TENEROS®

WHITE PAPER

Exchange 2010 Business Continuity Planning

www.teneros.com

Microsoft GOLD CERTIFIED Partner

Exchange 2010 provides a new architecture for implementing high availability (protection from server level downtime) and disaster recovery (protection from site level downtime). While some components of clustering have been simplified in 2010 to provide easier deployment, there is significant additional complexity and cost around network load balancing and site level failover. This white paper provides an overview of the Exchange 2010 HA and DR architecture along with the key architectural challenges to keep in mind during implementation. The document concludes by discussing the Teneros product offerings for Exchange 2010 along with the significant return on investment (ROI) benefits.

High Availability (protection from server level downtime)
Exchange 2010 has two critical components for implementing high availability, which add deployment complexity and cost: Database Availability Group (DAG) and network load balancers.

Database Availability Group (DAG)
This feature provides the ability to setup database level replication and failover among a group of Exchange mailbox servers. While easier to setup as compared to a conventional Exchange cluster, the underlying complexity is the same as an Exchange 2007 CCR cluster.

Network Load Balancers
In Exchange 2010 all Outlook traffic (LAN or WAN) has to pass through the Client Access Server (CAS), thereby making it a single point of failure. This new failure scenario can be mitigated by either of the two methodologies:

1. **Deploying two hardware load balancers in a redundant configuration.** The load balancers should support Exchange monitoring and protocol awareness to provide soft failure detection on CAS servers. In addition the load balancers need to have sufficient throughput handling capabilities to support internal email traffic on the LAN. While a cheap load balancer may suffice for lightly loaded external website traffic, supporting internal email traffic can be resource intensive. Load balancers from leading vendors such as F5 and Cisco can be a significant investment.

2. **Implementing a Windows network load balancing cluster**. Multiple Windows servers can be combined into a software load-balancing configuration. In addition to setting up a load balancing cluster, this requires installing additional NIC cards and configuring layer 2 and layer 3 network switches to enable traffic multicasting without network flooding. One challenge with using Windows network load balancer is that it can't detect soft failures. Hence if one of the CAS server stops serving users but is reachable on the network it can cause downtime for a significant part of the user population.

Deployment Complexity
The Windows network load balancing cluster can't be setup on the same servers that have a DAG setup, thereby adding additional complexity and costs. Minimum high availability configuration for an Exchange 2010 deployment is one of the two:

1. Two Exchange Mailbox servers in a DAG, 2 hardware load balancers in a redundancy mode

2. Two Exchange Mailbox + HUB servers in a DAG, 2 CAS servers in a windows network load balancing cluster

As a result, a minimum of four Exchange servers with two clusters (DAG and Windows NLB) are required to provide high availability. If only DAG is implemented without load balancing, the CAS role provides a single point of failure.

Disaster Recovery (protection from site level failure)
Site level failover is significantly more complex in Exchange 2010. Implementing a DAG across a WAN link may not provide the required failover protection. DAG uses Windows clustering technology for failover, which is a majority node set architecture. In other words, for a DAG cluster to be able to failover or continue to serve users, a majority of the nodes need to be available. This introduces challenges when DAG is deployed over a WAN link.

WAN Failover and Failback
Consider the scenario of a customer with one Exchange server on his primary site and a second Exchange server in the DR site with a DAG between them for site level failover. During the setup of DAG, the customer will be required to choose a location for a third node for the DAG cluster, referred to as a file share witness. In this setup, either of the two Exchange servers can only serve users if they can connect to the file share witness and thus establish a majority. Thereby the file share should be placed at the primary site as otherwise any loss of network connectivity between the primary and the DR sites will cause an email outage at the primary site due to a lack of a majority. If that is done, in the event of a true site level failure, the Exchange server at the DR site can't failover and serve users as it doesn't have the majority. As a result you must use the Windows failover cluster management tools to manage a datacenter switchover for a two-member DAG that is extended across multiple datacenters. In other words DAG member servers at the DR site need to be forced to create quorum manually through clustering tools, at which point the servers in the failed datacenter are internally (but only temporarily) removed from the DAG. This can easily lead to split brain, as when the primary site recovers it will attempt to start serving users since it has a quorum. In a two server DAG there is no easy way to prevent this from happening, however for a 3+ node DAG setup, Datacenter Activation Coordination Model (DAC) can be used to minimize split brain.

Cross Server Protection
Cross server protection for disaster recovery is also challenging in Exchange 2010. Consider an organization with two offices in New York and Chicago with end users and a local Exchange mailbox server at each location. Ideally the company may want to create a DAG between the two Exchange servers to provide a failover in the event of a server or site level outage. However this would create challenges. If the file share witness is placed in New York, any network connectivity loss between the two offices will result in immediate email downtime for Chicago users, even though Chicago is running perfectly healthy, and vice versa.

Requirements for Exchange 2010 Continuity
Summarizing the above discussion there are three key points to consider when evaluating Exchange 2010 continuity:

1. Protection from Mailbox database failures on the LAN that can lead to data loss or service unavailability

2. Protection from Client Access failures on the LAN due to CAS or BES server outages that can impact Outlook, OWA, Active Sync and Blackberry devices

3. Protection from Site level outages that impact the entire infrastructure including Mailbox, CAS, Blackberry and Active Directory/DNS

Teneros Exchange 2010 Continuity Offerings

Teneros provides a suite of offerings to provide full redundancy to the Exchange 2010 messaging stack at significantly reduced CAPEX and OPEX costs to the business, as well as flexible purchasing levels, to fit every budget. The offerings are easy to deploy and simplify the messaging environment significantly while increasing uptime to five nines. Teneros offerings for Exchange 2010 include:

1. Protection from Mailbox database failures on the LAN
2. Protection from Client Access failures on the LAN (CAS or BES server)
3. Protection from Site level outages that impact the entire infrastructure including Mailbox, CAS, Blackberry and Active Directory/DNS

Teneros Continuity Platinum

Continuity Platinum Level	
Protection from Mailbox database failures on the LAN	Yes
Protection from Client Access failures on the LAN (CAS or BES server)	Yes
Protection from Site level outages that impact the entire infrastructure including Mailbox, CAS, Blackberry and Active Directory/DNS	Yes

Businesses can reduce the cost and complexity of Exchange 2010 HA & DR through this all-inclusive offering that protects from database, CAS, Blackberry and site level failures. There is a significant cost saving by eliminating the need for setup of complex clusters, expensive network load balancers and remote datacenters as well as reducing the number of Exchange servers required. The Teneros Continuity Platinum offering for Exchange 2010 is delivered from Teneros data centers and provides failover for full Exchange functionality in less than 60 seconds, protecting all server roles including CAS, Hub and Mailbox. The service is easy to setup and can be used for planned maintenance as well as unplanned downtime due to server or software failure. In addition the business automatically gets the protection from site level failures as well, such as natural disasters, power outages and network cuts. Peripheral application infrastructure such as Blackberry server and Active Directory are also protected by failover protection.

The Teneros service can be setup within hours thereby eliminating significant implementation cost, time and complexity. Teneros provides a router, which when installed on the network, provides a secure connection to the Teneros data center. Data replication is real time and is fully encrypted and compressed for bandwidth optimization. Failover can be activated automatically from Microsoft Exchange management tools or manually through the Teneros user interface.

Teneros Continuity Platinum Benefits

	With Teneros	Without Teneros
CAPEX	Zero CAPEX	**Database protection**: Double the hardware and storage for DAG replicas **Client Access protection**: Two hardware load balancers or a two node or more windows software load balancing cluster**,** replica CAS server, redundant BES server with third party replication software **Site Level protection**: Redundant datacenter with hardware and storage for mailbox, CAS, Hub, BES and Active Directory
OPEX	Easy implementation and no ongoing management or monitoring	**Database protection**: Implement monitor and manage DAG cluster for local HA **Client Access protection**: Implement, monitor and manage network load balancing cluster using hardware load balancers or windows NLB; Implement and manage a third party disk replication cluster for BES **Site Level protection**: Implementation, monitoring and management of a remote disaster recovery infrastructure and managing exchange DAG clusters during WAN failover/failback to resolve issues related to quorum and DAC
IT Resources	Requires basic Exchange expertise for operation	Requires expertise in datacenter design, storage, networking, virtualization, replication, clustering and DNS
SLA	< 60 seconds failover	Best effort
Support during failures or disasters	24X7 with on demand Exchange, BES expertise	Internal critical IT resources may not be available during a disaster or a significant failure

Teneros Continuity Gold

Continuity Gold Level	
Protection from Mailbox database failures on the LAN	No
Protection from Client Access failures on the LAN (CAS and BES server)	Yes
Protection from Site level outages that impact the entire infrastructure including Mailbox, CAS, Blackberry and Active Directory/DNS	Yes

Businesses that choose to implement DAG clustering for local database high availability can leverage this offering to add protection from client access failures as well as site level failures. There is a significant cost saving by eliminating the need for setup of expensive network load balancers and remote datacenters as well as reducing the number of Exchange servers required. The Teneros Continuity Gold offering for Exchange 2010 is delivered from Teneros data centers and provides failover for Client Access Exchange and Blackberry functionality in less than 60 seconds as well as complete recovery from site level outages in less than 30 minutes. The service is easy to setup and can be used for client access and Blackberry server planned maintenance as well as unplanned downtime due to server or software failure. Additionally it provides the business full protection from site level failures.

The Teneros service can be setup within hours thereby eliminating significant implementation cost and complexity. Teneros provides a router, which when installed on the network, provides a secure connection to the Teneros data center. Data replication is real time and is fully encrypted and compressed for bandwidth optimization. Failover can be activated automatically from Microsoft Exchange management tools or manually through the Teneros user interface.

Teneros Continuity Gold Benefits

	With Teneros	Without Teneros
CAPEX	No CAPEX	**Client Access protection**: Two hardware load balancers or a two node or more windows software load balancing cluster**,** replica CAS server, redundant BES server with third party replication software **Site Level protection**: Redundant datacenter with hardware and storage for mailbox, CAS, Hub, BES and Active Directory
OPEX	Easy implementation and no ongoing management or monitoring	**Client Access protection**: Implement, monitor and manage network load balancing cluster using hardware load balancers or windows NLB; Implement and manage a third party disk replication cluster for BES **Site Level protection**: Implementation, monitoring and management of a remote disaster recovery infrastructure and managing exchange DAG clusters during WAN failover/failback to resolve issues related to quorum and DAC
IT Resources	Requires basic Exchange expertise for operation	Requires expertise in datacenter design, storage, networking, virtualization, replication, clustering and DNS
SLA	< 60 seconds failover	None
Support during failures or disasters	24X7 with on demand Exchange, BES expertise	Internal critical IT resources may not be available during a disaster or a significant failure

Teneros Continuity Silver

Continuity Silver Level	
Protection from Mailbox database failures on the LAN	No
Protection from Client Access Server failures on the LAN	No
Protection from Site level outages that impact the entire infrastructure including Mailbox, CAS, Blackberry and Active Directory/DNS	Yes

Companies can get affordable site level failure protection with the Teneros Continuity Silver. Even though a company may have invested significantly in implementing a DAG and network load balancing cluster for local high availability on the LAN (protection from database and client access failures), site level resilience adds significant cost and complexity with a poor return on investment due to the infrequent use. Teneros Site Protection service for Exchange 2010 provides full protection from natural disasters, power outages or any other site level failure at one-tenth the cost of implementing it in-house. The service is delivered from Teneros datacenters enabling full email functionality to be activated in less than 30 minutes. Peripheral application infrastructure such as Blackberry server and Active Directory are also protected by site level failover protection. The Teneros service can be setup within hours thereby eliminating significant implementation cost and complexity. Teneros provides a router, which when installed on the network, provides a secure connection to the Teneros data center. Data replication is real time and is fully encrypted and compressed for bandwidth optimization. Failover can be activated automatically from Microsoft Exchange management tools or manually through the Teneros user interface.

Teneros Continuity Silver Benefits

	With Teneros	Without Teneros
CAPEX	No CAPEX	**Site Level protection**: Redundant datacenter with hardware and storage for mailbox, CAS, Hub, BES and Active Directory
OPEX	Easy implementation and no ongoing management or monitoring	**Site Level protection**: Implementation, monitoring and management of a remote disaster recovery infrastructure and managing exchange DAG clusters during WAN failover/failback to resolve issues related to quorum and DAC
IT Resources	Requires basic Exchange expertise for operation	Requires expertise in datacenter design, storage, networking, virtualization, replication, clustering and DNS
SLA	< 30 minute failover	None
Support during failures or disasters	24X7 with on demand Exchange, BES expertise	Internal critical IT resources may not be available during a disaster or a significant failure

About Teneros

Founded in 2003, Teneros is the leading provider of Always-On™ email high availability, disaster recovery, archiving, eDiscovery, security, and spam solutions for Microsoft Exchange 2003, 2007, and 2010. Teneros offers Software-as-a-Service (SaaS) continuity solutions for email, combining superior technology and expert service in a single solution. Teneros solutions ensure continuous email operations through planned and unplanned downtime of corporate email servers. The result for Teneros customers is lowered costs and administrative burdens from email systems, simplified operations, and improved end-user productivity.

Support: 1.88.Teneros.1 • Tel: 650.641.7400 • www.teneros.com