Microsoft Exchange 2013 on VMware Availability and Recovery Options

vmware

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

List of Figures

1. Introduction

When designed according to VMware® best practices, VMware vSphere® provides availability options not possible in physical server deployments. For example, high availability becomes an option for all virtual machines, regardless of operating system or application. Also, the portability of virtual machines allows disaster recovery (DR) to span the virtual datacenter, leaving behind application silos.

By leveraging the inherent benefits of a VMware-based platform, a Microsoft Exchange Server 2013 deployment on VMware vSphere offers a choice of several availability and recovery options, each providing varying levels of protection and cost. This solution brief provides a description of the various options available. Topics include:

- vSphere Platform Advantages.
- Increase Availability Across the Exchange Lifecycle.
- Local Site Availability Options.
- Remote Site Availability Options.
- Backup and Restore Options.

2. vSphere Platform Advantages

High availability in Exchange has evolved greatly over the past decade. Exchange 2003 leveraged the more traditional shared disk clustering architecture with all of its inherent limitations. Exchange 2007 maintained its dependence on Microsoft Cluster Service and Windows Failover Clustering, but provided cluster continuous replication (CCR), the precursor to database availability groups (DAGs). Although very limited, CCR showed what was possible when clustering was decoupled from data storage, using log shipping for data replication and introducing the concept of multiple data copies. In Exchange 2010 and Exchange 2013, the DAG solves the limitations of CCR and is the only native high availability solution supported by Exchange.

vSphere platform features can complement and enhance the overall availability of Exchange by providing options that help to limit both planned and unplanned downtime. For many organizations, the features provided by vSphere might satisfy the availability requirements of their business without Exchange DAGs. For other organizations that require a greater degree of availability, DAGs can be combined with vSphere features to create an extremely flexible environment, with options for failover and recovery at both the hardware and application levels. Some of the advantages of the vSphere platform include:

- Virtual machine portability – Exchange servers are no longer bound to specific hardware. This can enhance availability in several ways:
    - Design decisions are no longer permanent – You can adjust your CPU, memory, and storage requirements with simple virtual machine reconfiguration.
    - Easily upgrade to newer hardware – As your Exchange environment grows or changes, Exchange virtual machines can be migrated to newer hardware to accommodate increased workloads.
- Hardware independence – Leverage increased flexibility when designing both production and disaster recovery components. DAG members and recovery servers can be virtualized, eliminating the need for identical and dedicated hardware.
- VMware vSphere High Availability (HA) protects your server from hardware and guest operating system failure – If a VMware ESXi™ host, or any critical component within the host, fails causing virtual machines to go offline, vSphere HA automatically powers on the Exchange virtual machines on another ESXi host. By combining vSphere HA with DAGs, you can mitigate both hardware and software failure risk for maximum availability.
- VMware vSphere Distributed Resource Scheduler™ (DRS) is VMware vSphere vMotion® with intelligence – DRS balances workloads and speeds recovery. As ESXi host utilization increases and available resources decrease, DRS migrates virtual machines using vSphere vMotion to balance resource utilization across a vSphere cluster. DRS can also help to recover more quickly after a server hardware failure. For example, if a physical server fails, vSphere HA reboots the virtual machine on another physical server. When the failed server is replaced, DRS migrates virtual machines to keep workloads balanced across the vSphere cluster.

3. Increase Availability Across the Exchange Lifecycle

Over the life of an Exchange environment, maintenance, upgrades, component failures, and failover and recovery testing test the availability of a design. Database availability groups can provide many of the features needed to accommodate these disruptive activities, but more complex Exchange designs are typically required. When deployed on vSphere, Exchange 2013 virtual machines can be part of an architecture that follows the typical lifecycle of an enterprise application without the disruption or downtime.

3.1 Eliminate Downtime Due to Maintenance Activities

The ability to eliminate downtime associated with managing a critical application and the underlying hardware increases the overall availability of the environment. The following are some of the common causes for maintenance-related downtime that are solved when using vSphere.

Issue – Traditional, physical environment upgrades and scale-up activities require a great deal of resources, including:

- Planning and implementation time from engineering resources, including application administration, server administration, and SAN administration.
- Sizing and acquisition of new hardware.
- Downtime required to perform upgrades, which results in higher costs and risks.

Solution – Scaling your environment using vSphere means scaling up Exchange virtual machines or adding more Exchange virtual machines as demand increases. This is much easier than scaling up physical servers.

Issue – Physical Exchange server environments are tightly bound to a storage technology and are extremely difficult to scale. Adding more storage capacity to Exchange virtual machines is less complex because vSphere emulates storage to a simple SCSI device. The end result is that the Exchange environment can be upgraded, regardless of the underlying storage technologies (iSCSI or Fibre Channel).

Solution – With the VMware vSphere Virtual Machine File System (VMFS), the storage capacity serving Exchange environments can be reduced or increased during operations with the hot add/remove storage functionality in vSphere. Virtualized Exchange environments can be scaled up, such as adding more memory or CPU resources, without interruption.

4. Local Site Availability Options

Local availability refers to providing a service that is highly available within a datacenter, site, or metro area network. Dependencies, connectivity, and application requirements often require keeping high availability local. This section reviews local availability options available to Exchange 2013 environments when virtualized on VMware.

4.1 vSphere HA, DRS, and vSphere vMotion

When deploying Exchange 2013, the high availability options available in a physical environment continue to be available in a virtual environment. vSphere features such as vSphere HA, vSphere Distributed Resource Scheduler, and vSphere vMotion are available to provide even higher levels of performance and recovery in the case of a host failure.

- vSphere HA provides easy-to-use and cost-effective high availability for applications running in virtual machines. In the event of a physical server failure, affected virtual machines are automatically restarted on other production servers with spare capacity. Additionally, if the virtual machine experiences a failure related to the guest operating system, the failure can be detected by vSphere HA and the affected virtual machine can be restarted to correct the failure.
- vSphere Distributed Resource Scheduler (DRS) collects resource usage information for all hosts and virtual machines and generates recommendations for virtual machine placement. These recommendations can be applied manually or automatically. DRS can dynamically load balance all virtual machines in the environment by shifting workloads across the entire pool of ESXi hosts. This allows critical Exchange virtual machines in the environment to have access to the CPU and memory resources needed to maintain optimal performance.
- vSphere vMotion leverages the complete virtualization of servers, storage, and networking to move a running virtual machine from one physical server to another. This migration is done with no impact to running workloads or connected users. During a vSphere vMotion migration, the active memory and execution state of the virtual machine are rapidly transmitted over the network to the new physical server, all while maintaining its network identity and connections.

In an Exchange 2013 environment all server roles can take advantage of these features to provide better availability than standalone physical deployments. Organizations that wish to provide high availability while controlling cost, management overhead, and simplifying the architecture can take advantage of these features instead of deploying multiple database copies with DAGs.

4.1.1 Example: Protecting Exchange with vSphere HA

Out-of-the-box vSphere features can help to protect your standalone Exchange virtual machine from server host failure. vSphere HA automatically reboots your Exchange virtual machine on another server if the current one fails. Virtual machines are restored to normal operation in the time that it takes to boot the operating system and start the Exchange services. After the original server hardware is fixed or replaced, DRS and vSphere vMotion can be used to quickly move the virtual machine back to its original ESXi host, with no additional downtime.

Figure 1. Protecting Exchange with vSphere HA

When a high availability event is triggered, the time to recover is much quicker than the time taken to recover from a physical server reboot. As described in *Using VMware HA, DRS and vMotion with Exchange 2010 DAGs* (http://www.vmware.com/files/pdf/using-vmware-HA-DRS-and-vmotion-with-exchange-2010-dags.pdf), vSphere HA recovered the tested virtual machine to full operation in just over three minutes. The following table outlines the results.

Table 1. vSphere HA Recovery Timeline

Task	Time (Elapsed Time)
vSphere host powered off initiated	3:29:34 PM (0:00:00)
Host failure detected	3:30:06 PM (0:00:32)
Ex2010-dagnode1 fails	3:30:14 PM (0:00:40)
Ex2010-dagnode1 restarted by vSphere HA	3:30:24 PM (0:00:50)
DAG node failure detected by ex2010-dagnode2	3:30:34 PM (0:01:00)
Databases begin to mount on ex2010-dagnode2	3:30:41 PM (0:01:07)
All databases mounted	3:30:43 PM (0:01:09)
Ex2010-dagnode1 OS running	3:31:07 PM (0:01:33)
Ex2010-dagnode1 begins copying and replaying log files	3:32:15 PM (0:02:41)
Ex2010-dagnode1 completes replication and replay of logs for all databases	3:32:36 PM (0:03:02)

Solutions focusing on simplicity and leveraging the VMware feature set provide the highest levels of flexibility and agility. The reduced complexity allows administrators to design for current needs, scale out as demand grows, and quickly respond to and identify the root cause when an issue occurs. Consider your availability requirements, and determine whether vSphere HA can be the end-to-end solution in your environment.

4.2 Load Balancing with vCloud Networking and Security

Although virtualization has allowed organizations to optimize their compute and storage investments, the network has mostly remained physical. VMware vCloud® Networking and Security™ solves datacenter challenges found in physical network environments by delivering software-defined networking and security. Using existing vSphere compute resources, network services can be delivered quickly to respond to business challenges.

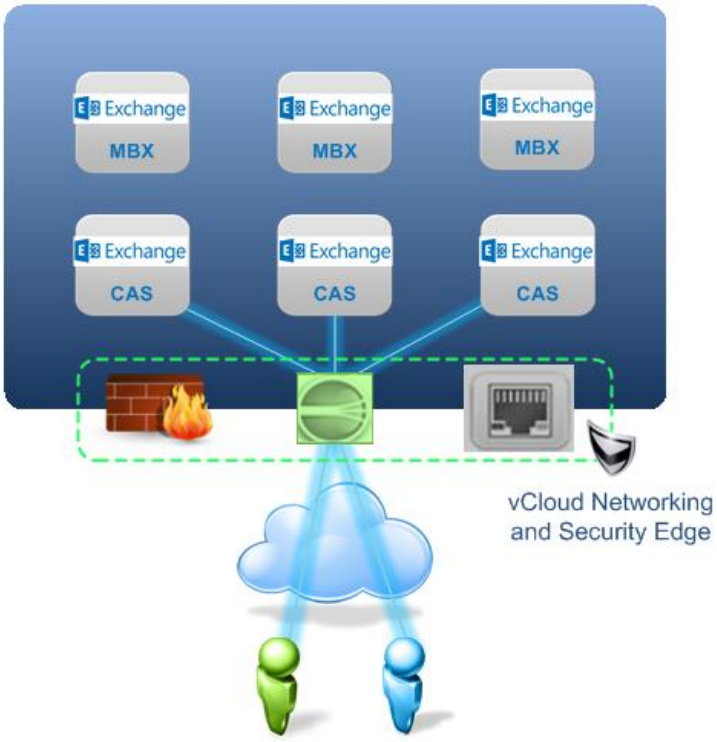
VMware vCloud Networking and Security Edge™ (Edge) provides a firewall for virtual datacenters and gateway services such as NAT, load balancing, VPN, and DHCP for virtual machines through a virtual appliance. Edge can be deployed in a high availability pair, providing better protection than hardware load balancing solutions without the additional hardware or management overhead. Edge supports both Layer 4 and Layer 7 load balancing of HTTP and HTTPS protocols, and supports multiple load balancing methods such as round-robin DNS and least-connection. Edge can support up to 10 members in a load balancer pool. When using the extra-large Edge virtual appliance, it can support up to 400,000 concurrent connections using Layer 7 proxy mode or 1,000,000 concurrent connections using Layer 4 mode.

More information on Edge configuration limits and throughput is available in *vCloud Networking and Security 5.1 Edge Configuration Limits and Throughput* (http://kb.vmware.com/kb/2042799).

4.2.1 Example: Client Access Array Load Balancing with Edge

Client Access servers in a Client Access server (CAS) array must be load balanced to provide a highly available and well performing experience for end users. To provide this functionality, a load balancing solution is recommended. How the load balancing solution is implemented can take various forms, including round-robin DNS and hardware and software load balancing. Dedicated load balancers can provide better load distribution over round-robin DNS by using number of connections or proprietary algorithms to determine the best target for the traffic. Edge provides many of the features found in more advanced load balancers while using your existing vSphere resources and without requiring any additional hardware expenses or maintenance.

Figure 2. vCloud Networking and Security Edge



4.3 Exchange 2013 Database Availability Groups

Exchange 2013 DAGs have changed the traditional server-failover model to a database-failover model, where individual databases can be activated on another Exchange server in the DAG. DAGs provide a non-shared storage failover cluster solution. DAGs use asynchronous log shipping technology to distribute and maintain passive copies of each database on Exchange DAG member servers. With the reduction in storage I/O and optimized storage patterns in Exchange 2013, direct-attached storage has become more attractive. However, designs that leverage these larger, slower, and failure-prone storage architectures must compensate by supporting more database copies to mitigate data loss. Commodity storage seemingly allows for larger mailboxes, which leads to larger databases. During storage failures, these large databases must be resynchronized after the storage failure is resolved. During this reseeding process, availability is compromised if more database copies are not available.

Although commodity storage for large mailboxes might be appealing for some use cases, many environments are designed on redundant, enterprise-class storage arrays and SANs. This allows customers to minimize the database sprawl and maintenance overhead of managing three and four times the number of databases. Exchange 2013 virtual machines become more resilient when running on SAN attached storage by leveraging vSphere features such as vSphere vMotion, vSphere HA, and DRS.

Exchange 2013 supports the use of DAGs on top of hypervisor-based clustering as detailed in *Exchange 2013 Virtualization* (http://technet.microsoft.com/en-us/library/jj619301(v=exchg.150).aspx).

You can find information on Exchange 2013 DAG with vSphere HA best practices in *Microsoft Exchange 2013 on VMware Best Practices Guide.*

4.3.1 Example: Exchange 2013 DAG Protected with vSphere HA

Virtualized Exchange 2013 DAG members can take advantage of vSphere HA for recovery in the case of ESXi host or guest operating system failure.

The following figure demonstrates a vSphere cluster supporting multiple DAG members and protected databases.

Figure 3. Normal State Exchange 2013 DAG with vSphere HA

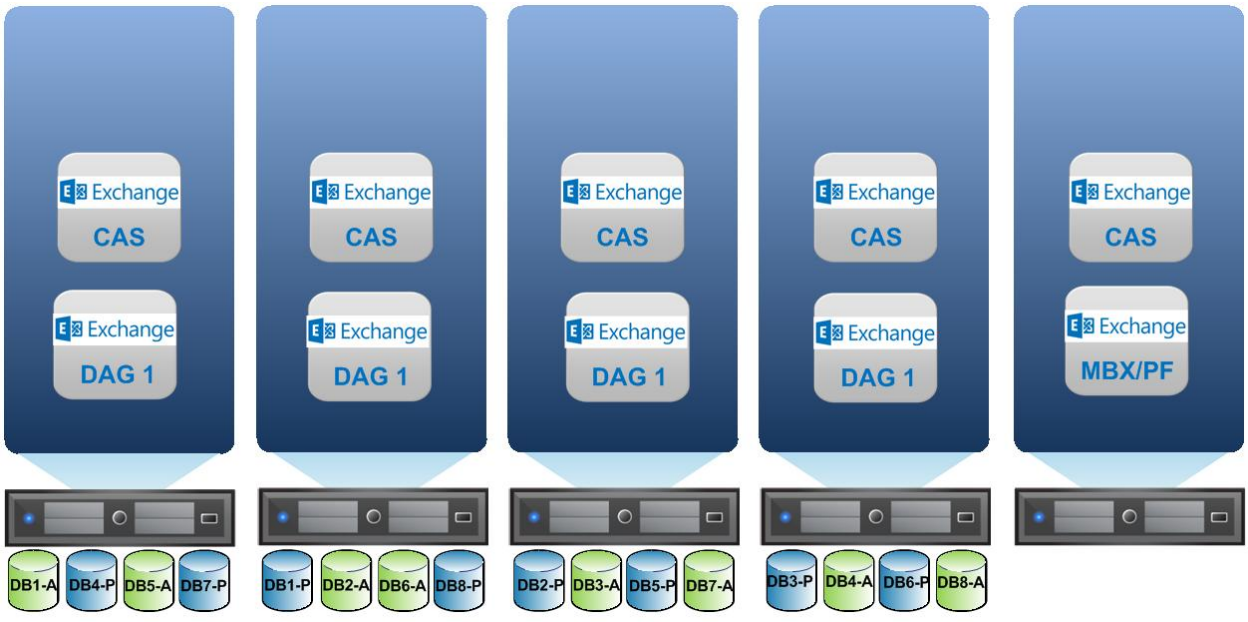
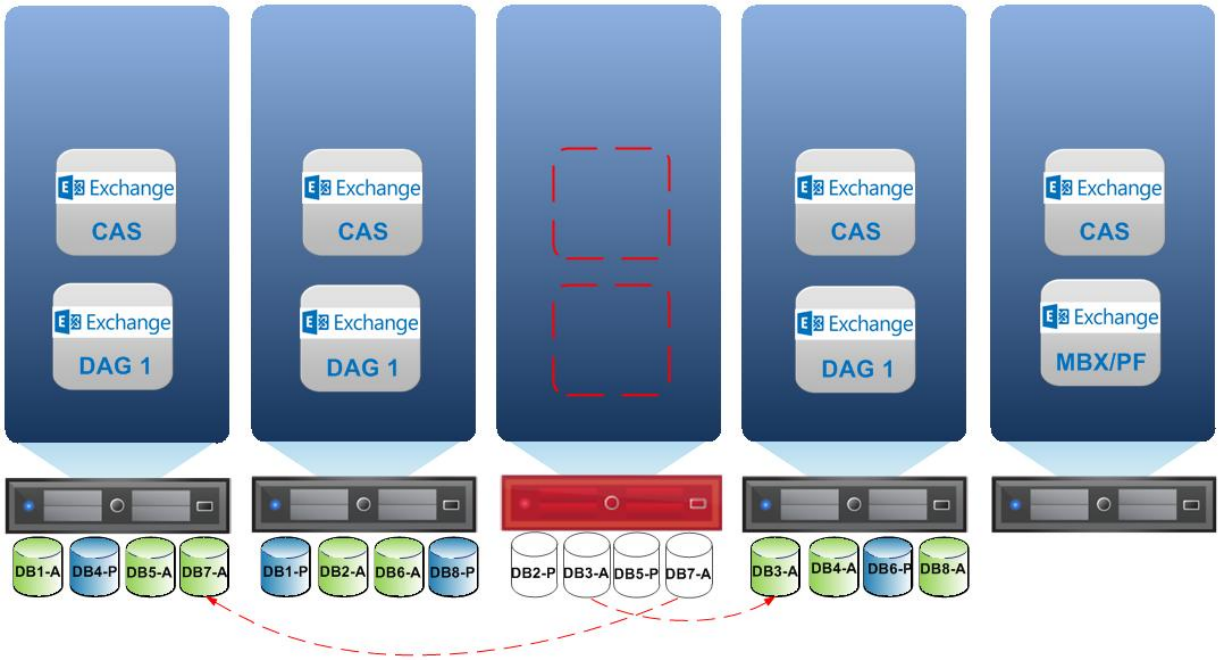
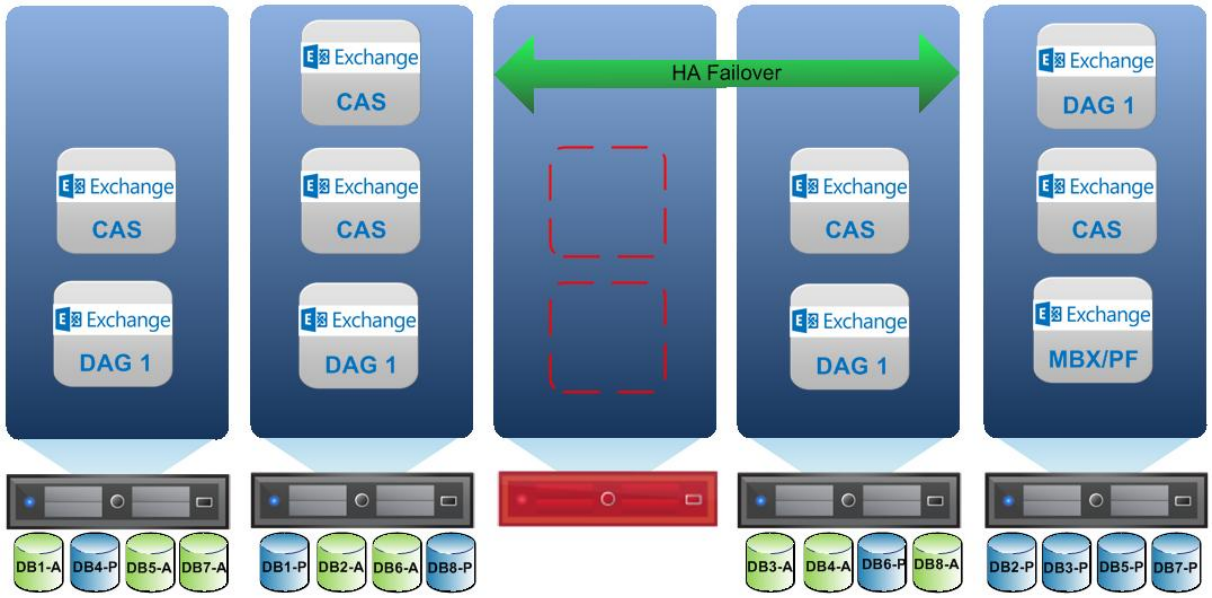


Figure 4. Database Failover



In the event of an ESXi host failure, virtual machines running on that host also fail, causing passive databases to be activated on surviving DAG members. Client Access servers establish connectivity to the newly activated databases, and client connections continue.

Figure 5. vSphere HA Failover and Database Synchronization



In the background, vSphere HA powers on the failed virtual machines on another ESXi host. This happens within minutes of the host failure, allowing DAG membership to be reestablished with no user interaction and bringing the now passive databases up to date and ready to take over in case of any further failures.

5. Remote Site Availability Options

Remote availability typically refers to disaster recovery. When applications are virtualized on vSphere, the options available to application architects are no longer application-specific. vSphere provides the flexibility to coexist with an application-specific approach or improve the availability design by meeting SLA requirements while reducing management overhead. This section reviews the options available when Exchange is virtualized. This includes both application-specific options and those that break the application silo and extend across the entire datacenter.

5.1 vCenter Site Recovery Manager

VMware vCenter™ Site Recovery Manager™ makes disaster recovery rapid, reliable, manageable, and affordable. vCenter Site Recovery Manager leverages vSphere and storage replication software from leading partners to deliver centralized management of recovery plans, automate the recovery process, and enable dramatically improved recovery plan testing. It transforms the complex hardcopy runbooks associated with traditional disaster recovery into an integrated element of virtual infrastructure management. vCenter Site Recovery Manager helps organizations to reduce the risk and worry of disaster recovery, which is yet another reason the VMware virtualization platform is an ideal platform for enterprise applications.

5.1.1 Example: vCenter Site Recovery Manager and Exchange 2013 DAGs

Using Exchange 2013 DAGs within the datacenter to provide high availability meets the requirements of most organizations. With DAGs, a failover can occur automatically at the database or server level and can take place within seconds of a detected failure. When designing a disaster recovery solution, automated failover might not be feasible in the respective environment. Many organizations require that the choice to activate the DR facility be a conscious decision that follows the change process. With vCenter Site Recovery Manager, disaster recovery can be implemented to protect the entire virtual datacenter, including Exchange, reducing the need for application silos.

An inherent limitation of using DAGs for disaster recovery is the ability to test failover. The process of testing involves activating databases in the DR facility and possibly migrating client and mail entry points. vCenter Site Recovery Manager enables failover testing with no production impact to confirm that the recovery time and recovery point objectives are met. Additionally, customizable recovery plans allow for adding custom scripts, virtual machine power-on priority, and workflow breaks.

To initiate recovery using vCenter Site Recovery Manager for a site protected with a DAG

1. Initiate the vCenter Site Recovery Manager recovery plan – A vCenter Site Recovery Manager recovery plan automates making the recovery site storage writable, registering virtual machines in the recovery site, and powering on virtual machines based on the order set in the recovery plan. During power-on, vCenter Site Recovery Manager updates virtual machine IP addresses if necessary.
2. Configure the DAG IP address and witness server – This step updates the DAG IP address, if the recovery site uses a different IP subnet than the protected site, and updates the witness server settings to specify a local witness server. This process can be done manually after one of the DAG nodes has come online, can be scripted and called from the vCenter Site Recovery Manager recovery plan, or can be configured as a scheduled task (that never runs) on a DAG member and called from the vCenter Site Recovery Manager recovery plan using the Windows command `schtask.exe`.
3. Update the DAG and DAG node DNS host (A) records – This can be done manually, using dynamic DNS, or scripted and called from vCenter Site Recovery Manager.
4. Update the DNS records for client access endpoints – Depending on the topology, DNS might require updating for the Exchange namespaces (such as Microsoft Outlook Web App and Autodiscover) that are now served from the recovery site.

Figure 6. Normal State vCenter Site Recovery Manager and Exchange 2013 DAG

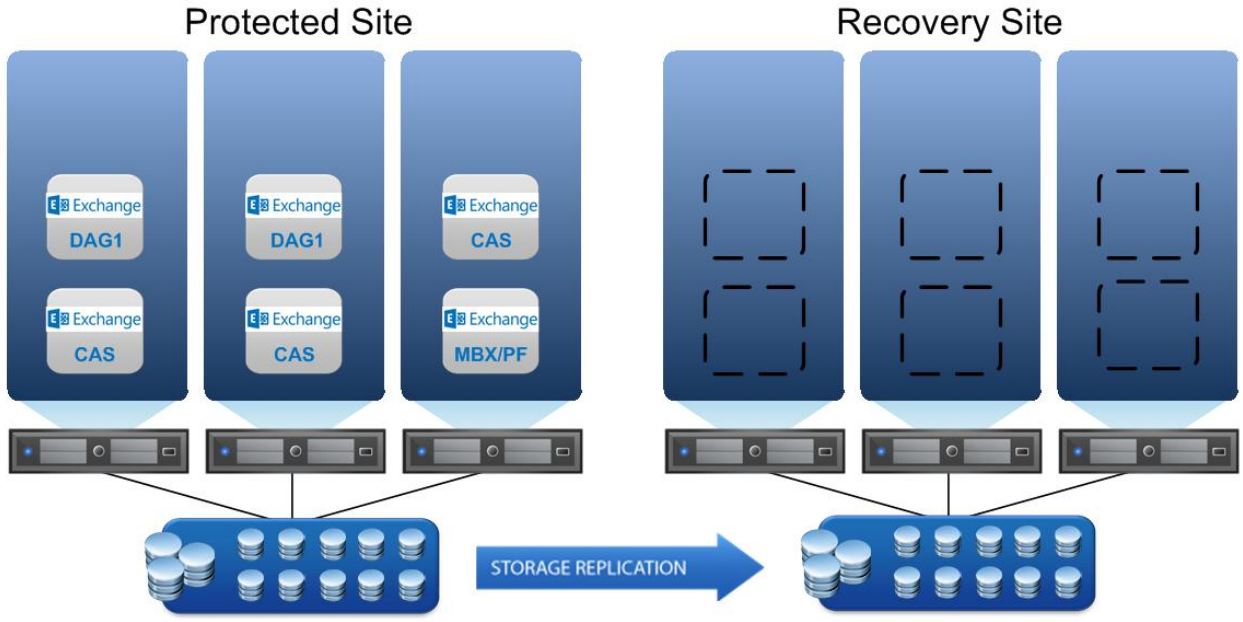
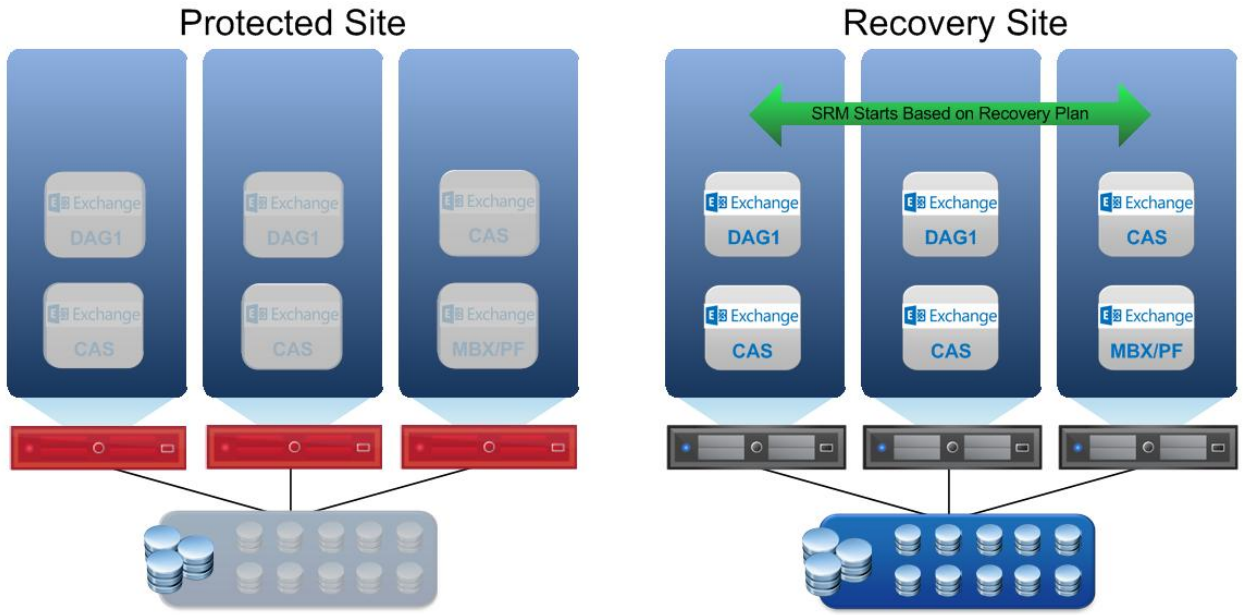


Figure 7. vCenter Site Recovery Manager Recovery of the Entire Site



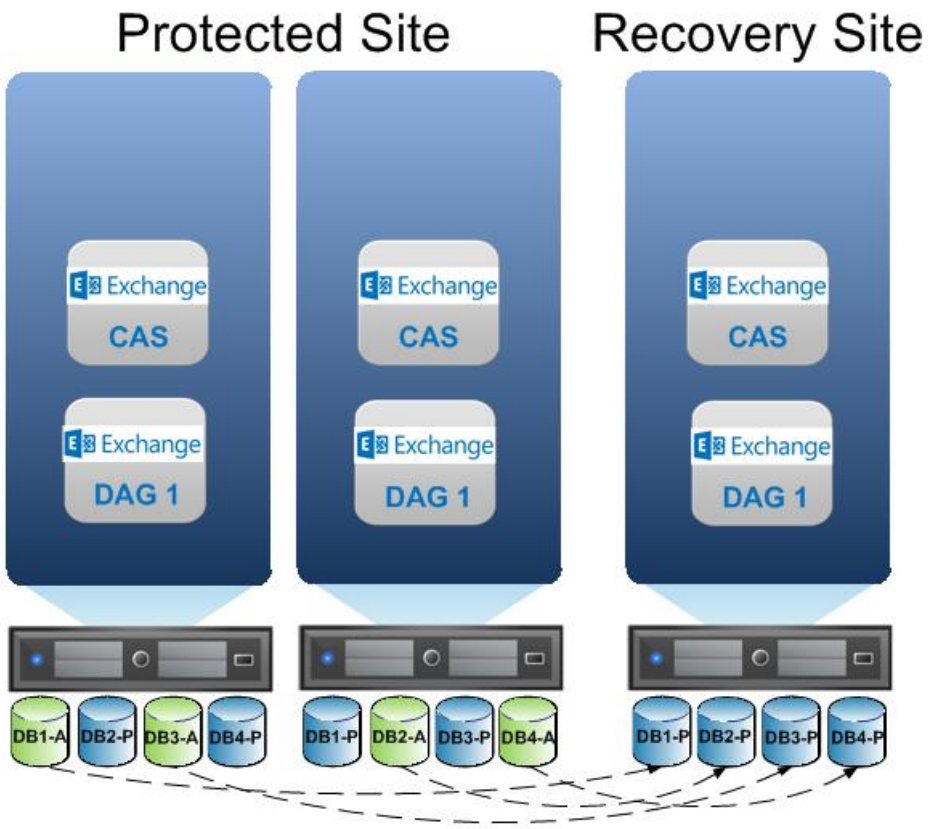
5.2 Exchange 2013 Stretched DAG with Lagged Log Replay

Database copies support lagged transaction log replay, or ReplayLagTime. With Exchange 2013 and DAGs, a mailbox database copy can be configured with an administrator-defined replay lag time to delay the replaying of log files into the passive database copy. This replay lag time can be up to 14 days. Replay lag provides protection against logical database corruption by providing the ability to recover up to the last copied and inspected log file, or to a specific point in time within the lag window, by manipulating the log files and running `eseutil`. When a lagged database is mounted with no log files to replay, Exchange 2013 can enable missing messages to be re-delivered using the Safey Net feature of Exchange 2013 transport.

5.2.1 Example: DAG with Lagged Log Replay

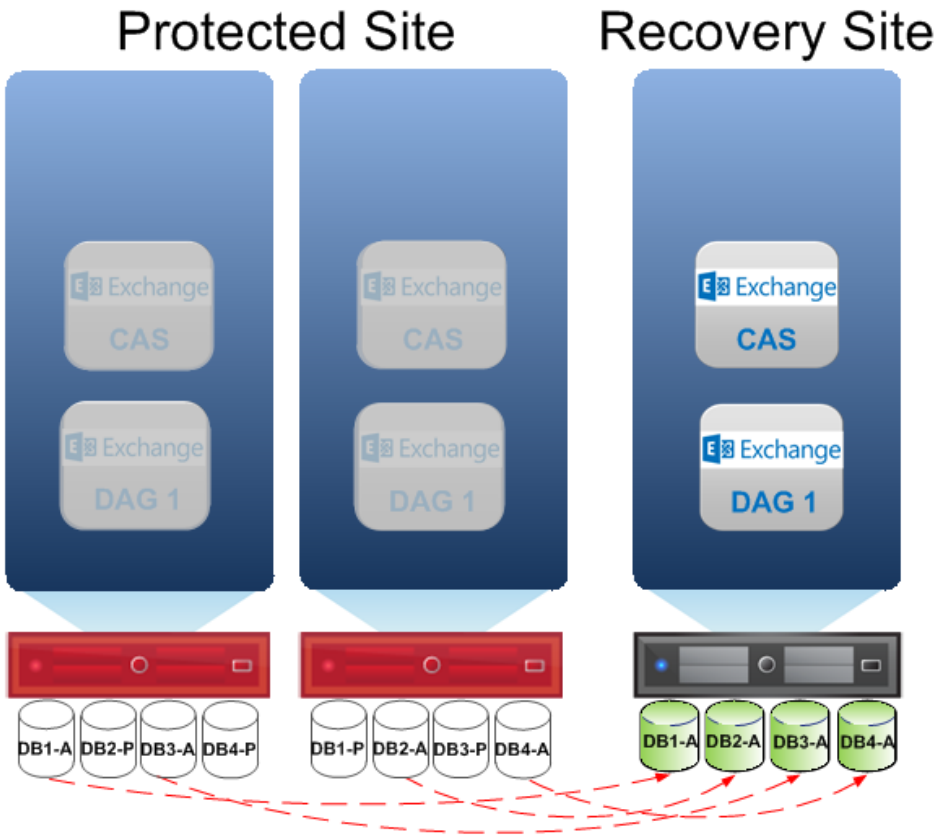
To maintain high availability within the datacenter and provide disaster recovery protection, a third database copy can be established at a DR datacenter. By implementing lagged log replay, you can avoid logical corruption by requiring manual activation of the DR databases. Disaster recovery plan testing should be performed to familiarize the operations team with the `eseutil` tool, which is required for point-in-time log replay, and with the various methods for activating a lagged database copy. When testing disaster recovery plans, take into account any impact disaster recovery testing might have on active client connections.

Figure 8. Normal State Stretched DAG with a Lagged Log Replay



During normal operations, passive database copies at the protected site are kept up to date so they can be activated rapidly in the event of a local failure. Passive database copies at the recovery site are kept up to date, minus the lag time defined by the administrator.

Figure 9. Manually Activated Lagged Databases



When required, lagged database copies must be manually activated by an administrator. This requires an understanding of the scope of the failure to determine how the lagged copies should be activated. Depending on the scope of the failure, recovery might involve a complete datacenter switchover.

5.3 Exchange 2013 Stretched DAG with Automated Failover

Exchange 2013 has made significant progress in simplifying the datacenter switchover process. By decoupling Client Access and Mailbox servers for site recovery, server roles can be recovered independently, and failover can be performed automatically. For organizations with three well-connected sites and that wish to implement a more automated datacenter failover methodology, this solution might be an option. The following items must be considered when designing for a stretched DAG architecture:

- Two copies of the data is the minimum requirement with one copy in each datacenter. Minor failures result in clients connecting across the local area, metro area, or wide area networks for access to mailbox data.
- Maintaining local high availability requires at least three copies of data.
- A third site with connectivity to both Exchange sites must be available for the file share witness. This site must be isolated from any network failures which might affect sites hosting Exchange 2013 DAG members.

5.3.1 Example: Stretched DAG with Automated Failover

Architecture changes in Exchange 2013 enable easier multisite DAG deployments. Collapsed namespaces and the decoupling of the CAS and Mailbox server recovery make automated datacenter

failover a viable option when all requirements are met. In this scenario, each site must be able to provide a load balanced client access array that is either registered in DNS using a single fully qualified domain name (FQDN), or using a geographic load balancing solution. If one CAS array fails to be accessible, for instance, due to load balancer failure, clients can be redirected to another site's CAS array and will proxy to the active mailbox database in the correct site.

The following figure demonstrates a multisite DAG deployment with an equal number of members in each site. Each site contains a load balanced client access array for client connectivity. All sites are connected, including the site housing the file share witness.

Figure 10. Normal State Stretched DAG with Automated Failover

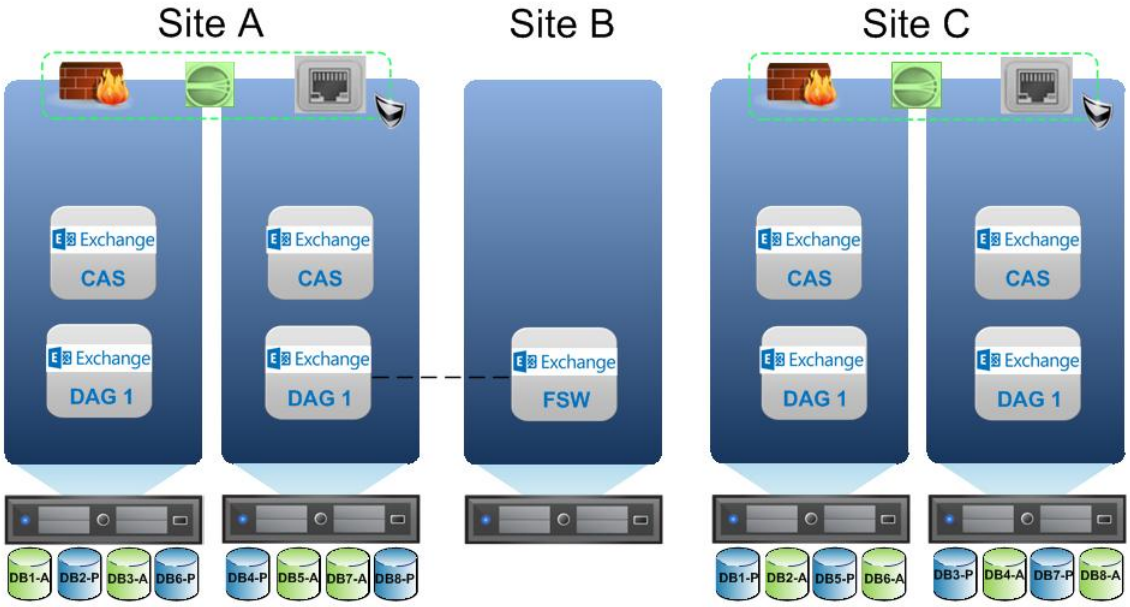
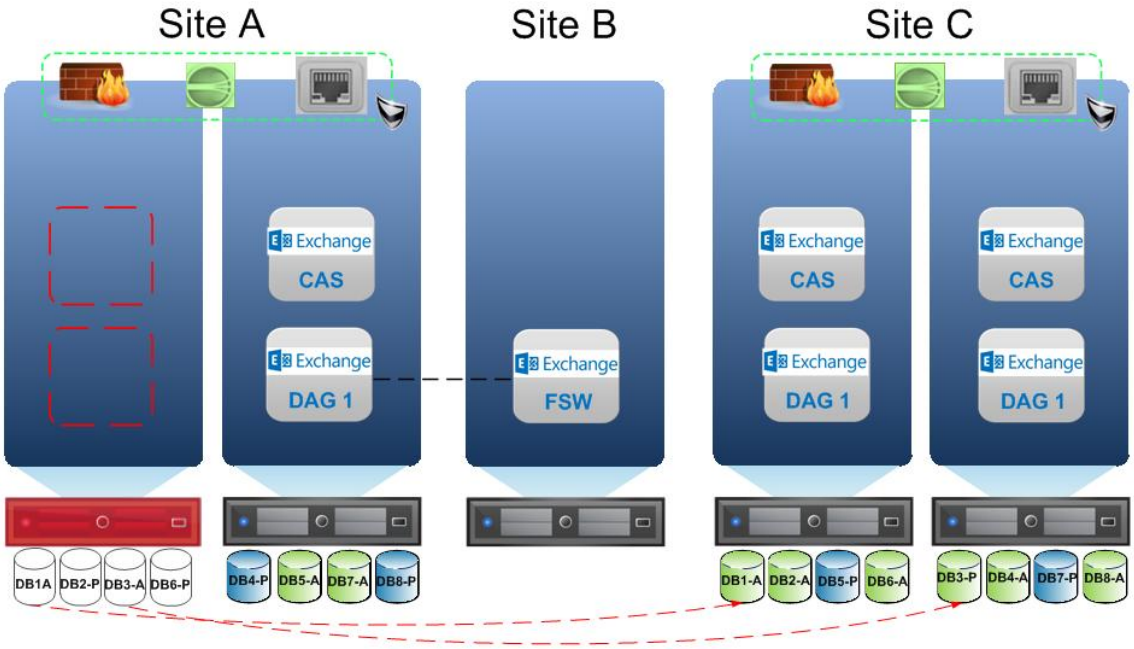
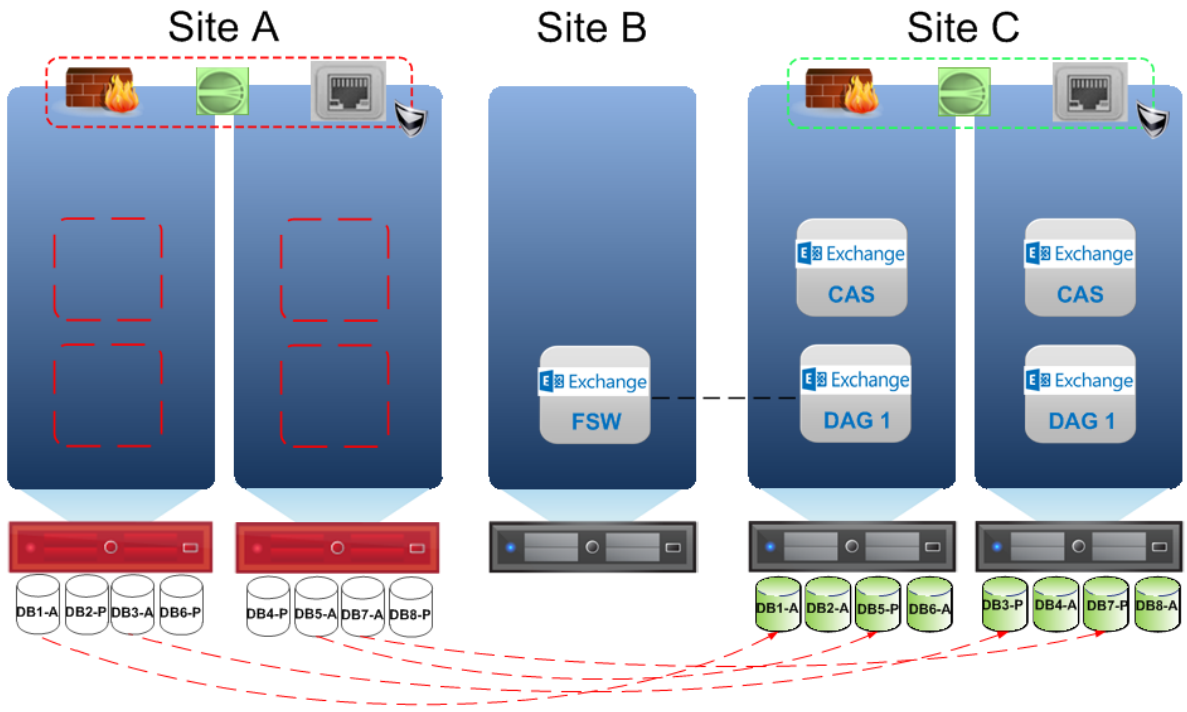


Figure 11. Scenario 1 – Single Server Failure



In the case of a single database or server failure, passive databases are automatically activated. Clients can connect to any available load balanced client access array and are proxied to their respective mailbox database.

Figure 12. Scenario 2 – Automatic Site Failover



If there is a complete site failure, automatic failover should occur if the secondary site is running and a DAG node can access the file share witness. Using the geographic load balancing solution, clients are directed to the available client access array and proxied to their respective mailbox database.

6. Backup and Restore Options

The feature set available to an application, when deployed in a virtual environment, is no different than what is available with a physical deployment. In fact, there are more options available for protecting entire virtual machines. This is especially useful for applications that require extensive configuration. For Exchange 2013, the virtual environment supports the standard methods for backup. These tend to be deployed using a third-party backup agent that uses a Volume Shadow Copy Service (VSS) requestor to coordinate with the Exchange VSS writer to prepare the database files for backup. Regardless of the backup solution required, VMware and VMware partners offer solutions for most situations.

6.1 vSphere Data Protection Advanced

VMware vSphere Data Protection Advanced™ is a backup and recovery solution powered by EMC Avamar and is designed for mid-size vSphere environments. It extends the capabilities of VMware vSphere Data Protection™ (available with all vSphere editions) to provide the most proven, efficient, and easy-to-use protection for virtual machines and offers greater scalability and integration with business-critical applications.

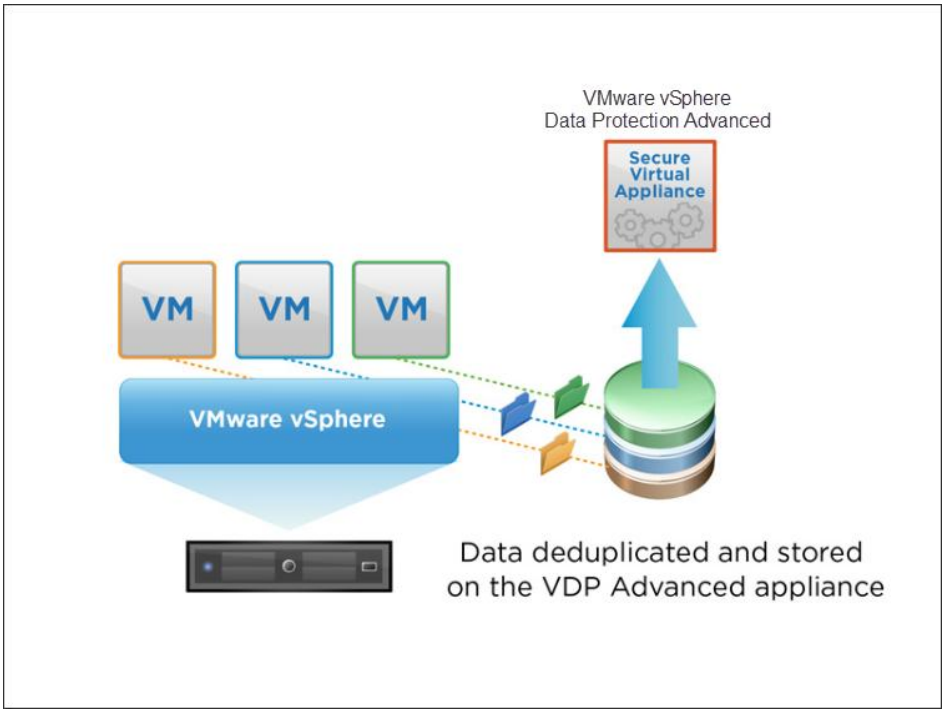
An Exchange-aware agent provides support for backing up Exchange databases. The lightweight agent installed inside the virtual machine deduplicates data, moving only unique changed blocks to the vSphere Data Protection Advanced appliance. vSphere Data Protection Advanced achieves the highest levels of deduplication at the guest level. Guest-level backup and recovery provide application-consistent states that are crucial for reliable protection of the Exchange server. The Exchange Server agent provides recovery of individual databases with options to restore to a recovery database to perform granular recovery of mailboxes and messages.

For additional information, refer to the *VMware vSphere Data Protection Advanced* product page (http://www.vmware.com/products/datacenter-virtualization/vsphere-data-protection-advanced/overview.html).

6.1.1 Example: Using vSphere Data Protection Advanced with Exchange Virtual Machines

With the integration of an Exchange-aware agent in the guest operating system, vSphere Data Protection Advanced can be used for both the Client Access and Mailbox Exchange server roles. Entire Client Access server virtual machines can be restored quickly in the case of operating system corruption or failure due to a bad patch. Mailbox server virtual machines can now also be protected with supported Exchange mailbox database backup and restore.

Figure 13. vSphere Data Protection Advanced



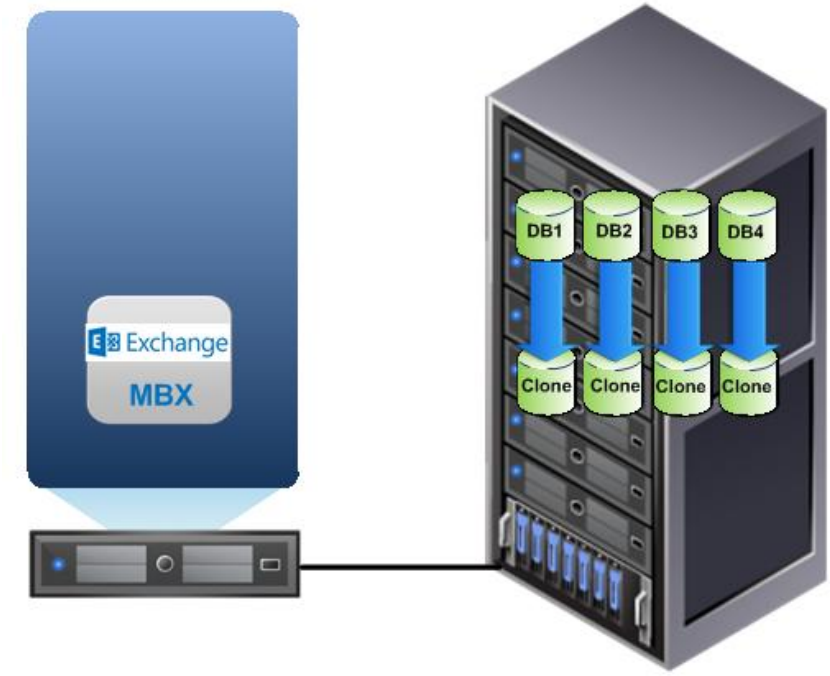
6.2 Array-Based Backup Solutions

Array-based solutions provided by many of the leading storage vendors continue to work with vSphere deployments of Exchange. Array-based backup solutions for Exchange use the Volume Shadow Copy Service (VSS) supported by Exchange 2013 to produce near-instant, application-aware clones or snapshots of Exchange databases. These local clones or snapshots can then be backed up to disk or tape, or cloned offsite to be used for disaster recovery. Guidance on proper deployment methods and any additional considerations when running in a virtualized environment must be provided by the storage vendor. VMware has a comprehensive list of ISV partners that provide array-based replication of Exchange servers for backup and restore operations.

6.2.1 Example: Exchange Mailbox Server Virtual Machine with Array-Based Backup Solution

An array-based backup solution provides integration with the Exchange application and the underlying storage solution. A software agent provided by your backup vendor coordinates with the Exchange VSS writers to create a supported backup image of your Exchange databases. These databases can later be streamed to tape as flat files for compliance or archive requirements with no I/O impact to the production data.

Figure 14. Array-Based Backup Solution



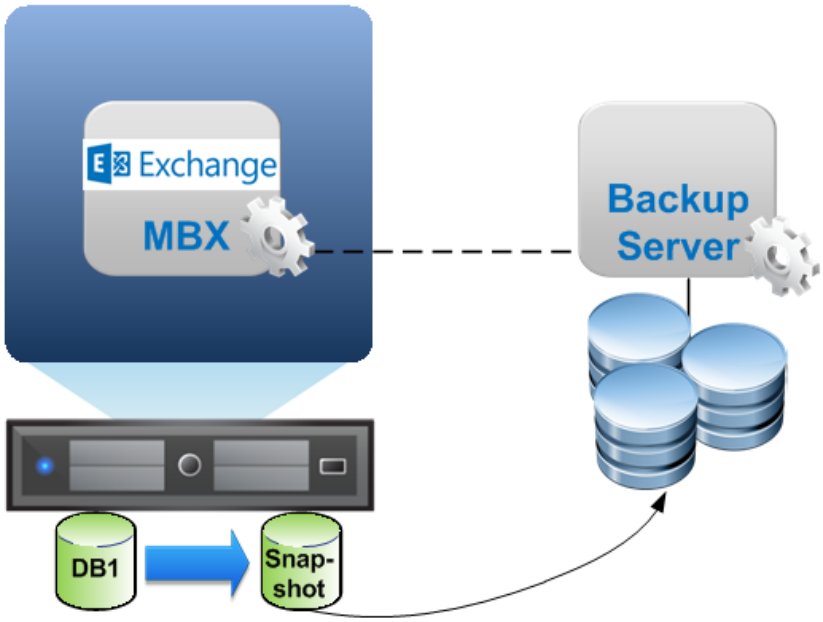
6.3 In-Guest Software Solutions

Many organizations have dedicated backup support teams or requirements that might not allow them to integrate the backup solution to the level that is available with vSphere. In these situations, traditional backup methods are desirable, and a virtualized environment enables their use. Many of the leading backup software providers are VMware partners and provide full support for using their backup solutions within a virtualized guest operating system. Backup administrators can continue to deploy and manage the backup agents, jobs, and restores the same way as with physical systems.

6.3.1 Example: In-Guest Exchange-Aware Backup Solution

Centralized backup management software controls the backup schedule, save set, and target location for all systems, both virtual and physical. Backup agent software loaded within the guest operating system allows the virtual machine guest operating system to be managed the same way as all other systems. Exchange-aware agents use the Exchange VSS writer to create a local VSS snapshot that is then used to create the backup image. This differs from the array-based option because the VSS snapshot taken in this solution uses the VSS snapshot cache local to the Windows operating system instead of creating the snapshot or clone at the array level.

Figure 15. Software-Based Backup Solution



7. Additional Information

VMware vSphere offers many tools and features to increase the availability of Exchange 2013. vSphere vMotion, vSphere HA, and DRS can help to reduce downtime and improve flexibility in your Exchange 2013 architecture while lowering costs. In some cases VMware and Exchange features can be combined to improve overall availability, however consider the following points when architecting a solution:

- vSphere vMotion, vSphere HA, and DRS are supported for all Exchange 2013 roles, including DAG nodes.
- Exchange 2013 DAG nodes can use Fibre Channel or iSCSI attached storage for Exchange data files. This pertains to storage handled by ESXi hosts (RDMs or virtual disks on VMFS volumes).
- Network-attached storage is not currently supported for Exchange, regardless of whether the Exchange server is physical or virtual.
- Use of software iSCSI initiators within guest operating systems configured in a DAG, in any configuration supported by Microsoft, is transparent to ESXi hosts, and there is no need for explicit support statements from VMware.

Visit *Virtualizing Exchange with VMware* (www.vmware.com/go/exchange) for more information.