sur la page **Edit Inbound Rule (Modifier la règle de trafic entrant)**, définissez le **Pattern (Modèle)** sur ***hserver.dll***.

Cette étape garantit que seules les demandes d'URL destinées au serveur de gestion WDM sont envoyées à la batterie de serveurs par le serveur proxy ARR.

Les propriétés de la batterie de serveurs sont désormais configurées.

Configuration du filtrage des demandes

À propos de cette tâche

Pour configurer le filtrage des demandes :

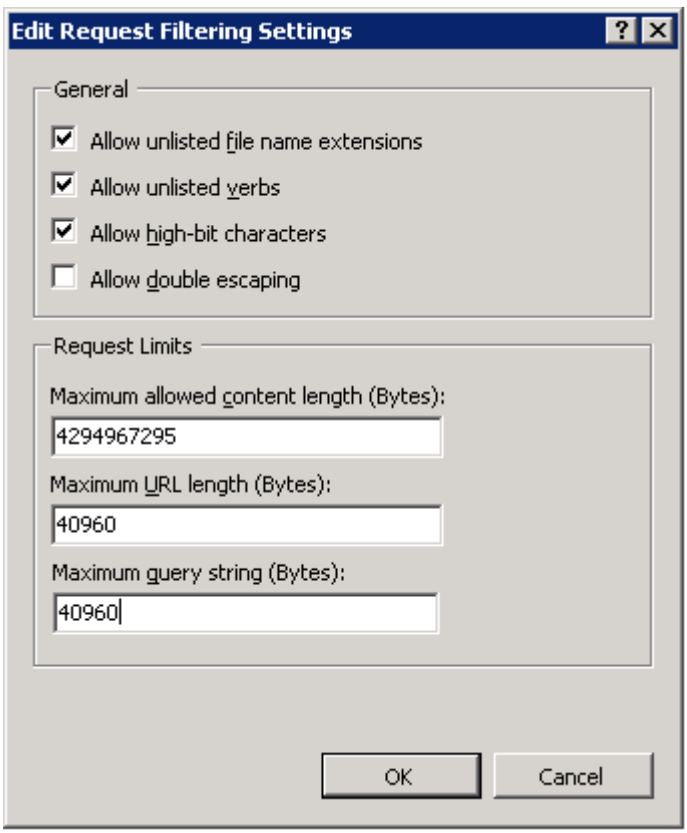
Étapes

1 Connectez-vous au serveur proxy ARR et lancez IIS Manager (Gestionnaire des services IIS).

2 Sélectionnez **Default Web Site (Site Web par défaut)** sous **Sites (Sites)**, puis, dans le volet droit, double-cliquez sur **Request Filtering (Filtrage des demandes)**.

3 Cliquez sur **Edit Feature Settings (Modifier les paramètres de fonction)**.

4 Définissez les **Request Limits (Limites des demandes)** comme indiqué ci-dessous :



5 Cliquez sur **OK** pour appliquer les paramètres.

Configuration du nom de domaine complet du proxy (Proxy FQDN, Proxy Fully Qualified Domain Name) dans les Préférences WDM

Pour achever la configuration de l'équilibrage de charge, vous devez préciser les détails du serveur proxy dans WDM.

À propos de cette tâche
Pour configurer le FQDN du proxy dans WDM :

Étapes

1 Connectez-vous au système où WDM est installé, puis démarrez la Console de l'interface utilisateur Web de WDM.
2 Sélectionnez **System (Système)** > **Console**.
3 Sous Manager Server Alias Name (Nom d'alias du serveur de gestion), entrez le FQDN du serveur proxy ARR.
4 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres.

Le serveur proxy ARR est maintenant enregistré dans la base de données WDM, et la configuration de l'équilibrage de charge est terminée.

Installation de composants WDM

La configuration de l'équilibrage de charge nécessite plusieurs installations de serveurs de gestion WDM. Cependant, vous devez vous assurer que l'un des systèmes de cette configuration est équipé d'une installation complète de WDM. Vous pouvez alors installer uniquement le serveur de gestion et le service ThreadX sur les autres systèmes. Pour plus d'informations sur l'installation des composants sélectionnés uniquement, voir Installation du serveur de gestion

Configuration de l'équilibrage de charge pour les périphériques Thread X 4.x

Lorsque vous souhaitez gérer un grand nombre d'appareils PCoIP (ThreadX), un seul service de gestionnaire ThreadX ne suffit pas. Configurer l'équilibrage de charge pour les appareils ThreadX vous permet de gérer un grand nombre de ces appareils.

Prérequis
Avant de configurer l'équilibrage de charge pour les périphériques Thread X, vous devez d'abord déterminer un système Windows 2008 R2 sur lequel installer le serveur de noms de domaine (DNS, Domain Name Server).

Pour plus d'informations concernant l'installation d'un DNS sur un serveur Windows 2008, rendez-vous sur http://technet.microsoft.com/en-us/library/cc725925.aspx.

Le mécanisme d'équilibrage de charge utilise la méthode de répétition alternée du DNS pour partager et distribuer les charges des ressources réseaux.

À propos de cette tâche
Pour configurer la répétition alternée du DNS (round-robin) :

Étapes

1 Connectez-vous au serveur DNS et lancez le DNS Manager (Gestionnaire DNS).
2 Sélectionnez le nom du serveur dans l'arborescence du volet gauche, effectuez un clic droit et sélectionnez **Properties** (Propriétés) dans le menu contextuel.

   La fenêtre **Properties** (Propriétés) s'affiche.
3 Cliquez sur l'onglet **Advanced** (Avancé) situé sur la fenêtre **Properties** (Propriétés).
4 Dans le volet **Server Options** (Options du serveur), assurez-vous que les options **Enable round robin** (Activer la répétition alternée) et **Secure cache against pollution** (Sécuriser le cache contre la pollution) sont sélectionnées.
5 Si vous devez classer les masques de réseau, sélectionnez l'option **Enable netmask ordering** (Activer le classement des masques de réseau). Cette fonction tente de définir les priorités des ressources locales pour les clients.
6 Cliquez sur le menu **View** (Vue) dans le Gestionnaire DNS, puis sélectionnez l'option **Advanced** (Avancé).

7 Développez le nœud **Domain** (Domaine) et, dans **Forward Lookup Zones** (Zones de recherche directes), sélectionnez le domaine. Par exemple, **WDMSQA11.com**.

8 Effectuez un clic droit et sélectionnez **New Host (A or AAAA)...** (Nouvel hôte (A ou AAAA)...).

La fenêtre **New Host** (Nouvel hôte) s'affiche.

9 Saisissez le nom de l'hôte virtuel de la batterie de serveurs Thread X qui participera à l'équilibrage de charge. Par exemple, ThreadXServer1.

Le FQDN du serveur s'affiche automatiquement.

10 Saisissez l'adresse IP du serveur.

11 Cliquez sur **Add Host** (Ajouter l'hôte).

12 Répétez les étapes **8 à 11** pour ajouter autant de serveurs Thread X que souhaité.

13 Sélectionnez le nœud **Domain** (Domaine) dans le **DNS Manager** (Gestionnaire DNS), effectuez un clic droit et sélectionnez **Other New Records** (Autres nouveaux enregistrements).

14 Dans la boîte de dialogue **Resource Record Type** (Type d'enregistrement de ressource, sélectionnez **SRV Location** (Emplacement SRV), puis cliquez sur **Create Record**(Créer enregistrement).

15 Dans la boîte de dialogue « New Resource Record » (Nouvel enregistrement de ressource), saisissez les valeurs suivantes :

- **Service Name** (Nom du service) - _PCOIP-broker
- **Protocol** (Protocole)- _tcp
- **Port Number** (Numéro de port) - 50000.
- **Host Offering this Service** (Hôte offrant ce service) – saisissez le nom d'hôte de la batterie de serveur Thread X.

16 Répétez les étapes **13 à 15** pour ajouter l'enregistrement SRV de **_PCOIP-tool**.

17 Configurer la mise en cache DNS :

a Dans le gestionnaire DNS, développez le nœud **Domain** (Domaine) et, à l'intérieur de celui-ci, sélectionnez le nœud **_tcp**.

b Sélectionnez **_PCOIP-tool** dans le volet droit, effectuez un clic droit et sélectionnez **Properties** (Propriétés).

c Dans la fenêtre **Properties** (Propriétés), vérifiez la valeur **Time to live (TTL)** (Durée de vie (TTL)). L'intervalle de mise en cache est appelé **Maximum TTL value** (Valeur TTL maximale) et la valeur par défaut est 1 heure. Vous pouvez la modifier si vous le souhaitez.

Le champ TTL est affiché à la condition que vous ayez sélectionné **Advanced View** (Vue avancée) dans le menu **View** (Vue) du serveur DNS.

La configuration de l'équilibrage de charge pour les périphériques Thread X est maintenant terminée. Vous pouvez utiliser vos serveurs de gestion WDM pour gérer un nombre important de périphériques Thread X.

Configuration de l'équilibrage de charge pour les appareils Thread X 5.x

Il est impossible de faire évoluer le serveur proxy de périphérique Teradici afin qu'il gère plus de 18 mille périphériques lorsqu'il est le seul serveur utilisé pour gérer, dans WDM, les périphériques ThreadX 5x d'un environnement de grande entreprise. Cela risquerait d'entraîner des problèmes ou des retards au niveau des archivages clients, des exécutions planifiées ou des exécutions en temps réel de commandes.

Toutefois, l'équilibrage de charge permet, dans une large mesure, de résoudre ces problèmes. Cette configuration permet en effet d'installer et d'exécuter plusieurs instances des serveurs proxy de périphérique Teradici sur divers systèmes ainsi que d'équilibrer la charge entre eux à l'aide d'un proxy, en procédant comme décrit ci-après.

Les composants de l'équilibreur de charge sont les suivants :

- Serveur proxy de périphérique Teradici
- Serveur proxy de haute disponibilité

WDM utilise le proxy HAProxy hébergé sur le serveur Ubuntu 16.04.1 LTS pour exécuter l'équilibrage de charge entre les serveurs proxy de périphérique Teradici. Le proxy HAProxy est un proxy d'équilibrage de charge qui permet également de bénéficier d'une haute disponibilité. Ce célèbre logiciel open source fonctionne aussi bien comme équilibreur de charge TCP/HTTP que comme solution de proxy exécutable sous Linux. Il est utilisé le plus souvent pour améliorer les performances et la fiabilité d'un environnement de serveur en répartissant la charge de travail sur plusieurs serveurs.

Cette section décrit la procédure à suivre pour installer et pour configurer l'équilibrage de charge du serveur proxy de haute disponibilité.

Étapes de création d'un enregistrement DNS_SRV :

Le micrologiciel 5.x utilise un enregistrement DNS_SRV en plus de l'enregistrement de texte qui contient l'empreinte du certificat SSL à utiliser dans la console de gestion.

WDM 5.7.3 prend en charge le micrologiciel Teradici 5.x avec fonctions complètes.

1 Le premier enregistrement requis est un enregistrement DNS_SRV pour _pcoip-bootstrap. L'enregistrement doit pointer vers le nom du proxy de périphérique Teradici (HAProxy).

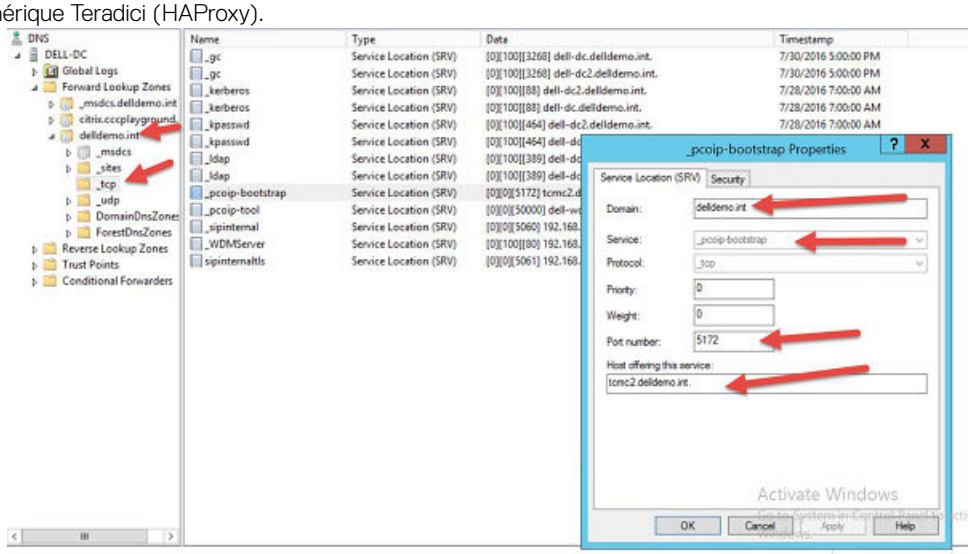


Figure 40. Enregistrement DNS_SRV pour _pcoip-bootstrap

2 Le deuxième enregistrement requis est un enregistrement A pointant vers le nom utilisé dans le champ **Host offering this service** (Hôte offrant ce service).

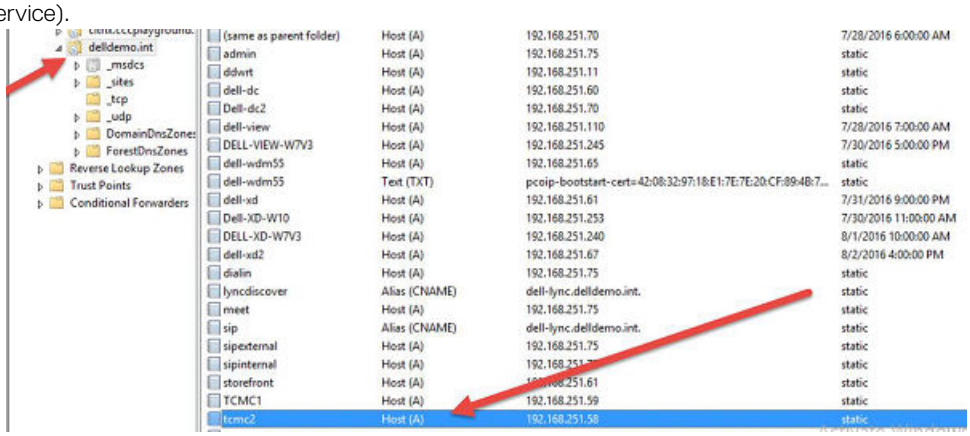


Figure 41. Enregistrement d'hôte

3 Le troisième enregistrement requis est un enregistrement TXT. L'enregistrement TXT est l'empreinte du certificat SSL utilisé par la console de gestion.

Suivez les étapes ci-après pour créer un enregistrement A pour l'hôte ainsi qu'un enregistrement TXT :

1 Cliquez sur le nœud de domaine (delldemo.int) et sélectionnez l'option **Other New Records** (Autres nouveaux enregistrements), puis Host (Hôte) (A ou AAAA, selon l'enregistrement A de la console de gestion).

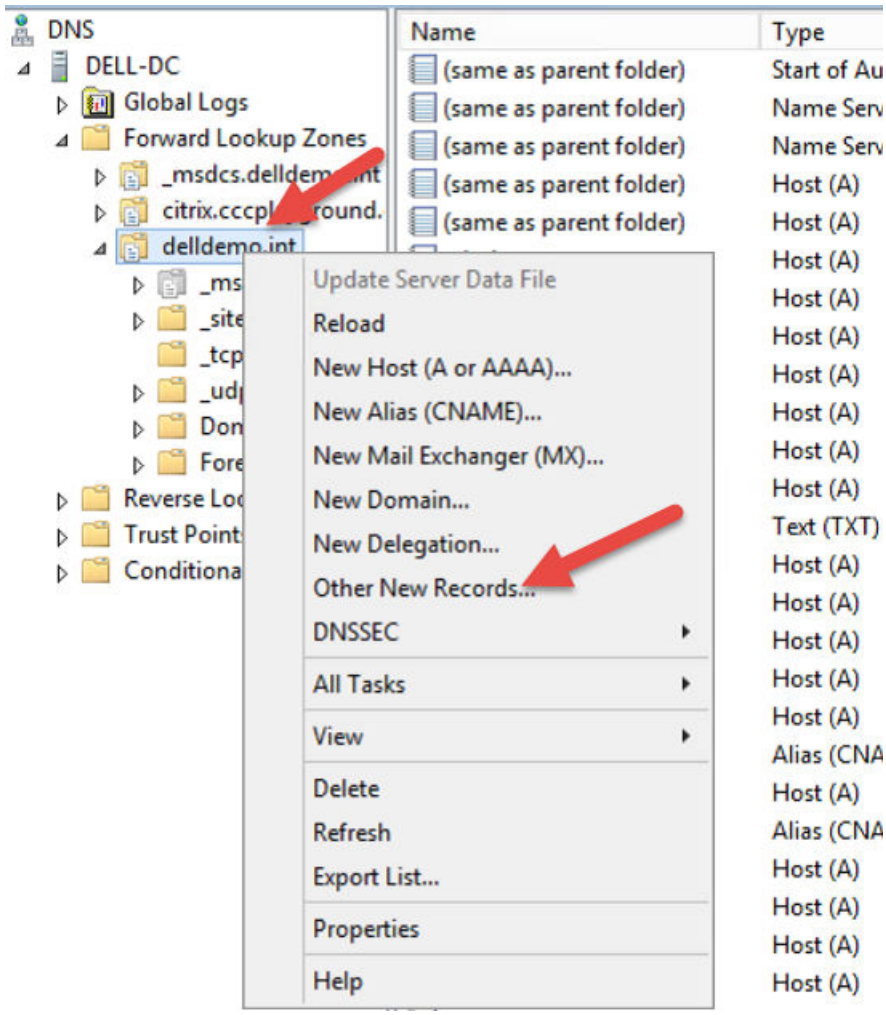


Figure 42. Création d'un enregistrement TXT

2 Cliquez sur le nœud de domaine (delldemo.int) et sélectionnez l'option **Other New Records** (Autres nouveaux enregistrements), puis Text (Texte) (TXT) pour créer le champ de texte qui inclut l'empreinte du certificat.

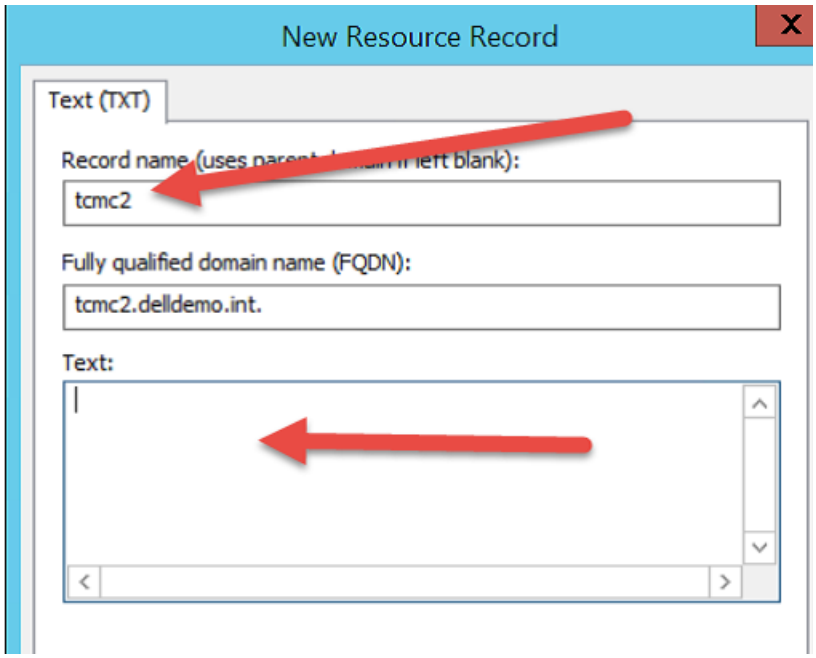


Figure 43. Nouvel enregistrement de ressource

L'empreinte SHA256 peut être obtenue à l'aide du navigateur Firefox.

Pour obtenir l'empreinte lorsque Wyse Device Manager (WDM) est installé avec le composant Teradici 5x :

1 Ouvrez le navigateur Firefox depuis le périphérique sur lequel le composant Teradici 5.x est installé. Dans le navigateur, appuyez sur les touches **Alt+T** pour ouvrir le menu Tools (Outils).

2 Dans la liste déroulante, sélectionnez **Options**.

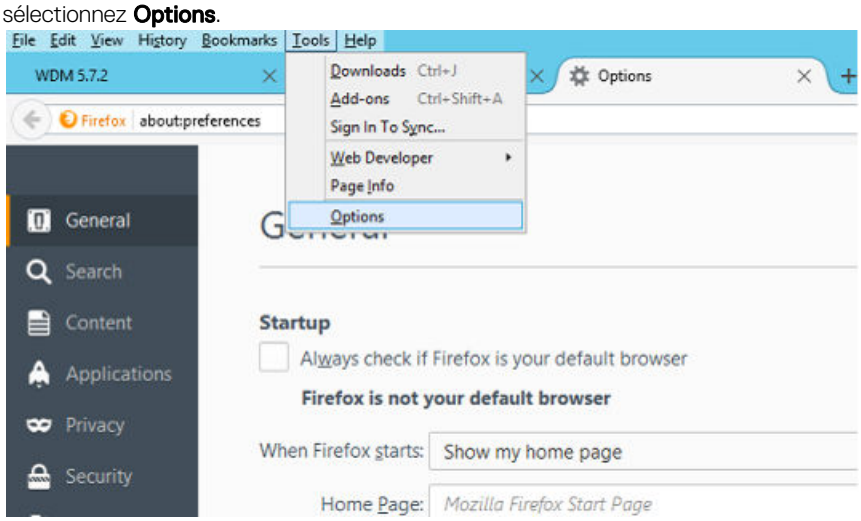


Figure 44. Onglet Général

3 Dans le volet gauche de la page **Options**, cliquez sur l'onglet **Advanced (Avancé)**, puis sur l'option **Certificates (Certificats)**.

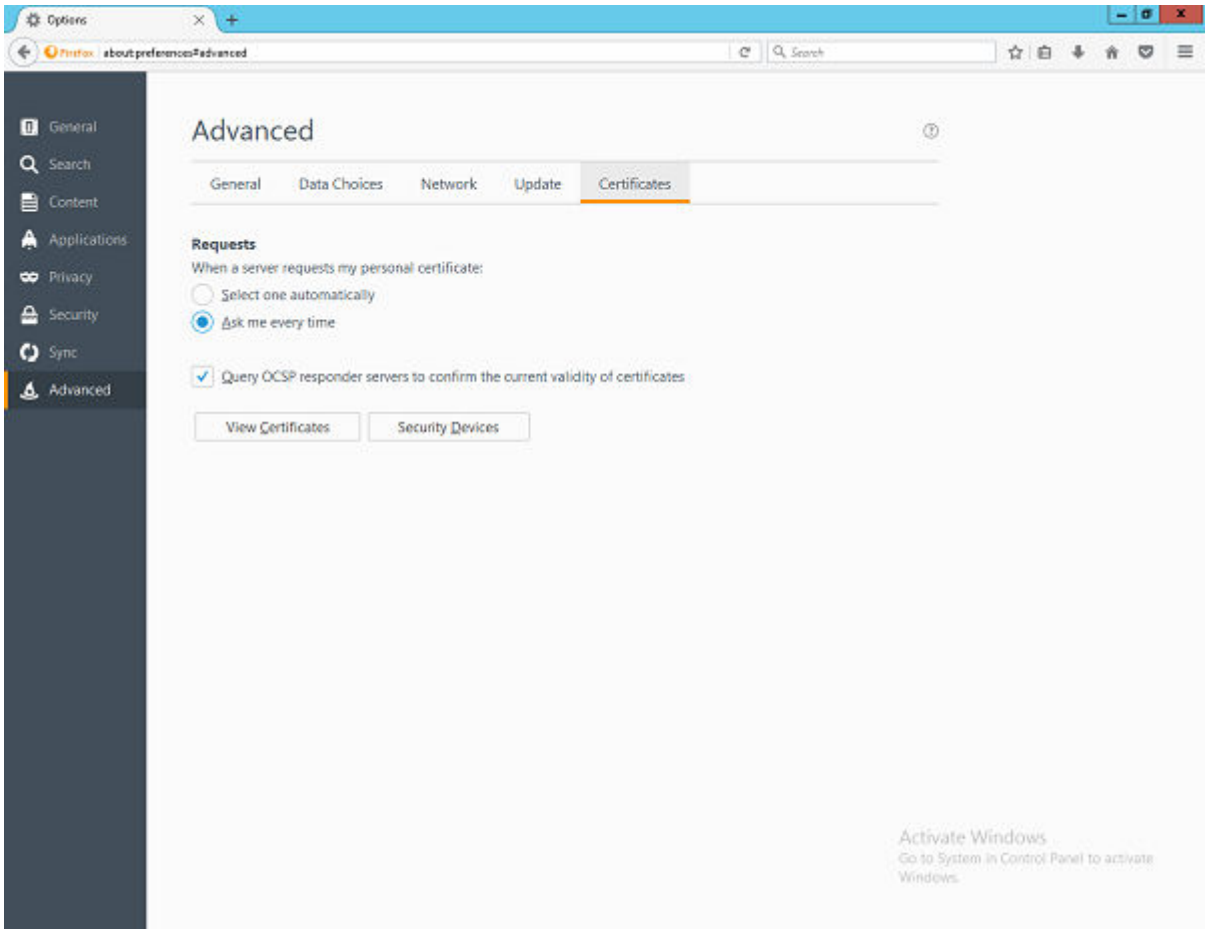


Figure 45. Avancé

4 Cliquez sur **View Certificates (Afficher les certificats)** pour ouvrir la fenêtre Certificate Manager (Gestionnaire de certificats).

5 Sélectionnez l'onglet **Authorities (Autorités)** dans la fenêtre **Certificate Manager (Gestionnaire de certificats)** et cliquez sur **Import (Importer)**.

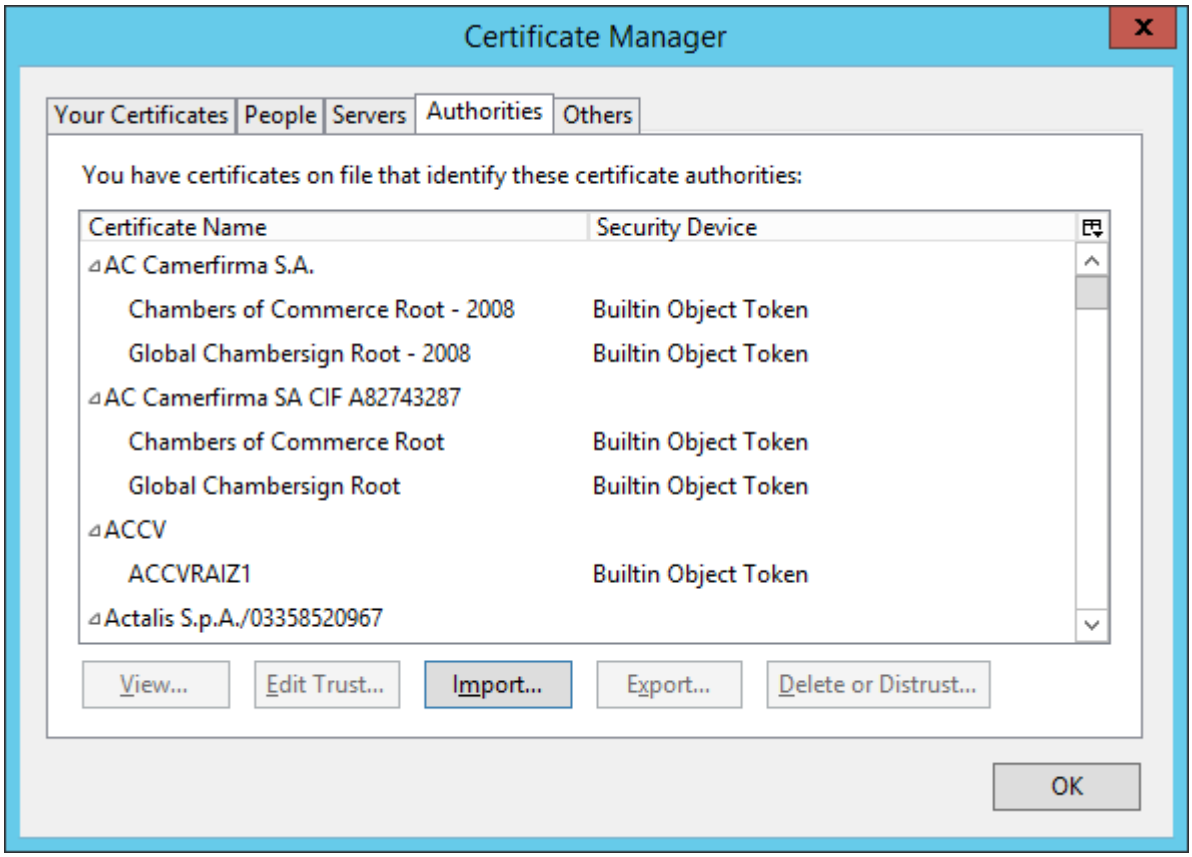


Figure 46. Gestionnaire de certificats

6 Dans la boîte de dialogue du navigateur de fichiers, accédez à l'emplacement d'installation de WDM, par exemple **\Wyse\WDM \Teradici**, où le chemin d'accès racine peut être **C:\Program Files (x86)** en fonction du système d'exploitation et du chemin d'installation.

REMARQUE : Si les composants Teradici sont installés via une procédure personnalisée ou configurés manuellement, les étapes ci-dessus doivent être suivies sur le même périphérique et le chemin d'accès au programme d'installation standard peut ne pas s'appliquer. Vous devez alors accéder à l'emplacement racine du dossier Teradici.

7 Sélectionnez le fichier **cert. pem**, puis cliquez sur **Open (Ouvrir)**.

8 Cliquez sur **View (Voir)** dans la fenêtre **Downloading Certificate (Téléchargement du certificat)**.

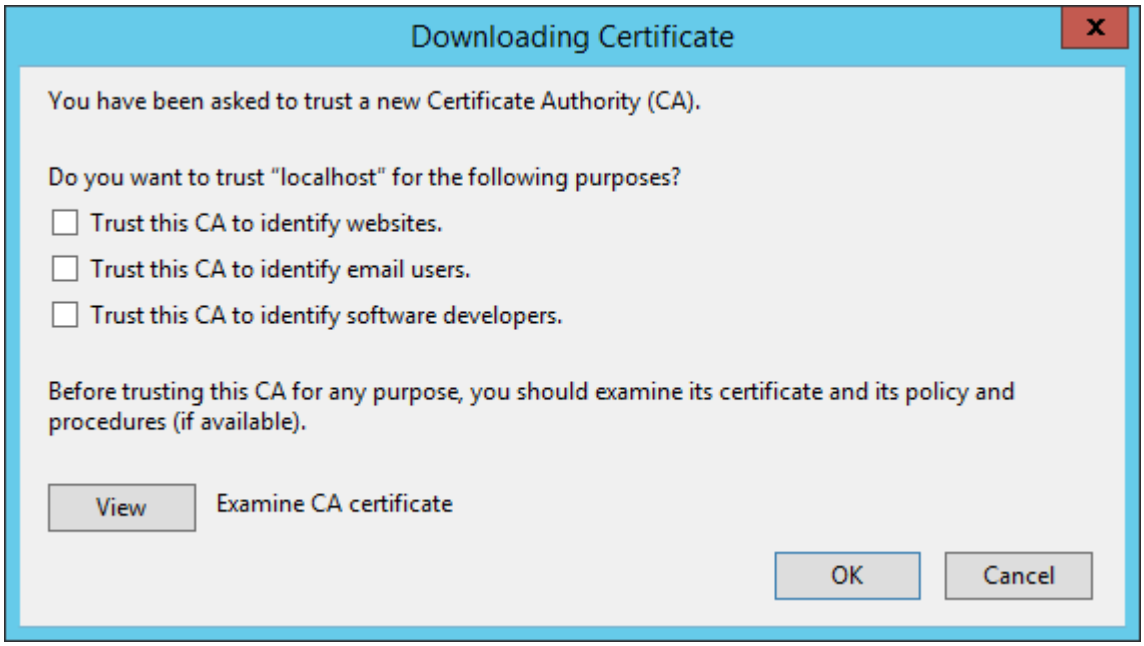


Figure 47. Téléchargement du certificat

9 Copiez la valeur de l'empreinte SHA256. Cliquez sur **Close (Fermer)** et fermez toutes les fenêtres Firefox.

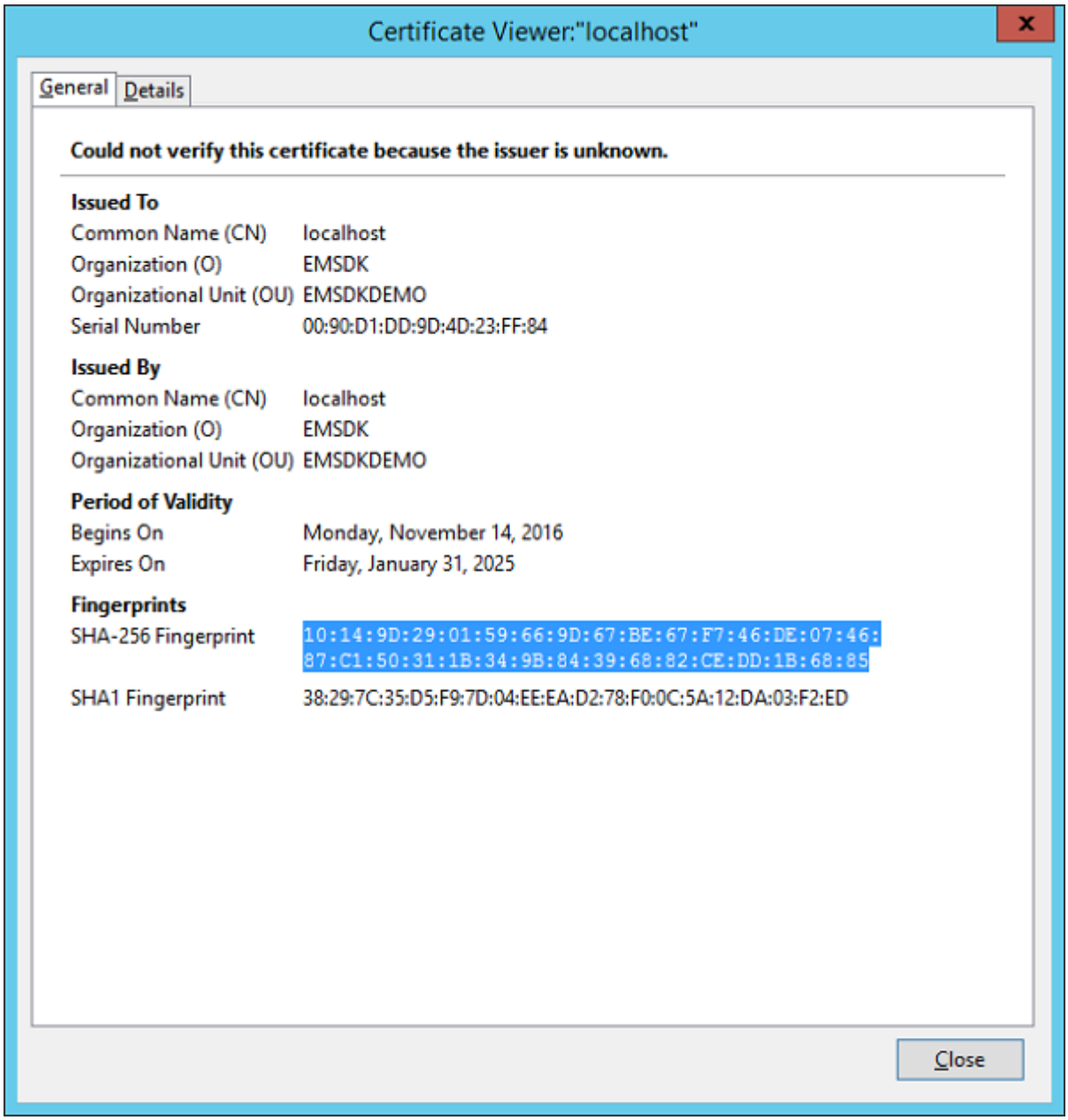


Figure 48. Visionneuse de certificats

REMARQUE : Dans le champ Text (Texte), le texte commençant par pcoip-bootstrap-cert= doit être ajouté à l'empreinte SHA256 qui a été obtenue.

Une fois l'empreinte du certificat copiée, effectuez l'opération suivante sur le serveur DNS :

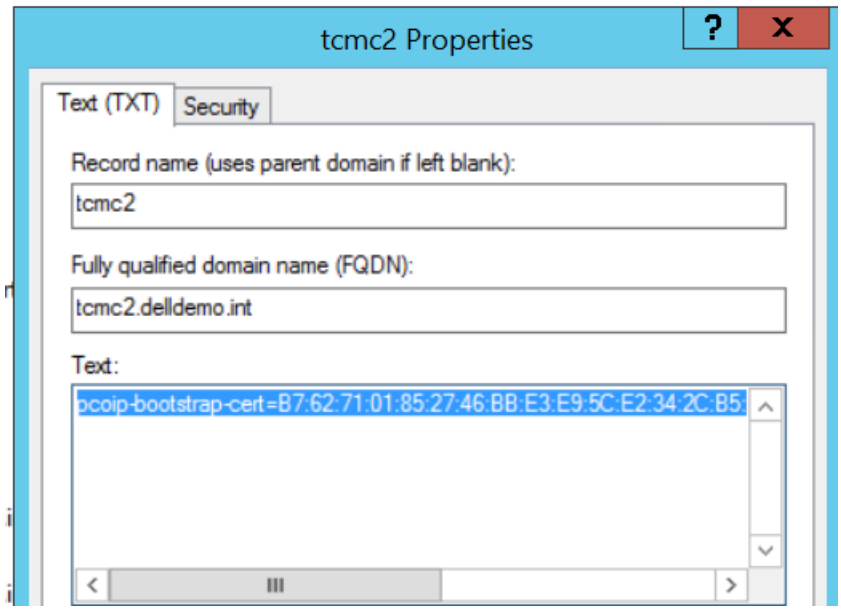


Figure 49. Propriétés tcmc2

10 Le quatrième et dernier enregistrement est un enregistrement PTR inverse pour l'hôte de gestion.

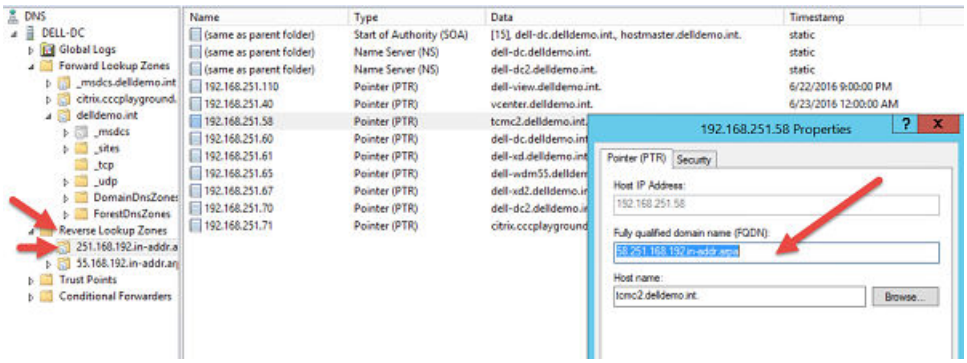


Figure 50. Enregistrement PTR

11 La zone doit correspondre au sous-réseau auquel l'hôte appartient. Par ailleurs, l'enregistrement correspond à l'adresse IP attribuée au proxy de périphérique Teradici (HAProxy).

Installation et configuration de HAProxy

HAProxy, l'équilibreur de charge pour les appareils ThreadX 5x, est configuré sur Ubuntu Linux version 16.04.1 avec HAProxy version 1.6.

Procédez comme suit pour installer et configurer HAproxy sur une machine Ubuntu Linux :

Lien de référence : https://haproxy.debian.net/#?distribution=Ubuntu&release=precise&version=1.6

1 Connectez-vous à la machine Ubuntu en fournissant les informations d'identification utilisateur utilisées lors de l'installation du système d'exploitation Ubuntu.

2 Ouvrez le terminal et exécutez les commandes suivantes pour installer HAProxy :

- sudo apt-get install software-properties-common
- sudo add-apt-repository ppa:vbernat/haproxy-1.6
- sudo apt-get update

- sudo apt-get install haproxy

3 Exécutez les commandes suivantes pour configurer HAProxy :

- Avant d'effectuer des modifications, sauvegardez la configuration d'origine avec la commande **sudo cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.original**
- À présent, modifiez le fichier de configuration avec la commande **sudo nano/etc/haproxy/haproxy.cfg**
- Dans le fichier de configuration, modifiez les sections suivantes conformément aux exigences :
  - Section globale : Maxconn <nombre maximum de connexions>
  - Tcp-in front-end : bind<IP du serveur HAProxy>:5172
  - Serveurs back-end : server <nom d'alias du serveur> <IP du serveur proxy de l'appareil Teradici>:5172
  - maxconn <nombre maximum de connexions par serveur proxy d'appareil Teradici>

REMARQUE : Pour assurer la haute disponibilité, l'administrateur peut ajouter d'autres serveurs back-end au-delà de la capacité totale de clients afin de garantir un basculement fluide.

- Après avoir modifié la configuration, enregistrez-la avec commande Ctrl + O
- La configuration d'exemple HAProxy est fournie comme suit :

```
global

log /dev/log local0

log /dev/log local1 notice

chroot /var/lib/haproxy

daemon

#maxconn is maximum allowed connections

maxconn 50000

par défaut

log global

mode tcp

timeout connect 5000ms

timeout client 50000ms

timeout server 50000ms

errorfile 400 /etc/haproxy/errors/400.http

errorfile 403 /etc/haproxy/errors/403.http

errorfile 408 /etc/haproxy/errors/408.http

errorfile 500 /etc/haproxy/errors/500.http

errorfile 502 /etc/haproxy/errors/502.http

errorfile 503 /etc/haproxy/errors/503.http

errorfile 504 /etc/haproxy/errors/504.http

tcp-in front-end

#remplacez l'IP par l'IP de votre machine proxy Linux
```

liaison 10.150.99.102:5172

serveurs default_backend

Serveurs back-end

#Ajoutez les adresses IP de la machine Windows back-end avec le port 5172

#Maxconn représente le nombre de connexions : remplacez 10 par la nombre limite #(inférieur à 20 000)

server1 server2 (Serveur1 Serveur2) sont seulement des noms, pas des mots clés

```
server server1 10.150.99.107:5172 maxconn 10

server server2 10.150.99.107:5172 maxconn 10
```

4 À présent, validez le fichier de configuration HAProxy avec la commande **sudo haproxy –f /etc/haproxy/haproxy.cfg –c**.

Si la configuration est valide, le message suivant s'affiche :

Configuration file is valid (Le fichier de configuration est valide)

5 Démarrez le service HAProxy en exécutant la commande suivante :

Sudo service haproxy restart

6 **Commande pour arrêter le service HAProxy**

Sudo service haproxy stop

7 **Commande pour vérifier la version de HAProxy**

Sudo haproxy –f

8 **Commande pour désinstaller HAProxy**

Sudo apt-get remove haproxy

ou

Sudo apt-get purge –auto-remove haproxy

Installation des serveurs proxy de périphérique Teradici

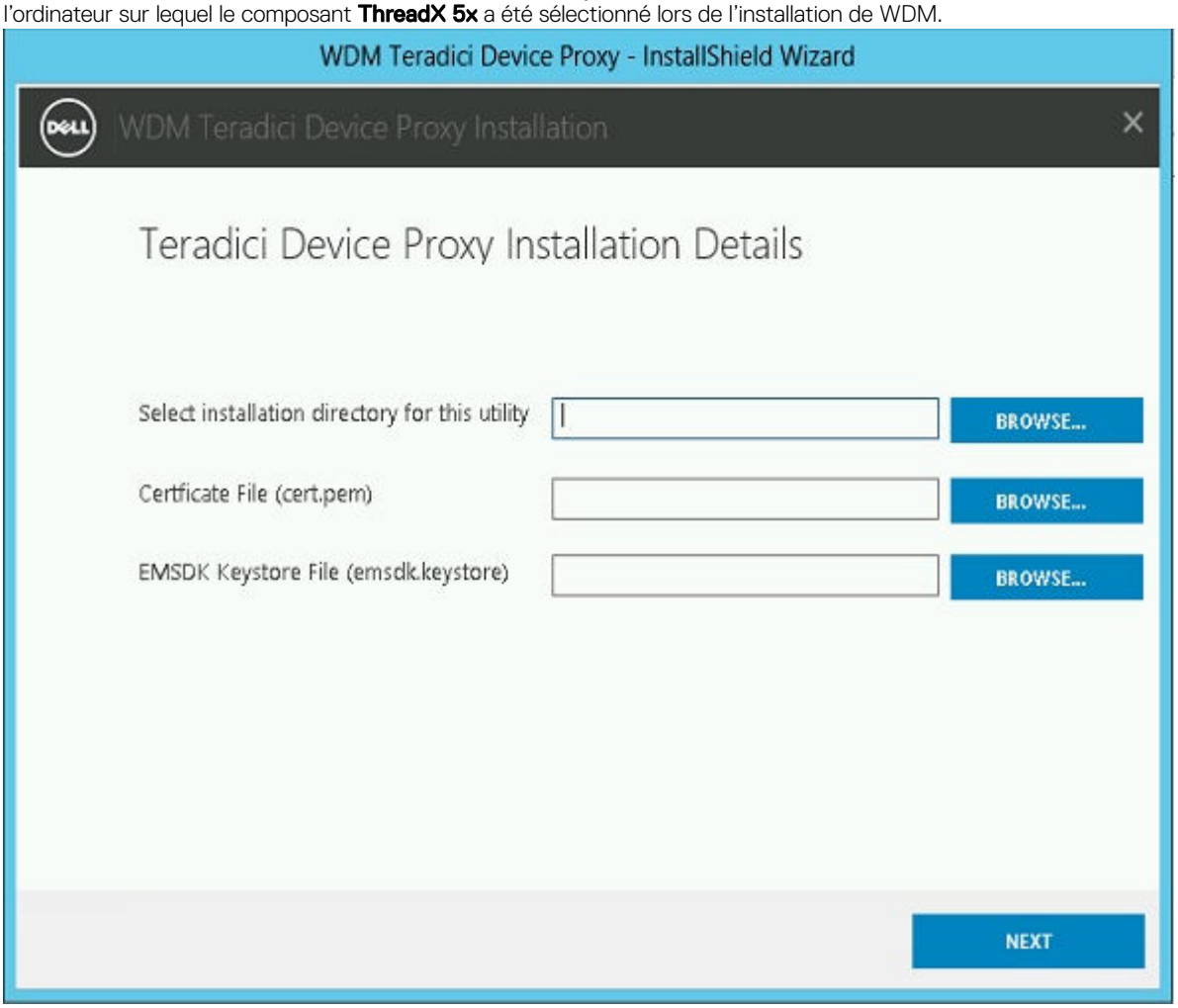
Les serveurs proxy de périphérique Teradici peuvent être installés sur un serveur exécutant les systèmes d'exploitation suivants :

- Windows 2012
- Windows 2012 R2
- Windows 2008 R2 64 bits
- Windows Server 2016

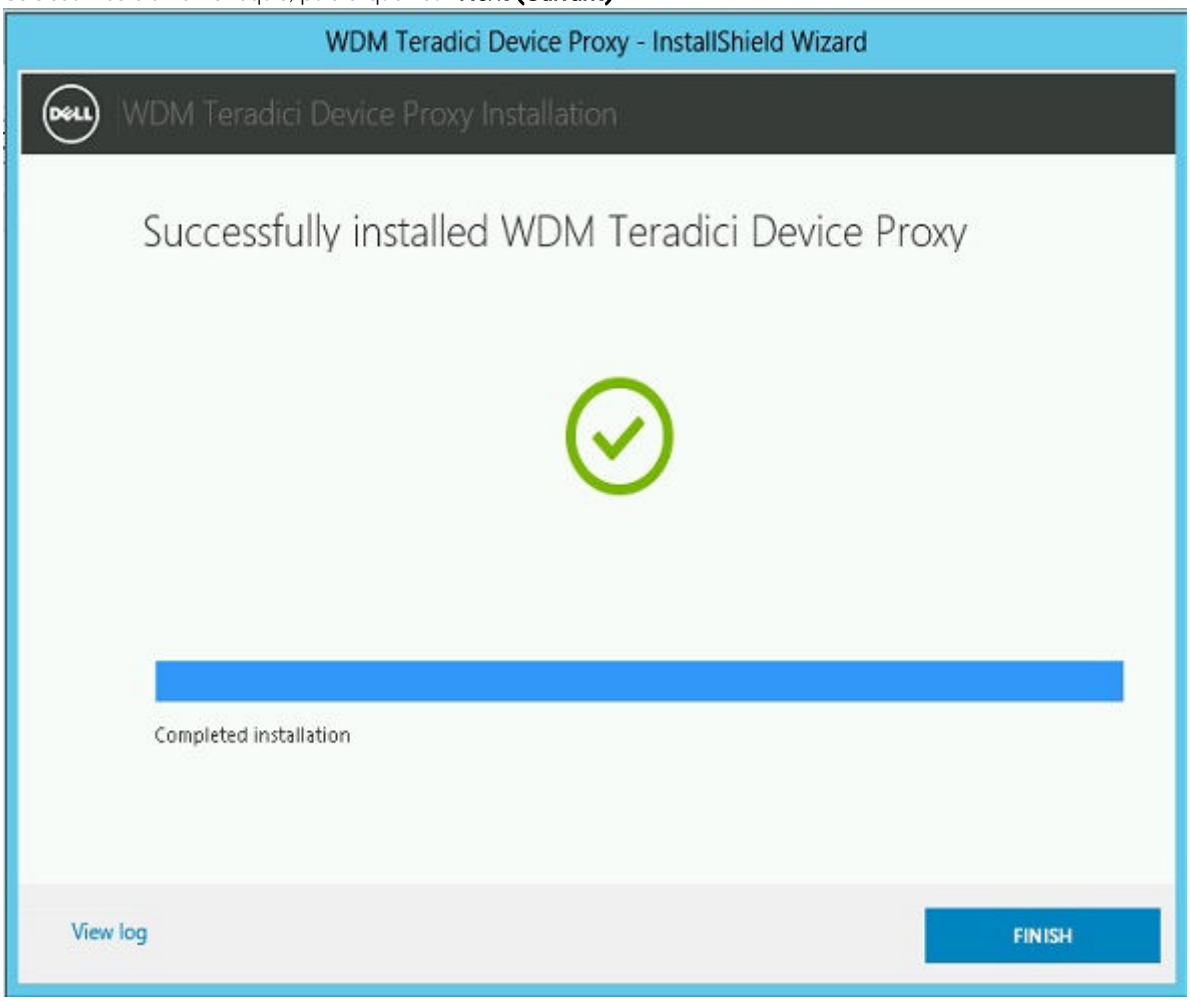
Suivez les étapes ci-après pour installer un serveur proxy de périphérique Teradici :

1 Connectez-vous au système en tant qu'administrateur.
2 Copiez le dossier **WDM installer (Programme d'installation de WDM)** sur l'ordinateur cible.
3 Accédez au dossier **TeradiciDeviceProxy**.
4 Double-cliquez sur le fichier **WDMTeradiciDeviceProxy.exe** pour installer le proxy de périphérique.
5 Entrez les informations suivantes :
   a Sélectionnez l'emplacement d'installation du proxy de périphérique Teradici et des composants dépendants.
   b Sélectionnez le fichier **Cert.pem** dans le dossier **<emplacement d'installation de WDM>\Teradici** sur l'ordinateur sur lequel le composant **ThreadX 5x** a été sélectionné lors de l'installation de WDM.

c Sélectionnez le fichier **emsdk.keystore** dans le dossier **<emplacement d'installation de WDM>\Teradici\EMSDK\config** sur l'ordinateur sur lequel le composant **ThreadX 5x** a été sélectionné lors de l'installation de WDM.



6 Saisissez les éléments requis, puis cliquez sur **Next (Suivant)**.



7 Cliquez sur **Finish (Terminer)**.

8 Le journal d'installation sera créé sous **<emplacement d'installation d'EMSDK>Teradici\Detail_TeradiciDeviceProxy.log**.

9 Accédez à **Start (Démarrer)** > **Administrative tools (Outils d'administration)** > **Services (Services)**.

10 Vérifiez que le service Windows ThreadX 5x Manager est installé et en cours d'exécution.

Ajout de serveurs proxy de périphérique Teradici dans WDM

Tâches

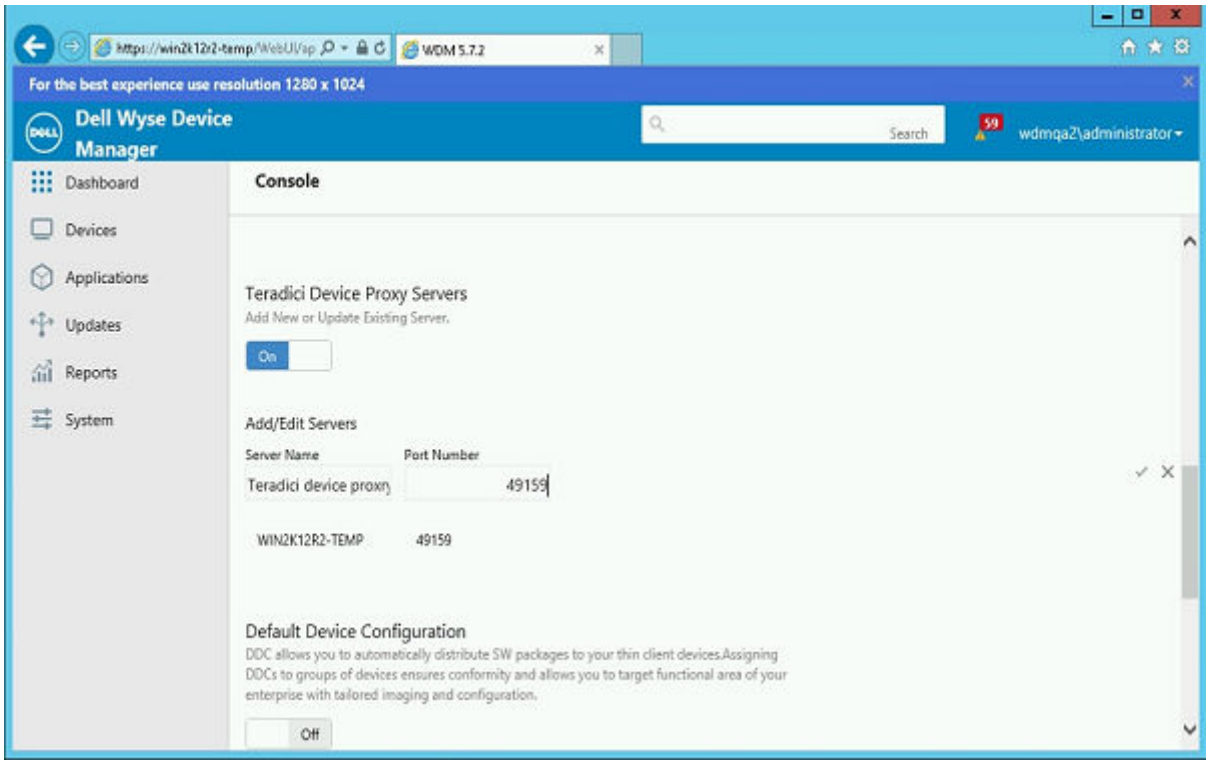
1 Ouvrez l'interface utilisateur Web de WDM et connectez-vous en tant qu'administrateur.

2 Accédez à **System (Système)** > **Console** et activez l'option **Teradici Device Proxy servers (Serveurs proxy de l'appareil Teradici)**.

3 Cliquez sur **Add Server (Ajouter un serveur)**.

4 Ajoutez le nom du serveur proxy de l'appareil Teradici dans le champ **Server Name (Nom de serveur)** et indiquez le numéro de port du service proxy de l'appareil Teradici dans le champ **Port Number (Numéro de port)**. La valeur par défaut est 49159.

REMARQUE : Le numéro de port par défaut doit être mis à jour dans WDM lorsqu'il est modifié. Pour plus d'informations, reportez-vous au *Wyse Device Manager 5.7.3 Administrator's guide (Guide de l'administrateur 5.7.3 de Dell Wyse Device Manager).*



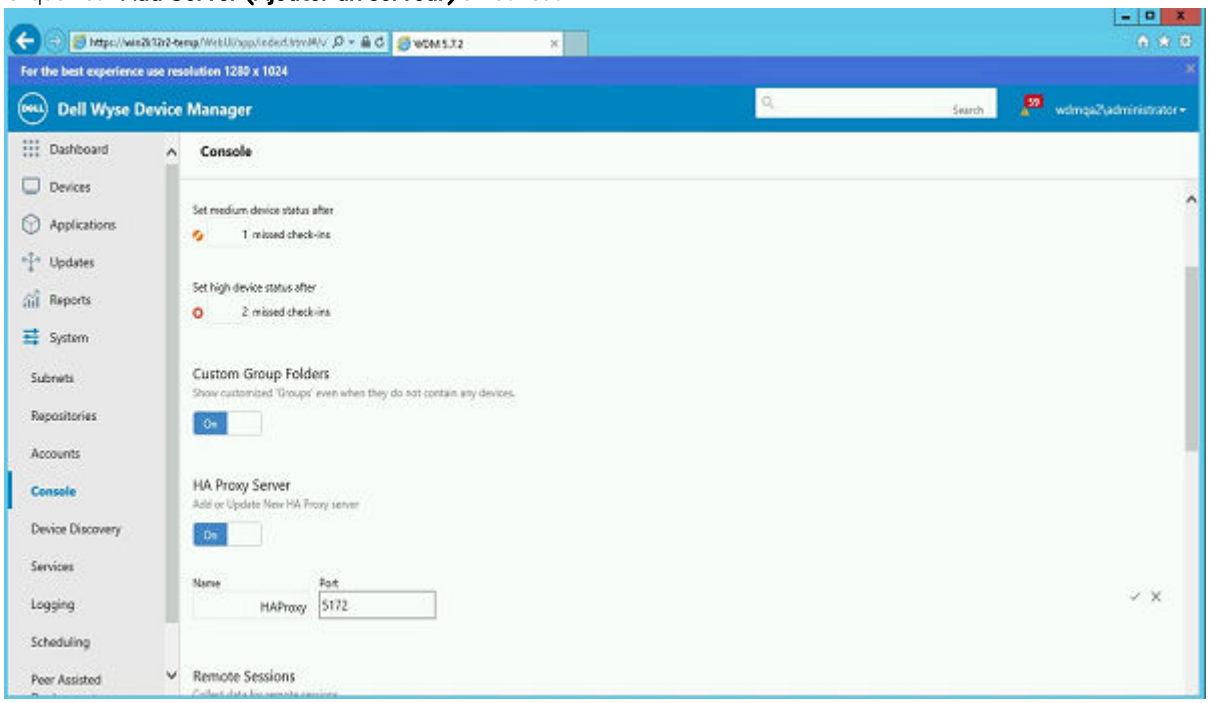
5 Cliquez sur la coche à droite des zones de texte pour enregistrer les valeurs.

Ajout d'un proxy HAProxy à WDM

Suivez les étapes ci-après pour ajouter un proxy HAProxy à WDM :

1 Connectez-vous à l'interface utilisateur Web de WDM en tant qu'administrateur.
2 Accédez à la page de console et activez l'option **HAProxy Server (Serveur HAProxy)**.
3 Cliquez sur **Add Server (Ajouter un serveur)**.
4 Ajoutez le nom du serveur HAProxy dans le champ Server Name (Nom du serveur) et attribuez le numéro 5172 au port.

5 Cliquez sur **Add Server (Ajouter un serveur)** à nouveau.



6 Cliquez sur la coche située à droite des zones de texte afin d'enregistrer les valeurs.

Redémarrage de l'API ThreadX

Suivez les étapes ci-dessous pour redémarrer l'API ThreadX :

1 Connectez-vous au serveur sur lequel le composant WDM ThreadX 5x a été installé.
2 Cliquez sur **Start menu (menu Démarrer)** > **Administrative tools (Outils d'administration)** > **Internet information service (IIS) manager (Gestionnaire IIS)**.
3 Développez le nœud racine (nom d'hôte du serveur) et sélectionnez **Application pools (Pools d'applications)** > **ASP .Net v4.0**.
4 Cliquez avec le bouton droit sur **ASP .Net v4.0** et sélectionnez **Stop (Arrêter)**.
5 Toujours avec le bouton droit, cliquez à nouveau sur **ASP .Net v4.0** et sélectionnez **Start (Démarrer)**.
6 Ouvrez l'interface utilisateur Web de WDM et connectez-vous en tant qu'administrateur.
7 Vérifiez l'état indiqué dans le tableau de bord.

Vérification de l'état dans le tableau de bord

1 Cliquez sur le tableau de bord et sélectionnez Teradici Servers (Serveurs Teradici).
2 Vérifiez que le composant ThreadX 5, le proxy Teradici HAproxy et le serveur proxy de périphérique Teradici sont en ligne.

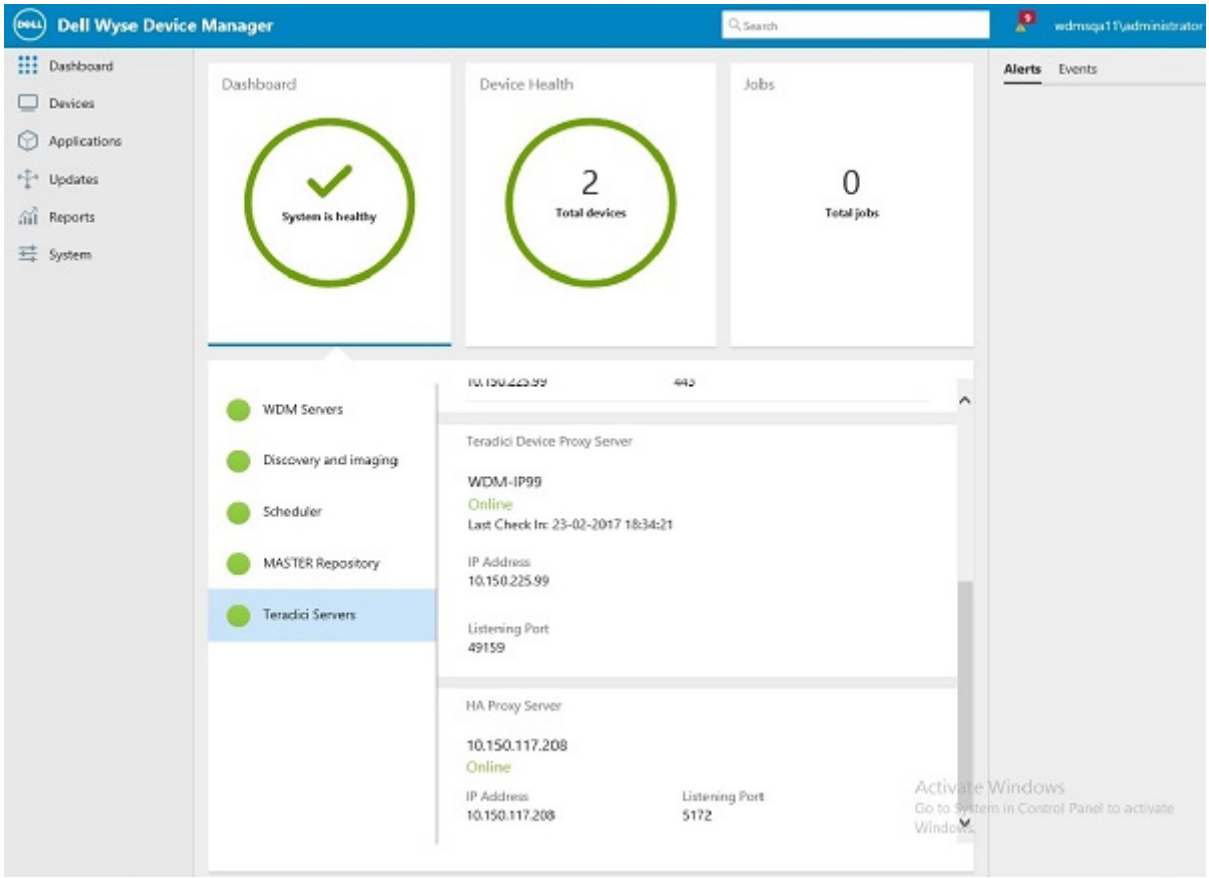


Figure 51. État indiqué dans le tableau de bord

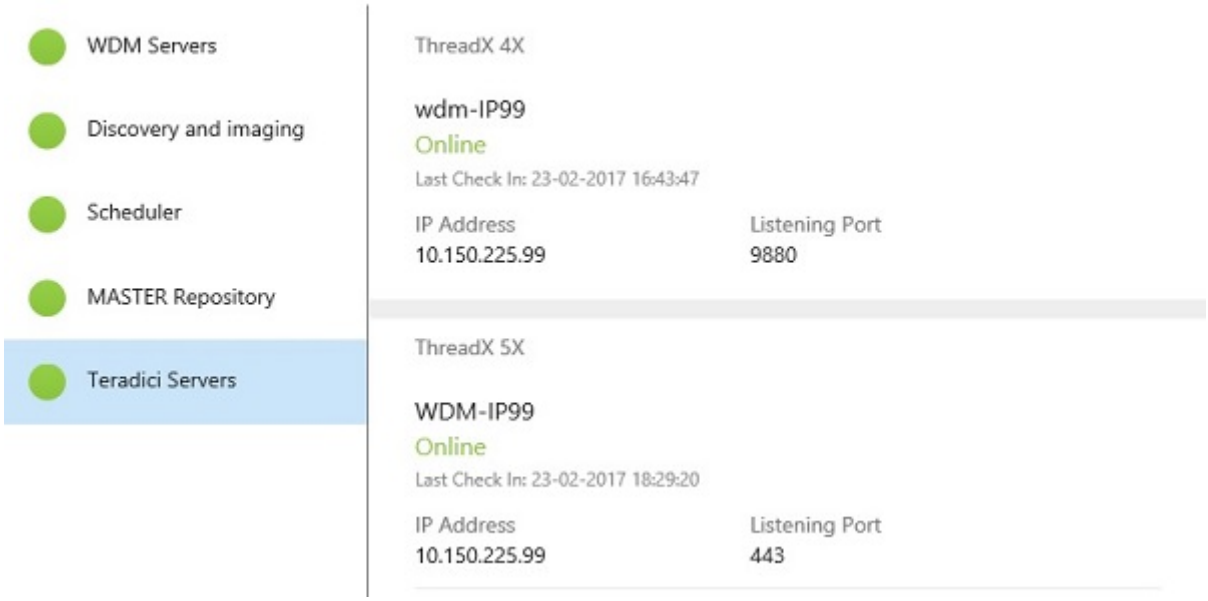


Figure 52. État indiqué dans le tableau de bord

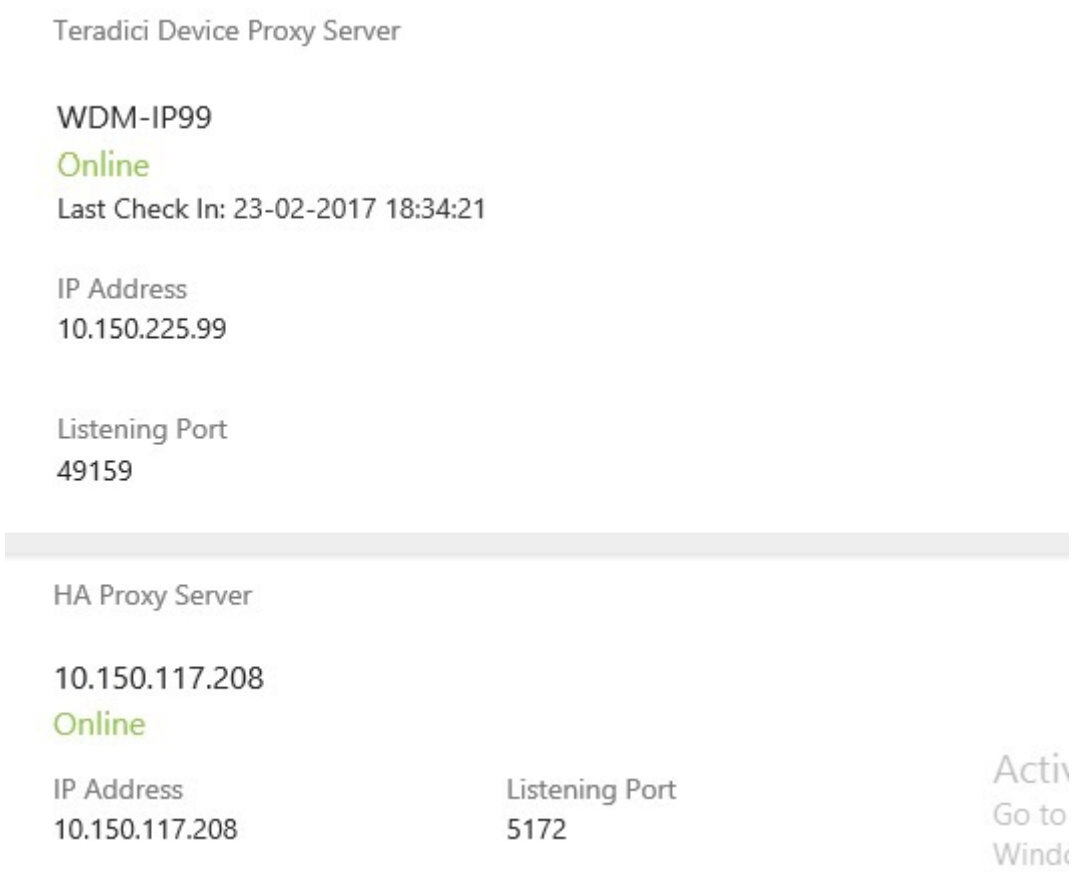


Figure 53. État indiqué dans le tableau de bord

7

Configuration de la haute disponibilité du service d'interface utilisateur Web

Lorsque vous disposez d'une seule instance de service d'interface utilisateur Web, si ce serveur tombe en panne, WDM ne peut plus être géré à partir de l'interface utilisateur Web. Par conséquent, il est recommandé de configurer la haute disponibilité (HA) du service d'interface utilisateur Web.

Vous pouvez utiliser un proxy d'équilibrage de charge tel que le serveur de proxy inverse ARR, que vous devez configurer pour prendre en charge la haute disponibilité du service d'interface utilisateur Web.

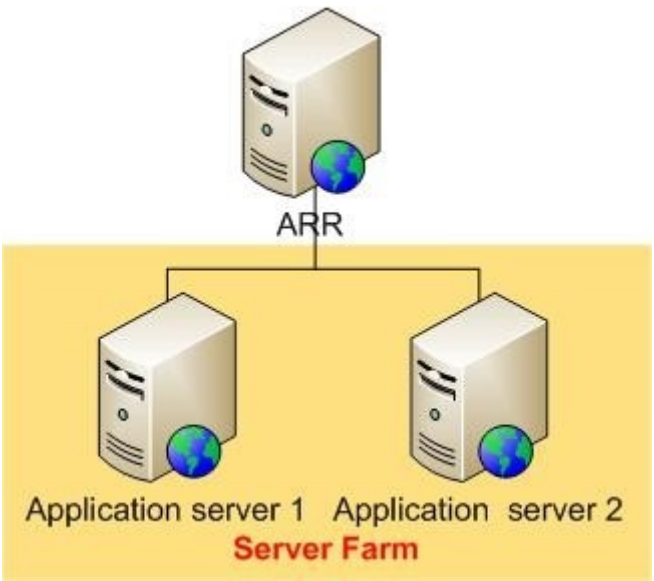


Figure 54. Haute disponibilité (HA) du service d'interface utilisateur Web

Sujets :

- Configuration du serveur proxy ARR
- Installation des Services d'information Internet — IIS
- Installation du module ARR
- Modification du modèle de processus du pool d'applications pour l'ARR
- Création d'une batterie de serveurs d'interface utilisateur Web
- Configuration du SSL sur le serveur proxy
- Configuration des propriétés de la batterie de serveurs pour l'ARR
- Journalisation sur le navigateur de l'interface utilisateur Web

Configuration du serveur proxy ARR

Le serveur proxy ARR (Application Routing Request) est le composant le plus important de l'équilibrage de charge. Ce serveur reçoit les requêtes provenant de systèmes clients légers et les achemine vers les différents serveurs de gestion WDM.

Prérequis

La version 7.0 d'IIS ou une version ultérieure doit être installée sur Windows 2008 (n'importe quel SKU).

À propos de cette tâche

La configuration du serveur proxy ARR comprend les étapes suivantes :

Étapes

1 Installation d'IIS.
2 Installation du module ARR.
3 Modification du modèle de processus du pool d'applications pour l'ARR.
4 Création d'une batterie de serveurs d'interface utilisateur Web.
5 Configuration du SSL sur le serveur proxy.
6 Configuration des propriétés de la batterie de serveurs pour l'ARR.

Installation des Services d'information Internet — IIS

1 Connectez-vous en tant qu'administrateur.
2 Accédez à **Control Panel (Panneau de configuration)** > **Programs and Features (Programmes et fonctionnalités)** > **Turn Windows features on or off (Activer ou désactiver les fonctions Windows)**.
3 Sélectionnez les options comme indiqué dans la capture d'écran suivante.

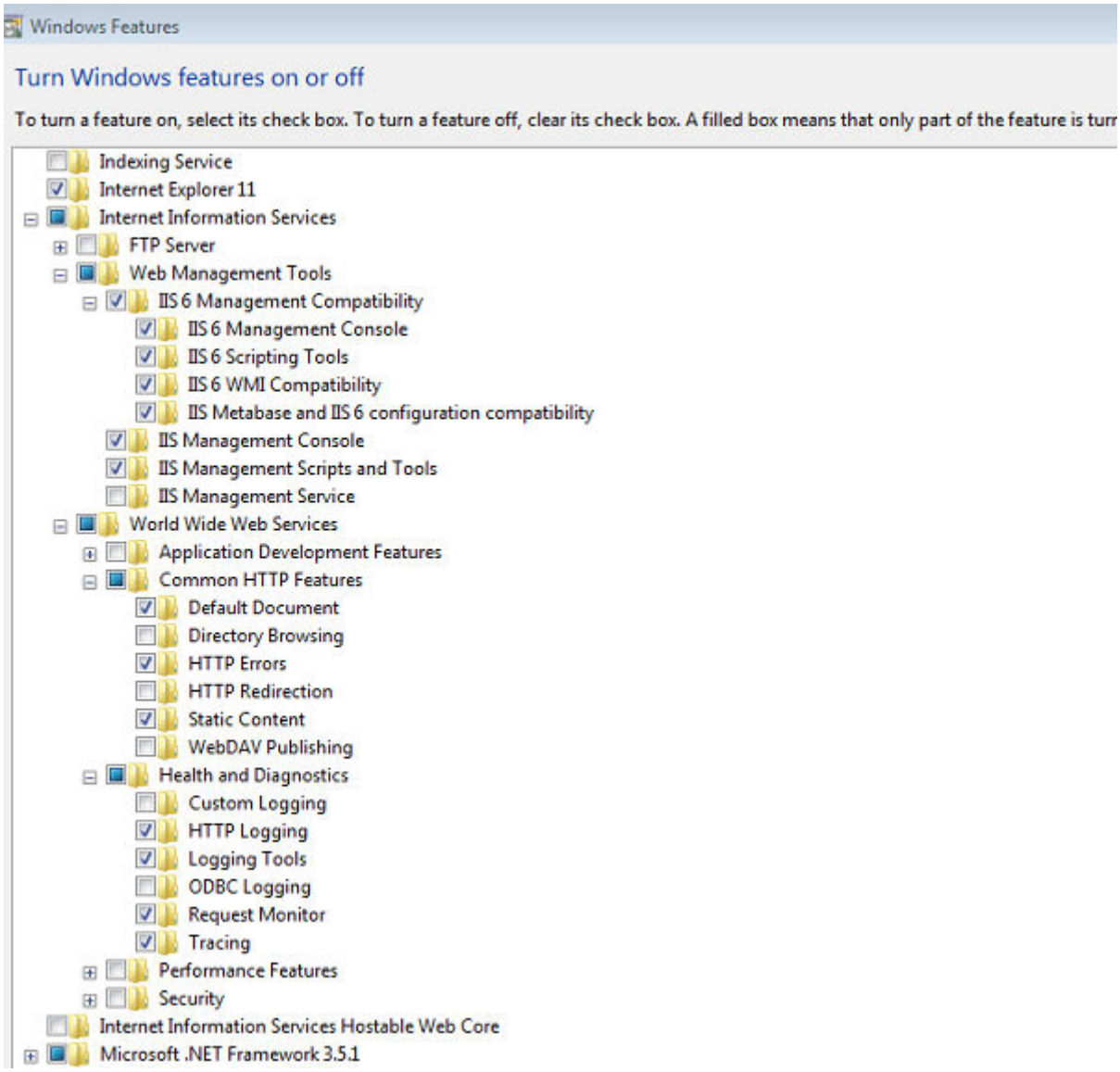


Figure 55. Fonctionnalités Windows

4 Cliquez sur **OK**.

Installation du module ARR

Vous devez installer l'ARR (Application Request Routing) version 3.0 sur le système que vous avez identifié pour qu'il serve de serveur proxy ARR. Le programme d'installation est disponible sur le site de téléchargements Microsoft à l'adresse support.microsoft.com. Téléchargez le fichier **ARRv3_0.exe** et installez-le.

Modification du modèle de processus du pool d'applications pour l'ARR

À propos de cette tâche

Toutes les requêtes et réponses HTTP pour les sites de contenu passent par l'ARR. Le processus de travail du site Web par défaut sur l'ARR doit toujours être en cours d'exécution, indépendamment du fait que le processus de travail pour certains sites soit en cours d'exécution ou non.

Vous devez désactiver la durée d'inactivité dans le modèle de processus du pool d'applications pour le site Web par défaut.

Étapes

1 Démarrer IIS Manager (Gestionnaire des services ISS).

2 Sélectionnez **Application Pools (Pools d'applications)**.

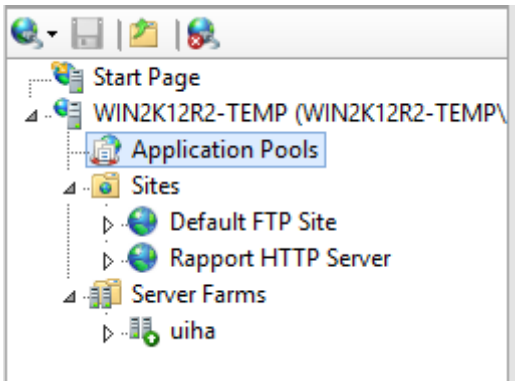


Figure 56. Pools d'applications

3 Sélectionnez **DefaultAppPool**.

4 Accédez à **Actions** > **Edit Application Pool (Modifier le pool d'applications)** > **Advanced Settings (Paramètres avancés)**.

5 Définissez le **Idle Time-out (minutes) (délai d'inactivité en minutes)** sur 0.

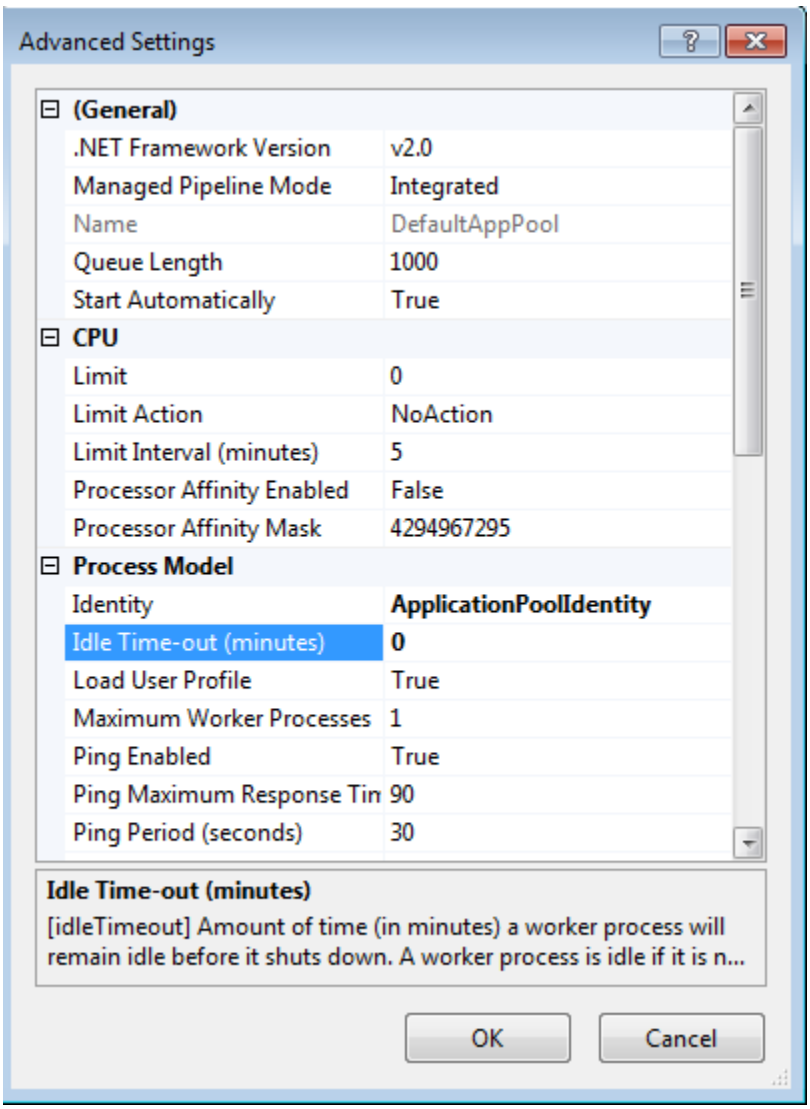


Figure 57. Paramètres avancés

6 Cliquez sur **OK** pour enregistrer les modifications.

Création d'une batterie de serveurs d'interface utilisateur Web

1 Démarrer IIS Manager (Gestionnaire des services ISS).

2 Faites un clic droit sur **Server Farms (Batterie de serveurs)** et sélectionnez **Create Server Farm (Créer une batterie de serveurs)**.

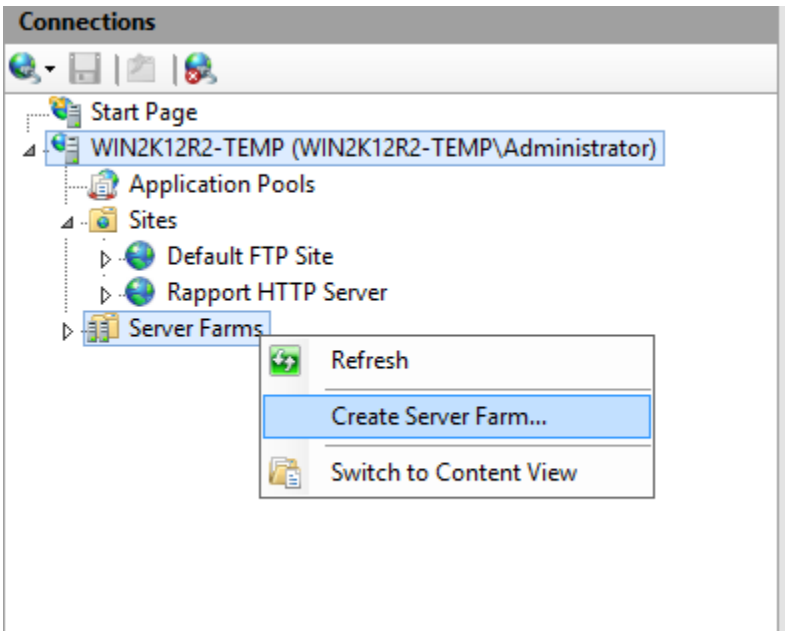


Figure 58. Batteries de serveurs

3 Entrez le nom de la batterie de serveurs

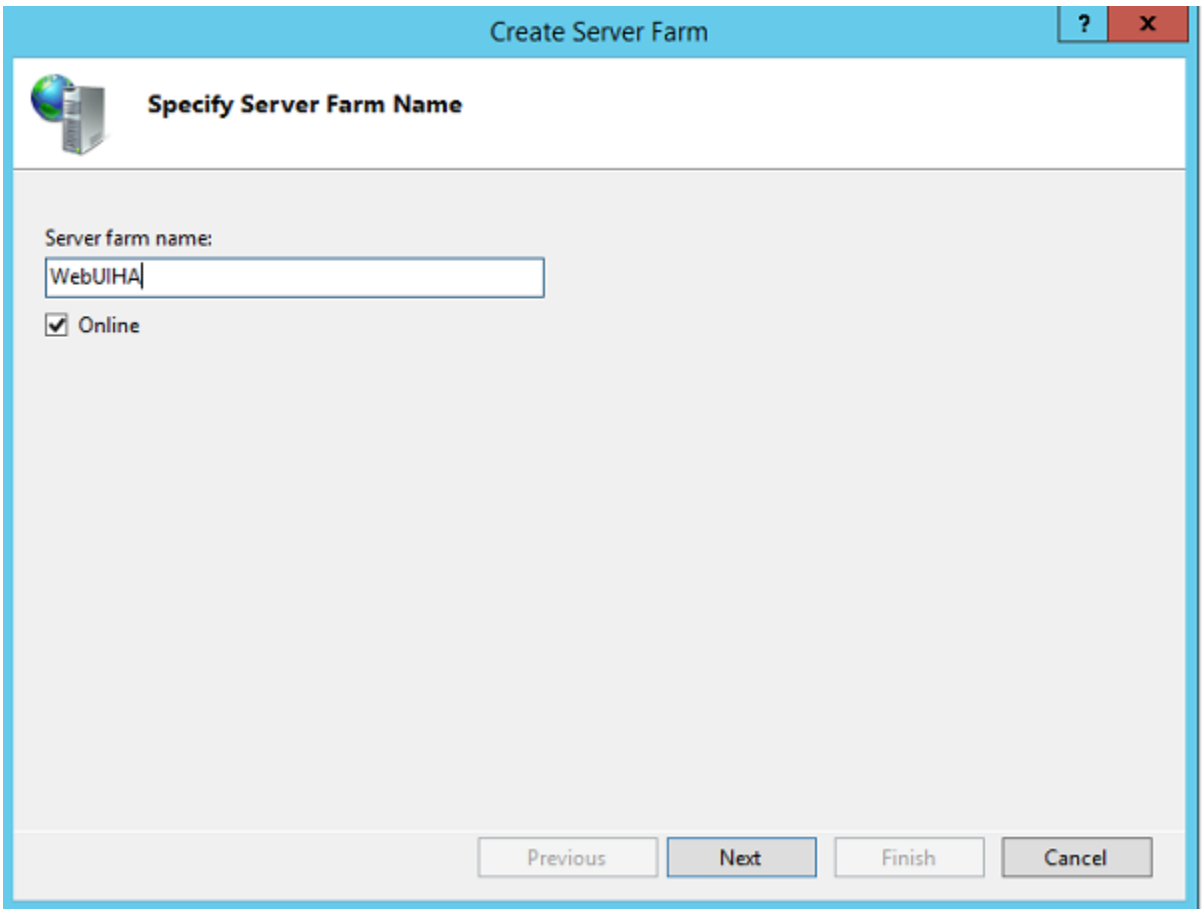


Figure 59. Créer une batterie de serveurs

4 Cliquez sur **Next (Suivant)**.

5 Sur la page **Add Server (Ajouter un serveur)**, ajoutez les serveurs d'application (serveurs d'interface utilisateur Web).

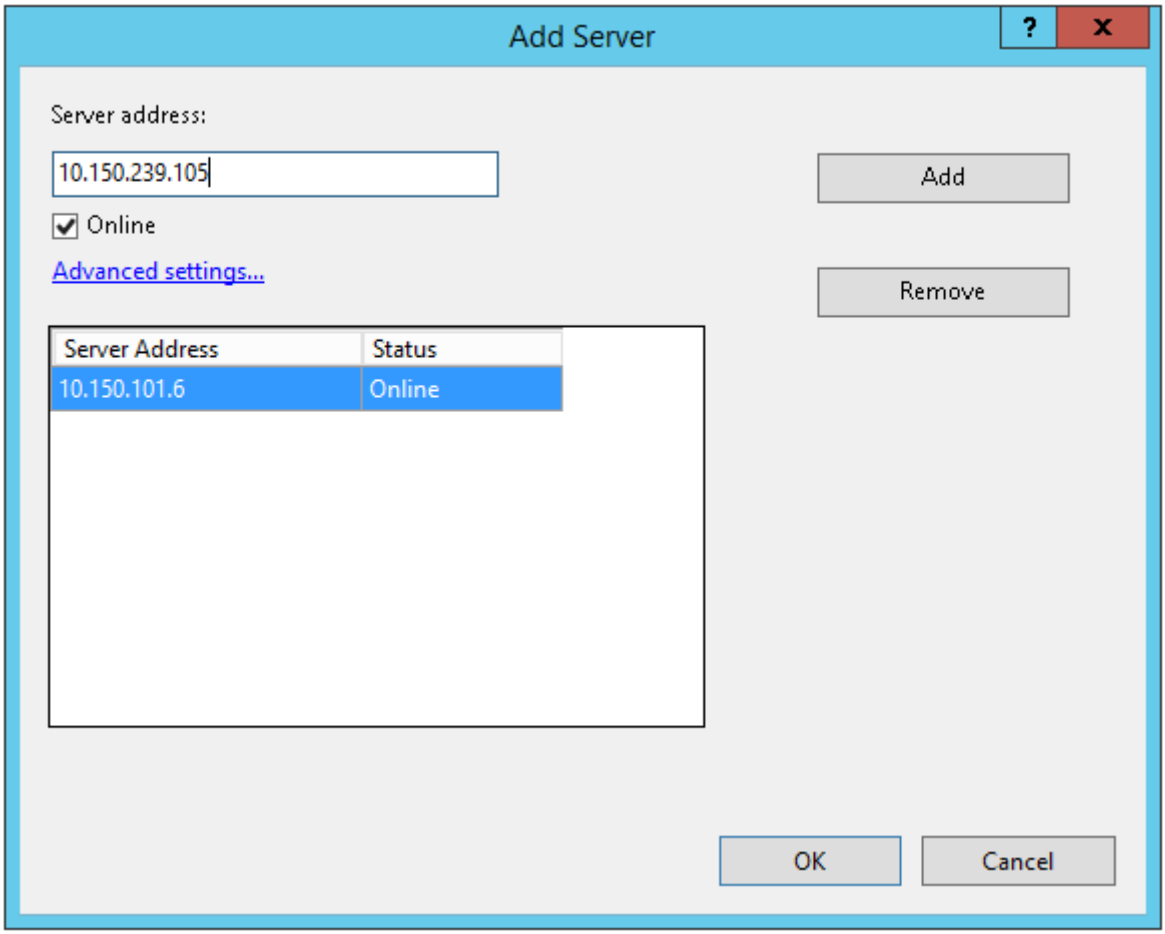


Figure 60. Ajouter un serveur

6 Cliquez sur **Finish (Terminer)** pour créer la batterie de serveurs, avec les entrées d'application saisies en tant que membres de la batterie de serveurs.

La fenêtre **Rewrite Rules (Règles de réécriture)** s'affiche.

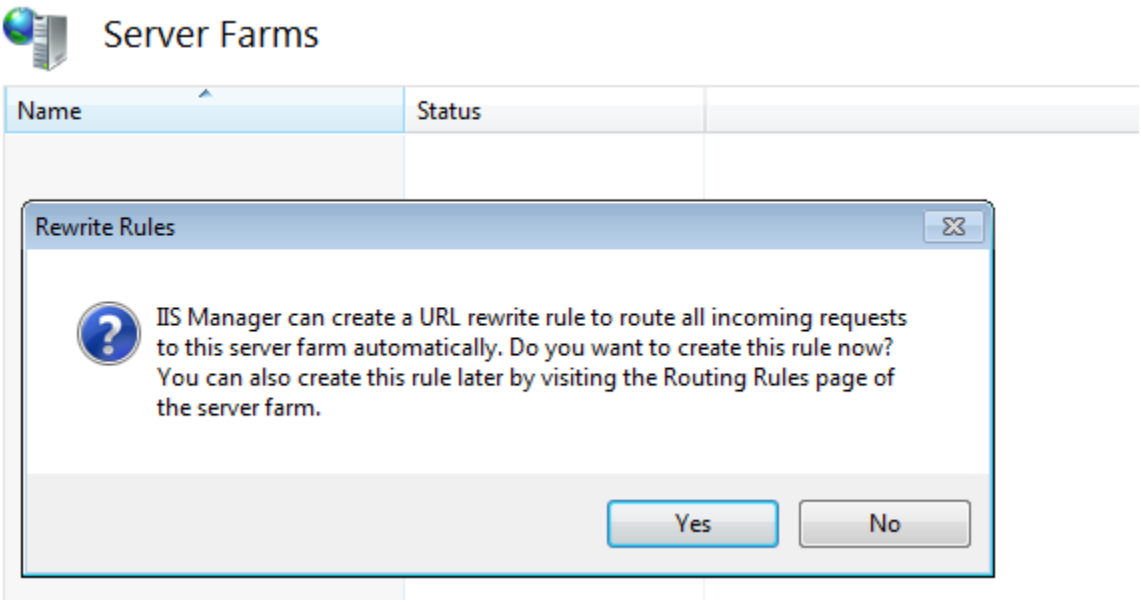


Figure 61. Règles de réécriture

7 Cliquez sur **Yes (Oui)** afin que IIS Manager 5Gestionnaire des services IIS) crée une règle de réécriture d'URL pour diriger toutes les demandes entrantes vers cette batterie de serveurs.

Configuration du SSL sur le serveur proxy

Pour configurer le SSL sur le proxy ARR, créez un certificat de domaine pour le serveur proxy. Attribuez ce certificat aux liaisons https pour le site Web concerné et activez le SSL.

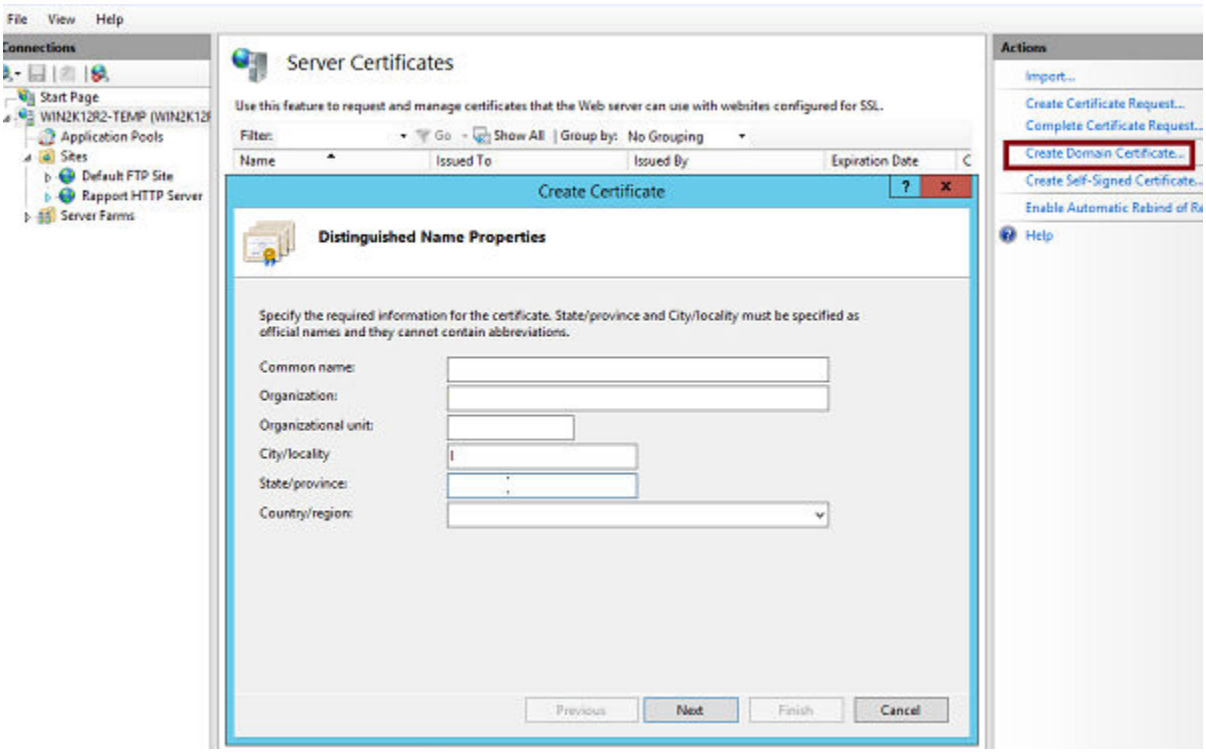


Figure 62. Certificats de serveur

La communication entre le serveur proxy ARR et les serveurs de gestion WDM doit s'effectuer via le protocole HTTPS. Par conséquent, vous devez désactiver la fonction SSL off-loading (Allègement SSL) et configurer le SSL sur chaque serveur de gestion WDM. Si vous utilisez un certificat auto-signé pour configurer le SSL sur le serveur de gestion WDM, importez ce certificat vers l'espace de stockage des Autorités de certification racine de confiance de l'ordinateur local, associé au serveur proxy ARR, en suivant les étapes mentionnées à l'adresse support.microsoft.com. IIS ARR exige qu'un certificat de confiance existe entre l'ARR et le serveur back-end auquel il se connecte, sinon celui-ci renvoie une erreur de sécurité et refuse d'acheminer les données vers le serveur back-end.

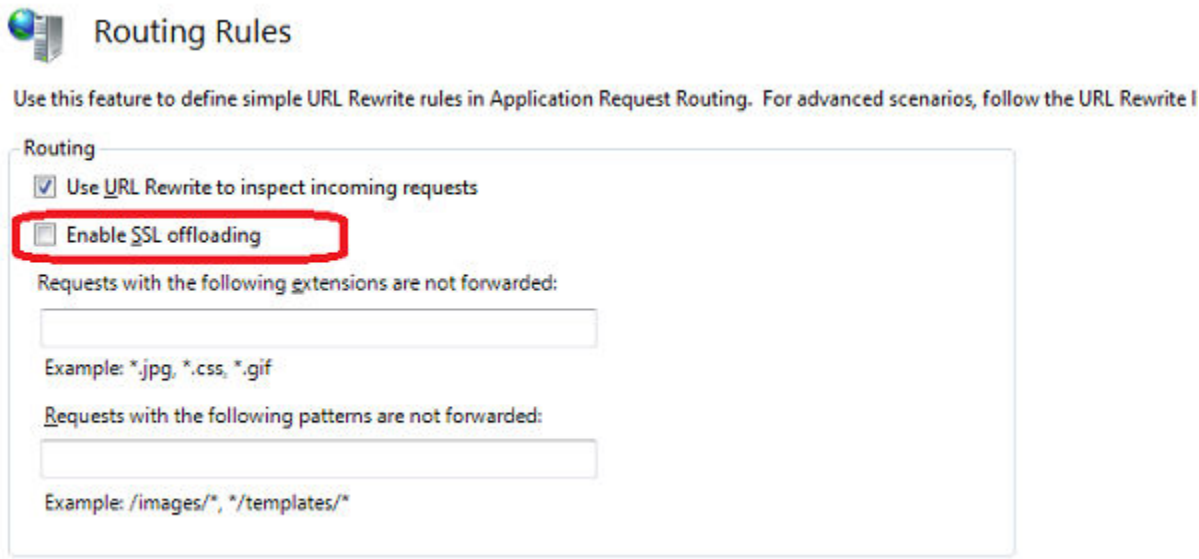


Figure 63. Règles de routage

Configuration des propriétés de la batterie de serveurs pour l'ARR

Une fois la batterie de serveurs créée et définie, vous devez déterminer des propriétés supplémentaires pour la gestion du comportement de l'ARR.

1 Connectez-vous au serveur proxy ARR et lancez IIS Server Manager (Gestionnaire des services IIS).

2 Sélectionnez la batterie de serveurs que vous avez créée. Les options suivantes s'affichent dans le panneau de droite :
   - Caching (Mise en cache)
   - Health Test (Test d'intégrité)
   - Load Balance (Équilibrage de charge)
   - Monitoring and Management (Surveillance et gestion)
   - Proxy
   - Routing Rules (Règles de routage)
   - Server Affinity (Affinité du serveur)

3 Sélectionnez **Caching (Mise en cache)**.
   a Déselectionnez l'option **Enable disk cache (Activer le cache du disque)** pour désactiver la mise en cache.
   b Réglez **Memory cache duration (Durée de la mise en cache mémoire)** sur 0.

4 Sélectionnez **Health Test (Test d'intégrité)**.
   a Saisissez le nom complet de domaine (FQDN) du serveur proxy ARR dans le champ **URL**. La valeur doit être la suivante : **https://<Proxy IP|FQDN>/hapi/ping**. Il s'agit de l'URL que l'ARR utilise pour envoyer des requêtes au serveur de gestion WDM pour vérifier l'intégrité d'une batterie de serveurs donnée.
   b Définissez l'intervalle de temps après lequel le test d'intégrité de l'ARR répète le contrôle d'intégrité. La valeur par défaut est de 30 secondes. Vous pouvez définir jusqu'à 180 secondes.

c Définissez le délai d'expiration de session pour l'URL que vous avez spécifiée. Il s'agit du délai après lequel, si le serveur ne répond pas, il est indiqué comme étant **Unhealthy (Défectueux)**.

d Définissez les **Acceptable Status codes (Codes d'état acceptables)** sur **200-399**. Si l'URL d'intégrité renvoie un code d'état qui ne correspond pas à la valeur indiquée dans **Acceptable Status Codes (Codes d'état acceptables)**, alors l'ARR marque le serveur comme défectueux.

e Définissez la valeur de texte **Server Healthy (Serveur sain)** dans le champ **Response Match (Correspondance des réponses)**. Le texte dans le champ **Response Match (Correspondance des réponses)** est comparé à l'entité de réponse de chaque serveur et, si la réponse d'un des serveurs ne contient pas la chaîne précisée dans la correspondance de réponse, alors ce serveur est indiqué comme étant défectueux.

f Cliquez sur **Verify URL (Vérifier URL)**. Cela devrait être effectué pour tous les serveurs de gestion WDM présents dans la batterie de serveurs.

5 Modifiez l'algorithme **Load Balance (Équilibrage de charge)**.

a Sélectionnez **Server variable hash (Hachage des variables du serveur)** dans la liste déroulante **Load balance algorithm (Algorithme de l'équilibrage de charge)**.

b Entrez la valeur de **Server Variable (Variable de serveur)** `HTTP_WDM_X_USER`.

c Cliquez sur **Apply (Appliquer)**.

6 Double-cliquez sur l'option **Monitoring and Management (Surveillance et gestion)** pour afficher l'état d'intégrité du serveur de gestion WDM, ainsi que d'autres options. Vous pouvez définir l'état sur Healthy (Sain) manuellement.

7 Double-cliquez sur **Proxy** pour configurer les paramètres du proxy :

a Réglez la valeur **Response buffer threshold (Seuil de mémoire tampon de réponse)** sur 0.

b Désélectionnez l'option **Keep Alive (Garder en vie)**.

c Changez la version **HTTP** en **HTTP/1.1**.

d Sélectionnez l'option **Reverse rewrite host in response headers (Hôte de réécriture inverse dans les en-têtes de réponse)**.

8 Double-cliquez sur **Routing Rules (Règles de routage)**.

a Cliquez sur **URL Rewrite (Réécriture d'URL)** sur le volet **Actions**.

b Sur la page **Edit Inbound Rule (Modifier la règle de trafic entrant)**, définissez le **Pattern (Modèle)** sur **(webui|hapi)/.***.

Cette étape garantit que seules les demandes d'URL destinées au serveur de gestion WDM sont envoyées à la batterie de serveurs par le serveur proxy ARR.

Les propriétés de la batterie de serveurs sont désormais configurées.

Journalisation sur le navigateur de l'interface utilisateur Web

1 Connectez-vous à l'interface utilisateur Web à l'aide de l'adresse IP du proxy ou d'un FQDN dans l'URL du navigateur.

2 Lorsque le serveur connecté est indiqué comme étant défectueux après le test d'intégrité mentionné ci-dessus, l'interface utilisateur Web se déconnecte.

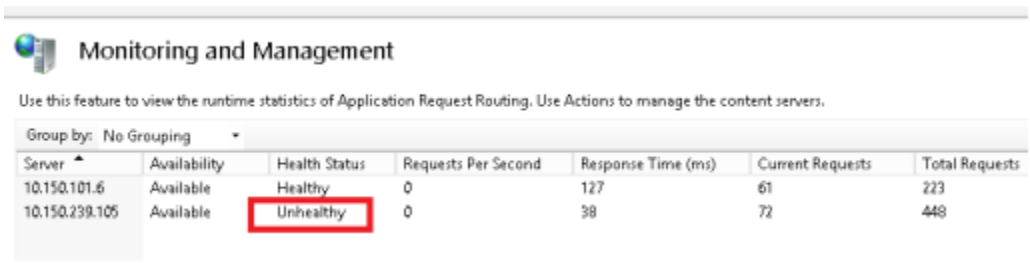


Figure 64. Surveillance et gestion

3 Connectez-vous à nouveau pour vous connecter à l'autre serveur back-end sain.

8

Installation manuelle de la base de données WDM à l'aide de scripts

Cette section indique les scripts de base de données pris en charge par WDM (Wyse Device Manager) et détaille les fonctionnalités associées.

Sujets :

Configuration requise

Prise en charge de la base de données WDM existante

L'installation de WDM prend en charge SQL Server 2008. La base de données contient tous les objets SQL Server, notamment les tables, vues et procédures stockées. Le programme d'installation de WDM stocke la base de données dans le dossier correspondant (**C:\Program Files (x86) \Wyse WDM\Database**, par défaut) et relie ce dossier au serveur sur lequel WDM doit être installé.

Ensuite, il met à jour les détails du serveur, les détails de l'utilisateur, les détails de configuration de la logithèque, et autres données sur le serveur.

Procédure suggérée d'installation de la base de données WDM

Les scripts sont utilisés pour installer la version 5.7.3 de la base de données WDM.

Conditions préalables : avant d'exécuter les scripts, le dossier de la base de données doit être créé et le pare-feu doit être désactivé au niveau du serveur de base de données.

REMARQUE : Les scripts suivants doivent être exécutés dans l'ordre où ils sont mentionnés. Sinon, vous devez supprimer la base de données et réexécuter la procédure dans son ensemble.

Fichiers de script

La base de données suivante sera utilisée pour installer la base de données de WDM 5.7.3 :

- CreateDatabase.sql
- Schema&User.sql
- Tables.sql
- Userdefinedtables.sql
- Views.sql
- Stored_Procedures.sql
- Default_Table_Data.sql

- CustomizeScript.sql

CreateDatabase.sql

Pour créer la base de données manuellement, exécutez le script suivant :

REMARQUE : Les scripts de base de données sont mentionnés ici à des fins de personnalisation.

```
CREATE DATABASE [RapportDB]

ON PRIMARY

(NAME = N'Rapport_dat', FILENAME = N'C:\Program Files (x86)\Wyse\WDM\Database\Rapport4.MDF,
SIZE = 42496KB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%)

LOG ON

(NAME = N'Rapport_log', FILENAME = N'C:\Program Files (x86)\Wyse\WDM\Database\Rapport4.LDF',
SIZE = 768KB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%)

GO
```

1 Le fichier script contient les scripts de création de la base de données RapportDB.

2 L'utilisateur ou l'administrateur peuvent modifier le chemin d'accès au fichier. Le chemin par défaut d'accès au fichier est C:\Program Files (x86)\Wyse\WDM\Database.

REMARQUE : Afin de confirmer que l'étape s'est terminée avec succès, accédez au dossier indiqué ci-dessus et vérifiez qu'il contient les fichiers Rapport4.mdf et Rapport4.ldf.

Schema&User.sql

Ce script permet de créer un compte d'utilisateur. Vous pouvez ajouter des autorisations et les attribuer au compte d'utilisateur de votre choix.

1 Le fichier de script contient les informations relatives à la création du schéma et du rôle d'utilisateur.

2 Les valeurs par défaut sont « rapport schema » et « rapport user ». Vous pouvez notamment modifier l'utilisateur ayant accès à WDM.

Tables.sql

Ce fichier de script contient un script pour l'ensemble des objets et contraintes de table.

REMARQUE : Les modifications personnalisées ne sont pas incluses dans ce fichier.

Userdefinedtables.sql

Ce fichier de script contient un script pour tous les objets de table définis par l'utilisateur.

REMARQUE : Les modifications personnalisées ne sont pas incluses dans ce fichier.

Views.sql

Ce fichier de script contient un script pour tous les objets de visualisation.

REMARQUE : Les modifications personnalisées ne sont pas incluses dans ce fichier.

Stored_Procedures.sql

Ce fichier de script contient un script pour tous les objets de procédure stockée.

REMARQUE : Les modifications personnalisées ne sont pas incluses dans ce fichier.

Default_Table_Data.sql

Ce fichier de script contient un script pour toutes les valeurs de données de table par défaut, notamment les informations relatives au système d'exploitation, à la plateforme, au type de gestion, aux groupes par défaut, aux progiciels par défaut ou encore aux paramètres par défaut.

REMARQUE : Les modifications personnalisées ne sont pas incluses dans ce fichier.

CustomizeScript.sql

Ce fichier de script contient un script pour les valeurs de données personnalisées.

Entrez le nom du serveur de base de données lors de l'exécution du script suivant. Une erreur s'affiche si vous ne procédez pas à cette opération.

REMARQUE :

---- Script personnalisé

```
Use RapportDB
Go
SET IDENTITY_INSERT [dbo].[License] ON
INSERT [dbo].[License]
([LicenseID], [Sales], [UnActivated], [Code], [License], [Utilize], [NumberOfClients],
[VendorID])
VALUES
(1, N'7V931PHY08K01LZHYXWKKP6GQ1', N'BR69T51SSP500PFW9W4R0Z0TL5', NULL, NULL, NULL, NULL, NULL)
SET IDENTITY_INSERT [dbo].[License] OFF
GO
SET IDENTITY_INSERT [dbo].[sysHash] ON
INSERT [dbo].[sysHash] ([ID], [Hash]) VALUES (2,
0x4458473935334D3151303452525452464347533834342485836)
SET IDENTITY_INSERT [dbo].[sysHash] OFF
Go
Begin
Declare @DBServerName varchar(200) = ''
Set @DBServerName = ''
If (@DBServerName is null or @DBServerName = '')
Begin
RAISERROR(N'Database Server Name Should not be Empty...', 16, 1)
End
Else
Begin
SET IDENTITY_INSERT [dbo].[Install] ON
INSERT [dbo].[Install]
([InstallID], [Module], [ServerName], [UserName], [Installed], [Status], [Information],
[RegKey], [RegName], [RegValue], [LatestHFID], [SiteID], [SiteName])
VALUES
(0, N'Rapport4DB', @DBServerName, N'administrator', GetDate(), N'MASTER', NULL, NULL, NULL,
NULL, N'00HF05070001516', 0, NULL)
SET IDENTITY_INSERT [dbo].[Install] OFF
End
End
Go
```

9

Troubleshooting

Cette section explique comment résoudre les problèmes que vous pouvez rencontrer lors de l'installation ou de la mise à niveau de WDM.

Sujets :

Erreur lors de l'installation de .NET Framework dans Windows 2012 et Windows Server 2016

Problème : l'installation de .NET Framework 3.5 sous Windows Server 2012 et Windows Server 2016 a échoué et le code d'erreur 0x800F0906 s'affiche

Résolution :

Méthode 1 :

1 Connectez-vous au système équipé de Windows Server 2012 et Windows Server 2016 et démarrez le Server Manager (Gestionnaire de serveur).

2 Installez les fonctionnalités .NET Framework 3.5 avec l'Assistant **Add Roles and Features (Ajout de rôles et de fonctionnalités)** du Server Manager (Gestionnaire de serveur).

3 Lors de l'installation, indiquez un chemin d'accès source alternatif en utilisant le lien situé en bas de l'Assistant.

Méthode 2 :

À l'aide de l'invite de commandes DISM, indiquez le paramètre du chemin d'accès aux fichiers sources :

Par exemple, si **D:** est le support DVD de Windows Server, alors le chemin d'accès aux fichiers sources est : DISM /Online /Enable-Feature /FeatureName:NetFx3ServerFeatures /FeatureName:NetFx3 /Source:D:\Sources\sxs

Méthode 3 :

1 Connectez-vous au système équipé de Windows Server 2012 et Windows Server 2016 et démarrez le Server Manager (Gestionnaire de serveur).

2 Installez le **Server Role Windows Server Update Services (WSUS) (Rôle du serveur du service WSUS)** à l'aide de l'Assistant **Add Roles and Features (Ajout de rôles et de fonctionnalités)** du Server Manager (Gestionnaire de serveur).

3 À l'aide de l'invite de commandes DISM, indiquez le paramètre du chemin d'accès aux fichiers sources : DISM /Online /Enable-Feature /FeatureName:NetFx3ServerFeatures /FeatureName:NetFx3.

4 Vérifiez que le service Windows Update est exécuté et qu'il est possible de se connecter au magasin Windows Update depuis l'endroit où les composants nécessaires peuvent être récupérés.

Échec lors de l'attachement de la base de données

Problème : échec lors de l'attachement de la base de données sous Windows 2012 Server, avec SQL Server 2012.

Résolution :

exécutez le service SQL « MSSQLSERVER » par le biais du compte « LocalSystem » du système cible pour l'installation de WDM.

Réessayez d'installer WDM.

Erreur lors de l'installation de la base de données WDM en configuration distribuée

Problème : lors de l'installation de la base de données WDM sur un système distinct possédant déjà la version de SQL Server prise en charge, alors l'erreur suivante peut s'afficher lorsque vous lancez l'exécutable **Setup.exe** : *Le programme d'installation n'a pas pu initialiser les bibliothèques requises*.

Résolution : vérifiez que **Microsoft Visual C++ Redistributable 2008**, **version 9.0.21022** est installé. Vous devez accéder à **Start (Démarrer)** > **Control Panel (Panneau de configuration)** > **Programs (Programmes)** pour voir si le package redistribuable est installé. S'il n'est pas installé, vous devez l'installer manuellement en exécutant le fichier **vcredist_x86.exe** disponible sous le dossier **Prereq** du programme d'installation WDM.

Échec de l'installation de la base de données après la désinstallation manuelle de SQL Server Express 2014

Problème : l'installation de la base de données WDM a échoué après la désinstallation manuelle de SQL Server Express 2014 et l'utilisation de l'option **Install New Database** (Installer une nouvelle base de données) du programme d'installation.

Résolution : pour résoudre ce problème :

1 Désinstallez SQL Server Express 2014 R2 dans le menu Add\Remove Programs (Ajouter/Supprimer des programmes).

2 Faites apparaître la fenêtre **Services** présente dans **Administrative Tools (Outils d'administration)** > **Control Panel (Panneau de configuration)**.

3 Supprimez le service **MSSQL$RapportDb**

.

4 Supprimez **MSSQL12.RAPPORTDB** du dossier d'installation de SQL Server Express.

5 Supprimez l'entrée de registre **RapportDB** présente dans **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server \Instance Names\SQL**.

6 Supprimez l'entrée de registre **MSSQL10_50.RAPPORTDB** présente dans **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Microsoft SQL Server**.

7 Supprimez l'entrée de registre **RAPPORTDB** présente dans **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server**.

8 Redémarrez le programme d'installation WDM.

Après une mise à niveau de WDM 5.5.1 vers WDM 5.7, la logithèque n'est pas sécurisée

Problème : Si WebUi est sélectionnée au cours de la mise à niveau, le serveur de gestion sera configuré pour Https, mais la logithèque WDM des logiciels ne sera pas configurée par le programme d'installation.

Résolution : définissez manuellement la logithèque sur HTTPS dans l'interface utilisateur WDM. Pour ce faire, accédez à **Configuration Manager (Gestionnaire de configuration)Software Repository (Logithèque)**.

Dépannage après le déploiement

Problème : erreur HTTP 404.0 - Introuvable. La Web.config de l'HApi devrait être ajoutée à l'aide d'un module de routage URL, si celle-ci venait à manquer :

Résolution : ajoutez la Web.config de l'HApi à l'aide d'un module de routage URL comme suit :

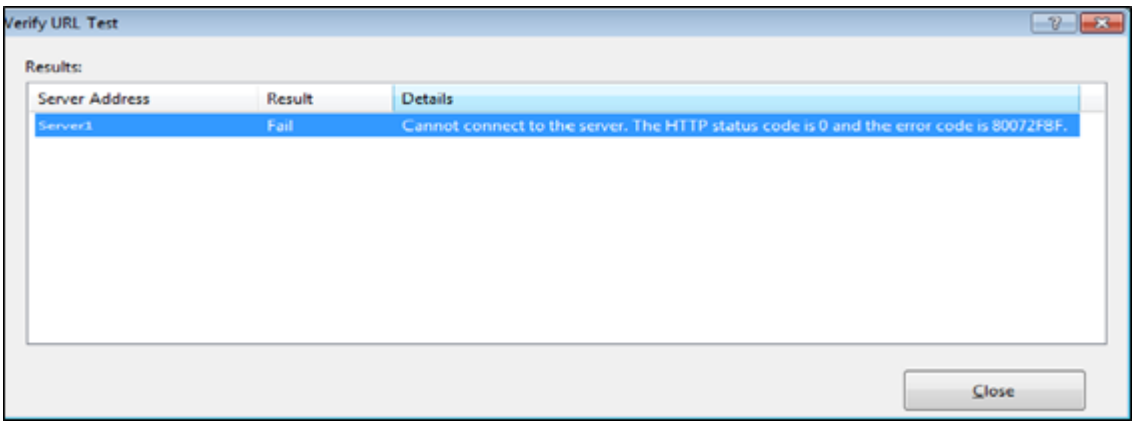
```
<system.webserver>
<modules>
<remove name= "urlroutingmodule-4.0"/>
<add name= "urlroutingmodule-4.0" type="system.web.Routing.urlroutingmodule" precondition="" />
</modules>
```

Dépannage des problèmes d'équilibrage de charge

Cette section décrit la façon de résoudre certains problèmes que vous pouvez rencontrer durant la configuration de l'équilibrage de charge.

Défaillance de la fonction de test d'intégrité dans le proxy ARR avec SSL

Problème : si le proxy ARR n'approuve pas le Certificat numérique du serveur du système principal, alors un échec du test d'intégrité peut survenir et afficher le code d'erreur 80072F8F.



Résolution : importez le certificat utilisé pour la configuration du SSL sur le serveur de gestion WDM dans **Trusted Root Certificate Authorities store for a local computer (Réserve des autorités de certification racine de confiance pour un ordinateur local)** située dans le système proxy ARR en vous référant à technet.microsoft.com.

Le proxy ARR renvoie le code d'erreur HTTP 502.3

Problème : le proxy ARR renvoie le code d'erreur HTTP Proxy 502.3 pour les anciens Agents WDM (HAgents) qui n'envoient pas la balise **HTTPHEADSUPP=2** lorsqu'ils s'enregistrent. Si le HAgent n'envoie pas la balise **HTTPHEADSUPP=2** lors de l'enregistrement, le serveur de gestion n'envoie pas l'en-tête du code d'état HTTP (200 OK) en réponse et le proxy ARR renvoie l'erreur. Seuls les clients envoyant la valeur **2** sont pris en charge dans la configuration de l'équilibreur de charge.

Résolution : vous pouvez exécuter la requête suivante sur la base de données WDM et lire la valeur :

```
SELECT [HttpHeadSupp]
FROM    [ClientNetwork]
where  [MAC] = <ClientMac>
```

Le proxy ARR renvoie le code d'erreur HTTP 502.4

Problème : le serveur proxy ARR renvoie le code d'erreur HTTP 502.4 lorsqu'un des serveurs de gestion (HServers) n'est pas disponible. La condition d'intégrité de tous les HServers dans **Server Farm** (Batterie de serveurs) peut être définie sur **Unhealthy** (Défectueux) car les tests d'intégrité configurés ont échoué.

Résolution : pour remédier à ce problème :

1 Connectez-vous au serveur proxy ARR et lancez IIS Server Manager (Gestionnaire des services IIS).

2 Sélectionnez la batterie de serveurs que vous avez créée et, sur le volet droit, sélectionnez **Monitoring and Management** (Surveillance et gestion).

3 Sélectionnez les « HServers » et, sur le volet **Action**, sélectionnez **Set Server as Healthy** (Définir le serveur comme sain).

4 Si la charge du « HServer » est élevée, essayez alors d'augmenter les valeurs d'**intervalle** et de **délai d'attente** dans la fonctionnalité **Health Test** (Test d'intégrité)

Activation du déchargement SSL sur le proxy

L'équilibrage de charge est uniquement pris en charge par les configurations HTTPS. Lors du débogage, si vous souhaitez afficher la réponse du serveur de gestion (HServer) dans la saisie **Wireshark**, alors vous pouvez changer la communication du proxy HServer en HTTP.

1 Connectez-vous au serveur proxy ARR et lancez IIS Manager (Gestionnaire des services IIS).

2 Double-cliquez sur la fonctionnalité **Routing Rules** (Règles de routage) et sélectionnez le paramètre **Enable SSL offloading** (Activer le déchargement SSL).

3 Activez à la fois la liaison HTTP et la liaison HTTPS sur le site Web des machines HServer et ne sélectionnez pas **Require SSL** (Exiger SSL) dans **SSL Settings** (Paramètres SSL).

..

Processus infini au cours de l'installation

Problème : l'installation se poursuit indéfiniment lors de l'installation de Microsoft Visual C++ Redistribuables ou Microsoft SQL Express 2008. Les systèmes d'exploitation pris en charge sont Windows 2012 Standard et Windows 2012 R2.

Résolution : ouvrez le Gestionnaire de tâches, et vérifiez si le processus « **Windows Modules Installer Worker** » est en cours d'exécution ou non sur votre Thin Client. Si ce processus est en cours d'exécution, vous devez l'arrêter pour que l'installation reprenne. Redémarrez le Thin Client une fois l'installation terminée.

Problème de l'équilibrage de charge

Problème : le serveur proxy ne répond pas quand l'adresse IPv6 est active.

Résolution : désactiver l'adresse IPv6 de la configuration de l'équilibrage de charge.

Mise à niveau de WDM sous Windows 2008 SP2 32 bits

Problème : Afin de mettre à niveau vers WDM 5.7 sous Windows 2008 SP2 32 bits, activez le service Windows Update.

Résolution : pour mettre à niveau vers WDM 5.7 sous Windows 2008 SP2 32 bits, activez le service Windows Update pour installer le hotfix KB980368. Après l'installation du hotfix KB980368, désactivez le service Windows Update pour installer WDM 5.7.

Échec de l'installation de la mise à niveau de Dell Wyse Device Manager

Problème : l'installation de la mise à niveau WDM a échoué lors de la connexion à la logithèque.

Résolution : une des causes du problème peut venir du fait que le nom de l'ordinateur utilisé pour la configuration possède plus de 16 caractères. Cette situation entraîne une incompatibilité entre le nom de l'ordinateur et le nom NetBIOS (tronqué à 15 caractères) pour l'installation. Pour confirmer ce problème, vérifiez si les variables système mentionnées ci-dessus sont différentes. Le cas échéant, installez WDM sur une configuration qui possède un nom d'hôte de 15 caractères maximum, puis exécutez à nouveau le programme d'installation de la mise à niveau.

Problème de configuration de l'environnement cloud

Problème : un message d'erreur s'affiche par intermittence lorsque vous exécutez le fichier `setup.exe` pendant l'installation de WDM dans l'environnement cloud.

Résolution

- **Scénario 1– Seul le message d'erreur est affiché**

  Fermez la boîte de dialogue du message d'erreur, puis exécutez à nouveau le fichier `setup.exe`.
- **Scénario 2 – Un message d'erreur s'affiche, ainsi que l'écran d'accueil qui s'exécute en arrière-plan**

  Fermez la boîte de dialogue du message d'erreur ainsi que l'écran de bienvenue, puis exécutez à nouveau le fichier `setup.exe`.

Erreur d'installation de WDM lors d'une mise à niveau

Problème : lors de l'installation de WDM, si vous utilisez un autre utilisateur que l'utilisateur par défaut de la base de données, vous ne pourrez pas procéder à l'installation de WDM dans une mise à niveau. Le message d'erreur **Unable to proceed with the installation, aborting installation** (Impossible de continuer l'installation. Abandon de l'installation) s'affiche.

Solution :

- Ouvrez l'interface GUI WDM.
- Effectuez un clic droit sur **Configuration Manager** (Gestionnaire de configuration) et sélectionnez **Utilities (Utilitaires)** > **Database Credential Manager (Gestionnaire d'informations d'identification de la base de données**.
- Un message d'avertissement s'affiche. Cliquez sur **OK**.
- Entrez le nom d'utilisateur et le mot de passe que vous avez utilisés pour installer WDM. Cliquez sur **OK** pour continuer.
- Refermez l'interface utilisateur de WDM et procédez à l'installation.
- Après l'installation, exécutez à nouveau **Database Credential Manager** (Gestionnaire d'informations d'identification de la base de données) disponible au chemin d'installation (`C:\Program Files(X86)\Wyse\WDM\Utilities\Database`).
- Fournissez le nom d'utilisateur et le mot de passe que vous avez utilisés pour installer WDM, puis redémarrez le serveur.