Dell DL4000 Appliance
Deployment Guide

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2015 - 12

Rev. A05

Contents

1 Setting up DL4000 Appliance 5

Introduction 5
Available configurations 5
Terms Used in This Document 6
Installation prerequisites 6
Network requirements 6
Recommended network infrastructure 7
Setting up the hardware 7
Installing the appliance in a rack 7
Cabling the appliance 7
Setting the storage enclosure configuration switch 7
Connecting the storage enclosure to the system 8
Connecting the Cable Management Arm (Optional) 8
Turning on the appliance 8
DL4000 disk configurations 8

2 Initial software setup 10

AppAssure Appliance Configuration Wizard 10
Configuring the network interface 11
Configuring host name and domain settings 11
Configuring SNMP settings 12
Rapid Appliance Self Recovery 13
Creating Windows and RASR virtual disk(s) 13
Executing RASR through the RASR USB key 13
Creating the RASR USB key 14
Provisioning storage 15
Provisioning selected storage 16
Configuring the DL4000 using fibre channel storage (optional) 16

3 Post installation tasks 18

Resetting the operating system to default settings 18
Accessing the Core Console 18
Updating trusted sites in Internet Explorer 19
Configuring browsers to remotely access the Core Console 19
Reviewing retention periods 19
Encrypting agent snapshot data 20
Configuring an email server and email notification template 20
Adjusting the number of streams 21

Protecting machines and checking connectivity to clients....21
Checking network connectivity....22
Checking the firewall settings....22
Verifying name resolution (if applicable)....22
Teaming network adapters....23
Reinstalling Broadcom Advanced Configuration Suite....23
Creating the NIC team....23
Configuring a Hyper-V Virtual Switch....24

4 Installing agents on clients....25
Installing agents remotely (push)....25
Deploying the agent software when protecting an agent....26
Installing Microsoft Windows agents at the client....27
Adding an agent by using the license portal....27
Installing agents on Linux machines....28
Location of Linux agent files....28
Agent dependencies....29
Installing the agent on Ubuntu....30
Installing the agent on Red Hat Enterprise Linux and CentOS....30
Installing the agent on SUSE Linux Enterprise Server....31

5 Getting help....32
Finding documentation and software updates....32
Finding software updates....32
Contacting Dell....32
Documentation feedback....32

1

Setting up DL4000 Appliance

Introduction

The Dell DL4000 appliance is the latest generation of backup to disk protection appliance powered by Dell AppAssure software. The appliance allows:

- Scalable storage capabilities to support organizations of any size
- Faster backups, as well as quicker recovery scenarios over conventional tape devices and backup methodologies
- Optional deduplication capability
- Continuous data protection for data center and remote office servers
- Quick and easy deployment experience that reduces the time required to begin protecting critical data
- Optional Fibre Channel configuration

Available configurations

The DL appliance comes in two configurations: Standard Edition and High Capacity Edition.

Table 1. DL4000 Standard Edition Capacity Configurations

Capacity	Hardware Configuration
5TB	DL4000 with Internal Storage Only
10TB	DL4000 with Internal Storage and 1 x MD1200 with 12 x 1TB Drives
20TB	DL4000 with Internal Storage and 1 x MD1200 with 12 x 2TB Drives
40TB	DL4000 with Internal Storage and 1 x MD1200 with 12 x 4TB Drives

Table 2. DL4000 High Capacity Edition Capacity Configurations

Capacity	Hardware Configuration
20TB	DL4000 with Internal Storage and 1 x MD1200 with 12 x 2TB Drives
40TB	DL4000 with Internal Storage and 1 x MD1200 with 12 x 4TB Drives
60TB	DL4000 with Internal Storage and 2 x MD1200 • First MD1200 with 12 x 4TB Drives (40TB)

Capacity	Hardware Configuration
	• Second MD1200 with 12 x 2TB Drives (20TB) OR • First MD1200 with 12 x 3TB Drives (30TB) • Second MD1200 with 12 x 3TB Drives (30TB)
80TB	DL4000 with Internal Storage and 2 x MD1200 • First MD1200 with 12 x 4TB Drives (40TB) • Second MD1200 with 12 x 4TB Drives (40TB)

NOTE: All models except for the Standard Edition 5TB model use the internal storage on the DL4000 for VM storage, archive storage, or other scratch space.

NOTE: Additional storage can be added through expansion shelves (Dell PowerVault MD1200). Additional storage can be added to any model, however the Standard Edition has a maximum capacity of 40TB and the High Capacity Edition has a maximum capacity of 80TB. Both editions allow for up to a maximum of four expansion shelves.

Each configuration includes the following hardware and software:

- Dell DL4000 system
- Dell PowerEdge RAID Controllers (PERC)
- Preinstalled operating system and Dell OpenManage system and storage management software
- AppAssure software

NOTE: If your appliance configuration does not include PowerVault MD1200 storage enclosures, ignore any references to PowerVault MD1200 and storage enclosures in this document.

Terms Used in This Document

The following table lists the terms used in this document to refer to various hardware and software components of the DL4000 appliance.

Table 3. DL4000 Appliance Hardware and Software Components

Component	Term Used
DL4000 Appliance	Appliance
DL4000 system	DL4000 system
PowerVault MD1200 storage enclosure	Storage enclosure
Dell AppAssure Software	AppAssure

Installation prerequisites

Network requirements

Your Appliance requires the following network environment:

- Active network with available Ethernet cables and connections
- A static IP address and DNS server IP address, if not provided by the Dynamic Host Configuration Protocol (DHCP)
- User name and password with administrator privileges

Recommended network infrastructure

Dell recommends that organizations use a 1 GbE backbone for efficient performance for use with AppAssure and 10 GbE networks for extremely robust environments.

Setting up the hardware

The appliance ships with a single DL4000 system. Before setting up the appliance hardware, see the *Dell DL4000 Appliance Getting Started With Your System* document that shipped with the appliance. Unpack and set up the DL Appliance hardware.

NOTE: The software is pre-installed on the appliance. Any media included with the system must be used only in the event of a system recovery.

To set up the DL Appliance hardware:

1. Rack and cable the DL4000 system and storage enclosure(s).
2. Turn on the storage enclosure(s) and then the DL4000 system.

Installing the appliance in a rack

If your system includes a rail kit, locate the *Rack Installation Instructions* supplied with the rack kit. Follow the instructions to install the rails in the rack unit, the system, and the storage enclosure in the rack.

Cabling the appliance

Locate the *Getting Started With Your System* document that shipped with your appliance. Follow the instructions to attach the keyboard, mouse, monitor, power, and network cables to the appliance.

Setting the storage enclosure configuration switch

Set the storage mode for the storage enclosure to unified mode as indicated in the following figure.

NOTE: The configuration switch must be set before turning on the storage enclosure. Changing the configuration mode after turning on the storage enclosure has no effect on enclosure configuration until the system is power cycled. For more information, see the *Dell PowerVault MD1200 Hardware Owner's Manual* at **dell.com/support/home**.

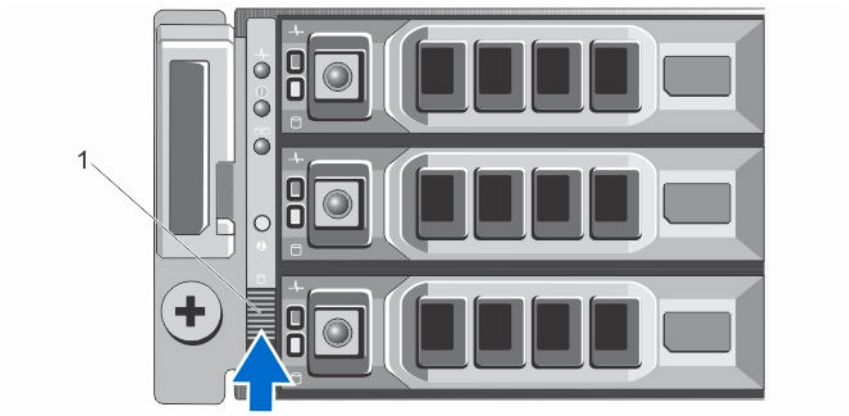

Figure 1. Setting the PowerVault MD1200 storage enclosure configuration switch

1. configuration switch

Connecting the storage enclosure to the system

Connect the data cable from the PowerEdge RAID Controller (PERC) installed in the Dell DL4000 system to the primary Enclosure Management Module (EMM) SAS **In** port of the storage enclosure.

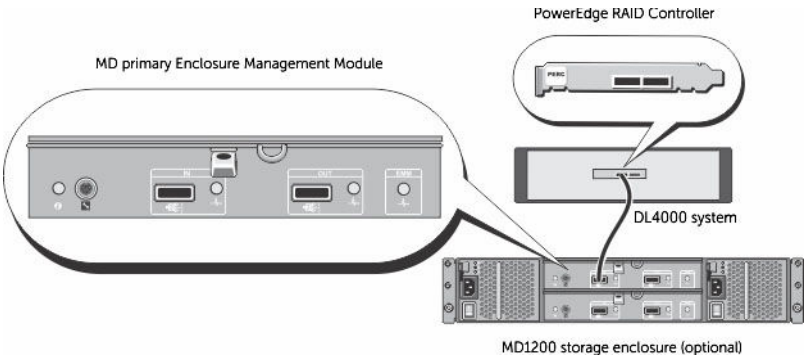

Figure 2. Connecting the SAS cable from the DL4000 system to the Powervault MD1200 storage enclosure

Connecting the Cable Management Arm (Optional)

If the appliance includes a Cable Management Arm (CMA), locate the CMA *Installation Instructions* that shipped with the CMA kit and follow the instructions to install the CMA.

Turning on the appliance

After cabling the appliance, turn on the MD1200 storage enclosure, and then turn on the DL4000 system.

NOTE: It is recommended that you connect the appliance to an Uninterrupted Power Supply (UPS) for maximum reliability and availability.

DL4000 disk configurations

The DL4000 supports SAS and nearline SAS drives only. The operating system resides on a RAID 1 (mirrored) virtual disk located in slots 0 and 1. For information on these disks, see the *Dell DL4000 Appliance Owner's Manual* at **dell.com/support/home**. Drive slots 2 through 9 are available for automatic

configuration by the AppAssure Appliance Configuration wizard (recommended) but can be manually configured for custom configurations if required.. The disks are auto-provisioned as RAID 6. Capacity expansion using an MD1200 storage enclosure is optional.

2

Initial software setup

When you turn on the appliance for the first time, and change the system password, the **AppAssure Appliance Configuration Wizard** runs automatically.

1. After you turn on the system, choose your operating system language from the Windows language options.
2. The Microsoft EULA (End User License Agreement) is displayed on the **Settings** page.
3. To accept the EULA, click **I accept** button.

   A screen to change the administrator password is displayed.
4. Click **OK** on the message that prompts you to change the administrator password.
5. Enter and confirm the new password.

   A message prompts you confirming that the password is changed.
6. Click **OK**.
7. From the **Dell readme.htm** screen, scroll down and click **Proceed**.
8. Log on using the changed administrator password.

The **AppAssure Appliance Configuration Wizard** welcome screen is displayed.

NOTE: The **AppAssure Appliance Configuration Wizard** may take up to 30 seconds to display on the system console.

CAUTION: Make sure you complete all the steps of AppAssure Appliance Configuration Wizard before performing any other task or change any settings on the Appliance. Do not make any changes through the Control Panel, use Microsoft Windows Update, update AppAssure software or install licenses, until the wizard is complete.

NOTE: Do not close the **AppAssure Appliance Configuration Wizard** until all the tasks have been completed.

AppAssure Appliance Configuration Wizard

CAUTION: Make sure you complete all the steps of AppAssure Appliance Configuration Wizard before performing any other task or change any settings on the Appliance. Do not make any changes through the Control Panel, use Microsoft Windows Update, update AppAssure software or install licenses, until the wizard is complete.

The **AppAssure Appliance Configuration Wizard** guides you through the following steps to configure the software on the appliance.

- Configuring the network Interface
- Configuring host name and domain settings
- Configuring SNMP settings

- Rapid Appliance Self Recovery

On completing the installation using the wizard, the Core Console launches automatically.

Configuring the network interface

To configure the available network interfaces:

1. On the **AppAssure Appliance Configuration Wizard Welcome** screen, click **Next**.
   The **network interfaces** page displays the available connected network interfaces.
2. Select the network interfaces that you want to configure.

   NOTE: The **AppAssure Appliance Configuration wizard** configures network interfaces as individual ports (non-teamed). To improve ingest performance, you can create a larger ingest channel by teaming NICs. However, this must be done after the initial configuration of the appliance.
3. If required, connect additional network interfaces and click **Refresh**.
   The additional connected network interfaces will be displayed.
4. Click **Next**.
   The **Configure selected network interface** page is displayed.
5. Select the appropriate internet protocol for the selected interface.
   You can choose **IPv4** or **IPv6**.

   The network details are displayed depending on the internet protocol you select.
6. To assign the internet protocol details, do one of the following:
   - To assign the selected internet protocol details automatically, select **Obtain an IPV4 address automatically**.
   - To assign the network connection manually, select **Use the following IPv4 address** and enter the following details:
     - **IPv4 Address** or **IPv6 Address**
     - **Subnet mask** for IPv4 and **Subnet prefix length** for IPv6
     - **Default Gateway**
7. To assign the DNS server details, do one of the following:
   - To assign the DNS server address automatically, select **Obtain DNS server address automatically**.
   - To assign the DNS server manually, select **Use the following DNS server address** and enter the following details:
     - **Preferred DNS sever**
     - **Alternate DNS server**
8. Click **Next**.
   The **Configure hostname and domain setting** page is displayed.

For information on NIC teaming, see Teaming Network Adapters.

Configuring host name and domain settings

You must assign a host name for the appliance. It is recommended that you change the host name before starting backups. By default, the host name is the system name that the operating system assigns.

NOTE: If you plan to change the host name, it is recommended that you change the host name at this stage. Changing the host name after completing the **AppAssure Appliance Configuration wizard** requires manually performing several steps.

To configure the host name and domain settings:

1. On the **Configure host name and domain setting** page, to change the host name for the appliance, in **New host name** enter an appropriate host name.
2. If you do not want the appliance to join a domain, select **No** in **Do you want this appliance to join a domain?**

   By default, **Yes** is selected.
3. To join the appliance to a domain, enter the following details:
   - **Domain name**
   - **Domain user name**

     NOTE: The domain user must have local administrative rights.
   - **Domain user password**
4. Click **Next**.

   NOTE: Changing the host name or the domain requires restarting the machine. After restarting the machine, the **AppAssure Appliance Configuration wizard** launches automatically. If the appliance is joined to a domain, after restarting the machine, you must log in as a domain user with administrative privileges on the appliance.

   The **Configure SNMP Settings** page is displayed.

Configuring SNMP settings

Simple Network Management Protocol (SNMP) is a commonly used network management protocol that allows SNMP-compatible management functions such as device discovery, monitoring, and event generation. SNMP provides network management of the TCP/IP protocol.

To configure SNMP alerts for the appliance:

1. On the **Configure SNMP Settings** page, select **Configure SNMP on this appliance** on the **Configure SNMP Settings** page.

   NOTE: Deselect **Configure SNMP on this appliance** if you do not want to set up SNMP details and alerts on the appliance and skip to step 6.
2. In **Communities**, enter one or more SNMP community names.

   Use commas to separate multiple community names.
3. In **Accept SNMP packets from these hosts**, enter the names of hosts with which the appliance can communicate.

   Separate the host names with commas, or leave blank to allow communication with all hosts.
4. To configure SNMP alerts, enter the **Community Name** and the **Trap destinations** for the SNMP alerts and click **Add**.

   Repeat this step to add more SNMP addresses.
5. To remove a configured SNMP address, in **Configured SNMP addresses**, select the appropriate SNMP address and click **Remove**.
6. Click **Next**.

   The **Create Windows and RASR virtual disk(s)** page is displayed.

Rapid Appliance Self Recovery

Rapid Appliance Self Recovery (RASR) is a bare metal restore process where the operating system drives and data drives are used to rebuild the default factory image.

Creating Windows and RASR virtual disk(s)

The DL4000 system supports:

- Two operating system drives, twelve data drives, and four internal hard drives
- Option to create Logical Unit Numbers (LUNs) for the Bare Metal Restore (BMR) information to be stored
- Option to create separate space for the Windows backup RASR file.

To create optional virtual disk(s):

1. Select the following virtual disks:
   a. Windows Backup virtual disk

      Windows backup virtual disk provides the target space to create Windows Server backups. To create a Windows Server backup, go to the **Backup** page in **Appliance** tab in AppAssure Core. If you skipped this option in the **AppAssure Appliance Configuration Wizard**, you will not be able to create a Windows Server backup and configure a backup policy in the **Backup** page. See Executing the RASR through RASR USB key for details.
   b. Bootable RASR virtual disk

      Bootable RASR virtual disk provides a redundant recovery volume to perform a RASR recovery. You can reboot to the redundant recovery volume by pressing< F8> during POST. After rebooting, follow the steps in Executing the RASR through RASR USB key.
2. Click **Next**.

   A thank you screen is displayed while the system is configuring. A Configuration complete message is displayed.
3. Click **Exit**.

   The Core Console launches automatically.
4. Continue the configuration process by Provisioning storage

Executing RASR through the RASR USB key

To execute the RASR using the RASR USB key:

1. Insert the RASR USB key created. See Creating the RASR USB Key.
2. Reboot the appliance through the RASR USB key.

   The following message is displayed:

   ```
   The secondary SD card is missing, not responding, or in write-protected
   mode. Do one of the following: 1) Install a SD card media in the secondary
   SD card reader. 2) Reseat or replace the SD card media.3) If write-
   protected mode is expected, then no respose action is required.
   ```

   Ignore the above message.
3. Click **Troubleshoot → Rapid Appliance Self Recovery**.

   The **Recovery Tool** screen is displayed.

4. Select the Windows operating system version.

   Windows cmd screen is displayed after which the RASR welcome screen is displayed.

5. Click **Next**.

   The **Prerequisites** screen is displayed.

   NOTE: Ensure all the hardware and other prerequisites are checked before performing the RASR.

6. Click **Next**.

   The **Recovery Mode Selection** screen is displayed with three options:

   - **System Recovery** — This option is disabled by default. To enable this option select the **Windows Backup virtual disk** when creating the virtual disks using the **AppAssure Appliance Recovery Wizard**. System Recovery allows you to select and restore from Windows backups that were created on Windows backup virtual disk.
   - **Windows Recovery Wizard** — This option is the default Microsoft Windows Recovery wizard that uses the network share to backup the operating system.
   - **Factory Reset** — This option will recover the operating system disk from the factory image.

7. Select **Factory Reset**.
8. Click **Next**.

   The **Storage Configuration** screen is displayed.

9. In the **OS Recovery** screen, RASR completed screen is displayed with the following message: `The system has been recovered successfully`.
10. Click **Finish** to exit the RASR.

Creating the RASR USB key

NOTE: After the initial setup of the software, the **AppAssure Appliance Configuration Wizard** starts automatically. The **Appliance** tab status icon is yellow.

To create a RASR USB key:

1. Navigate to the **Appliance** tab.
2. Using the left pane navigation, select **Appliance** → **Backup**.

   Create RASR USB Drive window is displayed.

   NOTE: Insert a 16 GB or larger USB key before attempting to create the RASR key.

3. After inserting a 16 GB or larger USB key, click on **Create RASR USB Drive now**.

   A **Prerequisite Check** message is displayed.

   After the prerequisites are checked **Create the RASR USB Drive** window displays the minimum size required to create the USB drive and **List of Possible target paths**.

4. Select the target and click **Create**.

   A warning dialog box is displayed.

5. Click **Yes**.

   The RASR USB Drive key is created.

6. NOTE: Make sure to use the Safely Remove USB Drive or the Windows Eject Drive function to prepare the USB key for removal. Otherwise, the content in the USB key may be damaged and the USB key will not work as expected.

   Remove the key, label, and store for future use.

Provisioning storage

The appliance configures available DL4000 internal storage and any attached external storage enclosures for:

- AppAssure Repositories

  NOTE: If fibre channel HBA is configured then the process of creating the repositories is manual. AppAssure will not create a repository automatically in the root directory. For more information, see Configuring The DL4000 Using Fibre Channel Storage (Optional).

- Virtual Standby of Protected Machines

NOTE: MD1200s with 1TB, 2TB, 3TB, or 4TB (for high capacity) drives connected to the H810 controller are supported. Up to four MD1200s are supported.

NOTE: The DL4000 high-capacity configuration supports either H810 PERC SAS adapter or a Fibre Channel HBA. For more information on configuring fibre channel HBAs, see the DL4xxx — Fibre Channel Implementation whitepaper located at dell.com/support/home.

Before you begin provisioning storage on the disk, determine how much storage you want for standby virtual machines. You can allocate any percentage of the available capacity to host standby virtual machines. For example, if you are using Storage Resource Management (SRM), you can allocate up to 100 percent capacity on any device being provisioned to host virtual machines. Using AppAssure's Live Recovery feature, you can use these virtual machines to quickly replace any failed server that the DL4000 protects.

Based on a medium-sized environment that does not need standby virtual machines, you can use all of the storage to back up a significant number of agents. However, if you need more resources for standby virtual machines and back up a smaller number of agent machines, you can allocate more resources for larger VMs.

When you select the **Appliance** tab, the AppAssure Appliance software locates the available storage space for all supported controllers in the system and validates that the hardware meets the requirements.

To complete disk provisioning for all available storage:

1. In the **Appliance** tab, click **Tasks**.

   The **Tasks** screen displays available internal storage capacity for the appliance. This capacity is used to create a new AppAssure Repository.

   CAUTION: Before proceeding ensure Step 2 through Step 4 is followed in this procedure.

2. Open the **Provisioning Storage** window by clicking **Provision** in the Action column next to the storage that you want to provision.
3. In the **Provisioning Task Action** section, ensure that the check box next to **Do this for only one provisioning task when more than one task is being provisioned at a time** is checked, unless you want to have a reserve on the first enclosure (in which case you would keep that setting checked).
4. In the **Optional Storage Reserve** section, select the box next to **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes** and indicate a percentage of storage to allocate. Otherwise, the percentage of storage indicated in the **Optional Storage Reserve** section will be taken from all of the attached disks.
5. Click **Provision All**.

NOTE: If, for example, you selected to allocate 30 percent of the storage for standby VMs, the **Provision All** command will provision the internal storage as 70 percent to the repository and 30 percent to standby VMs. If you had unchecked the setting **Do this for only one provisioning task when more than one task is being provisioned at a time**, then all external storage will be 100 percent provisioned to the repository, which will be added as extra storage space for the repository that is being created on the internal storage.

Provisioning selected storage

To provision selected storage:

1. In the **Appliance** tab, click **Tasks**.

   The **Tasks** screen displays available internal and external storage capacity for the appliance, whether it is available for provisioning or if it is already provisioned, or if there is a condition that is preventing the storage from being automatically provisioned. This capacity is used to create an ppAssure repository.

2. NOTE: It is recommended to provision the available internal storage before expanding to the external enclosure (MD1200).

   To provision only a portion of the available space, click **Provision** under **Action** next to the storage space that you want to provision.

   - To create new repository, select **Create a new repository**, and provide a name for the repository.

     By default, Repository 1 appears as the repository name. You can opt to overwrite the name.
   - To add capacity to an existing repository, select **Expand the existing repository**, and then select the repository from the **Existing Repositories** list.

   NOTE: To add capacity, it is recommended that you expand an existing repository instead of adding a repository. Separate repositories do not utilize capacity as efficiently because deduplication cannot occur across separate repositories.

3. Under **Optional Storage Reserve**, you can select the option to allocate a portion of storage for standby virtual machines, and then specify the percentage of storage to allocate for the VMs.
4. You can choose to deselect the check box **Do this for only one provisioning task when more than one task is being provisioned at a time** (selected by default).

   Deselecting this option applies the percentage of selected storage to only the selected storage device. Selecting this option lets you apply the percentage of selected storage to both internal storage and external enclosures.

5. Click **Provision**.

   The disk provisioning begins and the status of the AppAssure repository creation is displayed in the **Status** area of the **Tasks** screen. The **Status Description** displays **Provisioned**.

6. To view the details after disk provisioning completes, click **>** next to the status light.

   The **Tasks** page expands and displays status, repository, and virtual disk details (if allocated).

Configuring the DL4000 using fibre channel storage (optional)

The DL4000 high-capacity edition offers a fibre channel HBA storage option allowing for creation of repositories using fibre channel storage arrays.

NOTE: If the fibre channel configuration is ordered it will replace the slotted H810 PERC SAS adapter.

NOTE: For prerequisites, assumptions, and detailed information on the following steps, see the *DL4xxx — Fibre Channel Implementation* whitepaper located at **dell.com/support/home** .

To integrate and configure the DL4000 using the fibre channel storage:

1. Connect the DL4000 fibre channel HBA to a SAN switch.
2. Install either the Qlogic or the Emulex HBAs management software for any adapter that was ordered with the system.
3. Install the storage array multi-path software.
4. Perform the fibre channel zoning.
5. Create a fibre channel LUN to be assigned and used as a DL4000 repository.
6. Mount the fibre channel storage LUN.
7. Configure the DL4000 fibre channel storage as a backup repository.

3

Post installation tasks

After completing the **AppAssure Appliance Configuration Wizard** perform the following procedures to ensure that your backup appliance and the servers that the appliance is backing up are correctly configured.

NOTE: The appliance is configured with a 30–day temporary AppAssure software license. To obtain a permanent license key, log on to the Dell AppAssure License Portal at **www.dell.com/DLActivation**. For details on changing a license key in the AppAssure software, see the topic 'Changing A License Key' in the *Dell DL4000 Appliance User's Guide* at **dell.com/support/home**.

Resetting the operating system to default settings

To reset the operating system to default settings, perform the following:

1. Log on as administrator and open the command prompt.
2. Navigate to **c:\windows\system32\sysprep** and execute the command **sysprep.exe/generalize/oobe/reboot**.
3. Select:
   - **English** as the language
   - **United States** as the country/region
   - **US** as the keyboard layout

   NOTE: It is strongly recommended that you change the host name by using the **AppAssure Appliance Configuration Wizard**. If the **AppAssure Appliance Configuration Wizard** has completed, manually change the computer name to the previous name.

Accessing the Core Console

Ensure that you update trusted sites as discussed in the topic Update Trusted Sites In Internet Explorer, and configure your browsers as discussed in the topic Configuring Browsers To Remotely Access The Core Console. After you update trusted sites in Internet Explorer, and configure your browsers, perform one of the following to access the Core Console:

- Log on locally to your AppAssure core server, and then double-click the **Core Console** icon.
- Type one of the following URLs in your web browser:
  - **https://<yourCoreServerName>:8006/apprecovery/admin/core**
  - **https://<yourCoreServerIPaddress>:8006/apprecovery/admin/core**

Updating trusted sites in Internet Explorer

To update the trusted sites in Internet Explorer:

1. Open Internet Explorer.
2. If the **File**, **Edit View**, and other menus are not displayed, press <F10>.
3. Click the **Tools** menu, and select **Internet Options**.
4. In the **Internet Options** window, click the **Security** tab.
5. Click **Trusted Sites** and then click **Sites**.
6. In **Add this website to the zone**, enter **https://[Display Name]**, using the new name you provided for the Display Name.
7. Click **Add**.
8. In **Add this website to the zone**, enter **about:blank**.
9. Click **Add**.
10. Click **Close** and then **OK**.

Configuring browsers to remotely access the Core Console

To access the Core Console from a remote machine, you need to modify your browser settings.

NOTE: To modify the browser settings, log in to the system as an administrator.

NOTE: Google Chrome uses Microsoft Internet Explorer settings, change Chrome browser settings using Internet Explorer.

NOTE: Ensure that the **Internet Explorer Enhanced Security Configuration** is turned on when you access the Core Web Console either locally or remotely. To turn on the **Internet Explorer Enhanced Security Configuration**:

1. Open **Server Manager**.
2. Select **Local Server IE Enhanced Security Configuration** displayed on the right. Ensure that it is **On**.

Reviewing retention periods

AppAssure sets default retention periods that determine how often snapshots are taken and how long the snapshots are retained. The retention periods must be based on the needs of your environment. For example, if you are backing up servers that run frequently changing, mission-critical data that is essential for business continuity, snapshots must be taken frequently.

To review and change retention periods:

1. Open the Core Console.
2. Select the **Configuration** tab and then click **Retention Policy**.
3. Adjust the retention policy based on the needs of your organization.
4. Click **Apply**.

Encrypting agent snapshot data

The Core can encrypt agent snapshot data within the repository. Instead of encrypting the entire repository, it allows you to specify an encryption key during the protection of an agent in a repository which allows the keys to be reused for different agents.

To encrypt agent snapshot data:

1. From the AppAssure Core, click **Configuration** → **Manage** → **Security**.
2. Click **Actions**, and then click **Add Encryption Key**.
   The **Create Encryption Key** page is displayed.
3. Complete the following information:

Field	Description
Name	Enter a name for the encryption key.
Comment	Enter a comment for the encryption key. It is used to provide extra details about the encryption key.
Passphrase	Enter a passphrase. It is used to control access.
Confirm Passphrase	Re-enter the passphrase. It is used to confirm the passphrase entry.

NOTE: It is recommended that you record the encryption passphrase, as losing the passphrase makes the data inaccessible.

Configuring an email server and email notification template

If you want to receive email notifications about events, configure an email server and an email notification template.

NOTE: You must also configure notification group settings, including enabling the **Notify by email** option, before email alert messages will be sent. For more information on specifying events to receive email alerts, see 'Configuring Notification Groups For System Events' in *Dell DL4000 Appliance User's Guide*.

To configure an email server and email notification template:

1. From the Core, select the **Configuration** tab.
2. From the **Manage** option, click **Events**.
3. In the **Email SMTP Settings** pane, click **Change**.
   The Edit **Email Notification Configuration** dialog box appears.
4. Select **Enable Email Notifications**, and then enter details for the email server described as follows:

Text Box	Description
SMTP Server	Enter the name of the email server to be used by the email notification template. The naming convention includes the host name, domain, and suffix; for example, **smtp.gmail.com**.

Text Box	Description
Port	Enter a port number. It is used to identify the port for the email server; for example, the port 587 for Gmail. The default is 25.
Timeout (seconds)	To specify how long to try a connection before timing out, enter an integer value. It is used to establish the time in seconds when trying to connect to the email server before a time-out occurs. The default is 30 seconds.
TLS	Select this option if the mail server uses a secure connection such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL).
Username	Enter a user name for the email server.
Password	Enter a password for accessing the email server.
From	Enter a return email address. It is used to specify the return email address for the email notification template; for example, **noreply@localhost.com**.
Email Subject	Enter a subject for the email template. It is used to define the subject of the email notification template; for example, `<hostname> - <level> <name>`.
Email	Enter information for the body of the template that describes the event, when it occurred, and the severity.

5. Click **Send Test Email** and review the results.
6. After you are satisfied with the results of the tests, click **OK**.

Adjusting the number of streams

By default, AppAssure is configured to allow three concurrent streams to the appliance. It is recommended that the number of streams is equal to one more than the number of machines (agents) you are backing up. For example, if you are backing up six agents, the **Maximum Concurrent Transfers** must be set to seven.

To change the number of concurrent streams:

1. Select the **Configuration** tab and then click **Settings**.
2. Select change in **Transfer Queue**.
3. Change **Maximum Concurrent Transfers** to a number that is at least one more than the number of clients you are backing up.

Protecting machines and checking connectivity to clients

After configuring the DL Appliance and Core, verify that you can connect to the machines you plan to back up.

To protect a machine:

1. Navigate to the Core Console, and select the **Machines** tab.
2. In the **Actions** drop-down menu, click **Protect Machine**.
   The **Connect** dialog box is displayed.

3. In the **Connect** dialog box, enter the information about the machine to which you want to connect as described in the following table.

Host	The host name or IP address of the machine that you want to protect.
Port	The port number on which the AppAssure Core communicates with the agent on the machine.
Username	The user name used to connect to this machine; for example, administrator.
Password	The password used to connect to this machine.

4. Click **Connect**.
5. If you receive an error message, the appliance cannot connect to the machine to back it up. To resolve the issue:
   a. Check Network Connectivity.
   b. Check the Firewall Settings.
   c. Verify AppAssure Services and RPC are running.
   d. Verify Domain Name Service Lookups (if applicable).

Checking network connectivity

To check network connectivity:

1. On the client system to which you are trying to connect, open a command line interface.
2. Run the command **ipconfig** and note the IP address of the client.
3. Open a command line interface on the appliance.
4. Run the command **ping <IP address of client>**.
5. Depending on the result, do one of the following:
   - If the client does not reply to the ping, verify the server's connectivity and network settings.
   - If the client replies, check that the firewall settings allow the AppAssure components to run.

Checking the firewall settings

If the client is connected properly to the network, but cannot be seen by the Core Console, check the firewall to ensure that necessary inbound and outbound communications are allowed.

To check the firewall settings on the AppAssure Core and any clients that it backs up:

1. On the appliance, click **Start** → **Control Panel.**
2. In the **Control Panel**, click **System and Security**, under **Windows Firewall** click **Check firewall status**.
3. Click **Advanced Settings**.
4. In the **Windows Firewall with Advanced Security** screen, click **Inbound Rules**.
5. Ensure the AppAssure Core and ports display **Yes** in the **Enabled** column.
6. If the rule is not enabled, right-click on AppAssure Core and select **Enable Rule**.
7. Click **Outbound Rules** and verify the same for AppAssure Core.

Verifying name resolution (if applicable)

If the machine you are trying to back up uses DNS, verify that DNS forward and reverse lookups are correct.

To ensure that the reverse lookups are correct:

1. On the AppAssure appliance, go to C:\Windows\system32\drivers\etc hosts.
2. Enter the IP address of each client that backs up to DL4000.

Teaming network adapters

By default, the network adapters (NICs) on the DL4000 Appliance are not bonded, which affects the performance of the system. It is recommended that you team the NICs to a single interface. Teaming the NICs require:

- Reinstalling the Broadcom Advanced Control Suite
- Creating the NIC team
- Configuring a Hyper-V Virtual Switch

Reinstalling Broadcom Advanced Configuration Suite

To reinstall Broadcom Advanced Configuration Suite (BACS):

1. Identify the NICs on your system. To identify the NICs:
   a. Access the Dell Open Manage Server Administrator (OMSA).
   b. On the main page, click **System → Main Sytem Chassis → Slots**.
2. Uninstall the earlier versions of Broadcom drivers and management applications.
3. Download the appropriate Broadcom drivers and BACS onto your appliance.
   The following drivers are available at **dell.com/support**.
   - QLogic driver
     Click **Servers, storage, & Networking → Dell Software DL 4300 → Drivers & downloads → Category → Network → QLogic BCM57xx and BCM57xxx** .
   - Broadcom driver
     Click **Servers, storage, & Networking → Dell Software DL 4300 → Drivers & downloads → Category → Network → Broadcom Windows 64bit driver update for NetXtreme Ethernet adapters**.
4. Complete the installation by going through the installation wizard.

Creating the NIC team

NOTE: It is recommended not to use the native teaming interface in Windows 2012 Server. The teaming algorithm is optimized for outbound, not inbound, traffic. It offers poor performance with a backup workload, even with more network ports in the team.

To create NIC teaming:

1. Go to **Start → Search → Broadcom Advanced Control Suite.**

   NOTE: When using Broadcom Advanced Control Suite, only select the Broadcom network cards.
2. In the **Broadcom Advanced Control Suite**, select **Teams → Go to Team View.**
3. In the **Hosts list** on the left side, right-click on the host name of the DL4000 appliance and select **Create Team**.
   The **Broadcom Teaming Wizard** window is displayed.

4. Click **Next**.
5. Enter a name for the team and click **Next**.
6. Select the **Team Type** and click **Next**.
7. Select an adapter you want to be part of the team, and click **Add**.
8. Repeat these steps for all other adapters that are a part of the team.
9. When all adapters are selected for the team, click **Next**.
10. Select a standby NIC if you want a NIC that can be used as the default, if the team fails.
11. Select whether to configure **LiveLink**, and then click **Next**.
12. Select **Skip Manage VLAN** and click **Next**.
13. Select **Commit changes to system** and click **Finish**.
14. Click **Yes** when warned that the network connection is interrupted.

NOTE: The building of the team may take about five minutes.

Configuring a Hyper-V Virtual Switch

For virtual standby machines to communicate within a production environment, create a virtual switch. To create an external virtual switch, see *Configure Virtual Networks* section at **www.technet.microsoft.com**.

4

Installing agents on clients

Each client that is backed up by the AppAssure appliance must have the AppAssure agent installed. The Core Console enables you to deploy agents to machines. Deploying agents to machines requires pre-configuring settings to select a single type of agent to push to clients. This method works well if all clients are running the same operating system. However, if there are different versions of operating systems, you may find it easier to install the agents on the machines.

You can also deploy the Agent software to the agent machine during the process of protecting a machine. This option is available for machines that do not already have the Agent software installed. For more information on deploying the Agent software while protecting a machine, see the *Dell DL4000 Appliance User's Guide* at **dell.com/support/home**.

Installing agents remotely (push)

To install the agents remotely (push):

1. If the client is running an operating system version that is older than Windows Server 2012, verify that the client has the Microsoft.NET4 framework installed:
   a. On the client, start the **Windows Server Manager**.
   b. Click **Configuration → Services.**
   c. Ensure that Microsoft .NET Framework is displayed in the list of services.
      If it is not installed, you can get a copy to install from **microsoft.com**.
2. Verify or change the path to the agent installation packages:
   a. In the AppAssure Core Console, click the **Configuration** tab, and then click **Settings** in the left panel.
   b. In the **Deploy Settings** area, click **Change**.
   c. Complete the following information about the agent location:

Field	Description
Agent Installer Name	Specifies the exact path to the folder\file for the agent.
Core Address	Specifies the IP address of the appliance running the AppAssure Core. NOTE: By default, **Core Address** is blank. The **Core Address** field does not need an IP address as the installation files are installed on the appliance.

   d. Click **OK**.
3. Click the **Tools** tab, and then click **Bulk Deploy** in the left panel.

NOTE: If the client already has an agent installed, the installation program will verify the version of the agent. If the agent that you are trying to push is newer than the installed version, the installation program offers to upgrade the agent. If the host has the current agent version installed, then the bulk deploy will initiate protection between the AppAssure Core and agent.

4. In the list of clients, select all clients and click **Verify** to ensure that the machine is active and the agent can be deployed.
5. When the **Message** column confirms the machine is ready, click **Deploy**.
6. To monitor the status of the deployment, select the **Events** tab.

   After the agent is deployed, a backup of the client begins automatically.

Deploying the agent software when protecting an agent

You can download and deploy agents during the process of adding an agent for protection.

NOTE: This procedure is not required if you have already installed the Agent software on a machine that you want to protect.

To deploy agents during the process of adding an agent for protection:

1. From the **Protect Machine → Connect** dialog box, after entering the appropriate connection settings, click **Connect**.

   The **Deploy Agent** dialog box is displayed.
2. Click **Yes** to deploy the Agent software remotely to the machine.

   The **Deploy Agent** dialog box is displayed.
3. Enter logon and protection settings as follows:
   - **Host name** — Specifies the host name or IP address of the machine that you want to protect.
   - **Port** — Specifies the port number on which the Core communications with the Agent on the machine. The default value is 8006.
   - **User name** — Specifies the user name used to connect to this machine; for example, administrator.
   - **Password** — Specifies the password used to connect to this machine.
   - **Display name** — Specifies a name for the machine which appears on the Core Console. The display name could be the same value as the host name.
   - **Protect machine after install** — Selecting this option enables AppAssure to take a base snapshot of the data after you add the machine for protection. This option is selected by default. If you deselect this option, then you must force a snapshot manually when you are ready to start data protection. For more information about manually forcing a snapshot, see topic 'Forcing A Snapshot' in *Dell DL4000 Appliance User's Guide*.
   - **Repository** — Select the repository in which to store data from this agent.

     NOTE: You can store data from multiple agents in a single repository.
   - **Encryption Key** — Specifies whether encryption should be applied to the data for every volume on this machine to be stored in the repository.

     NOTE: You define encryption settings for a repository under the **Configuration** tab in the Core Console.
4. Click **Deploy**.

The **Deploy Agent** dialog box closes. There may be a delay before you see the selected agent appear in the list of protected machines.

Installing Microsoft Windows agents at the client

To install the agents:

1. Verify that the client has the Microsoft .NET4 framework installed:
   a. On the client, start the **Windows Server Manager**.
   b. Click **Configuration → Services.**
   c. Ensure that Microsoft .NET Framework appears in the list of services.
      If it is not installed, you can get a copy from **microsoft.com**.
2. Install the agent:
   a. On the AppAssure appliance, share the directory **C:\install\AppAssure** to the client(s) you plan to back up.
   b. On the client system, map a drive to **C:\install\AppAssure** on the AppAssure appliance.
   c. On the client system, open the **C:\install\AppAssure** directory and double-click the correct agent for the client system to begin the installation.

Adding an agent by using the license portal

NOTE: You must have administrative privileges to download and add agents.

To add an agent:

1. On the **AppAssure License Portal Home** page, select a group, and then click **Download Agent**.
   The **Download Agent** dialog box is displayed.
2. Click **Download**, located next to the installer version that you want to download.
   You can choose from:
   - 32 bit Windows installer
   - 64 bit Windows installer
   - 32 bit Red Hat Enterprise Linux 6.3, 6.4 installer
   - 64 bit Red Hat Enterprise Linux 6.3, 6.4 installer
   - 32 bit CentOS 6.3, 6.4 installer
   - 64 bit CentOS 6.3, 6.4 installer
   - 32 bit Ubuntu 12.04 LTS, 13.04 installer
   - 64 bit Ubuntu 12.04 LTS, 13.04 installer
   - 32 bit SUSE Linux Enterprise Server 11 SP2, SP3 installer
   - 64 bit SUSE Linux Enterprise Server 11 SP2, SP3 installer
   - Microsoft Hyper-V Server 2012

   NOTE: We support these Linux distributions and have tested under most of the released kernel versions.

   NOTE: Agents installed on Microsoft Hyper-V Server 2012 operate in the Core edition mode of Windows Server 2012.

   The **Agent** file downloads.

3. Click **Run** in the **Installer** dialog box.

   NOTE: For information about adding agents by using the Core machine, see topic 'Deploying An Agent (Push Install)' in the *Dell DL4000 Appliance User's Guide* at **dell.com/support/home**.

Installing agents on Linux machines

Download the distribution specific 32-bit or 64-bit installer on every Linux server that you want to protect by using the AppAssure Core. You can download the installers from the AppAssure License Portal at **https://licenseportal.com**. For more information, see Adding An Agent By Using The License Portal .

NOTE: The security around protecting a machine is based on the Pluggable Authentication Module (PAM) in Linux. After a user is authenticated using **libpam**, the user is only authorized to protect the machine if the user is in one of the following groups:

- sudo
- admin
- appassure
- wheel

For information on protecting a machine, see the section 'Protecting a Machine' in the *Dell DL4000 Appliance User's Guide* at **dell.com/support/home**.

The installation instructions differ depending upon the Linux distribution you are using. For more information on installing the Linux agent on your distribution, see the following:

- Installing The Agent On Ubuntu
- Installing The Agent On Red Hat Enterprise Linux and CentOS
- Installing The Agent On SUSE Linux Enterprise Server

NOTE: We support these Linux distributions and have tested under most of the released kernel versions.

NOTE: The Linux Agent installation overwrites any firewall rules that were not applied through UFW, Yast2, or **system-config-firewall**.

If you manually added firewall rules, then you must manually add AppAssure ports after the installation. A backup of existing rules will be written to **/var/lib/appassure/backup.fwl**.

You must add firewall exceptions to all servers running the AppAssure agent for TCP ports 8006 and 8009 for the AppAssure Core to access agents.

Location of Linux agent files

The Linux agent files are located in the following directories for all distributions:

Component	Location/Path
mono	/opt/appassure/mono
agent	/opt/appassure/aagent
aamount	/opt/appassure/amount
aavdisk and aavdctl	/usr/bin

Component	Location/Path
configuration files for aavdisk	/etc/appassure/aavdisk.conf
wrappers for aamount and agent	• /usr/bin/aamount • /usr/bin/aagent
autorun scripts for aavdisk and agent	• /etc/init.d/appassure-agent • /etc/init.d/appassure-vdisk

Agent dependencies

The following dependencies are required and are installed as part of the Agent installer package:

For Ubuntu	Dependency
The appassure-vss requires	`dkms, gcc, make, linux-headers-‘uname-r‘`
The appassure-aavdisk requires	`libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3`
The appassure-mono requires	`libc6 (>=2.7-18)`

For Red Hat Enterprise Linux and CentOS	Dependency
The nbd-dkms requires	`dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘`
The appassure-vss requires	`dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘`
The appassure-aavdisk requires	`nbd-dkms, libblkid, pam, pcre`
The appassure-mono requires	`glibc >=2.11`

For SUSE Linux Enterprise Server	Dependency
The nbd-dkms requires	`dkms, gcc, make, kernel-syms`
The appassure-vss requires	`dkms, kernel-syms, gcc, make`

For SUSE Linux Enterprise Server	Dependency
The appassure-aavdisk requires	`libblkid1, pam, pcre`
The appassure-mono requires	`glibc >= 2.11`

Installing the agent on Ubuntu

NOTE: Before performing these steps, ensure that you have downloaded the Ubuntu-specific installer package to the **/home/system directory**.

To install the AppAssure agent on Ubuntu:

1. Open a terminal session with root access.
2. To make the AppAssure Agent installer executable, type the following command:
   `chmod +x appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` and then press <Enter>.

   The file becomes executable.

   NOTE: For 32-bit environments, the installer is named **appassureinstaller_ubuntu_i386_5.x.x.xxxxx.sh**
3. To extract and install the AppAssure Agent, type the following command:
   `/appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` and then press <Enter>.

   The Linux Agent begins the extraction and installation process. Any missing packages or files required by the agent is downloaded and installed automatically as part of the script.

   NOTE: For information on the files required by the Agent, see Agent Dependencies.

After the installer completes, the Agent is running on your machine. For more information on protecting this machine with the Core, see the section Protecting Workstations and Servers in the *Dell DL4000 Appliance User's Guide* at **dell.com/support/home**.

Installing the agent on Red Hat Enterprise Linux and CentOS

NOTE: Before performing these steps, ensure that you have downloaded the Red Hat or CentOS installer package to the **/home/system directory**. The following steps are the same for both 32-bit and 64-bit environments.

To install an agent on Red Hat Enterprise Linux and CentOS:

1. Open a terminal session with root access.
2. To make the AppAssure Agent installer executable, type the following command:
   `chmod +x appassure-installer__rhel_amd64_5.x.x.xxxxx.sh` and then press <Enter>.

   NOTE: For 32-bit environments, the installer is named `appassureinstaller__rhel_i386_5.x.x.xxxxx.sh`.

   The file becomes executable.
3. To extract and install the AppAssure Agent, type the following command:

`/appassure-installer_rhel_amd64_5.x.x.xxxxx.sh` and then press <Enter>.

The Linux agent begins its extraction and installation process. Any missing packages or files required by the agent is downloaded and installed automatically as part of the script.

For information on the files required by the Agent, see Agent Dependencies.

After the installer completes, the Agent will be running on your machine. For more information on protecting this machine with the Core, see the section Protecting Workstations and Servers in the *Dell DL4000 Appliance User's Guide* at **dell.com/support/home**.

Installing the agent on SUSE Linux Enterprise Server

NOTE: Before performing these steps, ensure that you have downloaded the SUSE Linux Enterprise Server (SLES) installer package to the **/home/system directory**. The following steps are the same for both 32-bit and 64-bit environments.

To install the agent on SLES:

1. Open a terminal session with root access.
2. To make the AppAssure Agent installer executable, type the following command:
   `chmod +x appassure-installer_sles_amd64_5.x.x.xxxxx.sh` and then press <Enter>.

   NOTE: For 32-bit environments, the installer is named `appassureinstaller__sles_i386_5.x.x.xxxxx.sh`

   The file becomes executable.
3. To extract and install the AppAssure Agent, type the following command:
   `/appassure-installer_sles_amd64_5.x.x.xxxxx.sh` and then press <Enter>.

   The Linux Agent begins its extraction and installation process. Any missing packages or files required by the agent is downloaded and installed automatically as part of the script.

   For information on the files required by the Agent, see Agent Dependencies.
4. When prompted to install the new packages, type `y`, and then press <Enter>.
   The system finishes the installation process.

After the installer completes, the Agent is running on your machine. For more information on protecting this machine with the Core, see the section 'Protecting Workstations and Servers' in the *Dell DL4000 Appliance User's Guide* at **dell.com/support/home**.

5

Getting help

Finding documentation and software updates

In the AppAssure Core console there are direct links to AppAssure, Appliance documentation, and software updates. To access the links, click the **Appliance** tab, and then click **Overall Status**. Links to the software updates and documentation are located under the **Documentation** section.

Finding software updates

There are direct links to AppAssure and DL4000 Appliance software updates available from the AppAssure 5 Core Console. To access the links to software updates, select the **Appliance** tab, and then click **Overall Status**. Links to the software updates are located under the **Documentation** section.

Contacting Dell

NOTE: Dell provides several online and telephone-based support and service options. If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog. Availability varies by country and product, and some services may not be available in your area.

To contact Dell for sales, technical support, or customer-service issues:

1. Go to **dell.com/contactdell**.
2. Select your country or region from the interactive world map.
   When you select a region, the countries for the selected regions are displayed.
3. Select the appropriate language under the country of your choice.
4. Select your business segment.
   The main support page for the selected business segment is displayed.
5. Select the appropriate option depending on your requirement.

Documentation feedback

Click the **Feedback** link in any of the Dell documentation pages, fill up the form, and click **Submit** to send your feedback.