Quest™

DL4300 Appliance

Deployment Guide

Table of Contents

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.

Setting up DL4300 Appliance

Introduction

The Quest DL4300 appliance is the latest generation of backup-to-disk appliance powered by Quest 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

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 DL4300 appliance.

Table 1. DL4300 Appliance hardware and software components

The words in the document such as Appliance refers to DL4300 appliance, storage enclosure refers to Dell Storage MD1400 storage enclosure, and AppAssure refers to Quest AppAssure Software.

Component	Term Used
DL4300 Appliance	Appliance
Dell Storage MD1400 storage enclosure	Storage enclosure
Quest AppAssure Software	AppAssure

Parent topic

Available configurations

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

Table 2. DL4300 Standard Edition capacity configurations

The DL4300 Standard Edition system comes in 5 TB, 10–20TB, 30–40 TB, and 50–60 TB configurations. The 5 TB configuration has twelve 1 TB drives in the front chassis and four 1 TB drives in the middle pane. The 10–20TB configuration has twelve 2 TB drives in the front chassis and four 2 TB drives in the middle chassis. The 30–40 TB configuration has twelve 4 TB drives and four 4 TB middle pane drives. The 50–60 TB configuration has twelve 6 TB drives in the front chassis and four 6 TB drives in the middle pane.

Capacity	Hardware Configuration
5 TB	12 x 1 TB drives, 4 x 1 TB internal drives
10–20 TB	12 x 2 TB drives, 4 x 2 TB internal drives
30–40 TB	12 x 4 TB drives, 4 x 4 TB internal drives
50–60 TB	12 x 6 TB drives, 4 x 6 TB internal drives

Table 3. DL4300 High Capacity Edition capacity configurations

The High capacity Edition comes in 40 TB, 50 TB, 60 TB, 70 TB, 80 TB, 90 TB, 100 TB, 110 TB, 120 TB configurations with twelve 6 TB drives in the front chassis and four 6 TB drives in the middle pane.

Capacity	Hardware Configuration
40 TB, 50 TB, 60 TB, 70 TB, 80 TB, 90 TB, 100 TB, 110 TB, and 120 TB	12 x 6 TB drives, 4 x 6 TB internal drives

NOTE: Additional storage can be added through expansion shelves (Dell Storage MD1400). Additional storage can be added to any model, however the Standard Edition has a maximum capacity of 60 TB and the High Capacity Edition has a maximum capacity of 120 TB. Both editions support up to four expansion shelves.

Each configuration includes the following hardware and software:

- Quest DL4300 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 Dell Storage MD1400 storage enclosures, ignore any references to Dell Storage MD1400 and storage enclosures in this document.

Parent topic

Installation prerequisites

Parent topic

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

Parent topic

Recommended network infrastructure

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

Parent topic

Setting up the hardware

The appliance ships with a single DL4300 system. Before setting up the appliance hardware, see the *Quest DL4300 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 DL4300 system and storage enclosure(s).
2. Turn on the storage enclosure(s) and then the DL4300 system.

Parent topic

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.

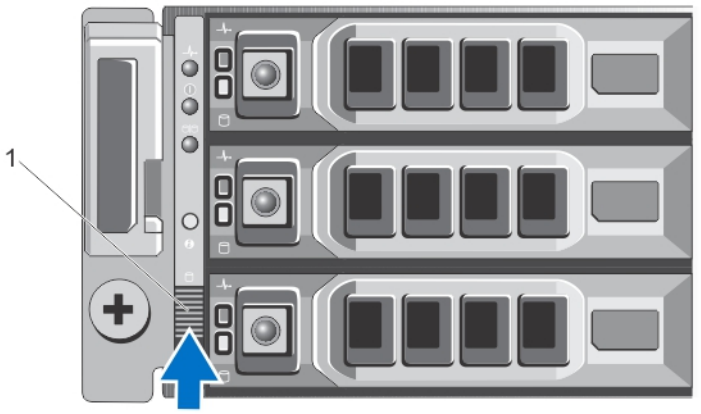
Parent topic

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 Storage MD1400 Enclosures Hardware Owner's Manual at Dell.com/support/home.

Figure 1. Setting the PowerVault MD1400 storage enclosure configuration switch



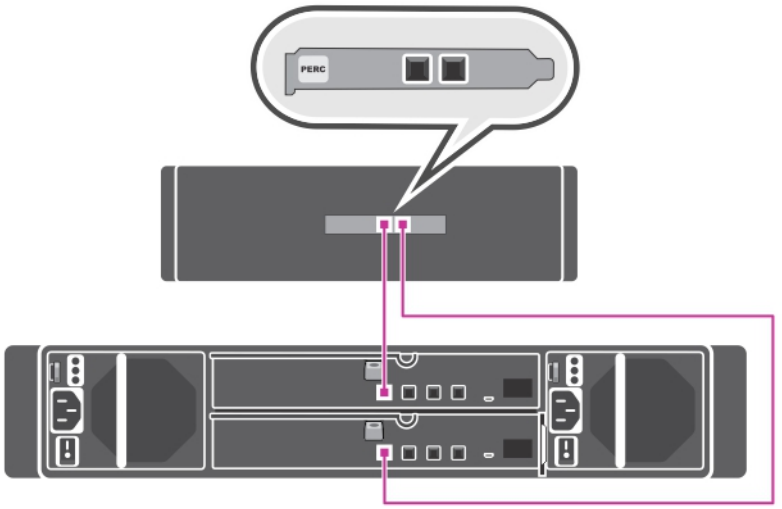
1. configuration switch

Parent topic

Connecting the storage enclosure to the system

Connect the data cable from the PowerEdge RAID Controller (PERC) installed in the Quest DL4300 system to the primary Enclosure Management Module (EMM) SAS port of the storage enclosure.

Figure 2. Connecting the DL4300 system to the MD1400 storage enclosure



Redundant port configuration

For redundant port configuration:

1. Connect one end of each SAS cable to port 0 and port 1 on the DL4300 system PERC controller.
2. Connect the other end of each SAS cable to port 1 on each Enclosure Management Module (EMM) on the MD1400 storage enclosure.

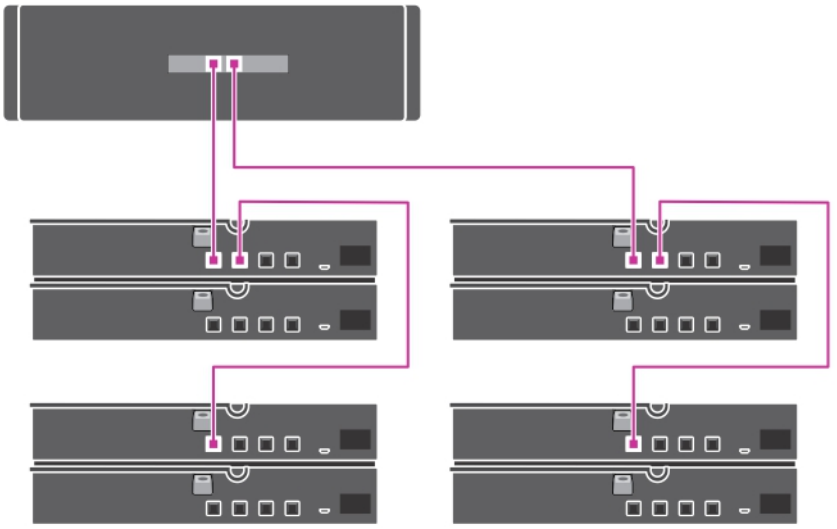
Single port configuration

For single port configuration:

1. Connect one end of the SAS cable to port 0 on the DL4300 system PERC controller.
2. Connect the other end of the SAS cable to port 1 on the Enclosure Management Module (EMM) on the MD1400 storage enclosure.

Multichain configuration

Figure 3. Multichain configuration



Multichain configuration supports up to four enclosures. The first two enclosures are daisy-chained with one of the enclosures connected to a single port on the controller card. The other two enclosures are daisy-chained with one of the enclosures connected to the second port on the controller card.

Parent topic

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.

Parent topic

Cabling the appliance

Locate the Getting Started With Your System document at Dell.com/support/home that shipped with your appliance. Follow the instructions to attach the keyboard, mouse, monitor, power, and network cables to the appliance.

Parent topic

Turning on the appliance

After cabling the appliance, turn on the MD1400 storage enclosure, and then turn on the DL4300 system.

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

Parent topic

DL4300 disk configurations

The DL4300 supports both nearline SAS drives and SATA drives. The operating system resides on a RAID 1 (mirrored) virtual disk located in slots 12 and 13. For information on these disks, see the Quest DL4300 Appliance Owner's Manual at Quest.com/support. Drives available in slots 0–11 and 14–17 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 MD1400 storage enclosure is optional.

Parent topic

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.

   The Microsoft EULA (End User License Agreement) is displayed on the Settings page.
2. To accept the EULA, click I accept button.

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

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

   The Select the language for AppAssure Appliance screen is displayed.
8. Select the language for your appliance from the list of supported languages.

   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.

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
- Creating Windows and RASR virtual disk(s)

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

Parent topic

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.

Parent topic

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.

Parent topic

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.

Parent topic

Creating Windows and RASR virtual disk(s)

The DL4300 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

    CAUTION: 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.

    Windows backup virtual disk provides the target space to create Windows Server backups. A disk space of 75 GB is allocated by default for the Windows backup VD that is created and you cannot increase the size of the Windows backup VD. Overtime, the data that is backed up may exceed 75 GB and if it does, you will not be able to perform backup or configure backup policy on the Backup page and an out of capacity error is displayed. In this case, the Windows backup can be reconfigured to a network share or to another disk volume on the DL Appliance. For more information, see Configure a Scheduled Shared Network Drive Backup Policy section in Recovering a Dell DL Backup and Recovery Appliance using Rapid Appliance Self Recovery (RASR) at Dell.com/supportmanuals.

    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

Parent topic

Recovery and Update Utility

The Recovery and Update Utility (RUU) is an all-in-one installer to recover and update DL Appliances (DL1000, DL1300, DL4000 and DL4300) software. It includes the AppAssure Core software and appliance-specific components.

RUU consists of updated versions of the Windows Server Roles and Features, ASP .NET MVC3, LSI Provider, DL Applications, OpenManage Server Administrator and AppAssure Core Software. In addition, the Recovery and Update Utility also updates the Rapid Appliance Self Recovery (RASR) content.

To download the most recent version of the RUU:

1. Go to the License Portal under the Downloads section and download the RUU installer or go to support.dell.com.
2. Run the RUU installer.

NOTE: Your system may reboot during the RUU update process.

NOTE: If you use RUU # 184 and your DL appliance has an AppAssure Core version lower (older) than 5.4.3.106, the core is upgraded to AppAssure Core 5.4.3.106.

NOTE: If you upgrade to RUU # 184, you may begin to see some inconsistencies in future runs of already scheduled Windows backups (through RASR) or may not be able to create a Windows Backup Policy. These inconsistencies occur due to space limitations of your Windows Backup storage location.

Other potential causes of these failures include:

1. Upgrading to Rapid Recovery, especially if more than the minimal deduplication cache is used.
2. Installing or updating any software (for example, Outlook) on the appliance.
3. Installing Windows Updates.
4. Adding/enlarging data files (such as deduplication cache).
5. Combinations of the preceding.

Parent topic

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:

- Restore factory settings
- Recover your appliance to a state just before failure

Parent topic

Creating the RASR USB key

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 32 GB or larger USB key before attempting to create the RASR key.
3. After inserting a 32 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.

NOTE: Make sure to use 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.

Parent topic

Executing RASR

NOTE: Quest recommends you to create RASR USB key after you have set up the Appliance. To create RASR USB key, see Creating the RASR USB Key section.

These steps help you to perform the factory reset.

To recover your appliance to a state before failure and to recover repositories, recovery points, and Settings, see Recovering a Dell DL Backup and Recovery Appliance using Rapid Appliance Self Recovery (RASR) document at Dell.com/support/home

.

To perform the RASR:

1. Insert the RASR USB key created.
2. Restart the appliance and select Boot Manager (F11).
3. In the Boot Manager Main Menu , select One-shot BIOS Boot Menu.
4. In the Boot Manager Boot Menu, select the attached USB drive.
5. Select your keyboard layout.
6. Click Troubleshoot > Rapid Appliance Self Recovery.
7. Select the target operating system (OS).

   RASR is launched and welcome screen is displayed.
8. Click Next.

   The Prerequisites check screen is displayed.

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

   The Recovery Mode Selection screen is displayed with three options:
   - System Recovery
   - Windows Recovery Wizard
   - Factory Reset
10. Select the Factory Reset option.

    This option will recover the operating system disk from the factory image.
11. Click Next.

    The following warning message is displayed in a dialog box: **This operation will recover the operating system. All OS disk data will be overwritten.**
12. Click Yes.

    The operating system disk starts restoring back to factory reset.
13. After the completion of Factory reset recovery process, In the RASR Completed screen, click Finish.

Parent topic

Executing the RASR through the Internal Dual SD Module

Your system is shipped with an Internal dual SD module and an SD card of 32 GB capacity.

To execute the RASR using the Internal Dual SD module (IDSDM):

1. Reboot the appliance through the IDSDM.

   CAUTION: Make sure that the SD Card is inserted in slot 1.

   The following message is displayed.

   ```
   The secondary SD card is missing, not responding, or in write-protected mode. Do one of the f
   ```

   Ignore the above message.

2. To continue executing the RASR through the Internal SD Module, perform step 5 through step 13 of the Executing the RASR through RASR USB key section.

Parent topic

Provisioning storage

The appliance configures available DL4300 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 the Quest DL4300 Appliance Deployment Guide.

- Virtual Standby of Protected Machines

NOTE: MD1400s with 1 TB, 2 TB, 4 TB or 6 TB (for high capacity) drives connected to the H830 controller are supported. Up to four MD 1400s are supported.

NOTE: The DL4300 high-capacity configuration supports either H830 PERC SAS adapter or two Fibre Channel HBAs. 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 to allocate for standby virtual machines. You can allocate any percentage of the available capacity remaining after creating the AppAssure repository to host standby virtual machines. For example, if you are using Storage Resource Management (SRM), you can allocate up to 100 percent capacity of the storage remaining after creating the AppAssure repository. Space can be allocated for standby VMs only on the appliances that are provisioned to host virtual machines. Using the AppAssure's Live Recovery feature, you can use these virtual machines to quickly replace a failed server that the appliance 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 > Provisioning.

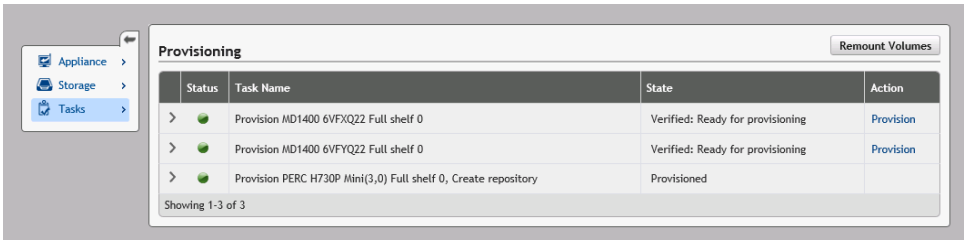
The Provisioning screen displays estimated capacity for provisioning. This capacity is used to create a new AppAssure Repository.

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

NOTE: Provision internal RAID controller to create the initial repository on your appliance.

Open the Provisioning Storage window by clicking Provision in the Action column next to the storage that you want to provision.

3. 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.
4. Click Provision.



The virtual disks for hosting repositories and virtual standby VMs are created.

Parent topic

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 AppAssure repository.

   NOTE: It is recommended to provision the available internal storage before expanding to the external enclosure (MD1400).

   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).

Parent topic

Configuring the DL4300 using fibre channel storage (optional)

The DL4300 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 H830 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 DL4300 using the fibre channel storage:

1. Connect the DL4300 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 DL4300 repository.
6. Mount the fibre channel storage LUN.
7. Configure the DL4300 fibre channel storage as a backup repository.

Parent topic

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 Quest DL4300 Appliance User's Guide at Quest.com/support.

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

Parent topic

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.

Parent topic

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.

Parent topic

Configuring browser settings in Internet Explorer and Chrome

To modify browser settings in Internet Explorer and Chrome:

1. Open Internet Explorer.
2. From the Tools menu, select Internet Options, Security tab.
3. Click Trusted Sites and then click Sites.
4. Deselect the option Require server verification (https:) for all sites in the zone, and then add http://<hostname or IP Address of the Appliance server hosting the AppAssure Core> to Trusted Sites.
5. Click Close, select Trusted Sites, and then click Custom Level.
6. Scroll to Miscellaneous → Display Mixed Content and select Enable.
7. Scroll to the bottom of the screen to User Authentication → Logon, and then select Automatic logon with current user name and password.
8. Click OK, and then select the Advanced tab.
9. Scroll to Multimedia and select Play animations in webpages.
10. Scroll to Security, check Enable Integrated Windows Authentication, and then click OK.

Parent topic

Configuring Mozilla Firefox browser settings

NOTE: To modify Mozilla Firefox browser settings in the latest versions of Firefox, disable protection. Right-click the Site Identify button (located to the left of the URL), go to Options and click on Disable protection for now.

To modify Mozilla Firefox browser settings:

1. In the Firefox address bar, type about:config, and then click I'll be careful, I promise if prompted.
2. Search for the term ntlm.

   The search should return at least three results.
3. Double-click network.automatic-ntlm-auth.trusted-uris and enter the following setting as appropriate for your machine:
   - For local machines, enter the host name.
   - For remote machines, enter the host name or IP address separated by a comma of the appliance system hosting the AppAssure Core; for example, IPAddress, host name.
4. Restart Firefox.

Parent topic

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.

Parent topic

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.

Parent topic

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 Quest DL4300 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.

   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.

Parent topic

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.

Parent topic

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).

Parent topic

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.

Parent topic

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.

Parent topic

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 DL4300.

Parent topic

Teaming network adapters

By default, the network adapters (NICs) on the DL4300 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

Parent topic

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.

Parent topic

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 DL4300 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.

Parent topic

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.

Parent topic

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 Quest DL4300 Appliance User's Guide at Quest.com/suppot.

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.

Parent topic

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 Quest DL4300 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.

Parent topic

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.

Parent topic

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 Quest DL4300 Appliance User's Guide at Quest.com/support.

Parent topic

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

NOTE: For information on protecting a machine, see the section 'Protecting a Machine' in the Quest DL4300 Appliance User's Guide at Quest.com/support.

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.

NOTE: 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`.

NOTE: 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.

Parent topic

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`

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`

Parent topic

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
```

The appassure-aavdisk requires

```
libblkid1, pam, pcre
```

The appassure-mono requires

```
glibc >= 2.11
```

Parent topic

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 Quest DL4300 Appliance User's Guide at Quest.com/support.

Parent topic

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 Quest DL4300 Appliance User's Guide at Quest.com/support.

Parent topic

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 Quest DL4300 Appliance User's Guide at Quest.com/support.

Parent topic

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.

Parent topic

Finding software updates

There are direct links to AppAssure and DL4300 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.

Parent topic

Contacting Quest

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Qeust product catalog.

Quest 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 Quest product catalog. Availability varies by country and product, and some services may not be available in your area. To contact Quest for sales, technical support, or customer-service issues, go to quest.com/support.

Parent topic

Documentation feedback

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

Parent topic