DL1300 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.

Introducing your Quest DL1300

Your Quest DL1300 combines backup and replication into a unified data protection product. It provides reliable application data recovery from your backups to protect virtual machines and physical machines. Your appliance is capable of handling up to terabytes of data with built-in global deduplication, compression, encryption, and replication to specific private or public cloud infrastructure. Server applications and data can be recovered in minutes for data retention and compliance purposes.

Your DL1300 supports multi-hypervisor environments on VMware vSphere, Oracle VirtualBox and Microsoft Hyper-V private and public clouds.

Quest DL1300 core technologies

Your appliance combines the following technologies:

- Live Recovery
- Universal Recovery
- True Global Deduplication
- Encryption

Parent topic

Live Recovery

Live Recovery is instant recovery technology for VMs or servers. It gives you near-continuous access to data volumes on virtual or physical servers.

DL1300 backup and replication technology records concurrent snapshots of multiple VMs or servers, providing near instantaneous data and system protection. You can resume the use of the server by mounting the recovery point without waiting for a full restore to production storage.

Parent topic

Universal Recovery

Universal Recovery provides unlimited machine restoration flexibility. You can restore your backups from physical systems to VMs, VMs to VMs, VMs to physical systems, or physical systems to physical systems, and carry out bare metal restores to dissimilar hardware.

Universal Recovery technology also accelerates cross-platform moves among virtual machines. For example, moving from VMware to Hyper-V or Hyper-V to VMware. It builds in application-level, item-level, and object-level recovery (individual files, folders, email, calendar items, databases, and applications).

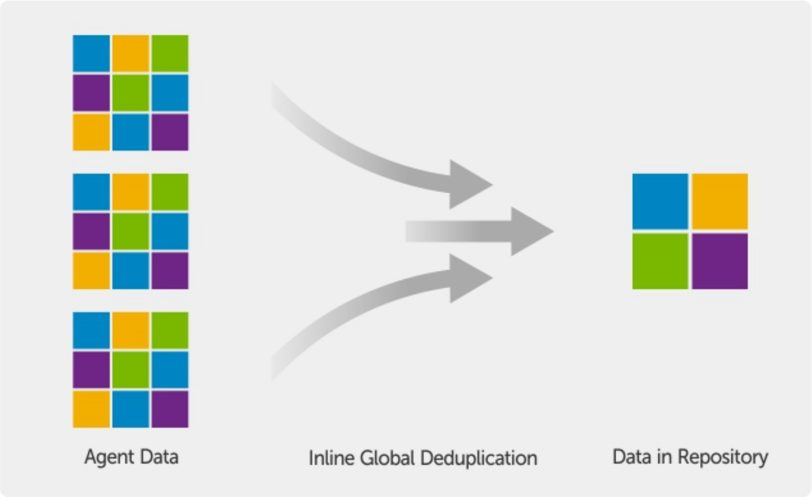
Parent topic

True Global Deduplication

True Global Deduplication eliminates redundant or duplicate data by performing incremental block-level backups of the machines.

The typical disk layout of a server consists of the operating system, application, and data. In most environments, the administrators often use a common version of the server and desktop operating system across multiple systems for effective deployment and management. When backup is performed at the block-level across multiple machines, it provides a more granular view of what is in the backup and what is not, irrespective of the source. This data includes the operating system, the applications, and the application data across the environment.

Figure 1. Diagram of True Global Deduplication



Parent topic

Encryption

Your DL1300 provides encryption to protect backups and data-at-rest from unauthorized access and use, ensuring data privacy. The data can be accessed and decrypted using the encryption key. Encryption is performed inline on snapshot data, at line speeds without impacting performance.

Parent topic

Quest DL1300 data protection features

Parent topic

Quest DL1300 Core

The Core is the central component of the DL1300 deployment architecture. The Core stores and manages machine backups and provides services for backup, recovery, retention, replication, archival, and management. The Core is a self-contained network, addressable computer that runs a 64-bit version of Microsoft Windows

Server 2012 R2 Foundation and Standard operating systems. The appliance performs target-based inline compression, encryption, and data deduplication of the data received from the agent. The Core then stores the snapshot backups in the repository, which resides on the appliance. Cores are paired for replication.

The repository resides on internal storage within the Core. The Core is managed by accessing the following URL from a JavaScript enabled web browser: https://CORENAME:8006/apprecovery/admin.

Parent topic

Quest DL1300 Smart Agent

The Smart Agent is installed on the core-protected machine. The Smart Agent tracks the changed blocks on the disk volume and then snaps an image of the changed blocks at a predefined interval of protection. The incremental block-level snapshots' forever approach prevents repeated copying of the same data from the protected machine to the Core.

After the agent is configured, it uses smart technology to track the changed blocks on the protected disk volumes. When the snapshot is ready, it is rapidly transferred to the Core using intelligent multi-threaded, socket-based connections.

Parent topic

Snapshot process

Your DL1300 protection process begins when a base image is transferred from a protected machine to the Core. In this phase, full copy of the machine is transported across the network under normal operation, followed by incremental snapshots forever. The DL1300 Agent for Windows uses Microsoft Volume Shadow copy Service (VSS) to freeze and quiesce application data to disk to capture a file-system-consistent and an application-consistent backup. When a snapshot is created, the VSS writer on the target server prevents content from being written to the disk. During the process of halting of writing content to disk, all disk I/O operations are queued and resume only after the snapshot is complete, while the operations in progress will be completed and all open files will be closed. The process of creating a shadow copy does not significantly affect the performance of the production system.

Your DL1300 uses Microsoft VSS because it has built-in support for all Windows internal technologies such as NTFS, Registry, Active Directory, to flush data to disk before the snapshot. Additionally, other enterprise applications, such as Microsoft Exchange and SQL, use VSS Writer plug-ins to get notified when a snapshot is being prepared and when they have to flush their used database pages to disk to bring the database to a consistent transactional state. The captured data is rapidly transferred and stored on the Core.

Parent topic

Replication — disaster recovery site or service provider

Replication is the process of copying recovery points from an AppAssure core and transmitting them to another AppAssure core in a separate location for disaster recovery. The process requires a paired source-target relationship between two or more cores.

The source core copies the recovery points of selected protected machines, and then asynchronously and continually transmits the incremental snapshot data to the target core at a remote disaster recovery site. You can configure outbound replication to a company-owned data center or remote disaster recovery site (that is, a "self-managed" target core). Or, you can configure outbound replication to a third-party managed service provider (MSP) or cloud provider that hosts off-site backup and disaster recovery services. When replicating to a third-party target core, you can use built-in work flows that let you request connections and receive automatic feedback notifications.

Replication is managed on a per-protected-machine basis. Any machine (or all machines) protected or replicated on a source core can be configured to replicate to a target core.

Replication is self-optimizing with a unique Read-Match-Write (RMW) algorithm that is tightly coupled with deduplication. With RMW replication, the source and target replication service matches keys before transferring data and then replicates only the compressed, encrypted, deduplicated data across the WAN, resulting in a 10x reduction in bandwidth requirements.

Replication begins with seeding: the initial transfer of deduplicated base images and incremental snapshots of the protected machines, which can add up to hundreds or thousands of gigabytes of data. Initial replication can be seeded to the target core using external media. This is typically useful for large sets of data or sites with slow links. The data in the seeding archive is compressed, encrypted and deduplicated. If the total size of the archive is larger than the space available on the removable media, the archive can span across multiple devices based on the available space on the media. During the seeding process, the incremental recovery points replicate to the target site. After the target core consumes the seeding archive, the newly replicated incremental recovery points automatically synchronize.

Parent topic

Recovery

Recovery can be performed in the local site or the replicated remote site. After the deployment is in steady state with local protection and optional replication, the DL1300 Core allows you to perform recovery using Verified Recovery, Universal Recovery, or Live Recovery.

Parent topic

Recovery-as-a-Service

Managed Service Providers (MSPs) can fully leverage DL1300 as a platform for delivering Recovery As A Service (RaaS). RaaS facilitates complete recovery-in-the-cloud by replicating customers' physical and virtual servers. The service provider's cloud are used as virtual machines to support recovery testing or actual recovery operations. Customers wanting to perform recovery-in-the-cloud can configure replication on their protected machines on the local cores to an AppAssure service provider. In the event of a disaster, the MSPs can instantly spin-up virtual machines for the customer.

The DL1300 is not multi-tenant. The MSPs can use the DL1300 at multiple sites and create a multi-tenant environment at their end.

Parent topic

Virtualization and cloud

The DL1300 Core is cloud-ready, which allows you to leverage the compute capacity of the cloud for recovery and archive.

DL1300 can export any protected or replicated machine to licensed versions of VMware or Hyper-V. With continuous exports, the virtual machine is incrementally updated after every snapshot. The incremental updates are fast and provide standby-clones that are ready to be powered up with a click of a button. The supported virtual machine exports are:

- VMware Workstation or Server on a folder
- Direct export to a Vsphere or VMware ESXi host
- Export to Oracle VirtualBox
- Microsoft Hyper-V Server on Windows Server 2008 (x64)
- Microsoft Hyper-V Server on Windows Server 2008 R2
- Microsoft Hyper-V Server on Windows Server 2012 R2

You can now archive your repository data to the cloud using platforms such as Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage, or other OpenStack-based cloud services.

Parent topic

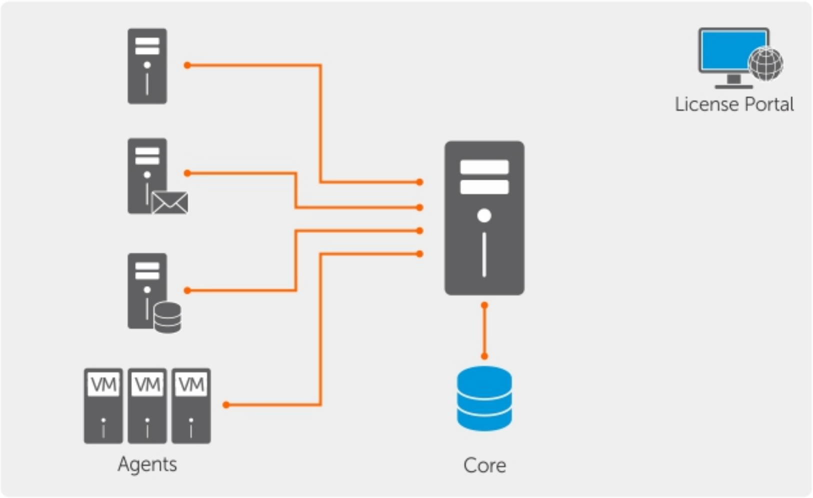
Quest DL1300 deployment architecture

Your DL1300 deployment architecture consists of local and remote components. The remote components may be optional for those environments that do not require leveraging a disaster recovery site or a managed service provider for off-site recovery. A basic local deployment consists of a backup server called the Core and one or more protected machines known as the agents. The off-site component is enabled using replication that provides full recovery capabilities in the disaster recovery site. The DL1300 Core uses base images and incremental snapshots to compile recovery points of protected agents.

Also, DL1300 is application-aware because it can detect the presence of Microsoft Exchange and SQL and their respective databases and log files. Backups are performed by using application-aware block-level snapshots. DL1300 performs log truncation of the protected Microsoft Exchange server.

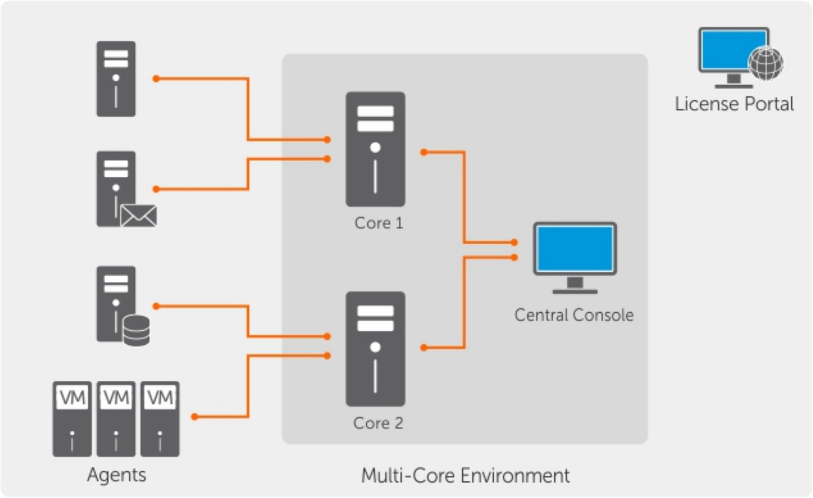
The following diagram depicts a simple DL1300 deployment. DL1300 Agents are installed on machines such as a file server, email server, database server, or virtual machines are connected to and protected by a single DL1300 Core, which consists of the central repository. The Quest software License Portal manages license subscriptions, groups and users for the agents and cores in your environment. The License Portal allows users to log in, activate accounts, download software, and deploy agents and cores per your license for your environment.

Figure 2. Quest DL1300 Deployment Architecture



You can also deploy multiple DL1300 Cores as shown in the following diagram. A central console manages multiple cores.

Figure 3. DL1300 Multi—Core Deployment Architecture



Parent topic

Other information you may need

NOTE: Always check for updates on Quest.com/support and read the updates first because they often supersede information in other documents.

NOTE: For any documentation related to Dell OpenManage Server Administrator, see Dell.com/openmanage/manuals.

Your product documentation includes:

Getting Started Guide

Provides an overview of setting up your system, and technical specifications. This document is shipped with your system.

System Placemat

Provides information on how to set up the hardware and install the software on your appliance.

Owner’s Manual

Provides information about system features and describes how to troubleshoot the system and install or replace system components.

Deployment Guide

Provides information on hardware deployment and the initial deployment of the appliance.

User’s Guide

Provides information about configuring and managing the system.

Release Notes

Provides product information and additional information on the Quest DL1300 Appliance.

Interoperability Guide

Provides information on supported software and hardware for your appliance as well as usage considerations, recommendations, and rules.

OpenManage Server Administrator User’s Guide

Provides information about using Dell OpenManage Server Administrator to manage your system.

Parent topic

Installing your Quest DL1300

Introduction

The DL Backup to Disk Appliance allows:

- 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

Parent topic

Available configurations

The DL appliance comes in the following configurations:

Table 1. Available configurations

The Dl000 system is available in 2 TB with no VMs configuration with 3 TB drive with a 200 GB operating system/software partition and 2 TB usable repository space. The DL1000 system is available in 3 TB with 2 VMs configuration with 4 TB drive with a 200 GB operating system/software partition, a 300GB partition for VM storage, and 3 TB usable repository space.

Capacity	Hardware Configuration
2 TB	Four 4 TB HDDs with 2 TB usable repository space
3 TB with 2 VMs	Four 4 TB HDDs with 3 TB usable repository space and adjustable VM space
4 TB with 2 VMs	Four 4 TB HDDs with 4 TB usable repository space and adjustable VM space

Each configuration includes the following hardware and software:

- Quest DL1300 system
- Dell PowerEdge RAID Controllers (PERC)
- Quest AppAssure software

Parent topic

Installation overview

The DL1300 installation involves installing the AppAssure Core and AppAssure 5 Agent services on the systems that have to be protected. If additional cores are set up then AppAssure 5 Central Management Console Services must be installed.

To install the DL1300 follow these steps:

1. Obtain the permanent license key. From the Core Console, you can manage your DL1300 licenses directly, change the license key, and contact the license server. You can also access the Quest AppAssure License Portal from the Licensing page in the Core Console.

   NOTE: The appliance is configured and shipped with a 30 day temporary software license.

2. Review installation prerequisites.
3. Setting up the hardware.
4. Setting up the initial software (AppAssure Appliance Configuration Wizard).
5. Installing the Core Management Console.

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 organizations to use switches of 1 GbE or above along with AppAssure for efficient performance.

Parent topic

Setting up the hardware

The appliance ships with a single DL1300 system. Before setting up the appliance hardware, see the *Getting Started Guide* for your system that shipped with the appliance. Unpack and set up the DL1300 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 DL1300 hardware:

1. Rack and cable the DL1300 system.
2. Turn on the DL1300 system.

Parent topic

Installing the DL1300 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 and the DL1300 in the rack.

Parent topic

Using the system without a rack

You can use the system without the server rack. When you are using the system without a rack, ensure that you follow these guidelines:

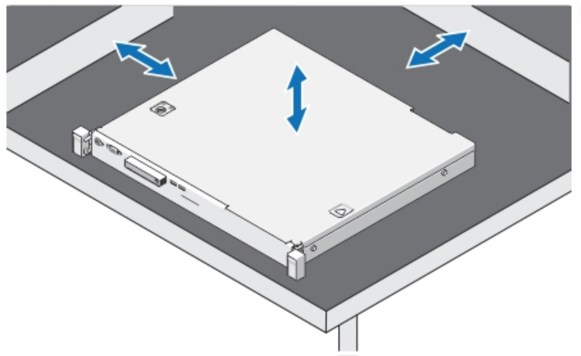
- The system must be placed on a solid, stable surface that supports the entire system.

  > NOTE: The system must not be placed vertically.

- Do not place the system on the floor.
- Do not place anything on top of the system. The top panel may deflect under the weight and cause damage to the system.
- Ensure adequate space around the system for proper ventilation.
- Ensure that the system is installed under the recommended temperature conditions as stated in the Technical Specification – Environmental Section of Quest DL1300 Appliance Owner’s Manual at Quest.com/support/home.

> CAUTION: Failure to follow these guidelines may result in damage to the system or physical injury.

Figure 4. Using the System Without a Rack



Parent topic

Cabling the appliance

Locate the Quest DL1300 Appliance Getting Started Guide that is shipped with the appliance and follow the instructions to attach the keyboard, mouse, monitor, power, and network cables to the DL1300 system.

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

Turning on the DL1300 Appliance

After cabling the appliance, turn on your system.

> NOTE: It is recommended that you connect the appliance to an uninterrupted power supply (UPS) for maximum reliability and availability. For more information, see the Quest DL1300 Getting Started Guide at Quest.com/support/manuals.

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 starts automatically.

1. After you turn on the system, choose your operating system language from the Windows language options.

   The Microsoft End User License Agreement (EULA) is displayed on the Settings page.

2. To accept the EULA, click I accept button.

A page 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.

   After entering the password, Press Ctrl+Alt+Delete to Sign in screen is displayed.
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 EULA screen is displayed.
9. To accept the EULA, click Accept EULA button.

   NOTE: You can run the AppAssure Appliance Configuration Wizard further only if you accept the EULA. Otherwise, the appliance will log you off immediately.

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.

Parent topic

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 Windows update service is disabled temporarily during the configuration process. Exiting the AppAssure Appliance Configuration Wizard before it is complete may cause errors in system operation.

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

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 are 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 you to perform several steps.

To configure the host name and domain settings:

1. On the Configure host name and domain setting page, in New host name text box enter an appropriate host name.

2. If you do not want to connect your appliance to a domain, select No in Do you want this appliance to join a domain?

   > NOTE: If your DL1300 is installed with Microsoft Windows Server 2012 Foundation edition, the option to join a domain will be disabled.

By default, Yes is selected.

3. If you want to connect your 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 AppAssure Appliance Configuration wizard is launched automatically. If the appliance is connected 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.

   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 it 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 Thank You page is displayed.
7. To complete the configuration, click Next.
8. Click Exit on the Configuration Complete page.

   The Core console opens on your default web browser.

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 quest.com/support.
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.

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 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

Configuring your Quest DL1300

Configuration overview

Configuration includes tasks such as configuring browsers to remotely access the DL1300 Core Console, managing licenses, and setting up alerts and notifications. After you complete the configuration of the Core, you can then protect agents and perform recovery.

NOTE: While using the DL1300 Backup To Disk Appliance, it is recommended that you use the Appliance tab to configure the Core.

Parent topic

Configuring browsers to remotely access the DL1300 Core Console

Before you can successfully access the Core Console from a remote machine, you must modify your browser's settings. The following procedures detail how to modify Internet Explorer, Google Chrome, and Mozilla Firefox browser settings.

NOTE: To modify browser settings, you must be logged on to the machine with administrator privileges.

NOTE: Because Chrome uses Internet Explorer settings, you must make the changes for Chrome 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, open Server Manager > Local Server > IE Enhanced Security Configuration option is displayed, ensure that it is On.

Parent topic

Configuring browser settings in Internet Explorer and Chrome

To configure browser settings in Internet Explorer and Chrome:

1. From the Internet Options screen, select the Security tab.
2. Click Trusted Sites and then click Sites.
3. 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 5 Core> to Trusted Sites.
4. Click Close, select Trusted Sites, and then click Custom Level.
5. Scroll to Miscellaneous → Display Mixed Content and select Enable.
6. Scroll to the bottom of the screen to User Authentication → Logon, and then select Automatic logon with current user name and password.
7. Click OK, and then select the Advanced tab.
8. Scroll to Multimedia and select Play animations in webpages.
9. Scroll to Security, check Enable Integrated Windows Authentication, and then click OK.

Parent topic

Configuring browser settings in Firefox

To modify browser settings in Firefox:

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 Core; for example, IP Address, host name.
4. Restart Firefox.

Parent topic

Accessing the DL1300 Core Console

Ensure that you update trusted sites as discussed in the topic Updating Trusted Sites In Internet Explorer, and configure your browsers as discussed in the topic Configuring browsers to remotely access the DL1300 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 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

Managing licenses

You can manage your DL1300 licenses directly from the Core Console. From the console, you can change the license key and contact the license server. You can also access the License Portal from the Licensing page in the Core console or you can access the license portal at https:// licenseportal.com.

The Licensing page includes the following information:

- License type
- License status
- Details of the repository
- Replication master cores (inbound)
- Replication slave cores (outbound)
- Simultaneous rolluos
- Rollup retention policy
- Encryption keys
- Vartual standby exports
- Mountability checks
- Exchange log truncations
- SQL log truncation
- Minimum snapshot interval

Parent topic

Contacting the license portal server

The Core Console contacts the portal server to update changes made in the license portal. Communication with the portal server occurs automatically at designated intervals; however, you can initiate communication on demand.

To contact the portal server:

1. Navigate to the Core Console and then click Configuration > Licensing.

   The Licensing page is displayed.
2. From the License Server option, click Contact Now.

Parent topic

Changing a license key

To change a license key:

1. Navigate to the Core Console, select Configuration > Licensing.

   The Licensing page is displayed.
2. From the License Details page, click Change License.

   The Change License dialog box is displayed.
3. Update the new license key. To update the license key:

   - Select the appropriate license key using the Browse tab in the Upload License File box.

     To download the appropriate license:

     1. Go to www.rapidrecovery.licenseportal.com.
     2. From the Software drop-down menu on the upper-left corner of the page, select Appliance.
        All the available licenses and related information is displayed.
     3. In the Actions column, click the download icon.
        The license is downloaded on your system.
   - Enter the license key in the Enter License Key field.
4. Click Continue.

   The license on your system is updated.

Parent topic

Changing the AppAssure language manually

AppAssure allows you to change the language that you had selected while running AppAssure Appliance Configuration Wizard to any of the supported languages.

To change the AppAssure language to the desired language:

1. Launch the registry Editor using `regedit` command.
2. Navigate to HKEY_LOCAL_MACHINE → SOFTWARE → AppRecovery → Core → Localization.
3. Open Lcid.
4. Select decimal.
5. Enter the required language value in the Value data box, the supported language values are:
   a. English: 1033

    b. Brazilian Portuguese: 1046
    c. Spanish: 1034
    d. French: 1036
    e. German: 1031
    f. Simplified Chinese: 2052
    g. Japanese: 1041
    h. Korean: 1042
6. Right-click and restart the services in the given order:
    a. Windows Management Instrumentation
    b. SRM Web Service
    c. AppAssure Core
7. Clear the browser cache.
8. Close the browser and restart the core console from the desktop icon.

Parent topic

Changing the operating system language during installation

On a running Microsoft Windows installation, you can use the control panel to select language packs and configure additional international settings.

To change operating system (OS) language:

> NOTE: It is recommended that the OS language and the AppAssure language be set to the same language. otherwise, some messages may be displayed in mixed languages.

> NOTE: It is recommended to change the OS language before changing the AppAssure language.

1. On the Start page, type language, and make sure that the search scope is set to Settings.
2. In the Results panel, select Language.
3. In the Change your language preferences pane, select Add a language.
4. Browse or search for the language that you want to install.

    For example, select Catalan, and then select Add. Catalan is now added as one of your languages.
5. In the Change your language preferences pane, select Options next to the language that you added.
6. If a language pack is available for your language, select Download and install language pack.
7. When the language pack is installed, the language is displayed as available to use for the Windows display language.
8. To make this language your display language, move it to the top of your language list.
9. Log out and log in again to Windows for the change to take effect.

Parent topic

Encrypting agent snapshot data

The Core can encrypt agent snapshot data within the repository. Instead of encrypting the entire repository, DL1300 allows you to specify an encryption key during the protection of an agent in a repository which allows the key to be reused for different agents.

To encrypt agent snapshot data:

1. From the Core, click Configuration → Manage → Security.
2. Click Actions, and then click Add Encryption Key.

   The Create Encryption Key page id 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. For more information, see Managing Security chapter in the Quest DL1300 Appliance User’s Guide.

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 are sent. For more information on specifying events to receive email alerts, see Configuring Notification Groups For System Events in the Quest DL1300 Appliance User's Guide at Quest.com/support.

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 is displayed.
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

Preparing to protect your servers

Overview

To protect your data using DL1300, you need to add the workstations and servers for protection in the Core Console; for example, your Exchange server, SQL Server, your Linux server, and so on.

In the Core Console, you can identify the machine on which an Agent is installed and specify which volumes, for example, a Microsoft Windows Storage Space, to protect. You can define the schedules for protection, add additional security measures such as encryption, and much more. For more information on how to access the Core Console to protect workstations and servers, see Protecting Machines.

Protecting machines

After configuring the 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 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 DL1300 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 Core and any clients that it backs up:

1. On the DL1300 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 Core and ports display Yes in the Enabled column.
6. If the rule is not enabled, right-click on Core and select Enable Rule.
7. Click Outbound Rules and verify the same for Core.

Parent topic

Checking DNS resolution

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 appliance, go to `C:\Windows\system32\drivers\etc` hosts.
2. Enter the IP address of each client that backs up to DL1300.

Parent topic

Teaming network adapters

By default, the network adapters (NICs) on the DL1300 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

Parent topic

Reinstalling Broadcom Advanced Configuration Suite

To reinstall Broadcom Advanced Configuration Suite:

1. Go to `C:\Install\BroadcomAdvanced` and double-click `setup`.

   The InstallShield Wizard is displayed.
2. Click Next.
3. Click Modify, Add, or Remove.

   The Custom Setup window is displayed.
4. Click CIM Provider, and then select This feature will be installed on local hard drive.
5. Click BASP, and then select This feature will be installed on local hard drive.
6. Click Next.
7. Click Install.
8. Click Finish.

Parent topic

Creating the NIC team

NOTE: It is recommended to not 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 DL1300 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: Building of the NIC team may take approximately five minutes.

Parent topic

Adjusting concurrent 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

Installing agents on clients

Each client that is backed up by the AppAssure appliance must have the AppAssure agent installed. The AppAssure 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 DL1300 Appliance User’s Guide at Quest.com/support.

Parent topic

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.NET 4 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 a machine

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. Navigate to Protect Machine → Connect, after entering the appropriate connection settings in the dialog box.
2. Click Connect.

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

   The Deploy Agent dialog box is displayed.
4. Enter login 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 that is displayed on the Core Console. The display name could be the same value as the host name.
   - Protect machine after install — Selecting this option enables DL1300 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 Forcing A Snapshot in the Quest DL1300 Appliance User's Guide at Quest.com/support.

- 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.

5. 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 .NET 4 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 5 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: Quest supports the above Linux distributions and has tested 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 Deploying An Agent (Push Install) in the Quest DL1300 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 Core. You can download the installers from the 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 Qeust DL1300 Appliance User's Guide at Qeust.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: 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 agent for TCP ports 8006 and 8009 for the 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 agent on Ubuntu:

1. Open a terminal session with root access.
2. To make the 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 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 installation process is complete, the Ubuntu Agent is installed on your machine. For more information on protecting this machine with the Core, see the topic 'Protecting Workstations and Servers' in the Quest DL1300 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 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 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 topic 'Protecting Workstations and Servers' in the Quest DL1300 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 DL1300 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 DL1300 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 DL1300 Appliance User’s Guide at Quest.com/support.

Parent topic

Common use cases

This section provides the most common use cases for the DL1300 and provides a high-level overview of the information and procedures required for each scenario. Where required, references to additional information is provided.

Protecting machines

The AppAssure backup and replication technology provides advanced protection of VMs or servers while enabling flexible application and data recovery. When a machine is protected, full and incremental snapshots of data are captured and stored in the core's repository. The AppAssure protection process leverages two key technologies – Snapshots and the Quest DL1300 Smart Agent that are described below.

Parent topic

Snapshots

The AppAssure Agent for Windows uses Microsoft Volume Shadow copy Service (VSS) to freeze and quiesce application data to disk to capture a file-system-consistent and an application-consistent backup. When a snapshot is created, the VSS, writer on the target server prevents content from being written to the disk. During the process of halting of writing content to disk, all disk I/O operations are queued and resume only after the snapshot is complete, while the operations already in flight will be completed and all open files will be closed. For more information, see topic Snapshot Process.

Parent topic

Quest DL1300 Smart Agents

The Smart Agent is installed on the machines that are protected by the DL1300 Core. The Smart Agent tracks the changed blocks on the disk volume and then snaps an image of the changed blocks at a predefined interval of protection. The incremental block-level snapshots' forever approach prevents repeated copying of the same data from the protected machine to the Core. When the snapshot is ready, it is rapidly transferred to the Core using intelligent multi-threaded, socket-based connections. For more information, see the topic Quest DL1300 Smart Agent.

Parent topic

Deploying Smart Agents

You must install the AppAssure Agent Installer on every machine in your environment protected by the DL1300 Core.

ℹ NOTE: These procedures are a summary. For detailed information, or specific instructions for Linux Agents, refer to the Quest DL1300 Appliance User's Guide.

Parent topic

Step 1: Obtaining the Agent Software

Smart Agent software can be obtained by following one of the following methods:

- Download from the AppAssure Core — Log into the Core Console and download the software to the agent machine. Select Downloads from the Tools tab, and then download the web installer for the Agent component.
- Download from the AppAssure License Portal — If you have registered your software in the Dell Software License Portal, you can log into the License Portal and download the software to the agent machine.
- Deploy the Agent Software when protecting a machine — You can deploy the Agent software to the machine you want to protect using the Protect a Machine Wizard.
- Use the Bulk Deploy feature — If the Core is installed, you can deploy the Agent software to multiple machines using the Bulk deploy feature, accessed from the Tools tab of the Core Console.

Parent topic

Step 2: Install the Agent Software

Launch the installer program as described below to install the software on each machine you want to protect in the Core. To install the Agent software on Windows machines:

1. From the machine you want to protect, double-click the Agent installer file.
2. On the Welcome page, click Next to continue with the installation.
3. On the License Agreement page, click I accept the terms in the license agreement, and click Next.

   ℹ NOTE: The Agent Installer verifies the existence of the prerequisite files. If the prerequisite files do not exist, the Agent Installer identifies which files are needed and displays the results accordingly; for example, Microsoft System CLR Types for SQL Server 2008 R2 (x64).

4. Click Install Prerequisites.
5. When the installation of the prerequisite files is completed, click Next.
6. On the Installation Options page, review the installation options. If necessary, modify them as described below:
   a. In the Destination Folder text field, review the destination folder for the installation. If you want to change the location, do the following:
      - Click the folder icon
      - In the Browse to Destination dialog box, select a new location. Click OK.

   b. In the Port Number text field, enter a port number to use for communication between the agent and the Core.

      ℹ NOTE: The default value is 8006. If you change the port number, make a note of it in the event that you need to adjust configuration settings at a later time.

7. Check for the installation options, click Install. When the installation is complete, the Completed page is displayed.
8. Select one of the following options, and then click Finish: Yes, I want to restart my computer now. No, I will restart my computer later.

ℹ NOTE: You must restart your system before using the Agent software.

Parent topic

Configuring protection jobs

When you add protection, you need to define connection information such as the IP address and port, and provide credentials for the machine you want to protect. Optionally, you can provide a display name to appear in the Core Console instead of the IP address. You will also define the protection schedule for the machine.

> NOTE: These procedures are a summary. For more detailed information, refer to the Quest DL1300 Appliance User’s Guide at Quest.com/support.

Parent topic

Protecting a machine

This topic describes how to start protecting the data on a machine that you specify.

> NOTE: The machine must have the AppAssure Agent software installed in order to be protected. You can choose to install the Agent software prior to this procedure, or you can deploy the software to the agent as you define protection in the Connection dialog box. To install the agent software during the process of protecting a machine, see topic 'Deploying The Agent Software When Protecting An Agent' in Quest DL1300 Appliance User’s Guide.

When you add protection, you must specify the name or IP address of the machine to protect and the volumes on that machine to protect as well as define the protection schedule for each volume.

To protect multiple machines at the same time, see topic 'Protecting Multiple Machines' in Quest DL1300 Appliance User’s Guide.

To protect a machine:

1. Reboot the machine on which the AppAssure Agent software is installed, if you haven’t already done so.
2. From the Core Console on the core machine, click Protect > Protect Machine on the button bar.

   The Protect Machine Wizard is displayed.
3. On the Welcome page, select the appropriate installation options:
   - If you do not need to define a repository or establish encryption, select Typical.
   - If you do not wish to see the Welcome page for the Protect Machine Wizard in the future, select the Skip this Welcome page the next time the wizard opens option.
4. Click Next.
5. On the Connection page, enter the information about the machine to which you want to connect as described in the following table.

   Text Box

   Description

   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. The default port number is 8006.

   Username

   The user name used to connect to this machine; for example, administrator.

   Password

The password used to connect to this machine.

6. Click Next. If the Protection page appears next in the Protect Machine Wizard, skip to Step 7.

   NOTE: If the Install Agent page appears next in the Protect Machine Wizard, this indicates that the Agent software is not yet on installed on the designated machine. Click Next to install the Agent software. The Agent software must be installed on the machine you want to protect, and that be restarted, before it can back up to the Core. To have the installer reboot the agent machine, select the After installation, restart the machine automatically (recommended) option before clicking Next.

7. The host name or IP address you specified in the Connect dialog box appears in this text field. Optionally, enter a new name for the machine to be displayed in the Core Console.
8. Select the appropriate protection schedule:
   - To use the default protection schedule, in the Schedule Settings option, select Default protection (3 hour snapshots of all volumes). With a default protection schedule, the Core will take snapshots of the agent machine once every 3 hours. Snapshots of the agent machine can be taken once every hour (minimum). To change the protection settings at any time after you close the wizard, including choosing which volumes to protect, go to the Summary tab for the specific agent machine.
   - To define a different protection schedule, in the Schedule Settings option, select Custom protection.
9. Select one of the following:
   - If you selected a Typical configuration from the Protect Machine Wizard and specified default protection, then click Finish to confirm your choices, close the wizard, and protect the machine you specified.
   - The first time protection is added for a machine, a base image (that is, a snapshot of all the data in the protected volumes) will transfer to the repository on the Core following the schedule you defined, unless you specified to initially pause protection.
   - If you selected a Typical configuration for the Protect Machine Wizard and specified custom protection, then click Next to set up a custom protection schedule. For details on defining a custom protection schedule, see Creating Custom Protection Schedules.
   - If you selected Advanced configuration for the Protect Machine Wizard, and default protection, then click Next and proceed to Step 12 to see repository and encryption options.
   - If you selected Advanced configuration for the Protect Machine Wizard and specified custom protection, then click Next and proceed to Step 10 to choose which volumes to protect.
10. On the Protection Volumes page, select the volumes on the agent machine that you want to protect. If any volumes are listed that you do not want to include in protection, click in the Check column to clear the selection. Then click Next.

    NOTE: It is recommended to protect the System Reserved volume and the volume with the operating system (typically the C drive).

11. On the Protection Schedule page, define a custom protection schedule.
12. On the Repository page, select Use an existing repository.
13. Click Next.

    The Encryption page is displayed.

14. Optionally, to enable encryption, select Enable Encryption.

    Encryption key fields appear on the Encryption page.

    NOTE: If you enable encryption, it will be applied to data for all protected volumes for this agent machine. You can change the settings later from the Configuration tab in the AppAssure 5 Core Console.

CAUTION: Quest AppAssure uses AES 256-bit encryption in the Cipher Block Chaining (CBC) mode with 256-bit keys. While using encryption is optional, Quest highly recommends that you establish an encryption key, and that you protect the passphrase you define. Store the passphrase in a secure location as it is critical for data recovery. Without a passphrase, data recovery is not possible.

15. Enter the information as described in the following table to add an encryption key for the Core.

    Text Box

    Description

    Name

    Enter a name for the encryption key.

    Description

    Enter a description to provide additional details for the encryption key.

    Passphrase

    Enter the passphrase used to control access.

    Confirm Passphrase

    Re-enter the passphrase you just entered.

16. Click Finish to save and apply your settings.

    The first time protection is added for a machine, a base image (that is, a snapshot of all the data in the protected volumes) will transfer to the repository on the AppAssure Core following the schedule you defined, unless you specified to initially pause protection.

Parent topic

Recovering data

With the DL1300, data is protected on both Windows and Linux machines. Protected machine backups are saved to the Core as recovery points that can be used to restore your data. Entire volumes can be restored replaced from a recovery point to the destination machines. To restore data from recovery points any one of the following methods can be performed:

- Recovery of files and folders
- Recovery of data volumes, using Live Recovery
- Bare metal restore, using Universal Recovery

Parent topic

Recovering directories or files

You can use Windows Explorer to copy and paste directories and files from a mounted recovery point to any Windows machine. This can be helpful when you want to distribute only a portion of a recovery point to your users. When you copy directories and files, the access permissions of the user who is performing the copy operation are used and applied to the pasted directories and files.

To restore a directory or file using Windows Explorer:

1. Mount the recovery point that contains the data you want to restore. For more information, see Mounting A Recovery Point For A Windows Machine topic in the Quest DL1300 Appliance User’s Guide.
2. In Windows Explorer, navigate to the mounted recovery point and select the directories and files that you want to restore. Right-click and select Copy.
3. In Windows Explorer, navigate to the machine location to where you want to restore the data. Right-click and select Paste.

Parent topic

Restoring volumes

From the Core Console, you can restore entire volumes from a recovery point of a non-system volume, replacing the volumes on the destination machine.

> NOTE: The procedure below is a simplified overview of the restore process. For detailed information or procedures on additional restore options, see topic ‘Restoring Volumes from a Recovery Point’ in the Quest DL1300 Appliance User’s Guide.

To restore volumes from a recovery point:

1. In the Core Console, click the Restore tab.

   The Restore Machine Wizard is displayed.
2. From the Protected Machines page, select the protected machine for which you want to restore data, and then click Next.

   > NOTE: The protected machine must have the Agent software installed and must have recovery points from which you will perform the restore operation.

   The Recovery Points page is displayed.
3. From the list of recovery points, search for the snapshot you want to restore to the agent machine.

   > NOTE: If required, use the navigation buttons at the bottom of the page to display additional recovery points. Or if you want to limit the amount of recovery points showing in the Recovery Points page of the wizard, you can filter by volumes (if defined) or by creation date of the recovery point.
4. Click any recovery point to select it, and then click Next.

   The Destination page is displayed.
5. On the Destination page, choose the machine to which you want to restore data as follows:
   - If you want to restore data from the selected recovery point to the same agent machine (for example, Machine1), and if the volumes you want to restore do not include the system volume, then select Recover to a protected machine (only non-system volumes), verify that the destination machine (Machine1) is selected, and then click Next. The Volume Mapping page appears. Proceed to Step 6.
   - If you want to restore data from the selected recovery point to a different protected machine (for example, to replace the contents of Machine2 with data from Machine1), then select Recover to a protected machine (only non-system volumes), select the destination machine (for example, Machine2) from the list, and then click Next . The Volume Mapping page appears. Proceed to Step 6.
   - If you want to restore from a recovery point to a system volume (for example, the C drive of the agent machine named Machine1), you must perform a BMR.
6. On the Volume Mapping page, for each volume in the recovery point that you want to restore, select the appropriate destination volume. If you do not want to restore a volume, in the Destination Volumes column, select Do not restore.
7. Select Show advanced options and then do the following:
   - For restoring to Windows machines, if you want to use Live Recovery, select Live Recovery.

Using the Live Recovery instant recovery technology in AppAssure 5, you can instantly recover or restore data to your physical machines or to virtual machines from stored recovery points of Windows machines, which includes Microsoft Windows Storage Spaces. Live Recovery is not available for Linux machines.

- If you want to force dismount, select Force Dismount.

  If you do not force a dismount before restoring data, the restore may fail with a volume in use error. The agent machine, when started from the boot CD, displays the Universal Recovery Console (URC) interface. This environment is used to restore the system drive or selected volumes directly from the Core. Note the IP address and authentication key credentials in the URC, which refresh each time you start from the boot CD.

8. If the volumes you want to restore contain SQL or Microsoft Exchange databases, on the Dismount Databases page, you are prompted to dismount them. Optionally, if you want to remount these databases after the restore is complete, select Automatically remount all databases after the recovery point is restored. Click Finish.
9. Click OK to confirm the status message that the restore process has started.
10. To monitor the progress of your restore action, on the Core Console, click Events.

Parent topic

Bare Metal Recovery

AppAssure provides the ability to perform a bare metal restore (BMR) for your Windows or Linux machines. BMR is a process that restores the full software configuration for a specific system. It uses the term “bare metal” because the restore operation recovers not only the data from the server, but also reformats the hard drive and reinstalls the operating system and all software applications. To perform a BMR, you specify a recovery point from a protected machine, and roll back to the designated physical or virtual machine. Other circumstances in which you may choose to perform a bare metal restore include hardware upgrade or server replacement.

Performing a BMR is possible for physical or virtual machines. As an added benefit, AppAssure allows you to perform a BMR whether the hardware is similar or dissimilar.

Parent topic

Prerequisites for performing a Bare Metal Restore for a Windows machine

Before you can begin the process of performing a bare metal restore for a Windows machine, you must ensure that the following conditions and criteria exist:

- Backups of the machine you want to restore — You must have a functioning AppAssure Core containing recovery points of the protected server you want to restore.
- Hardware to restore (new or old, similar or dissimilar) — The target machine must meet the installation requirements for an agent.
- Image media and software — You must have a blank CD or DVD and disk burning software, or software to create an ISO image. If managing machines remotely using virtual network computing software such as UltraVNC, then you must have VNC Viewer.
- Compatible storage drivers and network adapter drivers — If restoring to dissimilar hardware, then you must have Windows 7 PE (32-bit) compatible storage drivers and network adapter drivers for the target machine, including RAID, AHCI, and chipset drivers for the target operating system, as appropriate.
- Storage space and partitions, as appropriate — Ensure that there is enough space on the hard drive to create destination partitions on the target machine to contain the source volumes. Any destination partition should be at least as large as the original source partition.
- Compatible partitions — Windows 8 and Windows Server 2012 operating systems that are booted from FAT32 EFI partitions are available for protection or recovery, as well as are Resilient File System (ReFS) volumes. UEFI partitions are treated as simple FAT32 volumes. Incremental transfers are fully supported and protected. AppAssure 5 provides support of UEFI systems for BMR including automatic partitioning GPT disks.

Parent topic

Roadmap for performing a Bare Metal Restore for a Windows machine

NOTE: Following are basic steps used in the Bare Metal Restore (BMR) process. For detailed information on each step, see the Quest DL1300 Appliance User’s Guide.

To perform a BMR for a Windows machine:

1. Create a boot CD.
2. Burn the image to disk.
3. Boot the target server from the boot CD.
4. Connect to the recovery disk.
5. Map the volumes.
6. Initiate the recovery.
7. Monitor the progress.

Parent topic

Replicating recovery points

Replication is the process of copying recovery points and transmitting them to a secondary location for the purpose of disaster recovery. The process requires a paired source-target relationship between two cores.

The source core copies the recovery points of the protected agents and then asynchronously and continuously transmits them to a target core at a remote disaster recovery site. The off-site location can be a company-owned data center (self-managed core) or a third-party managed service provider's (MSP's) location or cloud environment. When replicating to a MSP, you can use built-in work flows that let you request connections and receive automatic feedback notifications. Possible scenarios for replication include:

- Replication to a Local Location— The target core is located in a local data center or on-site location, and replication is maintained at all times. In this configuration, the loss of the Core would not prevent a recovery.
- Replication to an Off-site Location— The target core is located at an off-site disaster recovery facility for recovery in the event of a loss.
- Mutual Replication— Two data centers in two different locations each contain a core and are protecting agents and serving as the off-site disaster recovery backup for each other. In this scenario, each core replicates the agents to the Core that is located in the other data center.
- Hosted and Cloud Replication— AppAssure MSP partners maintain multiple target cores in a data center or a public cloud. On each of these cores, the MSP partner lets one or more of their customers replicate recovery points from a source core on the customer's site to the MSP's target core for a fee.

Parent topic

Setting up your environment

If the bandwidth between the source core and the target core cannot accommodate the transfer of stored recovery points, replication begins with seeding the target core with base images and recovery points from the selected servers protected on the source core. The seeding process can be performed at any time, as part of the initial transfer of data to serve as the foundation for regularly scheduled replication, or in the case of re-instating replication for a previously replicated machine whose replication had been paused or deleted. In this case, the Build RP Chain option would let you copy not-yet replicated recovery points to a seed drive.

When preparing for replication, you should consider the following factors:

- Change Rate—The change rate is the rate at which the amount of protected data is accumulated. The rate depends on the amount of data that change on protected volumes and the protection interval of the volumes. If a set of blocks change on the volume, reducing the protection interval reduces the change rate.
- Bandwidth— The bandwidth is the available transfer speed between the source core and the target core. It is crucial that the bandwidth be greater than the change rate for replication to keep up with the recovery points created by the snapshots. Due to the amount of data transmitted from core to core, multiple parallel streams may be required to perform at wire speeds up to the speed of a 1 GB Ethernet connection.

  > NOTE: Bandwidth specified by the ISP is the total available bandwidth. The outgoing bandwidth is shared by all devices on the network. Make sure that there is enough free bandwidth for replication to accommodate the change rate.

- Number of Agents— It is important to consider the number of agents protected per source core and how many you plan to replicate to the target. DL1300 lets you perform replication on a per-protected server basis, so you can choose to replicate certain servers. If all protected servers must be replicated, this drastically affects the change rate, particularly if the bandwidth between the source and target cores is insufficient for the amount and size of the recovery points being replicated.

Depending on your network configuration, replication can be a time-consuming process.
The Maximum Change Rate for WAN Connection Types is shown in the table below with examples of the necessary bandwidth per gigabyte for a reasonable change rate.

Table 2. Maximum Change Rate for WAN Connection Types

The maximum change rate that can be achieved with DSL broadband at a bandwidth of 768 Kbps and up is 330 MB per hour. The maximum change rate that can be achieved with Cable broadband at a bandwidth of 1 Mbps and up is 429 MB per hour .The maximum change rate that can be achieved with T1 broadband at a bandwidth of 1.5 Mbps and up is 644 MB per hour. The maximum change rate that can be achieved with Fiber broadband at a bandwidth of 20 Mbps and up is 838 GB per hour.

Broadband	Bandwidth	Max Change Rate
DSL	768 Kbps and up	330 MB per hour
Cable	1 Mbps and up	429 MB per hour
T1	1.5 Mbps and up	644 MB per hour
Fiber	20 Mbps and up	8.38 GB per hour

For optimum results, you should adhere to the recommendations listed in the table above. If a link fails during data transfer, replication resumes from the previous failure point of the transfer once link functionality is restored.

Parent topic

Steps for configuring replication

NOTE: The information below is presented as a high-level overview of the steps required to perform replication. For complete procedures, go to the Quest DL1300 Appliance User’s Guide at Quest.com/support.

To replicate data using AppAssure, you must configure the source and target cores for replication. After you configure replication, you can then replicate agent data, monitor and manage replication, and perform recovery. Performing replication in AppAssure involves performing the following operations:

- Configure self-managed replication — For more information on replicating to a self-managed target core, see topic 'Replicating to a Self-Managed Target Core' in the Quest DL1300 Appliance User’s Guide at Quest.com/support.
- Configure third-party replication— For more information on replicating to a third-party target core, see topic 'Process of Replicating to a Third-Party Target Core' in the Quest DL1300 Appliance User’s Guide at Quest.com/support.
- Replicate an existing agent— For more information on replicating an agent that is already protected by the source core, see topic 'Adding a Machine to Existing Replication' in the Quest DL1300 Appliance User’s Guide at Quest.com/support.
- Consume the seed drive — For more information on consuming seed drive data on the target core, see topic 'Consuming the Seed Drive on a Target Core' in the Quest DL1300 Appliance User’s Guide at Quest.com/support.
- Set the replication priority for an agent— For more information on prioritizing the replication of agents, see topic 'Setting Replication Priority for an Agent' in the Quest DL1300 Appliance User’s Guide at Quest.com/support.
- Set a replication schedule for an agent— For more information on setting a replication schedule, see topic 'Scheduling Replication' in the Quest DL1300 Appliance User’s Guide at Quest.com/support.
- Monitor replication as needed— For more information on monitoring replication, see topic 'Monitoring Replication' in the Quest DL1300 Appliance User’s Guide at Quest.com/support.
- Manage replication settings as needed— For more information on managing replication settings, see topic 'Managing Replication Settings' in the Quest DL1300 Appliance User’s Guide at Quest.com/support.
- Recover replicated data in the event of disaster or data loss— For more information on recovering replicated data, see topic 'Recovering Replicated Data' in the Quest DL1300 Appliance User’s Guide at Quest.com/support.

Parent topic

Using virtual standby

AppAssure supports both a one-time export and continuous export (to support virtual standby) of Windows backup information to a virtual machine. Exporting your data to a virtual standby machine provides you with a high availability copy of the data. If a protected machine goes down, you can boot up the virtual machine to perform recovery.

When you export to a virtual machine, all of the backup data from a recovery point as well as the parameters defined for the protection schedule for your machine will be exported. You can also create a “virtual standby” by having protected data continuously exported from your protected machine to a virtual machine.

NOTE: Only the 3 TB with 2 VMs and 4 TB with 2 VMs configuration of DL1300 supports the one-time export and continuous export on virtual standby VMs.

Parent topic

Performing a one-time Hyper-V export

`To perform a one-time Hyper-V export:`

1. In the Core Console, navigate to the machine you want to export.
2. On the Summary tab, click Actions > Export > One-time.

   The Export Wizard displays on the Protected Machines page.
3. Select a machine for export, and then click Next.
4. On the Recovery Points page, select the recovery point that you want to export, and then click Next.

Parent topic

Defining one-time settings for performing a Hyper-V export

To define one-time settings for performing a Hyper-V export:

1. From the Hyper-V dialog box, click Use local machine to perform the Hyper-V export to a local machine with the Hyper-V role assigned.
2. Click the Remote host option to indicate that the Hyper-V server is located on a remote machine. If you selected the Remote host option, enter the parameters for the remote host described as follows:

   Text Box

   Description

   Host Name

   Enter an IP address or host name for the Hyper-V server. It represents the IP address or host name of the remote Hyper-V server.

   Port

   Enter a port number for the machine. It represents the port through which the Core communicates with this machine.

   User Name

   Enter the user name for the user with administrative privileges for the workstation with the Hyper-V server. It is used to specify the logon credentials for the virtual machine.

Password

Enter the password for the user account with administrative privileges on the workstation with Hyper-V server. It is used to specify the logon credentials for the virtual machine.

3. Click Next.
4. On the Virtual Machines Options page in the VM Machine Location text box, enter the path or location for the virtual machine. For example, D:\export. The VM location must have sufficient space to hold the VM metadata and virtual drives needed for the virtual machine.
5. Enter the name for the virtual machine in the Virtual Machine Name text box.

   The name that you enter appears in the list of virtual machines in the Hyper-V Manager console.
6. Click one of the following:
   - Use the same amount of RAM as the source machine to identify that the RAM use is identical between the virtual and source machines.
   - Use a specific amount of RAM to specify how much memory the virtual machine has after the export; for example, 4096 MB. (recommended)
7. To specify the disk format, next to Disk Format, click one of the following:
   - VHDX
   - VHD

   NOTE: Hyper-V Export supports VHDX disk formats if the target machine is running Windows 8 (Windows Server 2012) or higher. If the VHDX is not supported for your environment, the option is disabled.
8. On the Volumes page, select the volume(s) to export. For the virtual machine to be an effective backup of the protected machine include the protected machine’s boot drive. Example. C:\.

Your selected volumes should be no larger than 2040 GB for VHD. If the selected volumes are larger than 2040 GB, and the VHD format is selected, you will receive an error.

9. On the Summary page, click Finish to complete the wizard and to start the export.

Performing a continuous (virtual standby) Hyper-V export

NOTE: Only the DL1300 3 TB with 2 VMs and 4 TB with 2 VMs configurations support the one-time export and continuous export on virtual standby VMs.

To perform a continuous (virtual standby) Hyper-V export:

1. In the Core Console, on the Virtual Standby tab, click Add to launch the Export Wizard. On the Protected Machines page of the Export Wizard.
2. Select the machine you want to export and then click Next.
3. On the Summary tab, click Export > Virtual Standby.
4. From the Hyper-V dialog box, click Use local machine to perform the Hyper-V export to a local machine with the Hyper-V role assigned.
5. Click the Remote host option to indicate that the Hyper-V server is located on a remote machine. If you selected the Remote host option, enter the parameters for the remote host described as follows:

Text Box

Description

Host Name

Enter an IP address or host name for the Hyper-V server. It represents the IP address or host name of the remote Hyper-V server.

Port

Enter a port number for the machine. It represents the port through which the Core communicates with this machine.

User Name

Enter the user name for the user with administrative privileges for the workstation with the Hyper-V server. It is used to specify the logon credentials for the virtual machine.

Password

Enter the password for the user account with administrative privileges on the workstation with Hyper-V server. It is used to specify the logon credentials for the virtual machine.

6. On the Virtual Machines Options page in the VM Machine Location text box, enter the path or location for the virtual machine. For example, D:\export. The VM location must have sufficient space to hold the VM metadata and virtual drives needed for the virtual machine.
7. Enter the name for the virtual machine in the Virtual Machine Name text box.

   The name that you enter appears in the list of virtual machines in the Hyper-V Manager console.
8. Click one of the following:
   - Use the same amount of RAM as the source machine to identify that the RAM use is identical between the virtual and source machines.
   - Use a specific amount of RAM to specify how much memory the virtual machine has after the export; for example, 4096 MB (recommended).
9. To specify the Generation, click one of the following:
   - Generation 1 (recommended)
   - Generation 2
10. To specify the disk format, next to Disk Format, click one of the following:
    - VHDX (Default)
    - VHD

    NOTE: Hyper-V Export supports VHDX disk formats if the target machine is running Windows 8 (Windows Server 2012) or higher. If the VHDX is not supported for your environment, the option is disabled. On the Network Adapters page, select the virtual adapter to be connected to a switch.
11. On the Volumes page, select the volume(s) to export. For the virtual machine to be an effective backup of the protected machine include the protected machine’s boot drive. Example, C:\.

Your selected volumes should be no larger than 2040 GB for VHD. If the selected volumes are larger than 2040 GB, and the VHD format is selected, you will receive an error.

12. On the Summary page, click Finish to complete the wizard and to start the export.

    NOTE: You can monitor the status and progress of the export by viewing the Virtual Standby or Events tab

Parent topic

Managing recovery points

Periodic backup snapshots of all the protected servers accumulate on the Core over time. The retention policies are used to retain backup snapshots for longer periods of time and to help with management of these backup snapshots. The retention policy is enforced by a nightly rollup process that helps in aging and deleting old backups.

Parent topic

Archiving data

Retention policies enforce the periods for which backups are stored on short-term (fast and expensive) media. Sometimes certain business and technical requirements mandate extended retention of these backups, but use of fast storage is cost prohibitive. Therefore, this requirement creates a need for long-term (slow and cheap) storage. Businesses often use long-term storage for archiving both compliance and noncompliance data. The archive feature in AppAssure is used to support the extended retention for compliance and noncompliance data. It is also used to seed replication data to a remote replica core.

Parent topic

Creating an archive

To create an archive:

1. In the Core Console, click Tools > Archive > Create.

   The Add Archive Wizard dialog box appears.
2. On the Create page of the Add Archive Wizard, select one of the following options from the Location Type drop-down list:
   - Local
   - Network
   - Cloud
3. Enter the details for the archive as described in the following table based on the location type you selected in Step 3.

Table 3. Creating an archive

While creating the archive account on the local drive, enter the location path where you want to archive the output in the Output location text box. For example, d:\work\archive. While creating an archive on the network, enter the location path where you want to archive the output in the Output location text box, enter the user name in the User Name box to establish the logon credentials for the network share, enter a password for the network path in the Password text box. While creating an archive on the cloud, select an account from the Account from the Account dropdown box. Select a container associated with your account from the Container drop-down menu, enter the name for the folder in which the archived data is to be saved.

Option	Text Box	Description
Local	Output location	Enter the location for the output. It is used to define the location path where you want the archive to reside; for example, d:\work \archive.
Network	Output location	Enter the location for the output. It is used to define the location path where you want the archive to

Option	Text Box	Description
		reside; for example, \\servername \sharename.
	User Name	Enter a user name. It is used to establish logon credentials for the network share.
	Password	Enter a password for the network path. It is used to establish logon credentials for the network share.
Cloud	Account	Select an account from the drop-down list. NOTE: To select a cloud account, you must first add it to the Core Console. See topic 'Adding A Cloud Account' in Quest DL1300 Appliance User’s Guide.
	Container	Select a container associated with your account from the drop-down menu.
	Folder Name	Enter a name for the folder in which the archived data is to be saved. The default name is AppAssure-5-Archive-[DATE CREATED]-[TIME CREATED]

4. Click Next.
5. On the Machines page of the wizard, select which protected machine or machines contains the recovery points you want to archive.
6. Click Next.
7. On the Options page, enter the information described in the following table.

   Text Box

   Description

   Maximum Size

   Large archives of data can be divided into multiple segments. Select the maximum amount of space you want to reserve for creating the archive by doing one of the following:

   - Select Entire Target to reserve all available space in the path provided on the destination provided in Step 4. (for example, if the location is D:\work\archive, all of the available space on the D: drive is reserved).
   - Select the blank text box, use the up and down arrows to enter an amount, and then select a unit of measurement from the drop-down list to customize the maximum space you want to reserve.

   NOTE: Amazon cloud archives are automatically divided into 50 GB segments. Windows Azure cloud archives are automatically divided into 200 GB segments.

   Recycle action

Select one of the following recycle action options:

- Do not reuse: Does not overwrite or clear any existing archived data from the location. If the location is not empty, the archive write fails.
- Replace this Core: Overwrites any pre-existing archived data pertaining to this core but leaves the data for other cores intact.
- Erase Completely: Clears all archived data from the directory before writing the new archive.
- Incremental: Lets you add recovery points to an existing archive. It compares recovery points to avoid duplicating data that already exists in the archive.

Comment

Enter any additional information that is necessary to capture for the archive. The comment will be displayed if you import the archive later.

Use compatible format

Select this option to archive your data in a format that is compatible with previous versions of cores.

> NOTE: The new format offers better performance; however it is not compatible with older cores.

8. Click Next.
9. On the Date Range page, enter the Start Date and Expiration Date of the recovery points to be archived.
   - To enter a time, click on the time shown (default, 8:00 AM) to reveal the slide bars for selecting hours and minutes.
   - To enter a date, click the text box to reveal the calendar, and then click on the preferred day.
10. Click Finish.

Parent topic

Archiving to a cloud

You can archive your data to a cloud by uploading it to a variety of cloud providers directly from the Core Console. Compatible clouds include Windows Azure, Amazon, Rackspace, and any OpenStack-based provider.

To export an archive to a cloud:

- Add your cloud account to the Core Console. For more information see topic, 'Adding A Cloud Account' in Quest DL1300 Appliance User’s Guide at Quest.com/support.
- Archive your data and export it to your cloud account. For more information see topic, 'Creating An Archive' in Quest DL1300 Appliance User’s Guide at Quest.com/support.
- Retrieve archived data by importing it from the cloud location. For more information see topic, 'Importing An Archive' in Quest DL1300 Appliance User’s Guide at Quest.com/support.

Parent topic

Getting help

Finding documentation and software updates

Direct links to AppAssure and DL1300 Appliance documentation and software updates are available from the Core Console.

Documentation

To access the link for documentation:

1. On the Core Console, click the Appliance tab.
2. From the left pane, navigate Appliance > Documentation link.

Software updates

To access the link for software updates:

1. On the Core Console, click the Appliance tab.
2. From the left pane, navigate Appliance > Software Updates link.

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 Quest 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 Quest documentation pages, fill out the form, and click Submit to send your feedback.

Parent topic