Dell Wyse Device Manager 5.7.3

Installationsanleitung

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

2018–04

Rev. A00

Inhaltsverzeichnis

1

Einführung

Dell Wyse Device Manager (WDM) ist eine Software, mit der sich alle Dell Wyse Thin und Zero Clients verwalten lassen. WDM ermöglicht IT-Administratoren, die folgenden Funktionen auszuführen:

- Erstellung von Software-Images, Aktualisierung und Konfiguration von Thin- und Zero-Client-Geräten
- Asset Tracking von Geräten
- Überwachung der Integrität von Dell Geräten
- Verwaltung der Richtlinien und Netzwerkeinstellungen auf Geräten
- Externe Verwaltung und Shadowing von Geräten

WDM verwendet branchenübliche Kommunikationsprotokolle und eine komponentenbasierte Architektur für die effiziente Verwaltung der Geräte im Netzwerk. Dieses Handbuch enthält Informationen über die Voraussetzungen für die Installation von WDM und die Schritte zum Installieren und Konfigurieren von WDM in Ihrer Umgebung.

Themen:

Matrix Installationsprogramm

Die folgende Matrix beschreibt die verschiedenen Kombinationen von Microsoft SQL Server und Microsoft Windows Server, die das Installationsprogramm unterstützt.

Tabelle 1. Matrix Installationsprogramm

			Windows Server 2008 R2 mit SP1			
RapportDB-Authentifizierung		**SQL**			**Windows**	
	Enterprise	**Workgroup**	**Verteilt**	**Enterprise**	**Workgroup**	**Verteilt**
Windows 2008 R2 SP1 + SQL Server 2008 R2	Ja	Ja	Ja	Ja	Ja	Ja
Windows 2008 R2 SP1 + SQL Server 2008	Ja	Ja	Ja	Ja	Ja	Ja
Windows 2008 R2 SP1 + SQL Server 2012	Ja	Ja	Ja	Ja	Ja	Ja

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

Support-Matrix

Tabelle 2. Support-Matrix

Unterstützte Betriebssysteme für WDM Server	• Windows Server 2008 R2 Enterprise SP1 • Windows Server 2012 Standard • Windows Server 2012 R2 • Windows Server 2016 • Windows 7 Enterprise SP1 – 64-Bit
Unterstützte Betriebssysteme für das Upgrade aller WDM-Komponenten	• Windows 2008 R2 SP1 Enterprise • Windows 2008 Service Pack 2 32-Bit • Windows 7 Enterprise SP1—32-Bit • Windows Server 2012 Standard • Windows Server 2012 R2
Unterstützte Datenbanken	• Microsoft SQL Server 2008 R2 – Englisch • Microsoft SQL Server 2008 Enterprise – 32-Bit • Microsoft SQL Server 2012

	• Microsoft SQL Server 2014 • Microsoft SQL Server 2016 • Microsoft SQL Server 2012 Enterprise Edition für hohe Verfügbarkeit • Microsoft SQL Server 2016 Express SP1
Unterstützte Thin Clients	**Wyse ThinOS** • Wyse 3010 Thin Client mit ThinOS • Wyse 3020 Thin Client mit ThinOS • Wyse 3040 Thin Client mit ThinOS • Wyse 5010 Thin Client mit ThinOS • Wyse 5040 Thin Client mit ThinOS • Wyse 3030 LT Thin Client mit ThinOS • Wyse 5060 Thin Client mit ThinOS • Wyse 7010 Thin Client mit ThinOS **Wyse ThinOS PCoIP** • Wyse 5040 AIO Thin Client mit PCoIP • Wyse 5010 Thin Client mit PCoIP • Wyse 3030 LT Thin Client mit PCoIP • Wyse 5060 Thin Client mit PCoIP **Wyse Enhanced Microsoft Windows Embedded Standard 7 – Build 818 und höher** • Wyse 5010 Thin Client mit WES7 • Wyse 5020 Thin Client mit WES7 • Wyse 7010 Thin Client mit WES7 • Wyse 7020 Thin Client mit WES7 • Wyse 7010 erweiterte Gehäuse Thin Client mit WES7 • Wyse 3030 Thin Client mit WES7 **Wyse Enhanced Microsoft Windows Embedded Standard 7P – Build 850 und höher** • Wyse 7010 Thin Client mit WES7P • Wyse 7010 erweiterte Gehäuse Thin Client mit WES7P • Wyse 5020 Thin Client mit WES7P • Wyse 7020 Thin Client mit WES7P • Wyse 7040 Thin Client mit WES7P • Dell Latitude E7270 Mobile Thin Client • Wyse 5060 Thin Client mit WES7P • Latitude 3460 Mobile Thin Client **Wyse Enhanced Microsoft Windows Embedded 8 Standard – 64-Bit** • Wyse 5010 Thin Client mit WE8S • Wyse 5020 Thin Client mit WE8S • Wyse 7010 Thin Client mit WE8S • Wyse 7020 Thin Client mit WE8S **Windows 10 IoT Enterprise – 64-Bit**

	• Wyse 5020 Thin Client mit Win10 IoT • Wyse 7020 Thin Client mit Win10 IoT • Wyse 7040 Thin Client mit Win10 IoT **Wyse Enhanced SUSE Linux Enterprise** • Wyse 5010 Thin Client mit Linux • Wyse 5020 Thin Client mit Linux • Wyse 7010 Thin Client mit Linux • Wyse 7020 Thin Client mit Linux **ThinOS Lite** • Wyse 3010 Zero Client für Citrix • Wyse 3020 Zero Client für Citrix • Wyse 5010 Zero Client für Citrix **ThreadX/View Zero Client** • Wyse 5030 Zero Client • Wyse 7030 Zero Client • Wyse 5050 AIO Zero Client mit PCoIP **ThinLinux** • Wyse 3030 LT Thin Client mit ThinLinux • Wyse 3040 Thin Client mit ThinLinux • Wyse 7020 Thin Client mit ThinLinux • Wyse 5020 Thin Client mit ThinLinux • Wyse 5060 Thin Client mit ThinLinux
Unterstützte EOL Dell Wyse Thin Client-Plattformen	**Wyse Enhanced Microsoft Windows Embedded Standard 7 – Build 818 und höher** • C90LE7 • R90L7 • R90LE7 • X90c7 • X90m7 • Z90s7 **Wyse Enhanced Microsoft Windows Embedded Standard 7P** • X90m7P • Z90s7P **Wyse Enhanced Microsoft Windows Embedded 8 Standard – 32-Bit** • Wyse 5010 Thin Client mit WE8S • Wyse 7010 Thin Client mit WE8S • Z90D8E **Wyse Enhanced SUSE Linux Enterprise** • C50LE • R50L • R50LE

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

Unterstützte Lokalisierungen

WDM-Server unterstützt die folgenden Lokalisierungen auf den Plattformen Windows Server 2008R2 SP, Windows Server 2012 R2 und Windows Server 2016:

- Französisch
- Deutsch
- Spanisch
- Japanisch
- Chinesisch (vereinfacht)

Technischer Support für Dell Wyse

Technische Ressourcen des Self-Service-Portals, der Knowledge Base, Software-Downloads , Registrierung, Serviceverlängerungen/RMAs, Referenzhandbücher usw. finden Sie unter www.dell.com/wyse/support . Informationen zum Kunden-Support finden Sie unter www.dell.com/support/contents/us/en/19/article/Contact-Information/International-Support-Services/international-contact-center?ref=contactus und Telefonnummern für Basic und Pro Support sind unter www.dell.com/supportcontacts verfügbar.

HINWEIS: Vergewissern Sie sich vor dem Fortfahren, ob Ihr Produkt über eine Dell-Service-Tag-Nummer verfügt. Weitere Informationen zu Produkten mit Dell-Service-Tag-Nummer finden Sie unter www.dell.com/support/contents/us/en/19/article/Product-Support/Dell-Subsidiaries/wyse.

Zugehörige Dokumentation und Dienste

Technische Datenblätter mit Funktionen von Hardwareprodukten sind auf der Dell Wyse-Website verfügbar. Rufen Sie http://www.dell.com/wyse auf, wählen Sie Ihr Hardwareprodukt und laden Sie das technische Datenblatt herunter.

Um Support für Ihr Wyse-Produkt zu erhalten, überprüfen Sie die Service-Tag- oder Seriennummer Ihres Produkts.

- Für Produkte, die mit einer Dell Service Tag-Nummer gekennzeichnet sind, finden Sie Knowledge Base-Artikel und Treiber auf den Dell Wyse-Produktseiten.
- Für Produkte, die nicht mit einer Dell Service Tag-Nummer gekennzeichnet sind, finden Sie alle erforderlichen Support-Materialien in der Wyse Support-Domäne.

Dell Wyse Online-Community

Dell Wyse bietet eine Online-Community, innerhalb der Benutzer unserer Produkte nach Informationen zu Benutzerforen suchen und diese austauschen können. Besuchen Sie die Dell Wyse Online-Community-Foren unter: en.community.dell.com/techcenter/enterprise-client/wyse_general_forum/.

2

Voraussetzungen

In diesem Abschnitt werden die Voraussetzungen sowie die Hardware- und Softwareanforderungen aufgeführt, die Sie erfüllen müssen, um Ihre Umgebung für die Installation und Konfiguration von WDM vorzubereiten. Dieser Abschnitt besteht aus folgenden Unterabschnitten:

- Checkliste vor der Installation
- Hardwareanforderungen
- Softwareanforderungen
- Kommunikationsportanforderungen
- Aktualisierungsanforderungen
- Anforderungen für die Verwaltung von PCoIP-Geräten

Themen:

Checkliste vor der Installation

Stellen Sie vor der Installation von WDM sicher, dass folgende Anforderungen erfüllt werden:

- Der Server, auf dem Sie WDM installieren, sollte ausschließlich für WDM-Dienste und nicht zum Ausführen zusätzlicher Funktionen verwendet werden. Der Server sollte beispielsweise nicht als Domain-Controller, Sicherungs-Controller, Mailserver, Produktions-Web-Server, DHCP-Server, MSMQ-Server oder Anwendungsserver verwendet werden.
- Installieren Sie ein unterstütztes Betriebssystem auf dem Server, auf dem Sie WDM installieren. Weitere Informationen finden Sie unter Support-Informationen.
- Stellen Sie sicher, dass keine anderen Anwendungen, die IIS erfordern, auf dem System, auf dem Sie WDM installieren, ausgeführt werden.
- Stellen Sie sicher, dass alle erforderlichen Kommunikationsports verfügbar und für die Kommunikation zwischen Servern, Routern und Switches offen sind. Weitere Informationen finden Sie unter Anforderungen an Kommunikationsports.
- Stellen Sie sicher, dass Sie während der Installation Zugriff auf die Betriebssystem-CD-ROM und Ihre Microsoft Windows-Systemdateien haben. Das WDM-Installationsprogramm überprüft das System auf alle Softwareanforderungen. Wenn eine bestimmte Software nicht installiert ist, werden Sie vom Installationsprogramm aufgefordert, die erforderliche Software zu installieren. Daher müssen Sie über Zugriff auf die Betriebssystem-DVD oder den Netzwerkstandort für den Zugriff auf die Microsoft Windows-Systemdateien verfügen.
- Installieren Sie Adobe Acrobat Reader, um die Endbenutzer-Lizenzvereinbarung (EULA) und das Installationshandbuch zu lesen.
- Für die Nutzung der ThreadX 5.x-Komponenten muss mindestens Windows Server 2012 installiert sein.

Hardwareanforderungen

Das System, auf dem Sie WDM installieren, sollte die minimalen Systemanforderungen erfüllen oder übertreffen und ist abhängig vom Betriebssystem, das Sie installieren. Der tatsächlich erforderliche freie Speicherplatz hängt von der Anzahl und der Größe der Pakete ab, die Sie registrieren, und auch von der Anzahl der Geräte, die Sie verwalten möchten.

Tabelle 3. Serverhardwareanforderungen für ein 32-Bit-Betriebssystem

Kategorie	Mindestanforderungen	Empfohlene Konfiguration
CPU	2,5 GHz Dual-Core Intel oder AMD	Quad Core Intel oder AMD
RAM	4 GB Im Falle einer virtuellen Maschine sollten zu Beginn 2 GB zugewiesen werden.	4 GB
Minimaler freier Speicherplatz	40 GB	40 GB

Tabelle 4. Serverhardwareanforderungen für ein 64-Bit-Betriebssystem

Kategorie	Mindestanforderungen	Empfohlene Konfiguration
CPU	2,5 GHz Dual-Core Intel oder AMD	Quad Core Intel oder AMD
RAM	6 GB	8 GB
Minimaler freier Speicherplatz	40 GB	40 GB

Kommunikationsportanforderungen

WDM-Softwarekomponenten erfordern, dass bestimmte Kommunikationsports auf Ihren Servern, Routern und Switches offen bleiben. WDM hängt beispielsweise von den HTTP/HTTPS-Kommunikationsports für Operationen ab, die von WDM initiiert und an Geräte weitergegeben werden.

Weitergabevorgänge umfassen:

- Erteilung von Gerätebefehlen, wie z. B. Geräteinformationen aktualisieren, Neustart, Geräte- oder Netzwerkinformationen ändern, Gerätekonfiguration abrufen, usw.
- Verteilung von Paketen zu einem bestimmten Zeitpunkt.

Normalerweise ist Port 80 der Standard-HTTP-Port und Port 443 der Standard-HTTPS-Port. Wenn einer dieser Ports geschlossen ist, kann WDM Aktualisierungen oder Echtzeitbefehle nicht an Geräte weiterleiten.

Tabelle 5. Kommunikationsports

WDM-Komponente	Protokoll und entsprechende Ports	Port	Funktion
GUI	HTTP	80 280	Kommunizieren mit dem Web Service und dem Standard Service.
	FTP	21	Registrieren neue Pakete im Master Software Repository.
	OLE DB	1433 (Standardeinstellung)	Kommunizieren mit der WDM-Datenbank.

WDM-Komponente	Protokoll und entsprechende Ports	Port	Funktion
		Kann während der Installation konfiguriert werden.	
	VNC	5800 5900	Remote-Spiegelgeräte.
Web Service	HTTP	80 280	Kommuniziert mit dem Web Agent, der GUI und dem Standard Service.
	HTTPS	443 8443	Sichere Kommunikation mit dem Web Agent, der GUI und dem Standard Service.
	OLE DB	1433 (Standardeinstellung) Kann während der Installation konfiguriert werden.	Kommunizieren mit der WDM-Datenbank.
Web Agent	HTTP	80 280	Kommunikation mit dem Web Service.
	FTP	21	Lesen und Schreiben von Dateien in die Master- und Remote-Software-Repositories.
DHCP-Proxy und TFTP-Services	OLE DB	1433 (Standardeinstellung) Kann während der Installation konfiguriert werden.	Kommunizieren mit der WDM-Datenbank.
	HTTP	8008	Kommunizieren mit der GUI und dem Web Service.
DHCP-Proxy und TFTP-Services und PXE	DHCP	67 68 4011	Prozess-UDP-Anfragen von PXE-aktivierten Geräten zum Standard Service.
	TFTP	69	Herunterladen eines startfähigen Abbilds zur Aktivierung der Verwaltungsverarbeitung.
	HTTP	80	Kommunizieren mit dem Web Service hinsichtlich der Aktionen und des Status der aktuellen Aufgabe.
	FTP	21	Herunterladen und Hochladen von Dateien von/auf den Master- und Remote-Software-Repositories.
DHCP-Proxy und TFTP-Services sowie Legacy-Unterstützung für ältere WDM-Agenten.	UDP	44956 44957	Ermittlung von Geräten unter Verwendung von Subnetz-Directed Broadcasts, auf denen ältere WDM-Agenten (5.0.0.x

WDM-Komponente	Protokoll und entsprechende Ports	Port	Funktion
			und frühere Versionen) installiert sind.
	TCP	44955	Ermitteln Sie Geräte über IP Range Walking. Aktualisieren Sie Geräte, auf denen ein älterer WDM-Agent (5.0.0.x und frühere Versionen) installiert ist.
ThreadX 4.x Manager-Dienst	TCP	9880 50000	Kommunikation mit ThreadX 4.x-Geräten.
ThreadX 5.x Manager-Dienst	TCP	49159 5172	Kommunikation mit ThreadX 5.x-Geräten. **ANMERKUNG: Beide Kommunikationsports müssen zu den eingehenden Firewall-Regeln hinzugefügt werden. Falls erforderlich, kann Portnummer 49159 individuell angepasst werden kann. Der Standardport 49159 ist individuell eingerichtet. Dies muss manuell hinzugefügt werden.**

Anforderungen für die Verwaltung von PCoIP-Geräten

PCoIP-Geräte, die die ThreadX-Firmware ausführen, benötigen einen DNS Service Location (SRV)-Ressourceneintrag, um folgende Aktionen durchzuführen:

- **Partial Check-In (heartbeat)** (Teil-Check-in (Heartbeat)) – Das Gerät führt jede Stunde einen Heartbeat-Check-in durch.
- **Firmware Download Completion Status** (Abschlussstatus des Firmware-Download) – Der Firmware-Upload wird vom Server und der Abschluss des Downloadvorgangs anhand des DNS-SRV-Eintrags vom Gerät initiiert.
- **ThreadX 4.x** – Konfigurieren Sie FTP, wenn Sie beabsichtigen, die Firmware-Upgrade-Funktion für die PCoIP (ThreadX 4.x)-Geräte zu verwenden. Sie müssen dies im Software Repository aktivieren. Weitere Informationen zum Aktivieren von FTP finden Sie im Dell Wyse Device Manager Administrator's Guide (*Administratorhandbuch für den Dell Wyse Device Manager*).
- **ThreadX 5.x** – Konfigurieren Sie CIFS, wenn Sie beabsichtigen, die Firmware-Upgrade-Funktion für die PCoIP (ThreadX 5.x)-Geräte zu verwenden. Sie müssen dies im Software Repository aktivieren. Weitere Informationen zum Aktivieren von CIFS im Software-Repository finden Sie im *Dell Wyse Device Manager Administrator's Guide* (*Administratorhandbuch für den Dell Wyse Configuration Manager*).

Checkliste zum Installieren der WDM Enterprise Edition

Wenn Sie die WDM Enterprise Edition installieren, stellen Sie Folgendes sicher:

- Beziehen Sie Ihren WDM Enterprise Sales Key oder den Enterprise Evaluation Key, den Sie während der Installation verwenden, und greifen Sie auf diesen zu.
- Installieren Sie die unterstützte Version von SQL Server. Das WDM-Installationsprogramm bietet als Standardoption Microsoft SQL Express 2016, Sie können jedoch eine andere unterstützte Version von SQL Server wählen.
- Für die Verwendung von Dell Wyse PCoIP (ThreadX 4.x)-Geräten muss während der Installation die Verwendung von FTP-Diensten aktiviert werden.
- Für die Verwendung von Dell Wyse PCoIP (ThreadX 5.x)-Geräten muss während der Installation die Verwendung von CIFs aktiviert werden.

ANMERKUNG:

Wenn Sie beabsichtigen, PCoIP (Thread X) zu verwenden, erstellen und konfigurieren Sie einen DNS Service Location (SRV)-Datensatz. Weitere Informationen finden Sie unter Konfigurieren des Lastenausgleichs für ThreadX 4.x-Geräte und Konfigurieren des Lastenausgleichs für ThreadX 5.x-Geräte.

3

Installieren des Wyse-Geräte-Managers

WDM besteht aus den folgenden Komponenten:

- Datenbank
- Verwaltungsserver
- Software Repository
- Andere Dienste
- Weboberfläche

Sie können alle Komponenten auf dem gleichen System installieren, oder ein verteiltes Setup durchführen, wobei die jeweiligen Komponenten auf unterschiedlichen Systemen installiert werden.

WDM ist in den folgenden Editionen verfügbar:

- **Enterprise Edition** – Diese Edition erfordert einen bestimmten Lizenzschlüssel und umfasst sämtliche Funktionen von WDM. Mit dieser Edition können Sie eine sehr große Anzahl von Thin Client-Geräten verwalten. Sie können dieses Edition in einer verteilten Umgebung und jede Komponente auf unterschiedlichen Systemen installieren.
- **Workgroup Edition** – Diese Edition besteht aus einem kostenlosen Lizenzschlüssel und bestimmte Funktionen von WDM sind deaktiviert. Mit dieser Edition können Sie bis zu 10 000 Thin Client-Geräte verwalten. Sie müssen alle Komponenten auf dem gleichen System installieren und können mit dieser Edition kein verteiltes Setup nutzen.

ANMERKUNG: Auch die Workgroup-Lizenz muss aktiviert werden.

ANMERKUNG:

- Um das WDM-Installationsprogramm (Setup.exe) auszuführen, müssen Sie sich im System als Administrator anmelden.
- Sie können WDM nicht auf Servern mit anderen Diensten installieren, wie z. B. DNS, DHCP, AD-Domänendienste oder Dienste, die mit den Funktionen und Ressourcen von WDM in Konflikt geraten.
- Wenn Sie die WDM-Datenbank in einem eigenständigen oder verteilten Setup installieren und eine vorhandene SQL-Datenbank nutzen möchten, vergewissern Sie sich, dass es sich um eine vollständige Version von SQL Server und nicht um SQL Server Express handelt.
- Die Dell Community-Foren unterstützen die WDM Workgroup Edition.
- Die Threadx 5x-Verwaltungskomponente wird nur in der Enterprise Edition unterstützt.

Themen:

Installieren der WDM Workgroup Edition

Schritte

1 Extrahieren Sie die Inhalte des WDM-Installationsprogramms auf dem System, auf dem WDM installiert werden soll.

2 Navigieren Sie zu dem Ordner, in dem Sie das Installationsprogramm extrahiert haben, und führen Sie die Datei **Setup.exe** aus. Der Bildschirm **Welcome** (Willkommen) wird angezeigt.

Abbildung 1. Bildschirm „Welcome“ (Willkommen)

3 Klicken Sie auf **NEXT** (WEITER).

4 Unter „License Type“ (Lizenztyp) wählen Sie **WORKGROUP** und klicken auf **NEXT** (WEITER).

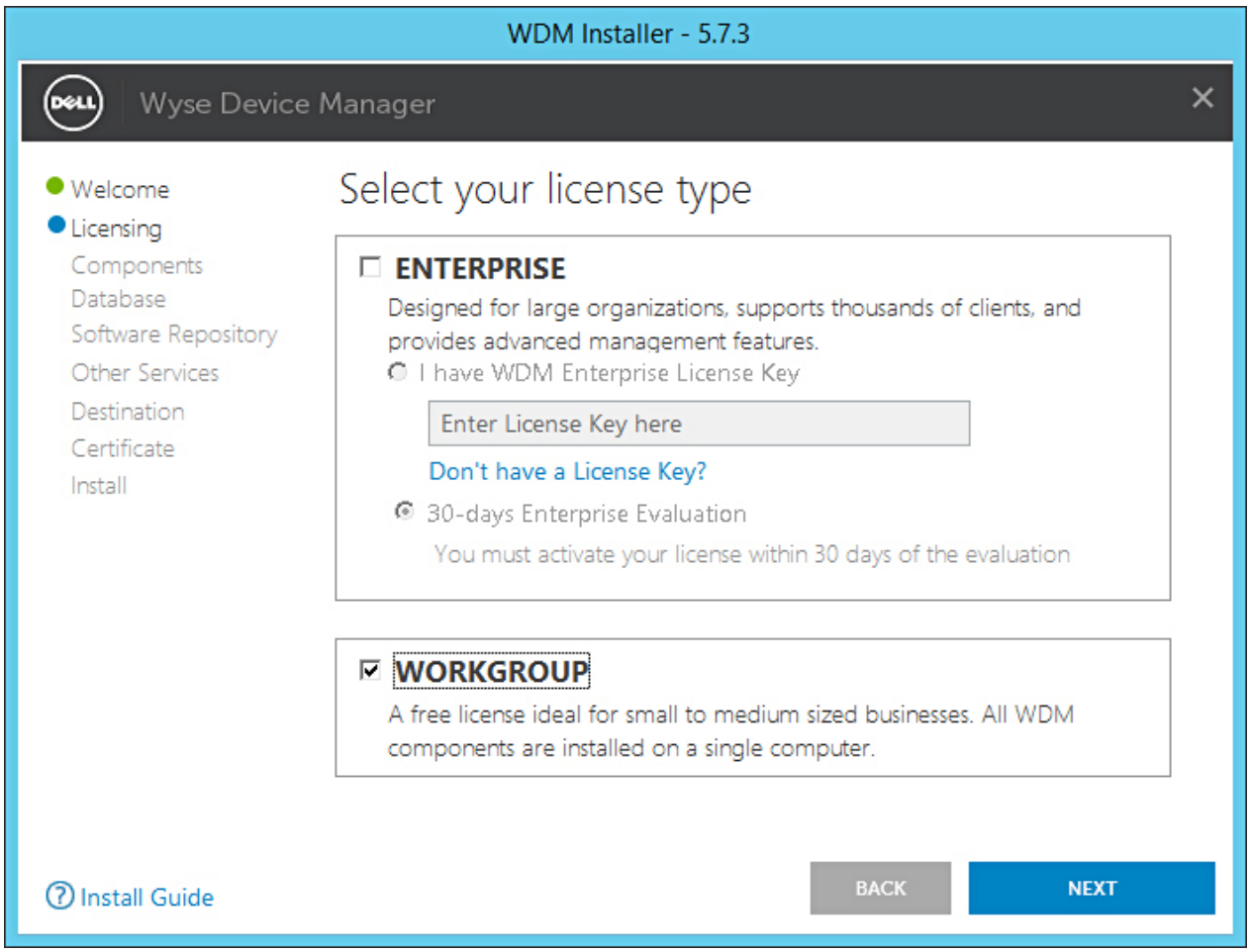


Abbildung 2. Workgroup-Lizenztyp

ANMERKUNG: Für die Workgroup Edition wird der Lizenzschlüssel innerhalb des Installationsprogramms bereitgestellt und Sie brauchen keine Details einzugeben.

Der Bildschirm **Components** (Komponenten) wird angezeigt.

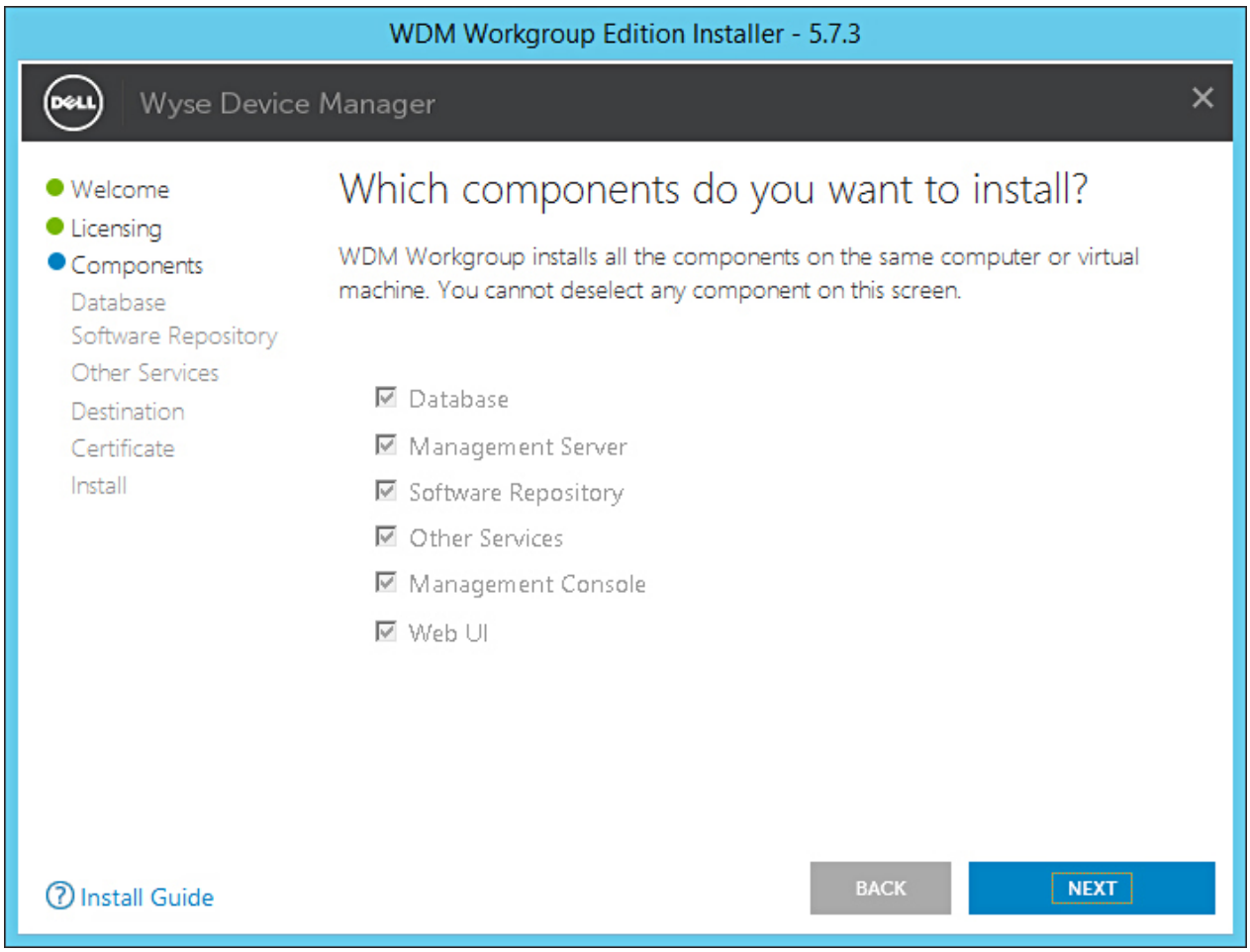


Abbildung 3. Bildschirm „Components“ (Komponenten)

5 Klicken Sie auf **NEXT** (WEITER).

ANMERKUNG: Alle Komponenten sind standardmäßig ausgewählt und es können keine Komponenten abgewählt werden.

Der Bildschirm **Configure Database** (Datenbank konfigurieren) wird angezeigt.

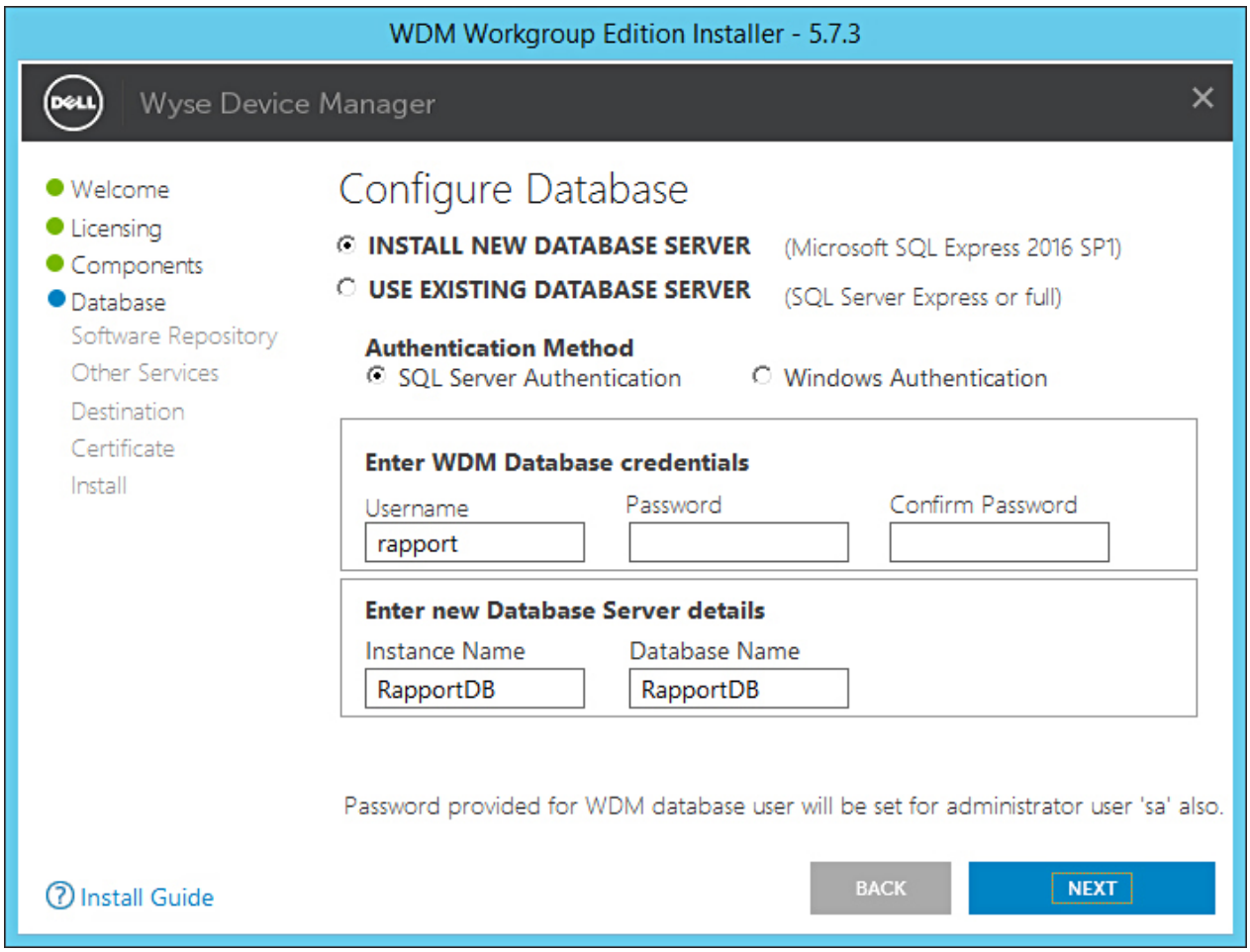


Abbildung 4. Bildschirm „Configure Database“ (Datenbank konfigurieren)

6 Wählen Sie im Bildschirm **Configure Database** (Datenbank konfigurieren) eine der folgenden Optionen aus:

- **Install New Database Server (Microsoft SQL Express 20016 SP1)** (Neuen Datenbankserver installieren (Microsoft SQL Express 20016 SP1)) – Wählen Sie diese Option aus, wenn keine unterstützte Version von Microsoft SQL Server auf dem System installiert ist, und fahren Sie mit Schritt 8 fort.
- **Use Existing Database Server (SQL Server Express or full)** (Vorhandenen Datenbankserver verwenden (SQL Server Express oder vollständig)) – Wählen Sie diese Option aus, wenn Sie bereits eine unterstützte Version von Microsoft SQL Server auf dem System installiert haben. Wenn Sie diese Option auswählen, stellen Sie sicher, dass sich der vorhandene Datenbankserver auf demselben System befindet, auf dem Sie die WDM-Workgroup Edition installieren, und fahren Sie mit Schritt 9 fort.

7 Wenn Sie die erste Option in Schritt 7 ausgewählt haben, wählen Sie die Authentifizierungsmethode aus.

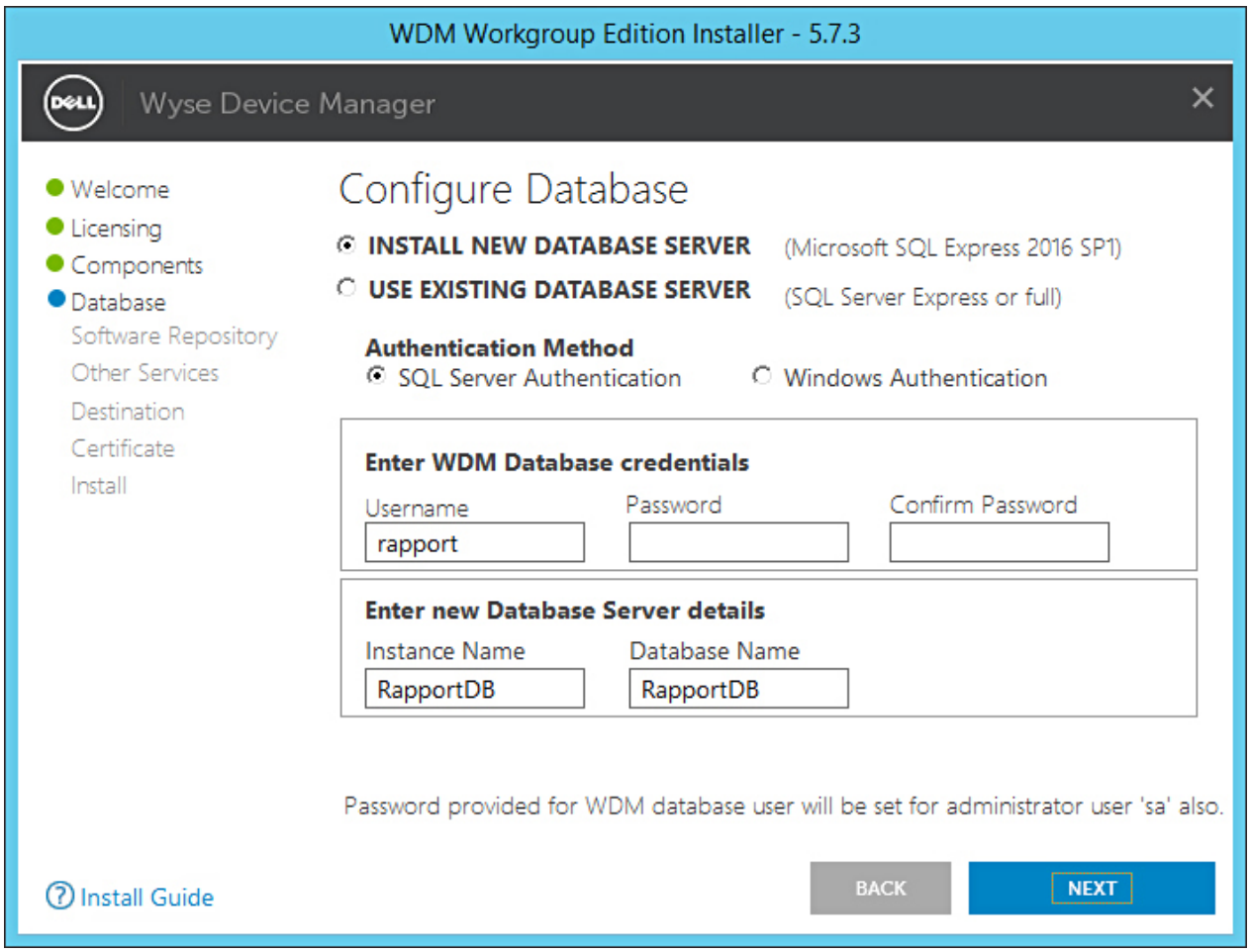


Abbildung 5. Option „Install New Database Server“ (Neue Datenbankserver installieren)

- **SQL Server Authentication** (SQL Serverauthentifizierung) – Diese Option ist standardmäßig ausgewählt. Gehen Sie folgendermaßen vor, um die SQL-Serverauthentifizierung zu konfigurieren:
  1. Geben Sie die WDM-Datenbank-Anmeldeinformationen ein.
  2. Geben Sie die neuen Datenbank-Anmeldeinformationen ein. Sie können den Instanznamen und den Datenbanknamen unter den neuen Datenbankserverdetails eingeben. Der Standard-Instanzname und -Datenbankname wird als RapportDB angezeigt.
- **Windows Authentication** (Windows-Authentifizierung) – Geben Sie die neuen Datenbankserverdetails ein. Der Standard-Instanzname und -Datenbankname wird als RapportDB angezeigt.

ANMERKUNG:

- Wählen Sie **Windows Authentication** (Windows-Authentifizierung) aus, wenn Sie die WDM-Datenbank über Ihre Windows-Anmeldeinformationen verbinden möchten.
- Das Kennwort muss den Komplexitätsanforderungen für Kennwörter des Windows-Betriebssystems entsprechen.

8 Wenn Sie die zweite Option in Schritt 7 ausgewählt haben, wählen Sie die Authentifizierungsmethode aus.

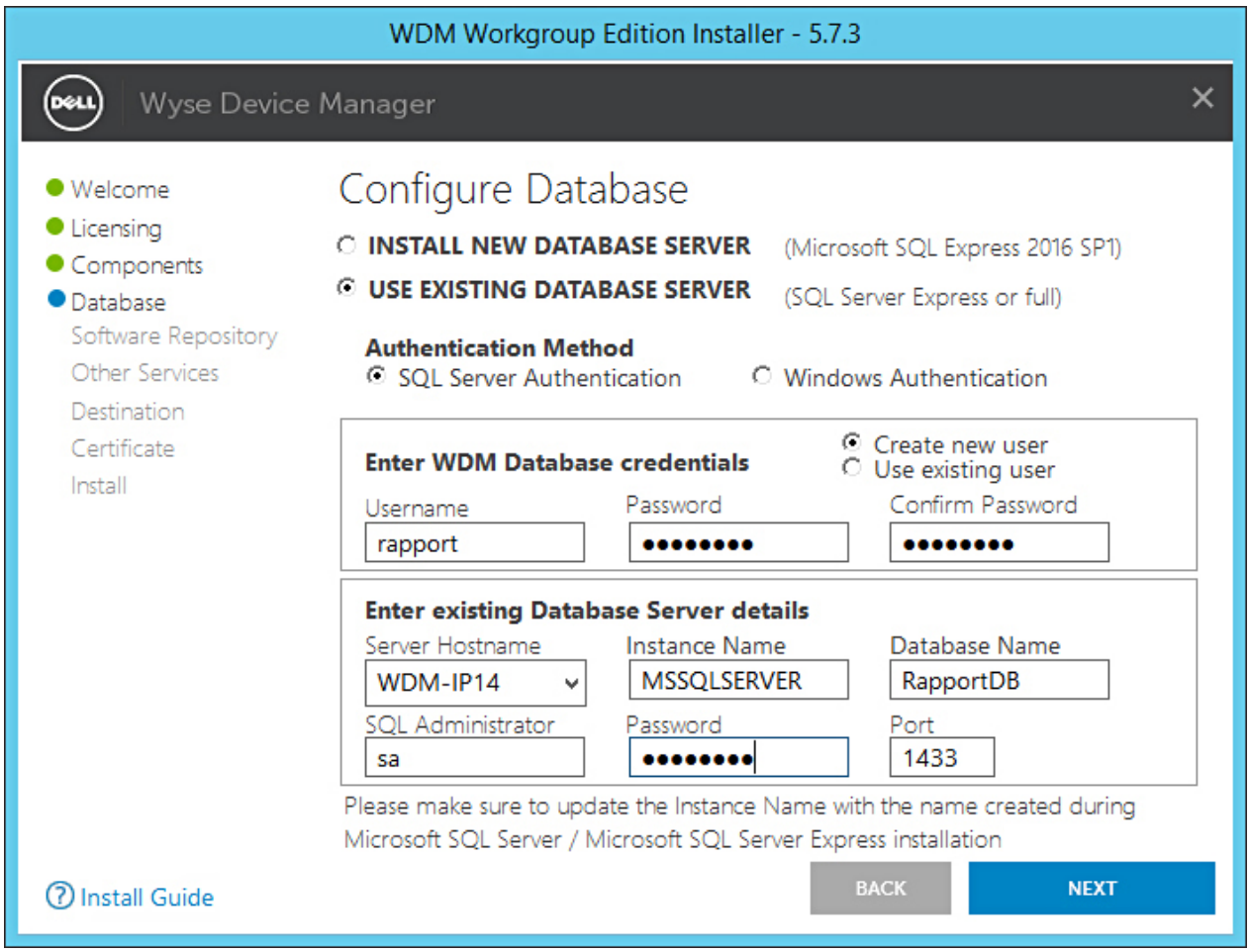


Abbildung 6. Option „Use Existing Database Server“ (Vorhandenen Datenbankserver verwenden)

- **SQL Server Authentication** (SQL Serverauthentifizierung) – Diese Option ist standardmäßig ausgewählt. Gehen Sie folgendermaßen vor, um die SQL-Serverauthentifizierung zu konfigurieren:
  1. Wählen Sie entweder die Option „Create new user“ (Neuen Benutzer erstellen) oder die Option „Use the existing user“ (Vorhandenen Benutzer verwenden) aus und geben Sie dann die WDM-Datenbank-Anmeldeinformationen ein.
  2. Geben Sie die vorhandenen Datenbankserverdetails, wie z. B. Server-Hostnamen, Instanznamen, Datenbanknamen, Portnummer sowie Namen und Kennwort des SQL-Administrators ein. Die Standardportnummer ist 1433.
- **Windows Authentication** (Windows-Authentifizierung) – Geben Sie die vorhandenen Datenbankserverdetails, wie z. B. Server-Hostnamen, Instanznamen, Datenbanknamen, Portnummer sowie Namen und Kennwort des SQL-Administrators ein.

9. Klicken Sie auf **NEXT** (WEITER).

   Der Bildschirm **Configure Software Repository Server** (Software Repository-Server konfigurieren) wird angezeigt.

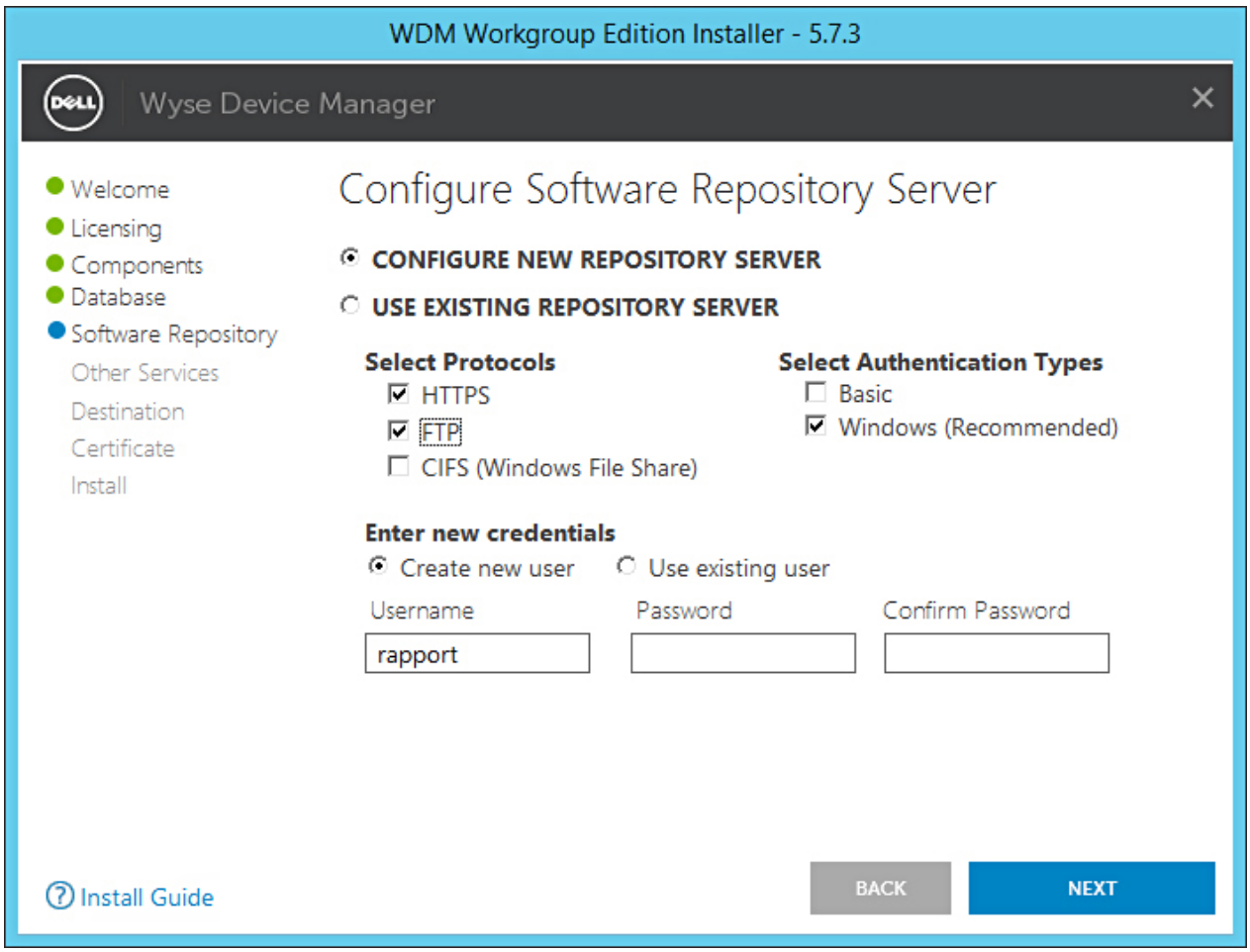


Abbildung 7. Bildschirm „Configure Software Repository Server“ (Software Repository-Server konfigurieren)

10 Auf dem Bildschirm **Configure Software Repository Server** (Software Repository-Server konfigurieren) können Sie eine der folgenden Optionen auswählen:

- **CONFIGURE NEW REPOSITORY SERVER** (NEUEN REPOSITORY-SERVER KONFIGURIEREN) – Wählen Sie diese Option, wenn das Installationsprogramm einen neuen Repository-Server konfigurieren soll. So konfigurieren Sie einen neuen Repository-Server:
  - Wählen Sie das Protokoll und Einstellungen zum Verteilen der Software auf die verwalteten Geräte aus. **HTTPS** ist standardmäßig ausgewählt. Sie können auch die Option **FTP** für ThreadX 4.x und **CIFS** für ThreadX 5.x auswählen.
  - Wählen Sie den Authentifizierungstyp aus. **Windows** ist standardmäßig ausgewählt.

    ANMERKUNG: Für Linux ist die Standardauthentifizierung erforderlich.
  - Erstellen Sie neue Benutzer-Anmeldeinformationen oder verwenden Sie die Anmeldeinformationen eines vorhandenen Benutzers.
- **USE EXISTING REPOSITORY SERVER** (VORHANDENEN REPOSITORY-SERVER VERWENDEN) – Wählen Sie diese Option aus, wenn das Installationsprogramm einen vorhandenen Repository-Server verwenden soll. So konfigurieren Sie den vorhandenen Repository-Server:
  - Wählen Sie das Protokoll und die Einstellungen zum Verteilung der Software auf die verwalteten Geräte aus. **HTTPS** ist standardmäßig ausgewählt. Sie können auch die Option **FTP** für ThreadX 4.x und **CIFS** für ThreadX 5.x auswählen.
  - Wählen Sie den Authentifizierungstyp aus. **Windows** ist standardmäßig ausgewählt.
  - Geben Sie die Serveranmeldeinformationen ein. Die Server-IP-Adresse ist grau unterlegt und der Standardbenutzername lautet „rapport“.

11 Klicken Sie auf **NEXT** (WEITER).

12 Wählen Sie die Services aus, die Sie installieren möchten, und klicken Sie auf **NEXT** (WEITER).

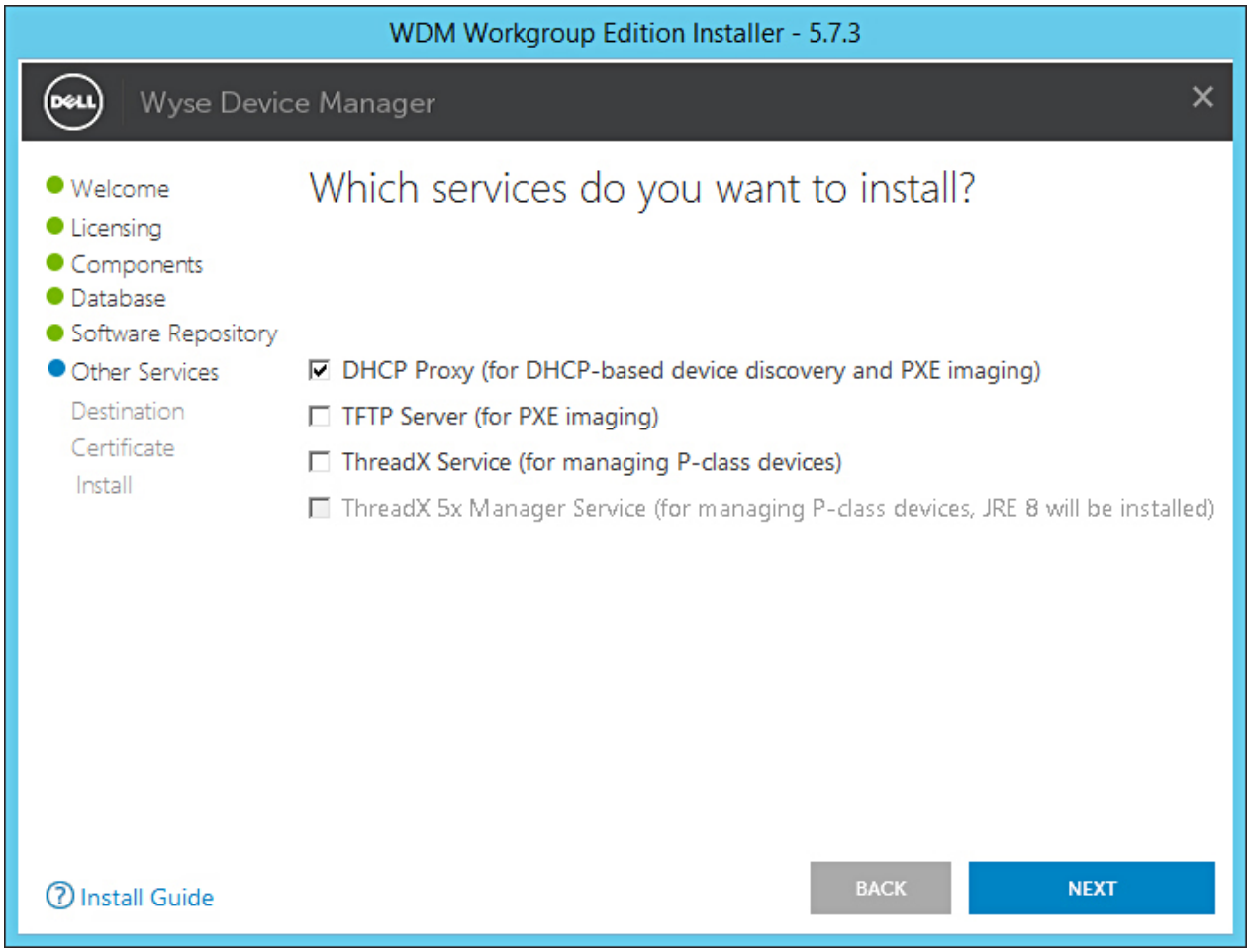


Abbildung 8. Bildschirm „Other Services“ (Andere Dienste)

ANMERKUNG: DHCP Proxy ist standardmäßig ausgewählt.

13 Geben Sie den Installationspfad ein und klicken Sie auf **NEXT** (WEITER).

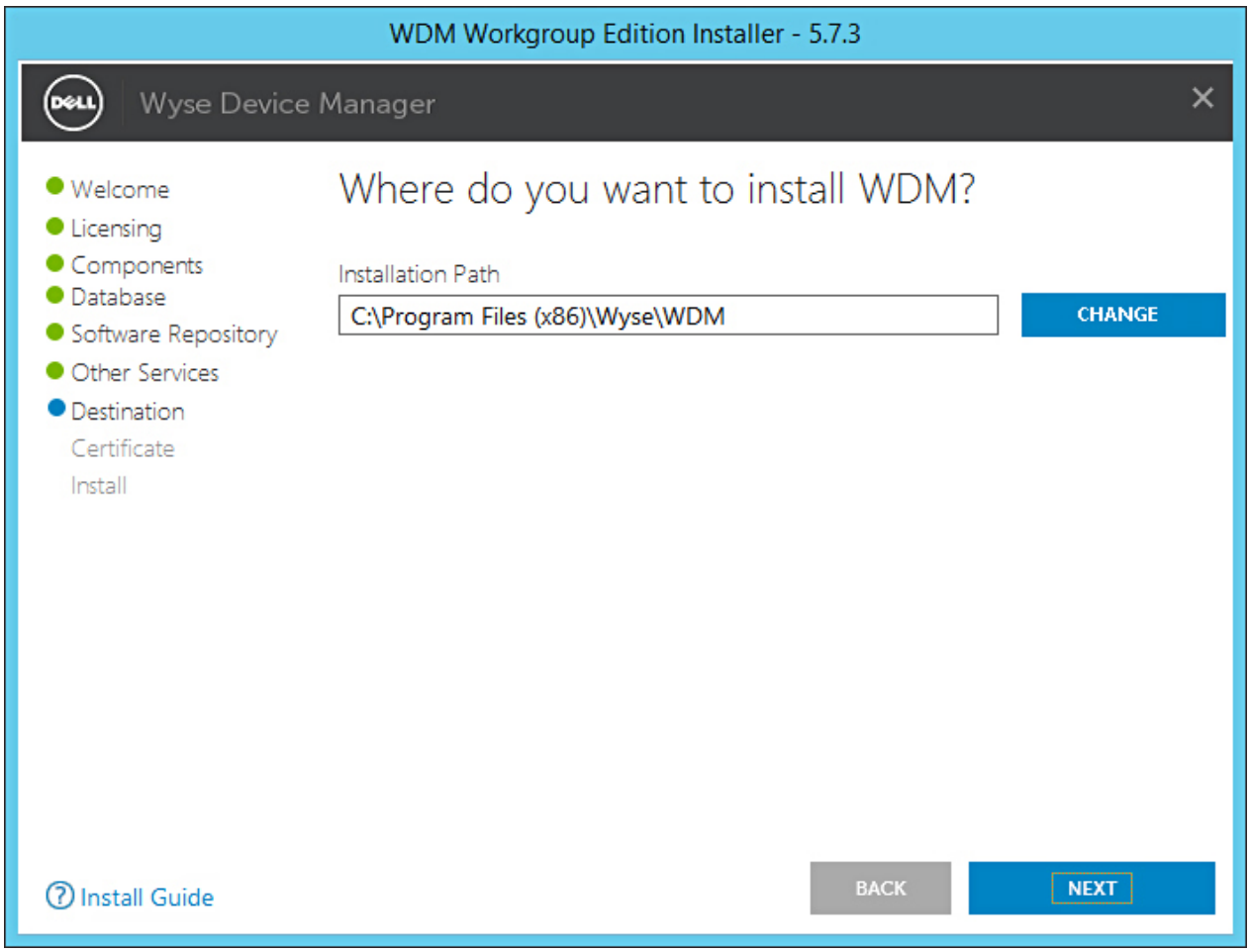


Abbildung 9. Bildschirm „Destination“ (Zielordner)

14 Wählen Sie das Zertifikat aus und importieren Sie es, um die Installation zu starten.

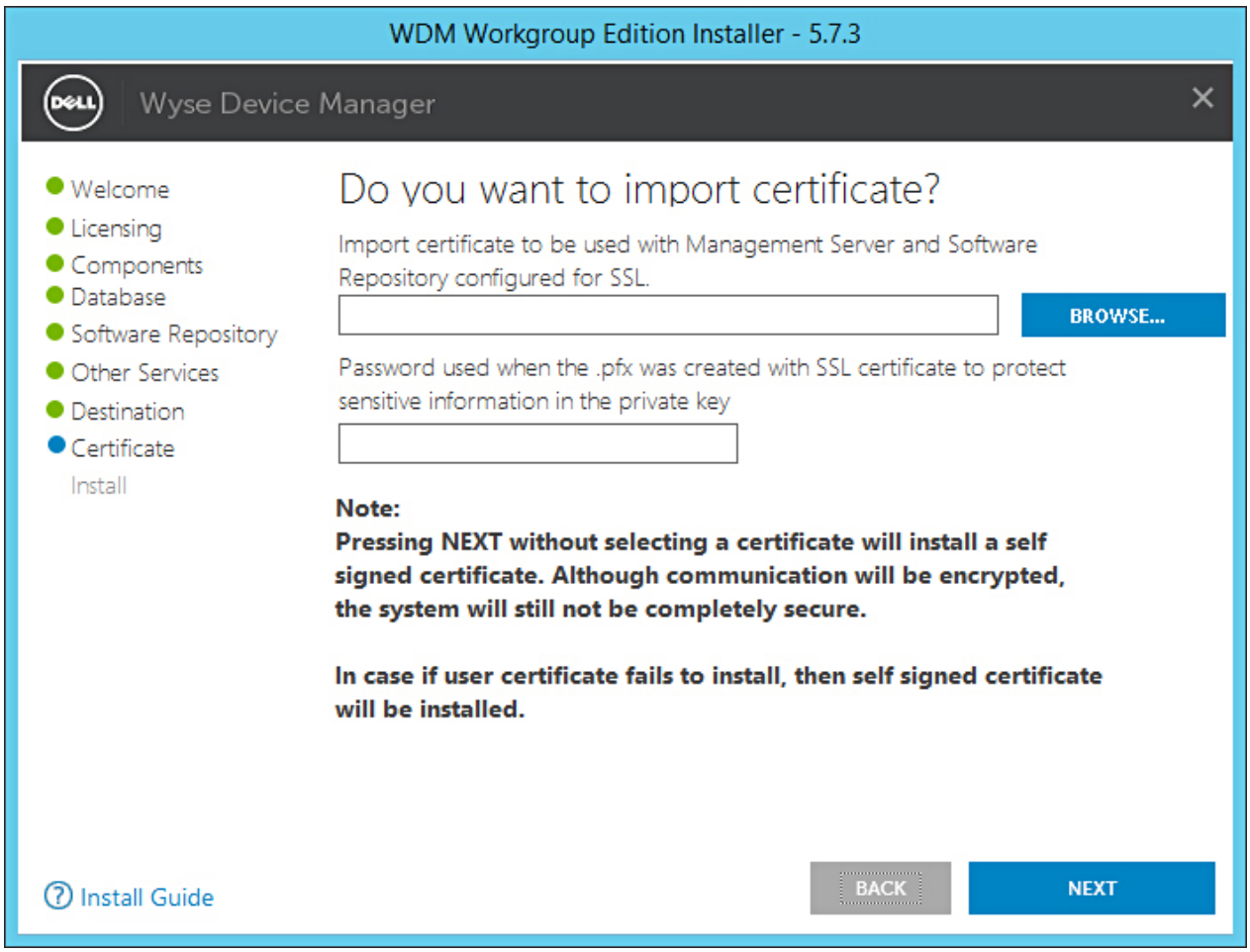


Abbildung 10. Bildschirm „Certificate“ (Zertifikat)

ANMERKUNG: Wenn Sie auf „NEXT“ (WEITER) klicken, ohne ein Zertifikat auszuwählen, installiert das Installationsprogramm ein selbstsigniertes Zertifikat. Die Kommunikation wird verschlüsselt, aber das System ist nicht ganz sicher. Das Zertifikat muss in Form einer .pfx-Datei vorliegen.

Der Fortschritt der Installation wird auf dem Bildschirm angezeigt. Nachdem die Installation abgeschlossen ist, werden Sie dazu aufgefordert, das System neu zu starten.

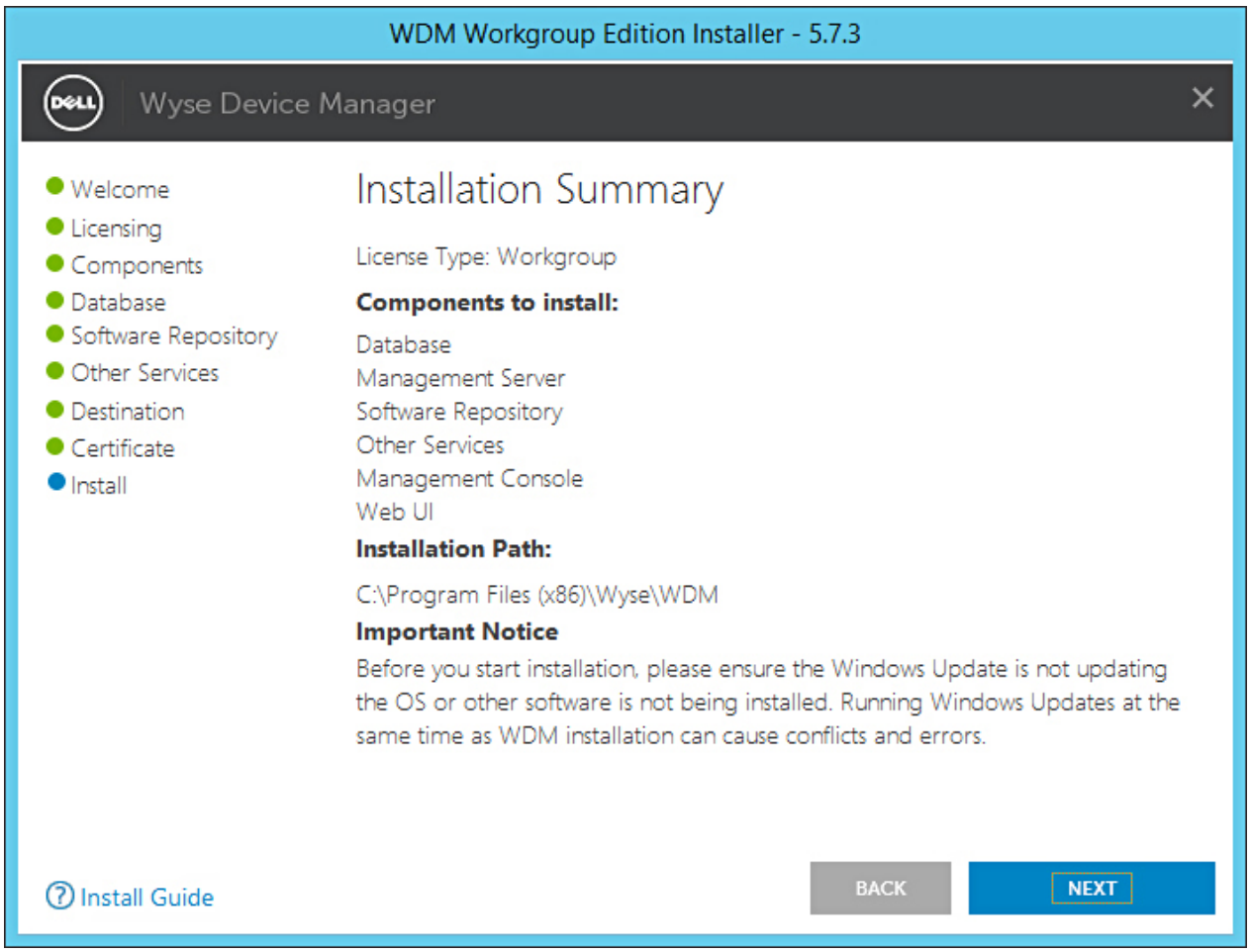


Abbildung 11. Bildschirm „Installation summary“ (Installationszusammenfassung)

15 Starten Sie das System neu, um die Änderungen in Kraft zu setzen.

Nächster Schritt

Nach der Installation stellen Sie sicher, dass die folgenden Kriterien erfüllt sind:

- WDM ist in **<drive C>\Inetpub\ftproot path** installiert und der Ordner „rapport“ wurde erstellt.
- Das Symbol der WyseDeviceManager 5.7.3 Web-UI wird auf dem Desktop erstellt.
- In IIS wird die HApi-Anwendung unter dem Ordner „Rapport HTTP Server“ erstellt.
- In IIS wird die MyWDM-Anwendung unter dem Ordner „Rapport HTTP Server“ erstellt.
- In IIS wird die WebUI-Anwendung unter dem Ordner „Rapport HTTP Server“ erstellt.

ANMERKUNG: Nach der Installation stellen Sie sicher, dass die Datenbank mit der bereitgestellten Instanz und dem Datenbanknamen erstellt wurde.

Installieren der WDM Enterprise Edition

1 Extrahieren Sie die Inhalte des WDM-Installationsprogramms auf dem System, auf dem WDM installiert werden soll.

2 Navigieren Sie zu dem Ordner, in dem Sie das Installationsprogramm extrahiert haben, und führen Sie die Datei **Setup.exe** aus.
Wenn der Server nicht über .Net Framework verfügt, dann wird .Net Framework automatisch installiert.

Der Bildschirm **Welcome** (Willkommen) wird angezeigt.

Abbildung 12. Bildschirm „Welcome“ (Willkommen)

3 Klicken Sie auf **NEXT** (WEITER).

4 Unter „License Type“ (Lizenztyp) wählen Sie **ENTERPRISE** aus.

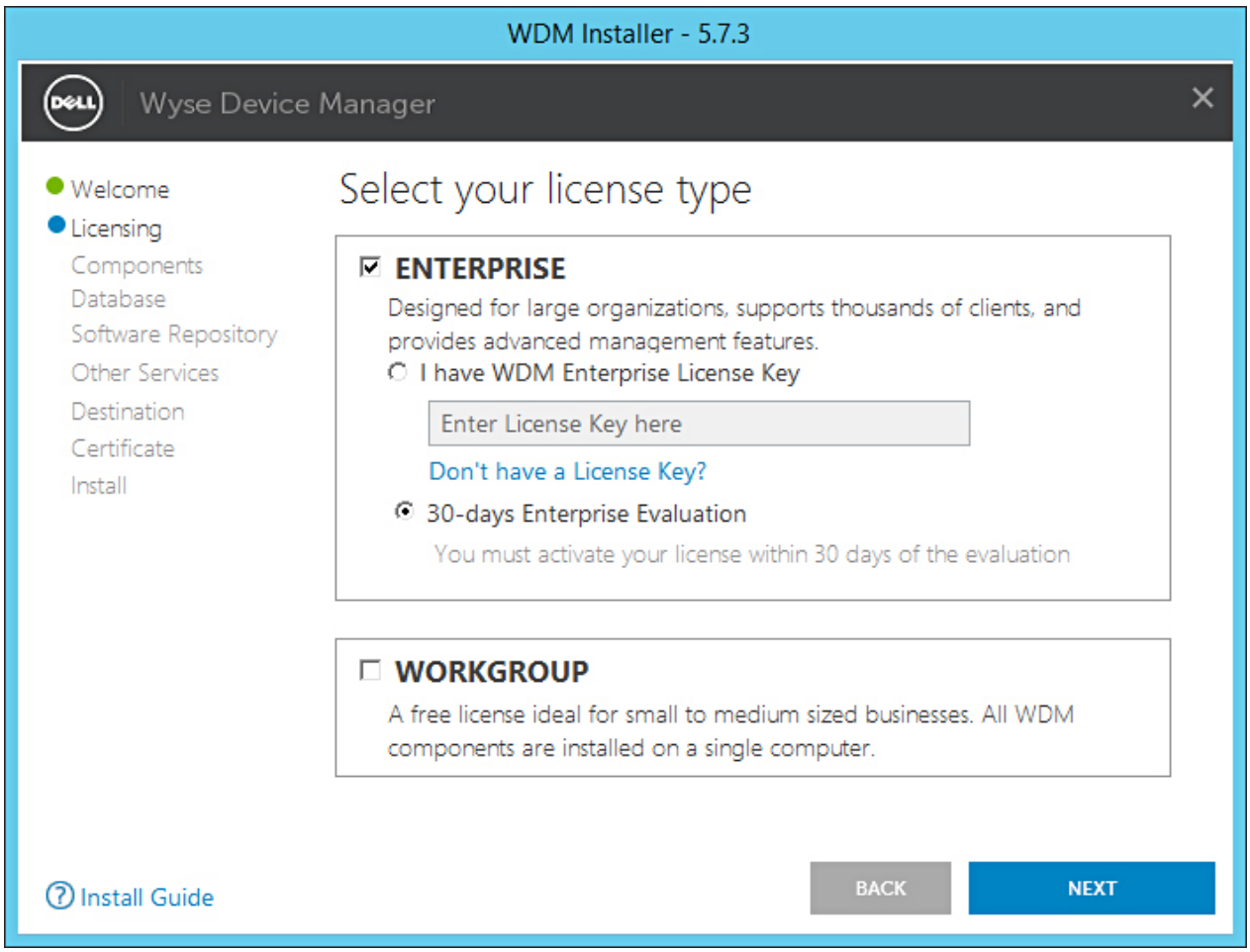


Abbildung 13. Enterprise-Lizenztyp

a Wenn Sie den WDM-Lizenzschlüssel haben, wählen Sie die Option **I have WDM Enterprise License Key** (Ich habe den WDM Enterprise-Lizenzschlüssel) aus und geben Sie den Lizenzschlüssel in das dafür vorgesehene Feld ein.

b Wenn Sie keinen Lizenzschlüssel besitzen, wählen Sie die Option **30–days Enterprise Evaluation** (30-tägige Enterprise Evaluation-Lizenz) aus.

Der Lizenzschlüssel wird standardmäßig eingegeben. Nach dem 30tägigen Testzeitraum müssen Sie jedoch den Lizenzschlüssel erwerben und ihn WDM hinzufügen. Weitere Informationen zum Hinzufügen des Lizenzschlüssels finden Sie im Dell Wyse Device Manager Administrator's Guide (*Administratorhandbuch für den Dell Wyse Configuration Manager*).

5 Klicken Sie auf **NEXT** (WEITER).

6 Wählen Sie die Komponenten aus, die Sie installieren möchten, und klicken Sie auf **NEXT** (WEITER).

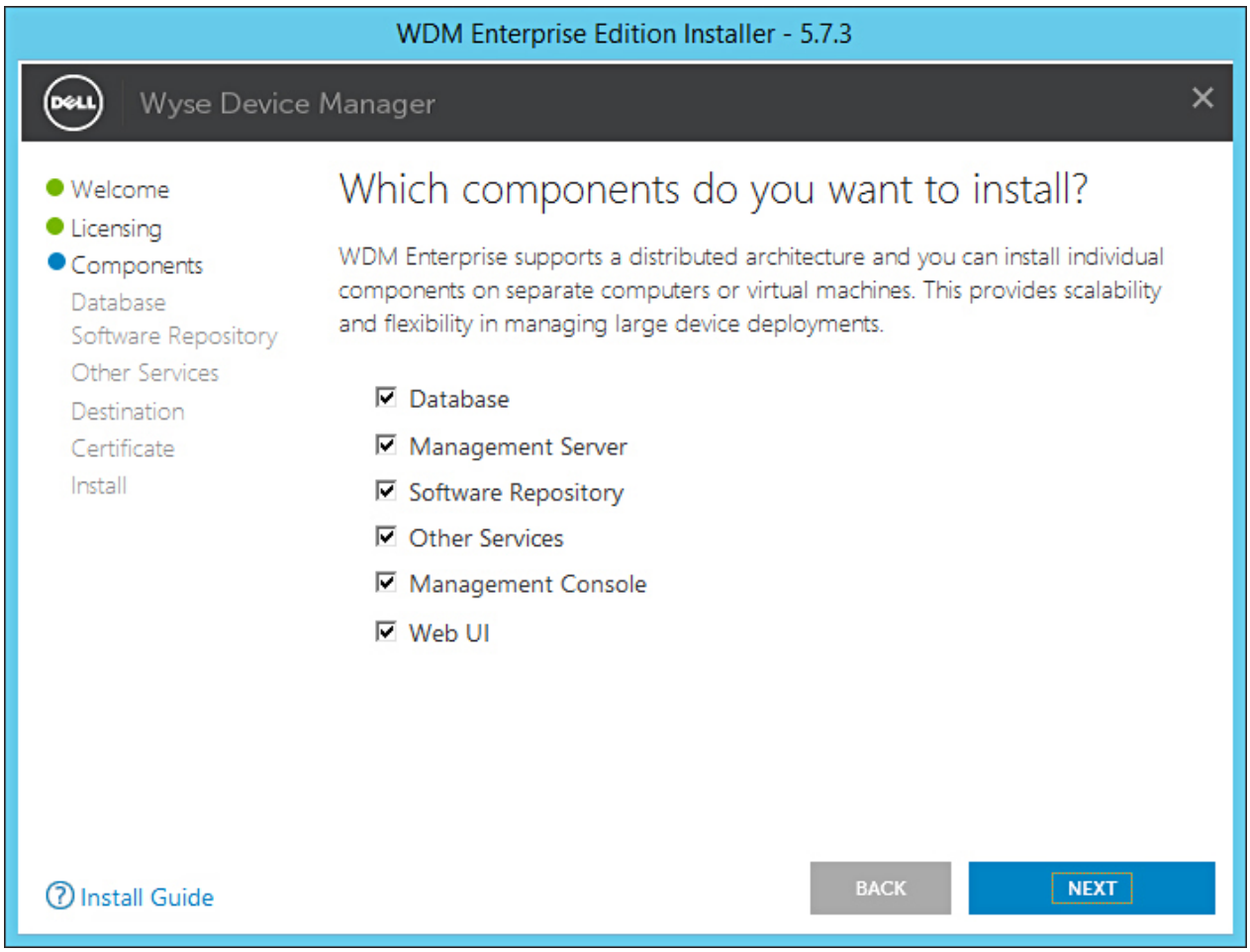


Abbildung 14. Bildschirm „“ (Komponenten)

Sie können alle Komponenten auf dem gleichen System oder jede Komponente auf einem anderen System installieren.

ANMERKUNG: Achten Sie beim separaten Installieren der Komponenten auf unterschiedlichen Systemen darauf, die Datenbank zuerst zu installieren. Wenn Sie die Datenbank nicht installieren, können Sie die verbleibenden Komponenten nicht installieren.

7 Wählen Sie im Bildschirm **Configure Database** (Datenbank konfigurieren) eine der folgenden Optionen aus:

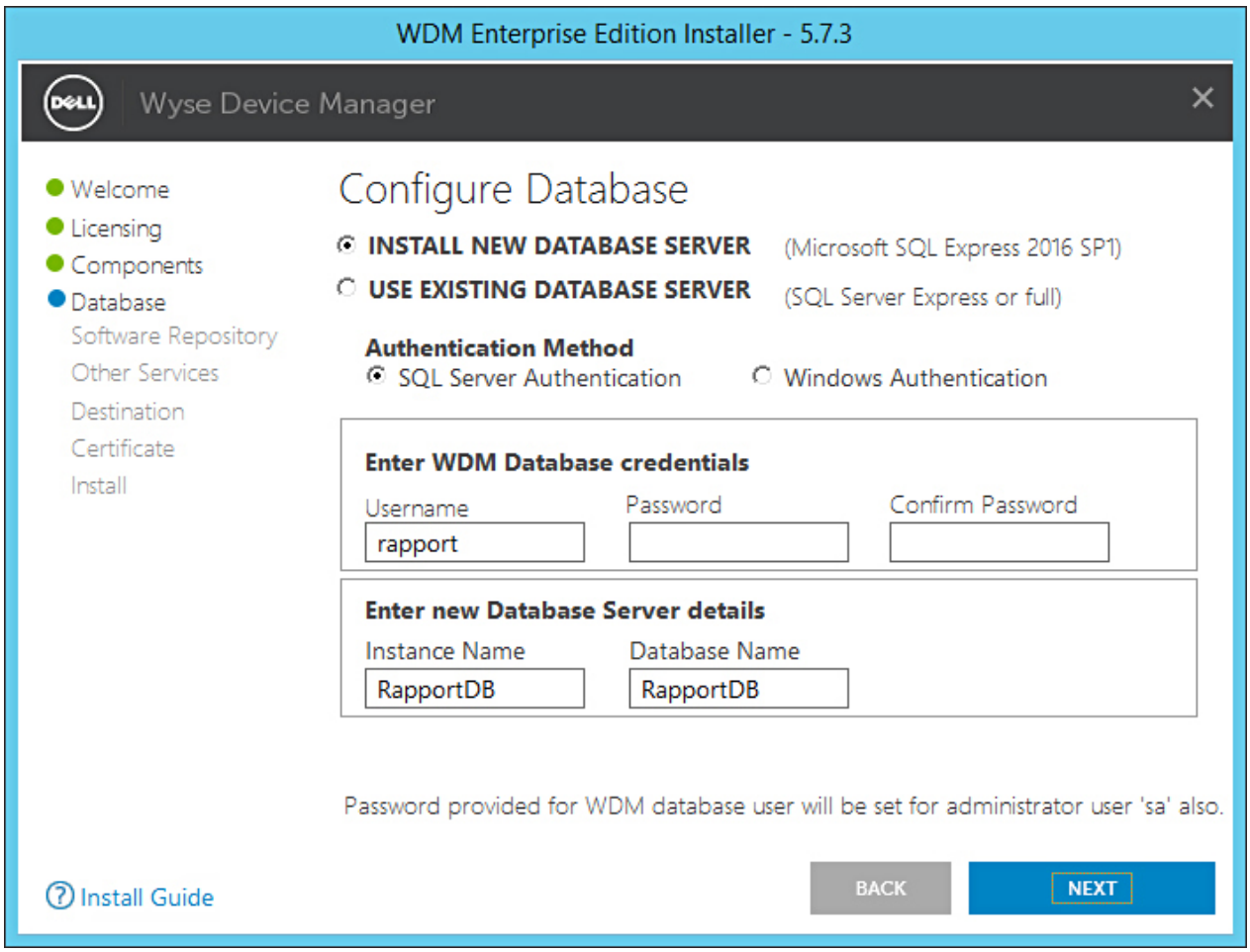


Abbildung 15. Bildschirm „Configure Database“ (Datenbank konfigurieren)

- **Install New Database Server (Microsoft SQL Express 20016 SP1)** (Neuen Datenbankserver installieren (Microsoft SQL Express 20016 SP1)) – Wählen Sie diese Option aus, wenn keine unterstützte Version von Microsoft SQL Server auf dem System installiert ist, und fahren Sie mit Schritt 8 fort.
- **Use Existing Database Server (SQL Server Express or full)** (Vorhandenen Datenbankserver verwenden (SQL Server Express oder vollständig)) – Wählen Sie diese Option aus, wenn Sie bereits eine unterstützte Version von Microsoft SQL Server auf dem System installiert haben. Wenn Sie diese Option auswählen, stellen Sie sicher, dass sich der vorhandene Datenbankserver auf demselben System befindet, auf dem Sie die WDM-Workgroup Edition installieren, und fahren Sie mit Schritt 9 fort.

8 Wenn Sie die erste Option in Schritt 7 ausgewählt haben, wählen Sie die Authentifizierungsmethode aus.

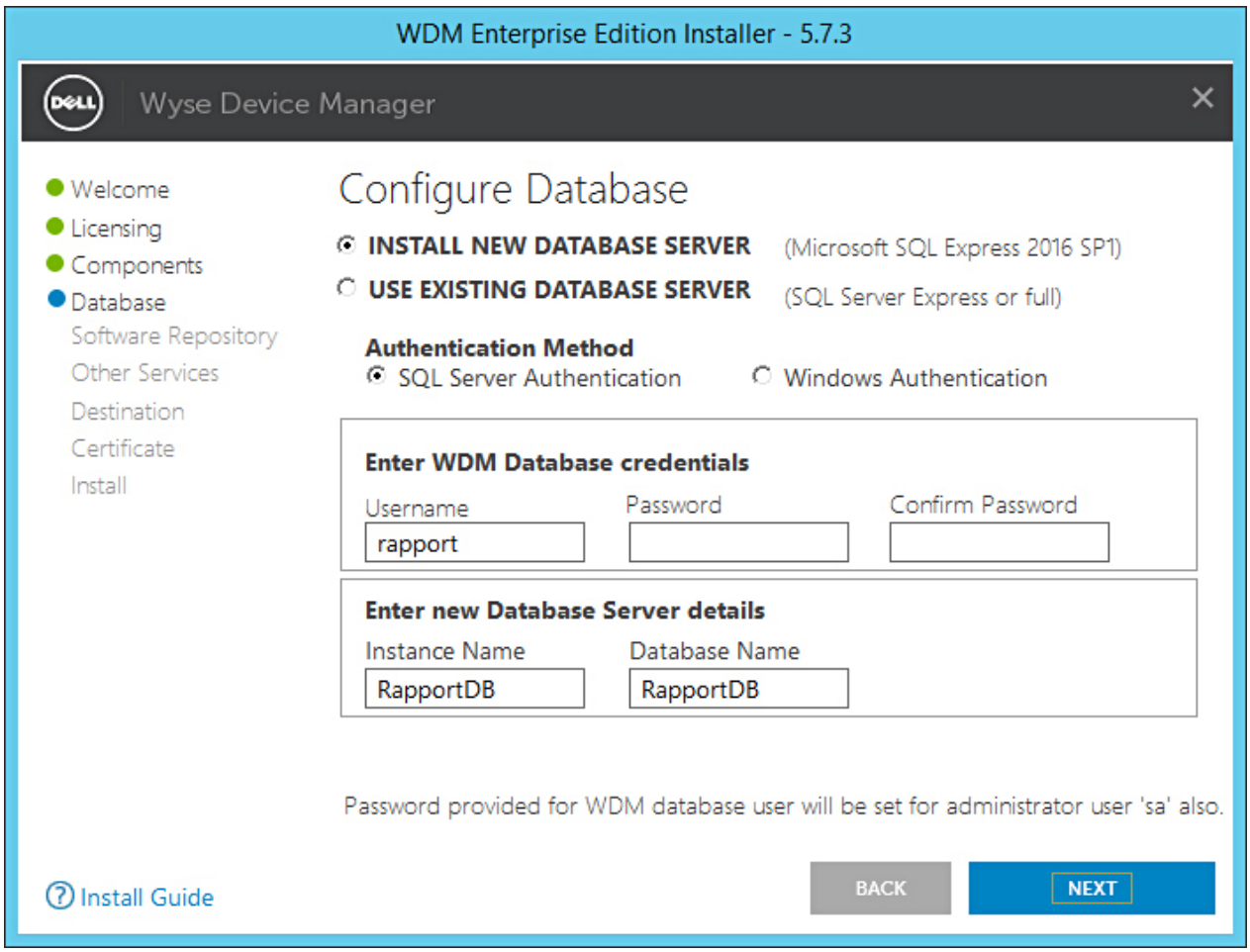


Abbildung 16. Option „Install New Database Server“ (Neue Datenbankserver installieren)

- **SQL Server Authentication** (SQL Serverauthentifizierung) – Diese Option ist standardmäßig ausgewählt. Gehen Sie folgendermaßen vor, um die SQL-Serverauthentifizierung zu konfigurieren:
  1. Geben Sie die WDM-Datenbank-Anmeldeinformationen ein.
  2. Geben Sie die neuen Datenbank-Anmeldeinformationen ein. Sie können den Instanznamen und den Datenbanknamen unter den neuen Datenbankserverdetails eingeben. Der Standard-Instanzname und -Datenbankname wird als RapportDB angezeigt.

  ANMERKUNG: Selbst wenn Sie Windows-Authentifizierung wählen, erfordert die WDM-Installation die SQL-Authentifizierung für den Zugriff auf die SQL-Datenbank. In einer eigenständigen Installation übernimmt das WDM-Installationsprogramm nach Abschluss der WDM-Datenbankinstallation das Zuweisen des Active Directory-Benutzers zur Datenbank, und derselbe Benutzer wird für die Installation der WDM-Services verwendet.
- **Windows Authentication** (Windows-Authentifizierung) – Geben Sie die neuen Datenbankserverdetails ein. Der Standard-Instanzname und -Datenbankname wird als RapportDB angezeigt.

  ANMERKUNG:
  - Wählen Sie **Windows Authentication** (Windows-Authentifizierung) aus, wenn Sie die WDM-Datenbank über Ihre Windows-Anmeldeinformationen verbinden möchten.
  - Das Kennwort muss den Komplexitätsanforderungen für Kennwörter des Windows-Betriebssystems entsprechen.

9 Wenn Sie die zweite Option in Schritt 7 ausgewählt haben, wählen Sie die Authentifizierungsmethode aus.

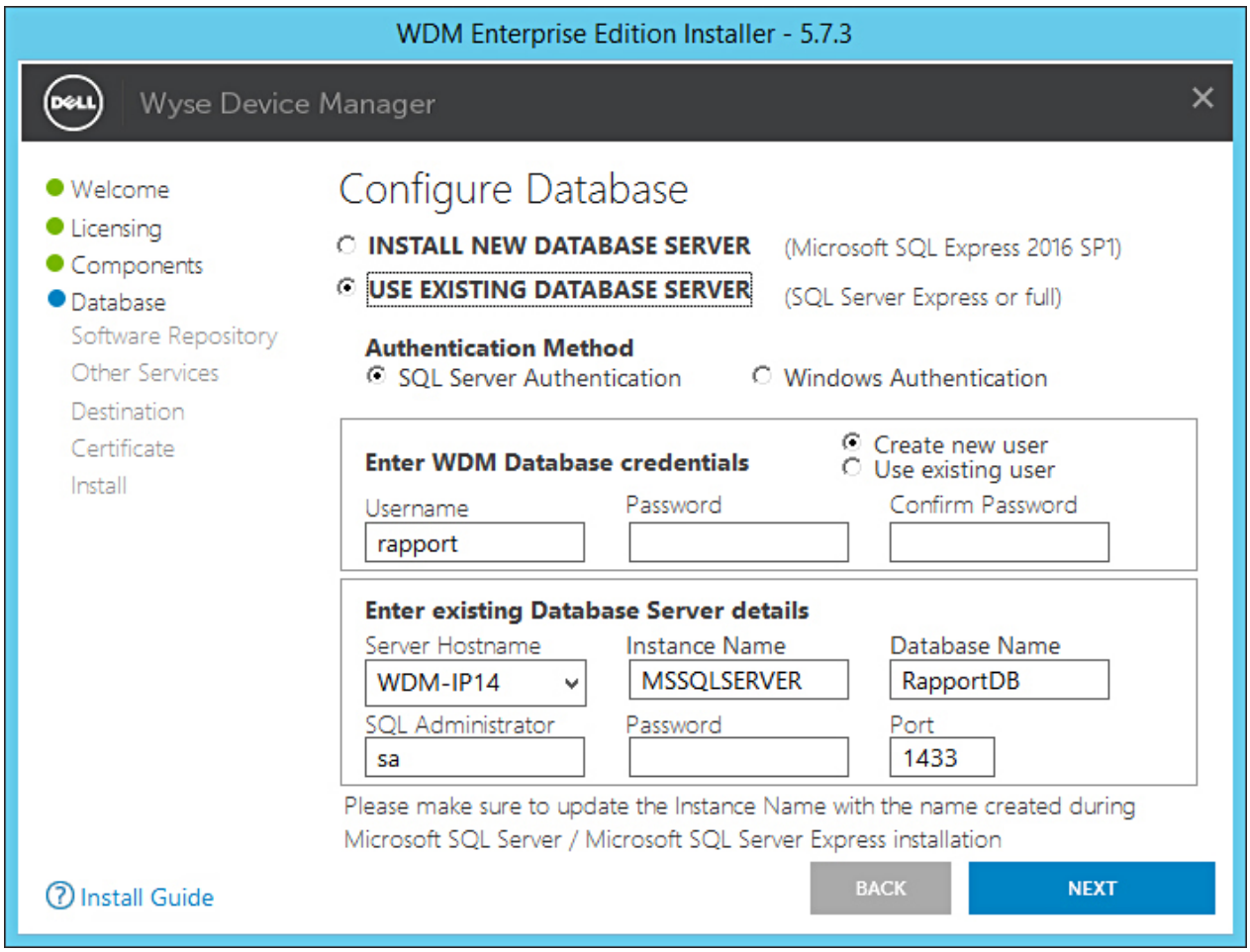


Abbildung 17. Option „Use Existing Database Server“ (Vorhandenen Datenbankserver verwenden)

- **SQL Server Authentication** (SQL Serverauthentifizierung) – Diese Option ist standardmäßig ausgewählt. Gehen Sie folgendermaßen vor, um die SQL-Serverauthentifizierung zu konfigurieren:
  1. Wählen Sie entweder die Option „Create new user“ (Neuen Benutzer erstellen) oder die Option „Use the existing user“ (Vorhandenen Benutzer verwenden) aus und geben Sie dann die WDM-Datenbank-Anmeldeinformationen ein.
  2. Geben Sie die vorhandenen Datenbankserverdetails, wie z. B. Server-Hostnamen, Instanznamen, Datenbanknamen, Portnummer sowie Namen und Kennwort des SQL-Administrators ein.
- **Windows Authentication** (Windows-Authentifizierung) – Geben Sie die vorhandenen Datenbankserverdetails, wie z. B. Server-Hostnamen, Instanznamen, Datenbanknamen, Portnummer sowie Namen und Kennwort des SQL-Administrators ein.

ANMERKUNG: Die Standardportnummer ist 1433. Dell empfiehlt, dass Sie die Portnummer manuell eingeben, da diese dynamisch ist. Der dynamische Portbereich für TCP/UDP liegt zwischen 49152 und 65535.

10 Klicken Sie auf **NEXT** (WEITER).

Der Bildschirm **Configure Software Repository Server** (Software Repository-Server konfigurieren) wird angezeigt.

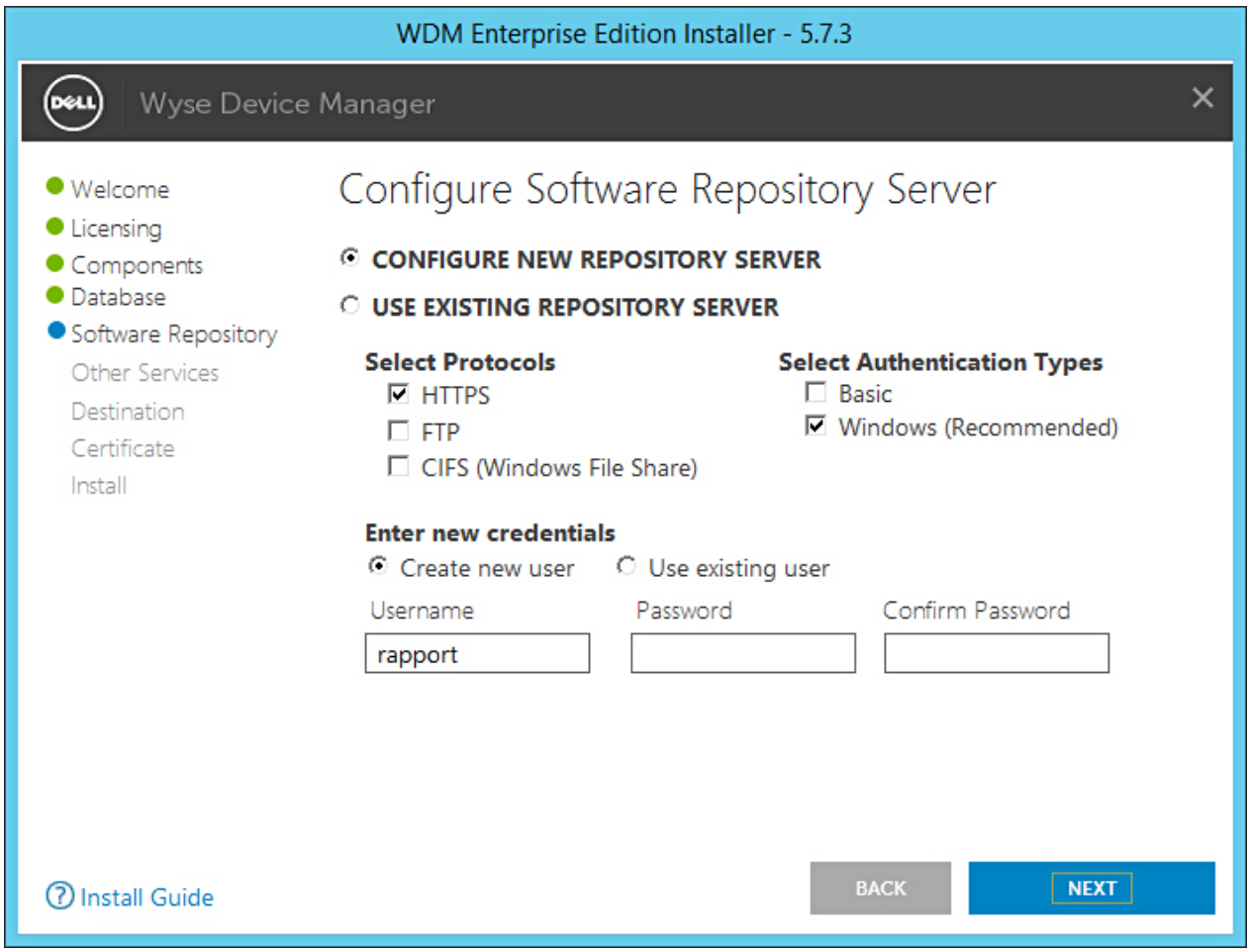


Abbildung 18. Bildschirm „Configure Software Repository Server“ (Software Repository-Server konfigurieren)

11 Auf dem Bildschirm **Configure Software Repository Server** (Software Repository-Server konfigurieren) können Sie eine der folgenden Optionen auswählen:

- **CONFIGURE NEW REPOSITORY SERVER** (NEUEN REPOSITORY-SERVER KONFIGURIEREN) – Wählen Sie diese Option, wenn das Installationsprogramm einen neuen Repository-Server konfigurieren soll. So konfigurieren Sie einen neuen Repository-Server:
  - Wählen Sie das Protokoll und Einstellungen zum Verteilen der Software auf die verwalteten Geräte aus. **HTTPS** ist standardmäßig ausgewählt. Sie können auch die Option **FTP** für ThreadX 4.x und **CIFS** für ThreadX 5.x auswählen.
  - Wählen Sie den Authentifizierungstyp aus. **Windows** ist standardmäßig ausgewählt.

    ANMERKUNG: Für Linux ist die Standardauthentifizierung erforderlich.
  - Erstellen Sie neue Benutzer-Anmeldeinformationen oder verwenden Sie die Anmeldeinformationen eines vorhandenen Benutzers.

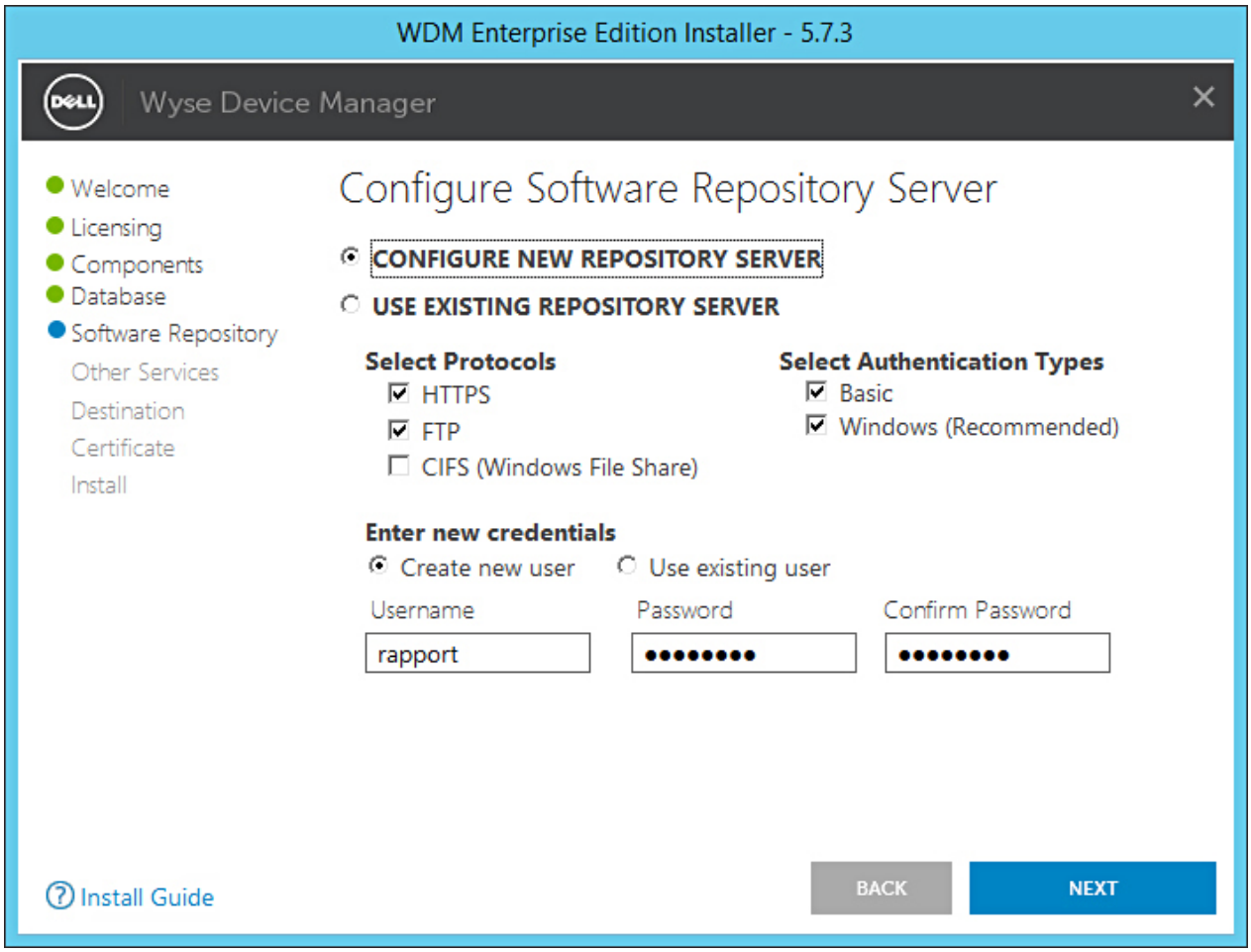


Abbildung 19. Option „CONFIGURE NEW REPOSITORY SERVER“ (NEUEN REPOSITORY-SERVER KONFIGURIEREN)

- **USE EXISTING REPOSITORY SERVER** (VORHANDENEN REPOSITORY-SERVER VERWENDEN) – Wählen Sie diese Option aus, wenn das Installationsprogramm einen vorhandenen Repository-Server verwenden soll. So konfigurieren Sie den vorhandenen Repository-Server:
  - Wählen Sie das Protokoll und die Einstellungen zum Verteilung der Software auf die verwalteten Geräte aus. **HTTPS** ist standardmäßig ausgewählt. Sie können auch die Option **FTP** für ThreadX 4.x und **CIFS** für ThreadX 5.x auswählen.
  - Wählen Sie den Authentifizierungstyp aus. **Windows** ist standardmäßig ausgewählt.
  - Geben Sie die Serveranmeldeinformationen ein. Die Server-IP-Adresse ist grau unterlegt und der Standardbenutzername lautet „rapport“.

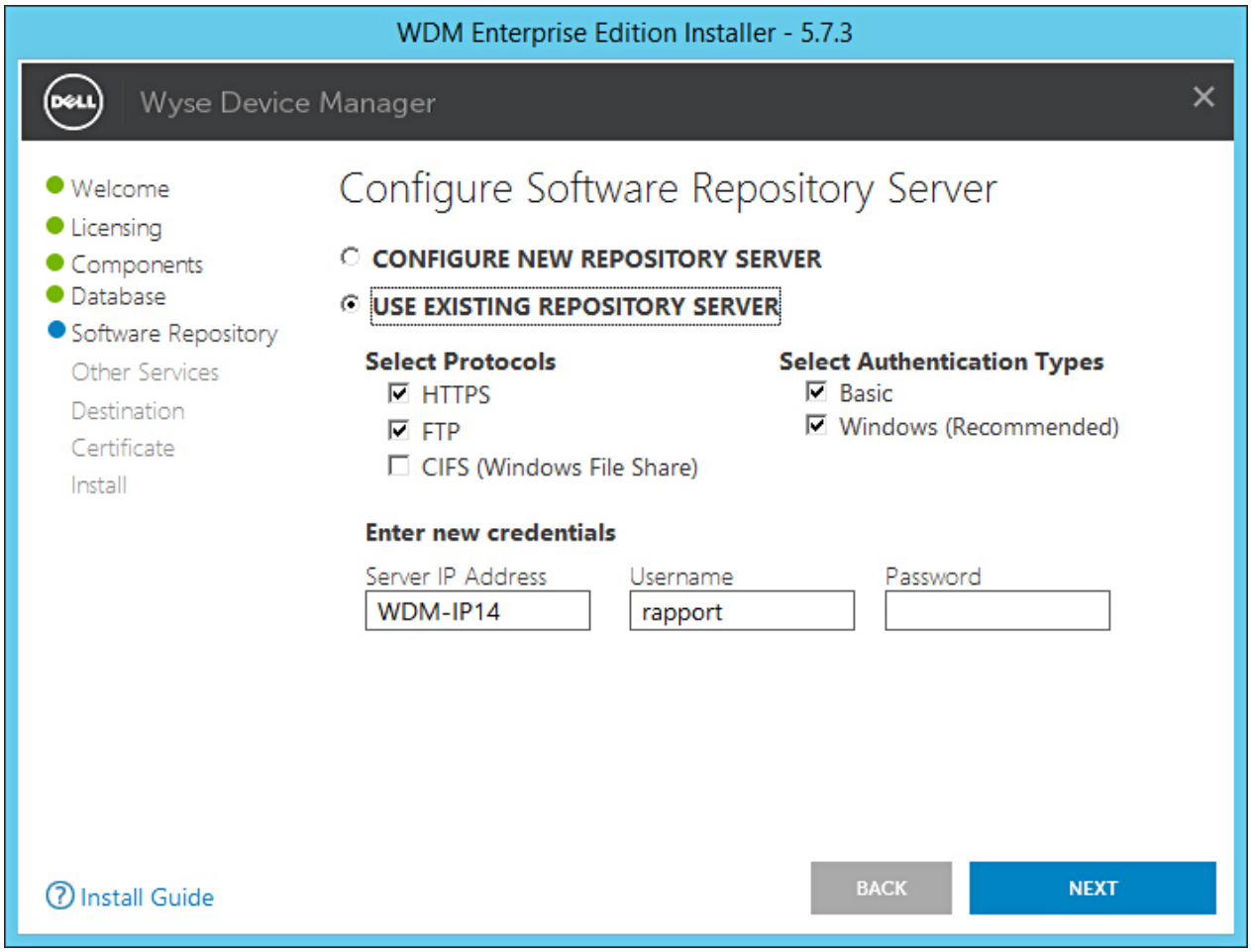


Abbildung 20. Option „USE EXISTING REPOSITORY SERVER“ (VORHANDENEN REPOSITORY-SERVER VERWENDEN)

12 Klicken Sie auf **NEXT** (WEITER).

13 Wählen Sie die Services aus, die Sie installieren möchten, und klicken Sie auf **NEXT** (WEITER).

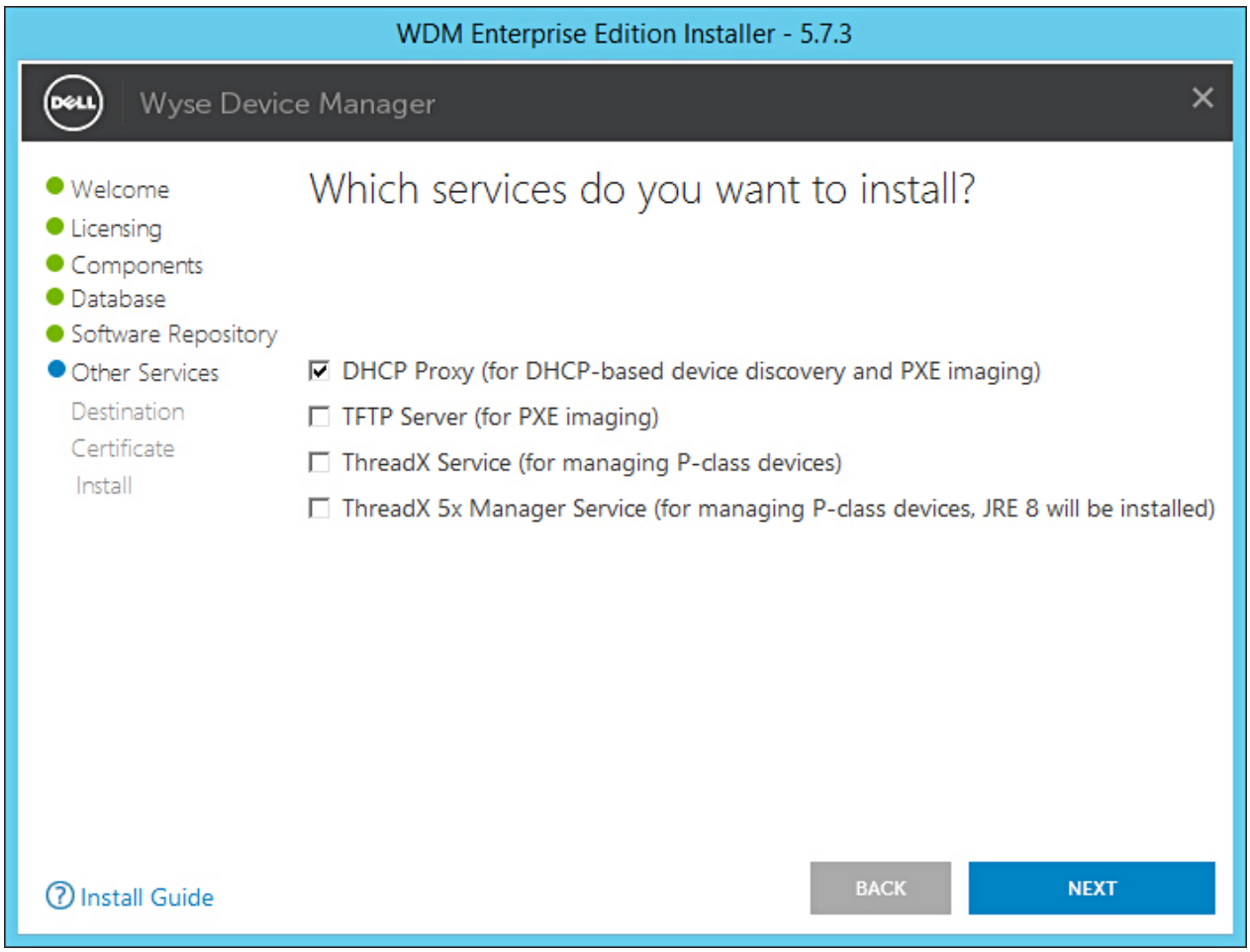


Abbildung 21. Bildschirm „Other Services“ (Andere Dienste)

ANMERKUNG: DHCP Proxy ist standardmäßig ausgewählt.

14 Geben Sie den Installationspfad ein und klicken Sie auf **NEXT** (WEITER).

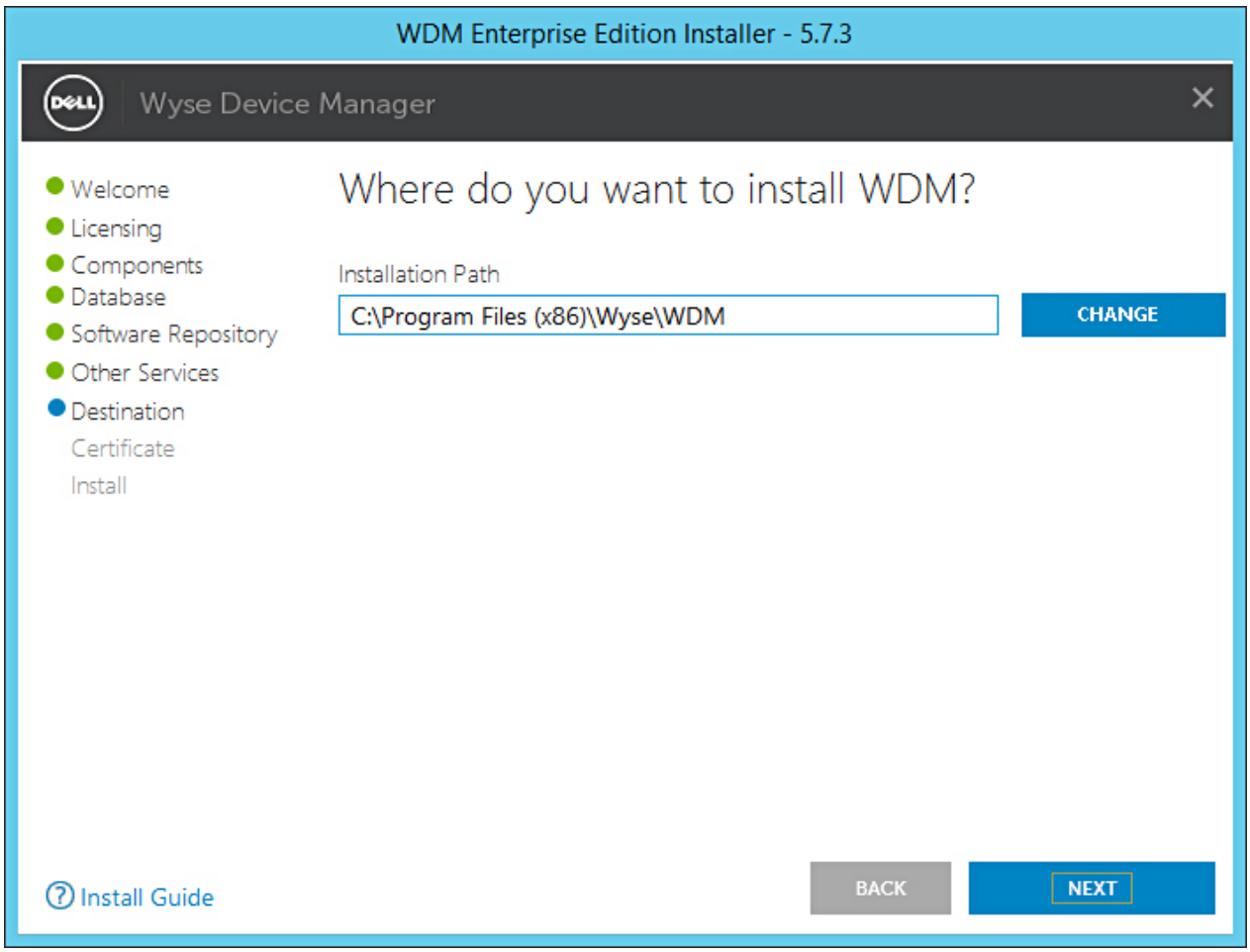


Abbildung 22. Bildschirm „Destination“ (Zielordner)

15 Wählen Sie das Zertifikat aus und importieren Sie es, um die Installation zu starten.

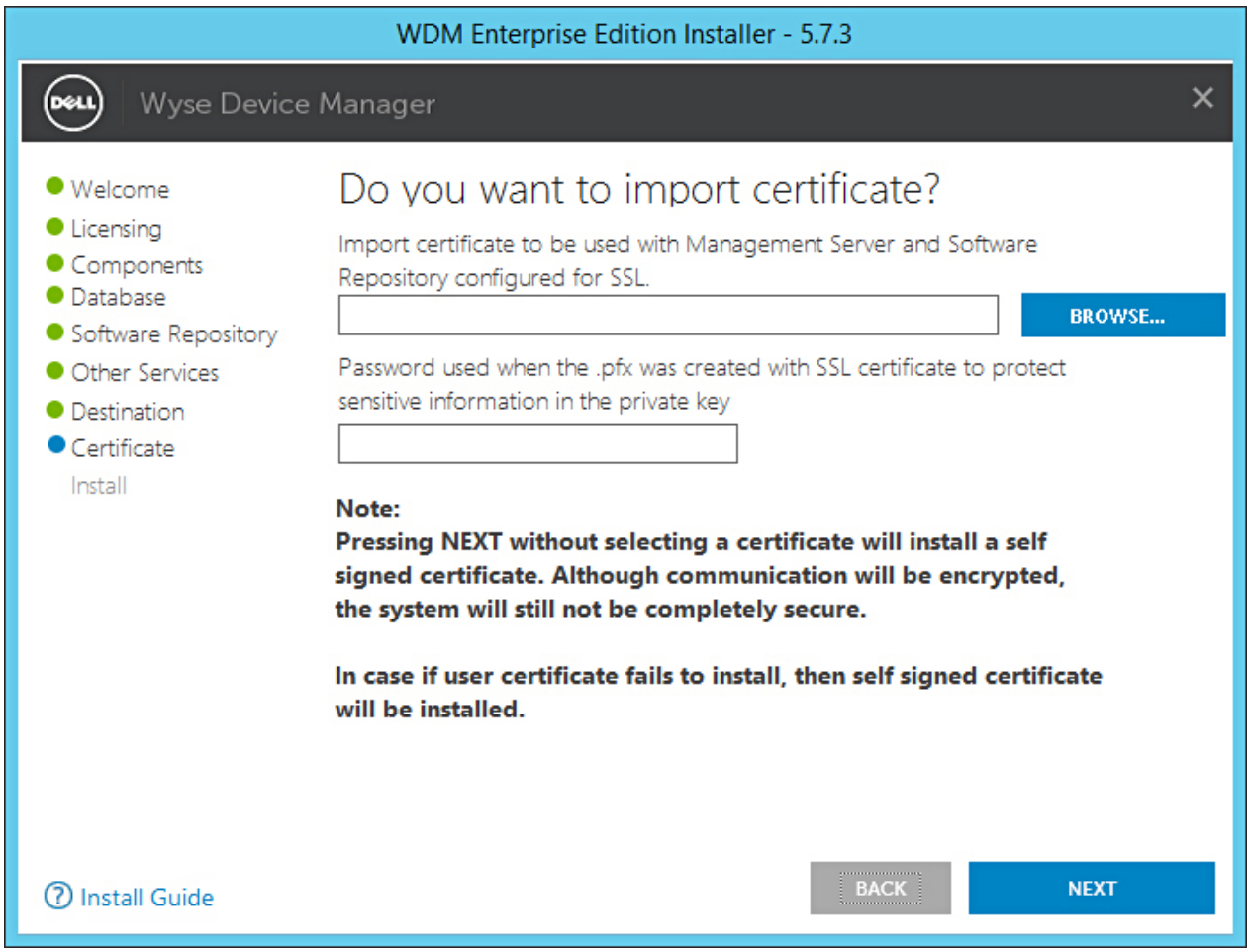


Abbildung 23. Bildschirm „Certificate“ (Zertifikat)

ANMERKUNG: Wenn Sie auf NEXT (WEITER) klicken, ohne ein Zertifikat auszuwählen, installiert das Installationsprogramm ein selbstsigniertes Zertifikat. Die Kommunikation wird verschlüsselt, aber das System ist nicht ganz sicher. Das Zertifikat muss in Form einer .pfx-Datei vorliegen.

Der Fortschritt der Installation wird auf dem Bildschirm angezeigt. Nachdem die Installation abgeschlossen ist, werden Sie dazu aufgefordert, das System neu zu starten.

Abbildung 24. Bildschirm „Installation summary“ (Installationszusammenfassung)

16 Starten Sie das System neu, um die Änderungen in Kraft zu setzen.

Installieren von WDM in einer Cloud-Umgebung

Info über diese Aufgabe

Zum Installieren von WDM in einer Cloud-Umgebung müssen Sie die Enterprise Edition installieren.

Schritte

1 Extrahieren Sie die Inhalte des WDM-Installationsprogramms auf dem System, auf dem WDM installiert werden soll.

2 Navigieren Sie zu dem Ordner, in dem Sie das Installationsprogramm extrahiert haben, und führen Sie die Datei **Setup.exe** aus.
Wenn der Server nicht über .Net Framework verfügt, dann wird .Net Framework automatisch installiert.

Der Bildschirm **Welcome** (Willkommen) wird angezeigt.

Abbildung 25. Bildschirm „Welcome“ (Willkommen)

3 Klicken Sie auf **NEXT** (WEITER).

4 Unter „License Type“ (Lizenztyp) wählen Sie **ENTERPRISE** aus.

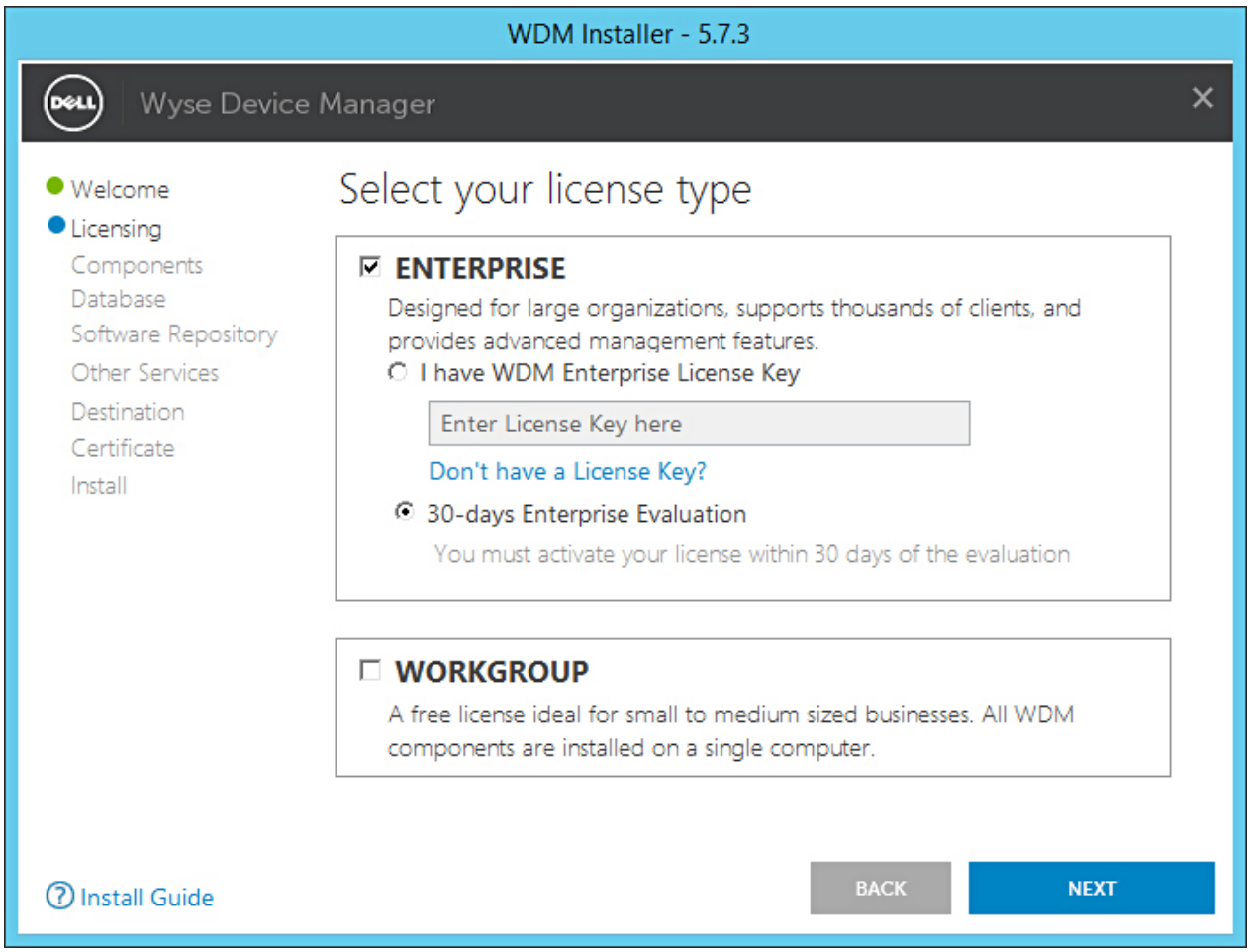


Abbildung 26. Enterprise-Lizenztyp

a Wenn Sie den WDM-Lizenzschlüssel haben, wählen Sie die Option **I have WDM Enterprise License Key** (Ich habe den WDM Enterprise-Lizenzschlüssel) aus und geben Sie den Lizenzschlüssel in das dafür vorgesehene Feld ein.

b Wenn Sie keinen Lizenzschlüssel besitzen, wählen Sie die Option **30–days Enterprise Evaluation** (30-tägige Enterprise Evaluation-Lizenz) aus.

Der Lizenzschlüssel wird standardmäßig eingegeben. Nach dem 30tägigen Testzeitraum müssen Sie jedoch den Lizenzschlüssel erwerben und ihn WDM hinzufügen. Weitere Informationen zum Hinzufügen von Lizenzschlüsseln finden Sie im *Dell Wyse Device Manager Administrator's Guide* (*Administratorhandbuch für den Dell Wyse Device Manager*).

5 Klicken Sie auf **NEXT** (WEITER).

6 Wählen Sie die Komponenten aus, die Sie installieren möchten, und klicken Sie auf **NEXT** (WEITER).

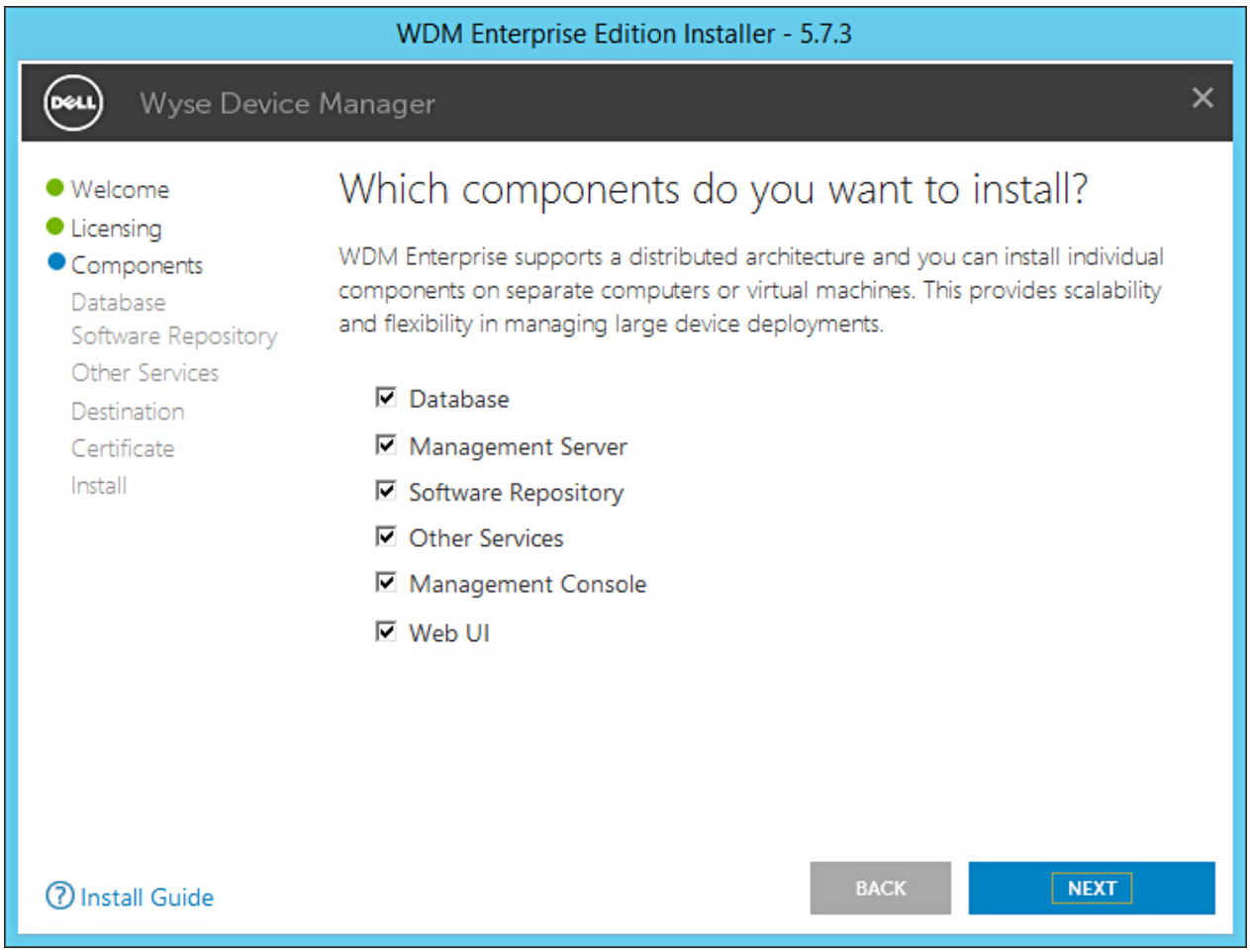


Abbildung 27. Bildschirm „Components“ (Komponenten)

Sie können alle Komponenten auf dem gleichen System oder jede Komponente auf einem anderen System installieren.

ANMERKUNG: Achten Sie beim separaten Installieren der Komponenten auf unterschiedlichen Systemen darauf, die Datenbank zuerst zu installieren. Wenn Sie die Datenbank nicht installieren, können Sie die verbleibenden Komponenten nicht installieren.

7 Wählen Sie im Bildschirm **Configure Database** (Datenbank konfigurieren) eine der folgenden Optionen aus:

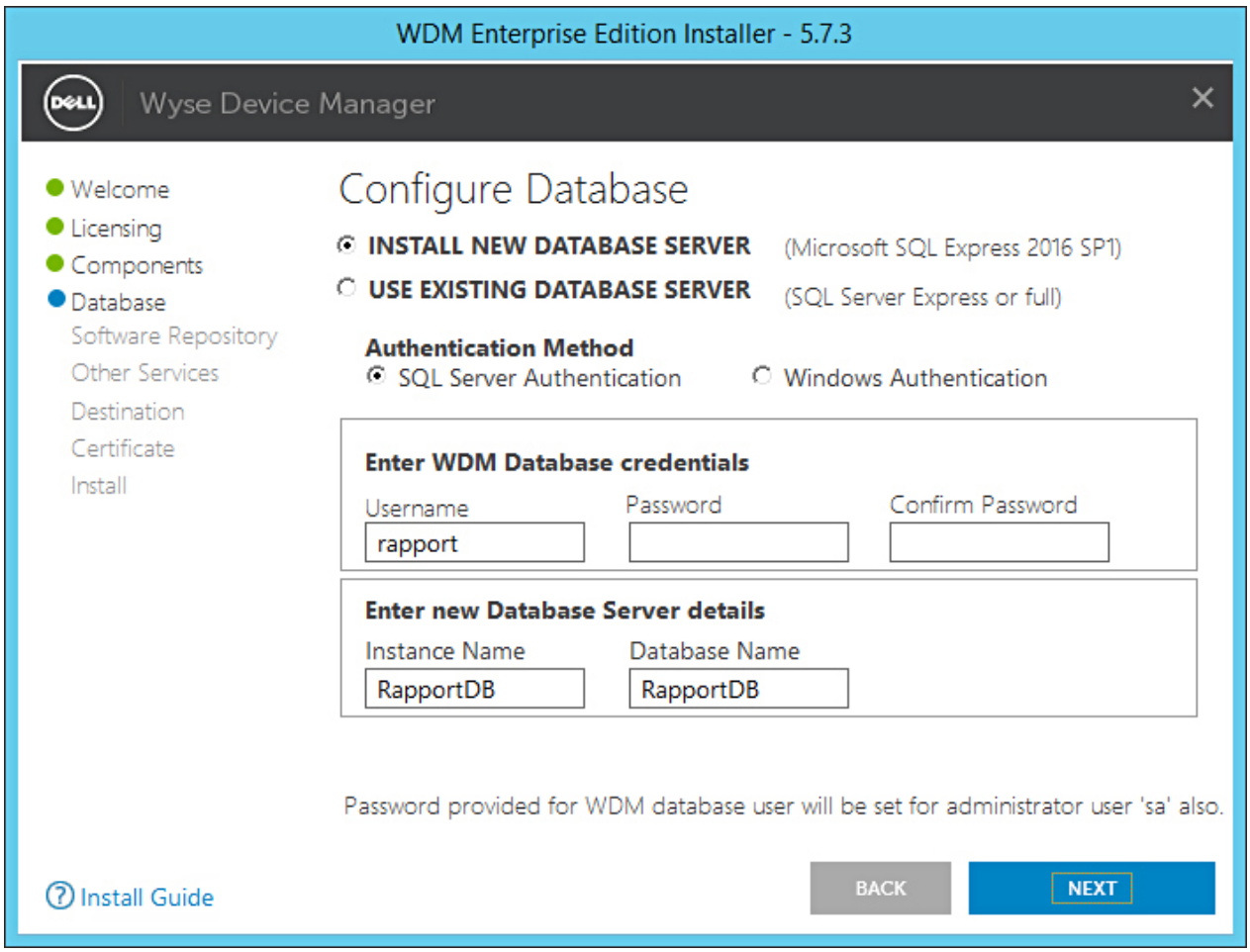


Abbildung 28. Bildschirm „Configure Database“ (Datenbank konfigurieren)

- **Install New Database Server (Microsoft SQL Express 20016 SP1)** (Neuen Datenbankserver installieren (Microsoft SQL Express 20016 SP1)) – Wählen Sie diese Option aus, wenn keine unterstützte Version von Microsoft SQL Server auf dem System installiert ist, und fahren Sie mit Schritt 8 fort.
- **Use Existing Database Server (SQL Server Express or full)** (Vorhandenen Datenbankserver verwenden (SQL Server Express oder vollständig)) – Wählen Sie diese Option aus, wenn Sie bereits eine unterstützte Version von Microsoft SQL Server auf dem System installiert haben. Wenn Sie diese Option auswählen, stellen Sie sicher, dass sich der vorhandene Datenbankserver auf demselben System befindet, auf dem Sie die WDM-Workgroup Edition installieren, und fahren Sie mit Schritt 9 fort.

8 Wenn Sie die erste Option in Schritt 7 ausgewählt haben, wählen Sie die Authentifizierungsmethode aus.

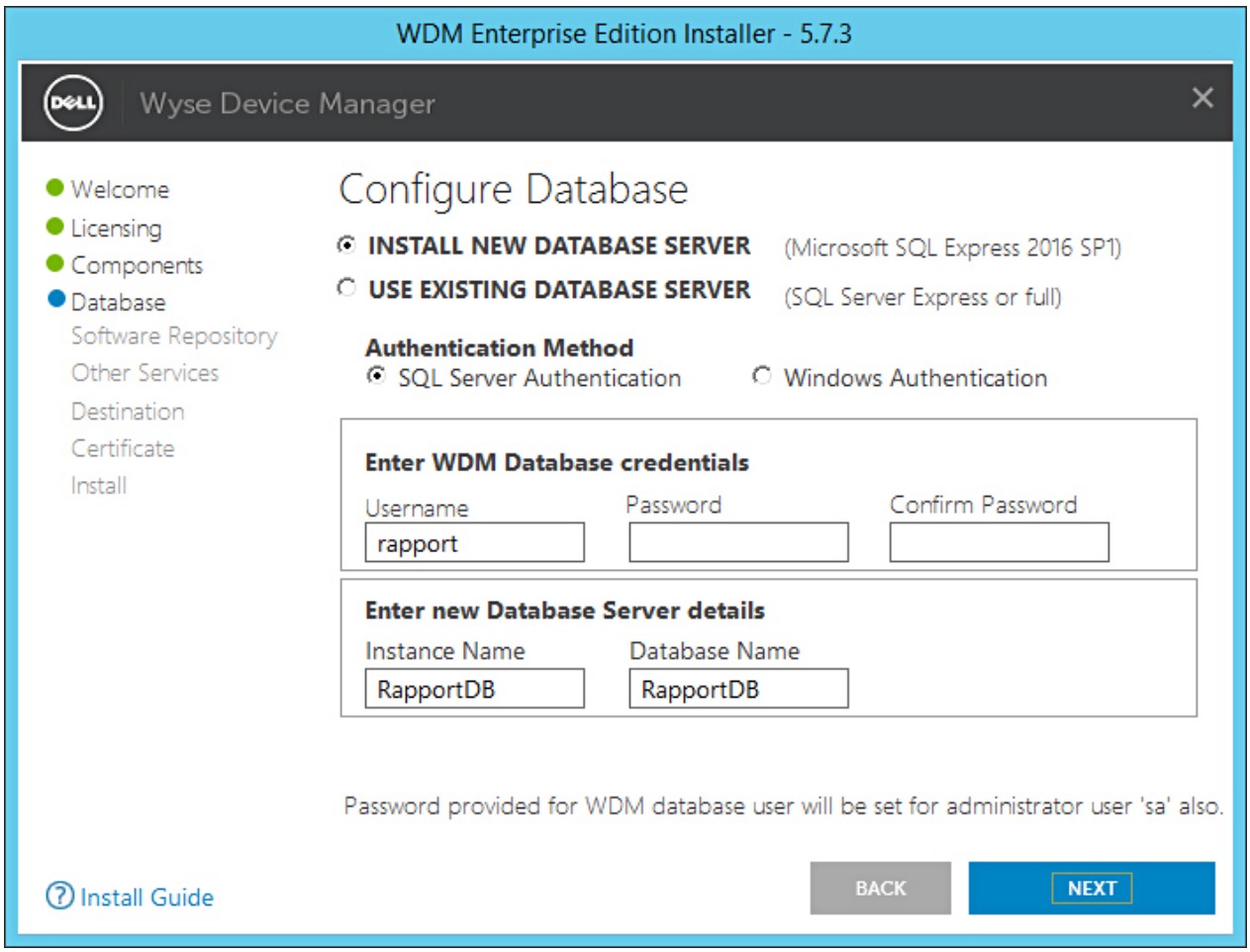


Abbildung 29. Option „Install New Database Server“ (Neue Datenbankserver installieren)

- **SQL Server Authentication** (SQL Serverauthentifizierung) – Diese Option ist standardmäßig ausgewählt. Gehen Sie folgendermaßen vor, um die SQL-Serverauthentifizierung zu konfigurieren:
  1. Geben Sie die WDM-Datenbank-Anmeldeinformationen ein.
  2. Geben Sie die neuen Datenbank-Anmeldeinformationen ein. Sie können den Instanznamen und den Datenbanknamen unter den neuen Datenbankserverdetails eingeben. Der Standard-Instanzname und -Datenbankname wird als RapportDB angezeigt.

  ANMERKUNG: Selbst wenn Sie Windows-Authentifizierung wählen, erfordert die WDM-Installation die SQL-Authentifizierung für den Zugriff auf die SQL-Datenbank. In einer eigenständigen Installation übernimmt das WDM-Installationsprogramm nach Abschluss der WDM-Datenbankinstallation das Zuweisen des Active Directory-Benutzers zur Datenbank, und derselbe Benutzer wird für die Installation der WDM-Services verwendet.
- **Windows Authentication** (Windows-Authentifizierung) – Geben Sie die neuen Datenbankserverdetails ein. Der Standard-Instanzname und -Datenbankname wird als RapportDB angezeigt.

  ANMERKUNG:
  - Wählen Sie **Windows Authentication** (Windows-Authentifizierung) aus, wenn Sie die WDM-Datenbank über Ihre Windows-Anmeldeinformationen verbinden möchten.
  - Das Kennwort muss den Komplexitätsanforderungen für Kennwörter des Windows-Betriebssystems entsprechen.

9 Wenn Sie die zweite Option in Schritt 7 ausgewählt haben, wählen Sie die Authentifizierungsmethode aus.

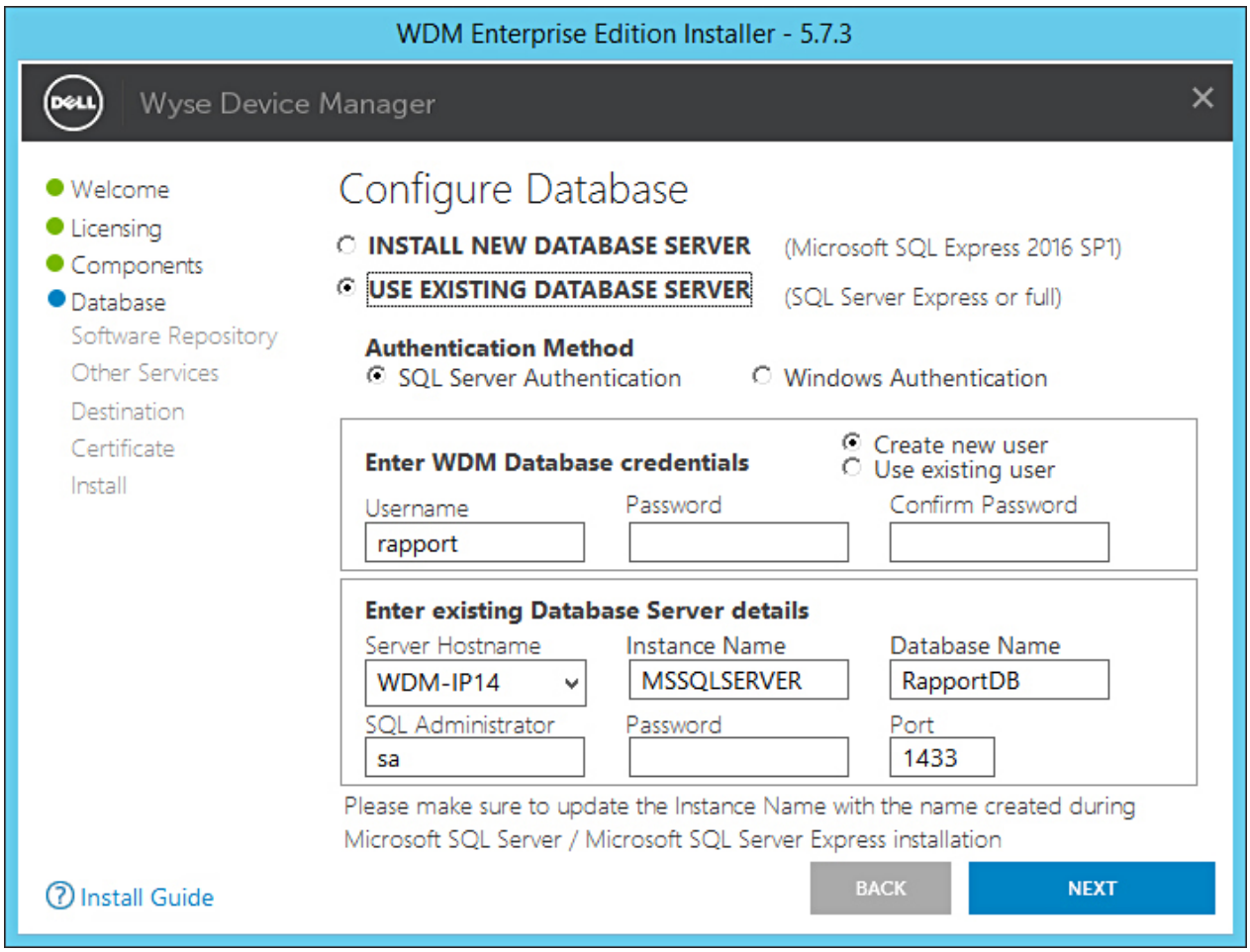


Abbildung 30. Option „Use Existing Database Server“ (Vorhandenen Datenbankserver verwenden)

- **SQL Server Authentication** (SQL Serverauthentifizierung) – Diese Option ist standardmäßig ausgewählt. Gehen Sie folgendermaßen vor, um die SQL-Serverauthentifizierung zu konfigurieren:
  1. Wählen Sie entweder die Option „Create new user“ (Neuen Benutzer erstellen) oder die Option „Use the existing user“ (Vorhandenen Benutzer verwenden) aus und geben Sie dann die WDM-Datenbank-Anmeldeinformationen ein.
  2. Geben Sie die vorhandenen Datenbankserverdetails, wie z. B. Server-Hostnamen, Instanznamen, Datenbanknamen, Portnummer sowie Namen und Kennwort des SQL-Administrators ein.
- **Windows Authentication** (Windows-Authentifizierung) – Geben Sie die vorhandenen Datenbankserverdetails, wie z. B. Server-Hostnamen, Instanznamen, Datenbanknamen, Portnummer sowie Namen und Kennwort des SQL-Administrators ein.

ANMERKUNG: Die Standardportnummer ist 1433. Dell empfiehlt, dass Sie Sie die Portnummer manuell eingeben, da diese dynamisch ist. Der dynamische Portbereich für TCP/UDP liegt zwischen 49152 und 65535.

10 Klicken Sie auf **NEXT** (WEITER).

Der Bildschirm **Configure Software Repository Server (Software Repository-Server konfigurieren)** wird angezeigt.

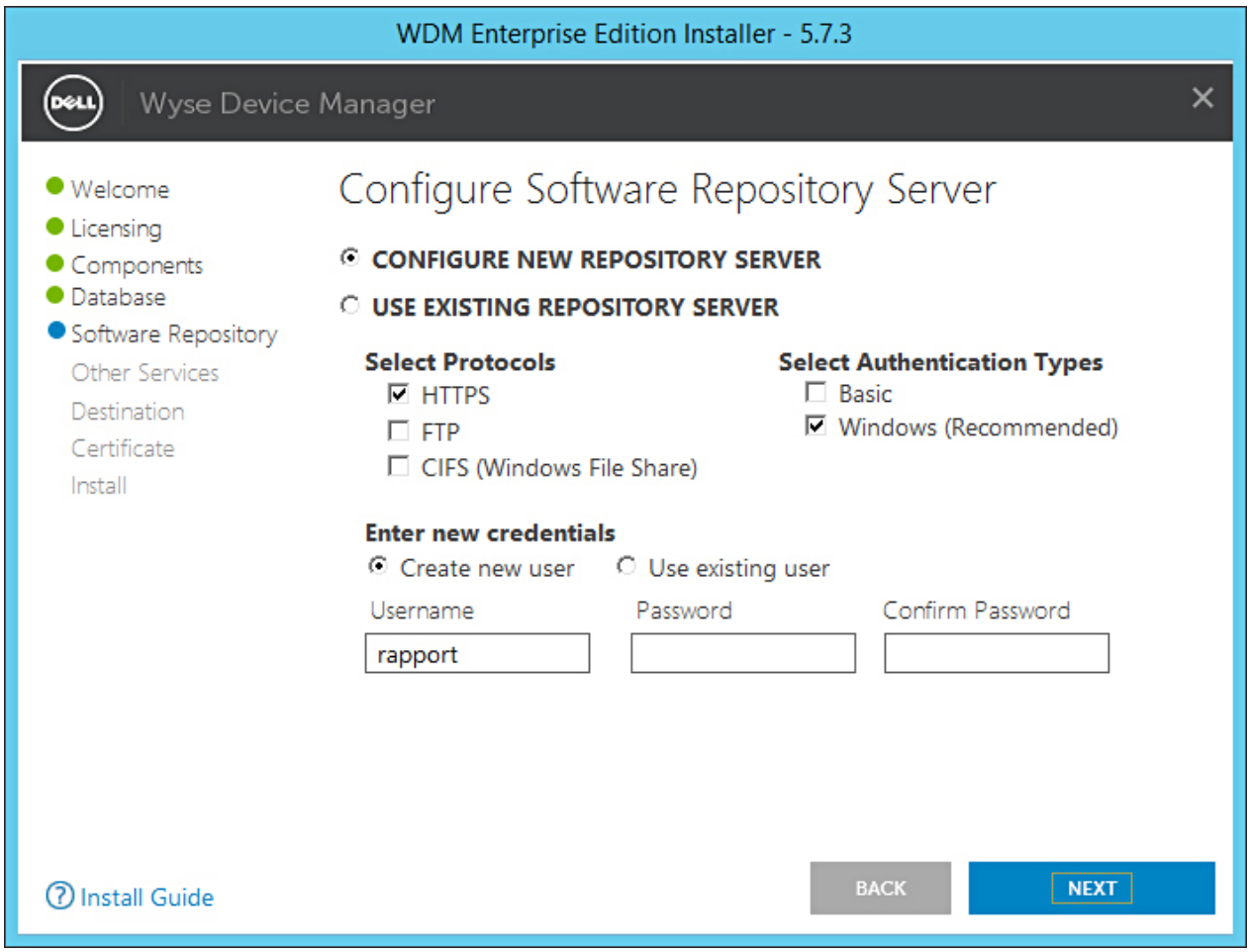


Abbildung 31. Bildschirm „Configure Software Repository Server“ (Software Repository-Server konfigurieren)

11 Auf dem Bildschirm **Configure Software Repository Server** (Software Repository-Server konfigurieren) können Sie eine der folgenden Optionen auswählen:

- **CONFIGURE NEW REPOSITORY SERVER** (NEUEN REPOSITORY-SERVER KONFIGURIEREN) – Wählen Sie diese Option, wenn das Installationsprogramm einen neuen Repository-Server konfigurieren soll. So konfigurieren Sie einen neuen Repository-Server:
  - Wählen Sie das Protokoll und Einstellungen zum Verteilen der Software auf die verwalteten Geräte aus. **HTTPS** ist standardmäßig ausgewählt. Sie können auch die Option **FTP** für ThreadX 4.x und **CIFS** für ThreadX 5.x auswählen.
  - Wählen Sie den Authentifizierungstyp aus. **Windows** ist standardmäßig ausgewählt.

    ANMERKUNG: Für Linux ist die Standardauthentifizierung erforderlich.
  - Erstellen Sie neue Benutzer-Anmeldeinformationen oder verwenden Sie die Anmeldeinformationen eines vorhandenen Benutzers.

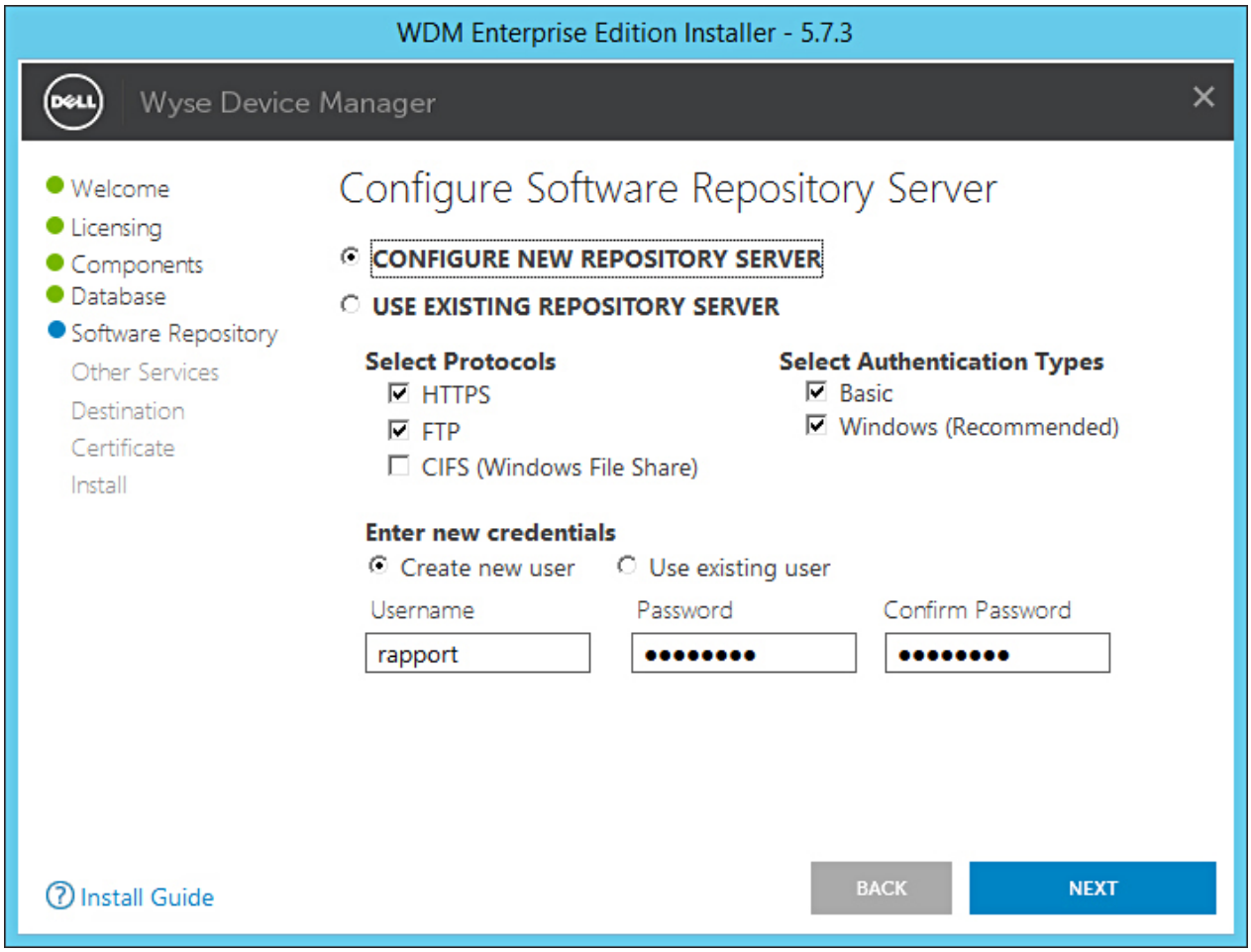


Abbildung 32. Option „CONFIGURE NEW REPOSITORY SERVER“ (NEUEN REPOSITORY-SERVER KONFIGURIEREN)

- **USE EXISTING REPOSITORY SERVER** (VORHANDENEN REPOSITORY-SERVER VERWENDEN) – Wählen Sie diese Option aus, wenn das Installationsprogramm einen vorhandenen Repository-Server verwenden soll. So konfigurieren Sie den vorhandenen Repository-Server:
  - Wählen Sie das Protokoll und die Einstellungen zum Verteilung der Software auf die verwalteten Geräte aus. **HTTPS** ist standardmäßig ausgewählt. Sie können auch die Option **FTP** für ThreadX 4.x und **CIFS** für ThreadX 5.x auswählen.
  - Wählen Sie den Authentifizierungstyp aus. **Windows** ist standardmäßig ausgewählt.
  - Geben Sie die Serveranmeldeinformationen ein. Die Server-IP-Adresse ist grau unterlegt und der Standardbenutzername lautet „rapport“.

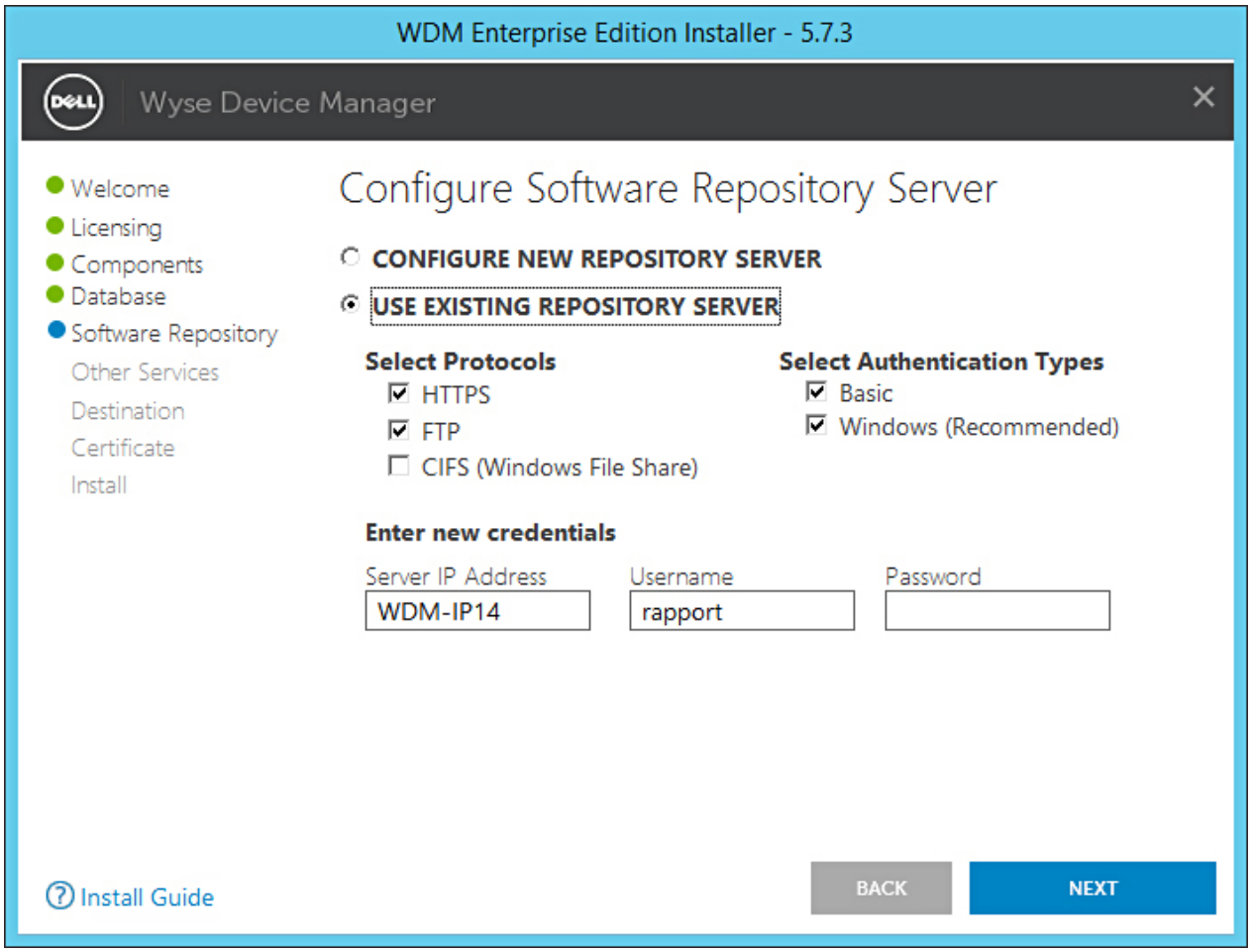


Abbildung 33. Option „USE EXISTING REPOSITORY SERVER“ (VORHANDENEN REPOSITORY-SERVER VERWENDEN)

12 Klicken Sie auf **NEXT** (WEITER).

13 Wählen Sie die Services aus, die Sie installieren möchten, und klicken Sie auf **NEXT** (WEITER).

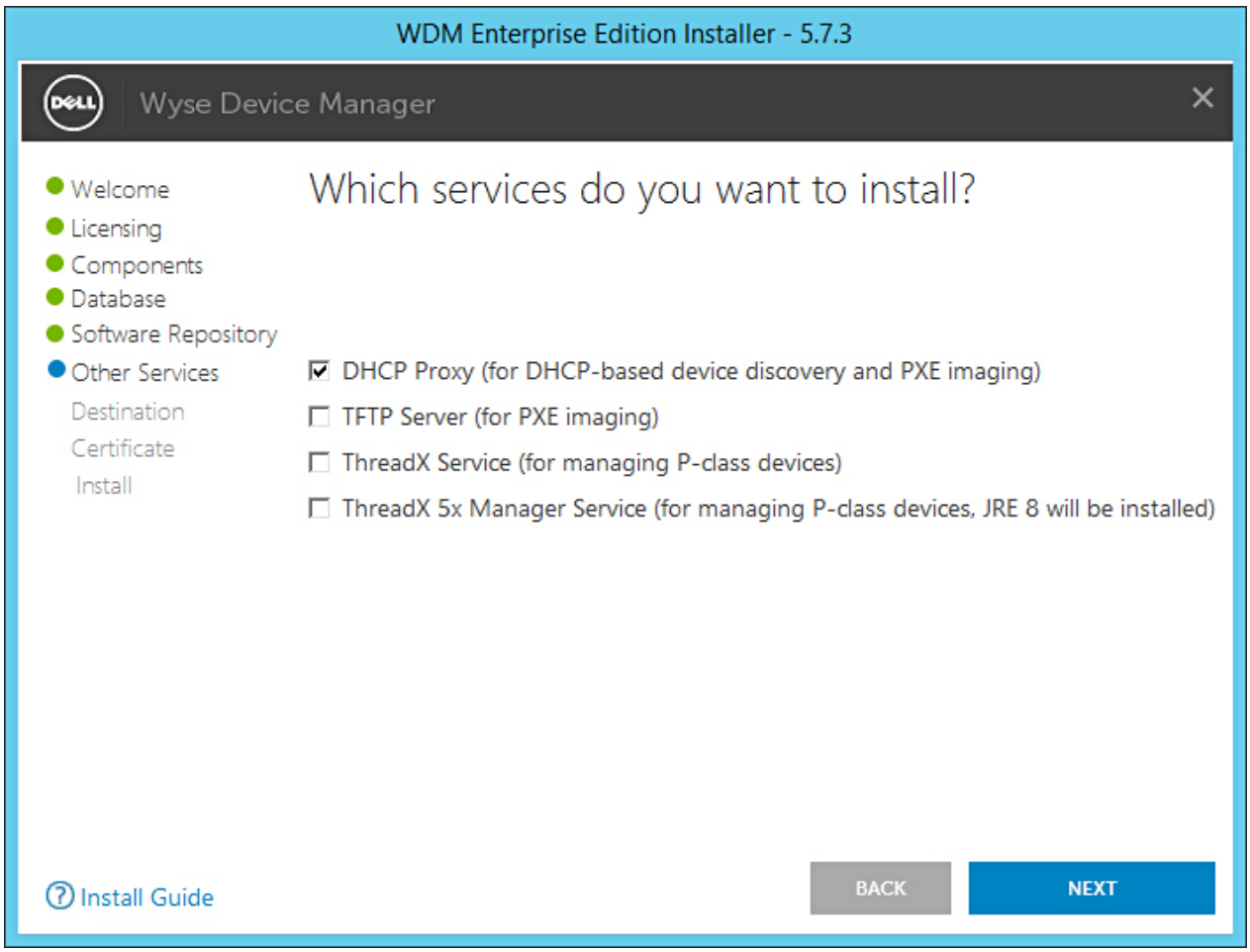


Abbildung 34. Bildschirm „Other Services“ (Andere Dienste)

ANMERKUNG: DHCP Proxy ist standardmäßig ausgewählt.

14 Geben Sie den Installationspfad ein und klicken Sie auf **NEXT** (WEITER).

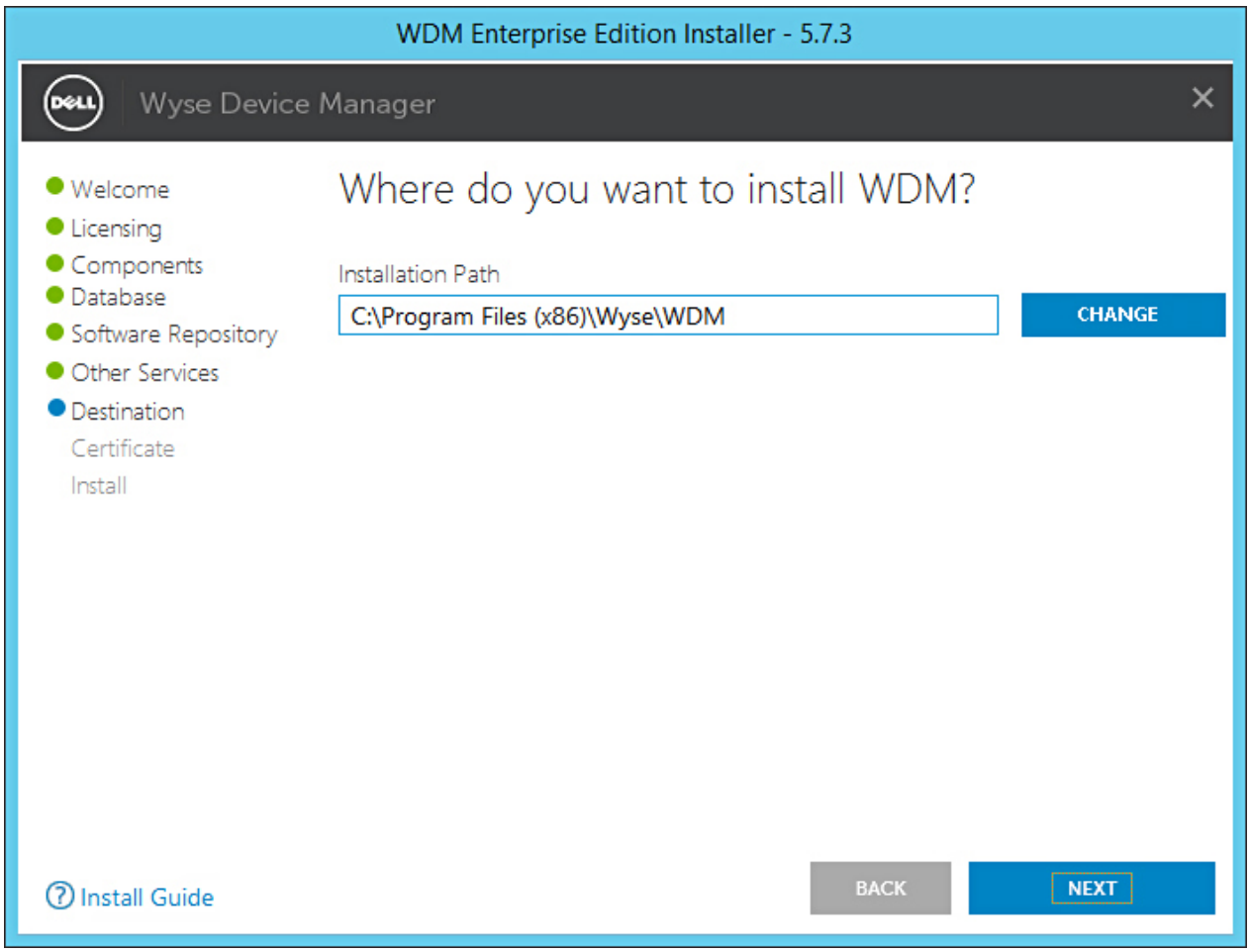


Abbildung 35. Zielordner-Bildschirm

15 Wählen Sie das Zertifikat aus und importieren Sie es, um die Installation zu starten.

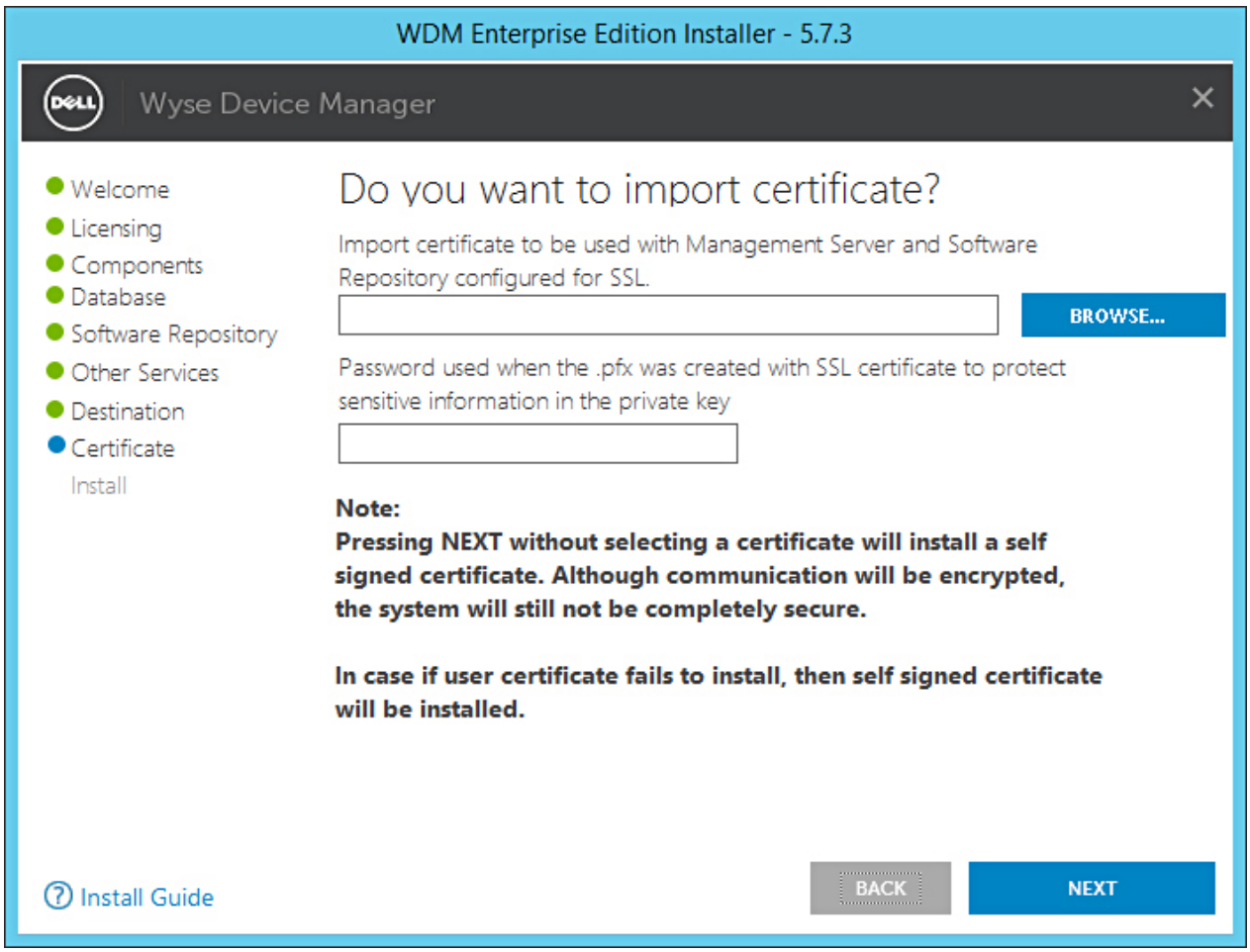


Abbildung 36. Bildschirm „Certificate“ (Zertifikat)

ANMERKUNG: Wenn Sie auf NEXT (WEITER) klicken, ohne ein Zertifikat auszuwählen, installiert das Installationsprogramm ein selbstsigniertes Zertifikat. Der Kommunikationen werden verschlüsselt, aber das System ist nicht ganz sicher. Das Zertifikat muss in Form einer .pfx-Datei vorliegen.

Der Fortschritt der Installation wird auf dem Bildschirm angezeigt. Nachdem die Installation abgeschlossen ist, werden Sie dazu aufgefordert, das System neu zu starten.

Abbildung 37. Bildschirm „Installation summary“ (Installationszusammenfassung)

16 Starten Sie das System neu, um die Änderungen in Kraft zu setzen.

Installieren von WDM in einem verteilten Setup

Sie können die WDM-Komponenten teilen und diese auf verschiedenen Systemen installieren. Dieses Setup wird als verteiltes Setup von WDM bezeichnet. Idealerweise können Sie die Komponenten folgendermaßen teilen:

- WDM-Datenbank
- WDM-Verwaltungsserver, WDM-Verwaltungskonsole und andere Dienste
- WDM Software Repository
- Weboberfläche

Für den Lastenausgleich können auch mehrere Instanzen des WDM-Verwaltungsservers und andere Dienste auf verschiedenen Systemen installiert sein. Weitere Informationen finden Sie unter Konfigurieren des Lastenausgleichs.

Die Installation von WDM in einem verteilten Setup ist am Besten für Großunternehmen geeignet, in dem eine große Anzahl von Geräten verwaltet wird. In diesem Abschnitt werden die folgenden Schritte ausführlich beschrieben:

- Installieren der WDM-Datenbank.
- Installieren des Verwaltungsservers und der Weboberfläche.
- Installieren des Software Repository.

Installieren der WDM-Datenbank

Voraussetzung

Vor der Installation der WDM-Datenbank auf einem System oder einer virtuellen Maschine (VM) stellen Sie sicher, dass Sie die unterstützte Version von Microsoft SQL Server installiert haben. Wenn Sie keinen SQL Server auf dem System haben, können Sie Microsoft SQL Express 2016 SP1 installieren, das im Lieferumfang des WDM-Installationsprogramms enthalten ist.

ANMERKUNG:

Achten Sie bei der Installation der WDM-Datenbank auf einer vorhandenen SQL Server-Datenbank darauf, dass Port 1433 auf dem System verfügbar ist.

Um die WDM-Datenbank zu installieren, müssen Sie **Database** (Datenbank) auf dem Bildschirm **Components** (Komponenten) auswählen und anschließend mit dem Installationsvorgang fortfahren.

Schritte

1 Extrahieren Sie die Inhalte des WDM-Installationsprogramms auf dem System, auf dem WDM installiert werden soll.

2 Navigieren Sie zu dem Ordner, in dem Sie das Installationsprogramm extrahiert haben, und führen Sie die Datei **Setup.exe** aus.

Wenn der Server nicht über .Net Framework verfügt, dann wird .Net Framework automatisch installiert.

Der Bildschirm „Welcome“ (Willkommen) wird angezeigt.

3 Klicken Sie auf **NEXT** (WEITER).

4 Unter „License Type“ (Lizenztyp) wählen Sie **ENTERPRISE** aus.

a Wenn Sie den WDM-Lizenzschlüssel haben, wählen Sie die Option **I have WDM Enterprise License Key** (Ich habe den WDM Enterprise-Lizenzschlüssel) aus und geben Sie den Lizenzschlüssel in das dafür vorgesehene Feld ein.

b Wenn Sie keinen Lizenzschlüssel besitzen, wählen Sie die Option **30–days Enterprise Evaluation** (30-tägige Enterprise Evaluation-Lizenz) aus.

Der Lizenzschlüssel wird standardmäßig eingegeben. Nach dem 30tägigen Testzeitraum müssen Sie jedoch den Lizenzschlüssel erwerben und ihn WDM hinzufügen. Weitere Informationen zum Hinzufügen des Lizenzschlüssels finden Sie im *Dell Wyse Device Manager Administrator's Guide* (*Administratorhandbuch für den Dell Wyse Configuration Manager*).

5 Klicken Sie auf **NEXT** (WEITER).

6 Wählen Sie die Komponente **Database** (Datenbank) aus.

7 Wählen Sie im Bildschirm **Configure Database** (Datenbank konfigurieren) eine der folgenden Optionen aus:

- **Install New Database Server (Microsoft SQL Express 20016 SP1)** (Neuen Datenbankserver installieren (Microsoft SQL Express 20016 SP1)) – Wählen Sie diese Option aus, wenn keine unterstützte Version von Microsoft SQL Server auf dem System installiert ist, und fahren Sie mit Schritt 8 fort.
- **Use Existing Database Server (SQL Server Express or full)** (Vorhandenen Datenbankserver verwenden (SQL Server Express oder vollständig)) – Wählen Sie diese Option aus, wenn Sie bereits eine unterstützte Version von Microsoft SQL Server auf dem System installiert haben. Wenn Sie diese Option auswählen, stellen Sie sicher, dass sich der vorhandene Datenbankserver auf demselben System befindet, auf dem Sie die WDM-Workgroup Edition installieren, und fahren Sie mit Schritt 9 fort.

8 Wenn Sie die erste Option in Schritt 7 ausgewählt haben, wählen Sie die Authentifizierungsmethode aus.

- **SQL Server Authentication** (SQL Serverauthentifizierung) – Diese Option ist standardmäßig ausgewählt. Gehen Sie folgendermaßen vor, um die SQL-Serverauthentifizierung zu konfigurieren:
  1 Geben Sie die WDM-Datenbank-Anmeldeinformationen ein.
  2 Geben Sie die neuen Datenbank-Anmeldeinformationen ein. Sie können den Instanznamen und den Datenbanknamen unter den neuen Datenbankserverdetails eingeben. Der Standard-Instanzname und -Datenbankname wird als RapportDB angezeigt.

ANMERKUNG: Selbst wenn Sie Windows-Authentifizierung wählen, erfordert die WDM-Installation die SQL-Authentifizierung für den Zugriff auf die SQL-Datenbank. In einer eigenständigen Installation übernimmt das WDM-Installationsprogramm nach Abschluss der WDM-Datenbankinstallation das Zuweisen des Active Directory-Benutzers zur Datenbank, und derselbe Benutzer wird für die Installation der WDM-Services verwendet.

- **Windows Authentication** (Windows-Authentifizierung) – Geben Sie die neuen Datenbankserverdetails ein. Der Standard-Instanzname und -Datenbankname wird als RapportDB angezeigt.

ANMERKUNG:

- Wählen Sie **Windows Authentication** (Windows-Authentifizierung) aus, wenn Sie die WDM-Datenbank über Ihre Windows-Anmeldeinformationen verbinden möchten.
- Das Kennwort muss den Komplexitätsanforderungen für Kennwörter des Windows-Betriebssystems entsprechen.

9 Wenn Sie die zweite Option in Schritt 7 ausgewählt haben, wählen Sie die Authentifizierungsmethode aus.

- **SQL Server Authentication** (SQL Serverauthentifizierung) – Diese Option ist standardmäßig ausgewählt. Gehen Sie folgendermaßen vor, um die SQL-Serverauthentifizierung zu konfigurieren:
  1 Wählen Sie entweder die Option **Create New User** (Neuen Benutzer erstellen) oder die Option „Use the existing user“ (Vorhandenen Benutzer verwenden) aus und geben Sie dann die WDM-Datenbank-Anmeldeinformationen ein.
  2 Geben Sie die vorhandenen Datenbankserverdetails, wie z. B. Server-Hostnamen, Instanznamen, Datenbanknamen, Portnummer sowie Namen und Kennwort des SQL-Administrators, ein.
- **Windows Authentication** (Windows-Authentifizierung) – Geben Sie die vorhandenen Datenbankserverdetails, wie z. B. Server-Hostnamen, Instanznamen, Datenbanknamen, Portnummer sowie Namen und Kennwort des SQL-Administrators, ein.

ANMERKUNG: Die Standardportnummer ist 1433. Dell empfiehlt, dass Sie Sie die Portnummer manuell eingeben, da diese dynamisch ist. Sie können eine fünfstellige benutzerdefinierte Portnummer für TCP/UDPim Bereich zwischen 49152 und 65535 eingeben.

10 Klicken Sie auf **NEXT** (WEITER).

11 Geben Sie den Installationspfad ein und klicken Sie auf **NEXT** (WEITER).

Daraufhin wird der Bildschirm **Installation Summary** (Installationszusammenfassung) angezeigt.

12 Klicken Sie auf **NEXT** (WEITER).

Der Fortschritt der Installation wird auf dem Bildschirm angezeigt. Nachdem die Installation abgeschlossen ist, werden Sie dazu aufgefordert, das System neu zu starten.

13 Starten Sie das System neu, um die Änderungen in Kraft zu setzen.

Informationen zur manuellen Installation der WDM-Datenbank mithilfe von Skripts finden Sie unter Manuelle Installation der WDM-Datenbank mithilfe von Skripts.

Installation der Management-Services

Info über diese Aufgabe

Sie können den Verwaltungsserver, die Verwaltungskonsole und die Weboberfläche auf demselben System oder auf verschiedenen Systemen installieren.

Schritte

1 Extrahieren Sie die Inhalte des WDM-Installationsprogramms auf dem System, auf dem WDM installiert werden soll.

2 Navigieren Sie zu dem Ordner, in dem Sie das Installationsprogramm extrahiert haben, und führen Sie die Datei **Setup.exe** aus.

Wenn der Server nicht über .Net Framework verfügt, dann wird .Net Framework automatisch installiert.

Der Bildschirm **Welcome** (Willkommen) wird angezeigt.

3 Klicken Sie auf **NEXT** (WEITER).

4 Unter „License Type“ (Lizenztyp) wählen Sie **ENTERPRISE** aus.

a Wenn Sie den WDM-Lizenzschlüssel haben, wählen Sie die Option **I have WDM Enterprise License Key** (Ich habe den WDM Enterprise-Lizenzschlüssel) aus und geben Sie den Lizenzschlüssel in das dafür vorgesehene Feld ein.

b Wenn Sie keinen Lizenzschlüssel besitzen, wählen Sie die Option **30–days Enterprise Evaluation** (30-tägige Enterprise Evaluation-Lizenz) aus.

Der Lizenzschlüssel wird standardmäßig eingegeben. Nach dem 30tägigen Testzeitraum müssen Sie jedoch den Lizenzschlüssel erwerben und ihn WDM hinzufügen. Weitere Informationen zum Hinzufügen des Lizenzschlüssels finden Sie im *Dell Wyse Device Manager Administrator's Guide* (*Administratorhandbuch für den Dell Wyse Configuration Manager*).

5 Klicken Sie auf **NEXT** (WEITER).

6 Wählen Sie **Management Server** (Verwaltungsserver), **Other Services** (Andere Dienste), **Management Console** (Verwaltungskonsole) und **Web UI** (Webbenutzeroberfläche) aus.

ANMERKUNG: Wenn Sie jede Komponente auf einem separaten System installieren, können Sie sie nacheinander mit den Schritten 1 bis 5 auswählen.

7 Wählen Sie im Bildschirm **Configure Database** (Datenbank konfigurieren) eine der folgenden Optionen aus:

- **SQL Server Authentication** (SQL Serverauthentifizierung) – Diese Option ist standardmäßig ausgewählt. Zum Konfigurieren der SQL Serverauthentifizierung geben Sie die Anmeldeinformationen für den WDM-Datenbankserver ein.
- **Windows Authentication** (Windows-Authentifizierung) – Geben Sie die WDM-Datenbankserverdetails, wie z. B. Servernamen, Instanznamen Datenbanknamen, Kennwort und Portnummer ein. Das Feld **Username** (Benutzername) ist grau unterlegt.

ANMERKUNG:

- Die Standardportnummer ist 1433. Dell empfiehlt, dass Sie Sie die Portnummer manuell eingeben, da diese dynamisch ist. Sie können eine fünfstellige benutzerdefinierte Portnummer für TCP/UDPim Bereich zwischen 49152 und 65535 eingeben.
- Wählen Sie **Windows Authentication** (Windows-Authentifizierung) aus, wenn Sie die WDM-Datenbank über Ihre Windows-Anmeldeinformationen verbinden möchten.

8 Klicken Sie auf **NEXT** (WEITER).

9 Wählen Sie die Services aus, die Sie installieren möchten, und klicken Sie auf **NEXT** (WEITER).

ANMERKUNG: DHCP Proxy ist standardmäßig ausgewählt.

10 Geben Sie den Installationspfad ein und klicken Sie auf **NEXT** (WEITER).

11 Wählen Sie das Zertifikat aus und importieren Sie es, um die Installation zu starten.

ANMERKUNG: Wenn Sie auf NEXT (WEITER) klicken, ohne ein Zertifikat auszuwählen, installiert das Installationsprogramm ein selbstsigniertes Zertifikat. Der Kommunikationen werden verschlüsselt, aber das System ist nicht sicher. Das Zertifikat muss in Form einer .pfx-Datei vorliegen.

Der Fortschritt der Installation wird auf dem Bildschirm angezeigt. Nachdem die Installation abgeschlossen ist, werden Sie dazu aufgefordert, das System neu zu starten.

12 Starten Sie das System neu, um die Änderungen in Kraft zu setzen.

ANMERKUNG: In einer verteilten Umgebung kann die Weboberfläche auf mehreren Konsolen installiert werden.

Installieren des Software Repository

Voraussetzung

Das Software Repository ist ein weiterer wichtiger Bestandteil von WDM. Die auf den Clientsystemen bereitzustellenden Pakete werden im Software Repository gespeichert. Vor der Installation des Software-Repository stellen Sie sicher, dass Sie die WDM-Datenbank installiert und konfiguriert haben.

Schritte

1 Extrahieren Sie die Inhalte des WDM-Installationsprogramms auf dem System, auf dem WDM installiert werden soll.

2 Navigieren Sie zu dem Ordner, in dem Sie das Installationsprogramm extrahiert haben, und führen Sie die Datei **Setup.exe** aus.

Wenn der Server nicht über .Net Framework verfügt, dann wird .Net Framework automatisch installiert.

Der Bildschirm **Welcome** (Willkommen) wird angezeigt.

3 Klicken Sie auf **NEXT** (WEITER).

4 Unter „License Type“ (Lizenztyp) wählen Sie **ENTERPRISE** aus.

a Wenn Sie den WDM-Lizenzschlüssel haben, wählen Sie die Option **I have WDM Enterprise License Key** (Ich habe den WDM Enterprise-Lizenzschlüssel) aus und geben Sie den Lizenzschlüssel in das dafür vorgesehene Feld ein.

b Wenn Sie keinen Lizenzschlüssel besitzen, wählen Sie die Option **30–days Enterprise Evaluation** (30-tägige Enterprise Evaluation-Lizenz) aus.

Der Lizenzschlüssel wird standardmäßig eingegeben. Nach dem 30tägigen Testzeitraum müssen Sie jedoch den Lizenzschlüssel erwerben und ihn WDM hinzufügen. Weitere Informationen zum Hinzufügen des Lizenzschlüssels finden Sie im *Dell Wyse Device Manager Administrator's Guide* (*Administratorhandbuch für den Dell Wyse Configuration Manager*).

5 Klicken Sie auf **NEXT** (WEITER).

6 Wählen Sie die Komponente **Software Repository** (Software-Repository) aus.

7 Wählen Sie im Bildschirm **Configure Database** (Datenbank konfigurieren) eine der folgenden Optionen aus:

- **SQL Server Authentication** (SQL Serverauthentifizierung) – Diese Option ist standardmäßig ausgewählt. Zum Konfigurieren der SQL Serverauthentifizierung geben Sie die Anmeldeinformationen für den WDM-Datenbankserver ein.
- **Windows Authentication** (Windows-Authentifizierung) – Geben Sie die WDM-Datenbankserverdetails, wie z. B. Servernamen, Instanznamen Datenbanknamen, Kennwort und Portnummer ein. Das Feld **Username** (Benutzername) ist grau unterlegt.

ANMERKUNG:

- Die Standardportnummer ist 1433. Dell empfiehlt, dass Sie die Portnummer manuell eingeben, da diese dynamisch ist. Sie können eine fünfstellige benutzerdefinierte Portnummer für TCP/UDPim Bereich zwischen 49152 und 65535 eingeben.
- Wählen Sie **Windows Authentication** (Windows-Authentifizierung) aus, wenn Sie die WDM-Datenbank über Ihre Windows-Anmeldeinformationen verbinden möchten.

8 Klicken Sie auf **NEXT** (WEITER).

9 Wählen Sie die Services aus, die Sie installieren möchten, und klicken Sie auf **NEXT** (WEITER).

ANMERKUNG: DHCP Proxy ist standardmäßig ausgewählt.

10 Geben Sie den Installationspfad ein und klicken Sie auf **NEXT** (WEITER).

11 Wählen Sie das Zertifikat aus und importieren Sie es, um die Installation zu starten.

ANMERKUNG: Wenn Sie auf NEXT (WEITER) klicken, ohne ein Zertifikat auszuwählen, installiert das Installationsprogramm ein selbstsigniertes Zertifikat. Der Kommunikationen werden verschlüsselt, aber das System ist nicht sicher. Das Zertifikat muss in Form einer .pfx-Datei vorliegen.

Der Fortschritt der Installation wird auf dem Bildschirm angezeigt. Nachdem die Installation abgeschlossen ist, werden Sie dazu aufgefordert, das System neu zu starten.

12 Starten Sie das System neu, um die Änderungen in Kraft zu setzen.

ANMERKUNG: In einer verteilten Umgebung kann die Weboberfläche auf mehreren Konsolen installiert werden.

Upgrade von WDM

Vorbedingungen

Die aktuelle Version von WDM unterstützt eine Aktualisierung von WDM Version 5.7.2 /5.7.2 Hot-Fix-Release. Es ist nicht möglich, ein Upgrade von einer anderen Version durchzuführen. Wenn Sie eine ältere Version von WDM ausführen, müssen Sie zunächst eine Aktualisierung auf Version 5.7.2 /5.7.2 Hot-Fix-Release und dann eine Aktualisierung auf die neueste Version durchführen.

ANMERKUNG: Nach der Aktualisierung auf WDM Version 5.7.3 müssen Sie alle Geräte mit den neuesten verfügbaren Agent-Paketen aktualisieren, um sicherzustellen, dass Ihre Geräte über WDM verwaltet werden können. Weitere Informationen finden Sie in den *Versionshinweisen zu WDM 5.7* unter support.dell.com.

Aufgabe

1 Extrahieren Sie den Inhalt des WDM-Installationsprogramms auf dem System, auf dem Sie WDM Version 5.7.2 /5.7.2 Hot-Fix-Release installiert haben.

2 Navigieren Sie zu dem Ordner, in dem Sie das Installationsprogramm extrahiert haben, und führen Sie die Datei **Setup.exe** aus.

Der Bildschirm **Welcome** (Willkommen) wird angezeigt.

3 Klicken Sie auf **Next** (Weiter).
Der Bildschirm **Upgrade Information** (Upgrade-Informationen) wird angezeigt.

4 Klicken Sie auf **Next** (Weiter). Der Bildschirm **User Credentials** (Benutzeranmeldeinformationen) wird angezeigt.

5 Geben Sie das Kennwort ein.

WICHTIG: Das Feld Password (Kennwort) ist für die SQL-Authentifizierung deaktiviert. Die müssen das Kennwort nur für die Windows-Authentifizierung eingeben.

6 Klicken Sie auf **Next** (Weiter).

Der Bildschirm **Important Information** (Wichtige Informationen) wird angezeigt.

7 Lesen Sie **Important Information** (Wichtige Informationen) durch und klicken Sie auf **Next** (Weiter).

Der Aktualisierungsvorgang beginnt.

8 Nachdem der Aktualisierungsvorgang abgeschlossen ist, klicken Sie auf **Restart Now** (Jetzt neu starten), damit die Änderungen im System wirksam werden, bevor Sie WDM verwenden.

ANMERKUNG: ThreadX 5.x wird unter Windows 2012 und höheren Versionen automatisch installiert, wenn ThreadX 4.x bereits auf dem System installiert ist.

Konfigurieren einer sicheren Kommunikation

Konfigurieren einer sicheren Kommunikation über SSL:

Es gibt verschiedene Möglichkeiten zur Installation von SSL in IIS 6.0 und IIS 7.0. Die Vorgehensweisen bei der Konfiguration von SSL in IIS 6.0 und IIS 7.0 werden nachstehend aufgeführt.

Konfigurieren von SSL in IIS 7.0 auf Windows Server 2008 R2

So konfigurieren Sie SSL in IIS 7.0:

1 Laden Sie das Dienstprogramm **SelfSSL7** über den Link SelfSSL.exe herunter.

2 Rufen Sie das Dienstprogramm **SelfSSL7.exe** mit den unten genannten Parametern auf:

```
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"
```

Konfigurieren einer sicheren Kommunikation über die Stammzertifizierungsstelle

Installieren der Stammzertifizierungsstelle in IIS 7 auf Windows Server 2008 R2

Verwenden Sie die folgenden Schritte:

Um das Zertifikat zu installieren, müssen zwei Schritte durchgeführt werden:

- Installieren Sie das Zertifikat auf dem **Domänen-Controller**-Server.
- Installieren Sie das Zertifikat auf dem **WDM**-Server.

Installieren des Zertifikats auf dem Domänen-Controller-Server

Verwenden Sie die folgenden Schritte:

1 Rufen Sie den **Server-Manager** auf.

2 Wählen Sie im Strukturbereich **Roles** (Rollen) > **Add Roles** (Rollen hinzufügen).

3 Wählen Sie im Assistenten **Add Roles** (Rollen hinzufügen) die Option **Server Roles** (Serverrollen) aus dem Strukturbereich aus.

4 Aktivieren Sie im Fenster **Server Role** (Serverrolle) die Option **Active Directory Certificate Servie** (Active Directory-Zertifikatdienste) unter **Roles** (Rollen).

5 Klicken Sie auf **Next** (Weiter) ->**Next** (Weiter). Aktivieren Sie unter **Role Services** (Rollendienste) die Optionen **Certification Authority** (Zertifizierungsstelle) und **Certificate Authority Web Enrolment** (Zertifizierungsstellen-Webregistrierung).

6 Wenn IIS nicht auf dem Server installiert ist, wird nach der Aktivierung der Option **Certification Authority Web Enrolment** (Zertifizierungsstellen-Webregistrierung) ein anderes Fenster **Add Required Role Services** (Erforderliche Rollendienste hinzufügen) angezeigt:

7 Klicken Sie im oben genannten Fenster auf die Schaltfläche **Add Required Role Services** (Erforderliche Rollendienste hinzufügen) und klicken Sie auf **Next** (Weiter), um das Fenster **Specifiy Setup Type** (Setuptyp angeben) aufzurufen.

8 Aktivieren Sie je nach Anforderung im oben genannten Fenster entweder das Optionsfeld **Enterprise** (Unternehmen) oder **Standalone** (Eigenständig) und klicken Sie auf **Next** (Weiter), um das Fenster **Specify CA Type** (Zertifizierungsstellentyp angeben) zu öffnen.

9 Aktivieren Sie im Fenster **Specifiy CA Type** (Zertifizierungsstellentyp angeben) je nach Anforderung entweder das Optionsfeld **Subordinate CA** (Stammzertifizierungsstelle) oder **Subordinate CA** (Untergeordnete Zertifizierungsstelle) und klicken Sie auf **Next** (Weiter), um das Fenster **Setup Private Key** (Privaten Schlüssel einrichten) zu öffnen.

10 Aktivieren Sie im Fenster **Setup Private Key** (Privaten Schlüssel einrichten) je nach Anforderung entweder das Optionsfeld **Create a new private key** (Neuen privaten Schlüssel erstellen) oder **Use existing private key** (Vorhandenen privaten Schlüssel verwenden) und klicken Sie auf **Next** (Weiter), um das Fenster **Configure Cryptography for CA** (Kryptographie für ZS konfigurieren) zu öffnen.

11 Wählen Sie im Fenster **Configure Cryptography for CA** (Kryptographie für ZS konfigurieren) finden Sie je nach Anforderung den Wert für das Feld **Select a cryptography service provider (CSP)** (Wählen Sie einen Kryptographiedienstanbieter (CSP) aus) aus dem Kombinationsfeld aus. Wählen Sie die **Key character length** (Schlüsselzeichenlänge) aus dem Kombinationsfeld und den Wert für das Feld **Select hte Hash algorithm for signing certificate issued by this CA** (Wählen Sie den Hashalgorithmus zum Signieren von Zertifikaten aus, die von dieser Zertifizierungsstelle ausgestellt werden) aus. Aktivieren oder deaktivieren Sie dann das Kontrollkästchen **Allow administrator interaction when the private key is accessed by the CA** (Administratorinteraktion bei jedem Zertifizierungsstellenzugriff auf den privaten Schlüssel zulassen) und klicken Sie auf die Schaltfläche **Next** (Weiter), um das Fenster **Configure CA Name** (Name der Zertifizierungsstelle konfigurieren) zu öffnen.

ANMERKUNG: Der allgemeine Name des Zertifikats sollte mit dem Computernamen des WDM-Servers übereinstimmen.

12 Geben Sie im Fenster**Configure CA Name** (Name der Zertifizierungsstelle konfigurieren) die Werte für die Felder **Common name for this CA** (Allgemeiner Name dieser Zertifizierungsstelle) und **Distinguished name suffix** (Suffix des definierten Namens) ein und klicken Sie auf **Next** (Weiter), um das Fenster **Set Validity Period** (Festlegen der Gültigkeitsdauer) zu öffnen.

13 Wählen Sie im Fenster **Set Validity Period** (Festlegen der Gültigkeitsdauer) die Gültigkeitsdauer für das Zertifikat aus, das für diese Zertifizierungsstelle generiert wurde, und klicken Sie auf **Next** (Weiter), um das Fenster **Configure Certificate Database** (Zertifikatdatenbank konfigurieren) zu öffnen.

14 Wählen Sie im Fenster **Configure Certificate Database** (Zertifikatdatenbank konfigurieren) den Pfad für **Certificate database location** (Speicherort der Zertifikatdatenbank) und **Certificate database log location** (Speicherort des Zertifikatdatenbankprotokolls) aus und klicken Sie auf **Next** (Weiter), um das Fenster **Add Roles Wizard** (Assistent "Rollen hinzufügen") für IIS zu öffnen.

15 Wählen Sie die Standardwerte aus und klicken Sie auf **Next** (Weiter) > **Install** (Installieren).

16 Daraufhin werden die **Active Directory Certificate Services** (Active Directory-Zertifikatdienste), **Web Server (IIS)** (Webserver (IIS) und **Remote Server Administration Tools** (Remoteserver-Verwaltungstools) installiert.

17 Navigieren Sie nach der Installation des Zertifikats zum **Internet Informationen Services Manager** (Internetinformationsdienste-Manager) des Domänen-Controllers.

18 Erweitern Sie im Strukturbereich **Server Manager** (Server-Manager) die Option **Roles** (Rollen) und klicken Sie dann auf **Web Server (IIS)** (Webserver (IIS)) > **Internet Information Services (IIS) Manager** (Internetinformationsdienste (IIS)-Manager), um das Fenster **IIS Manager** zu öffnen.

19 Wählen Sie im Strukturbereich den **Server** aus und doppelklicken Sie im rechten Fensterbereich auf **Server Certificate** (Server-Zertifikate).

20 Doppelklicken Sie im rechten Fensterbereich von **Server Certificates** (Serverzertifikate) auf **Create Domain Certificate...** (Domänenzertifikat erstellen ...), um mit der Erstellung eines Zertifikats zu beginnen.

21 Füllen Sie die angeforderten Informationen im Fenster **Create Certificate** (Zertifikat erstellen) aus und klicken Sie auf **Next** (Weiter), um **Online Certification Authority** (Onlinezertifizierungsstelle) zu öffnen.

22 Klicken Sie im Fenster **Online Authority Certification** (Onlinezertifizierungsstelle) unter **Specifiy Online Certification Authority** (Onlinezertifizierungsstelle angeben) auf **Select** (Ausäwhlen). Geben Sie einen Wert für **Friendly Name** (Anzeigename) für diesen an und klicken Sie auf **Finish** (Fertigstellen).

23 Nun ist die Installation des Zertifikats auf dem Domänen-Controller-Server abgeschlossen. Navigieren Sie zum Installationsort des Zertifikats auf dem WDM-Server.

Installieren des Zertifikats auf dem WDM-Server

Verwenden Sie die folgenden Schritte:

1 Klicken Sie in der Taskleiste auf **Start** > **Administrative Tools** (Verwaltungstools) > **Internet Information Services (IIS) Manager** (Internetinformationsdienste (IIS)-Manager), das Fenster **IIS Manager** zu öffnen.

2 Klicken Sie im Strukturbereich auf den **Server** und doppelklicken Sie im rechten Fensterbereich auf **Server Certificates** (Serverzertifikate), um das Fenster **Server Certificates** (Serverzertifikate) zu öffnen.

3 Füllen Sie die angeforderten Informationen im Fenster **Create Certificate** (Zertifikat erstellen) aus und klicken Sie auf **Next** (Weiter), um **Online Certification Authority** (Onlinezertifizierungsstelle) zu öffnen.

4 Klicken Sie im Fenster **Online Authority Certification** (Onlinezertifizierungsstelle) unter **Specifiy Online Certification Authority** (Onlinezertifizierungsstelle angeben) auf **Select** (Ausäwhlen). Geben Sie einen Wert für **Friendly Name** (Anzeigename) für diesen an und klicken Sie auf **Finish** (Fertigstellen).

5 Nun ist die Installation des Zertifikats auf dem WDM-Server abgeschlossen.

6 Navigieren Sie nach der Installation des Zertifikats zu **Server** > **Websites** > **Rapport HTTP Server** und klicken Sie im äußersten rechten Fensterbereich auf **Bindings...** (Bindungen), um das Fenster **Site Bindings** (Sitebindungen) zu öffnen.

7 Klicken Sie im Fenster **Site Bindings** (Sitebindungen) auf **Add** (Hinzufügen), um den Vorgang **Add Site Binding** (Sitebindung hinzufügen) durchzuführen.

8 Wählen Sie unter **Add Site Binding** (Sitebindung hinzufügen) im Kombinationsfeld **SSL Certificate** (SSl-Zertifikat) das zuletzt erstellte Zertifikat aus und klicken Sie auf die Schaltfläche **OK**.

9 Um nur die HTTPS-Kommunikation zu starten, wählen Sie **SSL-Einstellungen** unter **Server** > **Websites** > **Rapport HTTP Server** aus.

10 Aktivieren Sie unter **SSL Settings** (SSL-Einstellungen) das Kontrollkästchen **Require SSL** (SSL erforderlich) und klicken Sie auf **Apply** (Übernehmen), damit die Einstellung wirksam wird.

Installieren der Stammzertifizierungsstelle in IIS 7 auf Windows Server 2012 R2

Verwenden Sie die folgenden Schritte:

- Um das Zertifikat zu installieren, müssen zwei Schritte durchgeführt werden:
  - Installieren Sie das Zertifikat auf dem Domänen-Controller-Server.
  - Installieren Sie das Zertifikat auf dem WDM-Server.

Installieren Sie das Zertifikat auf dem Domänen-Controller-Server:

Verwenden Sie die folgenden Schritte:

1 Rufen Sie den Server-Manager auf.

2 Wählen Sie im **Dashboard** >> Option 2 **Add Roles and Features** (Hinzufügen von Rollen und Funktionen) aus.

3 Im Add Roles and Features (Assistenten zum Hinzufügen von Rollen und Funktionen) wählen Sie Installationstyp als >> Role-based for feature-based installation (Rollenbasierte oder funktionsbasierte Installation) aus.

4 In der Serverauswahl >> Wählen Sie einen Server aus dem Serverpool aus (standardmäßig ist der lokale Server ausgewählt).

5 Wählen Sie im Fenster Server Role (Serverrolle) die Rolle Active Directory Certificate Services (Active Directory-Zertifikatdienste) aus.

6 Durch die Auswahl der Rolle Active Directory Certificate Services (Active Directory-Zertifikatdienst) wird der Assistent zum Hinzufügen von Rollen und Funktionen automatisch gestartet und bietet Unterfunktionen>> Klicken Sie auf die Schaltfläche Add Features (Funktionen hinzufügen).

7 Klicken Sie auf Next (Weiter) -> Next (Weiter). Belassen Sie im Fenster Features (Funktionen) alle Standardwerte und klicken Sie auf Next (Weiter).

8 Daraufhin wird das Fenster AD CS angezeigt, klicken Sie auf die Schaltfläche Next (Weiter).

9 Wählen Sie im Fenster Role Service (Rollendienst) die Optionen Certificateion Authority und Certificate Authority Web Enrolment (Zertifizierungsstelle und Zertifizierungsstellen-Webregistrierung) aus.

10 Nach der Auswahl der Option Certificate Authority Web Enrolment (Zertifizierungsstellen-Webregistrierung) wird ein anderes Fenster zum Hinzufügen von Funktionen für Funktionen angezeigt, die für das untergeordnete Fenster Zertifizierungsstellen-Webregistrierung erforderlich sind.

11 Klicken Sie im Fenster oben auf die Schaltfläche Add Feature (Funktion hinzufügen) und klicken Sie auf Next (Weiter), um das Bestätigungsfenster anzuzeigen.

12 Klicken Sie dann auf die Schaltfläche Install (Installieren), um die Rolle des AD-Zertifikats zu installieren.

13 Im Fenster Results (Ergebnisse) kann der Fortschritt der Funktionsinstallation angezeigt werden.

14 Nach erfolgreicher Installation der Rolle für die AD-Zertifikatsstelle klicken Sie auf die Schaltfläche Close (Schließen).

15 Suchen Sie dann im Server-Manager>>auf der Dashboard-Konsole unter Benachrichtigungen die Meldung zur Bereitstellungsbestätigung.

16 Klicken Sie in der Meldung zur Bereitstellungskonfiguration auf den Link „Configure Active Directory Certificate Services on local server“ (Active Directory-Zertifikatdienste auf dem lokalen Server konfigurieren).

17 Daraufhin wird das Fenster AD CS-Bestätigung>> Anmeldeinformationen geöffnet. Geben Sie die entsprechenden Anmeldeinformationen ein und klicken Sie auf die Schaltfläche Next (Weiter).

18 Aktivieren Sie unter Role Services (Rollendienste) >> die Optionen Certification Authority and Certificate Authoroity Web Enorlment (Zertifizierungsstelle und Zertifizierungsstellen-Webregistrierung) und klicken Sie dann auf Next (Weiter).

19 Aktivieren Sie je nach Anforderung im Fenster Setup Type (Setup-Typ) entweder das Optionsfeld Enterprise (Unternehmen) oder Standalone (Eigenständig) und klicken Sie auf Next (Weiter), um das Fenster Ca Type (Zertifizierungsstellentyp angeben) zu öffnen.

20 Aktivieren Sie im Fenster CA Type (Zertifizierungsstellentyp) je nach Anforderung entweder das Optionsfeld Root CA (Stammzertifizierungsstelle) oder Subordinate CA (Untergeordnete Zertifizierungsstelle) und klicken Sie auf Next (Weiter), um das Fenster Private Key (Privaten Schlüssel einrichten) zu öffnen.

21 Aktivieren Sie im Fenster Private Key (Privaten Schlüssel einrichten) je nach Anforderung entweder das Optionsfeld Create a new private key (Neuen privaten Schlüssel erstellen) oder Use existing private key (Vorhandenen privaten Schlüssel verwenden) und klicken Sie auf Next (Weiter), um das Fenster Kryptographie für ZS konfigurieren zu öffnen.

22 Wählen Sie im Fenster Kryptographie für ZS konfigurieren

- je nach Anforderung den Wert für das Feld Wählen Sie einen Kryptographiedienstanbieter (CSP) aus dem Kombinationsfeld aus.
- Geben Sie die Schlüssellänge aus dem nächsten Kombinationsfeld an.
- Wählen Sie den Wert für das Feld Wählen Sie den Hashalgorithmus zum Signieren von Zertifikaten aus, die von dieser Zertifizierungsstelle ausgestellt werden aus.
- Aktivieren oder deaktivieren Sie dann das Kontrollkästchen Administratorinteraktion bei jedem Zertifizierungsstellenzugriff auf den privaten Schlüssel zulassen.
- Klicken Sie auf die Schaltfläche Next (Weiter), um das Fenster Configure CA Name (Name der Zertifizierungsstelle konfigurieren) zu öffnen. HINWEIS: Der allgemeine Name des Zertifikats sollte mit dem Computernamen des WDM-Servers übereinstimmen.

23 Geben Sie im Fenster CA Name (Name der Zertifizierungsstelle) konfigurieren die Werte für die Felder Allgemeiner Name dieser Zertifizierungsstelle und Suffix des definierten Namens ein und klicken Sie auf Next (Weiter), um das Fenster Specifiy Validity Period (Festlegen der Gültigkeitsdauer) zu öffnen.

24 Wählen Sie im Fenster Specify Validity Period (Festlegen der Gültigkeitsdauer) die Gültigkeitsdauer für das Zertifikat aus, das für diese Zertifizierungsstelle generiert wurde, und klicken Sie auf Next (Weiter), um das Fenster Certificate Database (Zertifikatdatenbank konfigurieren) zu öffnen.

25 Wählen Sie im Fenster Certificate Database (Zertifikatdatenbank konfigurieren) den Pfad für Speicherort der Zertifikatdatenbank und Speicherort des Zertifikatdatenbankprotokolls aus und klicken Sie auf Next (Weiter), um das Fenster Confirmation (Bestätigung) zu öffnen.

26 Klicken Sie dann im Fenster Confirmation (Bestätigung) auf die Schaltfläche Configure (Bestätigen), daraufhin wird das Fortschrittsfenster angezeigt.

27 Im Fenster Results (Ergebnisse) wird die Meldung über die erfolgreiche Konfiguration von Zertifizierungsstelle und Zertifizierungsstellen-Webregistrierung angezeigt.

28 Klicken Sie auf Schaltfläche Close (Schließen), um die Konfiguration von AD-CS abzuschließen.

29 Nun ist die Installation des Zertifikats auf dem Domänen-Controller-Server abgeschlossen. Navigieren Sie zum Installationsort des Zertifikats auf dem WDM-Server.

Installieren des Zertifikats auf dem WDM-Server:

Verwenden Sie die folgenden Schritte:

1 Klicken Sie in der Taskleiste auf Start > Verwaltungstools > Internetinformationsdienste (IIS)-Manager, um das Fenster IIS Manager zu öffnen.

2 Klicken Sie im Strukturbereich auf den Server und doppelklicken Sie im rechten Fensterbereich auf Serverzertifikate, um das Fenster Serverzertifikate zu öffnen.

3 Klicken Sie auf den Link Domänen-Zertifikat erstellen auf dem Fensterbereich ganz rechts und füllen Sie die angeforderten Informationen im Fenster Zertifikat erstellen aus und klicken Sie auf Next (Weiter), um Onlinezertifizierungsstelle zu öffnen.

4 Klicken Sie im Fenster Onlinezertifizierungsstelle unter Onlinezertifizierungsstelle angeben (in Ihrer AD-Controller-Maschine oder in Ihrem Setup erstellt) auf Auswählen. Geben Sie einen Wert für Anzeigename für diesen an und klicken Sie auf Fertig stellen.

5 Nun ist die Installation des Zertifikats auf dem WDM-Server abgeschlossen.

6 Navigieren Sie nach der Installation des Zertifikats zu Server > Websites > Rapport HTTP Server und klicken Sie im äußersten rechten Fensterbereich auf Bindings (Bindungen)..., um das Fenster Site Bindings (Sitebindungen) zu öffnen.

7 Klicken Sie im Fenster Site Bindings (Sitebindungen) auf Add (Hinzufügen), um den Vorgang Add Site Binding (Sitebindung hinzufügen) durchzuführen.

8 Wählen Sie unter Add Site Bindings (Sitebindung hinzufügen) HTTPS als Typ aus und wählen Sie Zertifikatsstelle unter IP-Adresse aus, wählen Sie das zuletzt erstellte Zertifikat aus dem Kombinationsfeld SSL-Zertifikat aus und klicken Sie auf die Schaltfläche OK.

9 Um nur die HTTPS-Kommunikation zu starten, wählen Sie SSL-Einstellungen unter Server > Websites > Rapport HTTP Server aus.

10 Aktivieren Sie in den SSL-Einstellungen das Kontrollkästchen SSL erforderlich und die Optionsschaltfläche Erforderlich für das Clientzertifikat und Einstellungen anwenden.

Deinstallieren einer eigenständigen Installation von WDM

Info über diese Aufgabe

Wenn Sie eine eigenständige Installation von WDM vorgenommen haben, bei der alle Komponenten auf demselben System installiert sind, können Sie die nachstehenden Schritte zur Deinstallation von WDM befolgen.

Schritte

1. Gehen Sie zu **Start** > **Control Panel (Systemsteuerung)**.
2. Klicken Sie auf **Programs (Programme)** > **Uninstall a program (Programm deinstallieren)**.
3. Wählen Sie **WDM 5.7.3** aus der Liste der Programme und klicken Sie auf **Uninstall** (Deinstallieren).

   Der Bildschirm **Uninstallation** (Deinstallation) wird angezeigt.
4. Klicken Sie auf dem Bildschirm **Welcome** (Willkommen) auf **Next** (Weiter).
5. Geben Sie die Anmeldeinformationen für den Zugriff auf die WDM-Datenbank ein.

   Sie müssen die SQL-Anmelde-ID und Anmeldeinformationen für SQL Server oder SQL Express angeben, je nachdem, wo Sie die WDM-Datenbank installiert haben.

   Wenn Sie Sie die falschen Anmeldeinformationen angeben, wird folgende Fehlermeldung angezeigt: **Unable to connect to database** (Es konnte keine Verbindung mit der Datenbank hergestellt werden).
6. Klicken Sie auf **Next** (Weiter).

   Nachdem die Komponenten deinstalliert sind, werden Sie dazu aufgefordert, das System neu zu starten.
7. Klicken Sie auf **Restart Now** (Jetzt neu starten), um die Deinstallation abzuschließen.

Nächster Schritt

Stellen Sie nach der Deinstallation sicher, dass Sie die folgenden Checklisten erfüllen:

- Das Symbol der WyseDeviceManager 5.7.3 **WebUI** sollte vom Desktop entfernt werden.
- In IIS sollte die HApi-Anwendung unter „Rapport HTTP Server“ gelöscht werden.
- In IIS sollte die MyWDM-Anwendung unter „Rapport HTTP Server“ gelöscht werden.
- In IIS sollte die WebUI-Anwendung unter „Rapport HTTP Server“ gelöscht werden.

Deinstallieren von WDM in einem verteilten Setup

Info über diese Aufgabe

Wenn Sie WDM in einem verteilten Setup installiert haben, müssen Sie die Komponenten nacheinander auf den Systemen deinstallieren, auf denen Sie sie installiert haben.

ANMERKUNG: Sie müssen alle anderen Komponenten auf den Systemen deinstallieren, auf denen Sie sie installiert haben, bevor Sie die WDM-Datenbank deinstallieren.

Schritte

1. Melden Sie sich in Ihrem System oder den Systemen an, auf denen Sie den Verwaltungsserver, die Verwaltungskonsole, andere Dienste, die Software Repository und die Weboberfläche installiert haben.
2. Gehen Sie zu **Start** > **Control Panel (Systemsteuerung)**.
3. Klicken Sie auf **Programs (Programme)** > **Uninstall a program (Programm deinstallieren)**.
4. Wählen Sie **WDM 5.7.3** aus der Liste der Programme und klicken Sie auf **Uninstall** (Deinstallieren).

   Der Bildschirm **Uninstallation** (Deinstallation) wird angezeigt.

5 Klicken Sie auf dem Bildschirm **Welcome** (Willkommen) auf **Next** (Weiter).

6 Klicken Sie auf **Next** (Weiter), um den Deinstallationsvorgang zu starten.

7 Melden Sie sich im System an, auf dem Sie WDM installiert haben.

8 Wiederholen Sie die Schritte 2 bis 5.

9 Geben Sie die Anmeldeinformationen für den Zugriff auf die WDM-Datenbank ein.

Sie müssen die SQL-Anmelde-ID und das Kennwort für SQL Server oder SQL Express angeben, je nachdem, wo Sie die WDM-Datenbank installiert haben.

Wenn Sie die falschen Anmeldeinformationen angeben, zeigt das Programm die folgende Meldung an: *Unable to connect to database* (Keine Verbindung mit der Datenbank möglich). Stellen Sie sicher, dass Sie die korrekten Anmeldeinformationen eingeben.

10 Klicken Sie auf **Next** (Weiter), um den Deinstallationsvorgang zu starten.

11 Nachdem die Datenbank deinstalliert wurde, starten Sie das System neu, wenn Sie dazu aufgefordert werden.

5

Konfigurieren des Hochverfügbarkeits-Datenbankclustering für WDM

Hochverfügbare Cluster (auch bekannt als HA-Cluster oder Failover-Cluster) sind Gruppen von Computern, die Serveranwendungen unterstützen, die bei minimalen Ausfallzeiten zuverlässig weiter genutzt werden können. Sie funktionieren durch die Nutzung von redundanten Computern in Gruppen oder Clustern, die fortlaufende Dienste bereitstellen, wenn Systemkomponenten ausfallen.

Wenn ein Server ausfällt, der eine bestimmte Anwendung ausführt, ist die Anwendung ohne Clustering so lange nicht mehr verfügbar, bis der ausgefallene Server wieder funktioniert. HA-Clustering schafft in dieser Situation Abhilfe – durch die Erkennung von Hardware-/Softwareproblemen und den sofortigen Neustart der Anwendung auf einem anderen System, ohne dass administrativer Benutzereingriff erforderlich ist. Dieser Prozess wird als **Failover** bezeichnet.

HA-Cluster verwenden in der Regel eine private Heartbeat-Netzwerkverbindung, die zur Überwachung der Integrität und des Status der einzelnen Knoten im Cluster dient.

Die am weitesten verbreitete Größe für ein HA-Cluster ist ein aus zwei Knoten bestehender Cluster.

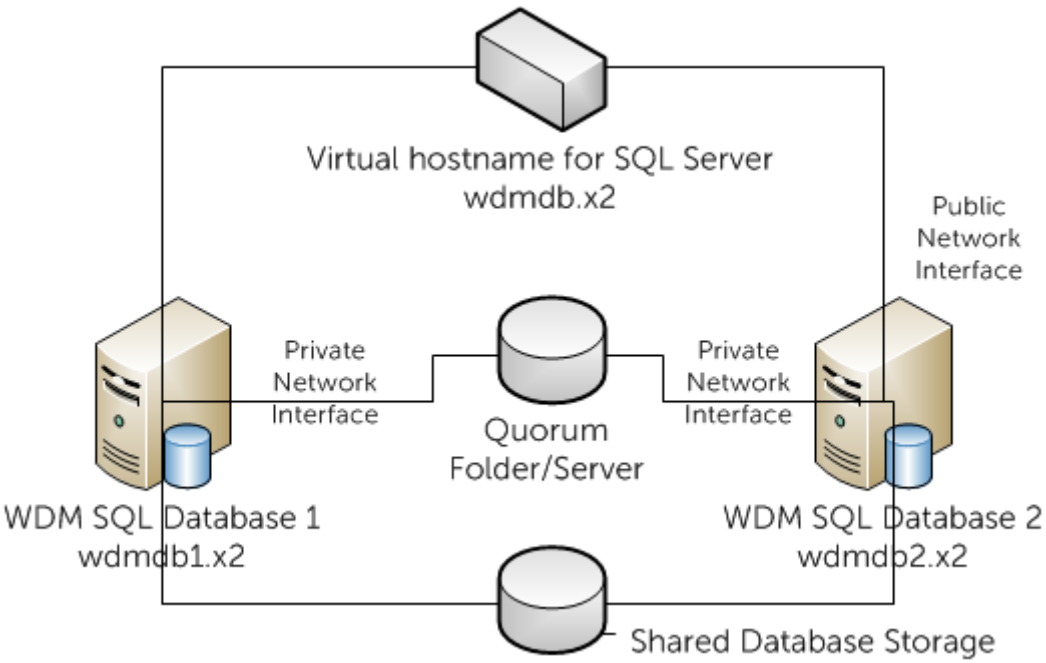


Abbildung 38. Hochverfügbarkeits-Datenbankclustering mit WDM

In diesem Abschnitt werden die Schritte zur Konfiguration von Hochverfügbarkeits-Datenbankclustering (High Availability, HA) für Dell Wyse Device Manager (WDM) Version 5.0 und höher beschrieben.

Themen:

- Erforderliche Komponenten für das Datenbankclustering
- Voraussetzungen für Datenbank-Clustering

- Konfigurieren der primären und sekundären VMs
- Erstellen eines Clusters auf dem primären Knoten
- Implementieren eines Knoten- und Dateifreigabemehrheit-Quorums
- Installieren von .NET Framework auf den primären und sekundären Knoten
- Installieren von SQL Server auf den primären und sekundären Knoten
- Post-Clustering-Verfahren
- Ausführen des HA-Konfigurationsdienstprogramms
- Hinzufügen einer Lizenz zum WDM

Erforderliche Komponenten für das Datenbankclustering

Die Hochverfügbarkeitsumgebung für WDM besteht aus folgenden Komponenten:

- **Primary Server or Primary Node** (Primärer Server oder primärer Knoten) – Dies ist eine der vier virtuellen Maschinen (VMs), auf dem Sie den Datenbankserver Microsoft SQL Server 2012 installieren müssen. Es müssen zwei Netzwerkkarten vorhanden sein, eine als öffentlich und eine als privat konfiguriert.
- **Secondary Server or Secondary Node** (Sekundärer Server oder sekundärer Knoten) - Dies ist die zweite VM und stellt eine hohe Verfügbarkeit beireit, wenn der primäre Server ausfällt. Es müssen außerdem zwei Netzwerkkarten vorhanden sein, eine als öffentlich und eine als privat konfiguriert.
- **Server for the Quorum folder** (Server für den Quorum-Ordner) **-** Dies ist die dritte der vier VMs und wird zur Erstellung des Quorum-Ordners benötigt.
- **WDM-Server** - Dies ist die vierte VM, auf der Sie WDM installieren müssen.

Voraussetzungen für Datenbank-Clustering

Für Datenbank-Clustering müssen folgende Voraussetzungen erfüllt werden:

- Vier VMware-VMs (virtuelle Maschinen), von denen zwei VMs jeweils zwei Netzwerkadapter aufweisen sollten.
- Unterstützte Version von Microsoft SQL Server-Datenbank (eigenständige Version). Weitere Informationen zu den unterstützten Datenbanken finden Sie unter Support-Informationen.

  ANMERKUNG: Die in diesem Handbuch behandelten Schritte für das Datenbank-Clustering werden unter Microsoft SQL Server 2012 durchgeführt. Datenbank-Clustering wird jedoch auch auf anderen unterstützten Versionen von SQL Server unterstützt.

  Alle VMs sollten mit einer Active Directory (AD)-Domäne verknüpft werden.
- Auf allen vier VMs sollte Windows Server 2008 R2 Enterprise oder höher installiert sein.

ANMERKUNG: Sie können SQL Server Express für das Database-Clustering nicht verwenden.

Konfigurieren der primären und sekundären VMs

Nach dem Erstellen der VMs auf dem Server müssen Sie diese so konfigurieren, dass Clustering unterstützt wird. Sie müssen sowohl die primären als auch die sekundären Knoten konfigurieren, indem Sie die folgenden Schritte ausführen:

Info über diese Aufgabe

So konfigurieren Sie die primären und sekundären VMs:

Schritte

1. Starten Sie den vSphere-Client auf einem beliebigen System im Netzwerk und wählen Sie die VM aus.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Edit Settings** (Einstellungen bearbeiten) aus. Klicken Sie auf **Add** (Hinzufügen) und fügen Sie eine weitere Netzwerkkarte hinzu (auch bezeichnet als Knoten).
3. Wählen Sie auf dem Bildschirm **Add Hardware** (**Hardware hinzufügen)** die Option **Ethernet Adapter (Ethernet-Adapter)** aus und klicken Sie auf **Next** (Weiter).

4 Wählen Sie das Subnetz aus der Dropdown-Liste **Network Label** (Netzwerkbezeichnung) aus und klicken Sie auf **Next** (Weiter).

5 Klicken Sie auf **Finish (Fertigstellen).**

6 Überprüfen Sie auf dem Bildschirm **VM Properties** (**VM-Eigenschaften**), ob zwei Knoten vorhanden sind.

7 Öffnen Sie den Bildschirm **Network Connections** (Netzwerkverbindungen) über den Pfad **Control Panel** (Systemsteuerung) → **Network and Panel** (**Netzwerk und Internet**) → **Network Connections** (Netzwerkverbindungen) und benennen Sie die Netzwerkverbindungen zu **Privat**e (Privat) und **Public** (Öffentlich) um.

ANMERKUNG: Es müssen zwei Subnetze für zwei Netzwerkkarten vorhanden sein, d. h. ein Subnetz für das öffentliche Netzwerk (PDB) und ein Subnetz für das private Netzwerk (PDB). Dasselbe gilt für die zwei Netzwerkkarten auf dem SDB-Server.

8 Stellen Sie sicher, dass die Option **Public Network** (**Öffentliches Netzwerk**) im Fenster **Advanced Settings** (**Erweiterte Einstellungen**) an erster Stelle steht.

9 Um das Fenster **Advanced Settings** (**Erweiterte Einstellungen**) zu öffnen, drücken Sie die Alt-Taste, um auf das Menü **Advanced** (Erweitert) auf dem Bildschirm **Network Connections** (Netzwerkverbindungen) zuzugreifen, und wählen Sie die Option **Advanced Settings** (**Erweiterte Einstellungen**) aus.

10 Wählen Sie auf dem Bildschirm N**etwork Connections** (Netzwerkverbindungen) die Option **Public** (**Öffentlich)** aus. Klicken Sie mit der rechten Maustaste auf diese Option und wählen Sie **Properties** (Eigenschaften) aus.

11 Wählen Sie im Fenster **Advanced Settings** (Erweiterte Einstellungen) die Option **IPv4** aus und klicken Sie auf **Properties** (Eigenschaften).

12 Geben Sie die Werte für **IP address, Subnet mask, Default gateway und the Preferred DNS server** (IP-Adresse, Subnetzmaske, Standardgateway und Bevorzugter DNS-Server) ein. Klicken Sie auf OK.

13 Wiederholen Sie die Schritte 10 und 11 für das private Netzwerk.

14 Stellen Sie sicher, dass das private Netzwerk nur die IP-Adresse und die Subnetzmaske enthält. Das Standard-Gateway oder die DNS-Server dürfen nicht definiert werden.

15 Stellen Sie sicher, dass die Server über dieses Netzwerk miteinander kommunizieren können, sodass die Knoten über das Netzwerk miteinander kommunizieren können.

16 Starten Sie den Server-Manager unter **Start** → **Administrative Tools** (Verwaltungstools). Wählen Sie **Features** (Funktionen) aus.

17 Klicken Sie auf **Add Features** (Features hinzufügen), um den **Add Features wizard** (Assistenten zum Hinzufügen von Features) zu starten.

18 Wählen Sie **Failover Clustering** (Failoverclustering) aus und klicken Sie auf **Next** (Weiter).

19 Stellen Sie sicher, dass die Option **Failoverclustering** auf dem Bildschirm, Anzeige; Dialog; Display **Confirm Installation Selections** (Installationsauswahl bestätigen) angezeigt wird. Klicken Sie auf **Install** (Installieren). Es wird der Installationsfortschritt angezeigt.

20 Überprüfen Sie nach Abschluss der Installation die Installationsergebnisse und klicken Sie auf **Close** (Schließen).

Nächster Schritt

Starten Sie den Server nach der Failoverclustering-Installation neu.

Überprüfen einer Konfiguration

Info über diese Aufgabe

Nachdem Sie Failoverclustering installiert haben, müssen Sie die Konfiguration auf dem primären Knoten überprüfen. So überprüfen Sie die Konfiguration:

Schritte

1 Starten Sie unter **Start** → **Verwaltungstools** den Server-Manager des primären Knotens.

2 Wählen Sie unter **Funktionen** den **Failovercluster-Manager** aus.

3 Klicken Sie auf **Konfiguration überprüfen**, um den Assistenten zu starten.

4 Klicken Sie auf **Weiter**, um die primären und sekundären Knoten hinzuzufügen.

5 Geben Sie den Hostnamen des primären Knotens ein.

6 Klicken Sie auf **Hinzufügen** und wählen Sie die Server aus. Der Bildschirm zeigt beim Hinzufügen der Server die folgende Meldung: *„Der Vorgang dauert länger als erwartet“*. Sie müssen einige Minuten warten, bis die Server hinzugefügt werden.

7 Nachdem die Server ausgewählt wurden, werden sie unter „Ausgewählte Server“ angezeigt. Klicken Sie auf **Weiter.**

8 Für Cluster mit mehreren Standorten muss keine Speicherüberprüfung durchgeführt werden. Um die Speicherüberprüfung zu überspringen, klicken Sie auf die entsprechende Option, um nur die von Ihnen ausgewählten Tests auszuführen, und klicken Sie dann auf **Weiter.**

9 Deaktivieren Sie auf dem Bildschirm **Testauswahl** die Option **Speicher** und klicken Sie auf **Weiter**, um fortzufahren.

Der Bildschirm „Bestätigung“ wird angezeigt.

10 Klicken Sie auf **Weiter**, um die Ausführung der Überprüfungstests auf den primären und sekundären Knoten (in diesem Fall Cluster1 und Cluster2) zu starten. Der Status der Überprüfungstests wird auf dem Bildschirm angezeigt.

11 Sehen Sie sich die Zusammenfassung der Überprüfung an und klicken Sie auf **Fertig stellen**.

Erstellen eines Clusters auf dem primären Knoten

Info über diese Aufgabe

Nachdem Sie die **Failovercluster-Manager**-Funktion auf dem primären Knoten installiert und überprüft haben, können Sie einen Cluster erstellen.

So erstellen Sie einen Cluster auf dem primären Knoten:

Schritte

1 Starten Sie den Server-Manager auf dem primären Knoten, wählen Sie **Failovercluster-Manager** unter **Funktionen** aus und klicken Sie auf **Cluster erstellen**.

2 Klicken Sie auf **Weiter** im Assistenten.

3 Klicken Sie zum Fortfahren auf **Weiter** und geben Sie auf dem Bildschirm **Server auswählen** den Hostnamen des primären Knoten ein. Klicken Sie anschließend auf **Hinzufügen**, um den Server hinzuzufügen.

4 Geben Sie den Namen des sekundären Knoten ein und klicken Sie auf **Hinzufügen**.

5 Nachdem die Server hinzugefügt wurden, klicken Sie auf **Next (Weiter)**, um fortzufahren. Sie werden aufgefordert, Ihr Cluster zu validieren. Wählen Sie **No (Nein)** aus, da Ihr Cluster bereits validiert wurde.

6 Wählen Sie die zweite Option auf dem Bildschirm aus und klicken Sie auf **Weiter**, um fortzufahren.

7 Geben Sie einen Namen für das Cluster und eine IP für die Cluster-Verwaltung ein. Der Name, den Sie angeben, wird für die Verwaltung des Clusters verwendet. Er sollte nicht mit dem Namen der SQL-Cluster-Ressource übereinstimmen, die Sie später erstellen. Geben Sie **WINCLUSTER** als Namen des Clusters ein. Geben Sie anschließend die IP-Adresse ein. Klicken Sie auf **Next** (Weiter), um fortzufahren.

> ANMERKUNG: **Dies ist auch der Computername, für den Sie die Berechtigungen für das Dateifreigabemehrheits-Quorum gewähren müssen, das später in diesem Dokument beschrieben wird. Weitere Informationen finden Sie unter Implementieren eines Knoten- und Dateifreigabemehrheit-Quorums.**

8 Bestätigen Sie den Vorgang und klicken Sie auf **Weiter**.

Der Cluster-Bildungsfortschritt wird auf dem Bildschirm angezeigt. Wenn Sie alle Schritte korrekt ausgeführt haben, wird die Cluster-Bildung erfolgreich abgeschlossen. Wenn ein gelbes Warnsymbol auf dem Bildschirm angezeigt wird, bedeutet dies, dass die Cluster-Bildung erfolgreich war, aber mit Warnungen abgeschlossen wurde.

9 Klicken Sie auf **View Report (Bericht anzeigen)** zur Anzeige der Warnungen während der Cluster-Bildung. Der Bericht wird angezeigt und Warnungen werden gelb markiert.

10 Ignorieren Sie die Warnmeldungen und klicken Sie auf **Fertig stellen**, um den Vorgang der Clustererstellung abzuschließen.

Implementieren eines Knoten- und Dateifreigabemehrheit-Quorums

Ein Quorum ist ein Design zur Verarbeitung von Szenarien, bei denen ein Problem mit der Kommunikation zwischen verschiedenen Sätzen von Clusterknoten auftritt, sodass zwei Server nicht versuchen, eine Ressourcengruppe gleichzeitig zu hosten und gleichzeitig auf dasselbe Laufwerk zu schreiben. Durch dieses Quorumkonzept zwingt das Cluster den Clusterdienst, in einer der Knotenteilgruppen zu stoppen, um sicherzustellen, dass es nur einen Besitzer einer bestimmten Ressourcengruppe gibt. Die Quorumkonfiguration „Knoten- und Dateifreigabemehrheit“ wird normalerweise bei Clustern mit mehreren Standorten verwendet. Diese Konfiguration kommt zum Einsatz, wenn eine gerade Anzahl von Knoten im Cluster vorhanden ist, sodass sie synonym zum Modus „Knoten- und Datenträgermehrheit“ verwendet werden kann. In dieser Konfiguration erhält jeder Knoten eine Stimme und zusätzlich erhält eine Remote-Dateifreigabe eine Stimme.

Info über diese Aufgabe

So konfigurieren Sie einen Knoten- und Dateifreigabemehrheit-Quorum:

Schritte

1. Wählen Sie die für die Erstellung des Quorum-Ordners vorgesehene VM aus, erstellen Sie einen Ordner mit dem Namen **Quorum** und geben Sie den Ordnerpfad frei.
2. Klicken Sie mit der rechten Maustaste auf den Ordner **Quorum** und wählen Sie **Freigeben für → Bestimmte Personen** aus.
3. Wählen Sie im Fenster **File Sharing (Dateifreigabe) Everyone (Jeder)** aus. Wählen Sie die **Read/Write permission (Lese-/Schreibberechtigung)** aus und klicken Sie auf **Share (Freigeben)**.

   Der Ordner wird als **\\<Name der VM>\Quorum** freigegeben.
4. Sie müssen nun den Quorumtyp ändern. Starten Sie den **Server-Manager** auf dem primären Knoten und wählen Sie dann **Failover Cluster Manager (Failover für Cluster-Manager durchführen)** unter **Features (Funktionen)** aus.
5. Klicken Sie mit der rechten Maustaste auf Ihren Cluster und wählen Sie **Weitere Aktionen → Clusterquorumeinstellungen konfigurieren** aus.
6. Wählen Sie die Option **Knoten- und Dateifreigabemehrheit (für Cluster mit speziellen Konfigurationen)** aus und klicken Sie auf **Weiter**.
7. Geben Sie den Pfad des freigegebenen Ordners ein, den Sie auf der dritten VM erstellt haben, und klicken Sie auf **Weiter**.
8. Bestätigen Sie den Pfad des freigegebenen Ordners und klicken Sie auf **Weiter**.

   Die Quorumeinstellungen für den Cluster wurden erfolgreich konfiguriert.
9. Klicken Sie auf **Fertig stellen**, um den Vorgang abzuschließen und die Quorumkonfiguration für den Cluster anzuzeigen.

Installieren von .NET Framework auf den primären und sekundären Knoten

Info über diese Aufgabe

Wenn Sie die eigenständige Version von SQL Server 2012 (oder eine beliebige andere unterstützte Version von SQL Server) auf den primären und sekundären Knoten installieren, muss Microsoft .NET Framework installiert sein.

So installieren Sie .NET Framework:

Schritte

1. Starten Sie **Server-Manager** auf den VMs, die Sie für die primären und sekundären Knoten vorgesehen haben.
2. Klicken Sie unter **Server-Manager** auf **Funktionen**, um den **Assistenten zum Hinzufügen von Funktionen** zu starten, und wählen Sie **.NET Framework 3.5.1-Features** aus.
3. Klicken Sie auf **Weiter**. Sie werden dazu aufgefordert, die erforderlichen Rollendienste und -funktionen für die Installation der .NET Framework 3.5.1-Features zu installieren.
4. Klicken Sie auf **Erforderliche Rollendienste hinzufügen**. Die Option .NET-Erweiterbarkeit ist standardmäßig ausgewählt. Klicken Sie auf **Next** (Weiter), um fortzufahren.
5. Bestätigen Sie die Auswahl der Installationseinstellungen und klicken Sie auf **Installieren**.
6. Nachdem die ausgewählten Komponenten installiert wurden, werden die Installationsergebnisse angezeigt.
7. Klicken Sie auf **Schließen**, um die .NET Framework-Installation abzuschließen.

Installieren von SQL Server auf den primären und sekundären Knoten

Die Installation von SQL Server auf beiden Knoten und die Konfiguration zum Betrieb in einem Cluster sind wichtige Schritte beim Setups eines Hochverfügbarkeits-Datenbank-Clusters. In diesem Abschnitt werden die Schritte zum Installieren und Konfigurieren der eigenständigen Version von SQL Server 2012 auf beiden Knoten beschrieben. Wenn Sie eine der unterstützten Versionen von SQL Server installieren möchten, finden Sie in den Installationsanweisungen von Microsoft weitere Informationen.

So installieren Sie eine eigenständige Version von SQL Server 2012 auf beiden Knoten:

1. Starten Sie das SQL Server 2012-Installationsmedium.
2. Klicken Sie auf **Installation** und wählen Sie **New SQL Server stand-alone installation or add features to an existing installation** (Neue eigenständige SQL Server-Installation oder Hinzufügen von Funktionen zu einer vorhandenen Installation) aus.

3 Stellen Sie sicher, dass auf dem Bildschirm „Setup Support Rules“ (Setupunterstützungsregeln) keine Fehler angezeigt werden. Klicken Sie auf **Next** (Weiter), um fortzufahren.

4 Geben Sie den Produktschlüssel ein und klicken Sie auf **Next** (Weiter).

5 Überprüfen Sie die Produktaktualisierung und klicken Sie auf **Next** (Weiter).

6 Nehmen Sie die Lizenzvereinbarung an und klicken Sie auf **Next** (Weiter).

7 Wählen Sie die Option **SQL Server Feature Installation** (SQL Server-Funktionsinstallation) aus und klicken Sie auf „Next“ (Weiter).

8 Wählen Sie auf dem Bildschirm **Feature Selection** (Featureauswahl) die Funktionen **Database Engine Services** (Datenbankmoduldienste) und alle darunter befindlichen Funktionen aus.

9 Wählen Sie die Funktion „Management Tools – Basic“ (Verwaltungstools – Einfach) und die darunter befindliche Funktion aus. Klicken Sie auf **Next** (Weiter).

10 Stellen Sie sicher, dass auf dem Bildschirm „Installation Rules“ (Installationsregeln) keine Fehler angezeigt werden. Klicken Sie auf **Next** (Weiter).

11 Stellen Sie sicher, dass auf dem Bildschirm **Instance Configuration** (Instanzkonfiguration) die Option **Default instance** (Standardinstanz) aktiviert ist.

12 Klicken Sie auf **Next** (Weiter), um den erforderlichen Speicherplatz anzuzeigen.

13 Klicken Sie auf **Next** (Weiter), um die Serverkonfiguration anzuzeigen.

14 Geben Sie die Domänen-Anmeldedaten für die Serverkonfiguration ein und klicken Sie auf **Next** (Weiter).

15 Wählen Sie auf dem Bildschirm „Database Engine Configuration“ (Datenbankmodulkonfiguration) **Mixed Mode** (Gemischter Modus) aus und geben Sie das SQL-Administratorkennwort ein. Klicken Sie anschließend auf **Add Current User** (Aktuellen Benutzer hinzufügen).

16 Klicken Sie im Fenster **Error Reporting** (Fehlerberichterstellung) auf **Next** (Weiter).

17 Klicken Sie auf **Next** (Weiter) und stellen Sie sicher, dass bei den Installations- und Konfigurationsregeln keine Fehler angezeigt werden.

18 Klicken Sie auf **Install** (Installieren), um mit dem Installationsprozess zu beginnen.

19 Nach Abschluss der Installation wird der Installationsstatus angezeigt. Zeigen Sie den Status an und klicken Sie auf **Close** (Schließen), um die Installation abzuschließen.

ANMERKUNG: Wenn bei der Installation von SQL Server eine Windows-Firewallwarnung angezeigt wird, können Sie die Warnung ignorieren und mit der Installation fortfahren. Falls erforderlich, können Sie Port 1433 zu der SQL Server-Firewall-Ausnahme hinzufügen.

Installieren des SQL Server-Failoverclusters auf dem primären Knoten

Nach der Installation von SQL Server 2012 sowohl auf dem primären als auch auf dem sekundären Knoten müssen Sie beide Knoten zur Unterstützung des Failover-Clustering konfigurieren.

So installieren Sie den SQL Server 2012-Failovercluster auf dem primären Knoten:

1 Starten Sie das SQL Server 2012-Installationsmedium.

2 Klicken Sie auf **Installation** und wählen Sie **New SQL Server failover cluster installation** (Neue SQL Server-Failovercluster-Installation).

3 Stellen Sie sicher, dass auf dem Bildschirm **Setup Support Rules** (Setupunterstützungsregeln) keine Fehler angezeigt werden. Klicken Sie auf **OK**.

4 Geben Sie den Produktschlüssel ein und klicken Sie auf **Next** (Weiter).

5 Nehmen Sie die Lizenzbedingungen an und klicken Sie auf **Next** (Weiter).

6 Prüfen Sie die Produktaktualisierungen und klicken Sie auf **Next** (Weiter).

7 Stellen Sie sicher, dass auf dem Bildschirm **Setup Support Rules** (Setupunterstützungsregeln) keine Fehler angezeigt werden. Ignorieren Sie die Warnhinweise und klicken Sie auf **Next** (Weiter).

8 Wählen Sie die Option **SQL Server Feature Installation** (SQL Server-Funktionsinstallation) auf dem Bildschirm **Setup Role** (Setup-Rolle) aus und klicken Sie auf **Next** (Weiter).

9 Wählen Sie alle Optionen unter Instance Features (Instanzfunktionen) → **Database Engine Services** (Datenbankmoduldienste) und **Shared Features (**Freigegebene Funktionen**)** → **Client Tools Connectivity** (Konnektivität der Clienttools) auf dem Bildschirm **Feature Selection** (Funktionsauswahl) aus. Klicken Sie auf **Next** (Weiter).

10 Stellen Sie sicher, dass auf dem Bildschirm **Feature Rules** (Funktionsregeln) keine Fehler angezeigt werden. Klicken Sie auf **Next** (Weiter).

11 Geben Sie auf dem Bildschirm **Instance Configuration** (Instanzkonfiguration) folgende Informationen ein:

- **SQL Server-Netzwerkname** - WINCLUSTER
- **Benannte Instanz** - WDMCLUST
- **Instanz-ID** - WDMCLUST

Klicken Sie auf **Next** (Weiter).

12 Überprüfen Sie den Bildschirm **Disk Space Requirements** (Erforderlicher Speicherplatz)und klicken Sie auf **Next** (Weiter).

13 Behalten Sie die Standardeinstellungen auf dem Bildschirm **Cluster Resource Group** (Clusterressourcengruppe) bei und klicken Sie auf **Next** (Weiter).

14 Da Sie ein Dateifreigabemehrheit-Clustering konfiguriert haben, müssen Sie ein Laufwerk auswählen. Klicken Sie auf **Next** (Weiter) auf dem Bildschirm **Cluster Disk Selection** (Cluster-Laufwerk-Auswahl).

15 Aktivieren Sie auf dem Bildschirm **Cluster Network Configuration** (Netzwerkkonfiguration für Cluster) die Option **IP4** und geben Sie die IP-Adresse für das SQL-Failovercluster ein. Klicken Sie anschließend auf **Next**(Weiter), um mit dem Bildschirm **Server Configuration** (Serverkonfiguration) fortzufahren.

16 Geben Sie die Domänenanmeldedaten für den SQL Server-Agent und das SQL Server-Datenbankmodul ein und klicken Sie auf **Next** (Weiter).

17 Wählen Sie auf dem Bildschirm **Database Engine Configuration** (Datenbankmodulkonfiguration) die Option **Mixed Mode** (Gemischter Modus) (SQL Server-Authentifizierung und Windows-Authentifizierung) aus und geben Sie das SQL Administratorkennwort ein.

18 Klicken Sie auf **Add Current User** (Aktuellen Benutzer hinzufügen), um den Administrator hinzuzufügen, und klicken Sie auf **Weiter**.

19 Sie werden aufgefordert, ein SQL Failovercluster zu installieren. Klicken Sie auf **Yes** (Ja) in der Eingabeaufforderung.

20 Klicken Sie auf die Registerkarte **Data Directories** (Datenverzeichnisse) im Bildschirm **Database Engine Configuration** (Datenbankmodul-Konfiguration). Geben Sie im Speicherort für das Datenstammverzeichnis **\\<*Name of the Quorum VM*>\quorum** ein. Klicken Sie auf **Next** (Weiter).

21 Überprüfen Sie den Bildschirm **Error Reporting** (Fehlerberichte) und klicken Sie auf **Next** (Weiter). Sie können die Warnungen ignorieren.

22 Stellen Sie sicher, dass keine Fehler auf dem Bildschirm **Cluster Installation Rules** (Regeln für die Clusterinstallation) angezeigt werden. Klicken Sie auf **Next** (Weiter).

23 Klicken Sie auf **Install** (Installieren), um mit der Installation zu beginnen.

24 Der Bildschirm mit dem **Installationsfortschritt** zeigt den Fortschritt der Installation an. Klicken Sie auf **Next** (Weiter), nachdem die Installation abgeschlossen ist.

25 Klicken Sie auf **Close** (Schließen), um die Installation abzuschließen. Der **Failovercluster-Manager** muss im **Server-Manager** unter **Features** (Funktionen) angezeigt werden.

Post-Clustering-Verfahren

Info über diese Aufgabe

Dieser Abschnitt behandelt die verschiedenen Schritte, die Sie ausführen müssen, nachdem Sie den Cluster-Setup abgeschlossen haben. Diese Schritte aktivieren Ihren Cluster für eine reibungslose Funktion.

Gehen Sie wie folgt vor:

Schritte

1 Stellen Sie in beiden Clusterknoten sicher, dass die SQL Server-Dienste mit den Domänen-Anmeldedaten gestartet wurden.

2 Starten Sie den **SQL Server-Konfigurationsmanager** und wählen Sie **SQL Server Services (SQL Server-Dienste) → SQL Server** aus. Klicken Sie mit der rechten Maustaste, und wählen Sie **Properties** (Eigenschaften).

3 Überprüfen Sie die Domänen-Anmeldedaten und klicken Sie auf **OK**.

4 Klicken Sie auf beiden Knoten auf die Registerkarte **AlwaysOn High Availability** (hohe Verfügbarkeit (AlwaysOn)) und wählen Sie die **Enable AlwaysOn Availability Groups** (AlwaysOn-Verfügbarkeitsgruppen aktivieren) aus. Klicken Sie auf **OK**.

5 Installieren Sie die WDM-Datenbank auf VMs, die Sie als primäre und sekundäre Knoten des Clusters vorgesehen haben.

6 Führen Sie das folgende Skript auf der Datenbank aus:

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

7 Stellen Sie bei der Installation der WDM-Komponenten ohne Datenbank sicher, dass Sie den Namen des SQL-Datenbankclusters in das Feld für die Server-IP-Adresse eingeben.

8 Erstellen Sie dieselbe Verzeichnisstruktur zum Datenbankspeicherort sowohl auf dem primären als auch auf dem sekundären Knoten. Wenn die Datenbank beispielsweise auf **C:\Program Files\WYSE\WDM\Database** im primären Knoten gespeichert ist, müssen Sie dieselbe Struktur auch auf dem sekundären Server erstellen.

9 Starten Sie SQL Server Management Studio auf dem primären Knoten. Melden Sie sich mit dem standardmäßigen SQL-Benutzernamen und das Kennwort an.

10 Klicken Sie mit der rechten Maustaste auf die **RapportDB** -Datenbank und wählen Sie **Properties** (Eigenschaften) aus.

11 Ändern Sie auf dem Bildschirm **Database Properties** (Datenbankeigenschaften) die Option **Recovery Model** (Wiederherstellungsmodell) zu **Full** (Vollständig).

12 Klicken Sie mit der rechten Maustaste auf „RapportDB“ und wählen Sie **Tasks (Aufgaben)→ Backup** (Sicherung) aus, um eine Sicherung von RapportDB zu erstellen.

13 Behalten Sie die Standardeinstellungen auf dem Bildschirm **Backup Database** (Datenbank sichern) bei und klicken Sie auf **OK**.

14 Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **AlywaysOn High Availability** (**Hohe Verfügbarkeit (AlwaysOn)**) und wählen Sie **New availability Group Wizard (Assistent für neue Verfügbarkeitsgruppe).**

15 Klicken Sie auf dem Bildschirm **New availability Group Wizard (Assistent für neue Verfügbarkeitsgruppe)** auf **Next** (Weiter).

16 Geben Sie einen Namen für die Verfügbarkeitsgruppe wie etwa **Rapport_cluster** ein und klicken Sie auf **Next** (Weiter).

17 Wählen Sie die Datenbank aus und klicken Sie auf **Next (Weiter)**.

18 Klicken Sie auf **Add Replica** (**Replikat hinzufügen**) und aktivieren Sie die Kontrollkästchen **Automatic Failover (up to 2)** (**Automatisches Failover (max. 2)**) und **Synchronous commit (upt to 3)** (**Synchroner Commit (max. 3)**.)

Wiederholen Sie diesen Schritt für den sekundären Knoten.

19 Klicken Sie auf **Next (Weiter).**

20 Wählen Sie die Option **Full** (Vollständig) aus und geben Sie den Pfad des freigegebenen Ordners ***<Name des Quorum-Moduls>* \Quorum** an. Klicken Sie auf **Next** (Weiter).

21 Stellen Sie sicher, dass auf dem Bildschirm **Validation** (**Überprüfung**) keine Fehler angezeigt werden. Klicken Sie auf **Next** (Weiter).

22 Falls Warnungen auf dem Bildschirm angezeigt werden, können Sie diese ignorieren und mit der Installation fortfahren.

23 Klicken Sie auf **Finish** (Fertigstellen), um die Installation von **New Availability Group** (Neue Verfügbarkeitsgruppe) abzuschließen.

24 Im Fortschrittsfenster wird der Fortschritt der Installation angezeigt. Klicken Sie auf **Next** (Weiter), nachdem die Installation abgeschlossen ist.

25 Sehen Sie sich die Ergebnisse an und klicken Sie auf **Close** (Schließen).

26 Die primären und sekundären Knoten werden in SQL Server Management Studio angezeigt.

27 Fahren Sie den sekundären Knoten herunter und stellen Sie sicher, dass der primäre Knoten im Cluster ausgeführt wird.

28 Starten Sie SQL Server Management Studio auf dem primären Knoten. Melden Sie sich mit dem standardmäßigen SQL-Benutzernamen und das Kennwort an.

29 Klicken Sie auf den Knoten **Security** (Sicherheit), wählen Sie **Login** (Anmeldung) aus, klicken Sie mit der rechten Maustaste auf **New Login** (Neue Anmeldung), um einen Rapport-Benutzer zu erstellen. Dieser Schritt ist wichtig, damit WDM funktioniert, während Sie den Benutzer für die SQL Server-Authentifizierung erstellen.

30 Wählen Sie **Server Roles** (Server Roles), aktivieren Sie das Kontrollkästchen **sysadmin** und klicken Sie auf **OK**.

31 Zeigen Sie den **Rapport**-Benutzer in **SQL Server Management Studio** an.

32 Wiederholen Sie die Schritte 28 – 31 auf dem sekundären Knoten.

Nächster Schritt

ANMERKUNG: Falls ein Failover von der primären zur sekundären Datenbank auftritt, müssen Sie die WDM-Benutzeroberfläche neu starten.

Ausführen des HA-Konfigurationsdienstprogramms

Info über diese Aufgabe

WDM muss mit dem Cluster verbunden werden, um einen einwandfreien Betrieb innerhalb des Clusters zu ermöglichen, und sicher zu stellen, dass keine Ausfallzeiten auftreten.

Das Dienstprogramm für die Hochverfügbarkeitskonfiguration (HA) ist verfügbar, nachdem Sie WDM auf einem anderen separaten Knoten als den primären und sekundären Knoten installiert haben.

Schritte

1 Melden Sie sich beim System an, auf dem WDM installiert wurde.

2 Starten Sie die **HAConfigureUtility** unter**Start** > **Alle Programme** > **Dell Wyse Device Manager** > **Utilities (Dienstprogramme)**.

3 Geben Sie folgende Informationen ein:

- **Configure Setup As (Setup konfigurieren als)** – Wählen Sie **Cluster** aus der Dropdown-Liste aus.
- **Database Name (Datenbankname)** – Dieser Wert wird standardmäßig angezeigt und kann nicht bearbeitet werden.
- **Database Server (Datenbankserver)** – Geben Sie den Hostnamen des Datenbankclusters an. Z. B. **WDMCLUSTER**.
- **Database User Name (Name des Datenbankbenutzers)** – Geben **rapport** als Datenbankbenutzer an.
- **Database Password (Datenbankkennwort)** - Geben Sie das Kennwort des rapport-Benutzers an.

4 Klicken Sie auf **Configure (**Konfigurieren).

Die Verbindungsdaten werden im unteren Bereich des Dienstprogramms angezeigt.

Hinzufügen einer Lizenz zum WDM

Info über diese Aufgabe

Damit WDM funktioniert ist eine Lizenz erforderlich. Der Lizenzierungscode wird basierend auf der Datenbank erzeugt. WDM wird normalerweise auf einer eigenständigen Datenbank installiert und dann in ein Cluster verschoben. Daher müssen Sie den Lizenzcode nach Abschluss des Cluster-Setup erneut für das Cluster erstellen.

So fügen Sie eine Lizenz auf WDM für den WDM-Server hinzu:

Schritte

1 Starten Sie Wyse Device Manager (WDM). Der folgende Fehler wird angezeigt: *„Application Function: ScopeItems_Expand: 13 Type mismatch“ (Anwendungsfunktion: ScopeItems_Expand: 13 Typabweichung)*.

2 Klicken Sie auf **OK** und fügen Sie die Lizenz von der WDM-Konsole hinzu.

3 Um ein Failover zu initiieren, fahren Sie die Datenbank auf dem primären Knoten herunter und starten Sie die WDM-Konsole neu.

6

Konfigurieren des Lastenausgleichs

Wenn Sie WDM zur Verwaltung von Thin Clients in einer sehr großen Unternehmensumgebung verwenden, kann ein einzelner WDM-Verwaltungsserver nicht für die Unterstützung einer so großen Anzahl von Geräten skaliert werden. Es können Probleme oder Verzögerungen bei Clientanmeldungen, geplanten Ausführungen oder der Ausführung von Befehlen in Echtzeit auftreten.

Mithilfe von Lastenausgleich können diese Probleme weitestgehend gelöst werden. In diesem Setup können Sie mehrere Instanzen von WDM-Verwaltungsservern auf verschiedenen Systemen installieren und ausführen und die Lastenausgleichsfunktion zwischen ihnen konfigurieren. WDM verwendet Microsoft Application Request Routing (ARR) für die IIS 7-Funktion für den Lastenausgleich zwischen Verwaltungsservern. In diesem Abschnitt wird die Einrichtung und Konfiguration von Lastenausgleich beschrieben.

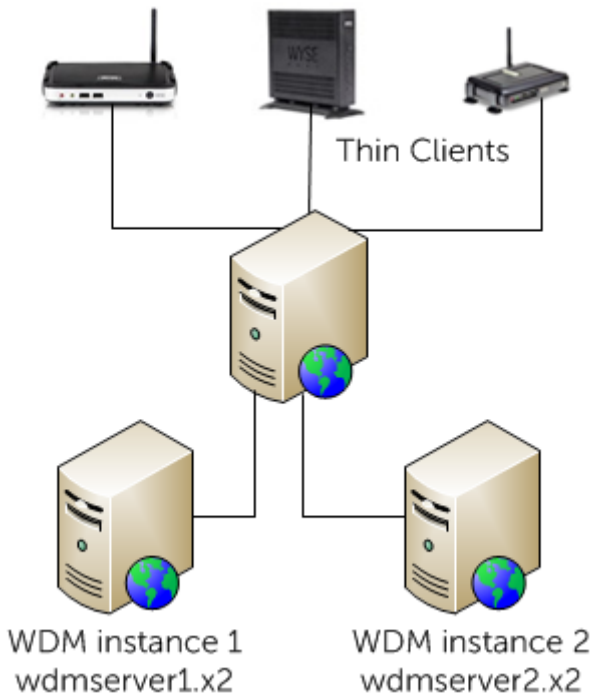


Abbildung 39. Setup des WDM-Lastenausgleichs

Themen:

- Einrichten des ARR-Proxyservers
- Installieren von WDM-Komponenten
- Konfigurieren des Lastausgleichs für ThreadX 4.x-Geräte
- Konfigurieren des Lastenausgleichs für ThreadX 5.x-Geräte

Einrichten des ARR-Proxyservers

Der Application Routing Request (ARR)-Proxyserver ist die wichtigste Komponente beim Lastausgleich. Dieser Server empfängt die Anfragen von Thin Client-Systemen und leitet sie zu den unterschiedlichen WDM-Verwaltungsservern weiter.

Voraussetzungen

Vor dem Einrichten des ARR-Proxyservers müssen Sie Folgendes sicherstellen:

- Das gesamte Setup sollte auf Windows Server 2008 R2 oder höher erfolgen.
- Installieren Sie alle Komponenten von WDM auf einem Server.
- Installieren Sie nur den WDM-Verwaltungsserver und den ThreadX 4.x-Dienst auf einem anderen Server.

ANMERKUNG: Sie können den ARR-Proxyserver sowie die WDM-Managementserver in verschiedenen Subnetzen in derselben Domäne einrichten.

Info über diese Aufgabe

Die Einrichtung des ARR-Proxyservers besteht aus folgenden Schritten:

Schritte

1 Installieren des IIS.
2 Installieren des ARR-Moduls.
3 Konfigurieren des Anwendungspoolprozesses für ARR.
4 Erstellen einer Serverfarm aus WDM-Verwaltungsservern.
5 Konfigurieren von SSL.
6 Konfigurieren der Serverfarmeigenschaften für ARR.
7 Konfigurieren der Anforderungsfilterung.
8 Einrichten des Proxy-FQDN in den WDM-Voreinstellungen.

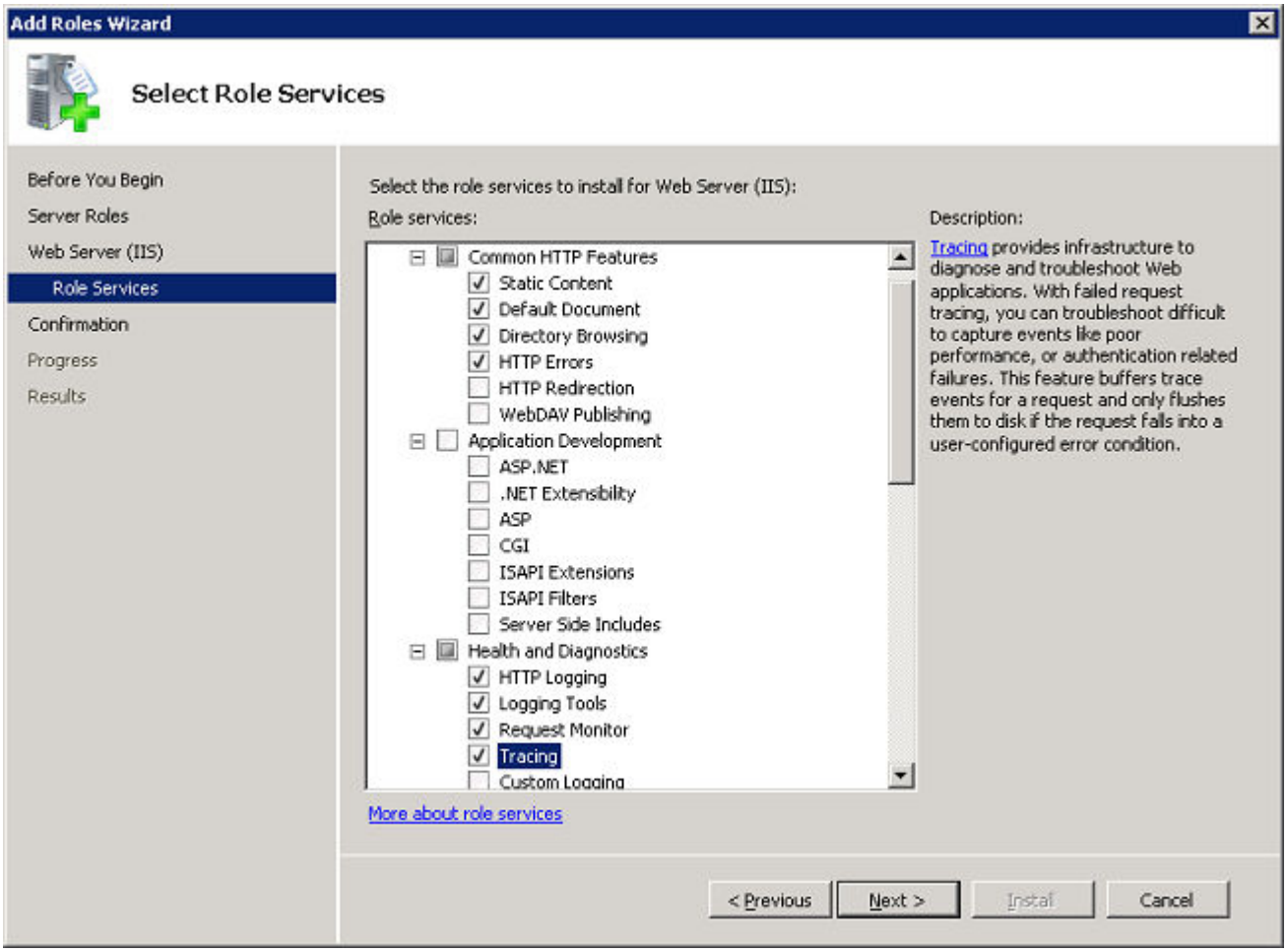
Installieren der Internetinformationsdienste – IIS

Info über diese Aufgabe

Installieren Sie Windows Server 2008 R2 auf einem der Systeme, das als ARR-Proxyserver vorgesehen ist.

Schritte

1 Melden Sie sich als Administrator an und führen Sie den **Server Manager** (Server-Manager) aus.
2 Wählen Sie unter Server-Manager **Roles** (Rollen) aus und klicken Sie im rechten Fensterbereich auf **Add Roles** (Rollen hinzufügen).
Der **Assistent „Add Roles“** (Rollen hinzufügen) wird angezeigt.
3 Wählen Sie **Server Roles** (Serverrollen) aus, aktivieren Sie **Web server (IIS)** (Webserver (IIS)) und klicken Sie anschließend auf **Next (Weiter).**



4 Wählen Sie die folgenden Optionen aus:

Option	Unteroptionen
Common HTTP Features (Allgemeine HTTP-Funktionen)	· Static Content (Statischer Inhalt) · Default Document (Standarddokument) · HTTP Errors (HTTP-Fehler) · Directory Browsing (Verzeichnissuche)
Health and Diagnostics (Integrität und Diagnose)	· HTTP Logging (HTTP-Protokollierung) · Request Monitor (Anforderungsüberwachung) · Logging Tools (Protokollierungstools) · Tracing (Nachverfolgung)
Management Tools (Verwaltungshilfsprogramme)	Wählen Sie alle Suboptionen aus.

5 Klicken Sie auf **Next** (Weiter), um die Zusammenfassung anzuzeigen.

6 Klicken Sie auf **Install** (Installieren), um IIS zu installieren.

Installieren des ARR-Moduls

Sie müssen Application Request Routing 3.0 auf dem System installieren, das Sie als ARR Proxy Server festgelegt haben. Das Installationsprogramm ist auf der Microsoft-Downloadsite unter https://www.microsoft.com/en-us/download/details.aspx?id=47333 verfügbar. Laden Sie die Datei **ARRv3_0.exe** herunter und installieren Sie sie.

Konfigurieren des Anwendungspoolprozesses für ARR

Alle HTTP-Anfragen und -Antworten für die Inhaltsseiten laufen durch Application Request Routing. Damit diese Option ordnungsgemäß funktioniert, müssen Sie sicherstellen, dass der Arbeitsprozess der Standardwebsite auf ARR ständig ausgeführt wird.

Info über diese Aufgabe

So konfigurieren Sie den Anwendungspoolprozess:

Schritte

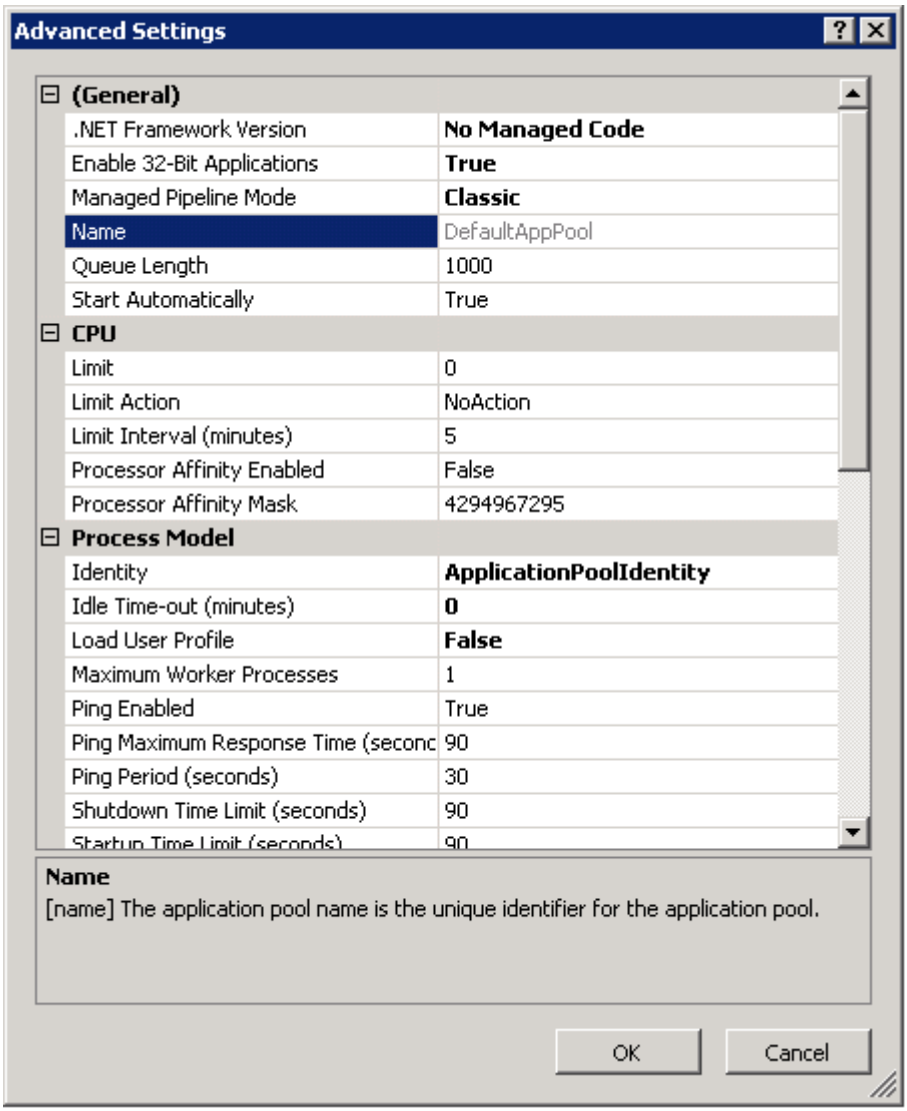
1 Melden Sie sich beim ARR-Proxyserver an und starten Sie den IIS Manager.

2 Wählen Sie unter dem Root-Knoten **Application Pools** (Anwendungspools) aus.

Im rechten Fensterbereich wird **DefaultAppPool** als Anwendungspool für die Standardwebsite angezeigt.

3 Wählen Sie **DefaultAppPool** aus und klicken Sie auf **Edit Application Pool** (Anwendungspool bearbeiten) im Fensterbereich **Action** (Aktion).

4 Wählen Sie **Advanced Settings** (Erweiterte Einstellungen), um das Fenster **Advanced Settings** (Erweiterte Einstellungen) anzuzeigen.



5 Ändern Sie den Wert unter **Process Model** (Prozessmodell) von **Identity** (Identität) von **LocalSystem** zu **ApplicationPoolIdentity**.

6 Ändern Sie den Wert für **Idle Time-out (minutes)** (Leerlauf-Zeitlimit (Minuten)) zu 0, um die Einstellung zu deaktivieren. Klicken Sie zum Speichern der Änderungen auf **OK**.

Erstellen einer Serverfarm aus WDM-Verwaltungsservern

Info über diese Aufgabe

So erstellen und definieren Sie eine Serverfarm:

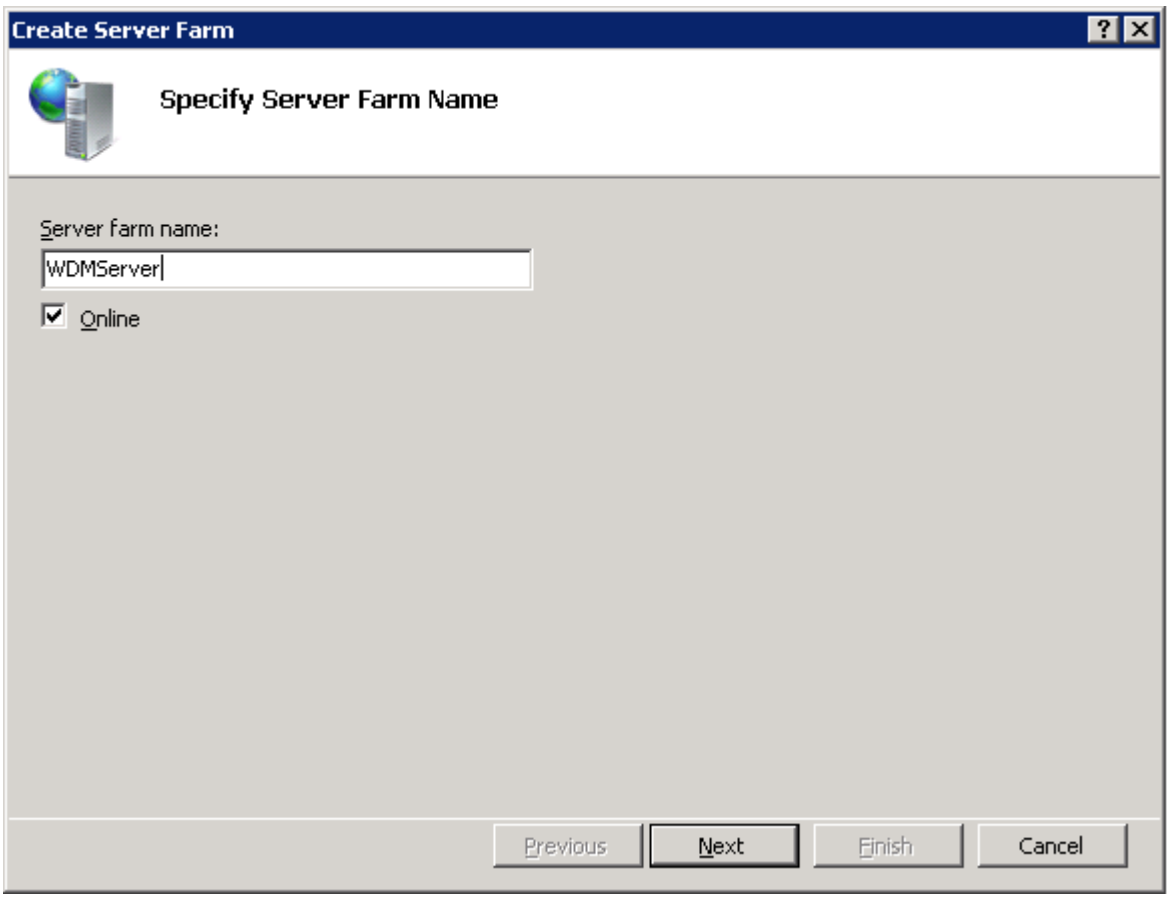
Schritte

1 Melden Sie sich beim ARR-Proxyserversystem an und starten Sie den IIS Manager.

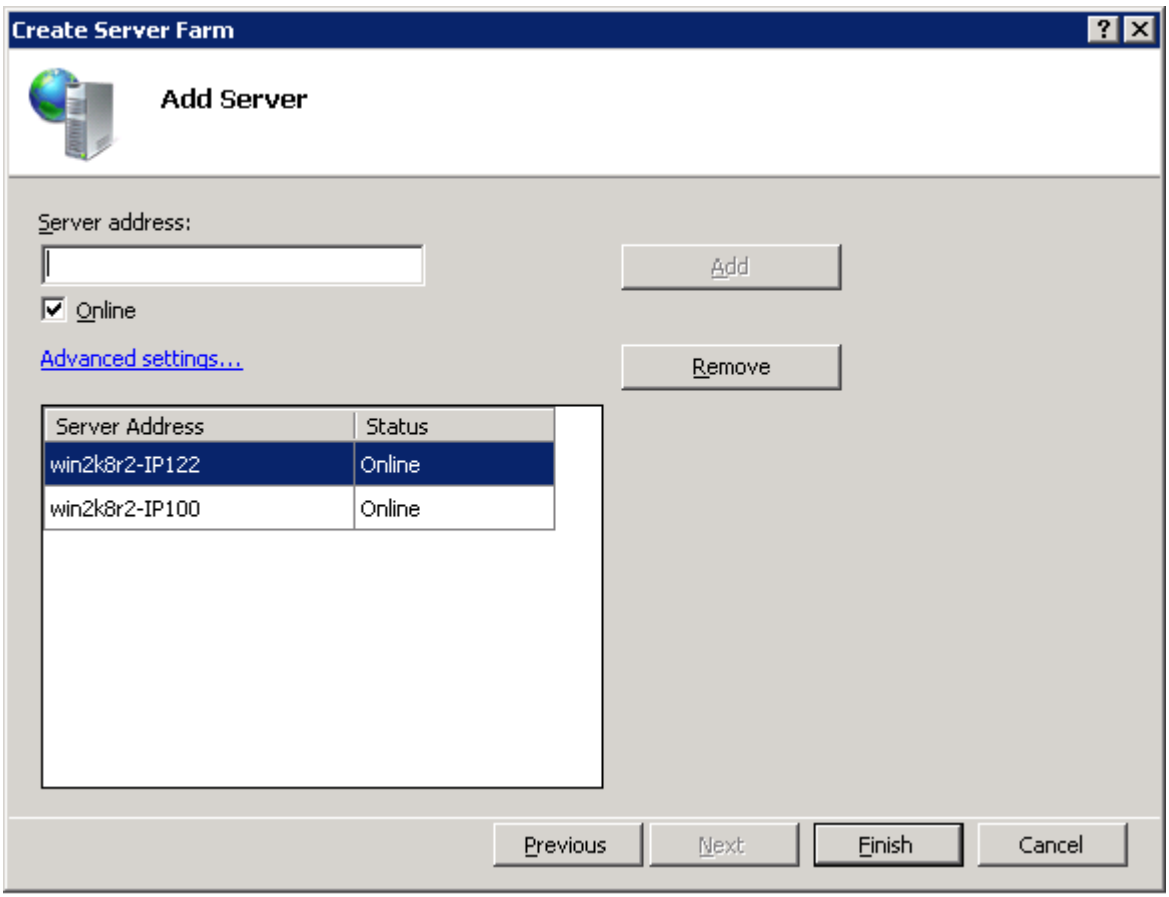
2 Wählen Sie unter dem Root-Knoten **Server Farms** (Serverfarmen) aus. Diese Option steht erst nach der Installation des ARR-Proxy-Moduls zur Verfügung.

3 Klicken Sie mit der rechten Maustaste darauf und wählen Sie **Create Server Farm** (Serverfarm erstellen) aus dem Menü aus.

Der Bildschirm **Create Server Farm** (Serverfarm erstellen) wird angezeigt.



4 Geben Sie einen Namen für die Serverfarm ein. Zum Beispiel: **WDMServerFarm**. Klicken Sie auf **Next** (Weiter), um die WDM-Verwaltungsserver hinzuzufügen.



5 Geben Sie den Hostnamen des WDM-Servers an und klicken Sie auf **Add** (Hinzufügen). Sie können alle Server hinzufügen, auf denen Sie den WDM-Verwaltungsserver installiert haben.

6 Klicken Sie auf **Finish** (Fertig stellen), um alle Server zur Farm hinzuzufügen.

Nachdem die Server hinzugefügt wurden und die Serverfarm erstellt wurde, werden Sie aufgefordert, die Routing-Regeln für alle Anfragen zur automatischen Weiterleitung an die Serverfarm umzuschreiben.

7 Klicken Sie auf **Yes** (Ja), damit der IIS Manager eine URL-Rewrite-Regel für die Weiterleitung aller eingehenden Anfragen an diese Serverfarm erstellen kann.

Konfigurieren von SSL

Eines der Merkmale bei ARR ist **SSL off-loading**. Hierbei handelt es sich um eine Funktion, bei der die Kommunikation zwischen den Clients und dem ARR Proxy-Server über SSL erfolgt und die Kommunikation zwischen dem ARR Proxy-Server und den WDM-Verwaltungsservern über Klartext stattfindet. Durch Aktivieren dieser Funktion können Sie die Serverressourcen auf den WDM-Verwaltungsservern maximieren.

Voraussetzung

Zuerst müssen Sie das SSL-Zertifikat auf dem ARR-Proxyserver erstellen.

Info über diese Aufgabe

So erstellen und konfigurieren Sie das SSL-Zertifikat:

Schritte

1 Melden Sie sich beim ARR-Proxyserver an und starten Sie den IIS-Manager.

2 Wählen Sie den Stammknoten aus und öffnen Sie die Seite **Serverzertifikate** aus dem rechten Fenster.

3 Klicken Sie im Bereich „Aktionen“ auf **Domänenzertifikat erstellen**.

4 Geben Sie den Namen des ARR-Proxyservers in den Assistenten **Zertifikat erstellen** ein.

5 Klicken Sie auf **Weiter**, um die Erstellung des Zertifikats abzuschließen.

6 Wählen Sie **Default Web Site** unter **Sites** aus und klicken Sie im Bereich **Aktionen** auf **Bindungen**.

7 Weisen Sie dem Zertifikat die **HTTPS**-Bindung zu.

8 Gehen Sie zu **Server Farm (Serverfarm)** und doppelklicken Sie auf **Created Farm (Erstellte Farm)**.

9 Doppelklicken Sie auf **Routing Rules (Routing Regeln)** und wählen Sie die Option **Enable SSL offloading (SSL-Offloading aktivieren)** aus, wenn Sie möchten, dass die Kommunikation zwischen dem ARR Proxy-Server und den WDM-Verwaltungsservern über Klartext erfolgt. Sie müssen außerdem die HTTP- und HTTPS-Ports zu den standardmäßigen Website-Bindungen auf den einzelnen WDM-Verwaltungsserversystemen hinzufügen.

ANMERKUNG:

Wenn Sie möchten, dass die Kommunikation zwischen dem ARR Proxy-Server und dem WDM-Verwaltungsserver auch über das HTTPS-Protokoll läuft, müssen Sie die Funktion **SSL off-loading** deaktivieren und SSL auf den einzelnen WDM-Verwaltungsservern konfigurieren. Wenn Sie ein selbstsigniertes Zertifikat zum Einrichten von SSL auf dem WDM-Verwaltungsserver verwenden, importieren Sie dieses Zertifikat in den **Speicher für vertrauenswürdige Stammzertifizierungsstellen** für einen lokalen Computer auf dem ARR Proxy Server, indem Sie die Schritte auf der Microsoft-Website befolgen: http://technet.microsoft.com/en-us/library/cc754841.aspx#BKMK_addlocal.

Konfigurieren von Serverfarmeigenschaften für ARR

Nachdem die Serverfarm erstellt und definiert wurde, müssen Sie zusätzliche Eigenschaften festlegen, um das Verhalten von ARR zu steuern.

1 Melden Sie sich beim ARR-Proxyserver an und starten Sie den IIS-Server Manager.

2 Wählen Sie die von Ihnen erstellte Serverfarm aus. Die folgenden Optionen werden im rechten Fenster angezeigt:
- Caching (Zwischenspeicherung)
- Health Test (Integritätstest)
- Load Balance (Load-Balance)
- Monitoring and Management (Überwachung und Verwaltung)
- Proxy
- Routing Rules (Routing-Regeln)
- Server Affinity (Serveraffinität)

3 Wählen Sie **Caching** (Zwischenspeicherung) aus.
   a Deaktivieren Sie die Option **Enable disk cache** (Datenträgercache aktivieren), um die Zwischenspeicherung zu deaktivieren.
   b Setzen Sie **Memory cache duration** (Speicher-Cache-Dauer) auf 0.

4 Wählen Sie **Health Test** (Integritätstest) aus.
   a Geben Sie den Fully Qualified Domain Name (FQDN) des ARR-Proxy-Servers im Feld **URL** ein. Der Wert sollte folgendermaßen lauten: **http(s)/<ProxyFQDN>/hserver.dll?&V93**. Dies ist die URL, die ARR zum Senden von Anfragen an den WDM-Verwaltungsserver verwendet, um den Zustand einer bestimmten Serverfarm zu überprüfen.
   b Legen Sie das Intervall fest, in dem der ARR Health Test den Integritätstest wiederholt. Die Standardeinstellung ist 30 Sekunden. Sie können den Wert auch auf 180 Sekunden einstellen.
   c Legen Sie ein Timeout für die URL fest, die Sie angegeben haben. Hierbei handelt es sich um die Zeitspanne, nach der der Server als **Unhealthy** (Fehlerhaft) gekennzeichnet wird, wenn er nicht reagiert.
   d Legen Sie den Wert für **Acceptable Status codes** (Zulässige Statuscodes) auf **200-399** fest. Wenn die URL für den Integritätstest einen Statuscode zurückgibt, der nicht mit dem Wert im Feld **Acceptable Status Codes** (Zulässige Statuscodes) übereinstimmt, markiert ARR diesen Server als fehlerhaft.
   e Stellen Sie den Textwert **Server Healthy** (Server fehlerfrei) im Feld **Response Match** (Antwortübereinstimmung) ein. Der Text unter **Response Match** (Antwortübereinstimmung) wird anhand der Antwortentität von jedem Server überprüft. Wenn die Antwort vom Server nicht die unter „Response Match“ (Antwortübereinstimmung) angegebene Zeichenkette enthält, wird der Server als fehlerhaft markiert.
   f Klicken Sie auf **Verify URL** (URL überprüfen). Die Prüfung sollte für alle WDM-Verwaltungsserver in der Serverfarm bestanden werden.

5 Ändern Sie den **Load Balance** (Lastenausgleichsalgorithmus).
   a Wählen Sie **Weighted Round Robin** (Gewichteter Roundrobin) aus der Dropdown-Liste **Load balance algorithm** (Lastenausgleichsalgorithmus) aus.
   b Wählen Sie **Even distribution** (Gleichmäßige Verteilung) aus der Dropdown-Liste **Load distribution** (Lastenausgleich) aus.
   c Klicken Sie auf **Apply** (Anwenden).

6 Doppelklicken Sie auf die Option **Monitoring and Management** (Überwachung und Verwaltung), um den Integritätsstatus und andere Statistiken des WDM-Verwaltungsservers anzuzeigen.

7 Doppelklicken Sie auf **Proxy**, um die Proxy-Einstellungen zu konfigurieren:
   a Setzen Sie den Wert von **Response buffer threshold** (Antwortpufferlimit) auf 0.
   b Deaktivieren Sie die Option **Keep Alive**.
   c Ändern Sie die **HTTP**-Version zu **HTTP/1.1**.
   d Wählen Sie die Option **Reverse rewrite host in response headers** (Umgekehrter Rewrite-Host in Antwortheader) aus.
8 Doppelklicken Sie auf **Routing Rules** (Routing-Regeln).
   a Klicken Sie im Fensterbereich **Actions** (Aktionen) auf **URL Rewrite** (URL-Rewrite).
   b Setzen Sie auf der Seite **Edit Inbound Rule** (Eingehende Regel bearbeiten) die Option **Pattern** (Muster) auf ***hserver.dll***.

   Durch diesen Schritt wird sichergestellt, dass der ARR-Proxyserver nur die für den WDM-Verwaltungsserver bestimmten URL-Anforderungen an die Serverfarm weiterleitet.

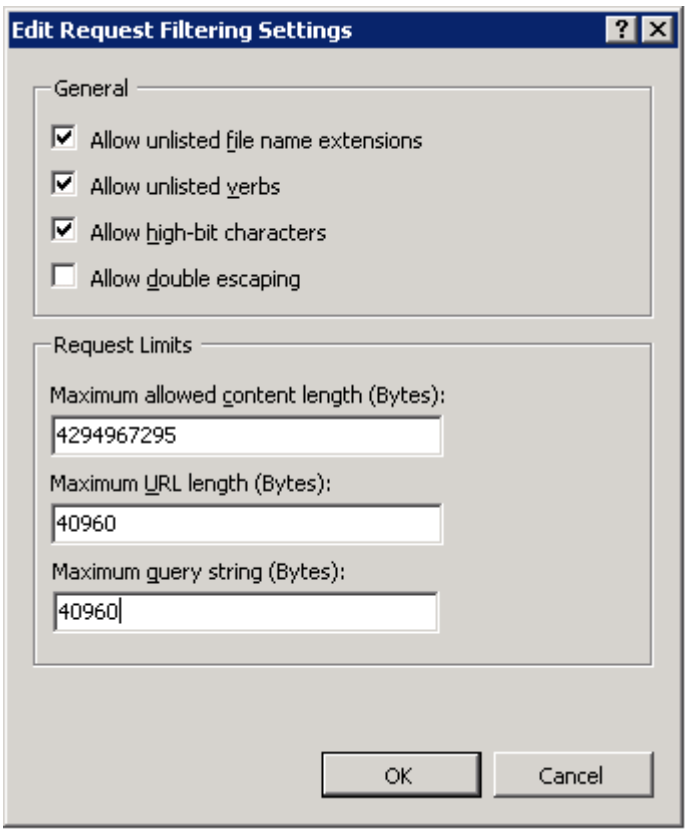
Der Serverfarmeigenschaften sind nun konfiguriert.

Konfigurieren der Anforderungsfilterung

Info über diese Aufgabe
So konfigurieren Sie die Anforderungsfilterung:

Schritte

1 Melden Sie sich beim ARR-Proxyserver an und starten Sie den IIS-Manager.
2 Wählen Sie **Default Web Site** (Standardwebsite) unter **Sites** (Websites) aus und doppelklicken Sie im rechten Fensterbereich auf **Request Filtering** (Anforderungsfilterung).
3 Klicken Sie auf **Edit Feature Settings** (Featureeinstellungen bearbeiten).
4 Legen Sie die **Request Limits** (Anforderungslimits) fest wie unten gezeigt:



5 Klicken Sie auf **OK**, um die Einstellungen zu übernehmen.

Einrichten des Proxy-FQDN in den WDM-Voreinstellungen

Um das Setup des Lastenausgleichs abzuschließen, müssen Sie die Informationen zum Proxyserver in WDM angeben.

Info über diese Aufgabe

So richten Sie den Proxy-FQDN in WDM ein:

Schritte

1 Melden Sie sich beim System an, auf dem Sie WDM installiert haben, und starten Sie die WDM Web UI-Konsole.

2 Wählen Sie **System** > **Console (Konsole)** aus.

3 Geben Sie unter „Manager Server Alias Name“ (Aliasname des Manager-Servers) den FQDN des ARR-Proxyservers ein.

4 Klicken Sie auf **Save (Speichern)**, um die Einstellungen zu speichern.

Der ARR-Proxyserver ist nun in der WDM-Datenbank aufgenommen. Hierdurch ist das Setup des Lastenausgleichs abgeschlossen.

Installieren von WDM-Komponenten

Für das Setup des Lastenausgleichs sind mehrere Installationen von WDM-Verwaltungsservern erforderlich. Sie müssen jedoch sicherstellen, dass eines der Systeme in diesem Setup über eine vollständige Installation von WDM verfügt. Sie können dann nur den Verwaltungsserver und den ThreadX-Dienst auf den anderen Systemen installieren. Weitere Informationen zur Installation nur der ausgewählten Komponenten finden Sie unter Installieren des Verwaltungsservers.Installation der Management-Services

Konfigurieren des Lastausgleichs für ThreadX 4.x-Geräte

Wenn Sie eine große Anzahl von PCoIP-(ThreadX-)Geräten verwalten möchten, ist die Skalierung eines einzigen ThreadX Manager-Diensts zur Verwaltung dieser großen Anzahl an ThreadX-Geräten u. U. nicht möglich. Durch Konfigurieren des Lastenausgleichs für ThreadX-Geräte können Sie eine große Anzahl solcher Geräte verwalten.

Voraussetzungen

Vor der Konfiguration des Lastenausgleichs für ThreadX-Geräte müssen Sie zuerst ein Windows 2008 R2-System bestimmen und den DNS-Server (Domain Name Server) auf dem System installieren.

Weitere Informationen zur Installation eines DNS-Servers auf Windows Server 2008 finden Sie unter http://technet.microsoft.com/en-us/library/cc725925.aspx.

Der Lastenausgleichsmechanismus basiert auf der DNS-Round-Robin-Methode zur Weitergabe und Verteilung der Netzwerkressourcenlasten.

Info über diese Aufgabe

So richten Sie den DNS-Round-Robin-Mechanismus ein:

Schritte

1 Melden Sie sich beim DNS-Server an und starten Sie den DNS-Manager.

2 Wählen Sie den Servernamen in der Struktur im linken Fensterbereich aus und klicken Sie mit der rechten Maustaste darauf. Wählen Sie anschließend **Eigenschaften** im Menü aus.

Das Fenster **Eigenschaften** wird angezeigt.

3 Klicken Sie im Fenster **Eigenschaften** auf die Registerkarte **Erweitert**.

4 Stellen Sie sicher, dass im Fensterbereich **Serveroptionen** die Optionen **Round Robin aktivieren** und **Zwischenspeicher vor Beschädigungen sichern** aktiviert sind.

5 Wenn Netzwerkmaskenanforderung notwendig ist, wählen Sie die Option **Enable netmask ordering (Netzwerkmaskenanforderung aktivieren)**. Diese Funktion versucht, lokale Ressourcen für Clients zu priorisieren.

6 Klicken Sie auf das Menü **Ansicht** im DNS-Manager und wählen Sie die Option **Erweitert** aus.

7 Erweitern Sie den Knoten **Domain** und wählen Sie unter **Forward Lookup Zones (Forward-Lookup-Zonen)** die Domain aus (zum Beispiel **WDMSQA11.com**).

8 Klicken Sie mit der rechten Maustaste darauf und wählen Sie **Neuer Host (A oder AAAA)...** aus.

Das Fenster **Neuer Host** wird angezeigt.

9 Geben Sie den virtuellen Hostnamen der ThreadX-Serverfarm ein, die am Lastausgleich beteiligt ist (zum Beispiel ThreadXServer1). Der FQDN des Servers wird automatisch angezeigt.

10 Geben Sie die IP-Adresse des Servers ein.

11 Klicken Sie auf **Host hinzufügen**.

12 Wiederholen Sie die Schritte **8-11**, um beliebig viele ThreadX-Server hinzuzufügen.

13 Wählen Sie den Knoten **Domäne** unter **DNS-Manager** aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Weitere neue Einträge** aus.

14 Wählen Sie im Dialogfeld **Ressourceneintragstyp** die Option **SRV-Speicherort** aus und klicken Sie auf **Eintrag erstellen**.

15 Geben Sie in das Dialogfeld „Neuer Ressourceneintrag“ die folgenden Werte ein:
- **Dienstname** – _PCOIP-broker
- **Protokoll** - _tcp
- **Portnummer** - 50000
- **Host, der diesen Service bietet** - Geben Sie den Hostnamen der ThreadX-Serverfarm ein.

16 Wiederholen Sie die Schritte **13-15** und fügen Sie den SRV-Eintrag **_PCOIP -Tool** hinzu.

17 Konfigurieren Sie die DNS-Zwischenspeicherung:
   a Erweitern Sie im DNS-Manager den Knoten **Domäne** und wählen Sie unter diesem den Knoten **_tcp** aus.
   b Wählen Sie im rechten Fensterbereich **_PCOIP -Tool** aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Eigenschaften** aus.
   c Überprüfen Sie im Fenster **Properties (Eigenschaften)** den Wert **Time to Live (TTL)**. Der Cache-Intervall wird als **Maximaler TTL-Wert** bezeichnet und der Standardwert ist 1 Stunde. Sie können dies ändern, wenn Sie möchten.

   Das Feld „Time to Live (TTL)“ wird nur angezeigt, wenn Sie **Erweiterte Ansicht** im Menü **Ansicht** des DNS-Servers ausgewählt haben.

Der Lastenausgleich ist nun für ThreadX-Geräte konfiguriert und Sie können mit Ihren WDM-Verwaltungsservern eine große Anzahl von ThreadX-Geräten verwalten.

Konfigurieren des Lastenausgleichs für ThreadX 5.x-Geräte

Wenn WDM zum Verwalten von ThreadX 5.x-Geräten in großen Unternehmensumgebungen verwendet wird, kann ein einzelner Teradici Device Proxy-Server, der für die Verwaltung von ThreadX 5x-Geräten über WDM genutzt wird, nicht für die Verwaltung von mehr als 18 000 Geräten skaliert werden. Es können Probleme oder Verzögerungen bei Client-Check-ins, geplanten Ausführungen und/oder der Ausführung von Befehlen in Echtzeit auftreten.

Mithilfe von Lastausgleich können diese Probleme weitestgehend gelöst werden. In diesem Setup können Sie mehrere Instanzen von Teradici Device Proxy-Servern auf verschiedenen Systemen installieren und ausführen und die Last zwischen ihnen mit einem Proxy wie nachfolgend beschrieben ausgleichen.

Die Komponenten des Load Balancer sind folgende:

- Teradici Device Proxy-Server
- HA-Proxy-Server

WDM verwendet den HAProxy, der auf dem Ubuntu-Server 16.04.1 LTS gehostet wird, um einen Lastausgleich zwischen Teradici Device Proxy-Servern durchzuführen. HAProxy ist ein Load-Balancer-Proxy, der je nach Konfiguration auch HA bieten kann. Er ist eine beliebte Open-Source-Software für TCP/HTTP-Load-Balancer und eine Proxy-Lösung, die für Linux eingesetzt werden kann. Die häufigste Verwendung dient der Erhöhung der Leistung und Zuverlässigkeit der Serverumgebung durch die Verteilung der Rechenlast auf mehrere Server.

Dieser Abschnitt beschreibt die Einrichtung und Konfiguration des Lastausgleichs des HA-Proxy-Servers.

Schritte zum Erstellen eines DNS_SRV-Datensatzes:

Firmware 5.x verwendet einen DNS_SRV-Datensatz zusätzlich zum Textdatensatz, der den Fingerabdruck des SSL-Zertifikats für die Verwendung in der Verwaltungskonsole enthält.

WDM 5.7.3 unterstützt Teradici 5.x-Firmware mit umfassenden Funktionen.

1 Der erste erforderliche Datensatz ist der DNS_SRV-Datensatz für _pcoip-bootstrap. Der Datensatz muss auf den Namen des Teradici Device Proxy (HAProxy) verweisen.

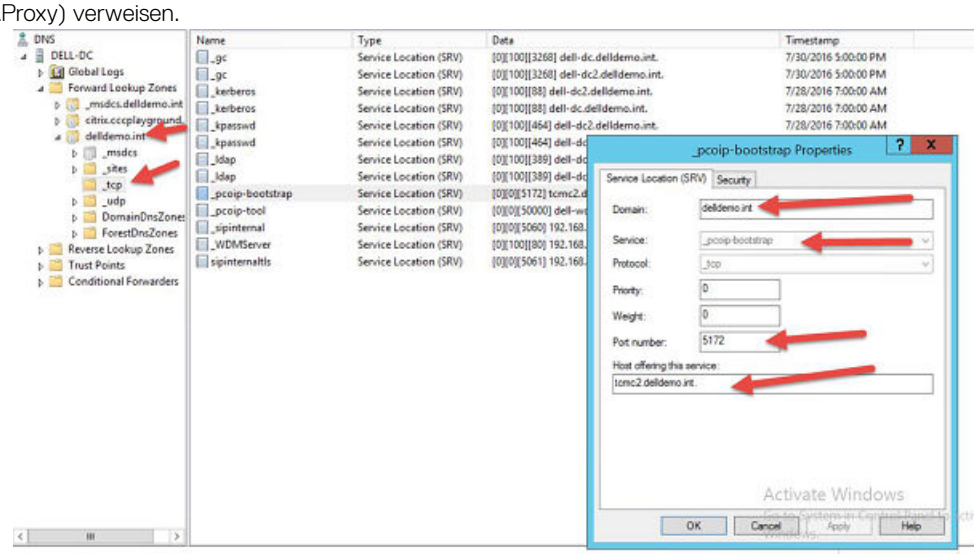


Abbildung 40. DNS_SRV-Datensatz für _pcoip-bootstrap

2 Der zweite erforderliche Datensatz ist ein A-Datensatz, der auf den im Feld **Host offering this service** (Host, der diesen Dienst bietet) verwendeten Namen verweist.

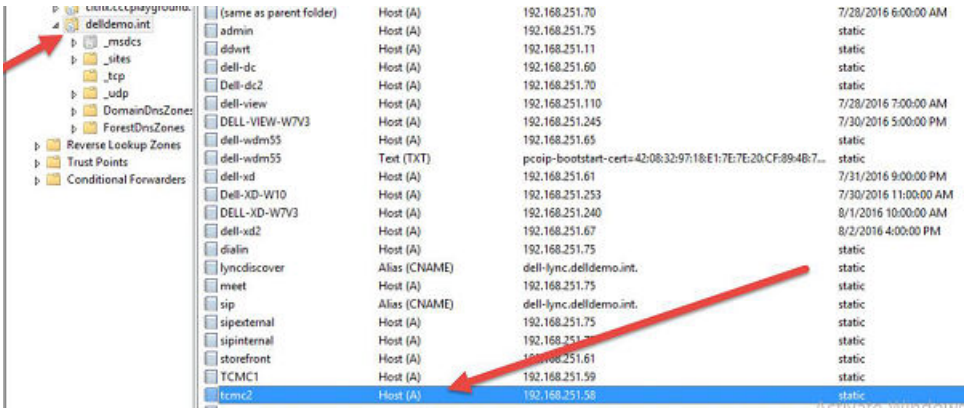


Abbildung 41. Host-Datensatz

3 Der dritte erforderliche Datensatz ist ein Txt-Datensatz. Der Txt-Datensatz ist der Fingerabdruck des SSL-Zertifikats, das von der Verwaltungskonsole verwendet wird.

Führen Sie die folgenden Schritte aus, um einen A-Datensatz für den Host sowie einen Txt-Datensatz zu erstellen:

1 Klicken Sie auf den Domain-Knoten (delldemo.int), wählen Sie **Other New Records** (Weitere neue Datensätze) und anschließend „Host“ (A oder AAAA) aus. Der Name ist der A-Datensatz der Verwaltungskonsole.

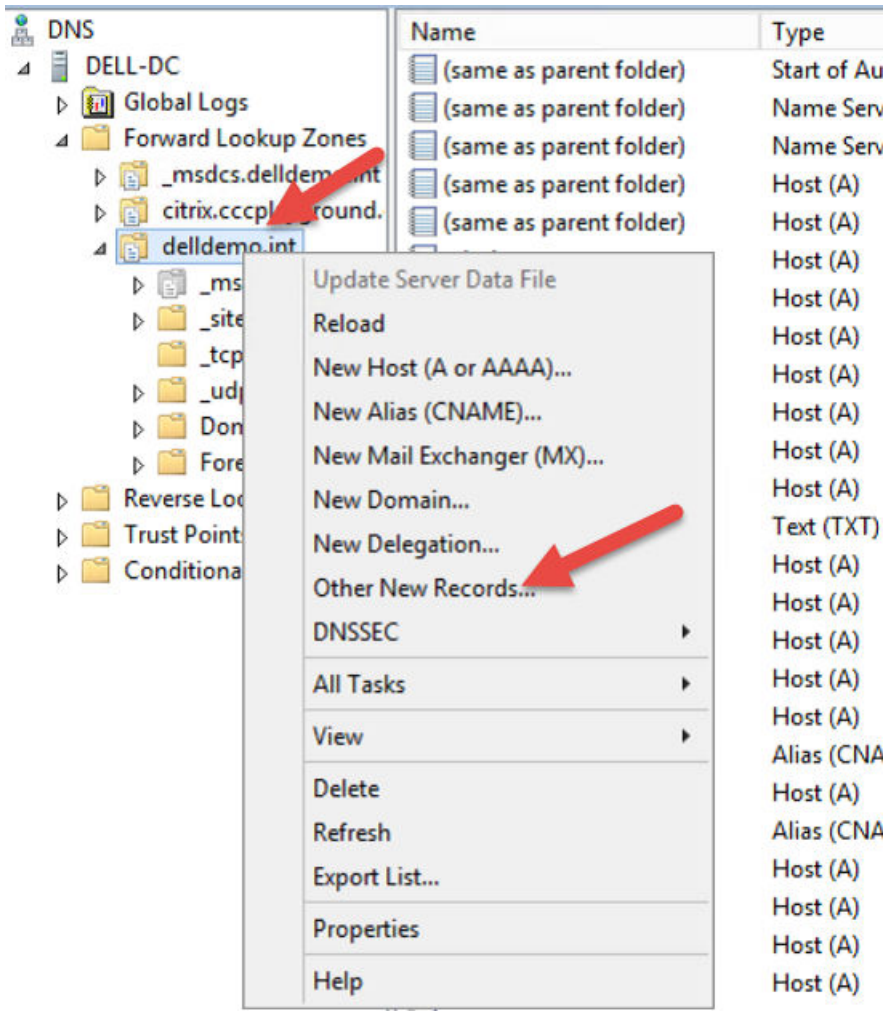


Abbildung 42. Erstellen des TXT-Datensatzes

2 Klicken Sie auf den Domain-Knoten (delldemo.int), wählen Sie **Other New Records** (Weitere neue Datensätze) und anschließend „Text“ (TXT) aus, um das Textfeld mit dem Fingerabdruck des Zertifikats zu erstellen.

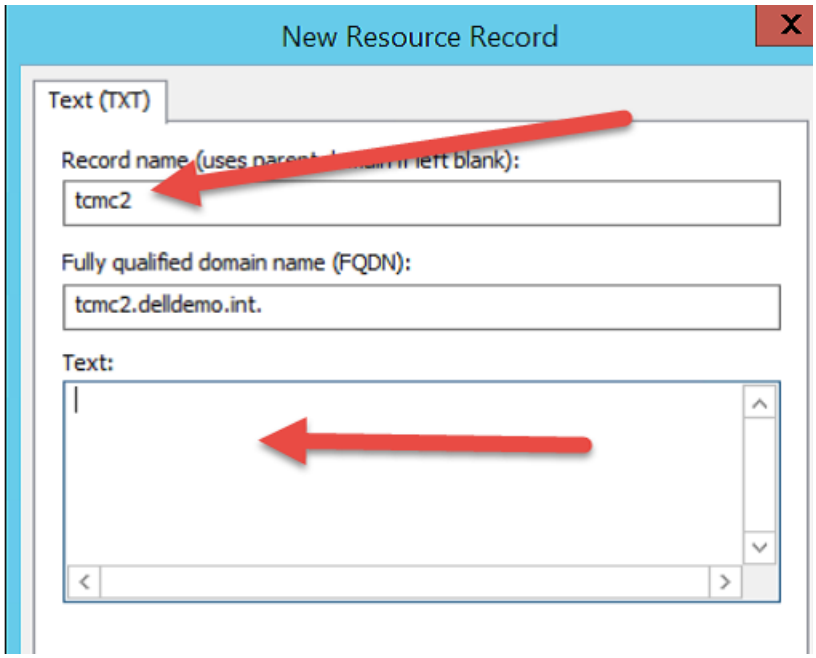


Abbildung 43. Neuer Ressourcendatensatz

Der Fingerabdruck Sha256 kann mit dem Firefox-Browser abgerufen werden.

Gehen Sie zum Abrufen des Fingerabdrucks folgendermaßen vor, wenn Wyse Device Manager (WDM) mit Teradici 5x installiert ist:

1 Öffnen Sie den Firefox-Browser von dem Gerät, auf dem die Teradici 5.x-Komponente installiert ist. Nach dem Öffnen des Browsers drücken Sie **Alt + T** zum Öffnen der Extras.

2 Wählen Sie in der Dropdown-Liste **Options** (Optionen) aus.

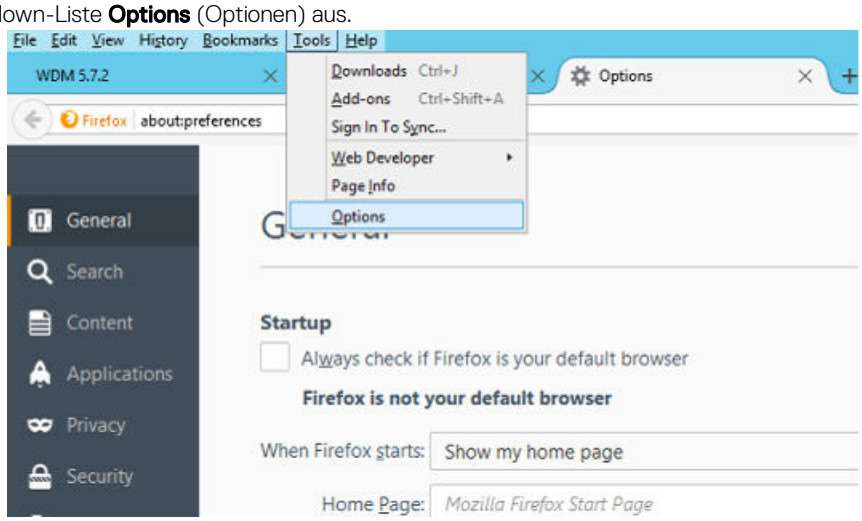


Abbildung 44. Registerkarte „General“ (Allgemein)

3 Klicken Sie im linken Fensterbereich der Seite **Options** (Optionen) auf die Registerkarte **Advanced** (Erweitert) und klicken Sie dann auf die Option **Certificates** (Zertifikate).

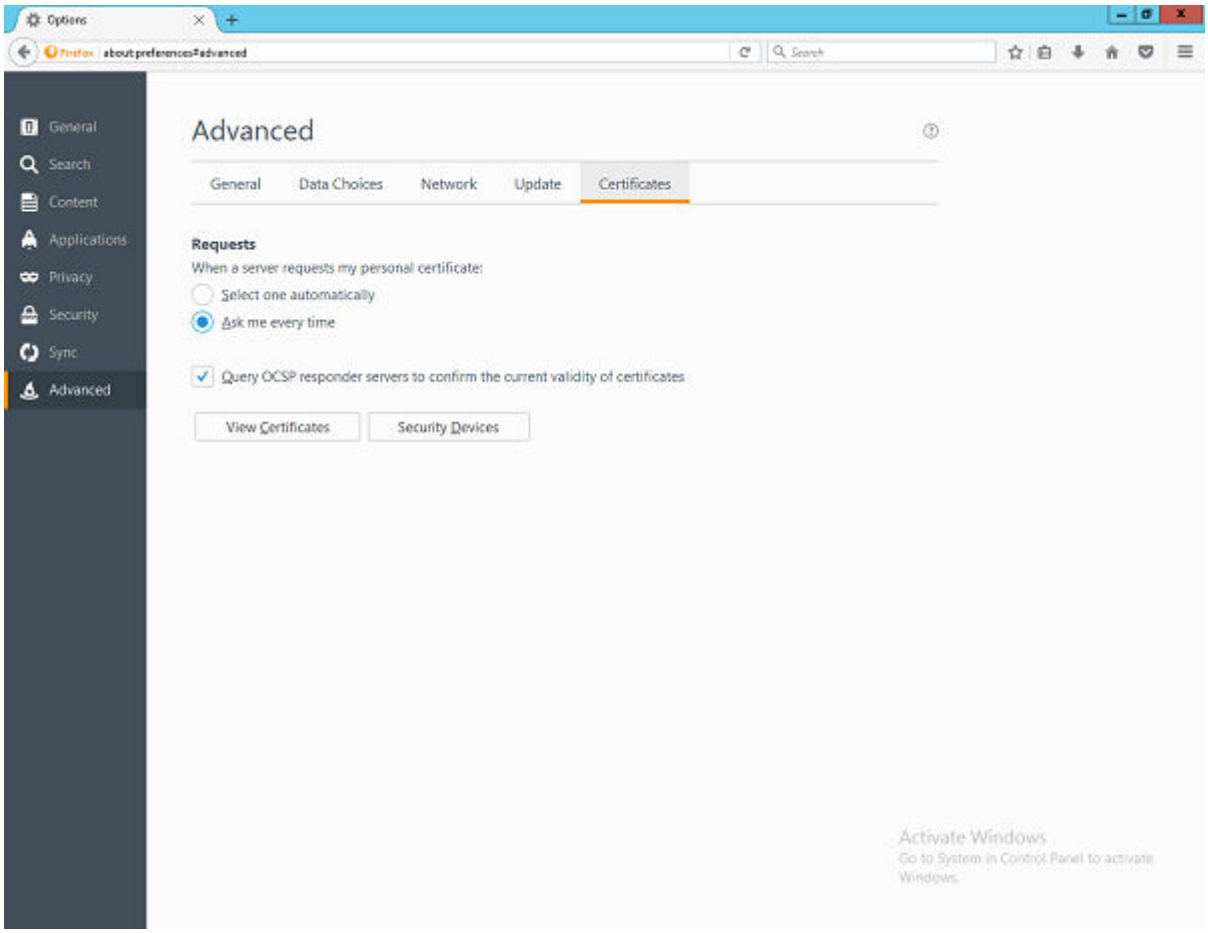


Abbildung 45. Advanced (Erweitert)

4 Klicken Sie zum Öffnen des Fensters „Certificate Manager“ (Zertifikat-Manager) auf **View Certificates** (Zertifikate anzeigen).

5 Wählen Sie die Registerkarte **Authorities** (Zertifizierungsstellen) im Fenster **Certificate Manager** (Zertifikat-Manager) aus und klicken Sie auf **Import** (Importieren).

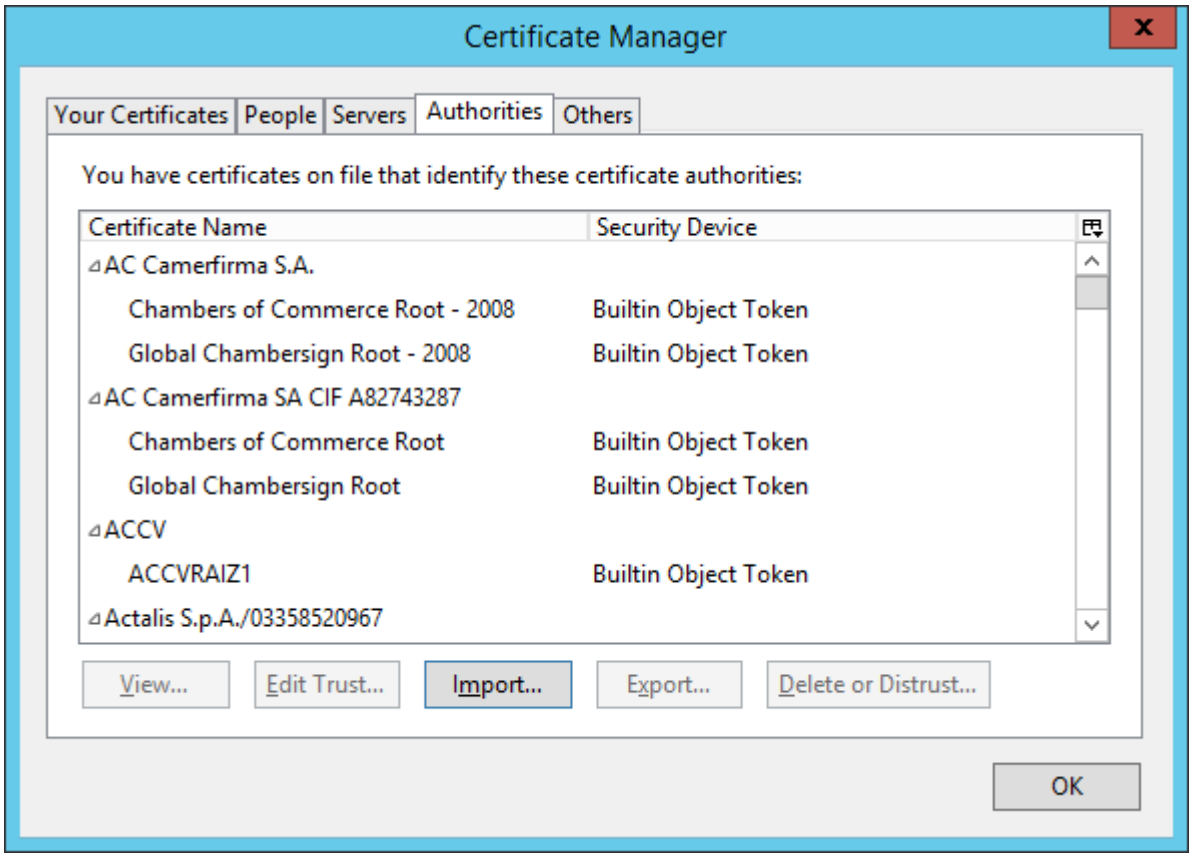


Abbildung 46. Certificate Manager (Zertifikat-Manager)

6 Navigieren Sie im Datei-Browser-Dialogfeld zum Speicherort der WDM-Installation, zum Beispiel: **\Wyse\WDM\TeraDici**. Je nach Betriebssystem und Installationspfad kann der Root-Pfad folgendermaßen lauten **C:\Program Files (x86)**.

ANMERKUNG: In manchen Fällen (wenn die Teradici-Komponenten benutzerdefiniert installiert oder manuell konfiguriert sind) müssen auf demselben Gerät die obigen Schritte beachtet werden und der standardmäßige Installationspfad trifft unter Umständen nicht zu. In einem solchen Fall navigieren Sie zum entsprechenden Root-Pfad, unter dem der Teradici-Ordner verfügbar ist.

7 Wählen Sie die Datei mit dem Namen **cert.pem** aus und klicken Sie dann auf **Open** (Öffnen).

8 Klicken Sie im Fenster **Downloading Certificate** (Zertifikat herunterladen) auf die Schaltfläche **View** (Anzeigen).

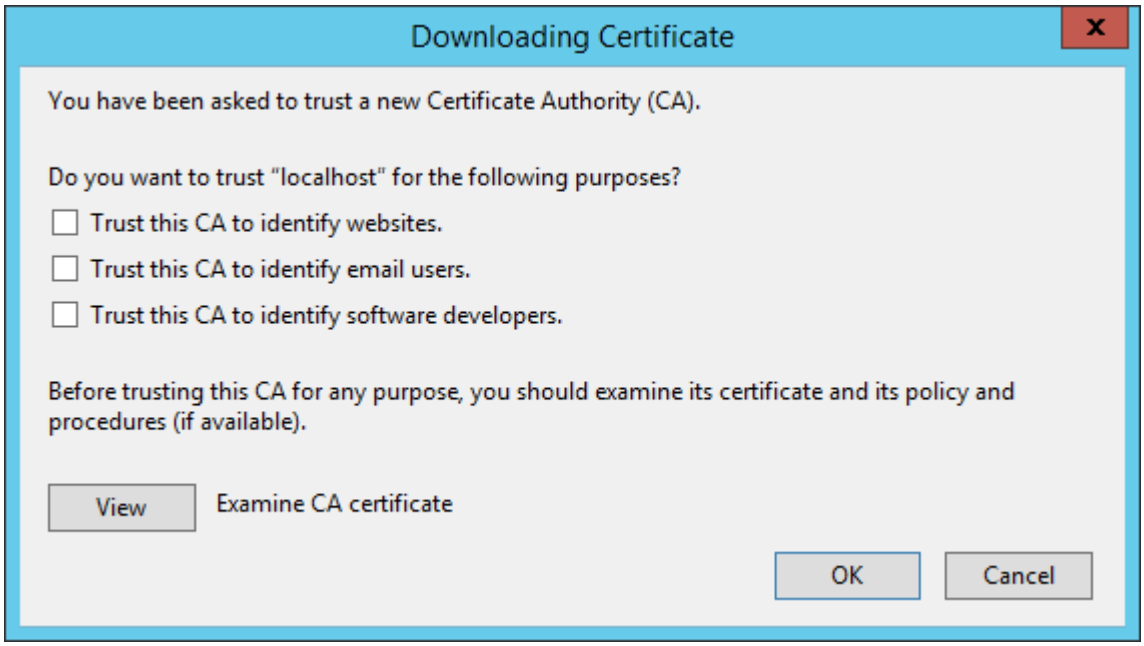


Abbildung 47. Downloading Certificate (Zertifikat herunterladen)

9 Kopieren Sie den Wert des Fingerabdrucks „sha256“ Klicken Sie auf **Close** (Schließen) und schließen Sie alle Firefox-Fenster.

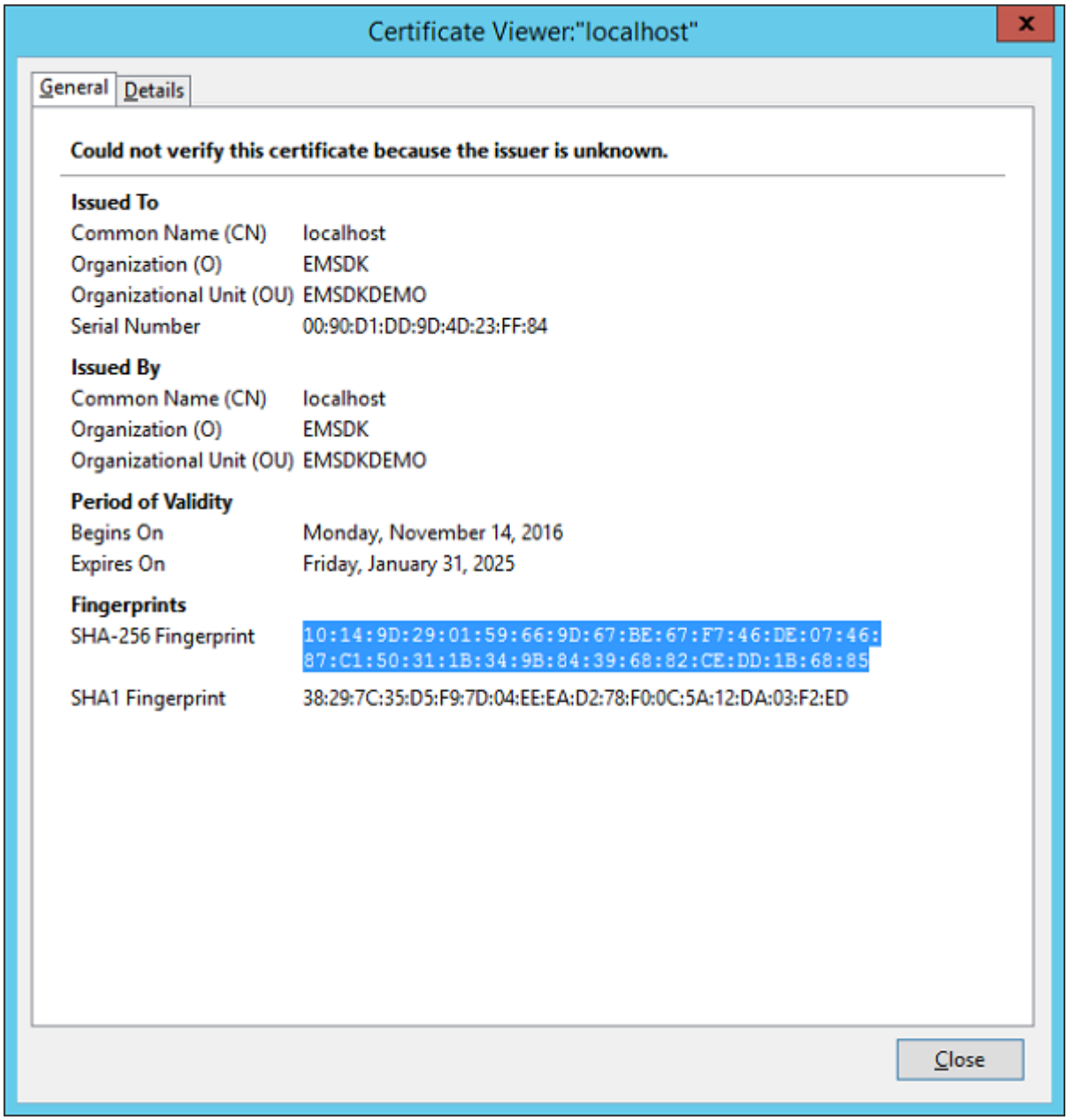


Abbildung 48. Certificate Viewer (Zertifikat-Viewer)

ANMERKUNG: Im Feld Text muss vor den bereits abgerufenen Fingerabdruck sha256 das Präfix pcoip-bootstrap-cert= gesetzt werden.

Nach dem Kopieren des Zertifikatfingerabdrucks führen Sie die folgenden Schritte auf dem DNS-Server durch:

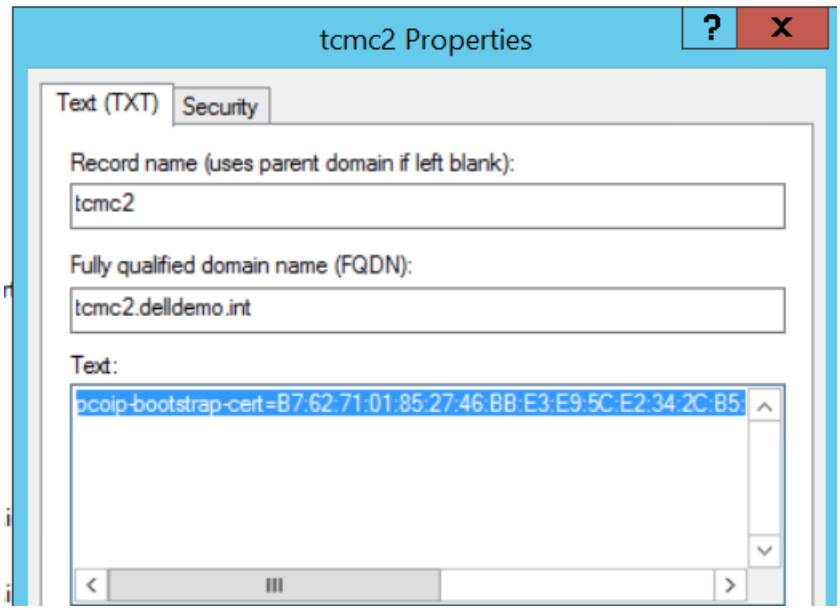


Abbildung 49. tcmc2-Eigenschaften

10 Der vierte und letzte Datensatz ist ein umgekehrter PTR-Datensatz für den Verwaltungs-Host.

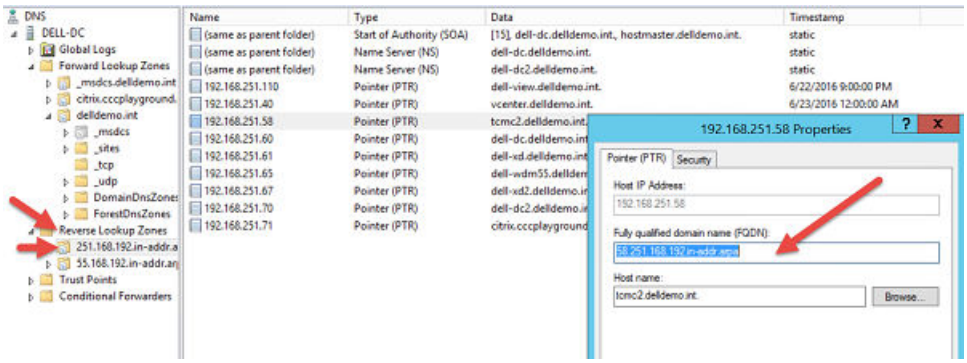


Abbildung 50. PTR-Datensatz

11 Die Zone muss mit dem Subnetz übereinstimmen, in dem sich der Host befindet, und der Datensatz ist die IP-Adresse, die dem Teradici Device Proxy (HAProxy) zugewiesen ist.

Installieren und Konfigurieren von HAProxy

HAProxy ist der Load-Balancer für ThreadX 5x-Geräte und wird auf Ubuntu Linux Version 16.04.1 mit HAProxy Version 1.6 konfiguriert.

Befolgen Sie die Schritte zum Installieren und Konfigurieren von HAproxy auf einem Ubuntu Linux-Computer:

Referenz-Link: https://haproxy.debian.net/#?distribution=Ubuntu&release=precise&version=1.6

1 Melden Sie sich beim Ubuntu-Computer durch Bereitstellen der Benutzeranmeldeinformationen an, die während der Installation des Ubuntu-Betriebssystems verwendet wurden.

2 Öffnen Sie das Terminal und führen Sie die folgenden Befehle zum Installieren von HAProxy aus:

- 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 Führen Sie die folgenden Befehle zum Konfigurieren von HAProxy aus:

- Sichern Sie ursprüngliche Konfiguration vor dem Bearbeiten mit dem Befehl **sudo cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.original**
- Jetzt bearbeiten Sie die Konfigurationsdatei mit dem Befehl **sudo nano /etc/haproxy/haproxy.cfg**
- In der Konfigurationsdatei bearbeiten Sie die folgenden Abschnitte je nach Anforderung:
  - Globaler Abschnitt: Maxconn <maximale Anzahl an Verbindungen>
  - Frontend tcp-in: bind <HAProxy-Server-IP>:5172
  - Back-End-Server: server <Server-Aliasname> <Teradici-Gerät Proxy-Server-IP->:5172
  - Maxconn <maximale Anzahl der Verbindungen pro Teradici-Gerät Proxy-Server>

ANMERKUNG: Um Hochverfügbarkeit zu erzielen, können Administratoren möglicherweise zusätzliche Back-End-Server über die Kapazität der Gesamt-Clients hinaus hinzufügen, um nahtloses Failover zu erhalten.

- Nach dem Bearbeiten der Konfiguration speichern Sie sie mit Befehl **Strg + O**
- Es wird folgende Beispiel-HAProxy-Konfiguration zur Verfügung gestellt:

```
global

log /dev/log local0

log /dev/log local1 notice

chroot /var/lib/haproxy

daemon

#maxconn is maximum allowed connections

maxconn 50000

defaults

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

frontend tcp-in

#IP mit IP Ihres Linux Proxy-Computers ersetzen
```

bind 10.150.99.102:5172

default_backend servers

backend servers

#Fügen Sie die IP-Adresse Ihres Windows-Computers mit mehreren Back-Ends mit 5172 als Port hinzu

Maxconn stellt die Anzahl der Verbindungen dar - ersetzen Sie 10 durch den Grenzwert # (unter 20000)

server1 server2 sind einfache Namen und keine Schlüsselwörter

```
server server1 10.150.99.107:5172 maxconn 10

server server2 10.150.99.107:5172 maxconn 10
```

4 Jetzt überprüfen Sie die HAProxy-Konfigurationsdatei mit dem Befehl **sudo haproxy -f /etc/haproxy/haproxy.cfg -c**.

Wenn die Konfiguration gültig ist, wird die folgende Meldung angezeigt:

Configuration file is valid (Konfigurationsdatei ist gültig)

5 Jetzt starten Sie den NetBackup-Dienst neu mithilfe des folgenden Befehls:

Sudo service haproxy restart

6 **Befehl zum Stoppen des HAProxy-Dienstes**

Sudo service haproxy stop

7 **Befehl zum Überprüfen der Version von HAProxy**

Sudo haproxy –f

8 **Befehl zum Deinstallieren von HAProxy**

Sudo apt-get remove haproxy

oder

Sudo apt-get purge –auto-remove haproxy

Installieren von Teradici Device Proxy-Servern

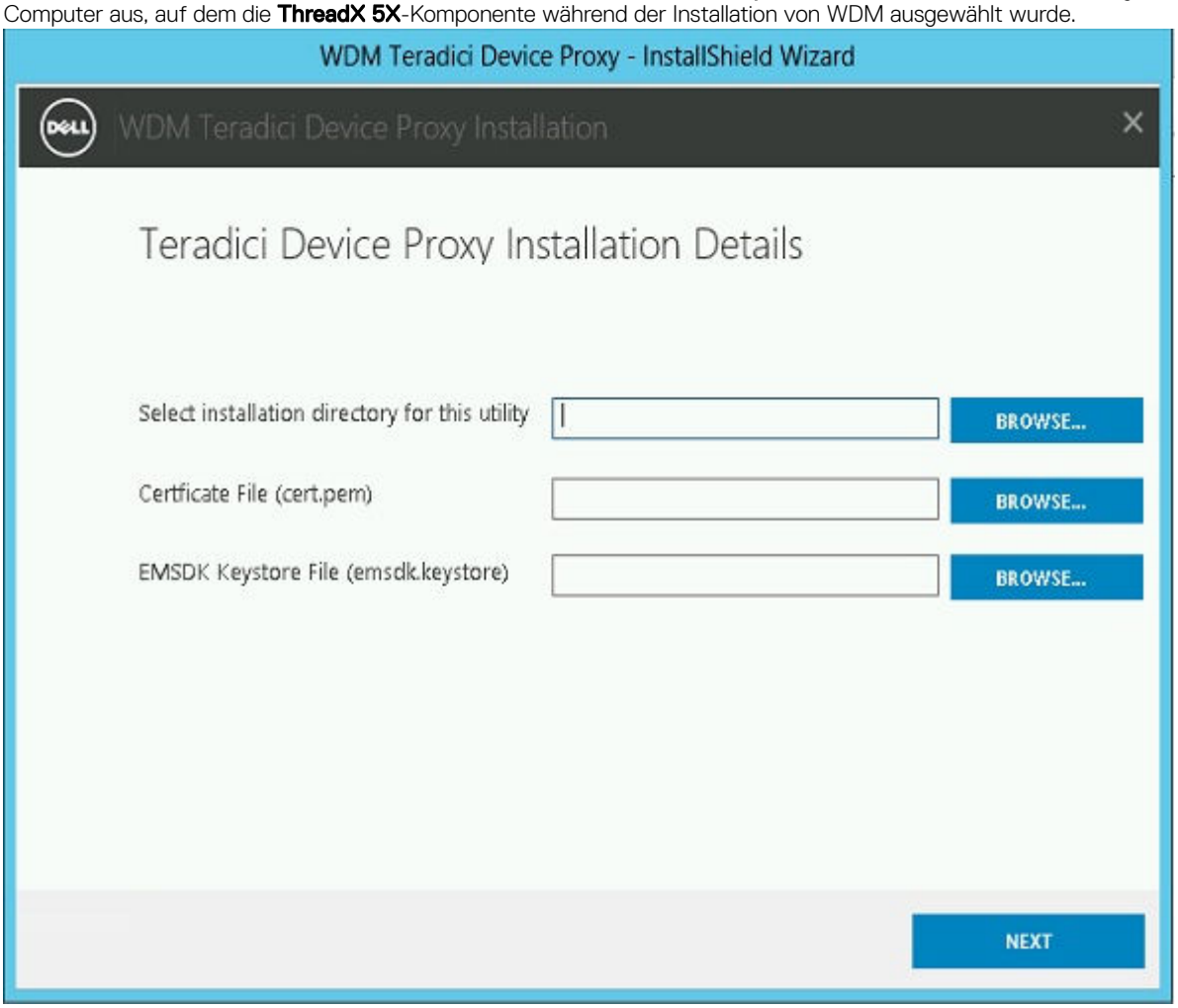
Teradici Device Proxy-Server können auf Servern installiert werden, auf denen die folgenden Betriebssysteme ausgeführt werden:

- Windows 2012
- Windows 2012 R2
- Windows 2008 R2 x64
- Windows Server 2016

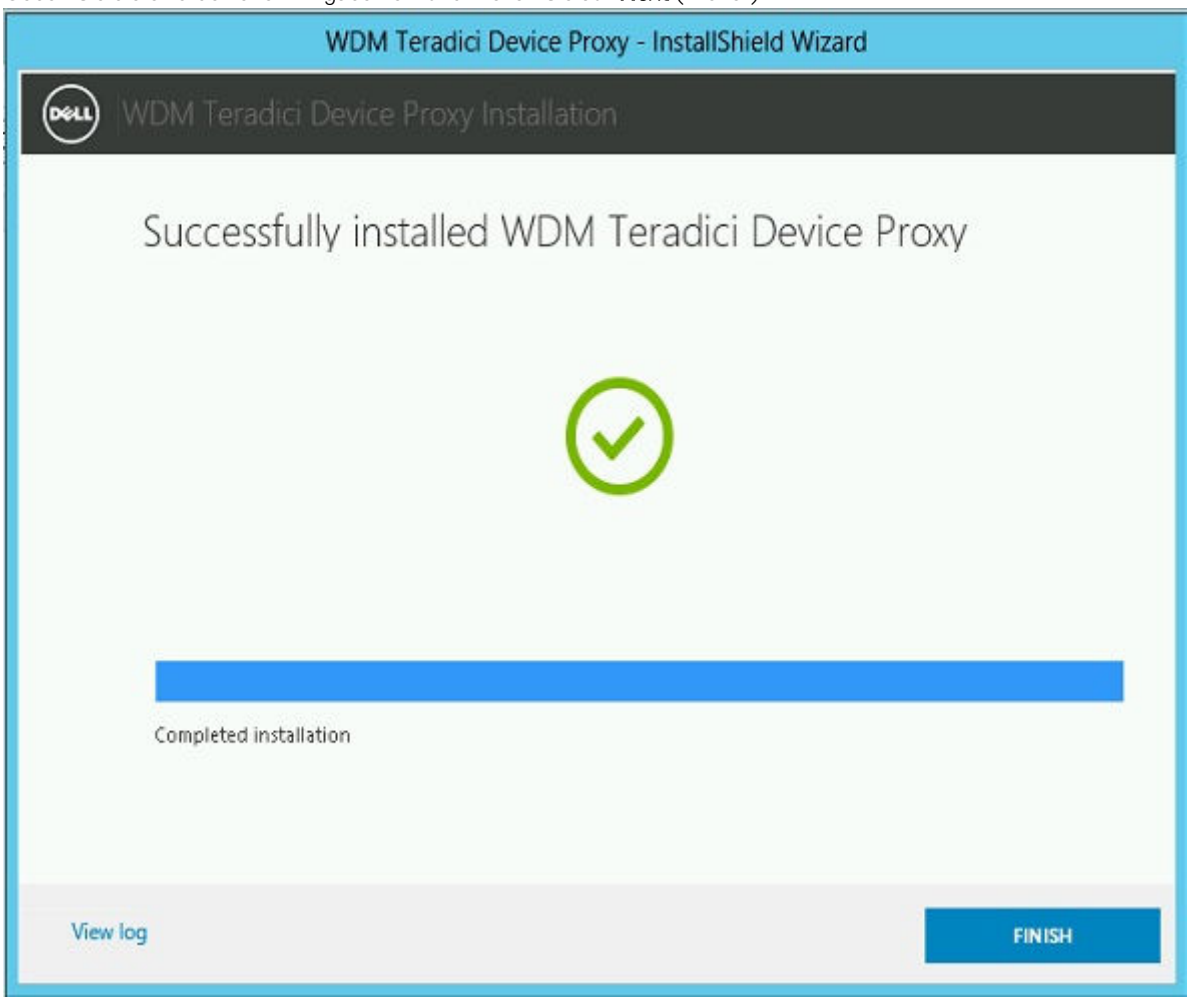
Führen Sie die Schritte zum Installieren des Teradici Device Proxy-Diensts aus:

1 Melden Sie sich als Administrator beim System an.
2 Kopieren Sie den Ordner **WDM installer** (WDM-Installationsprogramm) auf den Zielcomputer.
3 Gehen Sie zum Ordner **TeradiciDeviceProxy**.
4 Doppelklicken Sie auf die Datei **WDMTeradiciDeviceProxy.exe**, um diese zu installieren.
5 Geben Sie die folgenden Details ein:
   a Wählen Sie den Pfad aus, unter dem Sie Teradici Device Proxy und die abhängigen Komponenten installieren möchten.
   b Wählen Sie die Datei **Cert.pem** aus dem Ordner **<WDM-Installationsspeicherort>\Teradici** auf dem Computer aus, auf dem die **ThreadX 5X**-Komponente während der Installation von WDM ausgewählt wurde.

c Wählen Sie die Datei **emsdk.keystore** aus dem Ordner **<WDM-Installationsspeicherort>\Teradici\EMSDK\config** auf dem Computer aus, auf dem die **ThreadX 5X**-Komponente während der Installation von WDM ausgewählt wurde.



6 Geben Sie die erforderlichen Eingaben ein und klicken Sie auf **Next** (Weiter).



7 Klicken Sie auf **Finish** (Fertigstellen).

8 Das Installationsprotokoll wird unter folgendem Pfad erstellt **<Installationsspeicherort von EMSDK>\Teradici \Detail_TeradiciDeviceProxy.log**.

9 Klicken Sie auf **Start** > **Administrative tools (Verwaltung)** > **Services (Dienste)**.

10 Stellen Sie sicher, dass der ThreadX 5x Manager Windows-Dienst installiert ist und ausgeführt wird.

Hinzufügen von Teradici Device Proxy-Servern zu WDM

Tasks

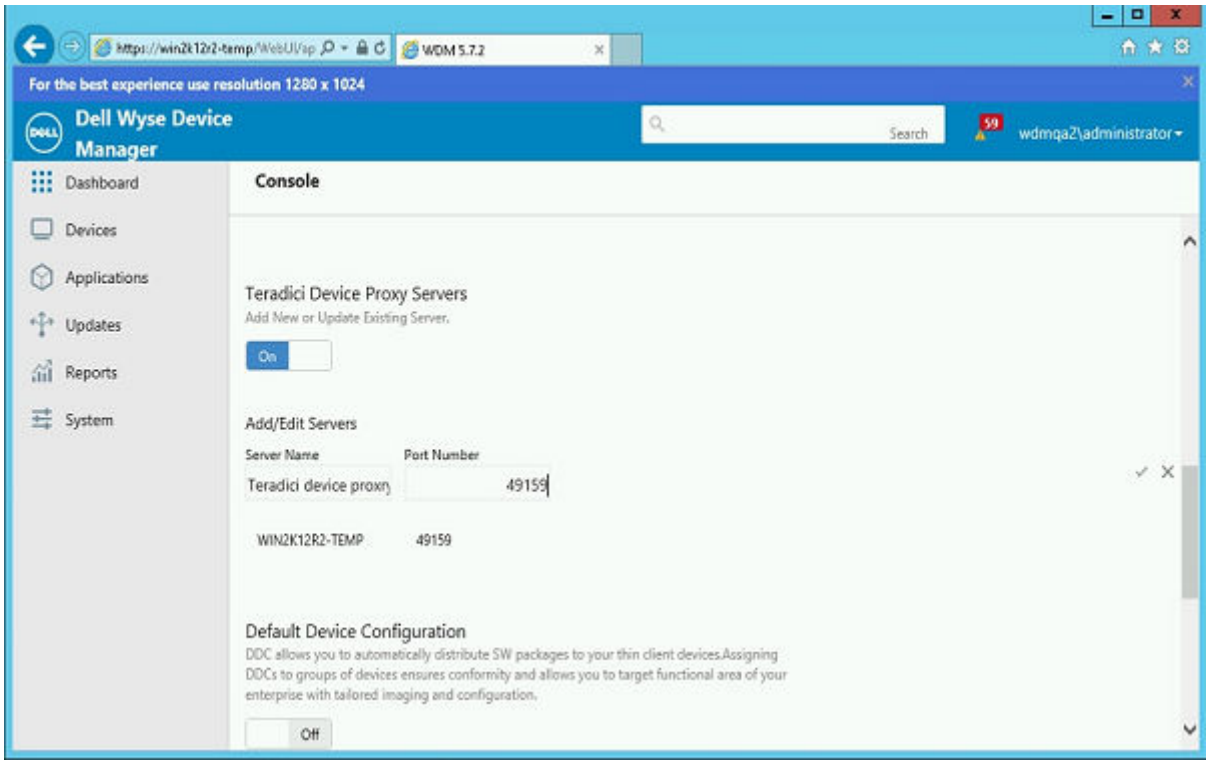
1 Öffnen Sie die WDM Web UI und melden Sie sich als Administrator an.

2 Gehen Sie zu **System** > **Console (Konsole)** und aktivieren Sie die Option **Teradici Device Proxy servers** (Teradici-Gerät Proxy-Server).

3 Klicken Sie auf **Add Server** (Server hinzufügen).

4 Geben Sie den Proxy-Servernamen des Teradici-Geräts in das Feld **Server Name** (Servername) und die Portnummer des Proxy-Dienstes des Teradici-Geräts in das Feld **Port Number** (Portnummer) ein. Der Standardwert ist 49159.

ANMERKUNG: Wenn die Standardportnummer geändert wird, muss sie in WDM aktualisiert werden. Weitere Informationen finden Sie im *Wyse Device Manager 5.7.3 Administrator's guide* (*Administratorhandbuch für den Dell Wyse Configuration Manager 5.7.3)-*



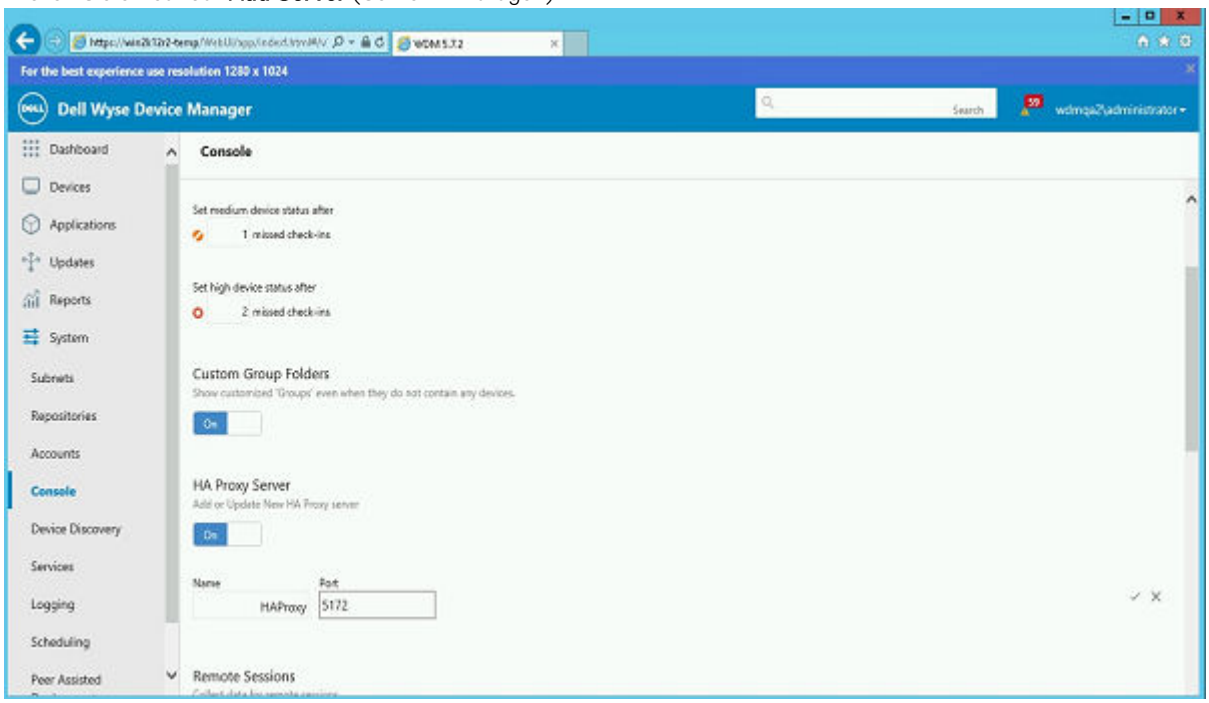
5 Klicken Sie auf das Häkchen auf der rechten Seite des Textfelder, um die Werte zu speichern.

Hinzufügen von HAProxy zu WDM

Befolgen Sie die Schritte zum Hinzufügen von HAProxy zu WDM:

1 Melden Sie sich bei WDM Web UI als Administrator an.
2 Gehen Sie zur Konsolenseite und aktivieren Sie die Option **HAProxy Server** (HAProxy-Server).
3 Klicken Sie auf **Add Server** (Server hinzufügen).
4 Geben Sie den HAProxy-Servernamen in das Servernamenfeld und die Portnummer 5172 ein.

5 Klicken Sie erneut auf **Add Server** (Server hinzufügen).



6 Klicken Sie auf das Häkchen auf der rechten Seite des Textfelds, um die Werte zu speichern.

Neustarten der Threadx-API

Gehen Sie wie folgt vor, um die Threadx API neu zu starten:

1 Melden Sie sich beim Server an, auf dem die WDM ThreadX 5x-Komponente installiert ist.
2 Klicken Sie auf das **Start menu (Startmenü)** > **Administrative tools (Verwaltungstools)** > **Internet information service (IIS) manager (Internet-Informationsdienst (IIS)-Manager)**.
3 Erweitern Sie den Root-Knoten (Host-Name des Servers) und wählen Sie **Application pools (Anwendungspools)** > **ASP .Net v4.0** aus.
4 Klicken Sie mit der rechten Maustaste aus **ASP .Net v4.0** und wählen Sie **Stop** (Anhalten) aus.
5 Klicken Sie erneut mit der rechten Maustaste auf **ASP .Net v4.0** und wählen Sie **Start** aus.
6 Öffnen Sie die WDM Web UI und melden Sie sich als Administrator an.
7 Überprüfen Sie den Status mithilfe des Dashboards.

Überprüfen des Status über das Dashboard

1 Klicken Sie auf das Dashboard und wählen Sie „Teradici Servers“ (Teradici-Server) aus.
2 Stellen Sie sicher, dass der Status von Thread5x, Teradici HAproxy und Teradici Device Proxy-Server „Online“ ist.

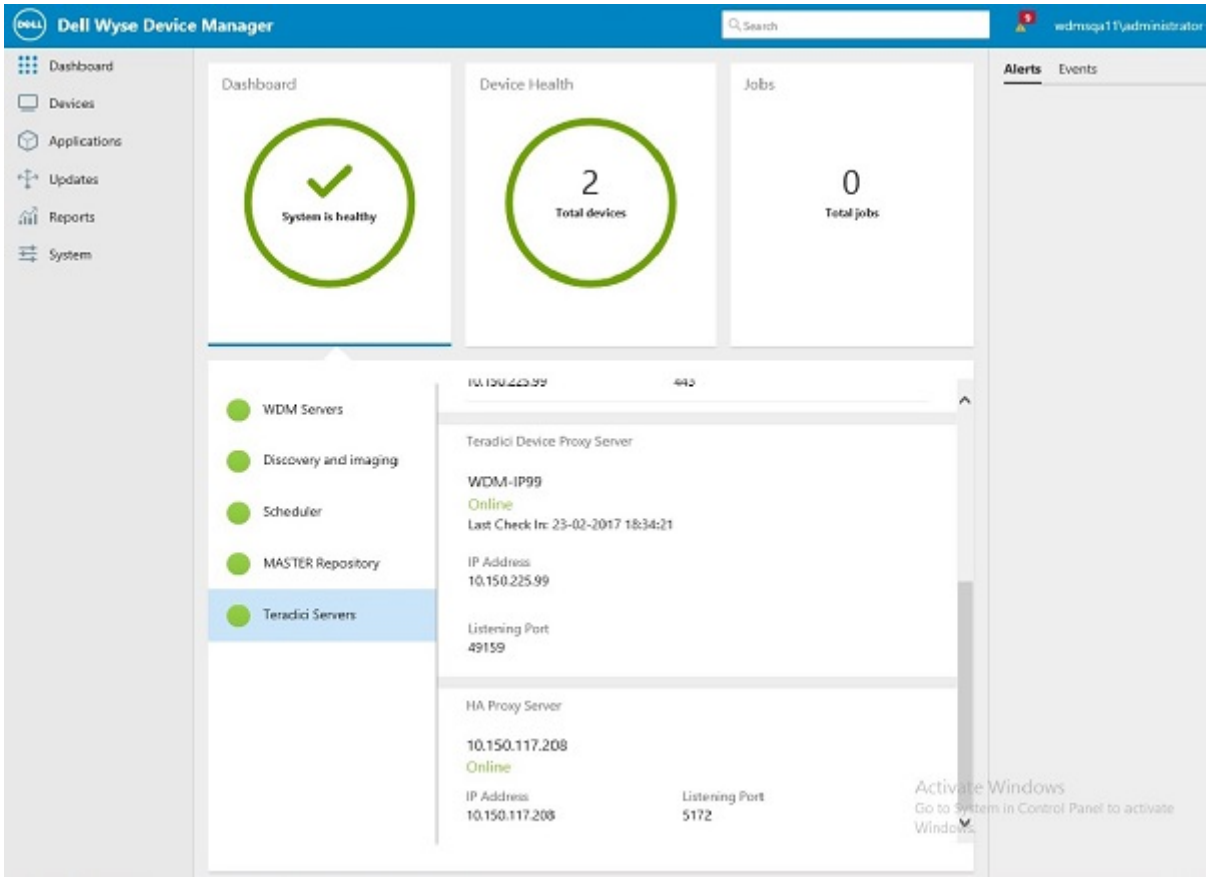


Abbildung 51. Status im Dashboard

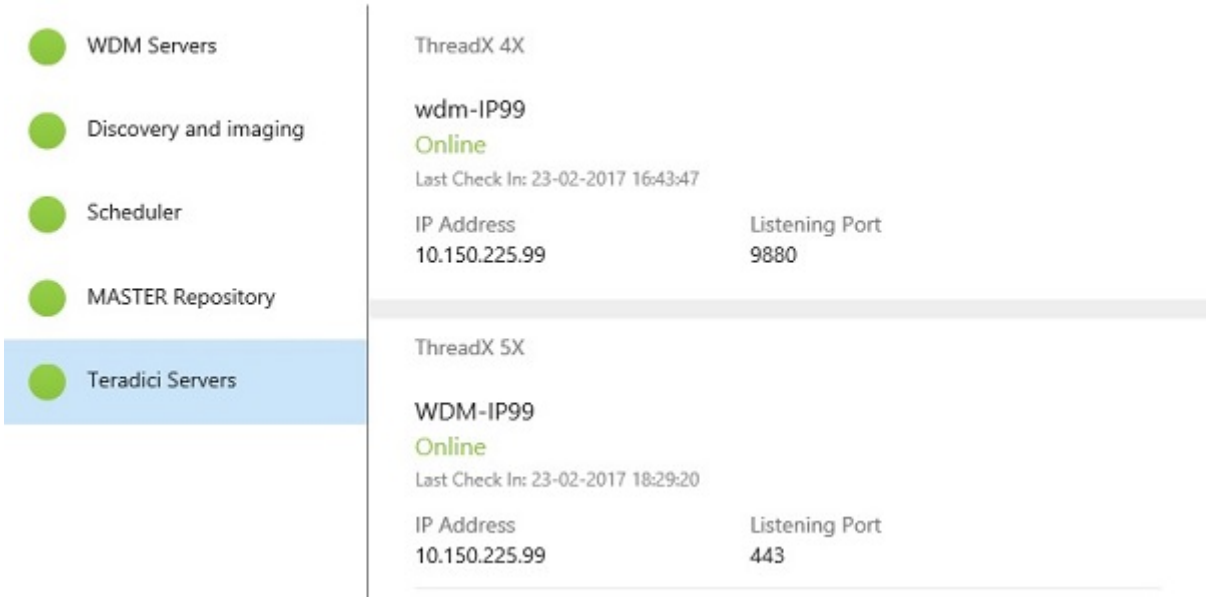


Abbildung 52. Status im Dashboard

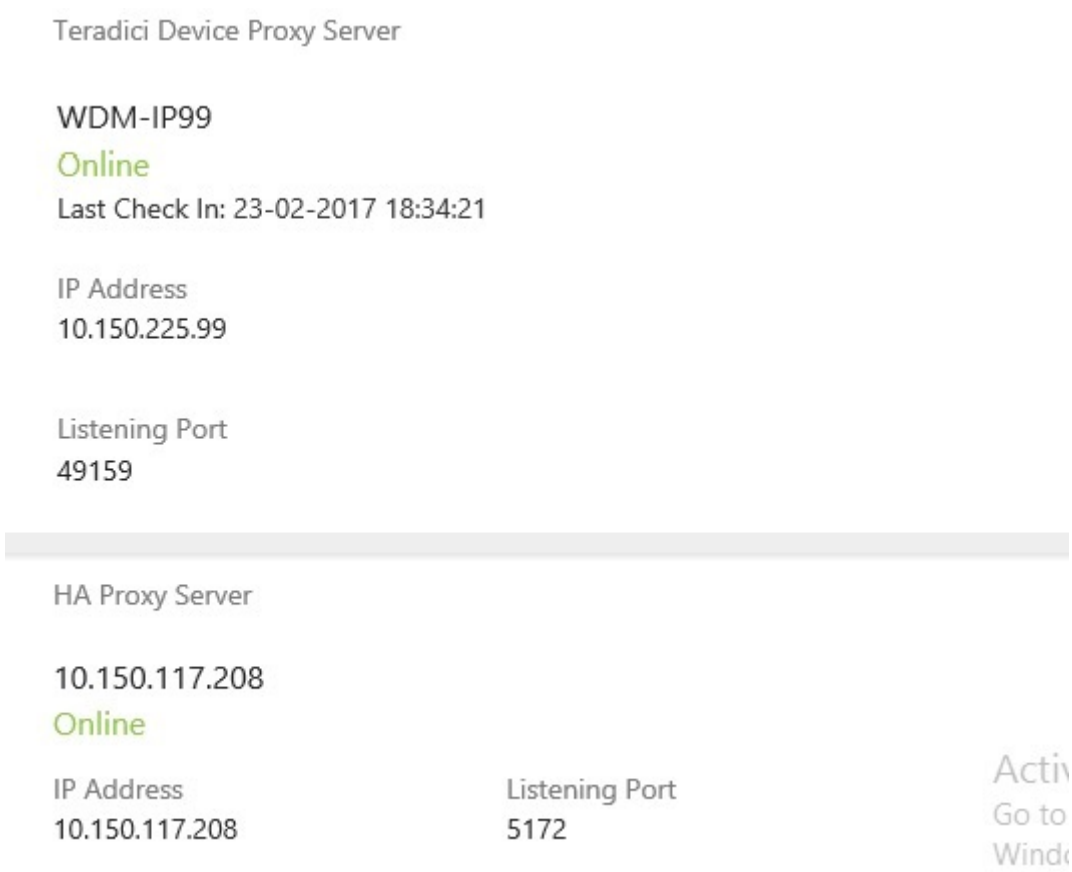


Abbildung 53. Status im Dashboard

7

Konfigurieren von hoher Verfügbarkeit des Web-UI-Service

Wenn Sie eine einzige Instanz des Web-UI-Service haben und dieser Server ausfällt, kann WDM nicht über die Web-UI verwaltet werden. Daher wird hohe Verfügbarkeit des Web-UI-Service empfohlen.

Sie können einen Lastenausgleich-Proxy wie z. B. ARR Reverse Proxy verwenden, wenn die Konfiguration hohe Verfügbarkeit des Web-UI-Service unterstützen muss.

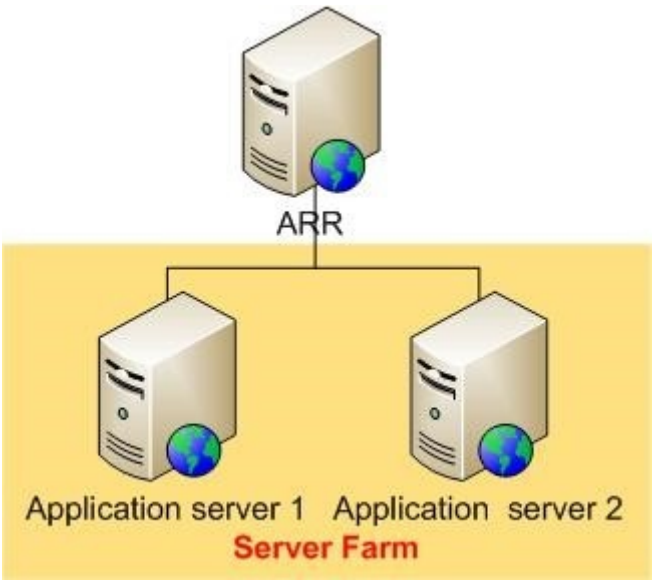


Abbildung 54. Hohe Verfügbarkeit des Web-UI-Service

Themen:

- Einrichten des ARR-Proxyservers
- Installieren der Internetinformationsdienste – IIS
- Installieren des ARR-Moduls
- Ändern des Anwendungspoolprozess-Modells für Application Request Routing
- Erstellen einer Serverfarm aus WDM-UI-Servern
- Konfigurieren von SSL auf dem Proxyserver
- Konfigurieren von Serverfarm-Eigenschaften für Application Request Routing
- Protokollierung auf dem Web-UI-Browser

Einrichten des ARR-Proxyservers

Der Application Routing Request (ARR)-Proxyserver ist die wichtigste Komponente beim Lastenausgleich. Dieser Server empfängt die Anfragen von Thin Client-Systemen und leitet sie zu den verschiedenen WDM-Verwaltungsservern weiter.

Voraussetzung
Es muss IIS 7.0 oder eine höhere Version auf Windows 2008 (beliebige SKU) oder einer höheren Version installiert sein.

Info über diese Aufgabe

Die Einrichtung des ARR-Proxyservers besteht aus folgenden Schritten:

Schritte

1 Installieren Sie IIS.

2 Installieren Sie das ARR-Modul.

3 Ändern Sie das Anwendungspoolprozess-Modell für Application Request Routing

4 Erstellen Sie eine Serverfarm aus WDM-UI-Servern.

5 Konfigurieren Sie SSL auf dem Proxy-Server.

6 Konfigurieren Sie Serverfarm-Eigenschaften für Application Request Routing.

Installieren der Internetinformationsdienste – IIS

1 Melden Sie sich als Administrator an.

2 Gehen Sie zu **Control Panel (Systemsteuerung)** > **Programs and Features (Programme und Funktionen)** > **Turn Windows features on or off (Windows-Funktionen ein- oder ausschalten)**.

3 Wählen Sie die im folgenden Screenshot dargestellten Optionen aus.

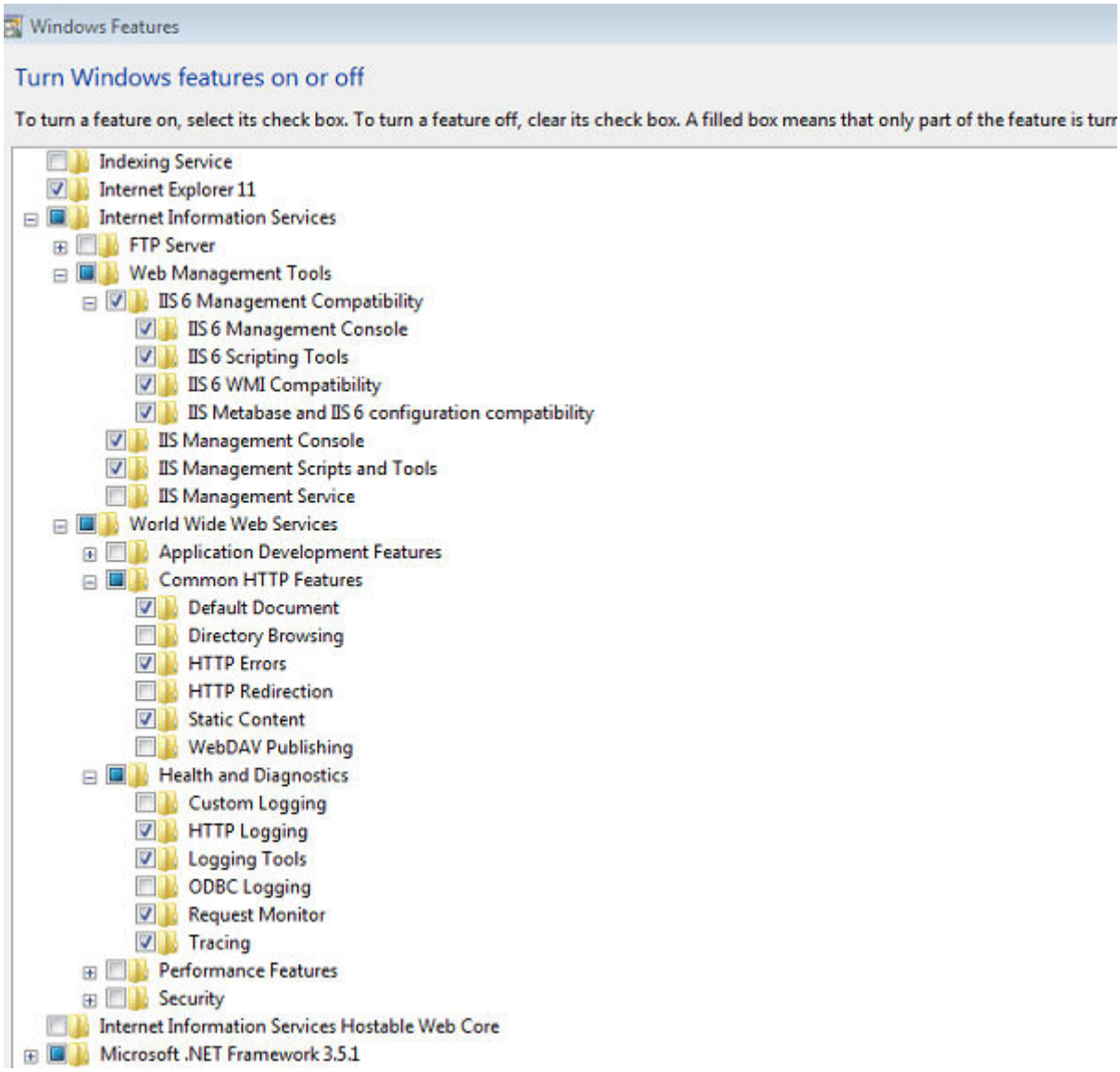


Abbildung 55. Windows-Funktionen

4 Klicken Sie auf **OK**.

Installieren des ARR-Moduls

Sie müssen Application Request Routing Version 3.0 auf dem System installieren, das Sie als ARR-Proxyserver identifiziert haben. Das Installationsprogramm ist auf der Microsoft-Downloadsite unter support.microsoft.com verfügbar. Laden Sie die Datei **ARRv3_0.exe** herunter und installieren Sie sie.

Ändern des Anwendungspoolprozess-Modells für Application Request Routing

Info über diese Aufgabe

Alle HTTP-Anfragen und -Antworten für Websites mit Inhalten durchlaufen Application Request Routing. Der Arbeitsprozess der Standard-Website auf Application Request Routing muss immer ausgeführt werden, unabhängig davon, ob die Arbeitsprozesse für einige der Websites ausgeführt werden oder nicht.

Sie müssen das Leerlauf-Zeitlimit unter dem Anwendungspoolprozess-Modell für Standard-Website deaktivieren.

Schritte

1 Starten Sie IIS Manager.

2 Wählen Sie **Application Pools** (Anwendungspools) aus.

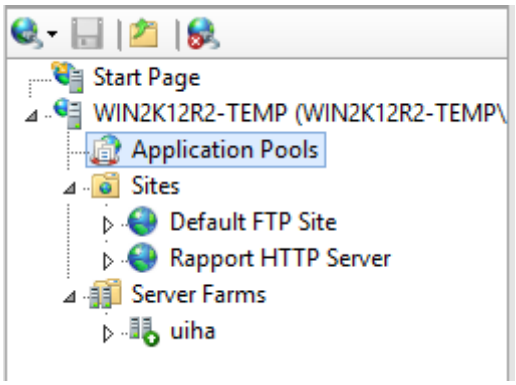


Abbildung 56. Anwendungspools

3 Wählen Sie **DefaultAppPool** aus.

4 Gehen Sie zu **Actions (Aktionen)** > **Edit Application Pool (Anwendungspool bearbeiten)** > **Advanced Settings (Erweiterte Einstellungen)**.

5 Ändern Sie **Idle Time-out (minutes)** (Leerlauf-Zeitlimit (Minuten)) zu 0.

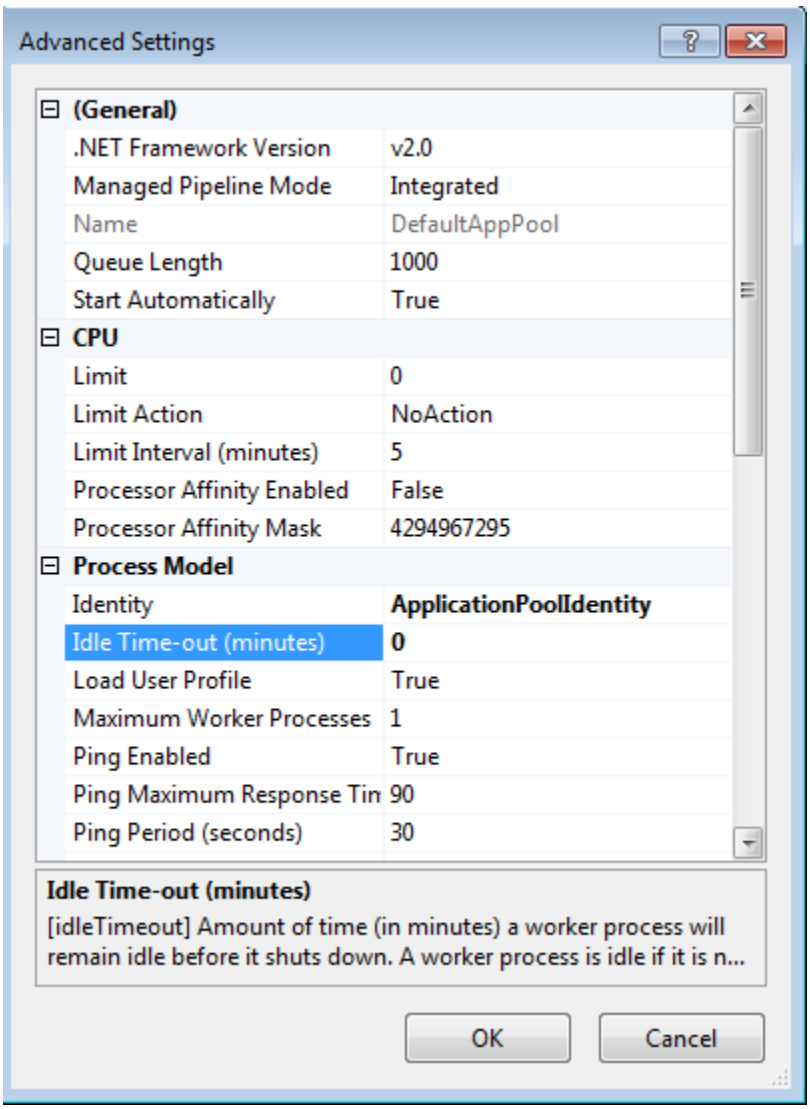


Abbildung 57. Erweiterte Einstellungen

6 Klicken Sie auf **OK**, um die Änderungen zu speichern.

Erstellen einer Serverfarm aus WDM-UI-Servern

1 Starten Sie IIS Manager.

2 Klicken Sie mit der rechten Maustaste auf **Server Farms** (Serverfarmen) und wählen Sie **Create Server Farm** (Serverfarm erstellen) aus.

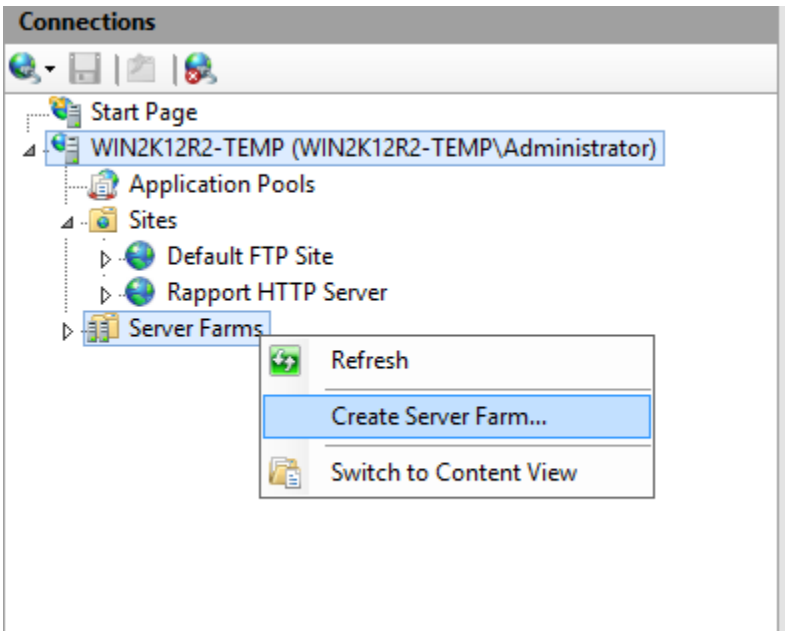


Abbildung 58. Serverfarmen

3 Geben Sie einen Namen für die Serverfarm ein.

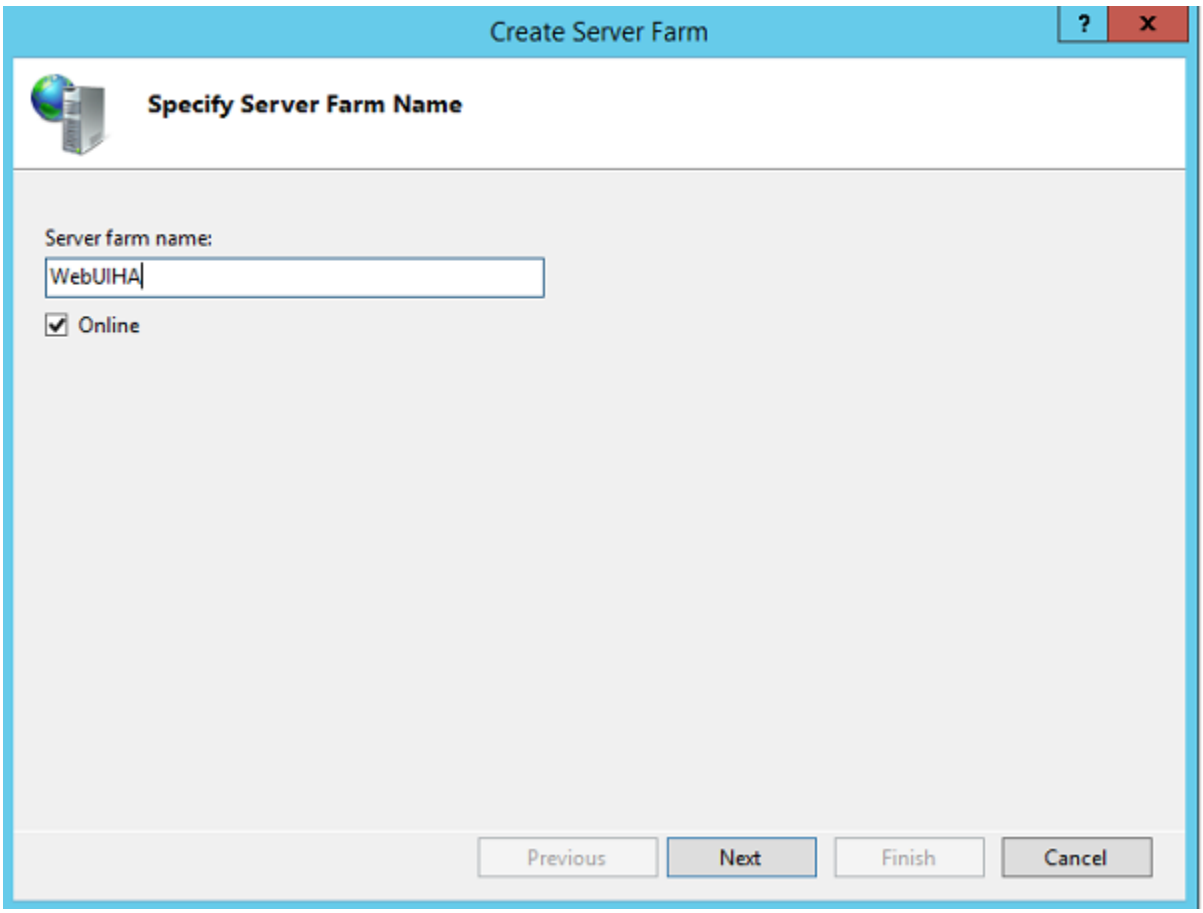


Abbildung 59. Serverfarm erstellen

4 Klicken Sie auf **Next** (Weiter).

5 Auf der Seite **Add Server** (Server hinzufügen) fügen Sie die Anwendungsserver (Web-UI-Server) hinzu.

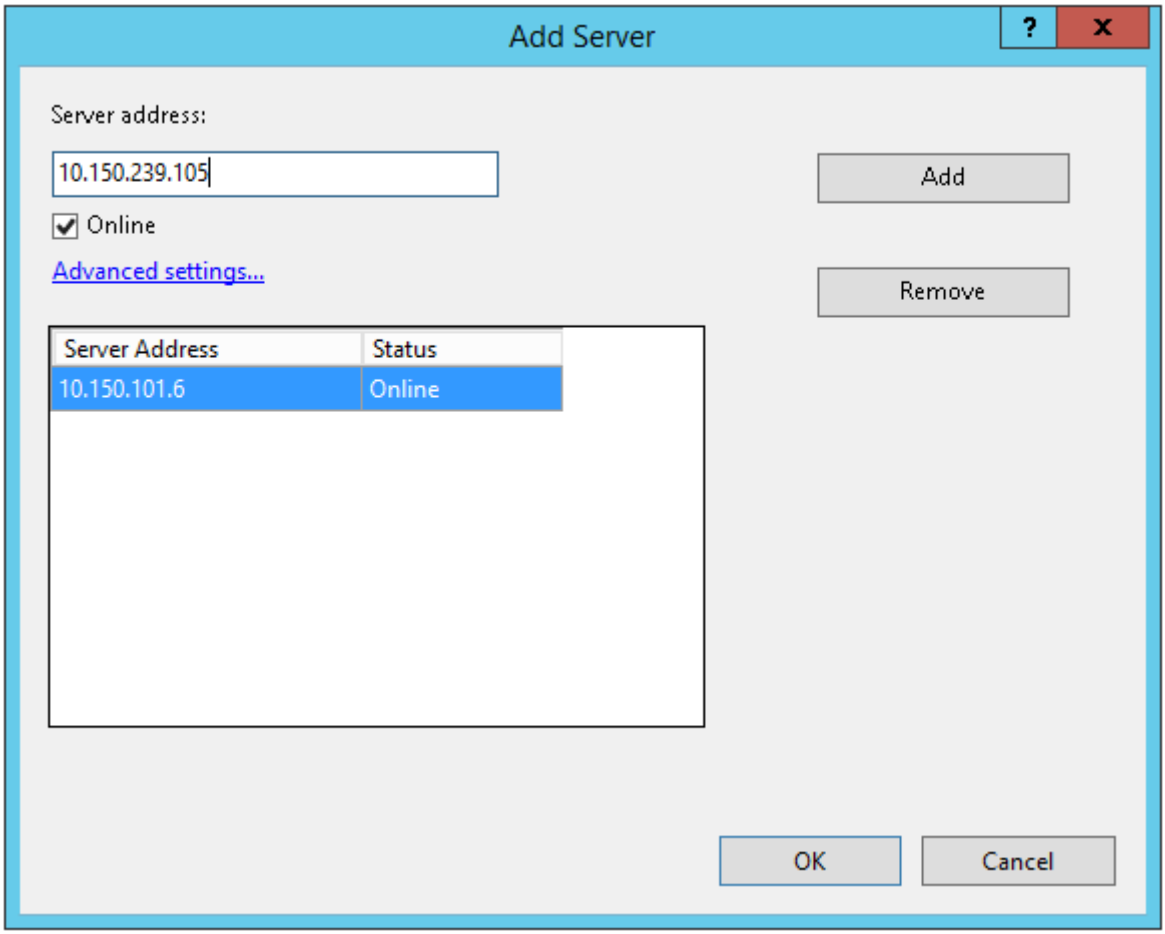


Abbildung 60. Server hinzufügen

6 Klicken Sie auf **Finish** (Fertig stellen), um die Serverfarm mit den eingegebenen Anwendungsservern als Mitglieder der Serverfarm zu erstellen.

Das Fenster **Rewrite Rules** (Regeln umschreiben) wird angezeigt.

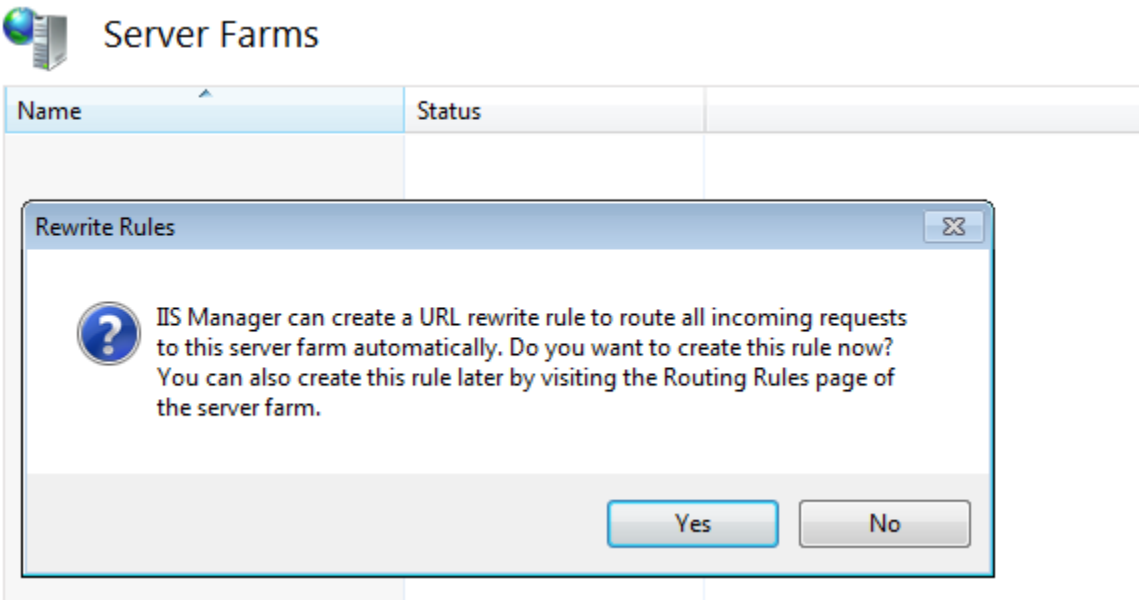


Abbildung 61. Regeln umschreiben

7 Klicken Sie auf **Yes** (Ja), damit der IIS Manager eine URL-Rewrite-Regel für die Weiterleitung aller eingehenden Anfragen an diese Serverfarm erstellen kann.

Konfigurieren von SSL auf dem Proxyserver

Zum Konfigurieren von SSL auf ARR Proxy erstellen Sie ein Domänenzertifikat des Proxy-Servers. Weisen Sie dieses Zertifikat der https-Bindung für die Website zu und aktivieren Sie SSL.

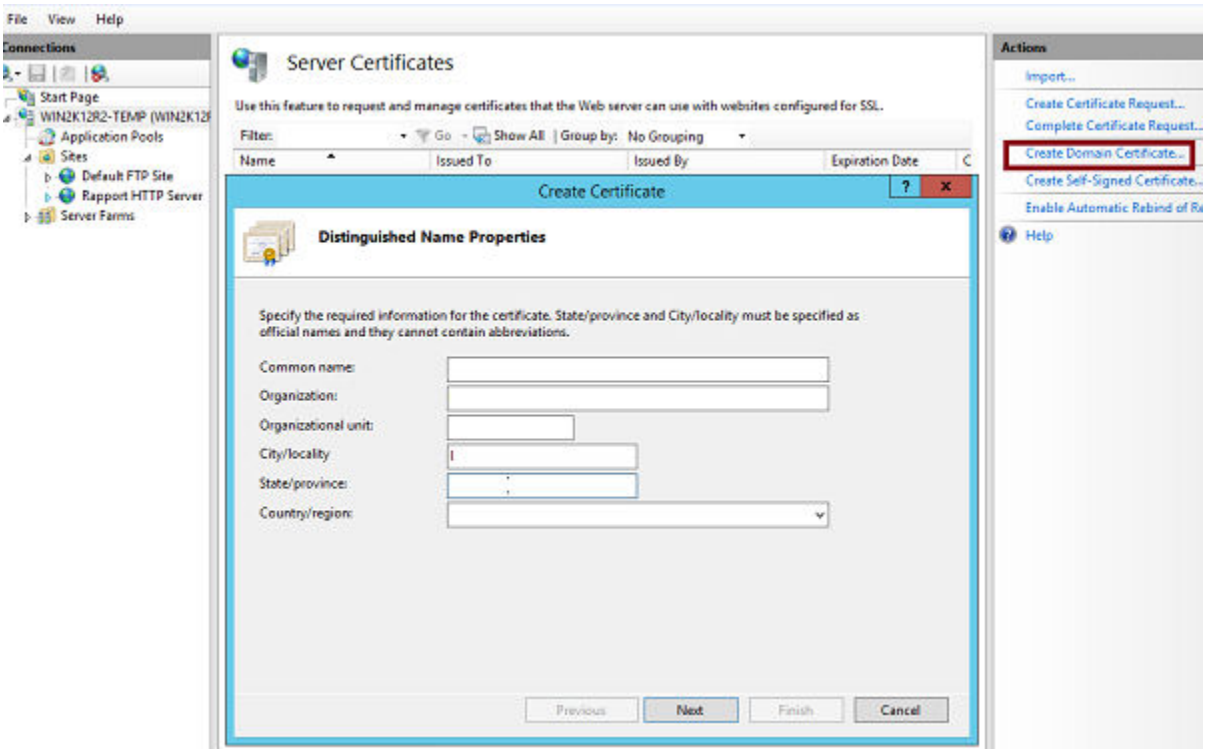


Abbildung 62. Serverzertifikate

Die Kommunikation zwischen dem ARR Proxy-Server und den WDM-Verwaltungsservern muss das HTTPS-Protokoll verwenden. Sie müssen daher die SSL-Auslagerungsfunktion deaktivieren und SSL auf den einzelnen WDM-Verwaltungsservern konfigurieren. Wenn Sie ein selbstsigniertes Zertifikat zum Einrichten von SSL auf dem WDM-Verwaltungsserver verwenden, importieren Sie dieses Zertifikat auf den Speicher der vertrauenswürdigen Stammzertifizierungsstelle für einen lokalen Computer auf dem ARR Internet-Proxyserver, indem Sie die Anweisungen unter support.microsoft.com befolgen. IIS ARR erfordert, dass ein vertrauenswürdiges Zertifikat zwischen ARR und dem Back-End-Server, mit dem es eine Verbindung herstellt, vorliegt; andernfalls gibt es einen Sicherheitsfehler zurück und lehnt die Route zum Back-End-Server ab.

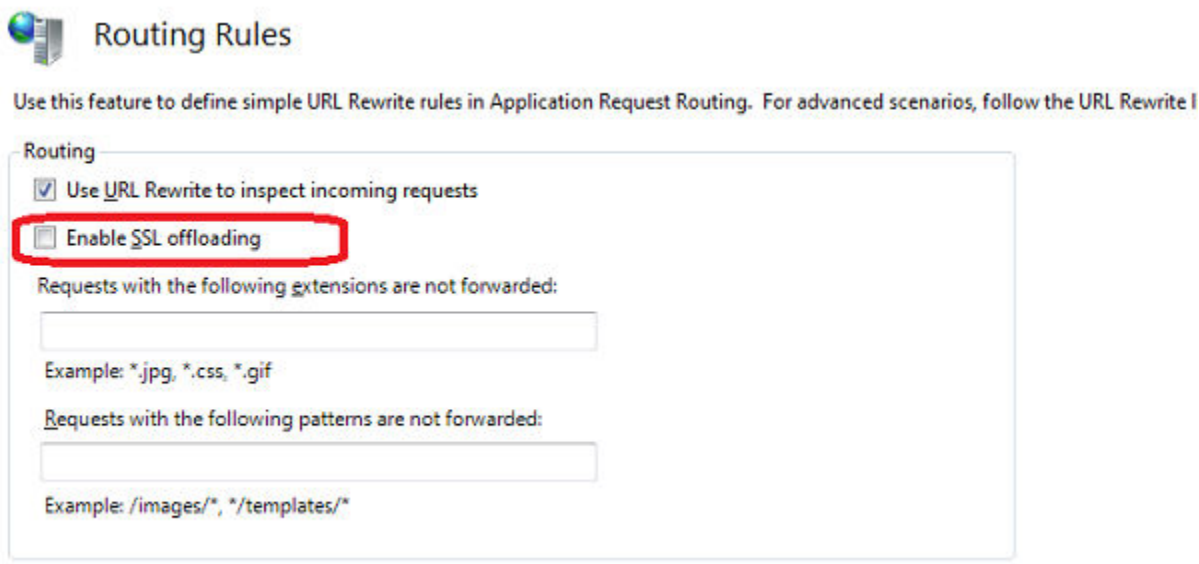


Abbildung 63. Routing-Regeln

Konfigurieren von Serverfarm-Eigenschaften für Application Request Routing

Nachdem die Serverfarm erstellt und definiert wurde, müssen Sie zusätzliche Eigenschaften festlegen, um das Verhalten von ARR zu steuern.

1 Melden Sie sich beim ARR-Proxyserver an und starten Sie den IIS-Server Manager.

2 Wählen Sie die von Ihnen erstellte Serverfarm aus. Die folgenden Optionen werden im rechten Fenster angezeigt:
- Caching (Zwischenspeicherung)
- Health Test (Integritätstest)
- Load Balance (Load-Balance)
- Monitoring and Management (Überwachung und Verwaltung)
- Proxy
- Routing Rules (Routing-Regeln)
- Server Affinity (Serveraffinität)

3 Wählen Sie **Caching** (Zwischenspeicherung) aus.
   a Deaktivieren Sie die Option **Enable disk chache** (Datenträgercache aktivieren), um die Zwischenspeicherung zu deaktivieren.
   b Setzen Sie die **Memory cache duration** (**Speicher-Cache-Dauer**) auf 0.

4 Wählen Sie **Health Test** (Integritätstest) aus.
   a Geben Sie den Fully Qualified Domain Name (FQDN) des ARR-Proxy-Servers im Feld **URL** ein. Der Wert sollte wie folgt lauten: **https://<Proxy-IP|FQDN>/hapi/ping**. Dies ist die URL, die ARR zum Senden von Anfragen an den WDM-Verwaltungsserver verwendet, um den Zustand einer bestimmten Serverfarm zu überprüfen.
   b Legen Sie das Intervall fest, in dem der ARR Health Test den Integritätstest wiederholt. Die Standardeinstellung ist 30 Sekunden. Sie können den Wert auch auf 180 Sekunden einstellen.

c Legen Sie ein Timeout für die URL fest, die Sie angegeben haben. Hierbei handelt es sich um die Zeitspanne, nach der der Server als **Unhealthy** (Fehlerhaft) gekennzeichnet wird, wenn er nicht reagiert.

d Legen Sie den Wert für **Acceptable Status codes** (Zulässige Statuscodes) auf **200-399** fest. Wenn die URL für den Integritätstest einen Statuscode zurückgibt, der nicht mit dem Wert im Feld **Acceptable Status Codes** (Zulässige Statuscodes) übereinstimmt, markiert ARR diesen Server als fehlerhaft.

e Stellen Sie den Textwert **Server Healthy** (Server fehlerfrei) im Feld **Response Match** (Antwortübereinstimmung) ein. Der Text unter **Response Match** (Antwortübereinstimmung) wird anhand der Antwortentität von jedem Server überprüft. Wenn die Antwort vom Server nicht die unter „Response Match" (Antwortübereinstimmung) angegebene Zeichenkette enthält, wird der Server als fehlerhaft markiert.

f Klicken Sie auf **Verify URL** (URL überprüfen). Die Prüfung sollte für alle WDM-Verwaltungsserver in der Serverfarm bestanden werden.

5 Ändern Sie den **Load Balance** algorithm (Lastenausgleichsalgorithmus).

a Wählen Sie **Server variable hash** (**Server-Variable-Hash**) aus der Dropdown-Liste **Load balance algorithm** (Lastenausgleichsalgorithmus) aus.

b Geben Sie für den Wert der **Server Variable** (Server-Variable) `HTTP_WDM_X_USER` ein.

c Klicken Sie auf **Apply** (Anwenden).

6 Doppelklicken Sie auf die Option **Monitoring and Management** (**Überwachung und Verwaltung**), um den Integritätsstatus und andere Statistiken des WDM-Verwaltungsservers anzuzeigen. Sie können den Status manuell auf „Fehlerfrei" einstellen.

7 Doppelklicken Sie auf **Proxy**, um die Proxy-Einstellungen zu konfigurieren:

a Setzen Sie den Wert von Response buffer threshold (**Antwortpufferlimit**) auf 0.

b Deaktivieren Sie die Option **Keep Alive**.

c Ändern Sie die **HTTP**-Version zu **HTTP/1.1**.

d Wählen Sie die Option **Rewrite-Host in Reverse rewrite hose in responde headers** (**Umgekehrter Rewrite-Host in Antwortheader**) aus.

8 Doppelklicken Sie auf **Routing Rules (Routing-Regeln).**

a Klicken Sie im Fensterbereich **Actions** (Aktionen) auf **URL Rewrite (URL-Rewrite).**

b Setzen Sie auf der Seite **Edit Inbound Rule** (**Eingehende Regel bearbeiten**) die Option **Pattern** (Muster) auf **(webui|hapi)/.***.

Durch diesen Schritt wird sichergestellt, dass der ARR-Proxyserver nur die für den WDM-Verwaltungsserver bestimmten URL-Anforderungen an die Serverfarm weiterleitet.

Der Serverfarmeigenschaften sind nun konfiguriert.

Protokollierung auf dem Web-UI-Browser

1 Melden Sie sich bei der Web-UI über die Proxy-IP oder den FQDN in der Browser-URL an.

2 Wenn der angemeldete Server basierend auf dem obigen Integritätstest fehlerhaft wird, meldet sich die Web-UI ab.

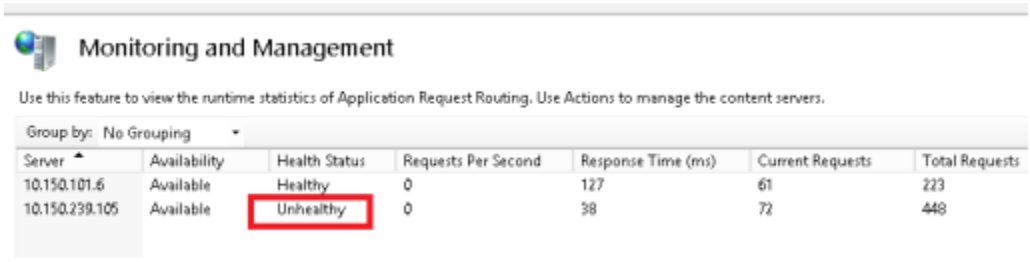


Abbildung 64. Monitoring and Management (Überwachung und Verwaltung)

3 Melden Sie sich erneut an, um eine Verbindung zu einem anderen funktionsfähigen Back-End-Server herzustellen.

8

Manuelle Installation der WDM-Datenbank mithilfe von Skripten

Dieser Abschnitt enthält Datenbankskripte, die von Wyse Device Manager (WDM) unterstützt werden, sowie zugehörige Details zur Funktionalität.

Themen:

Anforderungen

Unterstützung für vorhandene WDM-Datenbanken

Die WDM-Installation unterstützt SQL Server 2008. Die Datenbank enthält alle SQL Server-Objekte wie Tabellen, Ansichten, gespeicherte Verfahren usw. Das WDM-Installationsprogramm speichert die Datenbank im jeweiligen Ordner (standardmäßig **C:\Program Files (x86)\Wyse\WDM\Database**) und verbindet sie mit dem Servercomputer, auf dem WDM installiert werden muss.

Dann aktualisiert das Installationsprogramm die Serverdetails, Benutzerinformationen, Software Repository-Konfigurationsdetails usw. auf dem Servercomputer.

Empfohlene Möglichkeit zur Installation der WDM-Datenbank

Die Skripts werden zum Installieren der WDM-Datenbank Version 5.7.3 verwendet.

Voraussetzungen: Vor der Ausführung des Skripts muss der Datenbankpfadordner erstellt und die Firewall auf dem Datenbankserver deaktiviert werden.

ANMERKUNG: Die folgenden Skripte müssen in der gleichen Reihenfolge wie aufgeführt ausgeführt werden. Wird diese Anweisung nicht befolgt, müssen Sie die Datenbank löschen und den ganzen Vorgang erneut durchführen.

Skriptdateien

Die folgenden Datenbank-Skriptdateien werden zum Installieren der Datenbank von WDM 5.7.3 verwendet:

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

- CustomizeScript.sql

CreateDatabase.sql

Um die Datenbank manuell zu erstellen, führen Sie das folgende Skript aus:

ANMERKUNG: Die Datenbankskripte werden hier für Anpassungszwecke genannt.

```
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 Die Skriptdatei enthält Skripte zur Erstellung der RapportDB-Datenbank.

2 Benutzer oder Administratoren können den Pfad ändern. Der Standarddateipfad ist C:\Program Files (x86)\Wyse\WDM\Database.

ANMERKUNG: Überprüfen Sie den oben erwähnten Ordner, um den Schritt zu verifizieren. Dieser Ordner sollte Rapport4.mdf und Rapport4.ldf enthalten.

Schema&User.sql

Um ein Benutzerkonto zu erstellen, führen Sie das Skript aus. Sie können Berechtigungen zu jedem Benutzerkonto hinzufügen und zuweisen.

1 Die Skriptdatei enthält die Einzelheiten zum Erstellen von Schemata und Benutzerrollen.

2 Die Standardwerte sind „rapport schema“ (Rapport-Schema) und „rapport user“ (Rapport-Benutzer) Wenn Sie den WDM-Zugriffsbenutzer ändern möchten, können Sie dies hier tun.

Tables.sql

Diese Skriptdatei enthält Skripte für alle Tabellenobjekte und Einschränkungen.

ANMERKUNG: Benutzerdefinierte Änderungen sind in dieser Datei nicht enthalten.

Userdefinedtables.sql

Diese Skriptdatei enthält Skripte für alle Objekte des Typs „User Defined Table“ (Benutzerdefinierte Tabelle).

ANMERKUNG: Benutzerdefinierte Änderungen sind in dieser Datei nicht enthalten.

Views.sql

Diese Skriptdatei enthält Skripte für alle Objekte des Typs „View“ (Ansicht).

ANMERKUNG: Benutzerdefinierte Änderungen sind in dieser Datei nicht enthalten.

Stored_Procedures.sql

Diese Skriptdatei enthält Skripte für alle Objekte des Typs „Stored Procedure“ (Gespeicherte Verfahren).

ANMERKUNG: Benutzerdefinierte Änderungen sind in dieser Datei nicht enthalten.

Default_Table_Data.sql

Diese Skriptdatei enthält Skripte für alle standardmäßigen Tabellendatenwerte wie Betriebssystem, Plattform, Verwaltungstyp, Standardgruppen, Softwarepakete, Standardparameterdetails usw.

ANMERKUNG: Benutzerdefinierte Änderungen sind in dieser Datei nicht enthalten.

CustomizeScript.sql

Diese Skriptdatei enthält Skripte für alle Werte des Typs des Typs „Customize Data“ (Daten anpassen).

Geben Sie während der Ausführung des folgenden Skripts den Datenbankservernamen an. Ein Fehler wird angezeigt, wenn Sie keinen Servernamen eingeben.

ANMERKUNG:

---- Skript anpassen

```
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,
0x44584739353343D3151303452525452464347533834344248583 6)
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

Fehlerbehebung

In diesem Abschnitt wird beschrieben, wie Sie Probleme beheben, die möglicherweise bei der Installation oder Aktualisierung von WDM auftreten.

Themen:

.NET Framework-Installationsfehler in Windows 2012 und Windows Server 2016

Problem: Die Installation von .NET Framework 3.5 auf Windows Server 2012 und Windows Server 2016 schlägt mit dem Fehlercode 0x800F0906 fehl.

Lösung:

1. Methode:

1 Melden Sie sich beim System an, auf dem Sie Windows Server 2012 und Windows Server 2016 installiert haben, und starten Sie den Server-Manager.

2 Installieren Sie mithilfe des **Add Roles and Features (Assistenten zum Hinzufügen von Rollen und Features)** im Server-Manager die .NET Framework 3.5-Features.

3 Geben Sie während der Installation einen alternativen Quellpfad über den Link im unteren Bereich des Assistenten an.

2. Methode:

Geben Sie mithilfe von DISM über die Eingabeaufforderung den Parameter des Quelldateipfads an:

Wenn **D:** beispielsweise das Windows Server DVD-Laufwerk ist, würde der Quelldateipfad wie folgt lauten: DISM /Online /Enable-Feature /FeatureName:NetFx3ServerFeatures /FeatureName:NetFx3 /Source:D:\Sources\sxs.

3. Methode:

1 Melden Sie sich beim System an, auf dem Sie Windows Server 2012 und Windows Server 2016 installiert haben, und starten Sie den Server-Manager.

2 Installieren Sie die Serverrolle **Windows Server Update Services (WSUS)** mithilfe des **Add Roles and Features (Assistenten zum Hinzufügen von Rollen und Features**) im Server-Manager.

3 Geben Sie mithilfe von DISM über die Eingabeaufforderung den Parameter des Quelldateipfads an: DISM /Online /Enable-Feature / FeatureName:NetFx3ServerFeatures /FeatureName:NetFx3.

4 Stellen Sie sicher, dass der Windows Update-Dienst ausgeführt wird, und eine Verbindung zum Windows Update Store, über den die erforderlichen Komponenten abgerufen werden können, hergestellt werden kann.

Fehler beim Anfügen der Datenbank

Problem: Beim Anfügen der Datenbank auf dem Windows Server 2012 an den SQL Server 2012 tritt ein Fehler auf.

Lösung:

Führen Sie den SQL-Dienst „MSSQLSERVER“ mithilfe des „LocalSystem“-Kontos auf dem System aus, für das die WDM-Installation vorgesehen ist.

Wiederholen Sie die WDM-Installation.

Fehler während der Installation der WDM-Datenbank in einem verteilten Setup

Problem: Wenn Sie die WDM-Datenbank auf einem separaten System installieren, auf dem die unterstützte Version von SQL Server installiert ist, wird möglicherweise der folgende Fehler beim Ausführen der Datei **Setup.exe** angezeigt: *Setup was unable to initialize the required libraries. (Fehler beim Initialisieren der erforderlichen Bibliotheken während des Setups)*.

Lösung: Stellen Sie sicher, dass **Microsoft Visual C++ Redistributable 2008** (**Version 9.0.21022**) installiert ist. Sie müssen zu **Start** > **Control Panel (Systemsteuerung)** > **Programs (Programme)** navigieren, um zu überprüfen, ob das Redistributable Package installiert ist. Wenn es nicht installiert ist, müssen Sie es manuell installieren, indem Sie **vcredist_x86.exe** ausführen. Diese Datei finden Sie im Ordner **Prereq** des WDM-Installationsprogramms.

Fehlschlagen der Datenbankinstallation nach manueller Deinstallation von SQL Server Express 2014

Problem: Die Installation der WDM-Datenbank schlägt fehl, nachdem Sie die vorhandene SQL Server Express 2014-Version manuell deinstallieren und die Option **Install New Database** (**Neue Datenbank installieren**) im Installationsprogramm verwenden.

Lösung: So lösen Sie das Problem:

1 Deinstallieren Sie SQL Server Express 2014 R2 mit der Option „Add\Remove Programs“ (Programme installieren/deinstallieren).

2 Öffnen Sie das Fenster **Services** (**Dienste)** unter **Control Panel (Systemsteuerung)** > **Administrative Tools (Verwaltungs-Tools)**.

3 Löschen Sie den **MSSQL$RapportDb**-Dienst.

4 Löschen Sie **MSSQL12.RAPPORTDB** aus dem SQL Server Express-Installationsordner.

5 Löschen Sie den Registry-Eintrag **RapportDB** unter **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server \Instanznamen\SQL**.

6 Löschen Sie den Registry-Eintrag **MSSQL10_50.RAPPORTDB** unter **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server**.

7 Löschen Sie den Registry-Eintrag **RAPPORTDB** unter **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server**.

8 Starten Sie das WDM-Installationsprogramm neu.

Nach dem Upgrade von WDM 5.5.1 auf WDM 5.7 ist das Software Repository nicht sicher

Problem: Wenn die Weboberfläche beim Upgrade ausgewählt wird, wird der Verwaltungsserver auf Https konfiguriert. Die WDM-Software Repository wird jedoch nicht über das Installationsprogramm konfiguriert.

Lösung: Setzen Sie das Software Repository in der WDM-GUI manuell auf HTTPs. Um die Einstellung manuell vorzunehmen, gehen Sie zu **Configuration Manager (Konfigurations-Manager)Software Repository**.

Fehlerbehebung nach der Bereitstellung

Problem: HTTP-Fehler 404.0 - Nicht gefunden. Die Web.config-Datei von HApi, die mit einem URL-Routing-Modul hinzugefügt werden soll, fehlt.

Lösung: Fügen Sie der Web.config-Datei von HApi ein URL-Routing-Modul Folgendes hinzu:

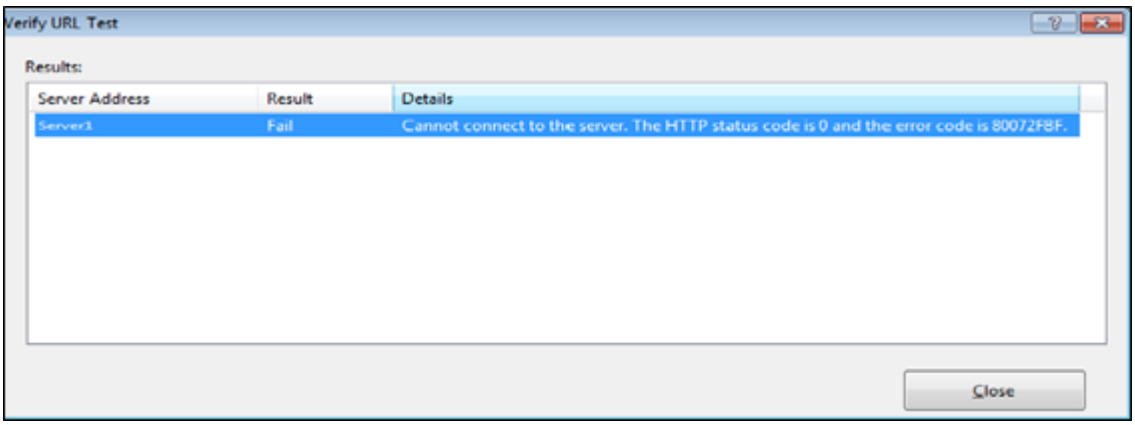
```
<system.webserver>
<modules>
<remove name= "urlroutingmodule-4.0"/>
<add name= "urlroutingmodule-4.0" type="system.web.Routing.urlroutingmodule" precondition="" />
</modules>
```

Fehlerbehebung bei Lastenausgleichsproblemen

In diesem Abschnitt wird die Behebung verschiedener Probleme, die beim Lastenausgleichs-Setup auftreten könnten, beschrieben.

Fehlschlagen des Integritätstests bei ARR-Proxy mit SSL

Problem: Wenn der ARR-Proxy feststellt, dass das digitale Zertifikat des Back-End-Servers nicht vertrauenswürdig ist, schlägt der Integritätstest möglicherweise mit dem Fehlercode 80072F8F fehl.



Lösung: Importieren Sie das Zertifikat, das für das SSL-Setup auf dem WDM-Verwaltungsserver verwendet wird, in den Ordner **Trusted Root Certificate Authorities store for a local computer** (Vertrauenswürdige Stammzertifizierungsstellen des Zertifikatspeichers des lokalen Computers) im ARR-Proxysystem. Lesen Sie hierzu technet.microsoft.com.

Zurücksendung des HTTP-Fehlercodes 502.3 seitens des ARR-Proxy

Problem: Der ARR-Proxy gibt den HTTP-Fehlercode 502.3 für ältere WDM-Agenten zurück (HAgents), die beim Anmelden nicht den Tag **HTTPHEADSUPP=2** senden. Wenn der HAgent beim Anmelden nicht den Tag **HTTPHEADSUPP=2** sendet, sendet der Verwaltungsserver daraufhin nicht den HTTP-Statuscode-Header (200 OK) und der ARR-Proxy gibt den Fehler aus. Nur Clients, die den Wert **2** senden, werden im Setup des Lastenausgleichs unterstützt.

Lösung: Sie können die folgende Abfrage auf der WDM-Datenbank ausführen und den Wert ablesen:

```
SELECT [HttpHeadSupp]
FROM    [ClientNetwork]
where  [MAC] = <ClientMac>
```

Zurücksendung des HTTP-Fehlercodes 502.4 seitens des ARR-Proxy

Problem: Der ARR-Proxy-Server gibt unter Umständen den HTTP-Fehlercode 502.4 zurück, wenn einer der Verwaltungsserver (HServers) nicht verfügbar ist. Der Status von allen HServern in der **Serverfarm** kann dabei auf **Fehlerhaft** gesetzt werden, weil die konfigurierten Integritätstests nicht bestanden wurden.

Lösung: Um dieses Problem zu beheben, führen Sie folgende Schritte durch:

1 Melden Sie sich beim ARR-Proxyserver an und starten Sie den IIS-Server Manager.

2 Wählen Sie die von Ihnen erstellte Serverfarm aus und im rechten Fensterbereich dann **Überwachung und Verwaltung**.

3 Wählen Sie die HServer aus und klicken Sie dann im Fensterbereich **Aktion** auf **Server als funktionsfähig festlegen**.

4 Wenn die Last auf dem HServer hoch ist, versuchen Sie, die Werte für **Intervall** und **Timeout** im Feature **Integritätstest** zu erhöhen.

Aktivieren von SSL-Offloading auf Proxy

Der Lastenausgleich wird nur beim HTTPS-Setup unterstützt. Wenn Sie für das Debugging die Antwort des Verwaltungsservers (HServer) bei der **Wireshark** sehen möchten, dann können Sie die HServer-Proxykommunikation zu HTTP ändern.

1 Melden Sie sich beim ARR-Proxyserver an und starten Sie den IIS-Manager.

2 Doppelklicken Sie auf die Funktion **Routing Rules** (Routing-Regeln) und wählen Sie die Option **Enable SSL offloading** (SSL-Offloading aktivieren) aus.

3 Aktivieren Sie sowohl die HTTP- als auch die HTTPS-Bindung auf der Website auf den HServer-Maschinen und deaktivieren Sie die Option **Require SSL** (SSL erforderlich) in den **SSL-Einstellungen**.

..

Endlosschleife während der Installation

Problem: Die Installation wird für unbestimmte Zeit fortgesetzt, während Microsoft Visual C++ Redistributables oder Microsoft SQL Express 2008 installiert werden. Es werden Windows 2012 Standard und Windows 2012 R2 als Betriebssysteme unterstützt.

Lösung: Öffnen Sie den Task-Manager und prüfen Sie, ob des **Windows Modules-Installationsprogramm** auf Ihrem Server ausgeführt wird oder nicht. Wenn dieses Verfahren ausgeführt wird, müssen Sie es beenden und die Installation wieder aufnehmen. Starten Sie den Server neu, nachdem die Installation abgeschlossen ist.

Lastenausgleichsproblem

Problem: Der Proxyserver antwortet nicht, wenn die IPv6-Adresse aktiviert ist.

Lösung: Deaktivieren Sie die IPv6-Adresse beim Setup des Lastenausgleichs.

WDM-Upgrade auf Windows 2008 SP2 32-Bit

Problem: Für das Upgrade von WDM 5.7 auf Windows 2008 SP2 32-Bit aktivieren Sie den Windows Update Service.

Lösung: Für das Upgrade von WDM 5.7 auf Windows 2008 SP2 (32 Bit) aktivieren Sie den Windows Update-Dienst, um den Hotfix KB980368 zu installieren. Nach der Installation des Hotfix KB980368 deaktivieren Sie den Hotfix KB980368 zur Installation von WDM 5.7.

Fehlschlagen der Installation des WDM-Upgrades

Problem: Die Installation des WDM-Upgrades schlägt fehl, wenn Sie eine Verbindung zum Software-Repository herstellen.

Lösung: Einer der Gründe für dieses Problem besteht darin, dass der Computername für das Setup mehr als 16 Zeichen lang ist. Dies führt dazu, dass der Computername und der NetBIOS-Name (gekürzt auf 15 Zeichen) für das Setup nicht übereinstimmen. Um dieses Problem zu lösen, überprüfen Sie, ob die oben erwähnten Systemvariablen unterschiedlich sind. Falls ja, installieren Sie WDM im Rahmen eines Setup mit einem Hostnamen, der maximal 15 Zeichen lang ist, und führen Sie das Installationsprogramm für die Aktualisierung anschließend erneut aus.

Problem beim Setup der Cloud-Umgebung

Problem: Es wird ab und zu eine Fehlermeldung angezeigt, wenn Sie die Datei `setup.exe` während der WDM-Installation in der Cloud-Umgebung ausführen.

Lösung

- **Szenario 1 - Nur die Fehlermeldung wird angezeigt**

  Schließen Sie das Dialogfeld mit der Fehlermeldung und führen Sie anschließend erneut die Datei `setup.exe` aus.
- **Szenario 2 - Es wird eine Fehlermeldung zusammen mit dem Willkommensbildschirm im Hintergrund angezeigt.**

  Schließen Sie das Dialogfeld mit der Fehlermeldung sowie den Willkommensbildschirm und führen Sie anschließend erneut die Datei `setup.exe` aus.

Fehler bei der Installation von WDM im Upgrade-Setup

Problem: Wenn Sie während der Installation von WDM andere Datenbankbenutzer als den Standardbenutzer verwenden, können Sie mit der Installation von WDM im Upgrade-Setup nicht fortfahren. Die Fehlermeldung **Unable to proceed with the installation, aborting installation (Installation kann nicht fortgesetzt werden; Installation wird abgebrochen)** wird angezeigt.

Lösung:

- Öffnen Sie die WDM-Benutzeroberfläche.
- Klicken Sie mit der rechten Maustaste auf **Configuration Manager (Konfigurationsmanager)** und wählen Sie **Utilities** > **Database Credential Manager (Manager für Datenbank-Anmeldeinformationen)**.
- Es wird eine Bestätigungsmeldung angezeigt. Klicken Sie auf **OK**.
- Geben Sie den Benutzernamen und das Kennwort des Benutzers ein, das Sie bei der Installation von WDM verwendet haben. Klicken Sie auf **OK**, um fortzufahren.
- Schließen Sie nun die WDM-Benutzeroberfläche und fahren Sie mit der Installation fort.
- Führen Sie den **Datenbank Credential Manager (Manager für Datenbank-Anmeldeinformationen)** unter dem Installationspfad `C:\Program Files(X86)\Wyse\WDM\Utilities\Database` nach der Installation erneut aus.
- Geben Sie Ihren bei der Installation von WDM verwendeten Benutzernamen und das Kennwort ein, und führen Sie anschließend einen Neustart des Servers durch.