mailsite®
FUSION

Clustering Strategies for MailSite Fusion SP
Version 10

CONTENTS

INTRODUCTION

This paper presents three strategies for deploying MailSite Fusion SP in a clustered environment. The advantages and limitations of each strategy are described, and instructions for configuring MailSite Fusion in each clustered environment are provided.

The specific clustering method and network architecture implemented by a MailSite Fusion SP site are highly dependent on the needs of that site, so these strategies are presented only as a guideline.

Note that in all of the cluster configurations presented in this document, MailSite runs on a stand-alone version of Microsoft Windows Server, not on a clustered version of Microsoft Windows.

In most service provider deployments the front-end MailSite application servers running on the Windows Servers would be running in a virtual machine environment. Virtualization makes it very easy to "clone" MailSite application server nodes and remove broken servers from the cluster for maintenance or replacement. In this document, images of front-end servers can represent virtual machines or physical machines.

Back-end servers hosting the SQL database and message store file system would typically be running on physical servers to benefit from the superior performance.

BASIC CLUSTERING

The simplest MailSite Fusion SP cluster includes a total of three Microsoft
Windows servers:

❑ Two server nodes running the MailSite Engine and Web Services such as
MailSite ExpressPro.

❑ One server running SQL Server and hosting the message store.
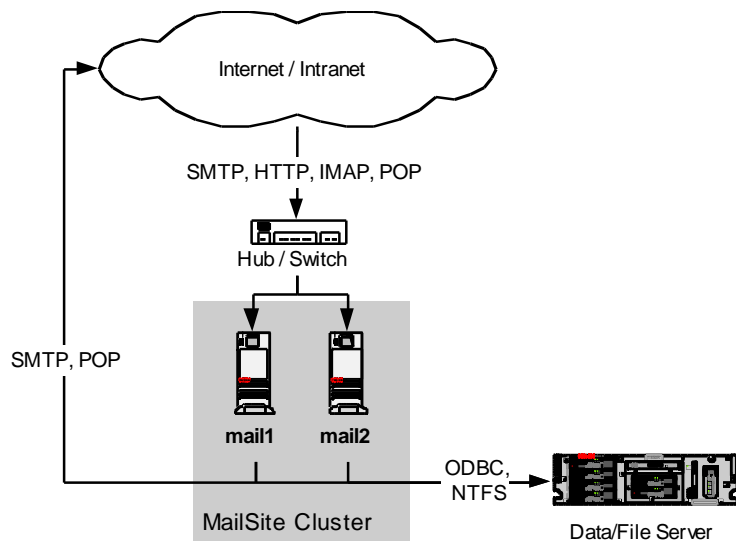
In this configuration email can arrive to
either of the MailSite nodes, which both
deliver messages to the message store on
the data server. Likewise, any POP, IMAP,
Windows SharePoint Service (WSS over
HTTP) or Exchange ActiveSync (EAS over
HTTP) transaction can be received by
either MailSite node, which can access user
mailboxes on the data server.

Email transactions can be balanced
between the two MailSite nodes by using
round-robin DNS. MailSite web transactions
are directed via DNS to one of the MailSite nodes, with the second node
available as a hot backup. Fail-over from one node to another is not automatic,
however; in the event of a system failure DNS must be manually modified to
redirect all requests to the surviving node.

The MailSite nodes access the shared configuration and mailbox database on
the data/file server via ODBC using TCP/IP.

Message Flow

Mail enters the cluster from the Internet or the local network via SMTP to either
MailSite node. Messages are temporarily stored in a spool directory on that node,
and are then relayed to a remote domain via SMTP or delivered to a mailbox
stored on the data/file server.

End users access mail by logging in to one of the two MailSite nodes via IMAP,
POP, ExpressPro, WSS or EAS. MailSite retrieves messages for the user from
the file server through the NTFS file system.

Benefits and Disadvantages

The benefit of this cluster configuration is simplicity and cost: no load balancer or other expensive hardware is required, and no complex setup is needed. Changes made to one MailSite node are applied to both nodes, so changes to security settings or other system parameters need only be done once. Monitoring is simplified because of the small number of servers used.

The disadvantages of this cluster configuration include limited fault-tolerance, limited scalability, and limited performance. MailSite ExpressPro and the MailSite services can all consume significant system resources, so running them on the same server will limit the performance of each application. Likewise, locating the message store and SQL Server database on the same server limits overall system performance.

Installation and Configuration

To configure this type of clustering, execute the following steps (please see the MailSite Administrator's Guide for details on installation and configuration):

1. Install SQL Server on the data server (if not already installed).
2. Create a SQL Server database for MailSite data.
3. Create a SQL Server login for MailSite.
4. Create a new NT domain user for MailSite. (If the servers are not in a Windows domain, create a new local Windows user on the data server.)
5. On the data server file system, create a directory for mailboxes (ex: C:\mailboxes) and a second for mail lists (ex: C:\lists). Grant the MailSite user (created in the previous step) Full Control of these directories and share them for all users. (Note: Because SQL Server databases and the message store are both disk-intensive, store messages and SQL Server files on separate drive volumes if possible.)
6. Install all MailSite components on both MailSite nodes, with MailSite services running as the Windows domain user created in previous steps. (If the servers are not in a Windows domain, install MailSite services as a new local user that has the same login name and password as the user created on the data server.)
7. Install the MailSite Console on the administrative workstation (not shown in the architecture diagram) that you will use to manage MailSite.
8. Change the MailSite Configuration Connector to SQL Connector on each MailSite node. When prompted for a data source, create a new ODBC data source on each MailSite node for the new SQL Server database.

9. Create email domains in MailSite. Set the mailbox root directory for each domain to a UNC path under the shared mailbox directory on the data server (ex: \\data\mailboxes\domain1.com). For each domain, enable the option to use multi-level mailbox directories. Set the mail list directory of each domain to a UNC path under the shared lists directory (ex: \\data\lists\domain1.com).
10. Create mailboxes in MailSite.

Monitoring

Both MailSite nodes should be monitored for CPU and memory usage. High CPU usage may reflect a large amount of incoming mail traffic or a high number of concurrent MailSite ExpressPro users. If CPU usage is high, review the Processes list of the Windows Task Manager to determine if smtpra.exe (incoming SMTP server), dllhost.exe (MailSite ExpressPro), or another process is responsible.

High memory usage may indicate a large number of concurrent users connected via POP, IMAP, WSS and EAS. Use the Windows Performance Monitor to determine the number of concurrent users for these services. If the usage is consistently high, consider adding more mail processing capacity.

The storage usage of the data/file server should be monitored to ensure that disks do not fill to capacity.

Backup

❑ Weekly full backup of the message store file server is recommended, with daily incremental backups.
❑ Daily backup of the messages in the spool directory of both MailSite nodes is recommended. This allows in-process mail to be restored in the event of a system failure.
❑ Weekly archiving of log files stored on each MailSite node is recommended.
❑ An automated daily backup of the SQL Server database in which MailSite Fusion data is stored is recommended. Use the SQL Server Enterprise Manager to configure automatic backups of the database, preferably to a separate file server (or backup tape).

Adding Capacity

To add email processing capacity to this configuration, the administrator can add a third MailSite node to the network. To add a new node to an existing cluster, follow the directions above for installing MailSite and configuring the SQL

Connector. Once the new node has been tested and is operational, update DNS to include the new node in the round-robin scheme.

For additional message store capacity, add disk drives to the file/data server. Use the available Windows Server configuration tools to add the new storage capacity to the existing volume on which mailbox directories are stored. If the file/data server cannot accommodate additional disks, bring a new file server with larger storage capacity online and move the message store for all (or some) MailSite domains to the new server. (Note that the mailbox root directory for each moved domain must be updated in MailSite to reflect the new message store location.)
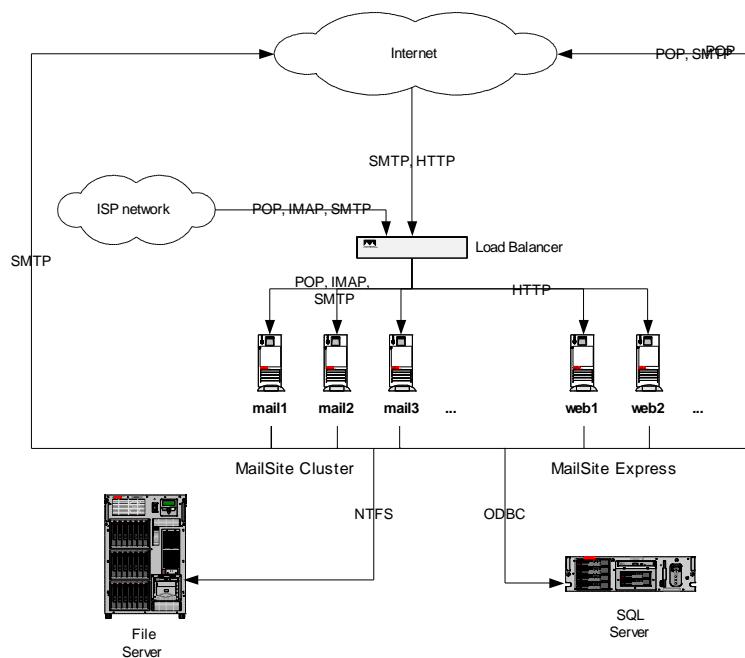
Failure Scenarios

❑ If the hub/switch fails: All mail service is unavailable until a new hub/switch is installed. Service should be restored when the faulty component is replaced.

❑ If a MailSite service (POP, SMTP, IMAP, HTTP) fails: Clients directed by round-robin DNS to the node on which the service failed are not able to use that service. Disable round-robin DNS and direct all client connections to the fully operational MailSite node before troubleshooting the failed service. Once the service is back online, restore round-robin DNS.

❑ If a MailSite node experiences a system failure: Clients directed by round-robin DNS to the failed node are unable to use any mail service. Disable round-robin DNS and direct all client connections to the operational MailSite node. Repair the failed server or bring another online to replace it, installing MailSite and configuring the SQL connector to use the shared database.

❑ If the IIS web server fails on one of the MailSite nodes: Clients directed by DNS to the web server that has failed are unable to use MailSite ExpressPro, EAS or WSS. Reconfigure DNS to direct all web clients to the fully operational MailSite node.

❑ If the data/file server experiences a system failure: All email services are unavailable to end users and the MailSite nodes will not accept incoming mail. Restore the server as quickly as possible, or replace it with a functioning server and restore the message store file system and SQL Server database from backup.

STANDARD CLUSTERING

The standard clustering architecture used for MailSite Fusion SP includes
several types of Microsoft Windows servers:

❑ Two (or more) nodes running MailSite services
❑ Two (or more) nodes running IIS and MailSite's Web Services
❑ One database server running SQL Server
❑ One file server hosting the message store
❑ One load balancing switch

In this configuration email can arrive to any of the MailSite nodes, which all
deliver messages to the message store on the file server. Likewise, any POP or
IMAP transaction can be received by any MailSite node. Web service
connections for ExpressPro, EAS or WSS can be made to any of the Web Services nodes. Fail-over from one node to another is automatic: in the event of a system failure, the load balancer removes the failed server from the group of nodes that receive email or web traffic.

Message Flow

Mail enters the system from the Internet or the ISP's local dial-up network via SMTP to any of the MailSite cluster nodes. Messages are temporarily stored in a spool directory on that node, and are then relayed to a remote domain via SMTP or delivered to a mailbox stored on the file server.

End users access mail by logging in to any of the MailSite cluster nodes via
IMAP or POP, EAS, WSS or by logging into MailSite ExpressPro on any of the
web server nodes. MailSite services running on the mail servers, and MailSite
Web Services running on the web servers, retrieve messages for the user from
the file server through NTFS.

Benefits and Disadvantages

The benefits of this configuration include greater fault-tolerance and increased performance and scalability over the Basic configuration. Administration of MailSite nodes remains relatively simple; all nodes share the same configuration data, so a change on one mail system affects all nodes. The use of a load-balancer provides automatic fail-over in the event of a system outage; client connections are routed away from servers that have failed or are under load to other MailSite nodes.

The disadvantages of this configuration include incomplete fault tolerance because the SQL server and the file server are both potential single points-of-failure. Furthermore, because all MailSite cluster nodes perform all functions, performance issues affecting one service—such as high IMAP usage causing high memory usage—can affect all other services. The increased number of nodes adds to the cost and complexity of deployment.

Installation and Configuration

To configure this type of clustering, execute the following steps (please see the MailSite Administrator's Guide for details on installation and configuration):

1. Install SQL Server on the data server (if it is not already installed).
2. Create a SQL Server database for MailSite data, with the database's transaction log and data file stored on separate drive volumes.
3. Create a SQL Server login for MailSite.
4. Create a new NT domain user for MailSite. (If the servers are not in a Windows domain, create a new local Windows user on each system using the same login name and password.)
5. On the file server, create a directory for mailboxes (ex: C:\mailboxes), a second for mail lists (ex: C:\lists). Grant the MailSite user (created in the previous step) Full Control of these directories and share them for all users.
6. Install the MailSite Engine on all of the MailSite nodes. When prompted, select the Secure method of installation and enter the name and password of the Windows user created in previous steps (the MailSite services will run as this user).
7. Install the MailSite Console the administrative workstation (not shown in the architecture diagram) that you will use to manage MailSite.
8. Set the spool location of each MailSite node to a local path (ex: C:\spool).
9. Change the MailSite Configuration Connector to SQL Connector on each MailSite node. When prompted for a data source, create a new ODBC data source on each MailSite node for the SQL Server database.

10. Create email domains in MailSite. Set the mailbox root directory for each domain to a UNC path under the shared mailbox directory on the data server (ex: \\data\mailboxes\domain1.com). Configure each domain to use multi-level mailbox directories. Set the mail list directory of each domain to a UNC path under the shared lists directory (ex: \\data\lists\domain1.com).
11. Create mailboxes in MailSite.
12. Install the MailSite Engine, MailSite ExpressPro, EAS and WSS on the web servers. After installation, use the Internet Services Manager to set the anonymous user for each of the MailSite Web Service applications to the new Windows user created in previous steps.

Monitoring

All MailSite nodes and web servers should be monitored for CPU usage. High CPU usage on a MailSite node may reflect a large amount of incoming mail traffic, while high CPU usage on a web server may indicate a high number of concurrent users on any one of the MailSite Web Services. If CPU usage is consistently high, review the Processes list of the Windows Task Manager to determine the process responsible.

High memory usage on MailSite nodes may indicate a large number of concurrent users connected via POP or IMAP. Use the Windows Performance Monitor to determine the number of concurrent users for these services. If the usage is consistently high, consider adding more mail processing capacity.

The storage usage of the file server should be monitored to ensure that disks do not fill to capacity.

Backup

❑ Weekly full backup of the message store file system is recommended, with daily incremental backups.
❑ Weekly archiving of log files generated by on each MailSite node is recommended.
❑ Daily backups of the spool directories on each MailSite node is recommended.
❑ An automated daily backup of the SQL Server database in which MailSite data is stored is recommended. Use the SQL Server Enterprise Manager to configure automatic backups of the database, preferably to a separate file server (or backup tape).

Adding Capacity

To add email processing capacity, deploy an additional MailSite node on the network. To add a new node to an existing cluster, follow the directions above for installing MailSite and configuring the SQL Connector. Once the new node has been tested and is operational, update the load-balancer to include the new node in its distribution of email client connections.

To accommodate a larger number of concurrent webmail users, deploy an additional web server and follow the above instructions for installing MailSite ExpressPro. After MailSite ExpressPro has been deployed and tested, update the load-balancer to include the new node in its distribution of web client connections. The same is true for Outlook connectivity through the EAS and WSS services.

For additional message store capacity, add disk drives to the file server. Use the available Windows Server configuration tools to add the new storage capacity to the existing volume on which mailbox directories are stored. If the file server cannot accommodate additional disks, bring a new file server with larger storage capacity online and move the message store for all (or some) MailSite domains to the new server. (Note that the mailbox root directory for each moved domain must be updated in MailSite to reflect the new message store location.)

Failure Scenarios

❑ If the load-balancer fails: All mail service is unavailable until a new load-balancer is installed. Service should be restored when the faulty component is replaced.

❑ If a MailSite service (POP, SMTP, IMAP) fails: Client connections for that service will be routed by the load-balancer to a MailSite node on which that service is still running. Users who had been connected to the service at the time of failure may be required to reinitialize their connection, but end users will otherwise not be affected by the failure. When the failed MailSite service has been restored, the load-balancer will automatically include it in its distribution of client connections.

❑ If a MailSite node experiences a system failure: The load-balancer will direct all client connections to the remaining nodes. Users who had been connected to the node at the time of failure may be required to reinitialize their connection, but end users will otherwise not be affected by the failure. Repair the failed system or bring another online to replace it, installing MailSite and configuring the SQL connector to use the shared database.

When the failed MailSite node has been restored, the load-balancer will automatically include it in its distribution of client connections.

❑ If a web server experience a hardware or software failure: The load balancer automatically directs client connections to the surviving web servers. Users who had been connected to one of the MailSite Web Services on the failed system may be required to reinitialize their client session. When the failed web server has been restored, the load-balancer will automatically include it in its distribution of client connections.

❑ If the file server experiences a system failure: Users are unable to access messages in their mailboxes, and MailSite is unable to process incoming or outgoing mail. Restore the system as quickly as possible, or replace it with a functioning system and restore the message store file system from backup.

❑ If the database server experiences a system failure: All email services are unavailable to end users and the MailSite nodes will not accept incoming mail. Restore the system as quickly as possible, or replace it with a functioning node and restore the SQL Server database from backup.

ADVANCED CLUSTERING

The advanced clustering architecture for MailSite Fusion SP includes several types of Microsoft Windows servers, each dedicated to a specific task using different Cluster Roles:

- ❑ Two (or more) nodes running SMTP services for incoming mail (mx1,mx2…).
- ❑ Two nodes running MailSite SMTP services for outgoing mail (mta1, mta2…).
- ❑ Two (or more) nodes running MailSite SMTP, POP and IMAP services for end users (mail1, mail2…). (These tasks can be optionally split among three different groups for maximum distribution of tasks.)
- ❑ Two (or more) nodes running IIS, the MailSite Engine and MailSite EAS AirSync, ExpressPro and WSS (web1, web2…).
- ❑ Two database servers running SQL Server Cluster.
- ❑ One file server hosting the message store.
- ❑ Two load balancing switches.
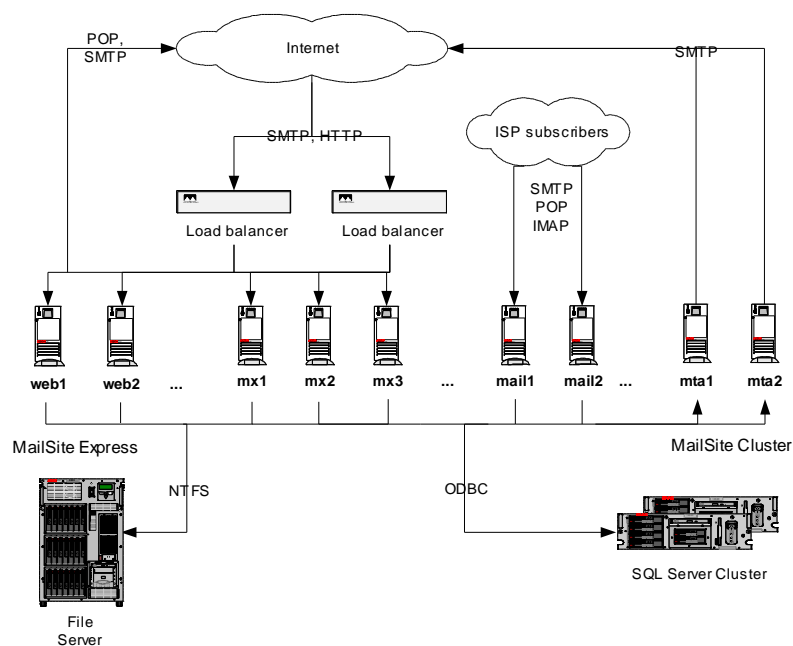
In this configuration the load balancers distribute incoming messages among the dedicated SMTP servers (mx1…), which each deliver mail to the message store on the file server. Routing rules forward all email destined for remote sites through the MailSite outgoing SMTP servers (mta1…). End user SMTP, POP and IMAP connections are distributed by the load balancers between the dedicated end user access nodes (mail1…). Webmail connections can be made to any of the MailSite Web nodes (web1…). Fail-over from one node to another is automatic: in the event of a system failure, the load balancer removes the failed server from the group of systems that receive email traffic.

Message Flow

Mail enters the system from the Internet to any of the MailSite incoming SMTP nodes (mx1…). Messages are temporarily stored by MailSite in a spool directory on the SMTP node, and are then delivered to the destination mailboxes in the message store (located on the file server). If the incoming SMTP node generates an automatic reply or bounce message, those messages are routed via SMTP to one of the outgoing SMTP servers (mta1…).

Mail sent by end users on the local ISP network is received by the MailSite nodes that provide end user access to mail services (mail1…). This mail is stored temporarily in a spool directory. If a message is destined for a user in a local domain, it is delivered to the recipient's mailbox on the file server. If the mail is destined for remote domains, it is routed via SMTP to the outgoing SMTP servers (mta1…).

The outgoing SMTP servers (mta1…) receive mail via SMTP from the incoming SMTP servers and end user access systems. Mail is temporarily stored in a spool directory on the local system and is relayed to remote domains via SMTP.

End users access mail by logging in to any of the end user access nodes (mail1…) via IMAP or POP, or by logging into MailSite ExpressPro, EAS or WSS on any of the web servers (web1…). MailSite services running on the mail servers, and MailSite Web Services running on the web servers, retrieve messages for the user from the file server through NTFS.

Benefits and Disadvantages

The benefits of this configuration include maximum performance, scalability and fault-tolerance. By separating tasks, the administrator is better able to locate and troubleshoot problems when they occur, and prevents high resource usage by one service from affecting others. The use of a redundant load balancer and clustered SQL Server eliminates all-but-one single-point-of-failure.

The disadvantages include one remaining single-point-of-failure – the file server, the high cost of a large number of servers and the complexity of deployment.

Installation and Configuration

To configure this type of clustering, execute the following steps (please see the MailSite Administrator's Guide for details on installation and configuration):

1. Install SQL Server on the data server (if it is not already installed) and configure SQL Server clustering.
2. Create a SQL Server database for MailSite data, with the database's transaction log and data file stored on separate drive volumes.
3. Create a SQL Server login for MailSite.
4. Create a new NT domain user for MailSite. (If the servers are not in a Windows domain, create a new local Windows user on each system using the same login name and password.)
5. On the file server, create a directory for mailboxes (ex: C:\mailboxes), and a second for mail lists (ex: C:\lists). Grant the MailSite user (created in the previous step) Full Control of these directories and share them for all users.
6. Install the MailSite Engine on all of the MailSite nodes (mail1…), with services running as the new Windows user created in previous steps.
7. Install the MailSite Console the administrative workstation (not shown in the architecture diagram) that you will use to manage MailSite.
8. Set the spool location of each MailSite node to a local directory (ex: C:\spool).
9. On the MailSite nodes that run POP, IMAP, and incoming SMTP, change the MailSite Configuration Connector to SQL Connector. When prompted for a data source, create a new ODBC data source on each MailSite node for the SQL Server database.
10. Create email domains in MailSite. Set the mailbox root directory for each domain to a UNC path under the shared mailbox directory on the data server (ex: \\data\mailboxes\domain1.com). Configure each domain to use multi-level mailbox directories. Set the mail list directory of each domain to a UNC path under the shared lists directory (ex: \\data\lists\domain1.com).
11. Create mailboxes in MailSite.
12. Install the MailSite Engine, MailSite ExpressPro, MailSite AirSync EAS, and MailSite WSS on the web servers (web1…). After installation, use the Internet Services Manager to set the anonymous user for each of the MailSite Web Service applications to the new Windows user created in previous steps.
13. Using the SQL Connector Wizard, add an "Outbound SMTP" Role in the cluster for the outgoing SMTP nodes and an "Inbound SMTP" Role for the incoming SMTP nodes.

14. On the outgoing SMTP nodes (mta1…), enroll them into the Outbound SMTP role. You may wish to restrict SMTP relay to the IP addresses of other MailSite nodes in the cluster by adding their IP addresses to the list of friendly SMTP hosts using the Security Wizard.

15. On the incoming SMTP nodes (mx1…), use the SMTP Security Wizard to set the relay, denial-of-service, anti-spam and anti-virus settings. SMTP security settings for these nodes should be tight because these nodes will be exposed to all incoming messages and abuse from the Internet.

Monitoring

Because MailSite nodes in this configuration are dedicated to specific tasks, monitoring resource usage by service is greatly simplified. Incoming SMTP nodes should be monitored for CPU and memory usage to track the level of incoming mail (including spam and possible denial-of-service attacks). End user access servers should be monitored for the level of POP and IMAP traffic. Web servers should be monitored for CPU and memory usage to measure the level of MailSite Web Service traffic. If resource usage is high for any group of servers, consider adding more servers to that group.

The storage usage of the file server should be monitored to ensure that disks do not fill to capacity.

Backup

❑ Weekly full backup of the message store file server is recommended, with daily incremental backups.

❑ Weekly archiving of log files generated by on each MailSite node is recommended.

❑ Daily backups of the spool directories on each of the MailSite nodes is recommended.

❑ An automated daily backup of the SQL Server database in which MailSite data is stored is recommended. Use the SQL Server Enterprise Manager to configure automatic backups of the database, preferably to a separate file server (or backup tape).

Adding Capacity

To add email processing capacity, deploy additional MailSite servers on the network. To add a new node to an existing cluster, follow the directions above for installing MailSite and configuring the SQL Connector. Once the new node has

been tested and is operational, update the load-balancer to include the new node in its distribution of email client connections.

To support a larger amount of outgoing SMTP traffic, add another dedicated outgoing SMTP node to the network. Update the load-balancers to include this new server in the list of nodes to which other MailSite nodes relay outgoing messages.

To accommodate a larger number of concurrent webmail users, deploy an additional web server and follow the above instructions for installing MailSite ExpressPro as required. After MailSite ExpressPro has been deployed and tested, update the load-balancer to include the new node in its distribution of web client connections.

For additional message store capacity, add disk drives to the file server. Use the available Windows Server configuration tools to add the new storage capacity to the existing volume on which mailbox directories are stored. If the file server cannot accommodate additional disks, bring a new file server with larger storage capacity online and move the message store for all (or some) MailSite domains to the new server. (Note that the mailbox root directory for each moved domain must be updated in MailSite to reflect the new message store location.)

Failure Scenarios

❑ If a load-balancer fails: All network transactions are automatically handled by the surviving load-balancer.
❑ If a MailSite service (POP, SMTP, IMAP) fails: Client connections for that service will be routed by the load-balancer to a MailSite node on which that service is still running. Users who had been connected to the service at the time of failure may be required to reinitialize their connection, but end users will otherwise not be affected by the failure. When the failed MailSite service has been restored, the load-balancer will automatically include it in its distribution of client connections.
❑ If an incoming SMTP MailSite node experiences a system failure: The load-balancer will direct all incoming mail to the remaining incoming SMTP nodes. Messages that were in transit at the time of failure will be spooled by the sending MTA and will be retransmitted. No end user connections are affected. Repair the failed system or bring another online to replace it, installing MailSite and configuring the SQL connector to use the shared database. As some messages may be in the spool on the affected system it

is important to attempt to repair the system. When the failed MailSite node has been restored, the load-balancer will automatically include it in its distribution of incoming SMTP connections.

❑ If an outgoing SMTP MailSite node experiences a system failure: The load-balancer will direct all outgoing mail to the remaining outgoing SMTP nodes. Messages that were in transit at the time of failure will be spooled by the sending MailSite node. No end user connections are affected. Repair the failed system or bring another online to replace it, installing MailSite and using the MSBACK utility to import the configuration profile of the failed system. As some messages may be in the spool on the failed system it is important to attempt to repair the system. When the failed MailSite node has been restored, the load-balancer will automatically include it in its distribution of outgoing mail.

❑ If a MailSite end user access node experiences a system failure: The load-balancer will direct all client connections to the remaining nodes. Users who had been connected to the node at the time of failure may be required to reinitialize their connection, but otherwise end users will not be affected by the failure. No incoming or outgoing mail is lost. Repair the failed server or bring another online to replace it, installing MailSite and configuring the SQL connector to use the shared database. When the failed MailSite node has been restored, the load-balancer will automatically include it in its distribution of client connections.

❑ If a web server experiences a hardware or software failure: The load balancer automatically directs client connections to the surviving web servers. Users who had been connected to a web service such as MailSite ExpressPro on the failed server may be required to reinitialize their client session. When the failed web server has been restored, the load-balancer will automatically include it in its distribution of client connections.

❑ If the file server experiences a system failure: Users are unable to access messages in their mailboxes, and MailSite is unable to process incoming or outgoing mail. Restore the server as quickly as possible, or replace it with a functioning server and restore the message store file system from backup.

❑ If a database server experiences a system failure: Use the SQL Server administrative tools to fail over database functionality from the failed server to the passive backup. Restore the failed server and reestablish the cluster as soon as possible.

USING ETRN WITH MAILSITE FUSION SP

It is not possible to support an ETRN service with clustered MailSite Fusion SP deployments.

All MailSite Fusion licenses support "store and forward" message spool services using the ETRN protocol. ETRN (Extended Turn) is an extension to the SMTP protocol that allows an SMTP server to send a request to another SMTP server to forward any e-mail messages for particular domains.

It is not possible, however, to support an ETRN service using clustered MailSite Fusion SP deployments. MailSite Fusion SP is designed for large scale mailbox hosting, not a store and forward service. Each MailSite Fusion SP server maintains its own mail spool in order to meet this requirement.

ETRN services can be provided using dedicated ETRN SMTP spool servers outside of the cluster, for which a separate MailSite Fusion license is required.

ADDITIONAL ASSISTANCE

MailSite Software Incorporated offers onsite training and professional services for MailSite Fusion customers. If you require additional assistance deploying MailSite Fusion SP in a clustered architecture on your network, please contact your MailSite Software, Inc. sales representative to inquire about a professional services engagement.

To provide feedback on this White Paper please send an email to feedback@mailsite.com or visit our website and open a Technical Support Case http://www.mailsite.com