

High Availability and Disaster Recovery for Exchange Servers Through a Mailbox Replication Approach

Introduction

Email is becoming ubiquitous and has become the standard tool for communication in many enterprises, big and small. Microsoft is the dominant player in the messaging platform market through its Exchange Server. Enterprises are clearly choosing the reliability, scalability, and performance of Exchange, combined with the feature-rich Microsoft Outlook and Outlook Web Access clients and built-in collaboration services for workflow and other applications.

Email has become a mission-critical application for most businesses today and it has long been a challenge to backup and restore email information. If a crash occurs and if the data is not restored, it can have devastating consequences for a business. So it is imperative for companies to effectively backup and recover data and protect them from huge losses in productivity and downtime.

High Availability Solutions for Exchange Servers

Failover Clustering

Microsoft Clustering enables users to prevent hardware failures by stringing redundant hardware, called nodes, together through a central cluster manager that coordinates load balancing and data activity. Typically, nodes share common storage space and have the capability of picking up load off of a node that goes down due to hardware or software malfunction. There are two types of cluster environments—active/active and active/passive. In the former, every node in the environment is live and capable of processing requests. When one active node goes down, the others simply process more requests as the load is evenly dispersed across the remaining nodes. In the latter, there is a single active node that processes all incoming requests. Upon hardware or software failure in the active node, the passive node is immediately and automatically brought up by the cluster manager to take over the normal function of processing

data requests. In this way, hardware exposure is mitigated through physical hardware redundancy.

Microsoft Exchange Server supports both active-active and active-passive cluster environments. Exchange Server Clustering provides high availability by protecting against a node failure. However, it does not prevent against storage failures. Given the size of typical cluster environments, multiple hard disks are used to build large storage arrays. In Network and System Administration, when large numbers of any one device are used, failure is expected. When a hard disk fails, application disruption is unavoidable, as all the nodes in the cluster could be using that one particular disk as shared storage which contains all files, including Exchange Server database files. As protection against this particular failure, RAID configurations are common. However, from a performance standpoint, this significantly slows down I/O in the subsystems due to writing the data to multiple disks at the same time. Administrators have to balance such performance degradation and understand that this particular implementation has limitations. Again RAID option is to protect against any hard disk failure but it cannot prevent site disasters.

In direct contrast to this storage dependency, using a Standby solution through mailbox replication prevents against hardware, software and storage failures. Standby servers are normally installed on unique, usually geographically independent, Exchange Servers which serve as a barrier to failures of any type.

Exchange Server Clustering environments are more cost-intensive compared to the Standby option. The primary reason for this is the high hardware and software requirements. Clustering requires Windows NT Enterprise Edition, Windows 2000 Advanced Server or Windows 2003 Enterprise Edition and Exchange Server Enterprise Edition. Additionally, it only supports hardware listed on the Microsoft Hardware Compatibility list. On the other hand, a Standby

or Failover server does not have any special hardware requirements and is simply a software solution to meet disaster recovery needs. An additional cost, LAN connectivity is required between Exchange Server cluster nodes to send and receive what is called a heartbeat signal, among other communications. This signal is used by each node to determine if other nodes are still available. In case any node is not available, the remaining nodes take over. With Standby, LAN or WAN network connectivity will work to replicate Exchange Server mailboxes. The speed of this process is directly related to the size of the mailboxes and network bandwidth.

File or Block Level Replication

Different kinds of replication techniques can be used to replicate data between two servers both locally and remotely. In block level, replication is performed by the storage controllers or by mirroring the software. In file-system level (replication of file system changes), the host software performs the replication. In both block and file level replication, it does not matter what type of applications are getting replicated. They are basically application agnostic, but some vendors do offer solutions with some kind of application specificity. But these solutions cannot provide the automation, granularity and other advantages that come with application-specific solution. Also, one needs to be concerned about the following:

- Typically, identical hardware/software in both production and replicated servers are needed.
- Replicated server is always in a passive mode – Cannot be accessed for reporting/monitoring purposes.
- Possibility of virus/corruption getting propagated from production server to replicated server.

Exchange 2007 Built-in High Availability Features

Exchange Server 2007 includes four features that provide high availability for Mailbox servers: Local Continuous Replication (LCR), Cluster Continuous Replication (CCR), Single Copy Clusters (SCC) and Standby Continuous Replication (SCR).

- *Local Continuous Replication (LCR)* LCR is a single-server solution that uses built-in asynchronous log shipping technology to create and maintain a copy, or replica, of a storage group on a second set of disks that are connected to the same server as the production storage group. LCR provides log shipping, log replay, and a quick manual switch to a secondary copy of the data.
- *Cluster Continuous Replication (CCR)* CCR is a clustered solution that uses built-in asynchronous log shipping technology to create and maintain a storage group replica on a second server. CCR is designed to be either a one or two datacenter solution, providing both high availability and site resilience.
- *Single Copy Clusters (SCC)* SCC is a clustered solution that uses a single copy of a storage group on storage that is shared between the nodes in the cluster. SCC is very similar to clustering in previous versions of Exchange Server, with some significant changes and improvements.
- *Standby Continuous Replication (SCR)* SCR is designed for scenarios that use or enable the use of standby recovery servers. SCR enables a separation of high availability and site resilience. SCR can be combined with CCR to replicate storage groups locally (using CCR for high availability) and remotely in a secondary site (using SCR for site resilience).

These high availability features provide good functionality but one has to be an experienced user of Exchange server to implement them. Also, here are some of

the constraints one will face when implementing the built-in high availability of features of Exchange 2007.

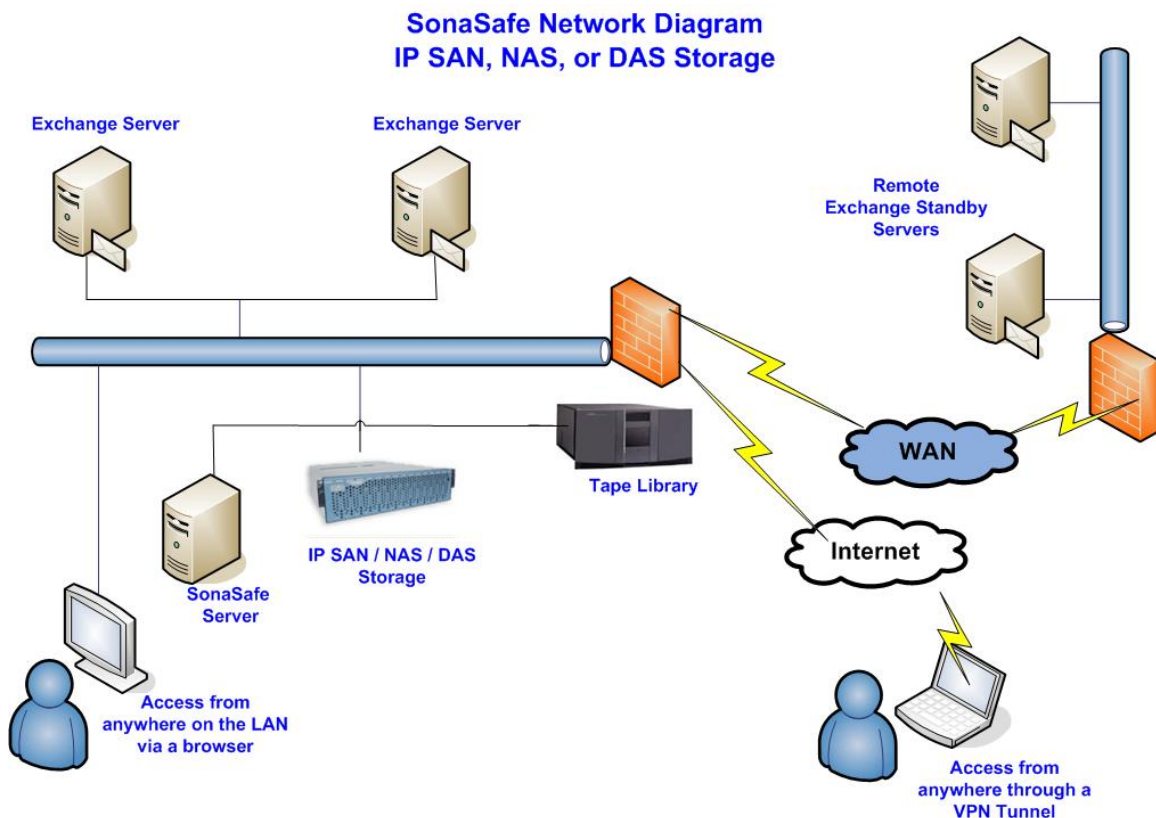
- Exchange Server 2007 runs on a 64-bit machine and hence costs more.
- For best performance, it is recommended that Active Directory Domain Controllers also run on a 64-bit machine, but it is not mandatory.
- No support for Exchange 2000 and Exchange 2003.
- Replication is done at storage group, level not at mailbox level.
- Ability to failover/failback just a single mailbox to test disaster recovery is not available.
- The replicated server is in a passive mode and cannot be accessed for reporting, monitoring and archival purposes.
- It cannot create replication for all storage groups at one time.
- It is a must to have only one mailbox store in a Storage Group, otherwise Exchange 2007 Replication will not work. This takes it back to the Exchange 5.5 world.

Sonasoftware Failover (Standby) Solution

Sonasoftware offers a unique solution which provides an integrated data protection, high availability and disaster recovery solution for Exchange servers. In Sonasoftware's SonaSafe solution, the backup is integrated with replication and the users get a two-in-one solution. Typically, customers have to go to two different vendors to implement two disparate solutions to achieve the same result. Also, it will cost three to four times more to implement these solutions compared to what is offered by Sonasoftware.

Sonasoftware's product, SonaSafe for Exchange Server, contains a unique architecture that not only creates easy to use backup tasks and schedules, but allows for efficient and simple recovery options, all the while minimizing chances of data loss. Considered two-tier architecture, SonaSafe for Exchange Server consists of an application and agent environment. The application is hosted by

an auxiliary server and houses the SonaSafe Recovery Catalog. The application server also hosts the network share that stores all the backup files. The files are stored on this network share and not on any particular target server so as to prevent loss of backup files. If the target server goes down, users would like to continue to access their backup files in order to rebuild the target server with as little downtime as possible.



With SonaSafe, the replication is done at a mailbox level and it is very application specific. One can pick and choose the mailboxes that need to be replicated. One can set up a granular plan for key executives, sales and IT people, in which the replication occurs more frequently to achieve the required Recovery Point Objective (RPO) and Recovery Time Objective (RTO). For everyone else in the

company, another plan can be set up where the replication intervals are not that frequent.

Another important feature of SonaSafe for Exchange Server solution is that the replicated or failover server is in an ACTIVE mode, unlike other solutions. The failover server can be accessed for reporting and monitoring purposes. With other replication solutions, the failover server is in a PASSIVE mode and cannot be used for maintenance, monitoring or reporting purposes.

Failover/Failback

When a disaster strikes the primary site, then all the users will be failed over to the remote site. Once the primary is rebuilt, one has to go through the failback process. With SonaSafe for Exchange server, the whole process is very easy to implement and can be done within a short period of time.

The only way to make sure that your disaster recovery solution works is to test it periodically. Unfortunately, to do that one has to failover the entire Exchange server. Exchange Administrators will be leery about doing this for fear of crashing the production Exchange server. With SonaSafe for Exchange server, one can create a test mailbox and use it for failover/failback testing periodically. Through this approach, customers can be fully assured that their disaster recovery solution will work when it is badly needed and have peace of mind.

Exchange Migration

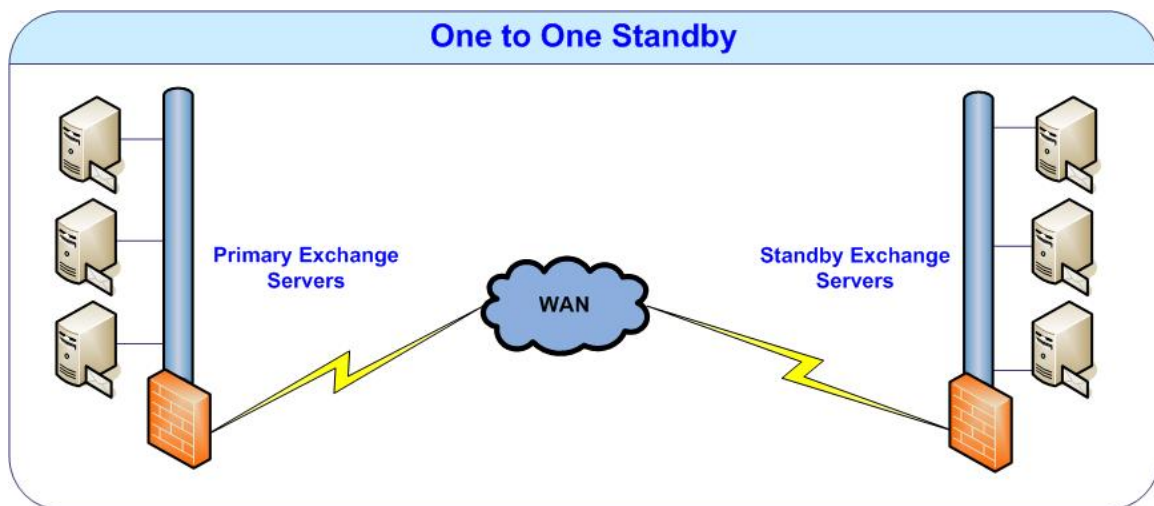
With SonaSafe, since the replication is done at a mailbox level, there is no need to have identical hardware for both primary and failover servers. This is not the case with other replication solutions. Also, there is no need to have identical versions of Exchange on primary and failover servers. In fact, one can run Exchange 2003 on primary server and Exchange 2007 on failover server. This feature can be used as a migration tool. For example, you can failover to the

failover server which runs Exchange 2007. Upgrade the original primary to Exchange 2007 and failback again. The whole exercise can be done very easily using a web-based interface.

Standby Scenarios

One-to-One Standby

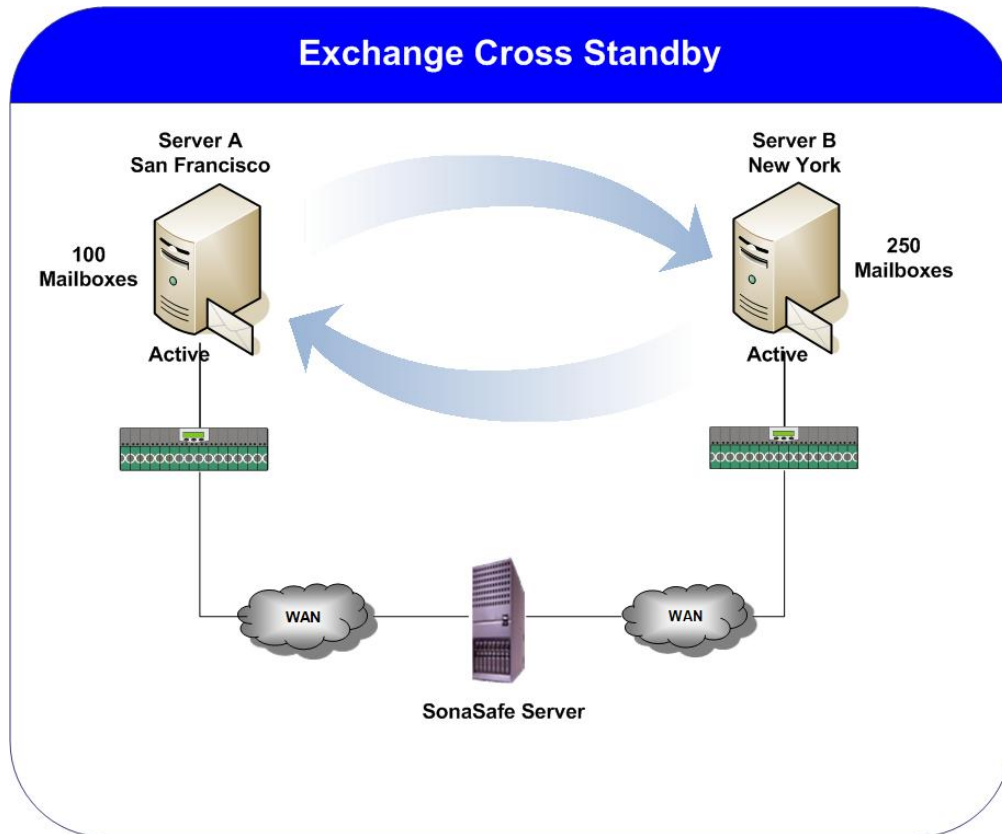
In the one-to-one standby scenario, for each primary server there is a failover server at the remote site. For example, one of our customers has two primary servers in San Jose and two failover servers in Denver. This is the typical scenario most of the implementations occur. Typically, companies have on average one to three Exchange servers, based on the number of (mailboxes employees) per Exchange server.



Cross Standby

One of Sonasoftware's customers has two offices, one in San Francisco and another one in New York. The customer has two Exchange servers, one each in San Francisco and New York. The customer didn't want to create a separate disaster recovery site, but wanted to use the two existing offices as a mutual failover site.

Because of the way SonaSafe architecture is implemented, this scenario was made possible.



The mailboxes get backed up locally at each site, but get replicated to the other site. In case the server in San Francisco goes down because of an earthquake, then all the users will be failed over to the server in New York. In this case, the Exchange server in New York will act as the primary server for users in New York and as the failover server for users in San Francisco.

Conclusion

Companies are impacted adversely with significant loss of productivity and revenue when an Exchange server goes down. With increasing dependence of business on Exchange server, customers are demanding instant failover to a local or remote server. This concept may mean survival of business in case of a major destruction. High availability and disaster recovery of Exchange servers

should be taken seriously and companies should implement the proper solution to protect them.

About Sonasoftware®

Sonasoftware Corp. automates the disk-to-disk backup and recovery process for Microsoft Exchange, SQL and Windows Servers with its groundbreaking SonaSafe® Point-Click Recovery® solutions. SonaSafe is the only product that provides an integrated backup/recovery and replication solution for Exchange and SQL servers. Designed to simplify and eliminate human error in the backup and recovery process, SonaSafe solutions also centralize the management of multiple servers and provide a cost-effective turnkey disaster recovery strategy for companies of all sizes. *For more information, please visit www.sonasoftware.com.*