

FUJITSU Software ServerView Suite ServerView RAID Manager

Copyright and trademarks

Copyright © 2009 - 2014 Fujitsu Technology Solutions GmbH

All rights reserved.

Delivery subject to availability; right of technical modifications reserved.

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

Contents

1 Basics	3
1.1 Supported RAID Levels	3
1.2 RAID Controller Functions	7
1.3 Supported Controllers and Devices	9
2 Login	10
2.1 Installation	10
2.2 Login	14
2.3 Security Certificate	21
2.4 System requirements	24
2.5 Licenses	25
3 The User Interface	26
3.1 Elements of the User Interface	26
3.2 Event Status Indicators and Icons	27
4 Properties	29
4.1 Displaying and Modifying Properties	29
5 Actions and Dialogs	46
5.1 Executing Actions	46
5.2 Creating Logical Drives	52
5.3 Modifying Logical Drives (migrating)	55
5.4 Processing Hot Spares	55
5.5 Foreign Configuration	58
5.6 Task	59
6 Events	65
6.1 Displaying Events	65
6.2 Events / SNMP Traps	66
6.3 Errors	114
7 Help	119
7.1 Help	119
7.2 Online Help	119
7.3 amCLI	120
7.4 Frequently Asked Questions - FAQs	129
8 Glossary	131

1 Basics

1.1 Supported RAID Levels

RAID is an acronym first defined in 1987 by researchers of the University of California, Berkeley as "Redundant Array of Inexpensive Disks". This storage technology allows a combination of multiple low-cost disk components into logical units (logical drives). A so called "RAID level" describes how data is distributed over the various disks of a logical drive. These distribution algorithms determine the balance of increasing data reliability through redundancy and/or increasing performance through parallel input/output transactions.

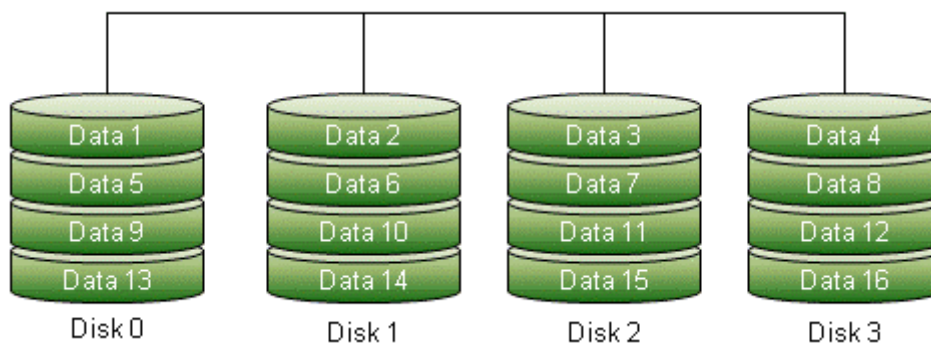
For marketing reasons the definition of RAID was later replaced by RAID manufacturers with the term "Redundant Array of Independent Disks". RAID technology should not be subject to a "low cost" expectation.

RAID is now a collective name for computer data storage schemes that can divide and replicate data among multiple disks.

The different RAID levels are named by the word RAID followed by a number, as in RAID-0, RAID-1, etc. A brief description of the best known RAID levels the controllers supported by ServerView RAID can configure follows:

1.1.1 RAID-0

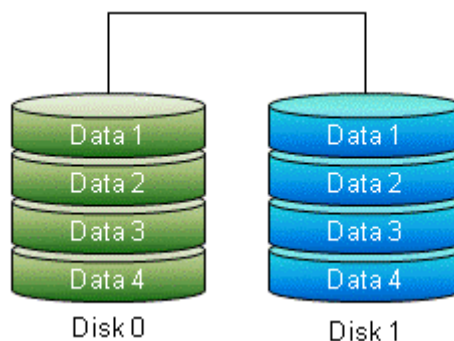
A RAID-0 is created by distributing (striping) data over two or more disks. Single striping (like that just mentioned) does not generate any redundancy for protecting data, but by distributing the data over multiple drives it provides the best read/write performance of all RAID types.



1.1.2 RAID-1

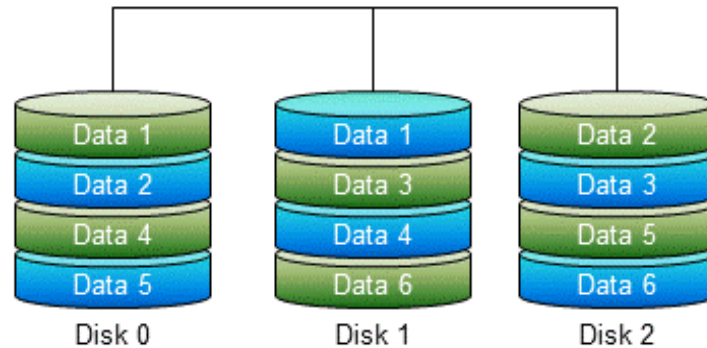
A RAID-1 consists of two disks. The data stored on the array is written to both drives. The mirroring of data provides a redundancy which ensures that no data is lost if one drive fails. However, only half the total capacity of the two disks is available because all data is written to both drives.

In comparison with a single drive RAID-1 offers no benefits in terms of write performance, but because the data is distributed over two drives it provides advantages in read performance (and data security).



1.1.3 RAID-1E

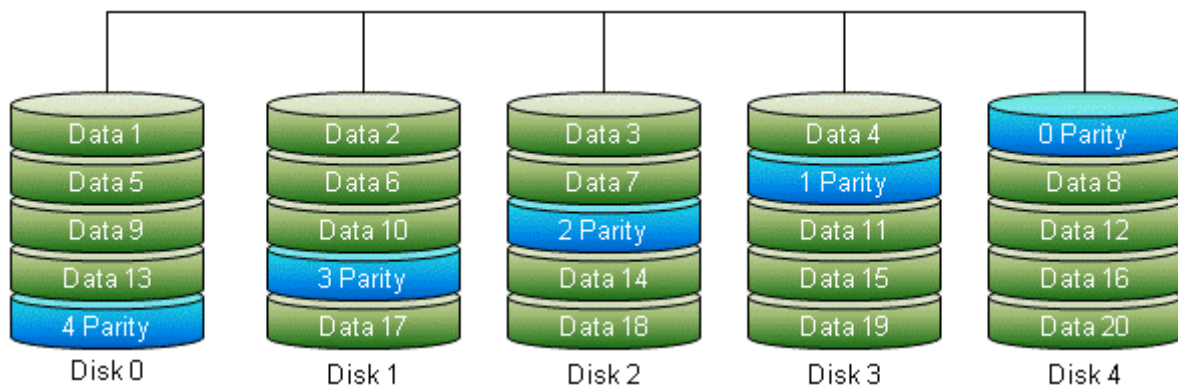
A RAID-1E consists of at least three drives. Some controllers require a configuration with an even drive count, e.g. SAS MegaRAID. Individual data blocks are mirrored onto the next disk (replication), and RAID-1E consequently offers better failsafe performance than **RAID-1**. However, neither two adjacent nor the first and last disks may fail simultaneously.



1.1.4 RAID-5

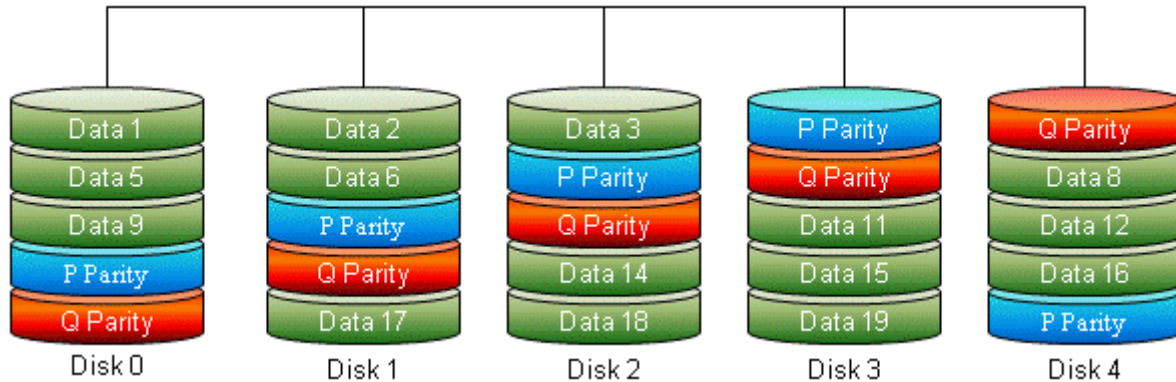
At least three drives are required to create a RAID-5. As with a **RAID-0** the data is distributed over various drives, but in the case of RAID-5 the capacity of a drive is used to store parity information. The parity information is also distributed over all the drives. The controller generates this parity whenever data is written to the array and distributed over all the drives. If a drive fails, the content of the failed drive can be restored from the data and the parity of the remaining drives.

The use of parity minimizes the capacity costs of redundancy. As only one drive is used to store the parity, two thirds of the total capacity (in a 3 disk configuration) can still be used for data. In the case of arrays with more disks the reduction of the usable total capacity is less. With RAID-5 the write performance is lower because parity data must first be generated for each write process. The read performance is good, however, because the requests are distributed over all drives.



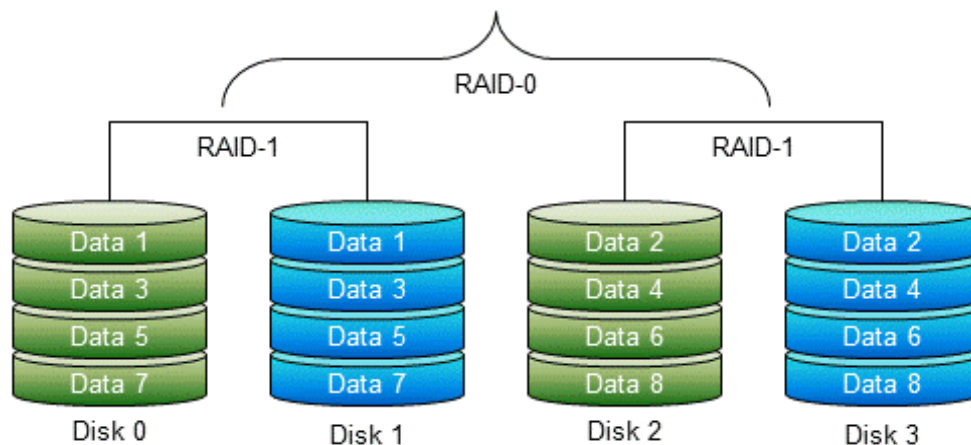
1.1.5 RAID-6

A RAID-6 requires at least four disks and functions in a similar way to a RAID-5, but can handle the failure of two disks. Some RAID controllers also offer a 3 disk configuration for RAID-6. Parity on 2 disks equals a double mirroring of data. In the case of a RAID-6 two pieces of parity information are calculated instead of one and these are distributed over all drives on a stripe-by-stripe basis. This is why a RAID-6 offers the highest level of security. Write access is a little slower than with **RAID-5**.



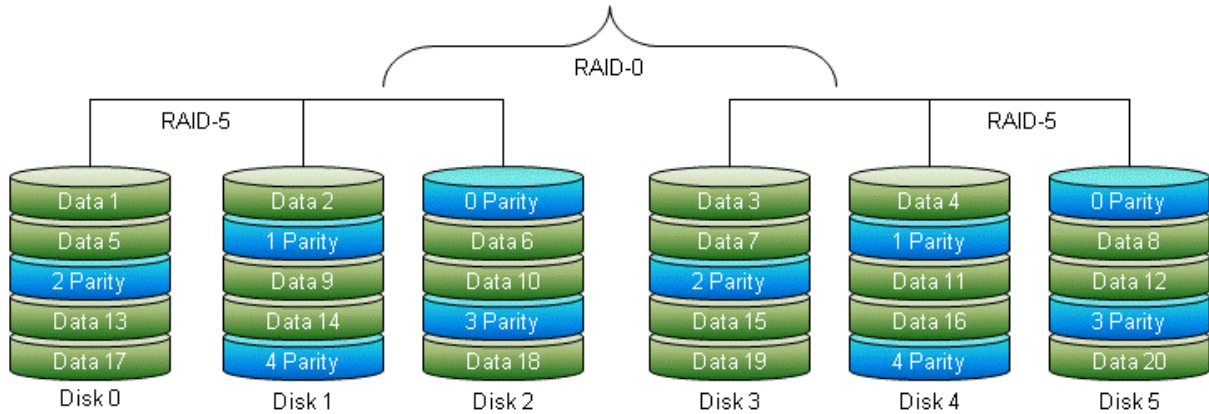
1.1.6 RAID-10

A RAID-10 is a dual-level array which is created by two or more equal-sized arrays of the type **RAID-1** being used to produce a **RAID-0**. A top-level array (RAID-0) shares the total data load with the second-level array (RAID-1), thus enhancing both the read and the write performance. As second-level arrays are RAID-1s, redundancy is also offered. However, only half the total capacity of the drives used is available in the array.



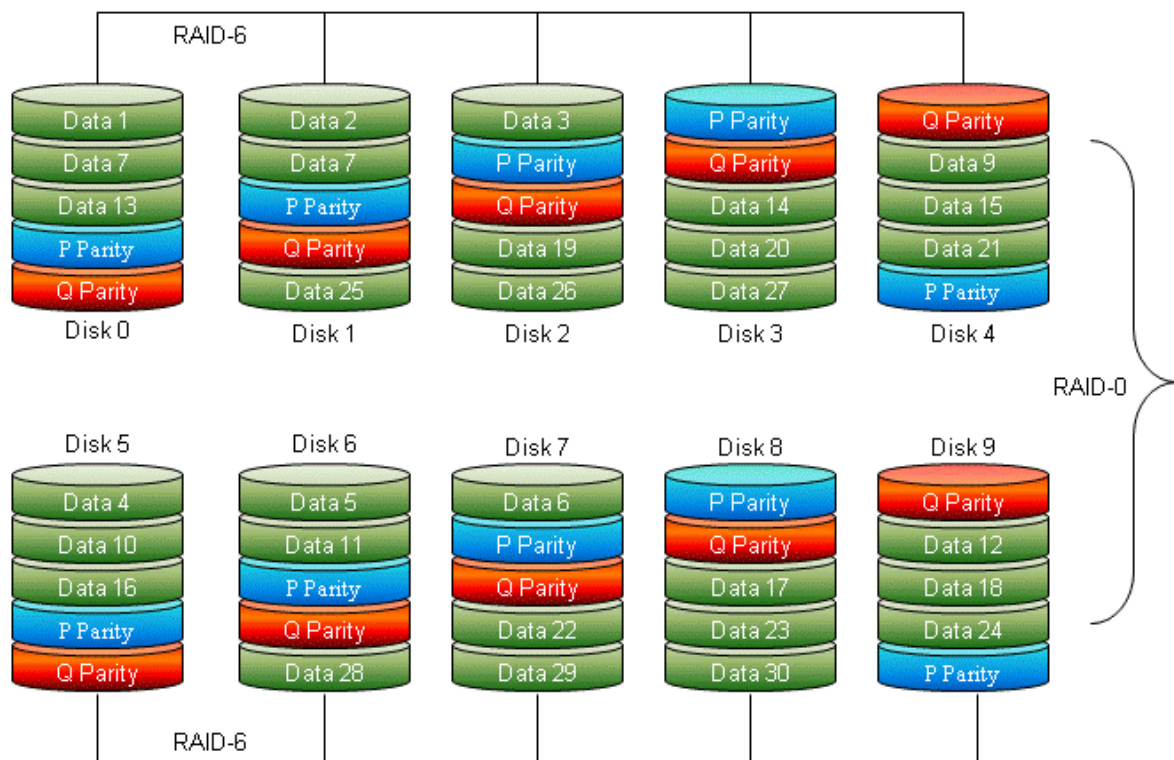
1.1.7 RAID-50

A RAID-50 is a dual-level array which is created by using at least two arrays of the type **RAID-5** to form a **RAID-0**. The top-level array (RAID-0) shares the data with the second-level array (RAID-5), thus enhancing both the read and the write performance. Since the second-level arrays use RAID-5, the parity provides efficient redundancy.



1.1.8 RAID-60

A RAID-60 is a dual-level array which is created by means of at least two arrays of the type **RAID-6** in order to form a RAID-0. The uppermost array (**RAID-0**) shares the data with the array on the second level (**RAID-6**), which increases the read and write accesses. Using RAID-6 on the second level also guarantees a high degree of data security.



1.1.9 Single Volume, JBOD

A single volume consists of a single disk. In the actual sense of the word this is not a real RAID type and is thus also referred to as a "none-RAID". According to the latest definition of the Storage Networking Industry Association a JBOD (Just a Bunch of Disks) is one of these although the term can sometimes refer to multiple physical disks.

1.1.10 Concatenation

A concatenation is formed by interconnecting two or more disks. In this case the drives can have different capacities and are interconnected from beginning to end. A global volume offers no redundancy and no performance benefits compared to a single drive; it is seen in the system merely as a correspondingly large drive.

1.1.11 RAID Volume

A RAID volume is created by interconnecting two or more arrays of the same type. In contrast to the dual-level arrays described above, arrays in a RAID volume need not have the same capacity but are interconnected (as described above under concatenation).

Note: Sometimes the term "volume" is also used as a synonym for array.

1.2 RAID Controller Functions

In the context of RAID terms are used and functions described which are explained in detail below.

1.2.1 Embedded RAID / Host RAID

"Embedded RAID" means hardware (ASIC) is provided on the RAID controller which relieves the system CPU (host) of RAID controller functions. As a result the server can devote itself to processing its core applications and the overall performance is improved. If this hardware support is not available, the term "host RAID" is used.

1.2.2 Drive Usage

For simplicity's sake the different RAID types under **Supported RAID Levels** all use complete disk drives of the same size. In fact the usable capacity of each drive is limited by the disk drive with the lowest capacity if drives with different capacities are used.

If, for example, a **RAID-1** is created from a 160-Gbyte and an 80-Gbyte drive, only half the capacity of the larger disk can be used, thus limiting it to 80-Gbyte. Furthermore, a small part is removed from each drive for the so-called RAID Signature.

1.2.3 RAID Signature

RAID controllers use a small segment at the beginning or end of each connected drive to store information on the drives and arrays attached to the controller. This segment is also referred to as RAID Signature and is not available for general use for saving user data.

1.2.4 Migration

Some RAID controllers support the modification of existing logical drives through expansion options, migration of one RAID type to another, and modification of the stripe size. The migration options depend on the RAID controller used.

Further information is provided under **Modifying Logical Drives**.

1.2.5 Online Capacity Expansion

Most operating systems of today support Online Capacity Expansion (OCE). OCE means that the additional capacity after a logical drive has been expanded can be used without rebooting the system. Details on the additional storage capacity are provided in the documentation for your operating system.

1.2.6 Cabinets

RAID controllers also support external drive enclosures which use SES or SAF-TE enclosure administration hardware. This extended hardware support enables additional administrative information for the enclosure, e.g. fan speed, temperature and voltage. Such enclosures generally offer further properties, e.g. hot swap.

1.2.7 Hot Swap

Either through the use of SATA technology or the above-mentioned drive enclosure RAID controllers support so called hot swap, i.e. disk drives can be replaced during ongoing operation without the system having to be rebooted.

Note: Hot swapping of hard disks is possible only if a disk was placed *Offline* beforehand.

1.2.8 Hot Spare

A hot spare is a physical drive which is available in a redundant logical drive as a replacement for a failed disk. If a drive fails the hot spare replaces it and the logical drive is recreated. The data is then reconstructed on this new disk during ongoing operation. Until reconstruction has been completed the access to the data takes a little longer but is possible at any time.

RAID controllers support the following hot spare types:

- Global hot spares support every logical drive for which the drive provides sufficient storage capacity for backup purposes.
- Dedicated hot spares support only logical drives which it has been assigned to back up.

Note: Some RAID controllers automatically assign newly added and unused drives to the global hot spares.

1.2.9 Consistency Check/Make Data Consistent (MDC)

The consistency check operation verifies correctness of the data in logical drives that use RAID levels 1, 5, 6, 10, 50, and 60. (RAID-0 does not provide data redundancy). For example, in a system with parity, checking consistency means computing the data on one disk and comparing the results to the contents of the parity disk.

Make data consistent (MDC) does not only verify the correctness of data but also attempts to correct inconsistent data automatically.

Note: It is recommended that you perform a consistency check at least once a month.

1.2.10 Copyback

The copyback feature allows you to copy data from a source disk of a logical drive to a destination disk that is not a part of the logical drive. Copyback is often used to create or restore a specific physical configuration for an array (for example, a specific arrangement of array members on the device I/O buses). Copyback can be run automatically or manually.

Typically, when a disk fails or is expected to fail, the data is rebuilt on a hot spare. The failed disk is replaced with a new disk. Then the data is copied from the hot spare to the new disk, and the hot spare reverts from a rebuild disk to its original hot spare status. The copyback operation runs as a background activity, and the logical drive is still available online to the host.

Copyback is also initiated when the first Self-Monitoring Analysis and Reporting Technology (SMART) error occurs on a disk that is part of a logical drive. The destination disk is a hot spare that qualifies as a rebuild disk. The disk with the SMART error is marked as failed only after the successful completion of the copyback. This avoids putting the array in degraded status.

1.2.11 Background Initialization (BGI)

Background initialization is a consistency check that is forced when you create a virtual drive. This is an automatic operation that starts 5 minutes after you create the virtual drive.

Background initialization is a check for media errors on the disks. It ensures that striped data segments are the same on all disks in a drive group. The default and recommended background initialization rate is 30 percent. Before you change the rebuild rate, you must stop the background initialization or the rate change will not affect the background initialization rate.

1.2.12 Patrol Read

Patrol read involves the review of your system for possible disk errors that could lead to disk failure and then action to correct errors. The goal is to protect data integrity by detecting disk failure before the failure can damage data. The corrective actions depend on the array configuration and the type of errors.

Patrol read starts only when the controller is idle for a defined period of time and no other background tasks are active, though it can continue to run during heavy I/O processes.

1.2.13 MegaRAID® CacheCade™ Pro 2.0

MegaRAID CacheCade Pro 2.0 read/write software eliminates the need for manually configured hybrid arrays by intelligently and

dynamically managing frequently accessed data and copying it from HDD volumes to a higher performance layer of SSD cache. Copying the most accessed data ('hot spot') to flash cache relieves the primary HDD array from time-consuming transactions which allows for more efficient hard disk operation, reduced latency, and accelerated read and write speeds. This provides significant improvements to overall system performance – two to twelve times that of HDD-only configurations – for a wide variety of server applications including web, file, online transaction processing (OLTP) database, data mining and other transaction-intensive applications.

1.2.14 MegaRAID® FastPath™

MegaRAID FastPath software is a high-performance IO accelerator for SSD arrays connected to a MegaRAID controller card. This advanced software is an optimized version of MegaRAID technology that can dramatically boost storage subsystem and overall application performance – particularly those that demonstrate high random read/write operation workloads – when deployed with a 6Gb/s MegaRAID SATA+SAS controller connected to SSDs.

Application workloads that will benefit most from MegaRAID FastPath software with SSD volumes are those with small and random IO patterns requiring high transactional throughput, such as OLTP.

1.3 Supported Controllers and Devices

ServerView RAID Manager permits administration of various RAID controllers and the devices attached to them.

1.3.1 Supported Controllers

ServerView RAID Manager supports all current variants from the different vendors. This support covers SCSI, SATA, and SAS, as well as RAID controllers on the mainboard and the expansion boards, and solutions with corresponding implementation and offers only those administrative options which are actually supported.

Most controller functions which are supported are described in this online help. However, as not all controllers always support all functions and new functions may be added through new controllers or driver software updates, it is helpful also to refer to the release information for the controller concerned and the current release status of ServerView RAID Manager.

1.3.2 Supported SCSI Devices

In addition to SCSI hard disk drives SCSI RAID controllers also support tape drives.

1.3.3 Supported Serial ATA Devices

Serial ATA RAID controllers support only SATA hard disk drives.

1.3.4 Supported SAS Devices

Serial Attached SCSI replaces the previous parallel SCSI interface. SAS RAID controllers support both SAS and SATA hard disk drives. Please take note of the relevant controller release information.

2 Login

2.1 Installation

If ServerView RAID Manager is not installed automatically during setup with the ServerView Installation Manager or you would like to use RAID management without the whole ServerView Suite installed on your system you can install ServerView RAID Manager independently.

2.1.1 General



If you have used or installed other programs for RAID management before ServerView RAID Manager is installed, you must uninstall them. Further information on this is provided in the relevant release notices.

Assuming that the current release of ServerView RAID Manager is Version 5.8.0, please perform installation as follows:

1. Open the console window (Linux/VMware) or Explorer (Windows) and navigate to the directory containing the current ServerView RAID Manager installation package.

RHEL5-32	ServerView_RAID-5.8-0.el5.i386.rpm
RHEL5-64	ServerView_RAID-5.8-0.el5.x86_64.rpm
RHEL6-32	ServerView_RAID-5.8-0.el6.i686.rpm
RHEL6-64	ServerView_RAID-5.8-0.el6.x86_64.rpm
RHEL7-64	ServerView_RAID-5.8-0.el7.x86_64.rpm
SLES10-32	ServerView_RAID-5.8-0.sles10.i386.rpm
SLES10-64	ServerView_RAID-5.8-0.sles10.x86_64.rpm
SLES11-32	ServerView_RAID-5.8-0.sles11.i586.rpm
SLES11-64	ServerView_RAID-5.8-0.sles11.x86_64.rpm
Windows 32 bit	ServerView_RAID.msi
Windows 64 bit	ServerView_RAID_x64.msi

2. For initial installation under Linux RHEL6-64 please enter `rpm -ivh ServerView_RAID-5.8-0.el6.x86_64.rpm`. An update installation is performed using `rpm -Uvh ServerView_RAID-5.8-0.el6.x86_64.rpm`. You can also delete the older version beforehand. To do this, enter `rpm -e ServerView_RAID`. You can then proceed as for initial installation. The procedures are all started by pressing the *Enter* key. On a Windows system you start the update/installation by double-clicking on the installation package. Follow the installation instructions which you are offered in the dialog boxes.



During installation on windows system, you can select installation type from the following 3 types:

- Standard
- Complete
- Custom

As for "Standard" and "Complete", components to be installed are identical, that is, every useful component will be automatically selected and installed. With "Custom", you can choose which hardware supports and/or SNMP support to be installed as you want. Since most components are enabled in "Custom" by default, you need to deselect unnecessary items before proceeding your installation process.

Note: When you are going to do upgrade installation, you must follow the same installation type and components you chose when installing previous version.

The Core Editions of Windows Server 2008 and newer provide a command line interface only. To install ServerView RAID Manager on these operating systems use the following command line: `msiexec SERVICES=start REBOOT=ReallySuppress ALLUSERS=1 /i ServerView_RAID.msi /qr`. Instead of `ServerView_RAID.msi` on 32-bit versions use `ServerView_RAID_x64.msi` on 64-bit versions.

3. To monitor RAID controllers of VMware ESXi servers you have to configure some settings after installation of ServerView RAID Manager (see **VMware ESXi** below).
4. If you want to work with the graphical user interface of ServerView RAID Manager and the Java Runtime Environment (JRE) has not yet been installed, it may be necessary to install a current Java Runtime Environment on your client.



To find out which combination of web browser and Java plugin can be used read the documentation of your web browser and the information provided by Oracle on java.com.

If there is no Java plugin available for a specific 64-bit web browser then prepare a 32-bit web browser environment.

5. To communicate with ServerView RAID Manager web browsers use an HTTPS connection (i.e. a secure SSL connection). Therefore ServerView RAID Manager needs a certificate (X.509 certificate) to authenticate itself at the web browser. During installation a self-signed certificate is created automatically. When connecting to ServerView RAID Manager the browser will issue a certificate error with suggestions how to proceed. To fulfill high-level security requirements typical for enterprise usage this self-signed certificate can be replaced by a certificate that is signed by a trusted Certificate Authority. Use **amCLI** to import such a certificate.

Example syntax:

```
amCLI -i <certificate file> <private key file>
```

To check which version of ServerView RAID Manager is installed you can do the following:

- Under Linux the `rpm -qa` command (entry on the console) outputs a list of all the installed RPM packages. If ServerView RAID Manager is installed, you are shown the package with the current version, for example `ServerView_RAID-5.8-0`.
- Under Windows you are shown the installation under *Start > Settings > Control Panel > Add or Remove Programs*.

To delete ServerView RAID Manager installation do the following:

- Under Linux you can delete the installation of ServerView RAID Manager by executing the command `rpm -e ServerView_RAID`.
- Under Windows you can delete the installation under *Start > Settings > Control Panel > Add or Remove Programs*.
- The Core Editions of Windows Server 2008 and newer require execution of a command line again. Use `wmic product where name="Fujitsu Software ServerView RAID Manager" call uninstall` to delete the installation.

2.1.2 VMware ESXi

On the Central Management Station (virtual or physical) with running ServerView RAID Manager use **amCLI** to add required server connection information for ESXi hypervisors to be managed.

Example syntax:

```
amCLI -e 21/0 add_server name=<FQDN or Hostname or IP> port=5989 username=root password=<ESXi root password>
```

This command adds an existing ESXi server to the ServerView RAID Manager configuration. The FQDN or Hostname requires an entry in DNS otherwise use the IP address of the server. The username must be "root" (or any other with these rights) and the password must be the valid password of this user on the ESXi server. This is required ESXi information to connect to the CIMOM using https on port 5989.

Note: Passwords including characters that have a special meaning for the used command line interpreter must be escaped by suitable means (e.g. double quotes).

After adding a server it is recommended to check the configuration and connection with *amCLI -e 21/0 verify_server name=<FQDN or Hostname or IP>*. If the result is "No Error", configuration and connection status are OK. Otherwise, please check the configuration of the ESXi server.

For changes to the configuration you can use *amCLI -e 21/0 modify_server name=<FQDN or Hostname or IP> ...* and to delete a server *amCLI -e 21/0 delete_server name=<FQDN or Hostname or IP>* with the name which was used by add server. A list of configured servers can be seen by using the command *amCLI -e 21/0 show_server_list*. For more syntax details use *amCLI -? exec 21/0*.

Note: If the CMS is rebooted or shut down no monitoring of ESXi servers takes place.

To increase performance of the ESXi connections some SFCB (integrated CIMOM) configuration parameters can be changed optionally in ESXi. Edit **/etc/sfcb/sfcb.cfg** and modify the following values:

```
keepaliveTimeout: 10000  
keepaliveMaxRequest: 10000
```

On the start screen of ESXi you can invoke the menu *Customize System*. Ensure that the parameter *Configure Lockdown Mode* is set to *Disabled*.

2.1.3 Registering trap information into SNMP manager

ServerView RAID Manager offers its own MIB file *RAID.mib* (Windows) or *FSC-RAID-MIB.txt* (Linux/VMware/Solaris) in which its **SNMP trap information** is defined.

If you are planning to use your own SNMP manager to receive SNMP traps from ServerView RAID Manager, it is highly recommended to integrate this file into the SNMP manager beforehand. That way, traps from ServerView RAID Manager can be processed properly in the SNMP manager. Otherwise, some traps may be displayed as 'Unknown trap'.

You can find the file in the following directory after installing ServerView RAID Manager:

- On Windows systems:
C:\Program Files\Fujitsu\ServerView Suite\RAID Manager\bin\RAID.mib
- On Linux systems:
/usr/share/snmp/mibs/FSC-RAID-MIB.txt

Note: Registering one of the files *RAID.mib* or *FSC-RAID-MIB.txt* is enough, since they have identical contents.



In case of registering *FSC-RAID-MIB.txt* into ServerView Operations Manager, it is necessary to rename the file into *RAID.mib* in advance. Please observe the letter case of the file name *RAID.mib*. ServerView Operations Manager is strictly case-sensitive.

Regarding more details how to register the file, please refer to your favorite SNMP manager's user guide. If you use ServerView Operations Manager, please refer to "*MIB Integration*" of "*ServerView Suite ServerView Event Manager*" (sv-event-mgr-en.pdf).

Please observe the other ServerView RAID Manager **system requirements** also.

2.2 Login

You log in as follows:

ServerView RAID Manager must be installed on the system to be administered. If this has not been done, please install ServerView RAID Manager.

Note: Under Windows you find or start the local application by clicking on *Start > Programs > Fujitsu > ServerView Suite > RAID Manager > RAID Manager*.

If ServerView RAID Manager is already installed on the target system, you can also start the RAID Manager directly via the **browser from an arbitrary client**. In the address bar, enter the FQDN (Fully Qualified Domain Name) followed by TCP port number 3173 (e.g. *https://<FQDN>:3173*). Confirm your input using the *CR* key to get access to the desired system. This works both locally and from a remote system.

Note: If there is an intervening firewall in the environment, you need to configure the network settings so that the port used by ServerView RAID Manager will not be blocked.

Note: When you run ServerView RAID Manager for the first time after installation, you must install a security certificate. Information on doing this is provided under **Security Certificate**.

If you have not turned on **Single Sign On and Role Based Access Control** the following login screen is displayed in the browser, after a connection has been successfully set up to the system.



Note: By the *Help* button at the top right the online help can be opened directly without the user needing to log in.

If required, choose a different language in the login screen by selecting the related national flag.

Enter the user name and the password which are to be used to log into this system. Then click on *Login* to enter **ServerView RAID Manager**.



For authentication and authorization purposes ServerView RAID Manager uses the interfaces provided by the operating system of the server to be monitored. Users who have been set up with administration rights can perform configuration via ServerView RAID Manager. Non-privileged users can obtain a read-only view of the RAID configuration on the server as well as get write access rights for ServerView RAID Manager.

To grant certain users without administration rights the possibility to take over configuration tasks or a read-only access, this can be done as follows:

RAID administrators

A user with write access rights for ServerView RAID Manager can be set up by creating a new user group with the name "raid-adm" (default) and adding an existing user to this group.

RAID observers

A read-only user can be set up by creating a new user group with the name "raid-usr" (default) and adding an existing user to this group.

To get more flexibility the names for the two user groups described above can be freely defined by editing the properties **Admin group** and **User group**. These properties can be found on the *Settings* tab of *System* category. If no group name is given there will be no check for membership in a user group during authentication. The settings are activated immediately.

On Windows the search order for group membership is fixed. First the local user groups of the system are checked, then the global groups in an active directory, and finally the local groups in an active directory.

On Linux the search order is defined in PAM configuration. On systems with very restrictive access control it may be necessary to configure PAM access by editing **/etc/security/access.conf** additionally.

All other users even though they can authenticate at the server have no authorization for the ServerView RAID Manager functionality.

The first user automatically has read/write authorization. Every subsequent user only has read authorization, but – provided they have appropriate administration rights – can obtain write authorization. The user who had write authorization up to this point is then informed of this.

2.2.1 Client / Browser Configuration

Please check and if necessary change the following settings for

- Internet Explorer:
Enable an encrypted communication by
Tools > Internet Options > Advanced > Security and enable *Use SSL 3.0* and *Use TLS 1.0*.

Add zone settings of browser as following:

1. Select *Tools > Internet Options*.
2. Click *Security* tab, and select *Local intranet* or *Trusted sites*.
3. Click *Sites* and add the server URL where ServerView RAID Manager is installed (<https://<FQDN>>).
4. Click *Close*.
5. Click *Custom level...*
6. Set *ActiveX controls and plug-ins* to *Enable*.

- Netscape/Firefox
Select *Edit > Settings > Advanced > Encryption* and enable the following items:
 - *SSL 3.0* and *TLS 1.0* (also *SSL 2.0*, only for older version).
 - *Enable Java*.

If you use a proxy server for the Internet you must bypass it to enable you to access the server. If you know the IP address of the system that you wish to administer remotely, you might select the following, for example, for

- Internet Explorer:
Tools > Internet Options > Connections > LAN/Settings... > Use a proxy server for your LAN/Advanced... and enter the IP address of the system to be administered in the *Exceptions* area.
- Netscape/Firefox:
Edit > Settings > Advanced > Proxy Server > Manual Proxy Server Configuration > No Proxy and enter the IP address of the system to be administered.



Do not use "Back", "Forward", or "Refresh" button of the browser.

There is no working web browser in Core Editions of Windows Server 2008 and newer installations.
To manage RAID controllers, prepare a client as described as follows and in **System requirements** and use ServerView RAID Manager on it.

2.2.2 Single Sign On and Role Based Access Control

If your server management environment is built around ServerView Operations Manager 5.0 or newer and the Single Sign On infrastructure (CAS - Central Authentication Service) and directory services extensions for Role Based Access Control (RBAC) are configured you can participate with ServerView RAID Manager.

After the first login to ServerView RAID Manager as described above switch to the Settings tab of your system where you can enable CAS and RBAC.

Edit either the CAS or the LDAP entry to enabled. Both entries are related at the moment so if you turn on CAS the setting for LDAP will be enabled automatically.

The screenshot shows the 'Settings' tab in the ServerView RAID Manager interface. It contains two main sections: 'Single Sign On' and 'Role based access control'. Each section has a table of settings and an 'Edit' button at the bottom.

Single Sign On	
CAS	Enabled
CAS port	3170
CAS server	<CAS server>
CAS base URL	/cas

Role based access control	
LDAP	Enabled
LDAP server	<LDAP server>
LDAP port	636
Allow non-secure access	Enabled
LDAP non-secure port	389
Base DN	DC=example,DC=com
Role DN	OU=SVS
User search base	DC=Users,DC=example,DC=com
User search filter	sAMAccountName=%u
Username	<Username>
Password	*****

i After turning on CAS and LDAP do not logout from ServerView RAID Manager until connection to CAS and LDAP is working correct or CAS and LDAP are turned off again. Otherwise you will not be able to login again.

If CAS and LDAP are mistakenly enabled with incorrect settings it is possible to turn them off again by using **amCLI**:

```
amCLI -s 21/3 CAS disabled
```

If you have enabled CAS and LDAP you see a few properties that have to be adapted to the existing environment. This information is available on the Central Management Station (CMS) where ServerView Operations Manager is installed.

Up to and including version 6.00 of ServerView Operations Manager open the following file on that system in your favorite editor:


- On Windows systems:
<ServerView directory>\jboss\server\serverview\conf\sv-sec-config.xml
- On Linux systems:
/opt/fujitsu/ServerViewSuite/jboss/server/serverview/conf/sv-sec-config.xml


Starting with version 6.10 of ServerView Operations Manager JBoss 7 is used. Open the following file on that system in an editor:

- On Windows systems:
<ServerView directory>\jboss\standalone\svconf\sv-sec-config.xml
- On Linux systems:
/opt/fujitsu/ServerViewSuite/jboss/standalone/svconf/sv-sec-config.xml

The XML tags in that file approximately match the properties in the Settings tab of ServerView RAID Manager. Change the properties accordingly.

CAS: CAS server CAS port CAS base URL LDAP: LDAP server LDAP port Base DN User search base User search filter Role DN Username Password	<pre> ... <ns0:cms> <ns0:serverUrl>https://<system_name>:3170</ns0:serverUrl> </ns0:cms> <ns0:authentication> <ns0:cas> <ns0:contextRoot>/cas</ns0:contextRoot> <ns0:uriLogin>/login</ns0:uriLogin> <ns0:uriServiceValidate>/serviceValidate</ns0:uriServiceValidate> <ns0:uriInsertTgt>/Insert/TGT</ns0:uriInsertTgt> </ns0:cas> </ns0:authentication> <ns0:authorization> <ns0:ldapServer> <ns0:serverUrl>ldaps://<system_name>:1474</ns0:serverUrl> <ns0:baseDN>dc=fujitsu,dc=com</ns0:baseDN> <ns0:userSearchBase>ou=users,dc=fujitsu,dc=com</ns0:userSearchBase> <ns0:userSearchFilter>uid=%u</ns0:userSearchFilter> <ns0:serverViewRDN>OU=SVS</ns0:serverViewRDN> <ns0:securityPrincipal>cn=svuser,ou=users,dc=fujitsu,dc=com</ns0:securityPrincipal> <ns0:securityCredentials><password></ns0:securityCredentials> </ns0:ldapServer> <ns0:department>CMS</ns0:department> </ns0:authorization> ... </pre>
---	---

 The names of the configured servers must match exactly.

 In newer version of ServerView Operations Manager the securityCredentials entry is encrypted. Ask your ServerView Operations Manager administrator for the password.

To test the connection to CAS you can execute the action "**Test CAS connection**". To test the connection to the directory service it is best practice to allow an unsecure communication first. Enable property "**Allow non-secure access**" and set port as configured. Now execute action "**Test LDAP connection**".

If both tests pass you have to set up the environment for secure connection to the directory service. You need a certificate file from the Central Management Station. This file can be either obtained manually or downloaded from the CMS.

The file containing the certificate can be found in the following directory on the CMS:

- On Windows systems:
<ServerView directory>\svcommon\data\download\pki
- On Linux systems:
/opt/fujitsu/ServerViewSuite/svcommon/data/download/pki

To download the file direct your browser to https://<system_name>:3170/Download/pki where you have to login by Central Authentication Service. Then store the certificate file `<system_name>.scs.pem` on your local system import it into your system's certificate store.

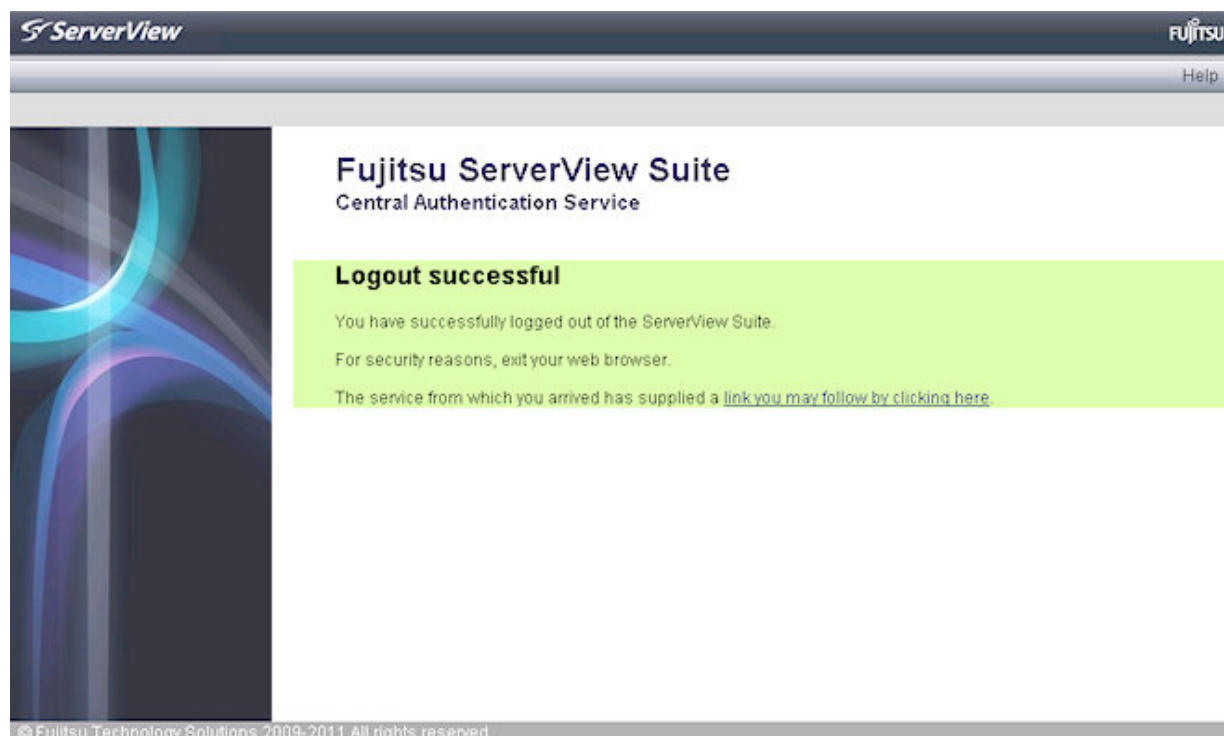
On Windows systems follow these steps to import the certificate:

1. Click *Start*, click *Run*, type **mmc**, and then click *OK*.
2. On the *File* menu, click *Add/Remove Snap-in*, and then click *Add*.
3. In the *Add Standalone Snap-in* dialog box, click *Certificates*, click *Add*, click *Computer account*, click *Next*, and then click *Finish*.
4. Click *Close*, and then click *OK*.
5. Expand *Certificates (Local Computer)*, expand *Trusted Root Certification Authorities*.
6. Right-click *Certificates*, click *All Tasks*, click *Import*, and then click *Next*.
7. In the *File name* box, type the file name or browse for your stored certificate file, and then click *Next*.
8. Click *Finish*, and then click *OK*.

On Linux systems you need to copy the certificate file into the CA certificate directory (often `/etc/ssl/certs/`) and reindex all certificates with `"c_rehash"`.

After successful installation return to ServerView RAID Manager, disable the unsecure access to LDAP, and execute "**Test LDAP connection**" again. If CAS and LDAP connection tests were successful ServerView RAID Manager is now prepared to participate in Single Sign On and Role Based Access Control.

If you logout now the following screen will be displayed:



After clicking the link on the right side of the logout screen the login screen from CAS will be displayed:



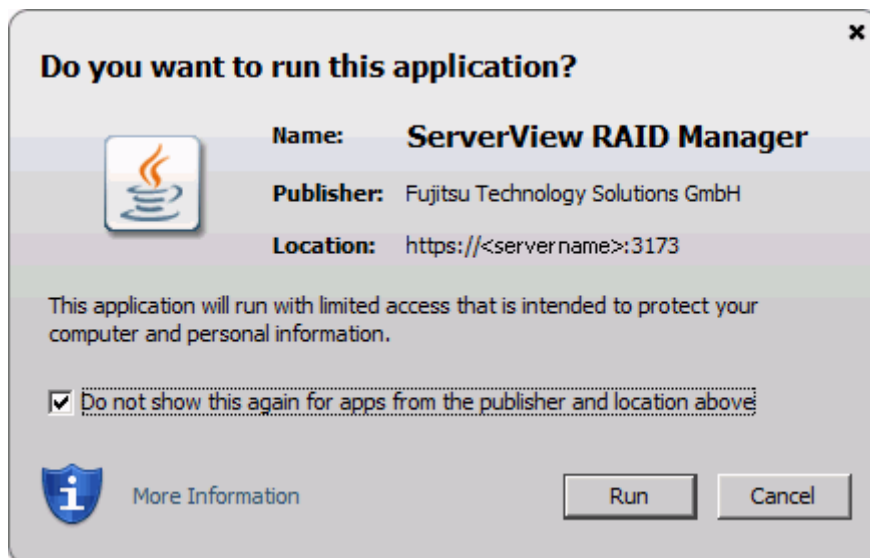
2.3 Security Certificate

If you do not install a security certificate when ServerView RAID Manager is installed, you can do so the first time you start it. Proceed as follows to do this depending on your browser and client.

1. Open your browser and enter the server name (FQDN) of the system followed by TCP port number 3173 into the address bar (e.g. `https://<FQDN>:3173`). Confirm your input using the **CR** key to get access to the desired system.

2.3.1 Internet Explorer 10

2. Open the browser *Tools > Internet Options* and select the *Trusted sites* zone on the *Security* tab. Click the *Sites* button, confirm the URL matches, and click *Add* then *Close*. Close the *Internet Options* dialog with *OK*. Afterwards refresh the current page.
3. If the browser issues the message *There is a problem with this website's security certificate*, click *Continue to this website (not recommended)*.
4. Now a *Security Warning* dialog will be displayed. Confirm that the URL matches your server name, and click *Continue*.
5. The Java Runtime Environment requests you to accept the ServerView RAID Manager applet – either once for the current session or, by enabling the *Do not show this again for apps from the publisher and location above* option beforehand, also for subsequent sessions.



Confirm by clicking on *Run*. In doing so you agree to an encrypted exchange of data and you are then shown the **login screen**.

6. In addition to the address bar of your browser, you will see *Certificate Error*. Click on this and then on *View Certificates*.
7. In the next window, *Certificate*, click on *Install Certificate*.
8. In the window then displayed, *Certificate Import Wizard*, click on *Next*.
9. The content of the *Certificate Import Wizard* window changes. Choose the *Place all certificates in the following store* setting and then click *Browse*.
10. The appearing *Select Certificate Store* window will ask you where to save the certificate. Select the *Trusted Root Certification Authorities* store and click *OK*.
11. Then you return to the *Certificate Import Wizard* window from step 9. Click on *Next*.
12. The content of the *Certificate Import Wizard* window is changed again. Click on *Finish*.
13. A *Security Warning* window is displayed. Confirm this by clicking on *Yes*.
14. In the next window of the *Certificate Import Wizard* which is displayed click on *OK*, then dismiss the *Certificate* window with *OK*.

15. After you have executed the steps described, close all instances of Internet Explorer, and restart your browser as described above under step 1.

2.3.2 Firefox 25

2. Click the *I understand the risks* link on the warning page that opens in Firefox when you come to this currently untrusted connection for the first time.
3. Click the *Add Exception* button to open the *Add Security Exception* dialog.
4. On the *Add Security Exception* window, click on *View*, then select the *Details* tab to inspect the certificate and check the issuer.
5. Click on *Export*, then on the *Save* button. After saving the certificate to a file click on *Close*.
6. Now you can close the *Add Security Exception* window by clicking on *Cancel*.
7. On the upper left hand side of the Firefox browser window click on the orange tab to open the *Options > Options* menu.
8. Go to *Advanced > Certificates* tab, then click on the *View Certificates* button to view stored certificates.
9. Click the *Servers* tab, then the *Import* button.
10. Select the certificate file saved in step 5 and click on *Open*.
11. Select the imported certificate, then click on *Edit Trust*, followed by selecting *Trust the authenticity of this certificate* radio button.
12. Click on *Edit CA Trust* to select at least the *This certificate can identify websites* option setting. Afterwards close this dialog by clicking *OK*.
13. Close the *Certificate Manager* and then the *Options* dialog by *OK*, followed by closing all browser instances.
14. Open *Java Control Panel* and select the *Enable Java content in the browser* on the *Security* tab.
15. Click the *Manage Certificates* button to get to the *Certificates* dialog.
16. Select the *Secure Site* certificate type in the top of the dialog, then click *Import* on the *User* tab.
17. Select the certificate file saved in step 5 and click on *Open* again.
18. Then click on *Close*, followed by *OK* to close all *Java Control Panel* dialogs.
19. Finally restart your browser as described above under step 1 and confirm the Java Runtime Environment requests as described above under step 5 of **Internet Explorer 10**.

2.3.3 Chrome 31

2. Click on the security *padlock icon* in the address bar of Chrome, then on the *Connection* tab. Here, you will find a *Certificate information* link. Click on it.
3. In the next window, *Certificate*, click on the *Details* tab, then on the *Copy to File* button.
4. Now the *Certificate Export Wizard* will be opened, click *Next* to get to the *Export File Format* screen.
5. Choose the *DER encoded binary X.509 (.CER)* format and click *Next*.
6. Click *Browse*, give the certificate file a descriptive name, and then *Save* it to your computer.
7. Click *Next* and *Finish* to proceed with the certificate export.
8. In the next window of the *Certificate Export Wizard* which is displayed click on *OK*, then dismiss the *Certificate* window with *OK*.
9. Open *Chrome Settings*, scroll to the bottom, and click the *Show advanced settings* link.
10. Under the *HTTPS/SSL* section, click *Manage certificates*.
11. In the following window click the *Import* button on the *Trusted Root Certification Authorities* tab.

12. In the window then displayed, *Certificate Import Wizard*, click on *Next*.
13. Click *Browse* and select the certificate file saved in the steps before, click *Open*, then click *Next*.
14. The content of the *Certificate Import Wizard* window changes and *Place all certificates in the following store* with *Trusted Root Certification Authorities* should be automatically selected, if not, follow step 9 and 10 of **Internet Explorer 10** description.
15. Then execute the steps 11-14 as described above under **Internet Explorer 10**, followed by closing all Chrome instances.
16. Finally open *Java Control Panel* and follow the steps 14-19 as described above under **Firefox 25**.



If only a red X can be seen at the top left-hand corner of the screen when ServerView RAID Manager is started, this means that installation of the security certificate took too long. In this case close the browser window and restart ServerView RAID Manager.



If you use the IP address instead of the hostname to connect to ServerView RAID Manager from a Windows Server 2003 operating system you will get a certificate alert although a valid security certificate is correctly installed. E.g. ServerView Operations Manager always uses the IP address to connect to ServerView RAID Manager. Newer operating systems do not show this behavior anymore.

2.4 System requirements

2.4.1 Hardware

At least 80 MB of disk space must be available on the server for installation purposes. Depending on the settings for ServerView RAID Manager, disk space must also be provided for the log files.

The client must be a PC that offers at least 600 MHz (Pentium III or equivalent) and 512 MB RAM.

2.4.2 Software

On some Linux distributions it may be necessary to install additional software packages, e.g. `pam`, `compat-libstdc++`, etc.

Prerequisite for RAID management of VMware ESXi is at least ESXi 3.5 Update 2. The ESXi hypervisor only supports SAS MegaRAID controllers for management. It is recommended to run a Linux or Windows based virtual machine on each ESXi system and install ServerView RAID Manager there.

A Java Runtime Environment (JRE) $\geq 1.5.0$ or higher is required for the GUI.

The operating systems for the servers involved are the Windows, Linux, and VMware versions released by Fujitsu.

In addition to the server operating systems the following operating systems are supported as clients: Windows XP SP3, Windows Vista, and Windows 7/8.

The browsers supported are Internet Explorer from version 7, Google Chrome from version 9, and Mozilla-based browsers such as Netscape or Firefox.

2.4.3 Settings

The networking of the managed server must be configured so that the IP address of its hostname can be resolved either via DNS or the hosts database.

The hostname (FQDN) of the server must be compliant with the naming conventions defined in RFC 952.



ServerView RAID Manager may only be used on the hardware and software specifically released for it. Further details can be found in the release information.

2.5 Licenses

Copyright (c) 1996 - 2013, Daniel Stenberg,

Copyright (c) 1995-2013 International Business Machines Corporation and others

Copyright (c) 1991-2013 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in <http://www.unicode.org/copyright.html>

Copyright (c) 1999 TaBE Project. Copyright (c) 1999 Pai-Hsiang Hsiao. All rights reserved.

Copyright (c) 1999 Computer Systems and Communication Lab, Institute of Information Science, Academia Sinica. All rights reserved.

Copyright 2000, 2001, 2002, 2003 Nara Institute of Science and Technology. All Rights Reserved.

Copyright (C) 2001 - 2005 - DINH Viet Hoa. All rights reserved.

Copyright (c) 1998-2010 Sendmail, Inc. All rights reserved.

RSA Data Security, Inc. MD5 Message-Digest Algorithm

Copyright (c) 2008 The NetBSD Foundation, Inc. All rights reserved.

(C) Copyright IBM Corporation 2006, 2007

(C) Copyright Eric Anholt 2006

Copyright (c) 2007, 2008, 2009, 2011, Oracle and/or its affiliates.

Copyright 2009 Red Hat, Inc. All Rights Reserved.

Copyright (c) 2008 Juan Romero Pardines

Copyright (c) 2008 Mark Kettenis

Copyright (C) 2000 The XFree86 Project, Inc. All Rights Reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>).

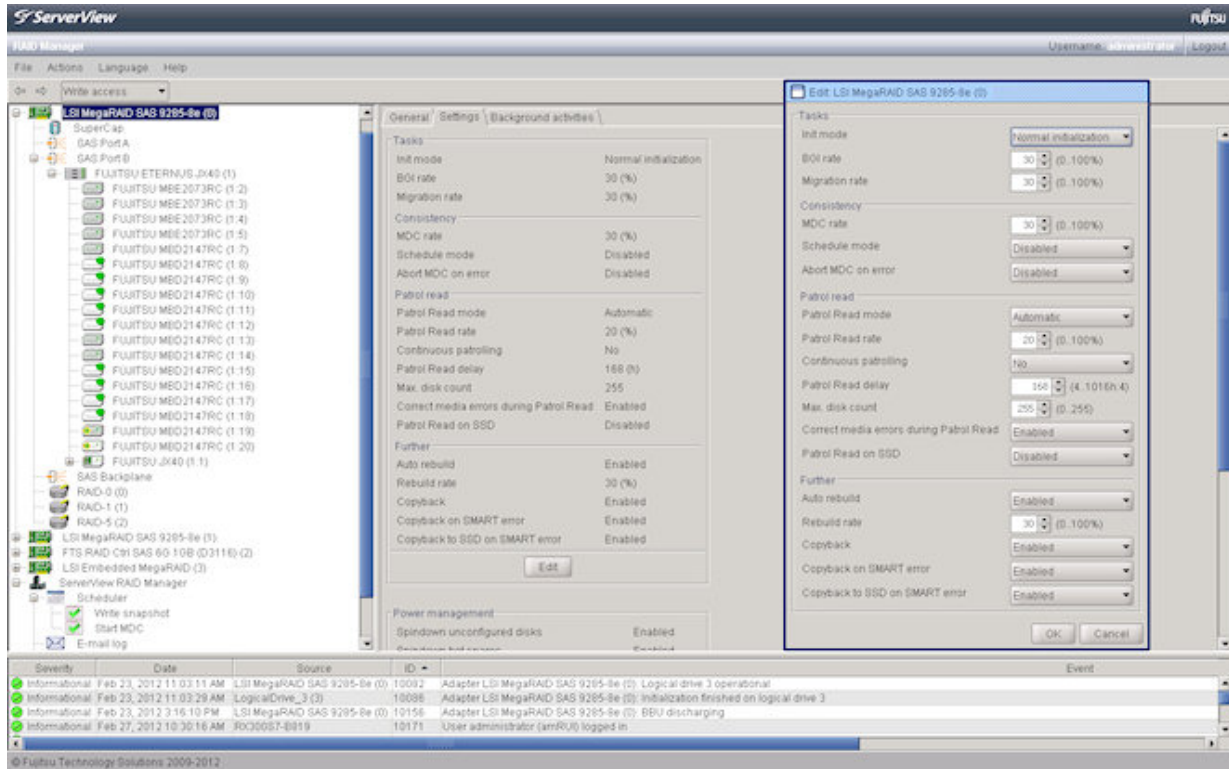
This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the University of Michigan at Ann Arbor

3 The User Interface

3.1 Elements of the User Interface

The figure below shows the ServerView RAID Manager main window with the typical controls.



Note: Depending on the operating system, browser, monitor, color scheme, and language used there may be differences between this figure and the display on your screen.

- At the top of the window you will find the **1st menu line** with the menu items:
 - File**
The menu item enables you to terminate your session and return to the **login screen** or to ServerView if you started the application there.
 - Actions**
After selection different **actions** will be offered, depending on the object selected.
 - Language**
About this menu item you can adjust another language variant.
 - Help**
By means of the last menu item you can get additional **information** about ServerView RAID Manager or you can call this **online help**.



Possible actions are displayed to you when you right-click on an object in the tree structure.

- Below the 1st menu line you will find the **2nd menu line**. You can use the two arrows to go one step forward or back. The button next to the two arrows enables you to change the write or read access to the objects.



The first user automatically has read/write authorization. Every subsequent user only has read authorization, but – provided they have appropriate administration rights – can obtain write authorization. The user who had write authorization up to this point is then informed of this.

- Beneath the two menu lines the window is divided into two halves. In the left-hand half all the objects of a system are displayed in a **tree structure**. In the right-hand half information on the objects selected in the tree structure are displayed in an **object window**.

The object window on the right contains (depending on the object selected) one or more **tabs**:

- *General*
Contains general data on an object (IP address, operating system, etc.) which you *cannot* change.
- *Settings*
Contains object settings which you can change. When you click on the *Edit* button a dialog box opens in which you can make the changes.
- *Layout*
Contains an overview with information on the structure of an object.
- *Background activities*
Contains activities that are currently running on an object such as a Patrol Read on an adapter.

- At the bottom edge of the user interface you will find an **event window**. This displays the latest events of all the RAID controllers which are managed by ServerView RAID manager. The delimiter bar enables you to enlarge or reduce this window. A double click on an event opens a **dialog**, with which it is easy to navigate through the events and to catch the whole detailed message at a glance.



An overview of the icons used in the tree structure can be found **here**.

3.2 Event Status Indicators and Icons

3.2.1 Event Status Indicators















The following status indicators in the event window of the ServerView RAID Manager main window indicate the weight of a reported event.





















 Information  Warning  Error

3.2.2 Icons













The following icons represent an object (device) in the tree structure of the ServerView RAID Manager main window. This icons can also contain various combinable flags which display the status or property of an object. An object without an additional indicator is always in the status OK.

3.2.2.1 Table of the object icons

Icon	Meaning	Icon	Meaning
	Adapter		Power supply
	BBU		Printer
	Beeper		Processor
	CacheCade		SAS port
	CD-ROM/DVD drive		SATA port
	Enclosure		Scanner
	Fan		Scheduler/Hosts

	File log		SCSI channel
	Hard disk (not used)		SSD (not used)
	Hard disk (used)		SSD (used)
	Jukebox		Switch
	Logical drive		System
	Mail log		System log
	Multiplexer		Tape
	Network device/ESXi server		Task
	Optical drive		Temperature sensor
	Plugin		WORM drive

3.2.2.2 Table of the additional indicators

Indicator	Example	Meaning
x character		Fan in "critical" status
! character		Power supply in "warning" status
Overflow		Logical drive where the bad block table has an overflow
Foreign configuration		Hard disk with foreign configuration
Energy-saving state		Hard disk in the energy-saving state
Plus character (light background)		Global hot spare
Plus character (gray background)		Dedicated hot spare
Yellow halo		Hard disk with "flashing" LED status (in order to pinpoint it)
1010 line of characters		Hard disk is rebuilding
Stopwatch		Hard disk is waiting
(Combination)		Logical drive with "warning" status is rebuilding
(Combination)		SSD with foreign configuration and in the "flashing" and "critical" statuses

4 Properties

4.1 Displaying and Modifying Properties

Depending on the entry marked in the tree structure the following is displayed in the object window under the tab

- *General* - the properties of the object in question which cannot be modified.
- *Settings* - the properties of the object in question which can be modified. Clicking on the *Edit* button opens a dialog box in which you can make changes.

To make them easier to find, the properties within the categories *System*, *Devices* and *ServerView RAID Manager* are listed in alphabetical order independently of the object.

4.1.1 System

- **Operating system**

- **Build**
Build number of the operating system.
- **Edition**
Edition of the operating system.
- **Features**
Additional features of the operating system.
- **Processor architecture**
Processor architecture
- **Product**
Product name of the operating system.
- **Service pack**
No. of the service pack.
- **Vendor**
Vendor of the operating system.
- **Version**
Version of the operating system.

- **Role based access control**

- **Allow non-secure access**
For test purposes or until a correct certificate is installed an access without encryption to the directory service can be allowed. This is not recommended for production environments.
- **Base DN**
The base DN (Distinguished Name) is the starting point in the directory hierarchy at which a search will begin, e.g. "dc=example,dc=com". The search base DN is an element of the search operation that works in conjunction with the search scope to define the subtree of entries that should be considered when processing the search operation. Only entries at or below the search base DN and within the scope will be considered candidates for matching against the search filter.
- **LDAP**
By default no RBAC is used by ServerView RAID Manager. Here you can enable RBAC via LDAP.
- **LDAP non-secure port**
If non-secure access is allowed you can modify the used port of your directory service here. The default port is 389
- **LDAP port**
Here you can modify the used (secure) port of your directory service. The default port is 636.

- **LDAP server**
Here you can insert the name or IP address of your directory server.
- **Password**
The directory service requires a password for authentication which can be supplied here.
- **Role DN**
This value is used in addition to the base DN when searching roles, e.g. "ou=svs". If no value is supplied, the subtree search will start from the base DN.
- **Username**
The directory service needs an username for authentication, e.g. "cn=Directory Manager", which can be supplied here.
- **User search base**
The node in the directory under which the users reside, for example "ou=users,dc=example,dc=com"
- **User search filter**
User search filter stores the unique search criterion for searching a specific user, e.g. "uid=%u".

• **Single Sign On**

- **CAS**
By default no SSO is used by ServerView RAID Manager and you always get a **login screen** if you call RAID Manager. Here you can enable SSO via CAS authentication.
- **CAS base URL**
URL under which all CAS services reside (default: /cas).
- **CAS port**
Here you can modify the used port of your CAS server. The default port is 3170.
- **CAS server**
Here you can insert the name or IP address of your CAS server.

• **System**

- **Admin group**
Members of this (optional) user group are granted administration rights.
- **Fully qualified domain name**
Fully qualified domain name of the system. It is an unambiguous domain name that specifies the system's position in the DNS tree hierarchy absolutely.
- **IP address**
IP address of the system.
- **Name**
Name of the system.
- **User group**
Members of this (optional) user group are allowed to view RAID configuration information.

4.1.2 Devices

• **Adapter**

- **Abort MDC on error**
Abort a consistency check on detection of the first inconsistency.
- **Activity**
Current activity of the RAID controller, e.g. *Patrol Read running*. Additionally for some activities a progress bar with percents and estimated time remaining will be displayed.
- **Additional status**
If available you can see here some additional information of the current status.

- **Alarm control**
Some RAID controllers have an audible alarm which is triggered by a wide range of conditions. Here you switch the alarm on or off.
- **Alarm present**
Displays whether the RAID controller has an audible alarm.
- **Auto flush interval**
Here you set the intervals at which the cache is to be emptied.
- **Auto inconsistency handling**
Here you select whether a check is to be started automatically. In the case of redundant systems (e.g. RAID-1, RAID-5, RAID-10) this action starts a check of the logical drive. The consistency check runs in the background, thus enabling you to continue working with the logical drive.
- **Auto rebuild**
Here you define whether a rebuild is to be started automatically when an error in the logical drive occurs. This setting generally only makes sense in conjunction with a hot spare.
- **BGI rate**
Here you set the background initialization rate.
- **BIOS build time**
Creation date of the BIOS version.
- **BIOS continue on error**
If enabled a user interaction during boot is only required for critical errors. Otherwise boot will be interrupted for every detected problem.
- **BIOS status**
If disabled logical drives cannot be used to boot from. They are not exposed via BIOS INT 13 from Option ROM.
- **BIOS version**
BIOS version of the controller.
- **Bus**
Number of the PCI bus to which the controller is connected.
- **CacheCade write cache capable**
Flag whether CacheCade can handle read and write I/O operations or read I/O operations only.
- **Chip revision**
Hardware version of the chip.
- **Chip temperature**
Chip temperature of the controller.
- **Cluster active**
Active status of the cluster.
- **Cluster enable**
Here you switch the cluster mode of the controller on or off.
- **Coercion mode**
Here you select whether the disk size can be artificially rounded up/down by the firmware to facilitate disk exchange.
- **Completed Patrol Read iterations**
Number of completed Patrol Read iterations.
- **Consistency check rate**
When a logical drive is checked this operation takes place in the background. Here you define the priority with which the consistency check is performed. The higher the priority, the greater the load placed on the system.
- **Continuous patrolling**
Here you can select that patrol read is running automatically without time interval.
- **Copyback**
Here you enable or disable copyback.

- **Copyback on SMART error**
Here you select whether the controller should attempt to start a copyback process if a SMART error is detected on the disk.
- **Copyback on SSD SMART error**
Here you select whether the controller should attempt to start a copyback process if a SMART error is detected on the SSD.
- **Copyback rate**
Here you define the priority with which the copyback is to be performed.
- **Correct media errors during Patrol Read**
Here you select whether the controller should attempt to fix any media errors found during Patrol Read.
- **Correctable errors**
Number of corrected controller errors.
- **Current CacheCade size**
Currently configured CacheCade size.
- **Device**
Device number on the PCI bus. Together with the bus number this determines the location of the controller.
- **Disk write cache**
Here you activate or deactivate the disk write cache of the controller or of all disks.
- **Driver date**
Creation date of the driver version.
- **Driver name**
Name of the controller driver.
- **Driver version**
Version of the controller driver.
- **Driver write cache**
For some controllers which have no hardware cache you can activate a software cache here which is implemented in the driver.
- **Estimated time remaining**
The estimate of time remaining to complete an activity.
- **Expose enclosure devices**
Here you select whether the firmware shows or hides attached enclosure management devices to/from the operating system.
- **Estimated lifetime**
Extrapolated lifetime of the adapter.
- **Firmware build time**
Creation date of the firmware version.
- **Firmware package version**
Firmware package version of the controller; describes firmware, BIOS, etc. as a package.
- **Firmware version**
Firmware version of the controller.
- **FlashROM size**
When a RAID controller has a FlashROM its size is shown here.
- **Function**
Some PCI modules have more than one function, e.g. 2 SCSI Cores (dual-chip as with the new dual-core processors). Together with the location via the PCI bus and PCI device the relevant function can be addressed unambiguously.
- **GB boundary**
Here you select whether or not values should be rounded down to gigabyte boundaries when logical drives are generated. This setting also allows a slightly smaller drive to be used for replacement.
- **Hardware version**
Hardware version of the controller.

- **Hot spare/auto rebuild**
Here you define whether new disks are integrated automatically and whether a rebuild is to be started automatically when an error in the logical drive occurs.
- **Hot spare support**
Here you define whether free disks are integrated automatically for erroneous and failed disks when an error in the logical drive occurs.
- **Hot swap support**
Here you define whether new disks are found automatically from the controller without a system reboot.
- **ID**
ID of the controller.
- **Inconsistency handling**
Here you define how the system is to react to controller problems.
- **Inconsistency handling interval**
Here you set the intervals at which a check is to be started automatically.
- **Init mode**
Here you select normal or quick initialization for generating the logical drives.
- **Initialization Rate**
Here you define the priority with which the initialization is to be performed.
- **Initiator ID**
Depending on the controller type the initiator ID for all of the controller's channels can be changed here. In cluster mode each device and consequently also the controller and its channel must have a unique ID.
- **Interrupt**
IRQ number assigned for this controller. In case of PCI systems this is determined dynamically.
- **Logical**
Current number of logical drives which are configured on this controller and maximum number of logical drives respectively.
- **Logical drive number for boot**
Force controller to boot from a specific logical drive. If the value is set to -1 the controller uses its default settings.
- **Manufacture date**
Date of manufacture of the adapter.
- **Max. CacheCade size**
Maximum configurable CacheCade size.
- **Max. disk count**
Number of disks on which a Patrol Read can be started at the same time.
- **MDC rate**
Here you set the priority for a consistency check, including debugging (Make Data Consistent).
- **MDC schedule continuous scheduling**
Here you see if the firmware starts a MDC immediately after finishing the previous one.
- **MDC schedule frequency**
Here you see the intervals at which the firmware starts MDC.
- **MDC schedule mode**
The mode with which the firmware handles MDC.
- **MDC schedule start time**
The start time at which the firmware starts the next MDC.
- **Memory size**
Size of the memory installed on the controller in Megabytes.
- **Memory type**
Type of the memory installed on the controller.

- **Migration rate**
Here you set the migration rate of the connected logical drives.
- **Name**
Model designation of the controller followed by an unique number. The number is sorted by the PCI location.
- **Native command queuing**
Here you see whether the controller supports native command queueing.
- **Next execution**
Time when next execution (of e.g. Patrol Read) takes place.
- **Number**
Number of channels/ports of the RAID controller.
- **NVData version**
NVRAM version of the controller.
- **NVRAM size**
If a controller has an NVRAM, its size is displayed here.
- **Offline on error**
If enabled a disk that sends too many unexpected sense codes in a specified time will be set to offline automatically.
- **Error count**
Maximum number of unexpected sense codes that may occur in a specified time.
- **Time interval**
Time interval to monitor the number of unexpected sense codes.
- **Offline on SMART error**
If enabled a disk encountering a SMART error will be set to offline automatically. If 'Copyback on SMART error' is enabled for the adapter this setting has no effect.
- **Operating system device name**
The device name of an adapter, a disk, or a logical drive in the underlying operating system.
- **Patrol Read delay**
For an automatic Patrol Read here you set the time (in hours) which must elapse between two operations.
- **Patrol Read mode**
Here you can disable a Patrol Read and select manual or automatic mode. In automatic mode the disks are always examined for errors at particular intervals. In manual mode you are offered an action for starting the operation.
In automatic mode a scheduled task for Patrol Read is ignored. If you want to start Patrol Read at an arbitrary time by a task manual mode must be set.
- **Patrol Read on SSD**
Here you specify if Patrol Read should handle SSD's or skip them.
- **Patrol Read rate**
Here you set the Patrol Read rate.
- **Physical**
Current number of devices which are connected to this controller and maximum number of devices respectively.
- **Preserved cache logical drive numbers**
List of logical drive numbers for which cache data has been preserved.
- **Product**
Product designation of the controller.
- **Protocol**
Channel/port protocol of the controller.
- **RAID-5 init**
Here you select whether or not an automatic initialization for generating RAID-5 drives. It wipes all existing data from the disks and sets up parity.

- **Rated write endurance**
Percentage of write endurance that is already used.
- **Rebuild policy**
Flag whether an automatic rebuild process may use hot spare disks only or suitable available disks additionally.
- **Rebuild rate**
Here you define the priority with which the rebuild is to be performed.
- **Remaining reserve space**
Remaining space of reserve area in percent.
- **Redundancy build rate**
Here you define the priority with which the redundancy build is performed.
- **Reserve space status**
Status of reserve area.
- **Reserve space warning threshold**
When the remaining reserve space falls below this threshold the status of the reserve space will change to Warning.
- **Segment**
PCI segments are logical collections of PCI busses. By using multiple PCI segments it is possible for a system to have more than 256 PCI busses.
- **Serial number**
Serial number of the controller.
- **Series name**
Series name of the controller.
- **Slot**
PCI slot where the controller is installed.
- **SMART poll interval**
Here you define the poll interval when SMART support is enabled.
- **SMART support**
Most disks provide the option of indicating future problems. Here you enable or disable problem message output.
- **Spindown configured disks**
Here you enable or disable the spindown of configured disks for power saving.
- **Spindown delay**
Here you define how much time must elapse before the spindown initiates.
- **Spindown delay**
Here you define how long a disk has to be idle before a spindown can occur.
- **Spindown hot spares**
Here you enable or disable the spindown of hot spares for power saving.
- **Spindown mode**
Here you switch the spindown mode of the controller on or off.
- **Spindown unconfigured disks**
Here you enable or disable the spindown of unconfigured disks for power saving.
- **Spinup delay**
Here you define how many seconds must elapse before the next cluster of drives is started up.
- **Spinup drive count**
Number of disks which are started up in parallel during a system reboot. The greater the number of disks that start simultaneously, the greater the power consumption.
- **Status**
Current status of the controller (OK, Warning, Failed).
- **Task rate**

Here you define the priority with which the background actions are performed. The higher the priority, the greater the load placed on the system.

- **Temperature**

Overall temperature of the controller.

- **Temporary offline**

Some RAID controllers can temporarily switch disks offline (and then online again) without the logical drive being affected.

- **Total data read**

Total amount of data (including meta data) read from the device during its past lifetime.

- **Total data written**

Total amount of data (including meta data) written to the device during its past lifetime.

- **UEFI driver version**

Version of driver for the UEFI preboot environment.

- **Uncorrectable errors**

Number of uncorrectable controller errors.

- **Vendor**

Name of the controller's vendor.

- **Write endurance**

Specified amount of data that can be written to the device during its lifetime.

- **Write throttling**

Various environmental factors can have an influence on handling write I/O operations. E.g. high chip temperatures may trigger the firmware to slow down processing of write I/O operations (partial). Other factors may even force the firmware to completely prevent write I/O operations.

- **BBU**

- **Additional status**

Additional information for describing the BBU status.

- **Auto learn mode**

Methods how to handle the necessity to recalibrate the BBU periodically. This can be done automatically after a defined period, manually when the firmware warns about a required recalibration, or turned off.

- **Auto learn period**

Period between required recalibrations.

- **Average time to empty**

The estimated time until the BBU will be depleted.

- **Average time to full**

If the BBU is charging, the estimated time until it is fully charged.

- **Capacitance**

Current percentage of the capacity of the capacitor.

- **Current**

Current flow at present in ampere.

- **Cycle count**

The number of times the BBU has been recharged.

- **Design capacity**

Design capacity of the BBU in ampere-hours (Ah).

- **Design voltage**

Nominal voltage designed by the manufacturer for the regular working.

- **Device name**

Device name of the BBU.

- **Intelligent BBU**

Indicator that the BBU has an integrated logic.

- **Learn delay interval**

Delay until a recalibration is started after the learn period has expired.

- **Manufacture date**

Date of manufacture of the BBU.

- **Max. error margin**

Percentage of the maximum error count. When this value reaches 100% the BBU will get failed status.

- **Module version**

Version number of the logic module.

- **Name**

Name of the BBU.

- **Next learn time**

Time until the next recalibration will be required.

- **Recalibration active**

The BBU is completely discharged and then recharged.

- **Recalibration needed**

It was recognized that the BBU performance no longer complies with the specifications. Recalibration is to be used to try to make the BBU "fit" again.

- **Relative state of charge**

Percentage of the BBU's current state of charge.

- **Remaining capacity**

BBU's current remaining capacity.

- **Serial number**

Serial number of the BBU.

- **Status**

Current status of the BBU. If the status is no longer normal this means that a bad BBU can no longer retain the power it has been charged with and loses voltage too quickly. The BBU should be replaced as soon as possible.

- **Temperature**

Current temperature of the BBU. If this rises significantly above the normal value during charging this indicates a faulty BBU.

- **Type**

Type designation of the BBU.

- **Vendor**

Vendor of the BBU.

- **Version**

Version number of the BBU.

- **Voltage**

Current voltage of the BBU. If the BBU is just being charged, higher values may be displayed by the charger.

- **Channel/Port**

- **Max. devices**

Maximum number of devices that can be connected to the channel/port.

- **Name**

Designation of the SCSI channel or port.

- **SAS address**

For SAS ports the unique address worldwide like FibreChannel.

- **Status**
Here you can enable or disable, i.e. deactivate, the channel.
- **Termination**
Termination of the SCSI channel.
- **Transfer speed**
Maximum transfer rate which this channel/port theoretically supports.
- **Transfer width**
Transfer width of the SCSI channel or port.

• Disk

- **Activity**
Current activity of the disk, e.g. *consistency check running*. Additionally for some activities a progress bar will be displayed.
- **Block size**
Smallest amount of memory a device will read or write.
- **Completed Patrol Read iterations**
Number of completed Patrol Read iterations.
- **Configurability**
Here you see whether the disk can be used for RAID configuration or not.
- **Config. size**
Capacity which the disk provides for a configuration independent of the current usage.
- **Copyback partner device number**
Copyback always involves two disks in the process. This is the device number of the other disk.
- **Copyback partner name**
Copyback always involves two disks in the process. This is the name of the other disk.
- **Current Patrol Read iteration progress**
Here you see the current progress of Patrol Read iteration.
- **Device number**
Unique drive number on the port.
- **Estimated time remaining**
The estimate of time remaining to complete an activity.
- **Firmware version**
Firmware version of the drive.
- **Foreign configuration**
Display whether a foreign configuration is on the disk. A foreign configuration can be imported or deleted by the controller action "**Manage foreign configuration..**".
- **Format in percent**
Amount of memory – in percent of the total amount – a device provides to the end user.
- **Formatted size**
Size of memory a device provides to the end user.
- **Guarded logical drives**
List of IDs of the logical drives which are guarded by this disk (in its role as hot spare).
- **Hardware errors**
Number of faulty blocks on the disk.
- **Last shield diagnostics**
Time of last completed shield diagnostics operation.
- **Media errors**
Number of faulty blocks on the disk.

- **Media type**
Type of storage media, e.g. HDD (Hard Disk Drive) or SSD (Solid State Disk).
- **Misc errors**
Number of other errors.
- **Name**
Designation of the drive.
- **Native command queuing**
Here you enable or disable native command queuing for the disk.
- **Operating system device name**
Device name of the (logical) disk, set by operating system.
- **Physical size**
Real capacity of the disk.
- **Power status**
Power condition of the device that shows whether the device is active or stopped (spindown).
- **Product**
Product designation of the drive.
- **Rotational speed**
Rotational speed of the disk.
- **SAS address**
Unique device address worldwide.
- **Serial number**
Unique serial number of the drive.
- **Shield counter**
How often the disk fell into shield state and did not fail in the 60 day probationary period.
- **Slot**
Location of the disk in the cabinet.
- **SMART errors**
Number of errors detected by the SMART function.
- **SMART flagged**
SMART problem detected.
- **Status**
Current status of the disk (Available, Operational, Global Hot-Spare, Dedicated Hot-Spare, Failed).
- **Target ID**
Unique drive number on the channel. With SCSI devices this is also the SCSI ID.
- **Temperature**
Temperature of the disk.
- **Transfer speed**
Data transfer speed. This can deviate from the theoretical values for the drive or the options for the controller since, for example in the case of SCSI devices, the transfer rate between the controller and all devices is negotiated.
- **Transfer width**
Data width; depends, among other things, on the bus type and drive.
- **Type**
Disk type.
- **Usage**
The usage by logical drives. Display the respective name, RAID level, and additionally capacity by tooltip.
- **Vendor**
Name of the vendor.

- **Write cache**
Here you activate or deactivate the disk write cache.

- **Enclosure**

- **Enclosure number**
Unique connection number of device in this place the enclosure on the RAID controller.
- **Hardware version**
Hardware version of the enclosure.
- **Logical ID**
The enclosure logical ID uniquely identifies the enclosure.
- **Name**
Model designation of the enclosure.
- **Product**
Product designation of the enclosure.
- **Serial number**
Serial number of the enclosure.
- **Status**
Current status of the enclosure.
- **Vendor**
Name of the vendor.

- **Fan, Power supply, Temperature sensor**

- **Additional status**
Additional information for describing the status of power supply or temperature sensor.
- **Critical temperature (high)**
The critical upper limit; the enclosure should not operate above this limit.
- **Critical temperature (low)**
The critical lower limit; the enclosure should not operate below this limit.
- **Fan speed**
Current speed of fan (low/medium/high).
- **Hardware version**
Hardware version of the power supply.
- **Location**
The position of of fan or temperature sensor.
- **Name**
Model designation of fan, power supply, or temperature sensor.
- **Part number**
Part number of the power supply.
- **Product**
Product designation of the power supply.
- **Serial number**
Serial number of the power supply.
- **Status**
Current status of fan, power supply, or temperature sensor.
- **Temperature**
Temperature display.

- **Warning temperature (high)**
Upper early warning threshold; a higher temperature indicates a thermal problem in the enclosure.
- **Warning temperature (low)**
Lower early warning threshold; a lower temperature indicates a thermal problem in the enclosure.

- **Logical drive**

- **Emulate 512e**
If enabled, the emulation of 512 byte block size can be turned off to directly expose 4 KB logical and physical block size.
- **Access mode**
Here you set the access mode which can be used to access the logical drive.
- **Activity**
Current activity of the logical drive, e.g. *consistency check running*. Additionally for some activities a progress bar will be displayed.
- **Additional status**
If available you can see here some additional information of the current status.
- **BGI**
Here you enable or disable the background initialization rate.
- **Cache mode**
Here you select whether read and write operations are forwarded directly or buffered in the cache.
- **CacheCade number**
Number of the CacheCade.
- **CacheCade type**
Flag whether the current CacheCade is configured to handle read and write I/O operations or read I/O operations only.
- **Default access mode**
Describes how and if the operating system can access the logical drive.
- **Default cache mode**
Here you select the default value for cache mode.
- **Default read mode**
Here you select the default value for read mode.
- **Default write mode**
Here you select the default value for write mode.
- **Disk cache mode**
Status of the disk cache mode.
- **Estimated time remaining**
The estimated remaining time to complete an activity.
- **Initialization status**
Initialization status of the logical drive.
- **Logical drive number**
Number of the logical drive.
- **Logical size**
Net capacity of the logical drive. In contrast to the drive vendors the size shown here is actually available to the operating system.
- **Name**
Name assigned when the logical drive was created.
- **Number of missing drives**
Number of missing disks in the logical drive.
- **Operating system device name**
Device name of the logical drive, set by operating system.

- **Physical size**
Sum total of the storage space used on the disk.
- **RAID level**
RAID level of the logical drive.
- **Read mode**
Here you define the read mode. The following settings are available:

Read-ahead	Advance read access to the memory takes place.
No read-ahead	No advance read access to the memory takes place.
Adaptive	When most of the last read accesses to successive sectors have taken place the controller switches to <i>Read-ahead</i> . When the read accesses have been distributed it switches back to <i>No read-ahead</i> .
- **SSD caching**
Flag whether a logical drive can make use of a second level cache (CacheCade).
- **Status**
Current status of the logical drive (Operational, Degraded, Failed).
- **Stripe size**
In the case of logical drives with striping (RAID types 0, 5, 10 and 50) the data is distributed to the associated disks in equally sized sections. The amount of data in each section is the stripe size.
- **Type**
RAID type of the logical drive.
- **Used capacity**
Used capacity of the respective disk in percent.
- **Write mode**
Here you define the write mode. The following settings are available:

Write-back	The controller sends a signal to the server when the data has been written to the controller's cache.
Write-through	The controller sends a signal to the server only when the data has been written to the disk.
Adaptive	When this setting is chosen and a charged BBU is connected the same procedure is followed as described under <i>Write-back</i> , otherwise the controller behaves as for <i>Write-through</i> .
Adaptive Write-back	This display appears when <i>Adaptive</i> is selected and the controller currently handles the write requests as described under <i>Write-back</i> . After a BBU failure the controller automatically switches to <i>Write-through</i> .
Adaptive Write-through	This display appears when <i>Adaptive</i> is selected and the controller currently handles the write requests as described under <i>Write-through</i> . When a charged BBU is available again the controller automatically switches back to <i>Write-back</i> .
Always Write-back	The controller always sends a signal to the server when the data has been written to the controller's cache even though the BBU is not present or currently not functional.

• **Processor (Expander)**

- **Device number/Target ID**
Unique device number/ID of the processor (expander) on the port/channel.
- **Enclosure number**
Number of enclosure whereof the processor (expander) is connected.
- **Firmware version**
Firmware version of the processor (expander).
- **Hardware version**
Hardware version of the processor (expander).

- **Name**
Model designation of the processor (expander).
- **Part number**
Part number of the processor (expander).
- **Port number/Channel number**
Unique connection number of the port/channel on the RAID controller.
- **Product**
Product designation of the processor (expander).
- **SAS address**
Unique device address worldwide.
- **Serial number**
Serial number of the processor (expander).
- **Status**
Current status of the processor (expander).
- **Type**
Type designation of the processor (expander).
- **Vendor**
Name of the vendor.

4.1.3 ServerView RAID Manager

• E-mail log

- **Logging**
By default no e-mail events were sent from ServerView RAID Manager. Here you can enable the sending.
- **Log level**
E-mail events are weighted differently. This option enables you to set a threshold from which the events are sent.
- **Password**
If the outgoing e-mail server requires authentication a password can be supplied here.
- **Recipient E-mail address**
Here you can insert the recipient(s) of the e-mails. Multiple e-mail addresses have to be separated by ';' or ','. A maximum of 1024 characters can be used.
- **Sender E-mail address**
Here you can insert a name that appears in the From: header field of the e-mail. Some outgoing e-mail servers require a valid e-mail address as sender.
- **Sender description**
Here you can insert a free form text that appears in the e-mail header.
- **SMTP port**
Here you can modify the used port of your outgoing e-mail server. The default port is 25. SMTP via SSL/TLS (SMTPS) is only possible via port 465.
- **SMTP server**
Here you can insert the name of your outgoing e-mail server.
- **Username**
If the outgoing e-mail server requires authentication a username or an e-mail account can be supplied here.

• File log

- **File name**
Here you can modify the name of the save file for file events which is used by ServerView RAID Manager.

- **File size**
You can modify the size of the save file for file events in steps of one Mbyte. Ten Mbytes is preset.
- **Logging**
By default file events are written to a ServerView RAID Manager log file. You can disable this logging here.
- **Log level**
Text file events are weighted differently. This option enables you to set a threshold from which the events are logged.
- **Log method**
By default a full save file for file events is assigned a new name and saved so that logging can continue in an empty file (Rotation method). If you wish you can also choose the Round Robin method. In this case the oldest entries in the full file are overwritten.
- **Max. save files**
Here you can restrict the maximum number of save files for file events that are retained when the Rotation method is used. If the upper limit is exceeded the oldest file is deleted.
- **Text format (additionally)**
Here you select whether events are additionally written to a text file without XML format directives.

• Plugin

- **Managed servers**
In this table you can see all servers managed by ServerView RAID Manager CIM (Common Information Model) plugins with their hostname, IP address, and operating system.
- **Name**
Name of the plugin.
- **Poll interval**
Here you can define the intervals at which the plugin queries the controller for changes (default: 2 seconds).
- **Vendor**
Name of the vendor.
- **Show BBU events**
If disabled the status of BBU's is always shown as Normal. Events for BBU's are suppressed.
- **Show tape events**
If disabled events for tapes are suppressed.
- **Version**
Version of the plugin or API.

• Scheduler, Task

- **Configurability**
Here you see whether the task can be modified or deleted.
- **Name**
Name of task which will be deduced automatically from the related action.
- **Next execution**
Time of the next task execution.
- **Object**
Path and name of the object on which the action will be executed.
- **Status**
Status of task. Between 1 and 4 execution failures Warning will be set. After more than 4 failures the task will be stopped by default and the status will be set to Error. With the action "**Reset error counters**" the error counter will be reset and the status will be cleared.

- **ServerView RAID Manager**

- **Backup file**

- Here you can modify the name of the ServerView RAID Manager backup file. You can save the current RAID configuration using ServerView RAID Manager action "**Write configuration**".

- **Poll interval**

- Here you can define the intervals at which ServerView RAID Manager asynchronously updates the various logs (default: 2 seconds).

- **Status**

- Functional status of ServerView RAID Manager. The following values are possible: Operational, Initializing, Failed, and Terminating.

- **Sense log delay**

- If an Unexpected sense event was logged a recurring identical event is support for this amount of time.

- **Status adapters**

- Consolidated status of all monitored controllers. For sake of simplicity only the following values are displayed: Ok, Warning, and Failed.

- **Status disks**

- Consolidated status of all monitored disks. For sake of simplicity only the following values are displayed: Ok, Warning, and Failed.

- **Status logical drives**

- Consolidated status of all monitored logical drives. For sake of simplicity only the following values are displayed: Ok, Warning, and Failed.

- **Status overall**

- Consolidated status of all monitored objects. For sake of simplicity only the following values are displayed: Ok, Warning, and Failed.

- **Version**

- Version of ServerView RAID Manager.

- **System log**

- **Logging**

- By default system events are written to a system file. You can disable this logging here. Depending on the operating system used you can have the event log displayed and manage it with the corresponding functions. Further information on this is provided in the help system for the operating system.

- **Log destination**

- Display where the system log information is written to.

- **Log level**

- System events are weighted differently. With this option you set a threshold from which the events are logged.

5 Actions and Dialogs

5.1 Executing Actions

Depending on the controller, disk or logical drive selected different actions can be executed via menu item *Actions*. The hardware type is also decisive for the functionality offered. For example, "Patrol Read" is not supported by all controllers and is consequently not always offered.

The actions which you can execute with the RAID Manager for particular objects are arranged alphabetically to permit easy reference. The associated description tells you which object (system, controller, disk, logical drive, etc.) they can be used for.



Please note that some actions are not possible with all controller types.

- **Add server...**

This command calls a dialog to add an existing ESXi server (host) to the ServerView RAID Manager configuration. Thus, the RAID controller of the hypervisor can be monitored and configured. For more information see **VMware ESXi**.

- **Alarm off**

The controller's alarm test is terminated and the alarm signal is deactivated.

- **Alarm on**

An alarm signal is activated for checking the controller.

- **Attach device**

Grant operating system access to a SSD device.

- **Cancel BGI**

Cancels initialization which was automatically started by a controller at low priority in the background.

- **Cancel consistency check**

The consistency check is aborted.

- **Cancel copyback**

The copyback is aborted.

- **Cancel initialization**

Initialization of the logical drive is aborted.

- **Cancel MDC**

The MDC (Make Data Consistent) is aborted.

- **Cancel Patrol Read**

The Patrol Read process is aborted.

- **Cancel rebuild**

The Rebuild process is aborted.

- **Cancel verification**

Aborts checking of the disk.

- **Clear bad block log**

The log of defective blocks is deleted.

- **Clear configuration**

The entire configuration (all logical drives, hot spares, etc.) is deleted.

Warning: Please pay attention of the confirmation. If you confirm it is also deleted if you are currently working on it.

- **Clear foreign configuration**

This action deletes the foreign configuration of all disks which the firmware has recognized as belonging together.

- **Clear log**

The save file(s) for file events from ServerView RAID is deleted.

- **Clear NVRAM log**

The log from the controller's NVRAM is deleted.

- **Create dedicated hot spare**
Creates a hot spare. When another disk fails the hot spare is automatically integrated into ongoing operations in place of the defective disk. This permits the data of the defective disk to be restored. A dedicated hot spare protects only a *selection* of redundant logical drives.
- **Create global hot spare**
Creates a hot spare. When another disk fails the hot spare is automatically integrated into ongoing operations in place of the defective disk. This permits the data of the defective disk to be restored. In contrast to a dedicated hot spare a global hot spare protects *all* redundant logical drives.
- **Create logical drive...**
This action calls a **dialog to create** a logical drive. Parts of one or more disks are combined to form a logical ("virtual") drive.
- **Create RAID volume**
Two logical drives of the same type (RAID level) are combined to form a logical drive.
- **Delete all logical drives**
All existing logical drives are deleted.
- **Delete dedicated hot spare**
Deletes a dedicated hot spare.
- **Delete global hot spare**
Deletes a global hot spare.
- **Delete last logical drive**
The logical drive created last (i.e. the logical drive with the highest index number) is deleted. It is recommended to back up data on all of the logical drives before deleting them.
Warning: It is also deleted if you are currently working on it.
- **Delete logical drive**
A logical drive is deleted. **Note:** Due to limitations in firmware this action is **not** offered for all MegaRAID and Integrated Mirroring RAID controllers. With these you can only delete either all logical drives at once or just the last one.
- **Detach device**
Revoke operating system access to a SSD device.
- **Disable SSD caching**
Cancel association between logical drive and SSD cache.
- **Discard preserved cache**
If the controller loses access to one or more logical drives, the controller preserves the data from the logical drive. This preserved cache, is preserved until you import the logical drive or discard the cache. Certain actions, such as creating a new logical drive, cannot be performed if preserved cache exists. **Note:** If there are any foreign configurations, import the foreign configuration before you discard the preserved cache. Otherwise, you might lose data that belongs to the foreign configuration.
- **Discharge**
Discharges the battery for the emergency power supply (Battery Backup Unit – BBU).
- **Display bad block log**
The defective drive device blocks which the controller found when checking the devices are displayed.
- **Enable SSD caching**
Allow firmware to use an existing SSD cache as additional caching layer for a logical drive.
- **Fast charge**
The battery for the emergency power supply (Battery Backup Unit – BBU) is charged rapidly.
- **Flush memory**
The data from the controller's cache (internal memory) is written to the disks. The cache is then empty.
- **Force detach device**
Revoke operating system access to a SSD device, even if the device is currently in use.
- **Force write access**
Forces write access when another user either does not want to or cannot transfer it.
Caution: This action should only be performed after you have thoroughly weighed up the pros and cons.

- **Format device**
A disk drive is formatted.
Warning: All data previously stored on the drive is lost. If the disk drive is used in a logical drive the data integrity of the logical drive is also impaired.
- **Get write access**
Takes over write access from another user.
- **Help**
This action calls the help about actions.
- **Import foreign configuration**
This action is used to import the foreign configuration of all disks which the firmware has recognized as belonging together. After this action has been executed, the logical drives which were built with these disks are available for further processing.
- **Locate**
An enclosure is located. An LED on the enclosure flashes either briefly or until location is aborted. In the case of some controllers the LED is set to remain constantly bright.
- **Locate**
A disk is located. An LED on the disk drive flashes either briefly or until drive location is aborted. In the case of some controllers the LED is set to remain constantly bright.
- **Locate**
A logical drive is located.
- **Logout**
This action is only offered for the system object and terminate your session. You return to the **login screen** or to ServerView if you started the application there.
- **Make offline**
A disk is switched "offline". The status of the affected logical drive changes to "degraded" or "partially degraded".
- **Make offline (redundancy)**
After creating a backup of the disk on a hot spare it is switched "offline". Then the disk is removed from the configuration and replaced by the previously created backup.
- **Make online**
A drive is placed back in service.
- **Make ready**
A disk which was switched "offline" and is no longer part of a logical drive can no longer be switched "online" but only be made available. Only then can it be included in the configuration again using the **Make Online** action.
- **Make ready (clear bad block table)**
A disk will be made available and simultaneously a bad block table will be cleared.
- **Manage foreign configuration...**
This action calls a **dialog to import or clear** foreign configurations.
- **Manage host...**
This action calls a dialog to change connection information or delete an ESXi host from the ServerView RAID Manager configuration. For more information see **VMware ESXi**.
- **Manage hot spare...**
This action calls a **dialog to create or delete** a hot spare.
- **Manage MegaRAID Advanced Software Options...**
This action opens a dialog which allows you to enter one or more keys to activate the corresponding software options. Software options which are already activated will be displayed. Installed test keys can be removed by using this action. For more information see **RAID Controller Functions**.
- **Manage task...**
This action calls a **dialog to create, modify or delete** a task.
- **Mark as missing**
Remove a specific disk from a logical drive.
- **Migrate logical drive...**

This action calls a **dialog to modify** a logical drive. A logical drive is transferred directly from one RAID type to another.

- **Recalibration**

The battery for the emergency power supply (Battery Backup Unit – BBU) is recalibrated. This action returns the battery to its ideal condition.

- **Release write access**

Releases write access for another user who urgently needs it.

- **Replace missing disk...**

With this action a free disk takes over the tasks of a failed disk.

If a disk in a logical drive fails in the new LSI, SAS/SATA solutions and if this is replaced by a new disk, the latter does not automatically take the place of the disk that has been replaced but must be activated manually. If the logical drive should continue to offer restricted functionality after this action has been completed successfully, the **rebuild** must be started manually.

- **Reset error counters**

This action automatically deletes the error event log for the disk drive and the error counter is set to zero. Also this action can reset the error counter and clear the **status** of Tasks.

- **Resume BGI**

The background Initialization process is resumed at the point where it was previously stopped.

- **Resume consistency check**

The consistency check is resumed at the place where it was previously stopped.

- **Resume copyback**

The copyback is resumed at the position where it was previously stopped.

- **Resume initialization**

The interrupted initialization of the logical drive is resumed.

- **Resume MDC**

The MDC (Make Data Consistent) is resumed at the point where it was previously stopped.

- **Resume migration**

Migration of a logical drive is resumed (see **Migrate logical drive**).

- **Resume Patrol Read**

The Patrol Read process is resumed at the point where it was previously stopped.

- **Resume rebuild**

The Rebuild process is resumed at the point where it was previously stopped.

- **Scan configuration**

All the information collected internally is deleted and then all the data is read in anew from controllers.

- **Send SNMP test event**

If SNMP is enabled and configured you can send a test trap with this action. Neither RAID Manager nor any other SNMP tool can verify that the trap reaches the destination correctly. You have to check yourself whether the trap reaches the destination properly.

- **Send test E-mail**

If you have enabled and configured the **E-mail log** you can send a test E-mail with this action.

- **Show NVRAM log**

The internal log from the controller's NVRAM (non-volatile memory) is displayed. This information is generally required by engineers for maintenance purposes.

- **Show PHY errors**

The SAS phy errors recorded are displayed. This information is generally required by engineers for maintenance purposes.

- **Show sense log**

A table with the last *n* SCSI items of sense information which occurred are displayed. SCSI sense information is generally present when a SCSI command has failed and the controller or the disk can supply additional information on why this happened.

- **Start consistency check**

In the case of redundant systems (e.g. RAID-1, RAID-5, RAID-10) this action starts a check of the logical drive. The consistency check runs in the background, thus enabling you to continue working with the logical drive. Depending on how the synchronization procedure has been set on the controller any error that is found is skipped or rectified if possible, or the consistency check is stopped and an error message is displayed.

Note: With some controllers the priority of this process can be changed via the *Settings* tab. The following rule applies here: The lower the priority, the longer the process, but this enables you to work better.

- **Start copyback...**

This action calls a dialog to select a disk to copy data from a logical drive to a new destination disk. For more information see **RAID Controller Functions**.

- **Start device**

A disk drive is started, i.e. the disk drive is brought up to its standard speed. With some high-speed disks this can take some time. As power consumption is higher when the disks start up not all of them should be started up at once.

- **Start initialization**

A logical drive is initialized. Before you write the first user data to a logical drive you should initialize this drive.

Note: Some controllers automatically perform initialization when the logical drive is created. This action is not offered for these drives.

Warning: Initialization destroys all user data on the logical drive.

- **Start MDC**

A consistency check takes place and, if it is possible to rectify any inconsistency which is found, this is done automatically (Make Data Consistent).

- **Start OCE**

If there is free storage space on all disks of an array this can be used to increase the capacity of the logical drive (Online Capacity Expansion). Afterwards existing filesystems can be adapted to the new capacity with operating system tools.

- **Start Patrol Read**

A Patrol Read process is started on a disk drive. In this case restricted access is still possible to the drive. Patrol Read examines the drive's interface for errors. If an error is detected which cannot be rectified automatically, this error is logged. The faulty part of the medium is assigned to the defective blocks. With some controllers the disk is automatically taken out of service if multiple errors are found.

This error check is not supported by every controller, but some controllers provide the option of performing a check automatically at freely selectable intervals.

- **Start rebuild**

In the case of critical logical drives of the type RAID-1, RAID-5 or RAID-10 this action starts rebuilding the logical drive. Generally the failed disk is automatically replaced by a hot spare and a rebuild is subsequently started automatically provided this is set on the controller. The action runs in the background, and as long as no further disk fails it is still possible to work with the logical drive.

Note: With some controllers the priority of this process can be changed via the *Settings* tab. The following rule applies here: The lower the priority, the longer the process, but this enables you to work better.

- **Start verification**

Starts a disk check.

- **Stop charge**

Terminates the battery charging process for the emergency power supply (Battery Backup Unit – BBU).

- **Stop device**

A disk drive is stopped. This action can sometimes make sense before a device is replaced.

- **Stop location**

Drive location is stopped and the LED is switched off.

- **Suspend BGI**

The background initialization process is stopped.

- **Suspend consistency check**

The consistency check is stopped. This can, for example, be necessary when more throughput capacity needs to be provided at short notice for the logical drives connected to the controller.

- **Suspend copyback**

The copyback is paused.

- **Suspend initialization**

Initialization of the logical drive is interrupted.

- **Suspend MDC**

The MDC (Make Data Consistent) is paused.

- **Suspend migration**

Migration of a logical drive is stopped (see **Migrate logical drive**).

- **Suspend Patrol Read**

The Patrol Read process is stopped. This can, for example, be necessary when more throughput capacity needs to be provided at short notice.

- **Suspend rebuild**

The Rebuild process is stopped. This can, for example, be necessary when more throughput capacity needs to be provided at short notice for the logical drives connected to the controller.

- **Set low power threshold**

Set a voltage threshold where firmware will issue warnings that the power is too low.

- **Test CAS connection**

If you have enabled and configured Single Sign On (SSO) via **CAS** you can check the connection to the CAS server with this action.

- **Test LDAP connection**

If you have enabled and configured role based access control (RBAC) via **LDAP** you can check the connection to the directory server with this action.

- **Unblock**

If an SSD cache drive (**CacheCade**) fails all associated logical drives are set to blocked (i.e. no access from operating system). The Unblock action reenables access from the operating system.

- **Write configuration**

Save the current RAID configuration into a **XML file** on the server.

- **Write NVRAM log**

Save the current internal controller log into a file on the server.

- **Write snapshot**

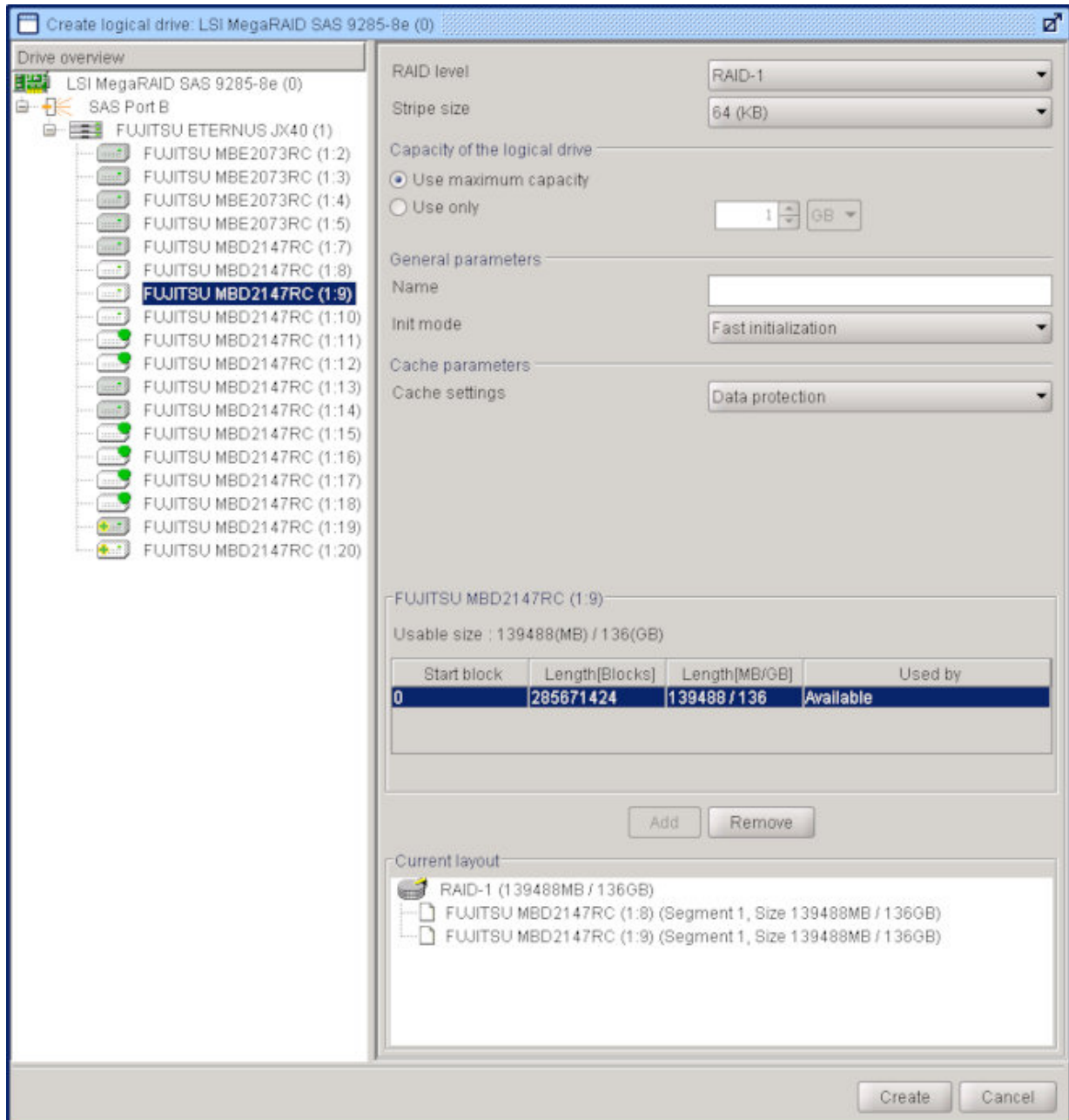
This automatic action produces - contrary to the manual action **Write configuration** - at least every 10 minutes a snapshot of the current RAID configuration.

5.2 Creating Logical Drives

Before you create a logical drive with ServerView RAID Manager, ensure that you are familiar with the **Supported RAID Types** and also know precisely which RAID level is most suitable for your application.

5.2.1 Create logical drive

Select a controller in the tree structure and start the *Create logical drive* action (via the pulldown menu of the *Actions* button or with a right mouse click). A dialog box is opened as in the example below for an LSI controller.



Depending on the controller type and RAID level you can change information and properties in the dialog box to create the logical drive.

- In the *RAID level* input field enter the RAID level you wish to create. The default for this field is "RAID-0".
- If a new logical drive requires a stripe size, this is displayed in the field of the same name. You can accept the default (64 kilobyte) or select a different size.

- Under *Capacity of the logical drive* you have two options for determining the size of the logical drive:
 1. *Use maximum capacity* (default)
The logical drive is created with maximum capacity.
 2. *Use only*
If you want to use a different value from the default, enable this button and enter the desired size in the two adjacent fields.
- Under *General parameters* you have further adjustable parameters:
 - In the *Name* input field you can accept the default name for the new logical drive or specify a new name. This name must be unique on the controller and may be up to 15 characters long (standard ASCII).
 - With *Init mode* you can select whether *no initialization* shall be executed automatically after creation of the logical drive or the initialization is executed *fast* or *normal*.
- With *Cache parameters* you have the possibility to modify the cache behavior of the logical drive:

The screenshot shows a dialog box titled "Cache parameters". It contains five settings, each with a label on the left and a dropdown menu on the right:

- Cache settings:** Advanced
- Read mode:** No read-ahead
- Write mode:** Write-through
- Cache mode:** Direct
- Disk cache mode:** Disabled

For ease of use you can carry out an optimization on *Data protection* (default) or on *Performance* under *Cache settings*.

If you choose the option *Advanced* instead you can modify all cache parameters separately. Further information to the various parameters can be found under **Displaying and Modifying Properties**.

On the left the dialog box contains a tree structure in which you select a hard disk and then make it available using the *Add* button. The hard disk that has been added is displayed under *Current layout*.

Logical drives generally (depending on the controller type and RAID level) consist of more than just one hard disk. You must therefore select and add a suitable number of hard disks. In our example (LSI controller and RAID-1) two hard disks are required. Then you can create the logical drive using the *Create* button. After you have pressed the *Create* button you must confirm creation of the logical drive again.

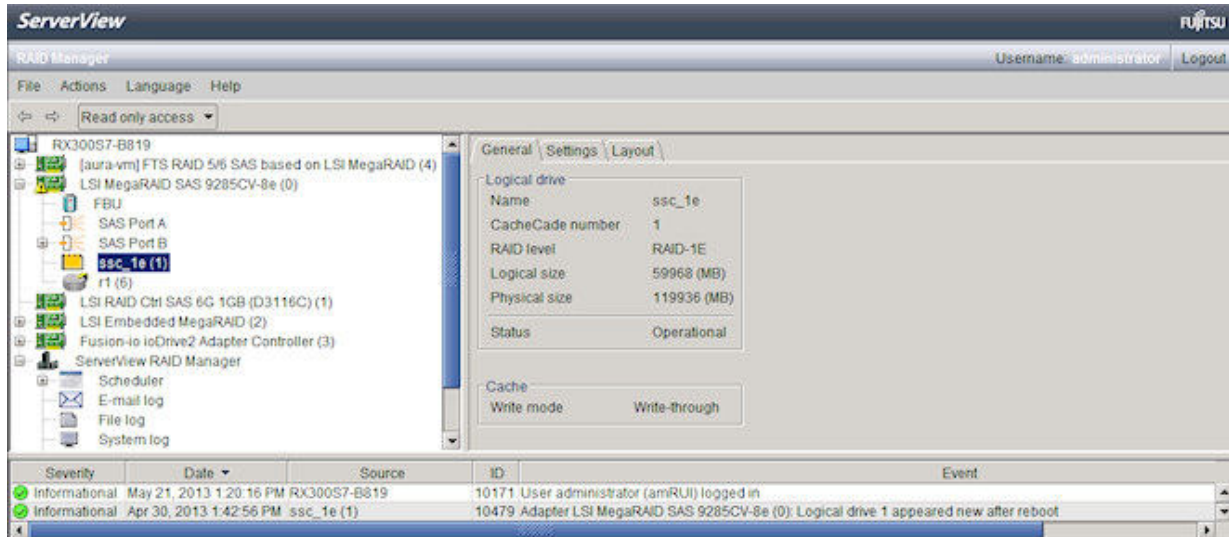
If you quit the dialog box via *Cancel*, no new logical drive is created.

5.2.2 Creating MegaRAID CacheCade Drives

This procedure does not create a user accessible logical drive but a drive that functions as a secondary tier of cache.

On controllers that support MegaRAID CacheCade and have the appropriate license installed select in the *Create logical drive* dialog a *RAID level* with (CacheCade) appendix. Then proceed as with creating a logical drive with SSD's.

After successful completion of the *Create logical drive* dialog a new object will appear in the tree structure as in the example below:




To grant access to the secondary tier of cache the action *Enable SSD caching* has to be executed on a logical drive.

5.3 Modifying Logical Drives (migrating)

The *Migrate Logical Drive* action enables you to

- migrate the RAID type to a different type
- expand the capacity of the logical drive

Note: Most operating systems of today support Online Capacity Expansion (OCE). OCE means that the additional capacity after a logical drive has been expanded can be used without rebooting the system. Details on the additional storage capacity are provided in the documentation for your operating system.

To make a modification select a logical drive () in the tree structure and start the *Migrate logical drive* action (via the pulldown menu of the *Actions* button or with a right mouse click). A dialog box is opened which contains *Parameters* and *Layout*.

1. Select the new RAID type in the pulldown menu. The migration options here depend on the RAID controller used.
2. Under *Layout* you can – if you are offered the option – expand the capacity by selecting hard disks in the tree structure and adding them to the logical drive using the *Add* button. You activate your modifications using the *Apply* button.

After you have pressed the *Apply* button you must confirm the modifications again. If you quit one of the dialog boxes using *Cancel* no changes are made.

The following rules apply for modifying a logical drive:

- Select the new RAID type for a migration. If the required type is not supported directly by the controller, you can then only delete the logical drive and create a new one.
- The capacity of the new logical drive must be at least the same as that of the current drive. If the capacity or the RAID type of the new logical drive requires a greater overall drive capacity than the current one, the additional capacity must be provided by the physical drives which are not yet used in this logical drive. In this case please select one or more physical drives which have sufficient free capacity.

Note: The name of a logical drive can – depending on the controller – be modified in the properties (*Settings* tab) of the logical drive.

5.4 Processing Hot Spares


Hot spares are used to protect redundant logical drives. If a disk in a redundant logical drive backed up by a hot spare fails, the hot spare automatically replaces the failed disk.

On some controllers a hot spare can be assigned in order to back up an individual logical drive or all logical drives on the controller. With other controllers it is automatically possible to use any free disk which is large enough as a backup.

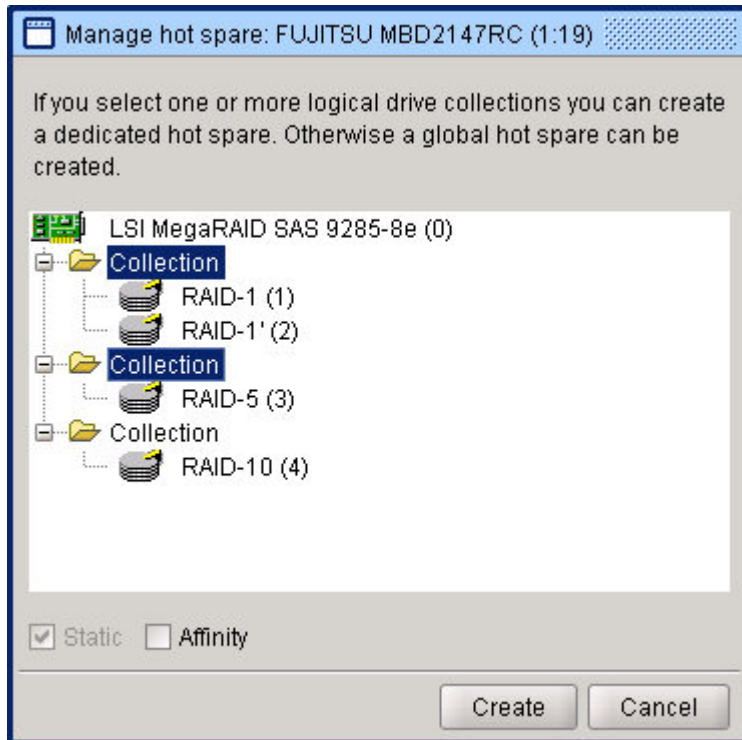
5.4.1 Manage hot spare

This action enables you to add or delete a global or dedicated hot spare.

5.4.1.1 Creating

To create a global or dedicated hot spare please select a free disk () on the left in the tree structure. Start the *Manage hot spare* action (via the pull-down menu of the *Actions* button or with a right mouse click).

In the dialog box which is now displayed (see example) please select one or more collections in order to create a dedicated hot spare. If you do not select a collection, a global hot spare is then created.






The static (or revertible) hot spare feature can be used to automatically restore a hot spare and logical drive to their original configuration. This function allows administrators who prefer to keep a hot spare in a specific slot within the enclosure to easily return to the preferred configuration without a manual rebuild. The static hot spare feature reduces or eliminates any administrator maintenance beyond replacement of the failed hard drive.

Note: The controller automatically reverts a hot spare only if the failed disk is replaced with a new disk in the same slot. If the new disk is not placed in the same slot, a manual "Replace missing" operation can be used to revert a previously commissioned hot spare.

Enclosure affinity is used to set the preference for a hot spare to be used to rebuild a physical disk that resides in the same physical enclosure. This does not preclude the hot spare from being provisioned to a second enclosure if there are no other hot spares present. For example, if there are two enclosures and each enclosure has a hot spare with affinity set, then upon a drive failure the hot spare will be provisioned from the same enclosure as the failed drive.

Note: You can configure hot spare enclosure affinity only if you are using an external storage enclosure.

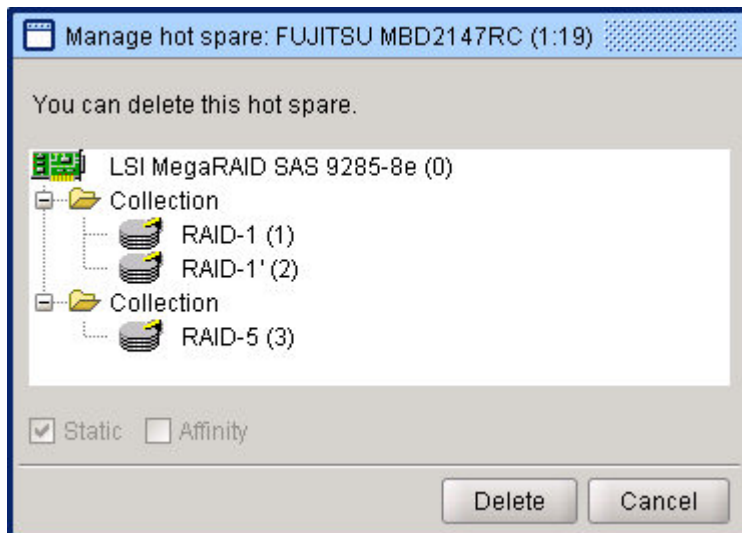
After you have clicked on the *Create* button you must confirm the action once again in another dialog box. Depending on what was selected in the previous dialog box, the drive which was originally unused becomes the hot spare and is flagged as a global () or dedicated () hot spare on the left in the tree structure.


 Please note that you can only create a hot spare with RAID types **with redundancy** (e.g. RAID-1, RAID-5, **not** RAID-0).

5.4.1.2 Deleting

To delete a hot spare please mark the hot spare () or () which you wish to delete on the left in the tree structure. Start the *Manage hot spare* action.

The dialog box which is now displayed shows you the configuration with the logical drives which are currently protected.



After you have clicked on the *Delete* button you must confirm the action once again in another dialog box. The assignment is now released and the previous hot spare is flagged as unused () on the left in the tree structure.

When you quit one of the dialog boxes by means of *Cancel*, no hot spare is created or deleted.

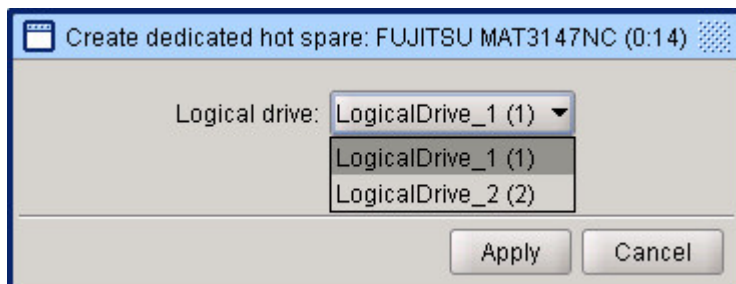
In some controllers the individual actions *Create dedicated hot spare*, *Create global hot spare*, *Delete dedicated hot spare* and *Delete global hot spare* are offered as alternatives to the *Manage hot spare* action described above.


5.4.2 Creating hot spares

With hot spare you can protect either a single logical drive (dedicated hot spare) or all logical drives on the controller (global hot spare). The example below describes how you create a dedicated hot spare.

In the tree structure select an unused drive () which is to function as a standby drive.


Start the *Create dedicated hot spare* action (via the pulldown menu of the *Actions* button or with a right mouse click). A dialog box is opened as in the example below.




In the pulldown menu select the required logical drive and create it using the *Apply* button. After you have pressed the button you must confirm the process once more in another dialog box. The drive that was previously unused is now identified as a dedicated hot spare () in the tree structure.


5.4.3 Deleting hot spares

This action enables you to delete hot spares which you have created. The example below describes how you delete a dedicated hot spare.

In the tree structure select the dedicated hot spare () that you want to delete.

Start the *Delete dedicated hot spare* action (via the pulldown menu of the *Actions* button or with a right mouse click). In the dialog box that appears you must confirm the deletion again. After successful deletion the previously dedicated hot spare is now marked in the tree structure as an unused drive ().

5.5 Foreign Configuration

The new flexible RAID Management enables disks of logical drives to be switched from one enclosure or adapter to another without the configuration being lost. A disk of this type is identified by a blue exclamation point (), which indicates a foreign configuration. This foreign configuration can be imported or deleted.



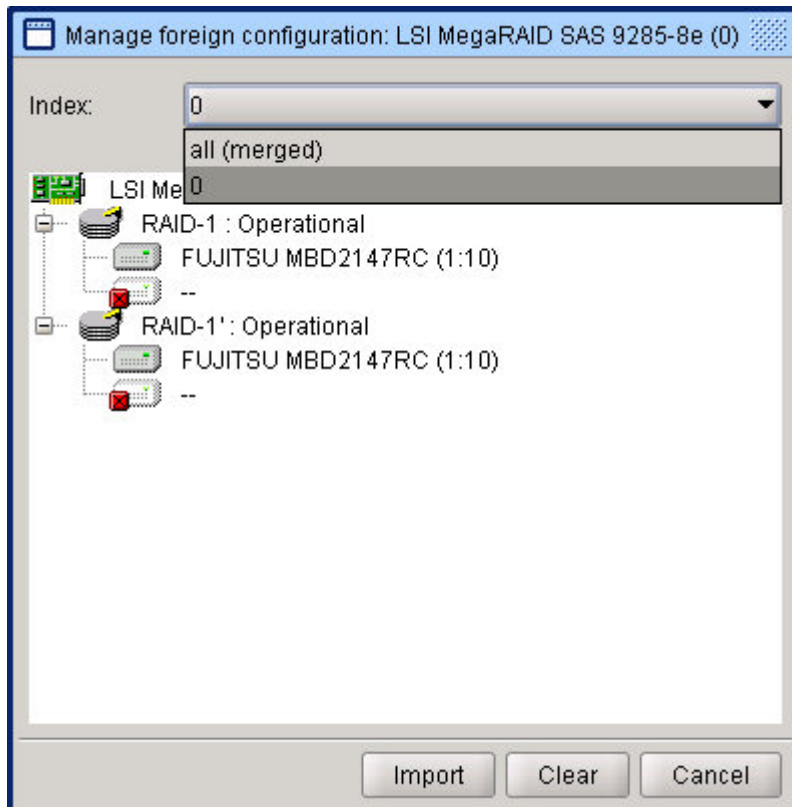
Configurations can be imported or deleted from disks only if the disk is already available again.

If this was not done automatically, please perform the function using the *Make ready* action (by means of the pull-down menu of the *Actions* button or by right-clicking on the disk). You can then start the dialog described below using the *Manage foreign configuration* action.

5.5.1 Manage foreign configuration

This action enables you to import or delete **one** individual foreign configuration or **all** foreign configurations.

In the dialog box (see the example below) use the index to select either one individual foreign configuration or *all (merged)* for all foreign configurations for processing and confirm your selection using the *Import* or *Clear* button.



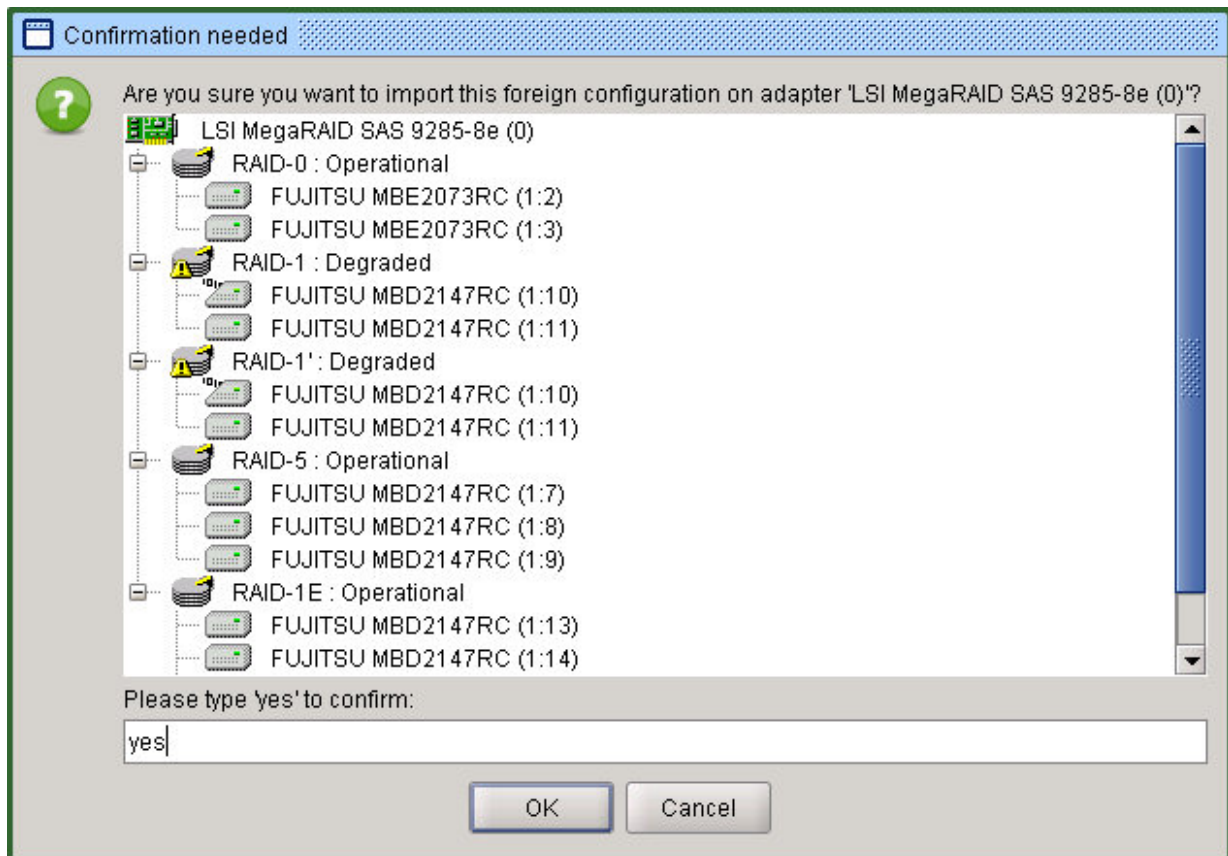
The *Cancel* button in one of the dialog boxes shown below enables you to abort the action without any effect on the existing configuration.

5.5.1.1 Import

When you select *Import*, the future overall configuration is displayed before the actual import operation begins.

When you select an individual foreign configuration, this is examined and imported regardless of the existing configuration.

When you select *all (merged)*, an attempt is made to combine all existing configurations with the foreign configurations.



The import is performed after you have confirmed this and clicked on the **OK** button.

5.5.1.2 Clear

When you select *Clear*, you must confirm the operation once again in another dialog box.

- When one individual foreign configuration is selected, it is cleared.
- When *all (merged)* is selected, all foreign configurations are deleted.

Note: If a disk which still contains an old configuration was replaced during maintenance work, it is also identified by a blue flag on the left of the tree. In this case you must delete the old configuration before you can use the disk again.

5.6 Task

In order to maintain the operational reliability of a RAID system, certain actions can be repeated at regular intervals. These include, for example the consistency check of the logical drives, the Patrol Read of the disks or the recalibration of existing BBUs.

When the appropriate object (system, controller, disk, logical drive, BBU) or an existing task object has been selected, the object action *Manage task* (the dialog described below) can be started via the button pull-down menu *Actions* or by clicking the right mouse button on the object.

5.6.1 Manage task

This action is used to create, modify or delete a task.

5.6.1.1 Create

If a task does not exist for the selected object and the desired action, you can define and create a task with the following properties.

Select via *Task* the action that is to be regularly carried out.

For each respective task an optional *Exception behavior* can be specified. You can deselect the default setting to *stop after 4 errors*. Furthermore you can change the default behavior that after an error a new attempt to start the task is made after 2 minutes, 1 hour, and 8 hours beyond the regular setting. That way you can arrange the number of attempts *skip on error* and the next regular start time for the task.

Manage task: RAID-1 (0)

Task
Start MDC ▼

Exception behavior
☒ stop after 4 errors
☐ skip on error

Frequency
Daily ▼

Start time
☐ now
☒ later Nov 11, 2011 11 h 11 min

Recurrence
Every 11 Day(s)

Create Cancel

Use *Frequency* to set the required period (from minute-by-minute to yearly). There are various settings depending on the *Frequency* selected which are used to define the action recurrences more exactly.

The *Start time* valid for the task, i.e. when the action is started for the very first time, has a default value *now* when creating the task. If the action cannot be started, because e.g. the action is already in use, the option *now* will not be offered. Additionally a time around 24 hours later than current time will be set as default time. Otherwise, if the problem happens when leaving the dialog a time around 8 hours later will be set automatically. A different starting time can be agreed upon by choosing *later* and with input of a valid date as well as a desired time. When the button *Create* is pressed, the required action is started either within the next minute or after expiration of a selected *later* start time.

Recurrence is used to select a value of 1 to 100 so that, depending on the choice of *Frequency*, the action can be repeated within a range of intervals (from 1 minute to 100 years).

Manage task: RAID-1 (0)

Task

Start MDC ▾

Exception behavior

☒ stop after 4 errors
☐ skip on error

Frequency

Weekly ▾

Start time

☐ now
☒ later
 Nov 11, 2011

11

h

11

min

Recurrence

Every

3

 Week(s)

Week day(s)

☐ Monday
 ☒ Tuesday
 ☐ Wednesday
 ☐ Thursday
 ☐ Friday
 ☐ Saturday
 ☐ Sunday

Create

Cancel

A weekly *Frequency* can also have one or more *Weekdays* in order to define the starting point more exactly. If no weekday is selected, the current weekday is automatically set as used in the pre-setting. Furthermore the selected weekdays will be considered by the calculation of the first starting point if *later* is selected.

If a monthly *Frequency* is selected, a day in the month must also be defined on which the respective action is to be started.

If an exact day in the month is defined, but this day is not in available certain months, then the corresponding months are automatically deselected and excluded as a selection option. February 29th is an exception. Such a selection is allowed as this day exists in certain years but not all of them. If necessary, the action is started on the next possible day of the following month, i.e. on March 1st. If no month is selected, the current month is automatically set as used in the pre-setting.

With the choice of *later* by the *Start time* the rule of the desired day of month and also the selected months will be considered by the calculation of the exact starting time.

When the button *Create* is pressed, the required action is started within the next minute or after another desired start time if *later* is selected. If thereby the *Frequency* is set at weekly, monthly or annually, the first start time is then in the current week or within a month or year, respectively.

When you quit the dialog by means of the *Cancel* button, no effect on any existing configuration will occur.

 If you want to create a task for Patrol Read you must set **Patrol Read mode** to manual beforehand. Otherwise the task for Patrol Read will be ignored.

5.6.1.2 Modify

Via the selection of an existing task object or by selection of an action in the dialog, for which the selected object already has a task defined, you can modify the settings of the task.

The *Start time* is preset at *later* when a task is modified. If this setting is not changed, the next start time is calculated when the *OK* button is pressed based on the set and, if necessary, any modified values. If the *Frequency* is set at weekly, monthly or annually, the next start time is then in the current week or within a month or year, respectively. Only a subsequent date is based on the value set in *Recurrence*.

If the *Start time* is changed to *now*, the action is started within the next minute after the button *OK* was pressed. If the action cannot be started, because e.g. the action is already running, the option *now* will not be offered. Otherwise, if the problem happens when leaving the dialog a time around 8 hours later will be set automatically.

Likewise, the status and the internal task error counter is reset after the button *OK* has been pressed.

When you quit the dialog via the *Cancel* button, no changes will occur.

5.6.1.3 Delete

The task is deleted when the button *Delete* is pressed. This does not influence, interrupt nor terminate any current action triggered by the task.

If you quit the dialog by means of the *Cancel* button, no effect on any existing configuration will occur.

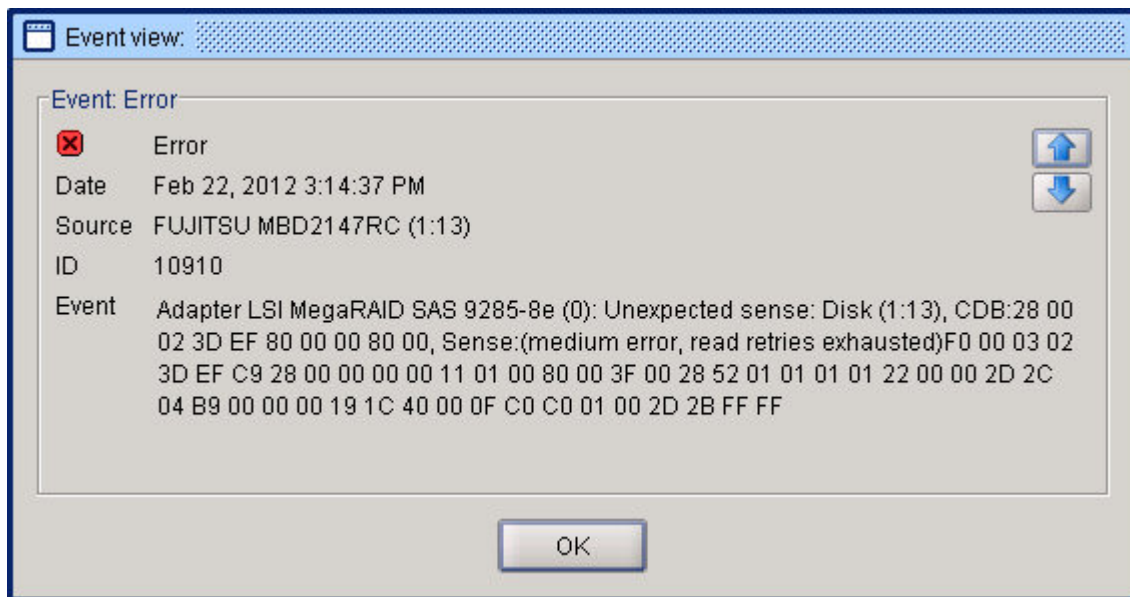
6 Events

6.1 Displaying Events

The event window is located at the lower edge of the user interface. It contains the latest events of all the RAID controllers which are managed by ServerView RAID Manager.




Severity	Date	Source	ID	Event
Error	Feb 22, 2012 3:14:37	FUJITSU MBD2147RC (1:13)	10910	Adapter LSI MegaRAID SAS 9285-8e (0): Unexpected sense: Disk (1:13), CDB:28 00 02 3D EF 80 00 00 80 00, Sense (medium error, read retries exhausted)
Informational	Feb 22, 2012 2:57:57	RX30057-0019	10171	User administrator (amrpu) logged in
Warning	Feb 22, 2012 2:55:50	FUJITSU MBD2147RC (1:13)	10045	Adapter LSI MegaRAID SAS 9285-8e (0): SMART error on disk (1:3)
Informational	Feb 21, 2012 3:13:19	FTS RAID C91 SAS 60 10B (D:3116) (2)	10311	Adapter FTS RAID C91 SAS 60 10B (D:3116) (2): BBU relearn will start in 2 days
Informational	Feb 19, 2012 3:31:24	LSI MegaRAID SAS 9285-8e (0)	10073	Adapter LSI MegaRAID SAS 9285-8e (0): Parity Read finished

You can use the delimiter bar to enlarge or reduce this window. The width of the columns can be changed by dragging its border in the table header. This is sometimes useful for long event messages. A double click on an event opens a dialog, with which it is easy to navigate through the events and to catch the whole detailed message at a glance.



The following information is available for each event:

- The type is additionally presented by an icon which indicates the severity of the event.

-  Error
-  Warning
-  Important Information

- Date and time at which the event occurred
- The name of the object which reported the event
- Event ID
- A brief message with a description of the event

ServerView RAID Manager logs all events in a Log file in plain text. This file is in XML format and is simple to read out and process.

In addition, all events are sent out as SNMP traps for further processing by ServerView Event Manager or any other management tool that can handle traps (e.g. IBM Tivoli, HP OpenView, etc.). Please refer to the ServerView documentation for further details and configuration options.

By default all events show up in the operating system's logging facility. On Windows based systems entries can be found in *Start > Settings > Control Panel > Administrative Tools > Event Viewer* (Application), on Linux systems in */var/log/messages*, and on Solaris systems in */var/adm/messages*.



Note that the message texts, IDs and error classes of the events are the same as those used in the **traps** and in file/system logging. The only difference is that the four error classes of the traps have been reduced to three error classes for the events (Informational = Information, Minor = Warning, Major and Critical = Error).

6.2 Events / SNMP Traps

The basis for the ServerView RAID SNMP Agent is the MIB file RAID.mib (Windows) or FSC-RAID-MIB.txt (Linux/VMware/Solaris). All the information and trap types are defined in this file. The traps of the MIB are listed below.

The message texts, IDs and error classes of the traps are the same as those used in the **event messages** in the interface and in file/system logging.

If the described recovery actions do not solve the problem please call your local Fujitsu Help Desk.

ID	Severity	Log Entry	Recovery action
1	Informational	Undefined event	If there are errors directly before or after this event, perform the proper recovery action for that error.
2	Informational	Connection to ServerView RAID Manager established	
3	Informational	Disconnected from ServerView RAID Manager	
4	Critical	Unexpected disconnect from ServerView RAID Manager	If problem persists after reboot, call your local Fujitsu Helpdesk.
5	Informational	Test event	
10000	Informational	Unknown event	If there are errors directly before or after this event, perform the proper recovery action for that error.
10001	Informational	Internal event	For information only.
10002	Minor	Write access of the ServerView RAID Manager revoked by user [...] ([...])	For information only.
10003	Major	BBU temperature out of range	1. Check installation of all air flow channels, closed housing, and unblocked louvers. 2. Check environmental temperature. 3. Check version of RAID controller/iRMC firmware, and BIOS.
10004	Major	BBU temperature unstable	1. Check version of RAID controller/iRMC firmware, and BIOS. 2. If problem persists replace BBU.

10005	Major	BBU temperature above threshold	<ol style="list-style-type: none"> 1. Check installation of all air flow channels, closed housing, and unblocked louvers. 2. Check environmental temperature. 3. Check version of RAID controller/iRMC firmware, and BIOS.
10006	Major	BBU voltage out of range	<ol style="list-style-type: none"> 1. Check connection between BBU data/power cable and RAID controller. 2. Check version of RAID controller/iRMC firmware, and BIOS. 3. If problem persists replace BBU.
10007	Major	BBU voltage unstable	<ol style="list-style-type: none"> 1. Check connection between BBU data/power cable and RAID controller. 2. Check version of RAID controller/iRMC firmware, and BIOS. 3. If problem persists replace BBU.
10008	Major	BBU voltage below threshold	<ol style="list-style-type: none"> 1. Check connection between BBU data/power cable and RAID controller. 2. Check version of RAID controller/iRMC firmware, and BIOS. 3. If problem persists replace BBU.
10009	Major	BBU communication error	<ol style="list-style-type: none"> 1. Check connection between BBU data/power cable and RAID controller. 2. Check version of RAID controller/iRMC firmware, and BIOS. 3. If problem persists replace BBU.
10010	Informational	BBU reconditioning started	
10011	Informational	BBU status becomes normal	
10012	Informational	BBU good	
10013	Critical	BBU failed	<p>Note: Only informational during recalibration process.</p> <ol style="list-style-type: none"> 1. Check connection between BBU data/power cable and RAID controller. 2. Check version of RAID controller/iRMC firmware, and BIOS. 3. If problem persists replace BBU.

10014	Major	BBU fast charging failed	Note: Do not interrupt the charging process by reboots or shutdowns. 1. Check version of RAID controller/iRMC firmware, and BIOS. 2. If problem persists replace BBU.
10015	Minor	BBU charge count exceeded	1. Initiate manual recalibration process (e.g. via ServerView RAID Manager). Note: Do not interrupt the charging process by reboots or shutdowns. 2. If problem persists replace BBU.
10016	Minor	BBU needs reconditioning	Note: By default BBU recalibration is automatically initiated every 30 days. 1. If scheduled BBU recalibration is disabled initiate manual recalibration process (e.g. via ServerView RAID Manager).
10017	Informational	SCSI sense data on disk ([..]) available: [..]	
10018	Informational	Asynchronous command finished	
10019	Informational	Adapter [..] suspended	
10020	Informational	Adapter [..] resumed	
10021	Informational	Disk ([..]) marked online	
10022	Critical	Disk ([..]) marked offline	Note: Only informational if affected disk was manually set offline otherwise: 1. If offline disk is member of an array initiate a rebuild to the offline disk. 2. If problem persists replace affected disk.
10023	Major	Disk ([..]) timed out	Note: In general additional error messages should occur. If there are no other actions defined call your local Fujitsu Helpdesk.
10024	Informational	Global hot spare created on disk ([..])	
10025	Minor	Global hot spare deleted on disk ([..])	For information only.
10026	Informational	Dedicated hot spare created on disk ([..])	
10027	Minor	Dedicated hot spare deleted on disk ([..])	For information only.
10028	Informational	Disk ([..]) marked available	
10029	Informational	Rebuild on disk ([..]) started	

10030	Major	Rebuild on disk ([..]) failed	1. Manually initiate a second rebuild (e.g. via ServerView RAID Manager). 2. If problem persists replace affected disk.
10031	Major	Bad block on disk ([..]) LBA [..] detected	Replace affected disk.
10032	Informational	New disk ([..]) detected	
10033	Minor	Disk ([..]) removed	Note: Only informational if affected disk has been removed otherwise: 1. Unplug affected disk, wait 30 seconds, reinsert it. 2. Replace affected disk. 3. Replace affected backplane or the data cable.
10034	Informational	Bad sector log entry on disk ([..]) cleared	
10035	Informational	Bad sector log on disk ([..]) updated	
10036	Major	Bad sector on disk ([..]) detected	Replace affected disk.
10037	Major	COD I/O error on disk ([..])	1. Manually initiate a rebuild (e.g. via ServerView RAID Manager) of affected disk. 2. If problem persists replace affected disk.
10038	Major	Error on disk ([..]) detected	Replace affected disk.
10039	Informational	Channel [..] was reset	
10040	Major	Retry I/O on disk ([..])	If the problem occurs repeatedly replace affected disk.
10041	Major	ECC error on disk ([..])	If the problem occurs repeatedly replace affected disk.
10042	Informational	Write modes changed	
10043	Major	Media error on disk ([..])	Replace affected disk.
10044	Minor	SMART warning on disk ([..])	Note: Disk reports a prefailure. The affected disk might fail soon. 1. Replace the disk during next maintenance.
10045	Minor	SMART error on disk ([..])	Replace affected disk.
10046	Major	Bad disk inserted in enclosure [..]	Replace affected disk.
10047	Major	Enclosure [..] powered down	If this error message is not a result of a planned power off of the external storage subsystem: 1. Check the power cable(s). 2. Check the mains voltage. 3. Replace affected power supply(s).
10048	Informational	Enclosure [..] powered up	

10049	Critical	Fan [...] in enclosure [...] failed	Replace affected fan within the external storage subsystem.
10050	Major	Temperature sensor [...] in enclosure [...] above threshold	1. Check installation of all air flow channels, closed housing, and unblocked louvers. 2. Check environmental temperature.
10051	Critical	Power supply [...] in enclosure [...] failed	1. Check the power cable. 2. Check the mains voltage. 3. Replace affected power supply.
10052	Critical	3.3V power failed for disk ([...])	1. Check whether all cables are correctly connected to the disk backplane connectors. 2. Replace affected disk.
10053	Critical	5.0V power failed for disk ([...])	1. Check whether all cables are correctly connected to the disk backplane connectors. 2. Replace affected disk.
10054	Critical	12V power failed for disk ([...])	1. Check whether all cables are correctly connected to the disk backplane connectors. 2. Replace affected disk.
10055	Informational	Rebuild started on logical drive [...]	
10056	Informational	Rebuild finished on logical drive [...]	
10057	Major	Rebuild failed on logical drive [...]	1. Manually initiate a second rebuild (e.g. via ServerView RAID Manager).
10058	Minor	Rebuild aborted on logical drive [...]	Note: Rebuild was probably aborted by user. Attention: The affected RAID array is still degraded. 1. The rebuild should be started again as soon as possible.
10059	Informational	Rebuild suspended on logical drive [...]	
10060	Informational	Consistency check started on logical drive [...]	
10061	Informational	Consistency check finished on logical drive [...]	
10062	Major	Consistency check failed on logical drive [...]	Failure happens only if a disk out of the logical drive failed. 1. Check state of logical drive. 2. If logical drive is not operational, check state of affected disk. 3. Check for additional error messages for affected disk.

10063	Minor	Consistency check aborted on logical drive [...]	Note: Consistency check was probably aborted by user. 1. The consistency check should be started again as soon as possible.
10064	Informational	Consistency check suspended on logical drive [...]	
10065	Informational	Consistency check started on uninitialized logical drive [...]	
10066	Major	Consistency check finished with errors on logical drive [...]	1. Manually initiate second consistency check (MDC). 2. If problem persists backup data from affected logical drive. 3. Delete and recreate affected logical drive. 4. Restore data.
10067	Major	Inconsistency detected on logical drive [...] at LBA [...]	Check if logical drive is initialized. If initialized check the following: 1. Backup your data. 2. Start a consistency check with fix. 3. Compare backup data with data on logical drive. 4. If different (data lost), restore last good data.
10068	Informational	Migration started on logical drive [...]	
10069	Informational	Migration finished on logical drive [...]	
10070	Major	Migration failed on logical drive [...]	Note: The logical drive is failed (multi dead). 1. Replace broken drives. 2. Create new configuration and restore last good data.
10071	Minor	Migration aborted on logical drive [...]	Note: Migration was probably aborted by user. For information only.
10072	Informational	Patrol Read started	
10073	Informational	Patrol Read finished	
10074	Minor	Patrol Read aborted	Note: Patrol read was probably aborted by user. For information only.
10075	Informational	Patrol Read stopped	
10076	Informational	Patrol Read suspended	
10077	Informational	Patrol Read resumed	
10078	Minor	Logical drive [...] degraded	1. Manually initiate a rebuild of affected disk (e.g. via ServerView RAID Manager). 2. If problem persists replace affected disk.

10079	Critical	Logical drive [...] failed	Note: Sometimes it is possible to recover without data loss. Further investigation is needed.
10080	Informational	Logical drive [...] created	
10081	Minor	Logical drive [...] deleted	For information only.
10082	Informational	Logical drive [...] operational	
10083	Major	Logical drive [...]: Error on disk ([...])	Replace affected disk.
10084	Major	Logical drive [...]: Bad block at LBA [...] detected	1. Try to rewrite data. 2. If problem persists replace affected disk.
10085	Informational	Initialization started on logical drive [...]	
10086	Informational	Initialization finished on logical drive [...]	
10087	Informational	BGI started on logical drive [...]	
10088	Informational	BGI finished on logical drive [...]	
10089	Minor	BGI canceled on logical drive [...]	Background initialization (BGI) resumes automatically after a certain period of time. For information only.
10090	Minor	Initialization canceled on logical drive [...]	For information only.
10091	Informational	Drive letter changed for logical drive [...]	
10092	Informational	Hot spare operation on logical drive [...] started	
10093	Major	Hot spare operation on logical drive [...] failed	1. Unplug affected disk, wait 30 seconds, reinsert it. 2. Replace affected disk.
10094	Major	Logical drive [...] forced from failed to degraded	1. Temporary offline case. 2. Try to rebuild remaining defect drive.
10095	Informational	Alarm enabled	
10096	Minor	Alarm disabled	For information only.
10097	Informational	Automatic inconsistency handling enabled	
10098	Informational	Automatic inconsistency handling disabled	
10099	Informational	Inconsistency handling interval changed	
10100	Informational	Rebuild rate changed	
10101	Informational	Patrol Read disabled	
10102	Informational	Patrol Read set to automatic	
10103	Informational	Patrol Read set to manual	
10104	Informational	Patrol Read delay changed	
10105	Informational	Initialization set to normal	
10106	Informational	Initialization set to fast	
10107	Informational	Initiator ID changed	
10108	Informational	Automatic rebuild enabled	

10109	Informational	Automatic rebuild disabled	
10110	Informational	New device set to automatic	
10111	Informational	New device set to CtrlM	
10112	Informational	MDC rate changed	
10113	Informational	MDC rate changed to [...] percent	
10114	Informational	BIOS enabled	
10115	Informational	BIOS disabled	
10116	Informational	BIOS stop on error enabled	
10117	Informational	BIOS stop on error disabled	
10118	Informational	Write cache on all disks enabled	
10119	Informational	Write cache on all disks disabled	
10120	Informational	Read-ahead on all disks enabled	
10121	Informational	Read-ahead on all disks disabled	
10122	Informational	Automatic resumption enabled	
10123	Informational	Automatic resumption disabled	
10124	Informational	Spinup drive count changed (after next reboot)	
10125	Informational	Spinup delay changed (after next reboot)	
10126	Informational	Consistency check rate changed	
10127	Informational	Temporary offline enabled	
10128	Informational	Temporary offline disabled	
10129	Informational	SMART enabled	
10130	Informational	SMART disabled	
10131	Informational	SMART poll interval changed	
10132	Informational	Configuration rescanned	
10133	Informational	Configuration cleared	
10134	Informational	Activity changed	
10135	Informational	Channel [...] termination set to wide	
10136	Informational	Channel [...] termination set to narrow	
10137	Informational	Channel [...] termination disabled	
10138	Informational	Channel [...] activated	
10139	Minor	Channel [...] disabled	1. Connection issue. 2. Check all of your cabling.
10140	Informational	Channel [...] set to dedicated	
10141	Informational	Channel [...] set to shared	
10142	Informational	Logical drive [...]: Read-ahead enabled	
10143	Informational	Logical drive [...]: Read-ahead disabled	
10144	Informational	Logical drive [...]: Adaptive read-ahead enabled	

10145	Informational	Logical drive [...]: Write mode set to Write-through	
10146	Informational	Logical drive [...]: Write mode set to Write-back	
10147	Informational	Logical drive [...]: I/O mode set to direct	
10148	Informational	Logical drive [...]: I/O mode set to cached	
10149	Informational	Max. transfer speed of disk (...) changed (after next reboot)	
10150	Informational	Bus width of disk (...) changed (after next reboot)	
10151	Major	BBU voltage problem detected	<ol style="list-style-type: none"> 1. Check connection between BBU data/power cable and RAID controller. 2. Check version of RAID controller/iRMC firmware, and BIOS. 3. If problem persists replace BBU.
10152	Major	BBU temperature problem detected	<ol style="list-style-type: none"> 1. Check installation of all air flow channels, closed housing, and unblocked louvers. 2. Check environmental temperature. 3. Check version of RAID controller/iRMC firmware, and BIOS.
10153	Informational	BBU charging	
10154	Critical	BBU failed	<p>Note: Only informational during recalibration process.</p> <ol style="list-style-type: none"> 1. Check connection between BBU data/power cable and RAID controller. 2. Check version of RAID controller/iRMC firmware, and BIOS. 3. If problem persists replace BBU.
10155	Informational	BBU normal	
10156	Informational	BBU discharging	
10157	Minor	Disk error fixed	For information only.
10158	Informational	Driver write cache enabled	
10159	Informational	Driver write cache disabled	
10160	Informational	Drive sizing (GB boundary) enabled	
10161	Informational	Drive sizing (GB boundary) disabled	
10162	Informational	Hot spare support and automatic rebuild enabled	
10163	Informational	Hot spare support and automatic rebuild disabled	

10164	Informational	Task rate changed	
10165	Informational	Inconsistency handling set to consistency check	
10166	Informational	Inconsistency handling set to consistency check (abort on first inconsistency)	
10167	Informational	Inconsistency handling set to MDC	
10168	Informational	Logical drive [...]: Name changed	
10169	Informational	Logical drive [...]: Cache write mode changed	
10170	Major	Reboot required	For information only.
10171	Informational	User [...] ([...]) logged in	
10172	Informational	User [...] ([...]) logged out	
10173	Informational	Hot spare enabled	
10174	Informational	Hot spare disabled	
10175	Informational	Hot swap enabled	
10176	Informational	Hot swap disabled	
10177	Informational	Write mode set to Write-back	
10178	Informational	Write mode set to Write-through	
10179	Informational	Write mode set to Adaptive	
10180	Informational	BBU charging started	
10181	Informational	Automatic initialization of RAID-5 enabled	
10182	Informational	Automatic initialization of RAID-5 disabled	
10183	Informational	Copyback enabled	
10184	Informational	Copyback disabled	
10185	Informational	Initialization set to clear	
10186	Informational	Verification started on disk ([...])	
10187	Informational	Verification finished on disk ([...])	
10188	Informational	Logical drive [...]: Cache read mode changed	
10189	Informational	Logical drive [...]: Cache mode changed	
10190	Informational	Logical drive [...]: Access mode changed	
10191	Informational	Logical drive [...]: BGI mode changed	
10192	Informational	Logical drive [...]: Disk cache mode changed	
10193	Informational	Firmware initialization started	
10194	Informational	Firmware version [...]	
10195	Major	Unable to recover cache data from TBBU	Call your local Fujitsu Helpdesk.
10196	Informational	Cache data recovered from TBBU successfully	
10197	Major	Cluster down; communication with peer lost	Call your local Fujitsu Helpdesk.
10198	Informational	[...] ownership changed from [...] to [...]	

10199	Informational	BGI rate changed to [...] percent	
10200	Major	Adapter cache discarded due to memory/BBU problems	
10201	Major	Unable to recover cache data due to configuration mismatch	Call your local Fujitsu Helpdesk.
10202	Informational	Cache data recovered successfully	
10203	Major	Adapter cache discarded due to firmware version IOncompatibility	1. Check version of RAID controller/iRMC firmware, and BIOS.
10204	Critical	Fatal firmware error: [...]	1. Disconnect AC and wait 30 seconds before reconnect.
10205	Informational	Factory defaults restored	
10206	Major	Flash downloaded image corrupt	1. Download again. 2. Retry flash.
10207	Major	Flash erase error	1. Replace affected RAID controller.
10208	Major	Flash timeout during erase	1. Retry flash. 2. Replace affected RAID controller.
10209	Major	Flash error	1. Retry flash. 2. Replace affected RAID controller.
10210	Informational	Flashing image: [...]	
10211	Informational	Flash of new firmware image(s) complete	
10212	Major	Flash programming error	1. Retry flash. 2. Replace affected RAID controller.
10213	Major	Flash timeout during programming	1. Retry flash. 2. Replace affected RAID controller.
10214	Minor	Flash chip type unknown	1. Retry flash. 2. Replace affected RAID controller.
10215	Major	Flash command set unknown	1. Retry flash. 2. Replace affected RAID controller.
10216	Major	Flash verification failure	1. Retry flash. 2. Replace affected RAID controller.
10217	Informational	Flush rate changed to [...] seconds	
10218	Informational	Hibernate command received from host	
10219	Informational	Event log cleared	
10220	Informational	Event log wrapped	
10221	Major	Multi-bit ECC error: ECAR=[...], ELOG=[...], ([...])	If the problem occurs repeatedly replace the RAID controller DIMM module (cache).

10222	Major	Single-bit ECC error: ECAR=[..], ELOG=[..], ([..])	If the problem occurs repeatedly replace the RAID controller DIMM module (cache).
10223	Major	Not enough adapter memory	1. Replace the RAID controller DIMM module (cache). 2. If problem persists replace RAID controller.
10224	Informational	Patrol Read rate changed to [..] percent	
10225	Informational	Migration rate changed to [..] percent	
10226	Informational	Shutdown command received from host	
10227	Informational	Test event: '[..]'	
10228	Informational	Time established as [..]; ([..] seconds since power on)	
10229	Informational	User entered firmware debugger	
10230	Informational	BGI corrected medium error (logical drive [..] at LBA [..] on disk ([..]) at LBA [..])	
10231	Major	BGI finished with uncorrectable errors on logical drive [..]	Initiate consistency check (e.g. via ServerView RAID Manager).
10232	Major	BGI detected uncorrectable multiple medium errors (disk ([..]) at LBA [..] on logical drive [..])	Replace affected disk.
10233	Major	BGI failed on logical drive [..]	1. Restart Background initialization (BGI). 2. Replace affected disk.
10234	Informational	BGI progress on logical drive [..] is [..]	
10235	Informational	Logical drive [..]: [..] changed	
10236	Informational	MDC corrected medium error (logical drive [..] at LBA [..] on disk ([..]) at LBA [..])	
10237	Major	Consistency check found inconsistent parity on logical drive [..] at stripe [..]	1. Start consistency check again. 2. If problem persists backup data from affected logical drive. 3. Delete and recreate affected logical drive. 4. Restore data.
10238	Informational	Consistency check logging disabled on logical drive [..] (too many Inconsistencies)	
10239	Informational	Consistency check progress on [..] is [..]	
10240	Major	Initialization failed on logical drive [..]	1. Start initialization again.
10241	Informational	Initialization progress on logical drive [..] is [..]	
10242	Informational	Fast initialization started on logical drive [..]	
10243	Informational	Full initialization started on logical drive [..]	
10244	Informational	Logical drive [..]: Property [..] updated	

10245	Major	Migration detected uncorrectable multiple medium errors (logical drive [...] at LBA [...] on disk ([...]) at LBA [...])	Replace affected disk.
10246	Informational	Migration progress on logical drive [...] is [...]	
10247	Informational	Migration resumed on logical drive [...]	
10248	Major	Resume migration of logical drive [...] failed due to Configuration Mismatch	1. Check the RAID configuration and the event log for additional information. 2. Backup data from affected logical drive.
10249	Informational	State change on logical drive [...] from operational to operational	
10250	Minor	Clear aborted on disk ([...])	For information only.
10251	Major	Clear failed on disk ([...]) (error [...])	1. Check version of RAID controller/iRMC firmware, and BIOS. 2. Verify that current RAID controller drivers are installed. 3. Disconnect AC and wait 30 seconds before reconnect.
10252	Informational	Clear progress on disk ([...]) is [...]	
10253	Informational	Clear started on disk ([...])	
10254	Informational	Clear finished on disk ([...])	
10255	Major	Error on disk ([...]) (error [...])	Replace affected disk.
10256	Informational	Format complete on disk ([...])	
10257	Informational	Format started on disk ([...])	
10258	Major	Hot spare SMART polling failed on disk ([...]) (error [...])	Call your local Fujitsu Helpdesk.
10259	Major	Disk ([...]) is not supported	Install supported disk.
10260	Informational	Patrol Read corrected medium error on disk ([...]) at LBA [...]	
10261	Informational	Patrol Read progress on disk ([...]) is [...]	
10262	Major	Patrol Read found an uncorrectable medium error on disk ([...]) at LBA [...]	Replace affected disk.
10263	Minor	Predictive failure: Disk ([...])	Note: Disk reports a prefailure. The affected disk might fail soon. 1. Replace the disk during next maintenance.
10264	Major	Puncturing bad block on disk ([...]) at LBA [...]	Replace affected disk.
10265	Minor	Rebuild aborted by user on disk ([...])	For information only.
10266	Informational	Rebuild complete on logical drive [...]	
10267	Informational	Rebuild complete on disk ([...])	
10268	Informational	Rebuild progress on disk ([...]) is [...]	

10269	Informational	Rebuild resumed on disk ([..])	
10270	Informational	Rebuild automatically started on disk ([..])	
10271	Major	Rebuild stopped on disk ([..]) due to loss of cluster ownership	1. Restart rebuild.
10272	Major	Reassign write operation failed on disk ([..]) at LBA [..]	Replace affected disk.
10273	Major	Unrecoverable medium error during rebuild on disk ([..]) at LBA [..]	Replace affected disk.
10274	Informational	Corrected medium error during recovery on disk ([..]) at LBA [..]	
10275	Major	Unrecoverable medium error during recovery on disk ([..]) at LBA [..]	Replace affected disk.
10276	Informational	Unexpected sense: Disk ([..]), Key/ASC/ASCQ: [..]: [..]	
10277	Informational	State change on disk ([..]) from available to available	
10278	Informational	State change by user on disk ([..]) from available to available	
10279	Major	Redundant path to disk ([..]) broken	Call your local Fujitsu Helpdesk.
10280	Informational	Redundant path to disk ([..]) restored	
10281	Minor	Dedicated hot spare ([..]) no longer useful due to deleted array	For information only.
10282	Major	SAS topology error: Loop detected	Check the SAS configuration and cabling.
10283	Major	SAS topology error: Unaddressable device	Check the SAS configuration and cabling.
10284	Major	SAS topology error: Multiple ports to the same SAS address	Check the SAS configuration and cabling.
10285	Major	SAS topology error: Expander error	1. Check the SAS configuration and cabling. 2. If problem persists replace affected backplane.
10286	Major	SAS topology error: SMP timeout	Check the SAS configuration and cabling.
10287	Major	SAS topology error: Out of route entries	Check the SAS configuration and cabling.
10288	Major	SAS topology error: Index not found	Check the SAS configuration and cabling.
10289	Major	SAS topology error: SMP function failed	Check the SAS configuration and cabling.
10290	Major	SAS topology error: SMP CRC error	Check the SAS configuration and cabling.
10291	Major	SAS topology error: Multiple subtractive	Check the SAS configuration and cabling.

10292	Major	SAS topology error: Table to table	Check the SAS configuration and cabling.
10293	Major	SAS topology error: Multiple paths	Check the SAS configuration and cabling.
10294	Major	Unable to access disk ([..])	1. Unplug affected disk, wait 30 seconds, reinsert it. 2. Replace affected disk. 3. Replace affected backplane.
10295	Minor	Dedicated hot spare not useful for all arrays	For information only.
10296	Minor	Global hot spare does not cover all arrays	Note: The size of the global hot spare is not sufficient to secure all arrays.
10297	Minor	Marking logical drive [...] inconsistent due to active writes at shutdown	Initiate consistency check (e.g. via ServerView RAID Manager).
10298	Informational	BBU present	
10299	Informational	BBU not present	If the system does not have a BBU this is for information only. If the system does have a BBU replace the BBU.
10300	Informational	New BBU detected	
10301	Informational	BBU has been replaced	
10302	Informational	BBU temperature is normal	
10303	Major	BBU has failed and cannot support data retention	If the error message occurs right after replacement of the BBU it can be safely ignored. The situation can occur due to the insufficient BBU charge. If the error message occurs during regular operation replace the BBU.
10304	Informational	BBU relearn started	
10305	Informational	BBU relearn in progress	
10306	Informational	BBU relearn finished	
10307	Minor	BBU relearn timed out	1. Initiate manual recalibration process (e.g. via ServerView RAID Manager). Note: Do not interrupt the charging process by reboots or shutdowns. 2. If problem persists replace BBU.
10308	Informational	BBU relearn pending: BBU is under charge	
10309	Informational	BBU relearn postponed	
10310	Informational	BBU relearn will start in 4 days	
10311	Informational	BBU relearn will start in 2 days	
10312	Informational	BBU relearn will start in 1 day	
10313	Informational	BBU Relearn will start in 5 hours	

10314	Minor	BBU removed	For information only.
10315	Informational	Enclosure (SES) discovered on [..]	
10316	Informational	Enclosure (SAF-TE) discovered on [..]	
10317	Minor	Enclosure [..] communication lost	1. Check data cable(s) to enclosure. 2. Check if enclosure is running.
10318	Informational	Enclosure [..] communication restored	
10319	Informational	Enclosure [..] fan [..] inserted	
10320	Minor	Enclosure [..] fan [..] removed	For information only.
10321	Major	Enclosure [..] I/O module [..] failed	Call your local Fujitsu Helpdesk.
10322	Informational	Enclosure [..] I/O module [..] inserted	
10323	Major	Enclosure [..] I/O module [..] removed	For information only.
10324	Major	Enclosure [..] shutdown	For information only.
10325	Minor	Enclosure [..] not supported; too many enclosures connected to port	Check your enclosure configuration.
10326	Major	Enclosure [..] firmware mismatch (I/O module [..])	Call your local Fujitsu Helpdesk.
10327	Major	Enclosure [..] sensor [..] bad	Call your local Fujitsu Helpdesk.
10328	Major	Enclosure [..] PHY bad for slot [..]	Replace affected disk.
10329	Major	Enclosure [..] is unstable	Call your local Fujitsu Helpdesk.
10330	Major	Enclosure [..] hardware error	1. Check data cable(s) to enclosure. 2. Check if enclosure is running.
10331	Major	Enclosure [..] not responding	1. Check data cable(s) to enclosure. 2. Check if enclosure is running.
10332	Minor	SAS/SATA mixing not supported in enclosure; [..] disabled	Check your disk configuration within enclosure.
10333	Informational	Enclosure (SES) hot plug on [..] was detected, but is not supported	
10334	Informational	Clustering enabled	
10335	Informational	Clustering disabled	
10336	Minor	Disk ([..]) too small to be used for auto rebuild	Check your disk configuration.
10337	Informational	BBU enabled; changing Write-through logical drives to Write-back	

10338	Minor	BBU disabled; changing Write-back logical drives to Write-through	Note: Only informational during recalibration process. 1. Check connection between BBU data/power cable and RAID controller. 2. Check version of RAID controller/iRMC firmware, and BIOS. 3. If problem persists replace BBU.
10339	Informational	Bad block table on disk ([..]) is 80 percent full	
10340	Major	Bad block table on disk ([..]) is full; unable to log Block [..]	Replace affected disk.
10341	Minor	MDC aborted due to ownership loss on logical drive [..]	1. Restart consistency check (MDC).
10342	Minor	BGI aborted due to ownership loss on logical drive [..]	1. Restart Background initialization (BGI).
10343	Major	BBU/charger problems detected; SOH bad	Replace the BBU.
10344	Minor	Single-bit ECC error: ECAR=[..], ELOG=[..], ([..]); warning threshold exceeded	If the problem occurs repeatedly replace the RAID controller DIMM module (cache).
10345	Major	Single-bit ECC error: ECAR=[..], ELOG=[..], ([..]); critical threshold exceeded	1. Replace the RAID controller DIMM module (cache). 2. If problem persists replace RAID controller.
10346	Major	Single-bit ECC error: ECAR=[..], ELOG=[..], ([..]); further reporting disabled	
10347	Minor	Enclosure [..] power supply [..] cable removed	Check the enclosure power cable(s).
10348	Informational	Enclosure [..] power supply [..] cable inserted	
10349	Informational	Enclosure [..] fan [..] returned to normal	
10350	Informational	BBU retention started on previous boot	
10351	Informational	BBU retention test passed	
10352	Major	BBU retention test failed	Note: In general additional error messages should occur. If there are no other actions defined call your local Fujitsu Helpdesk.
10353	Informational	Retention test started on previous reboot	
10354	Informational	NVRAM retention test passed	
10355	Major	NVRAM retention test failed	Note: In general additional error messages should occur. If there are no other actions defined call your local Fujitsu Helpdesk.
10356	Informational	[..] test finished [..] passes successfully	

10357	Major	[...] test failed on [...] pass. fail data: errorOffset=[...] goodData=[...] badData=[...]	Note: In general additional error messages should occur. If there are no other actions defined call your local Fujitsu Helpdesk.
10358	Informational	Self-check diagnostics finished	
10359	Informational	Foreign configuration detected	
10360	Informational	Foreign configuration imported	
10361	Informational	Foreign configuration cleared	
10362	Minor	NVRAM is corrupt; reinitializing	If the problem occurs repeatedly replace the RAID controller.
10363	Minor	NVRAM mismatch occurred	If the problem occurs repeatedly replace the RAID controller.
10364	Minor	SAS wide port [...] lost link on PHY [...]	1. Unplug affected disk, wait 30 seconds, reinsert it. 2. Check/replace cable between controller and affected disk. 3. Check version of RAID controller/iRMC firmware, and BIOS. 4. Replace affected disk.
10365	Informational	SAS wide port [...] restored link on PHY [...]	
10366	Minor	SAS port [...], PHY [...] has exceeded the allowed error rate	Note: Disk reports errors. The affected disk might fail soon. 1. Replace the disk as soon as possible.
10367	Minor	Bad block reassigned on disk ([...]) from LBA [...] to LBA [...]	If the problem occurs repeatedly replace the disk during next maintenance.
10368	Informational	Adapter hot plug detected	
10369	Informational	Enclosure [...] temperature sensor [...] differential detected	For information only.
10370	Informational	Disk test cannot start. No qualifying disks found	
10371	Informational	Time duration provided by host is not sufficient for self-checking	
10372	Informational	Disk ([...]) on array [...] row [...] marked as missing	
10373	Informational	Disk ([...]) replaced missing on array [...] row [...]	
10374	Informational	Enclosure [...] temperature sensor [...] returned to normal	
10375	Informational	Enclosure [...] firmware download in progress	
10376	Major	Enclosure [...] firmware download failed	Call your local Fujitsu Helpdesk.
10377	Minor	Disk ([...]) is not certified	Check the type of your disk.
10378	Minor	Dirty cache data discarded by user	For information only.

10379	Minor	Disks missing from configuration at boot	Check your RAID configuration.
10380	Minor	Logical drives missing drives and will go offline at boot: [..]	Check your RAID configuration.
10381	Minor	Logical drives missing at boot: [..]	Check your RAID configuration.
10382	Minor	Previous configuration completely missing at boot	Check your RAID configuration.
10383	Informational	BBU charging complete	
10384	Informational	Enclosure [..] fan [..] speed changed	
10385	Informational	Dedicated hot spare ([..]) imported as global due to missing arrays	
10386	Informational	Disk ([..]) rebuild not possible as SAS/SATA mixing is not supported in an array	
10387	Informational	I/O module [..] has been rebooted as part of enclosure firmware download. It will be unavailable until reboot completes	
10388	Minor	Logical drive [..] partially degraded	Replace affected disk.
10389	Minor	BBU requires reconditioning; please initiate a LEARN cycle	
10390	Informational	Coercion mode changed	
10391	Informational	BBU automatic learn mode changed	
10392	Informational	BBU automatic learn period changed	
10393	Informational	BBU learn delay interval changed	
10394	Informational	BBU next learn time changed	
10395	Informational	Max. disk count for Patrol Read changed to [..]	
10396	Informational	Continuous patrolling enabled	
10397	Informational	Continuous patrolling disabled	
10398	Major	MDC finished with errors on logical drive [..]	1. Manually initiate second consistency check (MDC). 2. If problem persists replace affected disk.
10399	Informational	Logical drive [..] disabled because RAID-5 is not supported by this RAID key	
10400	Informational	Logical drive [..] disabled because RAID-6 is not supported by this RAID key	
10401	Minor	Logical drive [..] disabled because SAS drives are not supported by this RAID key	Check the disks.
10402	Minor	Disks missing	Check your RAID configuration.
10403	Informational	Rebuild rate changed to [..] percent	
10404	Informational	Consistency check rate changed to [..] percent	
10405	Informational	SMART poll interval changed to [..] s	
10406	Informational	MDC started on logical drive [..]	

10407	Informational	MDC finished on logical drive [..]	
10408	Major	MDC failed on logical drive [..]	1. Manually initiate second consistency check (MDC). 2. If problem persists replace affected disk.
10409	Minor	MDC aborted on logical drive [..]	For information only.
10410	Informational	MDC suspended on logical drive [..]	
10411	Informational	MDC started on uninitialized logical drive [..]	
10412	Minor	State change on logical drive [..] from operational to degraded	Replace affected disk.
10413	Minor	State change on logical drive [..] from operational to partially degraded	Replace affected disk.
10414	Critical	State change on logical drive [..] from operational to failed	1. Check version of RAID controller/iRMC firmware, and BIOS.
10415	Informational	State change on logical drive [..] from degraded to operational	
10416	Minor	State change on logical drive [..] from degraded to degraded	Call your local Fujitsu Helpdesk.
10417	Minor	State change on logical drive [..] from degraded to partially degraded	For information only.
10418	Critical	State change on logical drive [..] from degraded to failed	1. Replace affected disks. 2. The array has to be recreated. Note: Data loss is probable.
10419	Informational	State change on logical drive [..] from partially degraded to operational	
10420	Minor	State change on logical drive [..] from partially degraded to degraded	Replace affected disk.
10421	Minor	State change on logical drive [..] from partially degraded to partially degraded	Call your local Fujitsu Helpdesk.
10422	Critical	State change on logical drive [..] from partially degraded to failed	1. Replace affected disks. 2. The array has to be recreated. Note: Data loss is probable.
10423	Informational	State change on logical drive [..] from failed to operational	
10424	Minor	State change on logical drive [..] from failed to degraded	For information only.
10425	Minor	State change on logical drive [..] from failed to partially degraded	For information only.
10426	Critical	State change on logical drive [..] from failed to failed	Call your local Fujitsu Helpdesk.
10427	Critical	State change by user on disk ([..]) from available to failed	For information only.

10428	Informational	State change by user on disk ([..]) from available to hot spare	
10429	Informational	State change by user on disk ([..]) from available to rebuilding	
10430	Informational	State change by user on disk ([..]) from available to operational	
10431	Informational	State change by user on disk ([..]) from failed to available	
10432	Critical	State change by user on disk ([..]) from failed to failed	For information only.
10433	Informational	State change by user on disk ([..]) from failed to hot spare	
10434	Informational	State change by user on disk ([..]) from failed to rebuilding	
10435	Informational	State change by user on disk ([..]) from failed to operational	
10436	Informational	State change by user on disk ([..]) from hot spare to available	
10437	Critical	State change by user on disk ([..]) from hot spare to failed	For information only.
10438	Informational	State change by user on disk ([..]) from hot spare to hot spare	
10439	Informational	State change by user on disk ([..]) from hot spare to rebuilding	
10440	Informational	State change by user on disk ([..]) from hot spare to operational	
10441	Informational	State change by user on disk ([..]) from rebuilding to available	
10442	Critical	State change by user on disk ([..]) from rebuilding to failed	For information only.
10443	Informational	State change by user on disk ([..]) from rebuilding to hot spare	
10444	Informational	State change by user on disk ([..]) from rebuilding to rebuilding	
10445	Informational	State change by user on disk ([..]) from rebuilding to operational	
10446	Informational	State change by user on disk ([..]) from operational to available	
10447	Critical	State change by user on disk ([..]) from operational to failed	For information only.
10448	Informational	State change by user on disk ([..]) from operational to hot spare	
10449	Informational	State change by user on disk ([..]) from operational to rebuilding	
10450	Informational	State change by user on disk ([..]) from operational to operational	

10451	Critical	State change on disk ([..]) from available to failed	Replace affected disk.
10452	Informational	State change on disk ([..]) from available to hot spare	
10453	Informational	State change on disk ([..]) from available to rebuilding	
10454	Informational	State change on disk ([..]) from available to operational	
10455	Informational	State change on disk ([..]) from failed to available	
10456	Critical	State change on disk ([..]) from failed to failed	Call your local Fujitsu Helpdesk.
10457	Informational	State change on disk ([..]) from failed to hot spare	
10458	Informational	State change on disk ([..]) from failed to rebuilding	
10459	Informational	State change on disk ([..]) from failed to operational	
10460	Informational	State change on disk ([..]) from hot spare to available	
10461	Critical	State change on disk ([..]) from hot spare to failed	Replace affected disk.
10462	Informational	State change on disk ([..]) from hot spare to hot spare	
10463	Informational	State change on disk ([..]) from hot spare to rebuilding	
10464	Informational	State change on disk ([..]) from hot spare to operational	
10465	Informational	State change on disk ([..]) from rebuilding to available	
10466	Critical	State change on disk ([..]) from rebuilding to failed	1. Manually initiate a second rebuild (e.g. via ServerView RAID Manager). 2. If problem persists replace affected disk.
10467	Informational	State change on disk ([..]) from rebuilding to hot spare	
10468	Informational	State change on disk ([..]) from rebuilding to rebuilding	
10469	Informational	State change on disk ([..]) from rebuilding to operational	
10470	Informational	State change on disk ([..]) from operational to available	
10471	Critical	State change on disk ([..]) from operational to failed	Replace affected disk.

10472	Informational	State change on disk ([..]) from operational to hot spare	
10473	Informational	State change on disk ([..]) from operational to rebuilding	
10474	Informational	State change on disk ([..]) from operational to operational	
10475	Major	MDC detected uncorrectable multiple medium errors (disk ([..]) at LBA [..] on logical drive [..])	Replace affected disk.
10476	Major	Disk ([..]) missing after reboot	Check your RAID configuration.
10477	Major	Logical drive [..] missing after reboot	Check your RAID configuration.
10478	Informational	Disk ([..]) appeared new after reboot	
10479	Informational	Logical drive [..] appeared new after reboot	
10480	Major	Puncturing of LBAs enabled	Call your local Fujitsu Helpdesk.
10481	Major	Puncturing of LBAs disabled	Call your local Fujitsu Helpdesk.
10482	Critical	Enclosure [..] I/O module [..] not installed	Call your local Fujitsu Helpdesk.
10483	Informational	Package version [..]	
10484	Informational	Media verification corrected error (logical drive [..] at LBA [..] on disk ([..]) at LBA [..])	
10485	Minor	State change on disk ([..]) from available to offline	For information only.
10486	Minor	State change by user on disk ([..]) from available to offline	For information only.
10487	Minor	State change by user on disk ([..]) from failed to offline	For information only.
10488	Minor	State change by user on disk ([..]) from hot spare to offline	For information only.
10489	Informational	State change by user on disk ([..]) from offline to available	
10490	Critical	State change by user on disk ([..]) from offline to failed	For information only.
10491	Informational	State change by user on disk ([..]) from offline to hot spare	
10492	Minor	State change by user on disk ([..]) from offline to offline	For information only.
10493	Informational	State change by user on disk ([..]) from offline to operational	
10494	Informational	State change by user on disk ([..]) from offline to rebuilding	
10495	Minor	State change by user on disk ([..]) from operational to offline	For information only.
10496	Minor	State change by user on disk ([..]) from rebuilding to offline	For information only.

10497	Minor	State change on disk ([..]) from failed to offline	For information only.
10498	Minor	State change on disk ([..]) from hot spare to offline	1. Manually set the disk to hot spare again (e.g. via ServerView RAID Manager). 2. If problem persists replace affected disk.
10499	Informational	State change on disk ([..]) from offline to available	
10500	Critical	State change on disk ([..]) from offline to failed	Replace affected disk.
10501	Informational	State change on disk ([..]) from offline to hot spare	
10502	Minor	State change on disk ([..]) from offline to offline	For information only.
10503	Informational	State change on disk ([..]) from offline to operational	
10504	Informational	State change on disk ([..]) from offline to rebuilding	
10505	Minor	State change on disk ([..]) from operational to offline	Note: Only informational if status change was forced by user otherwise: 1. Replace affected disk.
10506	Minor	State change on disk ([..]) from rebuilding to offline	Note: Only informational if status change was forced by user otherwise: 1. Replace affected disk.
10507	Informational	Data in cache flushed during power up	
10508	Major	Data in cache not flushed during power up	If the problem occurs repeatedly call your local Fujitsu Helpdesk.
10509	Informational	Rebuild resumed on disk ([..])	
10510	Informational	Automatic rebuild started on logical drive [..]	
10511	Informational	BGI restarted on logical drive [..]	
10512	Major	Logical drive [..]: Error on disk [..] [..]	Replace affected disk.
10513	Informational	Rebuild on logical drive [..] resumed	
10514	Major	Consistency check finished with errors on logical drive [..]: [..]	1. Manually initiate second consistency check (MDC). 2. If problem persists backup data from affected logical drive. 3. Delete and recreate affected logical drive. 4. Restore data.
10515	Major	Error on logical drive [..] detected	1. Check/replace cable between controller and affected disk. 2. If problem persists replace disk.

10516	Major	Disk ([..]) forced from failed to online	For information only.
10517	Minor	Transfer speed of disk ([..]) changed	1. Check/replace cable between controller and affected disk. 2. If problem persists replace disk.
10518	Major	SAS port ([..]) lost link	1. Unplug affected disk, wait 30 seconds, reinsert it. 2. Check/replace cable between controller and affected disk. 3. Check version of RAID controller/iRMC firmware, and BIOS. 4. Replace affected disk.
10519	Informational	SAS port ([..]) restored link	
10520	Informational	Cache mode changed to Write-back	
10521	Informational	Cache mode changed to Write-through	
10522	Minor	Global affinity hot spare ([..]) commissioned in a different enclosure	Check your RAID configuration.
10523	Minor	Foreign configuration table overflow	Call your local Fujitsu Helpdesk.
10524	Minor	Partial foreign configuration imported, disks not imported (device numbers): ([..])	Note: Only parts of your config were imported. 1. Call your local Fujitsu Helpdesk.
10525	Informational	Connector ([..]) is active	
10526	Critical	Adapter missing after reboot	Note: Only informational if controller was removed by user otherwise: 1. Unplug affected controller, wait 30 seconds, reinsert it. 2. If problem persists replace affected controller. 3. If problem persists replace mainboard.
10527	Informational	Adapter appeared new after reboot	
10528	Minor	Rebuild aborted on disk ([..])	Note: Only informational if rebuild was aborted by user otherwise: 1. Initiate a rebuild again (e.g. via ServerView RAID Manager).
10529	Major	Consistency check finished with ([..]) correctable errors on logical drive ([..])	1. Manually initiate second consistency check (MDC). 2. If problem persists backup data from affected logical drive. 3. Delete and recreate affected logical drive. 4. Restore data.

10530	Major	Consistency check finished with [...] uncorrectable errors on logical drive [...]	1. Backup data from affected logical drive. 2. Delete and recreate affected logical drive. 3. Restore data.
10531	Informational	MDC finished with [...] correctable errors on logical drive [...]	
10532	Major	MDC finished with [...] uncorrectable errors on logical drive [...]	1. Backup data from affected logical drive. 2. Delete and recreate affected logical drive. 3. Restore data.
10533	Informational	Error counters reset on disk ([...])	
10534	Minor	Changed adapter property detected after reboot	Check your adapter properties (e.g. via ServerView RAID Manager).
10535	Informational	Board revision [...]	
10536	Minor	Command timeout on disk ([...]), CDB:[...]	Note: Only if problem occurs repeatedly: 1. Check/replace cable between controller and affected disk. 2. If problem persists replace affected disk and/or backplane.
10537	Minor	Disk ([...]) reset (type [...])	Note: Only if problem occurs repeatedly: 1. Check/replace cable between controller and affected disk. 2. If problem persists replace affected disk.
10538	Minor	Bad block table on logical drive [...] is 80 percent full	Check for additional error messages for affected disk.
10539	Major	Bad block table on logical drive [...] is full; unable to log LBA [...] (on disk ([...]) at LBA [...])	Check for additional error messages for affected disk.
10540	Major	Uncorrectable medium error logged for logical drive [...] at LBA [...] (on disk ([...]) at LBA [...])	Check for additional error messages for affected disk.
10541	Informational	Medium error corrected on logical drive [...] at LBA [...]	Check for additional error messages for affected disk.
10542	Minor	Bad block table on disk ([...]) is 100 percent full	Replace affected disk.
10543	Minor	Bad block table on logical drive [...] is 100 percent full	Check for additional error messages for affected disk.
10544	Critical	Adapter needs replacement, faulty IOP detected	1. Replace affected RAID controller.
10545	Informational	Copyback started on disk ([...]) from disk ([...])	
10546	Informational	Copyback aborted on disk ([...]) from disk ([...])	

10547	Informational	Copyback complete on disk ([..]) from disk ([..])	
10548	Informational	Copyback progress on disk ([..]) is [..]	
10549	Informational	Copyback resumed on disk ([..])	
10550	Informational	Copyback automatically started on disk ([..])	
10551	Major	Copyback failed on disk ([..])	Check for additional error messages for affected disk.
10552	Minor	Early power off warning was unsuccessful	Call your local Fujitsu Helpdesk.
10553	Informational	BBU FRU is [..]	
10554	Informational	Disk ([..]) FRU is [..]	
10555	Informational	Adapter hardware revision ID [..]	
10556	Minor	Foreign configuration metadata needs to be upgraded, may become incompatible	For information only.
10557	Informational	BIOS continue on error enabled	
10558	Informational	BIOS continue on error disabled	
10559	Informational	Additional information for failed disk ([..]) - firmware version: [..], serial number [..], first use: [..], total running time: [..] days	
10560	Informational	If the logical size of logical drive [..] has changed use appropriate operating system tool to reread disk information	
10561	Informational	Enclosure device exposure changed	
10562	Informational	Abort consistency check on error changed	
10563	Informational	Abort MDC on error changed	
10564	Informational	Redundant path restored for disk ([..])	
10565	Minor	Redundant path broken for disk ([..])	Call your local Fujitsu Helpdesk.
10566	Informational	Redundant enclosure I/O module [..] inserted for I/O module [..]	
10567	Minor	Redundant enclosure I/O module [..] removed for I/O module [..]	Call your local Fujitsu Helpdesk.
10568	Minor	Patrol Read can't be started, all disks are either not online, or are in a logical drive with an active process, or are in an excluded logical drive	For information only.
10569	Informational	Copyback aborted by user on disk ([..]) from disk ([..])	
10570	Major	Copyback aborted on hot spare ([..]) from disk ([..]) as hot spare needed for rebuild	Call your local Fujitsu Helpdesk.
10571	Minor	Copyback aborted on disk ([..]) from disk ([..]) as rebuild required in the array	Call your local Fujitsu Helpdesk.
10572	Major	Cache discarded for logical drive (missing or offline) [..]	For information only.
10573	Informational	Redundancy building started on disk ([..])	

10574	Informational	Redundancy building finished on disk ([..])	
10575	Major	Redundancy building failed on disk ([..])	Call your local Fujitsu Helpdesk.
10576	Minor	Redundancy building aborted on disk ([..])	Call your local Fujitsu Helpdesk.
10577	Informational	Redundancy building suspended on disk ([..])	
10578	Informational	Disk ([..]) power management idle mode enabled	
10579	Informational	Disk ([..]) power management idle mode disabled	
10580	Informational	Disk ([..]) power management idle condition timer changed	
10581	Informational	Disk ([..]) power management standby mode enabled	
10582	Informational	Disk ([..]) power management standby mode disabled	
10583	Informational	Disk ([..]) power management standby condition timer changed	
10584	Informational	Copyback cannot be started as disk ([..]) is too small for disk ([..])	
10585	Informational	Copyback cannot be started on disk ([..]) from disk ([..]) as SAS/SATA mixing is not supported in an array	
10586	Informational	Firmware update started on disk ([..])	
10587	Informational	Firmware update completed on disk ([..])	
10588	Minor	Firmware update timeout on disk ([..])	Call your local Fujitsu Helpdesk.
10589	Minor	Firmware update failed on disk ([..])	Call your local Fujitsu Helpdesk.
10590	Informational	Adapter properties changed	
10591	Informational	Patrol Read properties changed	
10592	Informational	MDC schedule properties changed	
10593	Informational	BBU properties changed	
10594	Informational	MDC resumed on logical drive [..]	
10595	Informational	Spindown mode enabled	
10596	Informational	Spindown mode disabled	
10597	Informational	Spindown delay changed to [..] seconds	
10598	Informational	Spinup delay changed to [..] seconds	
10599	Informational	Redundancy build rate changed to [..] percent	
10600	Informational	Copyback rate changed to [..] percent	
10601	Minor	Periodic BBU relearn is pending. Please initiate manual learn cycle as automatic learn is not enabled	Initiate manual learn cycle as automatic learn is not enabled.
10602	Informational	Disk security key created	

10603	Informational	Disk security key backed up	
10604	Informational	Disk security key from escrow, verified	
10605	Informational	Disk security key changed	
10606	Minor	Disk security key, re-key operation failed	Call your local Fujitsu Helpdesk.
10607	Minor	Disk security key is invalid	Call your local Fujitsu Helpdesk.
10608	Informational	Disk security key destroyed	
10609	Minor	Disk security key from escrow is invalid	Call your local Fujitsu Helpdesk.
10610	Informational	Logical drive [...] is now secured	
10611	Minor	Logical drive [...] is partially secured	For information only.
10612	Informational	Disk ([...]) security activated	
10613	Informational	Disk ([...]) security disabled	
10614	Informational	Disk ([...]) is reprovisioned	
10615	Informational	Disk ([...]) security key changed	
10616	Major	Security subsystem problems detected for disk ([...])	Call your local Fujitsu Helpdesk.
10617	Major	Adapter cache preserved for missing or offline logical drive [...]	Check error messages for related logical drive and resolve problems.
10618	Major	Adapter cache preserved for missing or offline logical drives	Check error messages for related logical drives and resolve problems.
10619	Informational	Adapter cache discarded by user for logical drives	
10620	Informational	Adapter cache destaged for logical drive [...]	
10621	Minor	MDC started on an inconsistent logical drive [...]	For information only.
10622	Minor	Disk security key failure, cannot access secured configuration	Call your local Fujitsu Helpdesk.
10623	Minor	Disk security pass phrase from user is invalid	Call your local Fujitsu Helpdesk.
10624	Informational	Complete RAID configuration written to file '[...]' on the server	
10625	Minor	Abnormal shutdown sequence detected	
10626	Major	Internal hardware error	Call your local Fujitsu Helpdesk.
10627	Major	Internal hardware error during POST	Call your local Fujitsu Helpdesk.
10628	Informational	Bad block table of disk ([...]) threshold exceeded; table is about to overflow	
10629	Informational	Bad block table of disk ([...]) cleared	
10630	Critical	Disk ([...]) failed due to bad block table overflow	Replace affected disk.
10631	Critical	Disk ([...]) failure detected during POST	Replace affected disk.
10632	Critical	Failure detected during POST	Call your local Fujitsu Helpdesk.

10633	Critical	Multiple failure on disk ([..]) detected, internal info [..]	Replace affected disk.
10634	Informational	BGI started due to adapter exchange	
10635	Critical	Disk ([..]) failure detected by Patrol Read	Replace affected disk.
10636	Critical	Disk ([..]) failure detected after successfully building redundancy	Replace affected disk.
10637	Critical	Disk ([..]) failure detected after aborting building redundancy	Replace affected disk.
10638	Critical	Disk ([..]) failed	Replace affected disk.
10639	Critical	Disk ([..]) failed, internal info [..]	Replace affected disk.
10640	Informational	Adapter [..] was exchanged	
10641	Informational	Firmware upload started	
10642	Informational	Firmware upload is executing	
10643	Informational	Save configuration	
10644	Informational	Arrays [..] created	
10645	Informational	Arrays [..] deleted	
10646	Informational	Trace mode changed	
10647	Informational	Panic dump data deleted	
10648	Informational	Panic forced	
10649	Informational	Startup script set	
10650	Informational	EXBIOS parameter changed	
10651	Informational	Auto offline recovery mode changed	
10652	Informational	Clock time changed	
10653	Informational	Factory shipment settings restored	
10654	Informational	Internal log cleared	
10655	Informational	NVRAM log cleared	
10656	Informational	Unique key refreshed	
10657	Informational	Write check parameter changed	
10658	Minor	Operation failed	1. Replace affected RAID controller.
10659	Informational	New firmware version [..] detected	
10660	Minor	Array [..] without logical drive left	There is an array which has no logical drive. Create a logical drive to use the array.
10661	Minor	Incorrect calendar parameter detected	Check the scheduler settings.
10662	Major	Copyback on logical drive [..] aborted due to bad block table overflow	A large number of uncorrectable bad blocks were detected on logical drive. 1. Restore last good data.

10663	Major	Redundant copy on logical drive [...] aborted due to bad block table overflow	A large number of uncorrectable bad blocks were detected on logical drive. 1. Restore last good data.
10664	Informational	Bad block table expansion area initialized	
10665	Informational	Bad block table expansion area initialization failed	
10666	Informational	Disk error detected by write data on logical drive [...] during redundant copy	
10667	Minor	Bad block detected on disk ([...]), [...]	For information only.
10668	Informational	Multiple failure recovery on disk ([...]) successful	
10669	Informational	Hot spare available	
10670	Informational	Patrol Read (one cycle) started on disk ([...])	
10671	Informational	Patrol Read (one cycle) finished on disk ([...])	
10672	Minor	Error detected on disk ([...]), [...]	For information only.
10673	Informational	Error recovered on disk ([...]), [...]	
10674	Informational	Media error recovered on disk ([...]) by reassigning new block	
10675	Minor	Disk location in logical drive changed from port [...] to port [...]	For information only.
10676	Informational	Disk increased by cold swap on port [...]	
10677	Informational	Disk decreased by cold swap on port [...]	
10678	Informational	Disk exchanged by cold swap on port [...]	
10679	Informational	SAS interface rate changed on port [...]	
10680	Minor	Driver error	Check the driver version.
10681	Informational	Copyback started on disk ([...])	
10682	Minor	Copyback aborted on disk ([...])	For information only.
10683	Informational	Copyback complete on disk ([...])	
10684	Minor	Internal hardware error	1. Replace affected RAID controller.
10685	Major	Internal hardware error	1. Replace affected RAID controller.
10686	Major	Disk ([...]) bad block table overflow error	A large number of uncorrectable bad blocks were detected on the disk. 1. Restore last good data.
10687	Minor	Error with the remote BBU connector cable detected	Replace the BBU data/power cable.
10688	Critical	Multiple failure on disk ([...]) detected during POST, internal info [...]	1. Replace affected disk. 2. Replace affected backplane or the data cable.

10689	Critical	Disk ([..]) failed due to SAS/SATA interface error rate too high	1. Replace affected disk. 2. Replace affected backplane or the data cable.
10690	Informational	Operation to mark disk ([..]) offline (redundant copy) started	
10691	Informational	RAID migration registered for logical drive [..]	
10692	Informational	MDC aborted by user on logical drive [..]	
10693	Informational	Alarm set	
10694	Major	Logical drive [..] degraded due to bad block table overflow	A large number of uncorrectable bad blocks were detected on the disk. 1. Restore last good data.
10695	Critical	Disk ([..]) failed due to write error detection by driver	Replace affected disk.
10696	Minor	Abnormal capacity of disk ([..]) in logical drive detected	Check the array configuration.
10697	Minor	Illegal type of disk ([..]) in logical drive detected	Check the array configuration.
10698	Informational	Background recovery of logical drive [..] could not be started due to bad block table overflow	
10699	Informational	New hot spare ([..]) detected	
10700	Major	Internal PCI hardware error	Replace affected RAID controller.
10701	Minor	Bad block table was updated by disk ([..])	For information only.
10702	Minor	Invalid disk on port [..] during start up detected	For information only.
10703	Minor	Invalid disk on port [..] during hot swap detected	For information only.
10704	Minor	SMART error on disk ([..]) because internal error threshold on adapter is exceeded	Note: Disk reports a prefailure. The affected disk might fail soon. 1. Replace the disk during next maintenance.
10705	Minor	Firmware and driver version mismatch	Check the driver and firmware version.
10706	Informational	Reset received	
10707	Informational	Operation to mark disk ([..]) offline started	
10708	Informational	Operation to delete arrays [..] started	
10709	Informational	Operation to delete logical drive [..] started	
10710	Informational	Operation to delete global hot spare on disk ([..]) started	
10711	Critical	Disk ([..]) failed since it never entered ready state, [..]	Replace affected disk.

10712	Minor	Internal software interface error (function: [..])	Note: The driver encountered an error. 1. Check the status of the operating system. 2. Reboot your system.
10713	Minor	Device open error (device: [..])	Note: The driver encountered an error. 1. Check the status of the operating system. 2. Reboot your system.
10714	Minor	loctl send error (details: [..])	Note: The driver encountered an error. 1. Check the status of the operating system. 2. Reboot your system.
10715	Minor	Insufficient application memory (function: [..])	Note: The driver encountered an error. 1. Check the status of the operating system. 2. Reboot your system.
10716	Minor	System API error (code: [..], function/item: [..])	Note: The driver encountered an error. 1. Check the status of the operating system. 2. Reboot your system.
10717	Critical	Firmware initialization failed	1. Replace affected RAID controller.
10718	Critical	Firmware recovery failed	1. Replace affected RAID controller.
10719	Informational	loctl busy	
10720	Informational	Logical drive number for boot changed to [..]	
10721	Informational	Power state change on disk ([..]) from active to stopped	
10722	Informational	Power state change on disk ([..]) from stopped to active	
10723	Informational	Enclosure [..] element (SES code [..]) status changed	
10724	Informational	Firmware upload process finished	
10725	Informational	Disk firmware update process started	
10726	Informational	Disk firmware update process finished	
10727	Informational	Difference in time information changed	
10728	Informational	Factory shipment settings initialized	

10729	Minor	BBU requires reconditioning; please initiate recalibration	1. Initiate manual recalibration process (e.g. via ServerView RAID Manager). Note: Do not interrupt the charging process by reboots or shutdowns. 2. If problem persists replace BBU.
10730	Informational	Disk ([..]) rebuild not possible as HDD/SSD mix is not supported in an array	
10731	Informational	Copyback cannot be started on disk ([..]) from disk ([..]), as HDD/SSD mix is not supported in an array	
10732	Minor	Task [..] for object [..] cannot be started (error [..]). The scheduler will try to start the task again later	Check the error code. Then check the controller settings, scheduler settings and disk/logical drive/BBU status.
10733	Informational	Task [..] for object [..] was started by scheduler	
10734	Major	Task [..] for object [..] cannot be started (error [..]). The scheduler has disabled the task	Check the error code. Then check the controller settings, scheduler settings and disk/logical drive/BBU status.
10735	Informational	Bad block table of logical drive [..] cleared	
10736	Major	SAS topology error: [..]	1. Unplug affected disk, wait 30 seconds, reinsert it. 2. Replace affected disk. 3. Replace affected backplane or the data cable.
10737	Minor	BBU required reconditioning; recalibration initiated	For information only.
10738	Minor	Task [..] for object [..] could not be started at the normal execution time because the service or system was down	Check the scheduler settings.
10739	Minor	Task [..] for object [..] cannot be started (error [..]). The task will be set to the next regular execution time	Check the error code. Then check the controller settings, scheduler settings and disk/logical drive/BBU status.
10740	Informational	Cluster of medium errors corrected for logical drive [..] at [..] (on disk [..] at [..])	
10741	Informational	Host bus rescan requested	
10742	Informational	Adapter repurposed and factory defaults restored	
10743	Informational	Disk security key binding updated	
10744	Informational	State change on disk ([..]) from available to copyback	
10745	Informational	State change on disk ([..]) from available to JBOD	

10746	Informational	State change on disk ([..]) from failed to copyback	
10747	Informational	State change on disk ([..]) from failed to JBOD	
10748	Informational	State change on disk ([..]) from hot spare to copyback	
10749	Informational	State change on disk ([..]) from hot spare to JBOD	
10750	Informational	State change on disk ([..]) from rebuilding to copyback	
10751	Informational	State change on disk ([..]) from rebuilding to JBOD	
10752	Informational	State change on disk ([..]) from operational to copyback	
10753	Informational	State change on disk ([..]) from operational to JBOD	
10754	Informational	State change on disk ([..]) from copyback to available	
10755	Critical	State change on disk ([..]) from copyback to failed	Replace affected disk.
10756	Informational	State change on disk ([..]) from copyback to hot spare	
10757	Minor	State change on disk ([..]) from copyback to offline	For information only.
10758	Informational	State change on disk ([..]) from copyback to operational	
10759	Informational	State change on disk ([..]) from copyback to rebuilding	
10760	Informational	State change on disk ([..]) from copyback to copyback	
10761	Informational	State change on disk ([..]) from copyback to JBOD	
10762	Informational	State change on disk ([..]) from JBOD to available	
10763	Critical	State change on disk ([..]) from JBOD to failed	Replace affected disk.
10764	Informational	State change on disk ([..]) from JBOD to hot spare	
10765	Minor	State change on disk ([..]) from JBOD to offline	For information only.
10766	Informational	State change on disk ([..]) from JBOD to operational	
10767	Informational	State change on disk ([..]) from JBOD to rebuilding	
10768	Informational	State change on disk ([..]) from JBOD to copyback	

10769	Informational	State change on disk ([..]) from JBOD to JBOD	
10770	Informational	State change by user on disk ([..]) from available to copyback	
10771	Informational	State change by user on disk ([..]) from available to JBOD	
10772	Informational	State change by user on disk ([..]) from failed to copyback	
10773	Informational	State change by user on disk ([..]) from failed to JBOD	
10774	Informational	State change by user on disk ([..]) from hot spare to copyback	
10775	Informational	State change by user on disk ([..]) from hot spare to JBOD	
10776	Informational	State change by user on disk ([..]) from rebuilding to copyback	
10777	Informational	State change by user on disk ([..]) from rebuilding to JBOD	
10778	Informational	State change by user on disk ([..]) from operational to copyback	
10779	Informational	State change by user on disk ([..]) from operational to JBOD	
10780	Informational	State change by user on disk ([..]) from copyback to available	
10781	Critical	State change by user on disk ([..]) from copyback to failed	Replace affected disk.
10782	Informational	State change by user on disk ([..]) from copyback to hot spare	
10783	Minor	State change by user on disk ([..]) from copyback to offline	For information only.
10784	Informational	State change by user on disk ([..]) from copyback to operational	
10785	Informational	State change by user on disk ([..]) from copyback to rebuilding	
10786	Informational	State change by user on disk ([..]) from copyback to copyback	
10787	Informational	State change by user on disk ([..]) from copyback to JBOD	
10788	Informational	State change by user on disk ([..]) from JBOD to available	
10789	Critical	State change by user on disk ([..]) from JBOD to failed	For information only.
10790	Informational	State change by user on disk ([..]) from JBOD to hot spare	
10791	Minor	State change by user on disk ([..]) from JBOD to offline	For information only.

10792	Informational	State change by user on disk ([..]) from JBOD to operational	
10793	Informational	State change by user on disk ([..]) from JBOD to rebuilding	
10794	Informational	State change by user on disk ([..]) from JBOD to copyback	
10795	Informational	State change by user on disk ([..]) from JBOD to JBOD	
10796	Informational	State change on disk ([..]) from offline to copyback	
10797	Informational	State change by user on disk ([..]) from offline to copyback	
10798	Informational	State change on disk ([..]) from offline to JBOD	
10799	Informational	State change by user on disk ([..]) from offline to JBOD	
10800	Informational	Disk security is in external key management mode	
10801	Minor	Disk security failed to communicate with external key management system	Call your local Fujitsu Helpdesk.
10802	Informational	Disk ([..]) needs key to be [..] [..]	
10803	Minor	Logical drive [..] secure failed	For information only.
10804	Major	Controller encountered a fatal error and was reset	1. Replace affected RAID controller.
10805	Major	Configuration command could not be committed to disk, please retry	Call your local Fujitsu Helpdesk.
10806	Informational	COD on disk ([..]) updated as it was stale	
10807	Minor	Power state change failed on disk ([..]) (from active to stopped)	Replace affected disk.
10808	Minor	Power state change failed on disk ([..]) (from stopped to active)	Replace affected disk.
10809	Minor	Logical drive [..] is not ready	For information only.
10810	Informational	Logical drive [..] is ready	
10811	Informational	Test E-mail was sent successfully	
10812	Minor	Adapter has been replaced during reboot	For information only.
10813	Minor	Enclosure [..] power supply [..] removed	For information only.
10814	Minor	Enclosure [..] power supply [..] turned off	For information only.
10815	Informational	Enclosure [..] power supply [..] inserted	
10816	Informational	Enclosure [..] power supply [..] turned on	
10817	Minor	Enclosure [..] temperature sensor [..] below warning threshold	1. Check environmental temperature.
10818	Major	Enclosure [..] temperature sensor [..] below error threshold	1. Check environmental temperature.

10819	Minor	Enclosure [...] temperature sensor [...] above warning threshold	1. Check installation of all air flow channels, closed housing, and unblocked louvers. 2. Check environmental temperature.
10820	Major	Enclosure [...] temperature sensor [...] above error threshold	1. Check installation of all air flow channels, closed housing, and unblocked louvers. 2. Check environmental temperature.
10821	Informational	Power state change on disk ([...]) from active to transition	
10822	Minor	Power state change failed on disk ([...]) (from active to transition)	Replace affected disk.
10823	Informational	Power state change on disk ([...]) from stopped to transition	
10824	Minor	Power state change failed on disk ([...]) (from stopped to transition)	Replace affected disk.
10825	Informational	Power state change on disk ([...]) from transition to active	
10826	Minor	Power state change failed on disk ([...]) (from transition to active)	Replace affected disk.
10827	Informational	Power state change on disk ([...]) from transition to stopped	
10828	Minor	Power state change failed on disk ([...]) (from transition to stopped)	Replace affected disk.
10829	Minor	Reset on-board expander	For information only.
10830	Informational	Enclosure [...] temperature sensor [...] temperature increase detected	For information only.
10831	Informational	Enclosure [...] temperature sensor [...] temperature drop detected	For information only.
10832	Informational	Enclosure [...] fan [...] speed changed to low	
10833	Informational	Enclosure [...] fan [...] speed changed to medium	
10834	Informational	Enclosure [...] fan [...] speed changed to high	
10835	Informational	Disk ([...]) will be set offline due to SAS/SATA interface error rate too high	
10836	Informational	Write cache on disk ([...]) enabled	
10837	Informational	Write cache on disk ([...]) disabled	
10838	Informational	Native Command Queuing (NCQ) on disk ([...]) enabled	
10839	Informational	Native Command Queuing (NCQ) on disk ([...]) disabled	
10840	Informational	Automatic rebuild will use hot spares	
10841	Informational	Automatic rebuild will use available disks and hot spares	

10842	Informational	Patrol Read rate changed	
10843	Informational	Migration rate changed	
10844	Informational	Initialization rate changed	
10845	Informational	Consistency check resumed on logical drive [...]	
10846	Minor	Consistency check rejected on uninitialized logical drive [...]	Initiate manual MDC to initialize the logical drive.
10847	Informational	Initialization suspended on logical drive [...]	
10848	Informational	Initialization resumed on logical drive [...]	
10849	Informational	Logical drive [...] is used for CacheCade with capacity [...] MB	
10850	Informational	Logical drive [...] is using CacheCade [...]	
10851	Informational	Logical drive [...] is no longer using CacheCade [...]	
10852	Minor	CacheCade [...] capacity changed and is now [...] MB	For information only.
10853	Minor	BBU life has degraded and cannot initiate transparent learn cycles	1. Initiate manual relearn cycle. 2. If problem persists replace BBU.
10854	Informational	MegaRAID Advanced Software Options ([...]) key applied	
10855	Informational	MegaRAID Advanced Software Options ([...]) key transferred	
10856	Informational	MegaRAID Advanced Software Options serial number [...]	
10857	Minor	MegaRAID Advanced Software Options serial number mismatch. Key Vault serial number is [...]	Controller serial number does not match with MegaRAID Advanced Software Options key. Apply key to appropriate controller.
10858	Minor	BBU cannot support data retention for more than [...] hours	BBU capacity is decreased and buffering of data in controller cache is limited. To reach full data retention time replace BBU.
10859	Informational	Logical drive [...]: [...] changed	
10860	Minor	Logical drive [...] cannot transition to maximum power savings	For information only.
10861	Informational	Driver is loaded and operational	
10862	Informational	Logical drive [...] mirror broken	
10863	Informational	Logical drive [...] mirror joined	

10864	Minor	Disk ([..]) link [..] failed in SAS wide port	1. Unplug affected disk, wait 30 seconds, reinsert it. 2. Check/replace cable between controller and affected disk. 3. Check version of RAID controller/iRMC firmware, and BIOS. 4. Replace affected disk.
10865	Informational	Disk ([..]) link [..] restored in SAS wide port	
10866	Informational	Memory module FRU is [..]	
10867	Minor	FBU power pack is sub-optimal	1. Replace FBU.
10868	Minor	Foreign configuration auto-import did not import any drives	Attempt to import a foreign config failed. 1. Call your local Fujitsu Helpdesk.
10869	Minor	FBU firmware update required	1. Call your local Fujitsu Helpdesk.
10870	Minor	CacheCade [..] capacity exceeds maximum allowed size, extra capacity is not used	Call your local Fujitsu Helpdesk.
10871	Minor	Logical drive [..] protection information lost	1. Call your local Fujitsu Helpdesk.
10872	Informational	Diagnostics passed for disk ([..])	
10873	Major	Diagnostics failed for disk ([..])	Replace affected disk.
10874	Informational	Server power capability diagnostic test started	
10875	Informational	Disk cache settings enabled during rebuild for disk ([..])	
10876	Informational	Disk cache settings restored after rebuild for disk ([..])	
10877	Informational	Disk ([..]) commissioned as emergency spare	
10878	Minor	Reminder: Potential non-optimal configuration because disk ([..]) is commissioned as emergency spare	For information only.
10879	Informational	BGI suspended on logical drive [..]	
10880	Informational	BGI resumed on logical drive [..]	
10881	Informational	Migration suspended on logical drive [..]	
10882	Informational	Copyback suspended on disk ([..])	
10883	Informational	Reminder: MDC suspended on logical drive [..]	
10884	Informational	Reminder: BGI suspended on logical drive [..]	
10885	Informational	Reminder: Migration suspended on logical drive [..]	
10886	Informational	Reminder: Rebuild suspended on disk ([..])	

10887	Informational	Reminder: Copyback suspended on disk ([..])	
10888	Informational	Reminder: Patrol Read suspended	
10889	Informational	Erase aborted on disk ([..])	
10890	Major	Erase failed on disk ([..]) (error [..])	1. Call your local Fujitsu Helpdesk.
10891	Informational	Erase progress on disk ([..]) is [..]	
10892	Informational	Erase started on disk ([..])	
10893	Informational	Erase finished on disk ([..])	
10894	Informational	Erase aborted on logical drive [..]	
10895	Major	Erase failed on logical drive [..]	1. Call your local Fujitsu Helpdesk.
10896	Informational	Erase progress on logical drive [..] is [..]	
10897	Informational	Erase started on logical drive [..]	
10898	Informational	Erase finished on logical drive [..]	
10899	Minor	Potential leakage during erase on logical drive [..]	1. Call your local Fujitsu Helpdesk.
10900	Minor	BBU charging was suspended due to high BBU temperature	Bring system back to normal operating temperature.
10901	Informational	FBU firmware update finished	
10902	Minor	FBU firmware update failed	1. Call your local Fujitsu Helpdesk.
10903	Critical	Logical drive [..] access blocked as cached data in CacheCade is unavailable	Call your local Fujitsu Helpdesk.
10904	Informational	CacheCade disassociate started on logical drive [..]	
10905	Informational	CacheCade disassociate finished on logical drive [..]	
10906	Major	CacheCade disassociate failed on logical drive [..]	Call your local Fujitsu Helpdesk.
10907	Informational	CacheCade disassociate progress on logical drive [..] is [..]	
10908	Informational	CacheCade disassociate aborted by user on logical drive [..]	
10909	Minor	Unexpected sense: Disk ([..]), Key/ASC/ASCQ: [..]: [..]	For information only.
10910	Critical	Unexpected sense: Disk ([..]), Key/ASC/ASCQ: [..]: [..]	For information only.
10911	Informational	Rebuild suspended on disk ([..])	
10912	Informational	Rebuild resumed on disk ([..])	
10913	Informational	Link speed changed on SAS port [..] and PHY [..]	

10914	Minor	MegaRAID Advanced Software Options were deactivated for - [...]	Call your local Fujitsu Helpdesk.
10915	Informational	Logical drive [...] is now accessible	
10916	Informational	Logical drive [...] is using CacheCade	
10917	Informational	Logical drive [...] is no longer using CacheCade	
10918	Minor	Patrol Read aborted on disk ([...])	Note: If there are errors directly before or after this event, perform the proper recovery action for that error. 1. For information only.
10919	Minor	Transient error detected while communicating with disk ([...])	Note: Doesn't affect the normal operation of the system, but can lead to degraded performance due to retries. 1. Replace affected disk/backplane/cable at next service.
10920	Informational	Additional information for detected disk ([...]) - firmware version: [...], serial number [...]	
10921	Informational	RAID Manager started	
10922	Informational	RAID Manager stopped	
10923	Informational	State change on disk ([...]) from shielded to available	
10924	Minor	State change on disk ([...]) from shielded to offline	Replace affected disk.
10925	Critical	State change on disk ([...]) from shielded to failed	Replace affected disk.
10926	Informational	State change on disk ([...]) from shielded to hot spare	
10927	Informational	State change on disk ([...]) from shielded to rebuilding	
10928	Informational	State change on disk ([...]) from shielded to operational	
10929	Informational	State change on disk ([...]) from shielded to copyback	
10930	Informational	State change on disk ([...]) from shielded to JBOD	
10931	Critical	State change on disk ([...]) from shielded to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10932	Critical	State change on disk ([...]) from available to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.

10933	Critical	State change on disk ([..]) from offline to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10934	Critical	State change on disk ([..]) from failed to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10935	Critical	State change on disk ([..]) from hot spare to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10936	Critical	State change on disk ([..]) from rebuilding to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10937	Critical	State change on disk ([..]) from operational to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10938	Critical	State change on disk ([..]) from copyback to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10939	Critical	State change on disk ([..]) from JBOD to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10940	Informational	State change by user on disk ([..]) from shielded to available	
10941	Minor	State change by user on disk ([..]) from shielded to offline	Replace affected disk.
10942	Critical	State change by user on disk ([..]) from shielded to failed	Replace affected disk.
10943	Informational	State change by user on disk ([..]) from shielded to hot spare	
10944	Informational	State change by user on disk ([..]) from shielded to rebuilding	
10945	Informational	State change by user on disk ([..]) from shielded to operational	
10946	Informational	State change by user on disk ([..]) from shielded to copyback	
10947	Informational	State change by user on disk ([..]) from shielded to JBOD	
10948	Critical	State change by user on disk ([..]) from shielded to shielded	Replace affected disk.

10949	Critical	State change by user on disk ([..]) from available to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10950	Critical	State change by user on disk ([..]) from offline to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10951	Critical	State change by user on disk ([..]) from failed to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10952	Critical	State change by user on disk ([..]) from hot spare to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10953	Critical	State change by user on disk ([..]) from rebuilding to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10954	Critical	State change by user on disk ([..]) from operational to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10955	Critical	State change by user on disk ([..]) from copyback to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10956	Critical	State change by user on disk ([..]) from JBOD to shielded	1. Wait until checking in shielded state is completed. 2. Perform action according to upcoming status.
10957	Critical	Internal error	If problem persists after reboot, call your local Fujitsu Helpdesk.
10958	Critical	Incompatible PCI slot bandwidth	Reinstall adapter in a compatible PCI slot.
10959	Major	Write performance reduced	Check additional status property for more information.
10960	Major	Write operations disabled	Check additional status property for more information.
10961	Major	Temperature close to error threshold	Increase cooling or reduce write load.
10962	Critical	Temperature above error threshold	Increase cooling or reduce write load.
10963	Critical	Internal voltage out of range	If problem persists after reboot, call your local Fujitsu Helpdesk.
10964	Critical	Auxiliary voltage out of range	If problem persists after reboot, call your local Fujitsu Helpdesk.

10965	Critical	Flashback error	1. Backup data from affected adapter. 2. Replace adapter as soon as possible. 3. Restore data.
10966	Critical	Non-correctable PCI errors detected	If problem persists after reboot, call your local Fujitsu Helpdesk.
10967	Minor	Temperature above warning threshold	Increase cooling or reduce write load.
10968	Minor	Memory is close to wearing out	Formatting to a smaller size will free up reserve.
10969	Minor	Non-optimal PCI slot bandwidth	Reinstall adapter in an optimal PCI slot.
10970	Minor	Correctable PCI errors detected	For information only.
10971	Minor	Power loss protection disabled	Activate power loss protection.
10972	Minor	Write regulation activated due to power constraints of PCI slot	If this condition persists, switch to a higher powered PCI slot or attach external power cable.
10973	Minor	Write regulation activated due to high temperature	If this condition persists, increase air flow, lower room temperature or reduce write load.
10974	Minor	Write regulation activated to ensure adapter lifespan	If this condition persists, reduce write load.
10975	Minor	Running in minimal status	Check additional status property for more information.
10976	Minor	PCI power budget alarm	Switch to a higher powered PCI slot or attach external power cable.
10977	Minor	LEB map missing	If problem persists after reboot, call your local Fujitsu Helpdesk.
10978	Minor	Update in progress	The adapter will not be usable until formatting is complete.
10979	Minor	Reserves depleted	Formatting to a smaller size will free up reserve.
10980	Informational	Adapter normal	
10981	Critical	Attach failed	If problem persists, call your local Fujitsu Helpdesk.
10982	Minor	Detach failed	1. Force detach. 2. If problem persists, call your local Fujitsu Helpdesk.
10983	Informational	Attached	
10984	Critical	Detached	For information only.
10985	Informational	Format of disk ([..]) changed	
10986	Informational	File log cleared	

10987	Informational	Disk ([..]) will be set offline due to SMART error	
10988	Informational	Disk ([..]) will be set offline due to too many unexpected sense events	
10989	Minor	Protection information error in cache for logical drive [..] at LBA [..]	
10990	Minor	Flash downloaded image is not supported	
10991	Informational	BBU mode selected - [..]	
10992	Informational	Periodic BBU relearn was missed, and rescheduled to [..]	
10993	Informational	Adapter reset requested by host	
10994	Informational	Adapter reset requested by host, completed	
10995	Major	L3 cache error has been detected	
10996	Major	L2 cache error has been detected	
10997	Minor	Adapter booted in headless mode with errors	
10998	Major	Adapter booted to safe mode due to critical errors	
10999	Minor	Warning during boot - [..]	
11000	Major	Critical error during boot - [..]	
11001	Critical	Fatal error during boot - [..]	
11002	Informational	Peer adapter has joined high availability domain (ID: [..])	
11003	Major	Peer adapter has left high availability domain (ID: [..])	
11004	Informational	Disk ([..]) is managed by peer adapter	
11005	Informational	Disk ([..]) is managed by local adapter	
11006	Informational	Logical drive [..] is managed by peer adapter	
11007	Informational	Logical drive [..] is managed by local adapter	
11008	Minor	Logical drive [..] has a conflict in high availability domain	
11009	Informational	Logical drive [..] access is shared	
11010	Informational	Logical drive [..] access is exclusive	
11011	Minor	Logical drive [..] is incompatible in the high availability domain	
11012	Major	Peer adapter is incompatible	
11013	Major	Adapters in the high availability domain are incompatible	
11014	Major	Adapter properties are incompatible between local and peer adapters	

11015	Minor	Firmware versions do not match in the high availability domain	
11016	Minor	MegaRAID Advanced Software Options [...] do not match in the high availability domain	
11017	Informational	High availability cache mirror is online	
11018	Major	High availability cache mirror is offline	
11019	Critical	Logical drive [...] access blocked as cached data from peer adapter is unavailable	
11020	Minor	FBU power pack is not supported. Please replace the pack	
11021	Minor	Disk [...] temperature [...] C is above warning threshold	
11022	Major	Disk [...] temperature [...] C is above critical threshold	
11023	Informational	Disk [...] temperature [...] C is normal	
11024	Minor	Disk [...] IOs are being throttled	
11025	Informational	Disk [...] IOs are normal (no throttling)	
11026	Informational	Disk [...] has [...] % life left. Life left thresholds - warning: [...] %, critical: [...] %	
11027	Minor	Disk [...] life left [...] % is below optimal. Life left thresholds - warning: [...] %, critical: [...] %	
11028	Major	Disk [...] life left [...] % is critical. Life left thresholds - warning: [...] %, critical: [...] %	
11029	Major	Disk [...] failure, device locked-up	
11030	Minor	Driver needs to be upgraded [...]	
11031	Minor	Direct communication with peer adapter(s) was not established. Please check proper cable connections	
11032	Minor	Firmware image does not contain signed component	
11033	Minor	Authentication failure of the signed firmware image	
11034	Informational	Setting logical drive [...] as boot device	
11035	Informational	Setting disk [...] as boot device	
11036	Informational	The BBU temperature is changed to [...] C	
11037	Informational	The adapter temperature is changed to [...] C	
11038	Major	FBU capacity is too less to support data backup. Write-back logical drives will be converted to Write-through	
11039	Minor	FBU data backup capacity has decreased, consider replacement	

11040	Major	FBU device failed, cannot support data retention	
11041	Informational	Boot device reset, setting target ID as invalid	
11042	Minor	Write-back Nytro cache size mismatch between the servers. The Nytro cache size was adjusted to [...] GB	
11043	Minor	Logical drive [...] is not shared between servers but assigned for caching. Write-back Nytro cache content of the logical drive will be mirrored	
11044	Informational	Power [...] watts usage base IOs throttle started	
11045	Informational	Power base IOs throttle stopped	
11046	Informational	Adapter tunable parameter(s) changed	
11047	Informational	Adapter operating temperature within normal range, full operation restored	
11048	Minor	Temperature threshold exceeded for the adapter. This may indicate inadequate cooling in the system chassis. Adapter has switched to lower performance mode	
11049	Minor	Adapter defect or no adapter detected on host [...]	
11050	Major	Connection to host [...] failed	
11051	Informational	Connection to host [...] established	
11052	Informational	Adapter supports high availability mode, currently functioning with high availability feature set	
11053	Informational	Adapter supports high availability mode, currently functioning with single adapter feature set	
11054	Major	FBU components mismatch. Write-back logical drives will be converted to write-through	
11055	Informational	Adapter has entered maintenance mode	
11056	Informational	Adapter has returned to normal mode	
11057	Informational	Topology is in [...] mode	
11058	Major	Cannot enter [...] mode because [...] logical drive [...] would not be supported	
11059	Major	Cannot enter [...] mode because [...] disk ([...]) would not be supported	

6.3 Errors

Error code	Meaning
20000	Unspecified error occurred.
20001	No supported hardware found.
20002	Invalid command.
20003	Vendor API call failed.
20004	Invalid property.
20005	Invalid operation.
20006	Invalid parameter.
20007	Memory allocation failed.
20008	Invalid object ID.
20009	Invalid object type.
20010	Property type / value mismatch.
20011	Lock initialization failed.
20012	Vendor API initialization failed.
20013	Event initialization failed.
20014	Configuration key/value pair not found.
20015	Library loading failed.
20016	Library symbol not found.
20017	MPX initialization in progress.
20018	Write access denied.
20019	Consistency check not supported with this RAID level.
20020	Logical drive busy.
20021	Consistency check not suspended.
20022	Consistency check not running.
20023	Rebuild not supported with this RAID level.
20024	Logical drive not operational.
20025	Rebuild not running.
20026	Rebuild not suspended.
20027	Could not write, the file already exists.
20028	Invalid characters in filename.
20029	Could not open file.
20030	Can only start in manual mode.
20031	Adapter busy.
20032	No disks found.
20033	Patrol Read start in progress.
20034	Patrol Read not running.

20035	Alarm disabled.
20036	Recalibration not needed.
20037	Recalibration not running.
20038	Initialization not running.
20039	No BGI running.
20040	Location running.
20041	Location not running.
20042	Disk not available.
20043	Disk not hot spare.
20044	Disk failed.
20045	Reboot required.
20046	Disk(s) too small.
20047	Not enough disk(s) specified.
20048	Resulting disk space too small.
20049	No logical drive found.
20050	Disk not online.
20051	Disk not offline.
20052	Logical drive not offline.
20053	Migration not running.
20054	Disk busy.
20055	Verification not running.
20056	Parse error.
20057	Configuration mismatch.
20058	Logical drive not degraded.
20059	Disk missing.
20060	Selected Segment/drive not usable for the new logical drive.
20061	All segments of a logical drive must be attached to the same channel/port.
20062	All segments of a logical drive must be attached to the same array.
20063	The maximum logical drive count per channel/port is limited.
20064	The maximum logical drive count is limited.
20065	Not enough disks to create a logical drive.
20066	Too many disks to create a logical drive.
20067	Logical drive not creatable.
20068	Disks too small to create the logical drive.
20069	Estimated segment size is smaller than minimum supported segment size.
20070	Segment is too small for the logical drive.
20071	Add drives for creating a logical drive.
20072	All arrays full.

20073	Invalid number of arrays.
20074	No unconfigured disks.
20075	All arrays full and/or no unconfigured disks.
20076	Invalid number of disks.
20077	No space on disk.
20078	Disk already in use.
20079	Disk not available.
20080	Invalid disks specified for array.
20081	Invalid span depth.
20082	Invalid arrays for span depth.
20083	Invalid array count.
20084	Invalid array reference.
20085	Invalid size.
20086	Invalid logical drive count.
20087	Target IDs exhausted.
20088	Invalid RAID level.
20089	Invalid hot spare count.
20090	Spanning not possible.
20091	Number of spans exhausted.
20092	Number of drives per span exhausted.
20093	No configuration available.
20094	Specified size too small.
20095	Maximum number of drives to create the disk reached.
20096	Segment is too large for the logical drive.
20097	Previous span must use its full capacity if further spans need to be created.
20098	Current span will be too large to add the disk.
20099	Other span is too large to add the disk.
20100	The supported stripe size depends on the number of disks used.
20101	This stripe size is too large for the number of disks in the logical drive.
20102	There are segments which can never be used for another logical drive.
20103	Alarm not available.
20104	Patrol Read disabled.
20105	Patrol Read running.
20106	Migration running.
20107	Initialization running.
20108	Consistency check running.
20109	Not enough disks for migration.
20110	Disk cannot guard any logical drive as hot spare.

20111	MDC running.
20112	MDC not supported with this RAID level.
20113	MDC not running.
20114	MDC not suspended.
20115	Recalibration running.
20116	Different disk types in logical drive not supported.
20117	Different disk types in enclosure not supported.
20118	Hotplug of enclosures not supported.
20119	It is not possible to import this foreign configuration, it can be cleared only.
20120	Clear of foreign configuration failed.
20121	Timeout
20122	Different disk media types in logical drive not supported.
20123	Disk cannot be used for configuration.
20124	Currently the action can not be performed. It will be tried to start the action later.
20125	The service is shutting down.
20126	Too many instances are already running.
20127	Only stripe sizes above 8K are allowed for this RAID level with 3 disks per span.
20128	Plugin busy.
20129	BBU busy.
20130	Port busy.
20131	Enclosure busy.
20132	Processor busy.
20133	Foreign configuration incomplete. Try different index or clear this configuration.
20134	Disk used by LMD
20135	No hardware with supported firmware found.
20136	Unexpected error code.
20137	Service not available.
20138	Send / receive failed.
20139	gethostname() failed.
20140	Not implemented.
20141	Action not executed.
20142	Error during processing.
20143	Mailbox unavailable.
20144	Invalid mailbox name.
20145	Bad command sequence.
20146	User not local.
20147	Transaction failed.
20148	Authentication not supported.

20149	Encryption required for requested authentication mechanism.
20150	Authentication mechanism is too weak.
20151	A password transition is needed.
20152	TLS not available on server for temporary reason.
20153	TLS not supported by server.
20154	Connection refused.
20155	Bad username or password.
20156	Could not open TLS socket.
20157	Undefined recipient mail.
20158	Need at least one recipient.
20159	No sender.
20160	No message subject.
20161	No more connections to servers supported.
20162	Could not connect to server.
20163	No or invalid response from server.
20164	Logical drive not initialized.
20165	Initialization not suspended.
20166	CacheCade supports SSD's only.
20167	No trial software options found.

7 Help

7.1 Help

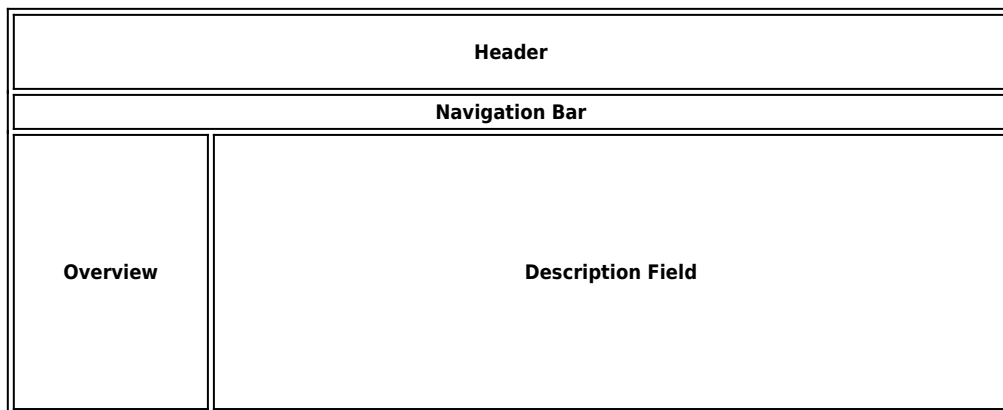
You can access the help system by clicking on *Help* on the right of the 1st menu line.

Here you can use *Contents and Index* to start an independent browser session in which you can view this help online. The menu item *Info about ServerView RAID Manager* provides you with version information on the product.

An introduction to the online help and which options you can use there is contained under **Help** in the table of contents.

7.2 Online Help

To be able to use the help effectively you should familiarize yourself briefly with the navigation. The online help window consists of four areas: *Header*, *Navigation Bar*, *Overview* and *Description Field*. The areas contain some functions which are described below.



7.2.1 Header

The header contains the logo and the application name.

7.2.2 Navigation Bar






These buttons enable you to activate and deactivate the **Overview**.



This button enables you to open the table of contents for the help.

Individual help topics are selected and pulled down in the table of contents using .

All help topics are opened with  and closed with .

The individual help texts in the help topics are displayed by clicking on  in the **Description Field**.



This button enables you to open the glossary for the help.

You search for the required keyword by selecting a button or scrolling.



You can activate the search function in the help using this button.

After you have entered the search criterion the relevant search results are displayed in the **Description Field**.



This button enables you to print out the help text displayed in the **Description Field**.



These buttons enable you to navigate within the pages called so far.

You use them to page forward or back one page.




This button enables you to quit the online help and close the window.

7.2.3 Overview

The overview contains the table of contents, the glossary or the search function depending on what you selected in the **Navigation Bar**.

7.2.4 Description Field

The selected help text is displayed in the description field.

You can print out the displayed text using the  button.

To print the entire help in manual format you must select the **Show Manual as PDF** entry in the table of contents, save the file if required, and then print the text using the print function of a PDF reader.

7.3 amCLI

amCLI is a command line interface to ServerView RAID Manager. It can be used to create, delete or manage RAID arrays or manage ServerView RAID Manager itself from the command line or from a script.

At the top level, amCLI has the following command options:

```
-c|--create: create a logical drive
-d|--delete: delete last logical drive
-e|--exec: execute a device-specific command
-g|--get: get a target's property
-i|--import: import a certificate
-l|--list: list information
-m|--migrate: migrate a RAID array to another RAID level
-r|--restore: restore the state from a file
-s|--set: set a target's property to a given value
-w|--write: write the current state to a file
-Z|--zap: zap a target
-?|--help: give a short help
```

Up to one of these may be specified, -?being the default.

7.3.1 Addressing scheme

All objects that can be manipulated by this command (the entire ServerView RAID Manager subsystem, adapters, physical drives, and logical drives i.e. RAID arrays) are identified by two numbers separated by a slash (/) character: the first number specifies a *module* and the second number is a (0-based) *index*: <mod/idx>. In this documentation, such a pair of numbers is referred to as the *address* of an *object*.

Currently, the following *module* numbers are supported:

mod	Module
21	ServerView RAID Manager
32	LSI SAS MegaRAID Adapter, SAS/SAS2/SAS3 IT/IR Adapter, MegaSR
36	Fujitsu Aries SAS Adapter
39	Linux Software RAID
40	LSI SAS MegaRAID Adapter, SAS/SAS2/SAS3 IT/IR Adapter (via CIM)
47	AMD Chipset RAID
48	Fusion-io ioDrive2

Note that *index* values need not be consecutive (e.g. if 27/5 and 27/7 exist, 27/6 must not necessarily exist, too), are relative to a module (i.e. 26/5 and 27/5 can both exist at the same time) and the numbering continues between adapters, logical and physical drives (i.e. 27/5 and 27/10 can be adapters, 27/6 and 27/7 can be physical drives and 27/8 and 27/9 can be logical drives).

In the following,

- SysIdx is an index of the "Server View RAID" module (i.e. *mod* will be 21),
- AdpIdx is an index of an adapter module (i.e. <mod/AdpIdx> must be the address of an adapter),
- PDIdx is an index of a physical drive (i.e. <mod/PDIdx> must be the address of a physical drive),
- LDIdx is an index of a logical drive (i.e. <mod/LDIdx> must be the address of a logical drive), and
- *idx* is not restricted to a specific object type (i.e. <mod/idx> can be the address of a module, a logical or a physical drive, as appropriate in the context).

Use `amCLI -l` to find the addresses of objects you wish to use.

7.3.2 Create a logical drive

Before creating a logical drive, you must decide which RAID level to use, what parameters the chosen RAID level requires and what (physical and/or logical) drives this logical drive should consist of. It is assumed here that you are familiar with the concepts of RAID and the various RAID levels.

7.3.2.1 Synopsis

```
amCLI [-c|--create] <mod/AdpIdx> raid=<raidLevel> parameters <mod/PDIdx>+
```

7.3.2.2 Parameters

- <mod/AdpIdx>: the address of the adapter which will manage the logical drive created,
- <raidLevel>: the desired RAID level of the logical drive to be created, (at present, RAID levels 0, 1, 01, 1e, 3, 4, 5, 5e, 5ee, 6, 10, 50, 60, "concat", and "single" are supported, but not all adapters support all RAID levels and some RAID levels are only supported by a single adapter type),
- *parameters* depend upon the *raidLevel* chosen:
 - span=<spanCount>: number of (sub-)logical drives this logical drive should be combined of,
 - stripe=<stripeSize>: how much data should be stored on a physical drive before continuing on the next physical drive,
 - <raidFlag>=<flag>: additional settings that can be passed to the adapter during logical drive creation, e.g. write cache mode, readahead mode, ... (eg `read_mode=adaptive`)
- size=<megabytes>: the size of the resulting logical drive.
- <mod/PDIdx>+: a (non-empty) list of addresses of physical and/or logical drives that should be used when creating the new logical drive.

Use `amCLI --help create <mod/AdpIdx>` to find out which RAID-levels and parameters the specified adapter supports.

7.3.2.3 Example

To create a RAID-5 array consisting of physical drives 29/5, 29/6, and 29/7 on the Adaptec StorLib FSA adapter 29/1 with default

parameters, the following command could be used:

```
# amCLI -c 29/1 raid=5 29/5 29/6 29/7
```

A confirmation is then required to execute this command (the input is treated case-insensitive):

```
Are you sure to create a new Logical Drive on Adapter '29/1'?
Type YES to confirm _
```

(Note that, depending on the command interpreter used, it may be possible to pipe a "yes" into this command.)

7.3.2.4 Note

ServerView RAID Manager will allocate an address for the new logical drive. Use `amCLI -l` to determine the address.

7.3.3 Delete last logical drive

This command deletes the logical drive with the highest *logical drive ID* on a given adapter (which is usually the logical drive most recently created).

7.3.3.1 Synopsis

```
amCLI [-d|--delete] <mod/AdpIdx>
```

7.3.3.2 Parameters

- `<mod/AdpIdx>`: the address of the adapter whose most recently created logical drive should be deleted.

7.3.3.3 Example

To delete the logical drive created above immediately after having created it, use

```
# amCLI -d 29/1
```

Again, an explicit confirmation is required to execute this command:

```
Are you sure to delete the last Logical Drive on Adapter '29/1'?
Type YES to confirm _
```

7.3.4 Execute operation on a device

This command starts execution of a device-specific command on a given device.

7.3.4.1 Synopsis

```
amCLI [-e|--exec] <mod/idx> <operation> <param>*
```

7.3.4.2 Parameters

- `<mod/idx>`: the address of the object that should execute the operation,
- `<operation>`: the command to execute, and
- `<param>*`: a (possibly empty) list of arguments required for the given command.

To find out which operations are supported by a given object and what additional parameters they require, use

```
amCLI [-?|--help] exec <mod/idx>
```

7.3.4.3 Examples

```
# amCLI -? exec 32/26
amCLI v5.7.0
Usage:
-e | --exec <32/PDIdx>   locate
-e | --exec <32/PDIdx>   stop_location
```

```

-e | --exec <32/PDIdx>    create_global_hot_spare
-e | --exec <32/PDIdx>    delete_global_hot_spare
-e | --exec <32/PDIdx>    create_dedicated_hot_spare <mod/LDIdx>
-e | --exec <32/PDIdx>    delete_dedicated_hot_spare
-e | --exec <32/PDIdx>    make_online
-e | --exec <32/PDIdx>    make_offline
-e | --exec <32/PDIdx>    make_ready
-e | --exec <32/PDIdx>    replace_missing_disk <mod/LDIdx>
# amCLI -e 32/26 locate

```

7.3.5 Get property

This command retrieves the value of a given property of a given object.

7.3.5.1 Synopsis

```
amCLI [-g|--get] <mod/idx> <property>
```

7.3.5.2 Parameters

- <mod/idx>: the address of the object and
- <property>: the name of the property to retrieve.

Use `amCLI -? get` to find out which object classes support which properties in general or `amCLI -? get <mod/idx>` to find out which properties a specific object supports.

7.3.5.3 Examples

```

# amCLI -? get 32/2
amCLI v5.7.0
Usage:
-g | --get <32/LDIdx> activity
-g | --get <32/LDIdx> status
-g | --get <32/LDIdx> disk_cache_mode
-g | --get <32/LDIdx> bgi
...
# amCLI -g 32/2 status
Operational

```

7.3.6 Import a certificate

This command imports a certificate.

7.3.6.1 Synopsis

```
amCLI [-i|--import] <certificate file> <private key file>
```

7.3.6.2 Parameters

- <certificate file>: the name of a file containing a certificate.
- <private key file>: the name of a file containing the private key.

7.3.6.3 Example

```
# amCLI -i cert.pem key.pem
```

7.3.7 List information

This command lists information available about a given object.

7.3.7.1 Synopsis

```
amCLI [-l|--list] [all|struct|<mod/idx>]
```

7.3.7.2 Parameters

- `all` lists the structure of the RAID subsystems with some information about each item
- `struct`, which is the default, lists the structure of the RAID subsystems without additional information, and
- `<mod/idx>`: the address of the object of which extensive information is required.

7.3.7.3 Example

```
# amCLI -l struct
21/3: System, 'hostname'
  32/1: SAS Adapter 0, 'LSI MegaRAID SAS PCI Express(TM) ROMB (0)'
    32/2: Logical Drive 0, 'LogicalDrive_0', RAID-0, 69472MB
    32/3: SAS Port 0
      32/11: Physical Drive 0, 'SEAGATE ST373454SS (0)', 69472MB
    32/4: SAS Port 1
      32/12: Physical Drive 1, 'SEAGATE ST336754SS (1)', 34464MB
  ...
```

7.3.8 Migrate a logical drive to a new RAID level

This command changes the RAID level of a logical drive, if this is possible in the current configuration and if it is supported by the adapter controlling the logical drive.

7.3.8.1 Synopsis

```
amCLI [-m|--migrate] <mod/LDIdx> [raid=<raidLevel>] parameters <mod/PDIdx>*
```

7.3.8.2 Parameters

- `<mod/LDIdx>`: the address of the logical drive to migrate,
- `<raidLevel>`: the desired new RAID level, and
- `<mod/PDIdx>*`: a (possibly empty) list of addresses of additional physical drives to use.
- *parameters* are specific to the desired new RAID level. At present, only the `stripeSize` can be changed during migration.

To find out which RAID levels a given logical drive can be migrated to and whether additional physical drives may be needed, use

```
amCLI -? migrate <mod/LDIdx>
```

7.3.8.3 Examples

```
# amCLI -l 32/2
32/2: Logical Drive 0, 'LogicalDrive_0', RAID-0, 69472MB
  Parents: 1
  Children: -
  Containers: 1
  Drives: 1 --> ( 32/11 )
  Properties:
    Unique ID: PCI:Bus=2&Device=14&Function=0&ID=0
    Logical Drive Number: 0
    Name: LogicalDrive_0, settable
    Logical Size: 69472 MB
    Physical Size: 69472 MB
    RAID Level: RAID-0
  ...
# amCLI -? migrate 32/2
amCLI v5.7.0
Usage:
  -m | --migrate 32/2
  [raid=(0|1|5)]
  (<PDIdx>)+
```

This means that logical drive 32/2 (a RAID-0 logical drive) can only be migrated to RAID levels 0, 1 or 5 and it may be possible to include additional physical drives (in this specific case they would be even required to migrate to RAID levels 1 or 5).

```
# amCLI -m 32/2 raid=1 32/8
```

A confirmation is again required:

```
Are you sure to modify Logical Drive '32/2' on Adapter '32/1'?
Type YES to confirm _
```

7.3.9 Restore state

This command restores the state of the RAID configuration from a file previously created by `amCLI -w`.

7.3.9.1 Synopsis

```
amCLI [-r|--restore] <filename>
```

7.3.9.2 Parameters

- `<filename>`: the name of a file containing a description of the configuration

7.3.9.3 Example

```
# amCLI -r OldState
```

Again, an explicit confirmation is required:

```
Are you sure to restore the configuration?
Type YES to confirm _
```

7.3.9.4 Warning

Restoring the state of the adapter managing the system disk may render the system unusable!

7.3.10 Set property

This commands sets the given property of a given object to a given new value.

7.3.10.1 Synopsis

```
amCLI [-s|--set] <mod/idx> <property> <value>
```

7.3.10.2 Parameters

- `<mod/idx>`: the address of the object,
- `<property>`: the property name, and
- `<value>`: the new property value.

Use `amCLI -? set` to find out which device classes support which properties in general or `amCLI -? set <mod/idx>` to find out which properties a given device supports.

7.3.10.3 Examples

```
# amCLI -? set 32/2
amCLI v5.7.0
Usage:
-s | --set <32/LDIdx> name <string>
...
# amCLI -g 32/2 name
LogicalDrive_0
# amCLI -s 32/2 name 'OS disk'
# amCLI -g 32/2 name
```

OS disk

7.3.11 Write state

This command saves the internal state of a specified object into a given file or prints it to the standard output.

7.3.11.1 Synopsis

```
amCLI [-w|--write] <mod/SysIdx> [<file>]
```

```
amCLI [-w|--write] <mod/AdpIdx> [<file>]
```

7.3.11.2 Parameters

- <mod/SysIdx>: the system's address (i.e. 21/0),
- <mod/AdpIdx>: the address of an adapter,
- <file> the name of a file in which the state will be stored. If no file name is given, the state is sent to *stdout*.

7.3.11.3 Example

```
# amCLI -w 32/1
<ServerViewRAIDManager Version="5.7.0">
  <SASAdapter UniqueID="PCI:Bus=2&Device=14&Function=0" AdapterNumber="0
...

```

7.3.12 Zap drive

This command clears an existing configuration of an adapter, e.g. deletes all logical drives, hot spares, etc.

7.3.12.1 Synopsis

```
amCLI [-Z|--zap] [<mod/idx>]
(Note the upper case Z)
```

7.3.12.2 Parameters

- <mod/idx>: the address of an adapter. If no adapter is given, the configurations on all adapters are cleared.

7.3.12.3 Example

```
# amCLI -Z 32/17
```

A confirmation is then required to execute this command (the input is treated case-insensitive):

```
Are you sure to zap Adapter '32/17'?
Type YES to confirm _
```

7.3.13 Help

The help command serves two purposes:

1. To remind the user of the syntax of the various commands and
2. to retrieve command- and object-specific options.

7.3.13.1 Synopsis

```
amCLI [-?|--help] [[create | get | set | exec | migrate] [<mod/idx>]]
```

7.3.13.2 Parameters

Without any additional parameters, `amCLI -?` will just print out the syntax of all `amCLI` commands. As `-?` is the default, typing `amCLI`

will do the same.

Additional parameters can be given to retrieve specific information about parameters of a given command when applied to a given object:

- create: show which RAID-levels and additional parameters the specified adapter supports (<mod/idx> must be the address of an adapter)
- get: show which properties can be queried with the amCLI -g command
- set: show which properties can be modified with the amCLI -s command
- exec: show information about commands available for the given object
- migrate: show which RAID-level a given logical drive can be migrated to and which additional parameters may be specified (<mod/idx> must be the address of a logical disk).

If no device is given, the syntax of the command is shown. If the address of an object is given, specific information about the execution of the command on that object is shown.

7.3.13.3 Examples

```
# amCLI -?
amCLI v5.7.0
Usage:
-c <mod/AdpIdx> raid=<raidLevel> [span=<spanCount>] [stripe=<stripeSize>]
  [<raidFlag>=<flag>] [size=<megabytes>] (<mod/PDIdx>)+
--create <mod/AdpIdx> raid=<raidLevel> [span=<spanCount>]
  [stripe=<stripeSize>] [<raidFlag>=<flag>] [size=<megabytes>]
  (<mod/PDIdx>)+
-d <AdpIdx>
--delete <AdpIdx>
...

# amCLI -? create
amCLI v5.7.0
Usage:
-c <mod/AdpIdx> raid=<raidLevel> [span=<spanCount>] [stripe=<stripeSize>]
  [<raidFlag>=<flag>] [size=<megabytes>] (<mod/PDIdx>)+
--create <mod/AdpIdx> raid=<raidLevel> [span=<spanCount>]
  [stripe=<stripeSize>] [<raidFlag>=<flag>] [size=<megabytes>]
  (<mod/PDIdx>)+

# amCLI --help create 32/17
amCLI v5.7.0
Usage:
-c | --create 32/17
raid=(0|1|5|6|10|50|60|1e)
[span=<(RAID-0:1)|
  (RAID-1:1)|
  (RAID-5:1)|
  (RAID-6:1)|
  (RAID-10:2..8)|
  (RAID-50:2..8)|
  (RAID-60:2..8)|
  (RAID-1E:1)>]
[stripe=<(RAID-0:(8kb|16kb|32kb|64kb|128kb|256kb|512kb|1mb)|
  (RAID-1:(8kb|16kb|32kb|64kb|128kb|256kb|512kb|1mb)|
  (RAID-5:(8kb|16kb|32kb|64kb|128kb|256kb|512kb|1mb)|
  (RAID-6:(8kb|16kb|32kb|64kb|128kb|256kb|512kb|1mb)|
  (RAID-10:(8kb|16kb|32kb|64kb|128kb|256kb|512kb|1mb)|
  (RAID-50:(8kb|16kb|32kb|64kb|128kb|256kb|512kb|1mb)|
  (RAID-60:(8kb|16kb|32kb|64kb|128kb|256kb|512kb|1mb)|
  (RAID-1E:(8kb|16kb|32kb|64kb|128kb|256kb|512kb|1mb)>]
[init_mode=(no_initialization|fast_initialization|normal_initialization)]
[read_mode=(readahead|no_readahead)]
[write_mode=(writeback|always_writeback|writethrough)]
[cache_mode=(cached|direct)]
```

```
[disk_cache_mode=(disabled|enabled)]
[cache_settings=(data_protection|performance|advanced)]
[name=<string>]
[size=<megabytes>]
(<PDIid>)+
```

7.3.14 Diagnostics

The exit status (or error level) approximates the error conditions defined by ServerView RAID Manager and takes on the following values:

Exit status	Description
0	Normal; no errors or warnings detected
1	Internal error
2	Invalid syntax
3	Invalid object
4	Memory failure
5	Operation not supported
6	Property not supported
7	Operation cannot be executed at this time
8	Communication with Core Service failed
10	Core Service initialization failed
11	Core Service database failed
12	Operation failed
13	Invalid parameter value
14	Login failed
15	Shutdown in progress
16	No administration rights granted
17	Cannot open file
18	Cannot read file
19	Cannot write file
20	Core Service is initializing

7.4 Frequently Asked Questions - FAQs

- Does ServerView RAID Manager use a secure connection?
 - Yes, RAID Manager uses an encrypted communication to the browser. The data transfer is secured by encryption protocols SSL 3.0, TLS 1.0, TLS 1.1, or TLS 1.2. Which protocol is used depends on the browser and its settings.
- When you start ServerView RAID Manager, only a red X appears in the upper left-hand corner.
 - Close the browser window/the browser and restart ServerView RAID Manager (e.g. by reentering the URL).
- When you start ServerView RAID Manager on Windows XP or Windows Server 2003, the browser window/the browser does not display anything.
 - As reaction on an attack against SHA-1 hash functions the **National Institute of Standards and Technology** (NIST) recommends the transition from SHA-1 to hash functions of the SHA-2 family (SHA-224, SHA-256, SHA-384, SHA-512). ServerView RAID Manager uses SHA-256 which is not available under every Windows XP or Windows Server 2003 installation. A hotfix (**KB968730**) is available from Microsoft.
- The browser suddenly no longer has contact to the server.
 - Check whether the service *amService* (Windows) or the daemon *amDaemon* (Linux) is running. If it is not, start it:
Windows: Via Computer Management → Services → ServerView RAID Manager
Linux: Using the `"/etc/init.d/aurad start"` command
The service check under Linux, for instance, is executed using `"ps -ef | grep amDaemon"` or `"/etc/init.d/aurad status"`.
- The progress display in the GUI suddenly stops after you have initiated an action.
 - Abort the session and restart ServerView RAID Manager.
- The expected results are not displayed in the log.
 - Check whether logging is enabled in ServerView RAID Manager (see system log property **Logging**). If this does not help, notify your service engineer.
- A logical drive cannot be deleted.
 - Check whether deletion is prevented by an ongoing activity (e.g. initialization). Interrupt or abort the activity and repeat the delete operation.
- You must or want to use ServerView RAID Manager with JRE 1.4, but the login screen remains dark.
 - Click in the browser window and press the *Enter* key once after you have loaded and initialized ServerView RAID Manager.
- Which service/daemon is installed in conjunction with ServerView RAID Manager?
 - The following service (daemon for Linux) will be installed:
amService/amDaemon: The central service/daemon of ServerView RAID Manager.
- What web server does ServerView RAID Manager use?
 - The web interface (GUI) is made available via the service/daemon *amService/amDaemon*, various extension modules being loaded dynamically at runtime. No "classical" web server such as Apache runs. *amService/amDaemon* uses a reduced HTTP as transport protocol to permit web browsers to work with ServerView RAID Manager.
- How can ServerView RAID Manager port be changed?
 - The 6th line of the `<installation directory>\bin\amDPatch.ini` file contains the entry "Port = 3173". You can change the port here. You cannot force a binding. If the port is not accessible from the outside, you must arrange this using the firewall.
- Is it possible to use IPv6 protocol with ServerView RAID Manager?
 - Yes, ServerView RAID Manager supports IPv4 and IPv6.
- Which authentication methods does ServerView RAID Manager support in **E-mail log** function?
 - ServerView RAID Manager supports the following SMTP authentication methods:
 - CRAM-MD5
 - DIGEST-MD5
 - LOGIN
 - NTLM
 - OTP
 - PLAIN
 - SCRAM
 - SRP
- Which SNMP version does ServerView RAID Manager support?
 - ServerView RAID Manager supports SNMP v1 only.
- Which settings have to be changed for SNMP on Linux?
 - During installation of ServerView RAID Manager entries are added to `/etc/.../snmpd.conf` that have to be explicitly activated for the underlying Linux distribution. These entries are marked with SVRA. On SuSE the '#' in the line starting with "rocommunity" has to be removed, and on RedHat and VMware the '#' in the line starting with "view". Then the SNMP daemon has to be restarted.
All further SNMP settings (community, trapsink, ...) are described in the manual of the distribution.

- User accounts on Windows.
 - When creating an account for ServerView RAID Manager on Windows it is recommended that the option *User must change password at next login* should not be checked and *Password never expires* should be checked. ServerView RAID Manager does not display a warning message when the password is expired.
- No login to Linux ServerView RAID Manager possible although users and groups have been created correctly.
 - Check file **/etc/security/access.conf**. Some operating systems have a very restrictive default user access control. To allow ServerView RAID Manager to be used with the newly created users and groups add lines like the following to the beginning of **/etc/security/access.conf**:
 +:<user or group name>:LOCAL
- No login to VMware ServerView RAID Manager possible although users and groups have been created correctly.
 - Similar to the previous item VMware vSphere 4.1 has a very restrictive default user access control. To allow ServerView RAID Manager to be used with the newly created users and groups use vSphere Client as described in **ESX Configuration Guide** and add administrator role privilege to them.
- No login to ServerView RAID Manager possible although user name and password was entered correctly in Japanese environment.
 - If you use 2 byte characters in the hostname, a login with this URL is not possible. Please change the name of the server to use only standard characters. Standard characters are A-Z, a-z, 0-9, -(hyphen). If this is not possible the IP address of the server can be used alternatively.

8 Glossary

Array

A group of several hard disks on which one or more logical drives are contained is called an array.

Array Initialization

See Initialization.

ATA

AT Bus Attachment. Standard parallel interface to IDE hard disk drives which is commonly used in desktop computers and some entry-level servers. A successor of ATA is SATA (Serial ATA interface).

Automatic Rebuild

Automatic procedure which restores faulty segments on preconfigured volumes. If a drive in a SAF-TE enclosure which has no hot spare assigned should fail, a rebuild starts only when the failed drive has been replaced by a new one.

Background Initialization

In the case of background initialization of a drive the redundant logical drive can be accessed while the initialization is running.

BGI

Background Initialization is a type of initialization which is started automatically in the background at low priority by an LSI controller. See also Initialization and Background Initialization.

Bus

See Channel.

Cache

Quickly accessible memory on a controller which serves as a buffer for data which is read from or written to devices.

Capacity

Total storage capacity available on a drive; often specified in megabytes or gigabytes. A distinction is made between physical and logical capacity.

CAS

CAS (Central Authentication Service) is an enterprise single sign-on solution for web services. Single sign-on (SSO) means a better user experience when running a multitude of web services, each with its own means of authentication. With a SSO solution, different web services may authenticate to one authoritative source of trust, that the user needs to log in to, instead of requiring the end-user to log in into each separate service.

Channel

Path between a controller and storage devices used for data transfer and control of information. Each channel of a controller is identified by a number between 0 and the maximum number of channels minus 1. A channel is also referred to as a port or bus.

Concatenation

Connection in sequential order.

Consistency Check

An action in which the controller checks all segments of the logical drive. Depending on the logical drive type various things can be checked and the checks can therefore take different lengths of time. RAID-5 checks the data for consistency and parity. RAID-1 checks whether both drives are consistent. See also MDC and Verify.

Create

See Automatic Rebuild.

Dedicated Hot Spare

A physical drive which, when required, takes over the place of a failed physical drive in a specially assigned, fault-tolerant logical drive.

Degraded

A redundant logical drive in which one or more members have failed. The data is still intact, but redundancy has been impaired and is in a worse status. The logical drive and all the data are still available, but a further drive failure leads to the failure of the logical drive and loss of data. A check plus correction can return an impaired logical drive to its optimal status.

Dirty Data

Data which has been written into a cache and has not yet been updated on the actual target volume.

Drive

See Physical and Logical Drive.

Enclosure

An enclosure for physical drives which generally contains several power supplies, fans, and temperature sensors. Enclosures are normally outside the computer to which they are connected. Some computers also contain internal enclosures.

Event

Notification or warning message when changes occur in the system.

Event Log

Information on controller activities or other events are stored in a file.

Expand

Assignment of more storage space to a logical drive.

Failed

Status of a non-redundant logical drive with a single drive failure or a redundant logical drive with multiple drive failures. The status generally results in a loss of data as access to the logical drive is no longer possible.

Failed Segment

A segment which is no longer used by a logical drive because it is either logically or physically damaged.

Fast Initialization

The logical drive is available immediately, but has a special internal status. In RAID-5 and RAID-50 the write performance is affected until a check plus correction has been performed on this logical drive.

Fault-tolerant Logical Drives

Logical drives with redundant components (RAID-1, RAID-5, RAID-10, RAID-50).

Format

A process performed by the firmware in which all data on the hard disk is totally deleted.

Global Hot Spare

Volume which can replace a failed component in the logical drives on the same controller. The available storage capacity must be at least as large as that of the failed component. See also Hot Spare.

Hot Spare

A physical volume available as a replacement if a drive fails. In a redundant logical drive this permits automatic data recovery. The storage capacity available must be at least as large as that of the failed component. See also Automatic Rebuild, Global Hot Spare and Dedicated Hot Spare.

Hot Swap

Replacement of system components while the system is running.

Initialization

A fault-tolerant logical drive must be initialized before it is used. This operation deletes all blocks on the logical drive. In RAID-5 a parity is then generated on the basis of the current content of the member segments, whereas RAID-1 copies the content of the first drive (master) to a second drive (slave). Depending on the RAID type initialization runs in the background at differing speeds. In addition, Fast Initialization is also provided for immediate access to a RAID-5 drive.

Initialized Logical Drive

A logical drive which is ready for read and write operations.

Java

Java is an object-oriented, platform-independent programming language developed by Sun Microsystems. All Java programs run on a wide range of platforms without any adjustments. However, to execute, JAVA programs generally need a special runtime environment, the virtual machine, and only this environment need be adjusted to the various operating systems.

JBOD

JBOD stands for Just a Bunch Of Disks. According to the latest definition of the Storage Networking Industry Association (SNIA) a single hard disk should be understood here today, whereas earlier it referred to multiple hard disks (also referred to as concatenation).

KByte

Is a unit of information or computer storage, commonly abbreviated as "KiB" and stands for 2^{10} bytes = 1,024 bytes.

LBA

Logical **B**lock **A**ddressing is an addressing method for hard disks. In contrast to other methods the sectors on the hard disk are counted singly, beginning with 0.

LED

A **l**ight-**e**mitting **d**iode is an electronic semiconductor which is used, for example, to indicate read or write operations on hard disks. Often an LED is also used for determining the location of the drives.

Locate

An aid in uniquely identifying hard disk which consists of the controller number, the channel or port number, the LUN, and the SCSI-ID.

Logical Drive

A drive which consists of one or more physical drives, mostly hard disks. For the operating system, all the storage volume available constitutes a single drive.

Logical Drive Order

The order in which, at system startup, the server's operating system recognizes individual hard disks and other devices connected to the controller.

LUN

Each SCSI device can contain up to eight subdevices. A LUN is the number of the logical unit - 0 through 7 - which has been assigned to this device. However, generally only one subdevice (LUN 0) exists.

MDC

Make Data Consistent is a consistency check with additional correction. Depending on the drive type various things can be checked and the checks can therefore take different lengths of time. RAID-5 checks the data for consistency and parity and optionally corrects parity errors. RAID-1 checks whether both drives are consistent. Either if inconsistencies found it will be try to correct if is possible to fix it. See also Consistency Check and Verify.

Migration

Process of transforming a logical drive from one RAID type to another, changing the strip size, or expanding the size of a logical drive by adding new disks.

Monitoring

The process for ascertaining, displaying, and logging system events.

Notification

Aid used by the system for communication relating to events that have occurred.

NVRAM

A non-volatile memory which can retain information even if the power supply is not maintained. This memory is often used on RAID controllers as a memory for the configuration and for error logging.

Offline

The status of a logical or physical drive which can no longer be accessed.

Offset

The distance from the start of a drive to the start of a segment.

Optimal

A logical drive in its normal operating status in which all components are present and fully operational.

Parity

A form of redundancy which is used for checking the user data for errors. Additional data is generated from the user data which is also stored and can be used to reconstruct the original data.

Patrol Read

Patrol Read examines the drive's interface for errors. If an error is detected which cannot be rectified automatically, this error is logged. The faulty part of the medium is assigned to the defective blocks. With some controllers the disk is automatically taken out of service if multiple errors are found.

Physical Drive

Generally a physical hard disk drive, also known as hard disk for short. This is a randomly accessed, rewritable data storage device.

Port

See Channel.

RAID Signature

From the RAID signature on a hard disk the RAID controller can recognize, among other things, whether the hard disk has already been initialized. In future it is to contain a complete, non-proprietary RAID configuration to make it easier to exchange drives or controllers.

RAID Volume

Two or more logical drives of the same type which need not necessarily have the same capacity are connected in a RAID volume.

RAID-0

A logical drive with one level, consisting of two equal-sized segments on different hard disk drives. RAID-0 uses the striping process to distribute the data evenly in equal-sized sections over the drives concerned.

RAID-0/1

See RAID-10.

RAID-1

A logical drive with one level, consisting of two equal-sized segments on different hard disk drives. Offers redundancy by storing the same data on both hard disks.

RAID-5

A logical drive with one level, consisting of three equal-sized segments on different hard disk drives. The capacity of one segment is used for parity data which is distributed over all the drives in equal-sized sections.

RAID-10

A logical drive. Two equal-sized RAID-1s are used to create a RAID-10. RAID-10 thus needs four physical drives.

RAID-50

A logical drive. Two equal-sized RAID-5s are used to create a RAID-50. RAID-50 thus needs six physical drives.

Reconfiguration

See Migration.

Redundancy

Redundancy is the general term to describe the additional existence of resources which are functionally identical or comparable if these are not normally required when operation is error-free. Here redundancy is used to manage data in a system with the aim of automatically replacing failed components by operational ones. For example, logical drives of the type RAID-5 are redundant because the surviving members can combine to replace the data of a failed component.

Replacement

See Hot Spare.

Role Based Access Control

Role based access control (RBAC) manages access control by defining a set of user roles (security roles). One or more roles are assigned to each user, and one or more user privileges are assigned to each role.

SAF-TE

SCSI Accessed Fault-Tolerant Enclosure.

SAS

Serial Attached SCSI is to replace the current parallel SCSI interface because the Terminators which are typical for SCSI are not required for SAS. SAS takes over the SATA connections. SATA devices can be used on SAS but not vice versa.

SATA

Serial ATA is a successor to ATA which transfers data serially instead of in parallel.

SCSI

Small Computer System Interface is a parallel high-speed communication method which permits data transfer rates of up to 320 Mbytes/s. The current specification supports up to 15 devices per channel.

SCSI ID

A unique number (0-15) which is assigned to each device on a SCSI bus.

Second Level Array

A logical drive can consist of more than one level. The logical device of the second level (lower level array in an array with two levels) is never visible for the operating system and can only be used by other logical devices. For example, a RAID-10 array's member in the top level is a RAID-0 array and in the second level two or more RAID-1 arrays.

Segment

Reserved area on a physical hard disk. A segment is always part of a logical drive and cannot be used by more than one logical drive at the same time.

Single Sign-On (SSO)

Single sign-on allows participating applications to share a single sign-on session. Users complete a centrally managed authentication experience once per browser session and while authenticated to CAS can log into multiple applications without again being prompted for credentials and without those applications ever seeing the user's password.

SMART

Self-Monitoring Analysis and Reporting Technology (SMART). This drive function is designed to determine the reliability status of a hard disk drive. If SMART detects a potential problem that could be serious, the user is notified and receives assistance on how to rectify this problem.

Spare Drive

See Hot Spare.

Striping Process

Small, contiguous data areas which are distributed over all hard disks in the logical drive are called stripes. For example, with the striping process RAID-0 distributes the data in equal-sized sections over the drives concerned to expedite access.

Stripe Size

In logical drives using the striping process (RAID Levels 0, 5, 10 and 50) the data is distributed over the member hard disks in equal-sized sections. The amount of data in each section is the stripe size.

Temperature Warning Threshold

The temperature threshold defined by the user above which a warning message is issued.

Terminator

In a SCSI bus system both ends of the cable route must be provided with a terminator. There are two types of termination, the passive one using resistors and the active one using an internal voltage source.

Verify

An action in which the controller checks all segments of the hard disks. This determines whether the hard disks are sending back data from the blocks. See also Consistency Check and MDC.

Virtual Drive Order

See Logical Drive Order.