

ServerView with Data ONTAP-v[™] V 1.02

Setting Up the Storage Control Blade and Getting Started

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@ts.fujitsu.com.

Certified documentation according to DIN EN ISO 9001:2008

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 9001:2008.

cognitas. Gesellschaft für Technik-Dokumentation mbH www.cognitas.de

Copyright and Trademarks

Copyright © 2011 Fujitsu Technology Solutions GmbH.

All rights reserved.

Delivery subject to availability; right of technical modifications reserved.

Delivery subject to availability; right of technical modifications reserved. All hardware and software names used are trade names and/or trademarks of their respective manufacturers.

- The contents of this manual may be revised without prior notice.
- Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
- No part of this manual may be reproduced in any form without the prior written permission of Fujitsu.

Microsoft, Windows, Windows Server, and Hyper V are trademarks or registered trademarks of Microsoft Corporation in the USA and other countries.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the USA and other countries.

NetApp, the NetApp logo, Data ONTAP, Data ONTAP-v, and FilerView are trademarks or registered trademarks of NetApp. Inc. in the U.S.A and/or other countries.

Before reading this manual

High safety use

This product has been designed and manufactured for general uses such as general office use, personal use, domestic use and normal industrial use. It has not been designed or manufactured for uses which demand an extremely high level of safety and carry a direct and serious risk to life or body if such safety cannot be ensured.

These uses include control of nuclear reactions in nuclear power plants, automatic airplane flight control, air traffic control, traffic control in mass transport systems, medical devices for life support, and missile guidance control in weapons systems (hereafter, "high safety use"). Customers should not use this product for high safety use unless measures are in place for ensuring the level of safety demanded of such use. Please consult the sales staff of Fujitsu if intending to use this product for high safety use.

Technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan

Documents produced by FUJITSU may contain technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan. Documents which contain such technology should not be exported from Japan or transferred to non-residents of Japan without first obtaining authorization in accordance with the above law.

Contents

1	Introduction	9
1.1	Target groups and purpose of this manual	10
1.2	Notational conventions	10
1.3	Documentation for ServerView Suite	11
2	Features	13
2.1	Storage capabilities	13
2.2	Hardware, software, and miscellaneous requirements	14
2.3	Scope of delivery and additional purchase options	15
3	Installation	17
3.1 3.1.1 3.1.1.1	First installation	17 17
	(MMB)	17
3.1.1.2	Blade slot selection	1/
3114	DVD access for the SCB	20
3.1.1.5	SCB BIOS settings	21
3.1.1.6	Checking SCB RAID controller configuration	22
3.1.2	Overview of installation and configuration steps	24
3.1.2.1	What you will need	24
3.1.2.2	Which steps will be performed during installation	24
3.1.3	Installation procedure	25
3.1.3.1	Booting the Storage Control Blade from the product DVD	25
3.1.3.2	User input for initial configuration	26
3.1.3.3	Next events and possible errors	38
3.2	Maintenance and update installations	40

4	Administration and start operation	41
4.1	Resources and user interfaces overview	41
4.2	Hardware management	45
4.2.1	SVOM integrated GUI of the SVA	45
4.2.1.1	Additional entries and functions in ServerView OM	45
4.2.1.2	Agent Deployment	48
4.2.1.3	Backup Manager	50
4.2.1.4	Blade Power Management	52
4.2.1.5	Storage Management	53
4.2.1.6	Notes regarding update management	53
4.2.2	Using the text UI of the SVA	54
4.2.2.1	Installing a VMWare ESX vSphere client	54
4.2.2.2	Logging in ESX and starting the SVA text UI	54
4.2.2.3	Changing the SVA password	57
4.2.2.4	Changing the SVA hostname and IP settings	57
4.2.2.5	Changing regional settings	59
4.3	Storage management	61
431	Calling NetApp Data ONTAP-v FilerView	61
4.3.1.1	Problems to load FilerView applets	62
4.3.2	Overview of Data ONTAP-v management interfaces	63
4.4	Setting up an iSCSI LUN	64
4.5	Data categories for backups	73
4.5.1	Initial configuration data	74
4.5.2	ServerView database	74
4.5.3	ServerView appliance snapshot	74
4.5.4	Data ONTAP-v administration tool setup and configuration	
	information	74
4.5.5	Data ONTAP-v system and configuration information	75
5	Recovery installation	77
5.1	The SVA is corrupt	78
5.2	The VSA is corrupted	78
5.3	ESX or the complete local disk (ESX, SVA, VSA) is corrupted	79

6	Diagnostics
6.1	Overview
6.1.1	Hardware
6.1.2	VMware ESX 4.1 software
6.1.3	ServerView appliance (SVA)
6.1.4	Data ONTAP-v appliance (VSA)
7	Appendix
7.1	Differences of Data ONTAP-v to Data ONTAP
7.1.1	Storage
7.1.2	Physical controller management
7.1.3	Licensing
7.2	Limits and restrictions for Data ONTAP-v
7.2.1	NFS
7.2.2	SAN
7.2.3	WAFL
7.2.4	Miscellaneous
7.3	IP configuration template
7.4	VSA EULA (End User License Agreement) 90
Abbrev	viations
Figure	s99
Index	

ServerView with Data ONTAP-v

1 Introduction

ServerView with Data ONTAP-v is the software component of the PRIMERGY VSX960 internal storage solution for PRIMERGY BX400 S1 / BX900 S1 blade server systems. It offers powerful SAN functions using one server blade (Storage Control Blade) and one storage blade only. ServerView with Data ONTAP-v is automatically integrated in ServerView Operations Manager (SVOM) during installation.

The figure below shows the architecture of ServerView with Data ONTAP-v. ServerView Appliance (SVA) and Data ONTAP-v Virtual Storage Appliance (VSA) are virtual machines. Both SVA and VSA run on the Storage Control Blade (SCB) as the only guest systems of a VMWare ESX host.



Figure 1: Architecture of ServerView with Data ONTAP-v and the VSX960 hardware

1.1 Target groups and purpose of this manual

This manual is intended for system administrators, network administrators and service technicians who already have a basic knowledge of hardware and software. The manual mainly provides an overview of the installation of ServerView with Data ONTAP-v and describes its SVOM integrated user interface for administration.

i This manual does not cover storage management using the ServerView with Data ONTAP-v software, its graphical FilerView user interface and its command line interfaces. Please refer to the Data ONTAP-v and Data ONTAP manuals you can find on and install from the ServerView with Data ONTAP-v product DVD (*Documentation/NetApp/Ontap801/801docs.zip*).

1.2 Notational conventions

The following notational conventions are used in this manual:

Caution	This symbol points out hazards that can lead to personal injury, loss of data, or damage to equipment.
l	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.
italic	Commands, menu items, names of buttons, options, file names, and path names are written in <i>italic</i> letters in the text.
<variable></variable>	Marked variables that must be replaced by current values.
Key symbols	Keys are presented according to their representation on the keyboard. If capital letters are to be entered explicitly, then the Shift key is shown, e.g. SHIFT - A for A.
	If two keys need to be pressed at the same time, then this is indicated by placing a hyphen between the two key symbols.

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



In this manual

- the ServerView appliance (virtual ServerView management station for the complete blade server system and management appliance for the Virtual Storage Appliance) is called SVA for short,
- the Virtual Storage Appliance (native NetApp Data ONTAP-v appliance) is called VSA for short.

1.3 Documentation for ServerView Suite

The documentation for the ServerView Suite can be found on the ServerView Suite DVD 2 supplied with each server system. The documentation can also be downloaded free of charge from the Internet. You will find the online documentation at *http://manuals.ts.fujitsu.com* under the link Industry standard servers.

For the Japanese market please use the URL: *http://primeserver.fujitsu.com/primergy/manual*

2 Features

2.1 Storage capabilities

- Central internal storage solution with powerful shared and virtual SAN access of all server blades within the PRIMERGY blade server system
- Space saving solution using one server blade and one storage blade only, incorporating up to 10 physical disks for user data, and making external storage devices needless
- Including VMware certified premium Virtual Storage Appliance NetApp Data ONTAP-v comprising many NetApp Data ONTAP features, e.g. SnapShot, FlexVol, SnapRestore, block based (iSCSI) and file based (CIFS, NFS) I/O
- Administration interfaces:
 - Easy to use ServerView (IM and OM) integrated GUI of the SVA for first installation, initial configuration, and various control purposes
 - Established and comprehensive NetApp FilerView interface embedded in the VSA for storage management
 - NetApp Data ONTAP CLI and *dvadmin* CLI (see section 4.3.2 on page 63 for an overview of managing interfaces)
- RAID protected and I/O path redundancy between application blades and storage system possible
- Flexible storage solution for SMEs and branch offices ("Data Center in a Box")

Refer to chapter "Appendix" on page 85 to get basic information about the differences between NetApp Data ONTAP-v and standard Data ONTAP and about limits and restrictions of Data ONTAP-v.

2.2 Hardware, software, and miscellaneous requirements

- PRIMERGY BX400 S1 / BX900 S1 Blade Server
- PRIMERGY BX920 S2 server blade (Storage Control Blade)
 - 1 CPU 2.26 GHz (or faster) as minimum, at least 4 cores (This means for example that a single CPU of Intel[®] Xeon[®] E5502 type does not fulfill this requirement.)
 - 2 internal disks, size at least 146 GB
 - 8 GB RAM memory
- PRIMERGY SX960 S1 storage blade
 - 5 or 10 SAS HDDs, hot spare (HS) configuration with 5 or more disks
 - RAID Ctrl SAS 6G 5/6 512MB (D2616) plus iBBU
- VMware ESX 4.1 classic is supported. ESXi 4.1 is not supported.

Miscellaneous preconditions

- The Storage Control Blade has to be configured without Mezzanine Cards, especially without FC or SAS types.
- The Storage Control Blade must be used for the SVA and the VSA only. Additional applications or virtual machines must not be used.
- The data disk array on the LSI RAID 5/6 controller must have at least 4-5 disks of equal size.
- The backup battery of the LSI RAID 5/6 controller must be installed and operational.
- Jumbo frames in the network configuration are not supported.
- Automatic integration of additional disks or disk arrays is not supported.
- The Storage Control Blade can be configured in blade slot 1 or slot 5 in the BX400 S1 blade server system only. The SX960 S1 storage blade (a double slot blade) can be configured in blade slots 2-3 or 6-7 to the right of the SCB.

 The Storage Control Blade can be configured in blade slot 6 or slot 14 in the BX900 S1 blade server system only. The SX960 S1 storage blade (a double slot blade) can be configured in blade slots 7-8 or 15-16 to the right of the SCB.



With PRIMERGY Blade Server BX400 S1 most of all modules of the PRIMERGY BX 900 S1 blade server system are usable. Therefore the name of those modules starts with "BX9".

2.3 Scope of delivery and additional purchase options

- ServerView with Data ONTAP-v DVD Media Kit
- NetApp Data ONTAP-v Basic License Key
- Additional license keys for additional NetApp storage management features are optionally available.
- One year service maintenance contract (for European market follow-up contracts recommended). The support contents are different in each country. For more information, please contact your sales representative.



The VMware ESX Server software DVD, the VMware ESX Server license, and the required hardware (see section above) are not included in delivery and must be purchased separately.

At least an essential or standard VMware ESX Server license is required.

3 Installation

3.1 First installation

3.1.1 Hardware setup and preparation in advance

An overall configuration documentation of the BX400 S1 / BX900 S1 blade server system is beyond the scope of this startup guide. However, the following BX400 S1 / BX900 S1 blade server system resources must be configured before the server and storages blades for ServerView with Data ONTAP-v will be powered on.

3.1.1.1 Configuration of the BX400 S1 / BX900 S1 management blade (MMB)

Verify with a browser or an external Ping that the MMB IP settings are correct. The MMB must be accessible via TCP/IP. (The BX400 S1 / BX900 S1 blade server can be initially configured via the ServerView Local Service Display.)

3.1.1.2 Blade slot selection

The Storage Control Blade (SCB) for ServerView with Data ONTAP-v can be installed in the BX400 S1 system unit in blade slot 1 or 5 only, the associated storage blade must be installed in the two empty slots to the right of the SCB. Typical configuration: SCB in slot 1 and storage blade in slots 2 and 3. Blade slots 4 to 8 can be used for additional server blades.

In the BX900 S1 system unit, slot 6 or 14 can be used for the SCB. The associated storage blade must be in installed in slot 7+8 resp. 15+16. All other slots can be used for additional server blades.

3.1.1.3 Configuration of the connection blade(s) (CB)

The BX400 S1system unit can be equipped with up to four / eight connection blades (CB) which are high speed LAN switches. Up to eight connection blades can be equipped in BX900 S1. Several models of CB can be used depending on customer needs. The following CB models are available:

- Connection Blade GbE Switch/IBP 18/6 (SB6)
- Connection Blade GbE Switch/IBP 36/8+2 (SB11)
- Connection Blade GbE Switch/IBP 36/12 (SB11A)
- Connection Blade 10 GbE Switch/IBP 18/8 (SBAX2)

The installation process requires a well defined network configuration.

The first LOM interface is used as the management/default interface. It is used to connect to the VMware ESX Service Console, the ServerView Appliance and the DataONTAP-v VM via the the first virtual switch (vSwitch0).

Figure 2 shows the network connections available after installation.



Figure 2: Network configuration after installation

Additional network connections to the DataONTAP-v VM can be configured depending on application needs. Figure 3 gives an example with three additional virtual switches (vSwitch1-3) connecting interfaces *e0b*, *e0c*, and *e0d* of the DataONTAP-v VM to the physical network interfaces of the SCB (onboard or additional LAN Mezzanine cards).



Figure 3: Network configuration with additional connections

3.1.1.4 DVD access for the SCB

You must assign the DVD drive in the front-side I/O module of the blade server system to the target Storage Control Blade so that it can boot the SVIM for VSX960 from the ServerView with Data ONTAP-v product DVD.

Booting the SVIM for VSX960 from a remote storage device (which must be configured via the iRMC management interface of the SCB) is supported but outside the scope of this document. (See chapter "Web user interface" of the "PRIMERGY BX400 / BX900 Blade Server System, ServerView Management Blade S1, User Interface Description, User Manual" and chapters "Advanced Video Redirection (AVR)" and "Remote Storage" of the "ServerView Suite, Remote Management, iRMC S2 - integrated Remote Management Controller, User Guide".)

- From a Web browser, enter the URL of the management blade (MMB) of your BX400 S1 / BX900 S1 blade server system and log in as administrator to start the MMB Web GUI.
- 2. If required, in the ServerView bar at the top of the screen, switch the user interface (in the *Experience* drop down list) from *Advanced* to *Standard*.
- 3. Click on the first button below the Storage Control Blade picture (*Assign* USB/DVD button).
- 4. As the default BIOS settings at the time of purchase might have been changed, make sure that the CD/DVD (USB) drive is set as the first boot device in the Storage Control Blade's BIOS.
 - 1. If required, in the ServerView bar at the top of the screen, switch the user interface (in the *Experience* drop down list) from *Standard* to *Advanced*.
 - You can check the Boot Priority Order in the BIOS settings in the MMB GUI menu tree on the left side: Navigate to Information / Operation → Operation → Backup/Restoration Management → BIOS → Backup tab page.
 - 3. You can change the boot device by logging into the iRMC S2 Web interface (enter the IP address of the iRMC S2 or its defined DNS name):
 - 4. Select the *Power Management* entry and change the *Boot Device Selector* in the *Boot Options* box to *USB* (activates this boot device for the next system start only).
 - Select Console Redirection → BIOS Text Console, boot the server blade (in warm or cold mode), press the F2 key while the POST is performed to access the server blade's BIOS, call the Boot menu and set the First Boot Device to USB (activates this boot device permanently).

3.1.1.5 SCB BIOS settings

Data ONTAP-v requires that some features must be disabled in the Advanced Processor Options BIOS menu.

The menu can be found in the BIOS setup in the *Advanced* tab page. You can reach the BIOS setup by pressing F2 during startup.

- Power Management Features must be disabled:
 - Enhanced SpeedStep [Disabled]
 - Enhanced Idle Power State [Disabled]
- Hyperthreading must be disabled:
 - Intel(R) HT Technology [Disabled]

SCB iRMC IP address

Configure the IP Address of the iRMC (integrated Remote Management Controller) in the BIOS menu: $Server \rightarrow IPMI \rightarrow LAN-Setting$. Verify that after power-on of the Storage Control Blade you can reach the iRMC IP with a browser and can open the SCB's Remote Management Contoller.





Figure 4: RAID controllers and VSX960 disks

The Storage Control Blade (SCB) has two SAS RAID controllers:

 The SCB onboard controller (LSI 106LS4SASIME-3030) with two attached SAS HDDs.

The VMWare ESX host and the virtual machines will be installed on this controller.

By default, the SVIM for VSX960 is configured to reinitialize the local disk array as RAID1 (mirrored) volume.

To guarantee that the SVIM for VSX960 can reconfigure the controller, please make sure that if there is an existing configuration, the array is either activated or manually deleted before starting the installation.

To manually clear or activate the local disk configuration before installation, please proceed as follows:

- Enter the LSI BIOS utility by pressing CTRL C when prompted during system POST.
- ► Go to the *RAID Properties* screen and select *Manage Array*.

- ► Either select *Activate Array* if it is inactive or *Delete Array* to destroy the configuration.
- The LSI RAID Ctrl SAS 6G 5/6 512MB (D2616) which is physically located in the SX960 storage blade with up to 10 SAS HDDs.

Depending on the HDD size, the setup will create at least two RAID5 arrays which will be used as disks for the Data ONTAP-v virtual machine.

The *Option ROM* for the RAID controller is enabled by default. This setting should not be changed to ensure that problems with the RAID configuration can be detected during POST.

Before starting an initial installation, any existing RAID configuration on the controller has to be cleared. If the controller contains a wrong RAID layout or if there are existing partitions on the arrays, installation might fail.

- Enter the LSI WebBIOS RAID configuration utility by pressing CTRL H when prompted during system POST.
- ► Go to the Configuration Wizard and select Clear Configuration.
- Confirm the selection by pressing *Next*.
- ► If there is a foreign configuration on the disks, or disks are in the *Bad* state, these states also have to be cleared before starting installation.

The installation program will reinitialize the local disk array depending on a setting in the SVIM for VSX960 deployment installation screen: Deployment \rightarrow Configuration for Disks and RAID Controllers \rightarrow check box Use existing Logical Disks

By default the box is unchecked and the local disk array will be reinitialized, erasing any existing configuration. If you check this box, it is necessary to prepare the local array manually by using the LSI BIOS utility (as described above).

i

3.1.2 Overview of installation and configuration steps

3.1.2.1 What you will need

Except for the hardware prerequisites mentioned in section "Hardware, software, and miscellaneous requirements" on page 14 and for the basic configuration settings addressed in section "Hardware setup and preparation in advance" on page 17, you will need the following things to conduct the installation:

- ServerView with Data ONTAP-v product DVD
- NetApp Data ONTAP-v Basic License Key
- VMware ESX 4.1 installation DVD
- VMware ESX 4.1 license (essential or standard)
- 3 IP addresses (in your private LAN) not yet used (see template on page 89)
- Approximately 90 minutes time (for a complete trouble-free installation)

3.1.2.2 Which steps will be performed during installation

The following lists provide a brief description of the steps that are performed in order to initially install and configure the server blade selected to become the Storage Control Blade in your ServerView Data ONTAP-v storage system.

- User input is only required in step 2 after booting the Storage Control Blade from DVD.
- In step 5 (after about 20 minutes) you will be prompted to change the DVD.
- In step 6 (after about 35 minutes) you are prompted to remove the DVD.

- Booting of the Storage Control Blade from the product DVD containing the ServerView Installation Manager (SVIM) for VSX960 (a SVIM adapted to the installation of ServerView with Data ONTAP-v)
- 2. Wizard guided user input for configuring the software components to be installed on the Storage Control Blade

(The parameter configuration will take approximately 5 -10 minutes.)

- 3. Preparation of the Storage Control Blade's local hard disk (boot partition)
- 4. Rebooting of the Storage Control Blade from the product DVD
- 5. Removal of the product DVD, rebooting thr SCB from its local hard disk
- 6. Insertion of the ESX DVD when prompted, installation of VMware ESX Server
- 7. Removal of the ESX DVD, rebooting of the installer into the ESX environment

(Steps 3 to 6 will take approximately 50 minutes.)

- 8. Start of the ESX SVIM Rollout Service that completes the ESX configuration
- Creation, start, and self-configuration of the ServerView appliance (SVA) including the management tool *dvadmin* for the Virtual Storage Appliance (VSA) executing NetApp Data ONTAP-v.
- 10. Creation of the VSA (including NetApp Data ONTAP-v)

(Steps 7 to 9 will take approximately 20 minutes.)

3.1.3 Installation procedure

3.1.3.1 Booting the Storage Control Blade from the product DVD

- Insert the ServerView with Data ONTAP-v product DVD into the DVD drive of the BX400 S1 / BX900 S1 blade server system.
- ► Boot the Storage Control Blade. This can be performed e.g. via
 - the MMB GUI of the BX400 S1 / BX900 S1 blade server system (Components \rightarrow Server Blades \rightarrow Server Blade- $x \rightarrow$ Power Management).
 - the iRMC GUI of the Storage Control Blade.
 - powering the Storage Control Blade off and on using the power switch.

3.1.3.2 User input for initial configuration

A SVIM wizard starts automatically and leads you through some pages asking for configuration data.



The SVIM on the product DVD of ServerView with Data ONTAP-v is exclusively adapted to install this software product on the selected Storage Control Blade. For other server blades in the system unit, please use the SVIM supplied with the standard ServerView DVDs.

i The

The preset values in the pages can be changed if they are not grayed out.

Language and keyboard selection



Figure 5: Language selection

Please select *English* (affects the SVIM language only). In this version other languages are not supported.

First installation

' ServerView	FU
Regional and language settings Keyboard layout: German	Installation Manager mode Standard mode C Update Manager Express PrimeCollect MDP (Multi Deployment Platform)
+ Intel(R) 82575ED Gigabit Dackplane Connection	
+ Onboard controller * Media disconnected	- Status backup media
-IPv4 settings	Update list of local drives Kescan
Get IP address automatically (DHCP)	C on local drive (floppy / USB stick)
C Take the following IP address:	Insert a media before pressing the "Continue" button
IP address; , , ,	C on local read only drive (CD / DVD) Insert a media before pressing the "Configure" button E:
Subnet mask:	
Default gateway:	Folder:
-IPv6 settings-	Account:
C Stateful address configuration (DHCPv6)	Password:
Stateless address auto configuration	
	No status backup

Figure 6: Selection of keyboard, Installation Manager mode, and configuration data storage

- You are strongly recommended to save the configuration data to a network or USB storage device. The configuration data is stored in a file named *serstartbatch.xml* which will be required later should a recovery installation be needed (see chapter "Recovery installation" on page 77).
 - Click the *Rescan* button and select a storage device which the configuration data is to be saved to.
- Click the *Continue* button.
- Click the *Rescan* button and select the target drive to store the configuration data.

Installation selections

ServerView Installation Manager					x
S ServerView					លព្រំស
Home Deployment Maintenance Information					Help Exit
	Welcome to	ServerView In	stallation M	anager for VSX 01	.02
	Type: BIOS-Vers.:	PRIMERGY EX920 S2 080015 Rev 3D15:3030 JBMC S2	Ident-No: BIOS-Date:	System_169 11/15/2010	
	RS8-Model:	-	RS8-FW:	-	
	DiskSpace:	245 GB	RAM:	6144 MB	
	RAID 1:	FTS RAID CHI SAS 6G 5/6 512M8 (D2616) (0)	MAC :	00-26-9E-82-80-04	
	Deple	2860 (1) Sj in Di	ystemconfiguration icluding ServerView ataONTAP-v Applia	und installation of ESX Appliance and nce	
	Maint	enance b	aintenance Tools v efore an Installatio	nhich can be used either n or Separately	
	Infor	mation Se	ersion and Usage erverView Installatio tegrated Tools	Information about in Manager and	
			N		

Figure 7: Welcome screen

• Click the *Deployment* button.

ServerView Installation Manager					×
S ServerView				FI	ปที่ทรม
Home Deployment Maintenance Information		_	_	Help	Exit
	Installation Manager Deployment Pro Typical Easy, flavless PRIMERGY Installation with Customised Easy, flavless PRIMERGY Installation with Management, RAD, disk and partitioning	cess Selection standard settings. Prep i individual settings for 5 g. OS parameters and Ac	ared for ServerView. System ddOn software.		
	Feature Setting of BIOS/BMC (SCU) RAID/Boot Disk Settings Disk Partitioning OS Parameters for Unatended Installation Installation of ServerView	Typical Not configurable Basic One Partition Basic Automatic	Customised Optional Extended Individual Individual Optional		
	(e.g. SNMP Agents, Update Agent) Installation of Add-on Software	No	Optional		
		₿. D	Back Next	Ca	incel

Figure 8: Deployment mode selection

• *Customised* is preselected. Click the *Next* button.

First installation

ServerView								F	ปกร
ome Deployment Maintenance Information	_	_	_	_	_	_	_	Help	Es
Configure your Unattended Operating System I Configuration File © Create a new configuration file. © Start an installation based upon an existing configuration file. Select the operating system	installatio	on Co	ntents o	f Config	uration File	2	_		1
Hypervisor 💌									
VMware ESX									
VMware ESX 4.1 Rollout									
*): unsupported or unknown support									
Server Management Configuration									
Edit Server Management Settings									
					N	8	ack Next	Ca	nce

Figure 9: OS selection

► Click the *Next* button.

RAID configuration

Configuration hass Storage configuration have ESX (8) oplications (1) ummary (1) VMware ESX Configuration for Disks and RAID Controllers Image last (8) oplications (1) ummary (1) Insert service partition for <i>GlobalFlash</i> on boot disk (de not check for PRI/ERGY EX300 or EX600) Image last (1) ummary (1) Insert service partition for <i>GlobalFlash</i> on boot disk (de not check for PRI/ERGY EX300 or EX600) Image last (1) ummary (1) Insert service partition for <i>GlobalFlash</i> on boot disk (de not check for PRI/ERGY EX300 or EX600) Image last (1) ummary (1) Insert service partition for <i>GlobalFlash</i> on boot disk (de not check for PRI/ERGY EX300 or EX600) Image last (1) ummary (1) Insert service partition for <i>GlobalFlash</i> on boot disk (de not check for PRI/ERGY EX300 or EX600) Image last (1) ummary (1) Insert service partition for <i>GlobalFlash</i> on boot disk (de not check for PRI/ERGY EX300 or EX600) Image last (1) ummary (1) Insert service partition for <i>GlobalFlash</i> on boot disk (de not check for PRI/ERGY EX300 or EX600) Image last (1) ummary (1) Insert service partition for <i>GlobalFlash</i> on boot disk (de not check for PRI/ERGY EX300 or EX600) Image last (1) ummary (1) Insert service partition for <i>GlobalFlash</i> on 000 Available Capacity (MB): 59556 Image last (1) ummary (1) Image last (1) ummary (1) Image last (1) ummary (1) Image last (1) ummary (1) Image last (1) ummary (1) Image last (1) ummary (1)	me Deployment Maint	enance Information	Help
Immary (1) Immart service partition for <i>Global#Each</i> on boot dak (de not check for PRILEEGY EX300 or EX500) All existing partitions will be deleted on disks where new partitions are defined. select Raid Controller LSI 10645ASIME-3030 (EX920 S2) SRAID Controller LSI 10645ASIME-3030 (EX920 S2) Disk 1 Isilogiclogical volume 3000 Available Capacity (MB: 59536 Remove Partition, He partition 1 /boot 512 evid3 prim, Remove Partition, He partition 3 / 8000 evid3 Remove Partition, He partition 3 / 8000 evid3 Remove Partition, He partition 4 None 100 vmfcore Remove Partition, He partition 4 None 100 vmfcore Remove Partition, He partition 5 storage1 11000- vmfs3 Remove Partition.	Configuration Mass Storage Configuration Where ESX (8) Acclications (1)	VMware ESX Configuration for Disks and RAID Controllers	
All existing partitions will be deleted on data where new partitions are defined. select Raid Controller LSI 10645ASIME-3030 (BX920 52) Br RAID Controller LSI 10645ASIME-3030 (BX920 52) Disk 1 Isilogidagical volume 3000 Available Capacity (MB): 55536 #- partition 1 /boot 512 ext3 prim. Remove Partition #- partition 2 swap 512 swap Remove Partition #- partition 3 / 8000 ext3 Remove Partition #- partition 1 Alone 100 vm/score Remove Partition #- partition 1 Alone 100 vm/score Remove Partition #- partition 5 storage1 11000- vmfs3 Remove Partition	Summary (1)	Insert service partition for GlobalFlash on boot disk (do not check for PRIMERGY BX300 of	or BX600()
eelect Raid Controller LSI 10645ASME-3030 (BX920 52) RAID Controller LSI 10645ASME-3030 (BX920 52) Disk 1 Inlogidsgical volume 3000 Available Capacity (MB): 59536 R- partition 1 /boot 512 ext3 prim. Remove Partition. R- partition 2 swap 512 swap Remove Partition. R- partition 1 Alone 100 vm/score Remove Partition. R- partition 1 Alone 100 vm/score Remove Partition. R- partition 5 storage1 11000- vmfs3 Remove Partition.		All existing partitions will be deleted on disks where new partitions are defined.	
B: RAID Controller LSI 10645ASIME-3030 (8X920 S2) Disk 1 Inlogicity olume 3000 Available Capacity (MB): 59536 H:- partition 1 /boot 512 ext3 prim. Remove Partition. Remove Partition. H:- partition 2 wap 512 swap Remove Partition. H:- partition 1 / 8000 ext3 Remove Partition. H:- partition 3 / 8000 ext3 Remove Partition. H:- partition 1 Atome 10 vm/score Remove Partition. H:- partition 5 storage1 11000- vmfs3 Remove Partition.		select Raid Controller LSI 1064SASIME-3030 (BX920 S2)	
Disk 1 Isilogicagical volume 3000 Add Partition Available Capacity (MB): 59536 59536 III- partition 1 /boot 512 ex3 prim. Remove Partition III- partition 2 swap 512 swap Remove Partition III- partition 3 / 8000 ex3 Remove Partition III- partition 4 None 00 vmfcore Remove Partition III- partition 5 storage1 11000- vmfs3 Remove Partition		RAID Controller LSI 1064SASIME-3030 (8X920 S2)	
H- partition 1 /boot 512 ext3 prim. Remove Partition. H- partition 2 ways 512 ways Remove Partition. H- partition 3 / 8000 ext3 Remove Partition. H- partition 1 Anone 00 vmKcore Remove Partition. H- partition 1 Anone 1000 vmKcore Remove Partition.		Ditsk 1 Isilogiclagical volume 3000 Addr Partition Available Capacity (MB): 59536	
H- partition 2 wap S12 swap Remove Partition H- partition 3 / 8000 ext3 Remove Partition H- partition 1 know 0 vmkcore Remove Partition H- partition 1 know 0 vmkcore Remove Partition H- partition 5 storage1 11000- vmfs3 Remove Partition		- partition 1 /boot 512 ext3 prim.	Remove Partition
Hi partition 3 / 8000 exit Remove Partition Hi partition 1 Alone 00 vmRcore Remove Partition Hi partition 5 storage1 11000- vmRs3 Remove Partition		Perition 2 swap 512 swap	Remove Partition
partition 4 None 100 vmicore Ramove Partition partition 5 storage1 11000+ vmfs3 Remove Partition		* partition 3 / 8000 ext3	Remove Partition
periode 5 storage1 11000- Thiss		partition 4 None 100 vmkcore	Remove Partition
		partition 5 storage1 11000- vinis5	Remove Partition

Figure 10: RAID configuration

The RAID configuration preset for the Storage Control Blade is displayed in the RAID Controller box.



You are strongly recommended to accept the displayed RAID and partition configuration which has been tailored for the correct operation of ServerView with Data ONTAP-v. Otherwise installation might fail.

• Click the *Next* button.

Configuration of VMware ESX

Home Deployment Maintenance Information Street Configuration USX Configuration Basic Configuration EVALUATE ESX Basic Configuration Easter Configuration Localization: Mapplication (1) Image: Configuration Password: Exception ESX RootPassword: Verify Password: Installation settings: Medium CD-ROM w (Grayed out controls seflect fixed default settings.) (Grayed out controls seflect fixed default settings.)		rujins
Configuration Mass Storage (1) VEXX Configuration Basic Configuration Easic Configuration Localization: Moyboard: Moyboard: Moyboard: Moyboard: EBX Root Password: Modum: CD-ROM V (Grayed out controls reflect fixed default settings.)	Help	Ex
Localization: Server/lew Appliant Ber Configuration German (Balin1) Preparations (1) TimeZone Burger Applications (1) Password: Bit Summary (1) Password: Password: Verify Password: Installation settings: Medium (Grayed out controls reflect fixed default settings.)		
Password: Venify Password: ESX Root Password: Venify Password: Installation settings: Medium: CD-ROM M (Grayed out controls reflect fixed default settings.)	ystem clock uses UTC	
Installation settings: Medium CD-ROM V (Grayed out controls reflect fixed default settings.)	Encrypt root password	
(Grayed out controle reflect fixed default settings.)		

Figure 11: Basic ESX configuration

Define a strong ESX Root Password (for later access to the ESX hypervisor console operation system) and repeat the entry.

A valid password requires a mix of upper and lower case letters, digits, and other characters.

- You can use a 7-character long password with characters from at least 3 of these 4 classes.
- You can use a 6-character long password containing characters from all the classes.

An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.

As in the first release of ServerView with Data ONTAP-v, only installation from the CD-ROM/DVD drive in the front side I/O module of your BX400 S1 / BX900 S1 blade server system (and from remote storage) is supported, *CD-ROM* is preselected as *Medium*.

• Click the *Next* button.

1		
ome Deployment Mainter	nance Information	Help bi
Configuration Mass Storage (1) VMware ESX Basic Configuration ESX, Configuration	VSX Configuration ESX Configuration	
ServerView Appliance Data ONTAPry Appliance	Network Configuration :	
StorageBlade	IP Address 17217.40.233	
SVAppliance EULA	Netmask : 2552552480	
DataONTAP-v EULA Applications (1)	Gateway : 172.17.48,1	
Summary (1)	Name Server : 17217.48.99	
	Use VLAN ID : 0	
	ESX License : License : (Grayed out controls reflect fixed default settings)	

Figure 12: ESX network configuration and licensing



The settings on this page are important for successful installation.

- Please change the preset Computer name for the Storage Control Blade (the ESX host) to a name of your choice.
- Enter the IP settings for the Storage Control Blade (the ESX host) according to the particular network settings of your BX400 S1 / BX900 S1 blade server system.



The values set here will be used as the basis for IP settings on subsequent pages.

- ► Enter your *ESX* License.
- Click the *Next* button.

Configuration of the ServerView appliance (SVA)

ome Deployment Mainten	ance Information			Help E
Configuration Mass Storage (1) VMware ESX Basic Configuration	VSX Configuration ServerView Appliance C	onfiguration		
ESX Configuration ServerView Appliance Data ONTAP-v Appliance StorageBlade	Virtual machine : VM name	svappliance vm		
ESK EULA SVAppliance EULA Data/SNTAP-v EULA Applications (1) Summary (1)	Network Configuration Computer name IP Address Netmask Gateway	: svahost 17217.49235 255255248.0 17217.48.1		
	Name Server IP Adress of Management Blade	172.17.48.99 172.17.49.240	1	
	Password: Admin Password:	Verify Paasword	:	Encrypt root password I
	(Grayed out controls reflect fixed a	lefault settings)		

Figure 13: SVA configuration

- Please change the preset VM name for the SVA virtual machine to a name of your choice. The prefix cannot be changed.
- Please change the preset *Computer name* for the SVA to a name of your choice.
- Please enter the IP settings for the SVA according to the particular network settings of your BX400 S1 / BX900 S1 blade server system.
- ► The *IP Address of Management Blade* field has to be filled with your predefined IP address.
- Define the Admin Password for later SVA access and repeat the entry. As the SVA usually is the central ServerView station to manage the whole BX400 S1 / BX900 S1 blade server system, the SVA password is your ServerView password, too.
- ► Click the *Next* button.

Configuration of Virtual Storage Appliance (VSA)

ServerView Installation Manager	the second s	2
ServerView		าปที่ระบ
Home Deployment Maintenar	nce Information	Help Exit
Configuration Mass Storage (1) Where ESX Basic Configuration ESX Configuration StorageEducation StorageEducation	VSX Configuration Data ONTAP-v Appliance Configuration Virtual machine : VM name :DataONTAP-v/vm	
	Network Configuration Computer name Inahost IP Address 122.17.49234 Netmask 25.255248.0 Gateway 172.17.4839 Name Server 172.17.4839	
	Password: Root Password:	out password
	Data ONTAP-v License : Ucence : Warning: A wrong License key may cause the installation to fail (Grayed out controls reflect fixed default settings.)	
	۱ <u>ــــــــــــــــــــــــــــــــــــ</u>	Back Next Cancel

Figure 14: VSA configuration

- Please change the preset VM name for the VSA virtual machine to a name of your choice. The prefix cannot be changed.
- Please change the preset *Computer name* for the VSA to a name of your choice.
- Please enter the IP settings for the VSA according to the particular network settings of your BX400 S1 / BX900 S1 blade server system.
- Set the *Root Password* (password for the user *root*) to enable later VSA access and repeat the entry.
 - The password must be at least eight characters long.
 - The password must contain at least one number.
 - The password must contain at least two alphabetic characters.
- ► Enter your *Data ONTAP-v License*.
- Click the *Next* button.

Storage blade configuration

Home Deskoyment Maintenance Information Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) Iff Mass Storage (1) If Mass Storage (1)	rul	
Configuration Mass Storage (1) Mass Storage Blade Configuration StorageBlade Configuration StorageBlade Configuration DataStore : Name of storage poils) :viapool Mass Storage Blade has more than 5 disks then a hot spare disk can be created. Create hot spare : (Gayed out controls reflect fixed default settings)	Help	Đ
<u> </u>		

Figure 15: Storage blade configuration

- Define the name for the storage pool(s) on the storage blade where the data disks will be installed. The prefix cannot be changed.
- If your storage blade is equipped with 5 or more physical disks, an optional hot spare disk can be configured by checking the Create hot spare option box.
- ► Click the *Next* button.

End user licenses agreement

The following three screens show the EULAs for VMware ESX, SVA/ServerView, and VSA/Data ONTAP-v.

► Check the Accept End User License box and click the Next button three times.
Application selection

ServerView Installation Manager		×
ServerView		กปไกรม
Home Deployment Mainter	ance Information	Help Dit
Configuration P Mass Storage (1) Wave SX (8) P Applications Solutions Solutions Solution	VMware ESX Application Wizard Select Applications @ ServerView Suite 3/3 @ DasCoffAfr Applance @ ServerView Solar Appres	
1		Back Next Carcel

Figure 16: Application selection

► No selection possible. Click the *Next* button.

Installation confirmation

ServerView					rujns
Home Deployment Maintenance	Information			Helç	Đ
Configuration Mass Storage (1) VMware (5X (8)	VMware ESX Installation Info				
Summary	Bootdisk Linux Controller: DriveName:	RAID: LSI 1064SASIME-2860 (1) Isilogiclogical volume 3000	PartitionSize: Capacity:	512 68660 mb	
	OperatingSystem Type: Installation Media: Timezone:	VMWare ESX 4.x odrom Europe/Berlin			
	DHCP DefaultGateway:	false 172.17.48,1	IP Address: SubnetMask;	17217.49.233 255.255.248.0	
	Save the Configura	tion to File senta	tbatchuml		
	Note that this file on t	the server is used as a workfile an	d will be overwritten. It she	ould not be used for permanent sto	orage.

Figure 17: Installation confirmation

• Click the *Start Installation* button.

Once installation has started, no more user configuration data is required or possible, but you will bet prompted to remove the DVD and to insert the ESX DVD later. When installation has been completed, the SVIM for VSX960 DVD is no longer required.

3.1.3.3 Next events and possible errors

- The disks will be configured and prepared for installation (RAID 1 mirrored array on 2 local disks). The SCB will reboot from DVD and all required files will be copied from DVD to hard disk.
- You will be prompted to remove the product DVD, and then the SCB will restart again from its local hard disk and will start the VMware ESX installation utility.

- **i** If the SCB's BIOS boot sequence does not point to the local disk RAID1 volume, you can use the boot menu (F12) to select it, or reboot into the BIOS setup and set the boot order to the local disk RAID1 volume.
- You will be prompted to insert the VMware ESX installation DVD.
- After ESX installation you will be prompted to press <u>Enter</u> to reboot the SCB into ESX from local hard disk.



Remove the VMware ESX DVD after pressing <u>Enter</u>, otherwise the SCB will reboot from DVD again.

If you forgot to remove the DVD, select *boot from first hard disk* in the initial ESX installation menu. Installation will then continue correctly.

 After the reboot at first the SVA appliance (virtual machine) including the Data ONTAP-v *dvadmin* utility will be installed in ESX. You can access the SVOM GUI using *https://<SVA IP address>:3170*.



After starting the SVA the installation script (running on the ESX host) must be able to reach the SVA via the local network. If installation does not continue at this point, check the IP settings of the ESX host and of the SVA appliance by running the *ping* command from a an external workstation. Check whether the SVA has started using the ESX vSphere client (see section "Installing a VMWare ESX vSphere client" on page 54).

- Then the VSA appliance (virtual machine) with Data ONTAP-v will be deployed in ESX (by the Data ONTAP-v *dvadmin* utility running on the SVA). The user data RAID array will be created on the VSA. You can access the Data ONTAP-v FilerView GUI using *https://<VSA IP address>/na admin*.
 - **i** Problems at this stage can be caused if the virtual data disk was not created. Without a valid DATA disk, the Data ONTAP-v will not start and will not communicate with the installing process. For troubleshooting, log in with SSH to the SVA. Inspect your disk configuration using the *dvadmin* commands *dvadmin vm disk show* and *dvadmin pool show*. For details refer to the *dvadmin* reference in the "NetApp Data ONTAP-v Installation and Administration Guide" which is part of the *Documentation/NetApp/Ontap801/801docs.zip* file you will find on the product DVD.
- If your VMware ESX license is not correct, a warning message is displayed and the VMware ESX will start for an evaluation period lasting 60 days. The license can be corrected by using an ESX vSphere client.

If your Data ONTAP-v license is not correct, you are prompted from the ESX console to retype your license. The VSA will not start without a valid license.



Once the initial VX960 installation has been completed, please wait for the completion message on the ESX console screen.

3.2 Maintenance and update installations

ServerView Update Manager Express is the recommended update management solution for the software components of ServerView with Data ONTAP-v and of the Storage Control Blade. All respective software components are compatible to VMware ESX Server.

The other components in the BX400 S1 / BX900 S1 blade server system (management blades, server blades and connection blades) should be updated using the ServerView Update Manager.

In the first release of ServerView with Data ONTAP-v, only BIOS, firmware, and the associated hardware drivers of your Storage Control Blade can be updated. You should update your system immediately after the initial installation of ServerView with Data ONTAP-v (see section "First installation" on page 17). The easiest way to accomplish this is to follow these steps:

- Boot the Storage Control Blade from the Data ONTAP-v product DVD to start its ServerView Installation Manager. Details are described in section "Booting the Storage Control Blade from the product DVD" on page 25.
- Select Update Manager Express as Installation Manager mode and click Continue (see figure 6 on page 27).
- ► Select the *Quick Mode* tab.
- ► Click the *Start* button.
- When the Update Manger Express has finished, remove the product DVD from the DVD drive and abort the Installation Manger.

Update Manager Express has a CLI which can also be used. For details, refer to the "Local System Update for PRIMERGY Servers" ServerView Suite manual.

4 Administration and start operation

4.1 Resources and user interfaces overview

After successful installation of ServerView with Data ONTAP-v the following resources and user interfaces are available to you:

SVA

Enhanced ServerView GUI (with SVOM)

With the GUI of the ServerView Suite you can obtain hardware, software, and environment information, diagnostic, and control over the servers and virtual machines of your BX400 S1 / BX900 S1 blade server system. A comprehensive online help system is incorporated. For details, refer to the ServerView Suite documentation.

GUI access via web browser: *https://<SVA IP address>:3170* or *http://<SVA IP address>:3169*, SVA user *admin*, password as chosen.

Text user interface (BIOS style)

Appliance console interface used for some configuration steps only. See section "Using the text UI of the SVA" on page 54.

Access via VMware ESX vSphere client, ESX user *root*, password as chosen.

SVA CLI

Here SVA tools and the Netapp *dvadmin* utility are available.

Access via SSH, SVA user *admin* or *root*, password as chosen.

RAID storage

ServerView RAID GUI for RAID storage management, equipped with an extensive built-in help feature.

Access via *https://<ESX IP address>:3173*, ESX user *root*, password as chosen.

VSA

NetApp Data ONTAP-v FilerView GUI

Standard GUI for managing the VSA and the (virtual) storage system.

Access via *http://<VSA - IP Address>/na_admin* (must be enabled in Data ONTAP-v) or *https://<VSA - IP Address>/na_admin*, VSA user *root*, password as chosen.

For information on how to enable the setting, please refer to Data ONTAP® 8.07- Mode File Access and Protocols Management Guide on the product DVD.

NetApp Data ONTAP-v CLI

CLI for managing the VSA and the (virtual) storage system.

Access via SSH or Telnet (both must be enabled in Data ONTAP-v), VSA user *root*, password as chosen.

For information on how to enable the setting, please refer to Data ONTAP® 8.07- Mode File Access and Protocols Management Guide on the product DVD.

NetApp Data ONTAP-v administration tool dvadmin

The *dvadmin* CLI is running on the SVA. Via *dvadmin* you can open a serial console to the VSA. This is essential in case you have to configure the Network or root volumes. With *dvadmin* you can view, control, configure, and diagnose the VSA and its virtual machine platform.

Access via SSH to the SVA (SVA user *admin* or *root*, password as chosen), and from there call the *dvadmin vm console connect <Data ONTAP-v vm name>* command to log into VSA, VSA user *root*, password as chosen.

For details, refer to section "Storage management" on page 61.

ESX/COS

SCB/ESX console screen

The VMware ESX Console Operating System (ESX COS) is available on the SCB.

Access via SSH (must be enabled), ESX user root, password as chosen.

vSphere client

You can open a Web page to the ESX IP address, download the vSphere client program from there and install it on your (Windows) PC. You use the vSphere client to view the configuration of the ESX host and its VMs, to maintain them, and to access the text UI of the SVA. See section "Using the text UI of the SVA" on page 54.



Do not use VMware vSphere vCenter to administer VSX960. This is currently not supported by Data ONTAP-v.

iRMC interfaces of the SCB

Standard server blade management interfaces of the Storage Control Blade (iRMC GUI, iRMC Remote Manager CLI and SMASH CLP).

Access via *https://<iRMC IP address>* or SSH (SSH must be enabled), iRMC user *admin*, and password as chosen.

MMB interfaces of the BX400 S1 / BX900 S1 blade server system

Standard blade server management interfaces of the BX400 S1 / BX900 S1 system unit (MMB GUI and OEM SM CLP / Telnet interface).

Access via *http(s)://<MMB IP address>* or Telnet/SSH, MMB user *admin*, password as chosen.



The GUIs mentioned above are based on Java. When starting one of the GUIs, Java looks for a security certificate and displays warning messages if no certificate is active. Please answer as follows to start the respective application when no certificate is active:

- When a warning message asks if you want to block execution of the application (*OPEN LOCK* icon), answer *NO* to avoid the GUI application being blocked.
- When a warning message asks if you want to run the application (*CLOSED LOCK* icon), answer *YES* to ensure that the GUI application starts despite the missing certificate.
- If the GUI application is stopped, please close all browser windows and start again.

Interface to	Type, Protocol/Port	Managed Objects	Default Admin. User
SVA	Enhanced ServerView GUI (with SVOM), https:// <sva address="" ip="">:3170 http://<sva address="" ip="">:3169</sva></sva>	BX400 S1 / BX900 S1 blade server system/components, SCB, server blades	SVA user admin
	SVA text user interface (BIOS-style) via VMware vSphere client	SVOM GUI enhance- ments and additional functions	ESX user root
	SVA CLI with SVA utilities and NetApp <i>dvadmin</i> utility via SSH	SVA and VSA and its VM platform	SVA user admin or root
RAID storage	ServerView RAID utility https:// <esx address="" ip="">:3173</esx>	RAID storage	ESX user root
VSA	NetApp Data ONTAP-v FilerView GUI https:// <vsa address="" ip="" na_admin="" or<br="">http://<vsa address="" ip="" na_admin<br="">(must be enabled)</vsa></vsa>	VSA and (virtual) storage system	VSA user root
	NetApp Data ONTAP-v CLI via SSH or telnet (both must be enabled)		
	NetApp Data ONTAP-v administration tool <i>dvadmin</i> (CLI) via <i>dvadmin</i> command from the SVA CLI	VSA and its VM platform	VSA user root (login to SVA required)
ESX / COS	SCB/ESX console screen via SSH (must be enabled)	VMware ESX, VMs	ESX user root
	VMware vSphere client, Windows application with TCP/IP connection to the ESX host		
iRMC of the SCB	ServerView iRMC GUI https:// <irmc address="" ip="">, Remote Manager CLI and SMASH CLP via SSH (must be enabled)</irmc>	SCB	iRMC user admin
BX400 S1 / BX900 S1 MMB	MMB GUI http(s):// <mmb address="" ip=""> and MMB OEM SM CLP via Telnet or SSH</mmb>	BX400 S1 / BX900 S1 blade server system/components	MMB user admin

Table 1: User interfaces overview

4.2 Hardware management

4.2.1 SVOM integrated GUI of the SVA

4.2.1.1 Additional entries and functions in ServerView OM

Start the SVOM of the SVA by entering the SVA IP address (https://<SVA IP address>:3170) in a Web browser.

After successful installation of ServerView with Data ONTAP-v the ServerView Operations Manager (SVOM) of the SVA displays the entry *Appliance* on its start page. This entry is new compared to the standard SV OM.



Figure 18: Start page of the ServerView Operations Manager with new entry Appliance

The new Appliance entry provides the links

- Agent Deployment (see section 4.2.1.2 on page 48)
- Backup Manager (see section 4.2.1.3 on page 50)
- Blade Power Management (see section 4.2.1.4 on page 52)
- Storage Management (see section 4.3 on page 61)

In addition to the new entry on its start page, the SVOM of the SVA is equipped with new functions (compared to the standard SVOM) that can be inspected in the ServerView Operations Manager main window.

- During installation, the SVA performs a complete automated examination of all blades in the BX400 S1 / BX900 S1 blade server system and adds the entries for the discovered nodes to the ServerView OM database.
- The list of management applications displays the entry *Storage Mgmt*, and the server list shows the *SVA* and the *VSA* as subnodes of the Storage Control Blade. You can navigate to the VSA, which presents the NetApp FilerView GUI, by clicking *Storage Mgmt* or the VSA entry.
 - To navigate to the VSA entry, click the Server List link on the SVOM start page.
 - Select the storage control blade.

C ServerList - Fujitsu Technolog	y Sol	utions								
รบุ๊กรบ	1	1	-	S	ervei	View	w Su	ite		
ServerList Administration Asset	t Maria	gement Event M	anigemen	t Monito	ring Update	Mänageme	nt Applian	ce Help		
Import Archive Import Server E	sport	Server Settings								
										ServerList
Al Servers	BX4									
BX40051em-044		2 2 40	000	00		V 🔾 1		000		
- SVAHost1-host		Name -	4		Network		Model		System	
DataONTAP-v-vm	0	SVAHost1-host			72.17.50.82		PRIMERGY	81/920 52	VMware ESX 4.1.0	
- Svapplance-vm		DotaONTAP-v-vm			72.17.51.255	12	NetApp		FreeBSD (64-bit)	
A Crouss	1	STOCOMON COVID			12.11.51.254					
	e				R.					2
	-	Alarm Details Alar	m Informati	on						
		Currently no alar	m selected							
								1.00		

Figure 19: ServerView server list entries for SCB, ESX host, VSA and SVA

Notes on the example above

- The BX400 S1 / BX900 S1 blade server system is called BX400S1em_044.
 - The Storage Control Blade (SCB) with the name *BX400S1em_044-01* is inserted in blade slot 1 (see the gray highlighted entry on the left hand panel). Here we can find:
 - The ESX host with host name SVAHost1-host. Clicking the entry in the right hand panel (or right-clicking the icon in the left hand panel and selecting Open) displays the ServerView Single System view of the PRIMERGY BX920 S2.
 - The VSA (*Data ONTAP-v-vm*), a guest virtual machine. Clicking the entry in the right hand panel (or right-clicking the *Data ONTAP-v* icon in the left hand panel and selecting *Open*) displays the FilerView GUI.
 - The SVA (*svappliance-vm*), a guest virtual machine. The entry and icon do not provide additional information in this view.

 An additional server blade (shown as an example only), called BX400S1em-044-06, is inserted in slot 6. It has, as yet, no agents deployed.

4.2.1.2 Agent Deployment

- ServerView agents on the Storage Control Blade are automatically deployed during installation. Use this function for additional server blades or server systems only.
- On the start page of the SVA Operations Manager, click the Agent Deployment link in the Appliance entry.

мдент рерюуше	nt - i ujitsu reciniowgy sututions	
Hostnar	ne:	
Login:		
Passwo	rd:	
OS Type		
•••••		
Event Messaries:		
Liferit messages.		

Figure 20: Agent Deployment page of the SVA

The ServerView software is organized into two parts, the ServerView manager plus its associated agents. ServerView Manager is preinstalled on the central management station, but the agents must be deployed to each server blade individually. Once deployment is completed, each server blade in the BX400 S1 / BX900 S1 blade server system can be managed by the ServerView with Data ONTAP-v management station.



Any changes to the virtual machine configuration of the SVA are not supported (e.g. extending or adding disks to the SVA). Agent Deployment will not work on the SVA itself, ServerView Agents are currently not supported on Open SuSE as used by the SVA.

- For the target server blade, specify the hostname or IP address and enter the login data for access as administrator.
- In the OS Type drop down list, select the default setting Determine (to apply a tool for detecting the OS), or select an OS (Linux or Windows) if you are sure or if the tool fails.

In our example, the additional server blade BX400S1em-044-06 is now manageable after agent deployment.

ServerList - Fujitsu Technolo	Server View Strifte	<u> </u>
TOJIISO	Serverview Suite	
ServerList Administration Asso	et Management Lvent Management Monitoring Update Management Appliance Help	
Import Archive Import Server	Export Server Settings	
A Al Senare		ServerList
E BX40051em-044	Extlositem 041-01	
E 🔂 8X40051em-044-01		
SVAHost1-host	Name / 🛆 🗐 🛞 Network. Model System	
DetaONTAP-v-vm	SYAHost1-host 172-17-50.82 PRIMERGY 5X920.52 Wildow EreePSD (644) FreePSD (644)	.1.0
3 8X10051cm-011-06	Stapplarke-ym 172.17.51.254	<i>my</i> .
		>
	Airm Details (Airm Information) Currently no alarm selected	

Figure 21: BX400S1em-044-06 now manageable

4.2.1.3 Backup Manager

• On the start page of the SVA Operations Manager, click the *Backup Manager* link in the *Appliance* entry.

Backup Manager - Fujitsu Technology Solutions	
Available backups:	
backup-2011-05-04-1100.tar.bz2	
backup-2011-05-04-1200.tar.bz2	
backup-2011-05-04-1300.tar.bz2	
backup-2011-05-04-1400.tar.bz2	
backup-2011-05-04-1500.tar.bz2	
Clear Create Restore Delete Download	
Upload	

Figure 22: Backup Manager page of the SVA

The backup manager allows you

• to clear the contents of the log window

- to create backups of the ServerView database of the Storage Control Blade stored as backup file in the Storage Control Blade's disk memory. This SQL database is a prerequisite for the Operations Manager software and is used for internal data storage.
- to restore it from one of the backups made in the past,
- to delete the selected file from the backup partition,
- to download a backup file from the Storage Control Blade to the browser's local system,
- or to upload a backup file which is local to the browser to the Storage Control Blade's disk memory.

The *Available backups* lists the backup files in the Storage Control Blade's disk memory which can be used for a restoration.

4.2.1.4 Blade Power Management

► On the start page of the SVA Operations Manager, click the *Blade Power Management* link in the *Appliance* entry.

Blade Power Management - Fujits	u Technology Solutions	ServerView	Suite	
ServerList Administration Asset Mar	segement Event Mesagement Mor	atoring Update Management #	Appliance Help	
		Agent Deployment Backup Ma	anager Blade Power Management	Storage Management
				Blade Power Management
PRIMERGY BX400	172.17.49.237			
	Solic Server Name 4 172:12.49:237-04 5 172:12.49:237-05 6 Not Present 6 Not Present 7 Not Present 8 Not Present 6	Depend on VSA	Ziart Automotically	Start Delay (Scat 0 0 0 0 0 0
				Refresh Apply

Figure 23: Blade Power Management page of the SVA with BX400 S1

The slots 1, 2 and 3 in the BX400 S1 figure are not available for power control, because the SCB is in slot 1 and the PRIMERGY SX960 storage blade in slots 2 and 3.

The figure shown is representative and not dynamically generated. Therefore your actual system may look physically different to this shown here.

For a BX900 S1 the figure shown above depict more slots that can be controlled but the operation is exactly the same as for a BX400 S1.

Sometimes the BX400 S1 / BX900 S1 system unit has to be powered down or rebooted.

With the help of this panel you can configure the power up behavior of those server blades in the BX400 S1 / BX900 S1 system unit which need resources from the VSA storage blade (e.g. NFS, iSCSI). You can configure that they will power on **only** after the VSA or SVA is online and ready (with optional additional delay).

- To power on automatically after the VSA is ready:
 - ► Enable the boxes *Depends on VSA* and *Start Automatically* on this screen.
 - ► Set the power options in the iRMC menu of the server blade Power Management → Power Options to Always power off.

Any Start delay that has been set is counted from when the VSA is ready.

- To power on automatically after the SVA is ready:
 - ► Enable the box *Start Automatically* on this screen.
 - ► Set the power options in the iRMC menu of the server blade Power Management → Power Options to Always power off.

Any Start delay that has been set is counted from when the SVA is ready.

- To power on independently of VSA or SVA start:
 - Do not enable a box on this screen.
 - ► Set the power options in the iRMC menu of the server blade Power Management → Power Options to Always power on.

The *Start Delay* allows you to specify a delay in seconds from VSA or SVA start to the server blade start. The value can be entered after double-clicking the field in the *Start Delay* column.

4.2.1.5 Storage Management

The *Storage Management* entry in the *Appliance* section of the SVOM start page starts the NetApp FilerView GUI. More information is provided in section "Calling NetApp Data ONTAP-v FilerView" on page 61.

4.2.1.6 Notes regarding update management

The SVOM included in the SVA has a small built-in repository used to deploy ServerView Agents, ServerView RAID, ServerView Update Agents and AIS connect. Update management itself is currently not supported on the SVA. Any attempt to activate the Update Management functionality will fail.

4.2.2 Using the text UI of the SVA

The functions of the SVA GUI are also available in the easy-to-use, BIOS-style text UI of the SVA.

The text user interface of the SVA must be used

- for changing the SVA password being defined during installation,
- for changing SVA hostname and IP address,
- and for changing the regional settings for the SVA set during installation.

Examples of how to use the text UI are described for three functions below. As the SVA is running on a VMWare ESX, an ESX vSphere client is used to call the SVA's text UI.

4.2.2.1 Installing a VMWare ESX vSphere client

- Start a Web browser on a Windows machine
 - that you use with administrator rights,
 - that has network access to the ESX host.
- ► Enter the IP address (or URL) of the ESX host (Storage Control Blade).
- Click Download the vSphere Client under Getting Started.
- ► Click *Save* to download the vSphere client installer.

The vSphere client installer is downloaded to your system.

- ► Double-click the downloaded *VMware-viclient<build> <number>.exe* file to run the vSphere client installer.
- ► Run through the installation process until you click *Finish*.

4.2.2.2 Logging in ESX and starting the SVA text UI

Start the vSphere client by selecting Start → Programs → VMware → VMware vSphere Client.

🖉 VMware vSphere Clie	ent		
vm ware [,]		1	
VMware vSphere [®]			
Client			
To directly manage a sing To manage multiple hosts, vCenter Server. IP address / <u>N</u> ame: <u>U</u> ser name: Password:	e host, enter the IP addre enter the IP address or n 172.17.50.82 root	iss or host na ame of a	ame.
<u>Canada</u>	Use <u>W</u> indows session	n credentials	s <u>H</u> elp

Figure 24: vSphere client start page

- Enter the IP address (or URL) of the ESX host (Storage Control Blade).
- Enter the user name *root* and the ESX password that was set during installation.
- Click Login and Ignore the security warning. (You can set up third-party certificates later.)
- Call the console of the SVA appliance:
 - In the inventory tree showing the ESX host and the virtual appliances and virtual machines running on it, select the SVA appliance and click the *Console* tab at the top of the vSphere client window.
 - To view the console in full screen mode, from the inventory tree, rightclick the SVA appliance and select *Open Console* in the displayed context menu.

Hardware management



Figure 25: Text console window of an SVA

When you start this interface for the first time, the program guides you through all its configuration pages.

Navigation

- Menu selection: Up, Down, Enter to select an menu item
- Output area: PageUp, PageDown to scroll
- Press Ctrl + Alt to release the pointer from the console.

4.2.2.3 Changing the SVA password

- Call the ESX vSphere client, connect to the ESX host and start the SVA console (see section 4.2.2 above).
- ► Select *Password* and press Enter.

	ServerView A	appliance	
Welcone			
Agent Deployment	Old password:	****	
Server Discovery	New password:	***	
Backups	Confirm:	***	
Password			
Nctwork Configuration			
Regional Settings			
License Manager			
Shutdown Appliance			
		[Apply][Close 1
			1
			ų
Pageurand			

Figure 26: Console window to change the SVA password

Navigation

- Field input: Arrow keys, Delete, Backspace to move the cursor
- Selection move: Tab to select the next element
- Button activation: Enter to activate the selected button

4.2.2.4 Changing the SVA hostname and IP settings

- Call the ESX vSphere client, connect to the ESX host and start the SVA console (see section "Using the text UI of the SVA" on page 54 above).
- Select Network Configuration and press Enter.

Hardware management

	ServerView	Appliance	
Welcome Agent Deployment Server Discovery Backups Password Network Configuration Regional Settings License Manager Shutdown Appliance	linstnome :	Cx1 Use DHCP sumppliance	
		[Apply] [Close 1

Network Configuration

Figure 27: Console window to change the SVA hostname and IP settings (1)

Navigation

- Checkbox switch: Space to switch the checkbox contents _
- Field input: Arrow keys, Delete, Backspace to move the cursor _
- Selection move: Tab to select the next element _
- Button activation: Enter to activate the selected button _
- If you do not want to use DHCP, uncheck Use DHCP to select the screen for ► entering the IP settings:

	ServerView A	ppliance	
Welcome Agent Deployment Server Discovery Backups Password Network Configuration Regional Settings Shutdown Appliance	Hustname: IP Address: Subnet Mask: Gateway: DNS 1: DNS 2:	[] Use DHCP svappliance 172.17.51.254 255.255.248.0 172.17.48.1 172.17.48.99 172.17.48.98 [Apply) [Close]
Network Configuration			

Figure 28: Console window to change the SVA hostname and IP settings (2)

Navigation

- Checkbox switch: Space to switch the checkbox contents
- Field input: Arrow keys, Delete, Backspace to move the cursor
- Selection move: Tab to select the next element
- Button activation: Enter to activate the selected button

4.2.2.5 Changing regional settings

- Call the ESX vSphere client, connect to the ESX host and start the SVA console (see section "Using the text UI of the SVA" on page 54 above).
- Select Regional Settings and press Enter.

Hardware management

	ServerView Appliance
Welcome	
Agent Deployment	Region: Zone:
Server Discovery	Antarctica ^ Amsterdam ^
Dackups	Asia Athens Bolicat
Passuord	Australia Belgrade
Nctwork Configuration	Canada Bratislava
Regional Settings	Etc Bucharest
Shutdown Appliance	Indian Chisinau
	Mideast v Dublin v
	Layout:German
	Timc: 05 : 16
	Date: 2011 - 02 - 12
	Language file: english.ing
	[Apply][Close]
Regional Settings	

Figure 29: Console window to change the regional settings

Navigation

- Checkbox switch: Space to switch the checkbox contents
- Field input: Arrow keys, Delete, Backspace to move the cursor
- Selection move: Tab to select the next element
- Button activation: Enter to activate the selected button (The "[^]" characters in an active selection field mean that the Enter key will bring a drop down list of choices.)

4.3 Storage management

Please note the documentation suite supplied on the ServerView with Data ONTAP-v product DVD. On the DVD you will find the ZIP file to install the Data ONTAP-v and Data ONTAP manuals here: Documentation/NetApp/Ontap801/801docs.zip

Refer to chapter "Appendix" on page 85 to obtain information about what is different in NetApp Data ONTAP-v compared with Data ONTAP and about the limits and restrictions of the Data ONTAP-v storage system.

4.3.1 Calling NetApp Data ONTAP-v FilerView

FilerView is the standard administration GUI of the NetApp Data ONTAP-v storage system.

On the start page of the SVA Operations Manager, click the *Storage Management* link in the *Appliance* entry (or enter the URL *https://<VSA IP address>/na_admin* in your web browser).

r Serve	view
	Data ONTAP™
	FilerView® helps you configure and monitor your filer.
	Filer At-A-Glance monitors the performance of your filer.
	Documentation is not installed <u>Click here</u> to install the ZIP file from the Data ONTAP TM CD-ROM or the <u>NOW site</u>
vol(1)	Manual pages for Data ONTAP commands are available on your filer.
er: rsion: atus:	vsahost7 NetApp Release 8.0.1 ● The system's global status is normal
	Is CIVEAP TM is licensed by NetApp, Inc. pyroth (c) NetApp, Inc. T195-E0007 All rights reserved. The About TWK the NetApril notices.



The first FilerView ... icon starts the FilerView application.

Storage management



Figure 31: NetApp Data ONTAP-v FilerView application start page

The topic entries suffixed by a question mark on the left hand side supply detailed help and support text.

4.3.1.1 Problems to load FilerView applets

NetApp Data ONTAP-v FilerView is the standard administration interface for the virtual storage system. If you are experiencing that not all FilerView applets can be loaded, you will need to disable TLS 1.0 from Java. Select the following on your windows system:

- Control panel -> Java -> Advanced Setting Tab -> Security List
- Uncheck the TLS 1.0 box.
- Restart the browser (kill all instances and restart new).

4.3.2 Overview of Data ONTAP-v management interfaces

Accessing Data ONTAP-v FilerView contained in the VSA is only one way to administer and manage the ServerView Data ONTAP-v storage system. There are two additional ways to interface ServerView Data ONTAP-v:

Data ONTAP-v dvadmin CLI

Connect to *dvadmin* on the virtual machine the SVA is running on. Use an SSH client and the SVA IP address. This enables you to use the *dvadmin* CLI.

- to manage the Data ONTAP-v platform (virtual machine the VSA is running on)
- and to manage Data ONTAP-v via a system console interface.

Data ONTAP-v CLI

Connect to ServerView Data ONTAP-v over the network and use the Data ONTAP-v command-line interface to manage the system directly. Use an SSH client and the VSA IP address.



For more Information, refer to

- the "Data ONTAP-v Installation and Administration Guide", the "Data ONTAP-v Release Notes", and the Data ONTAP manuals you can find on the ServerView with Data ONTAP-v product DVD (*Documentation/NetApp/Ontap801/801docs.zip*).
- the help systems of the FilerView interface and the man pages of the Data ONTAP CLIs.

4.4 Setting up an iSCSI LUN

The goal of this section is to describe an example of how to set up and attach an iSCSI LUN to a host system. This example is based on Windows 2008 R2 Server and utilizes the Data ONTAP-v[™] CLI only. However, if you prefer the graphical user interface of the Data ONTAP-v solution, you can use it instead.

For information on iSCSI setting, please refer to "Data ONTAP® 8.0 7- Mode Block Access Management Guide for iSCSI and FC" on the product DVD.

- Log into the VSA appliance and issue the command filer> iscsi start to start the iSCSI target service on the storage system.
- If there is only the boot volume available, you are highly recommended to create a dedicated volume for LUNs (You are not recommended to store any user data on volume /vol/vol0 in general.):

filer> vol create <vol-name> -1 en_US -s file aggr0 100g This command creates a volume of 100GB on the aggregate aggr0 and sets the volume language to en_US . Even when you have a non-English OS, the volume will be set to English language. It is best practice to disable the creation of automated snapshots with the command:

filer> snap sched <vol-name> 0 0 0

and adjust the space reserve value for snapshots in the previously created volume with the command

```
filer> snap reserve <vol-name> 0
```

It is also best practice to create *qtrees* on the root of a volume for every host to keep the flexibility for, e.g. later migration tasks. A *qtree* is very similar to a file system folder but can be managed by Data ONTAP-v. It can be created by issuing

filer> qtree create /vol/<vol-name>/<qtree-name>

- To create a LUN of 20GB you have to enter the following command: filer>lun create -s 20g -t windows_2008 /vol/<volname>/<qtree-name>/<LUN-name> As a result Data ONTAP-v will create the LUN object within the *qtree*. To align the LUN with the internal file system that is used by Data ONTAP-v it is necessary to specify a LUN type. In this example a Windows 2008 host will be attached and therefore the type of LUN, specified with the *-t* option, is *windows_2008*.
- The task of the next step is to make the LUN available for the host/initiator. This is done with the *igroup* command:

filer> igroup create -i -t windows <igroup-name> <initiatoriqn>

The previous command will create an *igroup* for iSCSI (-*i*) for windows hosts (-*t*). It is also necessary to specify a name for the *igroup* and the IQN of the iSCSI initiator. The IQN is a unique string of digits that identifies the initiator. The usual format of the IQN is

iqn.<registration date of the domain>.<subdomain>.<domain>:<hostname>.
For example iqn.1991-05.com.microsoft:host1 is a valid IQN.

The last step on the Data ONTAP-v CLI is to map the LUN to the igroup with the following command (If no LUN ID is specified, Data ONTAP-v will automatically use the next unused ID.):

filer>lun map /vol/<volume>/<qtree>/<lun> <igroup-name>
<LUN-ID>

The procedure above describes all steps that are necessary on a Data ONTAPv appliance. Nevertheless, this is only a rough overview. If there is a need for any additional information, the general Data ONTAP documentation should be able to cover any open questions.

All following steps are performed on the Windows host system / initiator to which the LUN is to be attached.

The following example uses the Windows GUI for iSCSI although all tasks can be performed with the iSCSI CLI *diskpart* command from the Windows command line.

Setting up an iSCSI LUN



Figure 33: Starting the iSCSI Initiator GUI

First of all the iSCSI Initiator GUI has to be started. Click on *iSCSI Initiator* in the start menu.



Figure 34: Starting the iSCSI service

If the iSCSI service has not been started before, this popup will appear. Press on *Yes* to start the iSCSI service.

he system wil Address	look for Targets on fol Port	lowing portals: Adapter	IP address
io add a targe io remove a ta hen dick Remo	t portal, dick Discover i rget portal, select the vc.	Portal. address above and	Discover Portal
NS servers he system is r Name	egistered on the follow	ing įSNS servers:	Refresh
io add an iSNS	server, dick Add Serve	er.	Add Server
o remove an i hen dick Remo	SNS server, select the ive.	server above and	Remove

Figure 35: Entering the VSA IP address

It is necessary to point the iSCSI initiator to a certain target.

Open the second tab (*Discovery*) and click on *Discovery Portal*. Enter the IP address of the Data ONTAP-v appliance that will be used for the iSCSI discovery and iSCSI I/O.

Alternatively you might want to use the iSNS service if an iSNS server exists on the network.

Setting up an iSCSI LUN

argen		Quick connect
iscovered targets		Refresh
Name	S	atus
ign. 1992 08.com.netapp:sn. 257	5019098 In	active
n connert using advanced ontingen	ic palent a target and then	
o connect using advanced option lick Connect.	s, select a target and then	Cognect
o connect using advanced option lick Connect. Ico completely disconnect a target nen dick Disconnect.	is, select a target and then	Corrnect Disconnect
o connect using advanced option lick Connect. or completely disconnect a target en dick Disconnect. or target properties, including co elect the target and click Proper	is, select a target and then , select the target and infiguration of sessions, ies.	Cognect Disconnect Properties

Figure 36: Connecting the target

A new target will appear in the first tab. At this time the iSCSI target is known by the initiator but not connected. Click on *Connect*.



Figure 37: Confirming the settings

Just check the settings and confirm with *OK*. As a result the target will be connected and the LUN is now attached to the Windows host.

L Server Manager	-			and the second se		_IDI X
He Action yew	Help					
🗢 🕸 🖄 🛅 🚺	X33051)	Disk Manageme	nt Volume List + Graphical View		Actions	
Roles		Volume 14	would Type Fie System Status		Disk Management	-
Features Features Find Diagnostics Configuration Storage Windows St	erver Backup	Cardata (D:) Se Carsystem (C:) Se	mple Basic NTFS Healthy (Primary I mple Basic NTFS Healthy (System,	Partition) Boot, Page File, Active, Crash Dump, Primary Par	More Actions	,
Disk Manag	Refresh Rescon Dis Create VHD Attach VHD	5				
	All Tasks					
	View					
	Help	a na la				
			(4)	<u>د</u>		
		California Basic 73, 57 GB Online	system (C) 39.99 GU NTFS Healthy (System, Boot, Page File, Active, C	data (0:) 33.57 GUNTES ir Healthy (Primary Partition)		
		Lico-ROM 0 DVD (E:) No Media				
		Unallocated	Primary partition			

Figure 38: Letting Windows search for the new disk

To make use of the new LUN it is necessary to partition and format the newly created disk.

Open the Service Manager, navigate to Storage and let Windows search for new disks using the Rescan Disks task.

Setting up an iSCSI LUN

Life Artise Har Hale					
and the set	e 10				
Server Manager (RX33051)	Disk Manageme	ent Volume List + Graphic	al Vew	Actions	
P Roles	Volume	avout Tune File System	Status	Disk Management	
Gur Features To Tagnostics To Tagnostics To Tagnostics To Tagnostics Storage Storage Disk Management	Ciedata (D:) S Ciesystem (C:) S	imple Basic NTFS	Healthy (Primery Partition) Healthy Grystem, Boot, Page File, Active, Crash Dump, Primary Par	More Actions	2
	4				
	CHIDisk 0 Basic 73.57 GB Online	system (C:) 39.99 GU NTFS Healthy (System, Boot, I	Age File, Active, (Healthy (Primary Partition)		
	GeiDisk 1 Unknown 20.00 GB Offine () Hotp	20.00 GB Unalocated			
	DVD (E:)	Properties	_		
		Primary partition	1		

Figure 39: Setting the disk online

Windows will recognize a new Disk.

► Set the disk to *Online* first.

Server Manager (RX33051)	Disk Managem	ent Volume List + Graphical View	N	Actions	
Roles	Volume L	ayout Type File System Statu	US	Disk Hanagement	_
Dispostos Dispostos Storage Mindows Server Backup Disk Management	Cardeta (D:) S Carsystem (C:) S	imple Basic NTFS Healt Imple Basic NTFS Healt	thy (Primary Partbon) Ithy (System, Boot, Page File, Active, Crash Dump, Primary Par Ithy (System, Boot, Page File, Active, Crash Dump, Primary Par	More Actions	
	<u>.</u>		2		
	Control Contro Control Control Control Control Control Control Control Control Co	system (C;) 39. 99 GB NTF5 Healthy Crystem, Boot, Page Fi	A data (D-) 33.57 (6 NTPS 1945 (2 NTPS) 1945 (2 NTPS)		
	Image: Constant of the second se	System (C) 35.97 CB ATES Healthy (System, Boot, Page Fi 20.00 GB Unalocated	Idata (D) 33.57 (6 NTFS 35.7 (6 NTFS) Healthy (Prmary Partson)		

Figure 40: Initializing the disk

► Initialize the disk by clicking *Initialize Disk*.

Setting up an iSCSI LUN

Server manager						
File Action View Help						
* 🔿 🙍 🖬 🖬 😰	6 5					
Server Manager (RX33051)	Disk Managemen	t Volume I	List + Graphical View		Actions	
Roles	Volume Lay	out Type	File System Status		Disk Management	
Barlands Barlands	Cirdata (Dr.) Sm Ciresystem (Cr.) Sm	ple Basic ple Dasic	NTFS Healthy (Primary) NTFS Healthy (System,	Partition) Uoot, Page File, Active, Crash Dump, Primary Pa	r More Actions	,
	Sasic Z3.57 GB Online	system (39.99 GB N Healthy (Se	(C:) VITF5 Vystem, liboot, Page File, Active, r	data (D) 33.57 (G MTFS Healthy (Drmary Partson)		
		system (39.99 GB N Healthy (Si 20.00 GB Unalocati	(C) HTF5 Vstem, Boot, Page File, Active, F New Sargie Volume	data (D) 33.57 (G MT5 Healthy (Drmary Partition)		
	La Disk 0 Basic 73,57 GB Online La Disk 1 Data 20,00 GB Online Charles 1 Data Charles 1	system (39.99 GB N Healthy (S 20.00 GB Unalocate	(c) 1175 1175 1175 1175 1175 1175 1175 117	data (D) 33.57 (G NTFS Iteatity (Primary Partiton)		
	LaDisk 0 Saic ZaS7 60 Online LaDisk 1 Baic ZaS7 60 Online LaDisk 1 Disc 1 Online LaDisk 1 Online Disc 1 Online Disc 1 Online Disc 1 Online Disc 1 Online Online Online	system (39.99 GB N Healthy (S 20.00 GB Unalocati	(C) 1975 System, Boot, Page File, Active, r New Sample Volume Here Sample Volume Here Sample Volume Here Martered Volume Properties	tata (D) 133.57 (G NTFS Healthy (Vimary Partition)		

Figure 41: Formatting the disk

To let the operating system make use of the new disk it has to be formatted with a file system.

► Select *New Simple Volume* to start the wizard and follow the instructions.
🏭 Server Manager			and the second		_ 🗆 🗵
File Action View Help					
	6° 59			r	
Server Manager (RX33051)	Disk Manageme	ent Volume List + Graphical View		Actions	
E au Features	Volume La	ayout Type File System Status	600 m	Disk Management	-
E gi reaures Teatres Configuration Configuration Songe Songe Disk Monagement	indeta (Dr.) Sr insCSI LU Sr Casystem (Cs) Sr	mple Basic NTPS Healthy (Pinnary mple Basic NTPS Healthy (Pinnary mple Basic NTPS Healthy (System	Petition) Petition) Boot, Page File, Active, Crash Dump, Primary Par	More Actions	,
	A Disk 0	(autom (C))	Auto (70)		
	73.57 GB Online	39.99 GB NTFS Healthy (System, Boot, Page File, Active, I	33.57 GD HTFS Healthy (Primary Partition)		
	L-# Disk 1 Basic 20.00 GB Online	ISCSI LUN (1-:) 20.00 GB NTFS Healthy (Primary Partition)			
	CD-ROM 0 DVD (E:) No Media				
	Unallocated	Primary partition	-		

Figure 42: The iSCSI LUN is ready for use

Finally the disk will be ready for use.

4.5 Data categories for backups

Every system that holds valuable information must be protected. VSX960 uses RAID1 on the local SCB disks where the software (ESX and Appliances) is installed, and RAID5 on the storage blade to protect user data. Besides this hardware level protection, we strongly recommend that you use commercial backup software to perform periodical backups of your data.

While this kind of backup software is beyond the scope of this guide, we would like to mention the important configuration information of VSX960, which should be backed up, too.

4.5.1 Initial configuration data

As described in section "Installation procedure" on page 25, you should save the configuration data to a network or USB storage device with the installation process. Once installation is completed, this configuration data is also available on the ESX host in file */svim/serstartbatch.xml*. Please save this file to an external device if you have not already done so. You will need this data if you need to reinstall the software stack (see chapter "Administration and start operation" on page 41.

4.5.2 ServerView database

Please refer to section "Backup Manager" on page 50 for backup of the ServerView database.

4.5.3 ServerView appliance snapshot

A snapshot captures the entire state of the virtual machine at the time you take the snapshot. Snapshots are useful when you need to revert to a previous state of the virtual machine. Use the vSphere client to take a snapshot. For more information, please refer to the "vSphere Virtual Machine Administration Guide" (VMware manual) at *vmware.com*.

4.5.4 Data ONTAP-v administration tool setup and configuration information

The Data ONTAP-v administration tool (*dvadmin*) is installed on the ServerView appliance. The *.dvadmin* directory contains important *dvadmin* setup and configuration information. You should periodically make a backup of this directory (or a snapshot of the SVA), and store it in a safe location in case you need to restore any important files. The *.dvadmin* directory is located under */root*.

4.5.5 Data ONTAP-v system and configuration information

The *dvadmin* tool can be used to back up Data ONTAP-v system information, including the virtual machine configuration (excluding data disks), and all of the information on the Data ONTAP-v system disks. Please refer to the "Data ONTAP-v Installation and Administration Guide" for more information (search for "vm config backup"). You may run the *dvadmin* monitor tool to perform this backup periodically. The backups are filed to the datastore where the Data ONTAP-v is installed. The snapshot (backup) of the Data ONTAP-v appliance can also be performed using the vSphere client snapshot utility.

5 Recovery installation

In extreme cases a recovery process may be necessary should one of the following scenarios occur:

- 1. The SVA is corrupted
- 2. The VSA is corrupted
- 3. ESX or the complete local disk (ESX, SVA, VSA) are corrupted

Recovery is to be used with caution and only after a thorough diagnosis of the problem shows that it was probably caused by a corruption of the appliances or the ESX operating system.

All the recovery scripts are available from the ESX console (assuming you can log in to ESX) in the */svim* folder. You can access the ESX console:

- From the video redirection feature of the SCB's iRMC remote management GUI by selecting the Storage Control Blade (ESX host) as video redirection source. (Enter the *Standard* MMB web GUI of the BX400 S1 system and click on the *Console* button below the Storage Control Blade picture. See also chapter "Advanced Video Redirection" of the "Remote Management, iRMC S2 - integrated Remote Management Controller" manual.)
- From a VGA screen connected directly to the socket at the front of the SCB (ESX host) via special VGA/USB adaptor (PY BX900 S1/BX400 S1 Y-Cable frontside for KVM connection to server blade. FTS Part number S26361-F4478-L1. (For the EMEA market.))
- From an SSH login to the ESX console. (Log in as user *root* with the ESX password.) SSH must have been enabled for the ESX console.

5.1 The SVA is corrupt

Use the *sva_recovery* [--*OverwriteSVABackup*] command to reinstall the SVA. The command will stop, unregister, and delete the running SVA and then reinstall it into ESX. The command utilizes the initial */svim/serstartbatch.xml* SVA configuration file (whose path can be supplied to the command using the *-c* (or *--configfile*) *PATH_TO_CONFIGFILE*). The SVA module must be in the */svim/appliances* folder.

When *sva_recovery* is called with the *--OverwriteSVABackup* option, or when the configuration backup file is not available, the restored SVA will be set to an initial configuration and any lost SVOM information has to be re-entered.

5.2 The VSA is corrupted

Use the *vsa_recovery* command to reinstall the VSA. When the command script has finished, a few manual actions are required to complete the reinstallation. The command will stop, unregister, and delete the VSA, then reinstall the VSA with the former UUID. The first part of reassigning the data disks residing on the storage blade is performed by the script, after which the following manual task has to be performed:

- 1. Log in to the SVA shell via SSH.
- 2. Power on the Data ONTAP-v virtual machine using the *dvadmin vm* <*Data ONTAP-v vm name*> *start* command.



Important: For initial startup of Data ONTAP-v use ALWAYS *dvadmin vm* start and not a start with VMware vSphere client. This is a requirement for a proper recovery of Data ONTAP-v.

- Establish a serial connection to the system console on the new VSA using the *dvadmin vm console connect <Data ONTAP-v vm name>* command. The VM will skip the automatic setup and enter the boot menu. If the boot menu is not entered automatically, press <u>Ctrl</u> - <u>C</u> during the first moments of the boot of Data ONTAP-v.
- 4. Select option 5 and boot it into maintenance mode.
- 5. Now you have to reassign the disks to the VSA in a second step (see also the example for this step below):
 - a) Find the old and new *sysids* by running the Data ONTAP-v *disk show -a* command.

- b) Reassign the disks to the new VSA by running the *disk reassign -s* <*old_sysid> -d < new-sysid>* command.
- 6. Reboot the VSA by using the *halt* command.
- 7. Finally you must reassign the license to Data ONTAP-v by running the *vsa_recovery --licenseDataONTAPv* command.

Example for step 5

*> disk show −a

Local Syst	tem ID: 2575	5919088			
DISK	OWNER		POOL	SERIAL NUMBER	HOME
0b.0 0a.0	vsahost vsahost	(2575919090) (2575919090)	Pool0 Pool0	6000c29d5d33c27ed6917efe13530c11 6000c2927acd844928256b4eed21c74a	vsahost vsahost

*>disk reassign -s 2575919090 -d 2575919088

```
Disk ownership will be updated on all disks previously belonging to Filer with sysid 2575919090. Would you like to continue (y/n)? y
```

5.3 ESX or the complete local disk (ESX, SVA, VSA) is corrupted

The data disks must be still usable.

Both cases will be dealt with using the same recovery installation procedure. It is similar to the first installation, but the VSA data disks remain unchanged in this case and no user data is lost. Proceed like the first installation (see section "First installation" on page 17), but select your *serstartbatch.xml* file (which was created in the first installation) as the *Configuration File* to activate a recovery installation (see figure 9 on page 30). The installation reassigns the data disks to the VSA in a first step and stops at the same point as in case 2 (section "The VSA is corrupted" on page 78). The same manual procedure is then necessary as previously described in section "The VSA is corrupted" on page 78, including adding the license:

1. Log in to the SVA shell via SSH.

2. Power on the Data ONTAP-v virtual machine using the *dvadmin vm* <*Data ONTAP-v vm name*> *start* command.



Important: For initial startup of Data ONTAP-v use ALWAYS *dvadmin vm* start and not a start with VMware vSphere client. This is a requirement for a proper recovery of Data ONTAP-v.

- Establish a serial connection to the system console on the new VSA using the *dvadmin vm console connect <Data ONTAP-v vm name>* command. The VM will skip the automatic setup and enter the boot menu. If the boot menu is not entered automatically, press <u>Ctrl</u> - <u>C</u> during the first moments of the boot of Data ONTAP-v.
- 4. Select option 5 and boot it into maintenance mode.
- 5. Now you have to reassign the disks to the VSA in a second step (see also the example for this step below):
 - a) Find the old and new *sysids* by running the Data ONTAP-v *disk show -a* command.
 - b) Reassign the disks to the new VSA by running the *disk reassign -s* <*old_sysid> -d <new-sysid>* command.
- 6. Reboot the VSA by using the *halt* command.
- 7. Finally you must reassign the license to Data ONTAP-v by running the *vsa_recovery --licenseDataONTAPv* command.

Example for step 5

```
*> disk show -a
```

Local Syst	tem ID: 257	5919088			
DISK	OWNER		POOL	SERIAL NUMBER	HOME
		-			
0b.0 0a.0	vsahost vsahost	(2575919090) (2575919090)	Pool0 Pool0	6000c29d5d33c27ed6917efe13530c11 6000c2927acd844928256b4eed21c74a	vsahost vsahost

*>disk reassign -s 2575919090 -d 2575919088

```
Disk ownership will be updated on all disks previously belonging to Filer with sysid 2575919090. Would you like to continue (y/n)?\ y
```

6 Diagnostics

6.1 Overview

The PRIMERGY VSX960 can be regarded as four major SW/HW building blocks, each with its diagnostic options. A summary of these four blocks is provided below.

6.1.1 Hardware

The PRIMERGY BX920 S2 server blade and SX960 S1 storage blade and the BX400 S1 / BX900 S1 blade server system log their correctable and uncorrectable errors in event log files.

Some of the errors are signaled visually by LEDS on the front panels. Defective/failed server blades or disks are signalized by a flashing error LED.

Management software supporting hardware diagnostics

- iRMC web interface of each PRIMERGY server blade (log in using the iRMC IP address). The sensors information, the system events log menus, and the power management features are very useful here. The iRMC provides video redirection to access the console of the server blade.
- MMB remote management web interface (log in using the BX400 S1 / BX900 S1 management blade IP address). Also provides video redirection and power control for all server blades in the BX400 S1 / BX900 S1 blade server system, shows the event log of the BX400 S1 / BX900 S1 and the environment status of all its HW components.
- ServerView Operations Manager running on the SVA (log in on port 3169 using the SVA IP address). Shows dedailed hardware and software configuration of the attached server blades, shows monitoring results of the ServerView agents running on the server blades, and produces alerts and warnings if needed.

- VMware vSphere client GUI (download from the ESX IP address, install it on the Windows PC, and start it with the ESX IP address as target host). It shows any events from the perspective of the virtual environment, VM configuration system protocols, resource (cpu/mem/disk) usage and bottlenecks. Allows network configuration. You can export the sytem protocols with the vSphere menu *file -> export system protocols*.
- ServerView Raid console on ESX server (log in on port 3173 using the ESX IP address). Reports disk hardware oriented events. Supports disk diagnostics and maintenance.

The iRMC and MMB Web interfaces will work also if the HW host has failed or is powered down. ServerView Operations Manager, ServerView RAID, and VMware vSphere GUI need a running ESX and/or SVA appliance to operate correctly. They might not work when a severe hardware error on the Storage control blade occurs. Refer to the standard PRIMERGY BX920 S2 server blade manuals for more details on how to diagnose HW errors.

6.1.2 VMware ESX 4.1 software

ESX logs activities and errors extensively. The *vm-support* utility on the ESX generates a TAR file with the relevant logs. This TAR file can be sent to the VMware support for diagnosis. Common logs on the ESX server: /*var/log/messages* and /*var/log/vmware/hostd*.log* (however, the content cannot intuitively be utilized and it is of help mostly for advanced VMware users).

A Summary of events and errors can be viewed with the vSphere client under the *Events* menu entry. Refer to the standard ESX 4.1 administration guide for more details on how to diagnose problems with the ESX host.

VSA installation

The VSA installation logs are kept on the ESX Server under /svim/rollout.out (summary) /opt/fujitsu/ServerViewSuite/Rollout/rollout.log (detailed log).

6.1.3 ServerView appliance (SVA)

The operating system of the SVA is Linux OpenSUSE. Messages, including OS error messages, are collected in */var/log/messages*. The diagnostics is a common Linux operating system diagnostics.

Logs for the ServerView Operations Manager installation and configuration are kept under /var/log/fujitsu/ServerViewSuite/ServerView/*log. Please refer to the ServerView Operations Manager manuals for the full diagnostic possibilities for the observed hosts and for the ServerView Operations Manager itself.

6.1.4 Data ONTAP-v appliance (VSA)

The *dvadmin* utility is described in detail in the NetApp "Data ONTAP-v Installation and Administration Guide" which includes a troubleshooting part. *dvadmin* errors will be kept under */var/log/dvadmin*(usually an empty folder). The *dvadmin help* command shows the available commands for *dvadmin*. The *dvadmin status* command shows the current status of the program (user, host, escape char). The dvadmin utility helps to diagnose the Data ONTAP-v appliance (VSA). Three dvadmin commands are available for Data ONTAP-v diagnostic:

- dvadmin vm log show <Data ONTAP-v vm name>
- dvadmin vm log save <Data ONTAP-v vm name> <log-save file name>
- dvadmin vm coredump <Data ONTAP-v vm name> <dump file name>

With these commands you can observe the current system log of the Data ONTAP-v appliance if the appliance was started before. (An offline appliance causes an empty log file.)

The *dvadmin vm coredump* command creates an Data ONTAP-v dump file that can be analyzed by NetApp service personnel (the VM will restart upon this command).

Except for debugging with the *dvadmin* utility (see part 3), you can debug the Data ONTAP-v OS by using its own debugging measures. You can connect to the Data ONTAP-v command line using the *dvadmin* command (*dvadmin vm console connect* <vm>) and use Data ONTAP-v CLI commands for debugging. Extensive help is available by typing *help* or ? in any position on the command line.

Useful commands are: *disk show*, *volume show*, *license*, *ifconfig -a*, *netdiag*, *route*, *aggr*.

Overview

You can use the Data ONTAP-v FilerView web GUI which provides a command line interface and other information from the *Filer* menu entry: *Status*, *Syslog messages*, *Report* (realtime status).

The FilerView GUI is called via *https://<VSA IP address>/na_admin*.

Performance and status monitoring can be observed from the FilerView menu with *Performance Meter* and *Filer At-A-Glance* (Java applications).

A full description of the build-in Data ONTAP-v diagnostic options can be found in the:

- NetApp "Data ONTAP-v Installation and Administration Guide"
- NetApp "Data ONTAP 8.0 7-mode System Administration Guide" (a general Data ONTAP manual, some of the details described differ from the Data ONTAP-v details)

7 Appendix

7.1 Differences of Data ONTAP-v to Data ONTAP

A Data ONTAP-v storage system runs Data ONTAP software on a virtual machine, so it can be regarded as a software controller. This section describes how a software controller is different from a typical hardware controller.

7.1.1 Storage

Storage is currently limited to the disks that are physically installed in the SX960 S1 storage blade.

Data ONTAP-v virtualizes storage from the disks that are available to the host server. In ServerView with Data ONTAP-v, these are the disks in the associated storage blade in the BX400 S1 / BX900 S1 blade server system.

Because the storage is connected to the server in the system, not directly to the Data ONTAP software, the virtual machine provides the storage status to Data ONTAP-v. Data ONTAP uses RAID0 groups to optimize performance and storage utilization. The storage system provides the parity protection for non-NetApp disks.

In addition to the data disks, Data ONTAP-v requires three virtual system disks in the storage pools for boot, NVRAM, and internal system information. These system disks are created automatically when the Data ONTAP-v system is installed.

7.1.2 Physical controller management

The provided Data ONTAP-v administration tool (*dvadmin*) provided must be installed on a separate virtual machine (on the same Storage Control Blade) for management of the software controller.

7.1.3 Licensing

Unlike a NetApp hardware controller, the Data ONTAP-v storage software must be licensed separately as a platform. You must specify a valid Data ONTAP-v license when you initially install, or deploy, Data ONTAP-v storage software on a host server.

You will receive the license with the Data ONTAP-v installation media so it can be used during Data ONTAP-v installation.

The Data ONTAP-v platform license is passed to Data ONTAP the first time the Data ONTAP-v virtual machine is powered on after it has been deployed. Only after Data ONTAP has validated the Data ONTAP-v license can you use the Data ONTAP console to add Data ONTAP feature licenses. See the Data ONTAP-v Release Notes for information about the Data ONTAP feature set licenses that are supported when using Data ONTAP-v.

Because each Data ONTAP-v virtual machine is licensed separately and locked to a specific host server, no cloning or VMotion of the Data ONTAP-v virtual machine is allowed. If the Data ONTAP-v software is booted on a different virtual machine than the one on which it was initially installed, or if the license is not valid, Data ONTAP-v will log an error message and shut down.

The Data ONTAP feature licenses purchased for Data ONTAP-v are valid only on the Data ONTAP-v system. Those feature licenses cannot be used on hardware controllers. Additionally, Data ONTAP feature licenses created for a hardware controller cannot be used on a Data ONTAP-v system.

7.2 Limits and restrictions for Data ONTAP-v

This section lists maximum performance values that could be proved under optimized conditions. Especially in virtual environments, this values might vary depending on the actual workload of the virtual machine. E.g., the performance of every protocol has an impact on the performance of all remaining protocols. When several protocols are used at the same time, the performance therefore might be lower than expected.

7.2.1 NFS

Limit Description	Limit
Max. clients	16384
Max. owners	16384
Max. StateIDs	65536
Max. access in an ACL	400

7.2.2 SAN

Limit Description	Limit
Max. LUNs	2048
Max. iGroups	256
Max. LUN maps	4096

7.2.3 WAFL

Limit Description	Limit
Max. Qtrees per volume	4998
Max. snapshots	255

7.2.4 Miscellaneous

Number of volumes allocated per server iSCSI: Max. number of volumes is 200.

Maximum size of one volume allocated to a server iSCSI/NFS: 2TB (not a NetApp limit, but specific for ServerView with Data ONTAP-v).

Number of NFS mounts allocated per server NFS: unlimited by VSA SW, it depends on the attached server.

Number of server connections for one shared volume iSCSI: Max. 64 iSCSI sessions per VSA.

NFS: unlimited.

7.3 IP configuration template

the default values are the values as shown on the screen during installation. Given values with (*) must be modified.

Setting	Defaults setting	Your setting	Remark
ESX Configuration			
Network Configurati	on		
Computer name	•		
IP Address	10.0.0.1		
Net mask	255.0.0.0		
Gateway	10.0.0.1		Leave this field empty if a gateway is not required.
Name Server	10.0.0.1		
Use VLAN ID	0		
SVA Configuration			
Virtual Machine Nar	ne		
VM name	svappliance-vm	svappliance-	The prefix svappliance- cannot be changed.
Network Configurati	on		
Computer name	svahost		-
IP Address	10.0.0.1*		You will need to change the IP address
Net mask	Same as for ESX		
Gateway	Same as for ESX		If the gateway for ESX was not set, the IP address of the ESX host is used.
Name Server	Same as for ESX		
IP Address of Management BI	ade 10.0.0.5		
VSA Configuration			•
Virtual Machine Nar	ne		
VM name	DataONTAP-v-vm	DataONTAP-v-	The prefix DataONTAP-v- cannot be changed.
Network Configurati	on	1	-
Computer name	vsahost		
IP Address	10.0.0.1*		You will need to change the IP address
Net mask	Same as for ESX		
Gateway	Same as for ESX		If the gateway for ESX was not set, the IP address of the ESX host is used.
Name Server	Same as for ESX		

Figure 43: IP configuration template

7.4 VSA EULA (End User License Agreement)

End User License Agreement Minimum Terms

IMPORTANT - READ CAREFULLY: This End User License Agreement ("EULA") is a legal agreement between You either as an individual or as an authorized representative of a business entity (hereafter referred to as "You" and/or "Your"), and Fujitsu. Fujitsu is willing to license to You the software product accompanying this EULA, which includes, without limitation, computer software features, protocols, authorized updates and upgrades or other supplements to the software, images, music, text and/or animations incorporated into the software, media, printed materials, or online or electronic documentation, provided by Fujitsu or made available for download (collectively referred to as the "Software"). Your download, installation and/or use of the Software constitutes acceptance of all of the terms stated herein. If You do not agree with all of these terms, You must promptly return the Software to Fujitsu or the authorized reseller from which You obtained the Software.

1. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein Fuiitsu and its licensors grant to You a non-exclusive, non-transferable, worldwide, limited license, without right of sublicense, to install and use the Software in object code form on one controller or blade for Your internal business use in accordance with the terms contained within Your ordering documentation (Your "Software Entitlement") or as specified in the user documentation accompanying the Software (the "Documentation"). The Software is licensed, not sold, to You. Use of the Software outside the scope of Your Software Entitlement or Documentation is unauthorized and shall constitute a material breach of this EULA and void the warranty and/or support obligations of which You may otherwise be entitled. If You have licensed the CIFS protocol, the following terms apply: You may install and use only one (1) copy of the Extended Server Implementation (ESI) and Domain Services Interaction Implementation only on the same server and for use as a file server as specified in the documentation accompanying the Software, and only (i) with respect to the ESI, to interoperate or communicate with native Microsoft Windows server operating system products that are functioning in a client capacity; and (ii) with respect to the DSII, to interoperate or communicate with the domain controller functionality in a Microsoft Windows server operating system product for purposes of obtaining services from the domain controller. You may not install or use the ESI or DSII on a computer that is running any Windows client or server operating system. Fujitsu's licensors shall be a direct and intended third party beneficiary of this EULA and may enforce their rights directly against You in the event of Your breach of this EULA.

2. License Restrictions. The Software is licensed to You for use on a storage controller or blade identified by a unique serial number. Subject to any express restrictions contained within Your Software Entitlement or Documentation, You shall not nor shall You allow any third party to: (a) decompile, disassemble, decrypt, extract, or otherwise reverse engineer or attempt to reconstruct or discover any source code or underlying ideas, algorithms, or file formats of, or of any components used in the Software by any means whatever; (b) remove or conceal any product identification, copyright, patent or other notices contained in or on the Software or Documentation; (d) use any "locked" or restricted feature, function, service, application, protocol, operation, or capability without first purchasing the applicable license(s) and/or obtaining a valid license enablement key from Fujitsu, even if such feature, function, service, application, protocol, operation or capability is technically achievable without a key; (e) sell, lease, rent, lend, sublicense, distribute or otherwise transfer in whole or in part the Software or the applicable license enablement key to another party or to a different storage controller or cluster; (f) use the Software to operate in a service bureau, managed service provider or commercial hosting services environment; or (g) modify the Software, incorporate it into or with other software, or create a derivative work of any part of the Software. Your modification of the Software will breach this EULA, and such derivative work is and shall be owned entirely by Fujitsu or its licensors; You hereby assign and agree to assign to Fujitsu or its licensor all right, title and interest in and to said derivative work. You acknowledge that the Software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility, aircraft operation, air traffic control or life support system. Fujitsu and its licensors disclaim any express or implied warranty of fitness for such uses. If You use the Software for such applications, You agree to indemnify, defend and hold Fujitsu and its licensors harmless from all claims, actions, losses, liabilities, damages, costs and expenses (including attorney fees) arising out of or relating to such prohibited uses.

3. Benchmark Results. The results of any benchmark or comparison tests run on Software are considered to be the confidential information of Fujitsu or its licensors. You may not publish or provide the results of any benchmark or comparison tests run on Software to any third party without the prior written consent of Fujitsu or its licensors.

4. Intellectual Property Rights. The Software is protected by intellectual property and copyright laws and treaties worldwide, and may contain trade secrets of Fujitsu or its licensors, who have and maintain exclusive right, title and interest in and to the Software, and reserve and retain all rights not expressly granted to You herein. No right, title or interest in or to any trademark, service mark, logo or trade name of Fujitsu or its licensors is granted under this EULA. All title and intellectual property rights in and to software content which is not contained in the Software, but may be accessed or used through use of the Software, is the product belonging to the respective content owner and may be protected by patents, intellectual property and copyright laws and treaties worldwide. This EULA grants You no rights to such content, but use of such content may be governed by the respective terms and conditions of use relating to such content.

5. Audit. You agree to give Fujitsu or its licensors and its independent accountants the right to examine Your books, records, systems and usage associated with the Software during regular business hours upon reasonable notice to verify compliance with this EULA. If such audit discloses non-compliance with this EULA, You shall promptly pay to Fujitsu and its licensors the appropriate license fees, plus the reasonable costs of conducting such audit.

6. Termination. This EULA is effective until terminated. Fujitsu may terminate this EULA immediately and without notice if You fail to comply with any term of this EULA. Upon termination, all rights to use the Software will cease, and You shall promptly destroy the original and all copies of the Software and any license enablement keys in Your possession or under Your control. Termination is not an exclusive remedy and all other remedies otherwise entitled by law shall remain. Sections 2 through 10 shall survive termination of this EULA.

7. Warranty Disclaimer. FUJITSU AND ITS LICENSORS, MAKE NO EXPRESS OR IMPLIED WARRANTIES WITH REGARD TO THE SOFTWARE. FUJITSU'S AND ITS LICENSORS' LIABILITY WITH RESPECT TO THE SOFTWARE UNDER ANY WARRANTY, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY IS LIMITED EXCLUSIVELY TO SOFTWARE REPLACEMENT. THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION ARE OTHERWISE PROVIDED "AS IS" WITHOUT ANY WARRANTY INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, ACCURACY, QUIET ENJOYMENT, CORRESPONDENCE TO DESCRIPTION, NONINFRINGEMENT, OR WARRANTY THAT THE SOFTWARE IS ERROR-FREE. SOME JURISDICTIONS DO NOT ALLOW LIMITATIONS OF IMPLIED WARRANTIES; THESE LIMITATIONS MAY NOT APPLY TO YOU.

IN NO EVENT SHALL FUJITSU'S LICENSORS BE LIABLE FOR ANY DAMAGES OF ANY KIND INCLUDING DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (WHICH SHALL INCLUDE WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS OR PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) WHETHER BASED ON CONTRACT, TORT OR OTHER LEGAL THEORY, ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

8. U.S. Government and Export Regulations. The Software is a Commercial-Off-The-Shelf ("COTS") product developed at private expense; no portion of the Software has been developed with U.S. Government, state or other public-sector funds; the Software contains trade secrets and confidential commercial or financial information exempt from disclosure by 5 U.S.C. Section 552(B) (3) and (4) (Freedom Of Information Act) and 18 U.S.C. Section 1905 (Trade Secrets Act); and the ownership of the Software and any reproductions shall remain with Fujitsu and its licensors. The Software is provided to U.S. Government Agencies other than the U.S. Department of Defense ("DOD") with RESTRICTED RIGHTS and all supporting Documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the U.S. Government is subject to the restrictions as set forth in the Commercial Computer Software -Restricted Rights clause at FAR 52.227-19(b)(2). If the sale is to a DOD agency, the Government's rights in Software, supporting Documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and the Commercial Computer Software and Commercial Computer Software Documentation clause at DFARS 227-7202. Contractor/Manufacturer is: NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089. Except as expressly licensed hereunder, all rights are reserved.

The Software is subject to U.S. export control laws and may be subject to export or import regulations in other countries. You agree to comply with all applicable regulations and obtain any applicable licenses or other authorizations to export, re-export, or import the Software. **9.** Third Party Software. Notwithstanding other statements in this EULA, third party software including free, copyleft and open source software components (collectively referred to as "Third Party Software") are distributed in compliance with the particular licensing terms and conditions attributable to the Third Party Software. Fujitsu provides the Third Party Software to You "AS IS" without any warranties or indemnities of any kind. Copyright notices and licensing terms and conditions applicable to the Third Party Software are included on the media on which You received the Software within a "NOTICE" file.

10. General. You may not transfer Your rights under this EULA without Fujitsu's prior written approval. Fujitsu does not waive any of its rights under this EULA by delaying to exercise its rights, or exercising only part of its rights at any time. Any notice, report, approval or consent required or permitted by this EULA shall be in writing. If any provision of this EULA shall be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that the obligations of the parties shall remain in full force and effect and enforceable. The United Nations Convention on Contracts for the International Sales of Goods is specifically disclaimed. This EULA is the final and complete agreement between the parties relating to the license of the Software hereunder and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communication between the parties.

Abbreviations

BIOS

Basic Input/Output System

ΒX

(PRIMERGY) Blade (Server) or (PRIMERGY Server) Blade

СВ

Connection Blade

CD(-ROM)

Compact Disk (- Read Only Memory)

CIFS

Common Internet File System

CLI

Command Line Interface

cos

Console Operating System (VMware ESX Hypervisor service console)

CPU

Central Processing Unit

DVD

Digital Versatile Disk

ESX

Elastic Sky X (VMware project)

EULA

End User License Agreement

GB

Gigabyte

GHz

Gigahertz

GUI

Graphical User Interface

HD(D)

Hard Disk (Drive)

HTTP(S)

Hypertext Transfer Protocol (Secure)

I/O

Input/Output

IM

Installation Manager

IP

Internet Protocol

iRMC

integrated Remote Management Controller

iSCSI

Internet Small Computer Systems Interface (SCSI protocol over TCP/IP)

LAN

Local Area Network

LED

Light Emitting Diode

LOM

LAN On Motherboard

MMB

Management Blade

NFS

Network File System

ОМ

Operations Manager

OS

Operating System

POST

Power On Self Test

RAID

Redundant Array of Independent Disks

RAM

Random-Access Memory

SAN

Storage Area Network

SAS

Serial-Attached SCSI

SCB

Storage Control Blade

SME

Small and Medium Enterprise

SS

Solid State (Drive)

SSH

Secure Shell

SV

ServerView

SVA

ServerView Appliance

SVIM

ServerView Installation Manager

SVOM

ServerView Operations Manager

SX

(PRIMERGY) Storage (Blade)

USB

Universal Serial Bus

VSA

Virtual Storage Appliance

Figures

Figure 1:	Architecture of ServerView with Data ONTAP-v and the VSX960 hardware 9
Figure 2:	Network configuration after installation
Figure 3:	Network configuration with additional connections 19
Figure 4:	RAID controllers and VSX960 disks 22
Figure 5:	Language selection
Figure 6:	Selection of keyboard, Installation Manager mode, and configuration data storage 27
Figure 7:	Welcome screen 28
Figure 8:	Deployment mode selection
Figure 9:	OS selection
Figure 10:	RAID configuration
Figure 11:	Basic ESX configuration
Figure 12:	ESX network configuration and licensing
Figure 13:	SVA configuration
Figure 14:	VSA configuration
Figure 15:	Storage blade configuration
Figure 16:	Application selection
Figure 17:	Installation confirmation
Figure 18:	Start page of the ServerView Operations Manager with new entry Appliance 45
Figure 19:	ServerView server list entries for SCB, ESX host, VSAand SVA47
Figure 20:	Agent Deployment page of the SVA
Figure 21:	BX400S1em-044-06 now manageable
Figure 22:	Backup Manager page of the SVA

Figure 23:	Blade Power Management page of the SVA with BX400 S1	52
Figure 24:	vSphere client start page	55
Figure 25:	Text console window of an SVA	56
Figure 26:	Console window to change the SVA password	57
Figure 27:	Console window to change the SVA hostname and IP settings (1)	58
Figure 28:	Console window to change the SVA hostname and IP settings (2)	59
Figure 29:	Console window to change the regional settings	60
Figure 30:	NetApp Data ONTAP-v FilerView pre-selection screen .	61
Figure 31:	NetApp Data ONTAP-v FilerView application start page .	62
Figure 32:	Data ONTAP-v management interfaces	63
Figure 33:	Starting the iSCSI Initiator GUI	66
Figure 34:	Starting the iSCSI service	66
Figure 35:	Entering the VSA IP address	67
Figure 36:	Connecting the target	68
Figure 37:	Confirming the settings	68
Figure 38:	Letting Windows search for the new disk	69
Figure 39:	Setting the disk online	70
Figure 40:	Initializing the disk	71
Figure 41:	Formatting the disk	72
Figure 42:	The iSCSI LUN is ready for use	73
Figure 43:	IP configuration template	89

Index

Α

abbreviations list 95 administration 41 advanced video redirection 20 agent deployment 46, 48 architecture 9

В

backup manager 46, 50 BIOS 21 blade power management 46, 52 blade slot 17 booting the SCB 25 BX900 15

С

CLOSED LOCK icon 43 Connection Blade 18

D

Data ONTAP-v CLI 63 Data ONTAP-v documentation 64 diagnostic hardware 81 SVA 83 VMware ESX 82 VSA 83 diagnostics 81 documentation ZIP file 61 dvadmin CLI 42, 63 DVD access 20

Е

ESX console (ESX COS) 42 ESX host 9 EULA 36

F

features overview 13 FilerView GUI 42, 61 first installation 17 front-side I/O module 20

I

installation 17 installation steps overview 24 introduction 9 iRMC IP address 21 iSCSI LUN 64

J

Java 43

L

license Data ONTAP-v 35 ESX 33 limits 87 NFS 87 SAN 87 WAFL 87 Local Service Display 17

Μ

maintenance installation 40 Management Blade 17 maximum volume size 88

Ν

notational conventions 10 number of NFS mounts 88 number of server connections 88 number of volumes 88

0

OM database 46 OPEN LOCK icon 43

Ρ

password ESX 32 SVA 34, 57 VSA 35 purchase options 15

R

RAID configuration 22, 31 RAID management GUI 41 recovery installation 77 remote storage 20 remote storage device 20 requirements (HW and SW) 14 restrictions 87

S

SCB 9 scope of delivery 15 security certificate 43 semigraphic UI 54 ServerView documentation 11 ServerView Update Manager Express 40 slot selection 17 storage blade 36 Storage Control Blade 17 storage management 46, 61 SVA 9, 11 SVA hostname 57 SVA IP address 57 SVIM for VSX960 20 SVOM integration 45

Т

text UI 41, 54

U

update installation 40 user input 26 user interfaces overview 41, 44, 63

V

```
vCenter 43
VSA 9, 11
VSA EULA 90
vSphere 43
vSphere client 43, 54
VSX960 9
```

Υ

Y-Cable 77