Backup and Recovery Options for Microsoft Exchange, Lync, and SharePoint Server 2013 on Dell PowerEdge VRTX Using Dell PowerVault DL4000

A Dell technical white paper
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2014</td>
<td>Initial release</td>
</tr>
</tbody>
</table>

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2014 Dell Inc. All Rights Reserved. Dell, the Dell logo, PowerEdge, PowerVault, OpenManage, AppAssure, and other Dell names and marks are trademarks of Dell Inc. in the US and worldwide. Microsoft, Windows, SharePoint, Lync, Hyper-V, SQL Server, Active Directory and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware, vCenter, and Workstation are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. All other trademarks mentioned herein are the property of their respective owners.
Table of Contents

Revision History .................................................................................................................. 2
Acknowledgements ............................................................................................................. 5
1 Executive summary ........................................................................................................... 6
   1.1 Scope ..................................................................................................................... 7
   1.2 Audience ............................................................................................................... 7
2 Solution architecture ....................................................................................................... 8
   2.1 Overview of PowerEdge VRTX ........................................................................... 8
   2.2 Overview of PowerVault DL4000 ....................................................................... 10
      2.2.1 Overview of AppAssure 5 ........................................................................... 12
3 Design considerations for UC&C data protection ......................................................... 14
   3.1 SQL Server data protection considerations ......................................................... 14
   3.2 Exchange Server data protection considerations ................................................. 14
   3.3 Application-aware data protection ...................................................................... 14
   3.4 Infrastructure protection for application services ................................................. 15
4 Protecting UC&C applications using PowerVault DL4000 ........................................... 16
   4.1 AppAssure application-aware agents ................................................................ 17
   4.2 Backup configurations and retention policy ....................................................... 17
   4.3 AppAssure snapshot process for Windows applications ..................................... 18
   4.4 AppAssure Recovery Assure ............................................................................. 19
5 How to recover UC&C application hosts and data using PowerVault DL4000 .......... 21
   5.1 Object-level granular recovery ........................................................................... 21
      5.1.1 Granular recovery of Microsoft Exchange 2013 .......................................... 21
      5.1.2 Granular recovery of Microsoft SharePoint 2013 ....................................... 23
   5.2 Application host volume level in-place recovery ................................................. 25
   5.3 Application host out-of-place recovery to a virtual server .................................. 27
   5.4 Application host out-of-place recovery to a physical server ............................... 30
6 Bare Metal Recovery of a VRTX Server node ............................................................... 33
   6.1 Lifecycle Controller server configuration export and import ............................. 33
   6.2 AppAssure protecting PowerEdge VRTX Server nodes .................................... 34
7 Replication of UC&C application for disaster recovery using PowerVault DL4000 ..... 36
7.1 AppAssure replication capabilities ........................................................................................................... 36
7.1.1 Replication modes ..................................................................................................................................... 36
7.1.2 Replication through seeding ..................................................................................................................... 36
7.1.3 Replication performance considerations .................................................................................................. 37
7.2 Replication of UC&C application services .................................................................................................. 37
7.3 Dealing with UC&C application services failure at onsite location ............................................................ 38
8 Solution summary ........................................................................................................................................... 39
A Additional Resources ........................................................................................................................................ 40
Acknowledgements

This technical white paper was developed by the following members of the Dell Global Solutions Engineering team:

- Engineering: Ravikanth Chaganti, Dharmesh Patel, Rizwan Ali, and Jenwei Hsieh
- Additional contributors: Paul Robichaux, Sean Douglas, and Hans Heilpern
1 Executive summary

The Dell™ PowerEdge™ VRTX shared infrastructure platform enables IT administrators to combine servers, storage, and networking into an easy-to-deploy chassis. Engineers at Dell Global Solutions Engineering have developed a novel architecture for running virtualized workloads using Microsoft® Hyper-V® on PowerEdge VRTX. On this shared virtualized infrastructure, the Microsoft Unified Communication and Collaboration (UC&C) solution (Microsoft Exchange, Lync®, and SharePoint® Servers) provides organizations with productivity tools, such as email, instant messaging, document sharing, and web conferencing.

This white paper focuses on data protection and recovery of the UC&C solution and is a follow-up to Microsoft Exchange, Lync and SharePoint Server 2013 on Dell PowerEdge VRTX with Microsoft Server 2012 Hyper-V. This paper discusses best practices and requirements of the Microsoft UC&C solution and how the Dell PowerVault™ DL4000 appliance running the Dell AppAssure™ software bundle addresses these requirements. Using Dell AppAssure Universal Recovery, application services can be resumed in minutes, reducing Recovery Time Objective (RTO) from hours to seconds. Additionally, incremental backups with inbuilt deduplication/compression technology provide Recovery Point Objective (RPO) of around 5 minutes.

Employing a complete application-aware backup is critical to the overall solution. AppAssure provides the following types of recovery mechanisms:

- Automatic recovery assurance of each backup
- Object level granular recovery of Exchange and SharePoint applications
- Application Virtual Machine (VM) in-place recovery of individual volumes
- Application VM out-of-place recovery through exporting application VM backups to:
  - Another virtual infrastructure (VMware® ESXi™, Microsoft Hyper-V) to run it as a VM
  - Physical server
  - Hyper-V infrastructure running on PowerVault DL4000
- Bare Metal Recovery (BMR) of a server node within the PowerEdge VRTX chassis
- Replication of application backups to:
  - PowerVault DL4000 at a remote site
  - AppAssure Core running in the cloud

The following is a high-level overview of the various sections in the white paper:

- Section 2: Introduces the key components used in this white paper, namely PowerEdge VRTX, PowerVault DL4000, and AppAssure software.
- Section 3: Describes design considerations and discusses best practices and requirements for protecting the UC&C applications.
- Section 4: Describes AppAssure backup capabilities that meet Microsoft best practices and requirements to protect the UC&C applications data by using PowerVault DL4000.
- Section 5: Describes AppAssure recovery capabilities ranging from individual object-level granular recovery to UC&C application host volume-level recovery to complete VM-level recovery of a VM or a physical server.
- Section 6: Describes AppAssure replication capabilities that allow a seamless replacement of a failed PowerEdge M620 server in a PowerEdge VRTX chassis.
1.1 Scope

The reference implementation of Microsoft UC&C applications is architected to enable small and medium-sized businesses (SMBs) to take advantage of the virtualized infrastructure on PowerEdge VRTX. SMB customers have the same application service uptime requirements as larger organizations, but cannot afford expensive onsite and offsite data protection solutions for their infrastructure. Any downtime due to failures in the UC&C application VMs, PowerEdge M620 servers, or the entire PowerEdge VRTX chassis can be disruptive to their business Service Level Agreements (SLAs).

This white paper discusses the data protection features offered by PowerVault DL4000 running AppAssure Data Protection software and describes how these features help in backup and recovery of the Microsoft UC&C applications. This white paper also describes the overall architecture of the data protection solution. The Microsoft UC&C application architecture on PowerEdge VRTX is detailed in an earlier reference implementation "Microsoft Exchange, Lync and SharePoint Server 2013 on Dell PowerEdge VRTX with Microsoft Server 2012 Hyper-V".

1.2 Audience

This white paper is intended for IT professionals and administrators who have deployed or are planning to deploy a Microsoft UC&C solution for up to 500 users on PowerEdge VRTX with PowerVault DL4000 appliance.

This white paper provides an overview of the solution components such as PowerEdge VRTX and PowerVault DL4000. However, the reader is expected to have sufficient understanding of Hyper-V, Exchange 2013, Lync 2013, SharePoint 2013, and PowerVault DL4000.
2 Solution architecture

The backup and recovery architecture using PowerVault DL4000 is based on Microsoft Exchange, Lync and SharePoint Server 2013 on Dell PowerEdge VRTX with Microsoft Server 2012 Hyper-V solution architecture. Figure 1 shows a high-level view of the solution architecture and its components.

2.1 Overview of PowerEdge VRTX

PowerEdge VRTX is a shared infrastructure platform that combines server, storage, and networking into an easy-to-deploy, modular chassis. The platform is designed to address and resolve IT concerns of SMBs. PowerEdge VRTX addresses the needs of virtualized workloads and projected storage capacity and performance.
PowerEdge VRTX uses I/O cards in the PCIe industry-standard format to provide shared storage of up to 48 TB in the 3.5-inch HDD bay chassis. The storage can be shared among four server nodes and managed through the PowerEdge VRTX Chassis Management Controller (CMC). Using CMC, virtual disks can be created and assigned to single or multiple server nodes (The virtual disks can be created and assigned to multiple server nodes only if clustering-aware software is installed.) The CMC web console can also be used to assign the PCIe slots to server nodes. Up to four PCIe slots can be assigned to a single server node. These mappings can be reassigned later, but the servers involved in the reassignment would need to be power cycled.
### Table 1 Overview of PowerEdge VRTX Infrastructure

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Compatibility</td>
<td>PowerEdge M520/PowerEdge M620/PowerEdge M820 servers</td>
</tr>
<tr>
<td>Form Factor</td>
<td>Stand-alone tower or 5U rack enclosure</td>
</tr>
<tr>
<td>Number of Servers</td>
<td>Up to 4 PowerEdge M520/M620 servers or Up to 2 PowerEdge M820 servers</td>
</tr>
<tr>
<td>I/O Cards</td>
<td>8 PCIe slots (supporting Ethernet, FC, GPU)</td>
</tr>
<tr>
<td>Power Supplies</td>
<td>Up to 4 PSUs (PSU and AC redundant options)</td>
</tr>
<tr>
<td>Chassis Storage</td>
<td>Up to twelve 3.5-inch NL-SAS, SAS HDDs/SSDs or Up to twenty five 2.5-inch NL-SAS, SAS HDDs/SSDs</td>
</tr>
<tr>
<td>Raid Controller</td>
<td>Shared PowerEdge Raid Controller (PERC 8; Entry Shared(^1) PERC or Fault Tolerant PERC)</td>
</tr>
<tr>
<td>Management</td>
<td>1 or 2 Chassis Management Controllers</td>
</tr>
<tr>
<td>Network</td>
<td>1 GbE pass-through module or 1 GbE internal switch module (8 external ports)</td>
</tr>
<tr>
<td></td>
<td>10 GbE internal switch module (8 external ports)</td>
</tr>
</tbody>
</table>

For more information on PowerEdge VRTX, see [Microsoft Exchange, Lync and SharePoint Server 2013 on Dell PowerEdge VRTX with Microsoft Server 2012 Hyper-V solution architecture](#)

## 2.2 Overview of PowerVault DL4000

Powered by the AppAssure software, PowerVault DL4000 is a fully configured 1U backup appliance that integrates 5.5 TB (expandable up to 85 TB) of storage capacity with snapshot, replication, deduplication, and compression software to quickly recover applications and data.

PowerVault DL4000 includes the following hardware and software:

- PowerVault DL4000 1U system
- PowerEdge RAID Controllers (PERC)
- Optional (up to two) PowerVault MD1200 2U storage enclosure

\(^1\) The reference architecture uses an Entry Shared PERC 8 controller.
• Preinstalled Windows Server® 2012 operating system and Dell OpenManage™ system and storage management software
• AppAssure 5 software

PowerVault DL4000 offers the following benefits:

• Eliminates the need for hardware sizing and backup software configuration. The DL4000 appliance is offered in Standard and High-capacity editions.
• Comes preinstalled with AppAssure software bundle (AppAssure Core, AppAssure Central Management Console, AppAssure Local Mount Utility, AppAssure backup agent, Appliance Configuration Wizard) with OpenManage and iDRAC7 Enterprise for remote management of the PowerVault DL4000 appliance.
• Enables business continuity by running virtual standby machines to quickly restore critical application services from the latest snapshot.

PowerVault DL4000 is available in Standard and High-capacity editions that scale from 5.5 TB to 85 TB in backup storage capacity with higher processing, memory, and networking power. See the Dell PowerVault DL4000 Owner’s Manual at dell.com/support/manuals for details about each configuration.

As shown in Figure 3, the operating system of the appliance resides on a RAID 1 (mirrored) virtual disk created by using the first two lower capacity drives. The AppAssure backup and virtual standby repository is auto-provisioned as a RAID 6 virtual disk on the remaining eight higher capacity drives.

![PowerVault DL4000 Disk Configuration](image)

**Figure 3** PowerVault DL4000 disk configuration

The backup and virtual standby repository can be expanded up to 85 TB in size with up to two PowerVault MD1200 storage enclosures attached to the PowerVault DL4000 system externally.

2.2.1 Overview of AppAssure 5

PowerVault DL4000 is preinstalled and configured to run the AppAssure 5 backup and recovery software. AppAssure 5 offers unified data protection by combining backup, replication, and recovery in a single solution that is engineered to protect VMs, physical machines, and cloud environments. AppAssure 5 also provides application awareness to ensure reliable application data and item-level recovery from your backups. AppAssure 5 delivers fast backup performance with aggressive near-zero RTO and RPO.

AppAssure 5 combines the following unique and innovative core technologies and major features:

- **Live Recovery**: Provides near-continuous access to data volumes on virtual or physical servers. The Live Recovery feature enables recovery of an entire volume with near-zero RTO and RPO within minutes. Services running on a server can be resumed directly from the backup file without waiting for a full restore to production storage.

- **Recovery Assure**: Performs automated recovery testing and verification of backups of file systems and applications data (Microsoft Exchange/Microsoft SQL Server®). It features a comprehensive integrity-checking algorithm that identifies data corruption early and prevents corrupted data blocks from being maintained or transferred during the backup process.

- **Universal Recovery**: Provides unlimited machine restoration flexibility—physical-to-virtual (P2V), virtual-to-virtual (V2V), virtual-to-physical (V2P), physical-to-physical (P2P)—and performs bare metal restores to dissimilar hardware. It accelerates cross-platform movements among virtual machines, that is, moving from VMware to Hyper-V and Hyper-V to VMware. Universal Recovery also supports recovering or exporting physical or virtual servers to cloud.

- **True Global Deduplication**: Reduces physical disk capacity requirements through block-level compression and target-based inline deduplication with forever incremental block-level backups. Built-in integrity checking prevents data corruption from affecting the quality of the backup and the archiving process.

- **Repository**: Uses Deduplication Volume Manager (DVM) to support multiple volumes, each of which can reside on different storage technologies such as DAS, SAN, NAS, or cloud. Each volume consists of a scalable object store that is deduplication enabled. DVM can combine a set of object stores into a volume that can be expanded by creating additional file systems.

- **Encryption**: Provides integrated encryption to protect backups and data-at-rest from unauthorized access and use, thereby ensuring data privacy. Encryption is performed inline on snapshot data at line speeds without affecting performance.

- **Replication**: Copies recovery points (snapshots) from a primary location and transmits them to a secondary location (AppAssure Core server) for disaster recovery. The replication process requires a paired source-target relationship between two core servers. This replication target core server could be located in a co-location data center, in a remote disaster recovery site, or in the cloud.
• **Retention and Archiving**: Customizes policies to specify the duration to maintain a backup recovery point. At the end of the retention period, the recovery points are removed from the retention pool. This process becomes inefficient and eventually fails when the amount of data and the period of retention grow rapidly. AppAssure 5 solves this problem by managing the retention of large amounts of data with complex retention policies and performing rollup operations for aging data using efficient metadata operations.

In AppAssure 5, the archive is internally optimized, and all data in the archive is compressed, encrypted, deduplicated, and rendered backward compatible with older AppAssure Core services.

For more information on the features, see AppAssure 5 User Guide.

AppAssure 5 offers the following tools to perform granular object-level recoveries for Microsoft Exchange 2013 and Microsoft SharePoint 2013 applications:

• **Local Mount Utility (LMU)**: Enables mounting a recovery point from a remote AppAssure 5 Core to the local server. When LMU runs on a Core, applications (such as Exchange, SharePoint, and SQL Server) recognize and display all mounts from that Core, including mounts performed through the AppAssure 5 Core Console.

• **Mailbox Restore for Exchange**: Works with AppAssure 5 Core and AppAssure 5 Local Mount Utility (LMU) to recover Exchange items from a full data store to an email message. The Exchange item is recovered from an AppAssure 5 recovery point. When AppAssure 5 Agent is installed on an Exchange Server and the Server is protected with an AppAssure 5 Core, the Exchange items stored on that Server can be recovered by using Mailbox Restore.

• **DocRetriever for SharePoint**: Enables recovery and restore SharePoint objects from the site collection level to the component level. Using DocRetriever, all the documents and objects within a SharePoint farm, site, and site hierarchy can be browsed directly (with intact permissions) from a backup. Objects can then be restored from the site collection to their original locations in the production SharePoint Server environment, any other location within the live SharePoint Server, or a file system. This can be performed without rebuilding the entire production database or using a SharePoint recovery farm.
3 Design considerations for UC&C data protection

Each enterprise application stores data in a format that is best suited for the application architecture and data retrieval requirements. For example, SharePoint Server stores all user data as a Binary Large Object (BLOB) in a SQL Server database. Similarly, Lync Server stores User Presence and Archiving and Monitoring data in a SQL Server database. The Exchange Server stores the mailbox data in a proprietary Jet database architecture.

3.1 SQL Server data protection considerations

Applications such as SharePoint and Lync depend on SQL Server database services to store the application data. Existing techniques such as mirroring and log shipping protect the SQL Server data during a SQL Server failure. The data is copied to a secondary server or another location. In an SMB usage scenario, building a highly available SQL Server database solution is not cost effective. Therefore, the data protection solution must support features such as disk-based, block-level backups and data deduplication. Additionally, the solution must provide near-continuous or continuous protection of application data.

3.2 Exchange Server data protection considerations

Using the Database Availability Group (DAG) architecture based deployments, the mailbox data in an active Exchange database is replicated to a passive copy of the database. In the event of a Mailbox server failure, the passive copy is activated to provide mailbox connectivity to end users. However, using a secondary server for protecting data means more investment for an SMB. Hence, when there is a single Mailbox role deployed to provide messaging services to end users, a data protection solution must be implemented to protect the mailbox data.

Starting with Exchange 2010, the built-in Single Instance Storage (SIS) feature of the Exchange database is removed². Hence, it is now necessary to look for an external deduplication solution to reduce the on-disk footprint of Exchange database backups.

3.3 Application-aware data protection

This feature enables creation of application-consistent point-in-time data snapshots. The application-aware data protection solution must be able to detect all the data stores being used by the application and automatically enable protection for them. This allows quick recovery of the application data and services in the event of a failure.

²Exchange 2010 and SIS (Exchange Team Blog)
It is also necessary to have item-level recovery for the application data. This enables restoring a single item from the backup instead of restoring the entire backup set.

3.4 Infrastructure protection for application services

In a virtualized infrastructure where the application services run as virtual machines, it is necessary to protect the virtual machines and not just the data stored in the virtual machines. The data protection solution must protect the Guest Operating System in the virtual machines as well as the application services and data. It should also protect the platform that hosts the virtual machines to enable quick recovery of virtual infrastructure from a failure event.
4 Protecting UC&C applications using PowerVault DL4000

PowerVault DL4000 provides complete application-aware backup and recovery of the Microsoft UC&C application services to meet aggressive RPO and RTO objectives. The AppAssure software is well suited for Microsoft UC&C application data protection because it offers an advanced data protection capability that unifies backup, recovery, and replication in a single software solution.

The Hyper-V Failover Cluster Service is configured to provide seamless application Virtual Machine (VM) migrations across different physical servers within the PowerEdge VRTX chassis. This ensures high availability of the servers (PowerEdge M620 servers) within a PowerEdge VRTX. At the physical disk level, redundancy is achieved by configuring RAID volumes across the physical hosts’ internal hard disks as well as across the PowerEdge VRTX shared storage.

The following data protection and recovery capabilities of PowerVault DL4000 provide quicker RTO and shorter RPO:

- **Application-aware AppAssure backup agents running on Microsoft UC&C Applications hosts** — provide automated backup configurations and recovery assurance through integrity, checksum, mountability, and attachability checks for each backup.
- **Object-level granular recovery tools for Microsoft UC&C applications** —
  - AppAssure Local Mount Utility and Dell Mailbox Restore tools enable granular recovery of Exchange 2013 application data objects in case of accidental deletion or corruption of individual objects, such as an email, a folder, or a mailbox.
  - AppAssure Local Mount Utility and DocRetriever tools enable granular recovery of SharePoint 2013 application data objects to retrieve an individual document, an item list, or a library in case of accidental deletion or corruption.
- **Individual volume level in-place recovery** — Enables individual volume level in-place recovery of all application hosts in case of application or data corruption within application VMs.
- **Application host out-of-place recovery** — Enables application host out-of-place recovery in the form of a virtual or a physical server in case of corruption at OS, application or data volume level, or in case of hardware failure within PowerEdge VRTX. A Hyper-V infrastructure running on PowerVault DL4000 appliance can be used to perform a live recovery of UC&C application VMs, thus considerably reducing the RTO.
- **PowerEdge VRTX Server Node Bare Metal Recovery (BMR) facility** — Protects PowerEdge VRTX server (M620) nodes by installing AppAssure agents and allows replacement or upgrade of a server node within PowerEdge VRTX. The Dell Lifecycle Controller server configuration export/import facility coupled with PowerEdge VRTX server node restore from AppAssure backup allows it to join the Hyper-V Failover Cluster seamlessly, a key to aggressive RTO even in case of a hardware level server node failure within PowerEdge VRTX.
- **Replicating PowerVault DL4000 to a DR Series, a co-location site PowerVault DL4000 or an AppAssure Core running in public cloud** — Addresses UC&C application services availability concerns in case of onsite hardware or network failures.
4.1 AppAssure application-aware agents

By using the AppAssure agent on UC&C application VMs, the VM, the installed applications, application configurations and data are protected. It also enables object-level granular recovery for Exchange and SharePoint applications.

AppAssure Core Console running on PowerVault DL4000 supports agent installation remotely on a machine or cluster, or bulk installation by connecting to an Active Directory or VMware vCenter/ESXi host.

Upon installation, the application-aware agents automatically verify the Exchange and SQL Server metadata to identify database and logs mount points (E:\, F:\, and G:\ as shown in Figure 4 for the Exchange host) and combine those volumes together as a single Protection Group. Therefore, AppAssure can create recovery points (snapshots) of the volumes simultaneously. The AppAssure agents installed on SharePoint, Lync, and Office Web Apps Server (OWS) application VMs are treated as generic OS-level backup agents, without any specific application-level configurations.

Figure 4  AppAssure protection group settings for Microsoft Exchange VM

4.2 Backup configurations and retention policy

After the AppAssure agent is installed on the application VMs, the default auto backup policy takes snapshots every 60 minutes. However, based on the application workload performance requirements and
business RPOs, the snapshot frequency for each protected application VM can be reduced to five minutes. All volumes of the host may be configured on a different snapshot schedule as required.

Immediately after deployment, the AppAssure agent automatically creates the first snapshot. AppAssure performs a full backup for the first snapshot and then performs continuous incremental backups as shown in Figure 5. Dell recommends installing the agent and performing the first backup when less application activity is expected.

![Figure 5](image)

**AppAssure forever incremental recovery points for Microsoft Exchange VM**

If the business requires retention of backup snapshots for longer periods, the retention periods can be modified. Rollup of aging recovery points are auto configured and can be performed manually. Additionally, global deduplication and continuous incremental block-level backup help to reduce overall disk space requirements for backup retentions. If required, AppAssure backup repository expansion to PowerVault MD1200 storage shall be considered for additional backup storage space.

### 4.3 AppAssure snapshot process for Windows applications

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 on the disk. During the process of halting of writing content on the disk, all operations of disk I/O modules are queued...
and resumed after the snapshot is complete. Any operations already in progress are completed and all open files closed. The process of creating a shadow copy does not significantly impact the performance of the production system.

AppAssure uses Microsoft VSS because it has built-in support for all Windows internal technologies (NTFS, Registry, Active Directory®, and so on) to move data to disk before creating the snapshot. VSS is used to quiesce system and application data to disk, but not to create the snapshot. The captured data is rapidly transferred to and stored on the AppAssure Core running on the PowerVault DL4000.

Using VSS for backup does not render the application server in backup mode for a long period, as it only takes a few seconds to create the snapshot. Additionally, the file system and application-consistent snapshots offer prime benefits by ensuring the backups are retrievable with consistent application and system states.

4.4 AppAssure Recovery Assure

AppAssure Recovery Assure can be configured to perform automated recovery testing and verification of backups of Microsoft Exchange and SQL Server applications. It allows AppAssure to identify data corruption early, and prevent corrupted data blocks from being maintained in the backup repositories. It operates in conjunction with continual incremental-forever backups. Every night, Recovery Assure validates the latest backup completed that day. If the backup is validated, a green mark appears on the management screen next to that backup as shown in Figure 6. This is AppAssure assurance of total application level recoverability in the event of a disaster. When data corruption is detected, the backup is identified as invalid and marked in red on the management console.

Recovery Assure automatically checks backups in the following ways:

- **Integrity check of a recovery point**
  AppAssure Core verifies the integrity of all data stored for each recovery point to ensure that data can be recovered from each snapshot or base image.

- **Checksum check of Microsoft Exchange database**
  For Exchange servers, AppAssure Core performs nightly checksums on each Exchange database (EDB). Exchange database page contains a checksum for each database page, which is calculated after each modification. AppAssure calculates the checksum of the backed-up EDB pages and compares it with the EDB checksum to ensure integrity of the backed-up page. It does this before log truncation as per Microsoft best practice. AppAssure performs checksum only on EDB pages that have changed since the last checksum verification.

- **Mountability check of Exchange database**
  Mountability check is conducted by simulating mount of the Exchange database on the AppAssure appliance using volumes that contains the EDB, and system and log paths. This ensures that the mount from the recovery point will work during a recovery. Any issues found during a mountability check or checksum will display red status on the dashboard indicating that a backup will not be recovered, and a new one should be taken.
- **Attachability check of SQL Server and SharePoint**

  The SQL Server databases are attached to an off-production SQL Server instance that is installed on the AppAssure Core on PowerVault DL4000. AppAssure Core attaches the most recent SQL Server recovery point to the SQL Server running on PowerVault DL4000 on a nightly basis. This check automatically determines whether SQL Server databases are properly backed up and tested for recovery. If a database fails to attach to SQL Server, then the AppAssure Core job fails.

  The following application-specific recovery assurance settings can be enabled for Exchange and SQL servers depending on organizational requirements:

  - Recovery points integrity check (Exchange and SQL)
  - Checksum check job (Exchange only)
  - Log truncation job (Exchange and SQL)
  - Automatic mountability check (Exchange only)
  - Attachability check (SQL only)

Figure 6  Successful checksum and mountability checks for an Exchange Recovery Point

To conduct SQL Server attachability checks, you will need a SQL Server CAL (Client Access License) on PowerVault DL4000.
5 How to recover UC&C application hosts and data using PowerVault DL4000

The AppAssure software running on PowerVault DL4000 provides different recovery mechanisms for Microsoft UC&C application hosts.

Depending on the type of failure, you may need to restore an object or entire volume from the previous point-in-time backup. PowerVault DL4000 offers seamless in-place recovery of one or more application data volumes to its original location. In case of OS level corruption or hardware failure, PowerVault DL4000 offers an out-of-place recovery of application host to a virtual or a physical server. If there is a server node hardware failure, it can be recovered on a new server node replaced within the same PowerEdge VRTX by using the AppAssure BMR facility. The PowerEdge VRTX volumes and failover cluster remain up and running amongst other server nodes, and the restored server node joins the failover cluster seamlessly to take back the application workload.

5.1 Object-level granular recovery

In case of accidental deletion or overwriting of individual objects in Exchange or SharePoint applications, the AppAssure Mailbox Restore and AppAssure DocRetriever tools perform selective granular object-level recoveries.

5.1.1 Granular recovery of Microsoft Exchange 2013

Mailbox Restore uses AppAssure Core and LMU (Local Mount Utility) to access the recovery point that contains the data store from which you can search and recover items. It allows you to perform live recovery from an Exchange item without unmounting the data store volume or disrupting the Exchange services.

AppAssure Recovery Assurance mountability and integrity checks are performed after each snapshot to ensure that the recovery point can be mounted and the object to be recovered is corruption free. Mailbox Restore enables you to search for individual items for recovery. After you identify the object that you want to recover, it can be exported either to a folder or PST. Mailbox restore allows performing a differential restore, that is, restoring only the differences between a rolled backup data store and the latest recovery point. It also allows preview of the contents, attributes, and attachments of a message or Exchange item before recovering. The preview pane enables you to confirm that the selected object is the one that you want to restore.

To use Mailbox Restore to recover an Exchange item, you must have Microsoft Outlook installed on the same machine on which Mailbox Restore is installed.

To use Mailbox Restore to recover an Exchange item, perform the following steps:

1. Launch the LMU utility and connect it to the AppAssure Core running on the PowerVault DL4000. See Figure 7.
2. Select the Exchange protected host and mount the recovery point.
3. Open the Exchange data store that you want to restore. The Mailbox Restore utility launches automatically.

4. Search for any combination of criteria, such as names of mailboxes or folders, across one or multiple Exchange database (.edb) files. See Figure 8. The Microsoft Outlook user interface provides a preview pane, where you can view the message or item before performing a recovery.

5. Recover the Exchange item by exporting it to the preferred location or restoring it to the original location.

![Figure 8](Local Mount Utility on Microsoft Exchange Server connecting to PowerVault DL4000)
You can restore an email message, folder, mailbox or whole database. After restoring an object, close the data store in Mailbox Restore and dismount the recovery point in LMU.

5.1.2 Granular recovery of Microsoft SharePoint 2013

You can restore SharePoint data from the highest component level (a SharePoint site collection that may contain one or more SharePoint sites) to the lowest component level (a single document, an item list, or a library).

When manually restoring from SharePoint data backup, the restored backup typically replaces any changes in your live SharePoint environment data. That is, any additions, modifications, or deletions that are completed since the backup are lost. By using DocRetriever, you can browse through the SharePoint site backup, select specific or all the data, and restore it to a location that you specify keeping SharePoint permissions intact, without having to rebuild the entire production database. You can also use DocRetriever to easily migrate SharePoint site collections from one location to another by copying or moving that data. DocRetriever performs all restore operations through the supported SharePoint APIs for compliance.

DocRetriever can be used in two modes:

- **Standard Mode**
  Using this mode, you can recover SharePoint data from an AppAssure recovery point. In this mode, a simple implementation includes a single server with front-end SharePoint web server containing the SharePoint farm, the DocRetriever Console, the local service database supporting the console and the DocRetriever agent.
You can install the DocRetriever console and associated service database on a separate workstation from the webserver and the DocRetriever Agent software.

- **Standalone Mode**
  Using this mode, you can view and restore information backed up from one or more recovery sources, namely an offline backup of a SharePoint farm, content database, SQL Server backup, or SharePoint backup. This mode does not rely on AppAssure backups for recovery.

To restore SharePoint data backup in an AppAssure recovery point, use the 'Standard Mode' configuration.

1. Install the DocRetriever agent on SharePoint VM and the DocRetriever Console on SQL Server VM along with LMU. Use LMU to connect to the AppAssure Core running on PowerVault DL4000, and click the SQL Server VM to retrieve the list of recovery points.
2. Perform a writeable mount of the recovery point from which you want to restore. See **Figure 7**.

![Figure 7](image)

**Figure 9**  Local Mount Utility to mount the Microsoft SQL Server database.

3. Launch the DocRetriever console, and complete the configuration to connect to the local SQL Server SharePoint instance and database sources.
4. Launch the open Recovery Point option to use the locally mounted SQL Server database by using LMU, and connect to DocRetriever agent on SharePoint VM to perform object level recovery. See **Figure 9** and **Figure 10**.
5.2 Application host volume level in-place recovery

To recover one or more UC&C Application host volumes to the previous point-in-time state, an in-place recovery can be performed from a specific recovery point using AppAssure Restore Machine Wizard. AppAssure recovery performs automatic volume mapping to recover volumes from the recovery point to its original location. The system volumes cannot be selected for in-place restore.

To restore a protected application host VM to a previous point-in-time, choose a specific recovery point and start in-place restore by selecting ‘Recover to a protected machine’ option, as shown in Figure 11. All non-system level volumes are auto-selected for in-place recovery. You can manually select all volumes from Exchange Volume Group with ‘Live Recovery’ and ‘Force Dismount’ options auto-selected. See Figure 12.

Figure 10  DocRetriever showing Microsoft SharePoint farm
Figure 11  In-place volume level recovery of Microsoft Exchange Application VM

Figure 12  In-place volume level recovery of an Exchange Volume Group

The application-aware restore detects that the volumes to be recovered are Exchange or SQL Server databases. Therefore, auto-dismount and remount are performed before and after the restore operation. See Figure 13.
Per the reference architecture, Exchange Server is configured to host four databases on each of the two volumes, E:\ and F:\, whereas G:\ is the logs volume. To perform a single database recovery, it is advisable to use Mailbox Restore instead of an out-of-place restore of the whole volume to the Recovery Volume.

5.3 Application host out-of-place recovery to a virtual server

In case of OS level corruption within application host VM, a PowerEdge M620 server node or a PowerEdge VRTX hardware failure may disrupt UC&C application services. AppAssure offers both one-time export and continuous export of Windows OS-based server backup in the form of a virtual machine. By performing one-time export of a protected host to a virtual machine, all the backup data from a recovery point and the parameters defined for the protection schedule will be exported. Creating ‘Virtual Standby’ allows protected data to be continuously exported from the protected machine to a virtual machine by incrementally updating after every snapshot captured from the source agent. This in turn allows faster RTO. Exporting data to a virtual standby machine provides a highly available copy of application data. In case the protected machine goes down, you can boot up the virtual machine running the standby server. As shown in Figure 14, both One-time and Virtual Standby export options are available in the protected host ‘Actions’ tab.
Figure 14  One-time or Virtual Standby export of a Microsoft Exchange Application VM

PowerVault DL4000 enables Hyper-V based exports to be run locally (up to two VMs in Standard Edition and up to four VMs in High-Capacity Edition) as shown in Figure 15.

Figure 15  Standby export as a Hyper-V VM locally on PowerVault DL4000
To bring up the standby VM on the PowerVault DL4000, create a separate virtual network interface as shown in Figure 16. Also, specify this virtual switch in the standby VM settings with VLAN ID tagging for internal application network traffic control as shown in Figure 17.

Figure 16  A Standby VM switch on PowerVault DL4000

Figure 17  VM settings for Virtual Switch with VLAN tagging
Irrespective of the type of application host virtual infrastructure, AppAssure supports exporting to different types of virtual infrastructure environment such as VMware Workstation™, ESXi, Hyper-V, and VirtualBox. Therefore, if there is a separate virtual infrastructure available (external to the PowerVault DL4000), both one-time and continuous (standby) exports can be performed seamlessly allowing faster RTO with flexible virtual environment recovery.

5.4 Application host out-of-place recovery to a physical server

This section describes how you can bring the application on a physical server, using a V2P (Virtual to Physical) type recovery. The RTO is not as fast as V2V (Virtual to Virtual) type recovery but if you do not have a virtual infrastructure running and you have a physical server with enough resources available, V2P recovery option should be considered.

The out-of-place recovery of an application VM is performed through BMR (Bare Metal Recovery) to a dissimilar hardware, in this case, a virtual to a physical server. To perform BMR, follow these steps:

1. Create a boot CD image.
2. Burn the image to disk or copying the ISO file to a mountable USB drive.
3. Start up the target server from the boot image.
4. Connect to the recovery console instance.
5. Map the volumes.
6. Initiate the recovery from a particular recovery point.
7. Monitor the process.

After the bare metal restore is complete, reboot the server to load the operating system and the software applications on the restored server. You can then establish unique settings required for your configuration, such as network configuration changes. Make sure that the selected physical server for the recovery matches the CPU and memory and the disks sizes of the VM are recovered.

To perform restore of an application VM, select a specific recovery point and choose ‘Recover to any target machine using a boot CD’ option. See Figure 18.
Figure 18  Recovering a protected VM to a physical server

Based on the type of server that you want to restore, you need to inject drivers (network, storage, etc.) into the boot CD. See Figure 19.

Figure 19  Driver Injection to create the boot CD

Boot the physical server using the boot CD and change the network adapter setting to assign the IP address, as shown in Figure 20, to allow AppAssure Core connection from PowerVault DL4000. Note down the Authentication Key, which is required in the Restore Machine Wizard to complete the recovery.
Additionally, BMR recovery to a dissimilar hardware is helpful for hardware upgrade or replacement of any other physical server in your environment, such as AD/DC server.

In addition to PowerEdge VRTX server nodes and UC&C application VMs running on PowerEdge VRTX, it is recommended to backup AD/DC/DNS servers to enable complete environmental recovery of the reference architecture solution.

If you want to protect your AD/DC/DNS server in addition to all application VMs using PowerVault DL4000, set “Maximum Concurrent Transfers” to at least one more than the number of hosts being backed up.
6 Bare Metal Recovery of a VRTX Server node

A PowerEdge VRTX server node can fail due to hardware component failure. If the failover cluster configuration is based on the reference architecture, UC&C application VMs can automatically move to the other server nodes within PowerEdge VRTX without any service downtime. Replacing the failed PowerEdge VRTX server node and reconfiguring it to be a failover cluster member is a time-consuming manual task that directly affects the RTO.

The reconfiguration steps include:

1. PowerEdge VRTX CMC configuration
2. RAID 1 configuration on internal disks
3. OS installation and network configurations
4. Hyper-V and failover cluster configurations

Using Lifecycle Controller server configuration export and import facility along with AppAssure backup of server nodes, you can perform this process faster, reducing the RTO considerably. This chapter describes both of these features in detail.

6.1 Lifecycle Controller server configuration export and import

The Lifecycle Controller in PowerEdge servers provides an option to secure systems firmware and configuration to a known coherent state by enabling export and import of server profiles. By using this feature, you can capture and restore all BIOS and firmware in any system state, including bare-metal or system down state. This capability provides an automatic one-touch solution for hardware or firmware problems in scenarios such as motherboard replacement or server system replacement.

The export and import server profile features are controlled by either of the following two interfaces:

- Unified Server Configurator (USC)
- Remote Services

The export profile feature creates a file that contains the configuration and the currently installed firmware packages for the Lifecycle Controller supported devices including iDRAC, BIOS, PERC RAID controllers, and NICs. The import profile feature updates the firmware of the devices and sets the configuration of the devices to those saved in the server profile.

In this solution reference implementation, you must export and import the server profile to perform a bare metal restore of Hyper-V hosts using the PowerVault DL4000.

For more information on Export and Import of server profiles, see http://en.community.dell.com/techcenter/extras/m/white_papers/20060874.aspx
6.2 AppAssure protecting PowerEdge VRTX Server nodes

Installing AppAssure agents on each of the PowerEdge VRTX server nodes enables you to take backups of the OS and its environment including network, storage, Hyper-V, and failover cluster configurations. AppAssure 5.4.1 does not support native backup of cluster shared volumes in a failover cluster mode configuration on Windows Server 2012. Installing AppAssure agents on each of the server nodes can back up local disks (operating system volumes) but not the cluster shared volumes. Because the application VMs are protected separately from the PowerEdge VRTX server nodes, the frequency of the backup of these server nodes can be set to the default interval of 60 minutes. Set other backup configuration settings to default values.

Recovering a failed PowerEdge VRTX server node to a new one from the AppAssure backup can be done by following the Bare Metal Recovery process:

1. Choose the ‘Recovery to any target machine using a boot CD’ option.
2. Inject the network and storage drivers into the boot CD.
3. Boot the new server node using the boot CD to perform recovery.
4. Reboot the server after successful recovery.

AppAssure BMR allows IP address changes to the network interfaces available in the BMR URC utility, but it does not currently support VLAN tagging. Because of this limitation, the AppAssure Core fails when trying to connect to the server node that is booted by using the BMR boot CD. The workaround is to move the server node LOM ports on the switch to access mode. After successful recovery, the LOM ports will be brought back into VLAN.

The recovered server node needs to log back in as a domain member. However, it may fail with authentication issues from the AD/DC certification authority. As a workaround, change the node to a WORKGROUP member and change it back to a domain member. This will create and acquire a new certificate from the AD/DC. No other changes are required at this point. Bring up the failover cluster manager, which displays node state as failed, and then changes to a healthy status. You can now manually move the application VMs selectively to this recovered server node, as shown in Figure 21.
Figure 21  Moving Exchange VM on recovered PowerEdge M620 server after joining the failover cluster
7 Replication of UC&C application for disaster recovery using PowerVault DL4000

In case of onsite hardware or network failures, the UC&C application services availability concerns can be mitigated by quickly bringing up the services at a remote location. The AppAssure intelligent self-optimizing algorithm based on compression and deduplication provides this facility with easy configuration and reduces bandwidth requirements.

7.1 AppAssure replication capabilities

The replication process in AppAssure 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 site.

AppAssure 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, and deduplicated data across the WAN, resulting in reduction in bandwidth requirements.

7.1.1 Replication modes

AppAssure offers multiple replication configurations, such as point-to-point, point-to-multipoint, multipoint-to-point, and multi-hop, providing multi-site failure type protections. Possible replication scenarios include:

- **Replication to an on-site location**: Both the source and target cores are located in an on-site location, and replication is maintained at all times. This configuration provides protection against loss of a core, but does not offer site-level protection.

- **Replication to an off-site location**: The target core is located at an off-site disaster recovery or a central data center facility providing protection against a site-level failure in an onsite location.

- **Mutual replication**: In this configuration, each core located on a separate data center protects against the failure of the other by protecting its local hosts and serving as the offsite disaster recovery backup for the other site.

- **Hosted and cloud replication**: AppAssure MSP (Managed Service Provider) maintains target cores in the data center or a public cloud for a fee through its pay-as-you-go model instead of upfront cost.

7.1.2 Replication through seeding

Seeding is the initial transfer of deduplicated base images and incremental snapshots of the protected agents. Initial replication can be seeded to the target core over a network connection or by creating and saving a seed drive on external media, and then transferring it to the target core. Seeding to the drive is useful for large sets of data or sites with slow links.

The data in the seeding archive is compressed, optionally encrypted, and deduplicated. If the total size of seeding archive is larger than the removable media, the archive can span multiple devices. Seeding is a
two-part process: copying and consuming. Copying involves writing the initial replicated data to removable media. Consuming involves the target core receiving seeded media and copying it to its repository. After seeding is complete, the replication can be enabled. The source core asynchronously and continuously transmits the incremental snapshot data to the target core.

7.1.3 Replication performance considerations
If the bandwidth between the source 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 source core. Consider the following factors when preparing for replication:

- **Change Rate**: Indicates the rate at which the amount of protected data is accumulated. It depends on the amount of data changes on protected volumes and the protection interval of those volumes.
- **Bandwidth**: Indicates the available transfer speed between the source and the target core. It is very important to ensure that the bandwidth is larger than the change rate. Multiple parallel stream-based replications between cores can be beneficial.
- **Number of Agents**: AppAssure replication configuration allows selective replication by selecting certain servers that you want to replicate from the source core. In case of larger change rate and reduced bandwidth, you can select only the most critical servers for replication.

If a link fails during data transfer, replication resumes from the previous failure point of the transfer once the link is restored. This is a great benefit, especially for larger data transfers.

7.2 Replication of UC&C application services
You can configure the onsite PowerVault DL4000 as a replication partner to another AppAssure Core running in an offsite location. The offsite location can be a company-owned data center (self-managed core such as PowerVault DL4000), a third-party managed service provider’s (MSP’s) location, or cloud environment. The UC&C applications running on PowerEdge VRTX are protected locally to a PowerVault DL4000, which is configured to replicate to a remote DR/MSP location PowerVault DL4000 or to an AppAssure Core running in the Public cloud. See Figure 22.
Figure 22  Microsoft UC&C Applications replicated to Remote DR site and/or a public cloud

A seeding operation is considered for existing Microsoft UC&C application on PowerEdge VRTX deployments. For new deployments, the replication partners must be established before application services are operational at the on-site location. Therefore, you do not need to start seeding based replication.

7.3 Dealing with UC&C application services failure at onsite location

Onetime or continuous exports of UC&C application VMs can be performed on the remote location PowerVault DL4000 to reduce the RTO. In addition, if there is a virtual infrastructure running with available resources in the offsite or DR location, the UC&C application VMs can be recovered from their last snapshot in a short time. Alternatively, the option is to use AppAssure V2P facility to bring up any of these application services on a physical server.
Solution summary

This white paper is a follow up to the reference architecture for running Microsoft Exchange, Lync and SharePoint Server 2013 on Dell PowerEdge VRTX with Microsoft Server 2012 Hyper-V. This white paper focuses mainly on the data protection aspects of this solution.

UC&C application downtime presents a significant problem for organizations, and data protection solutions that require hardware duplication can be costly. PowerVault DL4000 running the AppAssure software helps reduce downtime and disaster recovery costs by providing efficient data protection, recovery, and replication of Microsoft UC&C applications running on PowerEdge VRTX in a Hyper-V environment.

In this white paper, the key design considerations for UC&C application data protection per Microsoft best practices are described in ‘Design considerations for UC&C data protection’ section.

The remaining sections describe the AppAssure software’s backup, recovery and replication capabilities specifically developed towards UC&C application awareness inbuilt into each of these facilities.

AppAssure offers different recovery options for UC&C application-protected hosts, which include:

- Object-level granular recovery of Exchange 2013 and SharePoint 2013
- Volume level in-place recovery
- Out-of-place recovery to a virtual server, including dissimilar virtual server infrastructure
- Out-of-place recovery to a physical server, including dissimilar hardware

PowerEdge VRTX server node failures can be mitigated using Lifecycle Controller’s server XML export and import features with AppAssure backup of the server node operating system and configurations. An AppAssure-restored node automatically becomes part of the Microsoft Failover Cluster after you change network interface settings and log back into the domain.

UC&C Applications can be protected through AppAssure replication for a disaster recovery use case. AppAssure’s intelligent Read-Match-Write algorithm coupled with deduplication and encryption offers reduced bandwidth requirements. Replication can be configured to a remote Disaster Recovery site, an MSP co-location site, or a cloud. In case of primary site failure, standby VMs can be brought up on PowerVault DL4000 within a very short RTO.
Additional Resources

1. **Support.dell.com** is focused on meeting customer requirements with proven services.
2. **DellTechCenter.com** is an IT community where you can connect with Dell customers and Dell employees for sharing knowledge, best practices, and information about Dell products and installations.
3. Referenced or recommended Dell publications:
   a. [Dell PowerEdge VRTX](#)
   b. [Microsoft Windows Server 2012 Hyper-V Reference Architecture for Dell PowerEdge VRTX](#)
   c. [Microsoft Exchange, Lync and SharePoint Server 2013 on Dell PowerEdge VRTX with Microsoft Server 2012 Hyper-V](#)
   d. [PowerVault DL4000 Product Manual](#)
   e. [Dell AppAssure User’s Guide](#)
   f. [Dell AppAssure 5.4.1 Mailbox Restore for Exchange User Guide](#)
   g. [Dell AppAssure 5.4.1 DocRetriever for SharePoint User Guide](#)
   h. [Dell AppAssure Product Demos](#)
   i. [Dell AppAssure TrueScale Architecture Technical Brief](#)
   j. [Dell AppAssure Exchange Recovery Technical Brief](#)
   k. [Dell AppAssure Recovery Assurance Technical Brief](#)
   l. [Dell AppAssure Cloud Replication Technical Brief](#)
   m. [Dell AppAssure Local Mount Utility Technical Brief](#)
   n. [An AppAssure KB for a “Flat name of target computer could not be retrieved (2138)” error.](#)