

# PRIMERGY ServerView Suite

ServerView Deployment Manager V5.0

## **Comments... Suggestions... Corrections...**

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to [manuals@fujitsu-siemens.com](mailto:manuals@fujitsu-siemens.com).

## **Certified documentation according to DIN EN ISO 9001:2000**

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2000.

cognitas. Gesellschaft für Technik-Dokumentation mbH  
[www.cognitas.de](http://www.cognitas.de)

## **Copyright and Trademarks**

Copyright © 2008 Fujitsu Siemens Computers GmbH.

All rights reserved.

Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

---

# Contents

<b>1</b>	<b>Introduction . . . . .</b>	<b>9</b>
<b>1.1</b>	<b>Target Groups and Purpose of This Manual . . . . .</b>	<b>11</b>
<b>1.2</b>	<b>Changes Since the Previous Version . . . . .</b>	<b>12</b>
<b>1.3</b>	<b>System Requirements . . . . .</b>	<b>14</b>
1.3.1	Deployment Manager Packages . . . . .	14
1.3.2	Supported Operating Systems for Image Creation/Cloning . . .	15
1.3.3	Software Packages on the Deployment Server . . . . .	16
<b>1.4</b>	<b>Notational Conventions . . . . .</b>	<b>17</b>
<b>2</b>	<b>Deployment - Overview . . . . .</b>	<b>19</b>
<b>2.1</b>	<b>Supported Server Systems . . . . .</b>	<b>20</b>
<b>2.2</b>	<b>Cloning Process . . . . .</b>	<b>23</b>
2.2.1	Reference Installation . . . . .	24
2.2.2	Image Creation . . . . .	27
2.2.3	Cloning . . . . .	29
<b>2.3</b>	<b>Mass Remote Installation . . . . .</b>	<b>33</b>
<b>2.4</b>	<b>System Architecture . . . . .</b>	<b>36</b>
2.4.1	Hardware Architecture . . . . .	36
2.4.2	Software Architecture . . . . .	38
<b>3</b>	<b>Installing Deployment Manager . . . . .</b>	<b>41</b>
<b>3.1</b>	<b>Requirements . . . . .</b>	<b>42</b>
3.1.1	Installation of ServerStart/Installation Manager . . . . .	42
3.1.2	Installation of Operations Manager . . . . .	42
3.1.3	Installation of ServerView SNMP Agents . . . . .	43
3.1.4	Deployment Server . . . . .	43
3.1.5	Network Configuration . . . . .	45
3.1.5.1	LAN Connections . . . . .	46
3.1.5.2	LAN Connections (Blade Server) . . . . .	48
3.1.5.3	LAN Connection Topology and IGMP Settings (Switch Blade)	49
3.1.5.4	Multiple Segment Cloning . . . . .	50

## Contents

---

3.1.5.5	Multiple LAN Ports of Target Systems . . . . .	52
3.1.6	Creating an Image Repository . . . . .	52
<b>3.2</b>	<b>Installation in Windows 2008 . . . . .</b>	<b>53</b>
3.2.1	Actions before Installing Deployment Manager . . . . .	53
3.2.2	Actions after Installing Deployment Manager . . . . .	55
<b>3.3</b>	<b>Installation . . . . .</b>	<b>57</b>
3.3.1	Installing the Deployment Manager Front-end Package . . . . .	58
3.3.2	Installing the Deployment Services Package . . . . .	67
3.3.2.1	Configuring the Windows Firewall in Windows 2008 . . . . .	72
3.3.3	Preparation for Multicast Environment . . . . .	73
<b>3.4</b>	<b>Uninstalling/Removing Deployment Manager . . . . .</b>	<b>74</b>
<b>4</b>	<b>Using Deployment Manager . . . . .</b>	<b>77</b>
<hr/>		
<b>4.1</b>	<b>Starting Deployment Manager . . . . .</b>	<b>78</b>
4.1.1	Deployment Manager Start Window . . . . .	79
4.1.2	Selecting a Deployment Server . . . . .	80
4.1.3	User Authentication . . . . .	81
<b>4.2</b>	<b>Main Window . . . . .</b>	<b>82</b>
<b>4.3</b>	<b>Physical View . . . . .</b>	<b>84</b>
<b>4.4</b>	<b>Deployment View . . . . .</b>	<b>86</b>
<b>4.5</b>	<b>Installation View . . . . .</b>	<b>88</b>
<b>4.6</b>	<b>Displaying Server Information . . . . .</b>	<b>90</b>
<b>4.7</b>	<b>Adding Servers . . . . .</b>	<b>91</b>
4.7.1	Adding Bare Servers . . . . .	91
4.7.2	Adding Bare Servers by MAC Address . . . . .	104
<b>4.8</b>	<b>Task Management . . . . .</b>	<b>106</b>
4.8.1	Operations in the Task Window . . . . .	108
4.8.2	Displaying the Event Log . . . . .	110
<b>4.9</b>	<b>Specifying the Power Control of Target Servers . . . . .</b>	<b>112</b>
<b>4.10</b>	<b>Target System Configuration . . . . .</b>	<b>113</b>
<b>4.11</b>	<b>Deployment Server . . . . .</b>	<b>119</b>
4.11.1	Changing the Deployment Server . . . . .	119
4.11.2	Adding a New Deployment Server . . . . .	120
4.11.3	Removing a Deployment Server . . . . .	120

<b>4.12</b>	<b>Menus . . . . .</b>	<b>121</b>
<b>4.13</b>	<b>Exiting Deployment Manager . . . . .</b>	<b>122</b>
<b>5</b>	<b>Tools . . . . .</b>	<b>123</b>
<b>5.1</b>	<b>License Management . . . . .</b>	<b>123</b>
<b>5.2</b>	<b>Repository Management . . . . .</b>	<b>125</b>
<b>5.3</b>	<b>Deployment Configuration . . . . .</b>	<b>128</b>
5.3.1	Exporting the Deployment Configuration . . . . .	128
5.3.2	Importing the Deployment Configuration . . . . .	129
<b>5.4</b>	<b>Global Options . . . . .</b>	<b>131</b>
<b>6</b>	<b>Image Creation . . . . .</b>	<b>133</b>
<b>6.1</b>	<b>File-System-Dependent Image Creation . . . . .</b>	<b>134</b>
<b>6.2</b>	<b>File-System-Independent Image Creation (Raw Image Creation) . . . . .</b>	<b>135</b>
<b>6.3</b>	<b>Supported Operating Systems . . . . .</b>	<b>136</b>
<b>6.4</b>	<b>Windows 2008 Reference System . . . . .</b>	<b>138</b>
6.4.1	Configuring the Windows Firewall on the Reference System . .	138
6.4.2	Sysprep Restrictions . . . . .	139
<b>6.5</b>	<b>Starting the Image Creation Process . . . . .</b>	<b>140</b>
<b>7</b>	<b>Cloning . . . . .</b>	<b>155</b>
<b>7.1</b>	<b>Deployment Groups . . . . .</b>	<b>155</b>
7.1.1	Creating/Removing a Deployment Group . . . . .	156
7.1.2	Viewing and Modifying Deployment Group Properties . . . . .	158
7.1.3	Adding/Removing Servers to/from a Deployment Group . . . . .	159
<b>7.2</b>	<b>System Preparation Method “All Primergy” . . . . .</b>	<b>160</b>
<b>7.3</b>	<b>Starting the Cloning Process . . . . .</b>	<b>162</b>
<b>7.4</b>	<b>Get Batch Result . . . . .</b>	<b>178</b>

## Contents

---

<b>7.5</b>	<b>Cloning/Installing Baseboard Management Controllers . . .</b>	<b>179</b>
7.5.1	Displaying BMCs . . . . .	180
7.5.2	Changing the Deployment Configuration . . . . .	182
7.5.3	Cloning/Installing a BMC without Changing the Deployment Configuration . . . . .	183
7.5.4	Deleting a BMC . . . . .	183
7.5.5	Actions after Cloning / Installation . . . . .	184
<b>8</b>	<b>Installing PRIMERGY Servers . . . . .</b>	<b>185</b>
<b>8.1</b>	<b>Installation Groups . . . . .</b>	<b>185</b>
8.1.1	Creating/Removing an Installation Group . . . . .	186
8.1.2	Adding Servers to an Installation Group . . . . .	188
8.1.3	Removing Servers from an Installation Group . . . . .	190
<b>8.2</b>	<b>Viewing and Modifying the Properties of an Installation Group . . . . .</b>	<b>191</b>
<b>8.3</b>	<b>Installing the Server . . . . .</b>	<b>194</b>
<b>9</b>	<b>Deployment Example: Step by Step Deployment of Server Blades . . . . .</b>	<b>201</b>
<b>9.1</b>	<b>Reference Installation of a Server Blade . . . . .</b>	<b>202</b>
9.1.1	Preparing a Remote Installation Deployment Server . . . . .	202
9.1.2	Installing a Server Blade . . . . .	218
9.1.2.1	Remote Installation From the Deployment Server . . . . .	218
9.1.2.2	Install Your Server Blade Remotely . . . . .	221
<b>9.2</b>	<b>Image Creation Process . . . . .</b>	<b>225</b>
9.2.1	Preparing a Deployment Server for Cloning . . . . .	225
9.2.2	Creating an Image . . . . .	226
<b>9.3</b>	<b>Deploying an Image to Server Blades . . . . .</b>	<b>235</b>
9.3.1	Configure a Deployment Group . . . . .	235
9.3.2	Configuring the Target Systems . . . . .	239
9.3.3	Cloning: Deploying an Image to Server Blades . . . . .	241
<b>9.4</b>	<b>Installing SNMP Agents . . . . .</b>	<b>247</b>

<b>10</b>	<b>Deployment Process Details . . . . .</b>	<b>249</b>
<b>10.1</b>	<b>Cloning Deployment Process . . . . .</b>	<b>250</b>
10.1.1	Power Control via Remote Control . . . . .	254
10.1.2	System Preparation Phase . . . . .	255
10.1.3	Supported Storage Devices . . . . .	260
10.1.3.1	SCSI/IDE Drives . . . . .	260
10.1.3.2	RAID Devices . . . . .	260
10.1.3.3	FC and iSCSI Devices . . . . .	261
10.1.3.4	Partitioning and File System Formatting . . . . .	261
10.1.3.5	Multi-boot Operating System Partitioning . . . . .	262
10.1.3.6	Adding NDIS Driver to Deployment Manager . . . . .	263
10.1.4	Image Creation . . . . .	264
10.1.5	Tag File Handling . . . . .	265
10.1.6	PXE Protocol . . . . .	266
10.1.7	LAN Traffic and Deployment Methods . . . . .	267
<b>10.2</b>	<b>Mass Remote Installation Process . . . . .</b>	<b>269</b>
10.2.1	Functional Process Flow . . . . .	269
10.2.2	Creation of the Configuration Files . . . . .	272
10.2.3	Support of Generic Remote Installation Groups . . . . .	272
10.2.4	Status Frame for Each Installation Process . . . . .	273
10.2.5	Power Status Control . . . . .	273
<b>10.3</b>	<b>Handling the Deployment Table . . . . .</b>	<b>274</b>
10.3.1	Master Deployment Table . . . . .	275
10.3.2	Management Blade Specific Deployment Table . . . . .	279
10.3.3	Configuration in Deployment Manager . . . . .	285
10.3.3.1	Basic Initialization by Deployment Manager . . . . .	285
10.3.3.2	Basic Initialization of the MMB Deployment Table . . . . .	287
10.3.3.3	Installation Status and Cloning Status . . . . .	288
10.3.4	Roaming . . . . .	289
<b>11</b>	<b>Diagnostic . . . . .</b>	<b>295</b>
<b>11.1</b>	<b>Logging Files . . . . .</b>	<b>295</b>
11.1.1	General Logging Files . . . . .	295
11.1.2	Logging File for Installation . . . . .	296
11.1.3	Logging Files for Problem Diagnostics . . . . .	297
<b>11.2</b>	<b>Frequently Asked Questions . . . . .</b>	<b>303</b>

**Contents**

---

**12      High-Availability Support . . . . . 317**

---

**12.1      Installation . . . . . 318**

12.1.1      Operations Manager Installation . . . . . 318

12.1.2      Deployment Manager Installation . . . . . 319

12.1.3      Deployment Services Installation . . . . . 320

**12.2      Hints . . . . . 322**

12.2.1      User Accounts . . . . . 322

12.2.2      Repositories . . . . . 322

12.2.3      Actions Needed When No Cluster Software is Available . . . . 322

**12.3      Failover Scenarios . . . . . 323**

12.3.1      Deployment Manager and Deployment Services Packages  
            are Installed on Same Server . . . . . 323

12.3.2      Deployment Manager and Deployment Services Package  
            are Installed on Different Servers . . . . . 324

**13      Appendix - Network Techniques . . . . . 327**

---

**13.1      MAC Address Handling . . . . . 327**

**13.2      PXE . . . . . 327**

**13.3      DHCP . . . . . 329**

**13.4      VLAN (Virtual Local Area Network) . . . . . 329**

13.4.1      Example: Deployment over VLAN . . . . . 332

**Related Publications . . . . . 343**

---

**Index . . . . . 349**

---



---

# 1 Introduction

ServerView Deployment Manager (called simply Deployment Manager below) enables individual deployment, such as duplication and installation, of a single server. To reduce data center administration costs, full parallel mass remote cloning and mass remote installation on a group of servers selected from the ServerView database are supported. An automated individualization process allows each server instance to be put into operation quickly. Automated and time-controlled installation or cloning of servers is supported using centrally held boot images in an own image repository database.

Deployment Manager is a professional addition to the standard PRIMERGY ServerView Suite. As part of this suite, Deployment Manager is integrated in the user interface of ServerView Operations Manager (called simply Operations Manager below). It provides a central overview of installed or additionally available servers, existing images and assignment of servers to deployment or installation groups.

Server installation comprises a number of individual steps:

- Hardware preparation, BIOS settings, RAID configuration, etc.
- Installation of the operating system and parameterization (licensing, network configuration)
- Application environment setup
- User and service setup

Deployment Manager and ServerView ServerStart/Installation Manager (called simply ServerStart/Installation Manager below) support these steps. Automated installation ensures that more servers can be put into error-free operation with minimum effort.

Deployment Manager has the further advantage that servers can be quickly loaded with an operating system/application software image so that other tasks can be assigned to them. For example, by exchanging a hard disk image, you can allow a server that previously ran under Linux to perform a different task in Windows 2000.

## Highlights of Deployment Manager

- After image creation, the reference server remains 100% unchanged and returns back to normal mode.
- A Web user interface allows deployment and management over LAN via HTTPS from anywhere in the world.
- Support of Apache & IIS Web services.
- Unicast and multicast cloning enables optimum use of network bandwidth.
- The system is prepared directly by the specialist vendor with optimum support of each new Fujitsu Siemens server.
- The mass remote installation based on WinPE is MSA-certified by Microsoft and is the world's fastest solution for convenient configuration and installation of Windows and Linux operating systems in parallel.
- Support for a programming interface called *JobAPI Tandem*. The API specification can be found on the Deployment Manager CD in the *Documentation* directory.

## Supported systems

Deployment Manager now provides generic methods to enable the system preparation before cloning for all kinds of IA32-based servers. Deployment Manager is also certified especially for the following PRIMERGY servers for remote power control with BMC support:

- all BX300 Blade Server types
- all BX600 Blade Server types (incl. BX600 S2, BX600 S3)
- all BX620 Blade Server types (incl. BX620 S2, BX620 S2F, BX620 S3, BX620 S4)
- BX630 Scalable Server Blades (incl. BX630 Dual, BX630 Quad, BX630 Octal, BX 630 S2)
- BX660 Blade Server
- Econel 40, Econel 50, Econel 200, Econel 200 S2
- RX100, RX100 S2, RX100 S3, RX100 S4, RX100 S5
- RX200, RX200 S2, RX200 S3, RX200 S4
- RX220 S1
- RX300, RX300 S2, RX300 S3, RX300 S4
- RX600, RX600 S2, RX600 S3, RX600 S4
- RX800, RX800 S2, RX800 S3
- TX120, TX120 S2
- TX150, TX150 S2, TX150 S3, TX150 S4, TX150 S5, TX 150 S6
- TX200 / TX250, TX200 S2, TX200 S3, TX200 S4
- TX300, TX300 S2, TX300 S3, TX300 S4
- TX600, TX600 S2, TX600 S3

## 1.1 Target Groups and Purpose of This Manual

This manual is intended for system administrators, network administrators and service technicians who have a basic knowledge of hardware and software.

The manual explains how to create and manage image files with the Deployment Manager software and how to deploy these files. It also describes how to install PRIMERGY servers using ServerStart/Installation Manager configuration files (if ServerStart/Installation Manager is installed on the same system as Deployment Manager).

# 1.2 Changes Since the Previous Version

This edition is valid for the ServerView Deployment Manager V5.0 and replaces the following manual: “PRIMERGY ServerView Suite RemoteDeploy V4.1”, edition December 2007.

## Renaming of PRIMERGY ServerView products

- As of version 5.0 RemoteDeploy has been renamed ServerView Deployment Manager (Deployment Manager for short).
- As of version 4.7 ServerView S2 has been renamed ServerView Operations Manager (Operations Manager for short).
- As of version 1.70A RemoteView has been renamed ServerView Remote Management (Remote Management for short).
- As of version 4.61 GlobalFlash has been renamed ServerView Update Manager (Update Manager for short)
- As of version 3.0.10 ServerView RAID has been renamed ServerView RAID Manager (RAID Manager for short)
- As of version 7.806 ServerStart will be renamed ServerView Installation Manager. Therefore in this manual the following product name is used: ServerView ServerStart/Installation Manager (ServerStart/Installation Manager for short)

## Renaming of RemoteDeploy items

The following RemoteDeploy items have also been renamed:

Old	New
RemoteDeploy CD	ServerView Deployment Manager CD (Deployment Manager CD for short)
RemoteDeploy Manager package	Deployment Manager package
FSC RemoteDeploy Manager service	FSC Deployment Manager service

**Deployment Manager V5.0 contains the following changes and enhancements:**

- The system requirements have been updated.
- The installation of Deployment Manager on Windows 2000 is no longer supported.
- Deployment Manager can be installed on Windows 2008.
- During the installation of Deployment Manager (Deployment Manager package) an evaluation license key can be created.
- Deployment Manager supports Windows 2008 for image creation and cloning.
- Deployment Manager supports cloning and installing of Baseboard Management Controllers (BMC).

## 1.3 System Requirements

### 1.3.1 Deployment Manager Packages

Deployment Manager consists of two packages which can be installed on the same system or on different systems (see also [chapter “Installing Deployment Manager” on page 41](#)):

- *Deployment Manager* package

Web-based graphical user interface including the *FSC Deployment Manager* service.

This package can be installed under:

- Microsoft Windows 2003 Server (x86 and x64)  
(also domain controller)
- Microsoft Windows 2008 Server (x86 and x64)  
(also domain controller)

Refer to [section “Installation in Windows 2008” on page 53](#) for further information.

*Deployment Manager* package requires a Web server:

- IIS 5.0 or higher or
- Apache Web server that comes with the ServerView installation

- *Deployment Service* package

The deployment services including PXE service, TFTP service and deployment service (= cloning module).

This package can be installed under:

- Microsoft Windows 2003 Server (x86 and x64)  
(also domain controller)
- Microsoft Windows 2008 Server (x86 and x64)  
(also domain controller)

Refer to [section “Installation in Windows 2008” on page 53](#) for further information.



Windows Script Host (WSH) as of version 5.6 is required for the deployment services.

### 1.3.2 Supported Operating Systems for Image Creation/Cloning

Deployment Manager supports the following operating systems for image creation/cloning with personalization:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows Server 2003 (x86 and x64)
- Microsoft Windows Server 2008 (x86 and x64)



Before starting an image creation process, you must configure the Windows firewall on the reference system, see [section “Configuring the Windows Firewall on the Reference System” on page 138](#).

- Linux RedHat Advanced Server 3.0
- Linux RedHat Advanced Server 4.0 (x86 and EM64T)
- Linux RedHat Advanced Server 5.0 (x86 and EM64T)
- Linux SuSE Enterprise Server SLES 8
- Linux SuSE United Linux (with SLES 8)
- Linux SuSE Enterprise Server SLES 9 (x86 and EM64T)
- Linux SuSE Enterprise Server SLES 10 (x86 and EM64T)
- Reiser file system versions 3.5 and 3.6 on SuSE SLES 9 and SuSE SLES 10
- With restrictions: ESX 2.5 based on customer script; requirements for the configuration of the reference system need to be defined. Customer scripts for ESX 2.5 cloning are located on the Deployment Manager CD.
- ESX Server 3.0

Before image creation, a specific package must be installed on the reference system if Reiser is used as the root file system. This package can be found on the Deployment Manager CD in the directory *LINUX\_support/ReiserFS\_Cloning\_Support*.

For the cloning of an ESX Server 3.0 image, a specific ESX deployment configuration can be specified. For more information on support for ESX 3.0, see also the ReadMe file on the Deployment Manager CD.



All other operating system types can always be supported without personalization in raw snapshot mode. See also the ReadMe file on the Deployment Manager CD.

### 1.3.3 Software Packages on the Deployment Server

The following software packages must be available on the deployment server:

- A standard Windows 2003 Server, Windows Server 2003 SP 1 platform (no W2k3 domain server) or Windows 2008 Server.



Refer to [section “Installation in Windows 2008” on page 53](#) for further information.

- ServerStart/Installation Manager V6.605 (or higher) for PXE-based remote installation and/or deployment service (cloning module) for PXE-based remote image creation and cloning.
- ServerStart/Installation Manager as of version 6.611 if you specify a user name without administrator rights during installation of the *Deployment Manager* package.
- ServerStart/Installation Manager as of version 6.711 if you want to use WinPE MDP as deployment platform.
- A DHCP service (if none is already present in the LAN segment).
- A PXE service must run on the deployment server. It can be installed using either Deployment Manager or Installation Manager (as of revision 5).



PRIMERGY systems and the deployment server must be in the same network segment.



# 1.4 Notational Conventions

The following notational conventions are used in this manual:




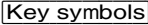


	<b>Caution</b>	This symbol points out hazards that can lead to personal injury, loss of data or damage to equipment.
		This symbol highlights important information and tips.
		This symbol refers to a step that you must carry out in order to continue with the procedure.
<i>italic</i>		Commands, menu items, names of buttons, options, variables, file names and path names are written in <i>italic</i> letters in text.
<code>fixed font</code>		System output is written using a <code>fixed font</code> .
<b>semi-bold fixed font</b>		Commands to be entered via the keyboard are written in a semi-bold fixed font.
<code>&lt;abc&gt;</code>		Angle brackets are used to enclose variables which are to be replaced by current values.
		Keys are presented according to their representation on the keyboard. If capital letters are to be entered explicitly, the Shift key is shown, e.g.  -  for A.  If two keys need to be pressed at the same time, this is shown by placing a hyphen between the two key symbols.

Table 1: Notational conventions

## References

If there are references to text or sections of text in this manual, the chapter or section heading is given in the reference, and the page given refers to the page on which the chapter or section begins.

References to related publications are quoted in the text as a brief title and a reference number in square brackets. The full title will be found in the “Related publications” chapter under the corresponding reference number.

**Screen outputs**

Please note that the screen output is partly dependent on the system used and therefore some details may not correspond exactly to the output you will see on your system. You may also see system-dependent differences in the menu items available.

---

## 2 Deployment - Overview

Today's standard server environment has significantly changed the requirements of server administration. In a typical IT environment a large number of servers are used and must be managed remotely and without consoles. There are server farms, for example, where hundreds of blade servers are installed and must be administered.

Scalability and ease of deployment or support for different tasks must be offered to fulfill the increasing demands on flexibility in IT systems. While a system may be used as a Web server for the Internet presence of a company during the day, it could be used as an FTP server at night with a different IP address. This must be achieved simply by remote administration rather than through physical operation. Administrators often have to set up the same software stack, such as the operating system and application software, on hundreds of identical servers in a server farm. In this case, manual installation is not feasible.

New strategies must be developed to deploy the boot image of a server over the LAN without any interaction. The basic idea of deployment is to create one or more central deployment servers to administer this enormous number of clients over the LAN. To manage the servers on the fly, special base management controllers (such as management blades for blade servers, or Kalypso service processors) are assigned inside of a server chassis to guide the servers during their boot and working phases.

Deployment is the convenient method of preparing server systems to start their work immediately. Deployment servers are responsible for preparing multiple servers and their environment from a central instance over the LAN. The servers can therefore start their work immediately.

Deployment Manager provides two procedures for deployment:

- Cloning

Cloning means to install a reference system, create an image file of that reference installation, and clone this image file to a group of servers to be installed with the same configuration parameters. This procedure is described in more detail in the [section “Cloning Process” on page 23](#).

- Mass remote installation

Mass remote installation means to use configuration files created with ServerStart/Installation Manager, assign them to servers or server groups, and then start the installation for all servers. This procedure is described in more detail in the [section “Mass Remote Installation” on page 33](#).

## 2.1 Supported Server Systems

Deployment Manager supports the following types of server:

- Generic IA32-based server
- PRIMERGY server
- PRIMERGY blade server

### Generic server

From the deployment point of view, a generic server is a server that has been ideally prepared, so that each device access can be handled via a standardized generic device or BIOS APIs.

Deployment Manager provides generic methods to support almost any kind of IA32-based server system. Cloning with Deployment Manager requires the following standard APIs:

- PXE boot capability as part of the BIOS code based on PXE specification V2.1
- A standard onboard NIC with full UNDI API support as required for PXE specification V1.2
- A fully prepared bootable storage device accessible via DOS Int13h BIOS API

For a generic server Deployment Manager expects a fully prepared storage device, e.g. with complete RAID configuration. This must be done by the user manually or by booting a PXE image in floppy emulation. This image can be a raw copy of a bootable DOS floppy providing the full knowledge to perform the system preparation of a target server unattended. The requirements for this Deployment Manager preparation image are similar to the MS ADS required preparation image. For the creation of MS ADS compatible PXE preparation images, each system vendor offering ADS-compatible server systems provides a Web page containing a prescription how to prepare such a system preparation image for each server type together with the required command line tools.

Finally, each image must initiate a reboot of its target server automatically in PXE mode (enabled static in the BIOS setting) to continue the Deployment Manager generic cloning phase. These kinds of images can be administered via the Deployment Manager repository management by a separate boot image repository.

An example of such a boot image can be found in the *Sample\_BootImages* directory on the Deployment Manager CD. See also the ReadMe file in this directory for further information.

Once a server fulfills the generic server requirements as described above, it can be cloned by Deployment Manager with the system preparation method *Generic Boot Image*. This type is seen as a common classification for all types of server prepared in the appropriate way in the system preparation phase, either by Deployment Manager or by the user themselves.

It is not necessary for a generic server to support remote management besides a static PXE boot mode, as configured once in the BIOS settings. PXE boots are initiated manually or just by a simple reboot driven by the locally running preparation image. A remote power on of a generic server can be done by "Wake On LAN" functionality integrated into Deployment Manager if the server supports "Wake On LAN".

Remote identification of a generic server is not possible. The initial MAC address must be added manually.

### **PRIMERGY server**

PRIMERGY servers are developed by Fujitsu Siemens Computers and can be supported in a much more detailed and convenient way than generic servers.

PRIMERGY servers are equipped with:

- Onboard or plugged-in service processor for remote management such as
  - automatic identification of MAC address by Operations Manager
  - automatic remote PXE boot
  - automatic modification of remote boot device table
- Remote management via SNMP or IPMI (Intelligent Platform Management Interface (Kalypso- or Kronos-supported))
- High-level system preparation, e.g. RAID controller and attached storage devices
- Fully supported by Fujitsu Siemens Computers service

Based on these services, Deployment Manager can directly check whether or not a cloning image is compatible with a given PRIMERGY server. After cloning, this server can be managed directly by Operations Manager and Remote Management.

PRIMERGY servers have at least 512 MB RAM and an onboard 100 Mbit LAN controller with one or more ports. The storage device may be a simple IDE or SCSI drive, an onboard RAID controller based on IDE, SATA, SCSI, or SAS and/or a SAN-attached storage device with an additional administration LAN port. These systems may exist in a floor-standing or rack housing with or without a local console.

### **PRIMERGY blade server**

A blade server system is a rack system with server plug-in cards of up to 20 server blades. Each server blade consists of one or two CPUs, one or two hard disks (IDE, IDE-RAID, SATA, SATA-RAID, SCSI, SCSI-RAID, SAS, SAS-RAID), at least 512 MB memory, at least 2 x 1 Gbit LAN ports, and the system chip set. To manage these server blades remotely both online and offline, two management blades are assigned inside of these racks with a local IPMI-based communication path to each server blade at each significant point in its life cycle, e.g. power off, BIOS boot phase, operating system boot phase. The hard disk may be controlled by a SCSI/IDE or IDE/SCSI RAID controller. Management blades have their own type of hardware to administer and control the server blades in respect of power, temperature, BIOS and so on.

To provide fast and stable connectivity to the server blades over the LAN, two or four switch blades are available in the same rack. 1 Gbit Ethernet channels or Fibre Channel connections are used. These consist of real 1 Gbit or 2 Gbit switch hardware with external connectors to the external LAN, and are hard-wired with internal port connections to each LAN chip port of each server blade in a chassis. Two LAN ports per blade are connected to these switch blades for redundancy purposes. Each LAN port has its own MAC address. It is important that the PXE BIOS uses port 0 by default to correctly handle the PXE protocol. In the CPU blade BIOS, you can define which port is used as the default PXE boot port.

A blade server can have a VGA connector and two USB 2.0 connectors for a USB floppy or USB CD-ROM drive for service purposes only. This is useful for native operating system installations on a reference server.

The racks may be assembled into a rack tower to concentrate the number of CPU blades per square meter. A server farm may consist of many of these rack towers.

### Detection of target servers

Deployment Manager obtains the list of server systems from Operations Manager front-end by reading the ServerView database.

Deployment Manager also offers an *Add Server* dialog to create server list entries for servers which are initially not detected by Operations Manager. In this case the MAC address, IP address and host name must be added manually. These servers are called bare servers. If a server is deployed and a ServerView agent is active and running on the clone, it will automatically be detected by the discovery cycle running during the lifetime of the Operations Manager front-end. Operations Manager will take over responsibility for that server entry and update all parameters received from the agent (including LAN port settings).

## 2.2 Cloning Process

The cloning process consists of the following steps:

- installation of a reference system
- image creation from that reference system
- cloning of an image to one or more target server systems

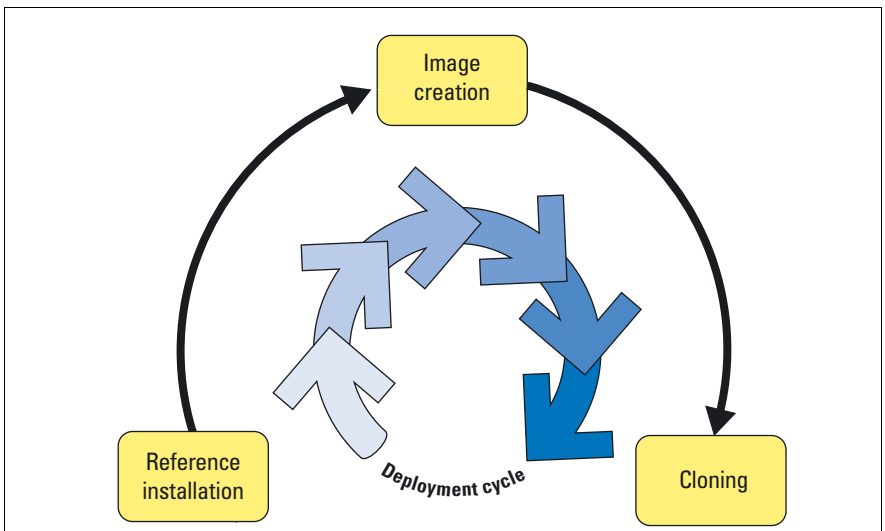


Figure 1: Cloning deployment cycle

The following sections describe these phases in more detail.

## 2.2.1 Reference Installation

First you must install and configure a server system (the reference system) manually. This so-called reference installation on the reference system is used to install further servers in the same way. For each kind of server to be installed via Deployment Manager, there must be one reference system.

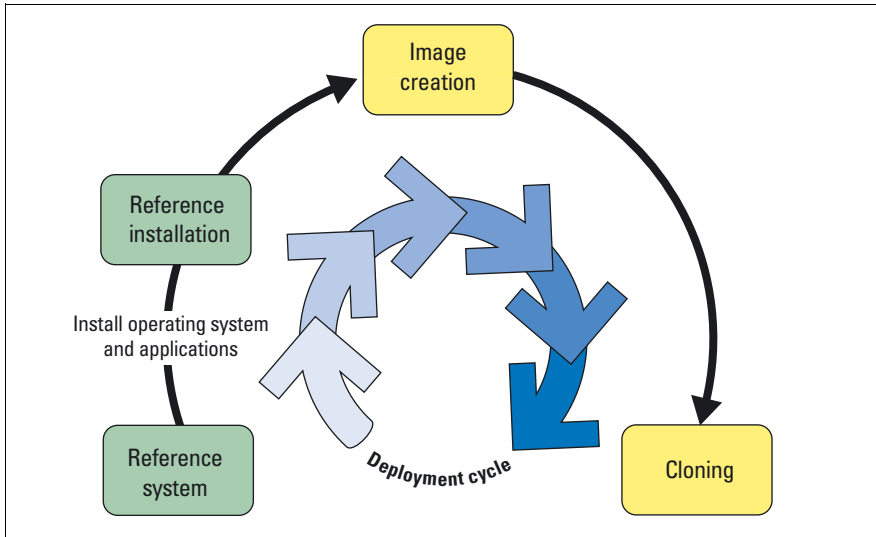


Figure 2: Deployment cycle - reference installation

A reference system is basically a simple server of a specific type. It may have additional devices attached, such as a monitor, mouse and keyboard, mass storage devices (e.g. RAID), USB CD-ROM and USB floppy drive in the case of local operating system installation via CD and floppy.

The hardware configuration must be detected by several agents and the system resources must be assigned by the BIOS and operating system instances. A large number of parameters of BIOS, storage systems and operating system must be defined previously and interactively in a separate configuration session or interactively in parallel with the installation process.

Detailed information on the installation process of the individual reference systems can be found in the corresponding installation documentation.



Installed applications on the reference system possibly may not run successfully on a target system after cloning without adaptation. In that case user-specific scripts are to be performed after the cloning process to ensure the successful operation.

After each basic operating system installation, you may install and configure appropriate applications which will be started on each cloned server immediately after reboot. Image creation software which is part of the deployment server software generates a copy of this installed hard disk as an image file and copies it to the deployment server repository. It is used as a reference (master) image for further cloning sessions. The server management front-end of the deployment software allows you to define assignments between clients and reference images.

Many parameters of the BIOS, storage systems (RAID) and operating systems can be defined interactively in a separate configuration session of ServerStart/Installation Manager before the installation, or interactively in parallel with the installation process using native operating system installation via local devices. You can use this installation as a reference installation for other servers with the same hardware and BIOS configuration. The other system may differ in memory size, hard disk size and RAID level.

The following methods of reference installation are supported:

- Local installation with ServerStart/Installation Manager
- Multiple remote installation with ServerStart/Installation Manager (maximum five clients)

A detailed description of ServerStart/Installation Manager can be found in the ServerStart/Installation Manager documentation which is available on the ServerBooks DVD.

### **Local installation with ServerStart/Installation Manager**

Local installation with ServerStart/Installation Manager requires a bootable USB CD-ROM and a graphical console with mouse, monitor and keyboard connected to the reference server for the master image generation. For blade servers the graphical console with mouse and keyboard is available using the KVM switch functionality via the management blade.

With this local installation method you can use the *Guided Mode* of ServerStart/Installation Manager which provides an online check of the defined configuration parameters with the target hardware.

**Multiple remote installation with ServerStart/Installation Manager and PXE**

You can use ServerStart/Installation Manager Remote Installation which you will find on the ServerStart/Installation Manager CD/DVD version 6.605 (or higher). To do this, you must install the ServerStart/Installation Manager CD/DVD on the PC from which you want to perform the installation. This PC acts as the deployment server for the remote installation. It can be a notebook or a server.

ServerStart/Installation Manager uses WinPE as the boot platform and is booted via PXE in the RAM of each target server. This allows any kind of remote access during the installation process.

Multiple remote installation is recommended for installing up to five clients.

Detailed information on the reference installation with ServerStart/Installation Manager can be found in the ServerStart/Installation Manager documentation.

## 2.2.2 Image Creation

From the reference system an image file is created which contains the configuration information on the reference system, e.g. on the hard disk, the configuration of the partitions, and all data of the operating system. It is independent of the RAID level, the BIOS settings and the memory size of the target systems.

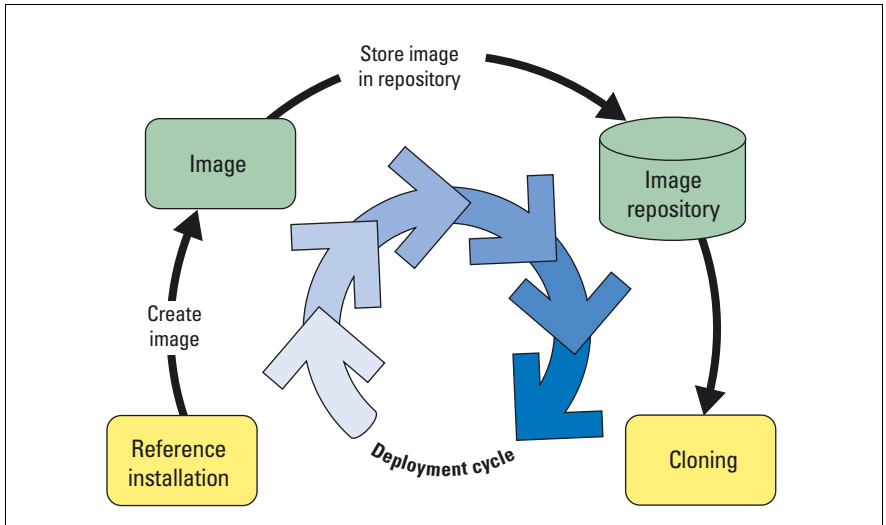


Figure 3: Deployment cycle - master image creation

The following methods of image creation are supported:

- File-system-dependent image creation  
This method is only available for supported file systems which only come with the supported operating systems (see [section “Partitioning and File System Formatting” on page 261](#)). In this case only used areas are copied to the image. This results in small image sizes and reduced cloning time. The target partition may be smaller than the partition on the reference system.
- File-system-independent image creation (raw image creation)  
This method is used for not supported file systems. In this case the complete partition information is copied to the image file and must be cloned to a partition with the same size. The image may be larger and the cloning process takes more time to recreate the partition.

- Snapshot image

A “snapshot image” can be used to restore the server after a system crash.

The images are stored in an image repository. This is located in a shared folder on any file server in the network. The image is used as a reference image for further cloning sessions.

Each image object in the repository refers to a set of files with identical names but different extensions:

- \*.img*      Reference to binary cloning image file (URL of a storage location somewhere in the network)
- \*.txt*      Image documentation (e.g. reference to a text document which is created during the image creation) could be used for describing an image in a Deployment Manager frame.
- \*.cfg*      A hardware and operating system parameter file. This information is used for later modification of an existing image and for a compatibility check against the assigned target hardware.

The image creation process can be started from Deployment Manager.

Detailed information on image creation can be found in the [chapter “Image Creation” on page 133](#).

How to use Deployment Manager is described in the [chapter “Using Deployment Manager” on page 77](#).

## 2.2.3 Cloning

The cloning process deploys an image to the servers. It prepares the hardware, BIOS and storage devices, copies the image onto the hard disks, and initiates a reboot of the target server. No configuration session is required during the cloning process or later.

The result is an identical system with the exception of variable parameters such as IP address, host name and SecureID (Windows systems only) of the operating system, which must be unique to each server.

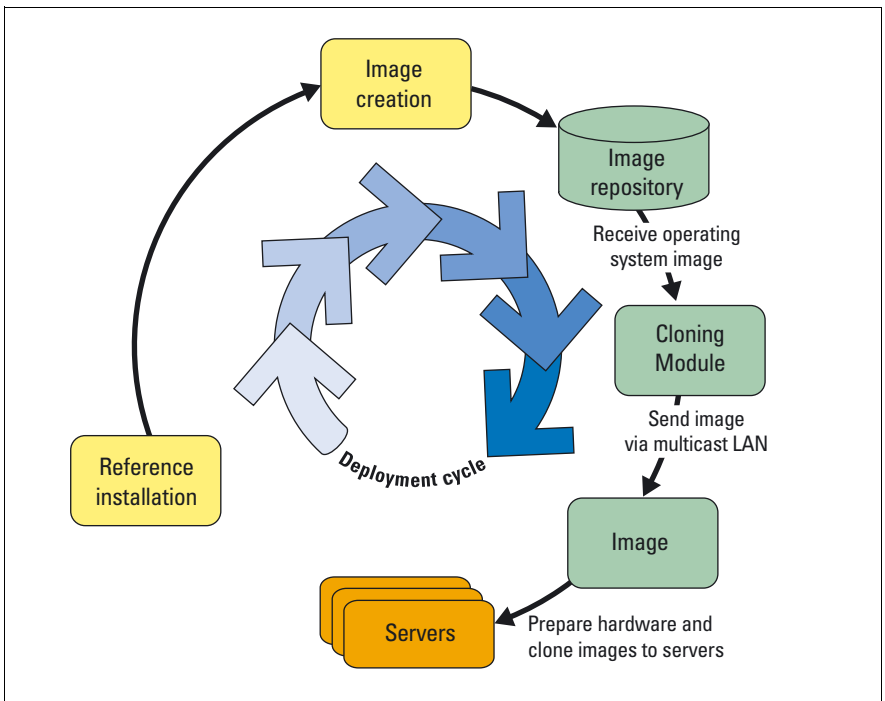


Figure 4: Deployment cycle - cloning

The hardware configurations of clone and reference system must be identical, except for the RAID level, memory size, CPU clock and hard disk capacity.

It is possible to define assignments between reference images and servers by setting up logical groups, called deployment groups, in the Deployment Manager front-end. Cloning images can be assigned to deployment groups and can be cloned simultaneously.

A server cannot be a member of more than one cloning group.

Deployment groups must be created manually. Each group has its own set of group attributes (parameters) relevant for all group members, e.g.

- Network path to master image in the Deployment Manager repository
- File system formatting type
- Final power status after post-cloning phase has finished

All physical clients of that deployment group will be cloned with that referring image, and the target storage device will be configured in the specified way specified for each server.

The attributes for a member of a physical group are basically defined in the deployment table, which contains an entry for each server listed in the physical server list. This deployment table is always the definitive reference for the current deployment status of the server indicating the last operation performed by Deployment Manager for that server or the currently running operation (e.g. *cloned* or *installed*). Deployment Manager always uses the parameters from this table. This helps to show the same status of each server if more than one Deployment Manager front-end has been started. If one front-end has initiated a job on a particular server, other front-ends are not able to access this server as long as the jobs are running. Each group member may have its own set of group parameters which may overrule the group settings for this server. Finally, each physical server, regardless of whether it is a member of a group or not, has its own set of individual physical settings which are stored server-specifically in the deployment table (for details see [section “Handling the Deployment Table” on page 274.](#))

A cloning session consists of several phases:

1. The target server is powered on.
2. The system is prepared.
3. The image is cloned to the server.
4. The post-preparation tasks are performed.

Each phase offers different alternatives depending on the types of servers to be cloned. Details can be found in [chapter “Deployment Process Details” on page 249.](#)

The cloning process with Deployment Manager works as follows:

#### Preparations

- The administrator defines a deployment group, assigns an appropriate image file, and adds the servers to the deployment group for deployment on the basis of the assigned image file.
- The deployment table is set up with the individual parameters for the servers: IP settings, host name etc. For each server in the group, a separate entry is created in the deployment table.

#### Starting the cloning process

- The administrator defines the cloning parameters and selects the servers for the deployment job.
- He/she initiates the cloning directly or configures the scheduler once per server in the deployment group.

#### Cloning process

- Deployment Manager prepares the system based on the preparation mode selected by the administrator:

<i>unchanged</i>	for already manually prepared target servers. No additional preparation tasks are performed.
<i>Generic Boot Image</i>	for target systems to be booted via a generic boot image created by the user themselves. The operations are performed via PXE boot from <ul style="list-style-type: none"><li>– a 1.44 MB floppy image or</li><li>– an external bootstrap image</li></ul> (See also <a href="#">“Generic server” on page 20.</a> )
<i>Blade optimized</i>	for blade server systems. The system preparation is performed via DOS agent (Haribote) during the cloning process for server blades. It involves unattended RAID preparation of the blade controller. This preparation mode can only be used if the deployment platform is <i>Caldera DOS</i> .
<i>All Primergy</i>	for target servers based on WinPE PXE boot (e.g. PRIMERGY servers). The RAID configuration is done via ServerStart/Installation Manager, see also <a href="#">section “System Preparation Method “All Primergy”” on page 160.</a>

- Deployment Manager performs the cloning task. It copies the image to the target system.
- Deployment Manager performs the post-preparation tasks defined by the administrator, e.g. executing user-defined installation scripts and changing the power status.

Deployment Manager stores the final deployment status of the server in the central deployment table.

The cloning process is described in detail in the [chapter “Deployment Process Details” on page 249](#).

Information on handling the cloning process via the Deployment Manager front-end can be found in the [chapter “Cloning” on page 155](#).



## 2.3 Mass Remote Installation

With Deployment Manager the unattended installation process of ServerStart/Installation Manager can be initiated for mass installation via the Deployment Manager console. Appropriate configuration files created with ServerStart/Installation Manager must exist. The Deployment Manager software is then accessible via Operations Manager.

The maximum number of supported target servers is basically unlimited but is influenced by the bandwidth of the network topology used. The final value must be determined for each environment. For example, in a 1 Gbit LAN topology about 20 to 25 concurrent installation jobs are a sensible limit.

The mass remote installation process consists of the following steps:

- Create installation groups
- Assign configuration files to installation groups
- Start mass installation process

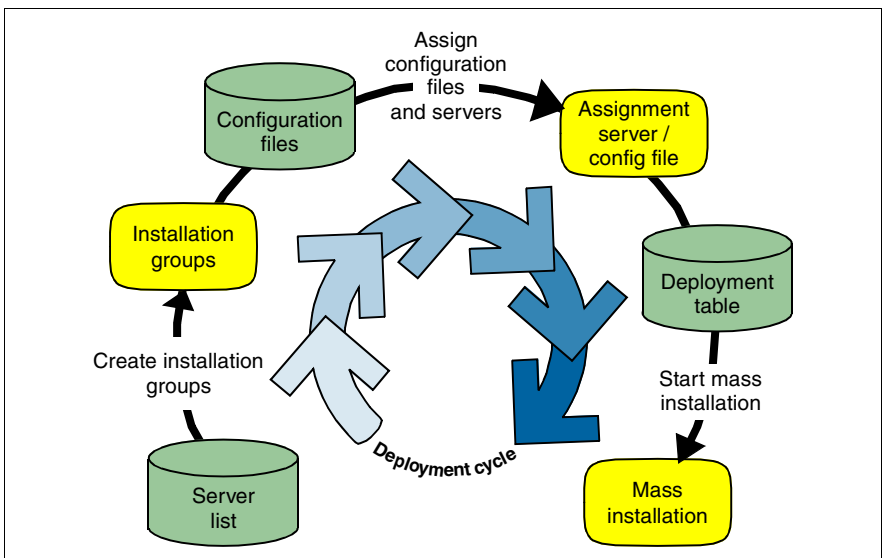


Figure 5: The deployment cycle for mass remote installation

Installation groups are formed in order to group servers of a specific type with specific characteristics. There are two methods for building installation groups:

- The same configuration file is assigned to all servers of the installation group.
- A different configuration file is assigned to each server of the installation group.

A server can be assigned to different installation groups, so it can take on different roles at different times.

The configuration files created by the ServerStart/Installation Manager wizards during the configuration phase are stored in a repository folder and can be assigned to servers or server groups for mass installation. The administrator assigns an appropriate configuration file to the members of an installation group. One configuration file can be used for all members of an installation group or a specific configuration file can be assigned to each server in the group.

At the start of the installation, the configuration files are merged in each individual server information contained in the Deployment Manager deployment table and the remote installation processes are started parallel. For detailed information on the deployment table, see [section “Handling the Deployment Table” on page 274](#).

The remote installation process with Deployment Manager works as follows:

#### Preparations

- The administrator defines a remote installation group and decides whether all servers in the group will have the same configuration file assigned or each server will have its own configuration file.
- The administrator adds servers to the installation group and assigns the appropriate configuration file to the group or different configuration files to individual servers.
- The deployment table is set up with the individual parameters for the servers: IP settings, host name and administrator password.

#### Starting the mass installation process

- The administrator sets the power control status for the group or for individual servers (power off or power on).
- The administrator initiates the remote installation directly or configures a scheduled installation job.

## Mass installation process

- A separate configuration file is created for each server in the group.
- Deployment Manager performs the installation task.
- Deployment Manager stores the final server status in the central deployment table.

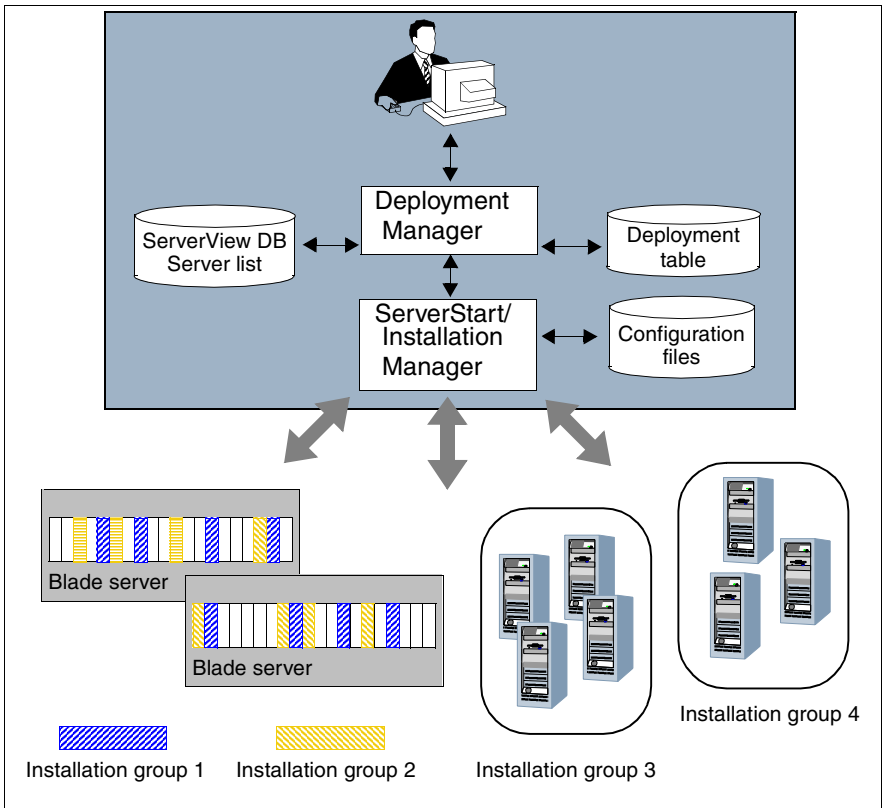


Figure 6: Mass installation with Deployment Manager

The installation process with Deployment Manager is described in detail in the [chapter “Installing PRIMERGY Servers” on page 185](#).

How to use the Deployment Manager front-end is described in the [chapter “Using Deployment Manager” on page 77](#).

## 2.4 System Architecture

### 2.4.1 Hardware Architecture

Deployment Manager is designed for a server-client architecture. It supports Windows 2003 Server or Windows 2008 Server operating systems as management platforms. Deployment Manager requires a Web server. This can be IIS 5.0 or higher or the Apache Web server that comes with the Operations Manager installation.

The clients, i.e. the Deployment Manager front-end user interfaces, can be installed on the management console or can be accessed via a Web interface from any workstation with Web browser in the network.

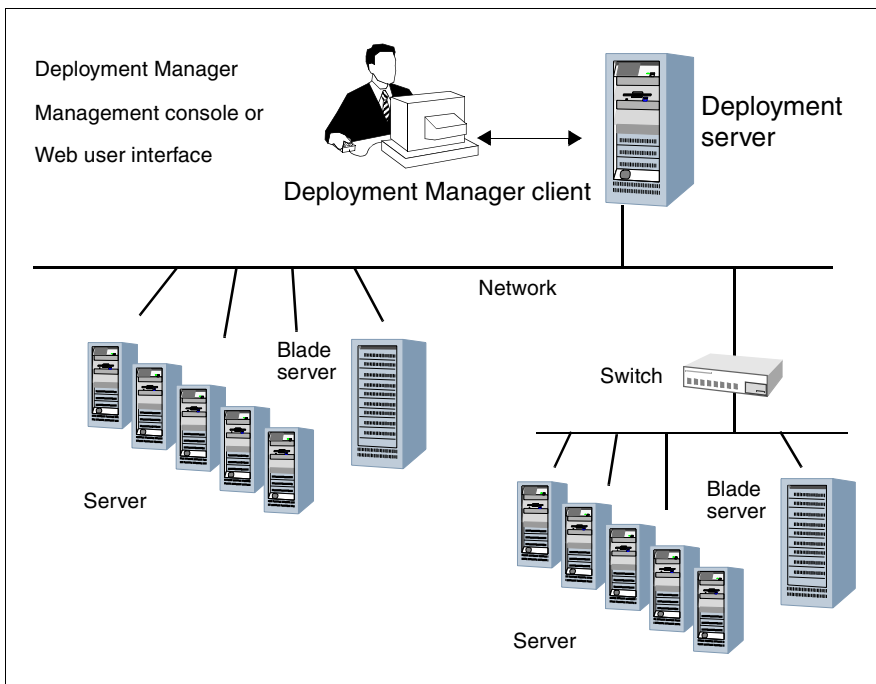


Figure 7: Topological overview of a deployment environment

## Deployment server

The deployment server contains the following software packages:

- a Windows 2003 (when available) Server (no W2k3 domain server) or a Windows 2008 Server platform



Refer to [section “Installation in Windows 2008” on page 53](#) for further information.

- ServerStart/Installation Manager v6.605 (or higher) for mass remote installation and for the support of mass cloning for all PRIMERGY servers
- a DHCP (Dynamic Host Configuration Protocol) service (if there is none present in the LAN segment). PXE requires an existing DHCP server.
- a PXE service coming from Deployment Manager or from ServerStart/Installation Manager or from the Update Manager tool.
- the Job API package for controlling deployment jobs via the Deployment Manager Web service based on SOAP (optional)

Only one deployment server can be in use by a Deployment Manager front-end per LAN segment, but several deployment servers can exist per LAN segment. If PXE and the DHCP service are installed on one machine, only one deployment server per segment is allowed.

Even if it is allowed to have more than one DHCP service and one PXE service in one LAN segment, it is recommended to have only one of each service. Otherwise, it can only be guaranteed which service will be used by the client, if the DHCP and PXE services are configured carefully. The DHCP service may be installed on the same server as the PXE service but this is not necessary.

The Deployment Manager cloning module requires Windows 2003 (for the PXE service) installed on the deployment server to support DHCP proxy functionality.

For fast image creation handling, the partition where the cloning module is installed should always have as much free space left as the currently used image size will be. Otherwise the image creation process may stop.

Using the raw mode for image creation, the size could be up to 80% of the disk size (normally 2/3 of the disk size).

LAN environment

For administrative purposes, the LAN may be organized hierarchically with external switches, hubs and gateways at each node point. For switches Virtual LAN (VLAN) software may be used to simulate hub or bridge functionality.

The deployment server must be placed inside of each LAN segment or on a higher level in the hierarchy behind switches or hubs. In these cases, the switch or hub ports must be configured to let through broadcasts coming from the PXE BIOS to the PXE boot server, as well as multicast broadcasts.

2.4.2 Software Architecture

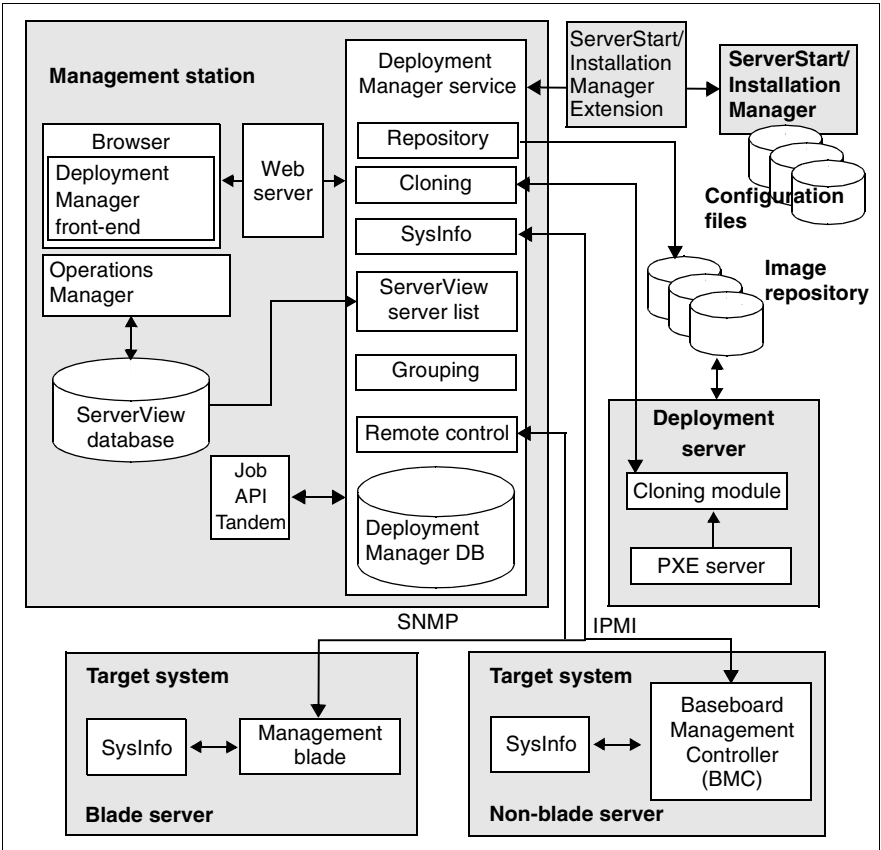


Figure 8: Architecture - overview

Deployment Manager obtains the list of server systems from Operations Manager by reading the ServerView database. Both the Deployment Manager front-end and Operations Manager can run on the same machine. This machine does not have to act as a deployment server on which the Deployment Manager cloning module and the PXE service are running.

But for easier installation and administration it is advisable to install all components (Deployment Manager (package *Deployment Manager* and package *Deployment Services*) and Operations Manager) on a deployment server.

### Deployment Manager service

The *Deployment Manager* service is the central node which manages jobs for deployment, provides status and parameters to the Deployment Manager front-end, and collects information from the ServerView database and ServerStart/Installation Manager. The *Deployment Manager* service itself consists of different building blocks for the different actions. One important block is the module which is responsible for the communication with the cloning module.

The cloning module may be located on a separate server, the deployment server.

Both the *Deployment Manager* service and the cloning module have access to the image repository which contains the images for cloning jobs.

### Remote control

Remote control is used to initiate requests to the target server especially for power control and server detection. Access to the service processors such as the management blade (via SNMP) and Kalypso BMC (via IPMI) is supported via remote control. PRIMERGY servers supporting none of these services can be rerouted via a message box to the Deployment Manager front-end to get the user to initiate tasks manually instead of remotely.

### ServerStart/Installation Manager Extension

The ServerStart/Installation Manager Extension is used to communicate with ServerStart/Installation Manager. It is session-oriented based on a ServerStart agent concept. Starting and stopping an agent identifies the start and the end of a session. In between, certain commands can be sent down to the running agent. Each agent has its session ID, based on which the Deployment Manager service can manage many tasks to different agents in parallel, as required, for example, for mass remote installation.

## Job API Tandem

The Job API Tandem is a SOAP-based Web service which is designed to offer largely the same function set as the Deployment Manager front-end. All functions coming in via the Job API are routed inside the *Deployment Manager* service, as they are created via the front-end and can be scheduled and routed to all connected engines.

The functions which are provided by the Job API are divided into the following function classes:

- API Management  
Manages the access and availability of Job API and connected engines.
- Server list Management  
Manages the server list and the deployment table.
- Power Management  
Manages the power status of servers.
- Repository Management  
Manages repositories and images inside of repositories.
- Directory Management  
Manages directories inside of repositories.
- Group Management  
Manages groups and group members.
- Deployment Management  
Manages the installation and deployment of one or a group of servers.
- Job Management  
Manages scheduled jobs and jobs which were sent to engines.

The Job API is an independent installation pack and can be provided on the Deployment Manager CD. Deployment Manager installation is not necessarily required for the Job API but reduces the set of functions offered accordingly. An own Job-API specification describing the details of the API is available on the Deployment Manager CD.



---

## 3 Installing Deployment Manager

Deployment Manager is distributed as an individual delivery unit via CD-ROM.

Deployment Manager consists of two installation packages:

- *Deployment Manager* package  
Web-based graphical user interface including the *FSC Deployment Manager* service.
- *Deployment Services* package  
The deployment services including PXE service, TFTP service and deployment service (= cloning module).

You can install both packages at the same time or separately from each other. The packages can be installed on different systems. If the two packages are installed in different locations, both computers must be within the same Windows network domain. In addition, the user account specified during the installation process must be a member of this network domain.

If an image repository is used by more than one computer in a LAN, you must release the repository for the user account that was specified during the installation process.

Deployment Manager must access the ServerView database. Both modules can be installed on one system. During the installation you will be asked where Operations Manager is installed.

The following add-on packages are available on the CD-ROM:

- *JavaRuntimeEnvironment* package  
Package for the Java runtime environment. This package is required for the graphical user interface of Deployment Manager.
- *ServerStart/Installation Manager* package  
Installs ServerStart/Installation Manager from the ServerStart/Installation Manager CD/DVD.
- *Job API* packages for IIS and Apache  
Installs a programming interface (API) for using the Deployment Manager functionality from an application. You will find the descriptions of the APIs on the Deployment Manager CD.

## 3.1 Requirements

- Java Runtime Environment (SUN JRE version 1.5)
- Web server (IIS or Apache)
- ServerView S2/Operations Manager as of version 4.20
- Installed DHCP server

The system requirements are described in [section “System Requirements” on page 14](#).

### 3.1.1 Installation of ServerStart/Installation Manager

ServerStart/Installation Manager is not required. If ServerStart/Installation Manager as of version 5.502 is installed on the deployment server, you can use the Deployment Manager function to create installation groups for mass installation of PRIMERGY servers with ServerStart/Installation Manager configuration files and the system preparation of non blade servers. In this case a ServerStart/Installation Manager version 6.605 or higher is needed. If an account without administrator rights is specified during installation of the *Deployment Manager* package, a ServerStart/Installation Manager version 6.611 or higher is needed.

If you select WinPE MDP as the deployment platform, you will need ServerStart version 6.711.



For full support of the BX630 scalable server blade, ServerStart/Installation Manager version 5.508 or higher is required.

You can also install ServerStart/Installation Manager from the ServerStart/Installation Manager CD/DVD.

### 3.1.2 Installation of Operations Manager

Deployment Manager is integrated in the user interface of Operations Manager. The Operations Manager package (as of version 4.20) must be installed before you start Deployment Manager.

This package is available on the PRIMERGY ServerView Suite Software CD which is a component of ServerView Suite. For more information on installing Operations Manager, see the Operations Manager installation guide contained on the ServerBooks DVD.

### 3.1.3 Installation of ServerView SNMP Agents

During the image creation process you can specify whether the server should be shut down before the image creation process is started (see [figure “Save Options window” on page 147](#)).

If you want to use this, you need to install and run ServerView SNMP agents on the server:

- On a Windows server platform, ServerView SNMP agents as of version 3.10.05.
- On a Linux server platform, ServerView SNMP agents as of version 3.10.06.

During the installation of the SNMP agents you must allow SNMP Set operations. How to install and configure these agents is described in the Operations Manager installation documentation on the ServerBooks DVD.

You must also configure the SNMP service in the *Properties* window on the system. In the *Security* tab, add the community with the relevant SNMP rights.

### 3.1.4 Deployment Server

Deployment Manager and ServerStart/Installation Manager support remote access to required resources over a LAN during the installation process. The deployment software is booted using the PXE boot service, allowing the unattended installation to be started on a remote server.

In order to perform a remote installation using ServerStart/Installation Manager or image creation/cloning using Deployment Manager, the following software packages must be available on the deployment server:

- A standard Windows 2003 Server or Windows 2008 Server platform



If you use Windows Server 2008, you have to configure the Windows firewall on the reference system, see [section “Configuring the Windows Firewall on the Reference System” on page 138](#).

- ServerStart/Installation Manager v5.502 (or higher) for PXE-based remote installation or/and
- Deployment service (cloning module) for PXE-based remote image creation and cloning (part of the Deployment Manager installation)
- A DHCP service (if none is already present in the LAN segment)



The deployment server and the target system must be in the same LAN segment (only with the deployment method *Multicast*). Only one deployment server can be in use but more than one can exist in one LAN segment.

The IP address of a deployment server must be static.

## PXE service

The Fujitsu Siemens Computers PXE service must run on the deployment server. It comes with either Deployment Manager, ServerStart/Installation Manager (as of revision 5) or Update Manager. These components are using the same PXE service.

Unless PXE Service API is standardized, other PXE services are not supported.



To avoid conflicts of PXE services during the installation, Deployment Manager automatically detects other PXE services on the LAN. This works only for aggressive services reacting to each PXE request independently of the client MAC address used.

If ServerStart/Installation Manager and Deployment Manager and maybe Update Manager are installed on the same machine, the basic PXE service will be shared between both modules. The installer of each product will enhance the basic PXE service by adding specific modules for their specific use of the basic service. With ServerStart/Installation Manager the PXE service will be installed/enhanced only if *ServerStart - remote installation* is selected in the first installation frame.

You can only install one PXE service per system. This service uses port 4011 (default) on the network. If more than one network interface card (NIC) is installed on the deployment server, the PXE service can be assigned to one of them. To reassign the NIC to the PXE service, edit the file *localipaddress.txt* in the installation folder *.\<Deployment Service installation path>\bin* of Deployment Service.

### DHCP service

If no DHCP service is installed on the deployment server, the PXE service is using the standard DHCP port. A PXE client must scan for a PXE service in the LAN segment by transmitting a broadcast on port 67.

If a DHCP service is present on the deployment server, the PXE service is installed as a DHCP proxy service (activated DHCP option: 60). In this case the DHCP service is able to directly report the IP address of a PXE service (NBS = NetBootService) to a DHCP client, whereupon the client can directly access the PXE service by its IP address on port 4011.

If DHCP and PXE service are installed on different systems, the 060 option must be disabled inside the DHCP service.

For more details on the PXE protocol, see the detailed description of the PXE service.

## 3.1.5 Network Configuration

Deploying operating systems requires a high-bandwidth network operating at least 100Mbps. In addition, special network services and techniques are used to control the transaction of transferred packages.

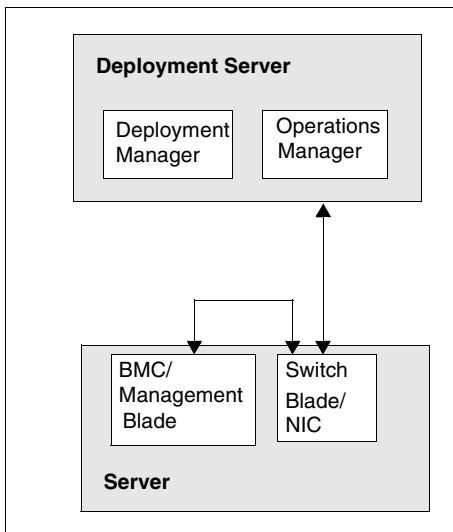
When extensive cloning images are to be transferred to a large number of clients, the standard multicast protocol is used. Each data package is sent over the LAN only once. Recipients must be members of the relevant multicast session group in order to collect and read these packages. Otherwise the transferred packages are ignored. After completion of a data transfer, each recipient returns an acknowledgment of receipt to the multicast server. When all receipts have been submitted, the server sends out the next data package.

If one of the session group members is using a 10Mbps LAN connection, the whole multicast session will run at 10Mbps. When it comes to multicast, therefore, it is highly advisable to set up a homogeneous LAN environment running at 100Mbps or faster.

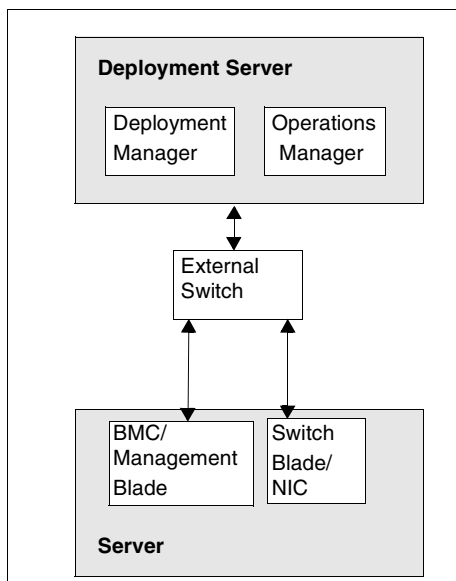
Managed switches and routers can control the transmission of multicast packages in order to prevent non-multicast session members from being bothered by them. This standard for IP multicasting in the Internet is called Internet Group Management Protocol (IGMP). With the IGMP protocol only members joining the current multicast session will see the sent out packages.

### 3.1.5.1 LAN Connections

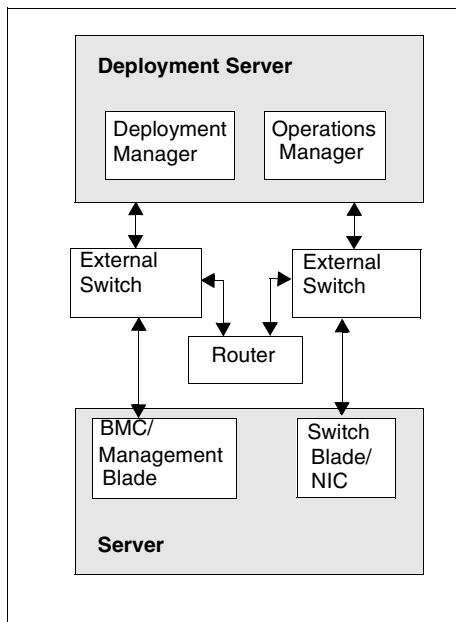
The LAN ports can be connected externally in one of the following ways (the following assumes that Deployment Manager and Operations Manager are installed on the same server):



See “[LAN Connection Topology and IGMP Settings \(Switch Blade\)](#)” on page 49, [02], [04]



See [“LAN Connection Topology and IGMP Settings \(Switch Blade\)”](#) on page 49, [06], [08], [10], [12]



See [“LAN Connection Topology and IGMP Settings \(Switch Blade\)”](#) on page 49, [05], [07], [09], [11]

For high-performance configurations a switch or router should be used instead of hubs.

### **3.1.5.2 LAN Connections (Blade Server)**

Each switch blade has ten downlink ports to the server blades and three uplink ports to level-3 switches. These LAN connections provide the only I/O functionality for the server blade.

The two management blades have separate LAN connections for maintaining accessibility to the system even if the standard traffic network connections are down.

In the Blade Server System manuals, you will find various examples of the blade system configuration and an overview of the LAN mapping.

The management blade is fixed at 10Mbps only (no autosensing). The other end of the management blade LAN should be configured as “10Mbps/full duplex fix”. If autonegotiation is configured on the switch/router side, the final connection is negotiated to 10Mbps/half. Collisions will occur.



### 3.1.5.3 LAN Connection Topology and IGMP Settings (Switch Blade)

The following table summarizes the LAN connection topology and IGMP settings of switch blades and external switches/routers:

External switch	Switch blade/ NIC	BMC/ Management blade LAN	Performance of deployment	
External switch not used				
	[01]	IGMP off	not same segment	not configurable
	[02]		same segment	governed by 10 Mbps <sup>*1</sup>
	[03]	IGMP on	not same segment	not configurable
	<b>[04]</b>		same segment	IGMP effective
	External switch used			
IGMP off	[05]	IGMP off	not same segment	not configurable
	[06]		same segment	governed by 10 Mbps <sup>*1</sup>
	[07]	IGMP on	not same segment	not configurable
	[08]		same segment	governed by 10 Mbps <sup>*1</sup>
IGMP on	[09]	IGMP off	not same segment	not configurable
	[10]		same segment	governed by 10 Mbps <sup>*1</sup>
	[11]	IGMP on	not same segment	not configurable
	<b>[12]</b>		same segment	IGMP effective

Table 2: LAN connection topology and IGMP settings

<sup>\*1</sup> When a large number of broadcast packets is sent to a broadcast group which contains 10Mbps ports, the overall performance of the broadcast is governed by the slowest port, e.g. 10Mbps.

IGMP enabling is only effective in cases [04] and [12]!

### 3.1.5.4 Multiple Segment Cloning

Deployment Manager uses unicast (image creation and cloning) and multicast (cloning only) data transfer.

Multicast and unicast transfers both work with a data flow control based on acknowledgment packages.

This means that for each data package an acknowledgment from the client is expected. Combined with certain timeouts, up to 2 retries are initiated before a connection is set to the status *broken*.

A data package has bypassed the router and obviously reached the client (cause of the reaction on the client screen), but the acknowledgment has not reached the server. This fakes the mutual progress of preparing the first partition, which is not the case.

To support cloning over multiple LAN segments via a router or VLAN border, you must set certain LAN ports to be passed through in the router configuration:

The ports of the router must be enabled in both directions:

TFTP: udp 69

and PXE: udp 67/4011

for the PXE protocol.

For unicast and multicast transfer of the Deployment Service:

TCP: 4971, 4972, 4973, 4975, 4977, 4979

UDP: 4971...4980

If not all ports (especially the TCP ports) are enabled in both directions, it is possible that the preparation of the transfer will have been successful but the data transfer itself will fail. Other multicast services in the LAN segment may use the same ports as well.

The port selection by the current deployment server can be initialized in the registry settings of Deployment Manager at:

`HKEY_LOCAL_MACHINE\SOFTWARE\FUJITSU\SystemcastWizard\CLONE`

Make the following settings:

Portbase = 0x0000136e(4974), and

PortRange = 0x00000010 (16)

After a reboot, the new settings are active. These settings are of interest when multiple deployment servers or multiple multicast applications are used in one segment.

If you want to transfer IP packages across multiple segment borders, the TTL counter in the header of an IP package must be set accordingly. With the *TTL* parameter, you can specify how many “hops” you allow multicast packets to make. Increasing the value means that multicast packets can be transferred over many routers.

A configuration is mandatory if multiple segment cloning is required. There is one entry with which you can manipulate TTL in the deployment server operating system registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\FUJITSU\SystemcastWizard\  
CLONE\MRestore  
-> Value: TTL
```

By default Deployment Manager uses the value 3.

### 3.1.5.5 Multiple LAN Ports of Target Systems

It is possible to use the other LAN port of servers for the deployment process. For this purpose the other LAN port of each server must be configured using the *Deployment Configuration* window (see [section “Target System Configuration” on page 113](#)).



When the other LAN port is to be used for deployment, both the deployment server and the other LAN port of the server must belong to the same LAN segment (only with the deployment method *Multicast*). The deployment server LAN port used for the PXE services is defined in the file *localipaddress.txt*.

### 3.1.6 Creating an Image Repository

- ▶ Create a shared network directory (UNC network path) on your deployment server (or on another server in the LAN segment).
- ▶ Share this folder so that it can be accessed remotely.



Both user profiles created in the course of the Deployment Manager installation (see [section “Installation” on page 57](#)) must be entitled to fully access that network share.

- ▶ Specify a repository name and the UNC network path in order to register the new share as an image repository in Deployment Manager.

The images will be stored in this directory.

## 3.2 Installation in Windows 2008

### 3.2.1 Actions before Installing Deployment Manager

Before you install Deployment Manager you must perform the following steps if you want to use IIS as the Web server.



If you installed the Apache Web server during the Operations Manager installation, no further actions are necessary.

1. Install IIS 7 on Windows Server 2008:

- ▶ Select *Start – Administrative Tools – Server Manager*.

The *Server Manager* window opens.

- ▶ Select *Roles*.

- ▶ Add the Web server (IIS) by clicking the *Add Roles* button under *Roles Summary*.

- ▶ Check the role services by clicking *Role Services*. To start Deployment Manager, the following services should be installed:

- Common HTTP Features

- HTTP Redirection

- Application Development

- CGI

- SAPI Extensions

- Security

- Basic Authentication

- Windows Authentication

- Management Tools

- IIS Management Scripts and Tools

- Management Service

- IIS 6 Management Compatibility

- IIS 6 Metabase Compatibility

- IIS 6 WMI Compatibility

- IIS 6 Scripting Tools

- IIS 6 Management Console

Server Manager window - Role Service

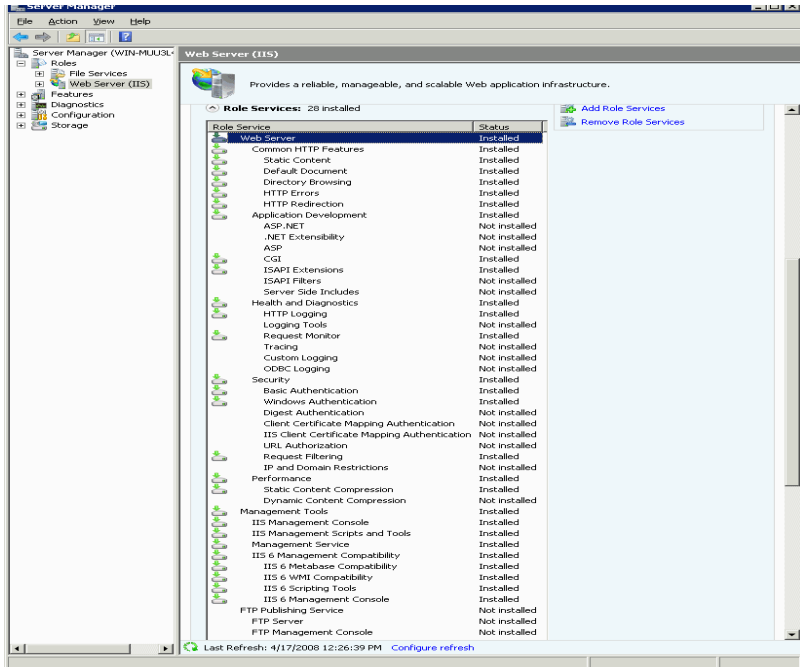


Figure 9: Server Manager window

2. Create the user *IIS\_User* and add it to the *IIS\_IUSRS* group:

- ▶ Select *Start – Administrative Tools – Computer Management*.  
The *Computer Management* window opens.
- ▶ Open *Local Users and Groups* and select *Users* in the left pane.
- ▶ Select *New User* from the context menu. The *New User* window is displayed.
- ▶ Enter the following values to create the new user:
  - User name: *IIS\_User*
  - Enter a password.
  - Uncheck the *User must change password at next logon* option.
  - Check the *Password never expires* option.

Click *OK* to add the new user.

- ▶ Add the user to the *IIS\_IUSRS* group. Select *Groups* in the left pane.
  - ▶ Select the *IIS\_IUSRS* group and choose *Add to Group* from the context menu. The *IIS\_IUSRS Properties* window is displayed.
  - ▶ Click *Add*. Enter the new user name (*IIS\_User*) in the *Select Users* window.
  - ▶ Click *OK*.
3. Edit the authentication in the Internet Information Services (IIS) Manager:
- ▶ Select *Start – Administrative Tools – Internet Information Services (IIS) Manager*.
  - ▶ Click your server in the left pane.
  - ▶ Double-click *Authentication* in the middle pane.
  - ▶ Select *Anonymous Authentication* and click the *Edit* button in the right pane.
  - ▶ In the *Edit Anonymous Authentication Credentials* window click the *Set* button.
  - ▶ In the *Set Credentials* window enter *IIS\_User* under user name. Enter a password and confirm the password.
  - ▶ Click *OK*.

### 3.2.2 Actions after Installing Deployment Manager

After installing Deployment Manager you must perform the following steps if you want to use IIS as the Web server.



If you installed the Apache Web server during the Operations Manager installation, no further actions are necessary.

1. Add *DMClient.exe* to the list of the CGI extensions allowed:
  - ▶ Select *Start – Administrative Tools – Internet Information Services (IIS) Manager*.
  - ▶ Click your server in the left pane.
  - ▶ Double-click *ISAPI and CGI Restrictions* in the middle pane.
  - ▶ Click *Add ...* in the right pane.

- ▶ In the *Add ISAPI or CGI Restriction* window enter the following values:
  - ISAPI or CGI path:  
*C:\inetpub\scripts\RemoteDeployEngine\DMClient.exe*
  - Description: *DMClient*
  - Check *Allow extension path to execute*.
  - Click *OK*.
- 2. Set *Impersonate User* to *False* for RemoteDeployEngine:
  - ▶ Select *Start – Administrative Tools – Internet Information Services (IIS) Manager*.
  - ▶ In the left pane expand the server entry.
  - ▶ Select *Default Web Site – Scripts – RemoteDeployEngine*.
  - ▶ Double-click *CGI* in the middle pane.
  - ▶ Under *Security* set *Impersonate User* to *False*.



### 3.3 Installation

Deployment Manager starts automatically after insertion of the CD-ROM. If the application fails to start, please open the *RDSetup.exe* file in the *setup* directory of the CD-ROM.

The following start window is displayed:

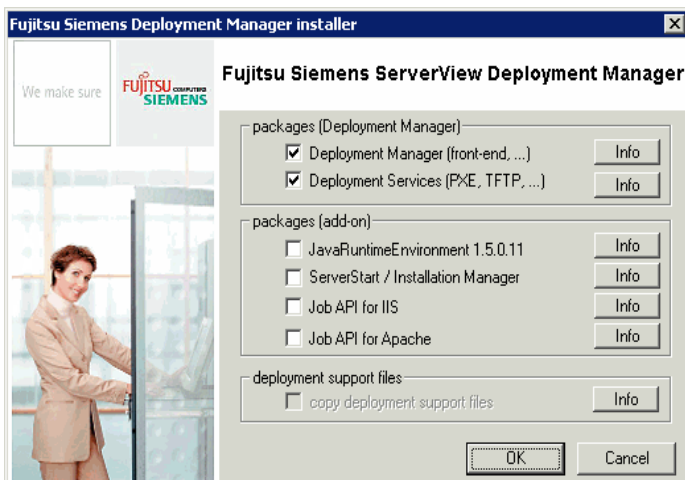


Figure 10: Start window

- Select the packages you wish to install. Click the *OK* button. For further information click the *Info* button.



If you select both Deployment Manager packages, the *Deployment Manager* package is the first package to be installed.

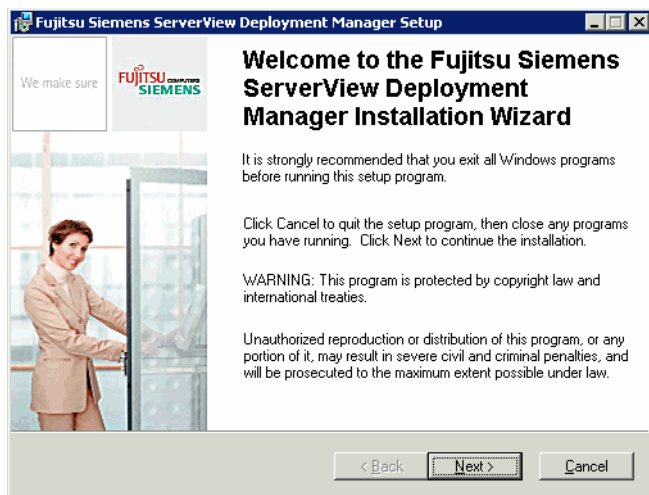
You can also install add-on packages, e.g. *Job API for IIS*.

For the deployment you need some files which are not available on the Deployment Manager CD. You can install the files after the installation of the deployment services (see [page 71](#)) or later.

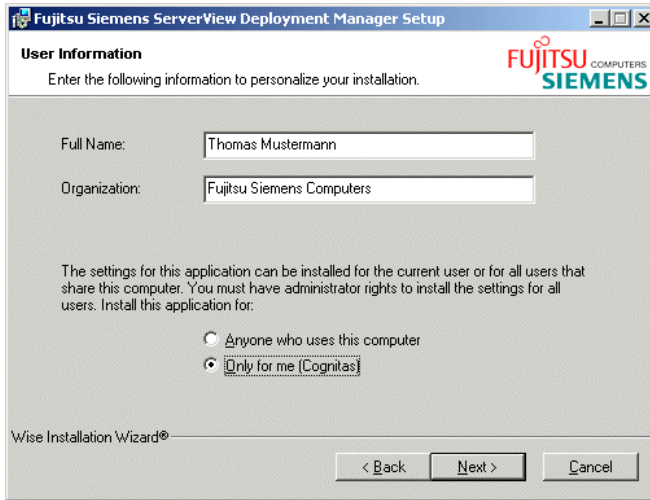
The following section describes the installation sequence for the *Deployment Manager* package. For a description of the installation sequence for the *Deployment Services* package, please see the [section “Installing the Deployment Services Package” on page 67](#).

### 3.3.1 Installing the Deployment Manager Front-end Package

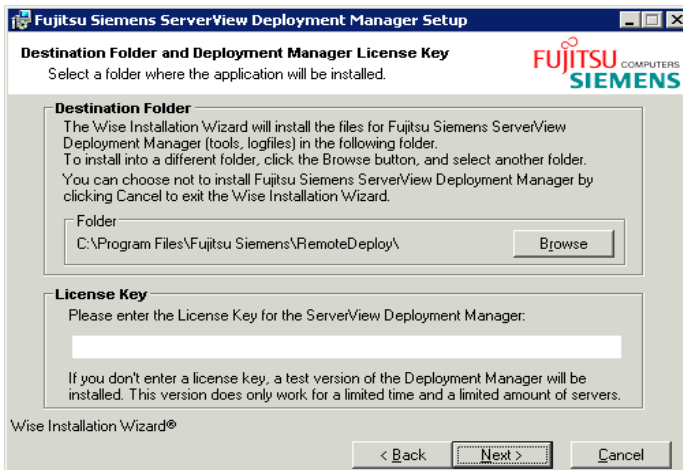
If you select the *Deployment Manager* package, the following window appears:



- ▶ Click the *Next* button.
- ▶ Approve the license agreement by marking the appropriate radio button.
- ▶ Click the *Next* button.



- ▶ Fill in your name and organization.
- ▶ Specify whether the Deployment Manager settings should only apply to the current user or to anyone who uses the target computer. Mark the appropriate radio button.
- ▶ Click the *Next* button.



- ▶ Enter the license key. If an update installation from the same major version is done, the license key specified during the previous installation is displayed.

Or, if you do not enter a valid license key, an evaluation key is created. After you start Deployment Manager a message window is displayed which shows when the evaluation key will expire.

Valid license keys can be installed later. Refer to [section “License Management” on page 123](#) for more information.

- ▶ Click the *Next* button.

- ▶ Set up your user account. The user profile you specify must already be available on the target system or domain.

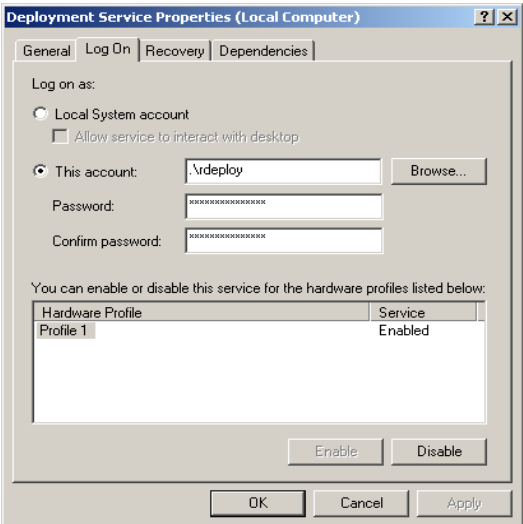
You can also create a new user. Click the *Create New User* button in the window. This opens the *Create New User* window. Enter the new user account.

**i** If the Deployment Manager packages (*Deployment Manager* package and *Deployment Services* package) are installed on different computers, one of the following requirements must be met:

- When using one or more domain accounts, both computers must be present in the same Windows network domain. In addition, the domain user account specified during the installation process must be a member of this network domain.
- When using local user accounts, both computers may be present in different network domains or in no domain at all. However, both local user accounts must be entitled to fully access the shared image repository. This can be achieved by setting up identical user accounts for Deployment Manager and services on the computer containing the repository. User names and passwords must match those of the local user accounts. If only one user account is to be used, it must be reproduced the same on all computers containing the *Deployment Manager* package, the *Deployment Services* package and/or image repository.

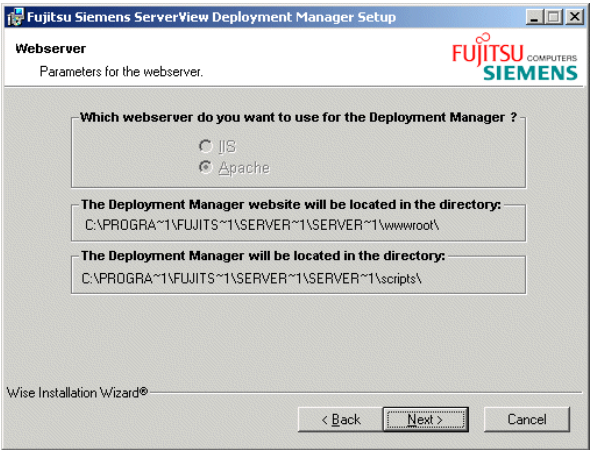
The user account which is defined during the installation of Deployment Manager is assigned to the deployment service *Deployment Service*. The user account which is defined during the installation of the deployment service is assigned to the service *Deployment Service*. If the password of one of both user was changed by the administrator using the user management of the control panel, the appropriate password setting must be changed in the server administration of the administration tools in the control panel as well.

Select *Start – Settings – Control Panel – Administrative Tools – Services*. Double-click the service (*FSC Deployment Manager* or *Deployment Service*) or select *Properties* from the context menu and change to the *Log On* tab.



This account shows the user name whose password has been changed. Change the password of that user. To activate the new settings click *OK* and stop and restart the service. Afterwards you should be able to logon to Deployment Manager again.

- Click the *Next* button.



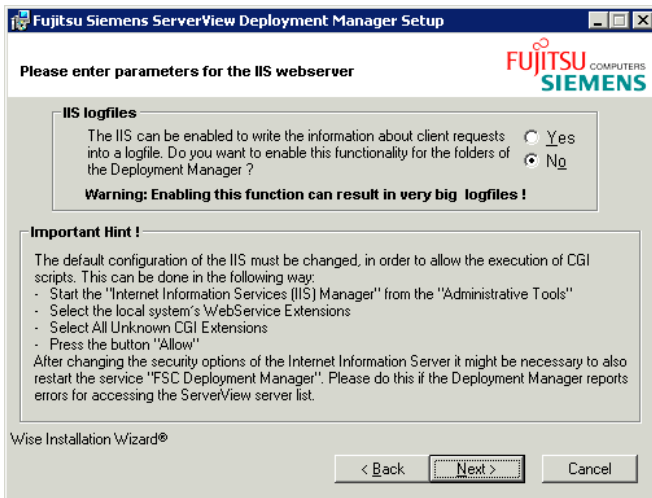
- Deployment Manager can be integrated into either the IIS (from Microsoft) or Apache Web server. If both Web servers are already installed, you can select the desired Web server for Deployment Manager. Mark the appropriate radio button.



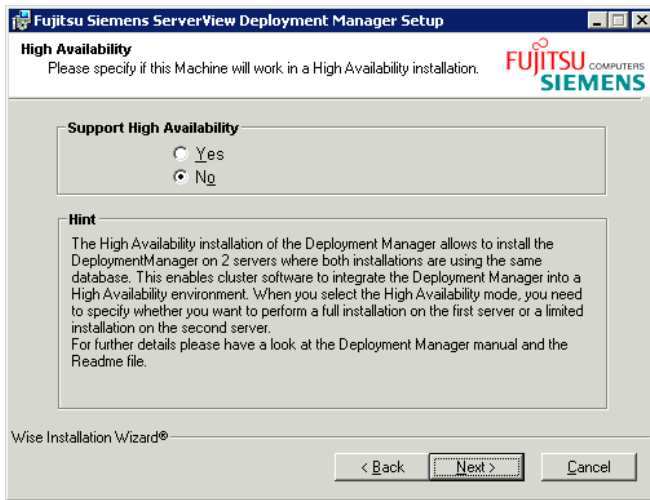
Apache Web server integration is only available if the Apache Web server has been installed along with the Operations Manager setup.

Otherwise the already installed Web server is used for Deployment Manager.

- Click the *Next* button. If you selected the IIS Web server, the following dialog appears:



- Click the *Next* button.



**Fujitsu Siemens ServerView Deployment Manager Setup**

**High Availability**  
Please specify if this Machine will work in a High Availability installation.

**Support High Availability**

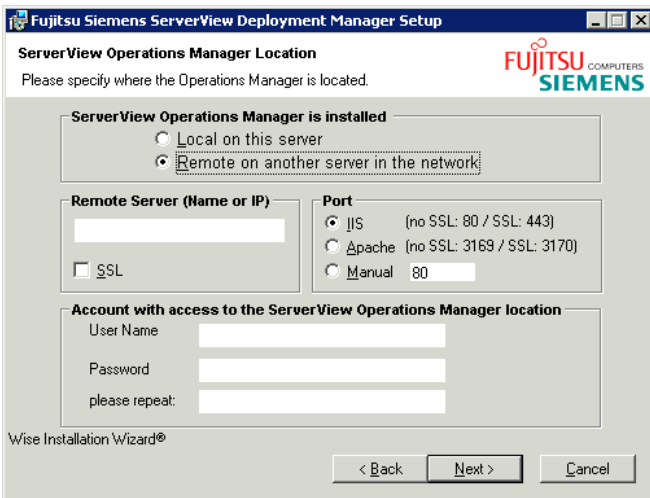
☐ Yes  
☒ No

**Hint**  
The High Availability installation of the Deployment Manager allows to install the Deployment Manager on 2 servers where both installations are using the same database. This enables cluster software to integrate the Deployment Manager into a High Availability environment. When you select the High Availability mode, you need to specify whether you want to perform a full installation on the first server or a limited installation on the second server.  
For further details please have a look at the Deployment Manager manual and the Readme file.

Wise Installation Wizard®

< Back   Next >   Cancel

- ▶ If you select the *No* option, a standard installation is performed (recommended). Select *Yes* to support the high-availability function. For more information see [chapter “High-Availability Support” on page 317](#).
- ▶ Click the *Next* button.



**Fujitsu Siemens ServerView Deployment Manager Setup**

**ServerView Operations Manager Location**  
Please specify where the Operations Manager is located.

**ServerView Operations Manager is installed**

☐ Local on this server  
☒ Remote on another server in the network

**Remote Server (Name or IP)**

☐ SSL

**Port**

☒ JIS (no SSL: 80 / SSL: 443)  
☐ Apache (no SSL: 3169 / SSL: 3170)  
☐ Manual 80

**Account with access to the ServerView Operations Manager location**

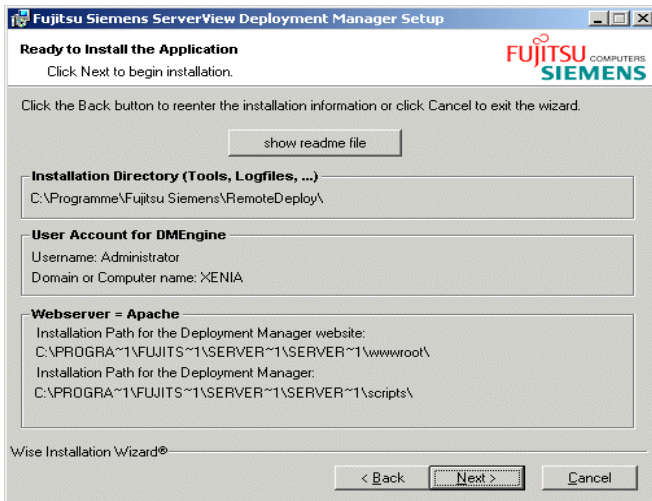
User Name   
Password   
please repeat:

Wise Installation Wizard®

< Back   Next >   Cancel



- Specify the location where Operations Manager is installed. If Operations Manager is installed on the same system, select the *local on this server* option and click *Next*. Otherwise you must specify the server name or IP address and the port. The user authentication is not mandatory.
- Click the *Next* button.



- Click the *Next* button to start the installation process.



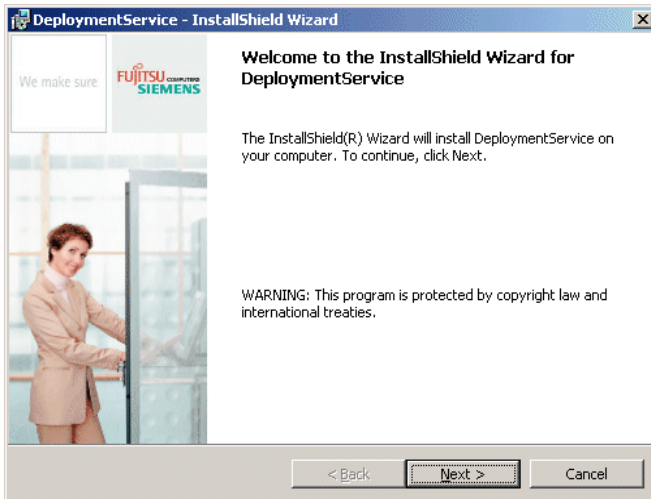
- Click the *Finish* button to exit the wizard.

Once the installation has been successfully completed, you can start Deployment Manager, see [section “Starting Deployment Manager” on page 78](#).

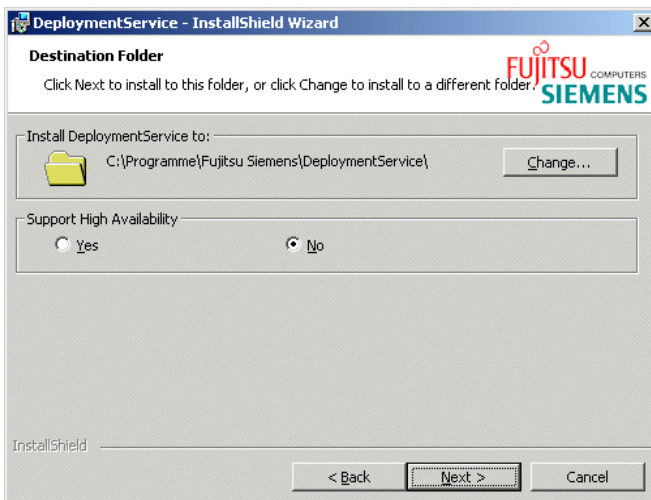
**i** In order to start Deployment Manager, a deployment server running the required deployment services must be installed in the LAN segment (see [section “Installing the Deployment Services Package” on page 67](#)).

### 3.3.2 Installing the Deployment Services Package

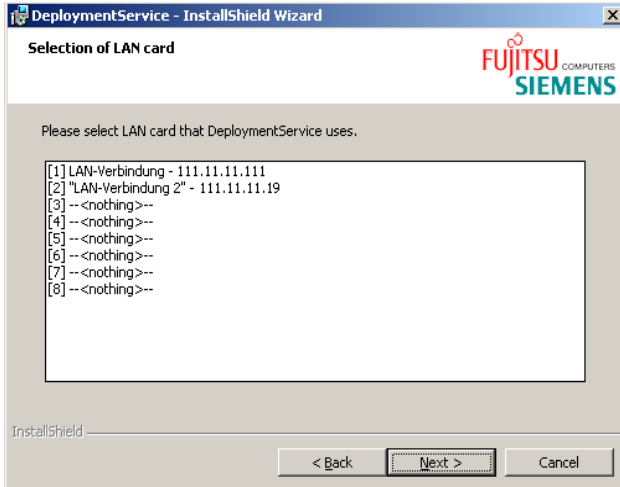
If you select the *Deployment Services* package, the following window appears:



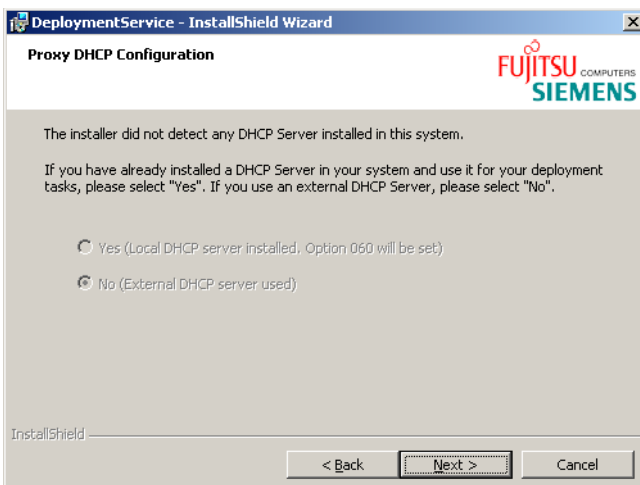
- Click the *Next* button.



- ▶ If you select the *No* option, a standard installation is performed (recommended). Select *Yes* to support the high-availability function. For more information see [chapter “High-Availability Support” on page 317](#).
- ▶ Click the *Next* button.



- ▶ Select the LAN port that should be used for deployment and click the *Next* button.



The PXE service requires a DHCP service to be present on the LAN.



The selected LAN port (IP address) is stored in the *localipaddress.txt* file in the same directory as the *PXEService.exe* file. By default, this is:  
*C:\Program Files\Fujitsu Siemens Computers\DeploymentService\bin*

- Specify whether the DHCP service is running on the PXE service target machine or another computer in the LAN segment. Mark the appropriate radio button.
- Click the *Next* button.

- Fill out the user account under which the deployment service is to be run.



You must enter this user account in Deployment Manager when connecting to a deployment server.

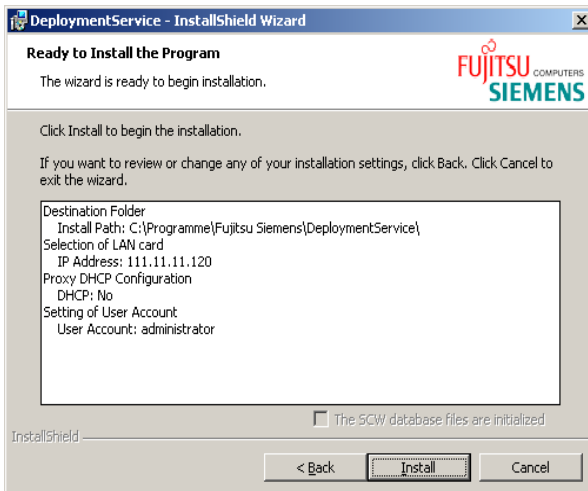
- The user account can either be a domain login [notation: <domain>\<user name>] or a local profile [notation: <computer name>\<user name>].

In the latter case, details of the computer name can be left out.

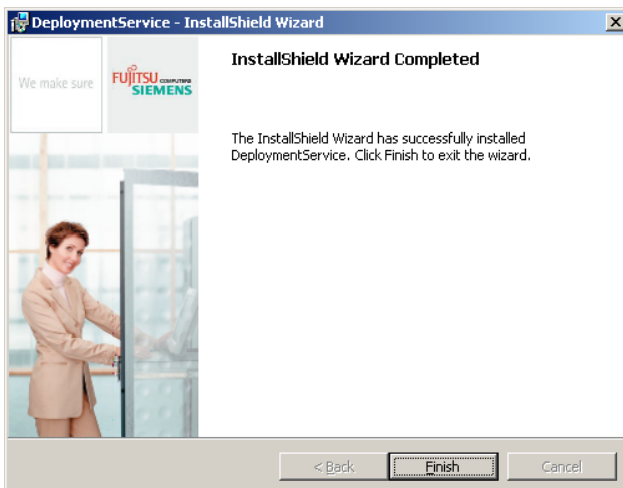


It is recommended that you enter the same values that were specified when installing the *Deployment Manager* package.

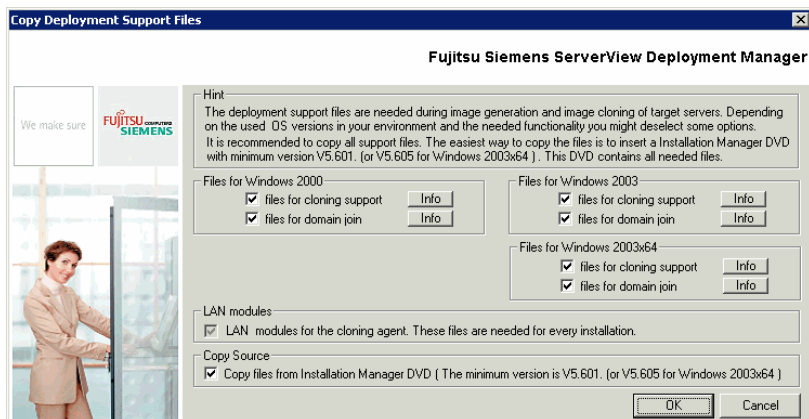
- Click the *Next* button.



- Click the *Install* button to start the installation process.



- Click the *Finish* button to exit the wizard.



- For the deployment you need some files which are not available on the Deployment Manager CD. The files are available on the ServerStart/Installation Manager CD/DVD as of version 6.605. For more information, see the *Hint* section. Click *OK* to start the installation.

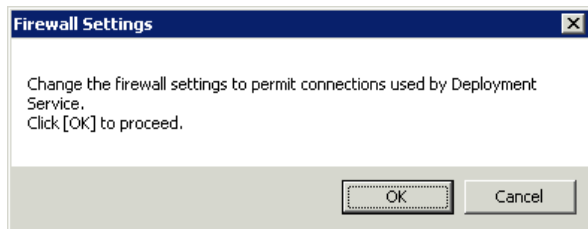


The LAN modules are mandatory for Deployment Manager. Without these modules, image creation and image deployment are not possible.

You can install these modules when you have finished the installation by executing *rdsetup.exe* on the Deployment Manager CD and selecting the *copy deployment supportfiles* button on the first screen.

### 3.3.2.1 Configuring the Windows Firewall in Windows 2008

If you install Deployment Manager in Windows 2008, the following message is displayed:



You can also change the firewall settings later at any time by calling the `fw_setting.vbs` script.

The `fw_setting.vbs` script is copied to the *<Deployment Manager installation path>\RemoteDeploy* directory. To execute the script proceed as follows:

- ▶ Start a command prompt.
- ▶ Change to the *<Deployment Manager installation path>\RemoteDeploy* directory.
- ▶ Execute the following command:

```
cscript.exe fw_setting.vbs
```



### 3.3.3 Preparation for Multicast Environment

The default range of IP addresses used by Deployment Manager is from 225.1.0.1 to 225.1.0.9. The range of IP addresses can be changed by modifying some information in the registry entry.

Default entry in the registry:

```
HKLM\SOFTWARE\Fujitsu\SystemcastWizard\CLONE  
MCastIPBase: REG_SZ: <base address>
```

Default is 255.1.0.0

(-> use from 225.1.0.1 to 255.1.0.9)



You should specify the IP address in *Class D*. *Class D* addresses are used for multicasting. The first four bits of the IP address are set to *1110*.

## 3.4 Uninstalling/Removing Deployment Manager



- It is highly recommended that you uninstall Deployment Manager rather than deleting its folder. This is because various components of a program can be spread all over your system and in the registry.
- The deployment services must be removed from the system before an update or reinstallation of Deployment Manager. If services remain on the system, the reinstallation may not be performed properly and error messages may be issued when the operating system is restarted.
- If you uninstall Deployment Manager (*Deployment Manager* and *Deployment Services* packages) and afterwards you install a new Deployment Manager version, you must clear the site-cache from the corresponding browser.

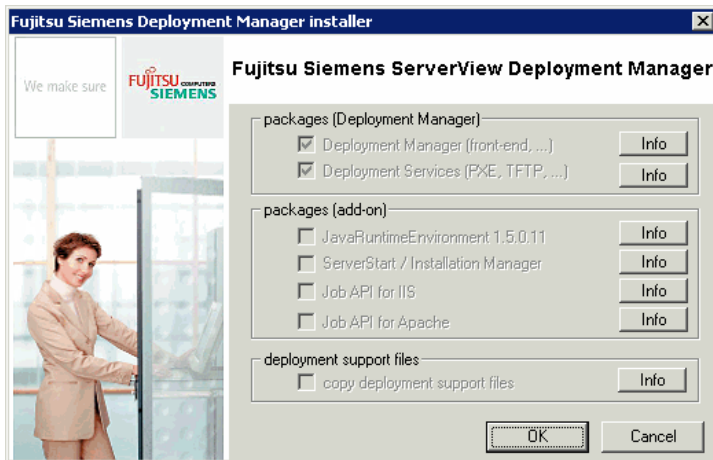
If you uninstall Deployment Manager (*Deployment Manager* and *Deployment Services* packages) and subsequently want to install an older version than before, you must delete the Java plug-in cache and remove the previous \*.jar and \*.gif files stored there. Otherwise a mixture of old and new modules will be running in the Deployment Manager front-end session and indeterminate errors may occur.

Additionally you must clear the browser cache for downloaded files.

- An upgrade from RemoteDeploy version 1.21 or 2.0 to version 3.0 and higher is supported.

### There are different methods of uninstalling:

1. Running uninstall from the *Programs* folder in the Windows *Start* menu.
  - ▶ Make sure Deployment Manager is not running.
  - ▶ Select *Start – Programs – Fujitsu Siemens ServerView – Deployment Manager*.
  - ▶ Select the *uninstall Deployment Manager completely* entry. The following window is displayed.



The packages which are installed are marked. Select the relevant packages which should be uninstalled.

- ▶ Confirm to uninstall the packages.
2. Running *Add/Remove Programs* from the *Control Panel*.
- ▶ Make sure Deployment Manager is not running.
  - ▶ Click the *Start* button on the Windows task bar.
  - ▶ Click the *Settings* entry.
  - ▶ Click the *Control Panel* menu entry.
  - ▶ Double-click the *Add/Remove Programs* icon.
  - ▶ Find the entry for the packages (*DeploymentService* or *Fujitsu Siemens ServerView Deployment Manager*) and select the *Add/Remove* button to remove the package.



These packages may have been installed on different computers.

- ▶ A screen will prompt you for confirmation. Click *yes* to start the uninstallation process.



During the uninstallation of the *Deployment Services* package, you can select whether you want to delete the SCW database and the SCW log files.



---

## 4 Using Deployment Manager

Web-based Deployment Manager is integrated in Operations Manager as a separate application. Deployment Manager handles all PRIMERGY servers that appear in the ServerView server list.

Operations Manager is the first application to detect the PRIMERGY servers and their system information:

- On request Operations Manager searches for the LAN to find all the existing servers in one segment.
- Operations Manager requests a list of system information for each non-blade server and for the management blade of each server blade contained in a blade chassis.
- Operations Manager creates a physical server list for each server and consolidates logical server groups based on the system information received.

How to start Operations Manager is described in the “Operations Manager” manual.

# 4.1 Starting Deployment Manager

## Starting via Operations Manager

Deployment Manager is integrated in Operations Manager. In Operations Manager select the *Deployment Manager* item from the *Deployment* menu in the Operations Manager main window. The Deployment Manager start window is displayed, see [section “Deployment Manager Start Window” on page 79](#).



The *Deployment* menu will only appear in Operations Manager if Deployment Manager has been installed.

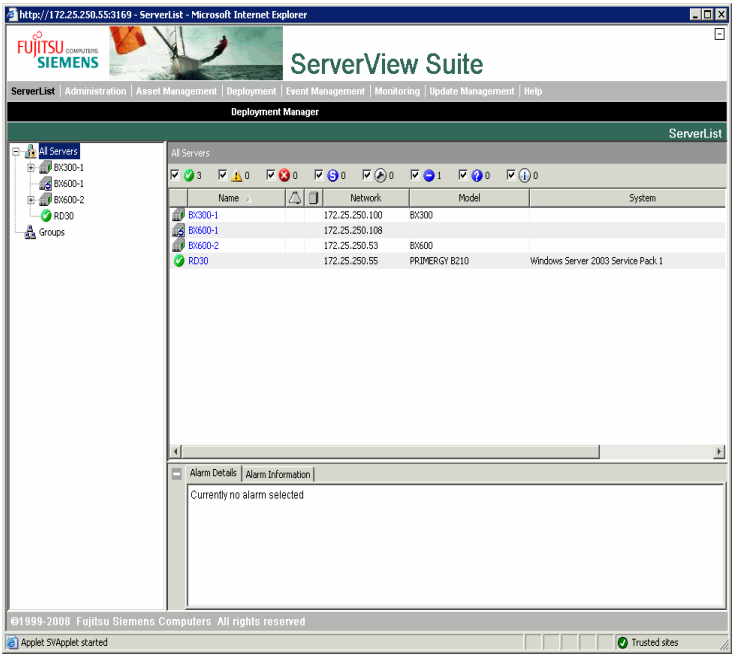


Figure 11: Operations Manager main window

## Starting via the Windows start menu

You can also start the Deployment Manager front-end via the Windows start menu:

*Start – Programs – Fujitsu Siemens ServerView – Deployment Manager – start Deployment Manager*

### Starting via a link

If you specified during the installation that Operations Manager is located remotely on another server in the network, the *Deployment* menu is not added to the menu bar of Operations Manager.

You can start Deployment Manager via the following link:

<http://<ip address>/RemoteDeploy/DeploymentManager.htm>

<ip address> must be replaced by the IP address of the Web server on which Deployment Manager is installed.

## 4.1.1 Deployment Manager Start Window

When you start Deployment Manager, the following start window opens:



Figure 12: Deployment Manager start window


Click the *Start* button to start Deployment Manager. You can then select a deployment server, see [section “Selecting a Deployment Server” on page 80](#).

If you mark the SSL check box, you can choose additional security mechanisms (encryption and user authentication).

Clicking the *about* link opens a window which displays information about the Deployment Manager version. Clicking the *help* link displays the online help system.

### 4.1.2 Selecting a Deployment Server

On startup you can select the deployment server you want to use. This determines the LAN segment for which deployment jobs can be executed. You can select one of the configured deployment servers from a list or add a new deployment server to the list, see the [section “Adding a New Deployment Server” on page 120](#).



After the installation of Deployment Manager, the list of deployment servers is empty. You must therefore first create a new deployment server.

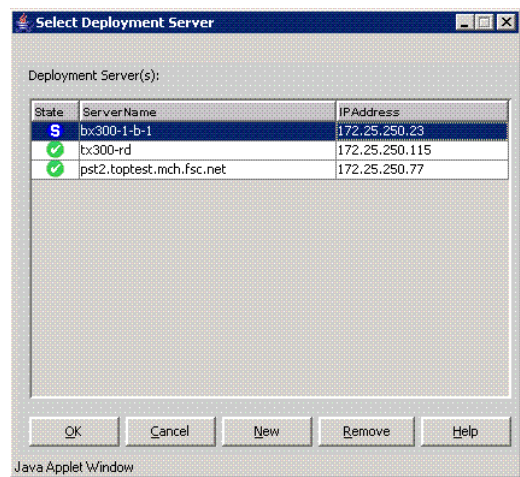


Figure 13: Selecting Deployment Server



### 4.1.3 User Authentication

When you have selected the deployment server, you must enter the user name and password for your selection. These must be the same as those specified during the installation of Deployment Manager (*Deployment Services* package). The user name and password are based on the authentication for the deployment service (cloning module).

The installation of the deployment services creates a (local) user group *Deployment Admins* on the deployment server where the cloning module is running. The user account used when the *Deployment Manager* service is started must be created on the deployment server. This user account is automatically added to the *deployment admins* group during installation of the deployment services. It can also be an existing account. The account must be created by the administrator.

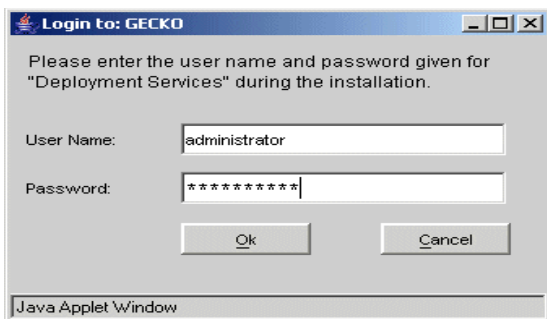


Figure 14: Login window

If you do not enter a valid license key during installation of the *Deployment Manager* package, an evaluation key is created. After you enter the user name and password a message window is displayed which shows when the evaluation key will expire. How to add a new license key is described in [section “License Management” on page 123](#).

## 4.2 Main Window

After successful authentication, the main window of Deployment Manager is displayed:

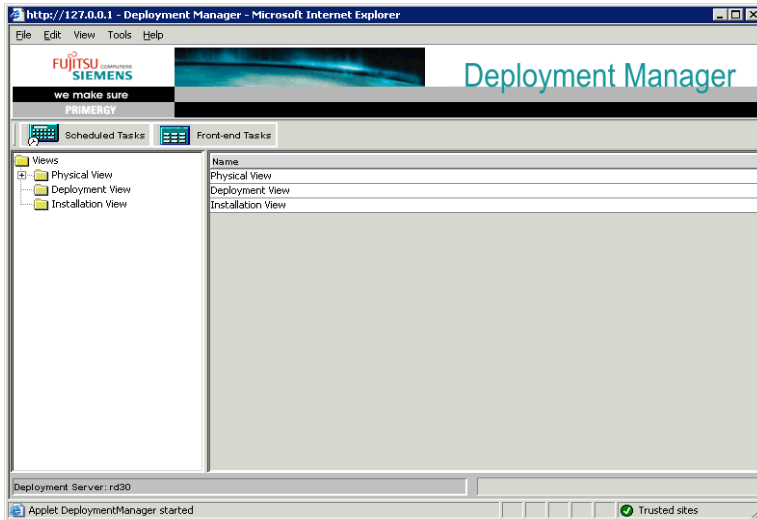


Figure 15: Deployment Manager - Main window

The menu bar contains the *File* menu, *Edit* menu, *View* menu, *Tools* menu and *Help* menu. The menu items are described in [section “Menus” on page 121](#).

The task bar contains the *Scheduled Tasks* and *Front-end Tasks* buttons. Click the *Scheduled Tasks* button to open the *Scheduled Tasks* window. This window contains a list of the defined scheduled tasks. Click the *Front-end Tasks* button to open the *Interactively Started Tasks* window. This window contains a list of the executed tasks. See [section “Task Management” on page 106](#) for detailed information.

The tree view on the left side of the main window consists of:

- Physical View

Double-clicking the *Physical View* displays all existing PRIMERGY servers from the ServerView server list (see [section “Physical View” on page 84](#)).

- Deployment View

Double-clicking the *Deployment View* displays existing deployment groups (see [section “Deployment View” on page 86](#)).

- Installation View (only if ServerStart/Installation Manager is installed)

Double-clicking the *Installation View* displays all created installation groups (see [chapter “Installing PRIMERGY Servers” on page 185](#)).

You can also use the symbols in the tree view to open or close the corresponding views.

Deployment Manager periodically checks the server list of ServerView for new server entries. The default interval is 60 seconds. You can also refresh the display by selecting *Refresh ...* in the *View* menu.

### 4.3 Physical View

The *Physical View* lists all existing PRIMERGY servers. This list is retrieved from the server list in ServerView, which runs on the same management station as Deployment Manager. You can also manually add bare servers to the list, see [section “Adding Servers” on page 91](#).

If you select a blade server from the *Physical View*, the corresponding server blades will be displayed in the right-hand frame.

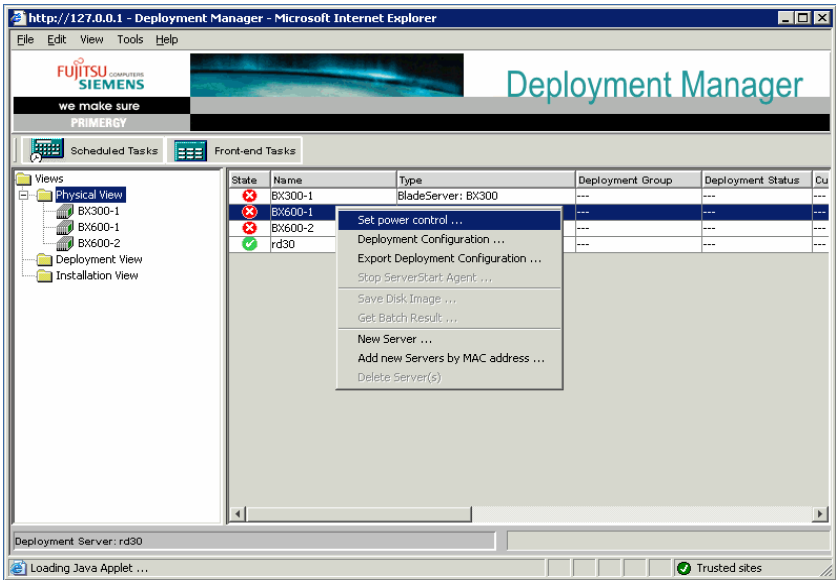


Figure 16: Physical View



You can add servers from the Physical View to a deployment group or installation group with drag&drop.

The context menus in the *PhysicalView* allows you to perform the following functions:

Function	See
Add a new server to the server list ( <i>New Server ...</i> )	<a href="#">section “Adding Bare Servers” on page 91</a>
Add a new server to the server list ( <i>Add new Servers by MAC address ...</i> )	<a href="#">section “Adding Bare Servers by MAC Address” on page 104</a>
Export the deployment configuration to a file ( <i>Export Deployment Configuration ...</i> )	<a href="#">section “Exporting the Deployment Configuration” on page 128</a>
Import the deployment configuration from a file ( <i>Import Deployment Configuration ...</i> )	<a href="#">section “Importing the Deployment Configuration” on page 129</a>
Configure the power status of the server ( <i>Set power control ...</i> )	<a href="#">section “Specifying the Power Control of Target Servers” on page 112</a>
Configure the server for deployment ( <i>Deployment Configuration ...</i> )	<a href="#">section “Target System Configuration” on page 113</a>
Stop a running ServerStart agent that might be active from a system information session ( <i>Stop ServerStart Agent ...</i> )	
Start the image creation process ( <i>Save Disk Image ...</i> )	<a href="#">section “Supported Operating Systems” on page 136</a>
Get the batch result for a list of selected servers ( <i>Get Batch Result ...</i> )	<a href="#">section “Get Batch Result” on page 178</a>
Delete servers from the server list ( <i>Delete Server(s)</i> )	

# 4.4 Deployment View

The *Deployment View* contains the deployment groups which are created on the selected deployment server. If you select a deployment group from the *Deployment View*, the servers in this group are displayed.

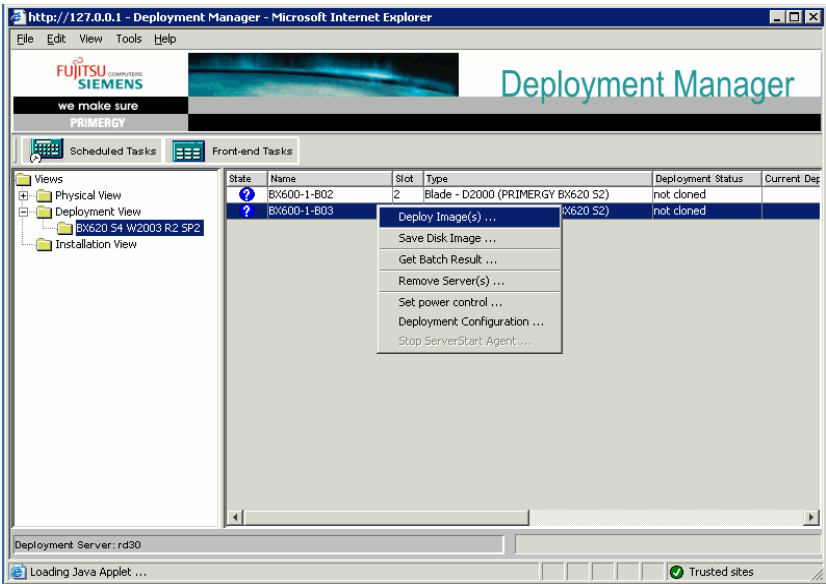


Figure 17: Deployment View

The context menus in the *Deployment View* allows you to perform the following function:

Function	See
Create a new deployment group ( <i>New Deployment Group ...</i> )	<a href="#">section “Creating/Removing a Deployment Group” on page 156</a>
Add servers to a deployment group ( <i>Add Server(s) ...</i> )	<a href="#">section “Adding/Removing Servers to/from a Deployment Group” on page 159</a>
Remove a deployment group ( <i>Remove Deployment Group ...</i> )	<a href="#">“Removing a deployment group” on page 157</a>
Start the deployment process ( <i>Deploy Image(s) ...</i> )	<a href="#">section “Starting the Cloning Process” on page 162</a>
Display the properties of a deployment group ( <i>Properties ...</i> )	<a href="#">section “Viewing and Modifying Deployment Group Properties” on page 158</a>
Configure the power status of the server ( <i>Set power control ...</i> )	<a href="#">section “Specifying the Power Control of Target Servers” on page 112</a>
Start the image creation process ( <i>Save Disk Image ...</i> )	<a href="#">section “Supported Operating Systems” on page 136</a>
Get the batch result for a list of selected servers ( <i>Get Batch Result ...</i> )	<a href="#">section “Get Batch Result” on page 178</a>
Remove servers from a deployment group ( <i>Remove Server (s)</i> )	
Export the deployment configuration to a file ( <i>Export Deployment Configuration ...</i> )	<a href="#">section “Exporting the Deployment Configuration” on page 128</a>
Configure the server for deployment ( <i>Deployment Configuration ...</i> )	<a href="#">section “Target System Configuration” on page 113</a>
Stop a running ServerStart agent that might be active from a system information session ( <i>Stop ServerStart Agent ...</i> )	

# 4.5 Installation View

The *Installation View* is only displayed if ServerStart/Installation Manager is installed. It contains the installation groups created by the user.

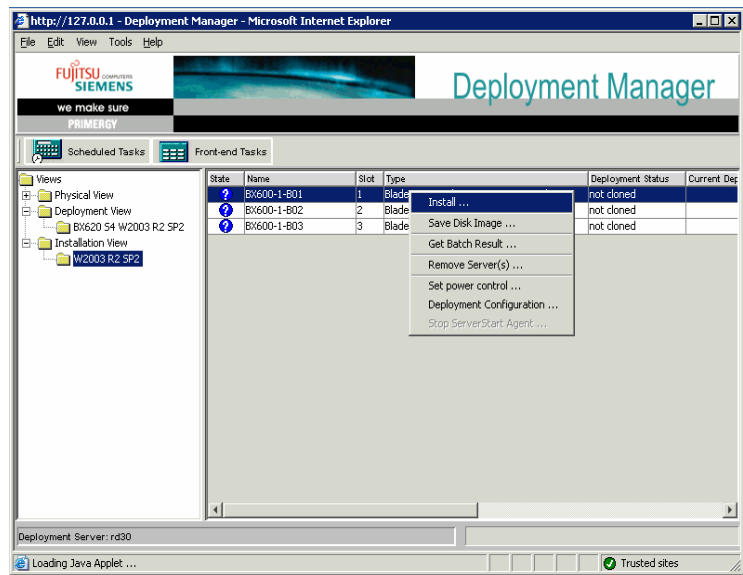


Figure 18: Installation View

The context menus in the *Installation View* allows you to perform the following functions:

Function	See
Create a new installation group ( <i>New Installation Group ...</i> )	<a href="#">section “Creating/Removing an Installation Group” on page 186</a>
Add server(s) to an installation group ( <i>Add Server(s) ...</i> )	<a href="#">section “Adding Servers to an Installation Group” on page 188</a>
Start the installation process ( <i>Install ...</i> )	<a href="#">section “Installing the Server” on page 194</a>
Remove installation groups ( <i>Remove Installation Group</i> )	<a href="#">“Removing an installation group” on page 188</a>



Function	See
Show the properties of an installation group ( <i>Properties ...</i> )	<a href="#">section “Viewing and Modifying the Properties of an Installation Group” on page 191</a>
Start the image creation process ( <i>Save Disk Image ...</i> )	<a href="#">section “Supported Operating Systems” on page 136</a>
Get the batch result for a list of selected servers ( <i>Get Batch Result ...</i> )	<a href="#">section “Get Batch Result” on page 178</a>
Remove servers from the list ( <i>Remove Server (s)</i> )	<a href="#">section “Adding Servers to an Installation Group” on page 188</a>
Configure the power status of the server ( <i>Set power control ...</i> )	<a href="#">section “Specifying the Power Control of Target Servers” on page 112</a>
Configure the server for deployment ( <i>Deployment Configuration ...</i> )	<a href="#">section “Target System Configuration” on page 113</a>
Stop a running ServerStart agent that might be active from a system information session ( <i>Stop ServerStart Agent ...</i> )	

## 4.6 Displaying Server Information

The following server information can be displayed in the *Physical View*, *Deployment View* or *Installation View*.

Column	Description
State	Server status. You will find a list of the icons and their meanings in the Operations Manager user guide.
Name	Name of the server
Slot	Slot number of the server blade (only displayed in the <i>Deployment View</i> and <i>Installation View</i> ). For non blade server "---" is displayed.
Type	The type of an entry: <i>Server</i> , <i>ServerBlade</i> , <i>BareServer</i> , <i>VMware Cluster</i>
Deployment Group	Corresponding deployment group (only displayed in the <i>Physical View</i> )
Deployment Status	Deployment status: <i>cloned</i> , <i>not cloned</i> , <i>cloning</i>
Current Deployment File	Currently deployed image or installation description file used for a server
ServerView IP	For non blade servers: Operations Manager IP address (only displayed in the <i>Physical View</i> )
IP Address 1	IP address of the first LAN port of the server
MAC Address 1	MAC address of the first LAN port of the server
Conf IP Addr 1	Configured IP address (only displayed in the <i>Physical View</i> )
IP Address 2	IP address of the other LAN port of the server
MAC Address 2	MAC address of the other LAN port of the server
Conf IP Addr 2	Configured IP address (only displayed in the <i>Physical View</i> )

For more information on the deployment table, see [section "Handling the Deployment Table" on page 274](#).

## 4.7 Adding Servers

You can add bare servers to the ServerView server list:

- Starting with RemoteDeploy version 3.0 you can add bare servers to the ServerView server list, see [section “Adding Bare Servers” on page 91](#).
- Starting with RemoteDeploy version 3.3 you can scan for new MAC addresses and then add the corresponding bare servers to the ServerView server list, see [section “Adding Bare Servers by MAC Address” on page 104](#). This function is only provided if ServerStart/Installation Manager is installed.

### 4.7.1 Adding Bare Servers

Starting with RemoteDeploy V3.0, you can add bare servers to the ServerView server list. At first these servers are displayed only in the *Physical View* of Deployment Manager. After a successful installation or cloning of such a server with Deployment Manager, these servers are also displayed in the ServerView server list.

You can add new bare servers in one of the following ways:

- Select *New Server ...* from the context menu in the *Physical View*.
- Select a server from the server list in the *Physical View* and select *New Server ...* from the context menu.
- Select the *New Server ...* entry from the *Edit* menu.

The *New Server* window looks different depending on whether ServerStart/Installation Manager is installed or not. The following figure shows the start window if ServerStart/Installation Manager is installed.

Figure 19: General settings - if ServerStart/Installation Manager is installed

### Name

Name of the new bare server. This name will be used as the host name of the new server when this server is installed or deployed with an image.

### DNS Suffix

Optional: Specify a DNS suffix.

### GUID (UUID)

Optional: GUID (globally unique identifier) of the server. There are different methods for finding out the GUID:

- Choose the *LIST* button in the *Network Adapters* window, see [figure 20 on page 94](#).
- Select the *System Info* button in the *Get System Information Options* window, see [figure 24 on page 102](#). This button displays the system information, including the GUID. The GUID is automatically inserted in this field.
- You can type in the GUID manually. During a PXE request the GUID is displayed locally on the server.

*SNMP Community*

Optional: Specify the SNMP community. The specified SNMP community is only used for the server entry in the ServerView database. Operations Manager will use this SNMP community for SNMP access to this server.

*PRIMERGY Type* (only if ServerStart/Installation Manager is installed)

Select the PRIMERGY server type from the drop-down list.

*Deployment Platform**Caldera DOS*

Caldera DOS deployment platform.

*WinPE MDP*

By default this button is selected. To use this option, Server-Start/Installation Manager as of version 6.711 must be installed on the deployment server and the *Do not use WinPE MDP* option must not be set in the *General Options* window.

*Administrator Account*

Account name for the administrator. This is the account name used to select an administrator user account for a cloned system. After this server has been cloned, the password for this user account is set to the specified password. During installation of this server, only the specified password is used to set the password of the administrative account, which is *Administrator* on Windows systems and *root* on Linux systems. If you are installing a server, the account name has no meaning. If the administrator account is left empty but a password is specified, the password of the account *Administrator* on a Windows operating system and *root* on a Linux operating system will be set to the specified password after an image is cloned.

*Administrator Password / Repeat Password*

When the bare server is installed, the password is used to set the administrator account. You must repeat the password.

Click *Next*. In the next window you must specify the network adapter settings.

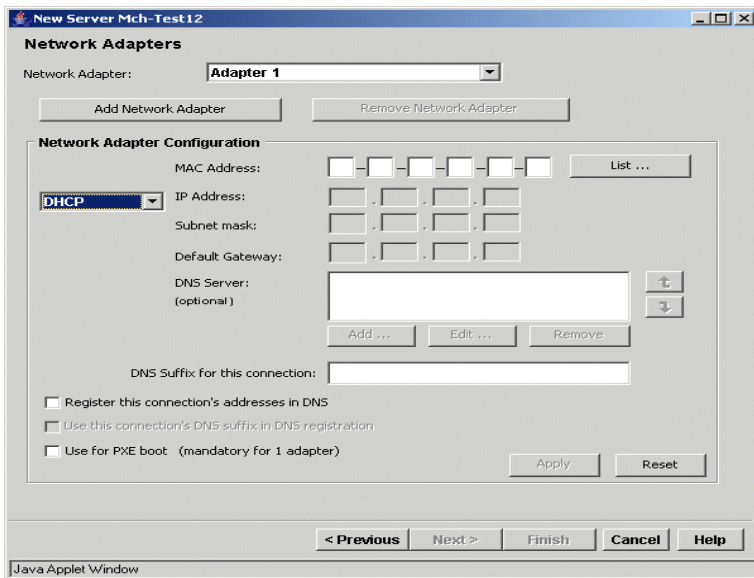


Figure 20: Network adapter settings

### Network Adapter

Select the network adapter from the list. You can use the *Add Network Adapter* and *Remove Network Adapter* buttons to add a network adapter or to remove the currently selected network adapter.

### Network Adapter Configuration

#### MAC Address

MAC address of the selected network adapter.

You can only select the *List* button if ServerStart/Installation Manager is installed. A new window is displayed. Click the *Help* button for detailed information.

#### DHCP or Non DHCP

Select *DHCP* for the assignment of a dynamic IP address. Select *Non DHCP* to enter a fixed IP address, subnet mask and default gateway.

*DNS Server*

You can assign a list of DNS servers to each LAN port. After an installation process or cloning process the IP addresses are assigned to the corresponding LAN ports. You can use the *Add/Edit/Remove* button to add, edit or remove a DNS server from the list.

*DNS Suffix for this connection*

Specify a DNS suffix for the selected network adapter. The configuration of the value is only supported when cloning a Windows disk image. In addition, the image must be created with RemoteDeploy as of version 4.0.

*Register this connection's addresses in DNS*

Allows you to register the IP address automatically in DNS. The configuration of the value is only supported when cloning a Windows disk image. In addition, the image must be created with RemoteDeploy as of version 4.0.

*Use this connection's DNS suffix in DNS registration*

Enables a DNS dynamic update to register the IP addresses and the connection-specific domain name of this connection. The configuration of the value is only supported when cloning a Windows disk image. In addition, the image must be created with RemoteDeploy as of version 4.0.

*Use for PXE boot*

If *Use for PXE boot* is activated, this indicates that the selected network adapter should be used for PXE boot (for cloning and installation). There must be one network adapter that is used for PXE boot.

*Apply*

Click *Apply* to confirm the settings (MAC address, IP settings, ...) for the selected network adapter.

*Reset*

Click *Reset* to reset the settings.

Click *Next*.

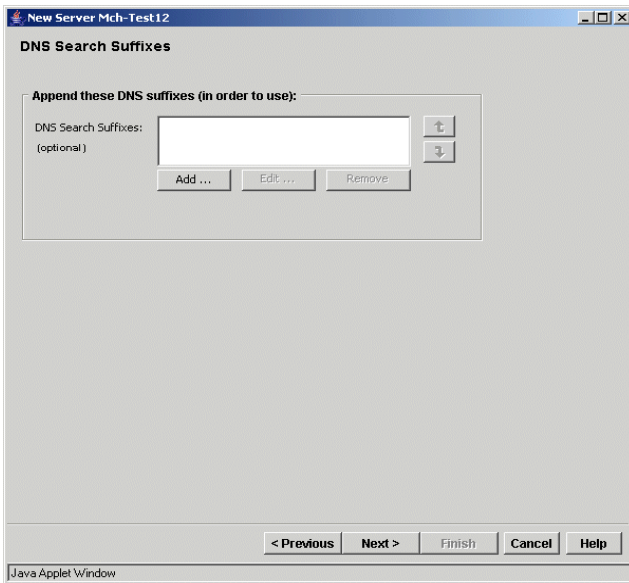


Figure 21: DNS Suffix managing

### *DNS Search Suffixes*

Specify a list of DNS suffixes which are used to extend a server name to a fully qualified server name when trying to resolve the IP address of a specified server name. Use the buttons *Add*, *Edit* and *Remove* to add, edit and remove suffixes. Use the arrow buttons to select the order.

Click *Next*. If you deploy an ESX 3.0 image to this server, further parameters can be specified.



**New Server Mch-Test12**

**Deployment Configuration for ESX Server Cloning**

☒ Assign virtual MAC addresses automatically

Virtual Switch: vSwitch0 Add Remove

Assigned Physical LAN Ports  
LAN Port 1

Virtual Switch Configuration

Portgroup: Service Console Add Remove

IP Configuration for Service Console

VLAN ID: (optional)

Virtual MAC Address:  -  -  -  -  -  Generate ...

DHCP IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 255

Default Gateway: 0 . 0 . 0 . 0

Apply Reset

< Previous Next > Finish Cancel Help

Java Applet Window

Figure 22: ESX Configuration

For the cloning of an ESX 3.0 image you can define optional parameters. If you do not specify an ESX deployment configuration, a default configuration is used – one virtual switch *vSwitch0* at physical port *vmnic0* with one *VM Network* and one service console; the IP configuration for the service console is defined based on the deployment configuration of the first LAN port.



#### Restrictions:

When creating an image from an ESX server, any partition with a VMFS file system will be recognized as an “unknown” file system and is saved block by block in a file-system-independent mode. This will produce a large image file and the backup and restore process will need a lot of time.

If an image from an ESX server with a VMFS partition is created and virtual machines are defined, there will be no personalization of virtual machines when cloning this image.

Therefore you are advised to install ESX 3.0 without a VMFS partition and to create a partition with a VMFS file system as part of the cloning process or to use the option *Skip existing partition with VMFS file system* during image creation. If this option is checked for the image creation job, the contents of an existing VMFS partition will not be stored in the image; the partition will be skipped during the image backup. When cloning such an image, a corresponding partition will be created and formatted with a VMFS file system, but its contents will be empty. Therefore no virtual machines should be defined on the system from which the image is to be created.

#### *Assign virtual MAC addresses automatically*

If the option is selected, a virtual MAC address is assigned to all ports automatically when the cloned system is first booted. Otherwise a virtual MAC address must be assigned to each port of the type *ServiceConsole* or *VM Network*.

#### *Virtual Switch*

Select a defined virtual switch. With the *Add* button you can add a new virtual switch to this configuration. With the *Remove* button you can remove the selected virtual switch from this configuration.

#### *Assigned Physical LAN Ports*

Displays the physical LAN port that is assigned to the virtual switch.

#### *Virtual Switch Configuration*

##### *Portgroup*

Displays the assigned port groups for the selected virtual switch. With the *Add* or *Remove* buttons you can add or remove a new port from the selected virtual switch.

##### *IP Configuration for <port>*

Displays the configuration for the selected port (*VM Network*, *Service Console* or *VMKernel*):

##### *VLAN ID:*

Specify a VLAN ID.

##### *Virtual MAC Address (only for Service Console and VMKernel)*

Virtual MAC address of the selected port.

Use the *Generate* button to generate a virtual MAC address.

This is only enabled if the *Assign virtual MAC addresses automatically* button is not checked. By default this button is checked and it is recommended that you use this default setting.

*DHCP / Non DHCP (only for Service Console)*

Select *DHCP* for the assignment of a dynamic IP address. Select *Non DHCP* to enter a fixed IP address, subnet mask and default gateway.

*Apply*

Click *Apply* to confirm the settings. If you do not click *Apply* and you select another port group, the defined settings from the previous port group will be lost.

*Reset*

Click *Reset* to reset the settings.

Click the *Next* button. In the next window you can select the method for remote access.

The screenshot shows a Java Applet window titled "New Server test2". Inside, the "BMC Account Settings" section is active. Under "Remote Access", the "BMC Support" radio button is selected, while "Wake on Lan" is unselected. Below these are input fields for "IP Address" (a dotted box), "User Name", "Password", and "Repeat Password". There are also spinners for "Timeout" (set to 3) and "Retries" (set to 1), both with "Seconds" and a help icon. A "Test connectivity" button is at the bottom of the form area. At the very bottom of the window are navigation buttons: "< Previous", "Next >", "Finish", "Cancel", and "Help".

Figure 23: Remote access settings

### *BMC Support*

Select *BMC Support* to specify the Baseboard Management Controller (BMC) settings. The following parameters are displayed:

#### *IP Address*

Specify the IP address that was assigned to the Baseboard Management Controller (or RSB). This is needed for remote power-on and remote configuration of the boot sequence for PXE boot.

#### *User Name / Password / Repeat Password*

Preconfigured user accounts/passwords:

- For server systems with BMC firmware v2.x  
user account *oem* with password *oem* or  
user account *admin* with password *admin*.

- BMC firmware v1.x does not support a user concept. To access those BMCs, use the RomPilot password.

It is recommended that you change this password as soon as possible.

*Timeout*

Timeout value for the access to BMC via Intelligent Platform Management Interface (IPMI).

*Retries*

Number of retries.

*Test connectivity*

Click the button to test whether the BMC can be accessed by the specified parameters.

*Wake on Lan*

*Wake on Lan* is selected by default if the selected server type does not support IPMI over LAN.

*Broadcast Address*

Broadcast address where the magic packet should be sent to. Additionally you can specify that the packet should be sent to UDP port 67 (otherwise it will be sent to UDP port 9) and specify the IP address of the server.

If the parameter is empty, the target must be in the same LAN segment.

Click *Finish* to add the new bare server. The new server is displayed in the *Physical View*.

Depending on the ServerStart/Installation Manager installation, you can specify further options for the system information session. Click *Next*. In the next window you can specify options for the system information session.

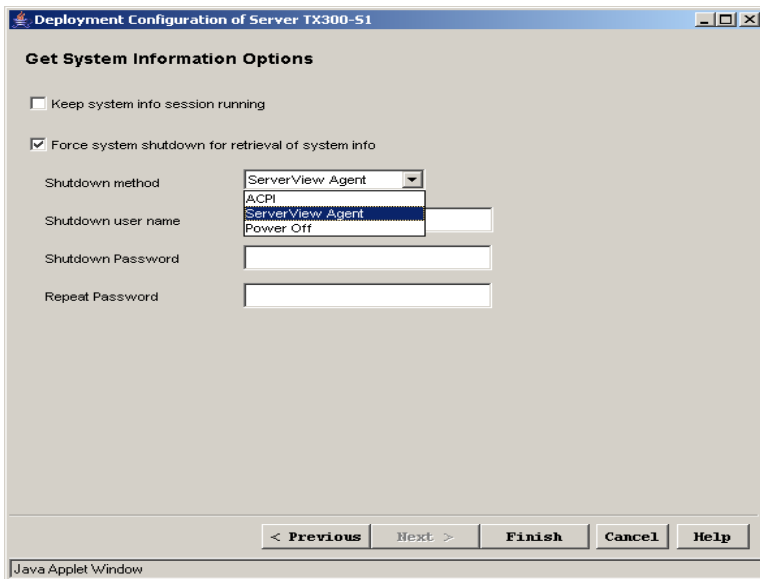


Figure 24: System information

*Keep system info session running*

If this option is checked, the system info session (WinPE on the target server) is not automatically stopped when the system information is retrieved.

If you want to start an installation process for this server after retrieving the system information, or you want to clone this server, selecting *Keep system info session running* improves the performance of corresponding deployment action.

You can stop a running ServerStart agent that might be active from a system info session. Select *Stop ServerStart Agent ...* from the context menu of a selected server.

*Force system shutdown for retrieval of system information*

Select this option to force a system shutdown before retrieving the system information.

*Shutdown method*

Select the shutdown method.

If the server is already installed and ServerView agents are running, you should use the *ServerView Agent* shutdown method.

*Shutdown user name / Shutdown Password / Repeat Password*

Preconfigured user accounts/passwords. You must repeat the password.

System information can be displayed using the *Next >* button. The *System Info* window is displayed. The first time you start the window, no values are displayed. Click the *Get System Info* button to start the retrieval of current information.

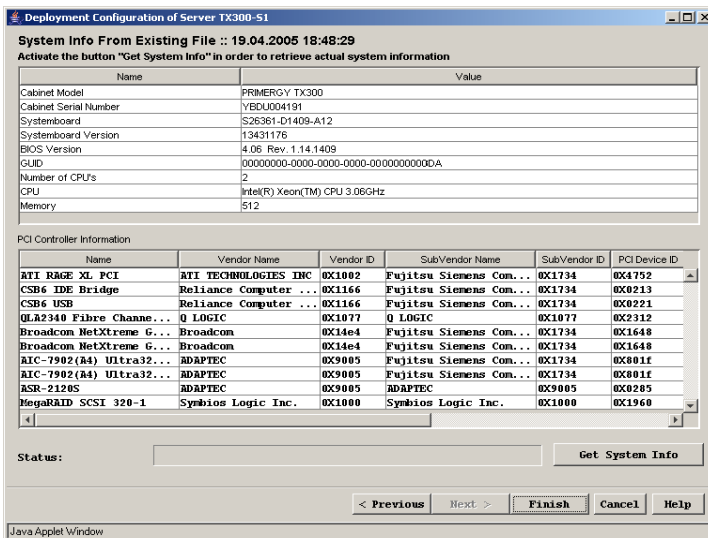


Figure 25: Baseboard Management Controller settings

The hardware configuration (system information) is also stored in the file `<Deployment Manager installation path>\RemoteDeploy\SystemInfo\<MAC_address>.xml`. A separate file is created for each server. A newly created file overwrites an existing one.

Click *Finish* to add the new bare server. The new server is displayed in the *Physical View*.

## 4.7.2 Adding Bare Servers by MAC Address

With RemoteDeploy V3.3, you can add bare servers on the basis of scanned MAC addresses to the ServerView server list. This function is only available if ServerStart/Installation Manager is installed.

The scanning for new MAC addresses is based on PXE requests made by servers which are not installed. This means that, in order to find a new server, this server must be powered on and the server must issue a PXE request which is recognized by the PXE service on the deployment server.

At first these servers are displayed only in the *Physical View* of Deployment Manager. After a server installation, they are also displayed in the ServerView server list.

You can add new bare servers in one of the following ways:

- Select *Add new Servers by MAC address ...* from the context menu in the *Physical View*.
- Select a server in the server list from the *Physical View* and select *Add new Servers by MAC address ...* from the context menu
- Select the *Add new Servers by MAC address ...* entry from the *Edit* menu.

The *Add Servers by MAC Address* window opens. In the first step you define a start and stop time/date for the scanning of PXE requests. After the scanning has stopped, the entries found are displayed in the window.



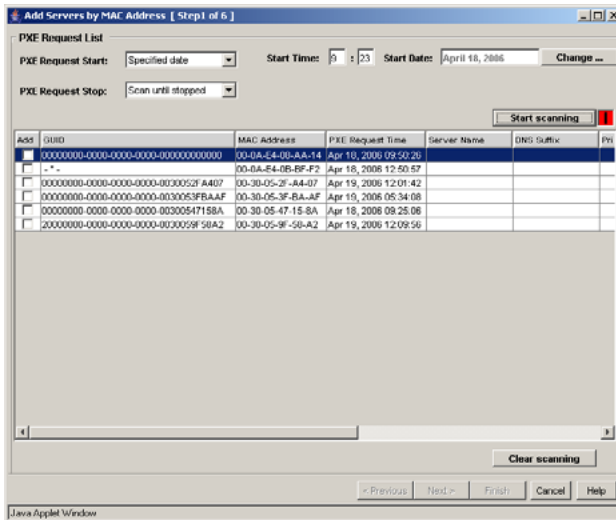


Figure 26: Scan result

Select the entries which are to be used to add a new bare server entry to the server list. In the next steps you can specify different parameters for the entry. For a detailed description refer to the online help by clicking the *Help* button.

# 4.8 Task Management

Deployment Manager distinguishes between two task types:

- Scheduled tasks

Scheduled tasks are defined in the *Save Disk Image* wizard, *Deploy Image* wizard or *Remote Installation* wizard. To open the *Scheduled Tasks* window, click the *Scheduled Tasks* button in the task bar of the main window.

- Front-end tasks

The *Interactively Started Tasks* window displays all executed tasks (non-scheduled tasks). To open this window, click the *Front-end Tasks* button in the task bar of the main window.

The following window shows the example of a *Scheduled Tasks* window.

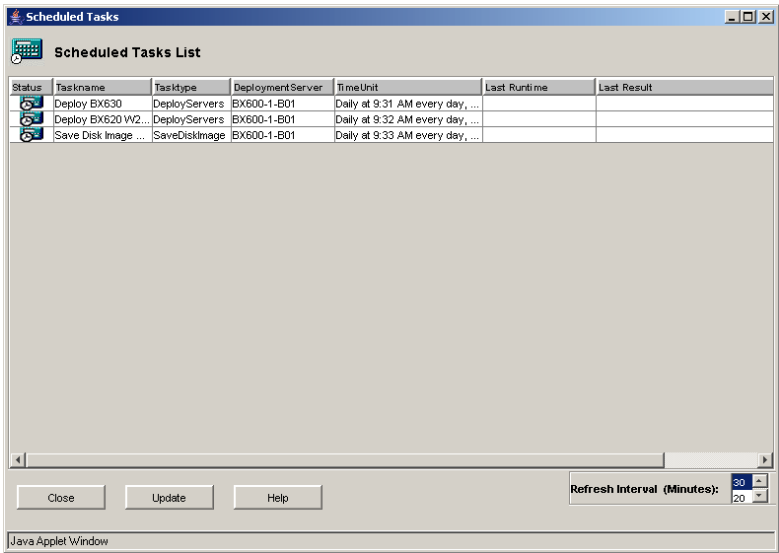










Figure 27: Example - Scheduled Tasks window

The task window contains the following information:

#### *Status*

The icon shows the current status:

	The task is registered as a scheduled task, but one which is not running.
	The task is started and currently running.
	The task was successfully executed and completed. It will not be scheduled again.
	The task was successfully executed and completed. It is scheduled for further execution (regularly repeated task).
	The task was executed unsuccessfully due to an error. No further retries or repetition of the task are scheduled.
	The task was executed unsuccessfully due to an error, but further retries of the task are scheduled.
	The task was executed unsuccessfully due to an error. No further retries are scheduled but the task is scheduled for further repetitions, as it is a regularly repeated task.
	The status of the task is unknown.

#### *Taskname*

Name of the task as defined in the *Save Disk Image wizard*, *Deploy Image wizard* or *Remote Installation wizard*.

#### *Tasktype*

Type of the task: *DeployServers* (created in the *Deploy Image wizard*), *SaveDiskImage* (created in the *Save Disk Image wizard*) or *InstallServers* (created in the *Remote Installation wizard*).

#### *DeploymentServer*

Name of the deployment server as specified in the *Save Disk Image wizard*, *Deploy Image wizard* or *Remote Installation wizard*.

#### *TimeUnit* (only in the *Scheduled Tasks* window)

Time as defined in the *Save Disk Image wizard*, *Deploy Image wizard* or *Remote Installation wizard*.

*Last Runtime*

Time and date of the last run of this task.

*Last Result*

Information on the last log entry of this task.

*Retry Counter* (only in the *Scheduled Tasks* window)

Retry counter as defined in the *Save Disk Image* wizard, *Deploy Image* wizard or *Remote Installation* wizard. This value defines how many retries should be performed if the task execution fails.

*RetryInterval* (only in the *Scheduled Tasks* window)

Time interval as defined in the *Save Disk Image* wizard, *Deploy Image* wizard or *Remote Installation* wizard. This value defines how many minutes should be waited between two attempts at a task.

*Task start time-window* (only in the *Scheduled Tasks* window)

Time as defined in the *Save Disk Image* wizard, *Deploy Image* wizard or *Remote Installation* wizard. This value defines the maximum period (in minutes) for retries of a task. Outside this period no retries will be performed, even if all retries as specified by the retry counter have not been used.

You can immediately update the display by clicking the *Update* button. You can also set a refresh interval using the *Refresh Interval* button.

## 4.8.1 Operations in the Task Window

The tasks window allows you to

- start and stop a task,
- delete a task,
- rename a task,
- display the event log,
- delete all log entries,
- display the batch result, and
- view and edit the settings (for scheduled tasks only).

### Start/stop a task

To start or stop a task, select the relevant task and choose *Start* or *Stop* from the context menu.

### Delete a task

To delete a task from the list, select the relevant task(s) and choose *Delete* from the context menu.

### Rename a task

To rename a task, select the relevant task in the *Taskname* column and choose *Rename* from the context menu.

### Display the event log

To display the event log of a task, select the relevant task and choose *Show Task EventLog* from the context menu. This opens the *Event Log* window, see [section “Displaying the Event Log” on page 110](#).

### Delete all log entries

To delete all log entries of one or more tasks, select the relevant task(s) and choose *Delete All EventLog Entries* from the context menu.

### Display the batch result

You can display the progress of a task. Select the relevant task and choose *Show Batch Results* from the context menu. This opens the *Batch Result* window, see [section “Get Batch Result” on page 178](#).

### View and edit task settings

You can modify the parameters of an existing scheduled task. Select the relevant scheduled task and choose *Properties* from the context menu. This opens the *Save Disk Image* window (see [figure “Save Disk Image wizard” on page 141](#)), the *Deploy Image* window (see [figure “Select Server\(s\) for Deploy Job window” on page 167](#)) or the *Remote Installation* window (see [figure “Remote Installation window” on page 194](#)). Now you can modify the parameters of this scheduled task. The next time this task runs, it will be started with the modified parameters.

### 4.8.2 Displaying the Event Log

You can display a list of log entries. In the relevant task window, select the task and choose *Show Task EventLog* from the context menu. This opens the *Event Log* window.

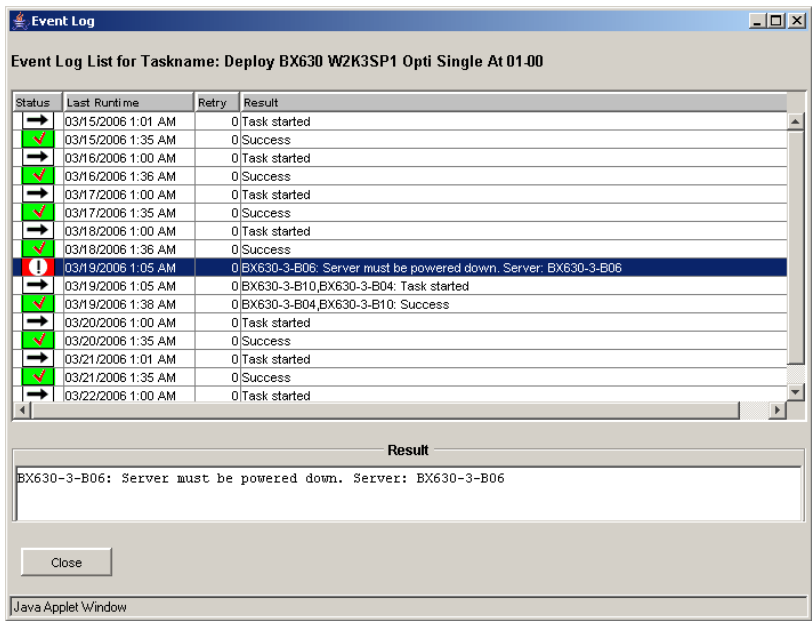






Figure 28: Example: Scheduled Task - Event Log window

The following information is displayed in the window:

*Status*

Status information for this log entry.

	Log entry for the start event.
	Log entry for successful execution of a task.
	Log entry for failed execution of a task.
	Log entry for canceling a task.

*Last Runtime*

The date and time when this entry was written.

*Retry* (for a scheduled task only)

The retry counter for this task execution.

*Result*

Text information about the log entry.

The *Result* field displays text information about a selected log entry.

You can delete log entries from the list. Select the relevant log entries and choose *Delete* from the context menu.

## 4.9 Specifying the Power Control of Target Servers

You can control the power status of a server in the *Deployment Manager [Power Control]* window. You open the window by selecting the *Set power control ...* entry from the context menu

- of a server in the *Physical View*, or
- of a deployment group or of a server in the deployment group in the *Deployment View*, or
- of a server in the installation group in the *Installation View*.

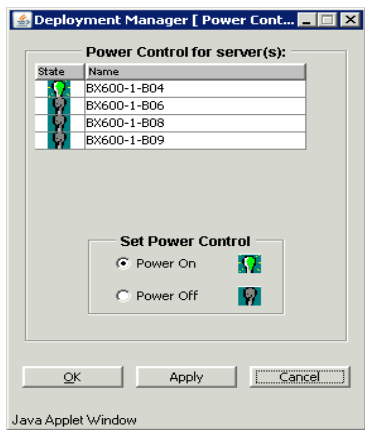





Figure 29: Deployment Manager [Power Control]

### State

This icon shows the power status of the server:

	Server is powered on.
	Server is powered off.
	Failed to retrieve power status of server.

### Name

Name of the server(s).



*Set Power Control*

Define the power status for the selected servers.

Click *Apply* or *OK* to activate the changes. Click *Cancel* to close the window without performing an action.

## 4.10 Target System Configuration

You must configure the target system before deploying the image to servers or before installing the servers. You open the *Deployment Configuration for <server>* window in one of the following ways:

- By selecting a blade server in the *Physical View* of Deployment Manager.
- By selecting a server from the displayed list in the *Physical View* of Deployment Manager.
- By selecting a deployment group in the *Deployment View*.
- By selecting one or more server(s) from the list displayed for a selected deployment group.
- By selecting one or more server(s) from the list displayed for a selected installation group.

Then select *Deployment Configuration ...* from the context menu. For a description of the windows, see also [section “Adding Bare Servers” on page 91](#).

The following example shows the deployment configuration of a server blade.

Use the *Help* button for a detailed description of the parameters.

Example: Deployment configuration of server blades

Deployment Configuration for Server: BX600-S3-1

ServerBlade(s):

Server Blade1

Slot Id:

1

Hostname:

BX62054-4-B02

Chassis Id:

PVT\_013

DNS Suffix:

GUID:

00020003-0004-0005-0006-000700080009

Administrator Account:

Administrator Password:

\*\*\*\*\*

Repeat Password:

\*\*\*\*\*

Network Configuration:

Network Configuration for

LAN Port 1

DHCP

IP Address:

0

0

0

0

MAC Address:

00-16-36-83-15-6C

SubNet Mask:

255

255

255

255

Default Gateway:

0

0

0

0

DNS Server:

(in order to use)

Add ...

Edit ...

Remove

DNS Search Suffixes:

(in order to use,  
not LAN port specific)

Add ...

Edit ...

Remove

DNS Suffix for this connection:

☒ Register this connection's addresses in DNS

☐ Use this connection's DNS suffix in DNS registration

ESX Deployment Configuration ...

LAN Port for PXE boot:

1

PRIMERGY Type:

PRIMERGY Type:

PRIMERGY BX620 54

Deployment Platform

☐ Caldera DOS

☒ WinPE MDP

Server states:

Blade state:

power-down

LAN state of slot:

empty

Ok

Apply

Reset

Cancel

Help

Java Applet Window

Figure 30: Example - Deployment configuration of a server blade

114

Deployment Manager

*ServerBlade(s)*

This list contains the server blades of the selected blade system or group.

*BladeServer Name*

This field shows the name of the selected blade server. The field is only displayed if you select a blade server.

*Slot Id*

This field shows the slot number of the server blade.

*Hostname*

Here you must specify a unique host name for all server blades in the group. The host name must not exceed 15 characters.

*Chassis Id*

Displays the chassis identification.

*DNS Suffix*

DNS suffix.

*GUID*

GUID of the server.

*Administrator Account/Administrator Password*

You can specify the administrator account and the administrator password. These are used to select an administrator user account for a cloned system. After this server is cloned, the password of this user account is set to the specified password. During installation of this server, only the specified password is used to set the password of the administrative account, which is *Administrator* on Windows systems and *root* on Linux systems. If you are installing a server, the account name has no meaning.

*Network Configuration**Network Configuration for*

Select the LAN port for the network configuration.

*DHCP / Non DHCP*

You must decide whether you want to use DHCP for a LAN port or to have static IP addresses for a LAN port which are manually assigned. If you want to use DHCP, select the corresponding option. In this case you do not have to specify an IP address, subnet mask or gateway. If you want to use manually assigned IP addresses you must select the *Non DHCP* option. In this case you must specify a unique IP address and a valid subnet mask.

*IP Address*

IP settings for each server blade.

*MAC Address*

Displays the MAC address for the selected server blade.

*SubNet Mask*

Subnet mask for the selected LAN port of this server blade.

*Default Gateway*

Default gateway for the selected LAN port of this server blade.

*DNS Server*

Displays the IP addresses of DNS servers used for the selected LAN port. You can add, edit or remove DNS servers.

*DNS Search Suffixes*

Specify a list of DNS suffixes which are used to extend a server name to a fully qualified server name when trying to resolve the IP address of a specified server name. Use the buttons *Add*, *Edit* and *Remove* to add, edit and remove suffixes. Use the arrow buttons to select the order.

*DNS Suffix for this connection*

Optional: You can specify a list of DNS suffixes, which are used to extend a server name to a fully qualified server name when trying to resolve the IP address of a specified server name.

*Register this connection's addresses in DNS*

Allows you to register the IP address automatically in DNS. The configuration of the value is only supported when cloning a Windows disk image. In addition, the image must be created with RemoteDeploy as of version 4.0.

*Use this connection's DNS suffix in DNS registration*

Enables a DNS dynamic update to register the IP addresses and the connection-specific domain name of this connection. The configuration of the value is only supported when cloning a Windows disk image. In addition, the image must be created with RemoteDeploy as of version 4.0.

*ESX Deployment Configuration*

Opens a new window for the ESX 3.0 deployment configuration.

*LAN Port for PXE boot*

In addition you can specify here the LAN port for each blade, via which the blade is reachable for the deployment process. By default this is LAN port 1.

*PRIMERGY Type*

This field only appears if ServerStart/Installation Manager is installed on the deployment server. It shows the PRIMERGY server type. For some blade servers you must select a PRIMERGY type. This is necessary, for example, for the different types of BX630 server blades if you want to perform a remote installation.

*Deployment Platform*

Displays the deployment platform used.

*Server states**Blade state*

Displays the current status of the server blade.

*LAN state of slot*

Defines the IP-LAN definition.

*AutomaticRecovery*

Displays the automatic recovery state.

*Cloning state*

Displays the cloning status.

*ServerView Agent Update Mode*

Controls the update behavior of the deployment table in the management blade by ServerView agents (if installed). If the update mode is set to *disabled*, the deployment table is read-only for the ServerView agents. If the update mode is set to *enabled*, the agent can synchronize the IP settings and host name with the current settings of active operating system, typically every minute. This process will overwrite manual modifications in the deployment table made via Deployment Manager, and cloning is prohibited. This mode is typically used for roaming of a blade server to another chassis.

*MasterImageReference*

URL in UNC notation to an image file (with the extension *\*.img*, *\*.cfg* or *\*.txt*).

Use the *Apply* button to save the configuration for each server blade, and use the selection list in the top left of the window to select the next server blade.

## 4.11 Deployment Server

Deployment servers are responsible for preparing the servers and their environment from a central instance via the LAN. The created image files are stored in the image repository. The preparation of a deployment server is described in the “ServerStart/Installation Manager” guide.

### 4.11.1 Changing the Deployment Server

You can change the deployment server while Deployment Manager is running. Select the *Deployment Server ...* entry from the *File* menu. The *Select Deployment Server* window is displayed:

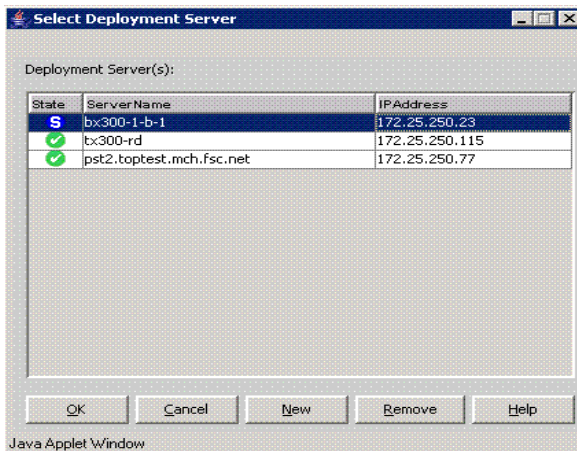


Figure 31: Select Deployment Server window

Select the deployment server from the *Deployment Server(s)* list and click *OK*. The *Login* window is then displayed. You must enter the user name and the password for the deployment server. These must be the same as those specified during the installation for the *Deployment Services* package. Deployment Manager waits until all currently running cloning jobs are finished before changing the deployment server.

### 4.11.2 Adding a New Deployment Server

You can add a new deployment server during startup of Deployment Manager (*New* button) or during runtime by selecting the *Deployment Server ...* entry from the *File* menu. Select the *New* entry in the *Select Deployment Server* window. The following window is displayed:

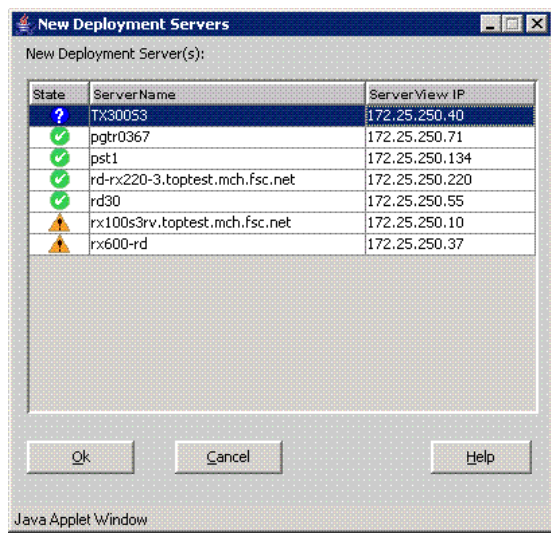



Figure 32: New Deployment Servers window

This window displays all servers in the ServerView server list (except blade systems) that are not already in the list of deployment servers. Select one or more servers in the list and click the *Ok* button. The selected server(s) are added to the list of deployment servers.

 You should only add servers which are installed as deployment servers.

### 4.11.3 Removing a Deployment Server

You can remove a deployment server from the *Select Deployment Server* window. Select the deployment server(s) and click the *Remove* button. The selected deployment server(s) are removed from the list.



## 4.12 Menus

This section describes the top menu level of the Deployment Manager window.

### File menu

The menu items in the *File* menu:

Deployment Group ...	Opens the <i>New Deployment Group</i> window to create a new deployment group.
Deployment Server ...	Opens the <i>Select Deployment Server</i> window.
Exit	Used to exit Deployment Manager.

Table 3: Menu items in the File menu

### Edit menu

The menu items in the *Edit* menu:

New Server ...	Opens the <i>New Server</i> window to add a bare server.
Add new Servers by MAC address ...	Only displayed if ServerStart/Installation Manager is installed. Opens the <i>Add Servers by MAC Address</i> window to add bare servers.
Delete Server(s)	Deletes server(s).
Add Server To Group ...	Add servers to a deployment group or installation group.
Remove Server(s) From Group ...	Removes servers from a deployment group or installation group.

Table 4: Menu items in the Edit menu

View menu

The menu items in the *View* menu:

Show ServerView Status Summary	Mark the checkbox to display the status overview.
LookAndFeel	Changes the Deployment Manager user interface.
Refresh ...	Used to refresh the display.

Table 5: Menu items in the View menu

Tools menu

License Management ...	Opens the <i>License Management</i> window.
Repository Management ...	Opens the <i>Repository Manager</i> window.
Export Deployment Configuration ...	Exports the deployment configuration of a list of selected servers to a file in XML format.
Import Deployment Configuration ...	Imports an exported deployment configuration from a file in XML format.
Options ...	Allows you to globally disable the use WinPE MDP as deployment platform.

Table 6: Menu items in the Tools menu

Help menu

Help Topics ...	Calls the Deployment Manager help.
About Deployment Manager	Displays the installed version of Deployment Manager.

Table 7: Menu items in the Help menu

4.13 Exiting Deployment Manager

Select *Exit* from the *File* menu. Deployment Manager waits until all currently running deployment jobs are finished. Deployment Manager is then terminated.

---

## 5 Tools

This section describes the different tools for Deployment Manager.

### 5.1 License Management

Deployment Manager requires at least one license. This license must be entered when Deployment Manager is installed. Without any license it is not possible to use the Deployment Manager functionality.

You can install several Deployment Manager licenses. Deployment Manager allows deploying as many servers as the sum of target licenses over all valid Deployment Manager licenses permits.

Therefore select *License Management ...* from the *Tools* menu. The *License Management* window is displayed:

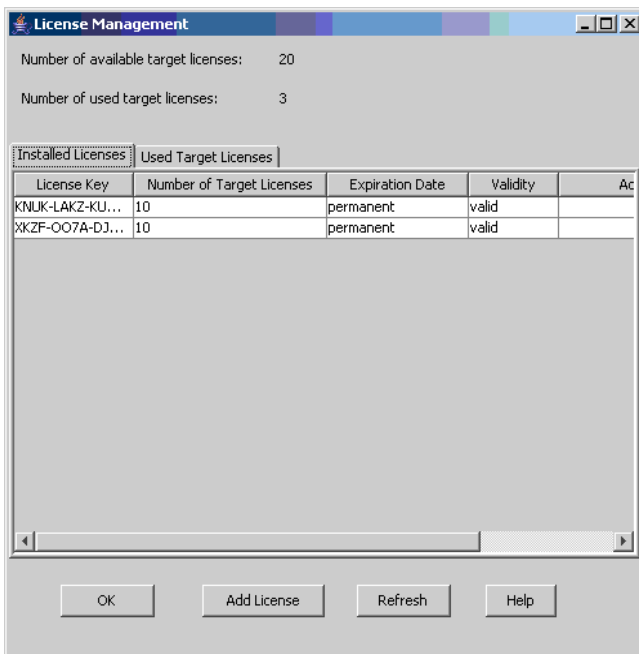


Figure 33: License Management window

*Number of available target licenses*

Displays the number of available licenses.

*Number of used target licenses*

Displays the number of occupied licenses.

The window displays the following tabs:

- *Installed Licenses* tab

The tab displays the list of installed license strings and their validity. It also displays the total number of target licenses (the number of target systems which can be deployed with this license).

- *Used Target Licenses* tab

The tab displays a list of servers (targets) that occupy a target license. Whenever a server is deployed or installed, this server occupies a license. A server always occupies only one target license; it can be deployed or installed as many times as desired.

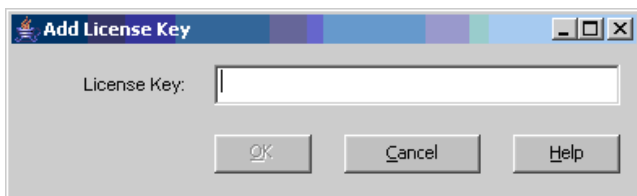
It is also possible to release an occupied target license by selecting a server in the list and selecting the *Release target license* entry from the context menu.

You can click the *Refresh* button to update the displayed information. Click the *OK* button to close the *License Management* window.

## Adding a new license

You can add new Deployment Manager license strings:

- ▶ Click the *Add License* button.
- ▶ The *Add License Key* window is displayed:



- ▶ Enter the new license string that you received from your service.
- ▶ Click *OK*.

The license string is added to the list of licenses.

## 5.2 Repository Management

All images are stored in image repository folders on the deployment server. You can add repositories, create new folders or delete a folder. Therefore select *Repository Management ...* from the *Tools* menu. The *Repository Manager* window is displayed:

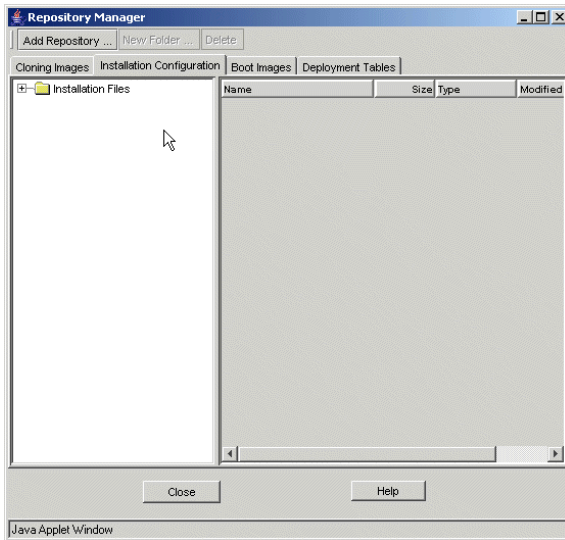


Figure 34: Add Repository window

If you click the *Help* button, further information is displayed.

The window displays the following tabs for the different image types:

- *Cloning Images* tab  
This tab displays all image files that are created via Deployment Manager. These images are used for the cloning process.
- *Installation Configuration* tab  
If ServerStart/Installation Manager is installed, this tab displays all configuration files that are created via ServerStart/Installation Manager. With the *Add Repository* button you must select the relevant repository.
- *Boot Images* tab  
This tab displays all boot images that are manually created. With the *Add Repository* button you must select the relevant repository.

– *Deployment Tables* tab

This tab displays the repositories for deployment configurations. These are used to export or import the deployment configurations of selected servers.

### Adding a new repository

You can add repositories which contain image files, configuration files or boot images:

- ▶ Select the corresponding image tab.
- ▶ Click the *Add Repository* button.

The *Add Repository* window is displayed:

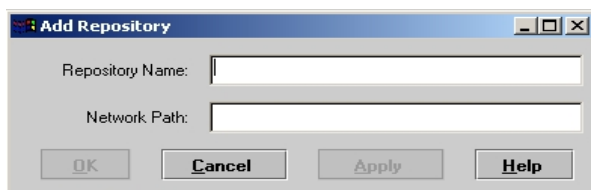


Figure 35: Add repository

*Repository Name*

Name of the repository.

*Network Path*

Complete network path, which contains the corresponding files.

Click *Apply* to confirm the settings. Click *OK* to close the window.

### Creating a new image folder

You can create a new image folder.

- ▶ Select the corresponding image tab.
- ▶ Select a repository or a subfolder of a repository.
- ▶ Click the *New Folder* button.

The *Add Folder To <image type>* window is displayed:

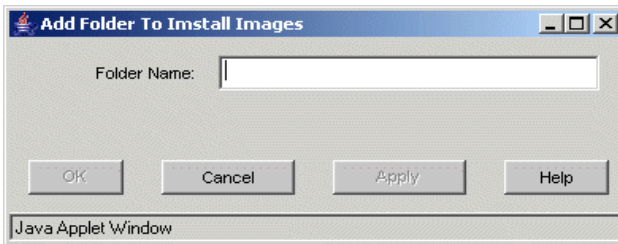


Figure 36: Example: Create new folder

Type in a name for the new folder. Click *Apply* to confirm the settings. Click *OK* to close the dialog.

### Deleting a repository

To delete a repository, select the image folder and click *Delete*.

## 5.3 Deployment Configuration

### 5.3.1 Exporting the Deployment Configuration

From selected servers in the server list you can export the deployment configuration to a file in XML format. This deployment configuration can then be imported. This enables you to change between different deployment configurations for servers whenever it is necessary.

You can start the export of a deployment configuration in one of the following ways:

- Select *Export Deployment Configuration ...* from the context menu in the Physical View.
- Select a server in the server list in the *Physical View*. Select *Export Deployment Configuration ...* from the context menu.
- Select *Export Deployment Configuration ...* from the *Tools* menu.

The *Export Deployment Configuration* window opens:

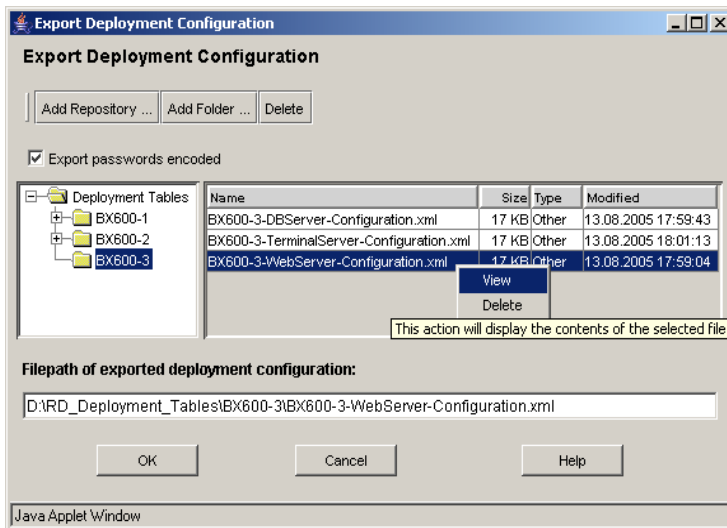


Figure 37: Export Deployment Configuration

The first time you start the export, you must add a repository in which the exported deployment configuration will be stored as an XML file.





The exported deployment configuration contains several passwords. By default these passwords are exported in encoded form. If you want to edit these passwords, uncheck the *Export passwords encoded* option.

Specify the file name and click *OK* to export the deployment configuration. To view the information on an exported configuration, select the relevant file and select *View* from the context menu. You can delete an exported file by selecting *Delete* from the context menu. For a detailed description click the *Help* button.

## 5.3.2 Importing the Deployment Configuration

You can import the deployment configuration from a file that was created by a previous export run.

You can start the import of a deployment configuration file in one of the following ways:

- Select *Import Deployment Configuration ...* from the context menu in the *Physical View*.
- Select a server in the server list in the *Physical View* and select *Import Deployment Configuration ...* from the context menu.
- Select *Import Deployment Configuration ...* from the *Tools* menu.

The *Import Deployment Configuration* window opens:

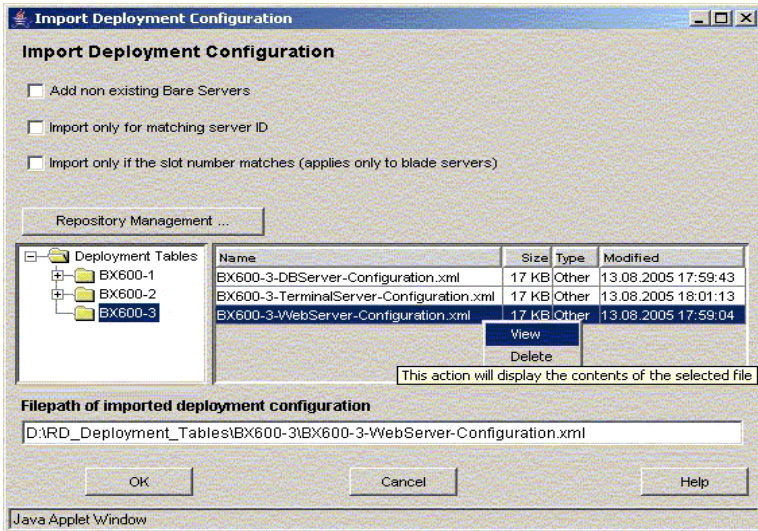


Figure 38: Import Deployment Configuration

#### *Add non existing Bare Servers*

The deployment configuration of bare servers which do not exist in the server list will be imported.

#### *Import only for matching server ID*

The deployment configuration of servers whose server ID stored in the file also matches the server ID found in the server list will be imported.

#### *Import only if the slot number matches (applies only to blade servers)*

The deployment configuration of server blades whose slot number stored in the file also matches the slot number found in the server list will be imported.

#### *Repository Management*

Opens the *Repository Manager* window, see [section “Repository Management” on page 125](#).

For a detailed description click the *Help* button.

## 5.4 Global Options

In the *Options* window you can specify global settings for Deployment Manager. You can

- specify that WinPE MDP should not be used as the deployment platform, or

To do this, select the *Options ...* entry from the *Tools* menu. This opens the *Options* window:

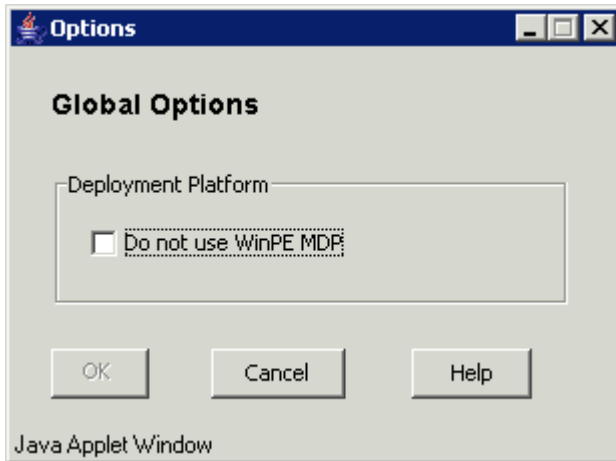


Figure 39: Options window

### *Deployment Platform*

Select the *Do not use WinPE MDP* checkbox to disable the use of WinPE MDP as the deployment platform.



You can only use WinPE MDP as the deployment platform if ServerStart/Installation Manager version 6.711 or higher is installed and the *Do not use WinPE MDP* option is not set in this window.



---

## 6 Image Creation

Once a reference system is completely installed and finally configured for the end user, the image creation process can be started via Deployment Manager.

Deployment Manager supports

- snapshot image creation. A “snapshot image” of a server can be used to restore the server after a system crash. A snapshot image can be created for selected servers at the same time.
- file-system-dependent image creation and
- file-system-independent image creation (raw image creation).



Only when creating a non-snapshot image from a Windows system:

If an error occurs during image creation, you should boot the Windows operating system normally. At the beginning of this boot there might be a “rollback” of changes already made. Do not interrupt this rollback. After the rollback has finished please check whether the files *CLCOMP.DAT* and *WIN.TAG* are present on the reference system. These files will exist if, for example, the creation of a non-snapshot image from a Windows system was aborted. Delete the files manually.

Before you start the image creation process make sure that all connected network drives are disconnected.

The created image is stored in an image repository. This is located in a shared folder on any file server in the network.

An image consists of the following files:

- *<image\_file\_name>.img*  
The file contains the image.
- *<image\_file\_name>.cfg*  
The file contains information about the image.
- *<image\_file\_name>.txt*  
The file contains user-defined text.

## 6.1 File-System-Dependent Image Creation

The following file systems are supported:

- FAT, FAT32 (Windows)
- NTFS, NTFS5 (Windows), NTF5
- EXT2, EXT3, Reiser file system (V3.5, 3.6) (Linux)
- Reiser file system with RemoteDeploy version 4.0



If the file-system-dependent image creation has been selected for a hard disk drive with unsupported file systems, the image is still created correctly.

If a customer has an implementation of several partitions with different file systems, the deployment engine will check for each partition whether the file system is supported (and add partition to image in FS-dependent mode) or not (and add partition to image in raw mode) and will save all partition information in one image file. This is the case if you specify that “used cluster algorithm” should be used. Otherwise, the file system type will not be checked and all data will be moved to the image file in raw mode (1:1).

Partitions with unsupported file systems will be read out according to the file-system-independent image creation process.

File-system-dependent image creation does determine the used clusters of each file in the file table of a file system, but only stores this file table and the used clusters in the image. With this method, the disk geometry is not limited because the used blocks are stored file-system-(partition)-oriented, not disk-sector-oriented.

The image is compressed and encoded (for security reasons) and written to a location defined by a UNC network path (UNC = Universal Naming Convention).

When using this kind of image, the cloning process first creates partitions with the appropriate size. Based on the information stored in the image header, these partitions are then formatted. Finally, the image is decoded and decompressed on the fly and the extracted clusters are written directly to the correct location in the file system. With this method, only the user data of a file system must be copied to a target drive.

If you have created an image of a 20 GB partition with 3 GB user data, only 3 GB user data must be written on the hard drive. The rest of the 20 GB is defined by the formatting process (if verification is selected, this will take extra time).

## 6.2 File-System-Independent Image Creation (Raw Image Creation)

The file-system-independent image is a 1:1 copy of a hard drive but is encoded and compressed in the same way as for the file-system-dependent method. The final image also has a similar size because of effective compression of the non-used areas. The hardcopy is read by sector containing information which depends on the drive geometry. This method requires that the hard drive of the target system is identical to the hard drive of the reference system.

The big difference is the extraction of this image, which takes about three times as long but is independent of the file system and thus the operating system. On the target side, each byte of the raw copy of the image must be written to the target drive which takes the majority of the cloning process.

If you have created an image of a 20 GB partition and 3 GB user data, you must write 20 GB to the hard drive again. On the other hand, you save the time required for formatting the drive (slow, especially with verification, but more flexible).

For partitions which are converted as dynamic disks, the image creation can be done only in raw mode.



Before you start the raw image creation you must clean the drive. This can be done via ServerStart/Installation Manager in Expert Mode. Start the *DiskManager* tool and select *CleanOut drive*.

## 6.3 Supported Operating Systems

Deployment Manager supports the image creation for:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows Server 2003 (x86 and x64)
- Microsoft Windows Server 2008 (x86 and x64)



Before starting an image creation process you have to configure the Windows firewall on the reference system, see [section “Configuring the Windows Firewall on the Reference System” on page 138](#).

- Linux RedHat Advanced Server 3.0
  - Linux RedHat Advanced Server 4.0 (x86 and EM64T)
  - Linux RedHat Advanced Server 5.0 (x86 and EM64T)
  - Linux SuSE Enterprise Server SLES 8
  - Linux SuSE United Linux (with SLES 8)
  - Linux SuSE Enterprise Server SLES 9 (x86 and EM64T)
  - Linux SuSE Enterprise Server SLES 10 (x86 and EM64T)
  - Reiser file system versions 3.5 and 3.6 on SuSE SLES 9 and SuSE SLES 10
- Before image creation, a specific package must be installed on the reference system if Reiser is used as the root file system. This package can be found on the Deployment Manager CD in the directory *LINUX\_support/ReiserFS\_Cloning\_Support*.
- with restriction: ESX 2.5 based on customer script, requirements for the configuration of the reference system need to be defined. Customer scripts for ESX 2.5 cloning are located on the Deployment Manager CD.
  - ESX Server 3.0
- For the cloning of an ESX Server 3.0 image, a specific ESX deployment configuration can be specified. For more information on support for ESX 3.0, see also the ReadMe file on the Deployment Manager CD.



**Restrictions:**

- Image creation is only supported for Linux reference systems that have the Fstab option *Mount in /etc/fstab* by set to *Device name* for all partitions. During a native installation of SuSE SLES 10 SP1, this option is set to *Device ID* by default. You must manually change this option for all partitions. If you install SuSE SLES 10 SP1 unattended with ServerStart/Installation Manager V6.711 or higher, *Device name* is set by default for all partitions.
- Any partition with a VMFS file system will be recognized as an "unknown" file system and is saved block by block in a file-system-independent mode. This will produce a large image file and the backup and restore process will need a lot of time. If an image from an ESX server with a VMFS partition is created and virtual machines are defined, there will be no personalization of virtual machines when cloning this image.

Therefore you are advised to install ESX 3.0 without a VMFS partition and to create a partition with a VMFS file system as part of the cloning process or to use the *Skip existing partition with VMFS file system* option during image creation. If this option is checked for the image creation job, the contents of an existing VMFS partition will not be stored in the image; the partition will be skipped during the image backup. When cloning such an image a corresponding partition will be created and formatted with a VMFS file system, but its contents will be empty.

Therefore no virtual machines should be defined on the system from which the image is to be created.



All other operating system types can always be supported without personalization in raw snapshot mode. See also the ReadMe file on the Deployment Manager CD.

## 6.4 Windows 2008 Reference System

### 6.4.1 Configuring the Windows Firewall on the Reference System

Before starting an image creation process, you must configure Windows Firewall with Advanced Security on the reference system.

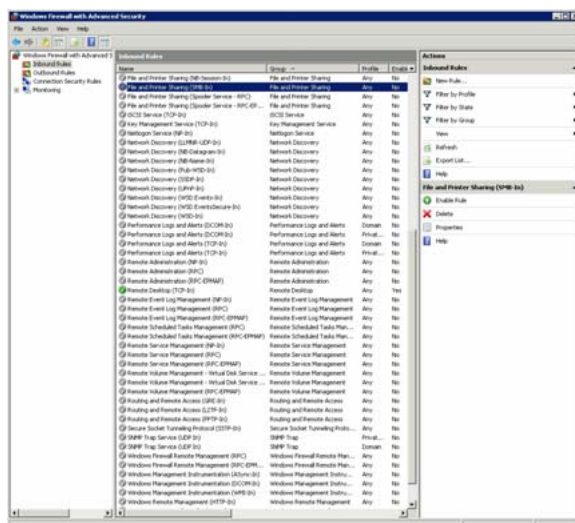
During system preparation, Deployment Manager tries to access the reference system with WMI and copies the *Client Agent* package (for temporary installation) to the reference system. If the reference system has Windows Firewall switched on (which is the default after a Windows 2008 installation), perform the following steps on the reference system before starting the image creation process:

- ▶ Select *Start – Administrative Tools – Windows Firewall with Advanced Security*.
- ▶ Select *Inbound Rules* in the left pane.
- ▶ Enable the following *Inbound Rules* (set to *Yes*):

## File and Printer Sharing (SMB-In)

## Windows Management Instrumentation (DCOM-In)

## Windows Management Instrumentation (WMI-In)



In a German installation the rules are called:

Datei- und Druckerfreigabe (SMB eingehend)  
Windows-Verwaltungsinstrumentation (DCOM eingehend)  
Windows-Verwaltungsinstrumentation (WMI eingehend)

## 6.4.2 Sysprep Restrictions

Note the following restrictions for Sysprep:

- Sysprep can only be called 3 times on Windows 2008.

Make sure that Sysprep has been called no more than twice on the reference system. Otherwise Sysprep will crash during the deployment process.

- Not all server roles support Sysprep.

The following server roles will no longer function after deployment:

- Active Directory Certificate Server (AD CS)
- Active Directory Domain Services (AD DS)
- Active Directory Federation Services (AD FS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Server (AD RMS)
- DNS Server
- Fax Server
- File Services
- Network Policy and Access Services
- Print Services
- UDDI Services
- Windows Deployment Services

The following server roles will continue to function with restrictions:

- Terminal Services  
Not supported in scenarios where the master Windows image is joined to a domain.
- Web Server (Internet Information Services)  
Does not support Sysprep with encrypted credentials in *applicationhost.config*.

## 6.5 Starting the Image Creation Process

You start the image creation process in the *Physical View* of Deployment Manager. How to start Deployment Manager is described in the [section “Starting Deployment Manager” on page 78](#).

Once you have selected the desired reference system, you can start the image creation process.



You can select different servers to create a snapshot image at the same time.

- In the *Physical View*, select the server and choose the entry *Save Disk Image ...* from the context menu of this server.
- In the *Deployment View*, select the server from the deployment group and choose the entry *Save Disk Image ...* from the context menu of this server.
- In the *Installation View*, select the server from the installation group and choose the entry *Save Disk Image ...* from the context menu of this server.

The *Save Disk Image for <server>* wizard or the *Save Disk Image for selected servers* wizard is started.

You can

- create a scheduled task for the image creation,
- define the properties for a new image,
- describe the basic and most important parameters of the configuration in text form,
- specify the image creation process,
- start the image creation process.



The desired reference system must have the power status off or you should select the option *Force shutdown of server before generating disk image* in the *Save Options* window.

## Scheduler Options

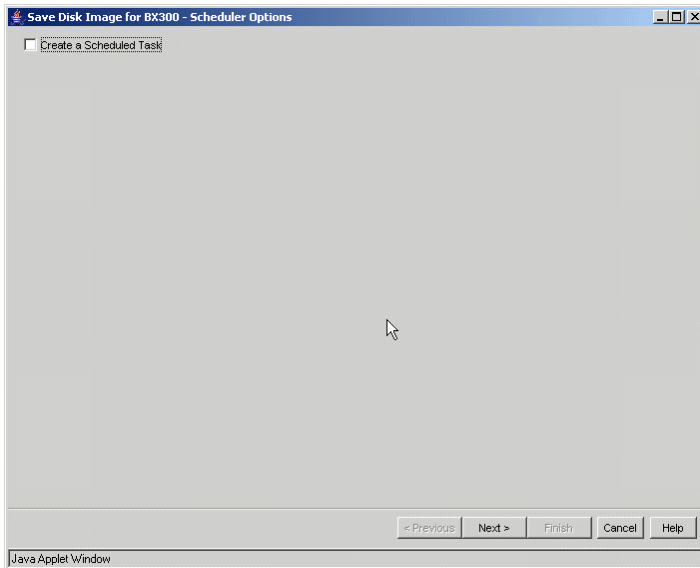


Figure 40: Save Disk Image wizard

In the first step you decide whether you want to create the image generation task as a scheduled task or not.

If you want to create a scheduled task, mark the check box; further parameters will appear.

If you do not want to create a scheduled task, click the *Next* button. The *Image Information* window is displayed; see [“Select Image Path” on page 145](#).

Figure 41: Scheduler Options window



A scheduled job will fail if the user name and password for the deployment server are changed between task definition and task execution.

The text field on the left side shows information on the scheduler settings that are available for *Create a Scheduled Task*. The text field on the right side shows information on the *Define Schedule Task Settings*.

### *Create a Scheduled Task*

#### *Taskname*

Task name for the new task. You can enter any string except the characters &, ".

#### *Deployment Server*

Name of the deployment server which is used for this task. By default this is the deployment server which you select at the start of Deployment Manager. You can select any server from the list of deployment servers. If you select another deployment server, you must specify the user name and password for a connection to it.

*Time Unit to perform this Task*

You can select the following values:

- *Once*  
The task will be performed once only. You can only specify the *Start date* for this job.
- *Daily*  
The task will be performed daily.
- *Weekly*  
The task will be performed weekly.
- *Monthly*  
The task will be performed monthly.

*Retry Counter*

Specify the number of retries for this task if the job fails.

*Retry Interval (Minutes)*

The time (in minutes) before the next attempt if previous attempts at a task failed and the number of retries does not exceed the retry counter. A value between 1 and 360 minutes can be specified for the retry interval.

*Task start time-window (Minutes)*

A time value between 10 and 600 minutes. If the task could not be started successfully within the time range beginning with the start time of the task and ending *xx* minutes later (*xx* is the specified value for *Task start time-window*), the task will be canceled. Also retries of the task will be made only during this time range.

Therefore the task will not be started after the task start time window has elapsed. It can happen that a task is handed over to the deployment server, but is only queued because too many other tasks are already running. If the *Task start time-window* elapses while a task stays in this state, the task will also be canceled. A running task will not be canceled when the *Task start time-window* elapses.

*Define Scheduled Task Settings**Set time you want this task to start*

Start time of the scheduled task. You can specify an hour between 0 and 11 and a minute between 0 and 59. You can also select whether the job will be started before noon (*AM*) or in the afternoon (*PM*).

*Select date you want this task to start* (only visible if you select *Once* or *Daily* as the time unit)

You can select the start date of the scheduled task from the calendar. Click the *Change start date* button to change the start date.

*Perform this task* (only visible if you select *Daily* as the time unit)

You can also select whether the task should be performed *Every Day*, *Weekdays* or *Every x days*.

Select the day(s) of the week you want this task to start (only visible if you select *Weekly* as the time unit)

You can specify that the task should be executed every week or every  $n$  week ( $n = 1 \dots 52$ ). You can also select the days of the week.

Select the day of the month you want this task to start (only visible if you select *Monthly* as the time unit)

You can specify for which months of the year the task should be executed. You can also specify on which day of the month a task should be executed. And you can specify a weekday and whether the task should be executed in the first, second, third, fourth or last week of a month.

Click the *Next* button; the *Select Image Path* window is displayed.



## Select Image Path

In the next step you select the repository and the position in this repository, and define the name of the image file.

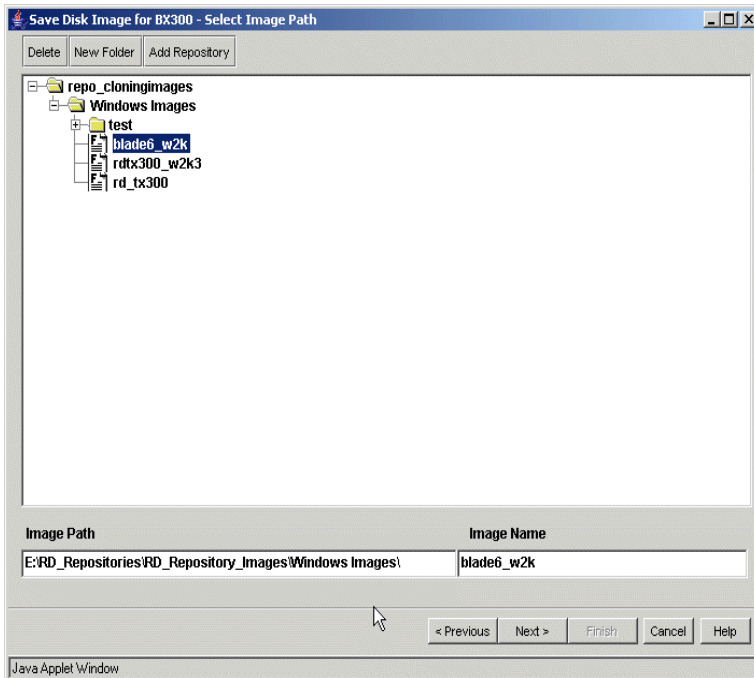


Figure 42: Select Image Path window

### Delete

Deletes an image, a folder or a repository.

### New Folder

Creates a new folder. If you click *New Folder*, a window is displayed in which you enter the folder name.

### Add Repository

Adds an existing repository to the list of disk image repositories. If you click *Add Repository*, a window is displayed in which you enter the repository name and its network path.

### Image Path

Shows the path of the image repository.

### Image Name

Enter the name of the image file. If you selected multiple servers for a snapshot image creation, append *%S* to the image name. After the image creation, *%S* is replaced with the server name.

The value *%D* is replaced by the day, *%M* is replaced by the month and *%Y* is replaced by the year. This is useful when defining a scheduled task that is repeated regularly and if the generated image files are to have different names for each repetition.

Click the *Next* button; the *Image Information* window is displayed.

### Image Information

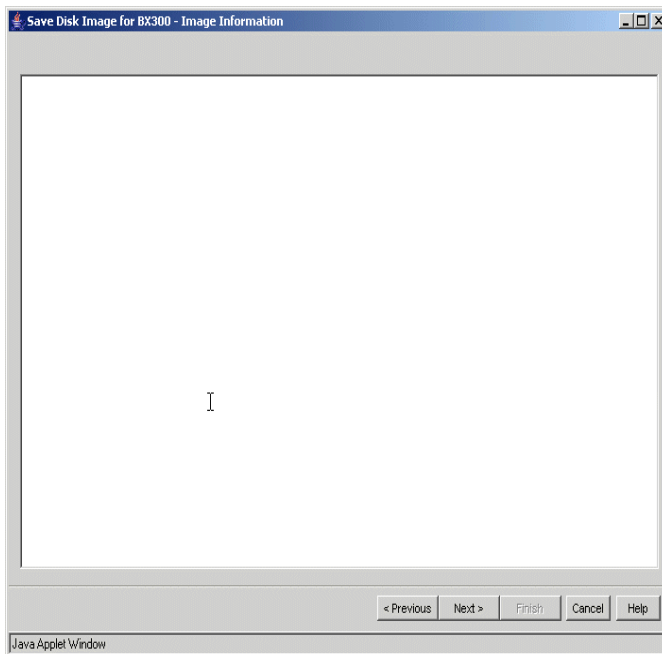


Figure 43: Image Information window

In this window you can enter any text that you want to be saved together with the image file. This can be information about the basic and most important parameters of the configuration (e.g. operating system type, release of service packs and installed applications, used drivers).

This information will be displayed under *Image Information* in the *Properties of Deployment Group: <image name>* window (see [section “Viewing and Modifying Deployment Group Properties” on page 158](#)).

Click the *Next* button; the *Save Options* window is displayed.

## Save Options

The screenshot shows a Java Applet window titled "Save Disk Image for BX600-1-B04 - Save Options". The window has a light gray background and a blue title bar. It contains the following elements:

- Logical disk number:** A dropdown menu set to "0". To its right is the text: "Selects the 'logical' disk from which the image will be created".
- Checkboxes:**
  - ☒ Verify file system
  - ☒ Compress image
  - ☐ Raw Mode
  - ☒ File-system-dependent ☐ Raise error for unsupported filesystem
  - ☐ Force system shutdown before generating disk image
- Final system status:** A dropdown menu set to "off".
- ☐ Snapshot image (useful for crash recovery of same system)
- Operating system:** A dropdown menu set to "Microsoft Windows 2008".
- Reference system:** An empty text field. To its right is the text: "(Optional, used for remote access to running reference system for preparation)".
- Administrator Name:** A text field containing "Administrator".
- Administrator Password:** An empty text field.
- Installation Medium:** A dropdown menu set to "FSC OEM".
- Language Version:** A dropdown menu set to "German (Germany)".
- ☒ Disable Firewall Rules WMI-in, DCOM-in and SMB-in after DeployImage/SaveDiskImage
- Language:** A dropdown menu set to "German".
- Buttons:** "< Previous", "Next >", "Finish", "Cancel", and "Help".
- Footer:** "Java Applet Window".

Figure 44: Save Options window

In this window you can select specific options for the image creation process.

### *Logical disk number*

Select the logical disc number from which the image should be created.

### *Verify file system*

The file system is checked before the image creation process is started.

### *Compress image*

The image file is compressed during the image creation.

*Raw Mode*

You can generate an image creation in disk raw mode. All blocks of the disks will be saved. This image can be deployed only to servers which have disks with the same size and the same disk layout. For more information, see the section “[File-System-Independent Image Creation \(Raw Image Creation\)](#)” on [page 134](#).

*File-system-dependent*

You can choose file-system-dependent image creation. Otherwise the image will be created file-system-independently. For more information, see the section “[File-System-Dependent Image Creation](#)” on [page 134](#).

*Raise error for unsupported file system*

Use this option only if the Raw Mode *option* is not checked and the *File-system-dependent* is checked. If an unsupported file system is detected, the image creation process will raise an error and stops.

*Force system shutdown before generating disk image*

You can specify that the server should be shut down before the image creation process is started.

You must install operating-system-specific ServerView agents on the relevant servers. How to install the agents and what settings you can make is explained in the Operations Manager installation manual.

*Shutdown user name*

User name as defined during the agent installation.

*Password*

Password as defined during the agent installation.

*Final system status*

You can specify whether the server should be shut down (*off*) or booted (*running*) after the image creation.

*Snapshot image (useful for crash recovery of same system)*

You can create a snapshot image file of a server. It can only be used for deployment on the same server, e.g. after a crash.



Only when creating a non-snapshot image from a Windows system:

If an error occurs during creation, check whether the files *CLCOMP.DAT* and *WIN.TAG* are present on the reference system. These files will exist if, for example, the creation of a non-snapshot image from a Windows system was aborted. Delete the files manually.

*Operating system (if Snapshot... is not selected)*

You specify the operating system installed on the reference system:

- *LINUX (Red Hat)*
- *LINUX (SuSE)*
- *ESX 3.0*
- *Microsoft Windows 2000/2003*
- *Microsoft Windows 2008*



If you select *Microsoft Windows 2000/2003* or *Microsoft Windows 2008*, you can specify a Windows domain for the image in the deployment process.

*Location of /etc (if LINUX (Red Hat), LINUX (SuSE) or ESX 3.0 is selected)*

You must enter the path of the physical location of the */etc* directory. By default this is */dev/sda2* for Red Hat and */dev/sda3* for SuSE.

*Fast image creation (if LINUX (Red Hat), LINUX (SuSE) or ESX 3.0 is selected)*

Fast image creation for EXT2/EXT3 file systems.

*Skip existing partition with VMFS file system (if ESX 3.0 is selected)*

If this option is selected for the image creation, the contents of an existing VMFS partition will not be stored in the image; the partition will be skipped. When cloning such an image, a corresponding partition will be created and formatted with a VMFS file system, but its contents will be empty. Therefore no virtual machines should be defined on the system from which the image is to be created.

*Reference system (if Microsoft Windows 2000/2003 or Microsoft Windows 2008 is selected)*

Displays either the IP address or the host name from the selected server. This value is used to access this system.

*Administrator Name (if Microsoft Windows 2000/2003 or Microsoft Windows 2008 is selected)*

You must enter the name of an account with administrator's rights. This must be a local account (no domain account) on the reference system. In some situations (e.g. when the reference system is a domain member) it is advisable to use the notation *<hostname>Administrator* instead of just *Administrator*, where *<hostname>* is replaced by the host name of the reference system.

*Administrator Password* (if *Microsoft Windows 2000/2003* or *Microsoft Windows 2008* is selected)

You must enter the administrator password of the specified administrator account on the reference system.

*Windows Product ID* (if *Microsoft Windows 2000/2003* is selected)

You must enter the product identification number of the operating system installed on the reference system.

*Installation Medium* (if *Microsoft Windows 2008* is selected)

Select the medium that was used for the installation of the reference system:

- *FSC OEM*  
FSC OEM (SLP-2) multi-language DVD.
- *Microsoft*  
All other DVDs.

*Language Version*

(if *Microsoft Windows 2008* and *Installation Medium FSC OEM* are selected)

Select the corresponding language version of the FSC OEM DVD. The Deployment Manager does not automatically recognize the installation language.

*Windows Product ID*

(if *Microsoft Windows 2008* and *Installation Medium FSC OEM* are selected)

Optional: Enter the product ID. For volume DVDs please leave the product ID empty. Do not enter a MAK (Multiple Activation Key) here. The MAK key can be entered during the image deployment.

*Disable Firewall Rules (...)* (if *Microsoft Windows 2008* is selected)

Before you start the image creation you must enable three firewall rules on the reference system, see [section “Configuring the Windows Firewall on the Reference System” on page 138](#).

Select this option to disable these firewall rules: The rules are disabled after the image deployment (the cloned system will have the three firewall rules enabled) and during rollback of the image creation (on the reference system).



Disabling firewall rules is only supported for English and German installations. You can add further languages. If you do this you must edit the *params.txt* file (section *DMFrontend\_BlockFirewall*) in the *RemoteDeployEngine* directory. After adding entries you must close and reopen the Deployment Manager front-end.

#### *Language*

If you select the *Disable Firewall Rules (...)* option, you must select the corresponding installation language.

You start the image creation process by clicking the *Finish* button.

Now the cloning module boots the reference system referenced by its MAC address with a DOS boot image via PXE and starts the image creation tool on DOS.



The automatic remote power on and the remote PXE boot configuration of the BIOS requires that the server is manageable by a management blade (blade system), an RSB or a BMC that support IPMI 1.5 over LAN. For non-blade systems you must have specified the correct BMC settings. If the server is not manageable in one of these ways, a dialog appears that asks you to initiate a PXE boot manually. Scheduled tasks for not manageable servers are not possible.

Once the image creation has been successfully started, a progress window is opened showing information on the image creation process.

Progress window

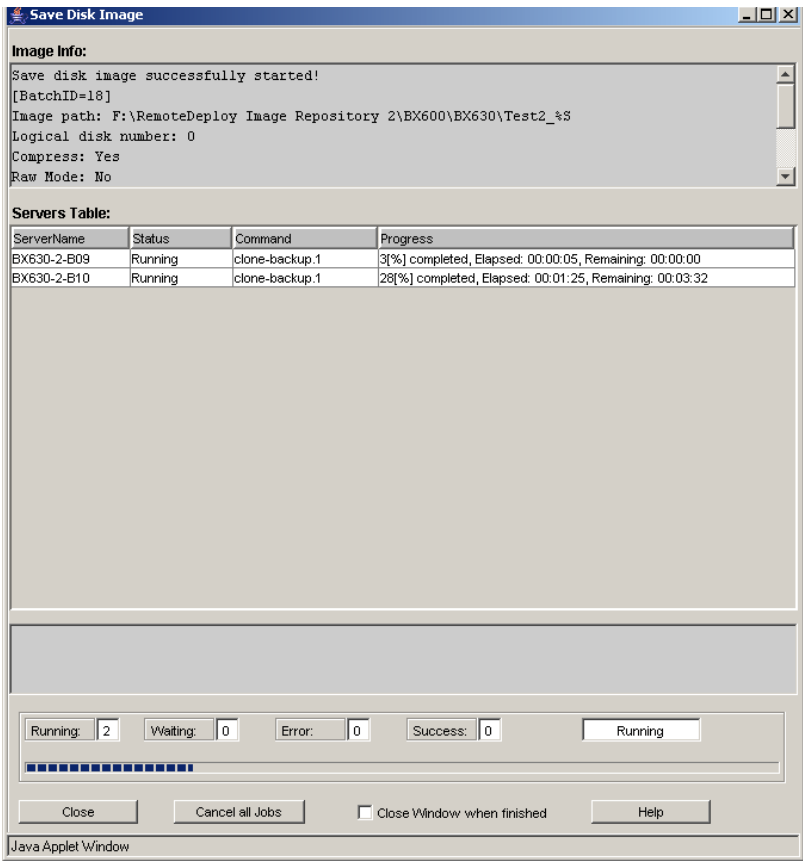


Figure 45: Example: progress window of a snapshot creation for multiple servers

The following information is given:

*ServerName*  
Name of the server.

*Status*  
Current state of the process displayed under *Phase Command* or *Command*.

*Phase Command / Command*  
Running process.



*Phase Progress / Progress*

Progress of the process in percent.

*Accepted Time*

Time when the current job was accepted by the cloning module.

*Start Time*

Time when the running process is started.

*Last Update*

Time of the last update of the *Status*, *Phase Command / Command* and *Phase Progress / Progress* information.

If you click the *Close* button, the progress window will close but the image creation process will continue running. If you click the *Cancel Job* button, the image creation process will be canceled. If you select the *Close Window when finished* option, the progress window will be closed once the image creation process is complete.



# 7 Cloning

The following sections describe how to build deployment groups before the cloning process can be started and how you configure the target systems for deployment.

## 7.1 Deployment Groups

Before you start the cloning process you need to consider which servers should get which image. Then you can build deployment groups consisting of one or more servers and one image file.

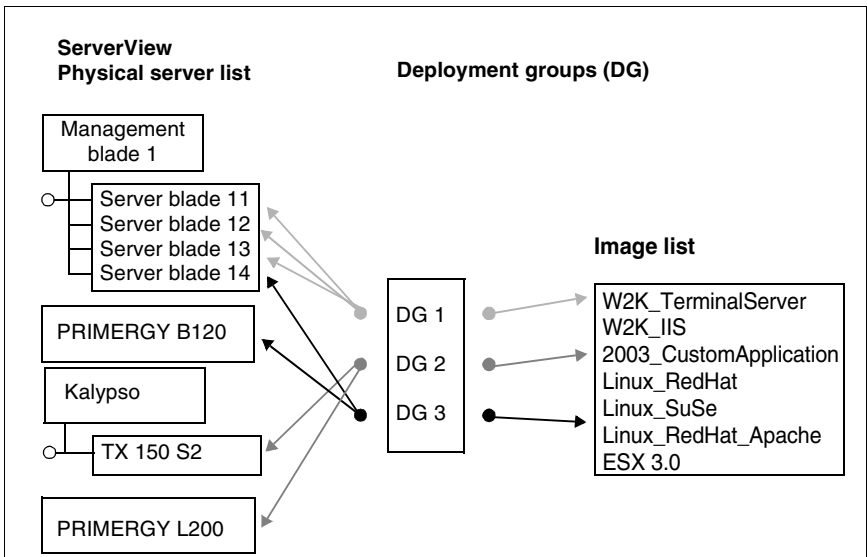


Figure 46: Deployment groups

Deployment groups with several servers help to reduce the workload of an administrator by organizing servers with the same configuration in one logical group. The servers getting the same image can then be cloned simultaneously by choosing only one deployment group.

## 7.1.1 Creating/Removing a Deployment Group

To create a new deployment group, select the *New Deployment Group ...* entry in the context menu in the *Deployment View* of Deployment Manager. The *New Deployment Group* window is displayed. You can select the new image file which is assigned to the new deployment group.

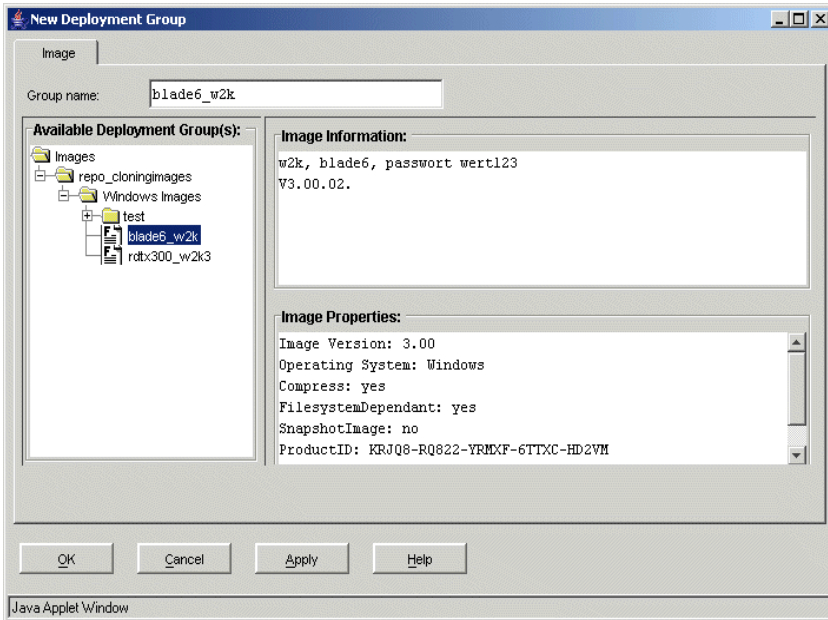


Figure 47: New Deployment Group window

On the left side you select the desired image, while on the right side you are shown information on the selected image.

The *Group name* field allows you to enter a separate name for the group. By default the field always displays the name of the selected image.

If you have not entered a separate group name, when you select an image the corresponding image name is always displayed as the group name in the text field. If you change your selection, the group name changes accordingly. If you have entered a separate non-empty group name, the group name does not change. Your input is valid. If you delete the contents of the text field, the default group name will be used again when an image is selected.

Select an image and click the *Apply* button. Select *OK* to close the window. In the *Deployment View* a new deployment group with the same name as the image file is displayed. You close the window by clicking the *Cancel* button.

Any server in the *Physical View* can be added to a deployment group, see [section “Adding/Removing Servers to/from a Deployment Group” on page 159](#).



An image file can only be assigned to one deployment group.

### Removing a deployment group

To remove a deployment group, select the desired group in the *Deployment View* and select the entry *Remove Deployment Group ...* from the context menu. The removal is only possible if no deployment job is running on any server in that group.

## 7.1.2 Viewing and Modifying Deployment Group Properties

You can view the properties of a deployment group. Select a deployment group in the *Deployment View* of Deployment Manager. In the context menu select the *Properties ...* entry.

The *Properties of Deployment Group: <group>* window is displayed:

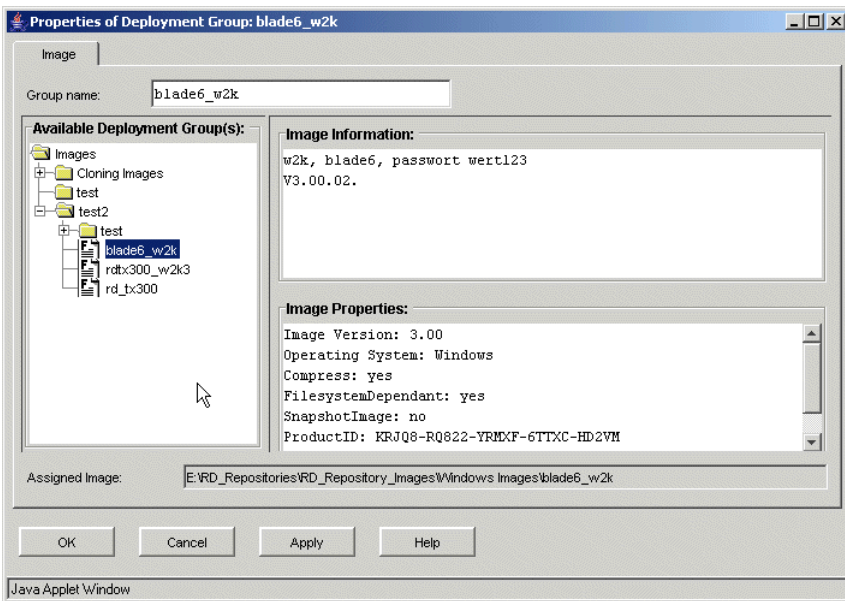


Figure 48: Properties of Deployment Group <group> window

The image information is displayed in the *Image Information* list.

In this window you can also change the image file for a selected deployment group. In the *Available Deployment Group(s)* list, select another image and click *Apply*. In the *DeploymentView* the deployment group gets the name of the new image. The assigned servers can later be cloned with this new image.

Before a different image is assigned, Deployment Manager checks whether a deployment group with the same name exists and whether a cloning process is running for any server in the deployment group. In such cases the image assignment is rejected.

### 7.1.3 Adding/Removing Servers to/from a Deployment Group

You can add servers to a deployment group in one of the following ways:

- Select the servers in the Physical View. You can add the servers to the deployment group with drag&drop. If the servers are not compatible with the image, a message box appears.
- Select a group in the Deployment View of Deployment Manager and select *Add Server(s)...* from the context menu. The *Add Server(s)* window is displayed:

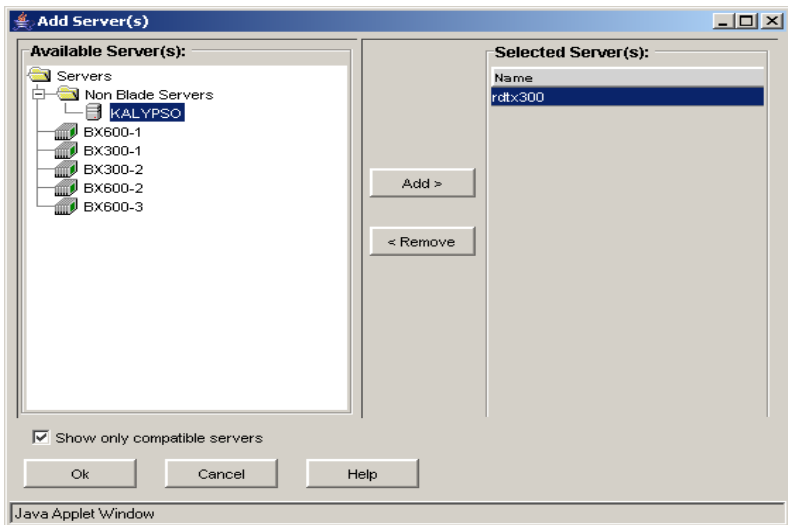


Figure 49: Add Server(s) window

The *Available Server(s)* list displays all servers which are compatible with the image (if *Show only compatible Servers* is marked) or all servers in the server list. Servers that are already in this deployment group are not listed. A server blade entry contains also the relevant slot number.

Select the server(s) and click the *Add* button. The *Selected Server(s)* list contains the servers which are to be added to the group. You can remove servers from this list by selecting the servers and clicking the *Remove* button.

Click the *OK* button to add the servers to the group.

## Removing servers from a deployment group

To remove a server from a deployment group, select the relevant deployment group in the *Deployment View*. The list on the right side of the main window displays the list of servers that belong to this group. Select the relevant servers in this list and choose *Remove servers* from the context menu.

## 7.2 System Preparation Method “All Primergy”

After starting the cloning process you can select different system preparation methods in the *Select System Preparation Method for Deploy Job* window (see [page 168](#)).

If you select the *All Primergy* system preparation method, this method is used by ServerStart/Installation Manager. There are two ServerStart/Installation Manager RAID Preparation modes:

- ServerStart/Installation Manager Classic RAID Preparation  
The ServerStart/Installation Manager Classic RAID Preparation is supported by RemoteDeploy V3.00 and higher. The RAID preparation is done exactly like during ServerStart/Installation Manager installation. The RAID preparation can be used for all RAID controllers. After the RAID preparation a reboot is always required. The ServerStart/Installation Manager installation on the local deployment server is always used (even when connected to a remote deployment server on a different LAN segment).
- ServerStart/Installation Manager MDP RAID Preparation  
The ServerStart/Installation Manager MDP RAID Preparation is supported by RemoteDeploy V4.10 and higher. It can only be used if the deployment platform is WinPE MDP and for RAID controllers supported by RAID Manager. After RAID preparation a reboot is required for the following controllers:

LSI 1030 SCSI Controller  
LSI 1020 SCSI Controller  
LSI 1020A SCSI Controller  
LSI Ultra320 SCSI Adapter

The remote ServerStart/Installation Manager installation is used when connected to a remote deployment server.

The following table shows legacy controllers which are not supported by RAID Manager:



Vendor	Family	Name
LSI/Mylex RAID Controller	Mylex U160 (Internal)	AcceleRAID 160 Controller
LSI/Mylex RAID Controller	Mylex U160 (Internal)	AcceleRAID 352 Controller
LSI/Mylex RAID Controller	Mylex U160 (Internal)	extremeRAID 2000 Controller
Adaptec RAID Controller	Mylex UltraWide (Internal)	(All controllers of this family)
Adaptec RAID Controller	Adaptec Legacy	2000S NightHawk I
Adaptec RAID Controller	Adaptec Legacy	2010S NightHawk II - 7901
Adaptec RAID Controller	Adaptec Legacy	2010S NightHawk II - 7902
Adaptec RAID Controller	Adaptec Legacy	2100S
Adaptec RAID Controller	Adaptec Legacy	3200S
Promise RAID Controller	Promise FastTrak	FASTTRAK 100LP ATA RAID Controller
Promise RAID Controller	Promise FastTrak	FASTTRAK 100LP ATA RAID Controller (Eco30)

Deployment Manager uses ServerStart/Installation Manager MDP RAID Preparation when the deployment platform is WinPE MDP and there is no legacy controller in the target system. If there is one of the above legacy controllers in a (non-blade) Primergy, you must specify the *Controller Vendor*, *Controller Family* and *Controller Name*. You must not leave the *Controller Family* or *Controller Name* set to *Any*, because otherwise Deployment Manager would not know to use ServerStart/Installation Manager Classic RAID Preparation. For blades, the *Controller Vendor*, *Controller Family* and *Controller Name* fields are already known to Deployment Manager and are therefore no longer user-selectable. The BX300 is the only blade with a legacy controller where ServerStart/Installation Manager Classic RAID Preparation is used automatically.

Detailed information on MDP is available in the MDP white paper on the Server-Books DVD.

## 7.3 Starting the Cloning Process

A cloning process can be executed for all servers that are in the same LAN segment as the currently selected deployment server. (The restriction to the same LAN segment as the deployment server is only valid if you use the Multicast deployment method.) The assigned image of a deployment group may be deployed to a list of selected servers in that group or to all servers in that group.



There is no automatic detection of whether servers are in the same LAN segment.

- Before you start the cloning process, specify the host names and IP addresses of all servers implied in the process. In the *Deployment Configuration for <server>* window, insert the host name and IP address of the desired servers. This provides the *Deployment Services* package with all required server parameters, see [section “Target System Configuration” on page 113](#).

The list of affected servers depends on the option of whether servers with the deployment status *cloned* should also be cloned. By default only servers which are not already cloned or installed are deployed (deployment status: *not cloned* or *not installed*).

- Select the *Deploy Image(s) ...* entry in the context menu of a deployment group, or for the list of selected servers in the list view when a deployment group is selected in the tree view of the main window.

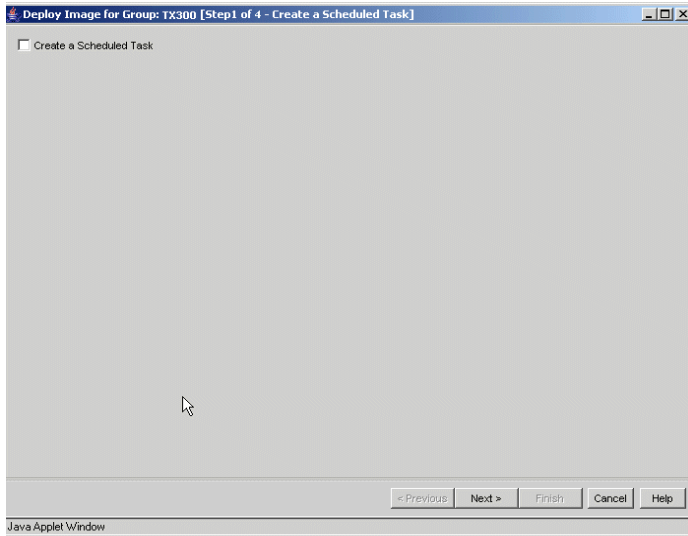


Figure 50: Create a Scheduled Task window (1)

In the first step you decide whether you want to start the cloning process as a scheduled task or not.

If you want to create a scheduled task, mark the check box; further parameters will appear.

If you do not want to create a scheduled task, click the *Next* button. The *Image Information* window is displayed; see [“Select Server\(s\) for Deploy Job” on page 167](#).

## Create a Scheduled Task

Figure 51: Create a Scheduled Task window (2)



A scheduled job will fail if the user name and password for the deployment server are changed between task definition and task execution.

The text field on the left side shows information on the scheduler settings that are available for *Create a Scheduled Task*. The text field on the right side shows information on the *Define Schedule Task Settings*.

### Create a Scheduled Task

#### Taskname

Task name for the new task. You can enter any string except the characters &, ".

#### Deployment Server

Name of the deployment server which is used for this task. By default this is the deployment server which you select at the start of Deployment Manager. You can select any server from the list of deployment servers. If you select another deployment server, you must specify the user name and password for a connection to it.

*Time Unit to perform this Task*

You can select the following values:

- *Once*  
The task will be performed once only. You can only specify the *Start date* for this job.
- *Daily*  
The task will be performed daily.
- *Weekly*  
The task will be performed weekly.
- *Monthly*  
The task will be performed monthly.

*Retry Counter*

Specify the number of retries for this task if the job fails.

*Retry Interval (Minutes)*

The time (in minutes) before the next attempt if previous trials at a task failed and the number of retries does not exceed the retry counter. A value between 1 and 360 minutes can be specified for the retry interval.

*Task start time-window (Minutes)*

A time value between 10 and 600 minutes. If the task could not be started successfully within the time range beginning with the start time of the task and ending *xx* minutes later (*xx* is the specified value for *Task start time-window*), the task will be canceled. Also retries of the task will be performed only during this time range.

Therefore the task will not be started after the task start time window has elapsed. It can happen that a task is handed over to the deployment server, but is only queued because too many other tasks are already running. If the *Task start time-window* elapses while a task stays in this state, the task will also be canceled. A running task will not be canceled when the *Task start time-window* elapses.

*Define Scheduled Task Settings**Set time you want this task to start*

Start time of the scheduled task. You can specify an hour between 0 and 11 and a minute between 0 and 59. You can also select whether the job will be started before noon (*AM*) or in the afternoon (*PM*).

*Select date you want this task to start* (only visible if you select *Once* or *Daily* as the time unit)

You can select the start date of the scheduled task from the calendar. Click on the *Change start date* button to change the start date.

*Perform this task* (only visible if you select *Daily* as the time unit)

You can also select whether the task should be performed *Every Day*, *Weekdays* or *Every x days*.

Select the day(s) of the week you want this task to start (only visible if you select *Weekly* as the time unit)

You can specify that the task should be executed every week or every  $n$  week ( $n = 1 \dots 52$ ). You can also select the days of the week.

Select day of the month you want this task to start (only visible if you select *Monthly* as the time unit)

You can specify for which months of the year the task should be executed. You can also specify on which day of the month a task should be executed. And you can specify a weekday and whether the task should be executed in the first, second, third, fourth or last week of a month.

Click the *Next* button; the *Select Server(s) for Deploy Job* window is displayed.

## Select Server(s) for Deploy Job

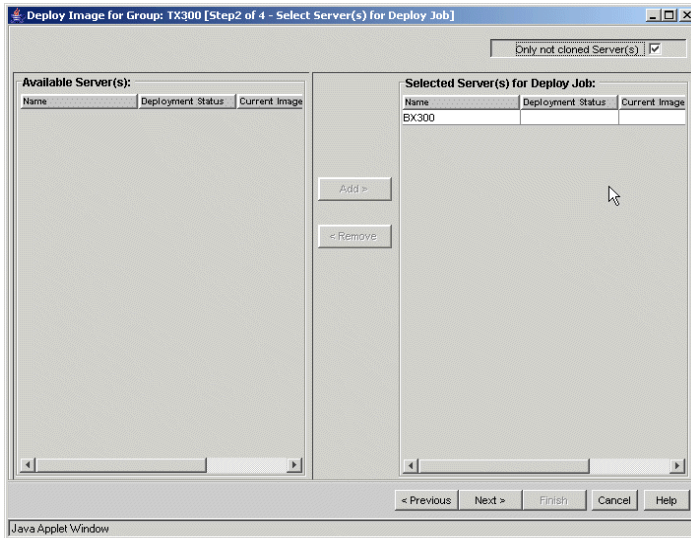


Figure 52: Select Server(s) for Deploy Job window

### *Only not cloned Server(s)*

If this check box is marked, only servers which are not cloned and not installed are displayed in the list *Selected Server(s) for Deploy Job*.

### *Available Server(s)*

Displays the servers which are already cloned or installed.

### *Selected Server(s) for Deploy Job*

Displays the servers which are not cloned and not installed.

Click *Add* to add servers to the list on the right-hand side. You can also remove servers from this list by clicking the *Remove* button.

Click the *Next* button; the *Select System Preparation Method for Deploy Job* window is displayed.

## System Preparation Method for Deploy Job

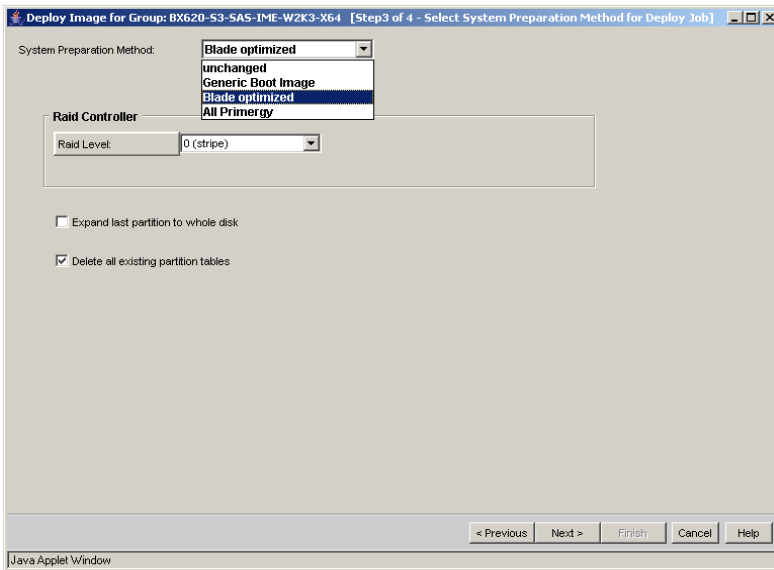


Figure 53: System Preparation Method

In this dialog you select the system preparation method for the deploy job. Depending on the selected method, different parameters will be displayed in this dialog.

- *unchanged*, see [page 169](#).
- *Generic Boot Image*, see [page 170](#).
- *Blade optimized* - only displayed for blade servers and when the deployment platform is *Caldera DOS*, see [page 171](#).
- *All Primergy* - only displayed if ServerStart/Installation Manager is installed, see [page 172](#).

For more information refer to [section “Cloning” on page 29](#).



## System Preparation Method for Deploy Job (Unchanged)

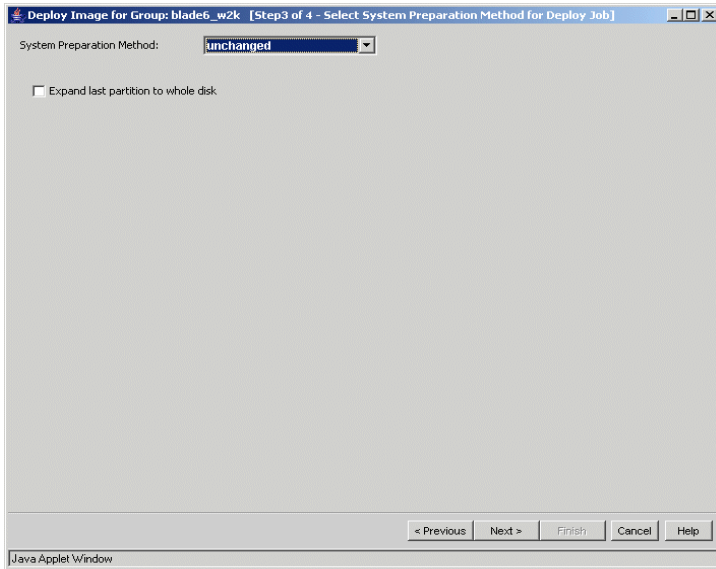


Figure 54: System Preparation Method - unchanged

If you select the system preparation method *unchanged*, the following parameter is displayed:

*Expand last partition to whole disk*

Expands the last partition of the image to use the rest of disk.

The system preparation (RAID configuration) must be done manually before starting a deployment job.

Click the *Next* button. The *Set Arguments for Deploy Job* window is displayed (see [page 174](#)).

## System Preparation Method for Deploy Job (Generic Boot Image)

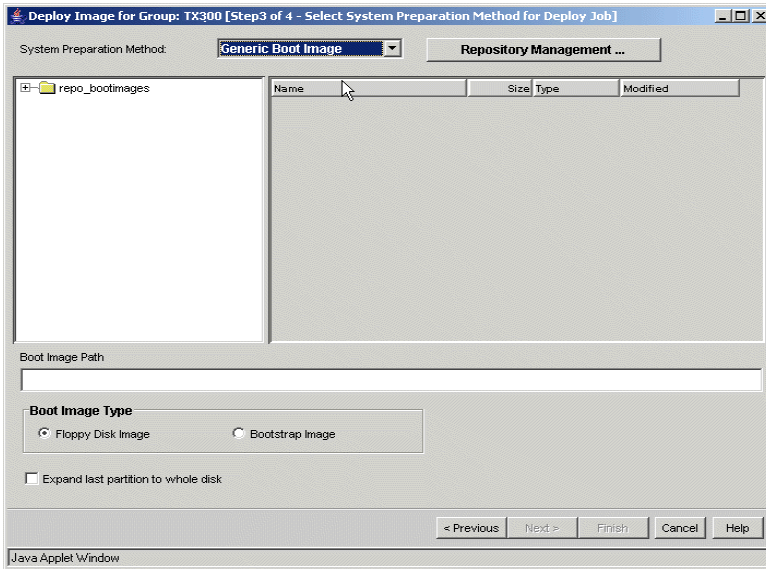


Figure 55: System Preparation Method - Generic Boot Image

If you select the system preparation method *Generic Boot Image*, the following parameters are displayed:

*Boot Image Path*

Displays the path where the selected image is stored.

*Boot Image Type*

Select the boot image type (see also [section “Image Creation” on page 27](#)).

*Expand last partition to whole disk*

Expands the last partition of the image to use the rest of disk.

Select the *Repository Management* button to start the repository management, see [section “Repository Management” on page 125](#).

Click the *Next* button. The *Set Arguments for Deploy Job* window is displayed (see [page 174](#)).

### System Preparation Method for Deploy Job (Blade optimized)

This preparation mode is only displayed when the deployment platform is *Caldera DOS*.

The *Blade optimized* system preparation method should be used only for a deployment job with Fujitsu Siemens blade servers.

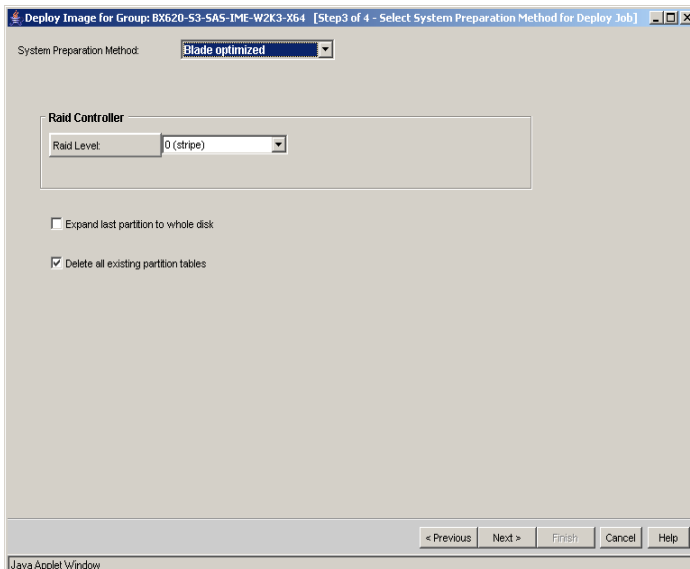


Figure 56: System Preparation Method - Blade optimized

If you select the system preparation method *Blade optimized*, the following parameters are displayed:

#### *Raid Controller*

You can select the RAID level that should be configured for the onboard RAID controller. You must select the same RAID level as for the creation.

- unchanged (applies previously determined RAID settings)
- 0 (stripe)
- single-disk mode (two level-0 RAID arrays will be configured)
- 1 (mirror)



For BX630 server blades (only 8-way) you can select the RAID level of the first and second RAID controller.

*Expand last partition to whole disk*

Expands the last partition of the image to use the rest of disk.

*Delete all existing partition tables*

Deletes all existing partition tables.

Click the *Next* button. The *Set Arguments for Deploy Job* window is displayed (see [page 174](#)).

**System Preparation Method for Deploy Job (All PRIMERGY)**

This system preparation is done by ServerStart/Installation Manager. For more information on the system preparation method see [section “System Preparation Method “All Primergy”” on page 160](#).

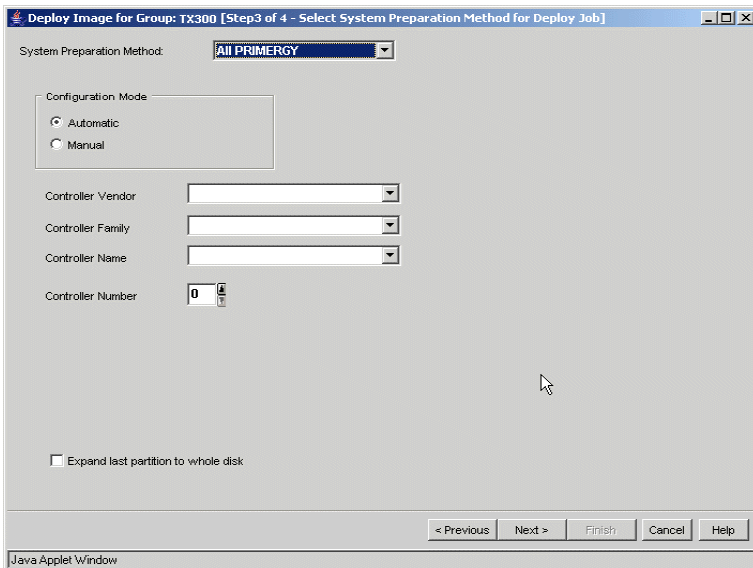


Figure 57: System Preparation Method - All PRIMERGY

If you select the system preparation method *All PRIMERGY*, the following parameters are displayed

*Configuration Mode*

Select the RAID configuration mode. In *Manual* mode you must define additional parameters.

*Controller Vendor*

Select the controller vendor.

*Controller Family*

Select the controller family.

*Controller Name*

Select the controller name.

*Controller Number*

Select the logical controller number as defined in the system.

*Expand last partition to whole disk*

Expands the last partition of the image to use the rest of disk.

The following parameters are displayed only if you select the configuration mode *Manual*:

*RAID Level*

Select the RAID level.

*Number of Disks*

Select the number of disks.

*Hot Spare*

A standby hard disk can be used to replace a defective hard disk.

Click the *Next* button. The *Set Arguments for Deploy Job* window is displayed (see [page 174](#)).

Set Arguments for Deploy Job

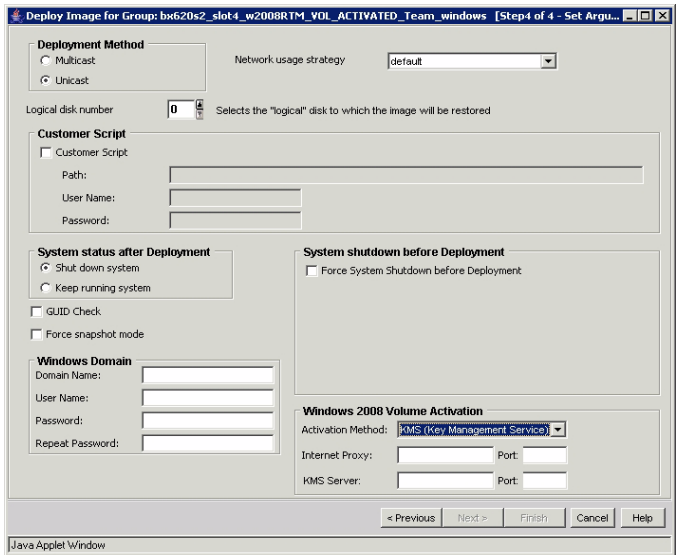


Figure 58: Set Arguments for Deploy Job window

Deployment Method

Select the deployment method (*Multicast* or *Unicast*) for the deployment process (see also [section “LAN Traffic and Deployment Methods” on page 267](#)).

Network usage strategy

Select the parameter for the network load.

Logical disk number

Select the disk on which the image should be deployed.

Customer Script

You can specify a customer script to be executed on the target system at the end of the deployment process. Mark the *Customer Script* option.



This functionality is supported only with images that were generated with RemoteDeploy as of version 1.2.

This function is not available for deployment of a snapshot image of a Windows-based system.

Path

Specify the path name for the customer script.

- For Windows target systems:  
The path name should be the network path name of the script in UNC notation. This means that you must use a network share where you store the script. You can also specify optional parameters for this script.

*Example*

`\\alpenmac\scripts\DomainJoin\domain_join.bat -domain my domain`

- For Linux target systems:  
The path name has the following format:  
`\\<server>\<path>\script_name [parameters]`  
`//<server>/<path>/script_name [parameters]`

*server*

FTP server name or the IP address of the FTP server.

*path*

Path to the script relative to the root of the FTP server.

*User Name/Password*

User name and password. This account information is used to access the customer script of the target systems. In the case of a Windows target system, the user account must have read and execute permission for the share and the specified subdirectory. In the case of a Linux target system, this account is used to access the FTP server.

*System status after Deployment*

Select the system status of the target systems after the deployment process.



This functionality is supported only with images that were generated with RemoteDeploy as of version 1.2.

*System shutdown before Deployment*

*Force System Shutdown before Deployment*

If you mark this check box, Deployment Manager will try to shut down the affected target system before the deployment process is started. You can select the shutdown method. If you select the shutdown method *graceful*, a user name and password are required.



The deployment process can only be started if all target systems are powered off.

*GUID check* (only displayed if you select the deployment method *Blade optimized* or *Unchanged*)

If you mark this check box, a check from the GUID value is performed between the server list and the target value. Only if the values are identical, the cloning process can be performed.

*Force snapshot mode*

If you select this option, an image (not a snapshot image) is cloned in the same way as a snapshot image, i.e. no adjustments are made in the post-preparation phase.

*Windows Domain*

If you deploy a Windows image (no snapshot image), you can specify a Windows domain. The image must be created with RemoteDeploy 3.30 or a later version, and at the moment of image generation the tool *netdom.exe* must be available for the deployment service (see online help and Readme file).

*Windows 2008 Volume Activation*

If you deploy a Windows 2008 image created from a volume installation, the cloned image can be automatically activated after the cloning process:

- *Activation Method*  
Select the activation method: *MAK (Multiple Activation Key)* or *KMS (Key Management Service)*
- *Internet Proxy*  
Optional: Specify a proxy server (IP address or name) to connect to the Internet. You can also enter a port number.
- *KMS Server*  
If you select the activation method *KMS (Key Management Service)*, you must specify the IP address or the name of the KMS server. Optionally, you can enter the KMS port number.
- *Key*  
If you select the activation method *MAK (Multiple Activation Key)*, enter the activation key.

*Set hostname in /etc/hosts \**

If you deploy a Linux or ESX image, the host name of the cloned system is entered in the */etc/hosts* file.



*Create a VMFS partition (only for ESX)*

Create a VMFS partition for ESX.

*Device for the VMFS partition (only for ESX)*

VMFS partition device name.

*Size of the VMFS partition (only for ESX)*

VMFS partition size.

*Type of the VMFS partition (only for ESX)*

VMFS partition type.

*VM storage name*

VM storage name.



The parameters *Create a VMFS partition*, *Device for the VMFS partition*, *Size of the VMFS partition* and *Type of the VMFS partition* are not displayed if you have selected the parameter *skip existing partition with VMFS file system* in the image creation for ESX.

You start the cloning process by clicking *Finish*. Once the cloning process is successfully started, the *Deploy Image - <group name>* progress window is displayed showing information on the cloning process.

## 7.4 Get Batch Result

The cloning progress of each server system to be cloned can be followed in the *Batch Result* window. To open the window, select *Get Batch Result ...* from the context menu of a server or deployment group.

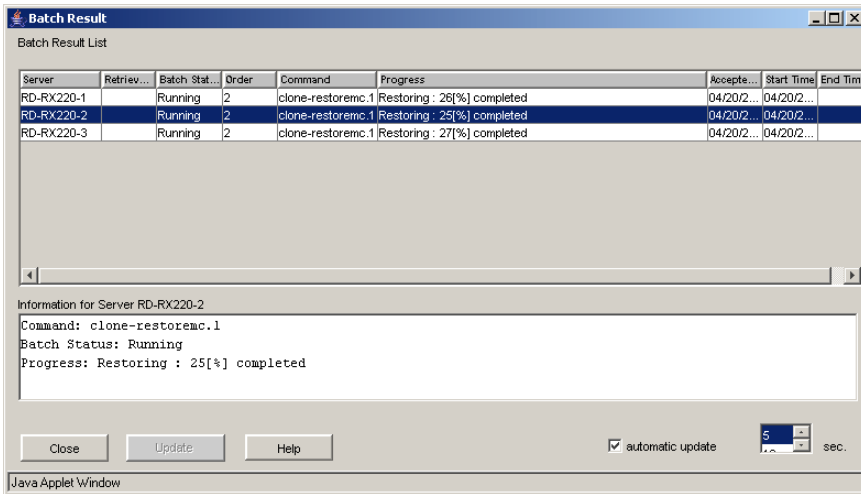


Figure 59: Batch Result window



As well as the *Batch Result* window which must be opened manually, a progress window is automatically displayed during the cloning process (the same as during image creation). This contains information on the status and the number of cloning processes currently running.

## 7.5 Cloning/Installing Baseboard Management Controllers

As of ServerView S2 version 4.52, Baseboard Management Controllers (BMC) can be added to the ServerView server list via the server browser. A special BMC icon shows the BMC (only Fujitsu Siemens BMCs) in the ServerView server list. The icon of a BMC in the server list reflects the status of the Global Error LED.

RemoteDeploy version 4.1 supports the cloning and installation of BMCs.

To access a BMC, Deployment Manager requires a valid user ID with the following privileges:

- Getting and setting the power status
- Getting and setting the boot order

The *admin* account on all current PRIMERGY systems has the required privileges.

### Cloning and installing older PRIMERGY systems

The steps below are necessary if you want to clone or install one of the following older PRIMERGY systems:

- RX200/TX200
- RX220
- RX300/TX300
- RX100 S2
- RX200 S2/TX200 S2
- RX300 S2/TX300 S2
- RX100 S3
- TX150 S2
- TX150 S3
- TX150 S4

1. Start Operations Manager, see the Operations Manager guide.
2. Open the *User Password Settings* window by selecting the *Users/Passwords* entry on the *Administration* menu.
3. Delete the *admin* account.
4. Add a new account with the required privileges.
5. Add the *admin* account again.



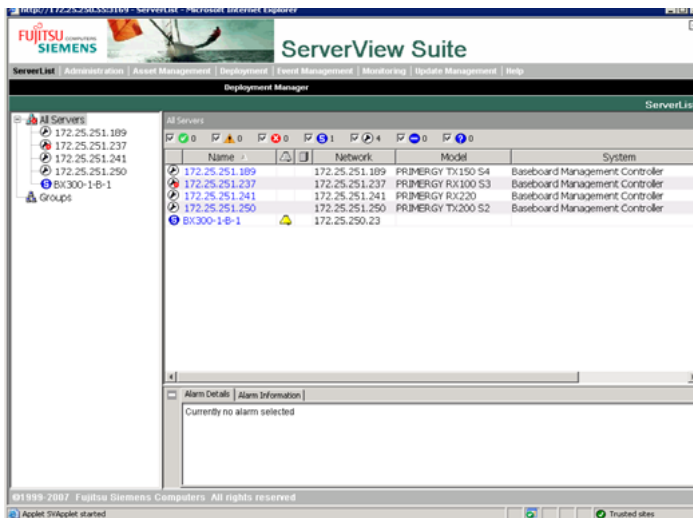
It is important that the privileged account is first in the search order.

You can change the account for each server later in the Deployment Manager front-end via the *Deployment Configuration* window.

## 7.5.1 Displaying BMCs

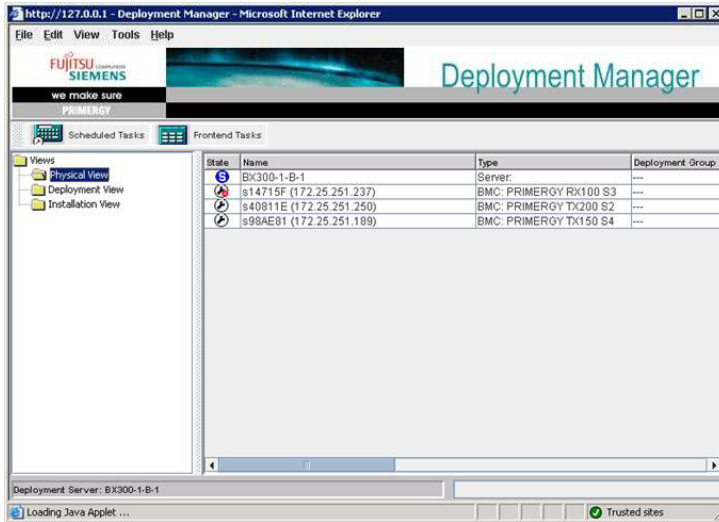
### Displaying BMCs in Operations Manager

The following window shows an example of BMC entries displayed in the Operations Manager *ServerList* window:



## Displaying BMCs in Deployment Manager

The Deployment Manager database is periodically updated from the ServerView database. The BMC entries are displayed in the *Physical View* of the Deployment Manager front-end:



The host names generated for the BMCs are based on the last 6 bytes of the MAC address.

BMCs can be added to deployment groups or installation groups.

## 7.5.2 Changing the Deployment Configuration

You can change the deployment configuration of a BMC in the Deployment Manager front-end.

- ▶ Select a BMC in the Physical View or in a deployment/installation group and choose the *Deployment Configuration ...* entry from the context menu. The *Deployment Configuration of BMC <name>* window opens.

You can change the following settings:

- ▶ In the *General Settings* window (first window) you should change the generated server name.
- ▶ In the *Network Adapters* window (second window) DHCP is selected by default. You can enter a static IP address to replace the default deployment configuration. Click the *Add Network Adapters* button to add deployment configurations for add-on PCI boards.
- ▶ The *BMC Account Settings* window (fifth window) displays the BMC configuration. You can change the user name and the password. Choose an account with the appropriate privilege.

A bare server entry will be added to the ServerView database. This entry takes the values from the BMC entry with the following changes:

- The server name and system name are set to the generated server name or to the server name entered in the *General Settings* window.
- The network address is set to “0.0.0.0”.

The GUID (UUID) is deleted in the ServerView database, but saved in the Deployment Manager database. After successful cloning or installation of the BMC, the GUID is set automatically in the ServerView database.

In the ServerView database the BMC and the bare server entries exist in parallel. But in the ServerView server list only the BMC entry is displayed.

In the Deployment Manager database, only the bare server entry exists. During the periodical update of the database, the *FSC Deployment Manager* service matches the BMC entry from the ServerView database to the bare server entry. I.e. the Deployment Manager server list displays a bare server entry with the values of the BMC entry.

### 7.5.3 Cloning/Installing a BMC without Changing the Deployment Configuration

BMCs can be cloned or installed immediately without changing the deployment configuration.

A default deployment configuration exists for every BMC:

- Includes only the onboard interfaces (reported by the BMC).
- DHCP is set for all interfaces.
- The target system name is set to the generated server name.
- The DNS suffix entry is empty.

Once the cloning or installation process is started, a bare server with the generated server name is created. You cannot change the generated name later.

### 7.5.4 Deleting a BMC

You can delete a BMC entry from Deployment Manager:

- ▶ Select the BMC in the Physical View or in a deployment/installation group.
- ▶ Choose *Remove Server(s)* or *Delete servers* from the corresponding context menu.

The BMC is also deleted from all groups automatically.

## 7.5.5 Actions after Cloning / Installation

The following actions are performed after successful cloning or installation of a BMC:

- The *FSC Deployment Manager* service changes the *BareServer* to type *Server* in the *ServerView* database. The following fields are also changed:
  - The *UUID* is set to the value from the corresponding BMC.
  - The *FullQualifiedName* is set. If a DNS suffix is specified in the *Deployment Configuration* window, the suffix is appended to the *ServerName*. Otherwise the *FullQualifiedName* is set to *ServerName*.
- The Deployment Manager front-end immediately displays a server instead of a bare server in the *Physical View*.
- Operations Manager initially displays a BMC entry and a server entry in parallel.
- After cloning/installing, the server is booted with the installed *ServerView* agents. The *FSC ServerView Services* service
  - contacts the DNS server with the given *FullQualifiedName* to get the network address of the server.
  - uses the network address to contact the *ServerView* agent on the server.
  - determines that the *UUID* delivered by the *ServerView* agent on the server is identical to the *UUID* of the BMC entry. The BMC entry is deleted from the *ServerView* database.
- Finally, Operations Manager displays only the server entry.



## 8 Installing PRIMERGY Servers

If ServerStart/Installation Manager as of version 6.605 is installed on the same system, the *Installation View* is displayed in the tree view on the right side of the Deployment Manager main window. The *Installation View* is used for mass installation of PRIMERGY servers.

The following sections describe how to create new installation groups, add or remove servers to/from an installation group, assign configuration files to a group, and start the installation process. The installation is performed via ServerStart/Installation Manager.

### 8.1 Installation Groups

Before you create a new installation group you need to consider which servers should get which configuration file. You can decide whether to create an installation group and assign one configuration file to this group, or whether to create an installation group and assign a configuration file to each server in this group.

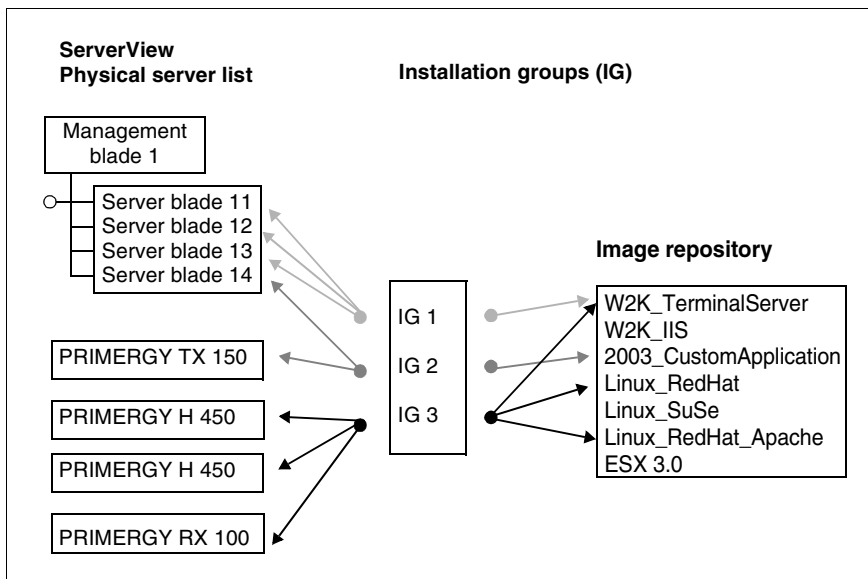


Figure 60: Installation groups

Installation groups with several servers help to reduce the workload of an administrator by organizing servers with the same configuration in one logical group. All servers in an installation group can be installed simultaneously.



If you assign configuration files to servers, make sure that these files are applicable for these servers. For example, an installation configuration file for a specific RAID controller requires that the installation target server contains this RAID controller.

### 8.1.1 Creating/Removing an Installation Group

Before you create an installation group, you must create repositories with configuration files, see [section “Repository Management” on page 125](#).

To create a new installation group, select *New Installation Group ...* from the context menu in the *Installation View*. The *New Installation Group* window is displayed.

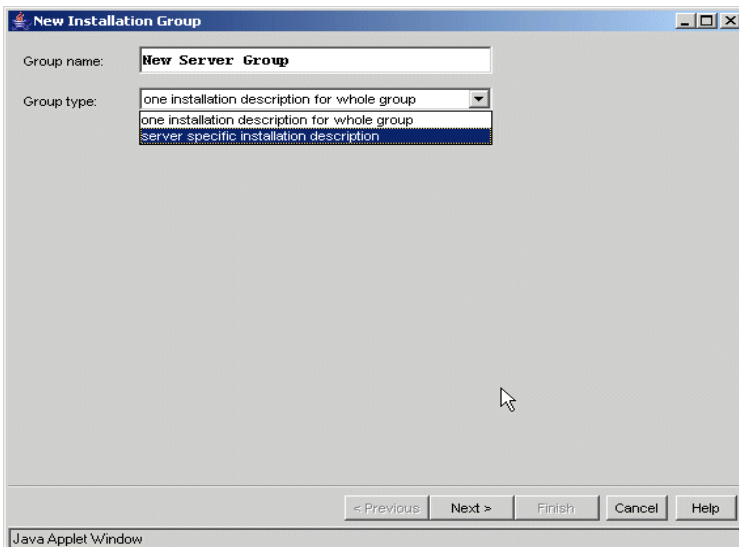


Figure 61: New Installation Group window

*Group name*

Name of the new group.

*Group type*

Select the type of the group:

- *one installation description for the whole group*  
All servers in the group are installed with one configuration file.
- *server specific installation description*  
The servers in the group can be installed with different configuration files.

If you select the group type *server specific installation description*, click *Finish*. You can assign the configuration files in the *Add Server(s)* window, see [section “Adding Servers to an Installation Group” on page 188](#).

Otherwise click *Next*. In the next window, you can assign a configuration file for the group.

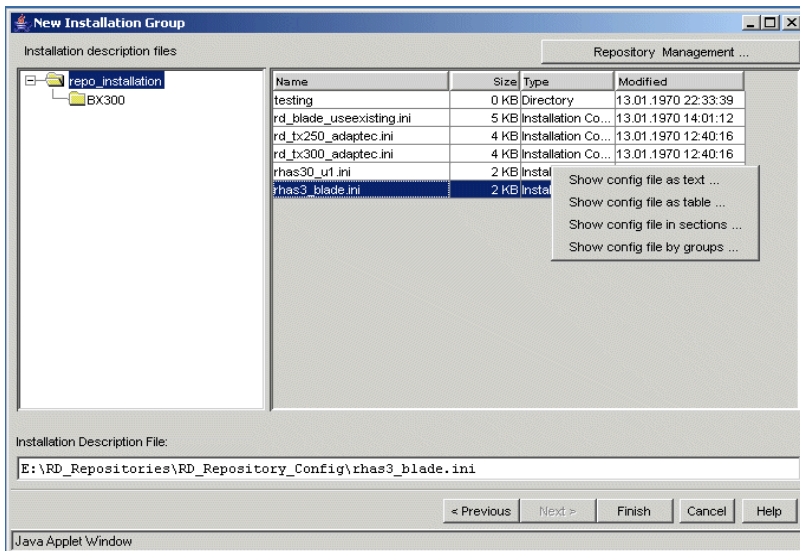


Figure 62: Select configuration file

Select the configuration file in the repository folder.

Click the *Repository Management ...* button to start the repository management, see [section “Repository Management” on page 125](#).

Select the *Show config* entries from a selected configuration file to display information from the configuration file. You can choose different formats for the presentation, e.g. ini format or table format.

Click *Finish*. The created installation group is displayed in the *Installation View*.

### Removing an installation group

To remove an installation group, select the desired group in the *Installation View* and select the entry *Remove Installation Group* from the context menu. The removal is only possible if no installation job is running on any server in that group.

## 8.1.2 Adding Servers to an Installation Group

To add servers to an installation group, select an installation group in the *Installation View* of Deployment Manager and select *Add Server(s)* from the context menu. The *Add Server(s)* window is displayed:

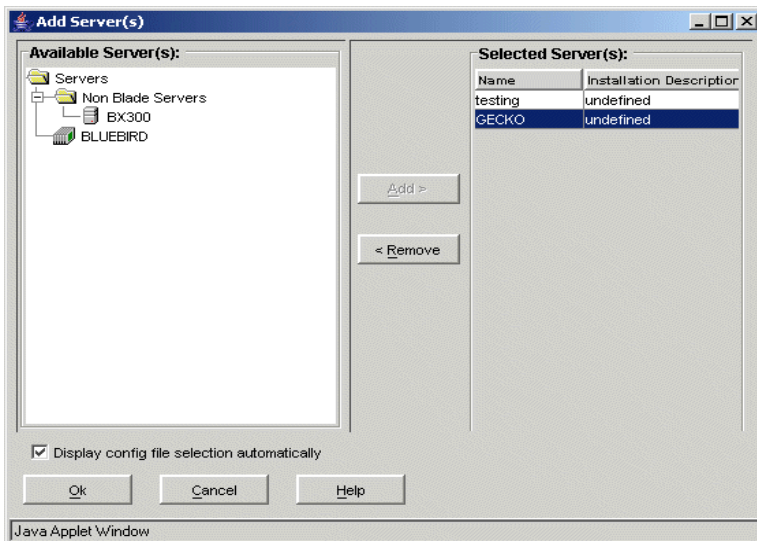


Figure 63: Example - Add Server(s) window

The *Available Server(s)* list displays the servers from the server list. To add servers to the installation group, select the server(s) and click the *Add* button. The *Selected Server(s)* list contains the servers which are to be added to the group. You can remove servers from this list by selecting the servers and clicking the *Remove* button.

The list on the right side displays the server name and the assigned configuration file (only if the group type is *one installation description for each server*). You must assign a configuration file to each server.

If the check box *Display config file selection automatically* is marked (the check box is only displayed if the group type is *server specific installation description*), the *Installation Description File* window is displayed after you have added a server. You can assign the configuration files to the servers. Otherwise you must choose *Set description file* from the context menu of the server in the *Add Server(s)* window. This also opens the *Installation Description File* window. See [“Assigning configuration files” on page 189](#).

Click the *Ok* button to add the servers to the group.

### **Assigning configuration files**

In the *Installation Description File* window, you can add configuration files to servers. This window is displayed if you mark the check box *Display config file selection automatically* or if you choose *Set description file* from the context menu of the server in the *Add Server(s)* window.

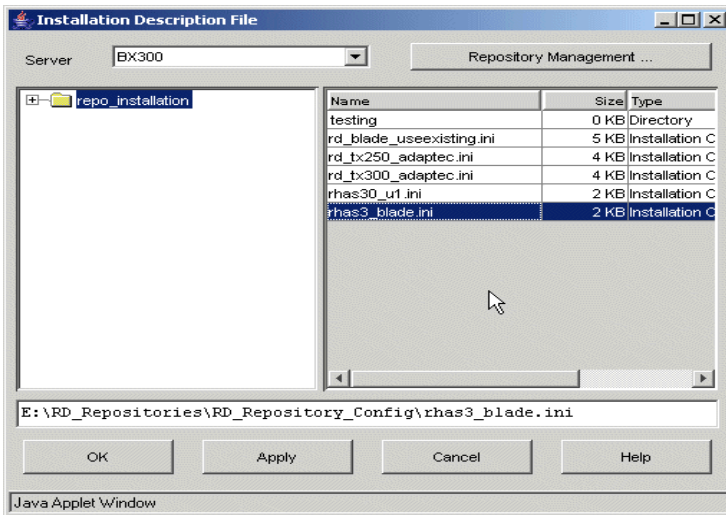


Figure 64: Installation Description File window

The list on the left side displays all existing repositories. If you select a repository, the list on the right side displays the corresponding configuration files. Select the configuration file and click the *Apply* button to confirm the settings.

Click the *Repository Management* button to start the repository management, see [section “Repository Management” on page 125](#).

You can select the next server from the server list and assign further configuration files. Click *Next* to close the window.

### 8.1.3 Removing Servers from an Installation Group

To remove a server from an installation group, select the relevant installation group in the *Installation View*. Select the relevant servers in the list and choose *Remove servers ...* from the context menu.

## 8.2 Viewing and Modifying the Properties of an Installation Group

You can display the properties of an installation group or change the assignment of configuration files. Select the installation group and select *Properties ...* from the context menu. The following window is displayed:

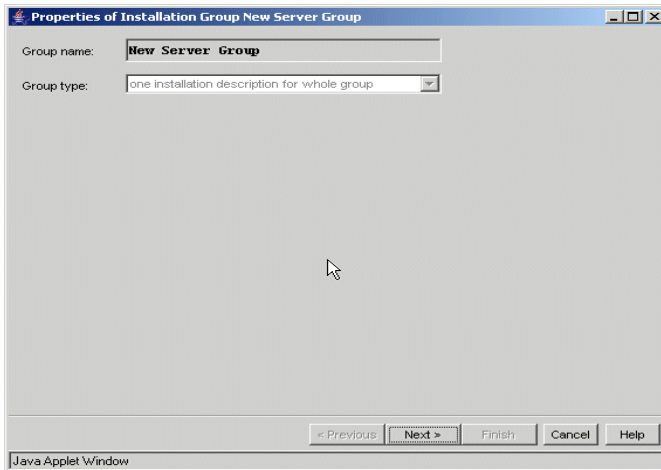


Figure 65: Installation group properties

Click the *Next* button. Depending on the group type, different windows are displayed:

- If you select the group type *one installation description for whole group*, the following window is displayed:

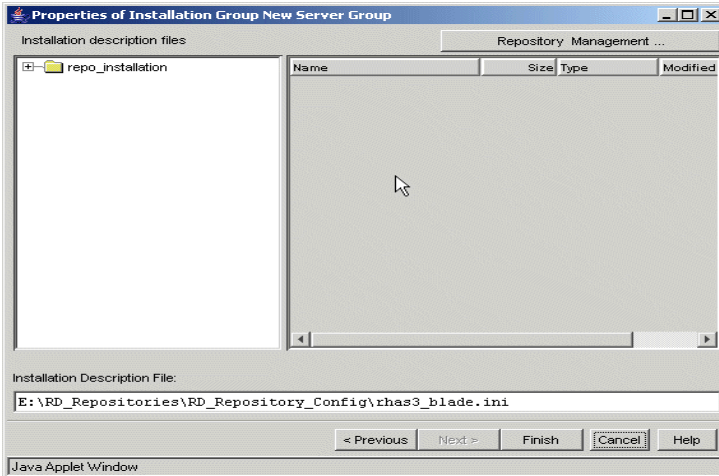


Figure 66: Installation group properties

Click the *Repository Management* button to start the repository management, see [section “Repository Management” on page 125](#).

You can change the assignment to the configuration file if you choose another path.

Click *Finish* to close the window.



- If you select the group type *server specific installation description*, the following window is displayed:

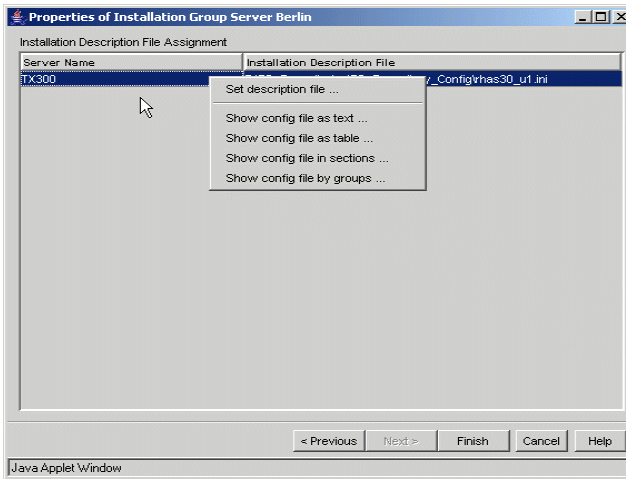


Figure 67: Select configuration file

You can change the assignments of configuration files if you select *Set description file ...* from the context menu. This opens the *Installation Description File* window, see [figure “Installation Description File window” on page 190](#).

Click *Finish* to close the window.

## 8.3 Installing the Server

You start the installation by selecting an installation group in the *Installation View* or by selecting a server in the *Installation View* and choosing *Install ...* from the context menu. Proceed as follows to install server(s) with the configuration files.

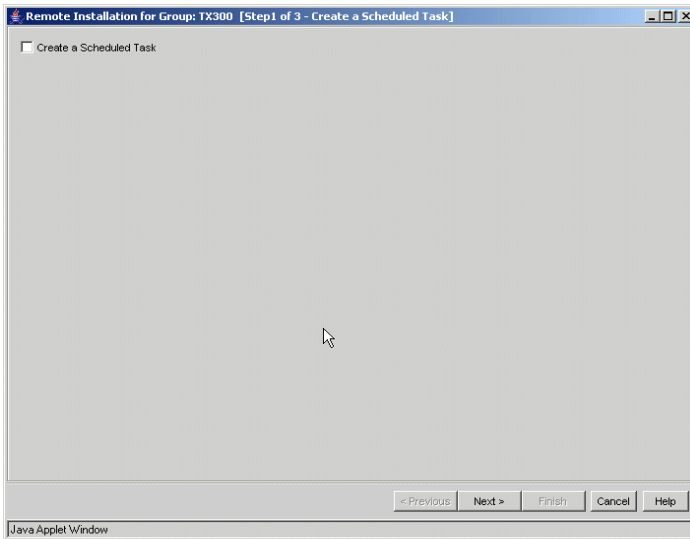


Figure 68: Remote Installation window

The first step is to decide whether you want to start the installation process as a scheduled task or not.

If you want to create a scheduled task, mark the check box; further parameters will appear.

If you do not want to create a scheduled task, click the *Next* button. The *Image Information* window is displayed; see [“Select Server\(s\) for Installation Job” on page 198](#).

## Create a Scheduled Task

**Save Disk Image for BX300 - Scheduler Options**

☒ Create a Scheduled Task

**Create a Scheduled Task:**

Taskname:

Deployment Server:

Time Unit to perform this Task:

Retry Counter:

Retry Interval (Minutes):

Task start time-window (Minutes):

**Define Scheduled Task Settings:**

Set time you want this task to start:

Start time:  :  ☐ AM ☐ PM

Select date you want this task to start:

Start date:

< Previous Next > Finish Cancel Help

Java Applet Window

Figure 69: Create a Scheduled Task window

**i** A scheduled job will fail if the user name and password for the deployment server are changed between task definition and task execution.

The text field on the left side shows information on the scheduler settings that are available for *Create a Scheduled Task*. The text field on the right side shows information on the *Define Schedule Task Settings*.

### Create a Scheduled Task

#### Taskname

Task name for the new task. You can enter any string except the characters &, ".

#### Deployment Server

Name of the deployment server which is used for this task. By default this is the deployment server which you select at the start of Deployment Manager. You can select any server from the list of deployment servers. If you select another deployment server, you must specify the user name and password for a connection to it.

*Time Unit to perform this Task*

You can select the following values:

- *Once*  
The task will be performed once only. You can only specify the *Start date* for this job.
- *Daily*  
The task will be performed daily.
- *Weekly*  
The task will be performed weekly.
- *Monthly*  
The task will be performed monthly.

*Retry Counter*

Specify the number of retries for this task if the job fails.

*Retry Interval (Minutes)*

The time (in minutes) before the next attempt if previous attempts at a task failed and the number of retries does not exceed the retry counter. A value between 1 and 360 minutes can be specified for the retry interval.

*Task start time-window (Minutes)*

A time value between 10 and 600 minutes. If the task could not be started successfully within the time range beginning with the start time of the task and ending *xx* minutes later (*xx* is the specified value for *Task start time-window*), the task will be canceled. Also retries of the task will be made only during this time range.

Therefore the task will not be started after the task start time window has elapsed. It can happen that a task is handed over to the deployment server, but is only queued because too many other tasks are already running. If the *Task start time-window* elapses while a task remains in this state, the task will also be canceled. A running task will not be canceled when the *Task start time-window* elapses.

*Define Scheduled Task Settings**Set time you want this task to start*

Start time of the scheduled task. You can specify an hour between 0 and 11 and a minute between 0 and 59. You can also select whether the job will be started before noon (*AM*) or in the afternoon (*PM*).

*Select date you want this task to start (only visible if you select *Once* or *Daily* as the time unit)*

You can select the start date of the scheduled task from the calendar. Click the *Change start date* button to change the start date.

*Perform this task (only visible if you select *Daily* as the time unit)*

You can also select whether the task should be performed *Every Day*, *Weekdays* or *Every x days*.

*Select the day(s) of the week you want this task to start (only visible if you select *Weekly* as the time unit)*

You can specify that the task should be executed every week or every  $n$  week ( $n = 1 \dots 52$ ). You can also select the days of the week.

*Select the day of the month you want this task to start (only visible if you select *Monthly* as the time unit)*

You can specify the months of the year in which the task should be executed. You can also specify the day of the month on which a task should be executed. And you can specify a weekday and whether the task should be executed in the first, second, third, fourth or last week of a month.

Click the *Next* button; the *Select Server(s) for Installation Job* window is displayed.

## Select Server(s) for Installation Job

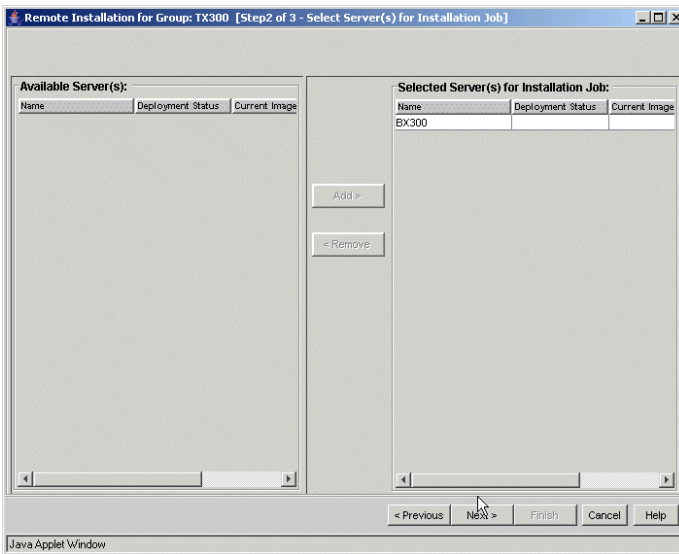


Figure 70: Select Server(s) for Installation Job window

### *Available Server(s)*

Displays the servers which can be added to the installation group.

### *Selected Server(s) for Installation Job*

Displays the servers which are to be installed.

Click *Add* to add servers to the list on the right-hand side. You can also remove servers from this list by clicking the *Remove* button.

Click the *Next* button; the *Set Arguments for Installation Job* window is displayed.

## Set Arguments for Installation Job

Remote Installation for Group: TX300 [Step3 of 3 - Set Arguments for Installation Job]

**System status after Installation**

☒ Shutdown system

☐ Keep system running

**System shutdown before Installation**

☒ Force System Shutdown before Installation

Shutdown Method: **forced**

Shutdown User Name:

Shutdown Password:

Repeat Shutdown Password:

**Access to ServerStart data**

ServerStart contents tree (UNC):  ☒ use default

Username for remote access:  ☒ use default

Password:

Repeat Password:

< Previous   Next >   Finish   Cancel   Help

Java Applet Window

Figure 71: Set Arguments for Installation Job window

### *System Shutdown before Installation*

If you mark the *Force System Shutdown before Installation* check box, Deployment Manager will try to shut down the affected target systems before the installation process is started.

You can select a shutdown method. If you select the shutdown method *graceful*, a user name and password are required.



The installation process can only be started if all target systems are powered off.

### *System status after Installation*

Select the system status of the target systems after the installation process.

### *Access to ServerStart/Installation Manager data*

Specify the parameters to access the ServerStart/Installation Manager data. If the check box *use default* is marked, the parameters as defined during the ServerStart/Installation Manager installation are displayed. It is recommended to use the default settings. Otherwise you must specify the directory where the ServerStart/Installation Manager data is stored, the user name and the password.

You start the installation process by clicking *Finish*. Once the installation process is successfully started, the *Remote Installation - <group name>* progress window is displayed showing information on the installation process.



---

## 9 Deployment Example: Step by Step Deployment of Server Blades

The following sections describe step by step how to deploy server blades in a blade system.

The deployment process is divided into three basic stages:

1. Reference Installation (see [section “Reference Installation of a Server Blade” on page 202](#))

First you use ServerStart/Installation Manager to configure and install an arbitrary server blade in a representative way. This reference installation is used to install further server blades in the same way.

2. Image Creation (see [section “Image Creation Process” on page 225](#))

From the reference system an image file is created which contains information on the hard disk, the configuration of the partitions, and all data of the operating system.

3. Cloning (see [section “Deploying an Image to Server Blades” on page 235](#))

The cloning process deploys an image to server blades. It prepares the hardware, BIOS and storage devices, copies the image onto the hard disks and initiates a reboot of the target system.

The result are systems which are installed and configured identically with the exception of variable parameters such as the IP address, host name and SecureID (SID for Windows systems only) of the operating system, which must be unique to each server blade.

How to enter the IP address of the management blade or switch blade for the first time is described in the “PRIMERGY BX Blade Server System” operating manuals.

## 9.1 Reference Installation of a Server Blade

At the very beginning you do not usually have any images to deploy. Therefore you use the PRIMERGY ServerStart/Installation Manager CD/DVD for the first installation of a server blade. There are two possibilities:

- Local Installation

Connect the USB CD-ROM and USB floppy disk drive to the server blade you want to install. To do so you need a special Y cable. In the BIOS setup, set the option *Boot from removable device*. Boot from ServerStart CD as of version 6.605 and start the installation. For more information on local installation see the “ServerView - ServerStart/Installation Manager” manual.

- Remote Installation (recommended)

Use ServerStart/Installation Manager *Remote Installation* which you can find on the ServerStart/Installation Manager CD/DVD. To do this you must install the ServerStart/Installation Manager CD/DVD on a PC from where you want to start the installation. This PC acts as deployment server for the remote installation. It can be a notebook or a server. For more information see the following section.

### 9.1.1 Preparing a Remote Installation Deployment Server

#### Check the basic requirements of your deployment server

- The operating system Windows 2003 Server or Windows 2008 Server must be installed.



Refer to [section “Installation in Windows 2008” on page 53](#) for further information.

- If you want to deploy Linux Red Hat on your blade system, an FTP server must be available on the deployment server.



In order to set up an FTP server on a Windows computer, the Microsoft Internet Information Server (IIS) or corresponding third party software must be installed.

- If you want to deploy ESX 3.0, see also the ReadMe file on the Deployment Manager CD.
- Internet Explorer 5.5 or higher must be installed.

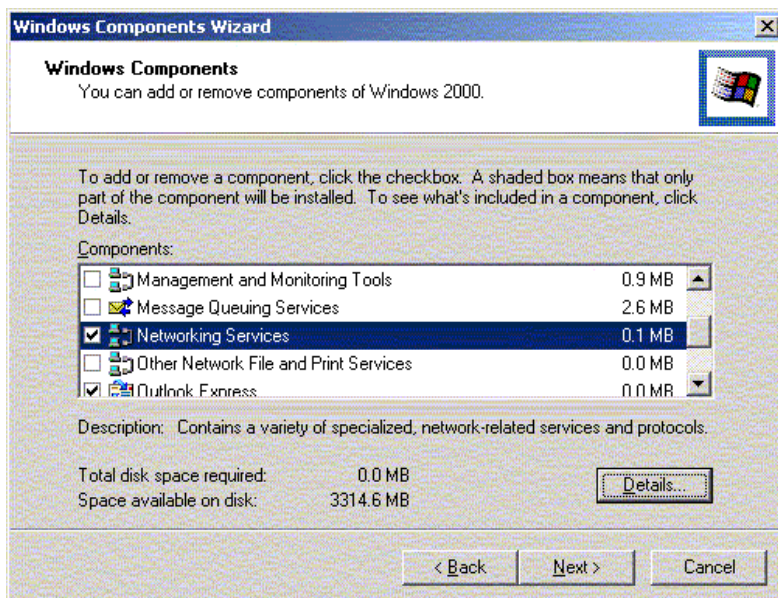
- A physical network connection to the server blade (via switch blade) must be established.

### Install and configure a DHCP server on your deployment server (if not already present in the LAN segment)

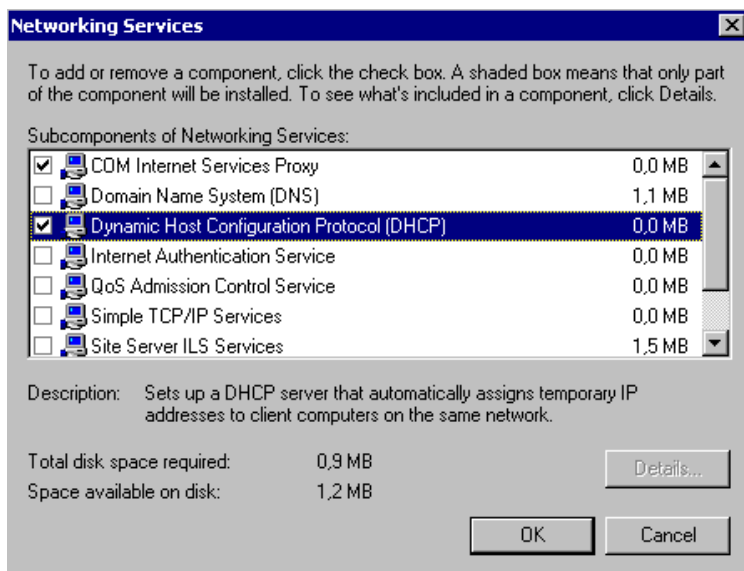


This step is only necessary if no DHCP server is yet present in the LAN segment.

- ▶ Start the installation process in the Windows control panel:
  - ▶ Choose *Start – Settings – Control Panel – Add/Remove Programs*.
  - ▶ Select *Add/Remove Windows Components*.
  - ▶ Select *Networking Services* and click *Details...*



- Enable *Dynamic Host Configuration Protocol (DHCP)* and click *OK*.



Use the DHCP manager to define a range of IP addresses. No special reservations, lease durations or server options are required.



All DHCP servers offer the DHCP client an IP address via a *DHCP Lease Offer*. This offer includes not only an IP address and the subnet mask but also the so-called *Lease Duration* which defines the duration of the offer and the IP address of the DHCP server making the offer.

- Activate your new scope.

### Install ServerStart/Installation Manager on the deployment server

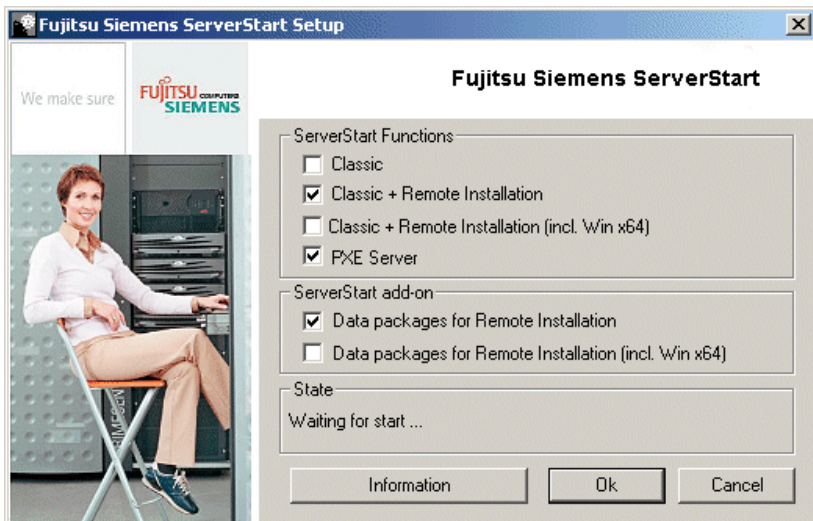
**i** The installation has to be performed under Windows 2000 or Windows 2003 with full administrative rights. Under Windows NT 4 the *Remote Installation* option will not be available.

- ▶ The following steps describe a ServerStart installation with version 6.605.

**i** You can call up the ServerStart application via the Windows Start menu: *Start – Programs – Fujitsu Siemens ServerStart – ServerStart (Start from HD)* (provided that the data packages for remote installation have been installed).

Insert the ServerStart CD/DVD. The application is started automatically.

**i** If the application fails to start, open the *SeStSetup.exe* file in the root directory of the CD-ROM/DVD.



- ▶ Make sure that the option *Classic + Remote Installation* is activated. The installer automatically selects the corresponding packages. Do not remove the selection.

This mode installs the following packages (for 32 bit OS):

- Fujitsu Siemens PXE service
- ServerStart data packages for remote installation
- ServerStart configuration front-end
- ServerStart remote boot platform



If the ServerStart installation procedure is started from the CD, you can choose between one of the following installation modes:

*ServerStart classic*

This module has to be installed in order to perform a local installation after configuration in *Preparation Mode*.

*ServerStart - remote installation*

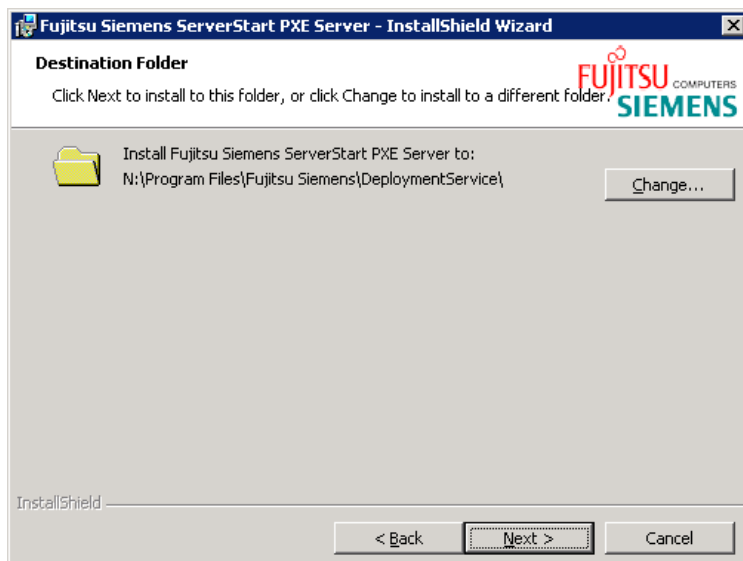
This module has to be installed in order to enable remote installation of Windows and Linux. The *Remote Installation* option (for installation of 32 bit OS) can only be chosen if ServerStart is being installed under Windows 2000 or Windows 2003.

- Click the *Next* button.

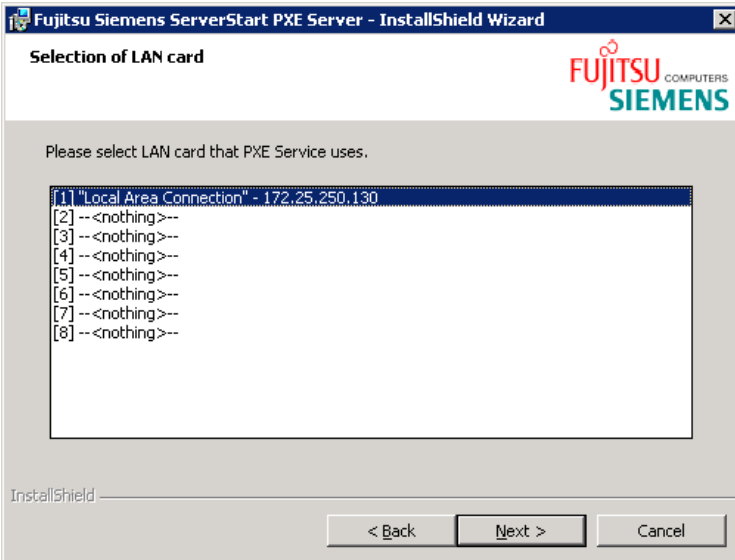
First the PXE Server package is installed.



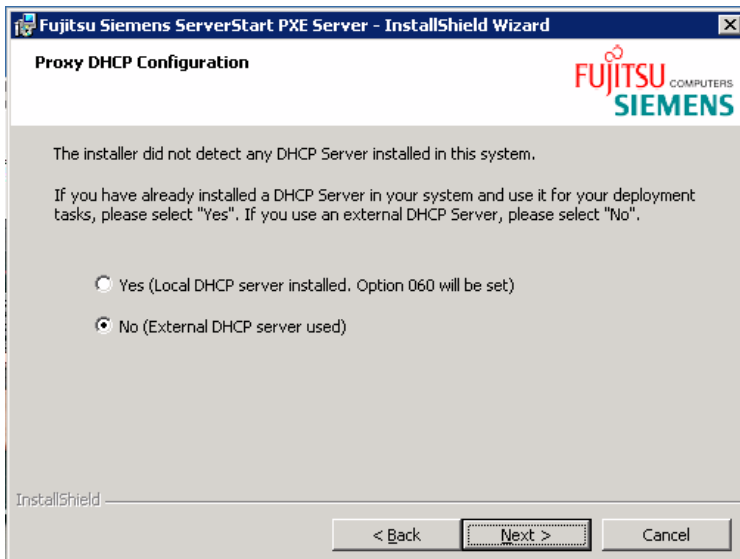
- Click the *Next* button.



- Specify the destination folder and click the *Next* button.



- Select the LAN card and click the *Next* button.





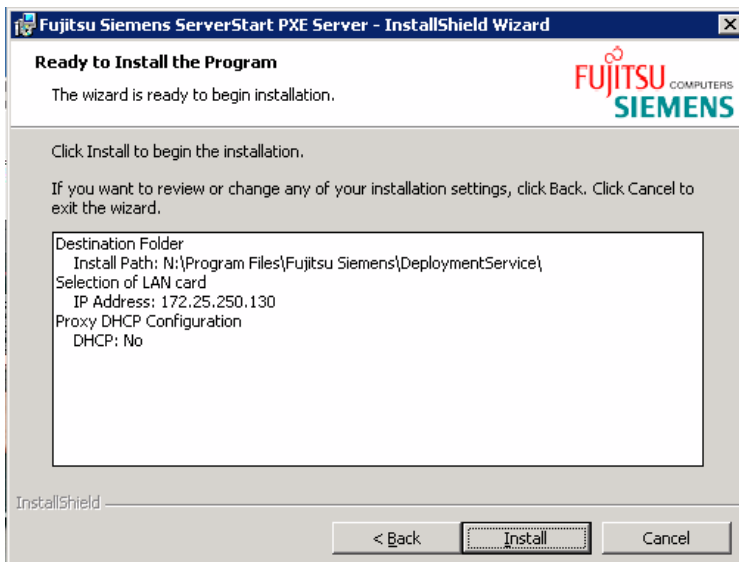
- Specify whether a DHCP server is located on the computer on which the ServerStart installation is currently being performed.

If the DHCP service is located on the deployment server, select *yes* in the ServerStart setup wizard after *is a DHCP server located on this machine?* In this case, ServerStart will automatically add a server option (060:PXE client) to the DHCP server.



Please note:

- If the details are wrong, the PXE server will be unavailable for the client.
  - Make sure that the LAN cable is connected to the computer before installing the PXE service.
  - In order to install the operating system from a shared directory on the local network, you must first copy the entire contents of the OS CD into this directory.
- Click the *Next* button.

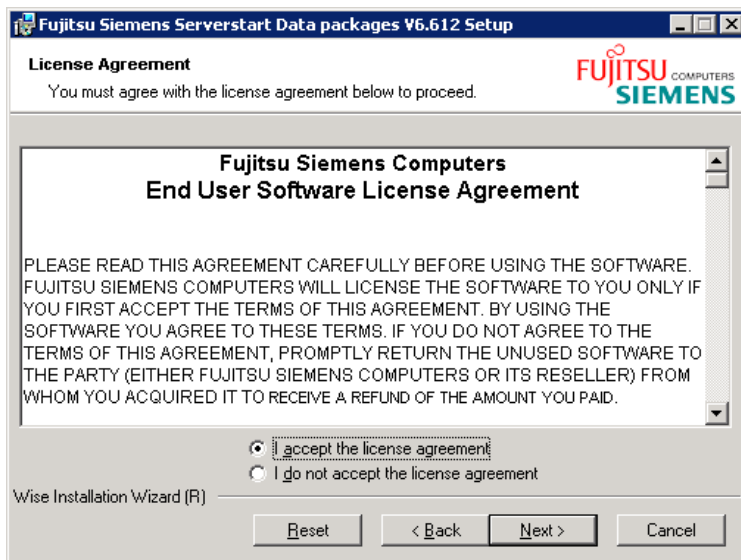


- Click *Install* to start the installation.

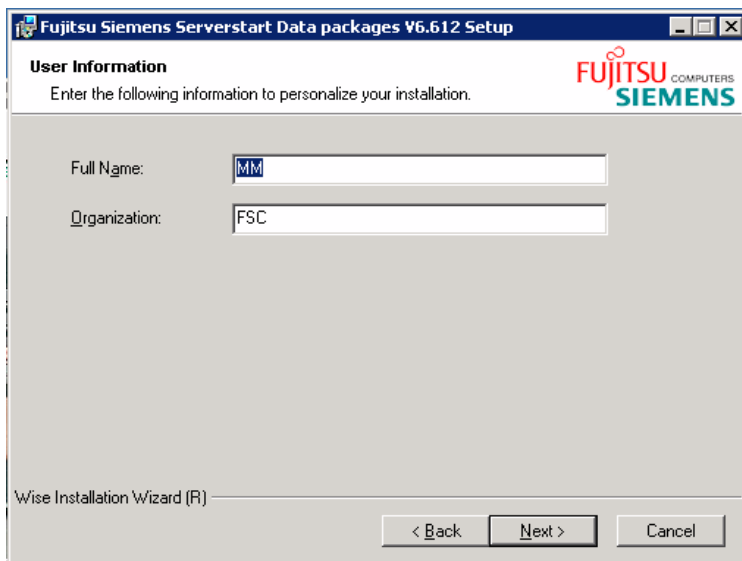
Next, the ServerStart data packages will be installed:



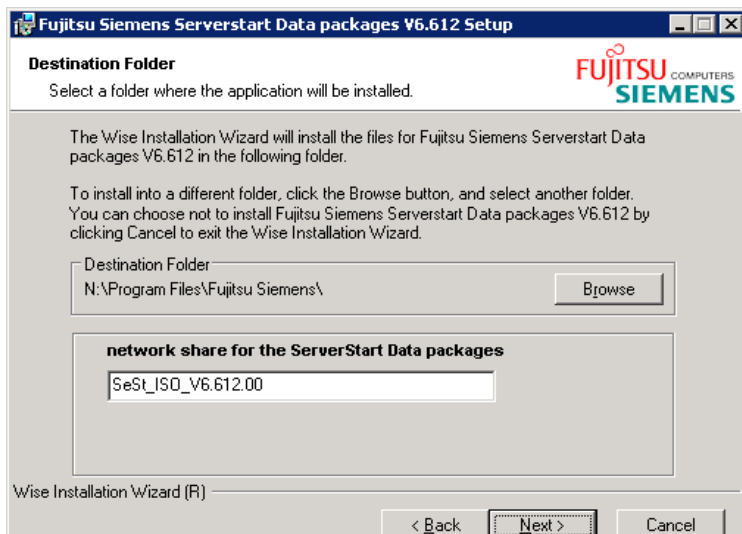
- Click the *Next* button.



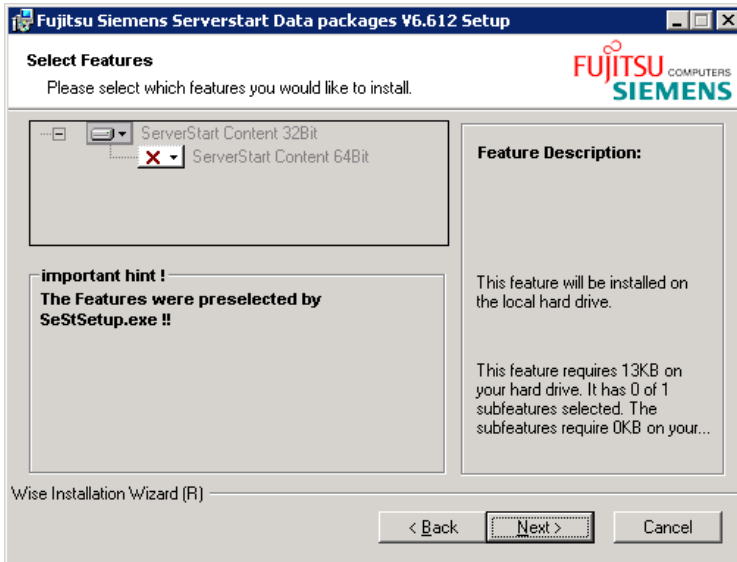
- To accept the license agreement, select the appropriate checkbox. Click the *Next* button.



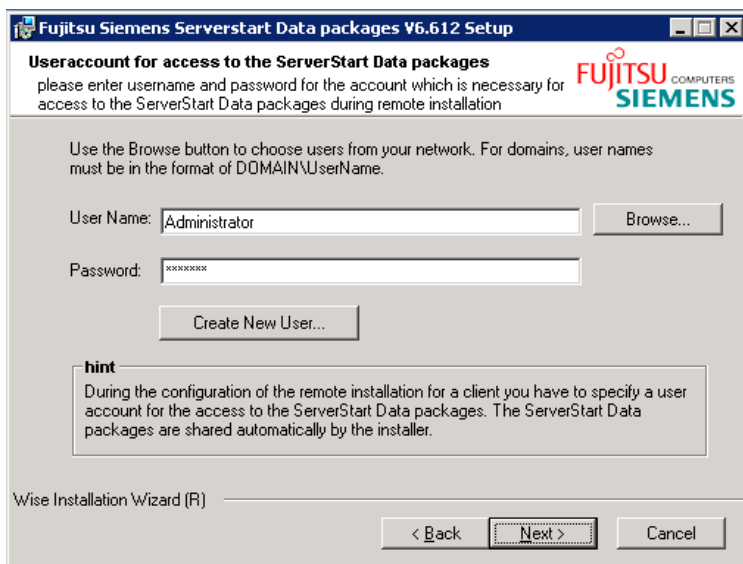
- Enter your name and the name of your company. Click the *Next* button.



- Specify the directory on your hard disk drive to which ServerStart data packages are to be installed and specify a label under which the content tree will be shared in the network. Click the *Next* button.



- Displays the features you want to install. Click the *Next* button.



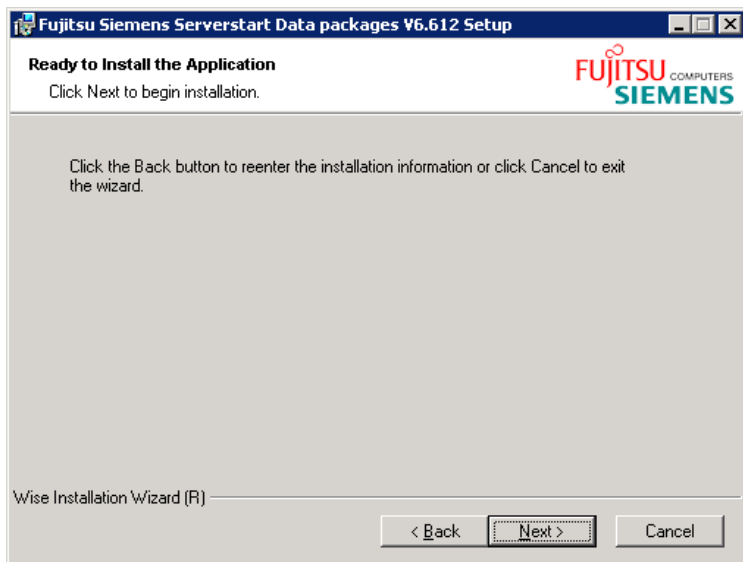
- Specify a user name and a password.



Please note:

During the configuration session for the remote installation of a client, it is necessary to specify a user account in order to access the remote installation data. The installation data is automatically shared on the network by the installer, but no specific user account is created.

- Click the *Next* button.

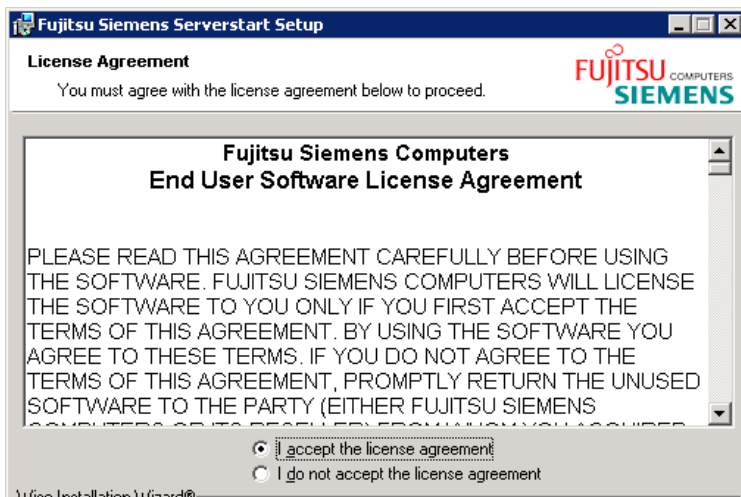


- Click the *Next* button to start the installation.

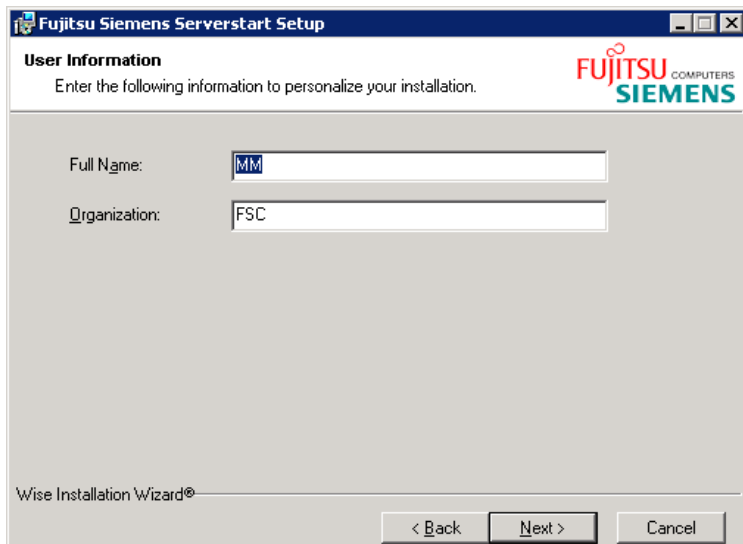
The ServerStart installation begins:



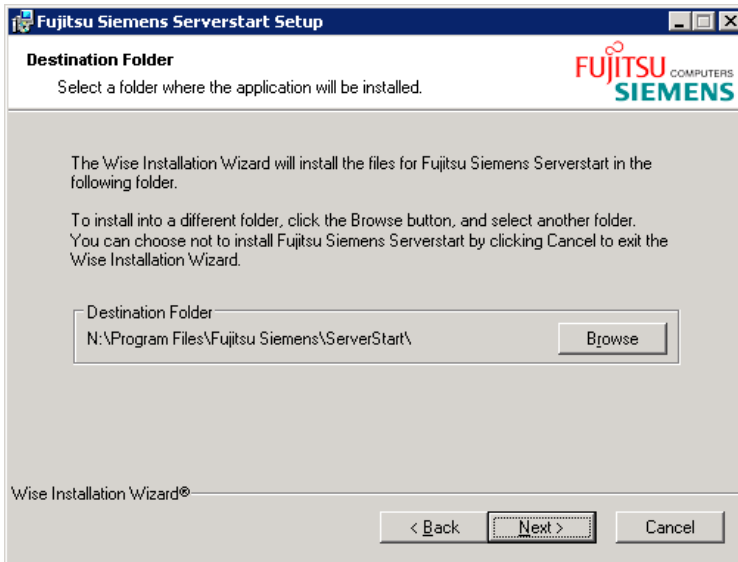
- Click the *Next* button.



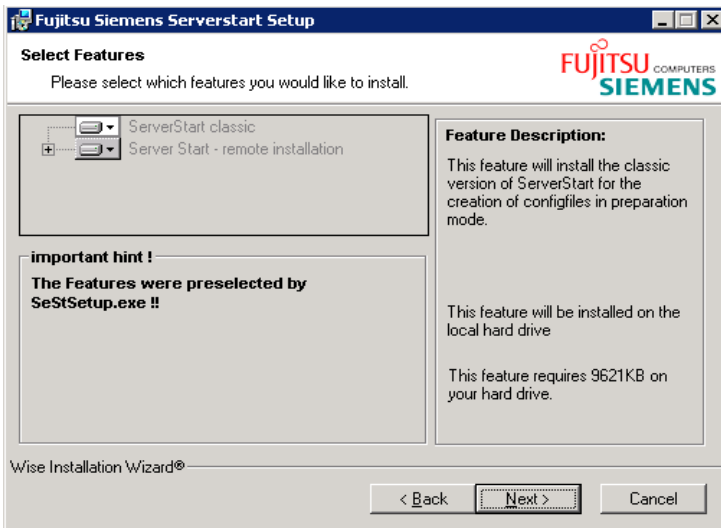
- To accept the license agreement, select the appropriate checkbox. Click the *Next* button.



- Enter your name and the name of your company. Click the *Next* button.

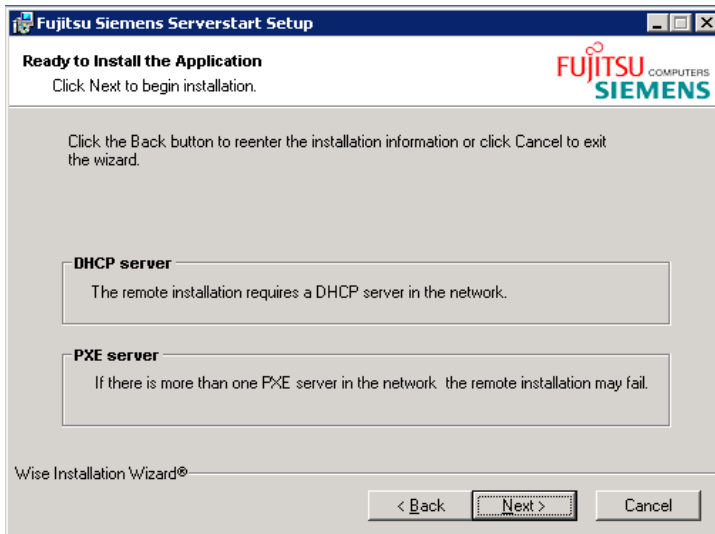


- Specify the directory on your hard disk drive to which ServerStart (the Server Start core) is to be installed. Click the *Next* button.





- Displays the functions you want to install. Click the *Next* button.



- Click the *Next* button to start the installation.

You can call the ServerStart application from the Windows Start menu.

## 9.1.2 Installing a Server Blade

In this section you will find an overview of the steps necessary to install a server blade. Further information can be found in the ServerStart manual.

### 9.1.2.1 Remote Installation From the Deployment Server

#### Phase 1: Defining the System Configuration



This phase can be performed on any Windows system.

- ▶ Install ServerStart/Installation Manager as an application on a Windows computer. Windows 2003 and Windows 2008 (as of version 7.804) are suitable operating systems.
- ▶ Select the functions that you want to install.



The *Remote Installation* program module must be installed (default setting) for remote installation of Windows and Linux to be possible.

- ▶ Call ServerStart/Installation Manager via the link created in the Windows Start menu during installation.
- ▶ In the structure view (*Tree View*), choose the required operating system.

- ▶ Run the configuration wizards in the specified order:

- Server Configuration Wizard
- RAID and Disk Wizard
- Operating System Wizard
- Application Wizard



Enter the location of the installation sources for the operating system, service pack and add-on application media in the form of a network path in UNC notation.

- ▶ Save the configuration file created during the configuration phase under a name of your choice (default name: *SerStartBatch.ini*).

### Starting the Remote Installation



The target hardware settings must have been made via the BIOS setup in PXE boot mode. In the case of blade servers, this can also be performed remotely via the management blade's HTTP user interface.

- ▶ Select the menu option *Remote Installation*.
- ▶ Choose the menu item *Click here to initiate the Remote Installation* process in the tree view to start installation. To do this, you must enter the following specifications:
  - The path name of the required configuration file (local or remote)
  - MAC address of the network card at the target server system via which the installation is to be performed. (For information on determining the MAC address, see [section “Install Your Server Blade Remotely” on page 221.](#))
  - Used PRIMERGY model, number of processors (in order to determine the correct boot kernel)

ServerStart/Installation Manager is booted remotely via the PXE protocol. Unattended installation is then started directly on the target hardware as in guided mode.

The *System Preparation* and *RAID Configuration* processes start.



A system restart may be initiated in order to activate the RAID cluster. The system is then booted again via PXE and installation is continued.

The hard disk drives are partitioned and formatted.

The operating system CD is automatically mapped via the specified network drive. The required installation data is copied to the target drive.

The service pack and application packages are automatically mapped via the specified network drive. The required installation data is copied to the target drive.

The subsequent installation operation now runs unattended provided that all the configuration parameters for installation of the operating system have been defined in the wizards. Any missing specifications are requested locally via the OS installation routine.


Any system restarts that are necessary after OS installation in order to install the applications and the middleware are performed automatically.

The server system is now configured and ready for operation.


### 9.1.2.2 Install Your Server Blade Remotely

**Remote Installation Target System**


To be able to initiate a remote installation process ServerStart needs some data:

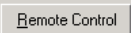


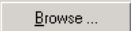
**Target system**

MAC address of target system:  

(The MAC address can be obtained via FSC ServerView, or by reading the console output during the boot process of the target system with PXE option switched on)

PRIMERGY model type:  



Configuration File:  

**Access to ServerStart data:**

ServerStart contents tree (UNC):


User name for remote access:

**Password confirmation:**


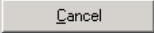
**Remote Installation Linux**

☐ Select floppy image boot

Boot image directory

Bootstrap Loader  

☒ Remote installation incl. SCU settings and/or RAID configuration



Mandatory field that have not yet been filled out, are colored yellow.

- You must specify the MAC address of your server blade.

There are several ways to find out the MAC address of a server blade:

- If you have already configured the access via the management blade, you can use the management blade's Web interface via the following address:

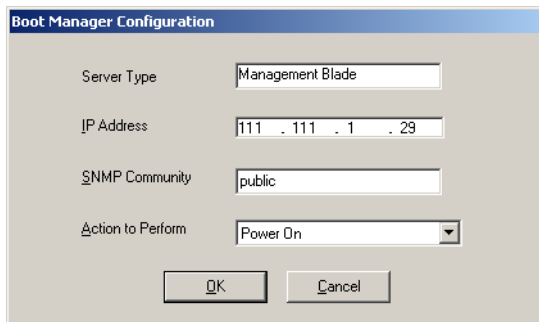
*http://<IP address of the management blade>*

default user: *root*; default password: *root*

Go to the menu *Deployment Parameter* and copy/paste the MAC address of the server blade.

- You can also unplug the server blade and read off the imprinted MAC address from the MAC/iSCSI address label on the rear side of the server blade.
  - You can start the server blade and read off the MAC address on the information screen of the BIOS.
- Select the appropriate blade server model from the *PRIMERGY model type* drop-down list.

The *Remote Control* button to the right of this list is enabled. You can define and execute the type of reboot via the *Boot Manager Configuration* menu.



The screenshot shows a window titled "Boot Manager Configuration". It contains four labeled input fields: "Server Type" with a text box containing "Management Blade", "IP Address" with a text box containing "111 . 111 . 1 . 29", "SNMP Community" with a text box containing "public", and "Action to Perform" with a dropdown menu showing "Power On". At the bottom of the window are two buttons: "OK" and "Cancel".

In this window you can specify the IP address of the management blade.

You can select an action to be performed (*Action to Perform* drop-down list) by the management blade:

- *Power On*: The server blade is switched on.
  - *Power Off*: The server blade is switched off.
  - *Normal Boot Mode / PXE Boot Mode*:  
The corresponding boot setting is made in the BIOS of the target server and the boot process is not executed.
  - *Shutdown*: The server blade is shut down.
  - *Normal Boot / PXE Boot*:  
The corresponding boot mode is set in the BIOS of the target server and the boot process is executed as stipulated.
- ▶ It is important to choose the correct type of processor system (mono or dual), otherwise the installation process will fail (XP uses different boot kernels for mono and dual systems). Current server blades usually have a mono processor system.
  - ▶ Enter the location of the configuration file which should be used for the installation.
  - ▶ Enter the location of the ServerStart/Installation Manager data and define a user name and user password for remote access.



You must type the password twice in the password text box. Press the tabulator key once between the two inputs. If you only type the password once, then this box will be colored red. In this case, repeat the input.

- ▶ Click *Start Installation*.



The ServerStart/Installation Manager Remote Boot Manager is now waiting for a PXE request from the target system (your assigned server blade).

- ▶ Make sure that, under *Boot Options* in the server blade's BIOS setup, *PXE-LAN-1* or *PXE-LAN-2* is set. You can configure the boot options either via the Web user interface of the management blade or via local BIOS Setup frames.

Take care that the chosen LAN device is connected to the same LAN segment (only with the deployment method *Multicast*) as the deployment server (check especially in a VLAN configuration).

- Start the server blade via PXEboot.

Again there is more than one way to do this: By using the server blade's power switch or remotely via the Web user interface of the management blade (see "Management Blade" guide under *Recovery - Power Control*).

The started server blade will be installed completely unattended, as will the operating system and the selected applications and service packs.

A status window is displayed showing you the progress of the installation process.



## 9.2 Image Creation Process

To create and save images for cloning, you use Deployment Manager (see [section “Creating an Image” on page 226](#)).

First you must prepare a server as deployment server for cloning, see [section “Deployment Server” on page 43](#).

Detailed information on the Deployment Manager is given in [chapter “Using Deployment Manager” on page 77](#).

### 9.2.1 Preparing a Deployment Server for Cloning

As deployment server for cloning you can choose any Windows 2000 or Windows 2003 server.

- If you want to locate the image repository on this server, make sure there is enough disk space to hold the images and configurations for the server blades.
- The deployment server must be added to the server list of ServerView.
- In this example it is assumed that Deployment Manager and Operations Manager are installed on the deployment server.

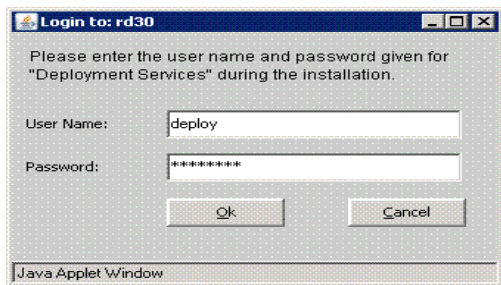
## 9.2.2 Creating an Image

- ▶ Start Operations Manager. How to start Operations Manager is described in the “Operations Manager” manual.
- ▶ Select in the Operations Manager main window in the menu bar the entry *Deployment – Deployment Manager*.

The Deployment Manager start window opens. Click the *Start* button. Once Deployment Manager has started, the *Select Deployment Server* window opens.

- ▶ Select a deployment server. If the list of deployment servers is empty, you must define one. Activate the *New* button. A new window opens displaying all servers in the ServerView server list. Select the server on which the *Deployment Services* package are installed.

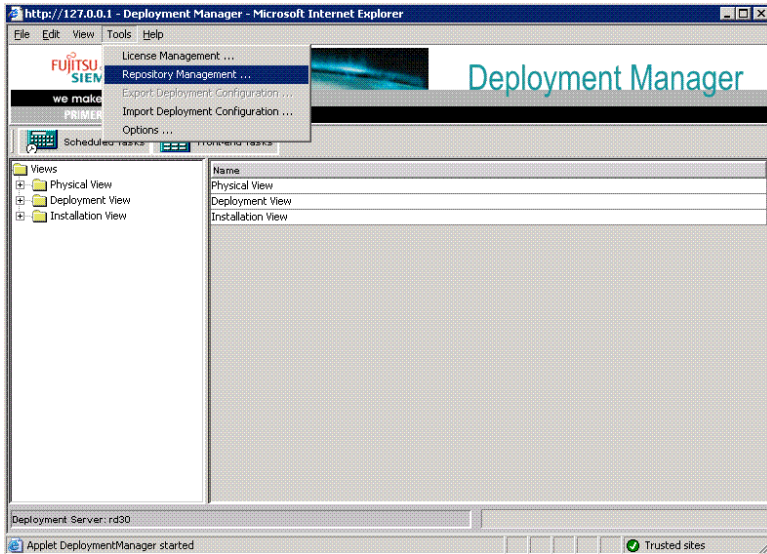
When you have selected the deployment server, a login window opens:



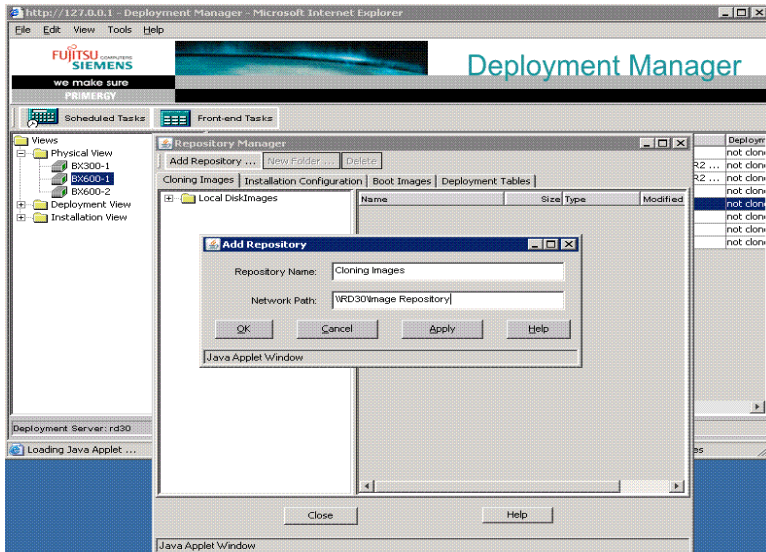
- ▶ Enter the user name and password of the account that you specified during installation of the deployment services and click *Ok*.

Before you create an image you must specify the image repository.

- Select *Repository Management ...* from the *Tools* menu.



- ▶ Select *Add Repository* in the *Repository Manager* window. In the *Add Repository* window enter the repository name and the network path. Click *Ok*.



If it is the first time you are saving an image, no image repository might have been defined yet. In this case you must define one:

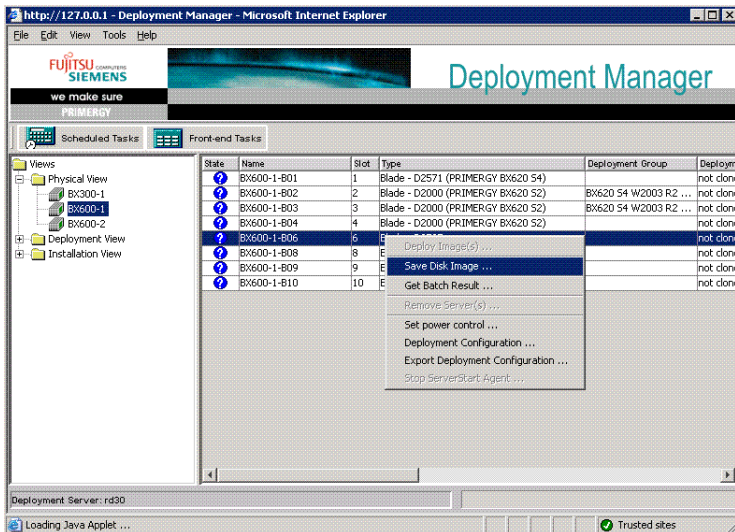
- ▶ Create a directory on your deployment server (or on another server in the LAN segment) where you want to store the images.
- ▶ Share this folder so that it can be accessed remotely.

**i** The user account specified during installation of the deployment services as well as the user account specified during installation of Deployment Manager must have full control of this share.

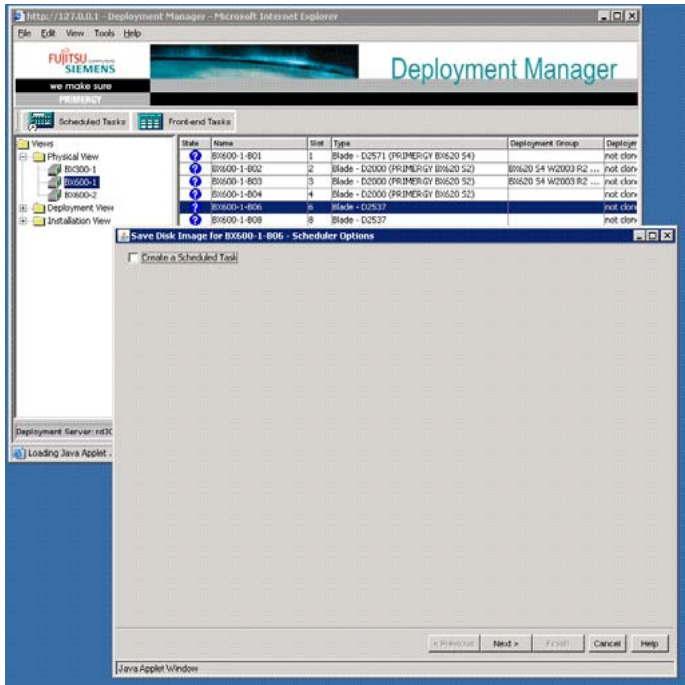
- ▶ In order to register this share as a repository in Deployment Manager, click the *Add Repository* button. You must specify a repository name and the network path name to the share. Then click *OK*.

In order to save the installation of one server blade to an image, open the *Physical View*.

- ▶ Select the blade system where this server blade is located. To allow this, the blade system must be in the server list of ServerView.
- ▶ In the list on the right-hand side, select the server blade (reference system). To create an image of the server blade, press the right mouse button and select the *Save Disk Image ...* entry from the context menu.

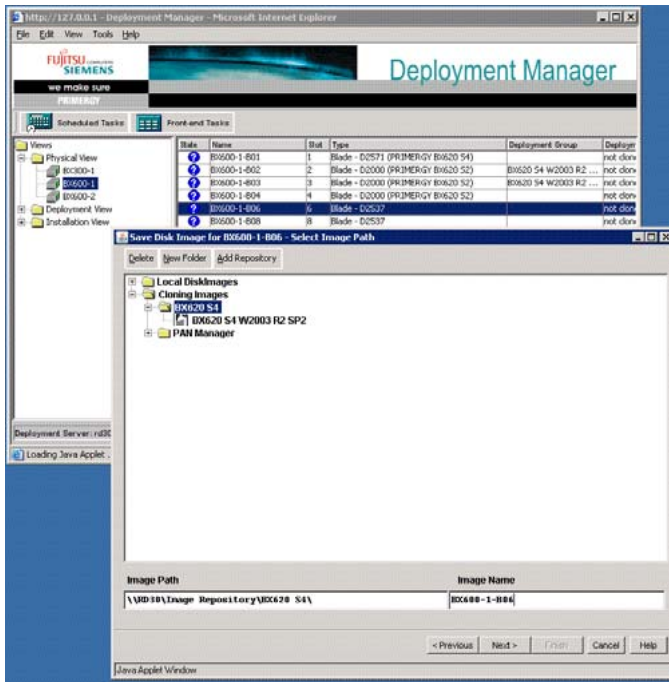


Now the window with the *Save Disk Image* wizard opens for the selected server.



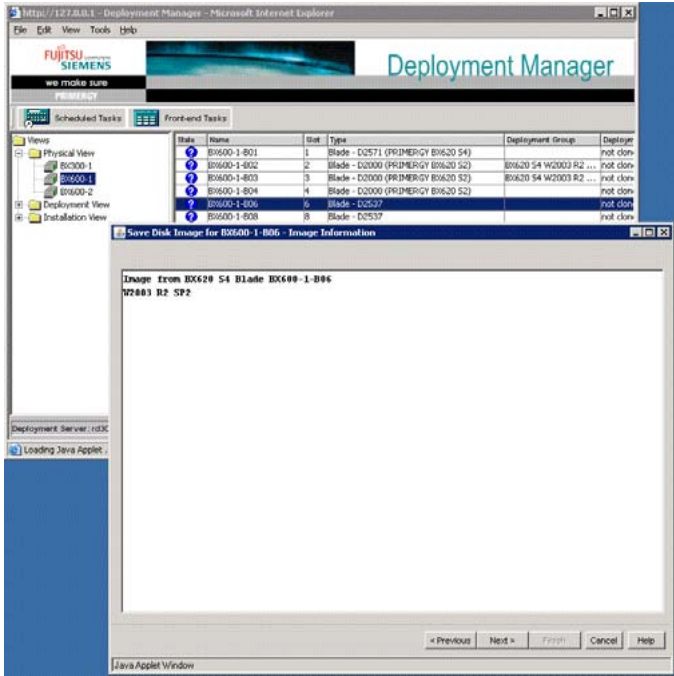
- In the first step do not mark the *Create a Scheduled Task* check box.

- Click *Next*. This displays the *Select Image Path* window.



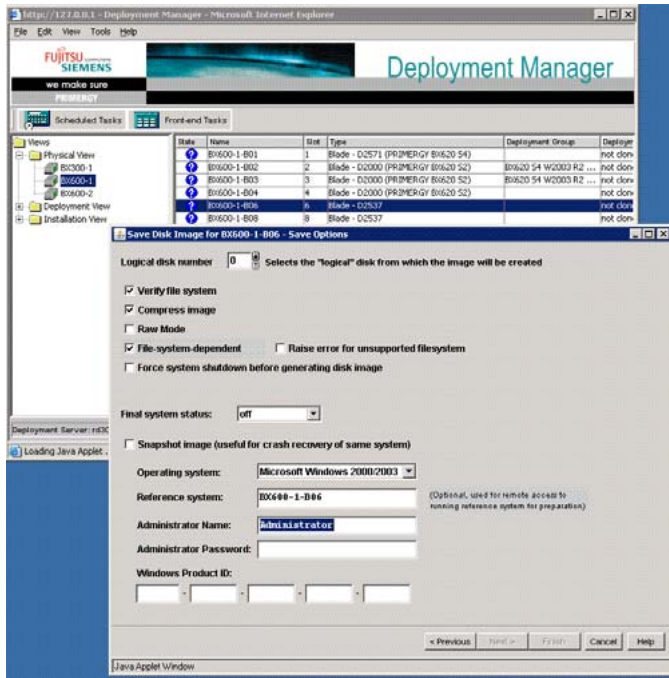
- Select the name for the image file and also the path where the image is to be saved (image repository). If necessary, add a new folder to save the image to your image repository.

- ▶ Click *Next*. This displays the *Image Information* window.
- ▶ Give the image a description. You can enter any text that you want to be saved together with the image file.





- ▶ Click *Next*. This displays the *Save Options* window.
- ▶ Choose the operating system and enter the necessary information for the image.



**i** Do not select the *Snapshot image ...* option if you want to use the created image for cloning other server blades.

#### Verify file system

The file system is verified before image generation if this option is selected.

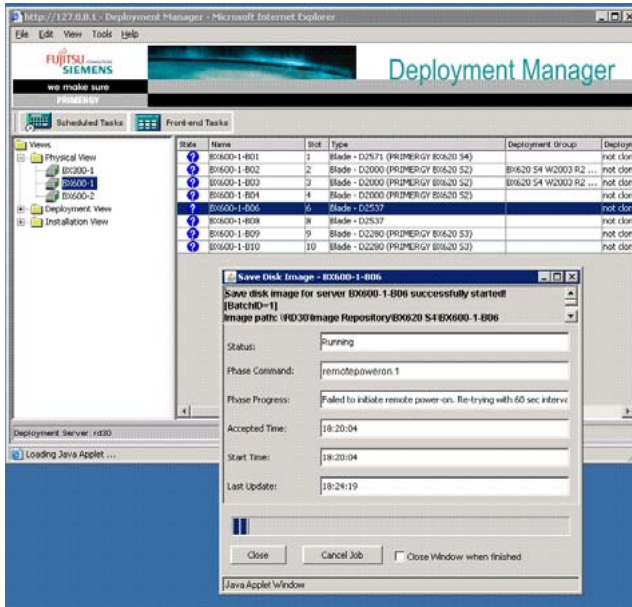
#### Compress image

The generated image will be compressed during generation if this option is selected.

### File system dependent

If this option is selected, only the used blocks of a file system will be saved in the image. This functionality is supported for the following file systems: FAT, FAT32, NTFS, NTFS5, EXT2, EXT3. If a disk contains several partitions, for non-supported file system types the whole partition, including the unused blocks, will be saved. For the partitions with a supported file system, only the used blocks will be saved. This reduces the size of the image files and also increases the speed of the image generation. If you want to restore an image on a disk that has a different size than the source disk, this option should be specified.

- ▶ Start the image creation by selecting *Finish*. A status window is displayed showing you the progress of the image creation process.



The image generation of a Windows 2000 system for cloning (not snapshot) requires that the host name and IP address of the reference system are correctly specified in the deployment table of the management blade. You can make the deployment configuration via the Deployment Manager (see section 9.3.1 on page 235).

## 9.3 Deploying an Image to Server Blades

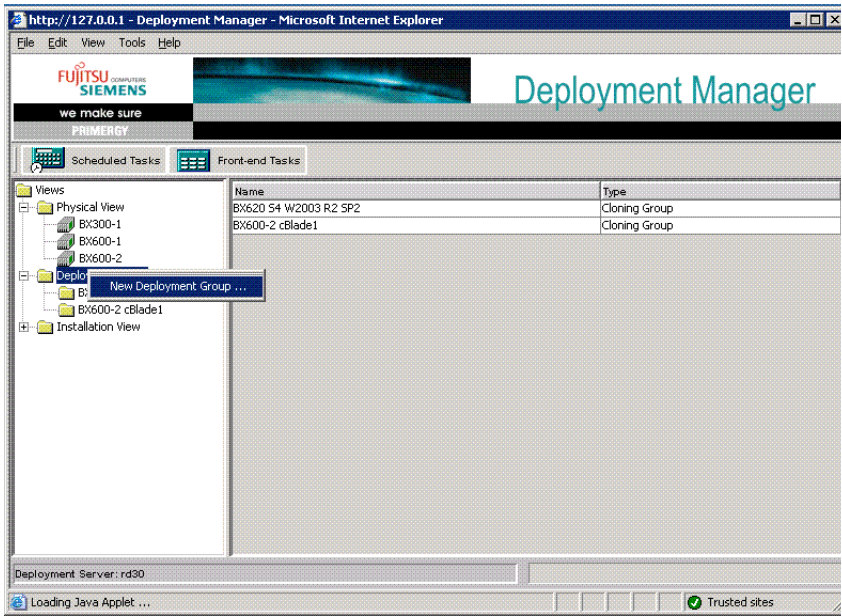
The deployment of images to server blades is done in three steps:

1. Define a deployment group (see [section “Configure a Deployment Group” on page 235](#)).
2. Configure the target systems (see [section “Configuring the Target Systems” on page 239](#)).
3. Transfer the image to a group of server blades to be installed (see [section “Cloning: Deploying an Image to Server Blades” on page 241](#)).

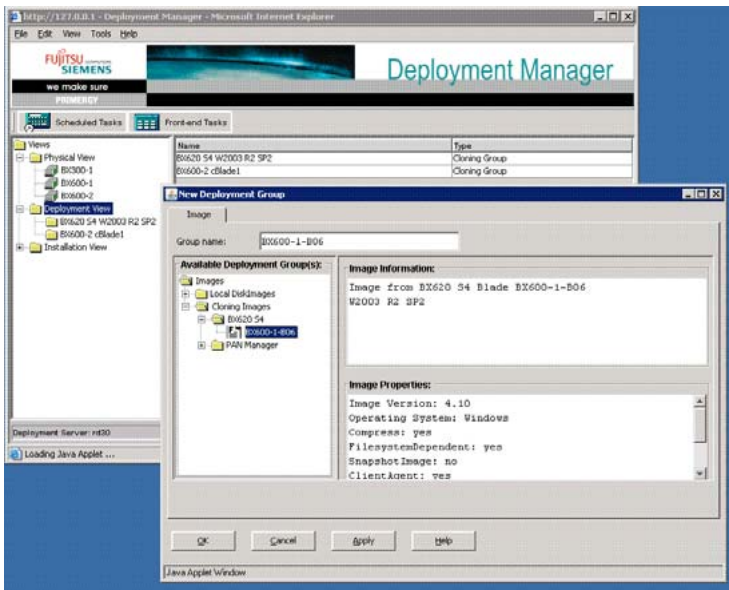
### 9.3.1 Configure a Deployment Group

A deployment group is defined by selecting an image from your image repository and assigning server blades to this image.

- To define a deployment group, select the *Deployment View*, press the right mouse button on the *Deployment View* item and select *New Deployment Group ...*



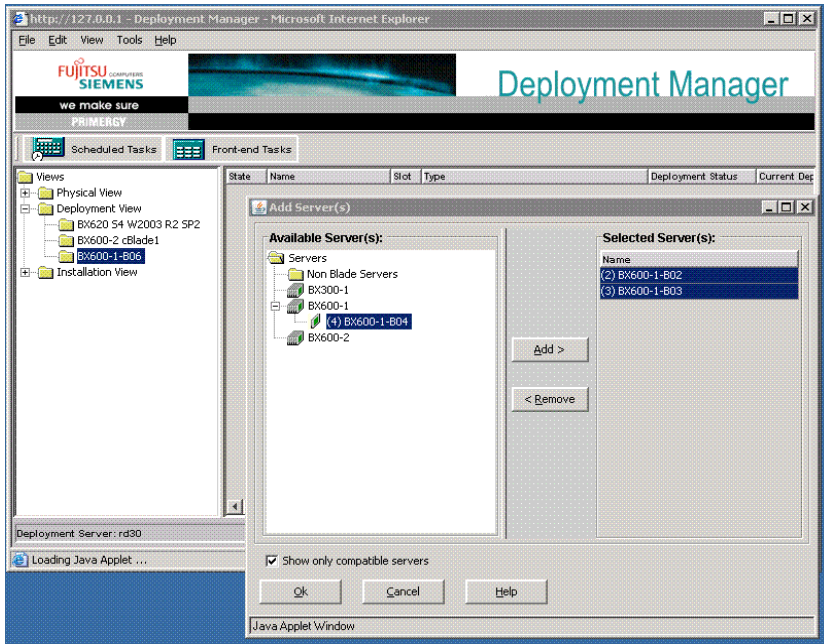
The *New Deployment Group* window opens.



- From your image repository, select the image you want to clone to other server blades and click the *OK* button. This creates a new deployment group to which the selected image is assigned.

In the next step you add server blades to this deployment group:

- Press the right mouse button on the tree node for the new deployment group and select *Add servers ...* . This will result in the new *Add Server(s)* dialog.

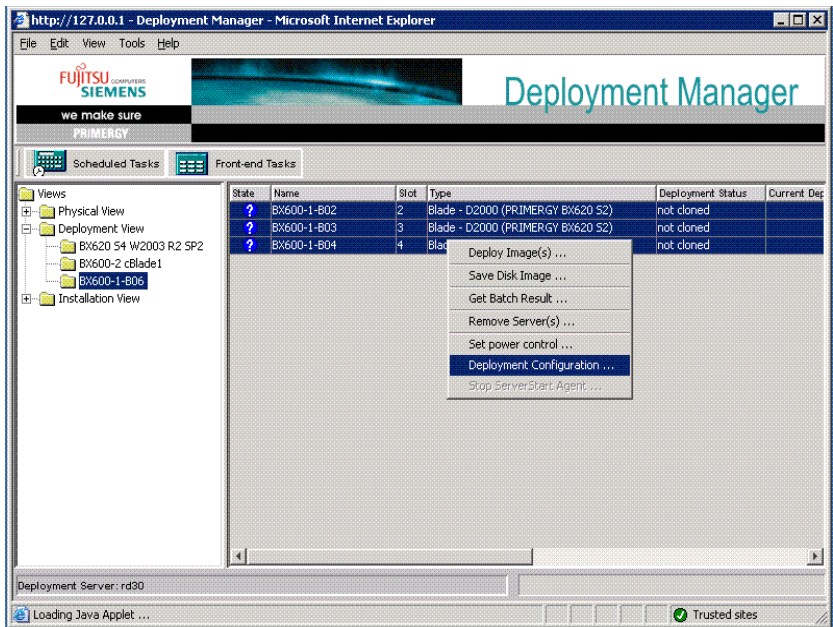


- Use the *Add* button to select the server blades you want to deploy with the image.
- To confirm your selection click the *Ok* button. The selected servers are assigned to the deployment group and the dialog is closed.

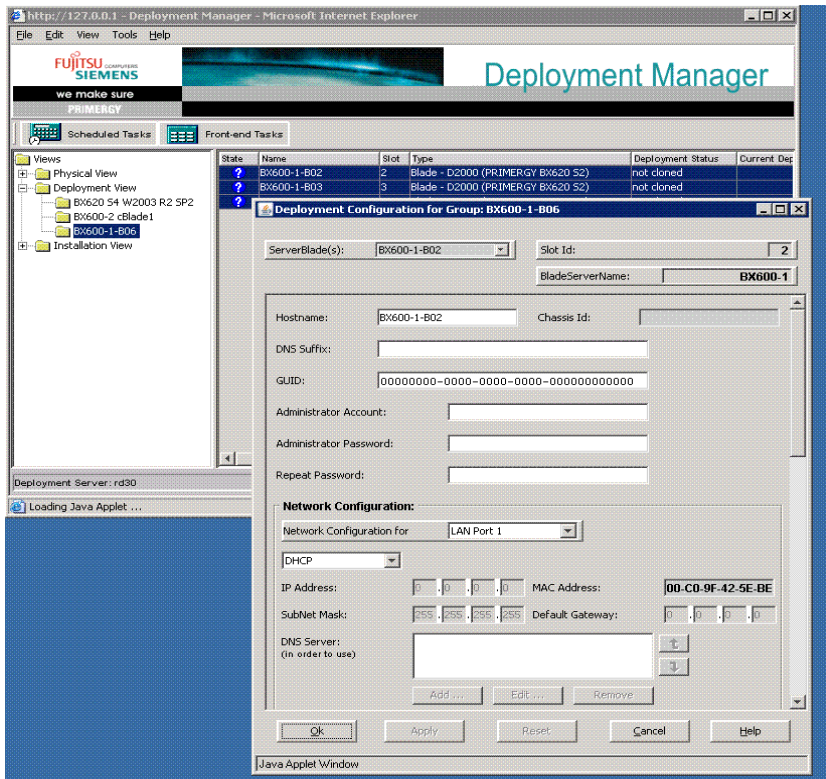
## 9.3.2 Configuring the Target Systems

Before deploying the image to server blades you need to do some configuration. You must specify the host name and the IP settings for the cloned systems.

- ▶ To start the deployment configuration select the relevant server blades. Press the right mouse button and select *Deployment Configuration...* from the context menu. (This feature is supported as of RemoteDeploy V1.10.01. With older versions: Configure the server blades via the user interface of the management blade, see “Management Blade” guide.)



This will open the *Deployment Configuration* window for the selected deployment group:



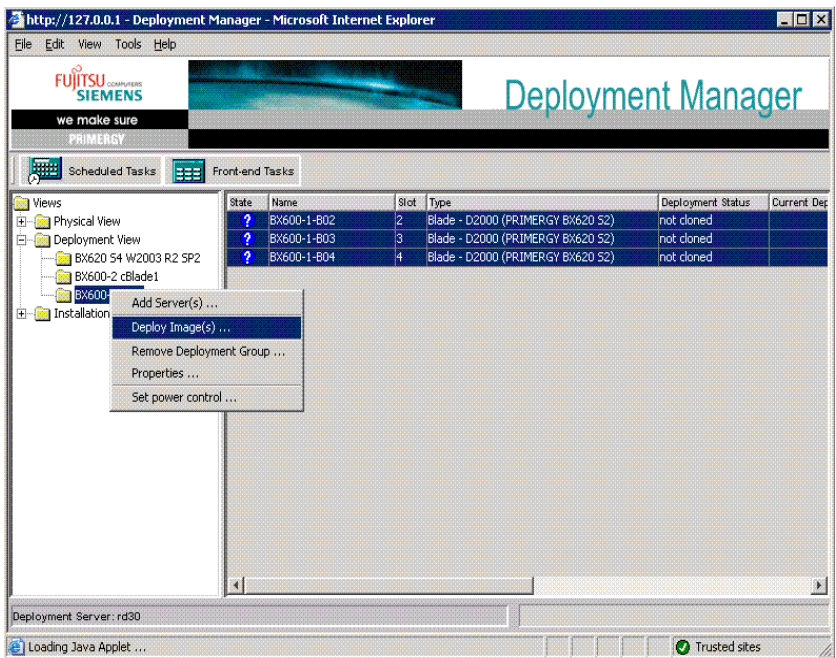
- Specify a unique host name for all server blades in the group.
- Configure the IP settings for each server blade for the first and second LAN port. You will need to decide whether you want to use DHCP for a LAN port or whether you want to have static IP addresses for a LAN port which are manually assigned. If you want to use DHCP, select the corresponding option. In that case you do not need to specify an IP address, subnet mask or gateway. If you want to use manually assigned IP addresses, you must select the option *Non DHCP*. In that case you must specify a unique IP address and a valid subnet mask.



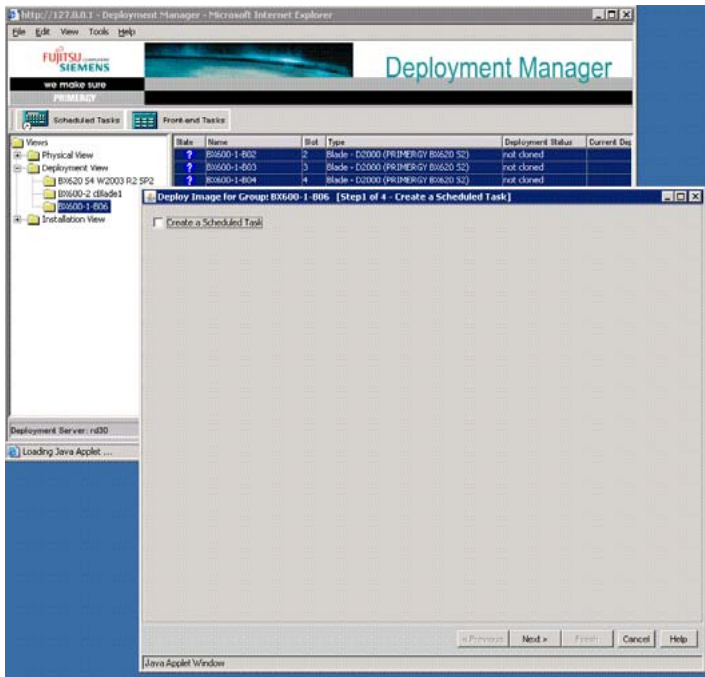
- In addition you can specify for each blade the LAN port via which the blade is reachable for the deployment process. To do this, use the option *LAN Port for PXE boot*. By default this is LAN port 1.
- Use the *Apply* button to save the configuration for each server blade, and use the selection list at the top left of the window to select the next server blade.

### 9.3.3 Cloning: Deploying an Image to Server Blades

- To deploy all blades in the deployment group with the specified image, select the deployment group in the deployment view, press the right mouse button and select *Deploy Image(s) ...* .

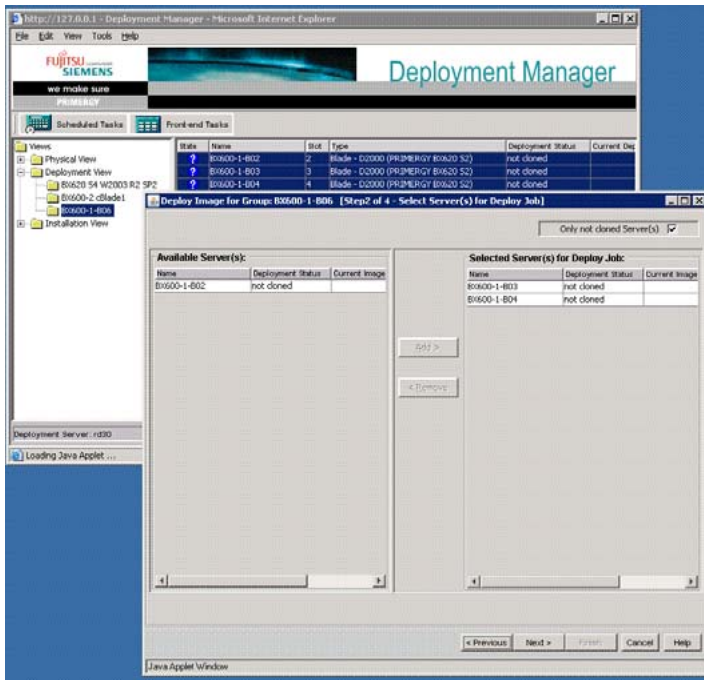


This opens the window with the *Deploy Image for Group: <group>* wizard.



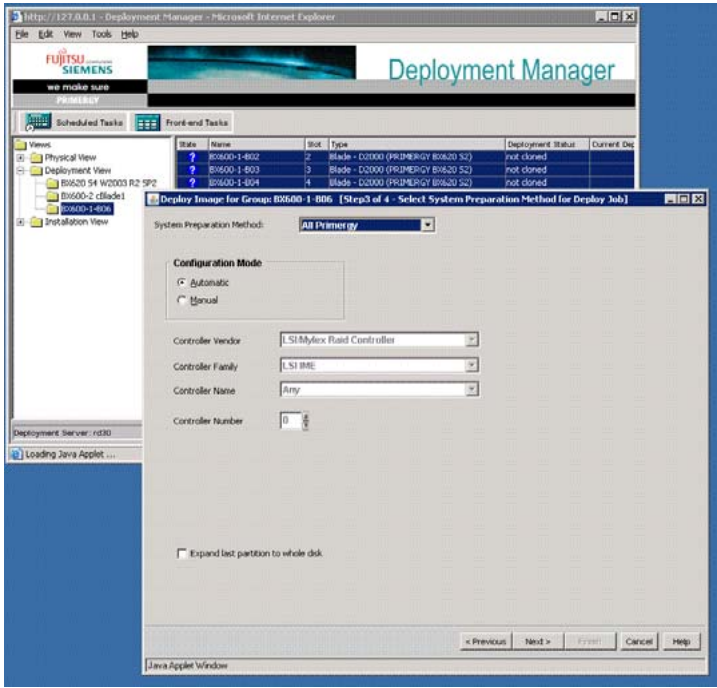
- In the first step do not mark the *Create a Scheduled Task* check box.

- Click *Next*. This will open the *Select Server(s) for Deploy Job* window.



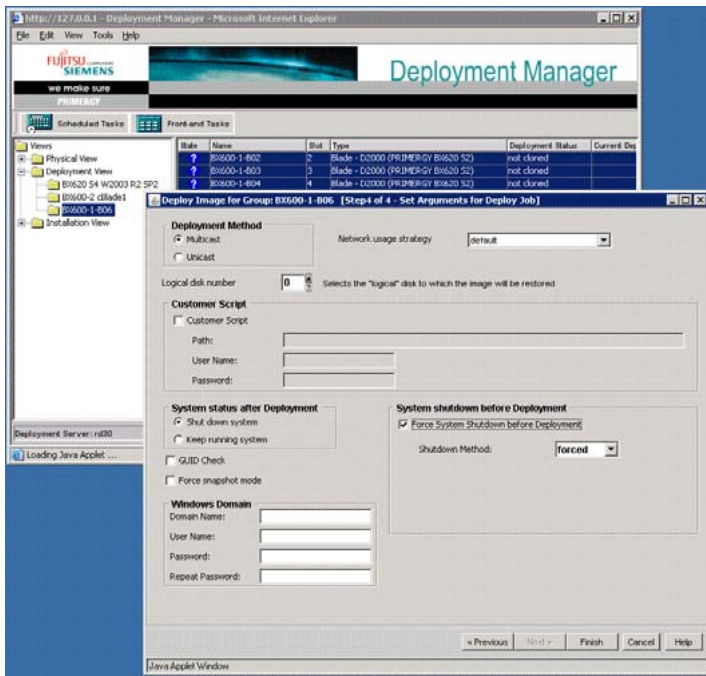
- Choose the server blades to be installed. Servers in the right-hand list can be moved to the left-hand list and vice versa. Depending on the cloning status of a server blade, the left-hand list will be affected by the *Only not cloned Server(s)* option at the top of the window.

- Click *Next*. This opens the *Select System Preparation Method for Deploy Job* window.



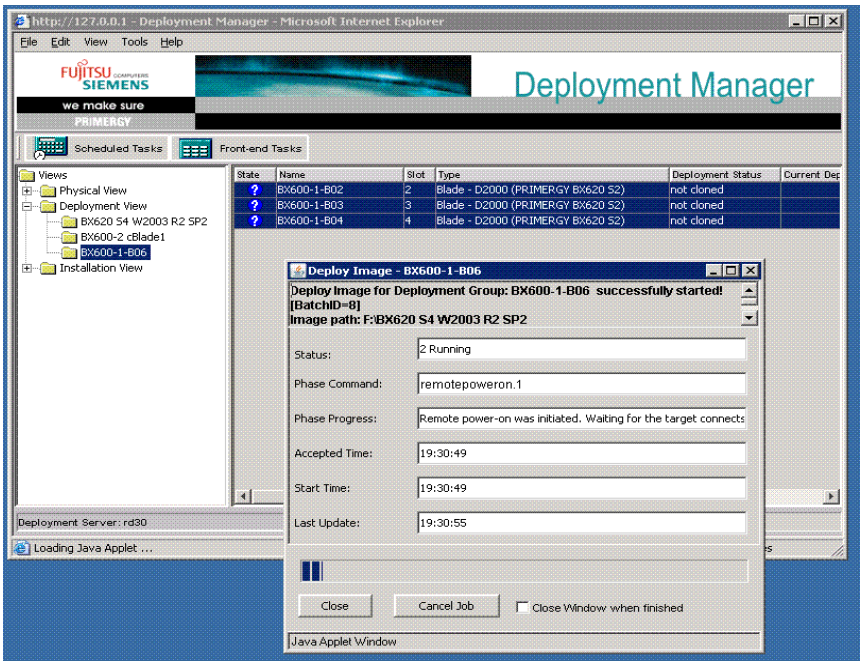
- Select the system preparation method *All Primergy* (when the deployment platform is WinPE MDP) or *Blade optimized* (when the deployment platform is Caldera DOS).

- Click *Next*. This opens the *Set Arguments for Deploy Job* window.



- Select the deployment method *Multicast* or *Unicast*. Default value is *Multicast*.
- Mark *Force System Shutdown before Deployment*.
- Click the *Finish* button to start the deployment.

All servers in the right-hand list will be installed. A status window is displayed showing the progress of the deployment process.



## 9.4 Installing SNMP Agents

If you intend to manage the server blade via Operations Manager or Deployment Manager, you must install *SNMP Agents*. As of ServerStart/Installation Manager version 5.304 you will find the SNMP agents on the PRIMERGY ServerView Suite Software CD.

- ▶ Place the PRIMERGY ServerView Suite Software CD in the CD-ROM drive. If the CD does not start automatically, click the *start.html* file in the CD's root directory.
- ▶ In the tree view, select *ServerView Suite – ServerView Agents*.
- ▶ On the right side choose the relevant SNMP agent by clicking the *\*.exe* entry in the *File* column.

### Starting the installation in Internet Explorer (Windows) and in Opera

- ▶ In the *File Download* window, select the option *Run this program from current location* (Internet Explorer) or *Open file* (Opera). Then confirm the subsequent certificate information (Internet Explorer only).

### Starting the installation in Netscape

- ▶ In the dialog window that appears, create a new directory on the hard disk in which the installation file is to be saved from the CD-ROM. Then run the installation from this location.

Operations Manager, Update Manager and Remote Management and others are also part of the PRIMERGY ServerView Suite Software CD.





---

## 10 Deployment Process Details

Operations Manager creates (via SNMP) a server list of physical clients with their MAC addresses (one per LAN port). This list is displayed in the Deployment Manager front-end (the servers are arranged in physical groups depending on their type).

If there are many physical groups, additional logical groups must be created based on the physical information. For cloning, deployment groups must be created which can be assigned to a cloning image that may contain an installed application. For remote mass installation, groups are formed for the assignment of configuration files created by ServerStart/Installation Manager.

Each group has its own set of attributes (parameters). The attributes for a member of a physical group are basically defined in the deployment table and are used for identification (MAC address) and LAN configuration of the client cloning. The MAC address of the server or management blade is required to allow Deployment Manager to access the initiating functions such as PXE reboot. This deployment table is always the definitive reference for the current status of the servers. Deployment Manager always uses the parameters from this table. This helps to show the same status of each server if more than one Deployment Manager front-end has been started. If one front-end has initiated a job on a particular server, other front-ends cannot access this server as long as the jobs are running. The deployment table is described in detail in [section “Handling the Deployment Table” on page 274](#).

Once a server is cloned or installed and the operating system is running with operating system agents from Fujitsu Siemens Computers, the agents will update the LAN parameters frequently (every 10 seconds) each time the administrator changes them in the operating system itself. This is done automatically unless DHCP mode is used for the operating system.

It is advisable to change LAN parameters carefully while the operating system agents are still running. Alternatively the operating system must be shut down or the agents must be stopped manually in the operating system.

Once a logical group is defined consisting of a list of servers, a particular image or configuration file can be assigned to that group. The attributes of a logical group are defined to control the deployment process itself in defining the parameters:

- UNC path to master image
- target RAID level (RAID 0, 1 or 2 x RAID 0)
- file system formatting type

## 10.1 Cloning Deployment Process



The following description of the cloning deployment process assumes that the deployment platform *Caldera DOS* is used.

A cloning session consists of several phases and offers different alternatives to be used for each phase:

1. Power control, i.e. remote PXE boot of target server
  - Initiated by *RemControl.dll* (default for ServerView Suite)
  - Initiated by SNMP commands accessing management blade or ServerView agents
  - Initiated by IPMI commands via Kalypso BMC
  - Initiated manually
2. System preparation
  - Via DOS agent at cloning (used by Haribote for server blades)  
Concerns unattended RAID preparation of blade controller only.
  - Via ServerStart/Installation Manager based on WinPE PXE boot
    - SCU Server Management settings in SM-BIOS
    - Unattended RAID preparation for all PRIMERGY servers
  - Boot of system preparation images created by yourself (as used for ADS)  
All actions applicable on a DOS or MiniLinux platform boot are possible. You will need to obtain appropriate tools yourself to make the system preparations on the target server.
  - Manually by the administrator
    - via ServerStart/Installation Manager in expert mode locally
    - via BIOS extensions of PCI controller in server boot phase
    - via Remote Management remote console
3. Clone of an image

All physical clients of a deployment group are cloned with the assigned image. Image-related actions can only be activated on logical groups.

If a server was removed from one logical group and is to be moved to another logical group, the *Status of Cloning* reflects whether the newly assigned image is already cloned or not. If not, and Deployment Manager is closed and restarted, it will not be reassigned to the old group because of the new image reference, but will be identified as a cloned client of that group.

#### 4. Post-preparation phase

- Individualization of a clone via
  - LAN parameters
  - host name
  - Microsoft Windows system ID: SID
- Start of customer scripts
  - ServicePack/Quickfix update
  - Driver update
  - Install applications/services
  - Configuration of operating system or application, e.g. Windows scripting

These phases are described in more detail in the following sections.

The figure below shows an overview of the phases during a cloning process.

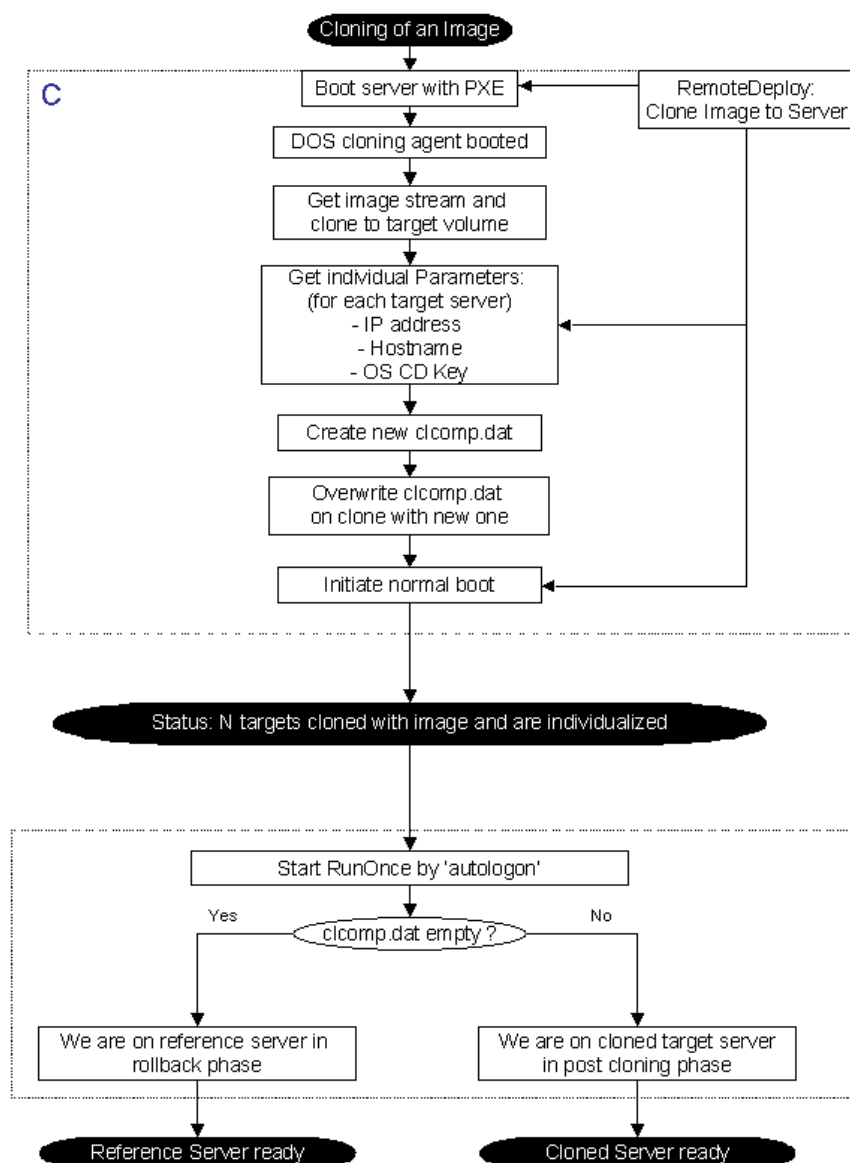


Figure 72: Deployment phases - Overview

As an example these are the basic deployment steps for a blade server system:

1. The blade server chassis is powered on and the management blades start discovering the hardware environment (number of server blades, switch blades and status of redundant second management blade).
2. On request, Operations Manager searches the LAN to find all present management blades in one segment.
3. Deployment Manager retrieves the list of management blades found from Operations Manager and requests a list of system information directly from the management blade about each blade server installed in a blade chassis.
4. Deployment Manager offers the administrator a physical server list based on the management blade information to create logical server groups based on the system information received.
5. The administrator may change these logical groups by adding or changing logical-group-specific parameters, and finally he/she activates a deployment process on a logical group.
6. Deployment Manager creates a list of related server blades and their MAC addresses and generates a cloning job for the cloning engine.
7. The cloning engine identifies each physical server blade on the LAN if required. It prepares LAN switch configurations for PXE access and initiates a Unicast or Multicast cloning process on each client.
8. The cloning engine contacts the management blade via *RemControl.dll* to initiate a PXE reboot of each related server blade.
9. The server blade PXE BIOS contacts the deployment PXE server to receive the first DOS boot image and starts that image containing the cloning agent.
10. The cloning agent prepares the server blade hardware like a RAID array and downloads via TFTP a second master image directly onto the prepared storage volume, which is reachable via an Int13h BIOS call with the logical device ID: 0.
11. The final clone will be patched for individual operating system parameters such as IP address, host name and system ID (Windows only).
12. The cloning agent initiates a normal reboot of its current server blade.

13. The final operating system boots:

- a) In the case of Linux, cloning is done by activating new LAN settings at run level 0.
- b) In the case of Windows, a RunOnce script is started to activate Microsoft system preparation and probably a customer script for additional configuration steps.

With RemoteDeploy V3.0 this is done by controlling the post-preparation phase using a temporarily installed agent.

### 10.1.1 Power Control via Remote Control

The remote control API (*RemControl.dll*) is used to initiate requests to the target server especially for power control and detection of servers. The service processors such as management blade (SNMP) and Kalypso (IPMI) access are supported via *RemControl.dll*.

For PRIMERGY servers which support none of these service APIs, a corresponding dialog is displayed on the Deployment Manager front-end to make the user initiate tasks manually instead of remotely. The advantage of this is that the program using the *RemControl.dll* always uses the same API.

By using the *RemControl.dll*, the ServerView suite provides a common API for power control of servers regardless of their managed server type. The different types of access are managed inside *RemControl.dll*, but the user of the API must offer the appropriate parameters used to enter each BMC-API.

#### Management Blade Power Control

The management blade requires the following parameters to access the power control functions:

- Management type = MMB
- IP address or host name of BMC (used by *RemControl.dll*)
- SlotID
- SNMP community string
- Timeout of access BMC API
- Number of retries to access BMC

For accessing the BMC by IP address or host name, Deployment Manager must be installed. (The *Deployment Manager* service is used to determine the MAC address via its Deployment Manager database.) If you use the MAC address for the same function, the *Deployment Manager* service is not necessary. If you use the MMB control, PXE boot mode can be initialized and ACPI PowerOff is supported.

### 10.1.2 System Preparation Phase

The real cloning process is independent of the server configuration. It just requires a server to have the following attributes:

- The server is in PXE boot mode or can be booted in PXE mode remotely.
- A DOS image with a minimum size of 1.44MB can be booted via PXE.
- One or more BIOS devices are available based on Int13h (which of them is used for cloning is selected by its logical device ID; default is Log-ID: 0).
- The deployment server is available over the whole cloning cycle via LAN.

A system preparation phase occurs immediately before the cloning to set up, for example, a RAID array on the target server.

Deployment Manager provides the following alternatives:

- Manual preparation
- Automatic preparation as part of a DOS session
- Preparation based on WinPE
- Customer system preparation image

## Manual Preparation

Within Deployment Manager nothing is done for system preparation. The Deployment Manager continues directly with the generic cloning job. The administrator must make sure that the attributes mentioned in [section “Power Control via Remote Control” on page 254](#) are implemented and a logical Int13h device is reachable via BIOS on DOS.

A typical method of RAID configuration is to use the BIOS extensions offered by each RAID controller using a key combination in the BIOS boot phase.

If remote PXE boot is not applicable, the BIOS boot device table must have the PXE boot device configured statically as the first boot device. In this mode, the PXE server can control whether a PXE boot will be performed or whether a PXE timeout will occur and the boot process will continue with the next boot device in the list (which should be the hard disk containing the final cloning image).

Server Management BIOS settings or Server Management configurations usually done by the SCU of ServerStart/Installation Manager must also be made manually (if required for the operating system; this is not required for Deployment Manager).

## Automatic Preparation as Part of a DOS Session

This is the standard preparation used for blade servers only as provided by the Haribote cloning engine.

The DOS session for cloning a blade server is usually split into two boot phases in the case of a RAID configuration:

1. Booting the cloning agent on DOS via PXE.
2. Starting a vendor DOS tool for detection of storage devices and initiating the defined RAID configuration.
3. Initiating a second PXE reboot which boots the DOS cloning agent again.

Now the system BIOS can support access to the new RAID array based on an Int13h device call. The cloning process will start on this prepared logical device.

4. A final normal reboot finalizes the cloning session by entering the post-cloning phase.



The RAID preparation is the only system preparation done by the Haribote cloning engine in Deployment Manager. This method is not used for non-blade servers. The *FSC Deployment Manager* service differentiates between blade and non-blade servers.

### Preparation Based on WinPE

For system preparation of all PRIMERGY servers, the preparation modules of ServerStart/Installation Manager are used.

The *FSC Deployment Manager* service calls the ServerStart/Installation Manager Extension via an API as described in [section “Software Architecture” on page 38](#).

The ServerStart/Installation Manager module stack for remote installation is extended by a separate module management controlled by the ServerStart/Installation Manager Extension and the ServerStart/Installation Manager manager. These modules can be used as individual functions via the ServerStart/Installation Manager Extension API.

Deployment Manager uses the following functions:

- Boot server with WinPE by PXE
- Get system information of server

This output contains all information on the server physics collected by the ServerStart/Installation Manager hardware detection module.

- Set/Get RAID configuration

This allows complete unattended RAID configuration for all RAID controllers used by PRIMERGY servers

If a bare server is to be entered to the server list, the ServerStart/Installation Manager Extension API is used as follows:

1. The *Add Server* dialog offers to collect additional server information.
2. The ServerStart agent is started and WinPE is booted via PXE.
3. *GetSystemInfo* is called to get the server parameters.
4. The ServerStart agent is stopped and the server is powered off.
5. A new entry is created in the ServerView server list with the retrieved parameters.

This allows the following cloning process:

- Deployment Manager – define RAID configuration
  - define cloning parameters and deployment group
- ServerStart/Installation Manager – start ServerStart agent and boot WinPE via PXE
  - configure RAID parameters
  - stop ServerStart agent and WinPE, release PXE service
- Deployment Manager – enter cloning job for DB API
- SCW (System Cast Wizard) – prepare cloning job image
  - initialize PXE service for DOS cloning agent boot image
    - set PXE mode via remote control
    - start PXE reboot via remote control
  - Check if the ServerView agent is available:
    - If yes, initiate a reboot via ServerView agent.
    - If no, initiate a shutdown followed by a power on
  - boot PXE DOS image
  - perform cloning

## Customer System Preparation Image

You can prepare your own system preparation phase if you want a particular server type to be supported in a particular way (must not be a PRIMERGY server).

For that purpose a generic system-preparation image PXE boot method is provided before starting the generic cloning phase.

The image must meet the following requirements:

- The size of the image is less than 1.44 MB
- The image is capable of being booted from and used as a local floppy disk copy.

This means that all the contents of a floppy disk that can be booted from the target server can also be used as a PXE image.

At the end of the system preparation process, a normal reboot is initiated. If the boot device table in the system BIOS has a PXE-capable LAN card as the first device, a PXE boot is automatically initiated instead. Any operating system can be used for the system-preparation image. The PXE boot works independently of the operating system.

Finally, to continue with a cloning process automatically the following process is implemented within Deployment Manager:

- Deployment Manager – define cloning parameters and target servers
- front-end – request PXE boot image path
- Deployment Manager – start ServerStart agent on server side without booting WinPE
- ServerStart/Installation Manager – boot given system preparation image via PXE
- check bootstrap boot status and return if PXE request from selected server was received
- Deployment Manager – stop ServerStart agent, release PXE service only
- finalize cloning job definition: without system preparation, no PXE boot, just PXE server initialization
- enter cloning job for DB API
- SCW – prepare cloning job image
- initialize PXE service for DOS cloning agent boot image
- set PXE mode via remote control, but do not initiate a PXE boot, reboot is initiated by preparation image process
- boot cloning agent DOS image via PXE
- perform cloning

The critical path in this scenario is the timing. The time between booting the system preparation image via PXE and the next PXE request from this server initiated by a reboot after finalizing the system preparation must cover the minimum of 30 seconds. If not, a PXE boot timeout will occur. This can be prevented by simply rebooting this target server in PXE mode. This is especially the case if more than four sessions are activated in the Haribote cloning engine.

Within a 1 Gbit environment a higher session value is possible by changing a special registry key. This value controls the number of parallel sessions for Unicast cloning sessions as well.

You can start a Unicast cloning job of, for example, 10 servers in one job, but only four servers are cloned in parallel at a time.

With Unicast mode each server is a session, with Multicast each job is a session.

## 10.1.3 Supported Storage Devices

### 10.1.3.1 SCSI/IDE Drives

SCSI and IDE drives are handled by the system BIOS by default as Int13h devices and do not require special tools for modification.

If the SCSI/IDE drive is mapped as the logical Int13h device, cloning will work without any system preparation. Manual mode should be used as the system preparation method.

### 10.1.3.2 RAID Devices

It is possible to create an image on a different RAID level than is used for the subsequent cloning task. The RAID controller chip set must support a BIOS configuration extension for the manual system preparation method. This extension can be used on a reference server with a connected local console or via Remote Management.

For blade servers only, the RAID functionality is prepared as part of the cloning process on DOS via the Haribote cloning engine directly.

For non-blade servers, unattended RAID configuration is used by the Server-Start/Installation Manager Extension which boots WinPE on the target system. With this method, all PRIMERGY servers and their RAID controllers are automatically supported as declared for the currently installed Server-Start/Installation Manager release.

After creation of a RAID array, an additional reboot must usually be initiated to activate the RAID array and make the new volume accessible to the cloning agent via BIOS support.

This second reboot is again a PXE boot and reloads the same DOS image as before.

### 10.1.3.3 FC and iSCSI Devices

Since RemoteDeploy V3.0, generic storage devices are supported which are visible as Int13h DOS devices and are detected by the system BIOS. Within the image creation or deployment configuration session of the Deployment Manager Web user interface, you can define the logical ID of such an Int13h DOS device. This is necessary if more than one storage adapter has enabled Int13h BIOS support, or one adapter provides more than one bootable volume. FC and iSCSI adapters basically behave in the same way as SCSI or RAID controllers in detecting and creating a boot device list of their attached storage devices.

Once this storage device list is visible on DOS as Int13h device (the adapter BIOS must be enabled for the last boot), Deployment Manager can perform image creation and mass cloning or mass remote installation on/from such devices generically.

Based on this method, it is possible to clone on nearly all storage devices found as DOS Int13h device.

Especially for FC and iSCSI device usage, the default UNDI LAN adapter no longer works for Broadcom NICs and must be replaced by the NDIS DOS driver, which is also available on the Deployment Manager CD. How to do this is described in [section “Adding NDIS Driver to Deployment Manager” on page 263](#).

### 10.1.3.4 Partitioning and File System Formatting

Partitioning is required to store the operating system master image in a partition. The sector algorithm used needs this partition orientation to decompress the used sectors to the right place.

If an image is created in raw mode, all format information is stored inside the image as part of the data packages. No pre-formatting is required for cloning.

If an image was created with file system optimization, the target volume will be pre-formatted to offer data block organization on the storage volume to put the used data sectors in the right place. This method requires a much smaller image size than the image created in raw mode. The cloning images are created on a partition basis even if this is offered on a disk basis in the Deployment Manager GUI.

The following file system formats are supported depending on the used operating system:

File system	DOS	Windows	Linux	ESX
FAT 16	x			
FAT 32		x		
NTFS4		x		
NTFS5		x		
NTFS5+		x		
Ext2			x	x
Ext3			x	x
Reiser file system (v3.5/3.6 on SuSE SLES 9/10)			x <sup>1)</sup>	

Table 8: Supported file systems for image creation

<sup>1)</sup> A specific package must be installed on the reference system before image creation if Reiser is used as the root file system. This package is available on the Deployment Manager CD.

Basically the file system analysis is done independently of the operating system used. But with regard to the operating system types supported for individualization, there are limits imposed by the operating system (e.g. W2k3 does not support FAT16).

But unknown or unsupported file systems can always be cloned in raw mode.

### 10.1.3.5 Multi-boot Operating System Partitioning

A hard disk with more partitions with different operating system instances can be used if you install a boot loader in the master boot record (MBR) of this hard disk.

For non raw mode image cloning, the MBR is created by the cloning agent and therefore no multi-boot loader is installed and supported.

This kind of installation can be cloned in raw mode only, but without individualization after cloning.

### 10.1.3.6 Adding NDIS Driver to Deployment Manager

With RemoteDeploy V3.0, NDIS and UNDI LAN protocol drivers are used by the DOS clone agent.

The following types of NIC vendor are currently supported:

- Intel pro1000 family by NDIS driver on all LAN ports (up to 4)
- Other (such as Broadcom)
  - Broadcom NDIS family driver for all known PRIMERGY systems released at Deployment Manager release time. Supports all LAN ports (up to 4)
  - by generic Intel UNDI driver on all LAN ports (up to 4)
  - by customer NDIS driver (by default, only the first LAN port is supported)

To add an additional NDIS driver or switch Broadcom to NDIS, the following steps are required to change the Deployment Manager installation folder:

1. Copy all driver files (typically \*.DOS only) to ...*\Program Files\Fujitsu Siemens\DeploymentService\ftp\agent\dos\boot* on the deployment server.
2. Modify the existing *DetNic.inf* file by adding a new entry with PCI vendor and device ID with the same format as the existing one.
3. Completely reboot the deployment server once.

For Broadcom NICs, a sample is provided on the Deployment Manager CD at *<DM-CD>:\setup\ftp\agent\dos\boot\AdditionalDrivers*.

For Broadcom NICs, two NDIS drivers are already configured. These NDIS drivers are stored in the *B57.dos* and *bxnd20x.dos* files in the ...*\Program Files\FujitsuSiemens\DeploymentService\ftp\agent\dos\boot* directory on the deployment server. Modifying these files is not recommended.

Bear in mind that, typically, NDIS drivers support only the first LAN port by default. You can change this by creating a *protocol.ini* file with vendor-specific settings.

Please check your NDIS driver documentation for details of LAN port selection, assignment and bindings.

## 10.1.4 Image Creation

The reference image is generated on a reference server with certain static machine-related parameters:

- IP address
- Host name
- Windows SecureID

These parameters can be changed during the cloning process to adapt to each target client.

The Deployment Manager service delivers the final values of each client inside the cloning job description based on the deployment table settings. The image must be modified directly after it is cloned to the target client storage volume.

In [figure 72 on page 252](#), the flow chart of a cloning process describes this procedure in Block "C" for a Windows cloning. The file *clcomp.dat*, created for the before image creation, is now patched with the final individualization parameters and the next `RunOnce` process to be started will use these parameters in a system preparation session.

For Linux cloning, the parameters are stored directly in the original operating system configuration files and are directly valid at the next boot. Therefore no post-cloning phase is required as for Windows.

The procedure is always the same, regardless of whether Unicast or Multicast is used.

Additional dynamic parameters per client are

- Administrator account
- Administrator password

These parameters are available in the deployment table. For further details on how to initialize these parameters, see [section "Handling the Deployment Table" on page 274](#).



10.1.5 Tag File Handling

A tag file can be used to detect whether a running system is still being modified by the deployment process. The tag file is stored in a specific directory. This directory might also be used to store log files.

The names and the handling will be part of the official specification and will also be communicated to customers.

The tag file can be used by third-party software (application or services, for example) to detect whether a cloned system is still being modified by the deployment process.

Directory and tag file

Operating System	Directory	Tag File
Windows	%Systemdrive%\DeploymentInfo\	DeploymentMode
Linux	/etc	.DeploymentMode

Deployment Manager log files on the target Linux system are stored in the */var/log/remotedeploy* directory.

Creating a tag file on Windows systems

The tag file will be created during image creation at the beginning of the preparation of the reference system. If the *%Systemdrive%\DeploymentInfo* directory does not exist, it will be created. If the directory exists, any existing log files that are known as Haribote log files will be removed; other log files should not be removed. If the *DeploymentMode* file already exists, it is simply retained; this does not cause an error.

Creating a tag file on LINUX systems

The tag file will be created at the end of the image cloning while the DOS cloning agent is running. The DOS cloning agent creates the tag file in the directory */etc*. If the tag file already exists, this does not cause a problem.

## Removing the tag file

The tag file will be removed at the end of the Haribote post-preparation. If a customer script was specified for a cloning job, the tag file will be removed just before the customer script is executed. If an error occurs during the post-preparation, the tag file will not be removed.

## 10.1.6 PXE Protocol

The following description is based on the Intel PXE specification from 1999 release 2.1.

Basically a DHCP server is a must for using PXE boot functionality in the current LAN segment! (A "DHCP proxy helper" functionality can be enabled in the router and works as well.)

In principle the PXE protocol works as follows:

1. The deployment server initiates a power-on of a particular server.
2. Assuming the BIOS parameters are set to PXE boot, after power-on the BIOS ignores all alternative existing boot devices and starts the PXE LAN boot extension.
3. The PXE BIOS issues a DHCP request to a DHCP server via broadcast.
4. The DHCP server offers an IP address and additional LAN parameters such as the boot (deployment) server IP address (if it is configured by the administrator).
5. A boot service broadcast is initiated:

If the boot server IP address is provided, the PXE BIOS can contact the boot server directly anywhere in the LAN (performing a check on port 4011).

If the boot server IP address is not provided, a broadcast on port 67 is sent which has to bypass a switch (e.g. with virtual LAN software) or hub depending on where the server is connected to the LAN.

6. The boot server offers a packet with the name of the boot image.
7. The PXE BIOS initiates an MTFTP or TFTP to receive the boot image file.
8. The boot image is copied to address 07c0h and started in floppy emulation mode.

This first boot image (normally based on DOS) with the maximum size of 2.88 MB (Deployment Manager uses only 1.44 MB) is used to prepare the storage devices so that the second operating system image can be stored from the deployment server onto the target drive.

A RAID array may have to be configured beforehand, and an additional reboot may have to be initiated again using PXE to activate the created RAID array (depending on the RAID controller type).

A second PXE boot can be avoided if an already initialized RAID array with the right RAID level is detected.

For security purposes, the cloning image must be decompressed and decrypted. Decompressing also stores the image in such a way that only used hard disk sectors are transferred and must be placed on the right position on the drive. Decrypting is used to ensure that this image will not be sent by an intruder.

### 10.1.7 LAN Traffic and Deployment Methods

Because of very large operating system images of up to several GB, different deployment methods are used to keep bandwidth on the network for other processes.

#### Unicast and Multicast Transfer

With a Unicast IP protocol, only one target system can receive a packet at any one time. The packet header includes the MAC address of only one recipient. If individual data per recipient is to be distributed, this is the preferred method.

The first DOS boot image containing the dynamic parameters of each client (IP address, host name) will be distributed in this way.

The disadvantage is that if, for example, 100 clients are to be cloned, this DOS image must be created 100 times, each with its individual parameters for cloning its target client.

If a RAID1 is created, and a second reboot with the same DOS image is required to activate the RAID array, these 100 DOS images must be transferred again, each with a size of up to 1.44 MB. This takes a few minutes to be prepared.

Multicast is the typical method for cloning many servers over the LAN using the same image each time.

The server sends only one image packet-by-packet over the LAN to the clients using a Multicast IP packet.

The clients are assigned via an IP Multicast address. Each client assigned via such a temporary address catches this kind of broadcast and stores the operating system image in its memory or disk, concatenating the user data.

Since each Multicast client receives the same image, dynamic parameters such as IP address, host name and SecureID are modified on the client side.

The multicast protocol used by Deployment Manager uses an acknowledgement package for each transferred data package from each listening client. The slowest one controls the speed of the process. If more than two retries to a certain client are necessary for a data package, this client will be phased out and the protocol continues without it. That means, if one of the target servers is connected by a 10 Mbit connection, the whole Multicast protocol runs at 10 Mbit/s only, irrespective of which speed is possible with the other members of that Multicast group. With Unicast it is different on account of a peer-to-peer connection between each server and client.

With Unicast mode each server is a session; with Multicast each job is a session.

### **Switch, Hub and Bridge Configuration**

The PXE protocol searches for the PXE server and the DHCP server via broadcast on port 67.

If these servers are placed behind bridges, hubs or switches with activated virtual LAN software, these devices must be programmed port-by-port to bypass these broadcasts.

These external devices usually provide configuration APIs, accessible via vendor-specific configuration tools or via a programming interface.

## 10.2 Mass Remote Installation Process

### 10.2.1 Functional Process Flow

The following process is started and the following modules are affected by a remote installation process:

1. Create remote installation group; decide if 1:1 or 1:N mode.
2. Assign configuration file(s) per server – (1:1) or per group (1:N) – and add the server to a remote installation group.
3. Set up deployment table with individualization parameters: IP settings, hostname and admin password.
4. Define the power control status per server (1:1) or per group (1:N).
5. Create the final configuration files for each group server by merging the override files and the given configuration files.
6. Initiate remote installation directly or via scheduler (once per server in an installation group).

#### *Windows*

- The Deployment Manager service gets the parameters from the installation group: MAC address and configuration file path.
- The Deployment Manager service fetches the ServerStart/Installation Manager content user from the registry to get permission for a ServerStart/Installation Manager Extension session and queries the password from the user (if it is not the deployment user itself).
- The Deployment Manager service starts the ServerStart agent; the result is a session handle.
- The Deployment Manager service initiates a remote installation job with the parameters:  
  
MAC address, server model, configuration file (stream or path with merged override files); the result is a job id.
- ServerStart/Installation Manager creates a status folder of the current server session and sets up the PXE service.

- ServerStart/Installation Manager initiates a PXE boot via *RemControl.dll*. (for Kalypso and MMB targets user and password are given by the Deployment Manager service)
- ServerStart/Installation Manager initiates a WinPE boot and starts the installation; internal reboots e.g. after RAID configuration are handled by ServerStart completely.
- The ServerStart/Installation Manager installation process on WinPE updates the progress file in the status folder assigned to the target server.
- The Deployment Manager service waits for job termination by polling the job.
- The Deployment Manager service gets status information on job result.
- If defined, a customer script is started by the ServerStart/Installation Manager installation process at the end of the installation on the target server. The finalization status of installation is offered immediately.
- You can follow the progress by selecting a server in the progress frame; (customer scripts progress is not shown in the progress frame).
- The Deployment Manager service stops the ServerStart/Installation Manager Extension session.

#### *Linux*

- The Deployment Manager service gets parameters from installation group: MAC address and configuration file path.
- The Deployment Manager service fetches the ServerStart/Installation Manager content user from registry to get permissions for a ServerStart/Installation Manager Extension session and queries the password from the user (if it is not the deployment user itself).
- The Deployment Manager service starts the ServerStart agent; the result is a session handle.
- The Deployment Manager service requests target information for the installation process. The result is ultimately required by the Linux installation setup later.
- The Deployment Manager service waits for job termination by polling.
- The Deployment Manager service gets the status information on the job result.

- The Deployment Manager service starts the system preparation job.
- The Deployment Manager service waits for job termination by polling.
- The Deployment Manager service gets the status information on the job result.
- The Deployment Manager service stops the ServerStart/Installation Manager Extension session.
- The image folder in the TFTP folder tree for original Linux installation is created.
- The TFTP folder is filled with the operating system dependent Linux ramdisk image and configuration file(s).
- The Linux installation image is booted.
- The Deployment Manager service waits for job termination by polling the job.
- The Deployment Manager service gets the status information on the job result.
- If defined, a customer script is started by the ServerStart/Installation Manager installation process at the end of the installation on the target server. The finalization status of the installation is offered immediately.
- You can follow the progress by selecting a server in the progress frame (customer script progress is not shown in the progress frame).
- The Deployment Manager service stops the user agent session.

### *ESX*

The process flow is the same as described above under Linux. The IP configuration for the service console is set based on the ESX deployment configuration. If you do not specify an ESX deployment configuration, the IP configuration for the service console is defined based on the deployment configuration of the first LAN port.

7. The Deployment Manager service stores the final status of the server in the central deployment table.

## 10.2.2 Creation of the Configuration Files

The configuration file (*SerStartBatch.ini*) is created by the ServerStart/Installation Manager Wizards (e.g. in *Preparation Mode*) and must be stored in a repository folder.

The configuration files are handled in the same way for remote installation as the image file and \*.cfg file are for cloning.

## 10.2.3 Support of Generic Remote Installation Groups

Remote installation groups are created with free group names. The name consists of just a string. There is no relation to the configuration file name. The assignment of servers to configuration files is offered in two ways:

- N:N relationship of configuration file and target server's MAC address, i.e. a list of pairs is created.

In this case each server requires its own configuration file.

The IP address and host name are directly stored inside each configuration file by ServerStart/Installation Manager Wizards.

- 1:N relationship of configuration file and target server's MAC address, i.e. a list of MAC addresses in one configuration file is created.

All servers are assigned to the same configuration file, but a merge of master configuration file parameters and deployment table entries is performed by ServerStart/Installation Manager Extension for individualization. ServerStart/Installation Manager will receive one configuration file and N overrule files.

In step 1 (RemoteDeploy V3.0) the configuration file is created and stored in INI format only as created by the ServerStart/Installation Manager browser/Wizards. In step 2 (future release) the format will be changed to the XML format as well.



## 10.2.4 Status Frame for Each Installation Process

In Deployment Manager one progress status frame combined with a job or server selection allows you to follow the progress output of a remote installation. Basically an already existing text file created for each installation process is passed through by the ServerStart/Installation Manager Extension up to the Deployment Manager GUI status frame using a “read status frame” function of the ServerStart/Installation Manager Extension API. This text file is updated every two seconds by the remote installation process on the target side and can be read by Deployment Manager in the same frequency.

On the Deployment Manager side, only one progress at a time can be selected in the status frame.

## 10.2.5 Power Status Control

With power status control settings you can define the end power status of the target server after each installation.

On the ServerStart/Installation Manager side the same implementation is required as is already available on the Deployment Manager cloning side.

The administrator can select the power mode in which the server is to remain after a job is done:

- PowerOff or
- PowerOn(online).

## 10.3 Handling the Deployment Table

Each logical group of servers has its own set of group attributes (parameters) which are relevant for all group members. Each group member may also have its own set of group parameters which may overrule the group settings for this server. Finally, each physical server, whether it is a member of a group or not, has its own set of individual physical settings which are stored in a server-specific deployment table.

The master deployment table is stored in the Deployment Manager database. Each server defined by a minimum of one valid PXE bootable MAC address, and therefore listed in the *Physical View* of Deployment Manager, has its entry in this table. Each entry consists of a set of parameters for deployment purposes only.

The master deployment table is common to all servers. For blade server systems only, the management blade contains an additional deployment table with specific attributes, which is periodically synchronized with the corresponding master deployment table entry of each server blade.

The master deployment table and the management blade deployment table are described in detail below.

### 10.3.1 Master Deployment Table

The following table shows the structure of one server entry in the master deployment table:

Index	Parameter	Detailed description	Default value	Size (in bytes)
1	<b>Serial ID (of Chassis)</b>	<b>Serial number</b> to identify the hardware and assign system information to the server list	0	16
2	<b>UUID (GUID)</b>	Unique identifier based on SMBIOS section 01: offset+08 (Format defined in DCE Specification)	0	16
3	<b>Slot ID</b>	Physical identification of a server in a chassis slot. For non-blade systems: used for rack identification	1.. <i>n</i> ( <i>n</i> =max. number of slots)	1
4	<b>List of physical LAN port parameters: 1 .. N (one entry per physical NIC)</b>	MAC addresses Must be set to 0-0-0-0-0-0-, if hardware was not found. The MAC address must be always unique and used for identification combined with UUID <b>IP address</b> IPv4 based (without leading "0") <sup>1</sup> <b>SubnetMask</b> IPv4 based (without leading "0") <sup>1</sup> <b>Default Gateway</b> IPv4 based (without leading "0") <sup>1</sup> <b>DNS server (s)</b> IPv4 based (without leading "0") <sup>1</sup>	"all bits 0"  "all bits 0" "all bits 1" "all bits 0" "all bits 0"	N * 24
5	<b>Hostname</b>	<b>Operating system related host name</b> Allows clone/installation engine to patch the right host name into operating system image/configuration file during cloning/installation process.	\$DNS\$	16
6	<b>URL to cloning image file</b>	<b>For cloning</b> URL in UNC notation (but in ASCII) to remote image file (*. <i>img</i> ) Format: \\server_name\<subpath>\<image_name>	\$NA\$	256

Table 9: Master Deployment Table

Index	Parameter	Detailed description	Default value	Size (in bytes)
7	<b>URL to operating system configuration file</b>	<b>For remote installation</b> URL in UNC notation (but in ASCII) to remote configuration file (*.cfg) Format: \\server_name\<subpath>\<cfg_name>	\$NA\$	256
8	<b>LAN Status (for blades only)</b>	<b>= 2 (empty slot)</b> The IP LAN definitions in this information field are changeable. The administrator must define the values correctly via Deployment Manager or management blade Web UI manually before starting the cloning job. If the update flag is set and the slot state is <i>empty</i> , the ServerView agent will update most parameters based on operating system configuration cyclically. <b>= 3 (preset slot)</b> The deployment parameters of this table for this slot is the reference. If a new or already installed blade is plugged in, the values from the deployment table should be used for the installation/adaptation. The management blade itself never does change that values in this mode (except MAC address).	2	1

Table 9: Master Deployment Table

Index	Parameter	Detailed description	Default value	Size (in bytes)
9	Automatic Recovery	<p><b>= 2 (disabled)</b> After hot replacement of a defective server blade no automatic deployment activities should be started.</p> <p><b>= 3 (enabled) <sup>2</sup></b> After hot replacement ServerView receives an event from the management blade of the replaced hardware.</p> <p>The Deployment Manager will be triggered by ServerView to check in the given server list, if the old MAC address was assigned to a backup image. If not, may be a master image was assigned. One of these images (first backup, than master image) will be used for automatically cloning of this image to the new server blade assumed the same hardware is used.</p>	2	1

Table 9: Master Deployment Table

Index	Parameter	Detailed description	Default value	Size (in bytes)
10	Deployment	<b>2=not deployed</b> The client does not contain a valid configuration of an operating system (at least not by Deployment Manager)  <b>3=Cloning</b> The cloning process is running and the status will switch to cloned until the acknowledgement from the engine was received by the Deployment Manager.  <b>4=Cloned</b> The assigned image was successfully cloned (without customer script)  <b>5=Installing</b> The installation process is running and the status will switch to installed until the acknowledgement from the engine was received by the Deployment Manager  <b>6=Installed</b> The given operating system configuration was successfully installed (without customer script)  <b>7=AgentMode</b> WinPE agent booted in RAM and idling	2	1
11	Admin user account	User account with admin/root policies created as root or in administrator group after cloning. For installation a build in account defined by the Server-Start/Installation Manager wizard in the configuration file and this field is not used.	“ “	128
12	Admin password	Encoded password of admin/root valid after cloning or installation is set on the target server.	“ “	128
13+14	OEM parameters string 1 + 2	Reserved for free customer usage.	“ “	2*128
15-20	Deployment Manager internal string 3-8	Reserved	“ “	128

Table 9: Master Deployment Table

Index	Parameter	Detailed description	Default value	Size (in bytes)
21	<b>Deployment Manager internal string 9 (Readable by all server management components)</b>	<b>UpdateMode==0 (disabled)   1 (enabled)</b> If <i>LAN status of slot</i> is empty and <i>Update Mode</i> is enabled, the ServerView agent can cyclically update the deployment table parameters of the current slot based on the operating system. To initiate a cloning, the update status must be disabled to avoid configuration conflicts in the deployment table settings with manual modifications.	0 (disabled)	128
22	<b>Deployment Manager internal string 10 (Read/write by Deployment Manager only)</b>	<b>BootPort=1...N</b> Selects NIC assigned for PXE boot corresponding to NIC port sub table at index 4 in this table.	1	128

Table 9: Master Deployment Table

<sup>1</sup> 4 bytes are used for IP V4, but space reserved for IP V6

<sup>2</sup> Option currently not supported

If a new server is created, the parameters are preset by the default settings as defined in the table above. You must manually update and modify the table before initiating a deployment process. You can do this via the Deployment Manager front-end (see [section “Target System Configuration” on page 113](#)).

### 10.3.2 Management Blade Specific Deployment Table

For blade server systems only, the management blade contains its own deployment table. In the case of a blade system, the Deployment Manager master deployment table must be synchronized with the corresponding management blade (MMB) deployment table entry by performing an update cycle (every minute and/or driven by an event).

If the MAC address is 0.0.0.0, the Deployment Manager master deployment table entry is removed; there is no blade in the slot. If the MAC address in the management blade table is valid, the following fields are read into the Deployment Manager master deployment table:

- Serial ID
- Slot ID
- MAC1+2

If a roaming operation was performed, i.e.:

- *Lan Status of slot = Preset*
- *Power Status = Online*

the following fields could have been modified (during server boot only) by the ServerView agent and must be read into the Deployment Manager master deployment table:

- Host name
- URL of cloning image file
- Deployment status (only if no cloning or installation process is currently running)

*IP1+2*, *SubNetmask1+2*, *Gateway1+2* are reference parameters for the clone and are read once at boot time. These fields can be written by the Deployment Manager database update process caused by modifications coming from the Deployment Manager GUI.

The remaining fields are either in the MMB or in the Deployment Manager master deployment table under full control of the Deployment Manager only, and are always updated in the MMB deployment table when a modification is made in the Deployment Manager master deployment table by the Deployment Manager directly.

The management blade is the master of the status of the following server blade fields in the MMB deployment table: *Serial ID*, *Slot ID*, *MAC1+2*, and *PowerStatus*.

Each deployment or administrating instance must access the management blade to inform it about the current list of plugged-in servers and its status and attributes.

The detailed structure of the management blade deployment table is shown below. This structure can be read and written either via LAN using the SNMP interface of the management blade or via IPMB channel, a local access path between the management and each server blade, directly by the server blade itself.



Index	Parameter	Detailed description	Default value	Size(in bytes)
1	<b>Chassis Id</b>	<b>Chassis serial number</b> to assign the system information table to the blade chassis.	0	10
2	<b>Slot Id</b>	<b>Physical identification of server blade slot</b> If no server blade is plugged in, no MAC address is available. This is the way only to assign and store slot-related system information. This is useful for hot-replacement functionality.	1 ... $n$ ( $n$ =max. number of slots)	1
3 + 4	<b>MAC Address 1+2</b>	<b>of each LAN port (1+2) per server blade:</b> Must be set to 0-0-0-0-0-0 by the management blade if a server blade is removed from a slot. The MAC address must always be unique and up-to-date for the current plugged-in server blade. Besides the slot ID, this is the second way of identifying a server blade by its slot. Additional LAN Cards (BX600 only) will be supported via the Deployment Manager master deployment table.	"all bits 0"	6
5 + 6	<b>IP Address 1+2</b> <sup>1</sup>	<b>of each LAN port 1+2 per server blade</b> 0.0.0.0 == DHCP mode	"all bits 0"	16
7 + 8	<b>SubNet Mask 1+2</b> <sup>1</sup>	<b>of each LAN port 1+2 per server blade</b>	"all bits 1"	16
9 + 10	<b>Default Gateway1+2</b> <sup>1</sup>	<b>of each LAN port 1+2 per server blade</b>	0	16
11	<b>Hostname</b>	<b>operating system related host name</b> Allows clone/installation engine to patch the right host name into operating system image a configuration file during cloning and installation process.This name is not LAN port related.	\$DNS\$	16
12	<b>URL to cloning image file</b>	<b>For cloning:</b> URL in UNC notation (but in ASCII) to remote image file (*.img)	\$NA\$	256

Table 10: Management Deployment Table

Index	Parameter	Detailed description	Default value	Size(in bytes)
13	<b>PowerStatus of blade</b>	<p>= <b>2</b> Power-down: waiting for boot When system is powered off and retry count isn't equal to zero.</p> <p>= <b>3</b> Standby: power-management mode Only on ACPI operating system, BMC knows the standby mode.</p> <p>= <b>4</b> System boot failure When system is powered off and retry count is equal to zero.</p> <p>= <b>5</b> BIOS setup or boot phase System is in POST.</p> <p>= <b>6</b> Online: ACPI: operating system booted</p>	2	1
14	<b>LAN status of slot</b>	<p>With this value you can control whether the deployment table will be reset on removal of the blade system hardware or whether the parameters remain in the deployment table as defined by the user:</p> <p>= <b>2 Empty slot</b> The IP LAN definitions in this field can be changed. The administrator must redefine the values correctly via Deployment Manager or management blade WebUI manually before starting a cloning job. In combination with the <i>Update</i> flag: If the update flag is set and the slot state is <i>empty</i>, the ServerView agent will update most parameters based on operating system configuration cyclically.</p> <p>= <b>3 Preset slot (Freeze)</b> The deployment parameters for this slot are the reference. If a new or already installed blade is plugged in, the values from the deployment table should be used for the installation and adaptation. The management blade itself never changes these values in this mode (except MAC address).</p>	2	1

Table 10: Management Deployment Table


Index	Parameter	Detailed description	Default value	Size(in bytes)
15	<b>Automatic Recovery</b>	<p><b>= 2 (disabled)</b> After hot replacement of a defective server blade, no automatic deployment activities should be started.</p> <p><b>= 3 (enabled)<sup>2</sup></b> After hot replacement, ServerView receives an event from the management blade of replaced hardware. Deployment Manager will be triggered by ServerView to check in the given server list whether the old MAC address was assigned to an image. If not, maybe a master image was assigned. One of these images (first backup, then master image) will be used for automatic cloning of this image to the new server blade assumed the same hardware is used.</p>	2	1
16	<b>Deployment status</b>	<p><b>= 2 (not-deployed)</b> The client does not contain a valid configuration of an operating system.</p> <p><b>= 3 (cloning)</b> The cloning process is running. The status will switch to cloned when the acknowledgement from the engine is received by Deployment Manager.</p> <p><b>= 4 (cloned)</b> The assigned image was successfully cloned (without customer script).</p> <p><b>=5 (installing)</b> The installation process is running and the status will switch to installed when the acknowledgement from the engine was received by Deployment Manager.</p> <p><b>=6 (installed)</b> The given operating system configuration was successfully installed (without customer script).</p> <p><b>=7 (agent mode)</b> WinPE agent booted in RAM and idling.</p>	2	1

Table 10: Management Deployment Table

Index	Parameter	Detailed description	Default value	Size(in bytes)
17 + 18	OEM parameter string 1 and 2	Reserved for free customer usage	" "	128
19 ... 24	Deployment Manager string 3-8	Reserved String 6 contains the list of DNS servers (in coded format) String 7 contains the DNS suffix.	" "	6*128
25	Deployment Manager string 9	<b>UpdateMode=&lt;0 (disabled&gt;   &lt;1(enabled)&gt;</b> If <i>LAN Status of slot</i> is <i>empty</i> and <i>UpdateMode</i> is enabled, the <i>ServerView</i> agent can update the deployment table parameters of the current slot based on the operating system settings cyclically.To initiate a cloning, the update status must be disabled to avoid configuration conflicts in the deployment table settings with manual modifications.	0	128
26	Deployment Manager string 10	<b>BootPort=&lt;1..n&gt;</b> Selects NIC assigned for PXE boot corresponding to NIC port sub-table.		

Table 10: Management Deployment Table

<sup>1</sup> 4 bytes are used for IP V4, but space reserved for IP V6  
<sup>2</sup> Option currently not supported.

- 
- The MAC address and slot ID must be used as identification keys for a client parameter set selection.
  - The parameter *PowerStatus of Blade* is continuously controlled by the management blade depending on its current status.
  - The remaining attributes are set to their default values by the management blade each time a new item of hardware is plugged into a slot or detected as new hardware after *PowerStatus* is on and *LAN status of slot* is *empty slot*.  
  
(Otherwise it is a roaming cycle.)

### 10.3.3 Configuration in Deployment Manager

#### 10.3.3.1 Basic Initialization by Deployment Manager

The deployment table inside the Deployment Manager database is a static table and resident even when Deployment Manager is off.

Automatic update and initialization of each server entry is performed by the Deployment Manager driven by different events:

1. Adding a new server

A new deployment table entry is created with the default settings as defined in [table 9 on page 275](#).

Additional attributes of a server are updated by the front-end *Add Server* window or via WinPE.

A deployment table entry requires a corresponding server list entry containing additional server attributes which are not part of the deployment table.

2. Disabling a server

Only bare servers can be removed from the server list. All other servers imported from the ServerView database cannot be deleted. They automatically own a deployment configuration which is filled with default values if no other values are assigned. An exception are blade servers which are pulled out of the chassis. If they are not to be plugged in again, their entry in the database is deactivated (Not-Present-Bit) and can be removed afterwards. They are also removed from the ServerView server list.

3. Modification of a server status

Basically each status change of a blade server deployment table is detected by a cyclical update between the management blade and Deployment Manager. Details are provided in the following sections.

The update process is described in [section “Management Blade Specific Deployment Table” on page 279](#).

#### 4. Import and export of the deployment table

Via the Job API Tandem, import and export functionality is offered for blade servers which allows the API user to modify a server entry.

The values that can be changed by the import functionality are limited to those also offered for modification by the Deployment Manager front-end.

Some parameters are under full control of the management blade or Deployment Manager and cannot be changed by a TANDEM user.

The administrator user and password fields are set to " " by default. In this status no action is activated for changing the administrator account. If the administrator enters the user name and password in these fields for cloning, the post-cloning phase will change these settings and for installation the individual configuration files for each server are patched by these settings before the installation process is started. The password is always stored encoded. Only at the point when the modification is initiated is the password decoded by the cloning agent or installation manager.

The URL of the cloning image file can be defined in parallel with the URL of the installation configuration file because a server may be a member of a cloning group and an installation group. Which URL is used depends on the currently initiated deployment job.

The boot port number in the Deployment Manager internal parameters string 10 enables to select the LAN port of a server used for PXE boot at the next deployment job on that server.

### 10.3.3.2 Basic Initialization of the MMB Deployment Table

At power-on of the blade chassis, the management blade must synchronize the system info table with the existing and non-existing hardware by snooping and comparing the MAC addresses in each slot.

Basic rules are:

- If a previously detected server blade was removed and the *LAN status of slot* is *empty slot*, the system info table entry of that slot must be reset to the default values.

If the *LAN status of slot* is *preset slot*, the removal of a blade could be part of a replacement cycle and only the MAC address must be reset to the default value.

- If a new server blade is detected (different MAC addresses as found in the system info table of that slot) and the *LAN status of slot* is *empty slot*, the new role of this blade must be manually defined by the administrator via the WebUI of the management blade or the Deployment Manager front-end.

The deployment table maintains the default values except that the MAC address is updated.

- If the *LAN status of slot* is *preset slot* and the operating system is booted with an active ServerView agent, it could be part of a roaming process and the activity is on the ServerView operating system agent side as described in [section “Roaming” on page 289](#).

This status can also be used for service manipulation of the same blade hardware as well. This might be helpful for exchanging hard drives or updating memory modules. The deployment table content remains unchanged until *LAN status of slot* is reset to *empty*.

The use of the update mode offered in the Deployment Manager internal parameter string 9 is described in detail in [section “Roaming” on page 289](#).

### 10.3.3.3 Installation Status and Cloning Status

In the case of multiple parallel installation and cloning tasks, the Deployment Manager documents each activated process by setting the deployment status accordingly to the current progress of each target server.

During the deployment process the *Deployment Status* is set to 3 (*cloning*) or 5 (*installing*) to declare that this server is reserved for this Deployment Manager process which has initiated the deployment job. All other Deployment Managers which might be installed and running in the same server view must not access servers with one of these states.

Once the deployment job is done, the URL of the cloning image or configuration file is updated and the *Deployment Status* is set to *cloned* or *installed* by the initiating Deployment Manager.

With the *Deployment Status* of *agent mode*, the server has entered the deployment agent level where WinPE is booted via PXE and idling, waiting for new commands from the Deployment Manager.



## 10.3.4 Roaming



The roaming functionality is supported only with the ServerView agents V3.00.04 (or higher) for Windows and Linux. The relevant agent must be installed on the target system in order to receive the deployment table automatically during a reboot. The operating system of the target server is updated with the LAN parameters found in the deployment table.

“Roaming” means that a fully installed server blade is running in one blade chassis and is to be moved to another. In this case the roaming blade is to be reconfigured for a possibly new LAN environment given by the preset parameters in the given deployment table entry of this new slot.

Make sure all applications are closed before you start a roaming process.

Before a roaming process of a server blade is started, the LAN parameters of the target slot must be preset to valid values of the new LAN segment and the *LAN state of slot* flag must be manually set to *preset* by the administrator.

It is also important to set the *Automatic Recovery* flag to *disabled* to disable the automatic re-cloning task. Otherwise the automatic recovery cycle will be initiated and the already installed operating system will be overwritten!

If there are different LAN parameters in the new LAN environment, and the installed operating system is not set to DHCP mode or no DHCP is present, the ServerView agents will try to receive the valid LAN parameters via the IPMB channel from the management blade. This is done automatically immediately after each reboot of the system.

When the *LAN state of slot* is set to *preset*, valid LAN parameters are available and can be used by the ServerView agents to auto-configure the LAN parameters inside the operating system. When the *LAN state of slot* (*preset* or *freeze*) flag is set to *empty* in the target slot, the agent updates its registry settings relating to the image path and clone status only as described in [table 11](#).

As the target system cannot detect the appropriate image of the running operating system automatically, the administrator must preset the *URL to Image* field manually via the WebUI of the management blade or Deployment Manager front-end to complete the roaming process and the status entries in the deployment table.

The following table shows the ServerView operations on the deployment table depending on the *LAN status of slot* and deployment status: *Deployment status*.

LAN status of slot (preset or freeze) = empty; Automatic Recovery = disabled		
DHCP	Deployment status	Deployment table handling of ServerView agent
Off (operating system)	not cloned / not installed	<ul style="list-style-type: none"> <li>– Read URL of image and configuration file from deployment table to registry</li> <li>– Read deployment status from deployment table to registry</li> </ul>
	cloning / installing	– nothing
	cloned / installed	<ul style="list-style-type: none"> <li>– Read URL image and configuration file from deployment table to registry</li> <li>– Read deployment status from deployment table to registry</li> <li>– If <i>Update Mode</i> is enabled <ul style="list-style-type: none"> <li>– write host name from operating system to deployment table</li> <li>– write IP settings from operating system to deployment table</li> </ul> </li> </ul>
On (operating system)	not cloned / not installed	<ul style="list-style-type: none"> <li>– Read URL of image and configuration file from deployment table to registry</li> <li>– Read deployment status from deployment table to registry</li> </ul>
	cloning / installing	– nothing
	cloned / installed	<ul style="list-style-type: none"> <li>– Read URL of image and configuration file from deployment table to registry</li> <li>– Read deployment status from deployment table to registry</li> <li>– If <i>Update Mode</i> is enabled <ul style="list-style-type: none"> <li>– write host name from operating system to deployment table</li> <li>– write IP default values to deployment table IP address: 0.0.0.0 Netmask: 255.255.255.255 Gateway: 0.0.0.0</li> </ul> </li> </ul>

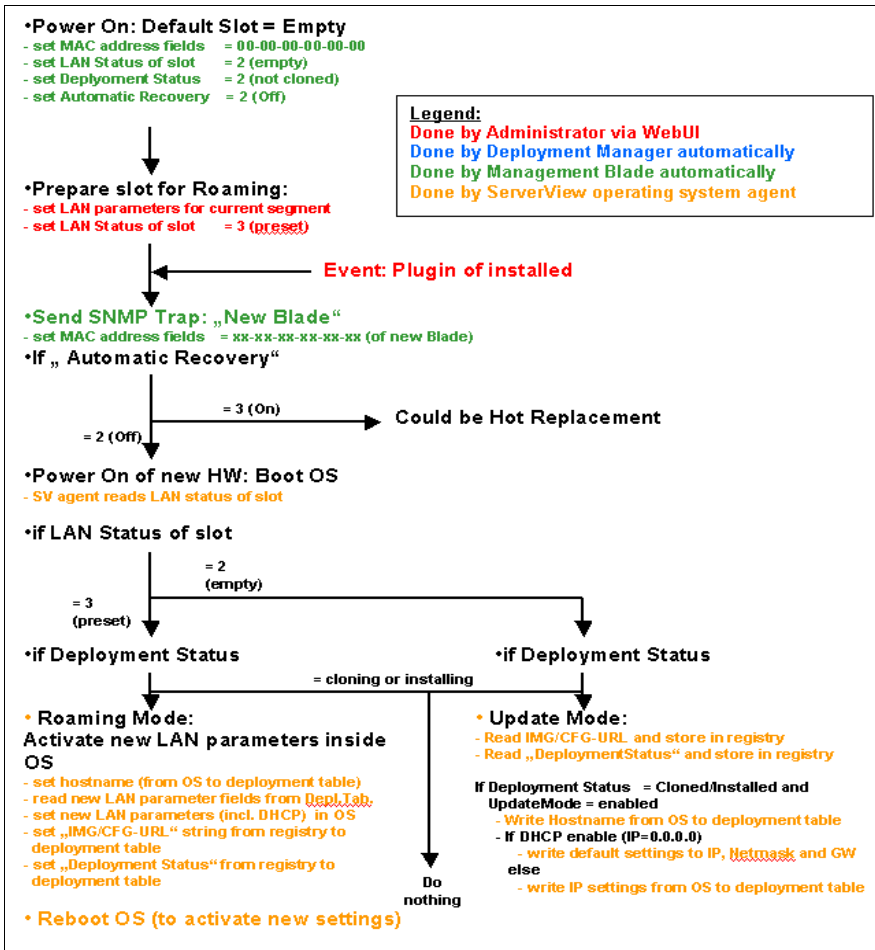
Table 11: Roaming state action of ServerView agent

<b>LAN status</b> of slot = preset; Automatic Recovery = disabled		
<b>DHCP</b>	<b>Deployment status</b>	<b>Deployment table handling of ServerView agent</b>
Off (Deploy-ment table)	not cloned / not installed	<ul style="list-style-type: none"> <li>– Read IP parameter from deployment table to operating system</li> <li>– Write host name from operating system to deployment table</li> <li>– Write URL of image and configuration file from registry to deployment table</li> <li>– Write deployment status from registry to deployment table</li> </ul>
	cloning / installing	– nothing
	cloned / installed	<ul style="list-style-type: none"> <li>– Read IP parameter from deployment table to operating system</li> <li>– Write host name from operating system to deployment table</li> <li>– Write URL of image and configuration file from registry to deployment table</li> <li>– Write deployment status from registry to deployment table</li> </ul>
On (Deploy-ment table)	not cloned / not installed	<ul style="list-style-type: none"> <li>– Read IP parameter from deployment table to operating system</li> <li>– Write host name from operating system to deployment table</li> <li>– Write URL of image and configuration file from registry to deployment table</li> <li>– Write deployment status from registry to deployment table</li> </ul>
	cloning / installing	– nothing
	cloned / installed	<ul style="list-style-type: none"> <li>– Set DHCP mode in operating system</li> <li>– Write host name from operating system to deployment table</li> <li>– Write URL of image and configuration file from registry to deployment table</li> <li>– Write deployment status from registry to deployment table</li> </ul>

Table 11: Roaming state action of ServerView agent

*Update Mode* is a flag stored and handled by Deployment Manager inside the reserved OEM strings in the deployment table. This mode can be manipulated via the Deployment Manager front-end only. If *Update Mode* is enabled, no cloning is possible because of possible conflicts between the update cycle of the ServerView agent and manual manipulations by the deployment user in the deployment table.

The following flowchart presents the roles entered during the roaming process.



If a service technician is going to make modifications to the existing blade hardware in one and the same slot, he/she can also use the *preset* state of *LAN status of slot* to freeze the deployment table settings, remove the blade hardware for modification, and replace the blade hardware. At the next boot the ServerView agent will detect the preset flag but this is basically always consistent with the settings inside the deployment table. So the write activities will be performed only once at boot time and the agent detects the preset state of the slot, but this does not have any effect because the same values are overwritten. The deployment table remains consistent.

If the hardware is removed without preset mode being set, the deployment table settings of that slot would be automatically removed by the management blade to reset the deployment table to an empty slot status.



---

# 11 Diagnostic

## 11.1 Logging Files

### 11.1.1 General Logging Files

#### Deployment Service log files

The Deployment Service always creates log files in the *C:\Program Files\Fujitsu Siemens\DeploymentService\bin\AutoLog* directory. There will be log files for the PXE service (*PXEService.exe.xxx*), for the TFTP service (*PXEMTFTP.exe.xxx*) and for the deployment service itself (*SCWDepSv.exe.xxx*). The *xxx* in the name of the files is replaced by a number. These files are overwritten when the maximum number of files is reached. The default for the maximum number of files is 4. This value and also the maximum file size can be changed by changing the *MaxNumOfLogFiles* and *MaxSizeOfLogFile* values for the *HKEY\_LOCAL\_MACHINE\SOFTWARE\FUJITSU\SystemcastWizard\Debug* registry key.

After changing the values in the registry, you must reboot the system.

Since these log files might be overwritten after some time, save them as soon as a problem concerning image creation or image cloning occurs and send them to your Service Department together with your fault report.

### FSC Deployment Manager service log files

The *FSC Deployment Manager* service always creates a *dmdebug.txt* log file in the following directory:

- *Inetpub\Scripts\RemoteDeployEngine*  
if Deployment Manager was installed under IIS
- *Program Files\Fujitsu Siemens\ServerView\ServerView Services\scripts\RemoteDeployEngine*  
if Deployment Manager was installed under Apache Web server from Operations Manager

When this file reaches a predefined size, it is saved as a *dmdebugold.txt* file.

Attach these two log files together with the *fscdm.mdb* file to any fault report concerning Deployment Manager that you send to your Service Department. Also read the section "7.2 Creating Diagnostic Data" in the Deployment Manager Readme file.

### 11.1.2 Logging File for Installation

During the installation of Deployment Manager a logging file (*InstallLog.txt*) is created under the folder *<Deployment Manager installation path>\RemoteDeploy*.

This shows which packages and files have been installed. This file is very useful to the Service Department of Fujitsu Siemens Computers for diagnostic purposes, especially in case of installation problems. Please always supply when reporting a fault.



### 11.1.3 Logging Files for Problem Diagnostics

The following three tables show the locations of log files that are generated in the event of a fault and are helpful if a fault is reported to the Service Department.

Should one of the faults described occur, please look in the path shown to see whether a log file has been created and submit this to the Service Department with your fault report.

#### Image Creation

Cloning Phase	Error Event	Where to find the log file(s)
Preparation		<b>Target System</b> [HDD] <i>C:\nicerror.log</i>
At Image Creation (DOS)		<b>Deployment Server</b> One or any of the following error logs: <ul style="list-style-type: none"> <li>– <i>&lt;LOGROOT&gt;\FJIMGBRS(&lt;HOSTNAME&gt;).ERR</i></li> <li>– <i>&lt;LOGROOT&gt;\LOADER(&lt;HOSTNAME&gt;).ERR</i></li> <li>– <i>&lt;LOGROOT&gt;\TFTP_ERR(&lt;HOSTNAME&gt;)</i></li> </ul> Remarks 1; Remarks 2 <b>Target System</b> One or any of the following logs: <ul style="list-style-type: none"> <li>– [RAMDRIVE] <i>C:\LOADER.ERR</i></li> <li>– [RAMDRIVE] <i>C:\FJFILECP.ERR</i></li> <li>– [RAMDRIVE] <i>C:\FJIMGBRS.ERR</i></li> </ul>
At Post-Preparation (Win)		<b>Target System</b> [HDD] all files in the <i>C:\WINDOWS\system32\LogFiles\DeploymentService</i> and <i>C:\WINDOWS\system32\LogFiles\SystemcastWizard</i> directory. The following files under <i>C:\Documents and Settings\Administrator\Local Settings\Temp</i> <ul style="list-style-type: none"> <li>– <i>NotifyErr.tmp</i></li> <li>– <i>nicerror.tmp</i></li> </ul>

Remarks 1:

*<LOGROOT> = <Deployment Service installation path>\tftp\log\ID#<Batch ID#*

*Example*

*C:\Program Files\Fujitsu Siemens\DeploymentService\tftp\log\ID#13*

Remarks 2:

*<HOSTNAME> = The name of the target system.*

*Example*

*C:\Program Files\Fujitsu Siemens\DeploymentService  
\tftp\log\ID#13\LOADER(RDBLADE15).ERR*

## Cloning of Windows Systems

Cloning Phase	Error Event	Where to find the log file(s)
At Mass Cloning of Standard Image (DOS)		<p><b>Deployment Server</b></p> <p>One or any of the following error logs:</p> <ul style="list-style-type: none"> <li>– <code>&lt;LOGROOT&gt;\FJIMGBRS(&lt;HOSTNAME&gt;).ERR</code></li> <li>– <code>&lt;LOGROOT&gt;\LOADER(&lt;HOSTNAME&gt;).ERR</code></li> <li>– <code>&lt;LOGROOT&gt;\TFTP_ERR(&lt;HOSTNAME&gt;)</code></li> </ul> <p>Remarks 1; Remarks 2</p> <p><b>Target System</b></p> <p>One or any of the following logs:</p> <ul style="list-style-type: none"> <li>– <code>[RAMDRIVE] C:\LOADER.ERR</code></li> <li>– <code>[RAMDRIVE] C:\FJFILECP.ERR</code></li> <li>– <code>[RAMDRIVE] C:\FJIMGBRS.ERR</code></li> </ul>
At Cloning of a single Snapshot-Image (DOS)		<p><b>Deployment Server</b></p> <p>One or any of the following error logs:</p> <ul style="list-style-type: none"> <li>– <code>&lt;LOGROOT&gt;\FJIMGBRS(&lt;HOSTNAME&gt;).ERR</code></li> <li>– <code>&lt;LOGROOT&gt;\LOADER(&lt;HOSTNAME&gt;).ERR</code></li> <li>– <code>&lt;LOGROOT&gt;\TFTP_ERR(&lt;HOSTNAME&gt;)</code></li> </ul> <p>Remarks 1; Remarks 2</p> <p><b>Target System</b></p> <p>One or any of the following logs:</p> <ul style="list-style-type: none"> <li>– <code>[RAMDRIVE] C:\LOADER.ERR</code></li> <li>– <code>[RAMDRIVE] C:\FJFILECP.ERR</code></li> <li>– <code>[RAMDRIVE] C:\FJIMGBRS.ERR</code></li> </ul>
At Post-Preparation (Win)		<p><b>Target System</b></p> <p>[HDD] all files in the <code>C:\WINDOWS\system32\LogFiles\DeploymentService</code> and the <code>C:\WINDOWS\system32\LogFiles\Systemcast Wizard</code> directory</p> <p>The following files under <code>C:\Documents and Settings\Administrator\Local Settings\Temp</code></p> <ul style="list-style-type: none"> <li>– <code>NotifyErr.tmp</code></li> <li>– <code>nicerror.tmp</code></li> </ul>

## Remarks 1:

*<LOGROOT> = <Deployment Service installation path>\tftp\log\ID#<Batch ID#>*

*Example*

*C:\Program Files\Fujitsu Siemens\DeploymentService\tftp\log\ID#13*

## Remarks 2:

*<HOSTNAME> = The name of the target system.*

*Example*

*C:\Program Files\Fujitsu Siemens\DeploymentService\tftp\log\ID#13\  
LOADER(RDBLADE15).ERR*

## Cloning of Linux Systems

Cloning Phase	Error Event	Where to find the log file(s)
At Mass Cloning of Standard Image (DOS)	<p>Possible cause of Linux-specific error:</p> <ol style="list-style-type: none"> <li>1. The target image has unknown distribution or unsupported version.</li> <li>2. The location of <i>/etc</i> specified by a user may be wrong.</li> <li>3. Specified IP address or subnetmask may be wrong.</li> </ol>	<p><b>Deployment Server</b></p> <p>One or any of the following error logs:</p> <ul style="list-style-type: none"> <li>– <code>&lt;LOGROOT&gt;\FJIMGBRS(&lt;HOSTNAME&gt;).ERR</code></li> <li>– <code>&lt;LOGROOT&gt;\LOADER(&lt;HOSTNAME&gt;).ERR</code></li> <li>– <code>&lt;LOGROOT&gt;\TFTP_ERR(&lt;HOSTNAME&gt;)</code></li> </ul> <p>Remarks 1; Remarks 2</p> <p><b>Target System</b></p> <p>One or any of the following logs:</p> <ul style="list-style-type: none"> <li>– <code>[RAMDRIVE] C:\LOADER.ERR</code></li> <li>– <code>[RAMDRIVE] C:\JFILECP.ERR</code></li> <li>– <code>[RAMDRIVE] C:\FJIMGBRS.ERR</code></li> </ul>
At Cloning of a single Snapshot-Image (DOS)		<p><b>Deployment Server</b></p> <p>One or any of the following error logs:</p> <ul style="list-style-type: none"> <li>– <code>&lt;LOGROOT&gt;\FJIMGBRS(&lt;HOSTNAME&gt;).ERR</code></li> <li>– <code>&lt;LOGROOT&gt;\LOADER(&lt;HOSTNAME&gt;).ERR</code></li> <li>– <code>&lt;LOGROOT&gt;\TFTP_ERR(&lt;HOSTNAME&gt;)</code></li> </ul> <p>Remarks 1; Remarks 2</p> <p><b>Target System</b></p> <p>One or any of the following logs:</p> <ul style="list-style-type: none"> <li>– <code>[RAMDRIVE] C:\LOADER.ERR</code></li> <li>– <code>[RAMDRIVE] C:\JFILECP.ERR</code></li> <li>– <code>[RAMDRIVE] C:\FJIMGBRS.ERR</code></li> </ul>
Cloning Phase: during post cloning/personalization		<ul style="list-style-type: none"> <li>– <code>/var/log/naconfig.log</code></li> <li>– all files in the <code>/var/log/remotedeploy/*</code> directory</li> </ul> <p>In addition get the following system files</p> <ul style="list-style-type: none"> <li>– <code>/var/log/messages</code></li> <li>– <code>/etc/resolv.conf</code> (when there are problems to set the DNS Server deployment configuration)</li> <li>– <code>/etc/sysconfig/network/*</code> (when there are problems to set the IP deployment configuration)</li> </ul>

Cloning Phase	Error Event	Where to find the log file(s)
Using a Custom Script (Linux)	<p>Possible cause of the error:</p> <ol style="list-style-type: none"><li>1. <i>ftp</i> command is not available.</li><li>2. The user name or password for ftp specified by a user might be wrong.</li><li>3. The specified path name of the script is not accessible.</li><li>4. The script is accessible, but the script fails to run correctly (exit code is not 0).</li></ol>	<p><b>Target System</b></p> <p><i>/etc/rc.d/ffsc.d/RDRRunOnce.err</i></p> <p><i>/etc/rc.d/ffsc.d/CLCOMP.DAT.err</i></p>

Remarks 1:

<LOGROOT> = <Deployment Service installation path>\tftp\log\ID#<Batch ID#>

Example

*C:\Program Files\Fujitsu Siemens\DeploymentService\tftp\log\ID#13*

Remarks 2:

<HOSTNAME> = The name of the target system.

Example

*C:\Program Files\Fujitsu Siemens\DeploymentService\tftp\log\ID#13\LOADER(RDBLADE15).ERR*

## 11.2 Frequently Asked Questions

nr.	Question	see Page
1	What do I need to know to be able to install Deployment Manager?	<a href="#">page 305</a>
2	What do I need to know to be able to use Deployment Manager?	<a href="#">page 306</a>
3	Which settings are carried out after the cloning process to configure the system as required?	<a href="#">page 307</a>
4	How come that I find that on Linux the IP address and the host name are not set after cloning?	<a href="#">page 307</a>
5	If I generate an image of a Red Hat Linux 7.2 and install this on a new server blade, will the settings for the IP address and the name in the deployment table of the management blade be transferred to the new Linux blade?	<a href="#">page 307</a>
6	Sometimes the DHCP server is not detected during PXE boot.	<a href="#">page 309</a>
7	I want to have all necessary deployment components in one blade system (deployment server, DHCP server, Deployment Manager and ServerView). To achieve this I want to install Windows 2000 on two of the five server blades and use the first as my deployment server. When I attempt to clone my second server blade 3, this server boots up and stops at the Windows 2000 logon prompt (prompting you to press <b>[Ctrl]-[Alt]-[Del]</b> ). If you then simply press the aforementioned key sequence, you are logged in automatically without prompting and sysprep begins. Why?	<a href="#">page 309</a>
8	A blade server completes sysprep and shuts down. It doesn't reboot automatically - I have to do this manually, whereby a PXE boot commences and the cloning begins. Why?	<a href="#">page 310</a>
9	The clone finishes and my blade 3 shuts down. When you refer back to the deployment server, the clone procedure completes successfully and you can see the images in your image folder. However, the deployment server does not indicate that the server has been cloned. It does however indicate that the deployment server is degraded. Is this the case?	<a href="#">page 311</a>
10	I have encountered some problems when I select a deployment server from the list and I am asked for a user name and password. I get the error <i>The login to server: REMOTEDEPLOY is incorrect. Open of CloningEngine engine failed. ScwOpenEngine failed: 0x274d/SCW Deployment Service not running.</i> The user I am trying to use is a user with administrator rights.	<a href="#">page 311</a>
11	While a cloning process is running, the management blade of the BX300 system affected is inaccessible. Why?	<a href="#">page 312</a>
12	How do I install Deployment Manager in a domain?	<a href="#">page 312</a>
13	Which shares are required for Deployment Manager and which are automatically created?	<a href="#">page 313</a>

Table 12: FAQ - Overview

nr.	Question	see Page
14	Which services must be installed and started for Deployment Manager?	<a href="#">page 313</a>
15	Is the SNMP protocol required for the deployment?	<a href="#">page 314</a>
16	How can I trace a deployment job?	<a href="#">page 314</a>
17	After remote deployment, I would like to use a different DHCP server from the one used for the original Deployment Manager installation. Must I re-install Deployment Manager? I have the PXE boot and the image creation working but not the cloning process.	<a href="#">page 314</a>
18	Error message: PXE boot of blade client leads to error: PXE-E51	<a href="#">page 315</a>
19	My computer continuously restarts when I start from a Sysprep image in Windows Server 2003?	<a href="#">page 315</a>
20	How to trace and store the SCW output on a Windows 2003 system?	<a href="#">page 315</a>

Table 12: FAQ - Overview



### 1. What do I need to know to be able to install Deployment Manager?

A so-called “deployment user” must be set up to provide a context for all deployment processes.

- This user is required for the installation of Deployment Manager and must be a member of the following three groups:
  - administrators (as named in OS language)
  - system group (as named in OS language)
  - “deployment admins” group (this membership is checked by the installer and added if necessary)
- Which server should be used as deployment server? This server must be on the same LAN segment as the target system(s) (only with the deployment method *Multicast*). A DHCP server must also be installed on this segment.
- If VLAN segments have been configured, it must be known which switch sockets have been allocated to which segment, so that it can be ensured that the deployment and DHCP servers and the target system, with its LAN port configured for PXE Boot, are all on the same segment.
- ServerView must be installed on the same server as Deployment Manager. The *Deployment Manager* package and *Deployment Services* package can be installed on different servers.

## 2. What do I need to know to be able to use Deployment Manager?

Deployment Manager takes over the administration of your computer for the supervision of time-controlled image creation and cloning procedures. The user must, however, remember that it is his/her task to ensure that the image will be used on more or less the same target hardware as the reference system from which the image was generated. The restrictions arise predominantly from the operating system's capability to communicate with generic hardware components.

The following system properties must be taken into account so that the cloned system can be booted:

- is it a single or multi-processor system?
- is the same type of processor used (clock frequency is not normally significant)?
- is the same boot device used in the same logical configuration?
- which RAID controller, SCSI disk, FC/SCSI controller of an external cabinet?
- is the same boot device listed in the BIOS-boot as first boot device?
- what is the RAID level on which the image is generated?
- if the RAID level for the cloning differs from that of the reference system, the resulting capacity must be such as to yield the same cluster size; if the cluster sizes differ, the image will be incompatible with the target system.
- is at least the minimum working memory installed for the operating system used?
- if the target system has more than one LAN port, which port is on the same LAN segment as the PXE server and is the port from which the PXE boot of the target system should be started?
- which IP addresses and host name are to be given to my target system? These values must be entered in the deployment table of each server (see [section "Management Blade Specific Deployment Table" on page 279](#)).
- how much hard disk space is available for an image repository? The minimum is the size of one image (standard W2k about 600 MB) but 10 GB or more is recommended, what is the IP address / host name of the file server to be used as an image repository? This is accessed in Deployment Manager when a repository is inserted.

### 3. Which settings are carried out after the cloning process to configure the system as required?

Cloning of a Linux image:

- files on the Linux system that have been modified by the cloning agent under DOS
  - */etc/sysconfig/network*
  - */etc/sysconfig/network-scripts/ifcfg-eth0*
  - */etc/sysconfig/network-scripts/ifcfg-eth1*
- by changing the paths, other Linux distributions can be adapted for this process.

### 4. How come that I find that on Linux the IP address and the host name are not set after cloning?

By default, the root drive of the Linux reference system is expected to be on */dev/sda2*. If the root drive is on another partition, this must be given during the creation process. If the entries do not agree, the IP address and host name will not be set.

When installed by ServerStart, Red Hat Linux 7.2 also sets */dev/sda2* by default. The cloning process itself remains unaffected by these settings.

### 5. If I generate an image of a Red Hat Linux 7.2 and install this on a new server blade, will the settings for the IP address and the name in the deployment table of the management blade be transferred to the new Linux blade?

**The server name and IP address settings in the deployment table of the management blade are not retained. After the deployment procedure, the settings return to the standard values. Is this correct?**

**After cloning, I get the error message, “Duplicate server name ....”.**

**Why does this happen?**

The deployment table in the management blade is the reference for all deployment settings, i.e. Deployment Manager takes the starting values from this table and uses them for cloning.

If the instruction is interrupted, these values are taken from there by Deployment Manager and passed to the cloning agent which transfers them to the target system.

With Linux, special tools are used with which the IP address and host name are set in the target system. This takes place directly from DOS and immediately after the cloning.

For Microsoft operating systems, these values are set using a RunOnce process and the original Microsoft tools, *Sysprep.exe*. Under some circumstances, this process can require several reboots (up to 3).

There are, however, for both Linux and Microsoft operating systems, SNMP agents for ServerView that periodically enter these values in the deployment table to maintain consistency between running operating systems and the deployment table. This has the advantage that only needs to change these values in the operating system and the most recently valid settings of the LAN parameters will always be found in the management blade.

If an enabled SNMP agent is cloned with the image, it can happen when cloning Microsoft operating systems that, on the first reboot of the cloned system, the SNMP agent still carries out this update procedure with the original reference server values. During the first two reboots (approx. 90 sec.) the cloned operating system continues to run with the old settings of the reference system. Since the LAN driver is turned off during this time, this should cause no problems. The agents, however, remain active and write the old values in the deployment table. Nevertheless, this is only a cosmetic problem, as the new values will be automatically written after 90 sec.

With Linux, the client is active with the new parameter values immediately after the first boot and this behavior does not occur.

With Linux and DHCP, Linux makes a record of the LAN configuration in a DHCP cache. This cache also contains the MAC address. So long as Linux uses this cache information for DHCP access, the old MAC address (from the reference system) will be given as a key, leading to the old IP address being leased and an addressing conflict on the network.

For this reason the cache file is deleted after cloning while still under DOS. This is no problem for the target system, as the file will be recreated on reboot. At the first reboot, this cache file does not yet exist on the target system, which then makes its request to the DHCP server using the new MAC address and is leased a new IP address.

If, however, the parameters in the cloned system are correct and the default values are nonetheless to be found in the management blade (IP address: 0.0.0.0, host name: \$DNS\$), it is recommended that the server blade should be configured by a service technician. A firmware update may be necessary.

If the message *Duplicated Servername* still occurs after a successful cloning process, the deployment user has defined at minimum two identical host names in the deployment table. If this is the case, Deployment Manager just reports this message as a warning, but the finally cloned targets does have received unique generated host names based on their MAC address to avoid a real conflict in the LAN segment. The warning is offered to check the deployment table for a correction.

## 6. Sometimes the DHCP server is not detected during PXE boot.

This happens if the first network port is not connected to a switch blade.

A switch blade installed in slot 1 is assigned to odd slot numbers and a switch blade in slot 2 is assigned to even slot numbers of CPU blades. Check this LAN configuration again (see also [section “Network Configuration” on page 45](#)).

**7. I want to have all necessary deployment components in one blade system (deployment server, DHCP server, Deployment Manager and ServerView). To achieve this I want to install Windows 2000 on two of the five server blades and use the first as my deployment server. When I attempt to clone my second server blade 3, this server boots up and stops at the Windows 2000 logon prompt (prompting you to press **[Ctrl] - [Alt] - [Del]**). If you then simply press the aforementioned key sequence, you are logged in automatically without prompting and sysprep begins. Why?**

In general it is possible to install Deployment Manager on a server blade but you must bear in mind these requirements:

- If you install Deployment Manager on a Windows 2000 server, service pack 2 or service pack 3 is required.
- If you install Deployment Manager on a Windows 2000 server with service pack 3, Management Blade Firmware version 1.12 or later is required.
- Deployment Manager is not supported on Windows 2000 domain controllers.
- Deployment Manager installed on a blade server may cause the error message *Duplicate server name exists* when Deployment Manager is started. To solve this issue, change the host name of the Deployment Manager server in the deployment table (WebUI - Deployment Configuration).
- Make sure that the ServerView Agent is not installed or activated on this blade (otherwise the host name in the deployment table will be automatically adjusted).

**8. A blade server completes sysprep and shuts down. It doesn't reboot automatically - I have to do this manually, whereby a PXE boot commences and the cloning begins. Why?**

If you create a (*sysprep*) image of e.g. a Windows 2000 server blade, the first boot of the server blade runs into the Windows 2000 logon prompt.

DO NOT LOG ON !!

There are some tasks running in the background (e.g. *sysprep* ...) and after about two minutes the server blade should automatically restart and boot into DOS via PXE to run the "Cloning Agent".

If your server blade still does not reboot:

1. Check the version of Deployment Manager (because this issue was a known problem until version 1.00.05).
2. Check the access (*ping*) from the deployment server (blade 1) to the server blade on which you want to create the image.
3. Do you have the correct password for the administrator account (of the server blade) entered in your Deployment Manager front-end?
4. Are your SNMP settings in the management blade correct? (Trap destination should be the IP of the deployment server: community: *public, read/create* ...)

**9. The clone finishes and my blade 3 shuts down. When you refer back to the deployment server, the clone procedure completes successfully and you can see the images in your image folder. However, the deployment server does not indicate that the server has been cloned. It does however indicate that the deployment server is degraded. Is this the case?**

There is no indication that you have created an image of blade 3 except when you look in the repository itself.

Later on, if you deploy (clone) this image to other blades (e.g. blades 5 and 7) these blades get the status *cloned*. That means only the target systems switch to the *cloned* status after deploying an image, not the “original” blade.

But your image creation process is not yet finished, and that’s the reason for the *degraded* status inside of ServerView.

By default, after the cloning engine has copied the image to the repository, the server blade boots again in Windows 2000 (with disabled network adapters - which is the reason for the degraded status in ServerView) and runs a rollback of the changes made during the first operating-system boot. After this rollback a 4th reboot (finalizing all tasks) reactivates the network interfaces and the image creation process is finished. The ServerView status should be corrected automatically as soon as the agents are active and connected to the LAN again.

**10. I have encountered some problems when I select a deployment server from the list and I am asked for a user name and password. I get the error *The login to server: REMOTEDEPLOY is incorrect. Open of CloningEngine engine failed. ScwOpenEngine failed: 0x274d/SCW Deployment Service not running*. The user I am trying to use is a user with administrator rights.**

The message *Deployment Service not running* does not point to a wrong account, but to a bad status of your services.

Please check whether these two services are installed on your deployment server:

- *Deployment Service* (start: automatic)
- *FSC Deployment Manager* (start: manual)

If the *Deployment Service* service is not installed, you must install the Deployment Service package ([section “Installing the Deployment Services Package” on page 67](#)).

Another possibility is that the user you have entered for using Deployment Manager is assigned to the above-mentioned services but someone has changed the password of this user. If this is the case, you must enter the right password in the *Properties – Log On* frame of each service assigned to that user as well.

Go to *Control Panel – Administrative Tools – Services*, select the listed services above and check the account info of each in the Property card *Log On*. There is a password field which must contain the same password as entered in the user administration. Unfortunately this is not done automatically by the Microsoft operating system.

### **11. While a cloning process is running, the management blade of the BX300 or BX 600 system affected is inaccessible. Why?**

This is caused by the multicast protocol which loads the management blade too heavily (as well as every other host on the segment that is not participating in the multicast protocol). By altering the IGMP settings in each switch in the segment, only the switch ports of the multicast protocol listeners are fed with the current cloning packet. Other switch ports do not then pass on this packet.

Alternatives:

- Use separate network segments for management blade and switch blade.
- With single network segment change IGMP setting of switch blade to *IGMP status: Enabled* and *Act as IGMP Querier: Enabled*

### **12. How do I install Deployment Manager in a domain?**

If you want to run Deployment Manager in a Windows 2000 domain with active directory and you want to assign an active directory domain user as Deployment Manager user, you must extend the user name to include the “backward-compatible domain name”, which is normally defined during creation of the active directory.

*Example*

AD domain name: *toptest.mch.fsc.net*

User: *deploy*

You must enter: *toptest\rddeploy* (as fully qualified user name)

If you are using a normal domain user you must enter:

*<domainname>\rddeploy*



### 13. Which shares are required for Deployment Manager and which are automatically created?

Two shares are created automatically:

- PMKit  
*<Deployment Service installation path>/DeploymentService/PMKit* used for preparation of Windows 2000.  
Rights: group *Deployment Admins* automatically set to *full control*
- SCWDB  
*<Deployment Service installation path>/DeploymentService/SCWDB* for the Deployment Manager database.  
Rights are automatically set to *administrators (local)*, *system*, *deployadmins* and *full control*.

One share is set manually:

- *<Image Repository path>* created manually by the customer.  
Rights: *<deployment user>* rights are looked up on the Deployment Manager.

The deployment engine and the deployment service must have read and write access to the share(s) for the image repository. These can, in principle, be two different users. If everything is installed on the deployment server and only one deployment server is used, an ordinary directory can also be used as repository and no shares are required.

### 14. Which services must be installed and started for Deployment Manager?

1. Deployment Service  
Description: "Fujitsu Siemens Computers Deployment Service"
2. PXE Services  
Description: "Fujitsu Siemens Computers PXE Services"
3. TFTP Service  
Description: "Fujitsu Siemens Computers TFTP Service"
4. FSC Deployment Manager  
Description: ""

**15. Is the SNMP protocol required for the deployment?**

Yes, ServerView and Deployment Manager make SNMP accesses to the management blade from the deployment server. The server blades do not make any use of SNMP.

The following commands from the SNMP set are used during deployment:

- Normal Power ON, Power OFF, PXE Boot on LAN Port 1 or 2
- Save master image reference
- Set cloning status
- Set complete deployment configuration table

With the new management blade firmware v1.34 it is possible and necessary to set the SNMP rights for Deployment Manager. By default the SNMP rights are set to *read only*. With the management blade firmware as of v1.34 you must set this rights to *read-write*.

**16. How can I trace a deployment job?**

A file named *dmdebug.txt* must be installed in the same directory as *DMEngine.exe*.

For Apache: `<ServerView installation path>\ServerView\Serverview  
Services\scripts\DeploymentManager`

For IIS: `\inetpub\scripts\DeploymentManager`

Only the actions of the *Deployment Manager* device are logged. There is no tracing facility for the current deployment service. To stop the debugging log, just change the file name.

**17. After remote deployment, I would like to use a different DHCP server from the one used for the original Deployment Manager installation. Must I re-install Deployment Manager? I have the PXE boot and the image creation working but not the cloning process.**

If, at the time of installing the cloning engine, a DHCP service was also installed on the deployment server and this is no longer to be used, the deployment service package must be re-installed so that the PXE service no longer runs in DHCP proxy mode but as a direct PXE service, directly on the port where the DHCP service used to run.

While the PXE client will obtain its IP address from this new DHCP service, the PXE service will search with a broadcast packet.

While nominating a Netboot service helps overcome the PXE packet limits, this is not sufficient, as this setting does not also apply for the multicast protocol so that PXE boot and image creation would work but not the cloning.

#### **18. Error message: PXE boot of blade client leads to error: PXE-E51**

In the switch blades configuration files the parameter *flow control* is set to *enabled*. The default value is *disable*. Set the parameter to *disable* and start the cloning process again.

#### **19. My computer continuously restarts when I start from a Sysprep image in Windows Server 2003?**

If a Windows Server 2003 image is created, please make sure that the telephone service is set to automatic or manually before doing the image creation. Otherwise W2k3 *Sysprep.exe* could remain in an endless mini setup loop.

Please see also at KB836426 of the Microsoft knowledge base under:  
<http://support.microsoft.com/>

#### **20. How to trace and store the SCW output on a Windows 2003 system?**

- Check the BIOS parameter *Continue C.R. after POST* on the server blade you want to create or deploy an image. [Note: Depending on the type of server blade this parameter might have a different name like "Console Redirection" with value "Enhanced".]

Set this BIOS parameter to *ON*.

- Open a telnet session with the parameter *f* to trace the image job. For example: *telnet -f <file name>.txt*
- Open the connection to the BX-System (*open <ip address> 3172*)
- Log on to the management blade, establish a console redirection to the server blade you want to create or deploy an image.
- Start in Deployment Manager the image creation process.
- The output data is stored in the *\*.txt* file.



---

## 12 High-Availability Support

As of version 4.0 you can use Deployment Manager in a high-availability configuration.

This means that

- the location of the databases (for *Deployment Manager* and *Deployment Services* packages) is configurable. It is possible to use an external filer as storage for the databases. The two databases for the two packages can be on different filers. A mapped network drive cannot be used.
- Deployment Manager can be installed on two servers which use the same databases. The *FSC Deployment Manager* and *Deployment Service* services are not started on the servers - it is up to the cluster software to start the services on the server that it elects to be the active one. Only one instance should run at the same time.
- The *FSC Deployment Manager* service and the *Deployment Service* service can detect the abnormal shutdown of the service (crash) and write a message to the event log.
- After a crash the *FSC Deployment Manager* service and the *Deployment Service* service can recover by setting the status of the jobs that were interrupted by the crash to *Error*.
- ACID support  
In databases, ACID stands for Atomicity, Consistency, Isolation, and Durability. These are considered to be the key transaction processing features of a database management system. Without them, the integrity of the database cannot be guaranteed.

### Requirements

Both servers must have the same host name and IP address. If there is cluster software available, this requirement should be provided by the cluster software. Otherwise this requirement can be achieved when the two servers are not up and running at the same time.

## 12.1 Installation

### 12.1.1 Operations Manager Installation

As a prerequisite, Deployment Manager needs access to a Operations Manager installation on the local server or on a remote server. The *Deployment Manager* package installer offers the *ServerView Operations Manager Location* window only when a *Full installation on first server* has been selected in the *High Availability* window. This window is not displayed when a *Limited installation on second server* is installed.

The parameters given in the *ServerView Operations Manager Location* window are added to the *Deployment Manager* database that is stored on a filer. In the failover scenario, the second server therefore uses the same Operations Manager location as the first server where the Operations Manager location has been entered.

For the configuration of the Operations Manager location, see [section “Installing the Deployment Manager Front-end Package” on page 58](#).



If both servers are members of a Windows cluster, you should select the cluster and not the currently active server when you add a new deployment server. You are allowed to add both servers to the list of deployment servers in addition, but this deployment server might not be accessible, depending on which host is the currently active one and has the *FSC Deployment Manager* service started.

#### Using two local Operations Manager installations

If the Operations Manager Installation is to be used, Operations Manager must be installed on both servers and the ServerView databases on both servers should be kept identical.

#### Using one remote Operations Manager installation

In this case Operations Manager must be installed on one remote server only and the servers must only be added to the ServerView database once.

## 12.1.2 Deployment Manager Installation

During the installation of the *Deployment Manager* package the *High Availability* window is displayed:

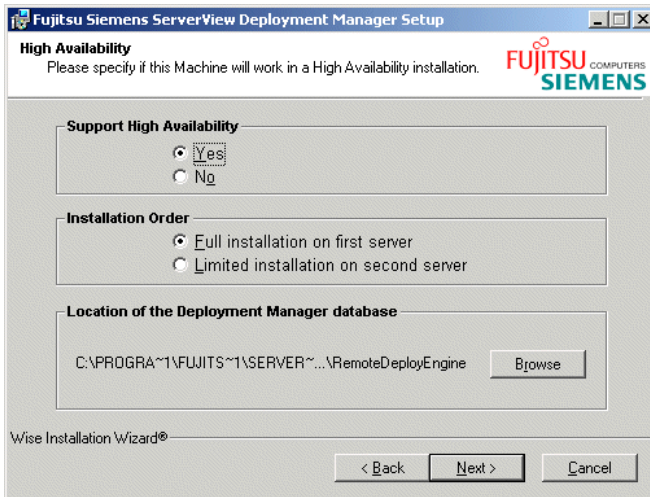


Figure 73: High Availability window - Support High Availability

### *Support High Availability*

Select the option *Yes*.

### *Installation Order*

#### *Full installation on first server*

If you select this option, the installation is similar to a standard installation without high availability but with the following differences:

- Specify a location of the Deployment Manager database that is accessible to the second server. The default value offered is only appropriate for a standard installation without high availability and must be changed to a directory in a mounted LUN (Logical Unit Number) on a filer. A mapped network drive cannot be used.

- The startup type of the *FSC Deployment Manager* service is set to *Manual* and the service is not started automatically after installation. It is up to the cluster software to start the service on the system that it elects to be the active one.

#### *Limited installation on second server*

As a prerequisite a *Full installation on first server* must already have been performed.

- Make sure that the location of the Deployment Manager database points to an already existing database on a filer. If the database is not found by the installer, an error message is displayed and the installation will fail. The database is not created if this option is selected.
- The startup type of the *FSC Deployment Manager* service is set to *Manual*. It is up to the cluster software to start the service on the system that it elects to be the active one.

## 12.1.3 Deployment Services Installation

During the installation of the *Deployment Services* package the *Destination Folder* window is displayed:

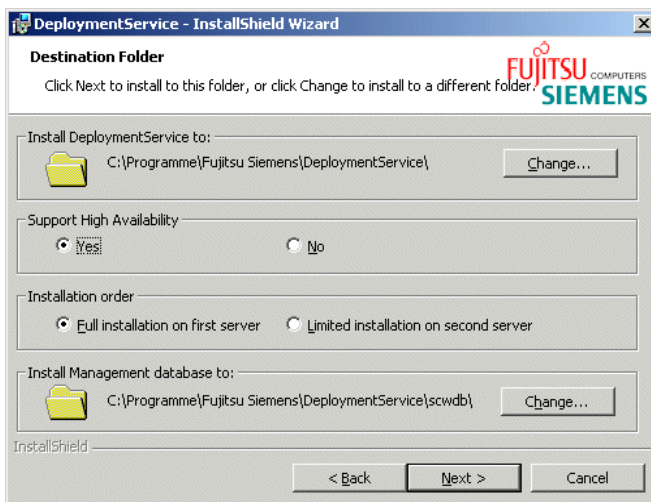


Figure 74: Destination Folder window - Support High Availability



*Support High Availability*

Select the option *Yes*.

*Installation order**Full installation on first server*

If you select this option, the installation is similar to a standard installation without high availability but with the following differences:

- Specify a location of the Deployment Service database that is accessible to the second server. The default value offered is only appropriate for a standard installation without high availability and must be changed to a directory in a mounted LUN on a filer. A mapped network drive cannot be used.
- The startup type of the *Deployment Service* service is set to *Manual* and the service is not started automatically after installation. It is up to the cluster software to start the service on the system that it elects to be the active one.

*Limited installation on second server*

As a prerequisite a *Full installation on first server* must already have been performed.

- Make sure that the location of the Deployment Service database points to an already existing database on a filer. If the database is not found by the installer, an error message is displayed and the installation will fail. The database is not created if this option is selected.
- The startup type of the *Deployment Service* service is set to *Manual*. It is up to the cluster software to start the service on the system that it elects to be the active one.

## 12.2 Hints

### 12.2.1 User Accounts

During installation of the *Deployment Manager* and *Deployment Services* packages, the user accounts for the *FSC Deployment Manager* service and *Deployment Service* service must be given. These user accounts are used to access the databases on the filer. The following combinations are recommended:

- During the installation the user specified a local account with the same name and password on both servers.
- During the installation on both servers the user specified the same domain account.

### 12.2.2 Repositories

Repositories should not be on one of the two servers, but in a directory in a mounted LUN on a filer or on a mapped network drive. When adding a repository, a UNC path name must be specified that is stored to the shared Deployment Manager database. Make sure that this UNC path is reachable from both servers.

### 12.2.3 Actions Needed When No Cluster Software is Available

Both servers do not have the *FSC Deployment Manager* and *DeploymentService* started after installation. It is assumed that some cluster software starts the services on the server that the cluster software elects to be the active one.

If there is no cluster software available, you must start the services on one of the servers (on one of the two servers that you elect to be the active one).

## 12.3 Failover Scenarios

### 12.3.1 Deployment Manager and Deployment Services Packages are Installed on Same Server

A typical failover scenario is:

- The first server crashes (more precisely: the server that has been selected as the active one by the cluster software crashes - it might as well be the server installed as the second server), *FSC Deployment Manager* service and *Deployment Service* service are not stopped correctly.
- The cluster software starts the *FSC Deployment Manager* service and *Deployment Service* service on the second server.
- The *FSC Deployment Manager* service and *Deployment Service* service on the second server detect that a crash has occurred.
- The *FSC Deployment Manager* service and *Deployment Service* service add event log entries.
- The *Deployment Service* service cancels all running jobs and marks the jobs with the status *Error* in the Deployment Service database.
- The *FSC Deployment Manager* service tries to cancel all running jobs. This does not work (because the *DeploymentService* service already canceled them), so the *FSC Deployment Manager* service marks the jobs with the status *Error* in the Deployment Manager database.

## 12.3.2 Deployment Manager and Deployment Services Package are Installed on Different Servers

In the following

- *first server Mgr/second server Mgr* denote the servers where the *Deployment Manager* package is installed.
- *first server Depl/second server Depl* denote the servers where the *Deployment Services* package is installed.

### The first server with the Deployment Manager package crashes

A typical failover scenario is:

- The *first server Mgr* crashes, the *FSC Deployment Manager* service is not stopped correctly.
- The cluster software starts the *FSC Deployment Manager* service on the *second server Mgr*.
- The *FSC Deployment Manager* service on the *second server Mgr* detects that a crash has occurred.
- The *FSC Deployment Manager* service adds an event log entry.
- The *FSC Deployment Manager* service tries to cancel all running jobs. This should work (because the *Deployment Service* service did not crash) and the *FSC Deployment Manager* service finally sets the status *Cancelled* in the Deployment Manager database. If the cancel does not work of the job, the *FSC Deployment Manager* service marks the jobs with the status *Error* in the Deployment Manager database.

**The first server with the Deployment Services packages crashes**

A typical failover scenario is:

- The *first server Depl* crashes, the *Deployment Service* service is not stopped correctly.
- The cluster software starts the *Deployment Service* service on the *second server Depl*.
- The *Deployment Service* service on the *second server Depl* detects that a crash has occurred.
- The *Deployment Service* service adds an event log entry.
- The *Deployment Service* service cancels all running jobs and marks the jobs with the status *Error* in the database.
- The *FSC Deployment Manager* service running on the *first server Mgr* finally retrieves the status from the *Deployment Service* service (reads status *Error* from Deployment Service database) and sets the status *Error* in the Deployment Manager database.



---

# 13 Appendix - Network Techniques

## 13.1 MAC Address Handling

The MAC (Media Access Control) address is a hardware address that uniquely identifies each node of a network.

There are several ways to find out the MAC address of a server:

- You can also unplug the server and read off the imprinted MAC address from the MAC/iSCSI address label on the rear side of the server.
- You can start the server and read off the MAC address on the information screen of the BIOS.

There are several ways to find out the MAC address of a server blade:

- If you have already configured the access via the management blade, you can use the management blade's Web interface (<http://<IP address of the management blade>>; default user: *root*; default password: *root*).
- You can also unplug the server blade and read off the imprinted MAC address from the MAC/iSCSI address label of the server blade.
- You can start the server blade and read off the MAC address on the information screen of the BIOS.

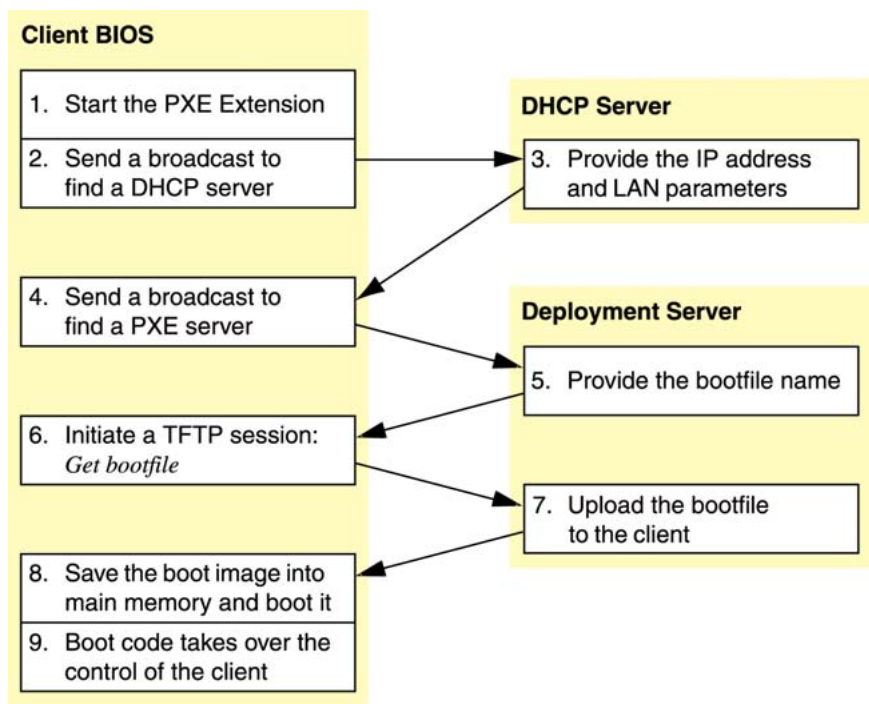
## 13.2 PXE

Short for Pre-Boot Execution Environment.

PXE is a boot mode of the LAN adapter. It does not become active until the system BIOS activates the LAN adapter as boot device during system boot and jumps to it. For this to happen, the LAN device must be set to the highest priority in the system BIOS boot device table. No jumpers are required for this.

PXE is a mandatory element of the WfM specification. To be considered compliant, the PXE must be supported by the computer's BIOS and its NIC.

## PXE Boot Algorithm



- 2-3 The boot process on the client side starts with a PXE broadcast to the DHCP server to receive a temporary IP address (mandatory).
- 4-5 A similar broadcast discovers the PXE boot server on port 67 or 4011 (depending on the information issued by the DHCP server) requesting a boot image name.
- 6-8 If the required information has been provided, a TFTP session is started to receive the boot image from the PXE server. The image size must not exceed 1.44 MB (floppy disk emulation mode). This boot image is copied to memory address 07C0h and started by the BIOS.
- 9 As long as the operating system kernel is not started and neither are the kernel drivers, any LAN access is performed using the PXE BIOS for further TFTP sessions.



## 13.3 DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol for assigning dynamic IP addresses to devices in a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static (reserved) and dynamic IP addresses.

**Further information on DHCP can be obtained at the following internet addresses:**

*Red Hat Linux 9: Red Hat Linux Customization Guide*

<http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/ch-dhcp.html>

*DHCP.org - Resources for DHCP (contains further Links)*

<http://www.dhcp.org/>

*ntfaq.com - Frequently asked questions concerning DHCP*

<http://www.ntfaq.com/Articles/Index.cfm?DepartmentID=774>

*DHCP-Handbook*

[http://www.dhcp-handbook.com/dhcp\\_faq.html](http://www.dhcp-handbook.com/dhcp_faq.html)

## 13.4 VLAN (Virtual Local Area Network)

The following VLAN description is based on blade servers.

A virtual LAN is a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them very flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

## VLAN Configuration

The PXE client running on the system does not support VLANs and does not send untagged frames.

VLAN requirements

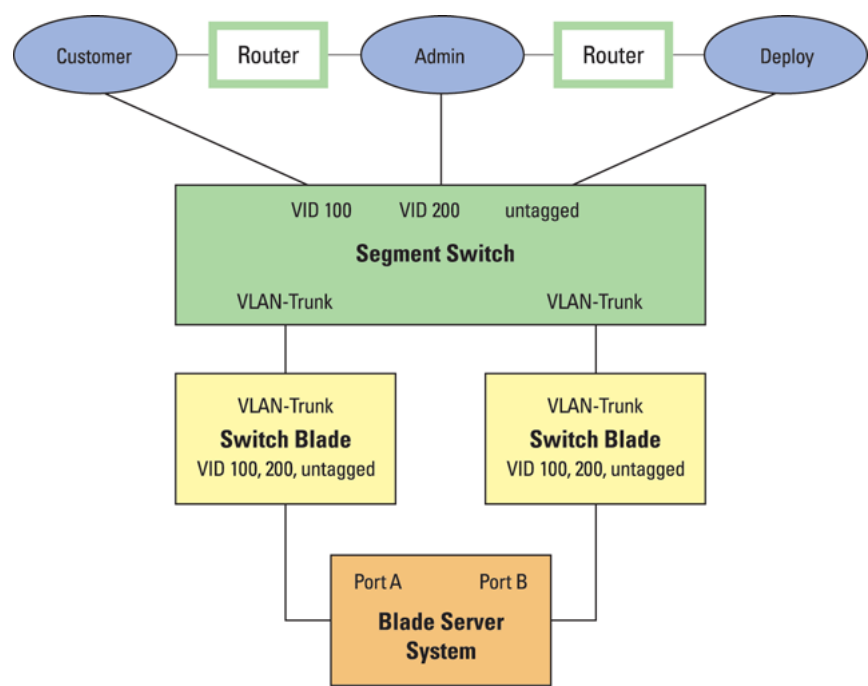
- The external switch in the LAN must support VLANs.
- The driver for the server network connectors (NIC) must allow integration in several VLANs.
- The image from the PXE server must already contain a driver which is pre-configured for VLANs.

## Example of a VLAN Configuration

- VLAN IDs must be assigned for all segments on the segment switch, except for the deploy segment.
  - I.e. data traffic toward the deploy segment is transmitted untagged.
  - If the PXE client sends an untagged frame, it is allocated to all three source ports by the switch blade. The untagged frame is only transferred to the untagged port (connected to the deploy segment) by the segment switch.
  - After the operating system has been booted on the server blade, it identifies several separate segments due to the VLAN configuration.
- All ports in the switch blade must recognize all VLAN IDs and must be configured for untagged frames at the same time. Even though the switch blade does not perform a segmentation, without VLAN configuration it would abandon all frames that carry a VLAN tag.

## Summary

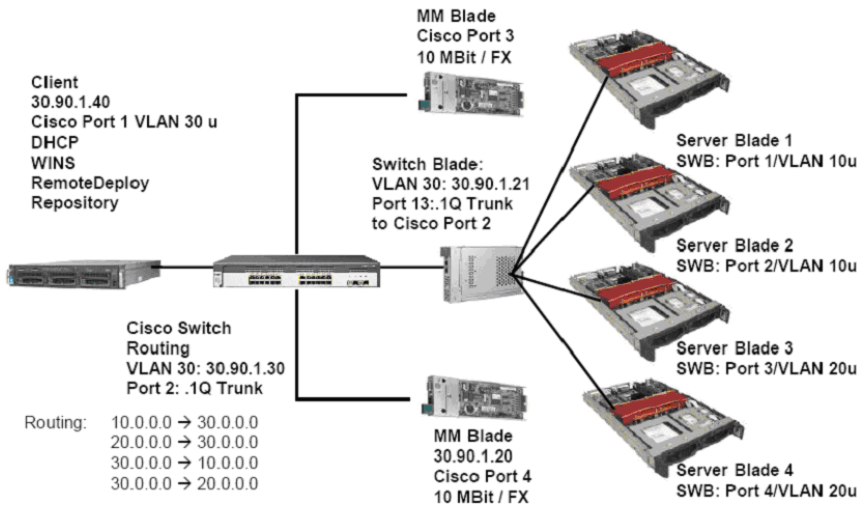
- PXE service data is only forwarded to the deploy segment.
- The VLAN configuration provides the splitting of segments after the boot process.
- Data exchange among the segments is only possible via a router.
- Full redundancy can be configured for both network controllers.



### 13.4.1 Example: Deployment over VLAN

The following example shows the deployment configuration of a BX300 blade server (contains one switch blade and four server blades) over VLAN.

#### Configuration / Preparation



**i** Make sure that an image is installed on all server blades.

*Configuration*

Client	30.90.1.40	255.0.0.0
Cisco switch	30.90.1.30	255.0.0.0
Switch blade 1	30.90.1.21	255.0.0.0
Switch blade 2	removed	255.0.0.0
Server blade 1	DHCP: 10.0.0.0	255.0.0.0
Server blade 2	DHCP: 10.0.0.0	255.0.0.0
Server blade 3	DHCP: 20.0.0.0	255.0.0.0
Server blade 4	DHCP: 20.0.0.0	255.0.0.0
Management blade	30.90.1.20	255.0.0.0

Connect the components, see figure above.

**Deploying images into different VLANS**

Requirements:

- Two VLANs which are not connected to each other. An image should be deployed into these VLANs from a third VLAN which is able to communicate with the other two.
- For the whole network you must have one deployment server, one DHCP server and one WINS server running.

Perform the following steps:

**1. Creating VLANs on the switch blades**

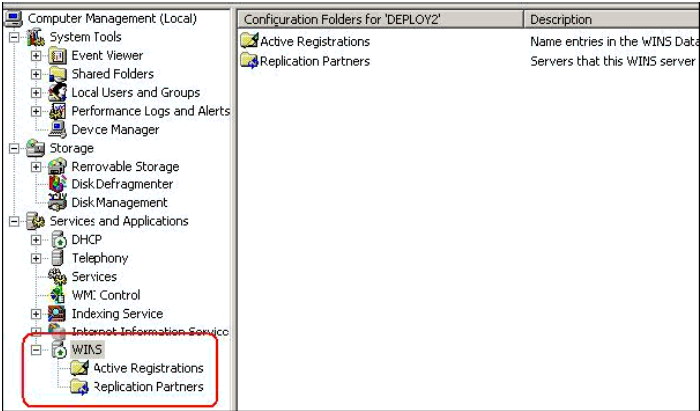
- Assign ports 1, 2 and 13 to VLAN 10 untagged and remove them from VLAN 1 or any other VLANs.
- Set PVID for ports 1 and 2 to 10 only.
- Assign ports 3, 4 and 13 to VLAN 20 untagged and remove them from VLAN 1 or any other VLANs. Leave port 13 in VLAN 10 also.
- Set PVID for ports 3 and 4 to 20 only.
- Assign port 13 to VLAN 30 untagged.
- Create a .1Q Trunk on port 13 and connect it to Cisco port 2. (Set frame type to tagged in egress rules (VLAN port configuration).)
- Assign VLAN 30 the IP address: 30.90.1.21 for the switch management (with CLI).

2. Creating VLANs on the Cisco switch

- Create a .1Q Trunk on port 2 which is connected to the switch blade.
- Assign port 1 to VLAN 30 untagged which is connected to the client.
- Assign VLAN 30 the IP address: 30.90.1.30 for the switch management

3. Configuring the client

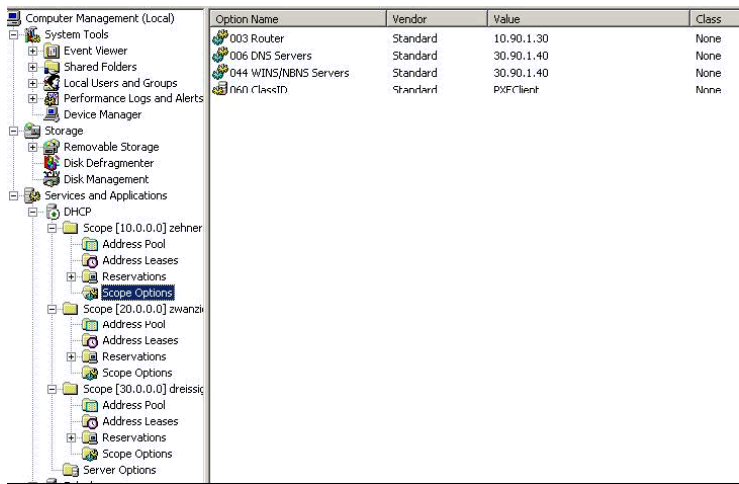
- Install a WINS\_Server on the client and configure it.
- Under *Control panel – Add/Remove Programs – MS Components – Network Services*, add WINS.



No configuration is necessary for WINS.

- Configure the DHCP server so that there is a range for each subnet:

	Range	WINS (044)	Gateway (003)
VLAN 10	10.90.1.1 to .10	30.90.1.40	10.90.1.30
VLAN 20	20.90.1.1 to .10	30.90.1.40	20.90.1.30
VLAN 30	30.90.1.1 to .10	30.90.1.40	30.90.1.30

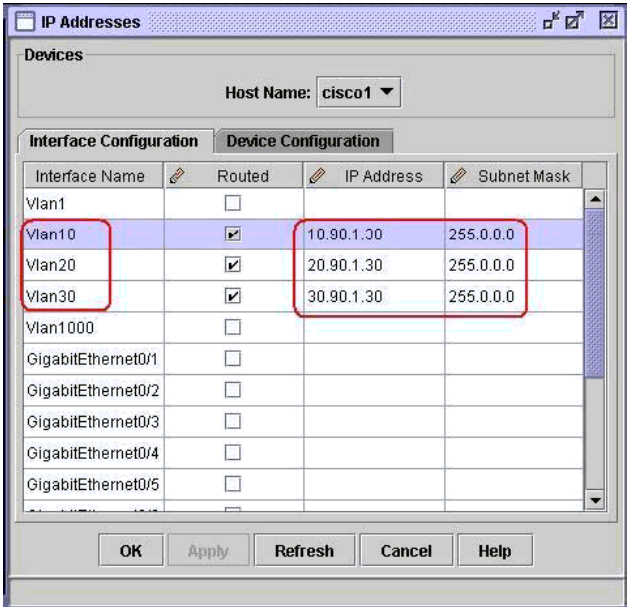


- Set up MMB with a new IP address (30.x.x.x)
- Set Cisco ports 3 and 4 to static access VLAN 30 and 10 Mb/s full or half duplex (depends on the MMB setting).
- Try to ping the server blades in VLAN 10 and VLAN 20 from the client. Also ping switch blade 1, management blade and Cisco switch. What IP address do they have? What is the result?

	IP address	Result of ping
Server blade 1		
Server blade 2		
Server blade 3		
Server blade 4		
Switch blade		
Management blade		
Cisco switch		

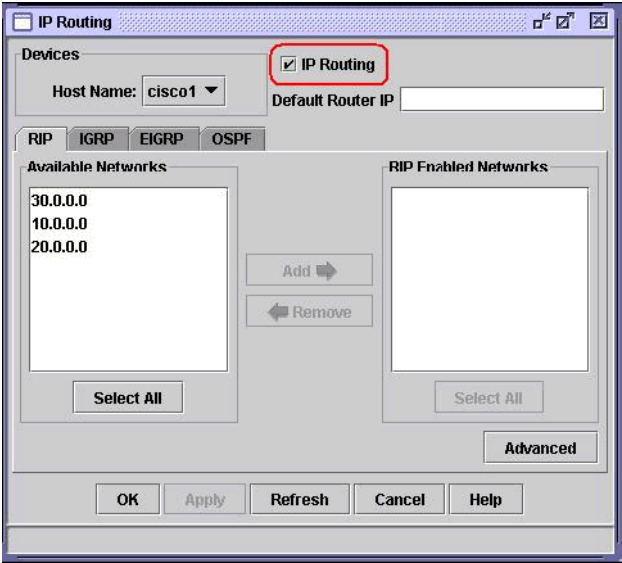
Is your result okay? Why?

4. Configuring routing on the Cisco switch (part 1)
- Create Vlan 10 and Vlan 20 under *Vlan – Vlan – Configure Vlans*.
  - Assign each VLAN an IP address.  
Under *Administration – IP Addresses*:



- Remove the IP address for *Vlan1*.
- Click *Apply*.
- Enable *IP Routing* under *Device – IP-Routing – Protocols*. Set the check mark to enable IP routing for 3550:





- Click *Apply*. For 3750 under *Device – IP-Routing – Protocols* select *enable/disable*.
- Try to ping the server blades in VLAN 10 and VLAN 20 from the client. Also ping switch blade 1, management blade and Cisco switch. What IP address do they have? What is the result?

	IP address	Result of ping
Server blade 1		
Server blade 2		
Server blade 3		
Server blade 4		
Switch blade		
Management blade		
Cisco switch		

Is your result okay? Why?

- Enable the *IP-Helper* function.  
You must configure a relay device when a switch sends broadcast packets that need to be responded to by a host on a different LAN. Examples of broadcast packets that the switch might send are DHCP, DNS and, in some cases, TFTP packets. You must configure this relay device to forward received broadcast packets on an interface to the destination host. If the relay device is a Cisco router, enable IP routing (ip routing global configuration command), and configure helper addresses by using the ip helper-address interface configuration command.

```
Cisco CLI:
en
conf t
int vlan 10
ip helper-address 30.90.1.40
```

Same for VLAN 20 with the same address.

- Enable the forwarding for UDP ports:  
Cisco CLI (Global parameter (config))  
en  
conf t  
ip forward-protocol udp (portnumber)

Do this for the ports *Bootps* 67, *Bootpc* 68 and *TFTP* 69.

5. IP address for server blades

- Execute an *ipconfig /release* and *ipconfig /renew* in the DOS window for each server blade.
- Then execute an *ipconfig /all*. Fill out the following lines.

	IP address	gateway	WINS	ping
Server blade 1				
Server blade 2				
Server blade 3				
Server blade 4				

- Try to ping the server blades in VLAN 10 and VLAN 20 from the client. Fill out the column above.

- Try to ping from a server blade in VLAN 10 and the VLAN 20 server blade.

What is the result? \_\_\_\_\_

#### 6. Configuring routing on the Cisco switch (part 2)

In order to define a secure routing, you must create an access list:

- Create an access list:

```
conf t
access-list 100 deny ip 10.0.0.0 0.255.255.255 20.0.0.0
0.255.255.255
access-list 100 permit ip any any
access-list 110 deny ip 20.0.0.0 0.255.255.255 10.0.0.0
0.255.255.255
access-list 110 permit ip any any
interface VLAN10
ip access-group 100 in
interface VLAN20
ip access-group 110 in
```

- Try to ping from a server blade in VLAN 10 and the VLAN 20 server blade.

What is the result? \_\_\_\_\_

- Try to ping the server blades in VLAN 10 and VLAN 20 from the client.

What is the result? \_\_\_\_\_

- Enable multicast routing:

```
conf en
Password: fsc
cisco1#conf t
cisco1(config)#ip multicast-routing distributed (on
Cisco 3750)
cisco1(config)#ip multicast-routing (on Cisco 3550)
Enable PIM Dense:
cisco1(config)#int vlan 10
cisco1(config-if)#ip pim dense-mode
cisco1(config-if)#exit
cisco1(config)#int vlan 20
cisco1(config-if)#ip pim dense-mode
```

```
cisco1(config-if)#exit
cisco1(config)#int vlan 30
cisco1(config-if)#ip pim dense-mode
```

```
cisco1(config-if)#exit
```

- Check IGMP snooping (it should be enabled by default)

```
cisco1#sh ip igmp snooping
vlan 1
```

```
-----
```

```
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
vlan 10
```

```
-----
```

```
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
vlan 20
```

```
-----
```

```
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
vlan 30
```

```
-----
```

```
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
```

**Deploying**

Now the entire configuration is ready for deploying:

1. First try to save the image from server blade 1.
2. Once the save process is complete, try to deploy this new image on server blades 2 - 4.



---

## Related Publications

The documentation for the PRIMERGY manuals can be found on the ServerBooks DVD supplied with each server system.

The documentation can also be downloaded free of charge from the Internet: You will find an overview of online documentation available on the Internet at <http://manuals.fujitsu-siemens.com/serverbooks/navigation/sv-suite-en.htm>.

- [1] **ServerView Suite  
Basic Concepts**
- [2] **PRIMERGY Glossary**
- [3] **PRIMERGY Abbreviations**
- [4] **Secure PRIMERGY Server Management  
Enterprise Security**  
PRIMERGY server management for secure,  
highly available platforms  
White Paper
- [5] **PRIMERGY ServerView Suite  
ServerStart/Installation Manager**  
User Guide
- [6] **PRIMERGY ServerView Suite  
Deployment Manager**  
User Guide
- [7] **PRIMERGY ServerView Suite  
Installation under Windows**  
User Guide
- [8] **PRIMERGY ServerView Suite  
Installation under Linux**  
User Guide
- [9] **PRIMERGY ServerView Suite  
Operations Manager**  
Server Management  
User Guide

## Related publications

---

- [10] **PRIMERGY ServerView Suite  
Inventory Manager**  
ServerView  
User Guide
  
- [11] **PRIMERGY ServerView Suite  
Archive Manager**  
ServerView  
User Guide
  
- [12] **PRIMERGY ServerView Suite  
Asset Management**  
Command Line Interface  
User Guide
  
- [13] **PRIMERGY ServerView Suite  
ServerView RAID Manager**  
User Guide
  
- [14] **PRIMERGY ServerView Suite  
AlarmService**  
ServerView  
User Guide
  
- [15] **PRIMERGY ServerView Suite  
Performance Manager**  
User Guide
  
- [16] **PRIMERGY ServerView Suite  
Download Manager**  
ServerView  
User Guide
  
- [17] **PRIMERGY ServerView Suite  
Update Manager**  
ServerView  
User Guide
  
- [18] **PRIMERGY ServerView Suite  
PrimeUp**  
User Guide



- [19] **PRIMERGY ServerView Suite  
Bootable Update CD**  
User Guide
- [20] **PRIMERGY ServerView Suite  
ServerView S2 Online Diagnostics**  
User Guide
- [21] **PRIMERGY ServerView Suite  
Local View**  
User Guide
- [22] **PRIMERGY ServerView Suite  
Customer Self Service (CSS)**  
User Guide
- [23] **PRIMERGY ServerView Suite  
PrimeCollect**  
User Guide
- [24] **PRIMERGY ServerView Suite  
ServerView Integration**  
Overview
- [25] **PRIMERGY ServerView Suite  
ServerView Integration in Microsoft SMS**  
User Guide
- [26] **PRIMERGY ServerView Suite  
ServerView Integration in Microsoft Operations Manager**  
User Guide
- [27] **PRIMERGY ServerView Suite  
ServerView Integration in Novell Remote Manager**  
User Guide
- [28] **PRIMERGY ServerView Suite  
ServerView Integration in HP OV NNM**  
User Guide
- [29] **PRIMERGY ServerView Suite  
ServerView Integration in HP OV Operations**  
User Guide

## Related publications

---

- [30] **PRIMERGY ServerView Suite  
ServerView Integration in Tivoli NetView**  
User Guide
- [31] **PRIMERGY ServerView Suite  
ServerView Integration in Tivoli/TEC**  
User Guide
- [32] **PRIMERGY ServerView Suite  
ServerView Integration in DeskView**  
User Guide
- [33] **PRIMERGY ServerView Suite  
Remote Management**  
User Guide
- [34] **PRIMERGY ServerView Suite  
iRMC - integrated Remote Management Controller**  
User Guide
- [35] **PRIMERGY ServerView Suite  
iRMC S2 - integrated Remote Management Controller**  
User Guide
- [36] **Baseboard Management Controller (BMC)  
Configuration for PRIMERGY Systems**  
User Guide
- [37] **RemoteView Service Board**  
Installation Guide
- [38] **RemoteView Service Board S2**  
User Guide
- [39] **RemoteView Service Board S2**  
Installation Guide
- [40] **PRIMERGY BX300 Blade Server System**  
Operating Manual
- [41] **PRIMERGY BX600 Blade Server System**  
Operating Manual

- [42] **PRIMERGY Blade Server System  
RemoteView Management Blade**  
User Interface Description  
User Guide
- [43] **PRIMERGY Blade Server System  
LAN Switch Blade**  
User Interface Description  
User Guide
- [44] **BIOS-Setup**  
Description
- [45] **PRIMEPOWER ServerView Suite**  
System Administration within a Domain  
User Guide
- [46] DuplexDataManager® für Windows NT  
**DuplexWrite**  
Product Manual
- [47] DuplexDataManager® for Windows NT  
**MultiPath**  
Product Manual
- [48] DuplexDataManager® for LINUX  
**DuplexWrite**  
Product Manual
- [49] **StorMan**  
Provisioning and managing virtualized storage resources  
Administrator and User Guide
- [50] **APC network management card**  
User's Guide
- [51] **VMware ESX Server**  
Installation Guide
- [52] **VMware ESX Server**  
Administration Guide



---

# Index

## A

- Add Server(s) window [159, 188](#)
- add-on packages [41](#)
- adding [126](#)
  - bare server [91](#)
  - bare server by MAC Address [104](#)
  - new deployment server [120](#)
  - new license [124](#)
  - repository [125](#)
  - server [91](#)
  - server blade to a deployment group [238](#)
  - server to a deployment group [159](#)
  - server to an installation group [188](#)
- All Primergy [31](#)
- assigning, configuration file [189](#)
- automatic recovery [277, 283](#)
- automatic system preparation [256](#)

## B

- bare server
  - add to the server list [91, 257](#)
- Baseboard Management Controller (BMC) [179](#)
- Batch Result window [178](#)
- batch result, displaying [109](#)
- Blade optimized [31](#)
- blade server [22](#)
- BMC
  - access [179](#)
  - cloning [179](#)
  - deleting [183](#)
  - deployment configuration [182](#)
  - displaying [180](#)
  - displaying in Deployment Manager [181](#)
  - in Operations Manager [180](#)
  - installing [179, 184](#)
- Boot Image Path [170](#)

- Boot Image Type [170](#)
- Boot Images tab [125](#)
- bridge configuration [268](#)

## C

- changing the deployment server [119](#)
- chassis serial number [281](#)
- clcomp.dat [264](#)
- clearing site-cache [74](#)
- Client Agent package [138](#)
- cloning [29, 155](#)
  - Add Server(s) window [188](#)
  - BMC [179](#)
  - Create a Scheduled Task window [164, 195](#)
  - New Deployment Group window [156](#)
  - phases [30](#)
  - post preparation [32](#)
  - preparation of a deployment server [225](#)
  - process [23, 31](#)
  - process flow [258](#)
  - select server for deploy job [167](#)
  - status [288](#)
  - system preparation [31, 250](#)
- Cloning Images tab [125](#)
- cloning module [39](#)
  - requirements [37](#)
- cloning process [29, 155](#)
  - phases [252](#)
  - progress [178](#)
  - result [29](#)
  - starting [162](#)
- cloning session
  - details [250](#)
- configuration file [34, 194, 272](#)
  - 1/N relationship [272](#)
  - assigning [189](#)
  - N/N relationship [272](#)

- ServerStart/Installation Manager 34
- URL 276
- configuration for Windows 2008 72
- configuring
  - target systems 239
  - Windows Firewall 138
- Create a Scheduled Task
  - window 164, 195
- creating
  - deployment group 156
  - evaluation key 60
  - image 226
  - image repository 52
  - new folder 125
  - new image folder 126
  - new installation group 186
  - scheduled task 141, 142, 163, 164, 194, 195
- customer image 258
- customer script, executing 174
- D**
- default gateway, server blade 281
- defining
  - deployment group 235
  - image repository 228
  - name of the image file 145
  - options for the image creation process 147
- deleting
  - BMC 183
  - folder 125
  - log entries 111
  - repository 127
  - task 109
- Deploy Image wizard 106, 163
- deploying
  - image to server blades 241
- deployment 19
  - example 253
- deployment configuration
  - BMC 182
  - export 128
  - import 129
  - starting 239
- Deployment configuration for "server" window 114
- deployment cycle
  - cloning 23
  - mass remote installation 33
- deployment environment 36
- deployment group 29, 155, 249
  - adding server 159
  - adding server blades 238
  - creating 156
  - defining 235
  - modifying 158
  - properties 158
  - removing 157
  - removing server 159, 160
  - viewing 158
- Deployment Manager 44
  - architecture 36
  - button 78
  - Deployment View 83, 86
  - engine 39
  - exiting 122
  - front-end 77
  - front-end tasks 82
  - installation 41, 57
  - installation packages 41
  - Installation View 83, 88
  - main window 82
  - management platforms 36
  - menu bar 82
  - operating systems 36
  - package 14, 41
  - Physical View 83, 84
  - scheduled tasks 82
  - software architecture 39
  - software package 58
  - start window 57, 79
  - starting 78
  - task bar 82
  - uninstalling 74
  - upgrading 74
  - using 77

- Web Server 14, 36
  - Deployment Manager "Power Control"
    - window 112
  - deployment method 174
    - multicast 267
    - unicast 267
  - deployment platform
    - WinPE MDP 131
  - deployment procedures 19
    - cloning 19
    - mass remote installation 19
  - deployment process 201
    - controlling 249
  - deployment server 19, 39, 43, 119
    - adding 120
    - adding a new 120
    - available software packages 16
    - changing 119
    - installing DHCP server 203
    - installing ServerStart/Installation Manager 205
    - Login window 226
    - preparation 119, 202
    - preparation for cloning 225
    - removing 120
    - requirements 202
    - selecting 80, 226
    - software packages 37, 44
    - user account 81
    - user authentication 81
  - deployment service 61
    - installation 81
    - removing 74
    - software package 67
  - Deployment Services
    - package 14, 41
  - deployment software 43
  - deployment status 278, 288
    - server blade 283
  - deployment table 30, 34, 249, 274
    - basic initialization 285
    - export 286
    - import 286
    - management blade 279
    - master 275
      - of the management blade 234
  - Deployment Tables tab 126
  - Deployment View 83, 86
    - functions 87
  - DHCP 329
  - DHCP manager 204
  - DHCP server
    - installing on deployment server 203
  - DHCP service 37, 45
  - displaying
    - batch result 109
    - BMC 180, 181
    - deployment groups 86
    - existing PRIMERGY servers 84
    - installation group properties 191
    - installation groups 88
    - log entries 109
    - server information 90
    - the event log 109, 110
  - documentation, structure 11
  - Dynamic Host Configuration Protocol 329
- E**
- Edit menu 121
  - editing, task settings 109
  - Event Log window 110
  - event log, displaying 109, 110
  - executing, customer script 174
  - exiting Deployment Manager 122
  - Expand last partition to whole disk 170
  - exporting
    - deployment configuration 128
    - deployment table 286
- F**
- FC device 261
  - file
    - image\_file\_name.cfg 133
    - image\_file\_name.img 133
    - image\_file\_name.txt 133

- InstallLog.txt 296
- localipaddress.txt 45, 52
- RDSetup.exe 57
- File and Printer Sharing (SMB-In) 138
- File menu 121
- file system
  - format 262
  - formatting 261
  - supported 134
- file-system-dependent
  - image creation 27, 134
- file-system-independent
  - image creation (raw mode) 27, 135
- files of an image 133
- frequently asked questions 303
- Front-end tasks 106
- Front-end Tasks button 82
- functions
  - from the Deployment View 87
  - in the Installation View 88
- fw\_setting.vbs script 72
- G**
- Generic Boot Image 31
- generic server 20
  - requirements for deployment 20
- Global Options 131
- GUID 275
- H**
- Help menu 122
- host name 275
  - operating system related 281
- hot replacement 277
- hub configuration 268
- I**
- IDE drive 260
- IGMP settings 49
- IIS Web server 53
- image
  - consisting files 133
  - image creation 27, 133, 226, 264
    - create scheduled task 141
    - file-system-dependent 27, 134
    - file-system-independent (raw mode) 135
    - methods 27
    - operating systems 136
    - process 225
    - progress 152
    - Progress window 152
    - raw mode 133
    - raw mode requirement 37
    - select image path 145
    - snapshot image 133
    - starting 151
  - image creation (raw image creation)
    - file-system-independent 27
  - image creation process 28
    - defining options 147
    - starting 133
  - image deploying, to server
    - blades 235
  - image file
    - defining the name 145
    - information 146
    - URL 275, 281
  - image folder, creating a new
    - folder 126
  - Image Information, window 146
  - image repository 28, 39, 125, 133
    - defining 228
    - selecting 145
  - importing
    - deployment configuration 129
    - deployment table 286
  - Inbound Rules 138
  - Installation Configuration tab 125
  - installation group 34, 185, 249, 272
    - adding server 188
    - assigning configuration files 34
    - creating a new 186
    - displaying properties 191
    - properties 191
    - removing 188



- removing servers 190
- installation packages of Deployment Manager 41
- installation status 288
- Installation View 83, 88, 185
  - functions 88
- installing
  - BMC 179, 184
  - Deployment Manager 41, 57
  - on Windows 2008 53
  - Operations Manager 42
  - server 194
  - server blade 218
  - ServerStart/Installation Manager 42
  - ServerView SNMP agents 43
  - SNMP Agents 247
- Internet Group Management Protocol (IGMP) 46
- IP address, server blade 281
- IPMI (Intelligent Platform Management Interface) 21
- ISCSI device 261
- J**
- JavaRuntimeEnvironment
  - package 41
- Job API packages 41
- Job API Tandem 40
- K**
- Kalypso 21
- L**
- LAN
  - connection 49
  - environment 38
  - path to master image 249
- LAN port 46
  - other 52
- LAN status 276
  - server blade slot 282
- license key 60
- license management 123
- local installation 25
  - server blade 202
- log entry
  - deleting 111
  - displaying 109
  - status 111
- logging file
  - for error diagnostic 297
  - for Installation 296
- logical groups 249
- Login window 81
  - of the deployment server 226
- M**
- MAC address 30, 221, 249, 275, 327
  - management blade 249
  - server blade 281
- main window
  - Deployment Manager 82
  - Operations Manager 78
- management blade 22
  - deployment table 234, 279
  - SNMP API 249
- management blade deployment table
  - basic initialization 287
- management console 36
- managing, server blade 247
- manual system preparation 256
- mass remote installation 33
  - Linux 270
  - power status control 273
  - process 33
  - process flow 269
  - status 273
  - Windows 269
- master deployment table 275
- master image, LAN path 249
- menu bar 82
- menus 121
- modifying
  - deployment group 158
- multi-boot operating system 262
- multicast IP protocol 267
- multicast protocol 45

Multiple Segment Cloning 50

## N

NDIS driver

add to Deployment Manager 263

network configuration 45

New Deployment Servers

window 120

New installation group window 186

new license, adding 124

new repository 126

New Server window 92

notational conventions 17

## O

operating system

multi-boot 262

supported for image creation 15

Operations Manager 39, 180

installing 42

main window 78

starting 77

Options window 131

other LAN port 52

## P

package

available on the deployment

server 16

Client Agent 138

Deployment Manager 14, 41

Deployment Service 41

Deployment Services 14

JavaRuntimeEnvironment 41

Job API 41

ServerStart/Installation

Manager 41

partitioning 261

password for administrator

account 278

physical groups 249

physical LAN port list 275

Physical View 83, 84

post preparation 251

power control 112, 250

management blade 254

status 34

power status 282

server 112

power status control

mass remote installation 273

preparing

deployment server 202

server 119

server systems 19

PRIMERGY server 21

progress

of a cloning process 178

of the image creation 152

Progress window 152

Properties of Deployment Group

"group" window 158

properties, installation group 191

PXE 327

Boot-Algorithm 328

protocol 266

service 37, 44

## R

RAID

device 260

level 171

raw image creation 27

RDSetup.exe file 57

recovery

automatic 277, 283

reference image 28

reference installation 24

local 25

mass remote 33

methods 25

of a server blade 202

phases 24

remote 26

reference system 24

configuring Windows Firewall (on

Windows 2008) 138

with Windows 2008 138

- RemControl.dll 250
- remote control API
  - RemControl.dll 254
- remote installation
  - five clients 26
  - process 34
  - server blade 202, 221
  - unlimited clients 33
- remote installation group 272
- Remote Installation window 194
- Remote Installation wizard 106, 194
- removing
  - deployment group 157
  - deployment server 120
  - deployment service 74
  - installation group 188
  - servers from a deployment group 159
  - servers from an installation group 190
- renaming a task 109
- repository
  - adding a new 126
  - deleting 127
  - folder 272
  - management 125
- Repository Manager window 125
- requirements, Deployment Manager 42
- roaming 289
  - LAN parameters 289
  - process 292
- S**
- Save Disk Image for "server" wizard 140
- Save Disk Image wizard 106, 141
- Save Options window 147
- scheduled task 106
  - creating 141, 142, 163, 194
  - for cloning process 163
  - for image creation 141
  - for remote installation 194
  - status 107
- Scheduled Tasks
  - button 82, 106
  - window 106
- Scheduler Options window 142
- script fx\_setting.vbs 72
- SCSI drive 260
- Select Deployment Server window 119
- Select Image Path window 145
- Select Server(s)
  - for Deploy Job window 166
  - for Installation Job window 197, 198
- Select System Preparation Method for Deploy Job window 160
- selecting
  - deployment server 80, 226
  - image path 145
  - image repository 145
- Selecting Deployment Server window 80
- serial number 275
- SerStartBatch.ini 272
- server
  - adding to deployment table 285
  - blade 22
  - generic 20
  - preparing 119
  - PRIMERGY 21
  - specifying host name 115
  - specifying LAN port 117
- server blade 22
  - default gateway 281
  - deploying an image 241
  - image deploying 235
  - information 90
  - IP address 281
  - local installation 202
  - MAC address 221
  - managing 247
  - power status 282
  - reference installation 202
  - remote installation 202, 221
  - slot Id 281

- server detection
    - bare server [23](#)
  - server list, periodically check [83](#)
  - server status, modifying [285](#)
  - ServerStart/Installation Manager [44](#)
    - Classic Raid Preparation [160](#)
    - configuration file [34](#)
    - extension [39](#)
    - installation [42](#)
    - installing on the deployment server [205](#)
    - MDP Raid Preparation [160](#)
    - package [41](#)
  - ServerView
    - database [23](#), [39](#), [41](#)
    - server list [77](#)
  - ServerView SNMP Agent,
    - installation [43](#)
  - Set Arguments
    - for Deploy Job window [174](#)
    - for Installation Job window [199](#)
  - site-cache, clearing [74](#)
  - slot
    - LAN status [282](#)
  - slot ID [275](#)
    - server blade [281](#)
  - snapshot image [28](#), [148](#)
  - SNMP (Simple Network Management Protocol) [21](#)
  - SNMP Agents installing [247](#)
  - SNMP API of the management blade [249](#)
  - software package
    - Deployment Manager [44](#), [58](#), [67](#)
    - Deployment Service [67](#)
  - specifying
    - host name for servers [115](#)
    - LAN port for servers [117](#)
  - start window of Deployment Manager [57](#)
  - starting
    - a task [109](#)
    - cloning process [162](#)
    - deployment configuration [239](#)
    - Deployment Manager [78](#)
    - image creation process [133](#)
    - Operations Manager [77](#)
      - via a link [78](#)
      - via Operations Manager [78](#)
      - via the Windows start menu [78](#)
  - status
    - log entry [111](#)
    - scheduled task [107](#)
  - stopping a task [109](#)
  - storage device
    - FC and ISCSI [261](#)
    - RAID [260](#)
    - SCSI/IDE drive [260](#)
  - subnet mask [281](#)
    - server blade [281](#)
  - supported
    - file systems [134](#)
    - operating systems [15](#)
    - systems [20](#)
  - Switch Blade [22](#)
  - switch configuration [268](#)
  - Sysprep restrictions [139](#)
  - system preparation [250](#), [255](#)
    - All Primergy [31](#), [160](#)
    - automatic [256](#)
    - Blade optimized [31](#)
    - customer image [258](#)
    - for cloning [31](#)
    - Generic Boot Image [31](#)
    - manual [256](#)
    - required attributes [255](#)
    - Unchanged [31](#)
    - with WinPE [257](#)
  - system preparation method
    - All Primergy [160](#)
  - System Preparation Method for Deploy Job window [168](#), [170](#), [171](#), [172](#)
  - system requirements [14](#)
- ## T
- tab
    - Boot Images [125](#)

- Cloning Images 125
- Deployment Tables 126
- Installation Configuration 125
- target groups 11
- target RAID level 249
- target system, configuration 113, 239
- task
  - deleting 109
  - renaming 109
  - starting 109
  - stopping 109
- task bar 82
- task management 106
- task settings
  - editing 109
  - viewing 109
- task types 106
- task window 107
  - operations 108
- Tools menu 122
- U**
- Unchanged 31
- unicast IP protocol 267
- uninstalling, Deployment Manager 74
- Update Manager 44
- update mode 292
- URL
  - configuration file 276
  - image file 275, 281
- user account
  - for administrator 278
  - on the deployment server 81
- using, Deployment Manager 77
- UUID 275
- V**
- View menu 122
- viewing
  - deployment group 158
  - task settings 109
- Virtual Local Area Network 329
- VLAN 329
  - configuration 330
  - requirements 330
- W**
- Web Server 14
  - Deployment Manager 36
- Web server
  - IIS 53
- window
  - Add Server(s) 159, 188
  - Create a Scheduled Task 164, 195
  - Deployment Manager "Power Control" 112
  - Image Information 146
  - License Management 123
  - Login 81
  - New Deployment Group 156
  - New Installation Group 186
  - New Server 92
  - Properties of Deployment Group "group" 158
  - Remote Installation 194
  - Save Options 147
  - Scheduler Options 142
  - Select Deployment Server 119
  - Select Image Path 145
  - Select Server(s) for Deploy Job 166
  - Select Server(s) for Installation Job 197, 198
  - Selecting Deployment Server 80
  - Set Arguments for Deploy Job 174
  - Set Arguments for Installation Job 199
  - System Preparation Method for Deploy Job 168, 170, 171, 172
- Windows 2008 53, 176
  - configuring Windows Firewall 72
  - on the reference system 138
- Windows Firewall 72

- with Advanced Security [138](#)
- Windows Management Instrumen-  
tation (DCOM-In) [138](#)
- Windows Management Instrumen-  
tation (WMI-In) [138](#)
- WinPE MDP [131](#)
- WinPE system preparation [257](#)
- wizard
  - deploy image [163](#)
  - remote installation [194](#)
  - Save Disk Image [141](#)
  - Save Disk Image for "server" [140](#)