Teneros Always-On® for Microsoft Exchange® 2010

Table of Contents

Executive Summary

Ongoing Operations, LLC is a market leader in providing Disaster Recovery solutions. The company offers a wide range of Disaster Recovery (DR) solutions for applications, systems and services that are critical for successful implementation of Disaster Recovery procedures, meeting the stringent standards of the financial services industry.

Organizations have become increasingly reliant on email as a primary method for communication and, as such, the messaging system in most environments has come to be considered a mission-critical application. Most people would agree that the average organization would be severely affected if the messaging environment were to go off-line for an extended period of time. Communications between employees would have to be in person or over the phone, document sharing would be more complex, communication with clients would be affected and productivity of employees both local and remote would suffer. This dependence on messaging makes it critical to have a disaster recovery plan as it pertains to the Exchange server messaging environment.

This document details the Disaster Recovery (DR) solution offered by Ongoing Operations for your messaging infrastructure when using Microsoft Exchange 2010 as your primary email/messaging solution.

Goals and Objectives

The high-level goal for the solution is to have no down time for email and calendars from anywhere while providing four 9's of uptime in a disaster scenario. This solution is delivered by best of breed messaging technology using native features of Microsoft Exchange 2010 Server.

Objectives for this solution are:

- Provide a Business Continuity/ Disaster Recovery solution for Email.
- Ensure a high level of Security
- Support Mobility
- Sustain Collaboration
- Enable enhanced serviceability

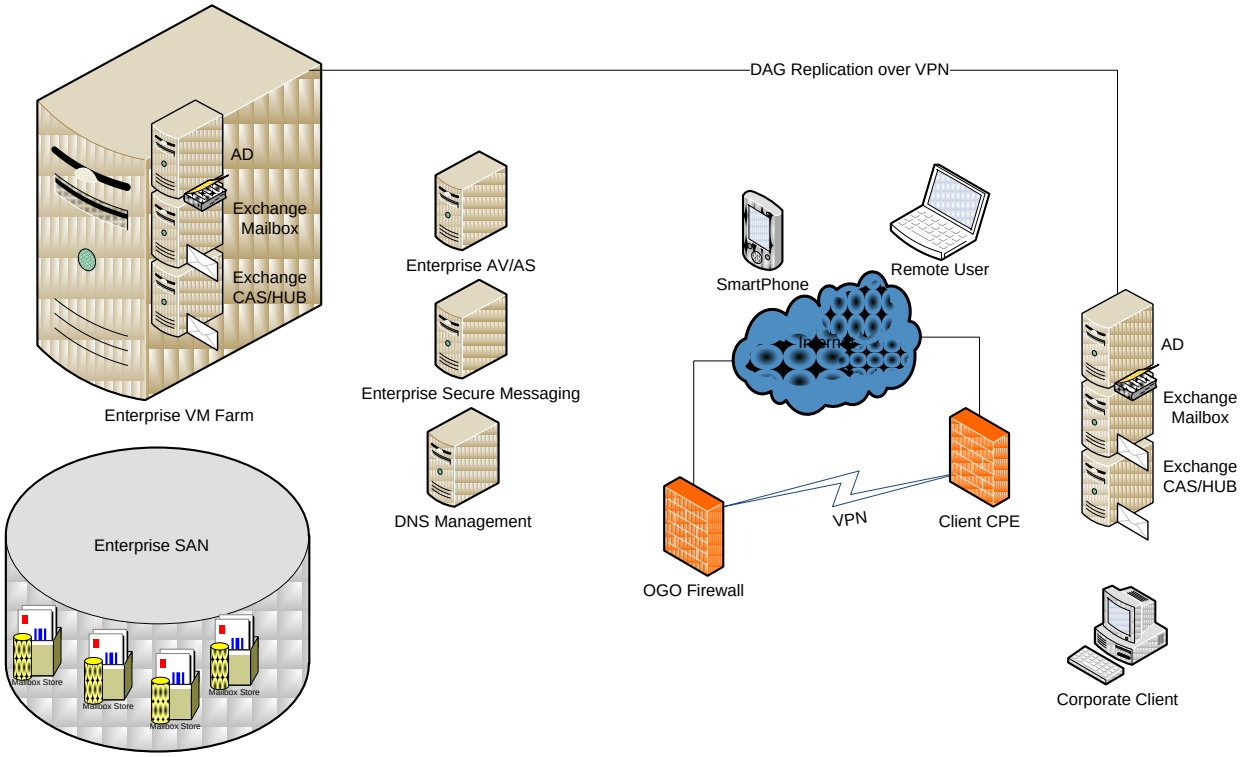
Solution Description

A Disaster Recovery (DR) solution should provide uninterrupted access, service and support in different failure situations that could take place, such as power failures in one or more locations, network loss at one or more locations or server failures. A complete DR solution should include offsite data and application access.

Ongoing Operations' *Teneros Always-On® for Microsoft Exchange® 2010* is based on the Database Availability Group (DAG) a native Exchange 2010 mailbox role feature that can perform automated recovery at the mailbox database level in the event of a hardware, storage or network failure. The DAG utilizes a subset of Windows 2008 failover clustering in order to monitor each node's health.

The DAG uses log shipping replication technology to replicate mailbox database transactions between members of a DAG. This replication technology has been improved and fine tuned in terms of resiliency and recovery over the past few years, since its introduction in Exchange Server 2007.

A schematic diagram of Teneros Always-On® for Microsoft Exchange® 2010



Design Considerations

The solution takes into consideration the following components of the Exchange server to provide the DR solution for your Exchange 2010 messaging environment.

1. Exchange Server

Various roles and functions of the Exchange server that are available at the primary site and needed for the proper functioning of the messaging environment are replicated on the DR site to provide uninterrupted email continuity to all users.

- Exchange Server Design
  - Mailbox Databases (Definition and Number)
  - Exchange Mailbox Replication
- Exchange Client Access Server
- Exchange Hub Transport Server
- Third party application Servers (Blackberry, Good link etc)

To setup a DAG on Exchange 2010 the following are required:

1. Two or more servers running Windows Server 2008, Enterprise Edition
2. Two network interfaces per server
3. Exchange Server 2010 Enterprise Edition
4. 1 File share witness per DAG

The file share witness cannot be hosted on a member of the DAG. A Hub transport server or a file server can be used.

2. Active Directory

Exchange server 2010 relies on an Active Directory (AD) infrastructure to do its job. An AD infrastructure running on Windows server 2003 or Windows server 2008 must be in place for Exchange 2010 deployment.

To install Exchange server 2010, the AD domain functional level must be Windows server 2003 or higher for each domain in the AD forest that will house an Exchange server 2010. Windows 2000 Mixed, Windows 200 Native, and Windows Server 2003 Interim modes are not supported

Each Active Directory (AD) site where an Exchange server 2010 is to be installed must have at least one Global Catalog server running on the latest 32-bit or 64-bit edition of Windows server 2003/2008 Standard or Enterprise Edition.

3. Bandwidth/Network

A site-to-site VPN needs to be established between the primary site where the Exchange server is located and the Ongoing Operations data center where the Exchange 2010 DR solution will be deployed.

Key parameters for consideration here are:

- Number of users
- Email usage(Log generation rate)
- Network Latency (Round trip time)
- Storage (Retention space for logs on the servers)
- Database size

Database replication within a Database Availability Group (DAG) is only supported between mailbox servers with less than 250 ms of round trip latency. We recommend less than 100 ms.

4. Exchange Server Management and Monitoring

The dependability and reliability of any application comes from proper maintenance and upkeep. Though Exchange server 2010 has continuous online defragmentation, compaction and contiguity maintenance for routine database maintenance, implementing and performing proper management and maintenance procedures will keep the system well tuned.

We plan to use the following tools that provide secure and reliable means to manage the servers remotely.

- Exchange Management Console (EMC)
- Exchange Control Panel (ECP)
- Remote Desktop Protocol (RDP)

We also plan to develop a solution leveraging the Remote Exchange Management Shell (EMS)

5. Exchange Backup/Recovery

Exchange 2010 provides no native methods to backup mailbox data in the traditional sense. Even for third party backups, the old style of streaming backups is no longer supported. The only option is to utilize a Volume Shadow copy Services (VSS) based backup. With DAGs and appropriate retention policy, there may be situations where backup for Exchange server 2010 might not be necessary at all.

A more detailed discussion on this topic is beyond the scope of this document.

6. SPAM and Virus Protection

The copy of the same software or mechanism used on your production server will be used on the servers at the DR location to provide spam filtering and virus protection.

7. Hardware and Software

The server machines that will be deployed at the DR Site for this solution will be deployed on Enterprise class server hardware fine tuned for this purpose. The whole environment will be running on ESX

software based virtual environment with Virtual Machines (VMs) running corresponding Microsoft Windows Operating Systems and utilizing resources matching the capabilities of your existing server configurations.

Solution Characteristics

With this solution in place your organization has the following benefits:

- Reliable and predictable SLA for end user Email continuity
- Always on messaging infrastructure and expertise
- Schedule Exchange Server maintenance without outage to the end users
- Planned DR testing capability

Assumptions

The deployment of the DR solution for Exchange 2010 assumes that your organization already has the necessary hardware and software infrastructure to host and run the Microsoft Exchange 2010 server, if it is already not in place.