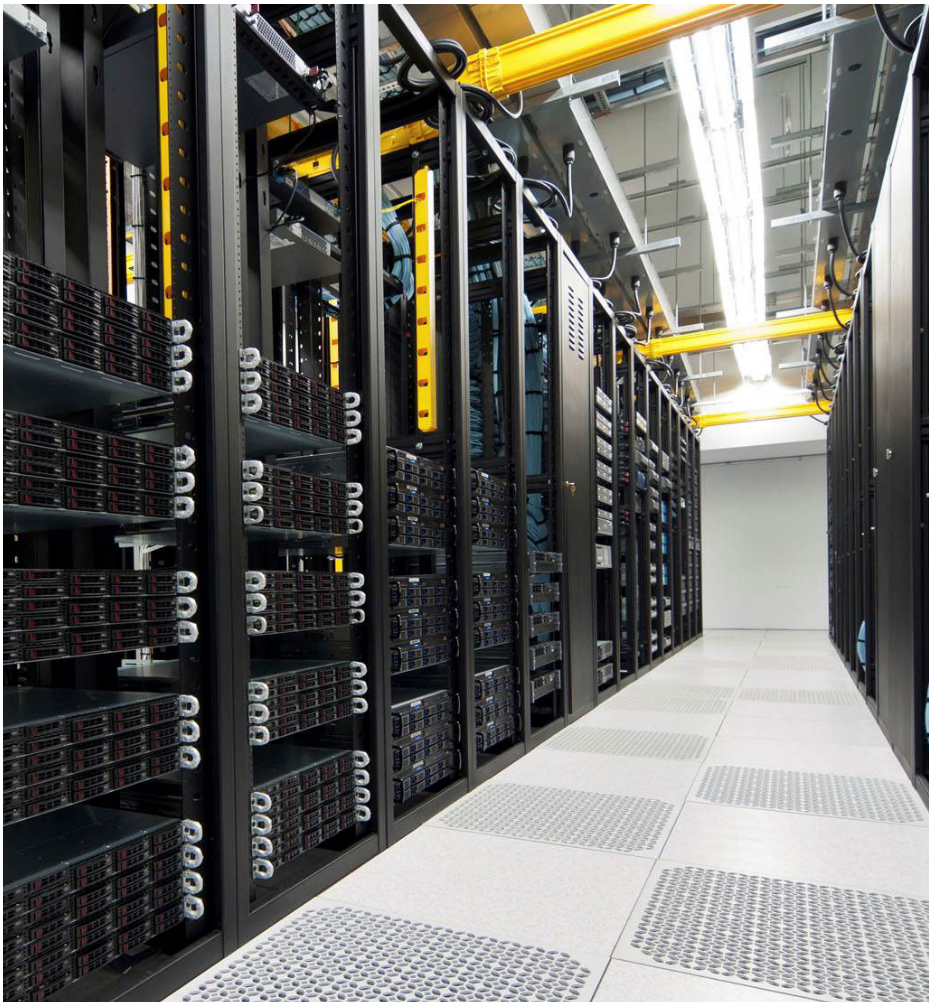
Dell AppAssure Backup, Replication, and Recovery Evaluators Guide

Business needs are putting extra pressure on your backup but your backup is broken...Traditional backups can't keep up.



Today, new problems must be solved

Data growth pegged at 800% over five years
(Gartner Group 2010 Data Center conference)

- Big Data will grow more than 60% between 2012 and 2015
  (IDC Press Release March 7, 2012)
- Cloud investments growing fast - $61 billion in 2012
  (Holger Kisker, Forrester Research blogpost 12/13/2011)
- Backup windows too large
- File/application-level backups don't meet latest RPO, RTO needs
  Snapshots alone limit recovery options
- PERHAPS THAT'S WHY many of companies plan to replace existing file/application-level backups with snapshot and replication alternatives

Dell AppAssure winner of TOP awards

This guide is written to help you analyze and evaluate the Dell AppAssure backup and recovery platform and will give you valuable insight for whenever you download and evaluate your trial copy of the software. It begins by introducing key features and functions and follows with eight function guides that point out the ease of use you can experience with Dell AppAssure software. If you have any additional questions, please visit www.appassure.com or contact AppAssure sales to schedule a demo with one of our sales engineers.

VM snaps and hardware snaps are not backup

What if... You lose an entire volume?
VMware (and Hyper-V) can snapshot the VMs

- Great for very short term protection (i.e. loading a service pack...)
- BUT it will not protect you from total loss

Hardware snaps are Copy On Write (COW) or similar

- They are tied to the original volume
- But if the original fails, the snaps are worthless

Both take up space and can cause space-related issues down the road

Dell AppAssure provides:

- Up to 288 snaps per day (as frequent as every 5 minutes!)
- Complete data integrity
- Replication for offsite failover

How do you plan for the worst?

- Replication is now critical to survival
- Backing up and moving tape is no longer sufficient
- Automation is key to always being ready
- Backup WITH replication is the new standard
- It is no longer only for the largest companies that can afford disk based replication

Dell AppAssure provides:

- Integrated backup AND replication in one product
- An affordable solution
- Local and offsite Virtual Standby for both physical and virtual systems for failover

How do you know you can recover?

- "Verify" option in most products inadequate and has no application understanding
- Random restore tests cost a lot of money in man hours
- Automation is the key to success
- More recent providers only look at the system, not the app.

Dell AppAssure provides:

- Recovery Assure™ automation of testing critical data
- Volume Integrity testing
- SQL and Exchange Database testing for mount / attach-ability
- In-depth checksum testing of Exchange Databases

Consider this

How often to you plan on taking Snapshots of your protected servers?

- Backing up every 15 minutes consumes more bandwidth than backing up every four hours.

What is your current daily data change rate on the protected servers?

- AppAssure tracks changes at the block level so it's extremely efficient. By only backing up these changes we ensure the minimum performance impact on the agent side and maximize storage savings. I.e. when a block in a database changes we only capture that block change. Traditional solutions will back up the entire database.
- Servers with a greater change rate will create larger snapshots and could require longer transfer times (AppAssure moves data in excess of 8GB/min).

Are you creating virtual hot standby clones?

- If you select this option, any protected server you can be automatically created and continuously updated as a Virtual machine. If your protected server should go down, simply fire up your Virtual Hot standby. It's important to note however that the creation of this Virtual machine, although powered off, will be continuously updated with the block level changes from the source server. This type of updating requires disk resources.

What kind of agents are you protecting?

- Exchange and SQL server agents usually see greater daily change rates, and as part of AppAssure's Assured recovery procedures, run a series of checks on the Data, ESEUTIL checks in the case of Exchange, and SQL Table Mountability checks. So the end result is that SQL and Exchange Agents consume more AppAssure Core CPU, and Disk I/O.

Are you Replicating your data offsite or into the cloud?

- Replicating data off site also consumes AppAssure Core CPU and storage bandwidth. It is also important to remember when replicating data to any offsite location, that you need to ensure your firewall and TCP-IP port settings are properly configured and you have proper access to whatever remote site you are using. As far as WAN bandwith remember that only compressed and de-duplicated data is sent to ensure the most efficient use of your WAN connection.

Contents

Evaluation Overview

Dell AppAssure evaluation considerations

Evaluation requirements: what functions are right for your business?

- Is reducing Recovery Point Objectives (RPO) or Recovery Time Objective (RTO) critical to your Service Level Agreements (SLA) or business needs?
- Is migrating from physical to virtual (P2V), virtual to virtual (V2V), or to the cloud (X2C) an end goal?
- Is protecting Microsoft applications such as Exchange, SQL, and/or SharePoint critical to your operations?
- Do you currently support multiple physical, virtual and/or cloud platforms and/or need to migrate between them?
- Is ease of use and a flexible web interface important?
- Do you want to be certain your backups can be recovered in the event?
- Would near zero performance impact on protected machines and recovery points as often as every five minutes secure your business goals?

What features are important to build the ideal data protection and disaster recovery solution?

- Single-pass Microsoft Exchange, SQL, SharePoint application backup with full system or granular recovery as well as application assurance
- Site-to-Site replication
- Automated replication of physical/virtual machines to ESX(i) or Hyper-V
- Ability to recover large non-system volumes in seconds using Dell AppAssure Live Recovery™
- Recover an entire system, single file, folder, or object anywhere
- Inline deduplication and compression at line speed to save on bandwidth and storage
- Protect physical, virtual and cloud machines all in one place
- Fast always incremental snapshots Dell AppAssure changed block tracking on physical, virtual, or cloud machines

Understanding Dell AppAssure

What is Dell AppAssure?

- Dell AppAssure is more than just a backup application, it's a recovery application
- Dell AppAssure tracks changed blocks of data on a protected system and saves that data with continual snapshots, for up to 288 recovery points per day
- Automated validation of Microsoft applications guarantees you can recover them every time anywhere
- Centralized console enables you to protect and centrally manage entire environment all from a single pane of glass

Protecting your network with Dell AppAssure is simple and easy.
Dell AppAssure requires just a few simple components to be installed in order to protect your environment:

- Dell AppAssure Core Server
- Storage for Dell AppAssure backups
- Dell AppAssure Agent(s)

All of the components are easily installed and configured.

Lets take a deeper look at each component.

Dell AppAssure Core Server

Functionality:

- Backup & Recovery:
- Centralized Management
- Centralized Storage Management
- Retention & Archive Policies
- Multi-Core, Multi Repository Scaling
- Compression and Deduplication
- Onsite/Offsite Replication
- Virtual Standby

Considerations:

- Runs on a dedicated 64-bit Windows Server
- Utilizes various storage types such as NAS, SAN or DAS
- Needs a multi core CPU

Off the shelf storage components

Considerations:

- Dell AppAssure supports common storage such as Direct Attached Storage (DAS), Network Attached Storage (NAS) and Storage Area Networks (SAN)
- Needs to be presented to the Dell AppAssure Core Server as a CIFS share or local storage (including ISCSI)
- Should have a business-class disk subsystem
- Storage system should not have native compression or deduplication
- Capacity should be large enough to match your backup retention goals

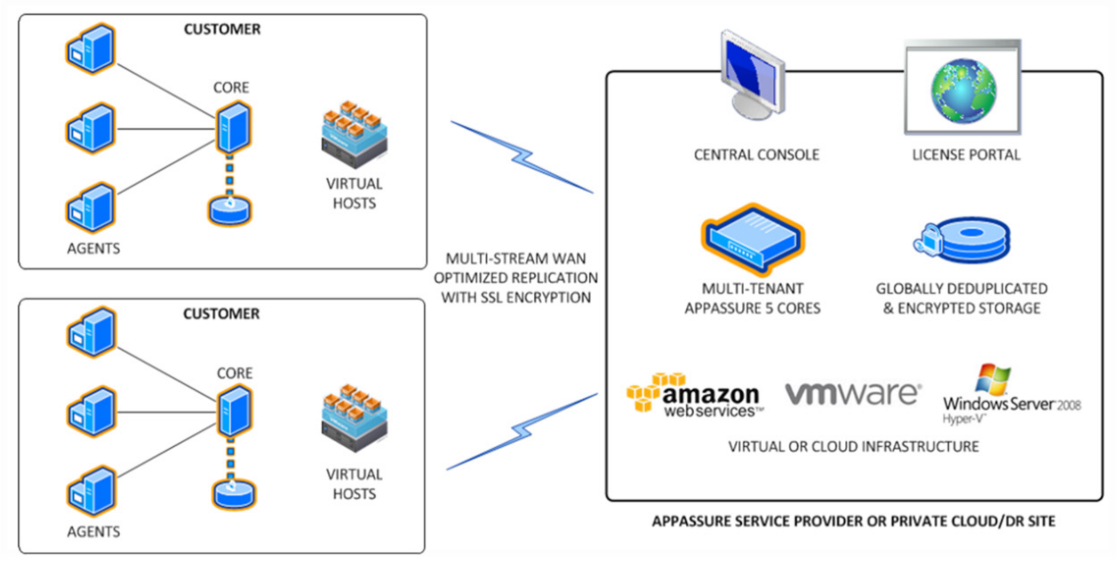
Dell AppAssure Smart Agent

Functionality:

- Change Block Tracking
- Near-Zero % CPU Utilization
- Creates application aware backups
- Data Volume (data & logs) grouping
- Microsoft SQL and Exchange log truncation
- Exchange mount and integrity checks
- SQL attachability checks
- Volume Integrity Check

OS Support:

- Windows Server 2003\2008\2008 R2\2008R2 SP1 core\2012
- Windows XP\Vista\7\8
- Red Hat Enterprise Linux 6.3
- CentOS 6.3
- SuSE Linux Enterprise Server 11 SP2


CUSTOMER
CORE
VIRTUAL HOSTS
AGENTS
CUSTOMER
CORE
VIRTUAL HOSTS
AGENTS
MULTI-STREAM WAN OPTIMIZED REPLICATION WITH SSL ENCRYPTION
CENTRAL CONSOLE
LICENSE PORTAL
MULTI-TENANT APPASSURE 5 CORES
GLOBALLY DEDUPLICATED & ENCRYPTED STORAGE
amazon webservices
vmware
Windows Server 2008 Hyper-V
VIRTUAL OR CLOUD INFRASTRUCTURE
APPASSURE SERVICE PROVIDER OR PRIVATE CLOUD/DR SITE

Dell AppAssure Backup, Replication, and Recovery Evaluator's Guide: How to Install and Configure the Core

Why read this guide

The Dell AppAssure Core Server is the heart of the backup and recovery platform. Purpose-built for centralized management, the Core holds the system's critical functionality, including retention and archiving policies, compression, deduplication and onsite and offsite replication functions.

The Core runs on a dedicated 64-bit Windows Server and utilizes a variety of storage types, such as NAS, SAN or DAS.

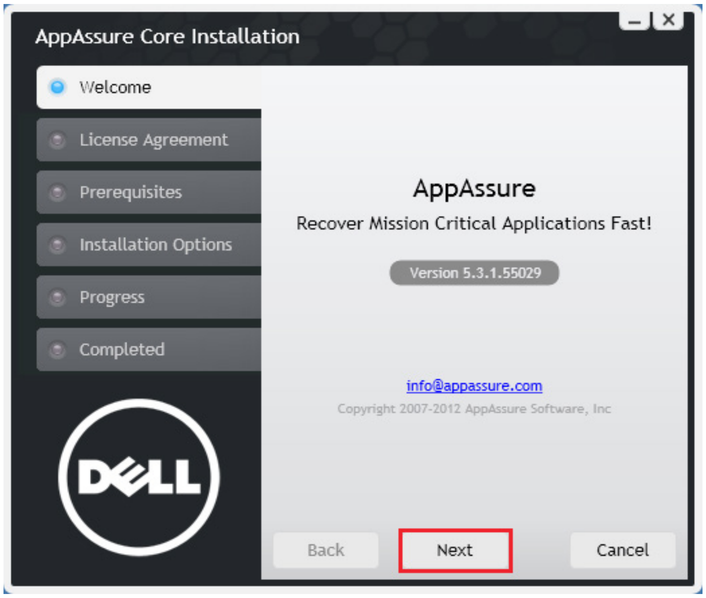
The Core is easily installed and configured in various environments.

How to install the Dell AppAssure Core

1. Installing the Dell AppAssure Core
2. Configuring the Dell AppAssure Core
3. Dell AppAssure configuration options

1. Dell AppAssure Core installation

Run the installer and follow the installation wizard to begin your evaluation. After accepting the Licensing Agreement, check and/or install any prerequisites.



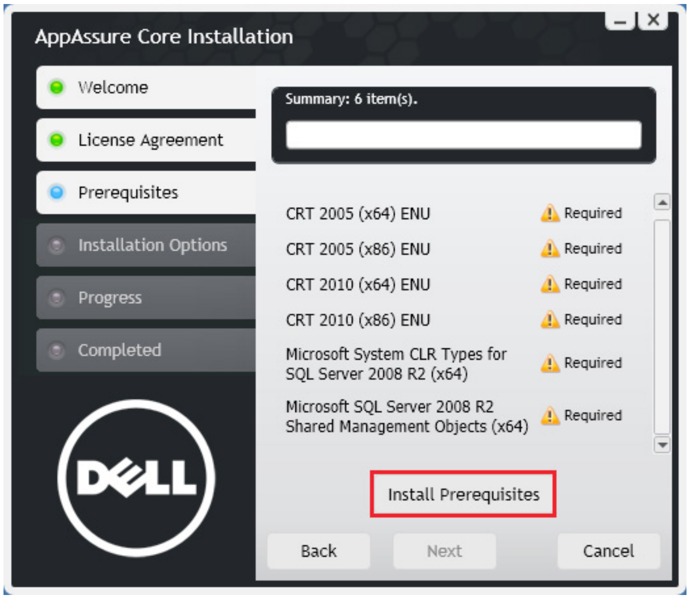
AppAssure

Recover Mission Critical Applications Fast!

Version 5.3.1.55029

info@appassure.com

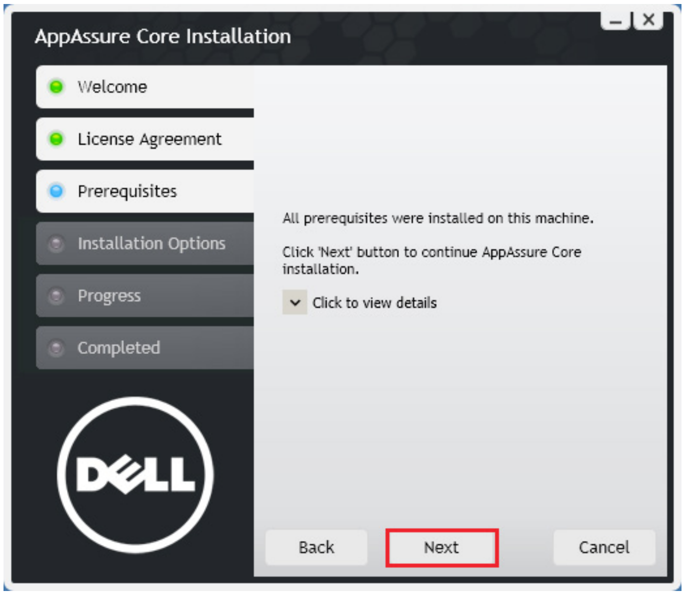
Copyright 2007-2012 AppAssure Software, Inc



Summary: 6 item(s).

CRT 2005 (x64) ENU	Required
CRT 2005 (x86) ENU	Required
CRT 2010 (x64) ENU	Required
CRT 2010 (x86) ENU	Required
Microsoft System CLR Types for SQL Server 2008 R2 (x64)	Required
Microsoft SQL Server 2008 R2 Shared Management Objects (x64)	Required

Once prerequisites are installed, click “Next.”

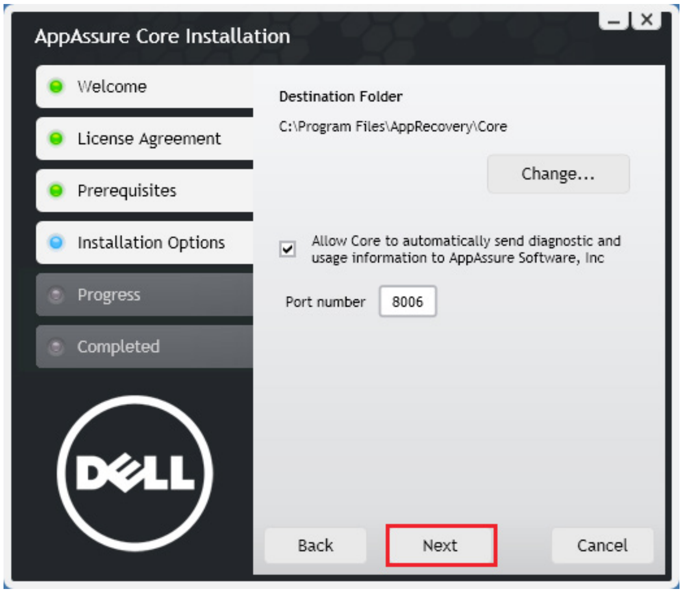


AppAssure Core Installation

All prerequisites were installed on this machine.

Click 'Next' button to continue AppAssure Core installation.

Choose the destination folder for installation, choose the port and click “Next.”



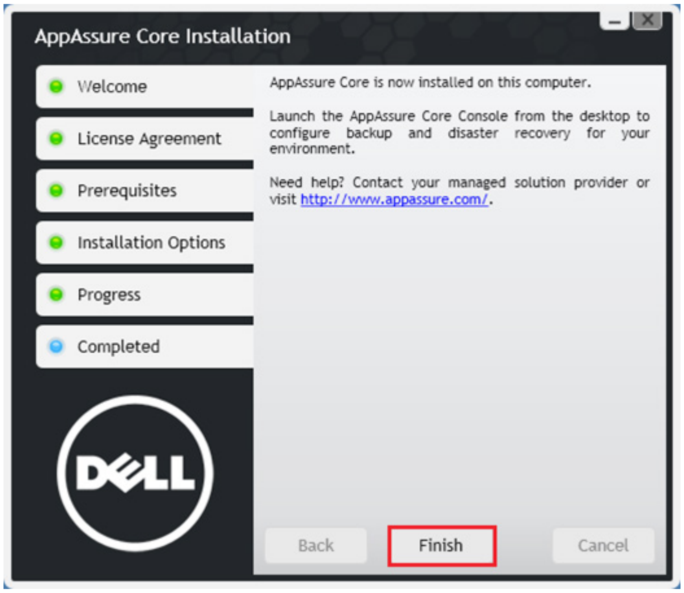
AppAssure Core Installation

Destination Folder
C:\Program Files\AppRecovery\Core

☑ Allow Core to automatically send diagnostic and usage information to AppAssure Software, Inc

Port number 8006

Once installed, click “Finish” to begin evaluation.



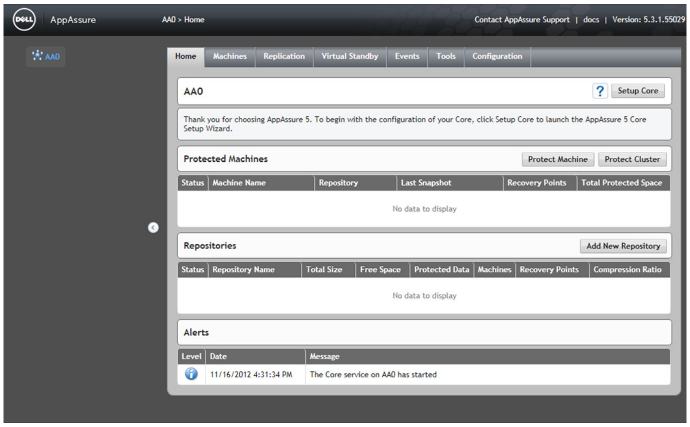
AppAssure Core Installation

AppAssure Core is now installed on this computer.

Launch the AppAssure Core Console from the desktop to configure backup and disaster recovery for your environment.

Need help? Contact your managed solution provider or visit http://www.appassure.com/.

Launching Dell AppAssure will bring you to the Core Console.



AA0

Thank you for choosing AppAssure 5. To begin with the configuration of your Core, click Setup Core to launch the AppAssure 5 Core Setup Wizard.

Protected Machines

Status	Machine Name	Repository	Last Snapshot	Recovery Points	Total Protected Space
No data to display					

Repositories

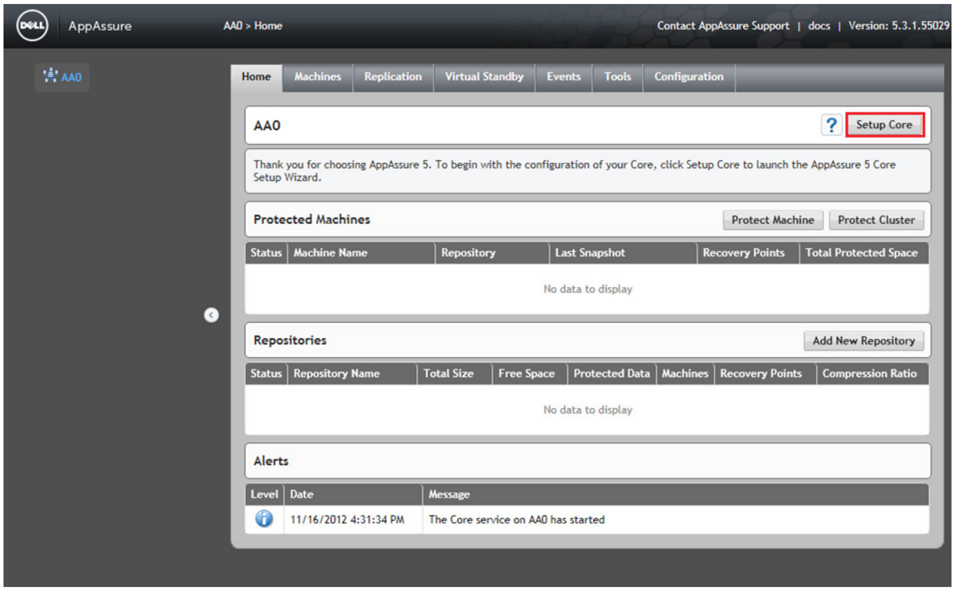
Status	Repository Name	Total Size	Free Space	Protected Data	Machines	Recovery Points	Compression Ratio
No data to display							

Alerts

Level	Date	Message
ⓘ	11/16/2012 4:31:34 PM	The Core service on AA0 has started

2. Configuring a New Dell AppAssure Core

Launch the Dell AppAssure Core Console from the Desktop Icon or the Start Menu and press “Setup Core” in the upper right of the screen to begin the configuration of the new Core.



AA0

Thank you for choosing AppAssure 5. To begin with the configuration of your Core, click Setup Core to launch the AppAssure 5 Core Setup Wizard.

Protected Machines

Status	Machine Name	Repository	Last Snapshot	Recovery Points	Total Protected Space

No data to display

Repositories

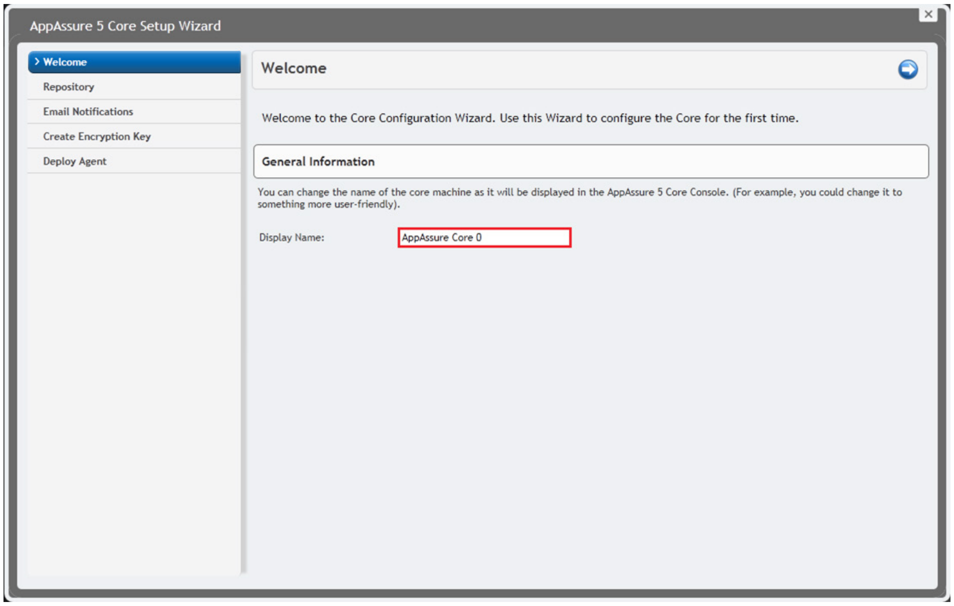
Status	Repository Name	Total Size	Free Space	Protected Data	Machines	Recovery Points	Compression Ratio

No data to display

Alerts

Level	Date	Message
ⓘ	11/16/2012 4:31:34 PM	The Core service on AA0 has started

To begin configuration, provide a Display Name for the new core you are configuring, then press the “Arrow” to proceed.



Welcome

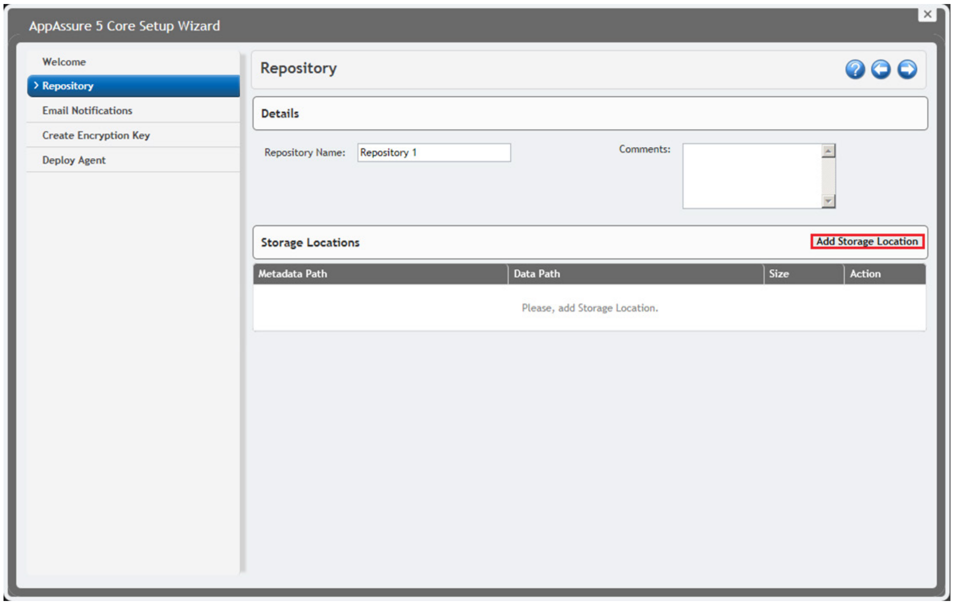
Welcome to the Core Configuration Wizard. Use this Wizard to configure the Core for the first time.

General Information

You can change the name of the core machine as it will be displayed in the AppAssure 5 Core Console. (For example, you could change it to something more user-friendly).

Display Name: AppAssure Core 0

First, configure storage for your backups; this a “Repository.” Click “Add Storage Location” to begin.

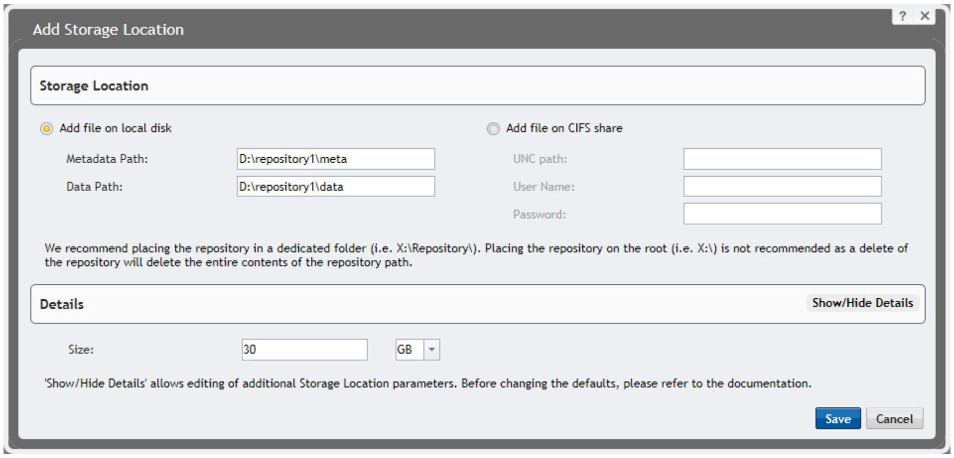


Repository Name: Repository 1

Comments:

Please, add Storage Location.

Provide the path for the new Repository in the “Metadata Path” and the “Data Path” or CIFS share. Select a size for the repository, then press “Save.”



● Add file on local disk

Metadata Path: D:\repository1\meta

Data Path: D:\repository1\data

○ Add file on CIFS share

UNC path:

User Name:

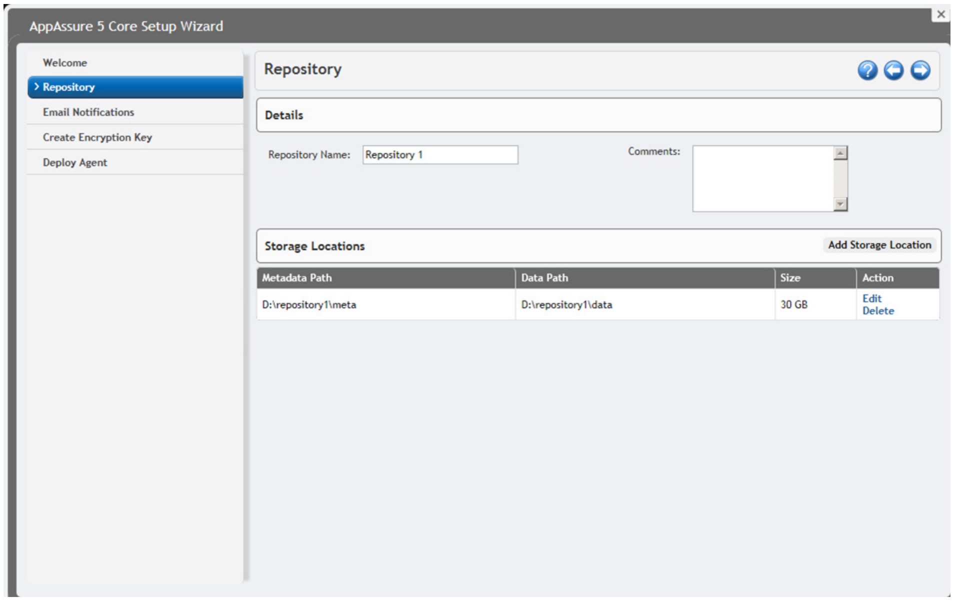
Password:

We recommend placing the repository in a dedicated folder (i.e. X:\Repository\). Placing the repository on the root (i.e. X:\) is not recommended as a delete of the repository will delete the entire contents of the repository path.

Size: 30 GB

'Show/Hide Details' allows editing of additional Storage Location parameters. Before changing the defaults, please refer to the documentation.

Once the Repository is created, you can edit, delete, or add more Storage Locations. Once complete click the "Right arrow."



Repository

Details

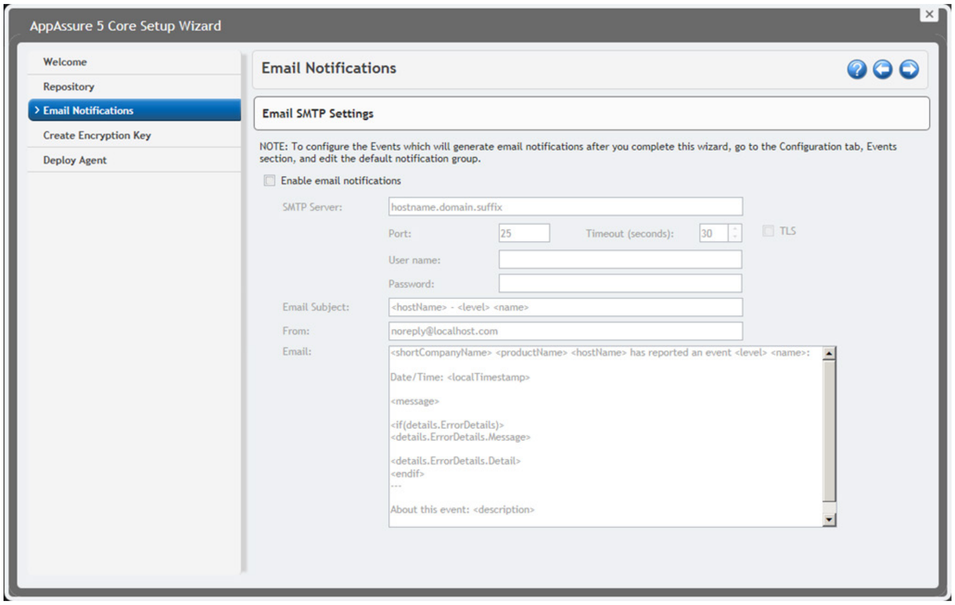
Repository Name: Repository 1

Comments:

Storage Locations

Metadata Path	Data Path	Size	Action
D:\repository1\meta	D:\repository1\data	30 GB	Edit Delete

Configure email notifications here by Enabling email notifications and filling in your SMTP server details. While AppAssure carries out backups automatically, if something is not right, like a backup failure due to data corruption, email notifications will let you know immediately so you can intervene to address it. Once completed press the "Next arrow."



Email Notifications

Email SMTP Settings

NOTE: To configure the Events which will generate email notifications after you complete this wizard, go to the Configuration tab, Events section, and edit the default notification group.

☐ Enable email notifications

SMTP Server: hostname.domain.suffix

Port: 25 Timeout (seconds): 30 ☐ TLS

User name:

Password:

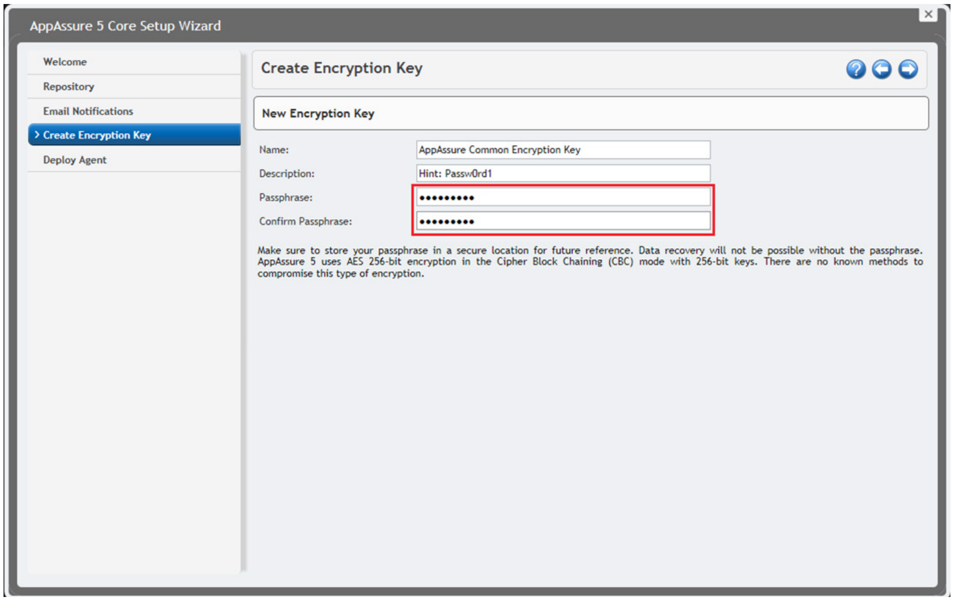
Email Subject: <hostName> - <level> <name>

From: noreply@localhost.com

Email:

```
<shortCompanyName> <productName> <hostName> has reported an event <level> <name>:

Date/Time: <localTimestamp>

<message>

<if(details.ErrorDetails)>
<details.ErrorDetails.Message>

<details.ErrorDetails.Detail>
<endif>
---

About this event: <description>
```

If encryption is required – for example when sending data offsite or to the cloud – use this screen to provide the name of the encryption key, a short description and a passphrase. Make a note to secure this passphrase so it can not be lost, as this is the only key for accessing your data. Once completed click the “Next arrow.”



Create Encryption Key

New Encryption Key

Name: AppAssure Common Encryption Key

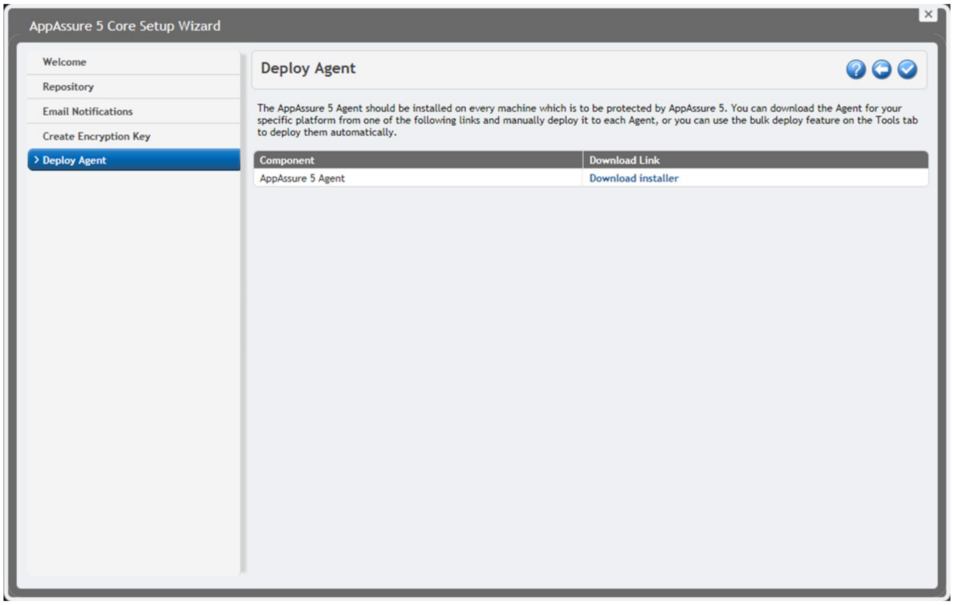
Description: Hint: Passw0rd1

Passphrase: •••••••••

Confirm Passphrase: •••••••••

Make sure to store your passphrase in a secure location for future reference. Data recovery will not be possible without the passphrase. AppAssure 5 uses AES 256-bit encryption in the Cipher Block Chaining (CBC) mode with 256-bit keys. There are no known methods to compromise this type of encryption.

You can use the Core Configuration wizard to Deploy Agents to machines you wish to protect. This is covered in detail in the Agent Configuration Guide. Press the checkmark button to complete the configuration.



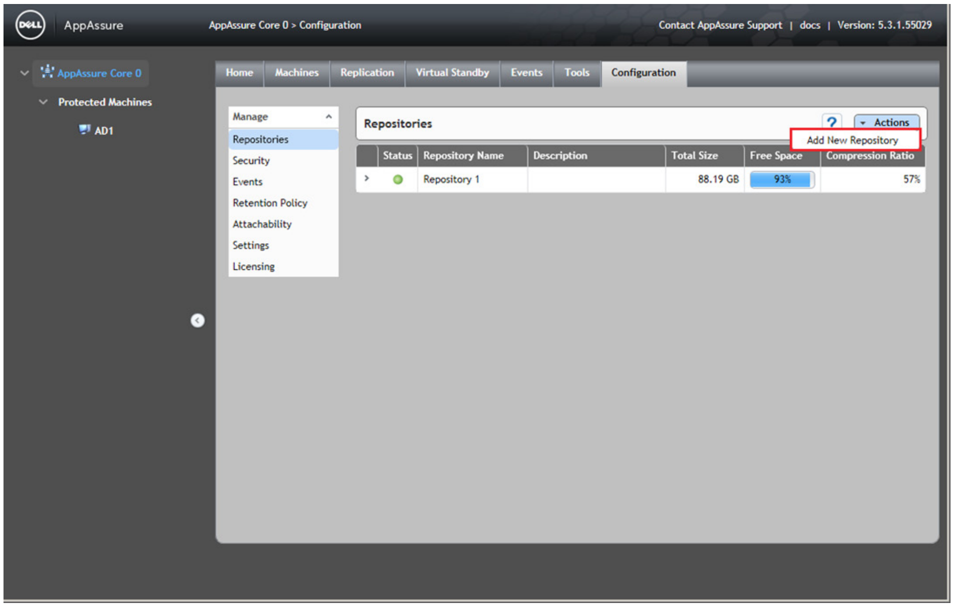
Deploy Agent

The AppAssure 5 Agent should be installed on every machine which is to be protected by AppAssure 5. You can download the Agent for your specific platform from one of the following links and manually deploy it to each Agent, or you can use the bulk deploy feature on the Tools tab to deploy them automatically.

Component	Download Link
AppAssure 5 Agent	Download installer

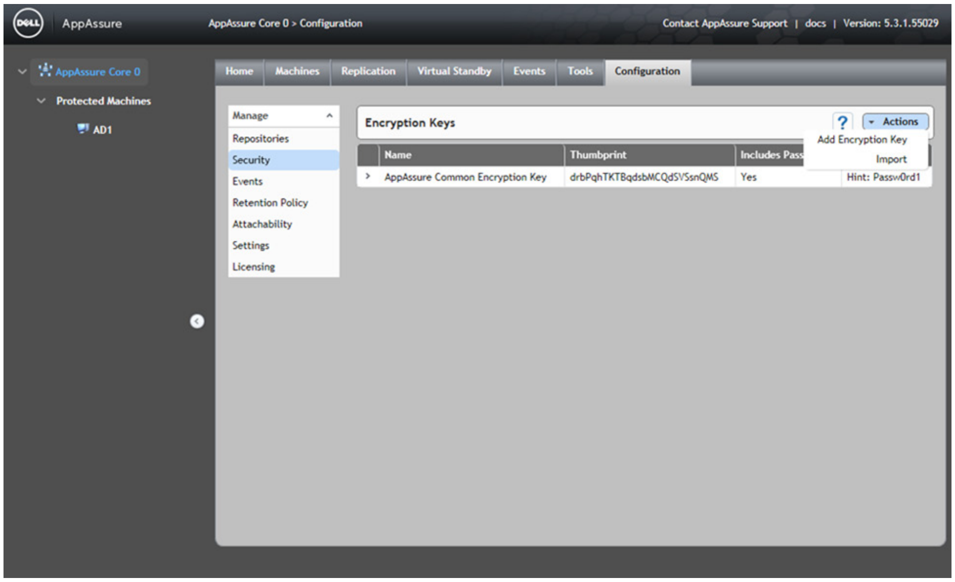
3. Dell AppAssure Core Configuration tab (options)

On the Configuration tab of the Core there are many optional items that can be edited. In the Repository section you can add or edit repositories.



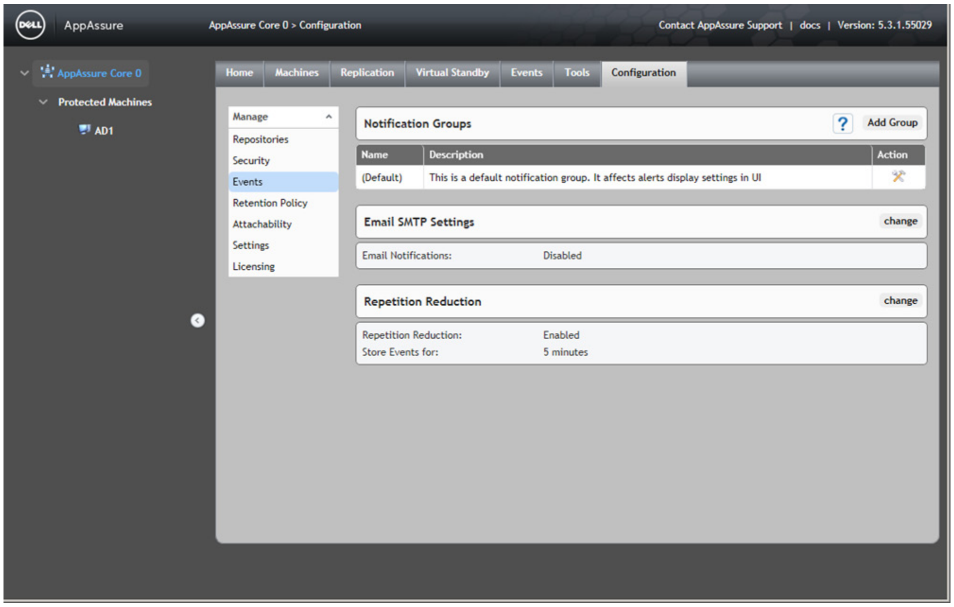
	Status	Repository Name	Description	Total Size	Free Space	Compression Ratio
>	●	Repository 1		88.19 GB	93%	57%

Use the Security Menu in the Configuration tab to add or import new encryption keys.



	Name	Thumbprint	Includes Pass	
>	AppAssure Common Encryption Key	drbPqhTKTBqdsbMCQdSVSsnQMS	Yes	Hint: Passw0rd1

The Events section is used to configure notification groups, email server settings, and event notification frequency.



Notification Groups

Name	Description	Action
(Default)	This is a default notification group. It affects alerts display settings in UI	

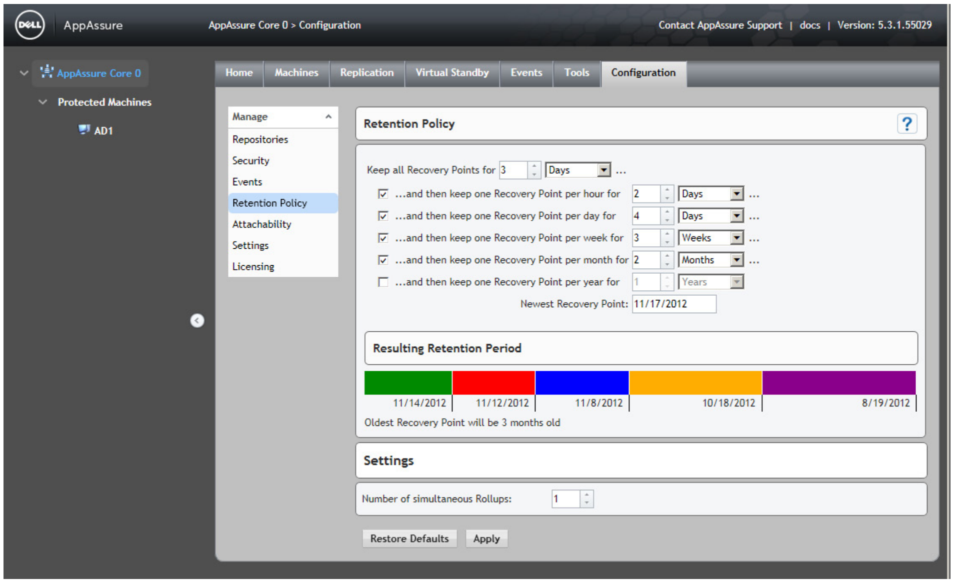
Email SMTP Settings

Email Notifications: Disabled

Repetition Reduction

Repetition Reduction: Enabled
Store Events for: 5 minutes

Use the Retention Policy section to specify how long Recovery Points will be retained. The default configuration allows for recovery period spanning 3 months.



Retention Policy

Keep all Recovery Points for 3 Days ...
☑ ...and then keep one Recovery Point per hour for 2 Days ...
☑ ...and then keep one Recovery Point per day for 4 Days ...
☑ ...and then keep one Recovery Point per week for 3 Weeks ...
☑ ...and then keep one Recovery Point per month for 2 Months ...
☐ ...and then keep one Recovery Point per year for 1 Years
Newest Recovery Point: 11/17/2012

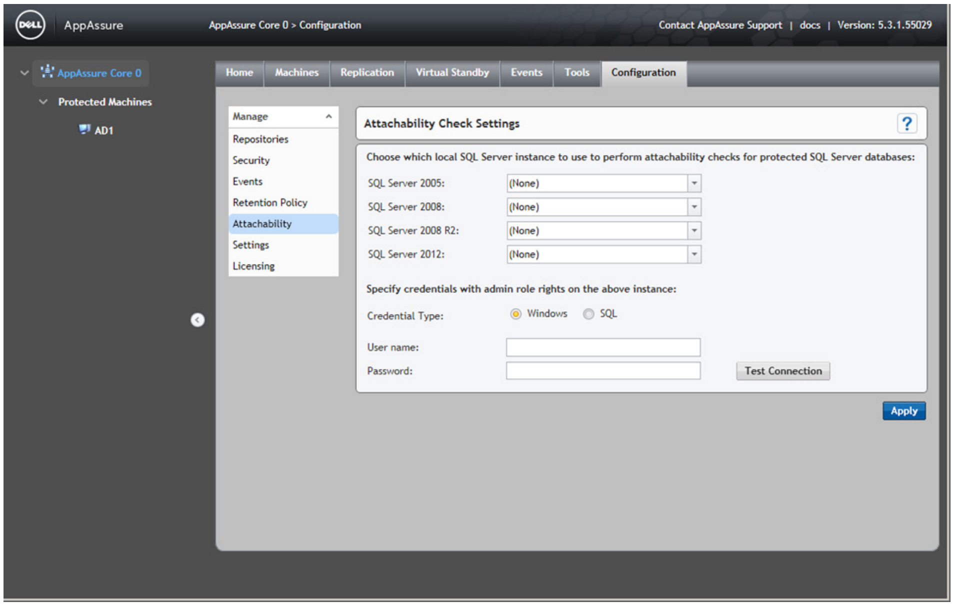
Resulting Retention Period

Oldest Recovery Point will be 3 months old

Settings

Number of simultaneous Rollups: 1

Use the Attachability section to configure the SQL Server instance that will be used to perform tests to ensure your SQL Server backup is recoverable. First, choose the SQL Server you want to use, and provide the credentials to access it.



Attachability Check Settings

Choose which local SQL Server instance to use to perform attachability checks for protected SQL Server databases:

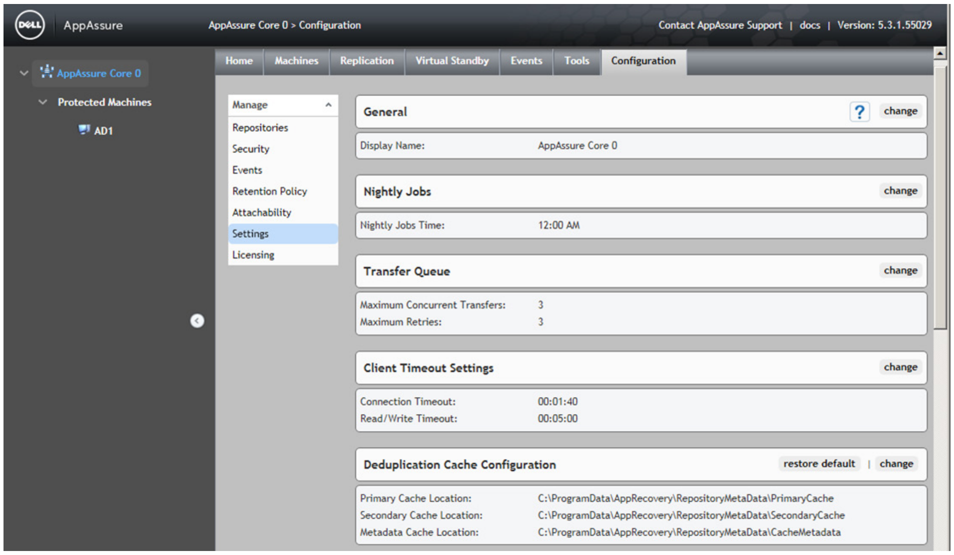
SQL Server 2005: (None)
SQL Server 2008: (None)
SQL Server 2008 R2: (None)
SQL Server 2012: (None)

Specify credentials with admin role rights on the above instance:

Credential Type: ● Windows ○ SQL

User name:
Password:

The Settings section is where you can change default settings for how the Core operates. Generally the default values are a best practice. (This is the first half of the screen).



General

Display Name: AppAssure Core 0

Nightly Jobs

Nightly Jobs Time: 12:00 AM

Transfer Queue

Maximum Concurrent Transfers: 3
Maximum Retries: 3

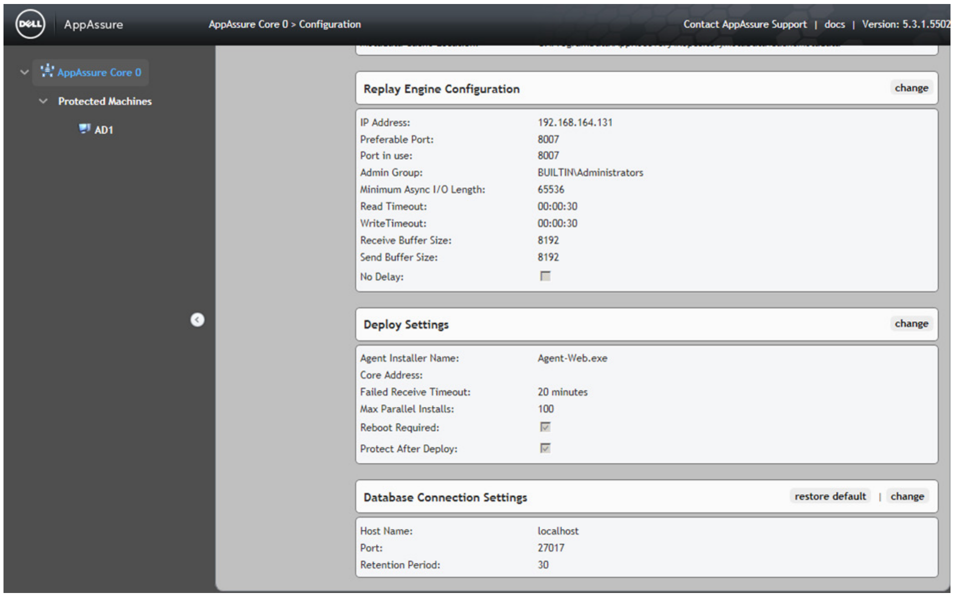
Client Timeout Settings

Connection Timeout: 00:01:40
Read/Write Timeout: 00:05:00

Deduplication Cache Configuration

Primary Cache Location: C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache
Secondary Cache Location: C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
Metadata Cache Location: C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

Settings section continued.



AppAssure
AppAssure Core 0 > Configuration
Contact AppAssure Support | docs | Version: 5.3.1.5502
AppAssure Core 0
Protected Machines
AD1

Replay Engine Configuration change

IP Address:	192.168.164.131
Preferable Port:	8007
Port in use:	8007
Admin Group:	BUILTIN\Administrators
Minimum Async I/O Length:	65536
Read Timeout:	00:00:30
WriteTimeout:	00:00:30
Receive Buffer Size:	8192
Send Buffer Size:	8192
No Delay:	□

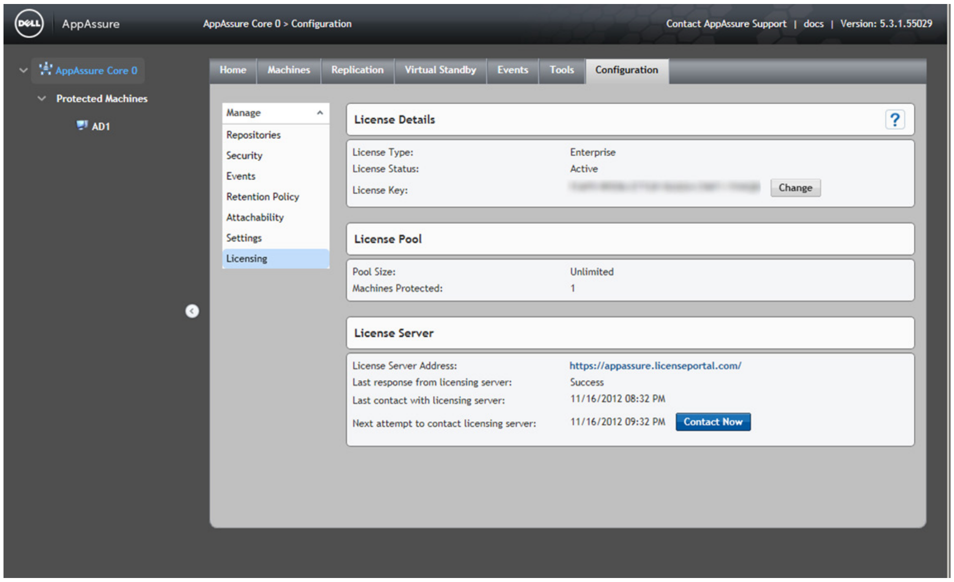
Deploy Settings change

Agent Installer Name:	Agent-Web.exe
Core Address:	
Failed Receive Timeout:	20 minutes
Max Parallel Installs:	100
Reboot Required:	☑
Protect After Deploy:	☑

Database Connection Settings restore default | change

Host Name:	localhost
Port:	27017
Retention Period:	30

The last section is Licensing. Here you can review your license type, status, the key itself, the amount of licenses available to you during your trial, and the License Server connection settings.



License Details ?

License Type:	Enterprise
License Status:	Active
License Key:	[redacted] Change

License Pool

Pool Size:	Unlimited
Machines Protected:	1

License Server

License Server Address:	https://appassure.licenseportal.com/
Last response from licensing server:	Success
Last contact with licensing server:	11/16/2012 08:32 PM
Next attempt to contact licensing server:	11/16/2012 09:32 PM Contact Now

Dell AppAssure Backup, Replication, and Recovery Evaluator's Guide:
How to Deploy Dell AppAssure Agents

Why read this guide

Dell AppAssure Smart Agents are ultra-lightweight agents that have the intelligence to allow inherently higher-levels of protection than agentless backup schemes, including higher-speed backups, super-efficient changed-block tracking, and needing only one backup pass for both granular and system-level recoveries. There is a small time commitment you have to make for all this performance: a one-time install on each protected machine.

How to Deploy Dell AppAssure agents

1. Deployment Notes
2. Active Directory deployment
3. vCenter/ESX(i) deployment
4. Manual deployment
5. New deployment
6. Deploying a Local Agent
7. Deploying a Linux Agent

The Dell AppAssure Agent

Dell AppAssure agents protect and manage the backup and recovery of individual machines in a variety of environments. Each agent allows for block tracking, data volume grouping and the creation application aware backups, with near-zero percentage CPU utilization.

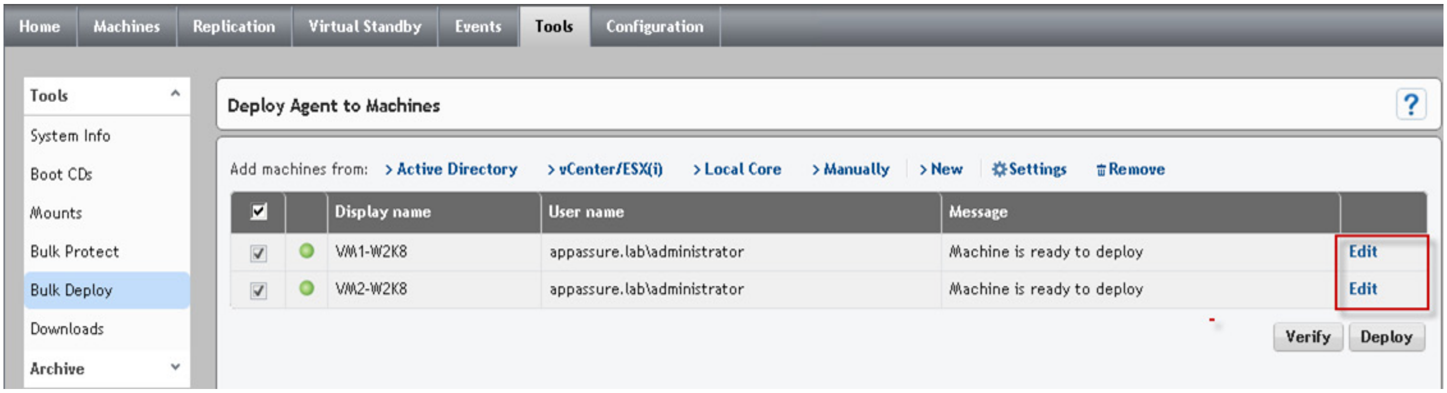
Dell AppAssure agents support the following operating systems:

- Windows Server 2003\2008\2008 R2\2008 R2 SP1\2012 core
- Windows XP\Vista\7\8
- Red Hat Enterprise Linux 6.3
- CentOS 6.3
- SuSE Linux Enterprise Server 11 SP2

Deployment notes

When deploying an AppAssure Smart Agent to a machine you wish to protect, that machine will automatically and immediately reboot, and from that point on will be automatically protected unless otherwise selected

But if you don't want the machine to reboot immediately, select the "Edit" button next to the machine to be deployed



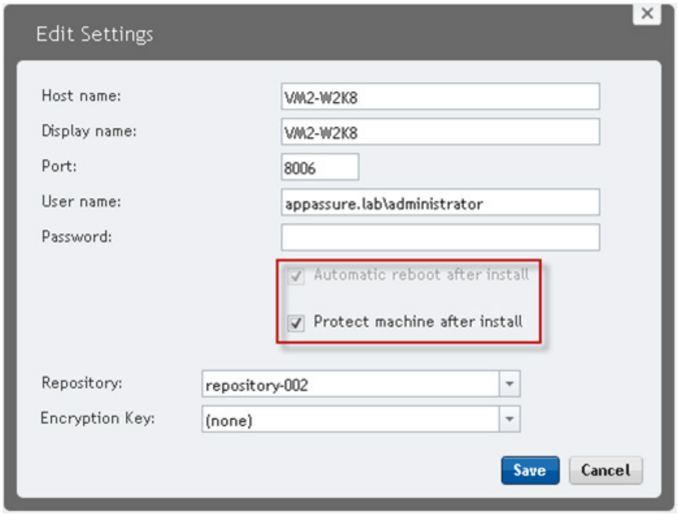
Deploy Agent to Machines

Add machines from:

☑		Display name	User name	Message	
☑	●	VM1-W2K8	appassure.lab\administrator	Machine is ready to deploy	Edit
☑	●	VM2-W2K8	appassure.lab\administrator	Machine is ready to deploy	Edit

On the pop-up screen deselect "Protect machine after install" and "Automatic reboot after install"

Just remember to reset the reboot command at some point in the near future so the machine can begin to be protected.



Edit Settings

Host name: VM2-W2K8

Display name: VM2-W2K8

Port: 8006

User name: appassure.lab\administrator

Password:

☑ Automatic reboot after install

☑ Protect machine after install

Repository: repository-002

Encryption Key: (none)

Assuming "Protect machine after install" has been selected the agent will begin creating its base image after its initial reboot.

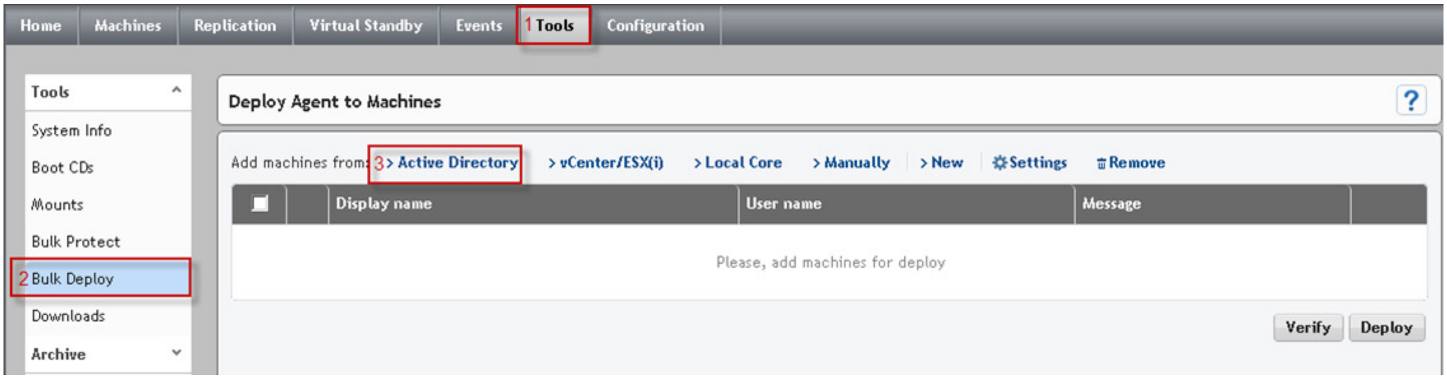
Dell AppAssure is application aware and will automatically protect all volumes on the system while accounting for dependencies.

By default, snapshots are created every 60 minutes, but can be set as frequently as every five minutes for high-transaction environments or at longer intervals for applications where data changes infrequently.

1. Active Directory deployment

To deploy Dell AppAssure via Active Directory:

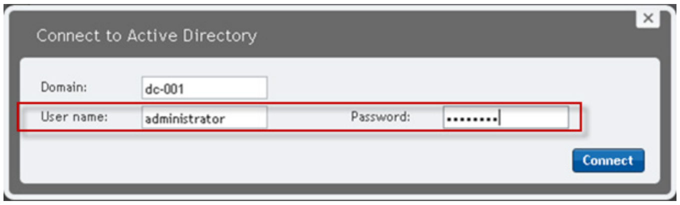
- Connect to the Dell AppAssure core server
- Go to Tools-> Bulk Deploy-> Active Directory



□	Display name	User name	Message

Please, add machines for deploy

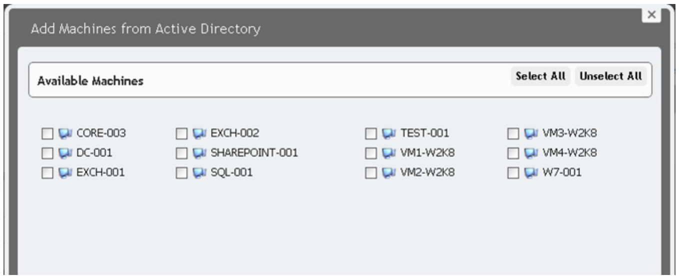
- Enter your domain controller's IP or host name
- Enter domain administrator's credentials


Connect to Active Directory

Domain: dc-001

User name: administrator Password: ••••••••

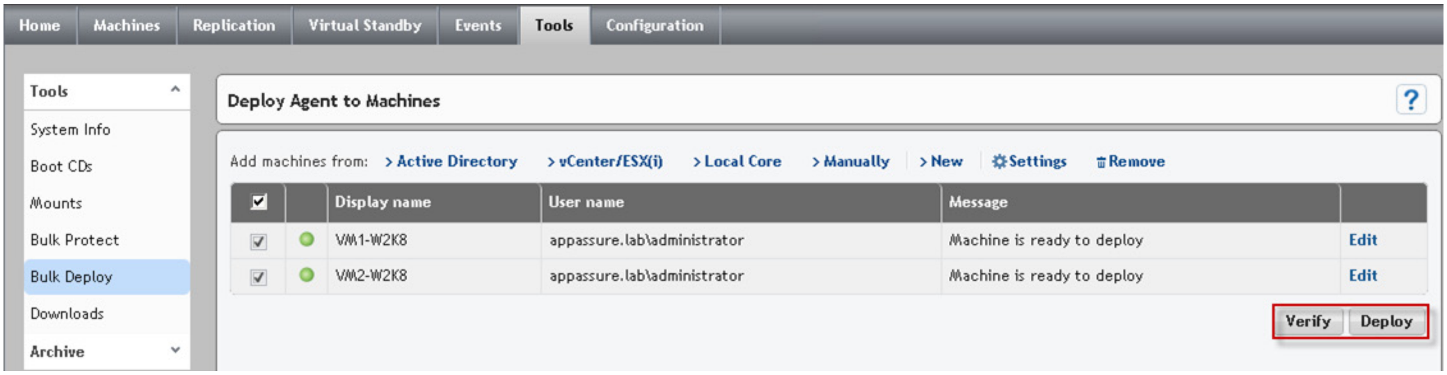
- Select the machines that you wish to deploy to
- Click "Add"


Add Machines from Active Directory

Available Machines

□ CORE-003	□ EXCH-002	□ TEST-001	□ VM3-W2K8
□ DC-001	□ SHAREPOINT-001	□ VM1-W2K8	□ VM4-W2K8
□ EXCH-001	□ SQL-001	□ VM2-W2K8	□ W7-001

- Click “Verify” to ensure the machines are online
- Once the machines have been verified click “Deploy” to begin the deployment

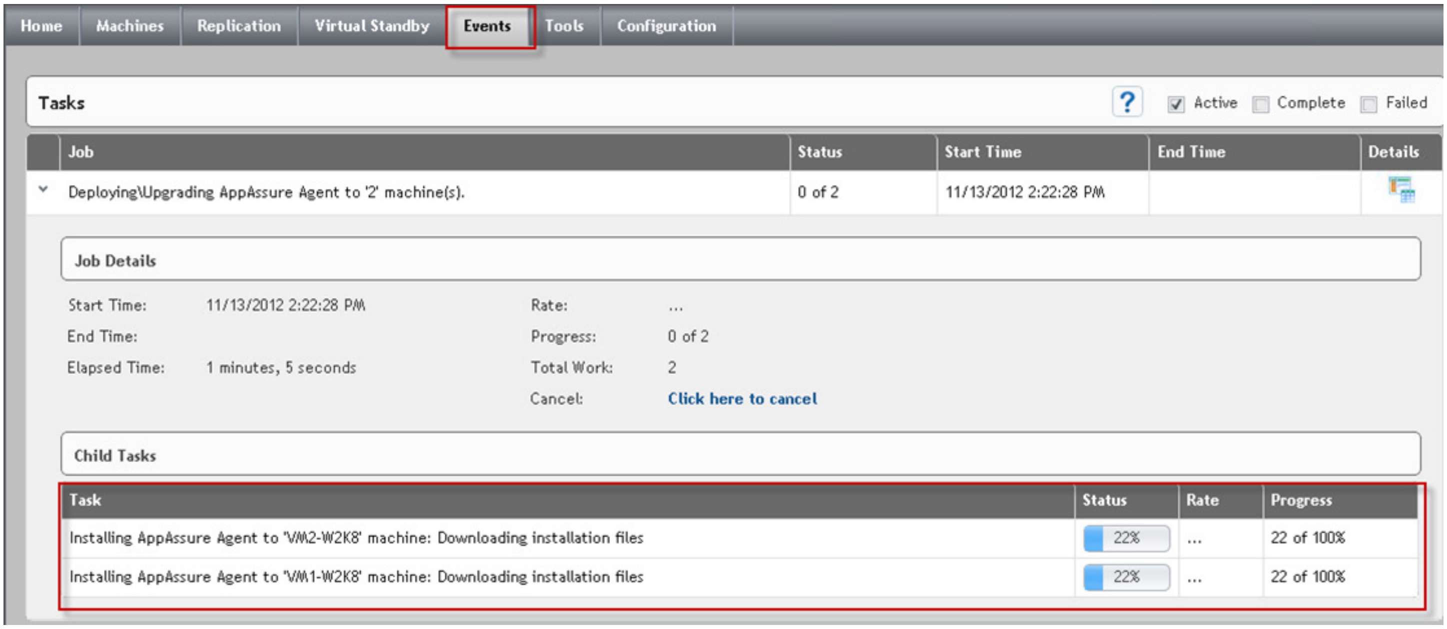


Deploy Agent to Machines

Add machines from:

☑		Display name	User name	Message	
☑	●	VM1-W2K8	appassure.lab\administrator	Machine is ready to deploy	Edit
☑	●	VM2-W2K8	appassure.lab\administrator	Machine is ready to deploy	Edit

- Click the “Events” tab to monitor the progress of the deployment



Tasks

	Job	Status	Start Time	End Time	Details
˅	Deploying\Upgrading AppAssure Agent to '2' machine(s).	0 of 2	11/13/2012 2:22:28 PM		

Job Details

Start Time:	11/13/2012 2:22:28 PM	Rate:	...
End Time:		Progress:	0 of 2
Elapsed Time:	1 minutes, 5 seconds	Total Work:	2
		Cancel:	Click here to cancel

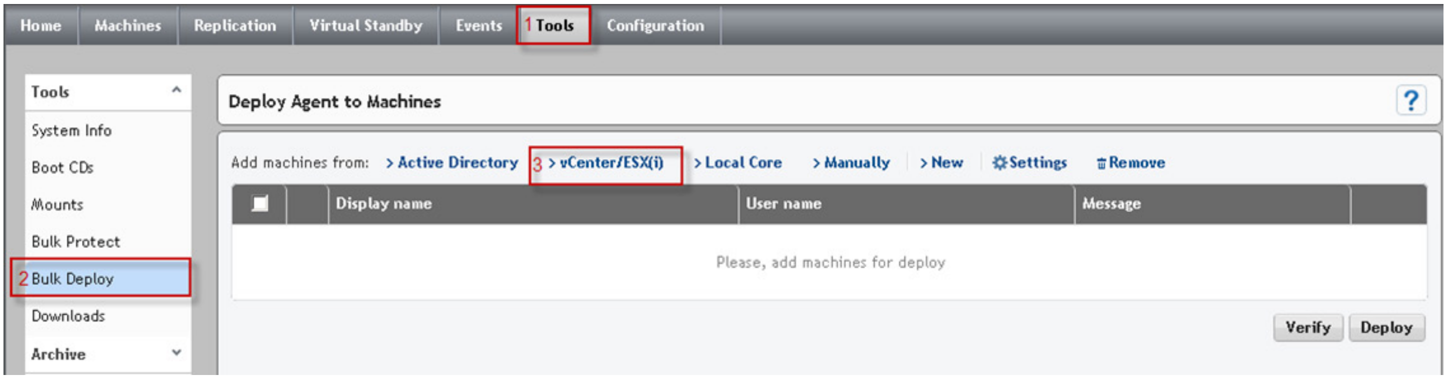
Child Tasks

Task	Status	Rate	Progress
Installing AppAssure Agent to 'VM2-W2K8' machine: Downloading installation files	22%	...	22 of 100%
Installing AppAssure Agent to 'VM1-W2K8' machine: Downloading installation files	22%	...	22 of 100%

2. vCenter/ESX(i) deployment

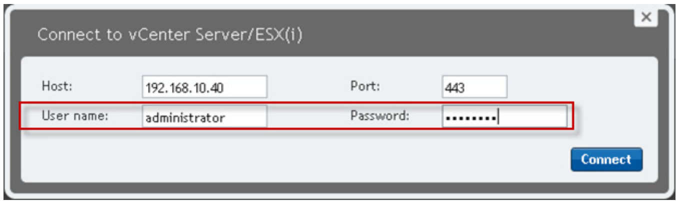
To deploy Dell AppAssure via vCenter/ESX(i):

- Connect to the Dell AppAssure core server
- Go to Tools-> Bulk Deploy -> vCenter/ESX(i)



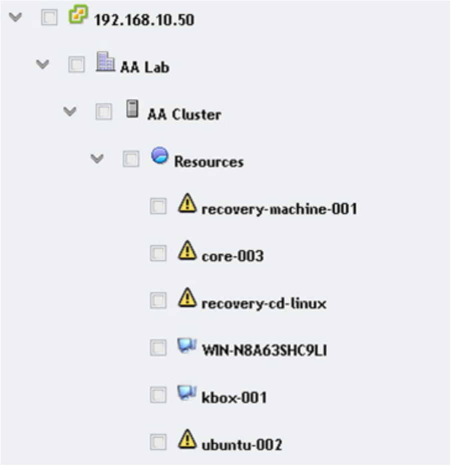
Please, add machines for deploy

- Enter the IP or hostname of your vCenter/ESX(i) server
- Enter administrator credentials



Host:	192.168.10.40	Port:	443
User name:	administrator	Password:	••••••••

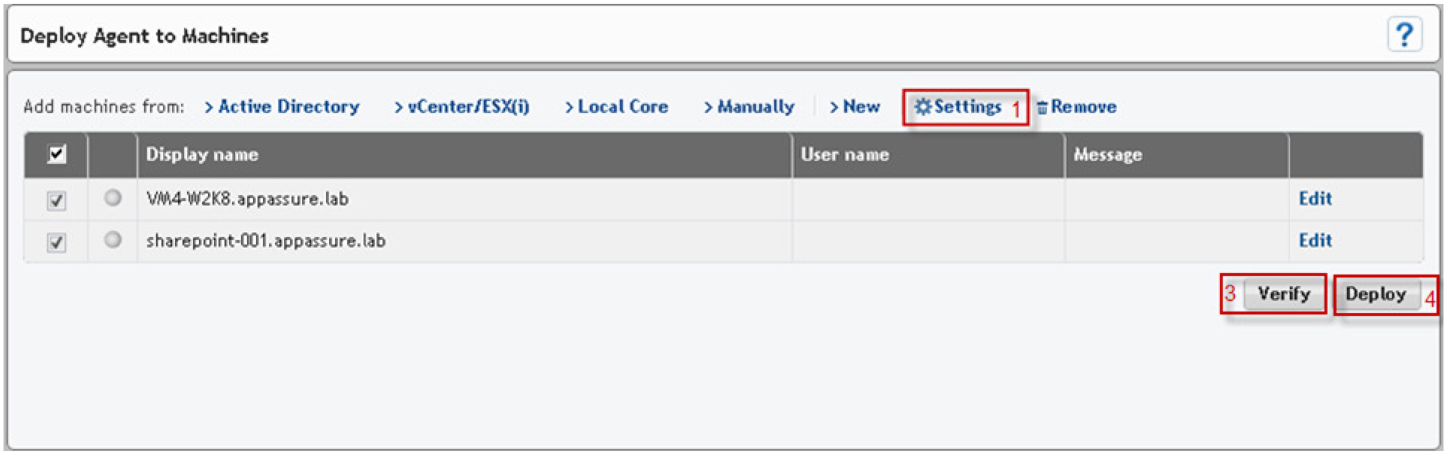
- Select the machines to which you are deploying the agents



□ 192.168.10.50
□ AA Lab
□ AA Cluster
□ Resources
□ recovery-machine-001
□ core-003
□ recovery-cd-linux
□ WIN-N8A63SHC9LI
□ kbox-001
□ ubuntu-002

After you have selected your machines you need to create a username:

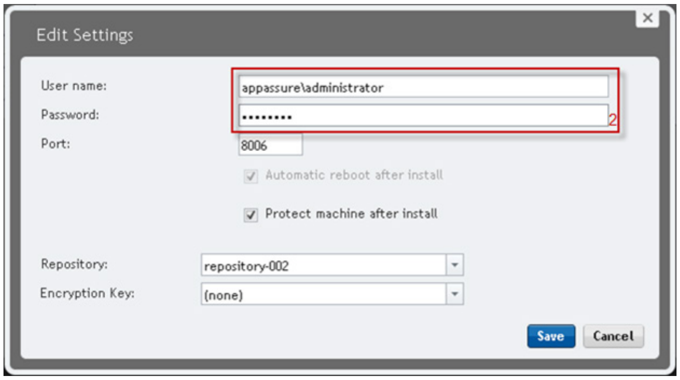
- Click on “Settings” and enter the username and password that you wish to deploy with
- Click “Verify” to validate installation credentials
- Click “Deploy” when ready



Deploy Agent to Machines

?
Add machines from: > Active Directory > vCenter/ESX(i) > Local Core > Manually > New Settings 1 Remove
3 Verify
Deploy 4

☑		Display name	User name	Message	
☑	○	VM4-W2K8.appassure.lab			Edit
☑	○	sharepoint-001.appassure.lab			Edit



Edit Settings

User name: appassure\administrator

Password: ••••••••

Port: 8006

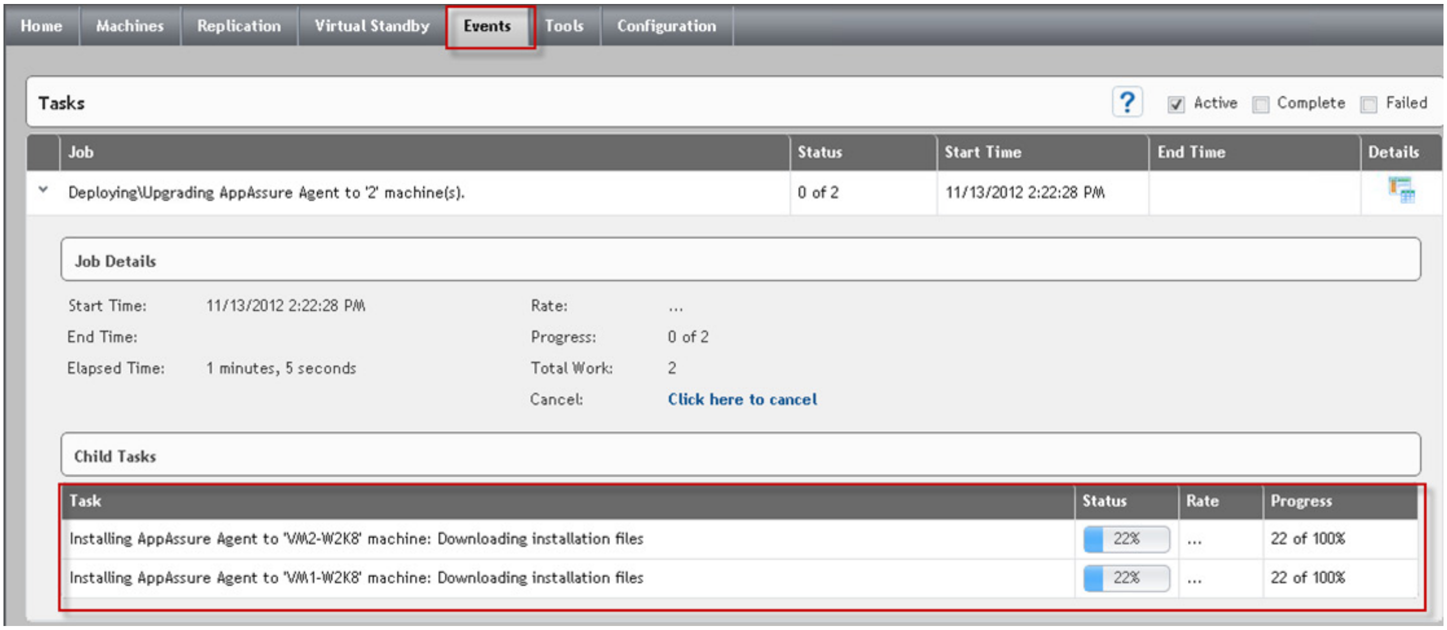
☑ Automatic reboot after install

☑ Protect machine after install

Repository: repository-002

Encryption Key: (none)

- After clicking deploy, click the “Events” tab to monitor the progress of the deployment



Tasks

☑ Active □ Complete □ Failed

Job	Status	Start Time	End Time	Details
Deploying\Upgrading AppAssure Agent to '2' machine(s).	0 of 2	11/13/2012 2:22:28 PM		

Job Details

Start Time: 11/13/2012 2:22:28 PM

End Time:

Elapsed Time: 1 minutes, 5 seconds

Rate: ...

Progress: 0 of 2

Total Work: 2

Cancel: Click here to cancel

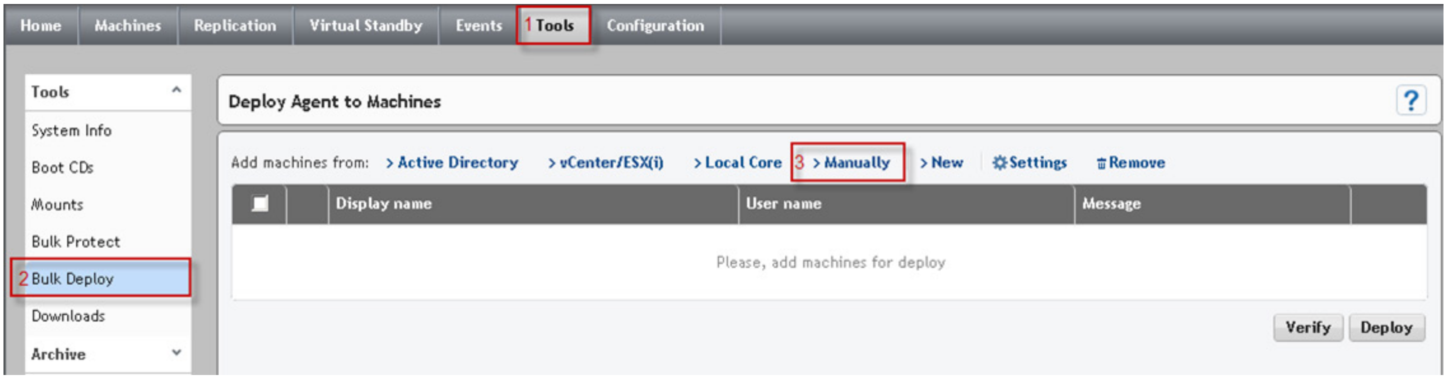
Child Tasks

Task	Status	Rate	Progress
Installing AppAssure Agent to 'VM2-W2K8' machine: Downloading installation files	22%	...	22 of 100%
Installing AppAssure Agent to 'VM1-W2K8' machine: Downloading installation files	22%	...	22 of 100%

3. Manual deployment

To deploy Dell AppAssure manually via the Core server:

- Connect to the Dell AppAssure core server
- Go to Tools-> Bulk Deploy -> Manually



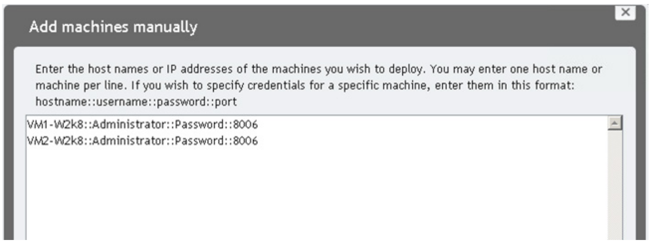
Deploy Agent to Machines

Add machines from:

□		Display name	User name	Message

Please, add machines for deploy

- Enter all of machines that you wish to deploy agents to
- Take note of the format for entering the names: hostname::username::password::port
- When done click "Add"

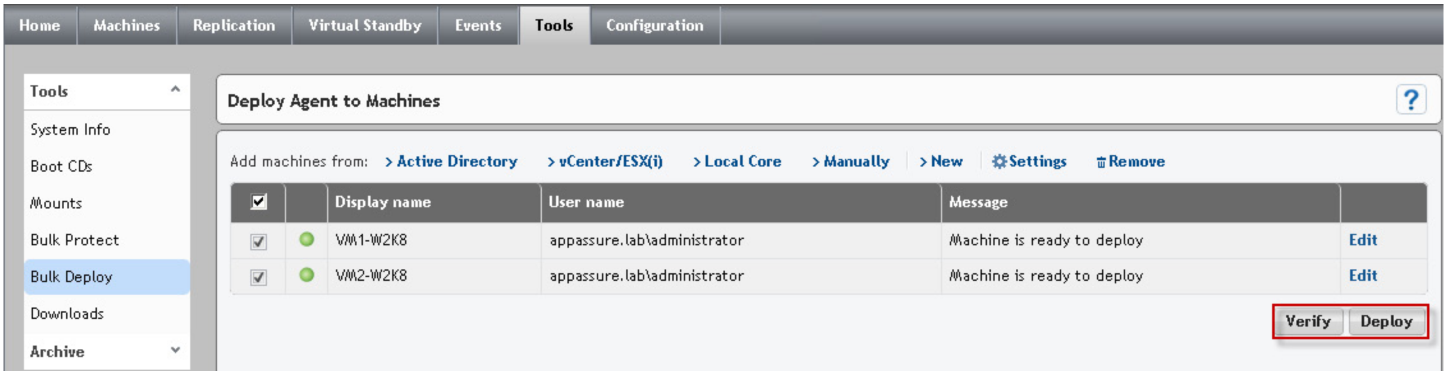


Add machines manually

Enter the host names or IP addresses of the machines you wish to deploy. You may enter one host name or machine per line. If you wish to specify credentials for a specific machine, enter them in this format: hostname::username::password::port

```
VM1-W2k8::Administrator::Password::8006
VM2-W2k8::Administrator::Password::8006
```

- Click "Verify" to ensure the machines are online and ready to deploy
- Once the machines have been verified click "Deploy"

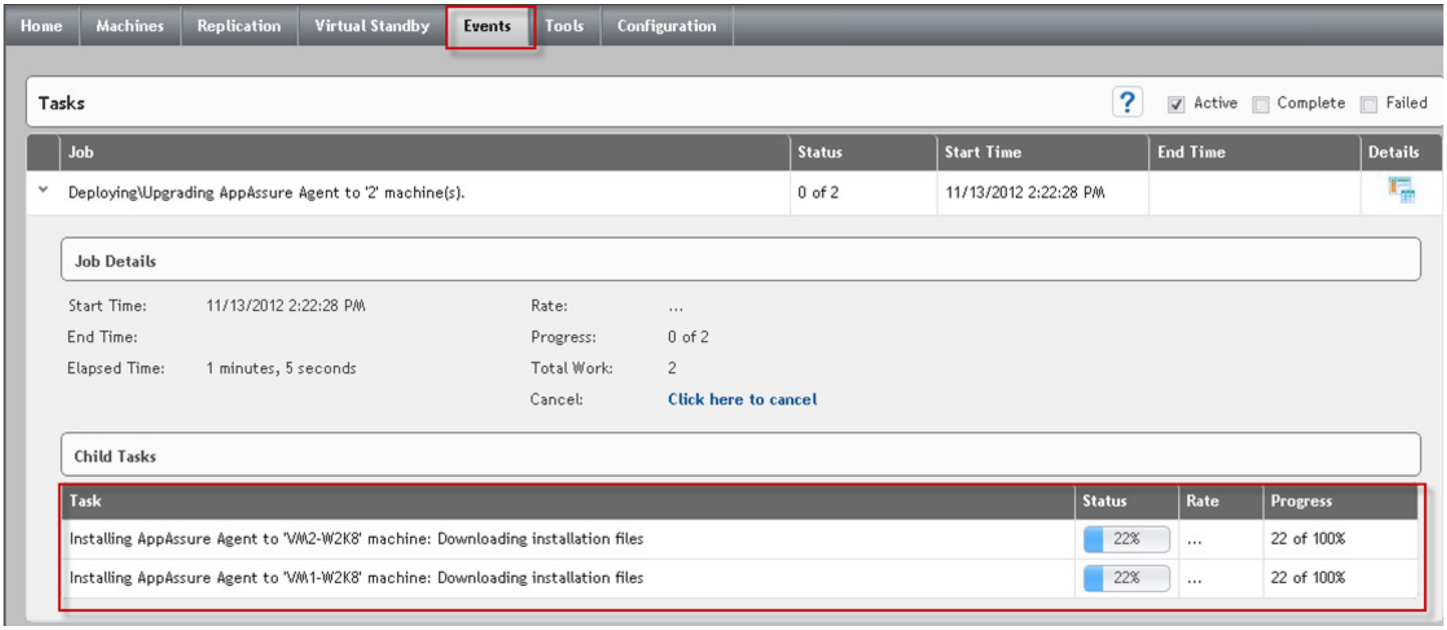


Deploy Agent to Machines

Add machines from:

☑		Display name	User name	Message	
☑	●	VM1-W2K8	appassure.lab\administrator	Machine is ready to deploy	Edit
☑	●	VM2-W2K8	appassure.lab\administrator	Machine is ready to deploy	Edit

After clicking deploy click the “Events” tab to monitor the progress of the deployment



Job	Status	Start Time	End Time	Details
Deploying\Upgrading AppAssure Agent to '2' machine(s).	0 of 2	11/13/2012 2:22:28 PM		

Job Details

Start Time:	11/13/2012 2:22:28 PM	Rate:	...
End Time:		Progress:	0 of 2
Elapsed Time:	1 minutes, 5 seconds	Total Work:	2
		Cancel:	Click here to cancel

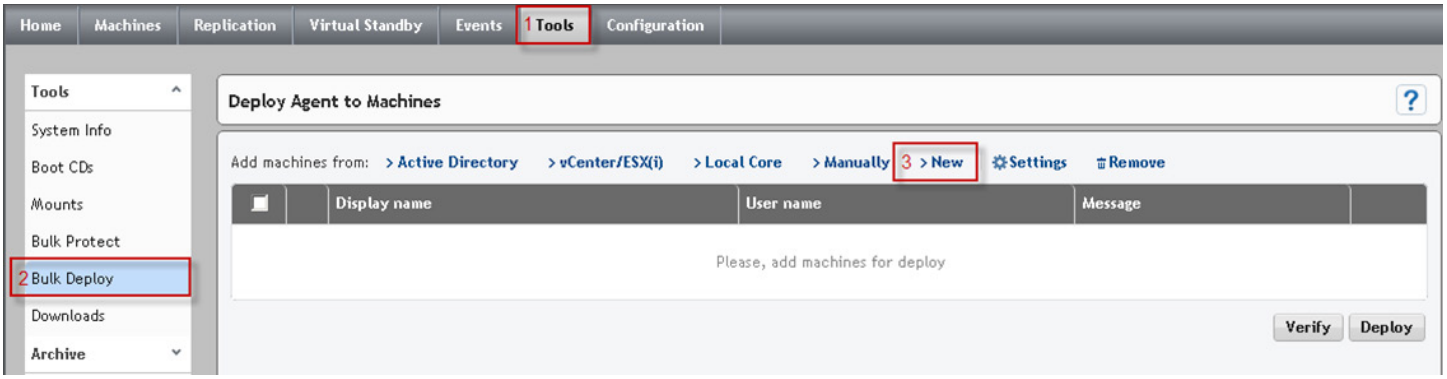
Child Tasks

Task	Status	Rate	Progress
Installing AppAssure Agent to 'VM2-W2K8' machine: Downloading installation files	22%	...	22 of 100%
Installing AppAssure Agent to 'VM1-W2K8' machine: Downloading installation files	22%	...	22 of 100%

4. New deployment

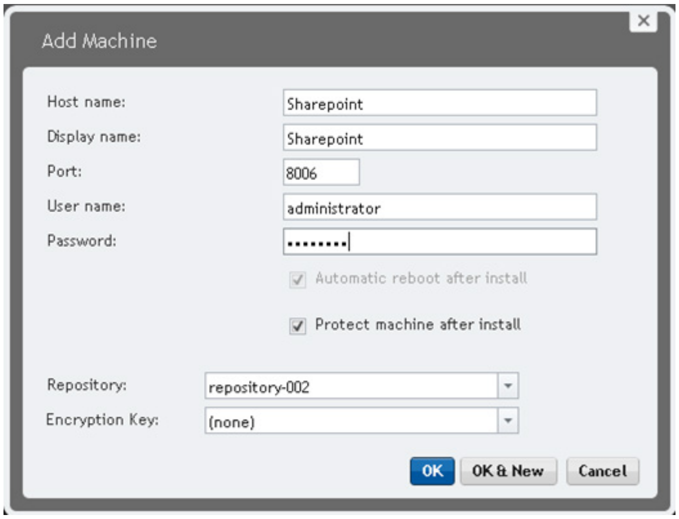
To deploy Dell AppAssure to a new machine via the Core server:

- Connect to the Dell AppAssure core server
- Go to Tools-> Bulk Deploy -> New



Please, add machines for deploy

- Enter the hostname and display name of the machine to which you wish to deploy
- Enter administrator credentials for that machine
- If you do not wish to reboot the machine automatically after the deployment, de-select “Protect machine after install”
- Select the repository that the machine should send its backups to

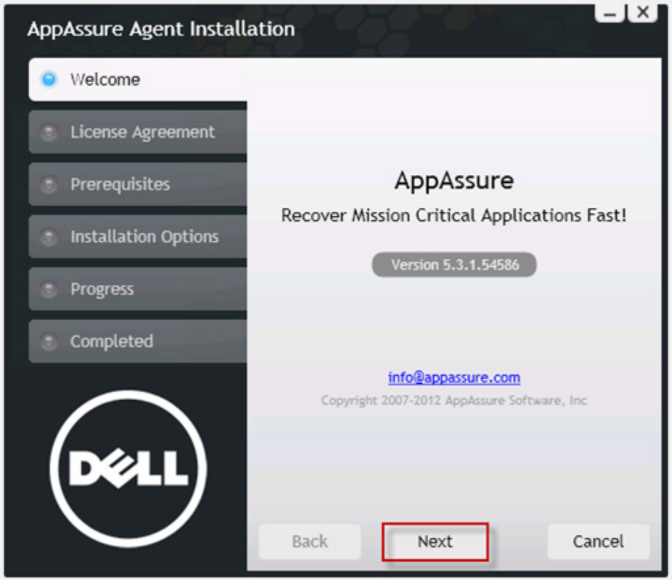


Add Machine

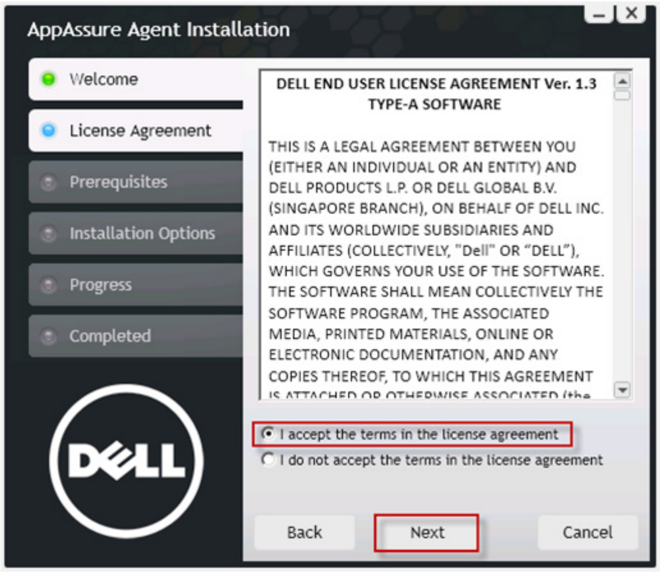
Host name:	Sharepoint
Display name:	Sharepoint
Port:	8006
User name:	administrator
Password:	••••••••
	☑ Automatic reboot after install
	☑ Protect machine after install
Repository:	repository-002
Encryption Key:	(none)

5. Local agent deployment

Download the Dell AppAssure agent from AppAssure.com
Run the installer locally on the machine that you wish to protect
Click “Next” to begin the installation process



After reading the license agreement you must then “Accept” the agreement. After accepting the agreement you can then click “Next” to proceed with the install

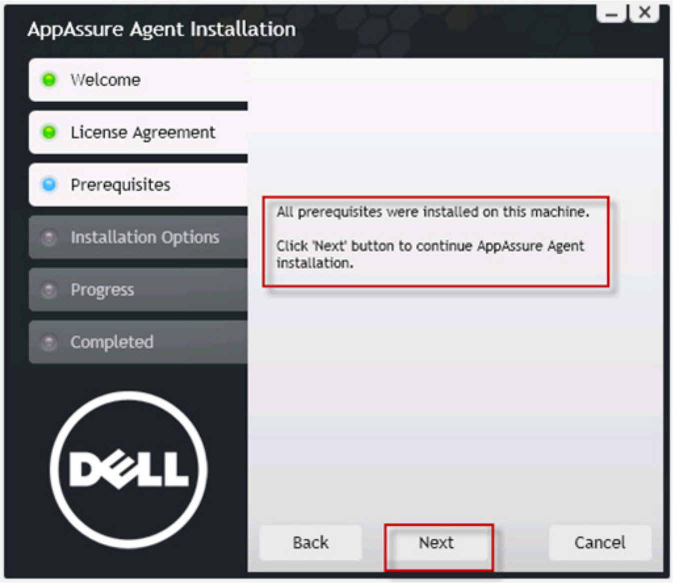


DELL END USER LICENSE AGREEMENT Ver. 1.3
TYPE-A SOFTWARE

THIS IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR AN ENTITY) AND DELL PRODUCTS L.P. OR DELL GLOBAL B.V. (SINGAPORE BRANCH), ON BEHALF OF DELL INC. AND ITS WORLDWIDE SUBSIDIARIES AND AFFILIATES (COLLECTIVELY, "Dell" OR “DELL”), WHICH GOVERNS YOUR USE OF THE SOFTWARE. THE SOFTWARE SHALL MEAN COLLECTIVELY THE SOFTWARE PROGRAM, THE ASSOCIATED MEDIA, PRINTED MATERIALS, ONLINE OR ELECTRONIC DOCUMENTATION, AND ANY COPIES THEREOF, TO WHICH THIS AGREEMENT IS ATTACHED OR OTHERWISE ASSOCIATED (the

● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement

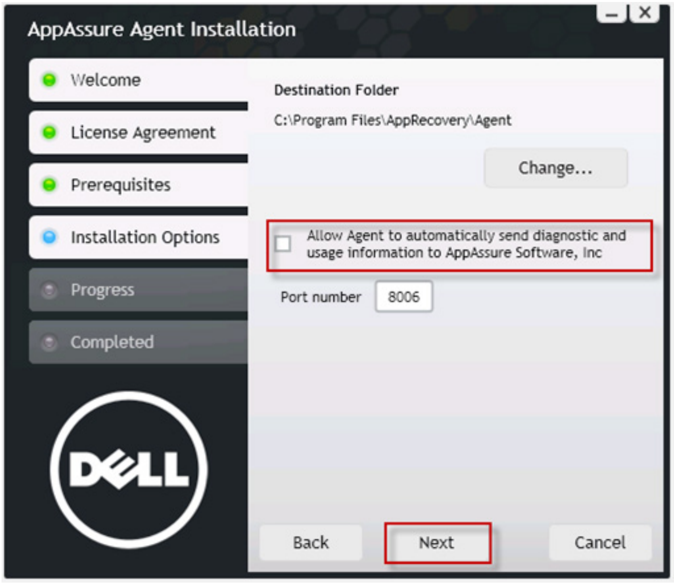
If your machine is missing any prerequisites, you will be prompted to allow Dell AppAssure to install the missing components for you
Once all prerequisites are met you can then click “Next” to proceed with the install



All prerequisites were installed on this machine.

Click 'Next' button to continue AppAssure Agent installation.

Dell AppAssure will send back diagnostic and usage information if you choose to allow
Choose “Next” to continue with the installation



Destination Folder

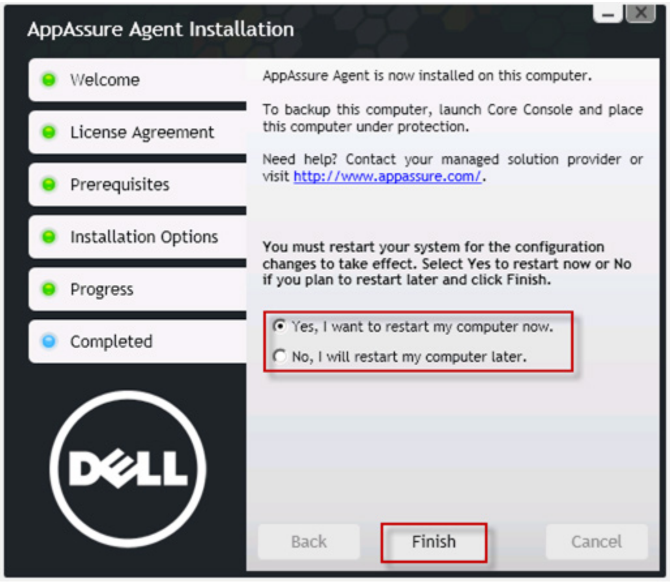
C:\Program Files\AppRecovery\Agent

□ Allow Agent to automatically send diagnostic and usage information to AppAssure Software, Inc

Port number 8006

Note: Enabling automatic feedback will allow the Dell AppAssure core to send logs periodically from all agents and cores to Dell.

To complete the installation and begin protecting your machine you must reboot the system
If you choose not to reboot you will not be able to begin taking backups of your system until a reboot has take place
Choose “Finish” to complete the installation



AppAssure Agent is now installed on this computer.

To backup this computer, launch Core Console and place this computer under protection.

Need help? Contact your managed solution provider or visit http://www.appassure.com/.

You must restart your system for the configuration changes to take effect. Select Yes to restart now or No if you plan to restart later and click Finish.

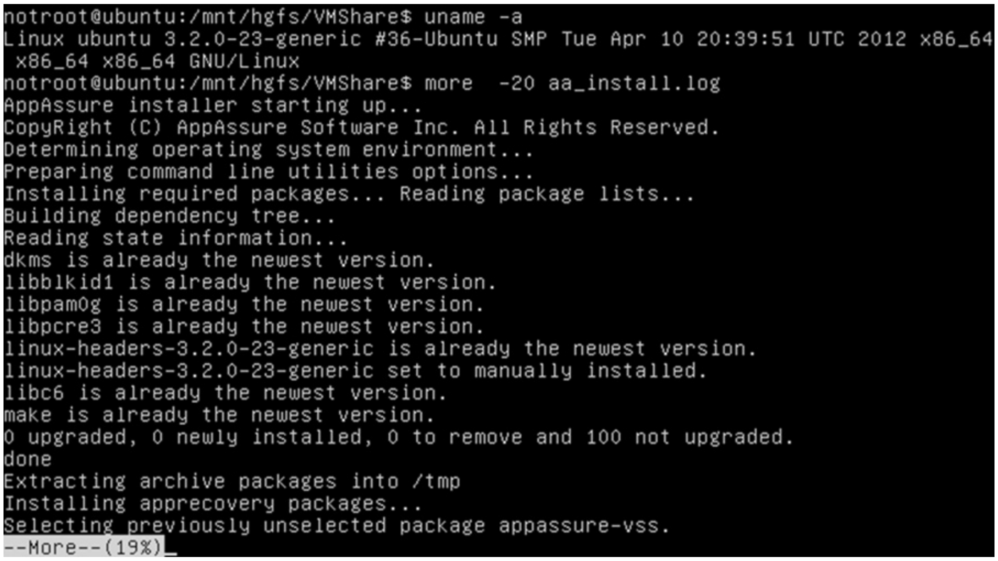
● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

6. Installation of Dell AppAssure Linux agent

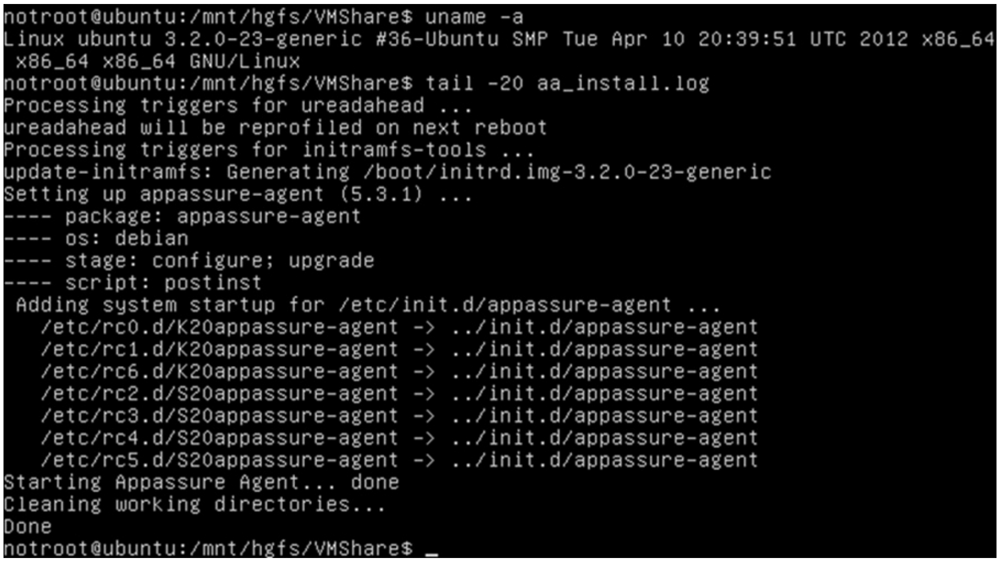
This installation is a manual process executed by root (sudo) in a terminal window, the following pre-requisites should be followed:

- Apply all outstanding patches to the base OS (sudo apt-get update)
- Download the Ubuntu Appassure Agent and copy it into /tmp
- Execute the installer script: cd /tmp; sudo ./appassure-installer-ubuntu-amd64-x.x. | tee > aa_install.log
- The installer produces a large log file which is saved in /tmp/aa_install.log in this example



```
notroot@ubuntu:/mnt/hgfs/VMShare$ uname -a
Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64
 x86_64 x86_64 GNU/Linux
notroot@ubuntu:/mnt/hgfs/VMShare$ more  -20 aa_install.log
AppAssure installer starting up...
CopyRight (C) AppAssure Software Inc. All Rights Reserved.
Determining operating system environment...
Preparing command line utilities options...
Installing required packages... Reading package lists...
Building dependency tree...
Reading state information...
dkms is already the newest version.
libblkid1 is already the newest version.
libpam0g is already the newest version.
libpcre3 is already the newest version.
linux-headers-3.2.0-23-generic is already the newest version.
linux-headers-3.2.0-23-generic set to manually installed.
libc6 is already the newest version.
make is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 100 not upgraded.
done
Extracting archive packages into /tmp
Installing apprecovery packages...
Selecting previously unselected package appassure-vss.
--More--(19%)_
```

The installer completes successfully and displays the message “Starting Appassure Agent… done”



```
notroot@ubuntu:/mnt/hgfs/VMShare$ uname -a
Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64
 x86_64 x86_64 GNU/Linux
notroot@ubuntu:/mnt/hgfs/VMShare$ tail -20 aa_install.log
Processing triggers for ureadahead ...
ureadahead will be reprofiled on next reboot
Processing triggers for initramfs-tools ...
update-initramfs: Generating /boot/initrd.img-3.2.0-23-generic
Setting up appassure-agent (5.3.1) ...
---- package: appassure-agent
---- os: debian
---- stage: configure; upgrade
---- script: postinst
 Adding system startup for /etc/init.d/appassure-agent ...
   /etc/rc0.d/K20appassure-agent -> ../init.d/appassure-agent
   /etc/rc1.d/K20appassure-agent -> ../init.d/appassure-agent
   /etc/rc6.d/K20appassure-agent -> ../init.d/appassure-agent
   /etc/rc2.d/S20appassure-agent -> ../init.d/appassure-agent
   /etc/rc3.d/S20appassure-agent -> ../init.d/appassure-agent
   /etc/rc4.d/S20appassure-agent -> ../init.d/appassure-agent
   /etc/rc5.d/S20appassure-agent -> ../init.d/appassure-agent
Starting Appassure Agent... done
Cleaning working directories...
Done
notroot@ubuntu:/mnt/hgfs/VMShare$ _
```

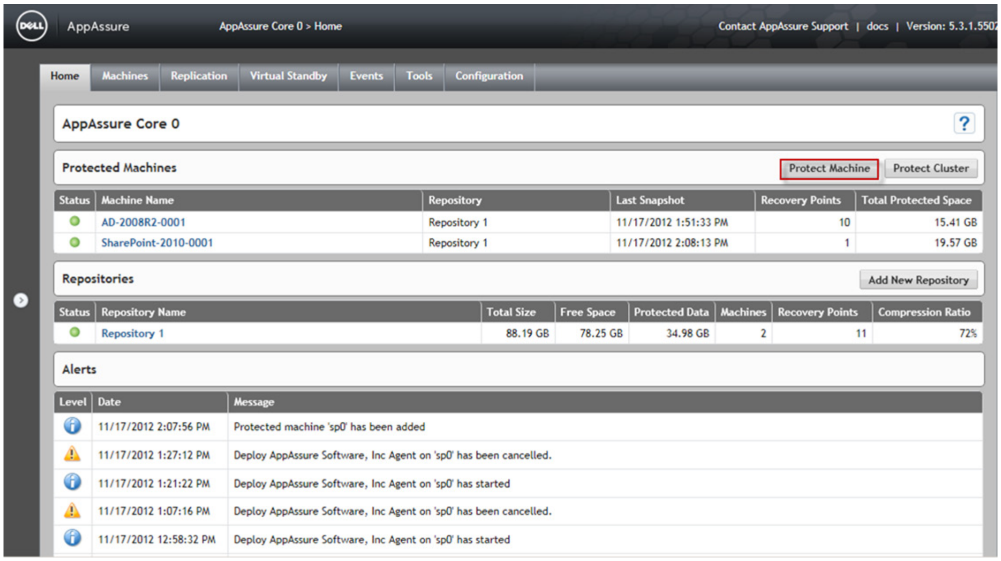
Dell AppAssure Backup, Replication, and Recovery Evaluator’s Guide: How to Manually Protect a Machine

Why read this guide

In some cases, including environments with expanded firewall and DNS settings, manual protection of the Dell AppAssure agent may be necessary.

How to manually protect a machine

After manual installation of an agent, that machine needs to be added to a Dell AppAssure Core and protected.
Click “Protect Machine.”



AppAssure Core 0

Protected Machines

Status	Machine Name	Repository	Last Snapshot	Recovery Points	Total Protected Space
●	AD-2008R2-0001	Repository 1	11/17/2012 1:51:33 PM	10	15.41 GB
●	SharePoint-2010-0001	Repository 1	11/17/2012 2:08:13 PM	1	19.57 GB

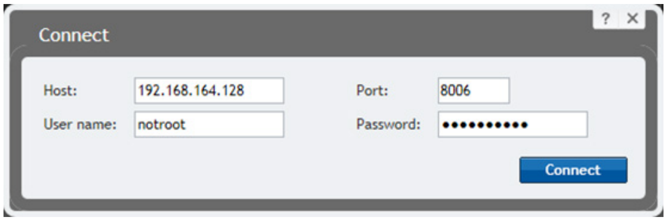
Repositories

Status	Repository Name	Total Size	Free Space	Protected Data	Machines	Recovery Points	Compression Ratio
●	Repository 1	88.19 GB	78.25 GB	34.98 GB	2	11	72%

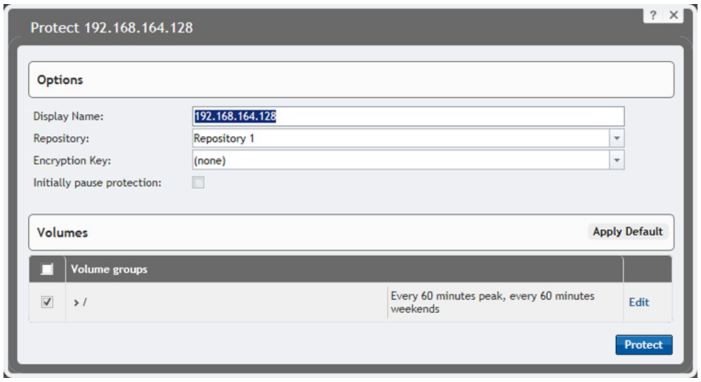
Alerts

Level	Date	Message
ⓘ	11/17/2012 2:07:56 PM	Protected machine 'sp0' has been added
⚠	11/17/2012 1:27:12 PM	Deploy AppAssure Software, Inc Agent on 'sp0' has been cancelled.
ⓘ	11/17/2012 1:21:22 PM	Deploy AppAssure Software, Inc Agent on 'sp0' has started
⚠	11/17/2012 1:07:16 PM	Deploy AppAssure Software, Inc Agent on 'sp0' has been cancelled.
ⓘ	11/17/2012 12:58:32 PM	Deploy AppAssure Software, Inc Agent on 'sp0' has started

First, connect to the machine you wish to protect. Provide the Host Name or IP address, the port, and credentials.
Once connected, configure the Display name, choose the Repository and encryption key. The Volume groups will be listed, and protection will be set at default value of 60 minutes between backups.



Host: 192.168.164.128
Port: 8006
User name: notroot
Password: ••••••••••



Protect 192.168.164.128

Options

Display Name: 192.168.164.128
Repository: Repository 1
Encryption Key: (none)
Initially pause protection: □

Volumes

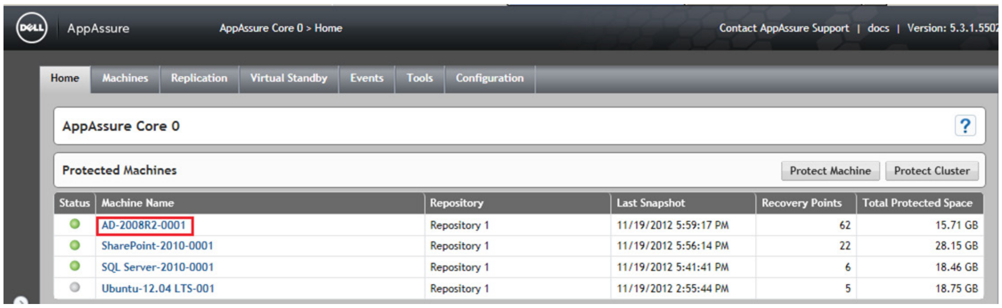
☑ › / — Every 60 minutes peak, every 60 minutes weekends

NOTE: Protection settings can also be modified from the default settings, detailed in the next section.

1. How to configure custom protection settings

Configuring protection schedules

Default settings direct the Dell AppAssure agent installed on each protected machine to perform a backup every 60 minutes throughout the day. You can adjust the frequency for longer intervals or to as little as every five minutes. Select the machine you wish to configure and continue to the next screen.

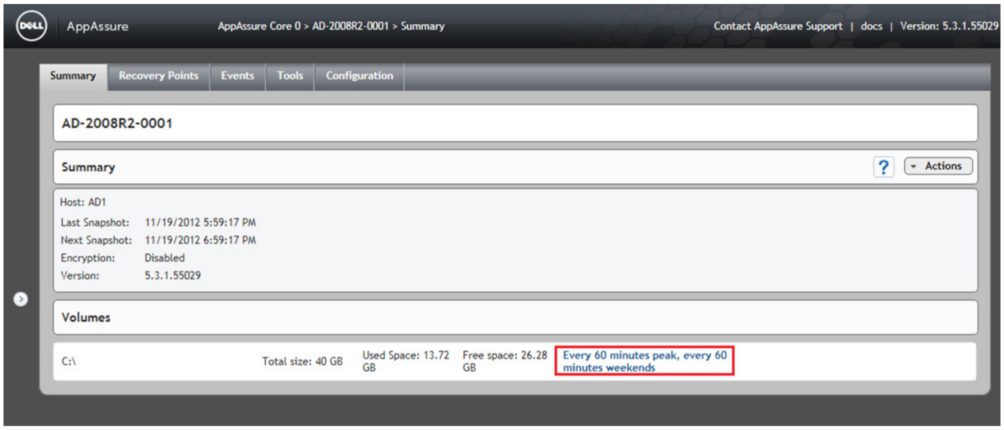


AppAssure Core 0

Protected Machines

Status	Machine Name	Repository	Last Snapshot	Recovery Points	Total Protected Space
●	AD-2008R2-0001	Repository 1	11/19/2012 5:59:17 PM	62	15.71 GB
●	SharePoint-2010-0001	Repository 1	11/19/2012 5:56:14 PM	22	28.15 GB
●	SQL Server-2010-0001	Repository 1	11/19/2012 5:41:41 PM	6	18.46 GB
○	Ubuntu-12.04 LTS-001	Repository 1	11/19/2012 2:55:44 PM	5	18.75 GB

Modify the default Protection Settings by selecting the Protection Settings highlighted below in red.


DELL
AppAssure
AppAssure Core 0 > AD-2008R2-0001 > Summary
Contact AppAssure Support | docs | Version: 5.3.1.55029
Summary
Recovery Points
Events
Tools
Configuration
?
Actions

AD-2008R2-0001

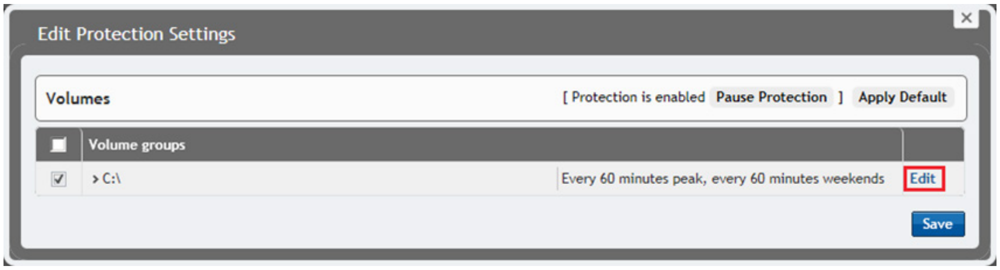
Summary

Host: AD1
Last Snapshot: 11/19/2012 5:59:17 PM
Next Snapshot: 11/19/2012 6:59:17 PM
Encryption: Disabled
Version: 5.3.1.55029

Volumes

C:\ Total size: 40 GB Used Space: 13.72 GB Free space: 26.28 GB Every 60 minutes peak, every 60 minutes weekends

Click “Edit” to change the protection schedule for this machine.

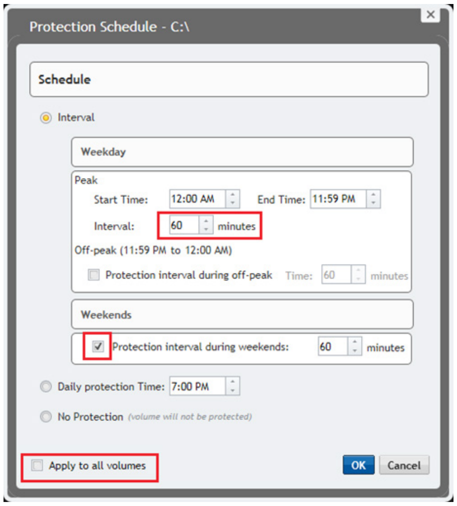


Edit Protection Settings

Volumes [Protection is enabled Pause Protection] Apply Default

☐	Volume groups	
☑	> C:\	Every 60 minutes peak, every 60 minutes weekends

Here you can edit the protection schedule of a machine. You can have a weekday and a weekend schedule, as well as weekday “Peak” and “Off Peak” schedules for protected volumes.
Or you can simply choose once-a-day protection.
You may also Apply this custom schedule to “all volumes.”
Once configured Press “OK” to proceed.



Protection Schedule - C:\

Schedule

● Interval

Weekday

Peak
Start Time: 12:00 AM End Time: 11:59 PM
Interval: 60 minutes
Off-peak (11:59 PM to 12:00 AM)
☐ Protection interval during off-peak Time: 60 minutes

Weekends

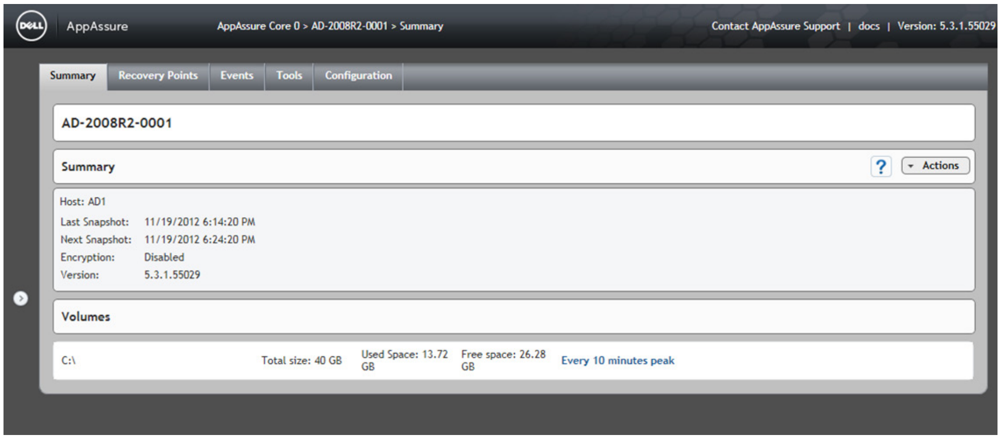
☑ Protection interval during weekends: 60 minutes

○ Daily protection Time: 7:00 PM

○ No Protection (volume will not be protected)

☐ Apply to all volumes

Once completed, the new Protection Schedule is configured and displayed in a summary window. Here you can see this particular machine will be protected every 10 minutes during peak periods.



AppAssure   AppAssure Core 0 > AD-2008R2-0001 > Summary   Contact AppAssure Support | docs | Version: 5.3.1.55029

AD-2008R2-0001

Summary

Host: AD1
Last Snapshot: 11/19/2012 6:14:20 PM
Next Snapshot: 11/19/2012 6:24:20 PM
Encryption: Disabled
Version: 5.3.1.55029

Volumes

C:\ Total size: 40 GB Used Space: 13.72 GB Free space: 26.28 GB Every 10 minutes peak

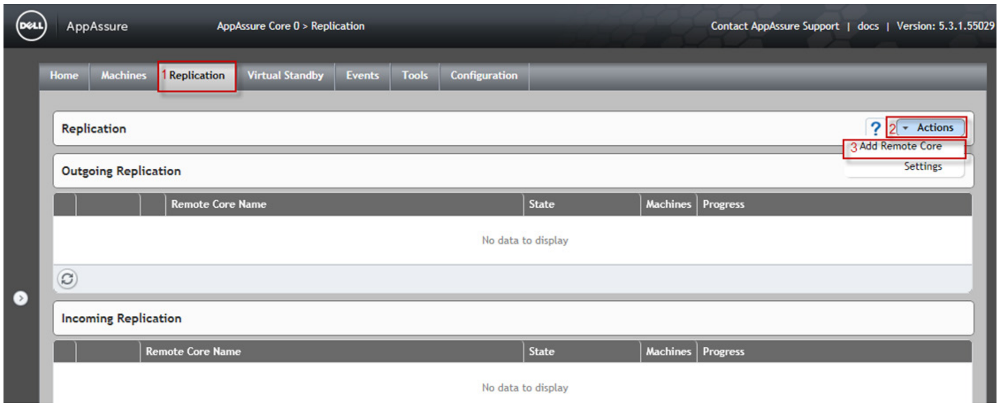
Dell AppAssure Backup, Replication, and Recovery Evaluator’s Guide: How to Configure Replication

Why read this guide

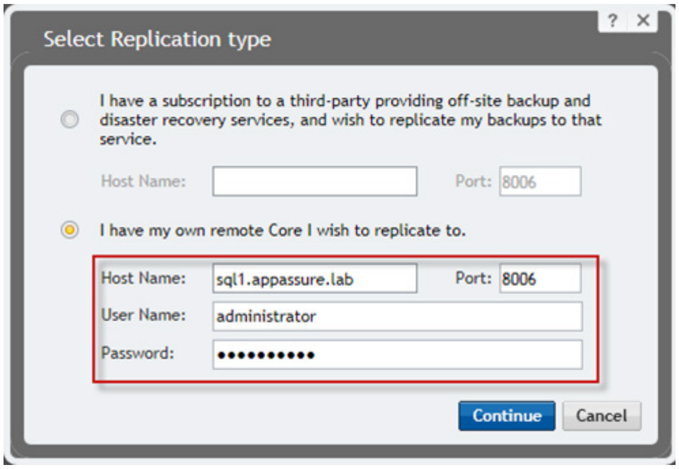
Replication is a key element in many data backup and recovery scenarios, and allows users to protect date by replicating it at alternative locations, physical or in the cloud. Dell AppAssure replication is a quick and easy way to install original recovery points on another Dell AppAssure Core.

Configuring replication

Protected machines may have their Recovery Points replicated to another Dell AppAssure Core. Core replication is used for redundancy by sending data to remote sites, datacenters, or Cloud sites.
To begin Replication, select Replication > Actions > Add Remote Core on the Core you wish to replicate.



Complete the “Select Replication type” pop-up by supplying the Core name (IP/host name), port, and the credentials for the Core.



Select Replication type

○ I have a subscription to a third-party providing off-site backup and disaster recovery services, and wish to replicate my backups to that service.

Host Name: Port: 8006

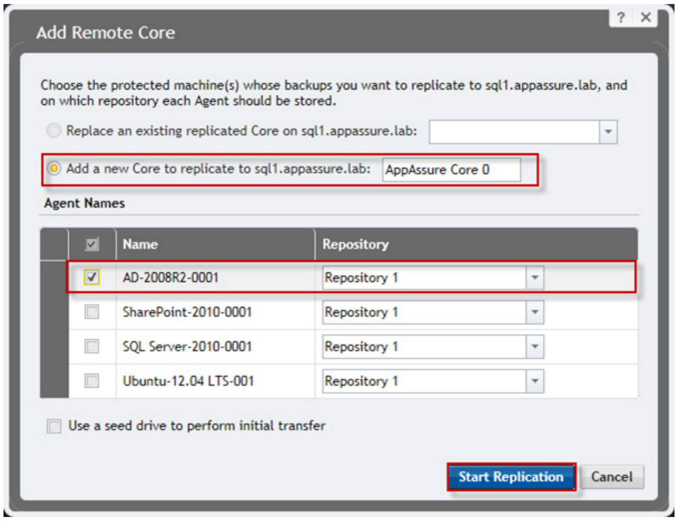
● I have my own remote Core I wish to replicate to.

Host Name: sql1.appassure.lab Port: 8006

User Name: administrator

Password: ●●●●●●●●●●

Specify the machines to be replicated on the “Add Remote Core” pop-up by selecting the checkboxes. If the remote Core has multiple Repositories, you may specify which repository here.
Press “Start Replication” to start the operation.



Add Remote Core

Choose the protected machine(s) whose backups you want to replicate to sql1.appassure.lab, and on which repository each Agent should be stored.

○ Replace an existing replicated Core on sql1.appassure.lab:

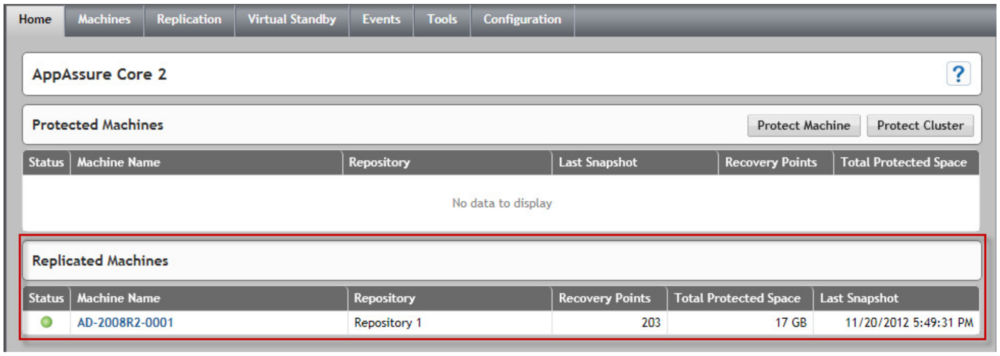
● Add a new Core to replicate to sql1.appassure.lab: AppAssure Core 0

Agent Names

☑	Name	Repository
☑	AD-2008R2-0001	Repository 1
□	SharePoint-2010-0001	Repository 1
□	SQL Server-2010-0001	Repository 1
□	Ubuntu-12.04 LTS-001	Repository 1

□ Use a seed drive to perform initial transfer

Once you’ve configured Replication you can see the Replicated Machines listed



AppAssure Core 2

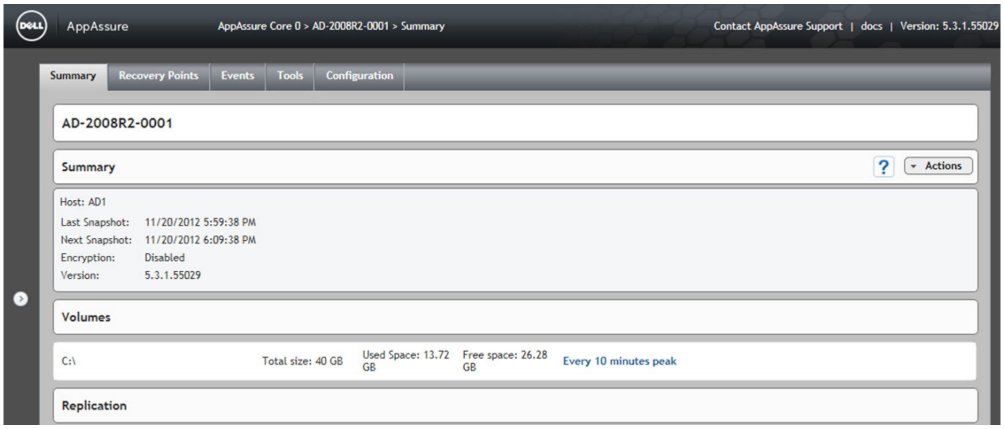
Protected Machines

Status	Machine Name	Repository	Last Snapshot	Recovery Points	Total Protected Space
No data to display					

Replicated Machines

Status	Machine Name	Repository	Recovery Points	Total Protected Space	Last Snapshot
●	AD-2008R2-0001	Repository 1	203	17 GB	11/20/2012 5:49:31 PM

Here is Summary sheet for the machine showing Recovery Points replicated to a second server:



AppAssure
AppAssure Core 0 > AD-2008R2-0001 > Summary
Contact AppAssure Support | docs | Version: 5.3.1.55029
Summary
Recovery Points
Events
Tools
Configuration
Actions

AD-2008R2-0001

Summary

Host: AD1
Last Snapshot: 11/20/2012 5:59:38 PM
Next Snapshot: 11/20/2012 6:09:38 PM
Encryption: Disabled
Version: 5.3.1.55029

Volumes

C:\ Total size: 40 GB Used Space: 13.72 GB Free space: 26.28 GB Every 10 minutes peak

Replication

Dell AppAssure Backup, Replication, and Recovery Evaluator's Guide: How to Configure Virtual Standby for ESX(i) and Hyper-V

Why read this guide

Dell AppAssure's Virtual Standby provides the ability to offer high availability to mission critical servers at all times. Any machine that is protected with Dell AppAssure can automatically be recovered as converted to a virtual machine on VMware ESX(i) or Workstation, or Microsoft Hyper-V platforms.

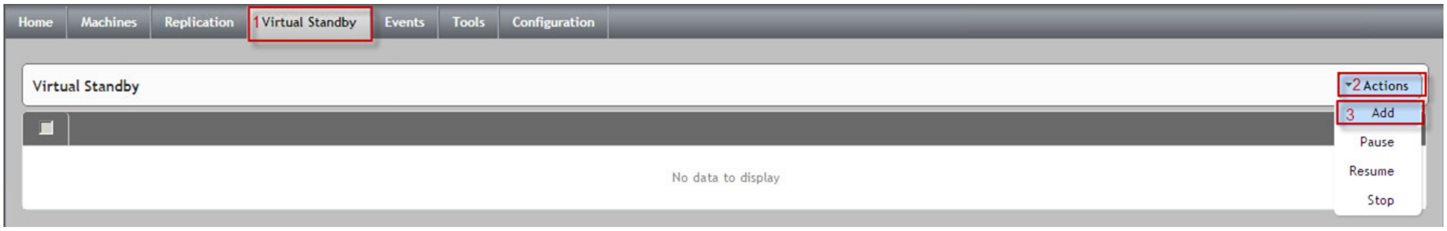
Dell AppAssure allows business to achieve much-improved business continuity for their IT services, as evidenced by its highly granular five-minute Recovery Point Objective's (RPO) and near-zero Recovery Time Objectives (RTO's) - far better than traditional recovery methods that can take hours or days.

Configuring

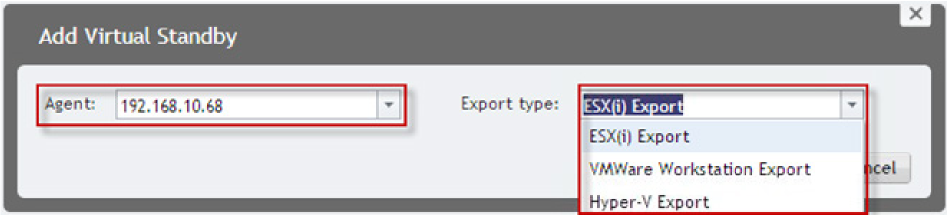
Virtual standby allows for the automatic creation of a virtual machine based on backups stored in the Dell AppAssure repository.

To create a virtual standby:

- Connect to the Dell AppAssure core server and click "Virtual Standby"
- Click "Actions"
- Click "Add"



- Select the machine to be used as a virtual standby
- Choose the type of virtual standby to be created for the selected agent

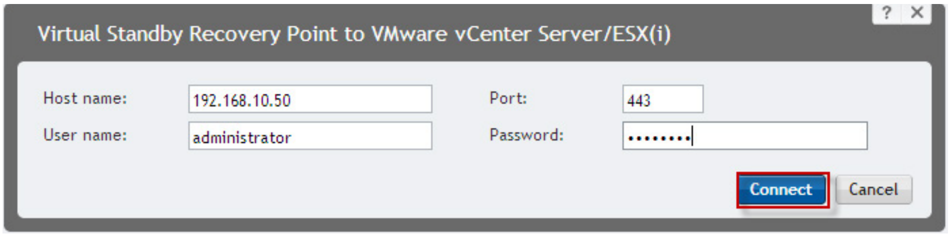

Add Virtual Standby

Agent: 192.168.10.68

Export type: ESX(i) Export

Note: Choosing VMware Workstation Export will generate a folder which contains all the files necessary to run the virtual machine.

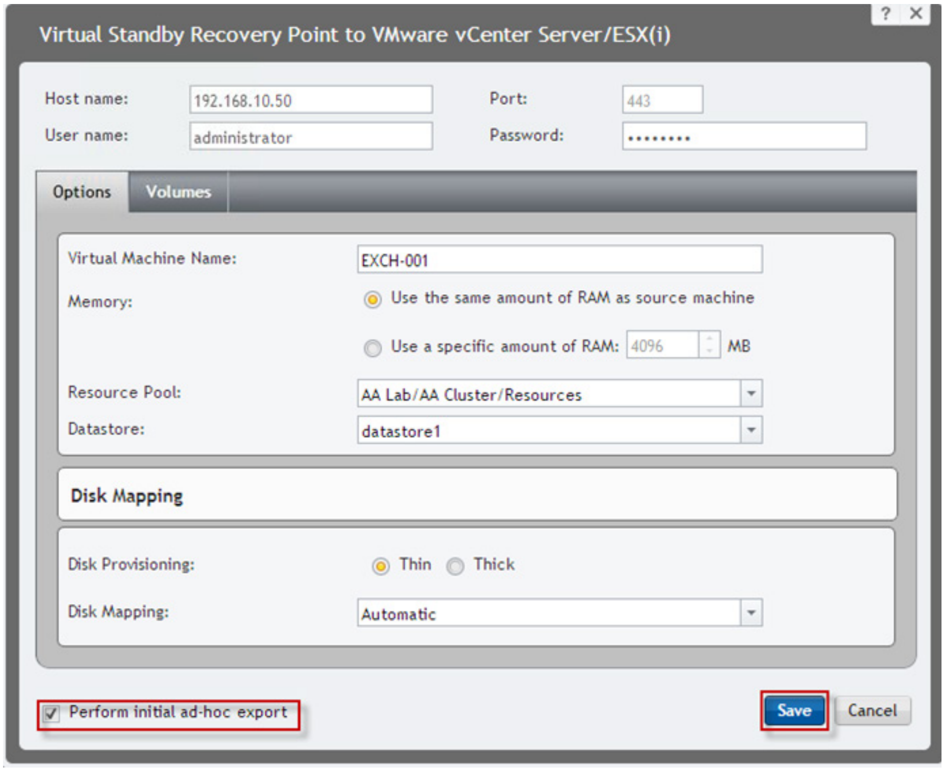
To create a virtual standby for ESX(i), enter the hostname/IP of the ESX(i) host or vCenter server along with administrator credentials. When done, press “Connect.”



Virtual Standby Recovery Point to VMware vCenter Server/ESX(i)

Host name: 192.168.10.50
User name: administrator
Port: 443
Password: ••••••••

In the pop-up window enter the desired configuration for the virtual standby machine.



Virtual Standby Recovery Point to VMware vCenter Server/ESX(i)

Host name: 192.168.10.50
User name: administrator
Port: 443
Password: ••••••••

Options | Volumes

Virtual Machine Name: EXCH-001
Memory: ● Use the same amount of RAM as source machine
○ Use a specific amount of RAM: 4096 MB
Resource Pool: AA Lab/AA Cluster/Resources
Datastore: datastore1

Disk Mapping

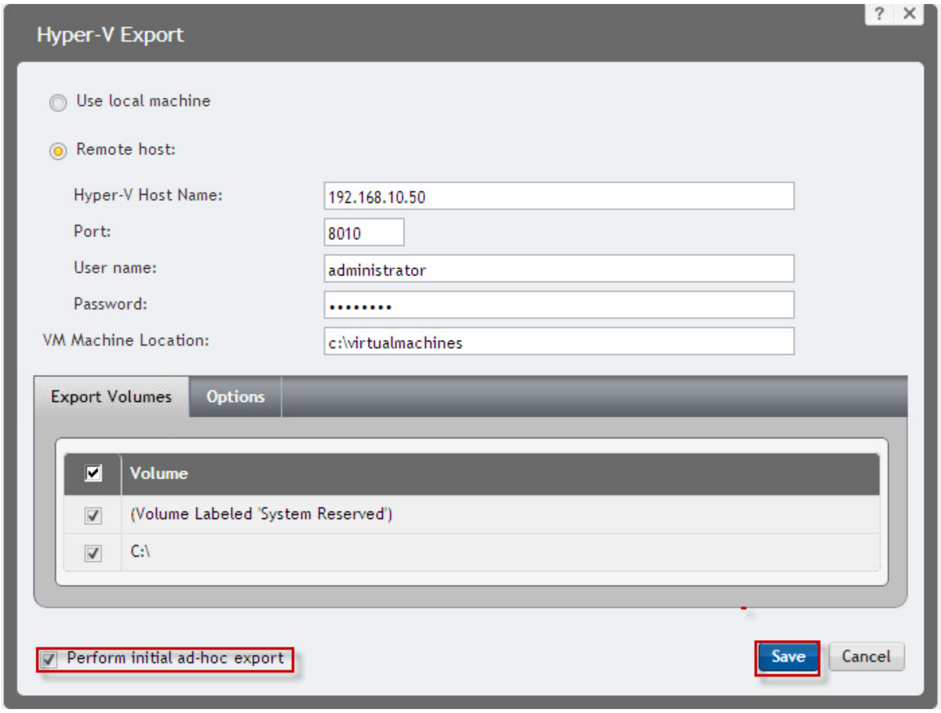
Disk Provisioning: ● Thin ○ Thick
Disk Mapping: Automatic

☑ Perform initial ad-hoc export

Note: “Perform initial ad-hoc export” will trigger an immediate conversion on a machine’s backup to a virtual standby upon selecting “Save.”

If choosing to export a machine to Hyper-V, Dell AppAssure will require the hostname/IP of a Hyper-V host.

In the Hyper-V export pop-up window, enter the desired configuration for the virtual standby.



○ Use local machine

● Remote host:

Hyper-V Host Name: 192.168.10.50

Port: 8010

User name: administrator

Password: ••••••••

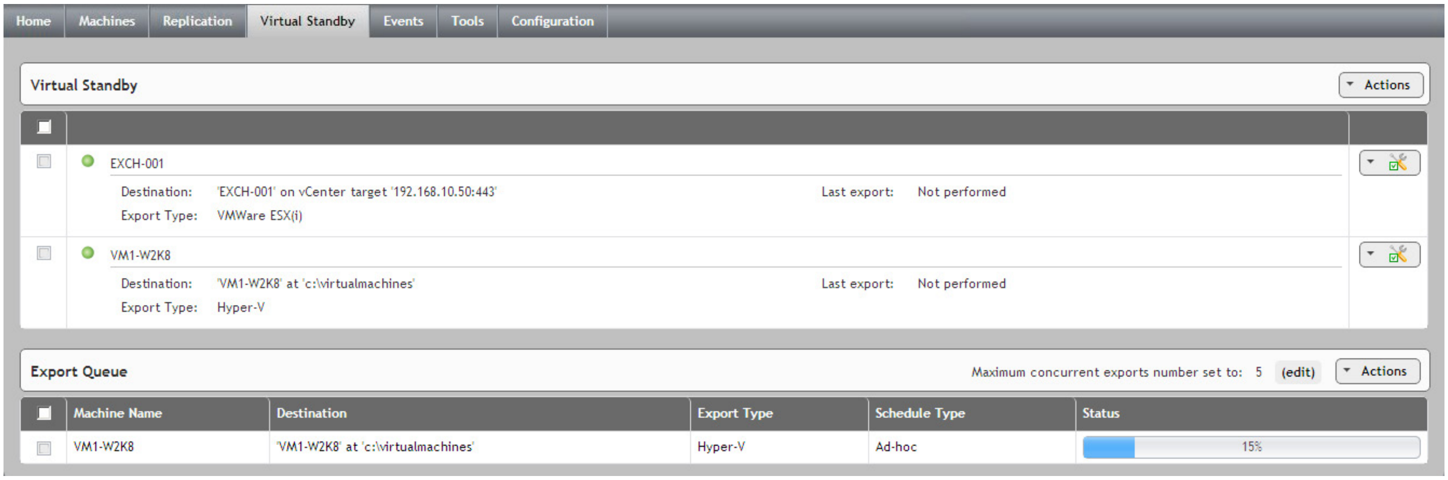
VM Machine Location: c:\virtualmachines

☑	Volume
☑	(Volume Labeled 'System Reserved')
☑	C:\

☑ Perform initial ad-hoc export

Note: "Perform initial ad-hoc export" will trigger an immediate conversion on a machines backup to a virtual standby upon selecting "Save."

After saving the configuration, the virtual standby task will be displayed and take place after every snapshot is taken.



Virtual Standby

□ ● EXCH-001

Destination: 'EXCH-001' on vCenter target '192.168.10.50:443'   Last export: Not performed

Export Type: VMWare ESX(i)

□ ● VM1-W2K8

Destination: 'VM1-W2K8' at 'c:\virtualmachines'   Last export: Not performed

Export Type: Hyper-V

Export Queue

Maximum concurrent exports number set to: 5

□	Machine Name	Destination	Export Type	Schedule Type	Status
□	VM1-W2K8	'VM1-W2K8' at 'c:\virtualmachines'	Hyper-V	Ad-hoc	15%

Dell AppAssure Backup, Replication, and Recovery Evaluator's Guide: How to do Live Recovery™ for Microsoft Exchange

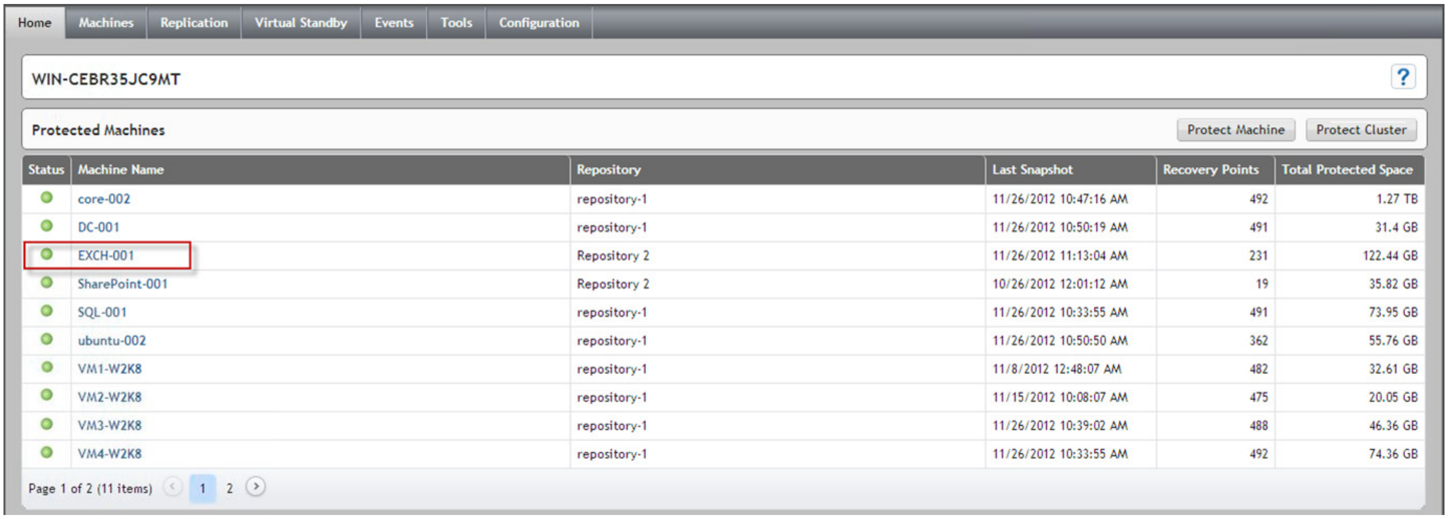
Why read this guide

For most businesses Microsoft Exchange Server is an essential and highly visible business communications tool. In this document we'll show how Dell AppAssure's Live Recovery feature can help your company achieve near-zero Recovery Time Objectives (RTO).

Live Recovery eliminates the need for hours-long Exchange recoveries after a failure. With just a few steps, an Exchange Server administrator can have users sending and receiving emails, and also accessing stored emails, within minutes of a server loss, even if very large amounts of mailbox and message data are being restored.

How to do Live Recovery™ for Microsoft Exchange

To begin a Live Recovery of an Microsoft Exchange server, connect to the Dell AppAssure core server and select your Exchange server.



WIN-CEBR35JC9MT

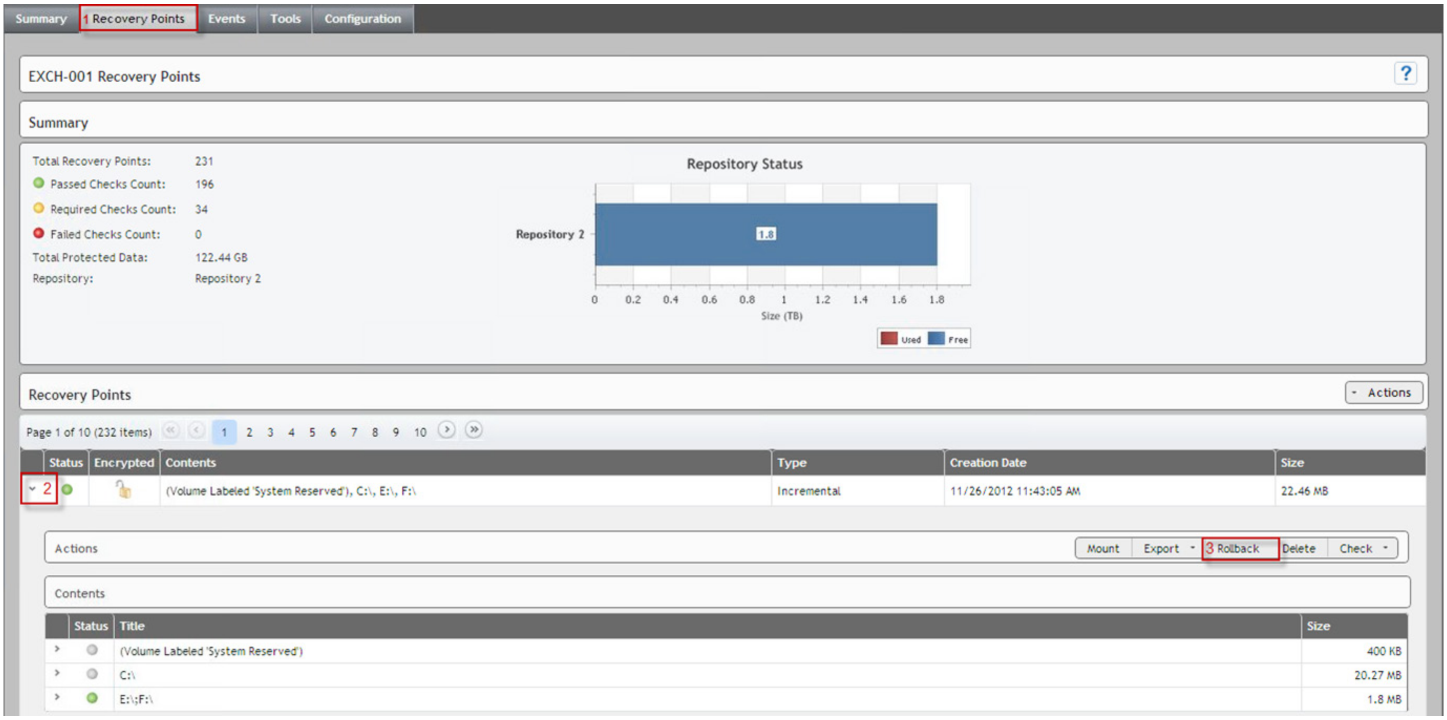
Protected Machines

Status	Machine Name	Repository	Last Snapshot	Recovery Points	Total Protected Space
●	core-002	repository-1	11/26/2012 10:47:16 AM	492	1.27 TB
●	DC-001	repository-1	11/26/2012 10:50:19 AM	491	31.4 GB
●	EXCH-001	Repository 2	11/26/2012 11:13:04 AM	231	122.44 GB
●	SharePoint-001	Repository 2	10/26/2012 12:01:12 AM	19	35.82 GB
●	SQL-001	repository-1	11/26/2012 10:33:55 AM	491	73.95 GB
●	ubuntu-002	repository-1	11/26/2012 10:50:50 AM	362	55.76 GB
●	VM1-W2K8	repository-1	11/8/2012 12:48:07 AM	482	32.61 GB
●	VM2-W2K8	repository-1	11/15/2012 10:08:07 AM	475	20.05 GB
●	VM3-W2K8	repository-1	11/26/2012 10:39:02 AM	488	46.36 GB
●	VM4-W2K8	repository-1	11/26/2012 10:33:55 AM	492	74.36 GB

Page 1 of 2 (11 items) 1 2

Once connected to your Exchange sever, select the "Recovery Point's" tab

- Select a recovery point and expand it by clicking the arrow to the left of the "Status" bubble
- Select "Rollback"



EXCH-001 Recovery Points

Summary

Total Recovery Points:	231
● Passed Checks Count:	196
● Required Checks Count:	34
● Failed Checks Count:	0
Total Protected Data:	122.44 GB
Repository:	Repository 2

Recovery Points

Page 1 of 10 (232 items) 1 2 3 4 5 6 7 8 9 10

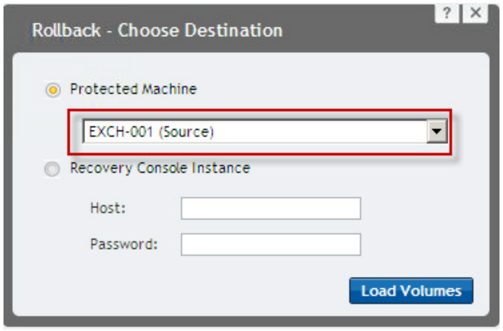
Status	Encrypted	Contents	Type	Creation Date	Size
●		(Volume Labeled 'System Reserved'), C:\, E:\, F:\	Incremental	11/26/2012 11:43:05 AM	22.46 MB

Actions

Contents

Status	Title	Size
●	(Volume Labeled 'System Reserved')	400 KB
●	C:\	20.27 MB
●	E:\;F:\	1.8 MB

- Select the Exchange server under "Protected Machine"
- Click "Load Volumes"



Rollback - Choose Destination

● Protected Machine

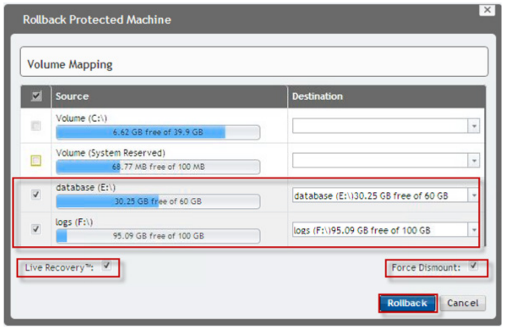
EXCH-001 (Source)

○ Recovery Console Instance

Host:

Password:

- Select the volumes to mount and the destinations to mount them to
- Enable the "Live Recovery" and "Force Dismount" options
- Click "Rollback" when ready



Rollback Protected Machine

Volume Mapping

☑	Source	Destination
□	Volume (C:\) 6.62 GB free of 39.9 GB	
□	Volume (System Reserved) 68.77 MB free of 100 MB	
☑	database (E:\) 30.25 GB free of 60 GB	database (E:\)30.25 GB free of 60 GB
☑	logs (F:\) 95.09 GB free of 100 GB	logs (F:\)95.09 GB free of 100 GB

Live Recovery™: ☑

Force Dismount: ☑

Dell AppAssure Backup, Replication, and Recovery Evaluator's Guide: How to do Bare-Metal Recovery (BMR)

Why read this guide

Bare-Metal Recovery (BMR) provides the ability to restore an entire system back to the original or dissimilar hardware. For example, a physical system can be restored to a virtual or cloud platform, and vice versa. This functionality separates the Operating System from a specific platform, providing portability.

Bare-Metal Recovery is most often used in disaster recovery scenarios or migration projects. This can be used to deploy new hardware in case of disaster, and also facilitate the migration to a public or private cloud.

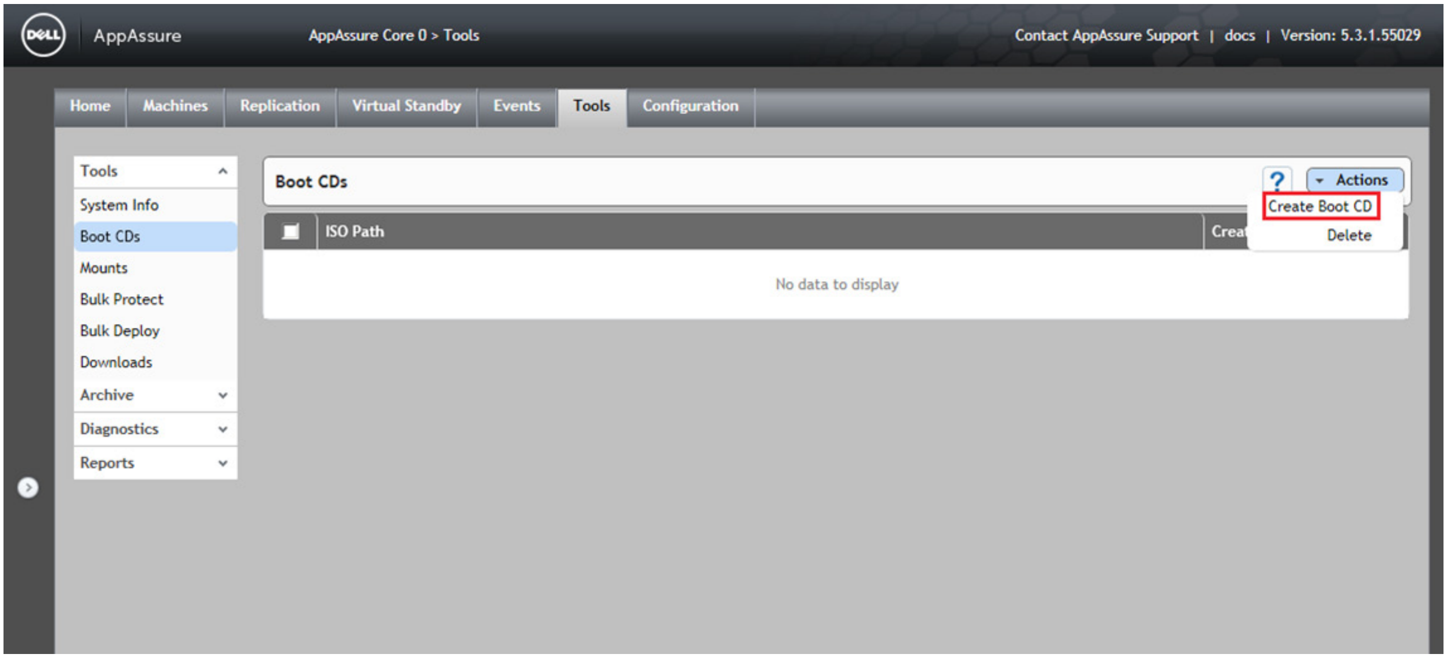
Installation Notes

1. Prepare Target Machine:

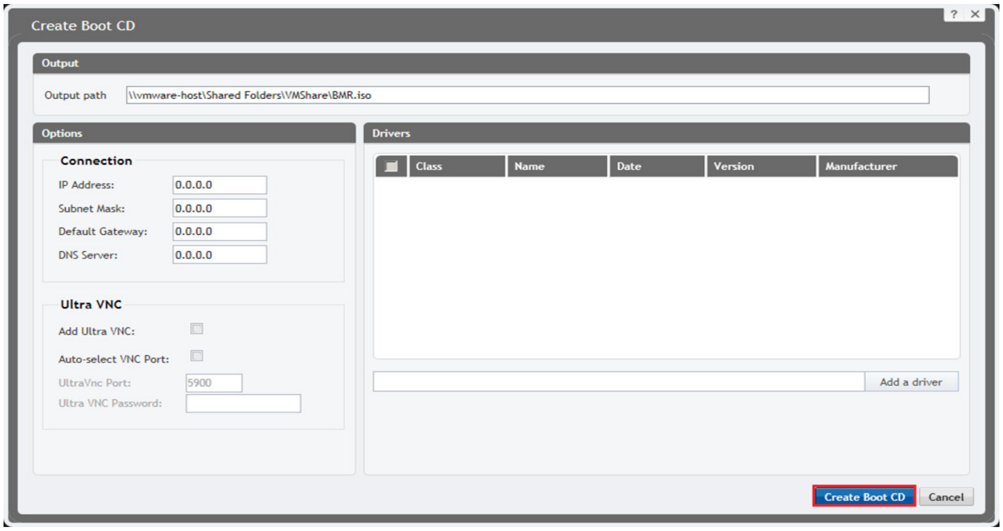
- The Dell AppAssure Boot CD can be created at the "Tools" tab of the Core Server. This will create an ISO CD image based on Microsoft WinPE.
- If restoring to a physical machine, burn the ISO image to a CD or DVD. If restoring to a Virtual Machine (VM) the ISO may be mounted as a virtual CD ROM.
- Once booted, this machine will be ready for the user to connect to it from the Core Server to begin the Bare-Metal Restoration process.

2. Connect to the target server's Boot CD via IP address to start the restore.

To begin creating the Boot CD open the "Tools" tab of Core and select the "Boot CDs" menu. In the Actions menu at the right of the screen select "Create Boot CD"



Enter the desired name of the Boot CD ISO in the Output Path field. To configure this Boot CD to use DHCP, you may leave the default (all zeros) under the "Connections" section; otherwise, enter your desired network configuration. Optionally, you may add Ultra VNC to this Boot CD so that you may remotely connect to it. You may also add custom drivers to this Boot CD via the "Add a driver" section. Press "Create Boot" CD to continue.



Create Boot CD

Output

Output path: \\vmware-host\Shared Folders\VMShare\BMR.iso

Options

Connection

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Ultra VNC

Add Ultra VNC: □

Auto-select VNC Port: □

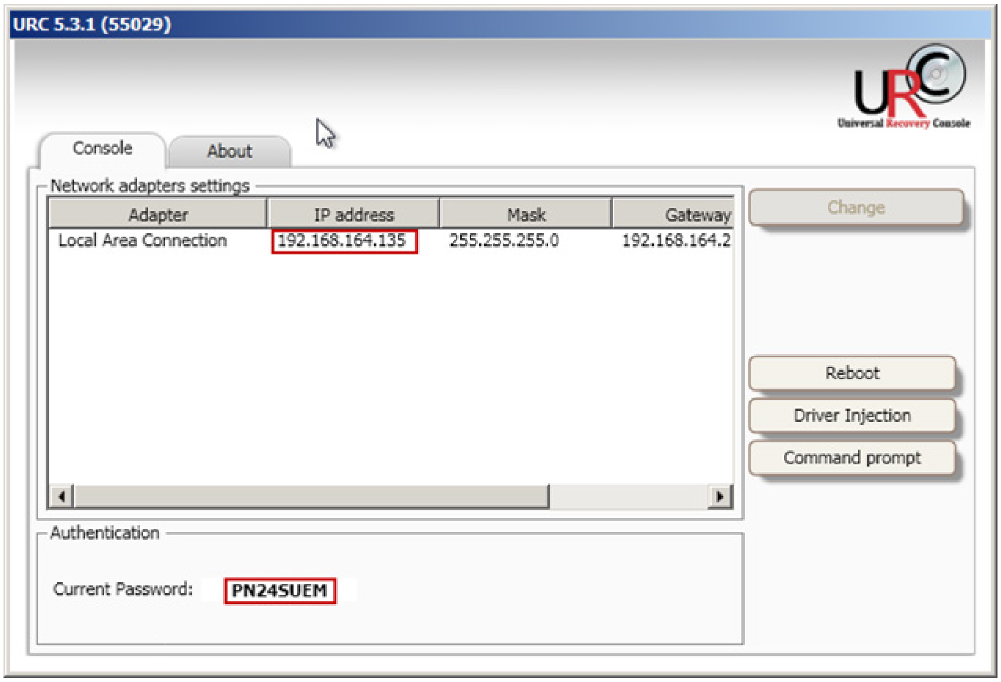
UltraVnc Port: 5900

Ultra VNC Password:

Drivers

□	Class	Name	Date	Version	Manufacturer

Once the machine is booted to the Boot CD the IP and password will be displayed. This information is required by the Core Server in order to begin recovery.



URC 5.3.1 (55029)

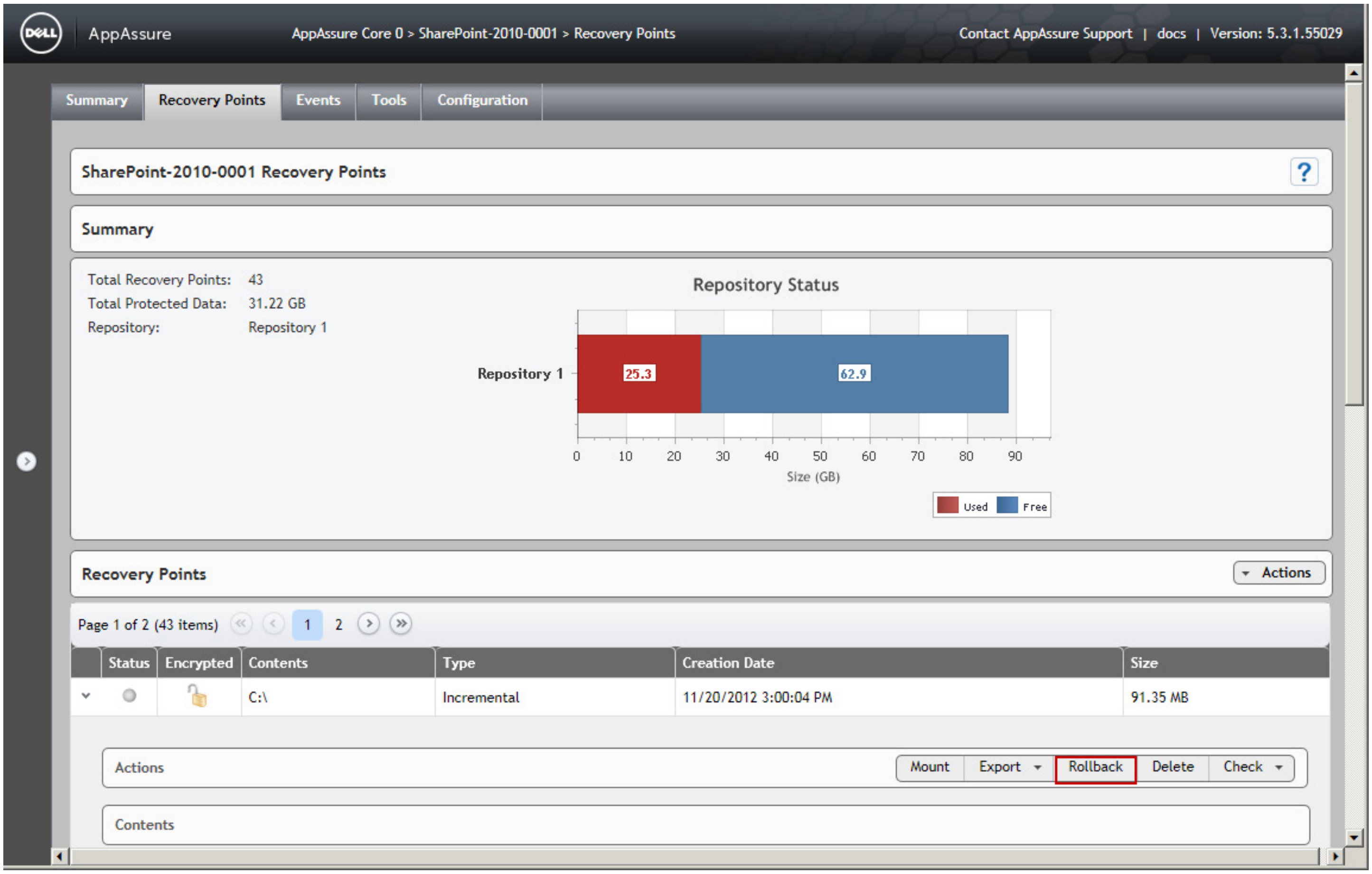
Network adapters settings

Adapter	IP address	Mask	Gateway
Local Area Connection	192.168.164.135	255.255.255.0	192.168.164.2

Authentication

Current Password: PN24SUEM

From the Dell AppAssure Core, browse to the Recovery Point of the Server you wish to restore. Select a Recovery Point and press the “Rollback” button.



SharePoint-2010-0001 Recovery Points

Summary

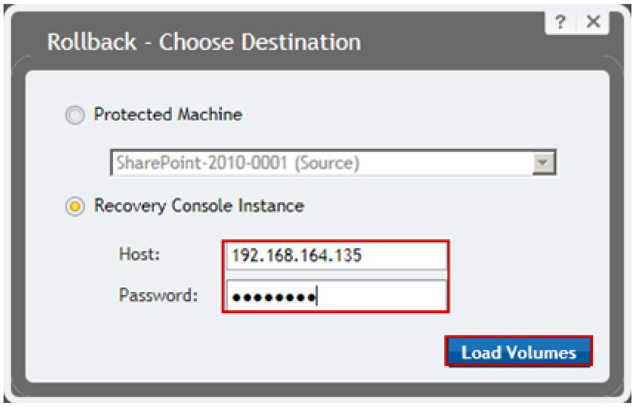
Total Recovery Points: 43
Total Protected Data: 31.22 GB
Repository: Repository 1

Recovery Points

Page 1 of 2 (43 items) 1 2

Status	Encrypted	Contents	Type	Creation Date	Size
○		C:\	Incremental	11/20/2012 3:00:04 PM	91.35 MB

In the pop-up window enter the IP address and password displayed on the Dell AppAssure Boot CD. Press “Load Volumes” when done.



○ Protected Machine

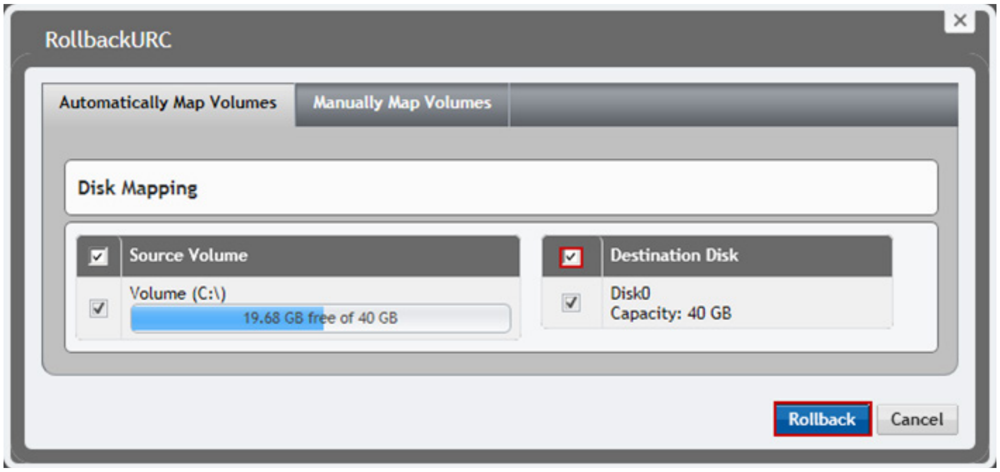
SharePoint-2010-0001 (Source)

● Recovery Console Instance

Host: 192.168.164.135

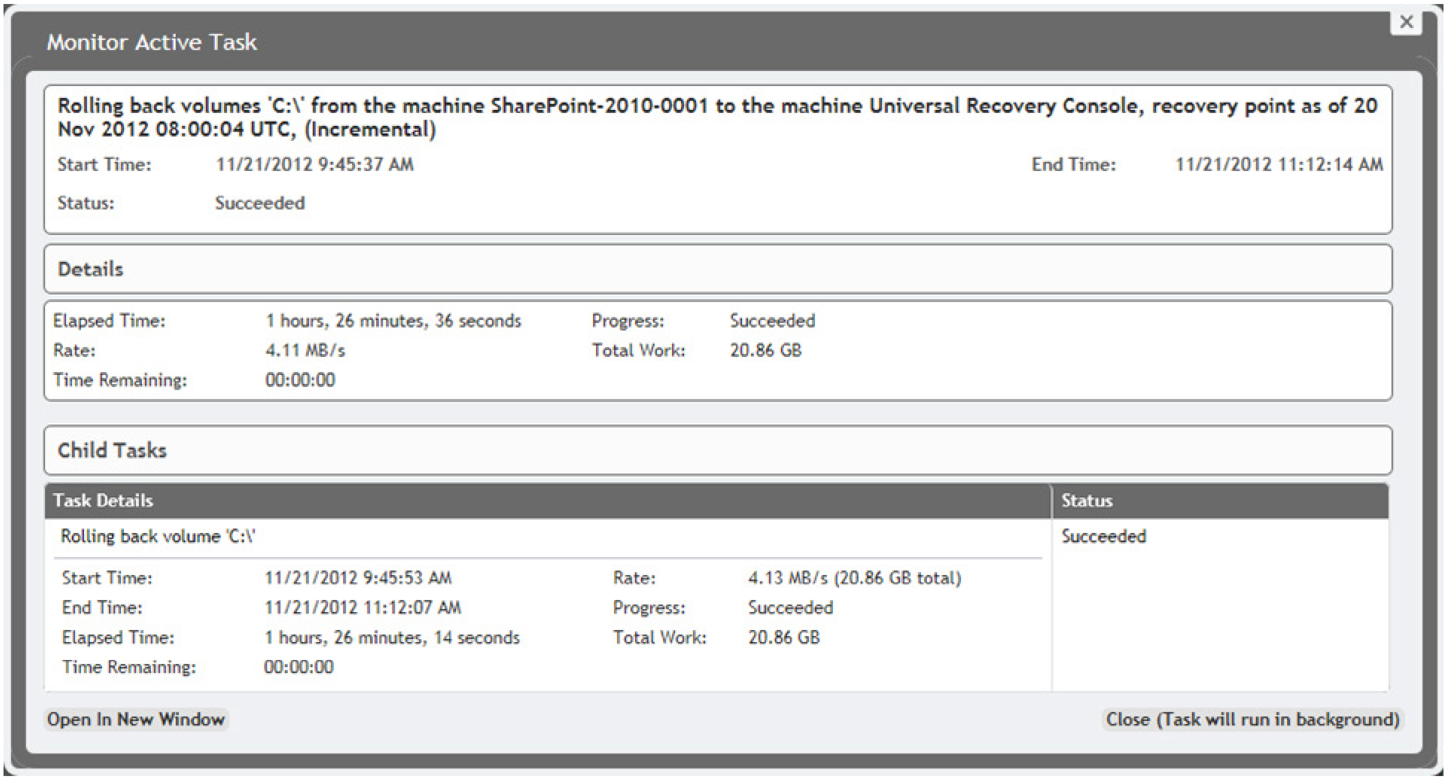
Password: ••••••••

Choose the appropriate Disk Mapping and click “Rollback” to begin the recovery.



	Source Volume		Destination Disk
☑	Volume (C:\) 19.68 GB free of 40 GB	☑	Disk0 Capacity: 40 GB

The summary screen will show statistics and progress of the recovery.



Rolling back volumes 'C:\' from the machine SharePoint-2010-0001 to the machine Universal Recovery Console, recovery point as of 20 Nov 2012 08:00:04 UTC, (Incremental)

Start Time: 11/21/2012 9:45:37 AM
End Time: 11/21/2012 11:12:14 AM
Status: Succeeded

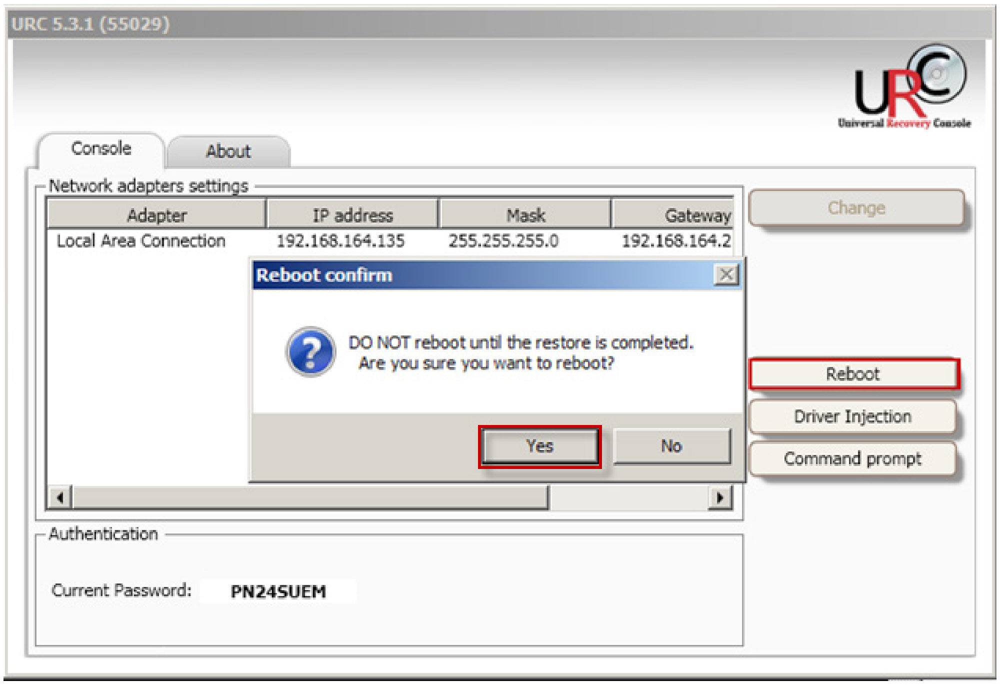
Details

Elapsed Time: 1 hours, 26 minutes, 36 seconds
Progress: Succeeded
Rate: 4.11 MB/s
Total Work: 20.86 GB
Time Remaining: 00:00:00

Child Tasks

Task Details	Status
Rolling back volume 'C:\' Start Time: 11/21/2012 9:45:53 AM End Time: 11/21/2012 11:12:07 AM Elapsed Time: 1 hours, 26 minutes, 14 seconds Time Remaining: 00:00:00 Rate: 4.13 MB/s (20.86 GB total) Progress: Succeeded Total Work: 20.86 GB	Succeeded

Press the “Reboot” button on the target machine and confirm the reboot by clicking the “Yes” button to complete the recovery process.



Adapter	IP address	Mask	Gateway
Local Area Connection	192.168.164.135	255.255.255.0	192.168.164.2

Reboot confirm

DO NOT reboot until the restore is completed.
Are you sure you want to reboot?

Current Password: PN24SUEM

Dell AppAssure Backup, Replication, and Recovery Evaluator's Guide: How to do a file and folder recover

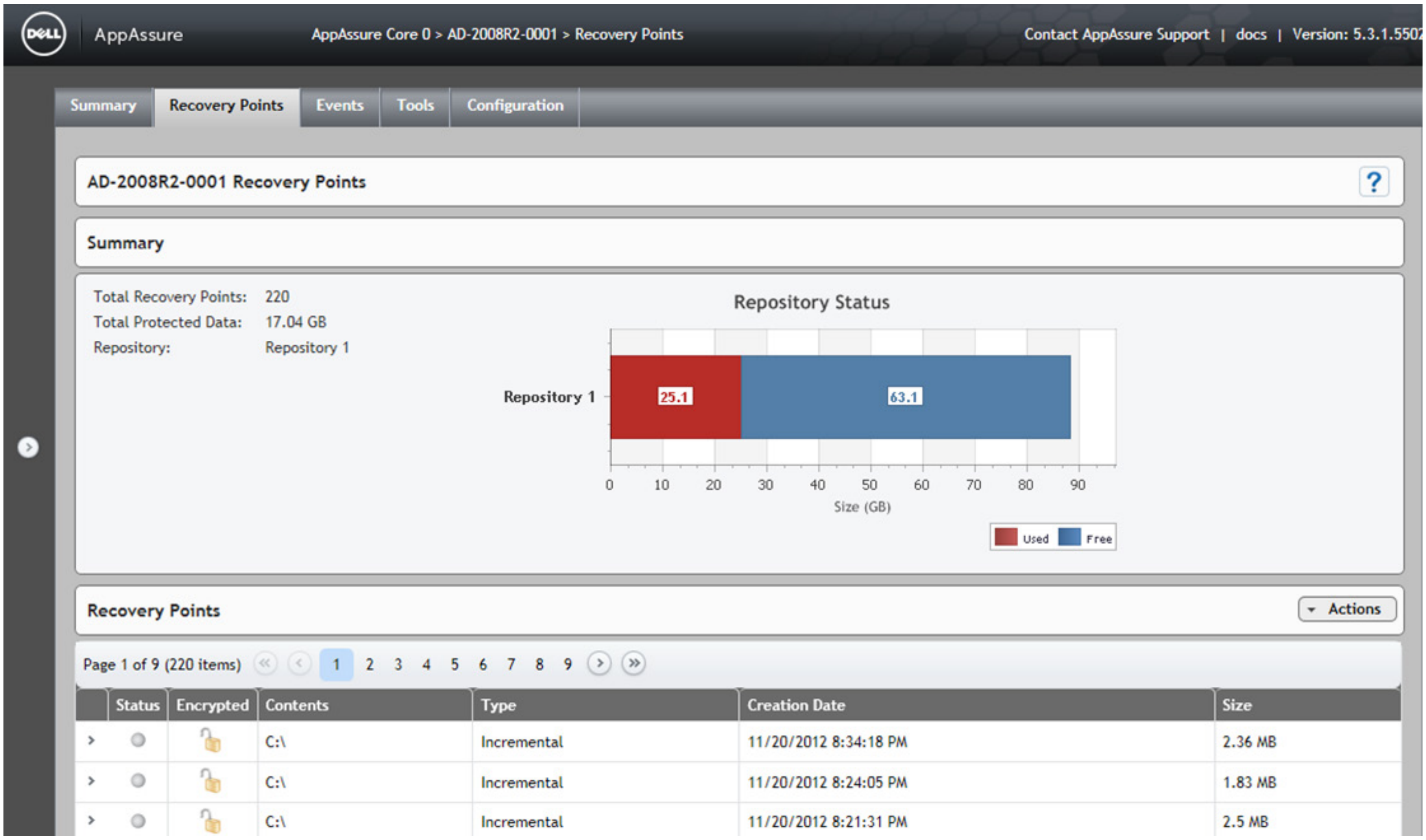
Why read this guide

Recovery Points, also referred to as snapshots (snaps), are backups taken at regular intervals which protect entire machines, their disks, applications, and data. Dell AppAssure allows users to access these Recovery Points using the familiar Windows Explorer interface for recovering files and folders.

Any Recovery Point can be mounted to a directory on the Core server, enabling administrators and users to inspect the data located in the Snapshot using native Windows search tools.

Configuring

Select the machine where the file for recovery was located, and then select the recovery point from that machine to begin.



AD-2008R2-0001 Recovery Points

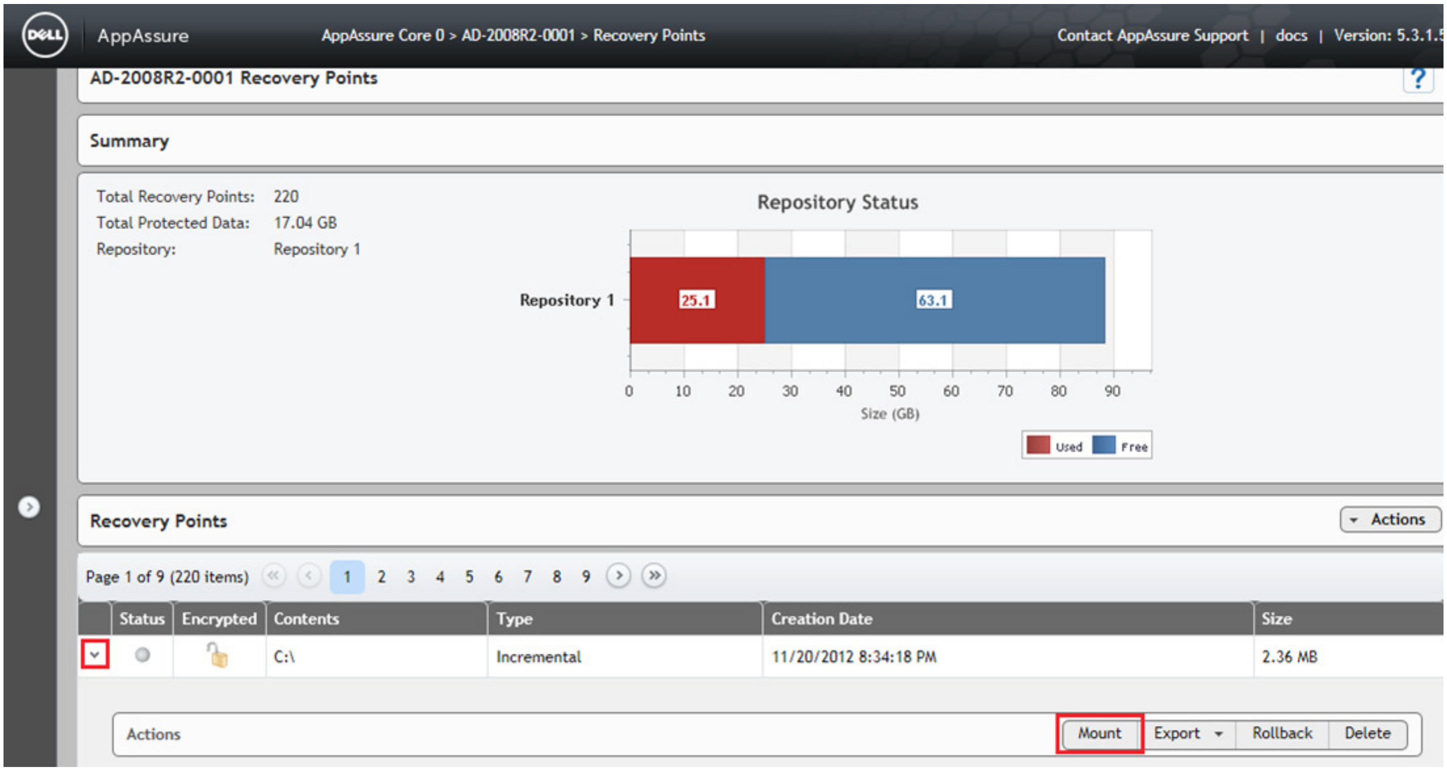
Summary

Total Recovery Points: 220
Total Protected Data: 17.04 GB
Repository: Repository 1

Recovery Points

	Status	Encrypted	Contents	Type	Creation Date	Size
›	○	🔓	C:\	Incremental	11/20/2012 8:34:18 PM	2.36 MB
›	○	🔓	C:\	Incremental	11/20/2012 8:24:05 PM	1.83 MB
›	○	🔓	C:\	Incremental	11/20/2012 8:21:31 PM	2.5 MB

Select the Recovery Point you want to access by clicking the ">" symbol next to the snapshot. It can also be expanded by clicking the ">" symbol. Once the point in time you want to select is chosen click "Mount" on the Action panel.



AD-2008R2-0001 Recovery Points

Summary

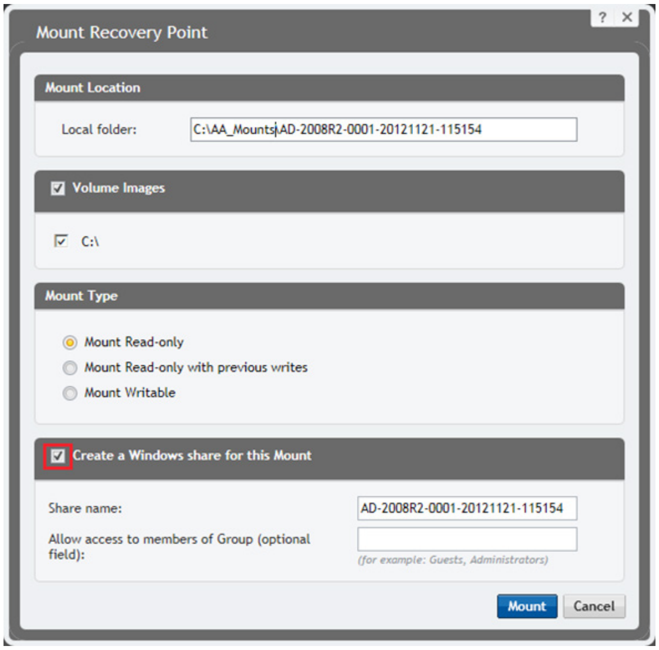
Total Recovery Points:	220
Total Protected Data:	17.04 GB
Repository:	Repository 1

Recovery Points

	Status	Encrypted	Contents	Type	Creation Date	Size
⌄	●		C:\	Incremental	11/20/2012 8:34:18 PM	2.36 MB

Actions

In the pop-up menu, define the location of the mount under "Mount Location", the "Mount Type" and decide whether or not to create a Windows share.
To create a Windows share of this Mount, click the checkbox "Create a Windows share for this mount", name the share, and optionally add groups who can access the share on the network.



Mount Recovery Point

Mount Location

Local folder: C:\AA_Mounts\AD-2008R2-0001-20121121-115154

☑ Volume Images

☑ C:\

Mount Type

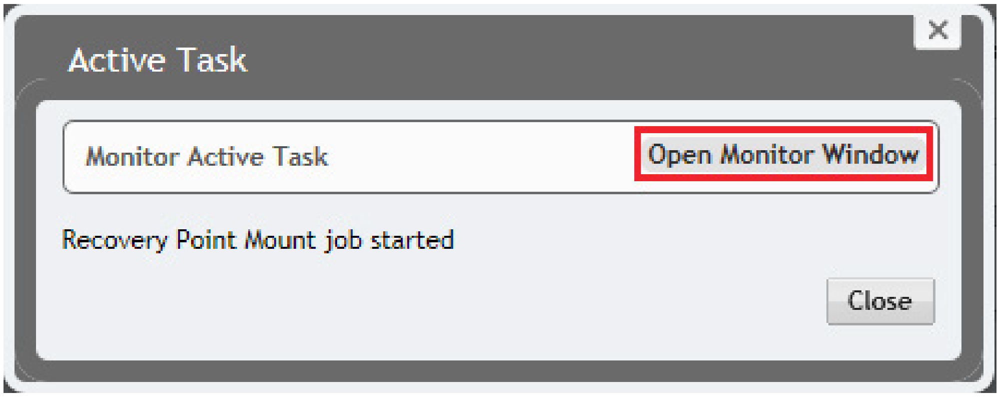
● Mount Read-only
○ Mount Read-only with previous writes
○ Mount Writable

☑ Create a Windows share for this Mount

Share name: AD-2008R2-0001-20121121-115154

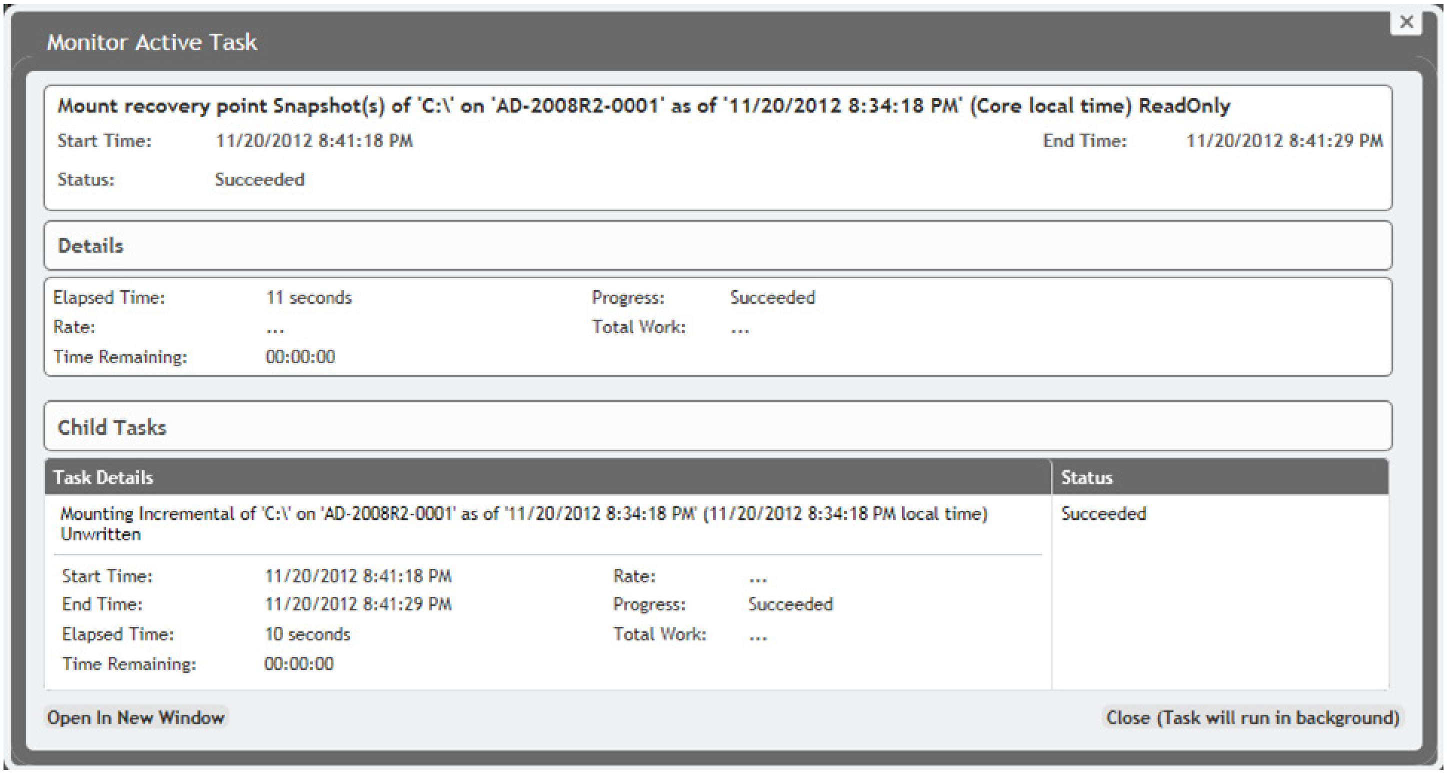
Allow access to members of Group (optional field): *(for example: Guests, Administrators)*

After clicking the “Mount” button, you can click on this pop-up window as shown to monitor the Mount process in the next window.



Recovery Point Mount job started

The Active Task window displays the status of the mount process and indicates when it’s completed successfully.



Mount recovery point Snapshot(s) of 'C:\' on 'AD-2008R2-0001' as of '11/20/2012 8:34:18 PM' (Core local time) ReadOnly

Start Time: 11/20/2012 8:41:18 PM

End Time: 11/20/2012 8:41:29 PM

Status: Succeeded

Details

Elapsed Time: 11 seconds

Progress: Succeeded

Rate: ...

Total Work: ...

Time Remaining: 00:00:00

Child Tasks

Task Details	Status
Mounting Incremental of 'C:\' on 'AD-2008R2-0001' as of '11/20/2012 8:34:18 PM' (11/20/2012 8:34:18 PM local time) Unwritten	Succeeded

Start Time: 11/20/2012 8:41:18 PM

Rate: ...

End Time: 11/20/2012 8:41:29 PM

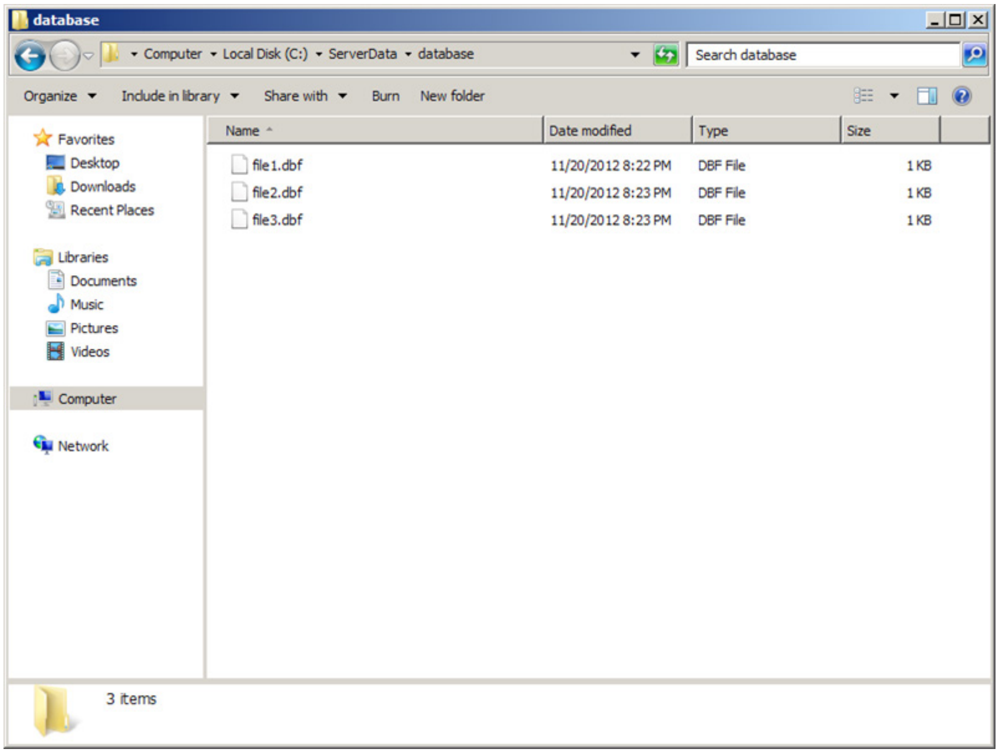
Progress: Succeeded

Elapsed Time: 10 seconds

Total Work: ...

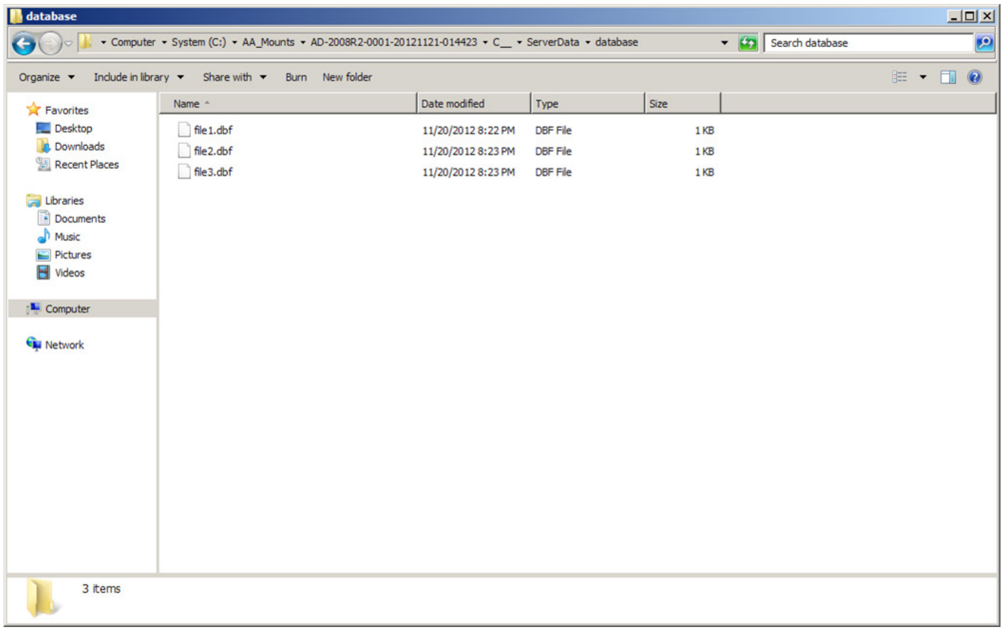
Time Remaining: 00:00:00

Opening Windows Explorer to the Mount location will allow you to browse the Recovery Point contents.



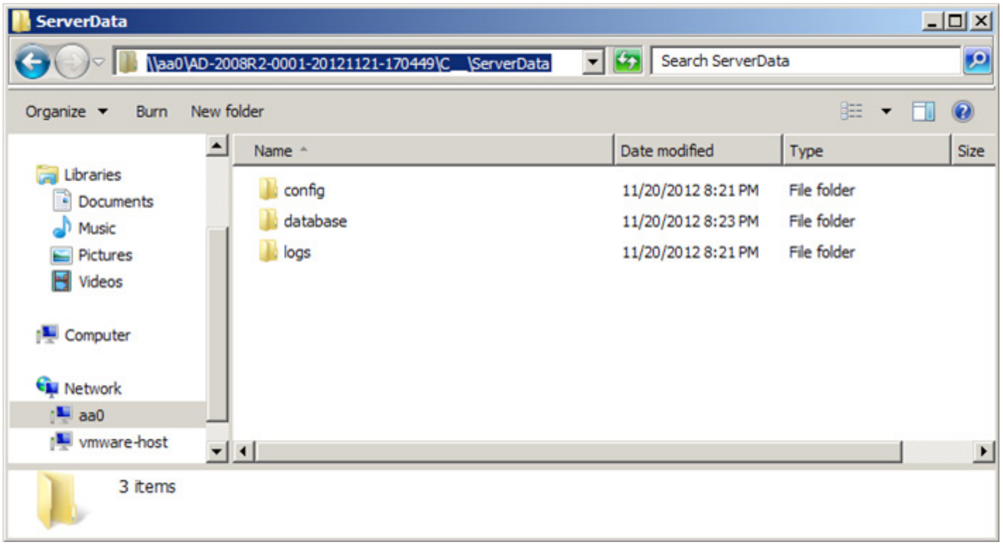
Name	Date modified	Type	Size
file1.dbf	11/20/2012 8:22 PM	DBF File	1 KB
file2.dbf	11/20/2012 8:23 PM	DBF File	1 KB
file3.dbf	11/20/2012 8:23 PM	DBF File	1 KB

Note that all mounts will take the format of: drive_letter\drivename\folder
Explorer is pointed (in this example) to C:\AA_Mounts\AD-2008R2-0001-20121121-014423\C_\ServerData\database



Name	Date modified	Type	Size
file1.dbf	11/20/2012 8:22 PM	DBF File	1 KB
file2.dbf	11/20/2012 8:23 PM	DBF File	1 KB
file3.dbf	11/20/2012 8:23 PM	DBF File	1 KB

The Mount's Windows share is also visible via Windows Explorer over the network.



ServerData

\\aa0\AD-2008R2-0001-20121121-170449\C__\ServerData

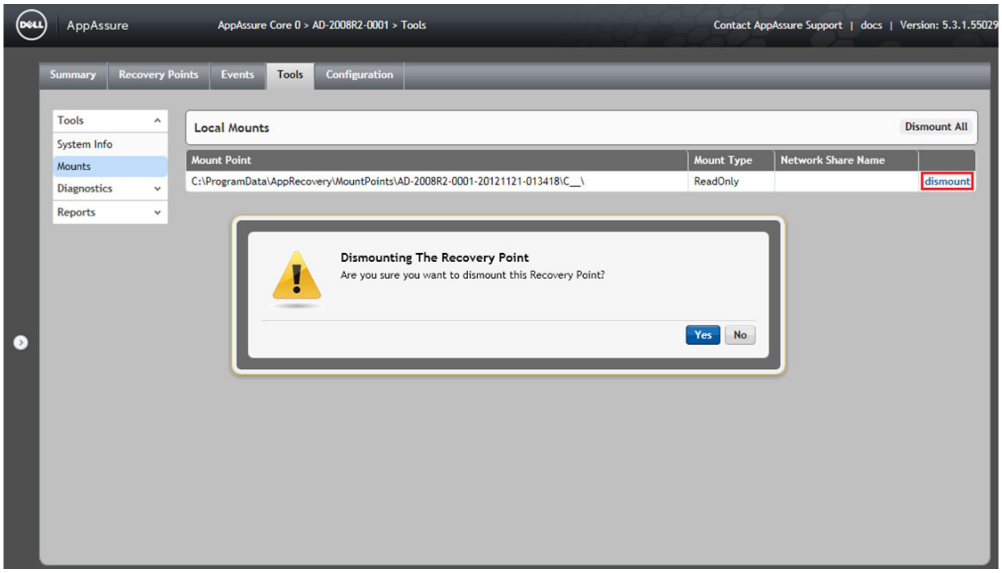
Name	Date modified	Type	Size
config	11/20/2012 8:21 PM	File folder	
database	11/20/2012 8:23 PM	File folder	
logs	11/20/2012 8:21 PM	File folder	

3 items

Mounted Recovery Points remain mounted until an administrator dismounts them via the Core Server by going to Tools > Mounts section.

Here, single or multiple Mounted Recovery Points can be dismounted.

To dismount, select "dismount" and confirm the action.



AppAssure Core 0 > AD-2008R2-0001 > Tools

Local Mounts

Mount Point	Mount Type	Network Share Name	
C:\ProgramData\AppRecovery\MountPoints\AD-2008R2-0001-20121121-013418\C__\	ReadOnly		dismount

Dismounting The Recovery Point

Are you sure you want to dismount this Recovery Point?

It All Boils Down To...

RPO - Recovery Point Objective

How Much Data Are You Willing To Lose?
5 Minute RPO... REALLY!

RTO - Recovery Time Objective

How Much Productivity Time Are You Willing To Lose?
Near ZERO RTO... REALLY!

Resources

Dell AppAssure Documentation, including User Guides
http://docs.appassure.com

Dell AppAssure Customer forum
http://forum.appassure.com

Sales and Pricing Information
www.appassure.com
sales@appassure.com

Twitter: @AppAssure
Facebook: http://www.facebook.com/appassure