

A background image showing a laptop on a desk with a speedometer overlay. The speedometer has numbers from 0 to 70 and a needle pointing towards 40. The scene is dimly lit, suggesting an office environment.

Protecting the Microsoft Exchange 2007 and 2010 Environment

 A Trend Micro White Paper | October 2009

TABLE OF CONTENTS

ABSTRACT.....	3
MICROSOFT EXCHANGE 2007 AND 2010 ROLES.....	3
THE THREAT LANDSCAPE.....	4
• From Chaos to Cash	
• Deployment scenarios with ScanMail™ for Microsoft® Exchange	
• High-Performance Scanning	
• Easy Administration	
PROTECTING YOUR BUSINESS WITH SCANMAIL.....	9
CONCLUSION.....	10
• Appendix A: Exchange 2007 Cluster Options	
• Exchange 2010 Cluster Options	

Protecting the Microsoft Exchange 2007 and 2010 Environment

ABSTRACT

Since its debut in 1996, Trend Micro™ ScanMail™ for Microsoft® Exchange has seen many changes in email threats as well as scanning technologies. From the early days of MAPI technology, to ESE, and finally VSAPI technology, ScanMail scanning software has always provided customers with a high-performance, low-administration solution that effectively keeps critical organizational email free of unwanted and malicious content in the face of an ever-evolving threat landscape.

This paper will outline some of the most relevant Microsoft Exchange 2007 and 2010 features, discuss key changes in the email threat landscape, and discuss how ScanMail functions within the Exchange 2007 and 2010 environment to continue combating the latest threats.

MICROSOFT EXCHANGE 2007 AND 2010 ROLES

Microsoft Exchange 2007 introduced the separation of Exchange tasks into individual server roles. The following server roles may be present in Exchange 2007 and 2010 deployments.

Client Access server role:

The Client Access server provides end users with Outlook Web Access, Exchange Active Sync, AutoDiscovery, and Outlook Anywhere (formerly known as RPC over HTTP). POP3 or IMAP4 client connections also pass through the Client Access servers. A light version (that provides access for roaming users) and a premium version are provided for the Client Access server.

Edge Transport server role:

The Edge server role is designed to operate on an organization's perimeter network. Instead of being deployed in the Exchange organization, it functions at the gateway and provides SMTP relay and smart host functions.

Hub Transport server role:

The Hub Transport role is required for all email routing within an organization. It provides the ability to apply transport rules and journaling rules, as well as deliver messages to recipients' mailboxes. Messages sent and received from the Internet are relayed through the Hub Transport server to other server roles.

Mailbox server role:

The Mailbox server hosts mailbox databases that provide email storage and advanced scheduling services for Microsoft Office Outlook users. The Mailbox server can also host public folder databases.

Unified Messaging server role:

The Unified Messaging server provides recipients the ability to access their Exchange mailbox over any telephone for email, voicemail, fax messages, calendaring, and contact information.

For more information about Microsoft Exchange server roles, please visit:

<http://technet.microsoft.com/en-us/library/aa996058.aspx>

THE THREAT LANDSCAPE

FROM CHAOS TO CASH

Enterprise security professionals understand that the motivation behind malware has shifted from creating chaos to making money. Cybercriminals reap financial gain by stealing and reselling valuable information including credit card numbers, personal identities, and intellectual property. Others propagate Trojans to take control of inadequately protected computers and servers, using them for future malicious endeavors or renting them to others for spam blasts, Denial of Service (DoS) attacks, malware campaigns, or targeted attacks. Trend Micro has created many resources to document this shift, including a 2007 Threat Roundup that can be found at the Trend Micro Threat Resource Center: <http://itw.trendmicro.com>. For further discussion of the latest attacks, visit the Trend Micro Malware blog: <http://blog.trendmicro.com/>

Of note, today's email threats have become much more sophisticated and insidious. Once installed on a PC, they use a range of techniques to beat traditional defenses and remain undetected for long periods of time. Such techniques often include the use of:

- Sophisticated and malicious spam campaigns for rapid or targeted propagation ahead of reactionary updates for security products
- Multiple, often sequential variants that may use non-standard compression tools to quickly change digital signatures and pass pattern-file based defenses
- Multi-stage attacks that connect to the web to download malware that is constantly evolving and includes increasing amounts of spyware
- Threats that rely on links to malicious sites rather than malware attachments
- Socially-engineered threats that reflect common business activities, current events, and other commonplace behavior to overcome increased end-user awareness and vigilance

Although the traditional antivirus scan engine still has an important role to play in enterprise security, an effective defense against today's threats requires much more extensive security measures. Organizations increasingly find that they need:

- 1) A strong antispam defense, including sender and content-oriented inspection, to help stop malware
- 2) Dedicated detection of malware that includes spyware, Trojans, and other threats—not just viruses
- 3) Zero-day protection that acts independently of pattern-file updates
- 4) Identification of links to malicious sites, instead of just malicious attachments
- 5) New security techniques and models to defeat cybercriminals at the “change the pattern-file game” that they have learned to play, and increasingly, win

For more information, read the white paper on Malware Today and Mail Server Security available at: <http://messagingsecurity.trendmicro.com/pr/tm/en-us/enterprise/ms/smex-lowestTCO.aspx>

DEPLOYMENT SCENARIOS WITH SCANMAIL™ FOR MICROSOFT® EXCHANGE

With the differences in Exchange roles, as well as the evolving threat landscape, there are various deployment scenarios for an organization's Exchange infrastructure as well as different recommendations on how to install ScanMail. In this white paper, we will discuss a multi-site deployment with multi-roles of Exchange 2007 and 2010 (**Figure 1.0**) and the important considerations for deploying ScanMail. To discuss alternative deployment scenarios, please contact a pre-sales engineer or support group from Trend Micro or a certified channel partner.

Protecting the Microsoft Exchange 2007 and 2010 Environment

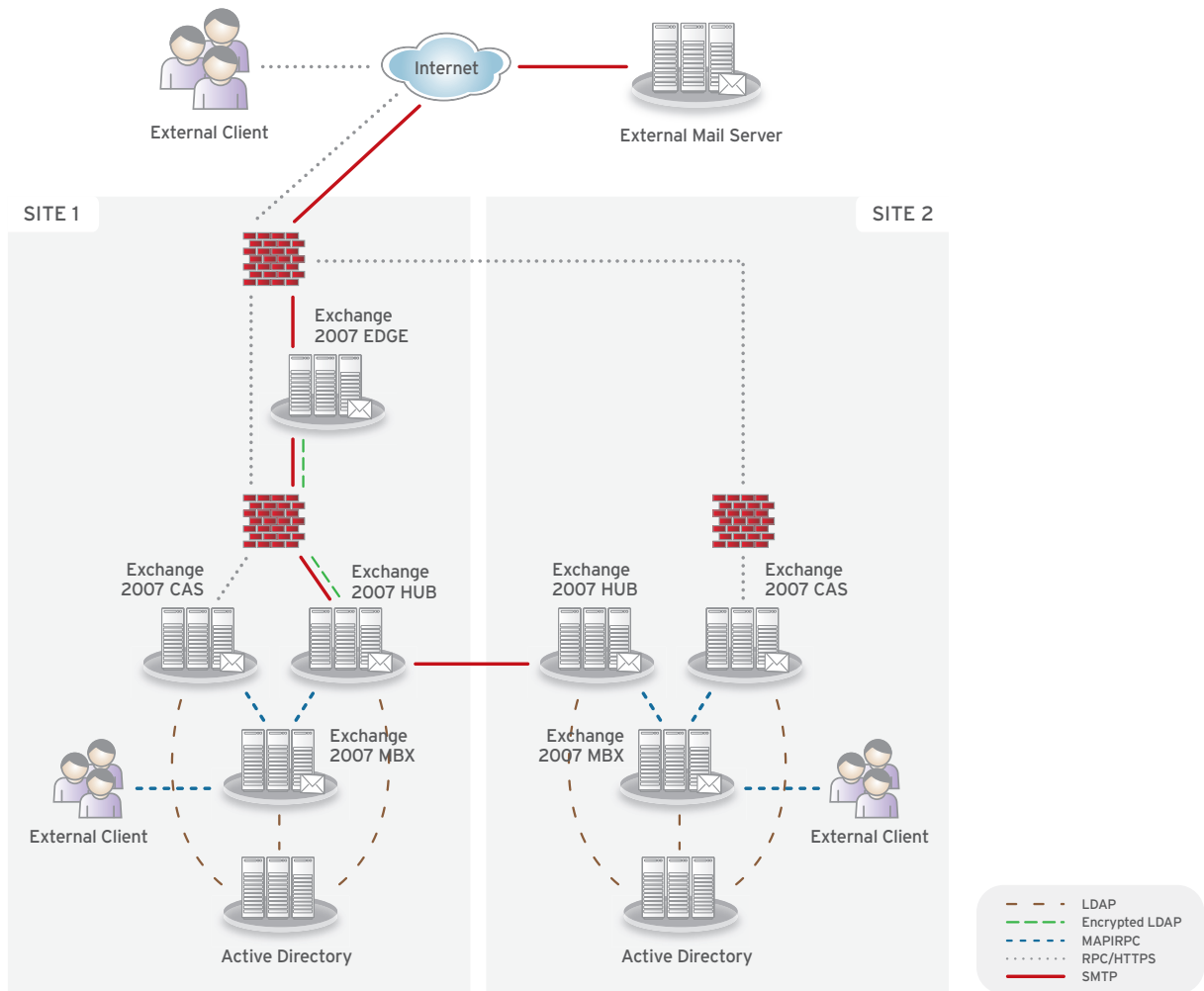


FIGURE 1.0: Multiple sites with multiple server roles

When installing and configuring ScanMail, some consideration must be taken into account to achieve the best results for each environment. In Exchange 2007 and 2010, ScanMail supports three server roles that serve very different purposes. For each role, organizations must consider security and performance to help ensure they are able to strike the balance that is most appropriate for their topology, business, and risk tolerance.

At the Edge

According to the Radicati Group, there are an estimated 1.3 billion email users worldwide that send and receive nearly 210 billion emails per day. Of that number, TrendLabsSM has found that almost 90% of email is unsolicited bulk email spam. In addition, at least 80% of spam is English-language.

Enabling Trend Micro™ [Email Reputation Services](#), which refuse connections (and messages) from illegitimate senders based on cloud-queries to the correlated threat intelligence of the Trend Micro™ Smart Protection

Protecting the Microsoft Exchange 2007 and 2010 Environment

Network™, will help stop threat while keeping connections available for legitimate email. This approach dramatically reduces the amount of bandwidth consumed to help ensure optimal performance and free up valuable CPU cycles on the Exchange servers. ScanMail 10 integrates Email Reputation Services and allows customers to configure and manage them directly from the ScanMail console. In addition, the built-in antispam engine will efficiently block spam from unknown senders including image spam, Microsoft Office document spam, and PDF spam.

Trend Micro is rated #1 against spam. For more information, please read:

http://www.westcoastlabs.com/downloads/productTestReport_0061/Anti-spam_Comparative_Report.pdf

Since spam is often a delivery mechanism for malware, many viruses, spyware, and Trojans may also be stopped by a strong antispam defense. However, a comprehensive malware defense continues to require traditional antivirus scanning, dedicated antispam detection, and zero-day protection. Accordingly, it is recommended that organizations enable antivirus and antispam protection. However, email threats increasingly utilize malicious URLs rather than attachments. For this reason, ScanMail 8.0 (SP1 and above) introduced Trend Micro's Web Reputation Services, a technology that uses cloud queries to the Smart Protection Network to detect URLs within messages that link to malicious or compromised websites.

By enabling antimalware settings at the Edge, you will be able to stop threats at the gateway and save even more CPU cycles reprocessing email on Exchange servers within the network. Optionally, content filtering and attachment blocking can be enabled at the Edge; however, the need to inspect attachments and identify true file types will cause a considerable reduction in performance.

Through the Hub

Since all email (incoming, outgoing, and internal) must go through the Hub transport in Exchange 2007 and 2010, it is crucial that antivirus scanning be performed here. By helping ensure that all email—including internal communications—is scanned for any malicious threats, Exchange environments will have the maximum protection. This is particularly important given the mobility of today's workforce and risk of infection while outside a company's LAN. Further, incoming email will continue to be scanned using the latest threat intelligence even after it has passed the Edge.

There is no need to worry about the performance impact of redundant scanning because the Trust Scan feature leverages the antivirus stamp to ensure that inspection only occurs when new threat intelligence has been received. Enabling antivirus on the Hub transport also provides you with zero-day protection through the use of the Trend Micro IntelliTrap engine. Content filtering, as well as attachment blocking, should be enabled on the Hub transport so that control of email flow and content is managed efficiently. This will allow you to control email flow and reduce internal use of bandwidth from Hub server to Hub server.

Organizations that have not deployed the Edge role or the [Trend Micro InterScan™ Messaging Security](#) solution at the email gateway should consider enabling Antispam and Web Reputation Services on the Hub transport. This measure will provide an extra layer of protection against increasingly sophisticated and malicious spam.

On the Mailbox Server

Given the rapid rate at which malware changes and new threats are released, it is prudent to install ScanMail and enable antimalware scanning on the Mailbox server role. By doing so, you will be able to perform manual and scheduled scans on the store scanning old email with newly updated pattern files and helping ensure that

Protecting the Microsoft Exchange 2007 and 2010 Environment

the store is free of malicious code. Similar to the Trust Scan feature, incremental scanning leverages the antivirus stamp to avoid redundant inspection. The option to scan email within a specific time period is also available. This capability is especially useful when upper management has requested that a specific email be removed from the store. Further, organizations that have concerns about sensitive content and “internal spam” (such as message threads with large distribution groups to which people “reply all”) should enable content filtering to perform routine maintenance and remove unwanted email based on advanced content filter matching rules.

EXCHANGE ROLE	PERFORMANCE	SECURITY	
Edge	<ul style="list-style-type: none">• Antispam• Email Reputation Service• Web Reputation Services	<ul style="list-style-type: none">• Antispam• Email Reputation Service• Web Reputation Services• Antivirus	<ul style="list-style-type: none">• [optional] Content filtering• [optional] Attachment blocking• [optional] Threat Management Services
HT	<ul style="list-style-type: none">• Antivirus• Content filter• Attachment blocking	<ul style="list-style-type: none">• Antivirus• Content filtering• Attachment blocking	<ul style="list-style-type: none">• [optional] Antispam• [optional] Web Reputation Services• [optional] Threat Management Services
MBX	<ul style="list-style-type: none">• Scheduled scan	<ul style="list-style-type: none">• Antivirus• Scheduled scan	<ul style="list-style-type: none">• [optional] Content filtering• [optional] Attachment blocking• [optional] Threat Management Services

Table 1.0 details the recommended deployment scenarios for ScanMail for Exchange based on the desired outcome when deploying multiple Exchange 2007 roles.

For more information on the content security technologies discussed above, please refer to *Protecting Your Business with ScanMail*. If you are utilizing Exchange 2007 or 2010 high availability clusters, please see Appendix A for further ScanMail deployment discussion.

HIGH-PERFORMANCE SCANNING

Trust Scan

With security installed on the Edge, Hub, and Mailbox servers, duplication of scanning could occur. But ScanMail™ offers the Trust Scan option to eliminate scanning redundancies.

The Trust Scan option allows the ScanMail servers to trust that an email has been scanned for malicious code by the preceding ScanMail server and therefore will not rescan it. To achieve this, ScanMail checks the message's VSstamp. If the VSstamp on the message is older than the VSstamp it currently has, it will perform a rescan. If not, the previous message inspection will be “trusted” and the message passed on as is. (For more information, see the Microsoft TechNet description: <http://technet.microsoft.com/en-us/library/aa996551.aspx>)

Trust Scan increases performance while decreasing message latency. (For more information, see the “What's New” section of the Getting Started Guide: http://www.trendmicro.com/ftp/documentation/guides/SMEXV8.0_b1181_ScanMailGSG.pdf)

Other Performance Optimization

In addition to avoiding duplicative scanning, ScanMail includes many performance optimizations, including a native 64-bit version written specifically for Exchange 2007 and 2010, configurable multi-threaded scanning, configurable CPU throttling, and other features to minimize the impact to your Exchange servers.

Protecting the Microsoft Exchange 2007 and 2010 Environment

EASY ADMINISTRATION

Trend Micro™ recognizes that managing Exchange security such as ScanMail™ is generally not an administrator's only job. Accordingly, ScanMail is designed to require minimal administration. A recent Osterman Survey details a few of the key ScanMail features that result in the lowest administration effort. They include:

Intuitive Manageability and Monitoring

With multiple servers in your environment, it may be necessary to change the configuration of every server. Trend Micro ScanMail provides a number of different ways to perform this, including a built-in server manager. The server manager will enable you to replicate settings from one ScanMail server to all the other servers in the same group. It also allows for the granularity of replicating only specific settings to specific servers.

In addition, you can manage ScanMail through the Trend Micro Control Manager™, a centralized management tool that can be used to administer all Trend Micro products. This allows you to have a clear view of your security infrastructure spanning across the mail security, web security, and desktop security solutions offered by Trend Micro.

Microsoft® Systems Center Operations Manager is also supported by ScanMail 10.x, a feature that allows you to monitor the performance and availability of ScanMail.

For more information, please refer to the "Managing ScanMail Servers" section of the Getting Started Guide located here: www.trendmicro.com/ftp/documentation/guides/SMEXV8.0_b1181_ScanMailGSG.pdf

At the same time, a new Outlook Junkmail folder integration provides the option to send questionable messages to the enduser in order to delegate quarantine management.

Easy Administration

Configuration setting changes and change control may slip through the cracks in large organizations with multiple Exchange servers managed by multiple email administrators. Fortunately, ScanMail 10 provides a role-based access feature that consists of two roles, the administrator role and the operator role. These roles can have specific access control granted to any areas of the console. In conjunction with the role-based access feature, ScanMail 10 also adds an audit logging function that will record any changes to the console or any action—such as releasing a quarantined email—taken within the ScanMail console based on the Active Directory accounts with permission to manage ScanMail.

Reporting

ScanMail provides a rich reporting function that gives customers the ability to report on email volumes, threats, data leaks, content violations, and antispam. Forty pre-configured and regionally tailored reports provide quick visibility into the state of email security. Additionally, by configuring the scheduled report, administrators receive regular, timely updates at pre-determined intervals.

Protecting the Microsoft Exchange 2007 and 2010 Environment

PROTECTING YOUR BUSINESS WITH SCANMAIL™

ScanMail for Microsoft® Exchange protects your business communications using an arsenal of award-winning proprietary threat scanning technologies.

MALWARE AND SPYWARE

ScanMail protects customers from the proliferation of these insidious threats before they get to end users. Through the use of specialized engines designed to search for specific threats, ScanMail is able to not only provide high-performance scanning, but also to ensure security is up-to-date with the most recent pattern files to stop the latest threats.

Over the last few years, malware has become more controllable while there has been an increase in other threats like spyware. Spyware consists of different payloads that attempt to achieve a different goal. Because of this, tackling spyware with its own dedicated spyware engine and pattern definition makes sense. ScanMail is able to scan while the virus (VSAPI) and spyware (SSAPI) engines are being updated, thereby providing customers with continuous scanning and the peace of mind that networks will be protected even during an update. Further, with the proliferation of variants that feature code that has been modified just enough to pass existing signature-based defenses (often through the use of compression), signature-independent, zero-day protection is a key security element provided by Trend Micro™ IntelliTrap technology.

SPAM

As previously mentioned, almost 90% of email on the Internet is spam, and that volume is expected to increase. In recent years, Trend Micro has invested heavily in the war against spam and has been rated the #1 antispam vendor by multiple independent antispam benchmark testing organizations, including most recently by West Coast Labs.

Trend Micro's Antispam solution employs multiple unique technologies:

- **Email Reputation Services** built into ScanMail enable the administrator to manage settings from within the ScanMail console, allowing an organization to refuse connections based on the sender's reputation.
- **Web Reputation Services** built into ScanMail allow for the inspection of any URL embedded in an email, ensuring that the URL does not point to a malicious website or compromised website that contains malicious content.

The combination of Email and Web Reputation Services, along with the leading conventional content security engines provided in ScanMail, protect you from the wide range of advanced threats.

For more information on how the Trend Micro™ Smart Protection Network™ provides up-to-the-minute protection, please visit: <http://us.trendmicro.com/us/trendwatch/core-technologies/smart-protection-network/>

DATA LEAKS

ScanMail 10 has a redesigned policy framework that gives administrators the flexibility to apply policies based on Active Directory (AD) users and/or groups. In addition, ScanMail provides the ability to group multiple AD user accounts and groups with SMTP addresses, thus forming specific security groups that administrators can manage with specific applied policies.

Protecting the Microsoft Exchange 2007 and 2010 Environment

Along with AD integration, ScanMail 10.x adds a range of privacy templates, providing the administrator the ability to apply a regional content filter policy to email. Administrators can also use traditional content filtering through the use of regular expressions that mitigate the risk of sending sensitive content to parties that should not have access to the content.

CONCLUSION

Microsoft® Exchange Server 2010 introduces important improvements to one of the leading email systems and provides organizations with the opportunity to move to more consolidated, efficient, and easy-to-manage architectures. However, with the increased prevalence, sophistication, and insidiousness of email threats, securing these systems is more critical than ever. In particular, deployment of security in front of the Exchange server at the email gateway has helped shut off the huge volume of unwanted and malicious incoming email, while inspection at the mail server plays a crucial role in protecting internal communications, continuing to inspect incoming messages, and securing outgoing email at the earliest point.

Independent research confirms the need for multi-layered protection. According to Osterman Research, malware infections rose from 25% in 2007 to 39% in 2009 despite increased email security (and email gateway security in particular) because cybercriminals have increased their level of sophistication. Now more than ever, mail server security is an essential part of enterprise security and even more important for organizations utilizing the Exchange Edge server role.

Further, employees spend more time working at home and remotely, leading to an increased risk that endpoint security will become outdated or will be circumvented. With the inclusion of contractors, partners, and customers within the network, the risks increase even more since this endpoint security is outside of the organization's control. This boundless network heightens the need for protection of both end-user emails and the intellectual property within those emails, making comprehensive, reliable mail server security essential for the continued flow of business communications.

APPENDIX A: EXCHANGE 2007 CLUSTER OPTIONS

Microsoft® Exchange 2007 provides high availability and fault tolerance by giving customers the following clustering options:

Single Copy Clusters (SCC):

A Single Copy Cluster uses shared storage to allow multiple servers or nodes to administer a single copy of the storage groups. The shared storage subsystem is typically a Storage Area Network (SAN) or Network-Attached Storage (NAS) that holds the database, transaction logs, and the quorum disk.

ScanMail™ 8.0 implementation on an Exchange 2007 SCC is the same as that of the active/passive approach when deploying ScanMail in Exchange 2000/2003 cluster environments. When ScanMail is installed in this cluster environment, it operates on each physical node, adding a cluster resource to all existing or selected Exchange virtual servers. Further, configuration data, active update, and other database files are installed in the shared storage location. ScanMail is designed to make the installation process as intuitive as possible. When installing ScanMail in a cluster environment, you simply install ScanMail on the Exchange virtual servers that you choose. ScanMail will then automatically detect the physical nodes and perform the installation.

Protecting the Microsoft Exchange 2007 and 2010 Environment

During operation, all ScanMail resources are shared across the nodes, which in turn are managed by the resource monitor. The resource monitor is responsible for loading and unloading all the cluster-related applications for ScanMail. In the event that a resource is not functioning correctly, it will failover to the other node in the cluster and utilize the local ScanMail instance.

For more information, please see: <http://technet.microsoft.com/en-us/library/bb125217.aspx>

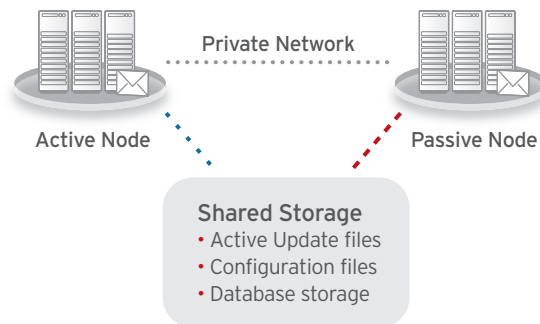


FIGURE 2.0: SCC environment

Cluster Continuous Replication (CCR):

The CCR implementation provides high availability without the need for shared storage. It uses the Majority Node Set (MNS) with file share witness; the quorum is based in the local disks on each node. A file share on the computer outside the cluster is also used to act as the witness to node activity. CCR is designed for site resilience in a one or two datacenter solution.

The ScanMail implementation in a CCR environment involves installation onto the virtual server, while configuration files are copied to the local files on each server.

Like the SCR deployment, the resource monitor is also responsible for monitoring and failover of resources in the CCR deployment. In the case of a failover, the ScanMail instance on the previously active node is awakened by the resource monitor. Database replication helps ensure data is current and that an organization's email security is maintained.

For more information, please see: <http://technet.microsoft.com/en-us/library/bb124521.aspx>

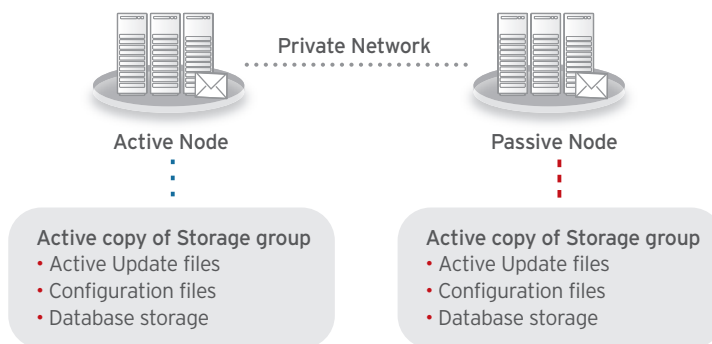


FIGURE 3.0: CCR environment

Protecting the Microsoft Exchange 2007 and 2010 Environment

EXCHANGE 2010 CLUSTER OPTIONS

Exchange 2010 has seen a significant change in clustering. The solution no longer has clustered mailbox servers, nor does it use the Windows Failover Cluster resources. Exchange 2010 is not a clustered application; it now uses its own internal high availability model. Prior to Exchange 2010, Exchange clustering was server-based. Exchange 2010 introduces database clustering which is called Database Availability Groups (DAG) and removes many of the previous cluster deployment limitations and complexities.

The cluster deployment types CCR and SCR introduced in Exchange 2007 are no longer available in Exchange 2010. Using the underlying technology from CCR and SCR, Exchange 2010 has combined the two cluster types to form the Database Availability Group (DAG). The DAG allows for on-site and off-site replication and allows for better site resilience because DAG performs continuous replication at the database level and not the traditional server level.

For more information, please see: [http://technet.microsoft.com/en-us/library/dd979799\(EXCHG.140\).aspx](http://technet.microsoft.com/en-us/library/dd979799(EXCHG.140).aspx)

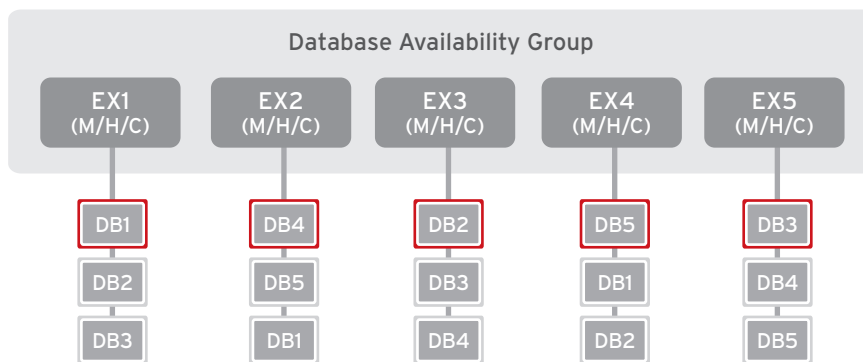


FIGURE 4.0: DAG environment

ScanMail for Exchange installs to each local server and saves its settings at the server level. This allows for ScanMail running on the passive server to still remain up-to-date with the current pattern files and updates required. In the event of a failover, ScanMail services will already be running and able to scan the databases that are housed on the specific server.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1+800-228-5651

phone: 1+408-257-1500

fax: 1+408-257-2003

www.trendmicro.com

