Dell EqualLogic Best Practices Series

Best Practices for Enhancing Microsoft Exchange Server 2010 Data Protection and Availability using Dell EqualLogic Snapshots

A Dell Technical Whitepaper

Storage Infrastructure and Solutions Engineering
Dell Product Group
October 2011

Table of Contents

Acknowledgements

This whitepaper was produced by the PG Storage Infrastructure and Solutions team between January 2011 and April 2011 at the Dell Labs facility in Round Rock, Texas.

The team that created this whitepaper:

Danilo Feroce, **Puneet Dhawan**, and **Margaret Boeneke**

We would like to thank the following Dell team members for providing significant support during development and review:

Dan Curran, **Bob Ganley**, and **Chris Almond**

Feedback

We encourage readers of this publication to provide feedback on the quality and usefulness of this information. You can submit feedback as follows:

Use the "**Start a new thread**" link here:

http://www.delltechcenter.com/page/Enhancing+Microsoft+Exchange+Server+2010+Data+Protection+and+Availability+with+EqualLogic+Snapshots

1 Introduction

IT professionals and businesses are constantly challenged by the exponential growth of the amount of data they have to manage. While data management encompasses several areas of an organization, ensuring the data protection and business continuity for the data content is one of the most critical aspects. Loss of data for mission critical applications and lack of application availability for users is not tolerable outside business continuity strategy boundaries.

A messaging infrastructure built upon Microsoft® Exchange has risen as one of the most critical corporate-wide services that demands diligent planning for its protection. The significant redesign of internal database storage functionalities in the Microsoft Exchange 2010 version now requires larger databases compared with previous versions and at the same time allows large to very large mailboxes. This has caused a substantial increase in the size of the data to be made highly available and recoverable.

In a similar context, IT professionals have to seriously consider what technologies can be exploited in order to achieve the difficult goals of data availability, resiliency, and fast recovery. Varying levels of continuity can be achieved depending on the nature of the application and on the tools and techniques employed to protect them.

1.1 Purpose and scope

This whitepaper introduces the advantages of protecting Microsoft Exchange mailbox data using the out-of-the-box Dell™ EqualLogic™ snapshot feature, which can be leveraged and integrated within vertical backup software solutions as well. It will guide Exchange and SAN administrators to understand and strengthen their Exchange recovery infrastructure with the help of lab validated test results. The scope of this paper is limited to local data protection and data availability only.

1.2 Target audience

This paper is primarily intended for IT professionals (IT managers, Solution Architects, Exchange and Storage Administrators, System and VMware Engineers) who are involved in defining and/or implementing data protection and recovery plans for Microsoft Exchange Server 2010 infrastructures and would like to investigate the benefits of using Dell EqualLogic storage. This document assumes that the reader is familiar with Microsoft Exchange functionalities, EqualLogic SAN operation, and VMware system administration.

1.3 Key benefits of snapshots for applications

Using EqualLogic SAN based snapshots within a wider data protection strategy provides key benefits:

- **SAN-based snapshot feature is provided out-of-the-box**: Volumes holding applications data can have one or more point-in-time copies taken seamlessly on the SAN, while application integration is maintained at the host level to ensure data consistency.
- **Simple management**: A host based set of GUI applications provides management, scheduling, and monitoring functionalities for all related activities with snapshots.
- **Host and network resources off-load during backup**: SAN snapshots allow minimizing the backup windows by off-loading the host local resources contention and LAN traffic to

the SAN level. They open new perspectives in dealing with the data protection strategies when integrated with backup applications.

- **Rapid creation of a recovery point**: The process of creating a SAN snapshot takes very little time. Thus it opens up the opportunity of establishing more frequent application recovery points, providing the choice of a more granular recovery point objective for the application data.
- **Fast recovery**: Recovering from a SAN snapshot is a fast operation because the dataset to be rolled back resides on the SAN and does not have to change media (tape to disk, or disk to disk over network), but it is already available to be brought online when required.

1.4 Terminology

The following terms will be used throughout this document.

Group: Consists of one or more Dell EqualLogic PS Series arrays connected to an IP network that work together to provide SAN resources to host servers.

Pool: Storage space that each member (array) is assigned to after being added to a group.

Auto-Snapshot Manager/Microsoft Edition: Microsoft® Windows Server® application offering the management and scheduling of application-consistent Smart Copy snapshots of Exchange Server databases (integrated with Windows Volume Shadow Copy Service) leveraging the built-in snapshot, clone, and replication facilities in PS Series arrays.

Snapshot: Point-in-time copy of the data residing on a given volume.

Clone: Physical copy of the data on any given volumes created in the same data pool.

Snapshot reserve: Storage space reserved as a percentage of each volume used to store snapshots.

Microsoft Volume Shadow Service (VSS): Technology included in Microsoft® Windows® that allows taking shadow copies of a data/volume in a consistent state, even when it has a lock.

VSS Requester: A component that requests the creation or manipulation of a shadow copy

VSS Writer: A component that guarantees the consistency of the data set to be backed up, typically provided by the application or by a system component.

VSS Provider: A component that creates and maintains the shadow copies in the software or in the hardware level.

DAG: Database Availability Group is a pool of networked servers that hosts multiple copies of the same Exchange databases.

2 Exchange Server data protection options and challenges

The traditional elements that should be identified before the definition of a business continuity plan (BCP) of any service are:

- Recovery Point Objective (RPO), which defines the maximum acceptable amount of data loss measured in time
- Recovery Time Objective (RTO), which defines the duration of time within which the service of your application must be restored
- Features, constraints, and potential of the technology underlying the infrastructure to be backed up and/or recovered

The RTO/RPO figures are an output of an exercise unique to each organization, commonly identified as business impact analysis (BIA), which evaluates the balance between the possible threats, the costs for implementing the recovery mechanisms and the risk acceptance of downtime or unavailability of a service.

A common set of limitations, valid across any line-of-business or corporate application protection strategy, with an impact in the process used to implement the RTO/RPO requirements into the technologies, are the following:

Backup window Represents the period of time when backups are allowed to run. In general this is selected based on the usage pattern of the line-of-business/corporate application (for example, 24x7x365 or 9 to 5) with the goal of minimizing the contention of users access and backup tasks on the application resources.

Backup frequency Determines how often the backups are scheduled to run. It represents the first factor to evaluate when the RPO is planned and influences the RTO because the amount of time required to recover a service is based on the number of backup sets that have to be brought back online.

Data retention Indicates the length of time that the backup sets are to be kept intact. It influences how far back in time the RPO can be. The main concerns around data retention are the legal and privacy aspects of it, not only the business related ones.

While the RTO/RPO variables are decided by the business needs of each organization, we will investigate the backup and recovery options that a business could choose for the mailbox database portion of a service based on Microsoft Exchange Server 2010.

Due to the many distinct elements of a Microsoft Exchange deployment, we decided to narrow our scope to the area where the user data is permanently stored, which means the Exchange servers identified by the Mailbox role. We should remember that from a holistic point of view, concerns about the restore of a service based on Exchange technologies must include, but are not limited to, the following elements:

- Active Directory®, where users and services configurations are stored, and authentication and authorization occur
- Exchange Servers with roles other than Mailbox (Client Access, Hub Transport, Unified Messaging and Edge Transport), that, from an high level, are in charge of accepting client connections, interconnect with PBX systems, and routing messages within or in/out of your organization
- Distributed email containers, external to the central messaging infrastructure, such as .PST files which can permanently store part of the users email history (in case their use is allowed in the organization)

2.1 Exchange store elements

Microsoft Exchange 2010 has changed the hierarchy for the logical components of its storage architecture when compared with the previous versions of the product. Databases are now the first hierarchical elements in the storage subsystem and are directly referenced at the Exchange organization level.

When the mailbox databases are created, different file system elements are distributed in the volume or volumes identified as storage containers for the specific database. The loss of any of these elements can represent a disruption of the service or a threat to the RPO in case of recovery.

Database file (*.edb) is the container for the mailbox data. It contains all the data until the last Exchange checkpoint and as such has to be backed up in order to recover a database.

Transaction Logs (*.log) are the container where all the transactions that occur on the database (create, modify, delete messages, etc.) are recorded. Each database owns its set of logs. In case of recovery, they are required to allow the replay of the transactions to the last point in time.

Checkpoint file (*.chk) is a container for metadata indicating when the last flush of data from the memory cache to the database occurred and as such is required in case the log replay process to a database file is performed. It is positioned in the same folder location as the logs.

Content index files (catalog folder, multiple file extension) are flat files, representing the Search Catalog, built by the Microsoft Search Service. The client applications connected to Exchange Server take advantage of this catalog by performing faster searches based on indexes instead of full scans.

The database files, logs, checkpoint, and search catalog will usually be hosted in one server unless you are using DAG (then all these files are copied and are hosted in multiple servers).

Note: A Database Availability Group (DAG) is a pool of up to 16 networked servers that hosts multiple copies of the same Exchange database or databases, where only one of the copies is active at a specific point-in-time within the group, and the other copies are passive and contain replicated data. The DAG technology represents the out-of-the-box foundation for Exchange 2010 mailbox database high availability.

For additional information about DAG refer to Microsoft documentation:
Understanding Database Availability Groups, available at:
http://technet.microsoft.com/en-us/library/dd979799.aspx

2.2 Exchange 2010 database protection options

Microsoft Exchange 2010 offers a native subset of features that help in protecting the data present in the mailbox databases and that can be coupled with traditional backup/recovery activities in order to provide a higher data protection: DAG (multiple copy of a mailbox database), recoverable items (multi-stages mailbox data deletion process), DAG lagged copy (point-in-time copy of the mailbox database).

Unlike its predecessors, Exchange 2010 offers support to back up its mailbox databases only through the Volume Shadow Copy Service (VSS). VSS is a framework and a mechanism that allows consistent copies of application datasets to be saved even when they are in use (mounted, open, or locked). To achieve this result, VSS coordinates its actions with the line-of-business/corporate application (i.e. Microsoft Exchange Server), the backup applications, and the storage container (system or hardware).

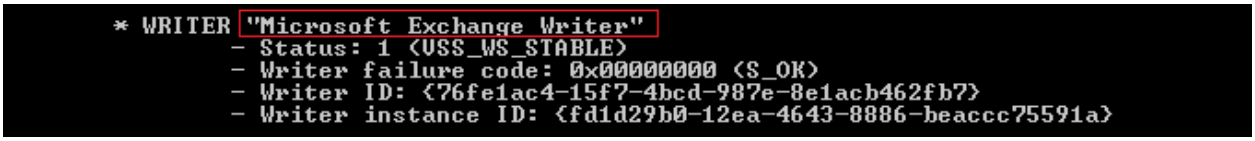
In this framework there are three main roles identified: the writers (applications such as Exchange Server), the requester (protection applications such as ASM/ME or backup applications such as Symantec™ Backup Exec™, CommVault Simpana®), and the providers (system provider or hardware provider, such as EqualLogic).

For additional information about Volume Shadow Copy Service (VSS) refer to Microsoft documentation:
Volume Shadow Copy Service, available at:
http://technet.microsoft.com/en-us/library/ee923636%28WS.10%29.aspx

Any Exchange-aware backup application that is able to interface the Exchange VSS writer will also be able to take consistent backups of a mailbox database. To verify the required VSS writer is referenced in the system, the following command can be issued in the CLI provided by the DISKSHADOW.EXE system tool:

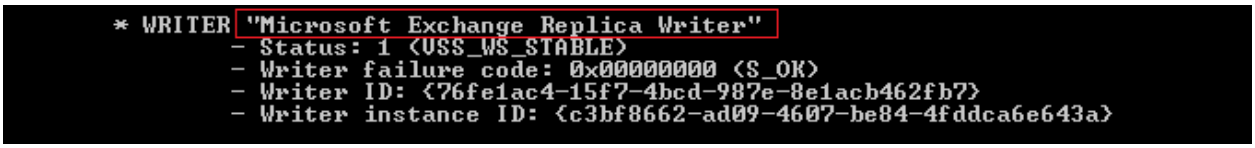
```
DISKSHADOW>list writer status
```

When the Exchange writer is present, the output should include an element similar to the one in the red box.



When an Exchange DAG is used, the backup of the passive copy or copies flow through the Microsoft Exchange Replication Service VSS writer while the backup of the active copy of the databases still happens through the regular VSS writer as shown above.

Once again, the presence of the required VSS writer is shown by DISKSHADOW.EXE:



Microsoft Exchange 2010 offers support for multiple ways to restore its mailbox databases and data. Every way offers different advantages in terms of RPO and RTO.

In-place DB restore: Represents the restore of the database (*.edb file) in the same location where it was originally. The data contained in the database is the data captured until the last checkpoint occurred. To open the database, it has to be brought to a 'Clean shutdown' state.

Soft Recovery: Represents the Transaction Log Replay process, which you may decide to perform after the restore of a database to bring it to a 'Clean shutdown' state, and then applying the required set of transaction log files. This recovery process is known as 'soft', as opposed to the 'hard' recovery process, because it happens without any loss of data; the transactions originally committed to the Exchange storage sub-system are extracted from the logs and applied to the database.

Recovery Database: Represents a special database that can be mounted (maximum one per each mailbox server) from a restored database as a special administrative resource not directly accessible by users. It can only be accessed through PowerShell commands to allow granular data to be extracted and exported to a regular database (merged into a mailbox or a folder).

Search Catalog: Is not strictly required to restore user data. It is a set of index files external to the databases, and can be rebuilt on demand. If these files are omitted from a restore, however, an impact in the level of service provided by the Exchange infrastructure (search response) has to be accepted. The rebuild phase of the Content Index (crawling) is time intensive and increases the amount of read access to the storage during the process.

Note: The previously named Microsoft Exchange Replication Service VSS writer is currently built to support database backup operations, but not restore operations. Thus it is not possible to restore directly to a passive copy of a DAG member while the replication service is active between the nodes.

3 Auto-Snapshot Manager and Exchange protection

Auto-Snapshot Manager/Microsoft Edition (ASM/ME) is a software component that is part of the EqualLogic Host integration Tools (HIT kit), a software toolkit available free of cost for customers running Dell EqualLogic PS Series arrays. ASM/ME offers an intuitive interface, implemented as a snap-in (up to version 3.5.1) within the Microsoft Management Console framework, and is able to create and manage snapshots and clones on the SAN arrays directly from the Windows host.

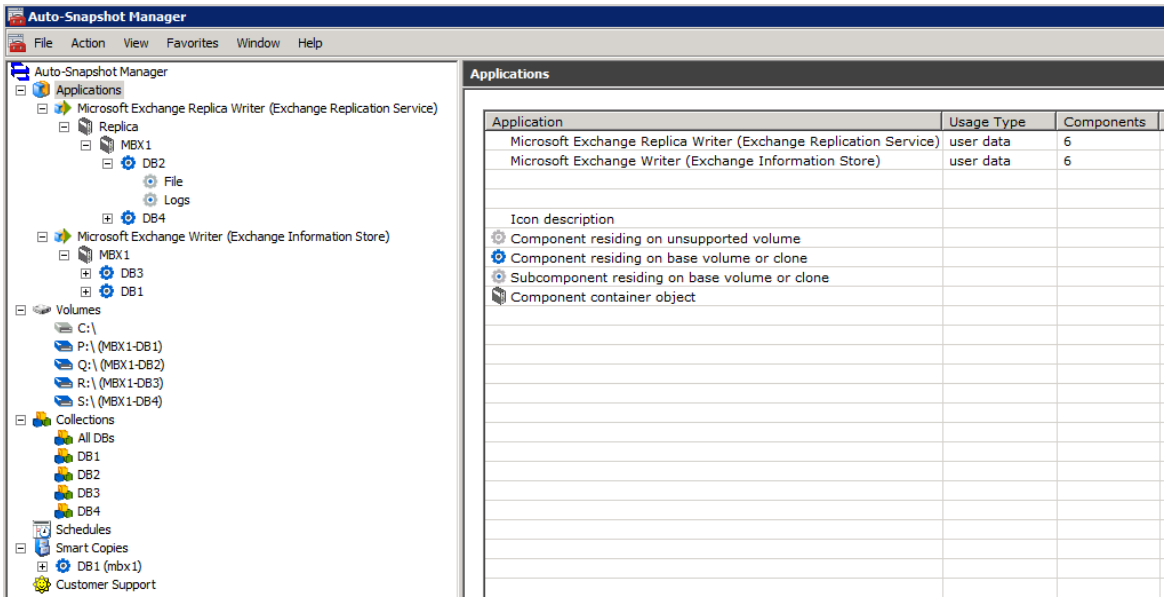


Figure 1 Auto-Snapshot Manager MMC interface on Microsoft Exchange Server

A Smart Copy snapshot represents a point in time consistent copy of an EqualLogic SAN volume: ASM/ME provides the support to take smart copies manually or automatically, manipulate them, and recover the data contained in a way consistent to the application. A Smart Copy snapshot is space efficient because it only stores the changes to the data since the snapshot was created. Note that because there is no physical separation of the media storing Smart Copy snapshots and the production volume, ASM/ME is not considered an alternative to long-term backup methods. ASM/ME and Smart Copies should be used in conjunction with a normal backup schedule for a higher level of data protection and shorter recovery times.

A Smart Copy snapshot consists of a combined set of elements: a SAN based snapshot and a backup document (metadata descriptor file, *.bcd) locally saved on the host. While a snapshot created directly on the EqualLogic SAN from the Group Manager console looks very similar to an ASM Smart Copy, it is not integrated with the host VSS components and as such will not be able to provide the same level of data consistency.

3.1 ASM/ME integration with Windows platform and VSS Service

ASM/ME, installed on a Windows server hosting volumes from an EqualLogic array, provides full integration with Microsoft Volume Shadow Copy Service. It plays the VSS requester role and works together the EqualLogic VSS Provider to correctly interact with the Exchange writers to take application-aware shadow copies.

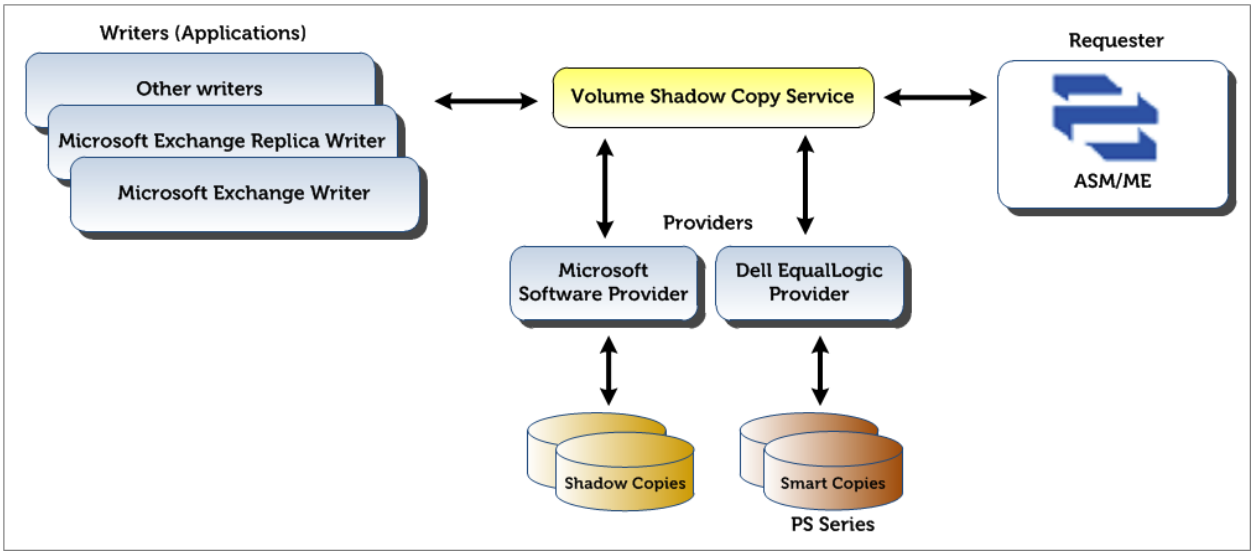


Figure 2 Architectural diagram of ASM/ME and Volume Shadow Service

The DISKSHADOW.EXE CLI command reported below provides access to the VSS configuration and objects.

```
DISKSHADOW>list providers
```

When the EqualLogic VSS HW provider is present in the system the output includes an element similar to the one in the red box.

```
* ProviderID: {d4689bdf-7b60-4f6e-9afb-2d13c01b12ea}
        Type: [3] VSS_PROV_HARDWARE
        Name: Dell EqualLogic VSS HW Provider
        Version: 3.5.1.5664
        CLSID: {5ea28b12-3213-4bee-8cdd-b6f935260aba}
```

When working in conjunction with Microsoft Exchange Server 2010, ASM/ME protects standalone Exchange installations as well as resilient DAG configurations, and can accomplish the tasks in Table 1.

Table 1 ASM/ME and Microsoft Exchange

Task	Description
Create Smart Copy	Creates an Exchange-aware SAN snapshot (or clone) of a mailbox database volume, associated with a backup document in the local host. The snapshot (or clone) is created as a 'copy' of the volume, and thus the transaction logs are not truncated by this process.
Collection	Represents a set of volumes grouped by an operational logic (consistent actions to multiple volumes). It can be treated as a single entity by the scheduler or by a recovery process.
Checksum Verification	Performs a data integrity checksum on the mailbox database, the checkpoint file and the log files residing inside the snapshot of a volume. The task is accomplished taking advantage of the Microsoft Exchange command line utility ESEUTIL.EXE.
Soft Recovery	Configures the database residing inside the snapshot to replay the transaction logs, bringing it in a 'clean shutdown' state. The task is accomplished taking advantage of the Microsoft Exchange command line utility ESEUTIL.EXE
Schedule Smart Copy	Generates a schedule that creates Smart Copies of a volume based on a defined frequency and recurrence, with or without including the Checksum Verification and Soft recovery options
In-place Restore	Restores a point in time copy of all the data in a mailbox database replacing the original volume
Brick Level Recovery	Restores a point in time copy of a mailbox database, creates an Exchange Recovery Mailbox Database (RDB), attaches the restore to it, and then mounts the RDB

For additional information about Dell EqualLogic ASM/ME, refer to the ASM documentation: *Auto-Snapshot manager for Microsoft User Guide*, available at: https://support.equallogic.com/support/download_file.aspx?id=1053
Note: A support account is required in order to access the download area of the website.

4 Test topology and architecture

We decided to use a real world scenario simulation to identify the benefits of using EqualLogic SAN snapshots to strengthen the Exchange 2010 data protection. The main areas which we identified to test were:

- The Smart Copy snapshot process impact and efficiency on an Exchange Server host
- The recovery scenarios where a Smart Copy snapshot can assist and improve recovery time or point objectives

To conduct the tests detailed in this paper, we deployed and tested a Microsoft Exchange Server 2010 configuration hosted by Dell EqualLogic storage and a virtual infrastructure built upon VMware vSphere 4.1 hypervisor.

Our test architecture consisted of a configuration designed to support the messaging services for a medium-sized organization (up to 5000 users), and to provide both high availability and resiliency by implementing a two node DAG, redundant client connectivity, and messages routing components. Our exercise targeted the local protection of a messaging service and, as such, the entire topology resided in a single datacenter.

4.1 Functional system design

The functional elements of the test infrastructure are shown in Figure 3. Some key elements of the design were:

- Single Active Directory forest, single domain, single site
- Redundant HUB transport servers and resilient Client Access servers (load balanced)
- Mailbox database servers configured within a DAG for HA and resiliency
- Dedicated resources for infrastructure management, load simulation and monitoring

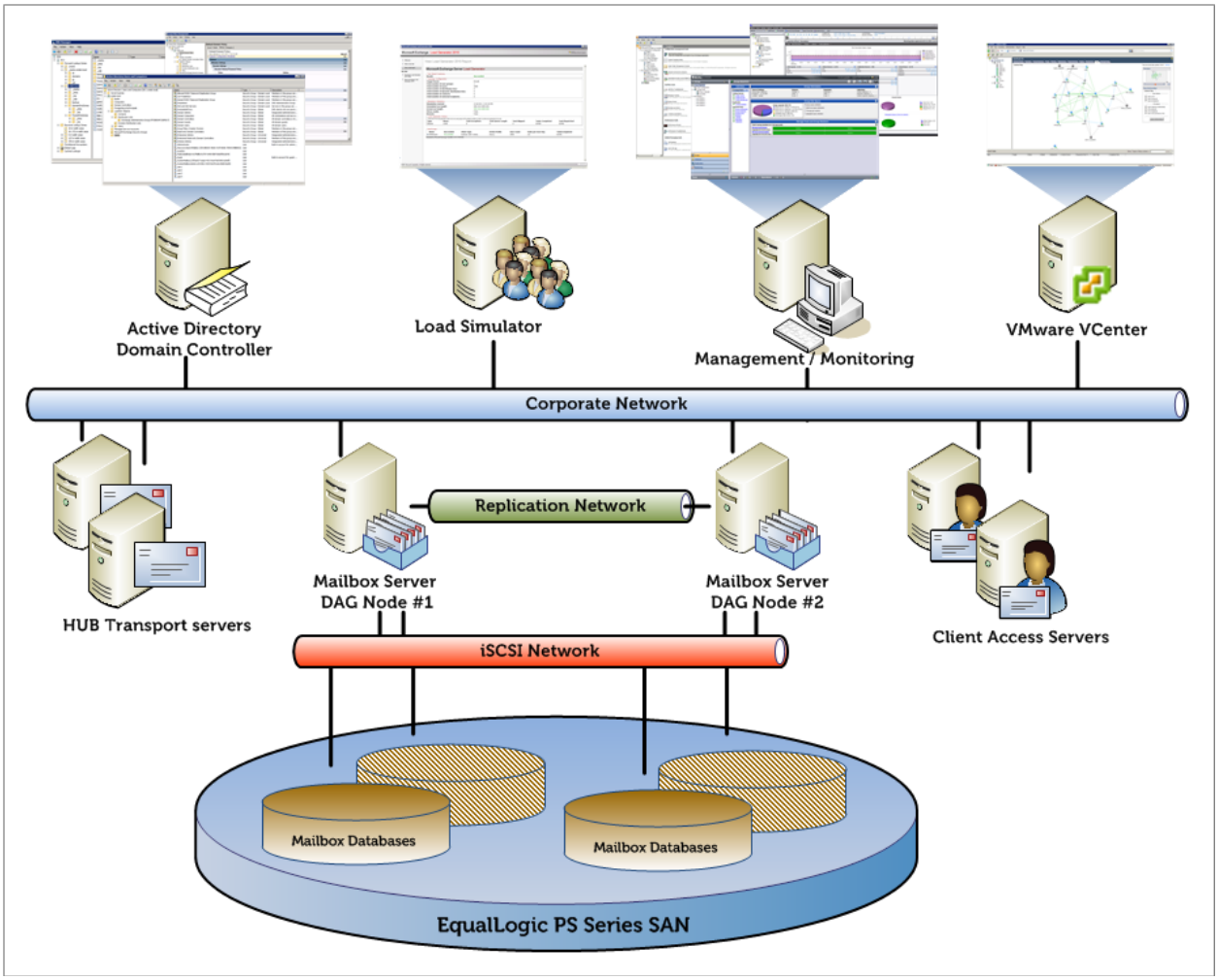


Figure 3 Functional system design diagram

4.2 Physical system configuration

The physical components of the test infrastructure were laid out as shown in Figure 4.

In order to provide more flexibility and datacenter density, we deployed this solution on Dell Blade servers. Some key elements of the physical deployment were:

- Single M1000E Blade enclosure containing the entire Exchange and testing infrastructure, utilizing four Blade servers (2 full slots and 2 half slots)
- Dual PowerConnect M6220 Ethernet switches to support regular IP traffic
- Dual PowerConnect 6248 and dual M6348 Ethernet switches to support the iSCSI data storage traffic
- Single EqualLogic iSCSI SAN provisioned with 4x PS6000XV arrays providing aggregate raw capacity of 26.8 TB (4x 16 disks, 450GB nominal each).

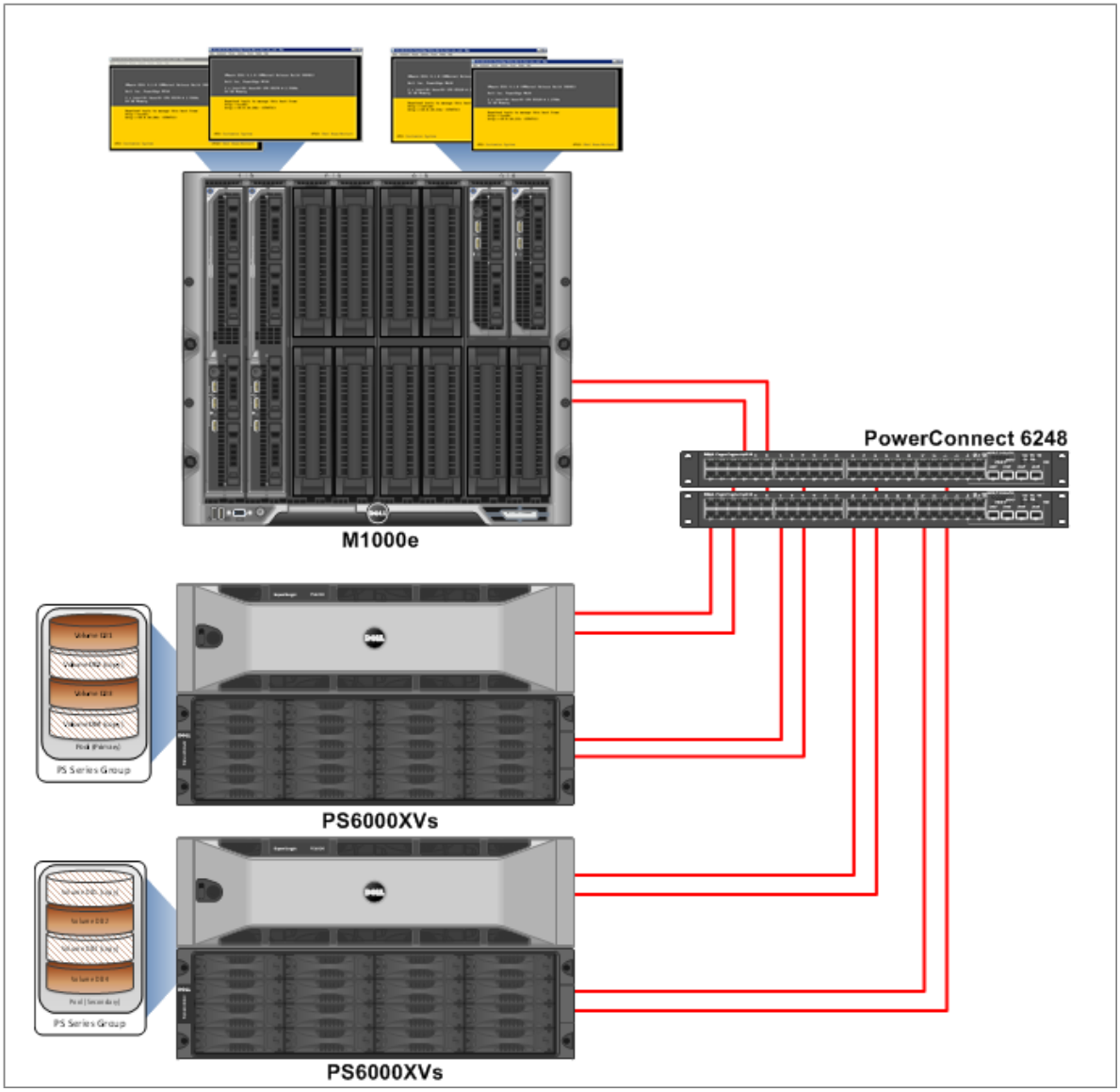


Figure 4 Physical system configuration diagram

More details of the test configuration setup (software, storage, hypervisor, virtual machines and network) are provided in Appendix A, as well as a detailed schematic diagram showing the various network connection paths across the blade chassis switch fabrics.

4.3 Storage layout

The EqualLogic SAN arrays and the volumes underlying the Exchange databases were setup as follows:

- One EqualLogic group configured with four PS6000XV members
- Two Storage pools defined within the group (one pool for each Exchange Mailbox server in the DAG), with two members in each pool
- RAID-50 policy selected for each member (14 disks active in the RAID group, two hot-spares for each member)
- 4 volumes created in each pool, one dedicated to each Exchange Mailbox database

- Snapshot reserve configured for each volume with enough room to accommodate and retain the number of snapshots planned for the tests

Figure 5 reflects the mailbox databases layout implemented on the EqualLogic SAN.

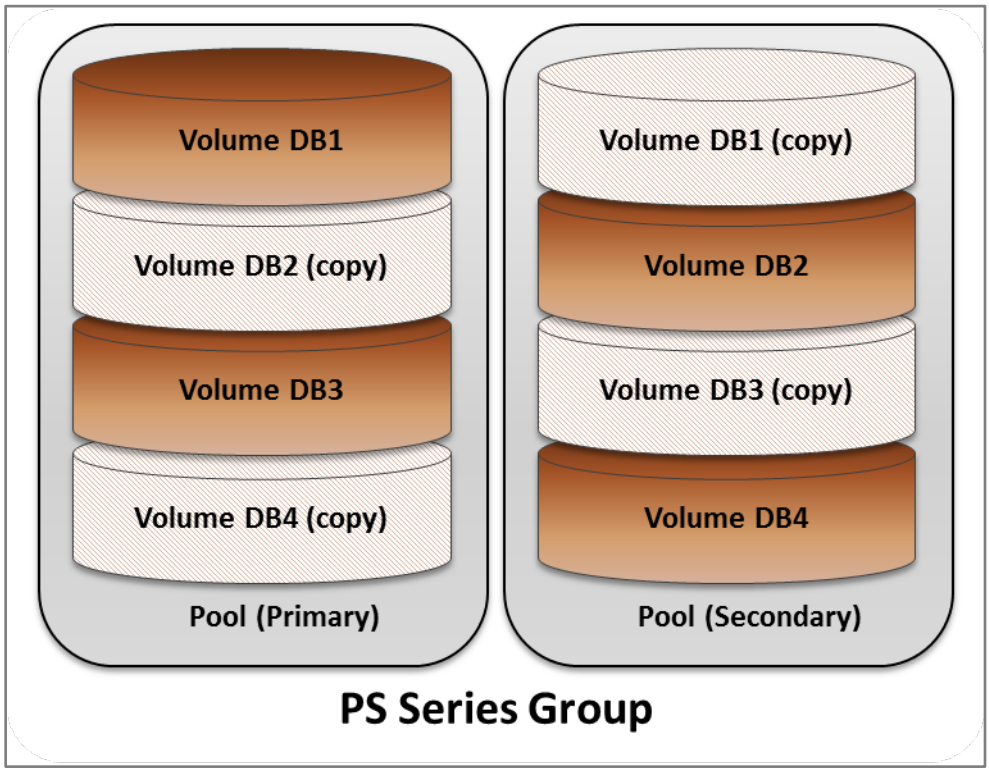


Figure 5 Mailbox databases layout

5 Test workload

The goal of the baseline workload was to simulate a regular corporate messaging activity during peak hours and then to apply different data protection and recovery techniques to measure the efficiency and impact on the local and network resources of each of them.

For the Microsoft Exchange mailbox database and users profile we applied the configuration reported in Table 2.

Table 2 Microsoft Exchange Mailbox profiling

Microsoft Exchange Server profile	
Number of simulated mailboxes/users	5000
Mailbox size	250MB
Mailboxes allocation	1250 mailboxes per mailbox database
Mailbox databases	4 databases Two active and two passive databases on each node of a two nodes DAG
User count per Mailbox database server	2500
Database + Logs volume	700GB each, one per mailbox database Basic disk, GPT partition, default alignment 64KB allocation unit size Accessed by drive letter
Capacity allocated	Database: 420GB each (average)
	Logs: circular logging NOT enabled 1400 logs/hour per database at maximum load Provisioned for up to 58 hours of continuous logs generation (1 log = 1 MB)
	Content Index: 200GB each database (average)
Exchange Search Indexer	Running
Exchange Maintenance	Enabled in background (24x7)

For additional information about Exchange Server 2010 storage configurations and best practices, refer to Microsoft documentation:
Understanding Storage Configuration, available at:
http://technet.microsoft.com/en-us/library/ee832792.aspx

5.1 Microsoft Load Generator considerations

Exchange Load Generator 2010 is a validation and stress tool able to generate client access workload against an Exchange 2010/2007 test infrastructure. The tool can simulate the access patterns of common client applications or protocols such as Microsoft Office Outlook 2007/2003 (online or

cached), POP, IMAP4, SMTP, ActiveSync, and Outlook Web App. Some key elements and considerations about Microsoft Exchange LoadGen are:

- Requires a fully functional Microsoft Exchange deployment
- Requires, and provides, an 'initialization' step to create Active Directory user accounts and mailboxes, and then populates the mailboxes according to the defined requirements
- Simulates user client tasks within a wide range: logon/logoff, browse calendar/contacts, create tasks/appointments, send emails, read and process messages, download Outlook Address Book (OAB), etc.
- Reports a high level pass/fail metric for each run (based on the number of the tasks planned to be executed, tasks achieved, and length of the tasks queue)
- Exchange 2010 Content Index size is usually 5-10% of its own mailbox database. It is a known behavior that the size of catalogs created upon mailbox databases built by LoadGen can grow over the expected percentage statistic. The root cause for that is within the message mix generation and consequent mailboxes population executed by the tool:
    - LoadGen populates the mailbox databases from a predefined small set of emails
    - Email content is an artificial Latin mix with few words concatenated
    - Little variety in the attachments, which are mostly text based and searchable, is used. Some real world attachments are just not searchable.

For the Microsoft Exchange LoadGen tool profile we used the configuration reported in Table 3.

Table 3 Exchange LoadGen profile

Microsoft Exchange LoadGen profiling	
Number of simulated mailboxes	5000
Client access type	Outlook 2007 online
Client access profile	Heavy (20/80, 132 tasks per user day)
Simulation day length	8 hours
Simulation test length	Variable (from 1 hour up to over 8 hours)

For additional information about Microsoft Exchange LoadGen 2010, refer to Microsoft documentation:
Tools for Performance and Scalability Evaluation, available at:
http://technet.microsoft.com/en-us/library/dd335108.aspx

6 Testing the impact of Smart Copy snapshots

The goal of this set of tests was to establish the impact we should expect from creating Smart Copy snapshots of mailbox database volumes under user load in the simulated test environment.

First, we evaluated the resource utilization of a single Smart Copy snapshot taken under varying and increasing user workloads. We kept the simulation active before and after taking the snapshot to verify any behavioral changes in the key indicators.

Test Details for one snapshot of one volume of an active mailbox database, with increasing workload:

Workload	Increasing workload of 20%, 40%, 60%, 80% and 100% of the reference 5000 concurrent users (Outlook 2007 online clients, heavy profile)
Duration	60 minutes, from the snapshot creation onwards
Key indicators	Time taken, host resources impact

Second, we evaluated the trend of a series of cumulative Smart Copy snapshots taken under the same user workload. We kept the simulation consistent for the entire duration of the test. We focused on the heaviest workload defined, to position the results in the worst scenario.

Test Details for cumulative snapshots of one volume of an active mailbox database, with same workload:

Workload	Steady workload of the reference 5000 concurrent users (Outlook 2007 online clients, heavy profile)
Duration	One snapshot every 60 minutes for a total of eight cumulative smart Copy snapshots. Snapshots series kept intact until the end of the test
Key indicators	Time taken, host resources impact

Last, we verified the behavior of creating Smart Copy snapshots under load when we simulated an operative critical situation. We took down one of the two nodes of the DAG, reproducing a business scenario where, for administrative or unpredictable reasons, the remaining node would have to bear the load of the entire active databases. This condition would likely be temporary in a real world environment, but we recorded it as proof point of the ability of creating Smart Copy snapshots as expected under different conditions.

Test Details for cumulative snapshots of one volume of an active mailbox database, with same workload, single host online:

Workload	Steady workload of the reference 5000 concurrent users (Outlook 2007 online clients, heavy profile). One node of the DAG was running all the 4 active databases.
Duration	One snapshot every 60 minutes for a total of eight cumulative Smart Copy snapshots. Snapshots series kept intact until the end of the test.
Key indicators	Time taken, host resources impact

The combination of the results for these series of tests helped us evaluate the cost of creating Smart Copy snapshots for an entire business day (identified by 8 hours) and to assess their variation while the amount of online users was variable. At the same time we verified if and how the occurrence of a critical situation would affect this status.

That test design should help in predicting the behavior in real world environments with either a constant or a variable number of connected users and different rotations of work hours.

6.1 Time taken results and analysis

Because the time taken to create a Smart Copy with EqualLogic and ASM/ME is very short, we measured it by observing the events recorded in the Application Event Log of the mailbox database servers.

Exchange Server service components (the Information Store and ESE engine) generate an extensive track of messages describing the course of preparing the required metadata for the VSS backup, the activation of a Shadow Copy instance, and the beginning of the database freeze. They also generate the reverse-ordered messages indicating the closure and end of each opened task.

Figure 6, Figure 7, and Figure 8 show the elapsed time between the beginning of the Shadow Copy activation and successful completion. The time taken for the database 'freeze' part of the process is also shown.

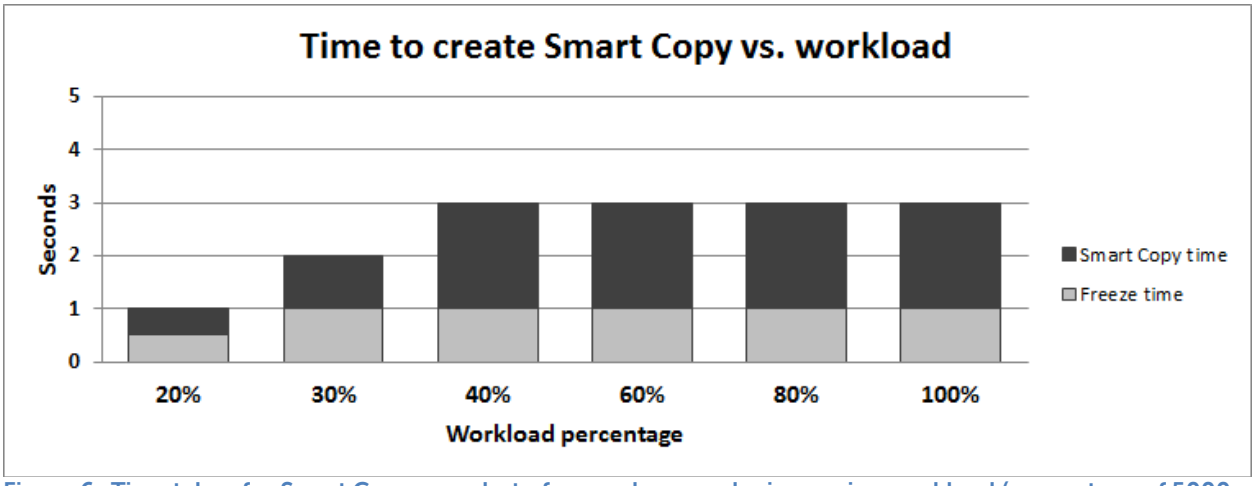


Figure 6 Time taken for Smart Copy snapshot of one volume under increasing workload (percentage of 5000 concurrent users)

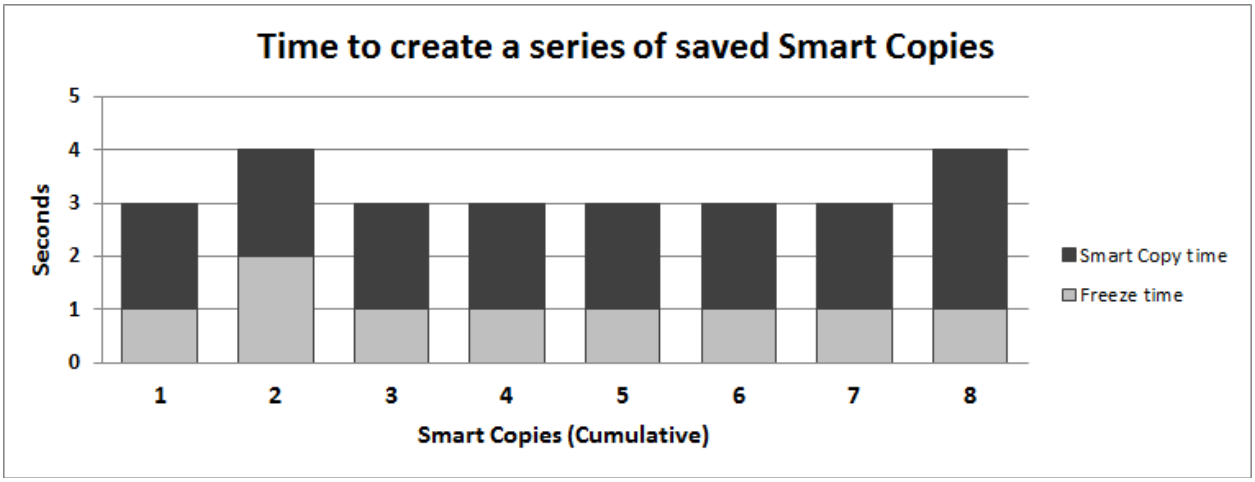


Figure 7 Time taken for 1 to 8 Smart Copy snapshots of one volume under a load of 5000 concurrent users

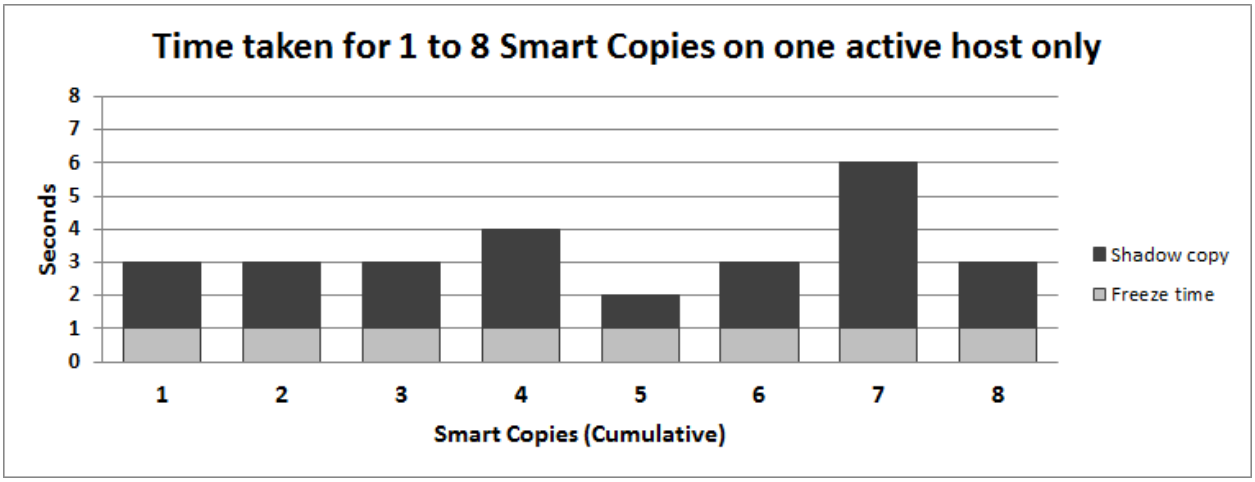


Figure 8 Time taken for 1 to 8 Smart Copy snapshots of one volume under a load of 5000 concurrent users with one active host only

These results clearly show that the process of creating a Smart Copy snapshot had a predictable and minimal duration, with an average time of less than 5 seconds. Also, and most important, the trend did not change with different workload conditions, even when a critical situation was simulated. A minor trend is that the snapshot duration increased slightly when the user load was increased and when the database count running on the same host was increased. This is due to the increased effort required for freezing the I/O in transit which is higher when the user load increases.

6.2 Host resources impact

When collecting performance indicators from a mailbox database server, the focus is generally on storage response time because it has a direct impact on the user experience, but other traditional indicators (processor, memory, and network) should be kept under surveillance as well to ensure overall monitoring of the environment.

With the profile of the users created as a fixed value (Outlook online, Heavy), the increase in storage access from a mailbox server progressed with the amount of workload applied. We retrieved some of the Exchange key performance indicators during all the tests, but the most significant indicators for our analysis were retrieved during the maximum workload.

Table 4 shows the Exchange KPIs that qualified the health of the mailbox database server during the load of 5000 concurrent users while creating and maintaining the cumulative eight Smart Copies. These values are the average of all the samples that were collected during the entire duration of the simulation. We did not identify any specific spike on any of these counters even at the outset of the snapshot process, therefore the identified KPIs where constantly under the recommended thresholds. We omitted the values reported under lighter workload as they were less significant for the analysis as they tracked even better performances.

Table 4 Exchange KPIs during cumulative snapshots with maximum workload

Performance Counters	2 active nodes	1 active node	Microsoft Threshold
RPC information store KPI			
MSExchange IS \ RPC Requests	1.3	5	< 70
MSExchange IS \ RPC Averaged Latency	1.7	1.7	< 10 ms
Active DBs KPI (databases and logs)			
MSExchange Database \ I/O Database Reads (Attached) Average Latency	8.7	9	< 20 ms
MSExchange Database \ I/O Database Writes (Attached) Average Latency	2.5	2.9	< 20 ms
MSExchange Database \ Database Page Fault Stalls/sec	0	0	0
MSExchange Database \ I/O Log Writes Average Latency	1.8	2.4	< 10 ms
MSExchange Database \ Log Record Stalls/sec	0.01	0,02	< 10
Passive DBs KPI (databases and logs)			
MSExchange Database \ I/O Database Reads (Recovery) Average Latency	8.2	N/A	< 200 ms
MSExchange Database \ I/O Database Writes (Recovery) Average Latency	2.4	N/A	< 200 ms
MSExchange Database \ I/O Log Reads Average Latency	2.5	N/A	< 200 ms
MSExchange Replication \ ReplayQueueLength (per database)	<=1	N/A	Low

We further analyzed the four pillar indicators of the system performances: disks, processor, memory, and network, in the quest of a spike of any kind from the described course. All the explored trends did not report any significant deviation, the only noticeable deflection from regular trends we could identify was the one shown below in Figure 9.

While the average utilization of the disk/volume was not changed, we tracked a disk read spike lasting a maximum of 30 seconds each time the Shadow Copy (freeze) initiated its activities. Figure 9 shows the disk read spike on the volume and the disk write pattern which kept a steady trend instead. We also show the disk read operations of the Exchange process (*store.exe*) as well, which we identified as the source of the short spike.

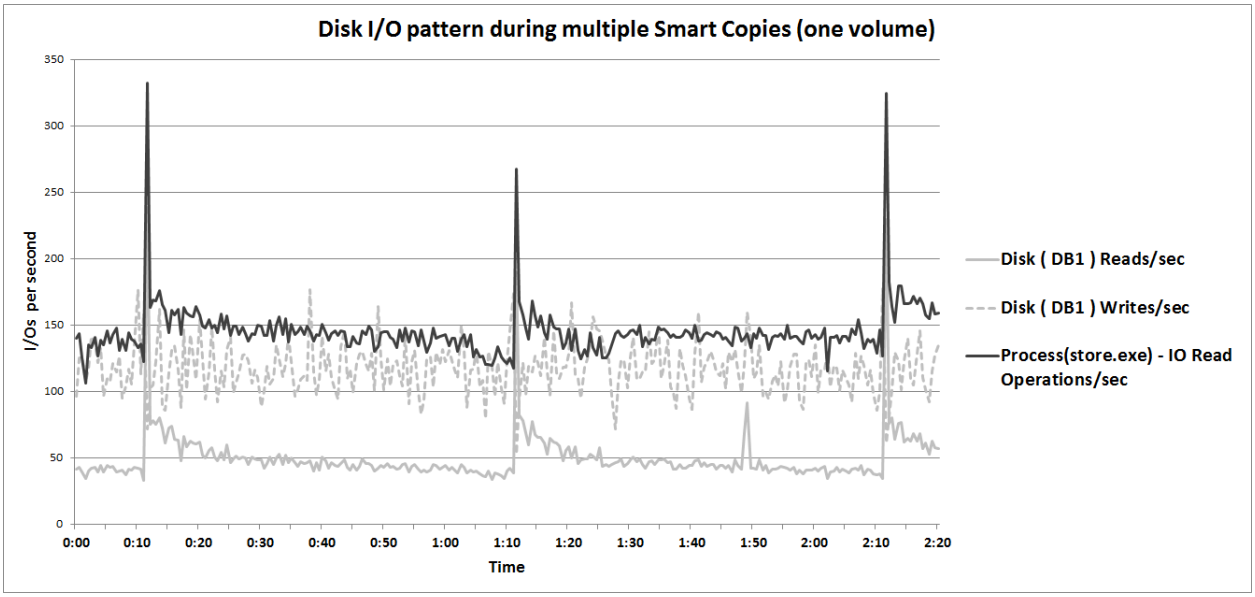


Figure 9 Disk I/O pattern during multiple Smart Copy snapshots on one volume

Note: I/O operations (reads or writes) counter values for processes reported by Performance Monitor include all the operations executed by the process against the entire disk sub-system, not only the volume we are analyzing, nevertheless the reads spike is clearly due to the process reported (store.exe).

The analysis of the Exchange KPIs combined with the systems indicators proved that the host impact while taking Smart Copies was minimal. Not only that the user experience would have been seamless in both regular operation and critical situation, but that the retrieved values matched against the Microsoft thresholds also showed the infrastructure would have room for additional workload, specifically in the storage subsystem.

6.3 Optional ASM/ME functionalities: checksum and verification

The choice to create a mailbox database snapshot has various aims: have offline access to production data to run tests or verification, or reuse the snapshot as a component of a wider recovery mechanism. Either way, one task that is necessary is the integrity check of the data (i.e. Exchange checksum verification). The outcome of this activity is valid collateral for the health of the production environment in one case, or is a signature of the consistency of the data that is available offline within the snapshot.

ASM/ME offers the opportunity to take ownership of this checksum verification process by seamlessly automating the usage of a Microsoft Exchange utility (ESEUTIL.EXE). This action verifies the integrity of the files contained within the Smart Copy snapshot.

The verification process can be activated in different ways:

Immediately	the task runs immediately after the Smart Copy snapshot has been created
On demand	the task runs when activated interactively, on a Smart Copy snapshot previously created
Global verification	the task runs as part of a broader schedule within defined time windows

Remote host the task runs as part of a schedule on a remote server, which has all the ASM/ME and Exchange software components installed (Management tools)

In any of these cases after the checksum runs, the backup document of the Smart Copy is updated accordingly.

We tested the impact of this activity when running on an 'on demand' basis directly on the Exchange host running in the DAG and overhauled the host resources during the running of the checksum verification against the mailbox databases residing in the Smart Copy snapshots. An outline of the operations that were automated by ASM is reported in the following list:

- Submit/schedule the checksum verification
- The snapshot is turned online and presented to the host, mounted as a mount point under the TEMP folder of the user account impersonating the job
- A scripted set of ESEUTIL commands are executed against the files in the volume in order to validate their integrity (checkpoint, logs, database)
- An execution log file (EqlExVerifier.log) is generated under the EqualLogic folder and the Smart Copy backup document is updated with the output of each run of ESEUTIL
- The volume is dismounted, disconnected and the snapshot is set back offline

While most of these steps did not considerably impact the local host resources of the Exchange server, the execution of the set of ESEUTIL commands did. We recorded an average processor utilization of 16% for the ESEUTIL process alone (split across up to 15 threads) when it was running against the files within the Smart Copy snapshot.

The time taken to execute the checksum verification was as reported in Table 5.

Table 5 Checksum verification time taken

File type	Size	Time taken	Bandwidth
Checkpoint (*.chk)	8KB	< 1 sec	N/A
Logs (*.log)	1MB each	< 1 sec each	N/A
Database (*.edb)	420GB	32 minutes	225 MB/second

The entire duration of this task would be variable depending on the amount of logs present in the volume at the time of the snapshot (it can be thousands). The conservative forecast for this duration is evaluated using the formula reported below, which is consistent with the performances of our simulated infrastructure:

$$Checksum\ Duration\ (in\ seconds) = 1 + \ (Number\ of\ logs * 1) \ + \frac{Size\ of\ database\ (in\ MB)}{Bandwidth\ (in\ MB/second)}$$

The checksum burden must be evaluated and should be taken into consideration carefully. The amount of CPU cycles taken by the Exchange command line utility can be added to the regular operation of the reference mailbox server, but, in the case of a critical situation, when the entire user workload of the database is owned by one single host, the additional impact of a running checksum

verification would bring the CPU utilization of the system very close to the upper recommended threshold.

The impact of ESEUTIL on the system can artificially be reduced adding a delay of 1 second for specified numbers of I/O by using the following parameter in the Windows registry (e.g. 1000 identifies the number of IOs):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EqualLogic\ASM\Settings]

"EseutilThrottle"=dword:00001000
```

Or, we advise and reinforce that, in the case where a time window to run this activity locally on the Exchange host cannot be identified, the entire sequence of checksum and verification should be scheduled and off-loaded to a different host connected to the SAN (Global verification). A different set of local resources will be dedicated to this process, either dedicated or shared with other services (usually on a dedicated backup server), and, as a consequence, the Exchange host will not be affected in any way.

For additional information about Dell EqualLogic ASM/ME, refer to the ASM documentation: *Auto-Snapshot manager for Microsoft User Guide*, available at: https://support.equallogic.com/support/download_file.aspx?id=1053
Note: A support account is required in order to access the download area of the website.

7 Recovery scenarios

As we showed how EqualLogic Smart Copy snapshots can be taken in an Exchange environment and overall what the efficiency and the cost will be in term of local host resources, we moved forward in the test plan to verify the recovery scenarios that will directly benefit from the use of these Smart Copy snapshots.

Remember that backup applications integrated in the Microsoft VSS framework, such as Symantec Backup Exec or CommVault Simpana powering a Dell PowerVault DL2200 backup-to-disk appliance, can directly request, create, and access Shadow Copies residing on EqualLogic Smart Copy snapshots. The Exchange database and logs can then be backed up directly from a Smart Copy snapshot through the backup media server accomplishing the result of off-loading host resources and reducing consistently, up to eliminating, the backup windows and the overlap with the activities of users. The integration of such technologies with the EqualLogic Smart Copy technology completes the set of functionalities required in a recovery scenario and provides an end-to-end protection solution.

7.1 Backup mechanisms applied to Exchange recovery

Different backup technologies allow recovering Exchange with different approaches. The method of backup for the store elements of Exchange defines the techniques of possible recovery. Traditional backup types are as follow:

Full Sometimes identified as reference or image, it represents a full point-in-time copy of the store elements selected within the backup catalog.

- **Advantages**
  - A backup set contains all the required data for recovery.
  - It is operationally easier to restore.
- **Disadvantages**
  - A backup set can have large capacity requirements.
  - It requires a longer backup window.

Incremental Provides a copy of the store elements that have changed since, or were not present at the time of the last incremental or full backup.

- **Advantages**
  - It requires less space, proportional with the change-rate of the data.
  - It requires shorter backup windows.
- **Disadvantages**
  - It is operationally more complicated to restore, more backup sets.
  - It requires more time to be restored, proportional with the number of backup sets.
  - It requires the entire sequence of backup sets to be restored.

Differential Provides a copy of the store elements that have changed since, or were not present at, the time of the last full backup.

- **Advantages**
  - It provides balanced window backup and capacity requirements.
  - It requires only two backup sets for a restore (full and differential).
- **Disadvantages**
  - The balance of time and capacity can still be unacceptable if more than one differential is taken before the next full backup.

When applied to a transactional database, such as Microsoft Exchange, incremental and differential backups have been strengthened by transaction log technologies. Performing an incremental or

differential backup is now translated into the transaction logs backup that requires only the copy of the logs generated since the last full backup, and does not include a copy of the entire database file, even if modified.

This technology then requires, at the time of recovery, a process named 'transaction log replay' to integrate all the changes tracked in the transaction logs into a previously restored full backup of a database.

Figure 10 illustrates a simple backup scenario and the operational effort required in order to restore from a transactional logs backup. The components required to recover up to the nearest time to the database failure are a total of 10 backup sets (marked in blue), and must include the most recent full backup (at time T0), each transactional log backup occurred between the full backup and the failure (T1 to T9), and the transaction log replay for all the logs generated after the last transactional logs backup (if the logs are available).

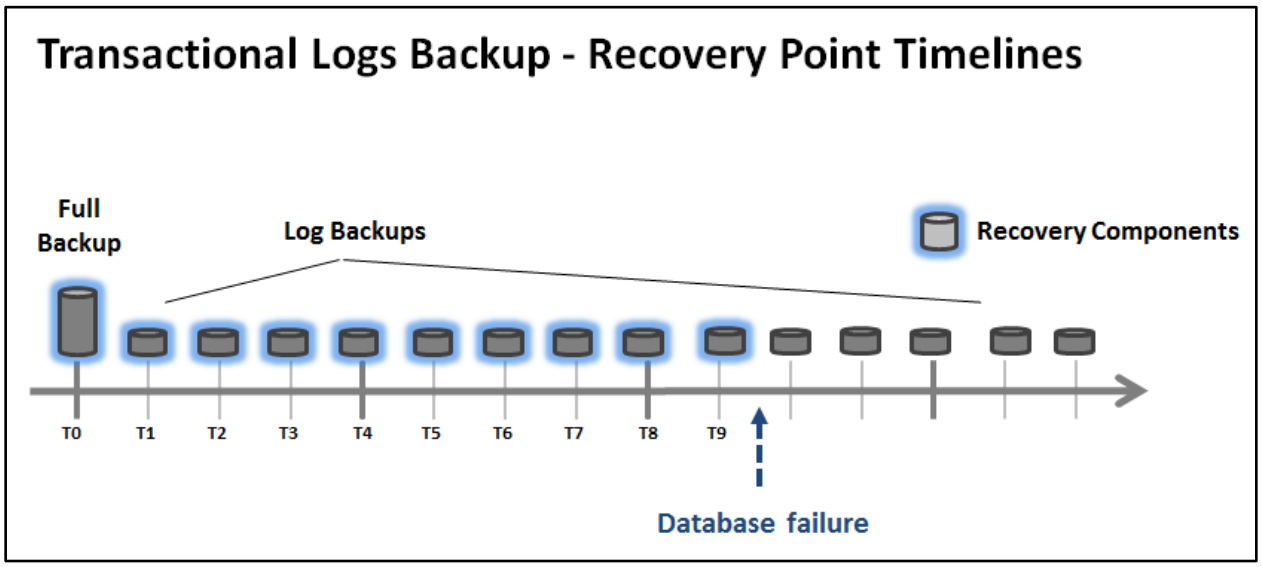


Figure 10 Transactional Logs Backup recovery point timeline

Figure 11 illustrates the operational difference when the Smart Copy snapshot technology is taken into account to protect Exchange mailbox databases. The components required to recover up to the nearest time to the database failure are 2 backup sets (again marked in blue), and should include the most recent Smart Copy snapshot (at time T8), each transactional log backup occurred between the Smart Copy and the failure (T9), and the transaction log replay for all the logs generated after the last incremental backup (if the logs are available).

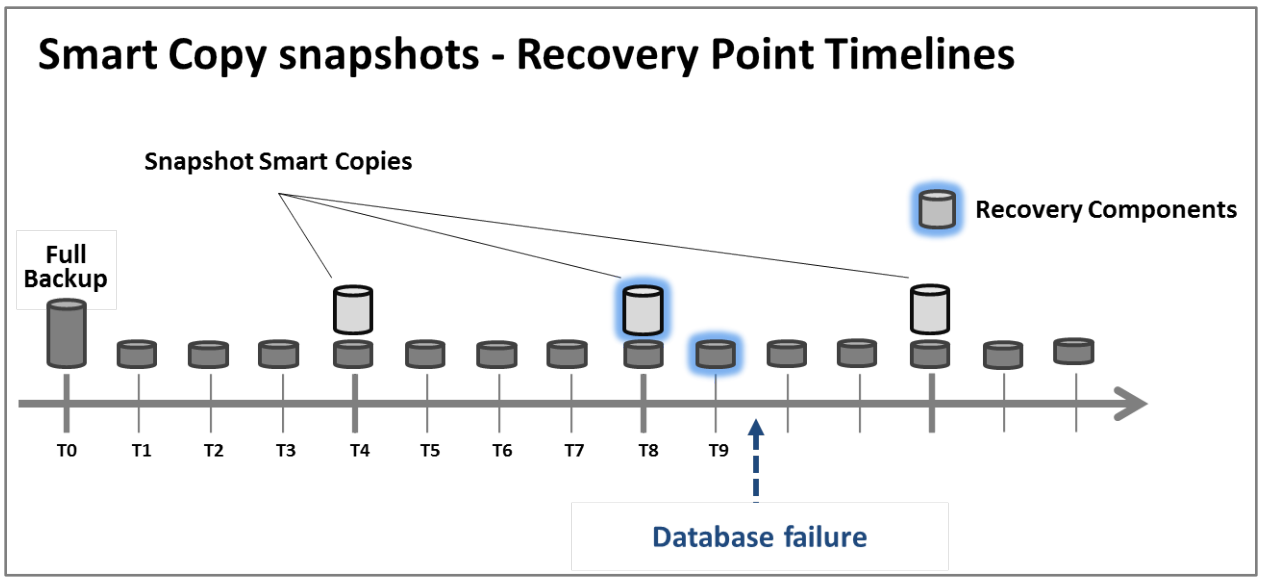


Figure 11 Smart Copy snapshots recovery point timeline

Simplification of the restore operations when using Smart Copy snapshots appears evident. During a database recovery scenario that requires restoring a full backup, an in-place restore of a snapshot will be much more time efficient because there is no data copy from the backup media. Additionally, the number of transactional logs backups to be restored can be considerably reduced in proportion with the frequency of Smart Copy snapshots taken and maintained on the EqualLogic SAN.

Overall, restoring data using Smart Copy snapshots can help considerably improve the achievable RTO of the Exchange environment.

7.2 Testing in-place full restore

Exchange storage administrators are faced with scenarios where damage (corruption, deletion, integrity violation) of the data contained in a mailbox database has occurred and has been transferred to the passive copy of the database in the other node of the DAG before an administrative corrective action has been taken. In such a scenario, using the Smart Copy snapshot, the Exchange database can be restored back to a known good state. Multiple point-in-time copy snapshots can be created and retained without additional increase in management complexity. Further, EqualLogic ASM provides fully automated functionality to restore the database to a point-in-time and replay logs that were not replayed at the time the snapshot was created.

To simulate the recovery task for the scenario outlined above, we tested and recorded the time required to bring back online a Smart Copy snapshot of one of the mailbox databases. Microsoft Exchange Replication Service VSS writer does not support restore operations, so we could operate a restore of a database in a DAG scenario to the active copy only.

First we evaluated the duration of the entire automated process provided out-of-the-box by ASM/ME. This includes restoring the database and applying the outstanding logs. We then simulated the minimal steps required to restore the database from the snapshot and then let the administrator manually apply logs to control the point-in-time state of the database.

Test Details for in-place restore of one database:

Details	Restore of one active database, where the second copy of the database has been suspended.
Key indicators	Time taken for restore

An outline of the operations that are automated by ASM/ME when performing a restore from a Smart Copy set is summarized in the following list:

1. Dismount of the current mailbox database (unless it is already down)
2. As a safety measure, a SAN snapshot of the current volume is taken
3. Integration with the Exchange VSS writer is prepared for the restore
4. Turn offline and disconnection of the original volume
5. Turn online and present to the host of the Smart Copy snapshot. The SAN snapshot assumes the volume role and replace the original volume
6. Transaction log replay and post restore operations performed by Exchange VSS writer
7. Mount of the recovered mailbox database

The outcomes of these operations are tracked in the Application Event Log of the mailbox database server. The *MSExchangeIS Mailbox Store* source tracks the mailbox database status changes (stop, start, and related information), and the *MSExchangeIS* source tracks the output received from the Exchange VSS writer (restore operations), and finally the *ESE* engine source tracks database level operations (integrity check and log replay).

The impact on the host local resources during the restore was imperceptible and limited to a relatively small disk write activity on the volume recovered, due to the transaction log replay. During the transaction log replay the database was offline, and so there was no other disk activity in contention with the recovery process.

The second test case simulates an automated mount of the snapshot and then the manual intervention of the administrator to recover the selected transaction logs. Since the total time taken to replay the logs depends on the number of them to be replayed and also since human intervention is required, the total time can vary for each environment. The amount of transaction logs present inside the snapshot and needed to be replayed to the mailbox database was significantly high, and as such required a consistent amount of time.

The time taken to execute the restore is reported in Table 6. In both test cases the duration of restoring (or mounting) the snapshot from the SAN was the same. The duration of the entire log replay process was variable and related to the number of logs that will be automatically replayed by ASM or manually by the administrator. While the automated ASM task provided a ready-to-access database, the administratively managed recovery was underlying the selection of the required logs.

Table 6 In-place full restore, time taken

Operation	Task	Duration	Next steps
ASM automated restore	Snapshot restore	25 sec	End-user access
	Log replay	548sec	
	Total (end-to-end restore) = 573 sec		
Smart Copy manual restore	Snapshot mount	25 sec	Selective Log replay process
	Log replay	<5 sec/log	
	Total (end-to-end restore) = Variable		

The number of transactions executed in the Exchange memory cache but not yet transferred to the mailbox database file is known as *log checkpoint depth*. This number can be significant when a high load is applied to a mailbox database, as Exchange Server 2010 aggressively keeps more transactions in the memory cache to save on the I/O to disk. The log checkpoint depth within an Exchange Server 2010 DAG configuration is by default higher than usual, varying from the regular 20MB (logs) to 100MB (logs), and because of this increases the number of outstanding logs to be replayed during the recovery operations.

For additional information about Log Checkpoint Depth, refer to Microsoft documentation: *Understanding the Mailbox Database Cache*, available at: http://technet.microsoft.com/en-us/library/ee832793.aspx

7.2.1 Considerations on Smart Copy in-place restore

As illustrated in the previous section, the in-place restore of a Smart Copy snapshot is similar to a restore from a full backup, because the snapshot contains a point-in-time image of the mailbox database. Furthermore the additional elements present on the storage volume (logs, content indexes), and consequentially on the snapshot, would be restored in the original place with the database. As compared to restoring from a full backup copy that requires data transfer from backup media to primary storage, restoring from snapshot provides a much faster and easier method for recovering the following elements:

- Mailbox database (at the level of last checkpoint)
- Transaction logs present on the disk at the moment of the Smart Copy (requiring Log replay process)
- Content Index (ready to be updated by the Search service without a full rescan from the scratch)

In reference to the recovery point timelines illustrated above in Section 7.1 in Figure 10 and Figure 11, the test described in the previous section unmistakably demonstrates how quickly a single Smart Copy snapshot can bring back online a full database at the 'T8' point-in-time while a traditional database recovery approach would have required nine different backup sets to be restored (T0 to T8) – one full database backup followed by eight incremental/transactional log backups.

The remaining portion of data to be restored, elapsed between T8 and T9, should be protected by an integrated backup solution as explained at the beginning of Section 7. This would take the same amount of time to be recovered in either approach (incremental backup or Smart Copy snapshot).

7.3 Testing Brick level recovery

In addition to performing in-place recovery of the Exchange databases, EqualLogic Smart Copy snapshots can be mounted as recovery databases to perform granular or brick level recovery. The goal of this test was to establish the time required to use a Smart Copy snapshot as an optional source of granular restore capability for user mailboxes or leaf objects (folders). The scenario addresses a real world situation where an Exchange administrator has reduced or disabled the quotas for the recoverable items feature, for example, to reduce the size of the database, to remove self-recover abilities from users, or for legal compliance. In these cases, the administrator can take advantage of snapshots to enable brick level recovery (at an administrative level only).

Test Details for the Recovery Database restore and setup:

Details Restore of one database, automatic configuration of a recovery database (or RDB)

Key indicator Time taken for restore

The tasks undertaken by ASM/ME are reported below:

1. Turn the Smart Copy online and present it to the host, on the mount point specified interactively
2. Automatic setup of an RDB pointing to the restored Smart Copy snapshot
3. Mount of the recovered mailbox database

Once again the outcomes of these operations were tracked in the Application Event Log of the mailbox database server (*MSExchangeIS Mailbox Store* and *ESE* engine). The host local resources were not impacted at all.

Table 7 reports the time taken to restore the Smart Copy snapshot and setup/mount the Exchange RDB.

Table 7 Brick level recovery, time taken

Operation	Task	Duration	Next steps
ASM automated RDB	RDB removal	20 sec (if present)	Administrator access
	Snapshot restore	25 sec	
	RDB setup	387sec	
	Total (end-to-end restore) = 412 sec or 432sec (in case of RDB already present and to be removed)		

When an RDB is mounted, it is available for administrative access only with limited protocols and at the command line exclusively. After the recovery database has been mounted, the time taken to recover any leaf object is dependent of type of object being recovered and hence is variable as per your

environment. The times presented in Table 7, however, show an example of how soon the administrator can start recovering mailbox items from the recovery database.

For reference only, we show a PowerShell command that can be used to restore data from an Exchange RDB. Where 'RecoveryDBn' is the name of the RDB, and 'John Smith' and 'TempJSmith' are examples of the source and target mailboxes names (using a mixed syntax of DisplayName and Alias attributes).

```
      [PS]>New-MailboxRestoreRequest -SourceDatabase 'RecoveryDBn'
-SourceStoreMailbox 'John Smith' -TargetMailbox 'TempJSmith'
```

7.4 Restore the high availability level in a DAG

The seeding activity is required when establishing a mailbox database copy in a DAG environment. During normal DAG operations, the passive copy of the database is kept in sync with the active copy by the log shipping and replay processes taken care by the Exchange Replication service. It can occur for administrative or unforeseen reasons that the passive copy is taken offline, is in a failed state, or goes out of sync from the active copy and requires not only a regular re-sync process, but a full update to return to normal operations. Reseeding the database after such a failure could take a long time and consume valuable resources on Exchange hosts. To bring back the DAG to its data redundancy status, it is important to minimize the time it takes to reseed a failed database. In this section, we will first look at the resource consumption by the Exchange seeding processes and then show how EqualLogic Smart Copy snapshots can help to avoid long reseeding times and resource consumption on the Exchange hosts.

Note: For planned maintenance on passive database nodes, Exchange administrators have the opportunity to suspend, and then resume, the replication activity. The suspension causes a side effect where the log truncation is frozen for the entire suspension time. Because the logs can fill up the volumes, depending on the load on the database, sometimes it can be more convenient to stop the replication and delete the copy if the planned suspension is too long.

The initial seeding or the full update proceedings are very similar in nature. They both require a complete transfer of the copy of the database, and generally of the Search Catalog also, unless it is planned to have the content index generated from scratch on the passive side, which causes resource consumption on the target Exchange host.

In the following tests, first we study the impact of DAG seeding/reseeding on the Exchange host resources. Then we prove how to increase the level of protection of a DAG in case of a temporary fault, with the help of the SAN infrastructure. We assessed the impact of seeding or reseeding a mailbox database copy over the IP network using the Exchange Replication service, then we checked the differences when executed using the iSCSI SAN network, off-loading the local host resources.

7.4.1 Testing the impact of DAG seeding over the network

We ran the tests with and without user load to identify and isolate the impact on local host resources. We decided to show the data of the scenario without user load because it better shows the resource utilization and the isolation of the activities was more identifiable.

We configured a dedicated 1Gbps network (see Appendix A3.2) between the two nodes of the DAG to handle the Replication traffic required for regular and exceptional DAG seeding procedures. First we used this network to measure the load of the seeding and reseeding procedures on the DAG hosts.

Test Details for one database, seeding process using the Replication network:

Details	Initial seeding or reseeding of the database using Exchange Replication service
Workload	No user workload applied
Key indicators	Host resources impact

The seeding activity can be started by the Exchange Management console or the PowerShell command line. We used the command line shown below (server and database names are reported with wildcards as the commands were reused differently during multiple instances of the same test). Additional command line options were not included because they were not essential to the tests. While running, both of these command lines immediately started the file transfer copy.

The commands for initial mailbox database seeding (including the content index), create the database copy object, and replicate the data:

```
[PS]>Add-MailboxDatabaseCopy -Identity DBn -MailboxServer MBXn
-ActivationPreference 2
```

The commands for full update of a mailbox database (including the content index) and replicating the data of a pre-existing database copy:

```
[PS]>Update-MailboxDatabaseCopy -Identity DBn\ MBXn
```

Figure 12 shows the data flow for a DAG seeding activity over the network.

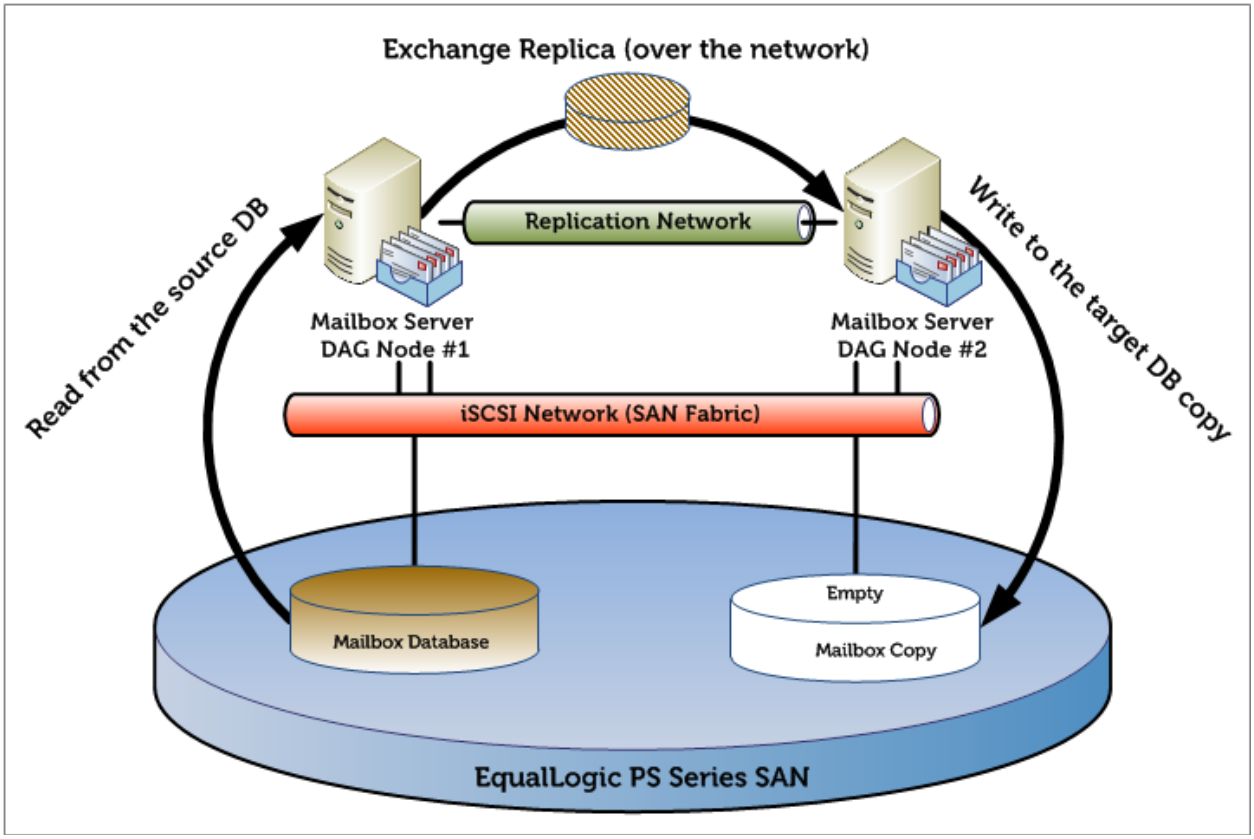


Figure 12 DAG seeding process data flow with Exchange replication over the network

Figure 13 and Figure 14 illustrate the CPU impact reported on both the source and target servers while proceeding with the mailbox database seeding. We show that the *msexchangerepl.exe* process running the Exchange replication service is the service responsible for the CPU utilization impact. The average processor utilization on the host servers was 15% on the source and 27% on the target, mostly attributed to the seeding process activity.

The last quarter of the test duration reported a different behavioral pattern of the Exchange replication service, with a sudden demand for increased processor cycles on the source and decreased on the target host. The root cause of the change was the sequential copy activity embedded in a seeding process (mailbox database and then content indexes). The seeding copy at that point switched from a single large file copy (database) to a group of smaller files (indexes), owned and accessed by different processes (*Information Store* initially and then *Search Indexer*). The additional short CPU load on the target server immediately after the database file copy was due to the database mount activity, while still proceeding with the index files transfer.

Note: Processor utilization counter values for all processes are calculated by Performance monitor against one logical processor only. We have computed the real values against our case of four logical processors to have a graphical comparison between total and per-process processor utilization.

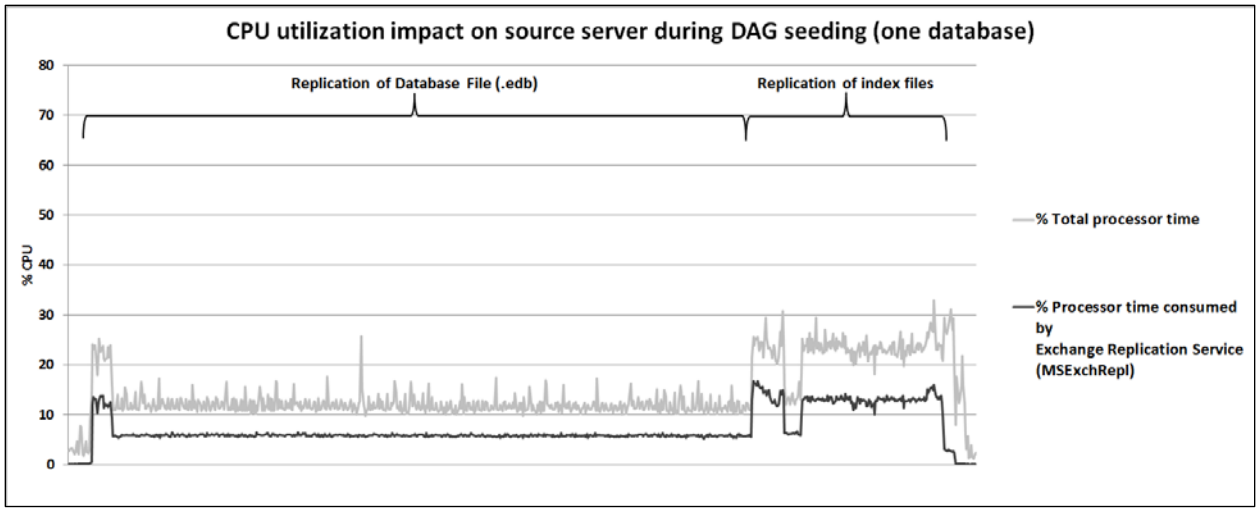


Figure 13 DAG seeding (1 database) over the replication network: source host CPU impact

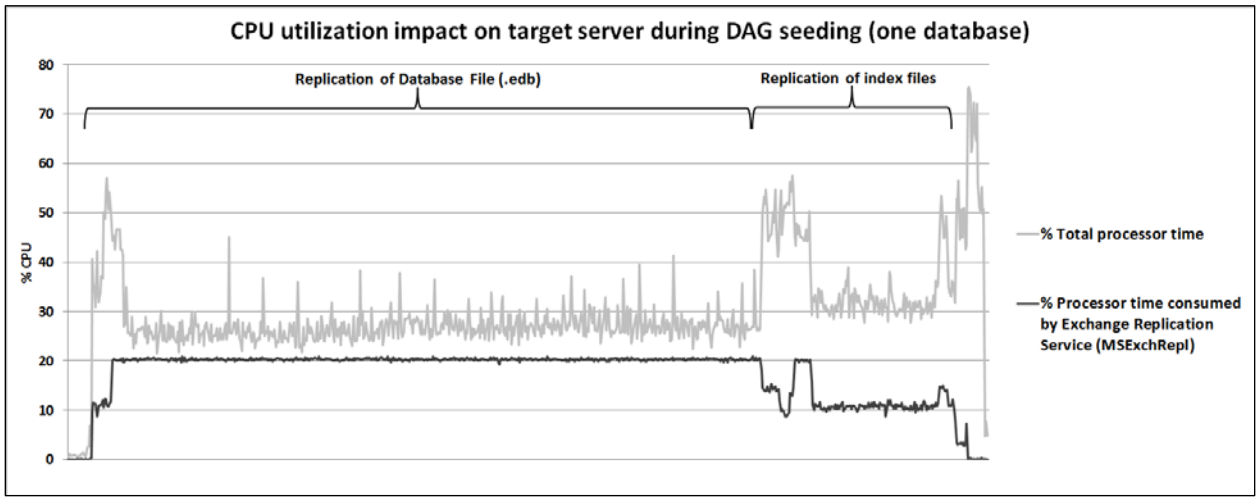


Figure 14 DAG seeding (1 database) over the replication network: target host CPU impact

In order to further understand the load on local host resources, we analyzed the disk access to both the source and target volumes, focusing on disk read access on the source and disk writes access on the target.

Figure 15 and Figure 16 show the disk access patterns of the two volumes used by the mailbox database copy process.

Note: The counter values for I/O operations (reads or writes) for processes reported by Performance Monitor include all the operations executed by the process against the entire disk sub-system, not only on the volume we are analyzing. Still, we reported them here because the monitored process matched the pattern of the volume access.

As illustrated previously in this section we found confirmation that during the operations all the source volume reads were handled by the Information Store during the timeframe of the pure database copy and when the mailbox database was mounted and then handled directly by the Replication service during the transfer of the Content Index. This would also explain the Replication service processor utilization increase during the last phase of the copy (when transferring the Content Index). This is

when the Replication service was executing the network transfer and also reading from the source volume.

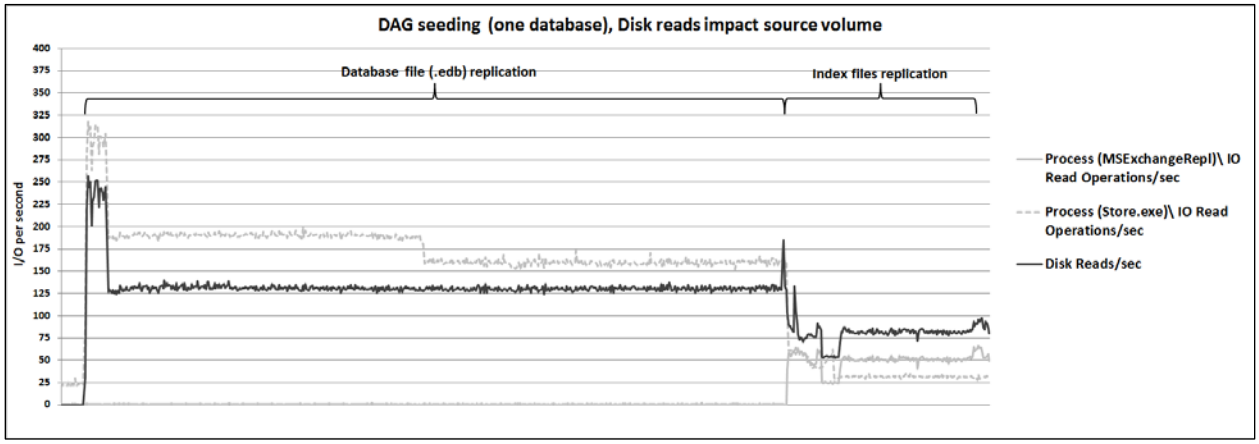


Figure 15 DAG seeding (one database) over the replication network: source volume impact

On the target we verified, as expected, that the Replication Service executed the vast majority of disk writes, while the Information Store had a reduced impact because the target database was dismounted at the time of the copy until the end of the database copy process.

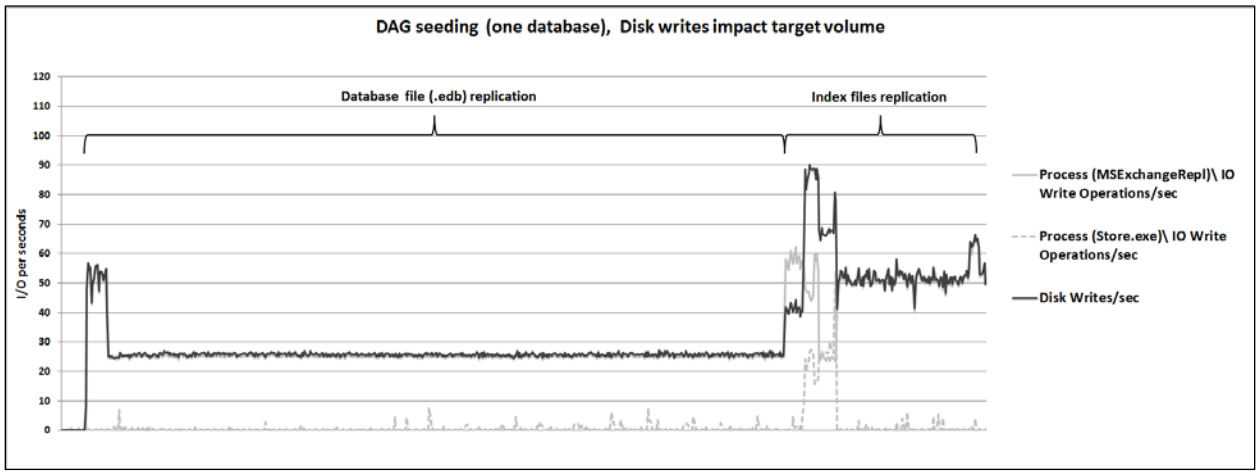


Figure 16 DAG seeding (one database) over the replication network: target volume impact

The last area we analyzed to fully understand the outcome was the network utilization pattern. The Exchange Replication dedicated 1GbE network was consistently utilized at close to 50% of the bandwidth available for the entire database copy process, and then was utilized nearly 30% during the multiple index files copy process.

The analysis of the seeding activity over the network clearly showed a considerable impact on the local host resources. We illustrated not only the bandwidth consumption on the replication network but also the CPU cycles utilization on both nodes and disk access on the source copy.

7.4.2 Testing DAG seeding supported by the SAN

When we came to the scenario where the seeding process could be helped by using a SAN based snapshot, we realized we had two different situations to address. We ran tests again with both user load and no user load, but there was no substantial difference for the performance at the SAN level.

We simulated a scenario where a DAG environment was running and was already protected by the Smart Copy snapshots on both nodes. In this context we had the advantage of starting the recovery process from the pre-existing snapshots on the node that owned the mailbox database passive copy.

Test Details for one database with the seeding process using the iSCSI SAN network:

Details	Reseeding of the database using a Smart Copy snapshot
Workload	User workload applied or not
Key indicator	Host resources impact

The steps needed to recover the required data on the target volume were as follows:

1. Create the definition of the mailbox database copy
2. Select the most recent SAN snapshot of the volume containing the target database mailbox copy
3. Proceed with a Soft recovery procedure by ASM/ME (if not already done)
4. For safety, proceed with a Checksum verification procedure by ASM/ME (if not already done)
5. Mount the Smart Copy snapshot to the target host
6. Resume the regular activity of Exchange Replication service for this mailbox database copy
7. Wait while all the transaction logs (generated between the point-in-time when the Smart Copy was taken and the copy was resumed) are transferred and replayed to the passive database

Figure 17 shows the data flow for a DAG reseeding process using a Smart Copy on the iSCSI SAN.

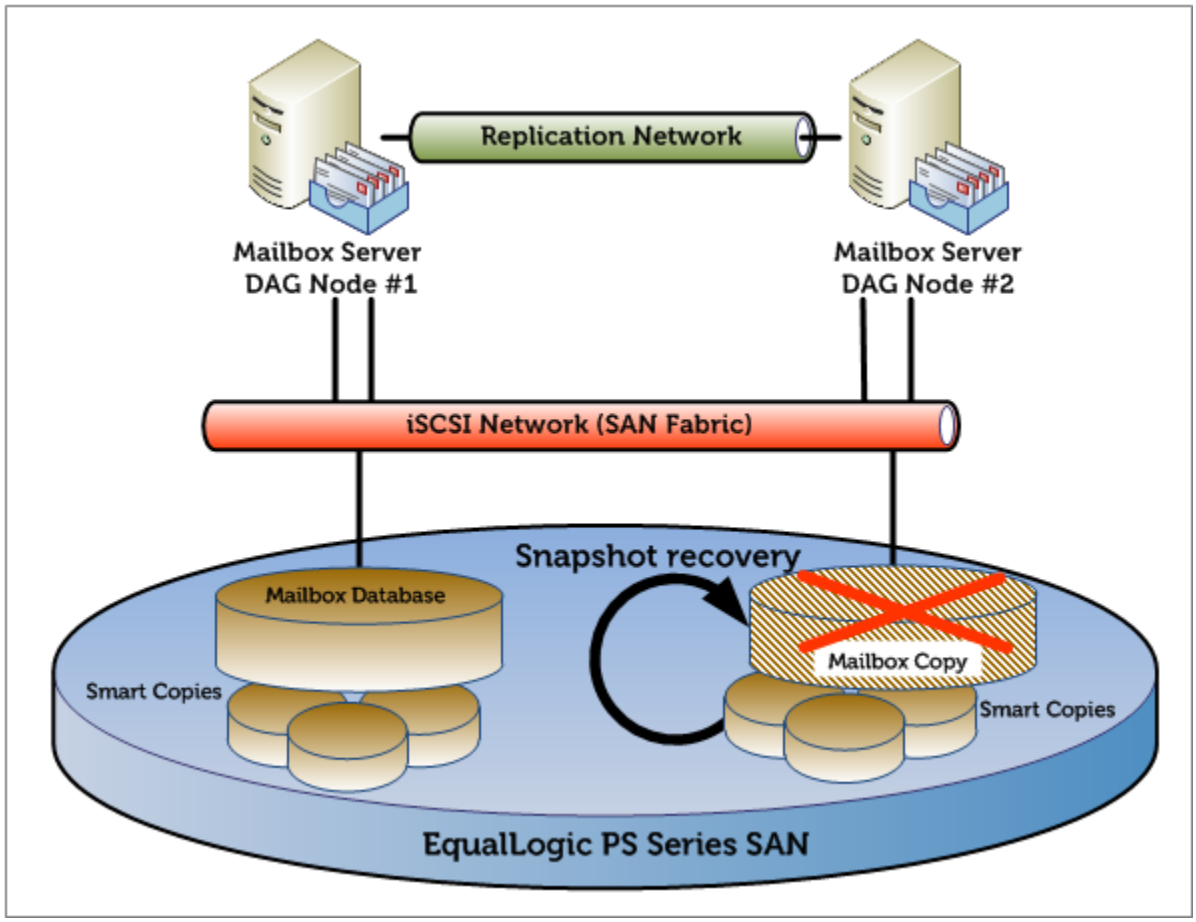


Figure 17 DAG seeding process data flow when reseeding from a preexisting Smart Copy snapshot

We compared the time taken to restore the data redundancy of one database across the two Exchange DAG nodes in case of loss of the secondary copy (corruption, deletion, etc.).

- In the first case we measured the time taken for seeding over the network with the native Exchange Replication mechanism
- In the second case we restored a Smart Copy snapshot from the SAN on the second node and then resumed the database replication in order to re-sync the database delta from the time the snapshot was taken to the current time at the primary database copy

We simulated the loss of the redundant database copy after 50 minutes from the last snapshot, so we then had around 1100 outstanding logs generated on the source node ready to be copied to the second node and replayed to the database copy. As shown in Table 8, our test took 243 minutes for Exchange reseeding over the replication network, however, when assisted by EqualLogic Smart Copy snapshot, the time taken to reseed was only about 15 minutes. This clearly shows the benefit of using snapshots to improve the time it takes to bring back the availability level of a DAG.

Table 8 compares the results from the two scenarios described above.

Table 8 Seeding over the network versus seeding supported by SAN

Operation	Items	Throughput	Duration
Seeding over the network	DB + Indexes	153 GB/h	Total (end-to-end restore) = 243 minutes
Operation	**Task**		**Duration**
Reseeding from Smart Copy snapshot	Snapshot restore		25 seconds
	Soft Recovery		9 minutes
	Replica Resume (copy logs part)		1 minute
	Replica Resume (log replay part)		5 minutes
			Total (end-to-end restore) <= 15 minutes

We then identified a scenario where an Exchange administrator is setting up a new DAG node, or he is recreating a volume after it has been deleted for administrative reasons. In this context, we have the original mailbox database copy, residing in the Primary pool of the EqualLogic SAN and protected by Smart Copy snapshots, but do not have any data available in the Secondary pool. The requirement was to copy all the volume data across the iSCSI SAN network instead of using the Exchange Replication service.

Test Details for one database, with the seeding process using the iSCSI SAN network:

Details Initial seeding of the database using a Smart Copy snapshot across two different pools

Workload User workload applied or not

Key indicators Host resources impact

The steps needed to recover the required data on the target volume were as follows:

1. Create the definition of the mailbox database copy
2. Select the most recent SAN snapshot of the volume containing the source database mailbox copy
3. Proceed with a Soft recovery procedure by ASM/ME (if not already done)
4. For safety, proceed with a Checksum verification procedure by ASM/ME (if not already done)
5. Create a clone of the snapshot (it will be assigned to the same storage pool)
6. Modify the new volume (cloned), setting its pool assignment to the target pool
7. Monitor the volume move to ensure it is happening correctly
8. Mount the new volume to the host connected to the target pool
9. Resume the regular activity of Exchange Replication service for this mailbox database copy

10. Wait while all the transaction logs (generated between the point-in-time when the Smart Copy was taken and the copy was resumed) are transferred and replayed to the passive database

Figure 18 shows the data flow for a DAG initial seeding process using the iSCSI SAN.

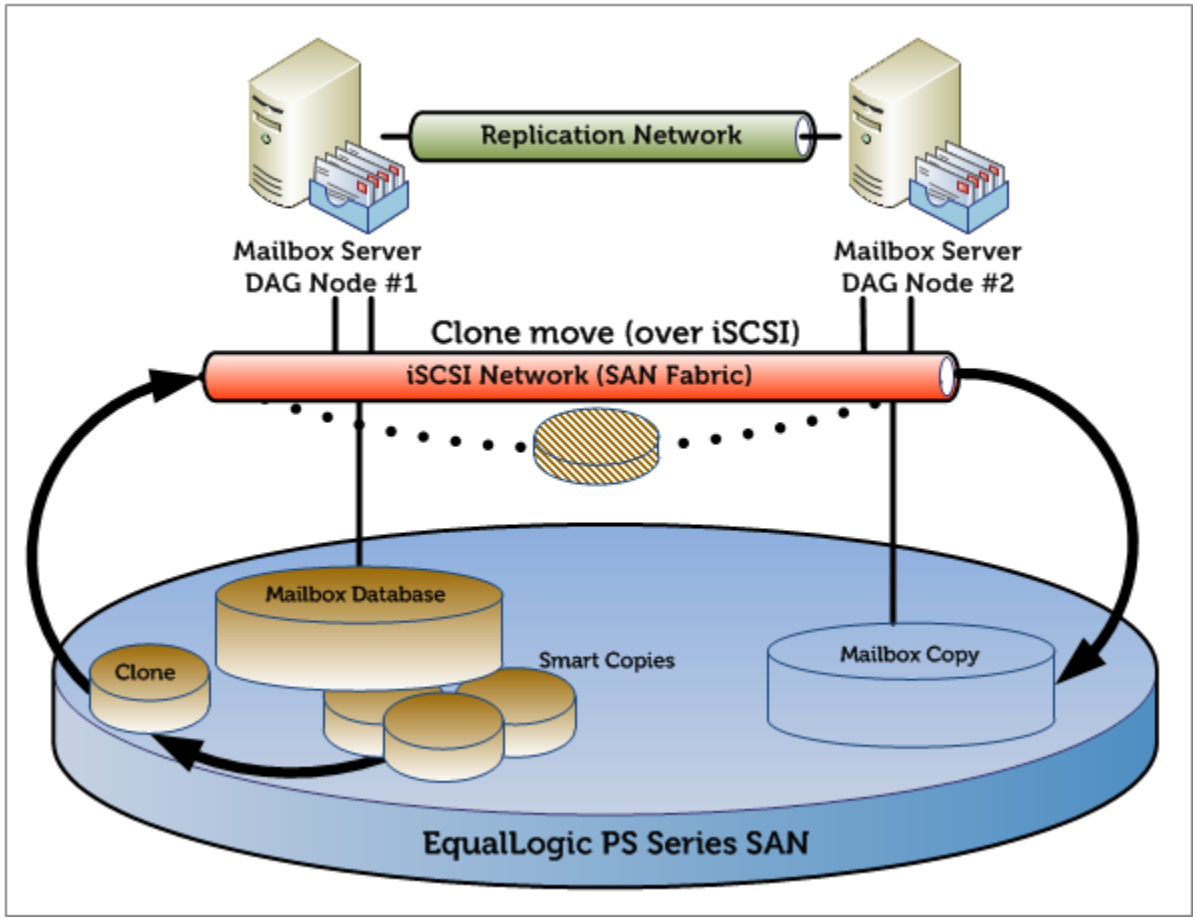


Figure 18 DAG seeding process data flow when seeding from a cloned Smart Copy snapshot

Table 9 shows a summary of the activity executed in each scenario.

Table 9 Seeding supported by SAN summary

Reseeding from a Smart Copy snapshot	Seeding from a cloned Smart Copy snapshot	Duration of each step
Define mailbox copy		5 seconds with PowerShell commands
Snapshot selection		Administrator intervention
Smart Copy soft recovery		Average <1 minute
Checksum verification		Proportional with DB size
N/A	Create a clone	5 seconds with the Group Manager GUI
N/A	Reassign cloned volume	5 seconds with the Group Manager GUI
N/A	Clone move	Proportional with the amount of GB to transfer and with the network bandwidth available on the iSCSI network
N/A	Mount the volume	Around 25 seconds
Mount Smart Copy	N/A	Around 25 seconds
Resume replication		5 seconds with the Exchange Management
Transaction log replay		Proportional with the number of logs

The outcomes of these two sets of tests proved that having a Smart Copy snapshots recovery strategy in place helped in off-loading the application hosts from the burden of the seeding activities. All the steps undertaken to recover the volume, and then the mailbox database copy, had no effect whatsoever on the hosts as they were performed on the EqualLogic SAN and on the iSCSI network directly (except for the transaction log replay), leaving all the host resources available to perform the regular Exchange Server tasks.

7.4.3 Seeding operations details

Seeding a mailbox database copy is possible even without starting the data transfer immediately at the time of the copy definition. Some options are not supported within the Exchange Management console, so the PowerShell CLI was used to issue the commands for this specific case.

The command for the initial mailbox database seeding (including Content Index) by creating the database copy object without replicating the data:

```
[PS]>Add-MailboxDatabaseCopy -Identity DBn -MailboxServer MBXn
-ActivationPreference 2 -SeedingPostponed:$TRUE
```

In the test case where a previous mailbox database was present, but a full update was required (for example, a corrupted database), we initially eliminated the passive copy as shown in the command below and deleted the remaining files from the volume:

```
[PS]>Remove-MailboxDatabaseCopy -Identity DBn\ MBXn
```

When the Smart Copy snapshot was recovered or the cloned volume was moved to its final location, we resumed the Exchange Replication service activities with the command below:

```
[PS]>Resume-MailboxDatabaseCopy -Identity DBn\ MBXn
```

Finally, to quickly monitor the status of the mailbox database copies and of the Content Index (not reported in the Exchange Management console GUI), we used one of the commands below:

```
[PS]>Get-MailboxDatabaseCopyStatus -Identity DBn\ MBXn
```

Or

```
[PS]>Get-MailboxDatabaseCopyStatus -Server MBXn
```

Note: When using the *SeedingPostponed* option associated with a point-in-time image copy of a mailbox database, we must ensure all the transaction logs from when the Smart Copy first occurred are preserved and available for the final transaction log replay process.
The transaction log chain must be maintained in order to be able to perform the full recovery required.

8 Best practice recommendations

We recommend the integration of Dell EqualLogic snapshots managed by Auto-Snapshot Manager as a complementary solution to Microsoft Exchange 2010 data protection. The benefits of this solution include reducing the over-provisioning of resources for backup activities on Microsoft Exchange production servers and curtailing the RTO allowed by an infrastructure correctly integrated with a traditional backup system.

Overall, the usage of Smart Copy snapshots addresses the challenges of both regular operations and critical situations. They are able to increase the level of protection by supporting a highly available environment, reducing the need for additional mailbox database copy deployments in a local datacenter.

Some things to keep in mind when planning to integrate these technologies into a production messaging infrastructure are as follows:

Plan for achievable RTO

Smart Copies streamline the recovery process when used in conjunction with transactional log backup sets provided by a third-party backup tool. The combination of these two technologies can considerably shrink the recovery time based on traditional technologies alone. Verify the level of integration with the third-party backup tool to integrate with.

Aggressively reducing the RTO has the disadvantage of requiring more snapshots to be created and can increase capacity requirements of your primary storage.

Understand the RPO requirements

Smart Copies provide brick level recovery capability in minutes. It is a best practice to match the frequency of the snapshots with the RPO when possible. If the RPO requirements are too granular, coordinate the snapshot creation process with native Exchange Server recoverable items to achieve a good compromise.

Monitor the production infrastructure

Informed decisions can only be made when you know the characterization of the workload. Before implementing a Smart Copy plan, monitor and understand the amount of load on the messaging environment, the rate of change, and the number of hourly/daily transaction logs produced per database.

Test the recovery process

Smart Copies have an intuitive GUI and provide command line options for operation. The integration with third-party backup tools can be limited or not, depending on the solution selected. Implement a recovery plan and test it regularly to verify that every choice is appropriate for your environment. The recovery of a production environment is a stressful process and to be successful it requires preparation.

Smart Copy snapshots versus SAN snapshots

Remember that ASM/ME is integrated with the application layer in Microsoft Exchange. Do not use direct SAN snapshots (for example, by using the PS Series group manager) to protect Exchange mailbox databases, because they will not be application-consistent.

Protect the ASM/ME backup documents

The default location for the ASM/ME backup documents is on the local disk of the host where ASM/ME is installed. Protect these documents by using a network or shared folder that is regularly backed up. The loss of a backup document will break the link between the Smart Copy and its corresponding SAN snapshot.

Capacity planning for Smart Copies

Snapshot reserve has a predictable utilization when the workload profile is known. Verify the workload against a real Smart Copy and plan accordingly for the percentage of space allocation required for the reserve area.

Creating ASM/ME Smart Copies

Plan to use the interactive scheduler or the command line to implement more time precise snapshots.

In case of high resource contention, do not schedule a large number of Smart Copies to be created at exactly the same point in time. Use a time off-set when appropriate.

Verify database consistency

Plan to regularly execute the checksum verification on the Smart copy snapshots. Use remote hosts or global windows features to create the most suitable schedule for this process, and offload the checksum processing from the mailbox database server.

Exchange mailbox databases layout

Do not create more than one Exchange mailbox database on a single volume. The Smart Copy snapshot operating unit is an entire volume; every object present on it will be saved and recovered accordingly. Plan to recover only the granular elements that have been damaged, nothing more.

The use of collections in ASM/ME is allowed. A Smart Copy of a collection of volumes containing multiple databases is treated as a single logical element and is backed up and recovered as a unit. Recovery from a collection to an Exchange Recovery Database is the only exception to the previous rule. A single database will be extracted from the collection and recovered.

Isolation of databases and logs is not required anymore in Exchange Server 2010 when deployed in a highly available configuration (DAG). Smart Copy interaction with the Exchange VSS writer requires database and log volumes to be protected by the same snapshot (or snapshot of a collection of volumes). Consider not splitting the database and logs into different volumes unless other restrictions apply, because you will risk causing a torn Smart Copy.

VSS timeout

Under rare circumstances of extreme load, the VSS service can time out when a requester makes an inquiry to create a shadow copy. Follow Microsoft resolution advice to correct this problem. Evaluate an increase of the VSS timeout value in the registry configuration editor if required.

General network best practices

- Use separate network infrastructures for the isolation of the LAN traffic from the SAN traffic (iSCSI).
- Use redundant elements (switches, ISLs) to provide a reliable network infrastructure
- Enable flow control for the switch ports where the PS Series arrays are connected
- Enable jumbo frames (large MTU) for the switch ports where the PS Series arrays are connected
- Disable spanning tree for the switch ports where the PS Series arrays are connected, and enable Portfast instead
- Evaluate jumbo frames (large MTU) for the LAN network when appropriate (limited by type of devices the traffic traverses)

General storage best practices

- Dedicate separate pools for databases connected to nodes in a DAG. Do not share the same disks for active and passive copies of an Exchange mailbox database.
- Choose the appropriate RAID level.
    - RAID-50 offers a good combination of performances and capacity requirements for Exchange mailbox database deployments
    - RAID-10 offers greater write data operations at a lower capacity levels
    - RAID-5/6 offer good performances and greater capacity. Supported by Microsoft, and requires careful validation if considered for deployment.
- Distribute the controllers network port connections appropriately to each network switch
- Use MPIO DSM provided by EqualLogic HIT Kit

General ESX and Virtual Machines best practices

- Use separate virtual switches for Virtual Machines with network traffic and iSCSI storage traffic
- Use Port Group and VLAN tagging to logically segregate different kinds of LAN traffic
- Enable jumbo frames (large MTU) for the iSCSI virtual switch
- Evaluate jumbo frames (large MTU) for the Virtual Machines virtual switch as well
- Use at least two physical network adapters for each virtual switch to achieve redundancy
- Use a guest OS iSCSI initiator when using ASM/ME to allow client integration with the SAN
- Use performance optimized network adapters of the type VMXNET3 for guest iSCSI connections (VMware tools required)
- Enable TSO and LRO on the guest network adapters for iSCSI storage traffic
- Do not allocate more virtual CPU than is really required in the virtual machines
- Do not overcommit memory on ESX hosts. Exchange virtual machines have a memory intensive workload.

General Exchange best practices

- Use Basic disk type for all the EqualLogic volumes
- Use GUID partition table (GPT) for Exchange volumes
- Use default disk alignment provided by Windows 2008 or greater
- Use NTFS with 64KB allocation unit for Exchange databases and logs partitions
- Deploy physically separated disks for guest Windows Operating System and Exchange data
- Isolation of logs and database is not required when deployed in a DAG
- Do not use circular logging when planning for granular recovery by the transaction log replay process
- Leave background database maintenance enabled (24x7) and account for the load
- Use dedicated network and network adapters to segregate Replication traffic in a DAG

Note: For general recommendations and information about Dell EqualLogic PS Series arrays, refer to: Dell EqualLogic Configuration Guide, available at: http://www.delltechcenter.com/page/EqualLogic+Configuration+Guide

Appendix A Test configuration details

A.1 Hardware configuration

Table 10 lists the details of the hardware components required for the configuration setup:

Table 10 Configuration – Hardware components

Test configuration – Hardware components:	
Servers	• Dell PowerEdge M1000e Blade enclosure • Dell PowerEdge M710 Blade Server o 2x Quad Core Intel® Xeon® X5570 Processors, 2.93 GHz, 8M Cache o RAM 64 GB o 2x146GB 15K SAS (RAID-1) o 4x Broadcom NetXtreme II 5709S Dual Port GbE Mezzanine Card • Dell PowerEdge M610 Blade Server o 2x Quad Core Intel® Xeon® E5520 Processors, 2.26 GHz, 8M Cache o RAM 32 GB o 2x73GB 15K SAS (RAID-1) o 2x Broadcom NetXtreme II 5709S Dual Port GbE Mezzanine Card
Network	• 2x Dell PowerConnect M6220 Blade Switches o installed in M1000e blade enclosure fabrics A1 and A2 • 2x Dell PowerConnect M6348 Blade Switches o installed in M1000e blade enclosure fabrics B1 and B2 • 2x Dell PowerConnect 6248 Switches o rack installed
Storage	• 4x Dell EqualLogic PS6000XV o Dual 4-port 1GbE controllers (Firmware 5.0.5) o 16 x 450GB 15K SAS disks (RAID-50)

A.2 Network configuration

Two physical networks were built in order to provide full isolation between regular IP traffic and iSCSI data storage traffic. Also, each IP network was segregated from the others by the use of VLANs with tagged traffic. In order to achieve network resiliency for hardware faults, we paired (stack or lag) at least two physical switches for each network.

Table 11, Table 12, and Table 13 summarize the different networks required for the configuration setup and their usage:

Table 11 Configuration – Switch modules

Switch Module	Placement	Purpose
PowerConnect M6220 #1	M1000e I/O Module A1	Regular IP traffic
PowerConnect M6220 #2	M1000e I/O Module A2	Regular IP traffic
PowerConnect M6348 #1	M1000e I/O Module B1	iSCSI data storage traffic
PowerConnect M6348 #2	M1000e I/O Module B2	iSCSI data storage traffic
PowerConnect 6248 #1	Rack	iSCSI data storage traffic
PowerConnect 6248 #2	Rack	iSCSI data storage traffic

Table 12 Configuration – Hosts to switches connection

Server	Interface	Number of NIC ports	Purpose
PowerEdge M710	LOM on A1	2	Regular IP traffic
	LOM on A2	2	
	Mezzanine Card on B1	2	iSCSI data storage traffic
	Mezzanine Card on B2	2	
	Total ports = 8 (4 on Fabric A, 4 on Fabric B)		
PowerEdge M610	LOM on A1	1	Regular IP traffic
	LOM on A2	1	
	Mezzanine Card on B1	1	iSCSI data storage traffic
	Mezzanine Card on B2	1	
	Total ports = 4 (2 on Fabric A, 2 on Fabric B)		

Table 13 Configuration – VLANs

VLAN ID	Switch it is implemented on	Purpose
100	PowerConnect M6220	Management (Service Console)
200	PowerConnect M6220	Public (Corporate)
300	PowerConnect M6220	Replication (Exchange)
1 (default)	2x PowerConnect M6348 2x PowerConnect 6248	iSCSI

Figure 19 presents the diagram of the network connections between the 4 blade servers and the storage arrays:

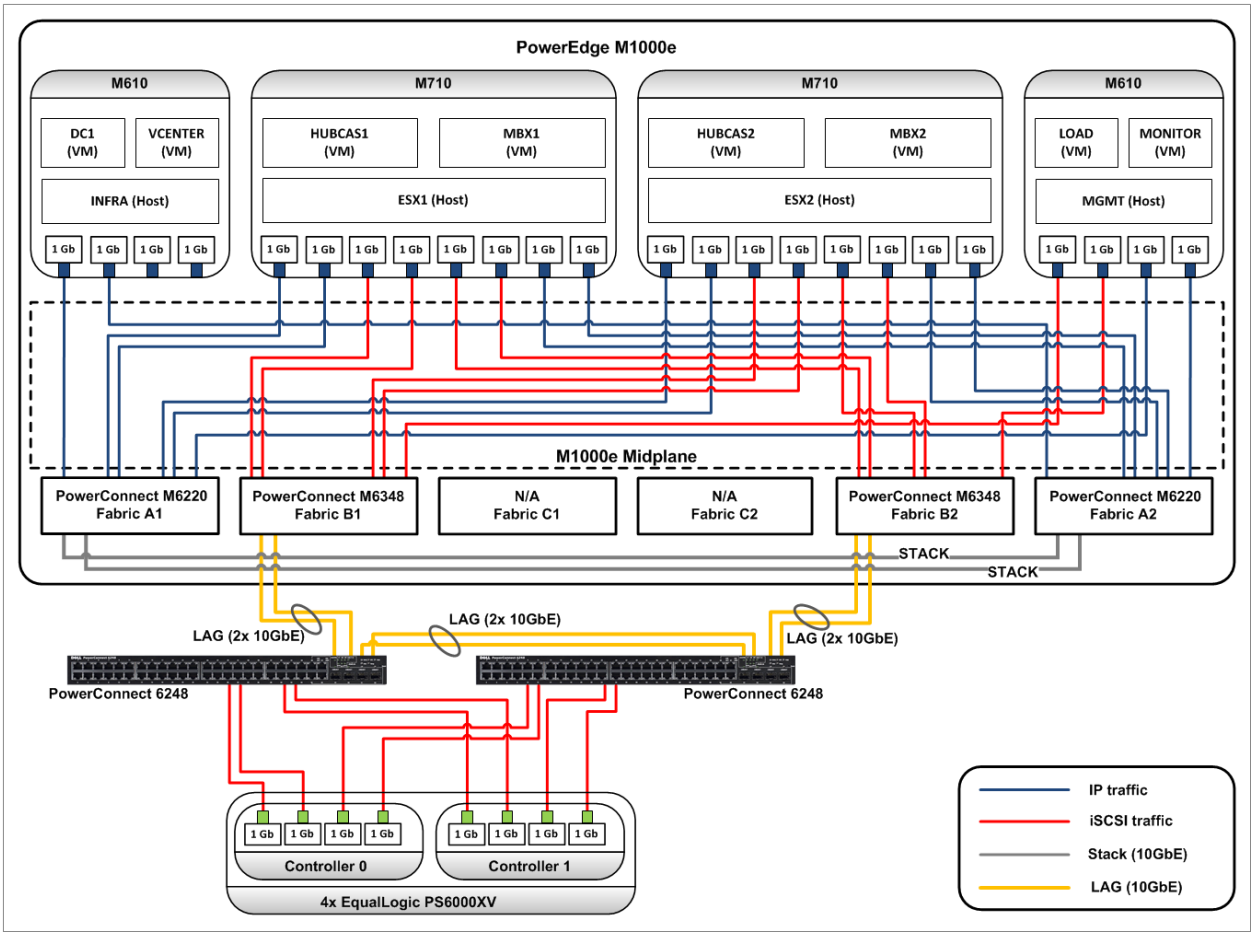


Figure 19 Network connectivity diagram

A.3 Host hypervisor and virtual machines configuration

A virtual infrastructure built with VMware vSphere hosted all the components of both the messaging and test infrastructure. Some key elements of the virtual infrastructure configuration were:

- VMware 4.1 ESXi deployed on 4 hosts, all centrally managed by the same vCenter server
- 2 hypervisor hosts (M710s) configured as a cluster, with HA and DRS features turned off
- 2 hypervisor hosts (M610s) configured as standalone
- All guests deployed from a single template
- Guest VM OS disks statically deployed into the local VMFS data store of its respective host
- Guest iSCSI initiator used to access volumes hosted on the EqualLogic SAN

Table 14 lists the relation between the hypervisor host and each of the virtual machines, with a brief summary of the virtual resources allocated for each virtual machine:

Table 14 Configuration – Host and guest allocation

Host	VM	Purpose	vCPUs	Memory	Network Adapters
INFRA (M610)	DC1	Active Directory Domain Controller	4	8GB	E1000
	VCENTER	VMware vCenter Server	2	4GB	2x E1000
ESX1 (M710)	MBX1	Exchange Server Mailbox Role DAG node 1	4	48GB	2x E1000
					4x VMXNET3
	HUBCAS1	Exchange Server Client Access and HUB Transport roles 1	4	8GB	E1000
ESX2 (M710)	MBX2	Exchange Server Mailbox Role DAG node 2	4	48GB	2x E1000
					4x VMXNET3
	HUBCAS2	Exchange Server Client Access and HUB Transport roles 2	4	8GB	E1000
MGMT (M610)	LOAD	Exchange Load Generator	2	4GB	E1000
	MONITOR	SAN/systems monitoring	2	4GB	2x E1000

A.3.1 ESXi Virtual Network Configuration

The networks of the ESXi hypervisor servers were configured following the guidelines listed below:

- One virtual switch aggregating all the network adapters designated for regular IP traffic, with the default load balancing policy ('Route based on the originating virtual switch port ID')
  - Management Network port group (VMkernel type) – all hosts
  - vCenters port group (Virtual Machine type) – only for the INFRA host
  - Public Network port group (Virtual Machine type) – all hosts
  - Exchange Replication network port group (Virtual machine type) – only for the ESX1/ESX2 hosts
  - Each port group traffic segregated by tagged packets (VLANs)

- One virtual switch aggregating all the network adapters designated for iSCSI storage traffic, with the default load balancing policy ('Route based on the originating virtual switch port ID')
  - iSCSI network port group (Virtual machine type) – only for SAN attached virtual machines

Table 15 reports the relationship between virtual switches, network adapters and VLANs for each hypervisor host.

Table 15 Configuration – Virtual switches, port groups and network adapters

Host	Virtual switch	Network Adapters	Port Group	VLAN ID
INFRA (M610)	vSwitch0	vmnic0, vmnic1	Management	100
			vCenters	100
			Public	200
ESX1 (M710)	vSwitch0	vmnic0, vmnic1, vmnic2, vmnic3	Management	100
			Public	200
			Replication	300
	vSwitch1	vmnic6, vmnic7, vmnic8, vmnic9	iSCSI	NONE
ESX2 (M710)	vSwitch0	vmnic0, vmnic1, vmnic2, vmnic3	Management	100
			Public	200
			Replication	300
	vSwitch1	vmnic6, vmnic7, vmnic8, vmnic9	iSCSI	NONE
MGMT (M610)	vSwitch0	vmnic0, vmnic1	Management	100
			Public	200
	vSwitch1	vmnic2, vmnic3	iSCSI	NONE

The vSwitch0 and vSwitch1 layout on the ESX1 host are shown in Figure 20 and Figure 21.

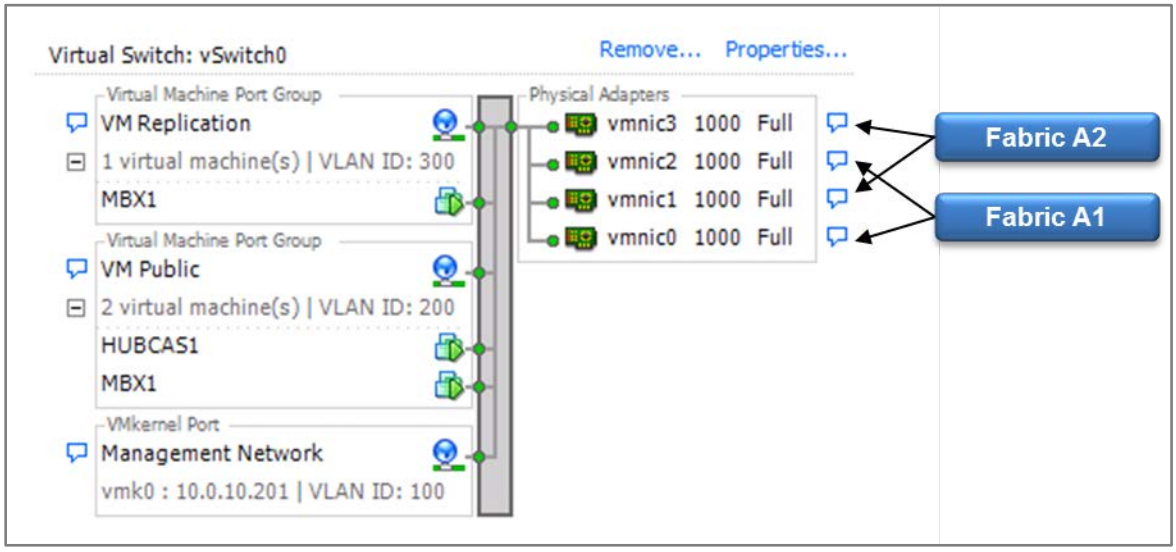


Figure 20 Configuration – vSwitch0

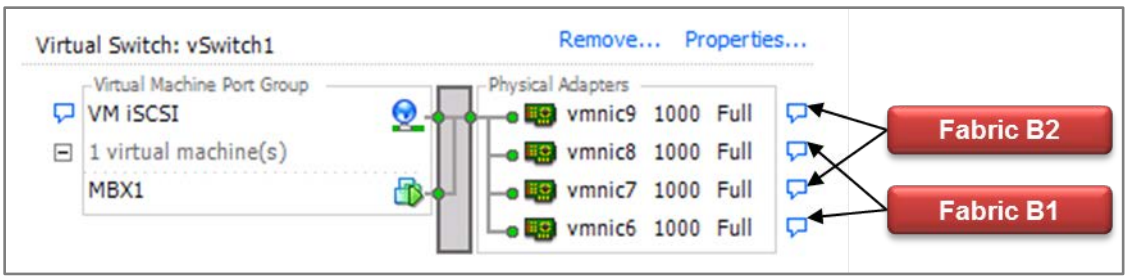


Figure 21 Configuration – vSwitch1

A.3.2 Virtual Machines Network configuration

The assignment of the virtual network adapters for each virtual machine was configured as follow:

- One virtual network adapter to access the Public (Corporate) VLAN
- One virtual network adapter to access the Exchange Replication VLAN (only for Mailbox role servers in a DAG)
- Four virtual network adapters to access the iSCSI network (only for Mailbox role servers)
- MPIO (Multi-path I/O) enabled on the iSCSI network adapters, provided by EqualLogic DSM module
- One virtual network adapter to access the respective network in order to manage or monitor it

Table 16 summarizes the connection of each virtual NIC to the respective virtual switch and network.

Table 16 Configuration – Virtual machines network adapters

VM	#vNIC	Adapters type	Virtual Switch	Port Group	VLAN ID
DC1	#1	E1000	vSwitch0	Public	200
VCENTER	#1	E1000	vSwitch0	Public	200
	#2	E1000		vCenters	100
MBX1 / MBX2	#1	E1000	vSwitch0	Public	200
	#2	E1000		Replication	300
	#3	VMXNET3	vSwitch1	iSCSI	NONE
	#4	VMXNET3		iSCSI	NONE
	#5	VMXNET3		iSCSI	NONE
	#6	VMXNET3		iSCSI	NONE
HUBCAS1 / HUBCAS2	#1	E1000	vSwitch0	Public	200
LOAD	#1	E1000	vSwitch0	Public	200
MONITOR	#1	E1000	vSwitch0	Public	200
	#2	E1000	vSwitch1	iSCSI	NONE

A.4 Software components

The setup of all the servers (physical and virtual) required the deployment of the following software components:

- Bare-metal hypervisor: VMware 4.1 ESXi on all host servers
- Operating System: Windows Server 2008 R2 on all virtual machines
- Active Directory Domain Services and DNS Server roles for the domain controller (DC1 virtual machine)
- VMware vCenter Server, Client and CLI for the virtual infrastructure management (VCENTER virtual machine)
- Microsoft Exchange Server 2010 custom installed depending on the role of the server (MBX1/2, HUBCAS1/2 virtual machines)
- EqualLogic Host Integration Toolkit to access the storage SAN with MPIO and to use ASM/ME
- EqualLogic SAN Headquarters and Microsoft Exchange Management tools to monitor the health and performances of the infrastructure elements (MONITOR virtual machine)
- Microsoft Exchange Load Generator to simulate client access traffic against the Exchange infrastructure (LOAD virtual machine)

Table 17 lists the detailed software components and version required for the configuration setup:

Table 17 Configuration – Software Components

Test Configuration – Software Components:	

Operating systems	• Host: VMware ESXi 4.1.0 update 1Enterprise (build 348581)
	  o Dell OpenManage Server Administrator 6.5.0
	• Guest: Microsoft Windows Server 2008 R2 Enterprise Edition Service Pack 1 (build 7601)
	  o EqualLogic Host Integration Toolkit 3.5.1
	  o MPIO enabled using EqualLogic DSM for Windows for storage-connected guests

Application	• Microsoft Exchange 2010 Enterprise Edition Service Pack 1 (build 218.15) • Microsoft Filter Pack 2.0 • VMware vSphere 4.1.0 vCenter Server and Client (build 345043) • VMware vSphere 4.1.0 CLI (build 254719)
Monitoring tools	• Dell EqualLogic SAN Headquarters 2.1 (build 2.1.0.5342) • Microsoft Performance Monitor (built-in the Windows Operating System) • Performance and Mail Flow tools (Microsoft Exchange Management tools)
Simulation tools	• Microsoft Exchange Load Generator 2010 (build 14.01.0180.003)

For additional information about Exchange Server 2010 requirements, pre-requisites, and installation, refer to Microsoft documentation:
Exchange 2010 System Requirements, available at:
http://technet.microsoft.com/en-us/library/aa996719.aspx
Exchange 2010 Prerequisites, available at:
http://technet.microsoft.com/en-us/library/bb691354.aspx
Install Exchange Server 2010, available at:
http://technet.microsoft.com/en-us/library/bb124778.aspx

Related Publications

The following Dell publications are referenced in this document or are recommended sources for additional information.

- *Dell EqualLogic Configuration Guide*
  http://www.delltechcenter.com/page/EqualLogic+Configuration+Guide
- *Auto-Snapshot manager for Microsoft User Guide*
  https://support.equallogic.com/support/download_file.aspx?id=1053
- *Dell PowerEdge Blade Server and Enclosure Documentation:*
  http://support.dell.com/support/edocs/systems/pem/en/index.htm
- *Dell PowerConnect 62xx Documentation:*
  http://support.dell.com/support/edocs/network/PC62xx/en/index.htm
- *Dell PowerConnect M6220 Documentation:*
  http://support.dell.com/support/edocs/network/PCM6220/en/index.htm
- *Dell PowerConnect M6348 Documentation:*
  http://support.dell.com/support/edocs/NETWORK/PCM6348/en/index.htm
- *Sizing and Best Practices for Microsoft Exchange 2010 on VMware vSphere and EqualLogic storage*
  http://www.delltechcenter.com/page/Sizing+and+Best++Practices+for+Microsoft+Exchange+2010+on+VMware+vSphere+and+EqualLogic+Storage

The following Microsoft publications are referenced in this document or are recommended sources for additional information.

- *Volume Shadow Copy Service*
  http://technet.microsoft.com/en-us/library/ee923636%28WS.10%29.aspx
- *Exchange 2010 System Requirements*
  http://technet.microsoft.com/en-us/library/aa996719.aspx
- *Exchange 2010 Prerequisites*
  http://technet.microsoft.com/en-us/library/bb691354.aspx
- *Install Exchange Server 2010*
  http://technet.microsoft.com/en-us/library/bb124778.aspx
- *Understanding Storage Configuration*
  http://technet.microsoft.com/en-us/library/ee832792.aspx
- *Understanding Database Availability Groups*
  http://technet.microsoft.com/en-us/library/dd979799.aspx
- *Tools for Performance and Scalability Evaluation*
  http://technet.microsoft.com/en-us/library/dd335108.aspx