

# EMC VisualSAN<sup>®</sup>

## Version 2.2.1 Release Notes

These release notes contain information about EMC VisualSAN<sup>®</sup> version 2.2.1, which is an update version of the EMC VisualSAN 2.2.0 application. These notes supplement the version 2.2.0 Release Notes. For more information on version 2.2.0, refer to the [version 2.2.0 Release Notes](#).

For the most up to date information on this release, visit [support.dell.com](http://support.dell.com).

These notes include the following sections:

[Product Description](#)

[New Features and Changes](#)

[Before You Begin Installation](#)

[System Requirements](#)

[Supported Devices](#)

[Application Launch Requirements](#)

[License Keys](#)

[Known Issues](#)

## Product Description

This release is an update to the EMC VisualSAN application, the central management console for Storage Area Networks (SAN). The primary features of EMC VisualSAN are automatic discovery of SAN devices, representation of discovered elements, event management, zone management, asset inventory reporting, and application launch. EMC VisualSAN also includes a support management feature.

This update adds support for several devices and corrects some known operational issues. These release notes describe the features, system and configuration requirements, and known issues that affect the operation of the software.

[top](#)

## New Features and Changes

## Added Device Support

This release adds support for the following devices:

- McData Sphereon 4500 Fabric Switch
- Brocade SilkWorm 3900 Switch
- Emulex 9802-DC Fibre Channel HBA
- Microsoft Windows Server 2003 as the SAN Host

For more information on the supported firmware versions and required software, refer to the [Supported Devices](#) section of this document.

## Fixed Problems

### **4325 Changes in fan speed were not displayed in the application**

The application was not displaying changes in fan speed status. Fan speed displays for devices using the EMC CLARiiON® device manager and the PowerVault 660F. This problem has been corrected.

### **4460 DAEs connected on different buses display incorrectly on the Topology Map**

This problem occurred on configurations involving EMC CLARiiON FC4700 or EMC CLARiiON CX600 devices. When two DAEs were connected to the DPE, one on bus 0 and one on bus 1, the **Topology Map** displayed one DAE connected to the other, when it should display both DAEs connected to the DPE. This problem has been corrected.

### **4903 Zone control operations cannot be performed until Zone Settings are entered**

Previously, users had no way to know that they needed to enter a username and password before making any zone modifications. A notification message was added to the **Zone Explorer** dialog box to inform users of this requirement. This problem has been corrected.

### **4973 SNMP Traps for the EMC CLARiiON FC4700 caused exceptions**

Variable bindings were not included in SNMP Trap information for EMC CLARiiON FC4700 devices and caused SNMP traps to trigger exceptions. This problem has been corrected.

### **4959 VisualSAN incorrectly displayed ports on the EMC CLARiiON CX200 device**

After restarting the EMC CLARiiON CX200 device, EMC VisualSAN displayed the device with two back end ports instead of one. This problem has been corrected.

### **5040 Adding a plug-in module rearranged the menu and toolbar options**

After adding a plug-in module, the menu and toolbar options were randomly rearranged and not appended to the current menu and toolbar scheme. This problem has been corrected. Menu and toolbar options for plug-in modules are now determined by the order of plug-ins within the **visualsan.properties** file and the order of the item within the plug-in.

### **5078 SNMP Read Community was not populated for the PowerVault 530F device**

The appliance device manager did not provide the SNMP Read Community information for discovery. This information is now defined on the **Attributes** tab of the **Device Properties** dialog box. This problem has been corrected.

### **78974 Enhanced PowerVault 136T SNMP Trap Support**

Previously, SNMP traps sent from the PowerVault136T Remote Management Unit (RMU) and Fibre Channel Bridge were formatted incorrectly. In the VisualSAN Event Viewer and **Related Event** dialog box, correct trap information did not appear. This problem has been corrected and the following changes were made to the PowerVault 136T attributes:

- The **Storage Host** field was removed from the device attributes because it is not applicable data.
- The **IP Address** field in the device attributes now displays the IP address of both the RMU and Fibre Channel Bridge. Previously, only one IP address was displayed.
- The **SNMP Read Community** field previously displayed **Public** regardless of the device's actual SNMP community. This field now displays the SNMP Read Community set for the device.
- The **Properties** tab for tape drives displays the manufacturer and model. Previously, this tab displayed **Not Available** instead of actual data.

[top](#)

## **Before You Begin Installation**

Before installing the VisualSAN update, close all applications including the VisualSAN user interface. If the user interface is not closed, installation terminates and you are not able to continue. In addition, an error message is logged in the `patchinstalllog.txt` in the `[installation_directory]\diagnostics\log\` directory. This update modifies VisualSAN program files, so before beginning this update, you must close the application and stop its services.

This update performs the necessary configuration checking and ensures that the following conditions are true for the system:

- Is running on a Windows environment.
- Is the local Management Station.
- Meets the minimum system requirements and has 35 MB of free disk space. The free space is required for the update installation only.

- Has a valid version of VisualSAN already installed. This update is compatible with certain versions of VisualSAN; if the installation program detects that the update is incompatible, the installation will not proceed.

If any of the preceding conditions are not met, setup is terminated and an error is logged in `patchinstalllog.txt`. Before attempting installation again, check the error log and correct the error condition.

**Notice:** After installing the patch upgrade, it is not possible to remove the patch and revert to the previously installed version of VisualSAN. To do so, you must completely remove the VisualSAN application.

**Important!** If you have made any edits to the files listed in the [File Manifest](#), you may want to make a backup copy before beginning the update process.

[top](#)

## System Requirements

If you are upgrading from version 2.2.0, then your system has already met the minimum system requirements. Additionally, this update requires 35 MB of free disk space to run the upgrade installation and update your management console to VisualSAN version 2.2.1.

Configuration	Minimum Hardware	Recommended Hardware	Software
Management Station	Intel® Pentium® III 500-MHz system with: <ul style="list-style-type: none"> <li>• 512 MB of RAM</li> <li>• 35 MB free disk space required for the update installation</li> </ul>	Intel® Pentium® III 1000-MHz system with: <ul style="list-style-type: none"> <li>• 1024 MB of RAM</li> <li>• 35 MB free disk space required for the update installation</li> </ul>	Microsoft® Windows® 2000 Professional (SP2, SP3)  Windows 2000 Server (SP2, SP3)  Windows 2000 Advanced Server (SP2, SP3)  Optional: A Web server needs to be installed and configured in order to publish the application.
Web User Interface (applet)	Pentium III 500-MHz system with:	Pentium III 500-MHz system with:	Windows 2000 Professional (SP2, SP3)

	<ul style="list-style-type: none"> <li>• 256 MB of RAM</li> </ul>	<ul style="list-style-type: none"> <li>• 512 MB of RAM</li> </ul>	<p>Windows 2000 Server (SP2, SP3)</p> <p>Windows 2000 Advanced Server (SP2, SP3)</p> <p>Windows XP Professional</p> <p>For Windows, Microsoft Internet Explorer version 5.0 or later or Netscape Navigator version 6.2 or later</p> <p>Java Runtime Edition (JRE) 1.3.1_03</p>
--	---	---	--

In addition, for all systems, ensure the following:

- EMC VisualSAN supports discovery of Windows SAN hosts only. Support for other operating systems will be provided in a future release.
- If you are using Microsoft SQL Server 7.0 or SQL Server 2000, set the **Authentication Method** to **Mixed Mode**. This setting enables connection by either Windows Authentication or SQL Server Authentication. For more information on this setting, refer to [msdn.microsoft.com](http://msdn.microsoft.com).
- To receive SNMP traps from the application, the Windows SNMP Trap Service must be running. To verify this, double-click **Services** in **Administrative Tools**.
- EMC VisualSAN needs access to the Domain Name Service (DNS) in order to resolve IP addresses into host names. Resolving an IP address involves communication with a Domain Name Server running DNS. It is necessary to ensure that all hosts have their DNS settings configured correctly; otherwise pauses in operation can occur while waiting for DNS connections to time out. If you are unsure of the DNS settings for a host, you can disable the DNS settings for the host in order to avoid this delay.  
To verify that the DNS client is running, double-click **Services** in **Administrative Tools**.
  - To display accurate device names, the DNS table must reference both the hostname to the IP address and the IP address to the hostname.
- Display settings are configured as follows, as required by the application user interface:
  - Screen Area — 800 by 600 pixels or greater

- Colors — 256 colors or greater

To verify these settings in Windows, double-click **Display** in the **Control Panel**, and click the **Settings** tab.

- A valid domain user account name and password are required to access the application or applet. If the Management Station is not included in a domain, a valid user account on the local Management Station is required to login to the application. In this case, the Management Station's hostname should be entered instead of the domain name. To restrict access to the applet, security must be setup through the Web server (for example, Internet Information Services [IIS]).
- The Web server must be configured to point to **visualsan.html** in the EMC VisualSAN directory in order to publish the application.
- The EMC VisualSAN installation requires a C drive to be available to write temporary files even if the software is not being installed on the C drive. This issue will be addressed in a future release.
- It is recommended that only one Management Station be installed per SAN.
- To perform zone control and zone visualization, make sure that all switches in a fabric are set to the same username and password.

[top](#)

## Supported Devices

Model	Software/Firmware Levels	Software Configuration Required for Discovery
<b>FC Storage Arrays</b>		
Dell PowerVault 650F	Firmware (Flare) version 5.11.17 or higher	Dell OpenManage™ CLI or NAVICLI on Management Station. Dell PowerVault SAN 5.0 (or higher) software configuration. Dell PowerVault 650F SNMP Agent installed on one Data Managed Node per PowerVault 650F zone.

PowerVault 630F	Firmware (Flare) version 5.11.17 or higher	Dell OpenManage CLI or NAVICLI on Management Station. Dell PowerVault SAN 5.0 (or higher) software configuration.
PowerVault 660F	Firmware version 7.82-00 or higher SES version 1.9.5 or higher	Dell OpenManage Array Manager 3.1.2 with SNMP patch.
PowerVault 224F	Firmware version 7.82-00 or higher SES version 1.9.5 or higher	Dell PowerVault SAN 5.0 (or higher) software configuration.
FC5300-DPE	Any valid Dell   EMC firmware level with Access Logix	NAVICLI on Management Station. Valid Dell   EMC SAN Configuration with Access Logix*.
FC4500-DPE	Any valid Dell   EMC firmware level with Access Logix	NAVICLI on Management Station. Valid Dell   EMC SAN Configuration with Access Logix*.
FC4700-DPE	Any valid Dell   EMC firmware level with Access Logix FA MIB Software Package required	NAVICLI on Management Station. Valid Dell   EMC SAN Configuration with Access Logix*. The SNMP community of <b>PUBLIC</b> must be entered into EMC VisualSAN to discover this device. The FA MIB

		Software Package is required for discovery.
FC4700, FC4500, FC5300-DAE	Any valid Dell   EMC firmware level	NAVICLI on Management Station.
CX600	Any valid Dell   EMC firmware level with Access Logix. FA MIB Software Package required	NAVICLI 6.2 or higher on Management Station. Valid Dell   EMC SAN Configuration with Access Logix*.
CX400	Any valid Dell   EMC firmware level with Access Logix. FA MIB Software Package required	NAVICLI 6.2 or higher on Management Station. Valid Dell   EMC SAN Configuration with Access Logix*.
CX200	Any valid Dell   EMC firmware level with Access Logix. FA MIB Software Package required	NAVICLI 6.2 or higher on Management Station. Valid Dell   EMC SAN Configuration with Access Logix*.
DAE2-Fibre	Any valid Dell   EMC firmware level	NAVICLI 6.2 or higher on Management Station.
DAE2-ATA	Any valid Dell   EMC firmware level	NAVICLI 6.4 or higher on Management Station.
<b>Tape Devices - SAN Attached</b>		
PowerVault 120T DLT4000 AL	Firmware D116	Dell Tape Discovery Agent installed on Tape Backup System and SNMP write

		community set. See the Dell Tape Discovery Agent readme for details.
PowerVault 120T DLT7000	Firmware D116	Dell Tape Discovery Agent installed on Tape Backup System and SNMP write community set. See the Dell Tape Discovery Agent readme for details.
PowerVault 130T DLT4000/DLT7000	Firmware 1604	Dell Tape Discovery Agent installed on Tape Backup System and SNMP write community set. See the Dell Tape Discovery Agent readme for details.
PowerVault 128T LTO	Firmware 1.40.D or higher required	The SNMP read community of <b>PUBLIC</b> must be entered into EMC VisualSAN to discover this device.
PowerVault 136T	RMU Firmware 160D.00004 or higher Library Firmware 2.73 or higher Fibre Channel Module 4.22.412 or higher	RMU Firmware 160D.00004 or higher Library Firmware 2.73v Fibre Channel Module 4.22.412 or higher
<b>SAN Appliances</b>		
PowerVault 530F	Firmware version 2.23	Dell PowerVault SAN 5.0 (or higher) software configuration. Configuration must be saved in OLConfig from the

		PowerVault530F console in order for EMC VisualSAN to discover backend HBAs.
<b>SAN Switches</b>		
PowerVault 51F	Firmware version 2.5.0d	PowerVault SAN 5.0 (or higher) software configuration.
PowerVault 56F	Firmware version 2.5.0d	PowerVault SAN 5.0 (or higher) software configuration.
DS-8B	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
DS-16B	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
DS-16B2 Silkworm 3800	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
Brocade Silkworm 3200	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
Brocade SilkWorm 3900	Firmware version 4.0.2.c or higher for discovery and zoning.	Valid Dell   EMC SAN Configuration*.
DS-16M	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
DS-32M	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
DS-16M2 McData Sphereon 3216	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
DS-32M2 McData Sphereon 3232	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
McData Sphereon 4500	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN

		Configuration*.
<b>SAN Bridges and Routers</b>		
PowerVault 35F	PowerVault 35F firmware 2.2 d9913n or higher.	PowerVault 35F firmware 2.2 d9913n or higher.
<b>FC Host Bus Adapters Dell PowerVault SAN 5.0 or higher</b>		
QLogic FC HBA 2200/2200F	Driver version 8.00.09.22 or higher BIOS version 1.76 or higher	PowerVault SAN 5.0 (or higher) software configuration. QLogic QMS SNMP Agent installed on all Managed Hosts.
QLogic FC HBA 2200/66 MHz	Driver version 8.00.09.22 or higher BIOS version 1.76 or higher	PowerVault SAN 5.0 (or higher) software configuration. QLogic QMS SNMP Agent installed on all Managed Hosts.
<b>FC Host Bus Adapters Dell   EMC SAN</b>		
QLogic 2310	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
Emulex LP8000	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
Emulex LP9002L	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
Emulex LP9802	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
Emulex LP9802-DC	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
Emulex LP982	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
QLogic 2340	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN

		Configuration*.
QLogic 2342	Any valid Dell   EMC firmware level	Valid Dell   EMC SAN Configuration*.
<b>MSCS Clusters</b>		
MSCS Clusters	Windows 2000 Advanced Server with Windows Cluster Service	Dell Cluster SNMP Agent on each cluster node.
<b>SAN Host (Managed Node)</b>		
SAN Host	Microsoft Windows 2000 Server, Advanced Server, Professional (SP2,3)	SNMP Enabled. Dell OpenManage Server Administrator is not required, but EMC VisualSAN will be able to gather more information about the server if it is installed.
SAN Host	Microsoft Windows NT 4.0 Server, Advanced Server (SP5,6a)	SNMP Enabled. Dell OpenManage Server Administrator is not required, but EMC VisualSAN will be able to gather more information about the server if it is installed.
SAN Host	Microsoft Windows Server 2003 Standard Edition, Web Edition, Enterprise Edition	SNMP Enabled. Dell OpenManage Server Administrator is not required, but EMC VisualSAN will be able to gather more information about the server if it is installed.
<b>Dell PowerVault NAS on SAN</b>		
PowerVault 750N	N/A	Dell   EMC SAN Configuration*. Dell Cluster SNMP Agent required on

		NAS Cluster Nodes.
PowerVault 755N	N/A	Dell   EMC SAN Configuration*. Dell Cluster SNMP Agent required on NAS Cluster Nodes.
PowerVault 770N	N/A	Dell   EMC SAN Configuration*. Dell Cluster SNMP Agent required on NAS Cluster Nodes.
PowerVault 775N	N/A	Dell   EMC SAN Configuration*. Dell Cluster SNMP Agent required on NAS Cluster Nodes.

\*See the EMC Support Matrix for details. The EMC Support Matrix is updated every month with new firmware levels.

**Notes:**

- The previous list of devices has been validated to work with the EMC VisualSAN application. While VisualSAN may discover other unsupported devices, using VisualSAN with these devices is not recommended, and may cause VisualSAN instability and potential loss of VisualSAN data.
- All devices must be configured to send SNMP Traps to the Management Station for Event Handling.
- All clustered NAS devices are represented and listed as a Cluster Server rather than a NAS device. Both cluster and NAS attributes are populated for the device.

[top](#)

## Application Launch Requirements

EMC VisualSAN allows users to launch the appropriate applications by right-clicking the discovered devices. The most common SAN applications will appear automatically on right click of the devices, while other launchable applications can be added manually.

<b>Application</b>	<b>Management Station Requirements</b>	<b>Managed Node Requirements</b>	<b>Activated by Right-Click</b>
Dell OpenManage Server Administrator	Internet Explorer or Netscape Navigator	Dell OpenManage Server Administrator.	Host and NAS.
Dell OpenManage Cluster Assistant with ClusterX	ClusterX Console, Dell Software Agent	Dell Cluster SNMP Agent, Dell Software SNMP Agent.	Clustered Host and Clustered NAS.
Dell OpenManage Array Manager	ArrayManager Console.	Array Manager Agent, Dell Software SNMP Agent.	Host, PowerVault 660F, and NAS.
Dell OpenManage Storage Consolidation	Storage Consolidation Console, Dell Software SNMP Agent.	Storage Consolidation Agent, Dell Software SNMP Agent.	Host.
VERITAS® BackupExec™	VERITAS Backup Exec	VERITAS Backup Exec, Dell Software SNMP Agent.	Tape backup host, PowerVault 128T, 130T, and 120T.
Computer Associates® ARCserve™	Computer Associates ARCserve, Dell Software SNMP Agent.	Computer Associates ARCserve, Dell Software SNMP Agent.	Tape backup host, PowerVault 128T, 130T, and 120T.
QLogic QMSJ	QMSJ Console, Dell Software SNMP Agent.	QMSJ Agent, Dell Software SNMP Agent.	Host and HBA.
QLogic SANblade Manager	Launch point from EMC VisualSAN will be provided in a later release.	Launch point from EMC VisualSAN will be provided in a later release.	
PowerVault NAS Manager	Internet Explorer or Netscape Navigator	N/A	PowerVault 750N, PowerVault 755N, PowerVault 770N, and PowerVault 775N
Brocade Web UI	Internet Explorer or	N/A	FC Switch.

	Netscape Navigator		
McData Web UI	Internet Explorer or Netscape Navigator	N/A	FC Switch.
PowerVault 35F Web UI	Internet Explorer or Netscape Navigator	N/A	PowerVault 35F.
PowerVault 128T Web UI	Internet Explorer or Netscape Navigator	N/A	PowerVault 128T.
Data Administrator	Data Administrator, Dell Software SNMP Agent.	Data Agent, Dell Software SNMP Agent.	Host and PowerVault 650F.
Data Supervisor	Data Supervisor, Dell Software SNMP Agent.	Data Agent, Dell Software SNMP Agent.	Host and PowerVault 650F.
Navisphere Manager 5.2.5 and 5.3.	Navisphere Manager 5.2.5 and 5.3	Navisphere Agent 5.2.5 and 5.3	FC4700, FC4500, FC5300
Navisphere Manager 6.0 and higher	See Navisphere setup guidelines.	See Navisphere setup guidelines.	VisualSAN detects the Navisphere WebContent 6.X (Navisphere Management UIs) if it is installed on the management station, and adds it as a launchable management attribute. In addition, users can add support for launching Navisphere 6.X or higher by adding the Management URL for the Navisphere Management Server from the array's properties page.

**NOTE:** When using EMC VisualSAN through a Web browser, the local station must have the same configuration as the Management Station in order to launch the supported applications.

[top](#)

## License Keys

License Keys for this product can be retrieved from the following website:  
<http://www.dell.com/EMC/VisualSAN/>

License keys can be entered through the EMC VisualSAN user interface through the **Settings**→**License Administrator**→**License**→**Enter License Key** menu.

[top](#)

## Known Issues

For information on issues reported in the version 2.2.0 release, refer to the [VisualSAN Version 2.2.0 Release Notes](#).

### **2954 Communicating with the Login service and proxy server is unsuccessful**

*This issue has been updated since release 2.2.0.*

When the property `DB_DBMS` in **system.properties** is set to `FreeTDS`, the application and applet cannot communicate with the Login service and proxy server. This issue is due to a security setting that restricts the JDBC driver from creating a socket to communicate with the SQL Server.

This issue has been corrected by opening the default port for MSDE, port 1433. If the SQL Server uses a port other than 1433, you need to:

- Edit the `DB_PORT` in `[installation_directory]\config\nm\system.properties` and the `config\nm\java2.policy` with the new correct port number.
- In Windows, stop and restart the VisualSAN services.

### **5317 Cold-start SNMP Traps for the Brocade SilkWorm 3900 are formatted incorrectly**

When the Brocade SilkWorm 3900 is powered on, a cold-start SNMP trap is generated and displayed in the VisualSAN Event Viewer. However, this trap information is non-descriptive and does not indicate that the trap was generated from a cold-start.

### **5327 Deleting LUNs in Navisphere does not remove them from VisualSAN**

LUNs created in Navisphere Manager are appropriately added to VisualSAN. However, when LUNs are deleted from Navisphere or one of its components, the modification is not updated in VisualSAN and the LUNs continue to display in OK status.

### **75698 Traps from the Brocade SilkWorm 3900 switch do not display in VisualSAN**

While other traps such as the power supply failure traps are displayed in the VisualSAN Event Viewer, the traps for a fan failure and recovery are not being displayed.

[top](#)

## **File Manifest**

This update includes a file manifest that lists all files that were edited with this update. The files listed below are completely overwritten as part of the update process. Any modifications previously made to any of the following files are not preserved:

```
[installation_directory]\Release_Notes_2.2.0.html
[installation_directory]\VisualSAN.html

[installation_directory]\config\nm\Silkworm.properties
[installation_directory]\config\nm\TrapsLookup\NaviTrapDescr.properties

[installation_directory]\diagnostics\log\patchinstalllog.txt

[installation_directory]\lib\app.jar
[installation_directory]\lib\cm.jar
[installation_directory]\lib\common.jar
[installation_directory]\lib\dell.jar
[installation_directory]\lib\intl.jar
[installation_directory]\lib\nm.jar
[installation_directory]\lib\pm.jar
[installation_directory]\lib\thirdparty.jar
```

In addition to these overwritten files,

```
[installation_directory]\config\nm\vendorsettings.properties and
[installation_directory]\config\nm\devicemgr.properties are modified. New
information is appended to the end of these files.
```

---

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purchase. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

*EMC<sup>2</sup>*, *EMC*, *VisualSAN*, *CLARiiON*, and *Navisphere* are registered trademarks of EMC Corporation. All other trademarks used herein are the property of their respective owners.

Copyright © 2003 EMC Corporation. All rights reserved.

---

©2003 Dell Computer Corporation. All rights reserved. Reproduction in any manner whatsoever without the written permission of Dell is strictly forbidden.

Trademarks used in this text: *Dell*, the *DELL* logo, *Dell OpenManage*, and *PowerVault* are trademarks of Dell Computer Corporation; *Intel* and *Pentium* are registered trademarks of Intel Corporation; *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation; *VERITAS* is a registered trademark and *Backup Exec* is a trademark of VERITAS Software; *Computer Associates* is a registered trademark and *ARCserve* is a trademark of Computer Associates, International.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.