


Microsoft
Windows Server 2003

Advanced Mail Server Configurations

Microsoft Corporation

Published: March 2003

Abstract

This white paper describes advanced configuration options for Windows Server 2003 family operating systems that are configured as mail servers. These options include configuring multiple mail servers to use a single mail store or a remote mail store, configuring e-mail aliasing, and changing the greeting message.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, Windows, and the Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	1
Scenario 1: Configuring Multiple Mail Servers to Use a Single Mail Store or a Remote Mail Store	2
To configure multiple mail servers to use a single mail store or remote mail store:	2
To change the GUID	3
To set mail store security and permissions:	4
Scenario 2: Configuring E-Mail Aliasing	7
To create an e-mail alias:	7
Scenario 3: Changing the Greeting Message	9
To change the greeting message:.....	9
Related Links	10

Introduction

On a Windows Server 2003 mail server, you can configure a number of advanced options. These options include configuring multiple mail servers to use a single mail store or a remote mail store, configuring e-mail aliasing, and customizing the greeting message.

This white paper provides instructions on how to configure each of these advanced options. We recommend that you review the E-mail Services Help before reading this white paper. To access E-mail Services Help, click **Start**, click **Help and Support**, click **Internet and E-mail Services**, and then click **E-mail services**.

Scenario 1: Configuring Multiple Mail Servers to Use a Single Mail Store or a Remote Mail Store

In a standard mail server configuration, each mail server has a corresponding local mail store. However, you can configure multiple mail servers to use a single mail store or a remote mail store. The advantage of using multiple mail servers is that doing so adds redundancy to your deployment and allows your network to handle more traffic. The advantage of using a remote mail store is that you can then use a dedicated file-storage device, such as a network-attached storage (NAS) device.

Important:

To perform the following procedure, you must be using either Active Directory integrated authentication or encrypted password file authentication.

The mail servers must be in the same Active Directory domain as the computer on which the mail store is configured.

To configure multiple mail servers to use a single mail store or remote mail store:

1. Follow the instructions in Windows Server 2003 Help for installing E-mail Services on each computer that you want to use as a mail server. These instructions are provided in the Help topic "To install e-mail services."

To view this topic, click **Start**, and then click **Help and Support**.

Click **Internet and E-mail Services**, click **E-mail services**, and then click **POP3 service**.

Click **How To**, click **Set Up the POP3 Service**, and then click **Install e-mail services**.

2. On each mail server, select either Active Directory integrated authentication or encrypted password file authentication. Instructions for this procedure are provided in the Help topic "Set the authentication method."

To view this topic, click **Start**, and then click **Help and Support**.

Click **Internet and E-mail Services**, click **E-mail services**, and then click **POP3 service**.

Click **How To**, click **Set Up the POP3 Service**, and then click **Set the authentication method**.

3. Make any additional changes to the configuration of the individual mail servers, such as setting the logging level or port, or configuring secure password authentication (SPA).
4. Follow the instructions in Windows Server 2003 Help for configuring a directory or drive as a shared folder to be used as the mail store. These instructions are provided in the Help topic "Share a folder or drive." To view this topic, click **Start**, and then click **Help and Support**.

Click **Disks and Data**, click **Managing Files and Folders**, click **Shared Folders**, click **How To**, and then click **Share a folder or drive**.

5. Depending on whether you are using encrypted password file authentication or Active Directory integrated authentication, do one of the following:

If you are using encrypted password file authentication, you must use the same globally unique identifier (GUID) on each mail server. To do so, select one mail server, identify its GUID, and then configure all other mail servers to use that same GUID. The GUID is located at: HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\pop3 service\auth\authguid. The GUID is displayed in the **Data** column. Or, if you double-click the **authguid** key, the GUID is displayed in **Value data**.

To change the GUID

1. Click **Start**, click **Run**, and then type:

regedit

2. Go to HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\pop3 service\auth\authguid.
3. Double-click the **authguid** key, and then, in **Value data**, type the GUID.
4. After modifying the registry, you must restart the POP3 service. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
5. At the command prompt, type:

net stop pop3svc

6. After the service has stopped, at the command prompt, type:

net start pop3svc

If you are using Active Directory integrated authentication, you must wait for Active Directory replication to occur so that all mail servers can access the new mail store. The replication time varies, depending upon the number of domain controllers in your deployment. For more information about Active Directory replication, see the Windows Server 2003 Help topic "Replication overview."

To view this topic, click **Start**, and then click **Help and Support**. Click **Active Directory**, click **Concepts**, click **Understanding Active Directory**, click **Understanding Sites and Replication**, and then click **Replication overview**.

6. Follow the instructions in Windows Server 2003 Help for setting the mail store to configure each mail server in your deployment to use the new mail store you created. If you created a remote shared folder as the mail root, the path will be in the form: [\path\share](#).

To view the Help topic for this procedure, click **Start**, and then click **Help and Support**. Click **Internet and E-mail Services**, click **E-mail services**, click **POP3 service**, click **How To**, click **Set Up the POP3 Service**, and then click **Set the mail store**.

7. After setting the mail store, you must restart the POP3 service. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
8. At the command prompt, type:

net stop pop3svc

9. After the service stops, at the command prompt, type:

net start pop3svc

To set mail store security and permissions:

1. On the computer on which the mail store is configured, open Windows Explorer.
2. Right-click the shared folder or drive that you want to use as the mail store, and then click **Sharing and Security**. Verify that **Share this folder** is selected.
3. On the **Sharing** tab, click **Permissions**, click **Everyone**, and then click **Remove**.
4. Click **Add**, click **Object Types**, select **Computers**, and then click **OK**.
5. In **Select Users, Computers, or Groups**, type: **Domain Admins; Network Service; System;** and the names of all mail servers in your deployment, each separated with a semi-colon (;), and then click **OK**.
6. Click **Domain Admins**, and then click **Full Control**.
7. Repeat the previous step for **Network Service, System** and each mail server account, and then click **OK**.
8. On the **Security** tab, repeat steps 4-7.
9. On the **Security** tab, click **Advanced**.
10. Verify that the option **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here** is selected.
11. Select **Replace permission entries on all child objects with entries shown here that apply to child objects**, click **OK**, click **Yes** when prompted, and then click **OK**.
12. Create e-mail domains and mailboxes.

To view the Help topic for these procedures, click **Start**, and then click **Help and Support**. Click **Internet and E-mail Services**, click **E-mail services**, click **POP3 service**, click **How To**, and do one of the following:

- To view the Help topic for creating e-mail domains, click **Manage Domains**, and then click **Create a domain**.
- To view the Help topic for creating mailboxes, click **Manage Mailboxes**, and then click **Create a mailbox**.

Caution:

Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

Important:

If you change any of the POP3 service server properties, such as the port or the logging level, from any of the mail servers in your deployment, the discretionary access control lists (DACLS) on the mail store will be set to the default values. You must reset the DACLS on the mail store as described earlier, in the procedure "To set mail store security and permissions."

Notes:

- If you have more than one mail server in your deployment, you must repeat the appropriate procedure to create an e-mail domain on each mail server in your deployment that requires access to that e-mail domain. If you are deleting an e-mail domain, you must repeat the appropriate procedure on each computer in your deployment.

For more information about creating or deleting domains, see the corresponding Help topics in “Manage Domains.” To view the Help, click **Start**, and then click **Help and Support**.

Click **Internet and E-mail Services**, click **E-mail services**, click **POP3 service**, click **How To**, and then click **Manage Domains**.

- You must wait for Active Directory replication to occur before POP3 service user accounts are available in Active Directory. Although you can create mailboxes from any of the servers, replication must occur among domain controllers before mailbox size quotas can function or POP3 service user accounts can log on to the Active Directory domain.
- When you enable quotas, there is a default limit set on the Network Service and System accounts. Depending upon how you have configured disk quotas, you can set a quota limit so that the Network Service and System accounts are close to or beyond their quota limits. If there are mailboxes that do not have a user account and quota limit associated with them, the e-mail files in those mailboxes are considered as part of either the Network Service account or the System account. If the Network Service or System accounts are close to or beyond their quota limits, e-mail for those mailboxes will not be delivered.

Therefore, you must review the quota limits on the Network Service and System accounts and adjust them accordingly. If all mailboxes in your deployment have a quota limit associated with them, however, it is not necessary to set a quota limit on the System or Network Service accounts.

- Quotas are enforced only on the computer that is configured with the mail store. If you have set quota limits on other mail servers in the Active Directory domain, you must create them again on the mail store.
- If you are using encrypted password file authentication, quotas will be enforced against the computer accounts that write to the mail store. This continues until you configure a quota for each mailbox account. For more information about creating quotas for e-mail accounts, see the Windows Server 2003 Help topic “Configuring disk quotas for the POP3 service.”

To view this topic, click **Start**, and then click **Help and Support**. Click **Internet and E-mail Services**, click **E-mail services**, click **POP3 service**, click **Concepts**, click **Using the POP3 service**, and then click **Configuring disk quotas for the POP3 service**.

- You cannot modify a quota until the associated account has first written to the mail store.
- When you create a new e-mail domain, the first mail server on which you perform this procedure adds the new e-mail domain to the local Simple Mail Transfer Protocol (SMTP) server and creates the mail-store directory for the e-mail domain. You must repeat this process to give other mail servers in your deployment access to the new e-mail domain. However, only the SMTP domain will be added to the server on which you are performing the procedure. This is because the mail-store directory for the e-mail domain already exists.

- When you delete an e-mail domain, the first mail server on which you perform this operation removes its local SMTP domain and the mail-store directory for the e-mail domain. You must remove the SMTP domain entry from all of the other mail servers in your deployment. To do so, repeat this process by performing the delete operation at the command line of each mail server in your deployment. To perform this operation, at a command prompt, type:
winpop delete domain
 - Some options must be configured on each mail server in your deployment. These options include the following: setting the mail store, setting the logging level, setting Secure Password Authentication (SPA), and setting the authentication method. Other operations, such as creating or deleting mailboxes, can be performed on any mail server in your deployment because these operations affect the entire e-mail domain.
 - For more information about setting permissions on a shared resource, see the Windows Server 2003 Help topic “Set permissions on a shared resource.” To view this topic, click **Start**, and then click **Help and Support**. Click **Disks and Data**, click **Managing Files and Folders**, click **Shared Folders**, click **How To**, and then click **Set permissions on a shared resource**.
 - For more information about setting permissions on a folder, see the Windows Server 2003 Help topic “To set, view, change, or remove permissions on files and folders.” To view this topic, click **Start**, and then click **Help and Support**. Click **Security**, click **Access Control**, click **How To**, click **Set, View, Change, or Remove Permissions on an Object**, and then click **Set, view, change, or remove permissions on files and folders**.
-

Scenario 2: Configuring E-Mail Aliasing

You can use aliasing to configure an e-mail address so that all e-mail sent to it is routed to another e-mail address. For example, all e-mail sent to `postmaster@example.com` could be routed to the e-mail address `someone@example.com`.

With aliasing, you can maintain separate e-mail addresses for public and private use, obscure network user accounts, route e-mail across multiple e-mail domains, and create simple and consistent e-mail addresses for interacting with customers. This reduces the public exposure of internal e-mail addresses. Reducing this exposure can be a security benefit.

Aliasing works by creating a hard link between the alias e-mail account mailbox folder and one or more other e-mail account mailbox folders. A hard link creates a new and different name for an existing file or directory path. It does not create a copy of the file or directory or change the contents of the file or directory. To create an alias, you create a hard link between the alias e-mail account and the e-mail account to which you want the e-mail to be routed, which is known as the target e-mail account. Creating a hard link changes the alias e-mail account's mail-store directory to the path of the target e-mail account's mail-store directory. As a result, any e-mail sent to the alias e-mail account is routed to the target e-mail account.

To implement aliasing, you must use the `linkd.exe` tool, which is available in the *Windows 2000 Resource Kit* and the *Windows Server 2003 Resource Kit*.

After you download this tool, you must create a new directory in the mail store for the alias account. You use the `linkd.exe` tool to create a hard link between the mail-store directory of the alias account and the target account.

There is no user account associated with the e-mail alias. If you are using Active Directory integrated authentication or local Windows accounts authentication, you cannot retrieve e-mail using the alias credentials. If you are using encrypted password file authentication, however, you can retrieve e-mail using either the alias e-mail account name or the target account name. This is because the password is the same for both mailboxes.

To create an e-mail alias:

1. Click **Start**, click **Run**, and then type:

cmd

2. At the command prompt, type:

mkdir mailroot\domain\p3_aliasAccount.mbx

3. Go to the directory in which `linkd.exe` is stored.

4. At the command prompt, type:

linkd mailroot\domain\p3_aliasAccount.mbx mailroot\domain\p3_targetAccount.mbx

Important:

The directory name that you create for the alias account must not conflict with any existing directory names. It must also follow the naming guidelines for mailboxes specified in the following table.

Authentication method	Prohibited characters
Active Directory integrated authentication	@ () / \ [] : ; , " < > * = ? +
Local Windows accounts authentication	@ () / \ [] : ; , " < > * = ? +
Encrypted password file authentication	@ () / \ [] : ; , " < > * = ?

Notes

- E-mail that is sent to both the alias account name and the target account name produces multiple copies of the same e-mail in the target account mailbox.
 - Performing administrative operations (such as locking or deleting a mailbox) on the alias mailbox or the domain in which the alias exists also affects the target mailbox. For example, if you lock the alias mailbox, the target mailbox will also be locked.
 - If you want to delete either a domain that contains a mailbox to which an alias points, or a mailbox to which an alias points, you must first delete the alias mailbox.
-

Scenario 3: Changing the Greeting Message

When the POP3 service accepts an incoming connection, it responds by sending the following message: "Microsoft Windows POP3 Service Version 1.0." This message identifies the server configuration and provides information that can potentially be used by attackers. You can customize this message to obscure the transmission of any information about the server configuration. The greeting message has a 259-character limit. Simply obscuring the transmission of information, however, is not an effective security measure. It must be augmented with additional security practices, such as those described in the POP3 service Help topic "Best practices." To view this Help topic, click **Start**, and then click **Help and Support**. Click **Internet and E-mail Services**, click **E-mail services**, click **POP3 service**, and then click **Best practices**.

To customize the POP3 greeting message, you must create a new REG_SZ string key in the Windows Server 2003 registry. You can then assign a custom string value to the key that will be used as the greeting message.

To change the greeting message:

1. Click **Start**, click **Run**, and then type:
regedit
2. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Pop3 Service
3. Click the **Edit** menu, click **New**, and then click **String Value**.
4. To name the new string value, in the name column, type **Greeting**.
5. In the details pane, right-click **Greeting**, and then click **Modify**.
6. In **Value Data**, type the new greeting message, and then click **OK**.
7. You must stop and then restart the POP3 service for the new greeting message to take effect.

Caution:

Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

Note:

The default message will be used if the custom greeting message is longer than 259 characters or if it contains any invalid characters. Invalid characters include all non-printable ASCII characters and angle brackets (< and >).

Related Links

For more information about E-mail Services, see the Windows Server 2003 Help at the [Microsoft Web site](#).

For the latest information about Windows Server 2003, see the [Microsoft Web site](#).