BrightStor® ARCserve® Backup for Windows

Agent for Microsoft Exchange Guide

r11.5

Contents

Chapter 4: Performing Document Level Backups and Restores 73

Chapter 5: Performing Brick Level Backups and Restores 109

Chapter 1: Introducing the Agent

BrightStor® ARCserve® Backup is a comprehensive, distributed storage solution for applications, databases, distributed servers, and file systems. It provides backup and restore capabilities for databases, business-critical applications, and network clients.

Among the backup agents BrightStor ARCserve Backup offers is the BrightStor® ARCserve® Backup Agent for Microsoft Exchange (the agent) and the optional BrightStor® ARCserve® Backup Agent for Microsoft Exchange-Premium Add-on (the add-on).

- **BrightStor ARCserve Backup Agent for Microsoft Exchange**—Works with BrightStor ARCserve Backup to back up and restore Microsoft Exchange Server (Exchange Server) databases, allowing you to ensure your messaging solution is reliable and secure. It includes the following types of backup and restore:

  – Database Level backup and restore

  – Brick Level backup and restore

- **BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on**—Installed as an optional add-on component to the BrightStor ARCserve Backup Agent for Microsoft Exchange. It also lets you protect Exchange Server, but is a more robust solution that maximizes performance and power. It includes the following types of backup and restore:

  – Database Level backup and restore

  – Document Level backup and restore

The following sections include more information about Exchange Server, the agent, the add-on, and the backup and restore types included with each.

Microsoft Exchange Server Description

Microsoft Exchange Server is a centralized corporate messaging system that enables you to manage electronic mail and other messaging tools for your organization from a single location.

Exchange Server Organization

A Microsoft Exchange Server messaging system comprises several administrative units, the largest of which is the organization. The organization hierarchy varies depending on the version of Exchange Server you are using:

- **Exchange Server 5.5**—In Exchange Server 5.5, the organization hierarchy includes sites (domains) that contain groups of local servers that share the same directory information. Each server consists of the Directory and Information Store databases:

  - The Directory database includes information about an organization's recipients, distribution lists, servers, and messaging infrastructure.

  - The Information Store database provides server-based storage, holds users' mailboxes and public folders, and enforces security. The information store also replicates public folders, enforces storage limits, and delivers messages to users on the same server. It maintains information in two databases—the public and private information stores. The public information store maintains information stored in public folders. The private information store maintains all messages in users' mailboxes. For more information about Exchange Server 5.5, see your Microsoft Exchange Server documentation.

- **Exchange Server 2000 and 2003**—In Exchange Server 2000 and 2003, the organization hierarchy includes organizations, administrative groups, servers, and storage groups. The organization is the highest level in the hierarchy and includes the entire enterprise. An administrative group is a set of servers that share an administrative security context. Each server in the administrative group can have up to four storage groups. Each storage group includes up to five database stores that can be mounted and dismounted independently. For more information on the Exchange Server 2000 and 2003 organization hierarchy, see your Microsoft Exchange Server documentation.

  Note: If you are using Exchange Server 2003 and want information on performing Volume Shadow Copy Server backups, see the *Microsoft Volume Shadow Copy Service Guide*.

Agent Overview

The agent integrates with BrightStor ARCserve Backup to let you back up and restore Exchange Server databases and database components (such as mailboxes). It also integrates with the Exchange Server's backup and restore API function enabling you to perform online backups.

Backup and Restore Types to Use with the Agent

The agent offers the following types of Exchange Server backup and restore:

- **Database Level Backup and Restore**—Use this type to back up and restore a server's storage groups and databases and to restore the system in disaster recovery scenarios. This type can be used only to back up an entire database and cannot be used to perform a more granular level of backup and restore, such as backing up individual folders.

   Important! *Every time you back up your Exchange Server, you should perform a Database Level backup.*

- **Brick Level Backup and Restore**—Use this type to perform folder-level backup and restore jobs using Messaging Application Programming Interface (MAPI). This type is useful for recovering mailboxes and folders to original or alternative locations. This type should be used for a granular level of backup and restore, such as backing up individual folders, and should not be used to back up an entire database.

   Note: Brick Level backup and restore does not support Single Instance Storage (SIS), an architecture included with Exchange Server that maintains duplicate files with a minimum of disk, cache, and backup media overhead. As a result, when you use Brick Level backups your backups can be equal to or larger than the original database size.

For more information on these types, see chapters "Performing Database Level Backups and Restores" and "Performing Brick Level Backups and Restores."

Agent Benefits

The agent provides great flexibility and security when managing your data storage requirements. It allows you to:

- Manage backups of Exchange Server databases, mailboxes, and public folders from a remote location.

- Perform online database backups using Exchange Server's backup and restore API.

- Schedule Exchange Server backups using the powerful Backup Manager.

- Back up to a wide array of storage devices.

The agent is installed on the Exchange Server and handles all communication between BrightStor ARCserve Backup and the Exchange Server database during backup and restore. This includes preparing, retrieving, transmitting, interpreting, and processing data packets that are sent back and forth across the network.

When BrightStor ARCserve Backup starts to back up a database or database component, it sends a request to the agent. The agent retrieves the data from the Exchange Server (using the Exchange Server backup and restore API functions) and sends it to BrightStor ARCserve Backup, where the full database or the components are backed up to your storage media. Similarly, the agent transfers database information when data is restored from storage media.

Add-on Overview

The add-on is an optional product that is available only if you install the agent. The add-on offers advanced configuration options, performs folder level backups and message level restores, and supports advanced filtering during backup. It also maximizes performance and flexibility by supporting complete messaging single instance storage, multi-threading, and by offering the most granular level of restore. You should use the add-on when you want the flexibility to restore individual objects, such as a mailbox, folder, or even a single message. The add-on can also be used to simplify many administrative tasks, such as auditing, migration, pruning, and aging. Using the add-on, you can back up many messaging objects including posts, tasks, notes, journal entries, mail messages, events, appointments, meeting requests, and contacts.

Backup and Restore Types to Use with the Add-on

The add-on offers the following types of Exchange Server backup and restore:

- **Database Level Backup and Restore**—Use this type to back up and restore a server's storage groups and databases, and to restore the system in disaster recovery scenarios. This type can be used only to back up an entire database and cannot be used to perform a more granular level of backup and restore, such as backing up individual folders.

  Important! *Every time you back up your Exchange Server, you should perform a Database Level backup.*

- **Document Level Backup and Restore**—Use this type instead of Brick Level backup and restore to perform folder level backups and message level restores. It maximizes performance and flexibility by supporting SIS, multi-threading, and advanced filtering and configuration options. This type should be used for a granular level of backup and restore, such as backing up individual folders, and as a supplement to Database Level backups.

  Important! *If you use Document Level Backup and Restore, you do not need to use Brick Level backup and restore.*

For more information on these types, see the chapters "Performing Database Level Backups and Restores" and "Performing Document Level Backups and Restores."

The add-on offers many benefits, including:

- Complete messaging single instance storage

- Push agent technology

- Multi-threading

- Multi-streaming support

- Document level restore

- Migration support

- Enhanced cluster support

- Job continuation

Chapter 2: Installing the Agent

The BrightStor ARCserve Backup Agent for Microsoft Exchange, and the optional BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on, can be installed locally or remotely on a BrightStor ARCserve Backup client machine. This chapter includes the information that you need to install and configure the agent and add-on.

System Requirements

See the readme file on the installation CD-ROM for hardware and software requirements for installing and running the agent and the add-on. Check http://ca.com for any updates to the requirements.

Installation Prerequisites

Before installing the agent, you must satisfy the following prerequisites:

- Ensure your system requirements meet the minimum requirements needed to install the BrightStor ARCserve Backup. For a list of requirements, see the readme file.

- Ensure that you have Administrator privileges.

- Ensure that you know the name and password of the machine you are installing the agent on.

- Ensure that your Exchange Server is running.

- If you will be performing remote backups, ensure that File and Printer Sharing for Microsoft Networks is enabled on the agent machine that you will be backing up.

- The NetLogon service must be started to support pass-through authentication of account logon events for computers in a domain.

Install the Agent

Before you install the agent and add-on, keep the following in mind:

- Install the agent on the server where you have Exchange Server installed.

- You must install agents on the local drives of all Exchange Servers.

- To install the add-on, you **must** also install the agent. You cannot install the add-on separately.

- If your Exchange Server has high CPU usage during normal operations, you should have a separate server for the Backup Manager and should not install it on the same server where you install the agent and add-on.

The agent and add-on follow the standard installation procedure for the system components, agents, and options of BrightStor ARCserve Backup. For the detailed steps in this procedure, see *Getting Started*.

When installing the agent, add-on, or both, consider installing the Client Agent for Windows and the Disaster Recovery Option. The Client Agent allows you to back up your System State and the Disaster Recovery Option lets you recover the entire server in case of a disaster.

When you install the agent, the CA BrightStor ARCserve Backup RPC service (dbasvr.exe) is installed. When you install the add-on, the CA BrightStor Universal Agent is installed. Because the add-on uses push technology and shares the transport layer with the Client Agent for Windows, see the Windows Client Agents configuration section in the *Client Agents Guide* for more information about configuring network communication for the add-on.

Install the Add-on on a Cluster

For the add on to work properly on a cluster, the cluster resource type BrightStor ARCserve Backup **Exchange Agent Notifier** must be registered and the resource instance type BrightStor ARCserve Backup **Exchange Agent Notifier** must be created. The binaries for the cluster resource type are CAExCluRes.dll and CAExCluResEX.dll. The installation procedure registers the cluster resource type and creates the cluster resources instance for you automatically when you install the add on on local nodes. If you would rather register and create the cluster resources manually, see the Register the Cluster Resources Manually section that follows.

After the cluster resources are registered, you must specify a common location for the check point file. This location should be accessible from all possible nodes on which a virtual server can potentially run. This allows job continuation and incremental and differential jobs to properly execute even if they fail over to a different node. To set this destination, use the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\BrightStor ARCserve
Backup\ExchangeDocumentAgent\Parameters
Value Name:        <VirtualServerName>_ChkPath
Value Type:        REG_SZ
Value Data:        <Path>
```

For example, if virtual server EXVS1 is using drive g: as a disk resource to store data and virtual server EXVS2 is using drive h: as a disk resource to store data, add the following registry key on all nodes that are possible owners of these virtual servers.

```
Value Name:        EXVS1_ChkPath
Value Type:        REG_SZ
Value Data:        g:\CA\Temp

Value Name:        EXVS2_ChkPath
Value Type:        REG_SZ
Value Data:        h:\CA\Temp
```

Register the Cluster Resources Manually

When you install the add on on local nodes, the installation procedure registers and creates the cluster resources automatically. If you would rather register and create the cluster resources manually, use the following procedure:

1. Ensure that the agent and add on are installed on all nodes on which Exchange Virtual Server could potentially run and the agent and add on install directory is the same on all nodes.

2. If the resource type is not already registered, run the following command:

```
Cluster.exe restype "BrightStor ARCserve Backup Exchange Agent
Notifier" /create /dll: CaExCluRes.dll /type:"BrightStor ARCserve
Backup Exchange Agent Notifier"
```

Note: If your resource type is already registered, BrightStor ARCserve Backup Exchange Agent Notifier is displayed under the Cluster Configuration\Resource Types branch in the Cluster Administrator:
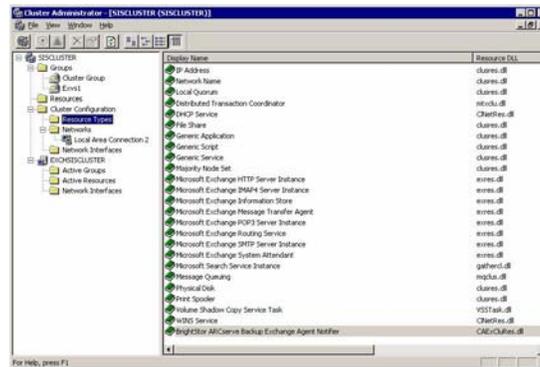
3. Run the following command to register the extension dll:

    ```
    Cluster.exe/REGEXT:"C:\WINNT\cluster\CAExCluResEx.dll"
    ```

4. Use the Cluster Administrator to create the BrightStor ARCserve Backup
    Exchange Agent Notifier cluster resource instance in the Exchange Virtual
    Server group. As a best practice, append the Exchange Server name to the
    cluster resource instance name. For example, BrightStor ARCserve Backup
    Exchange Agent Notifier – (VS1) is the cluster resource instance name and
    VS1 is the Exchange Server name. When the New Resource dialog opens,
    enter the name and description of the resource instance, select BrightStor
    ARCserve Backup **Exchange Agent Notifier** in the Resource type field,
    select the name of your Exchange Server virtual group in the Group field,
    and click Next.
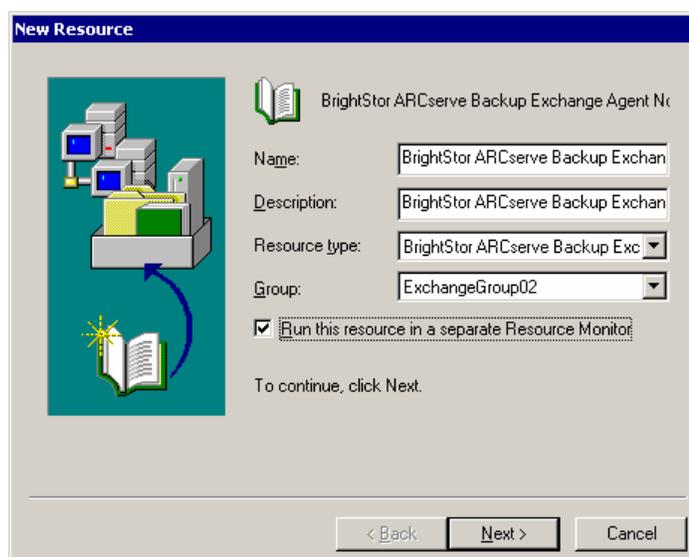
5. When the Possible Owners dialog opens, the nodes in the cluster on which the resource can be brought online are automatically displayed in the Possible owners box. Click Next.
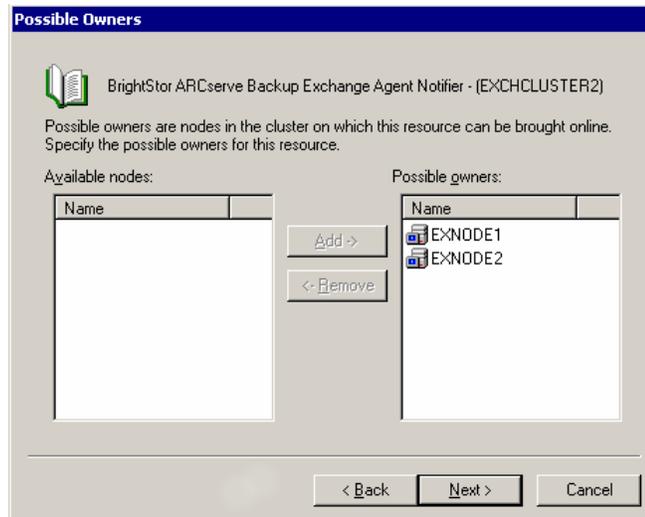
6. When the Dependencies dialog opens, click Finish to end the resource creation process, and then click OK.
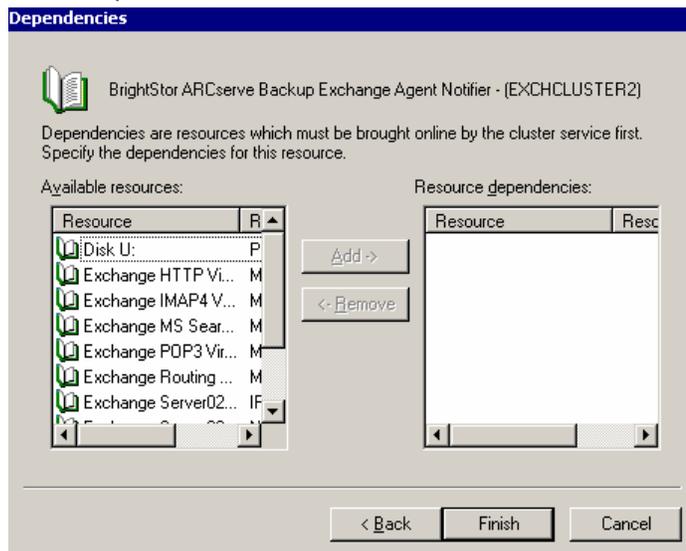
7. Open the Cluster Administrator and confirm that the BrightStor ARCserve Backup Exchange Agent Notifier resource is displayed:
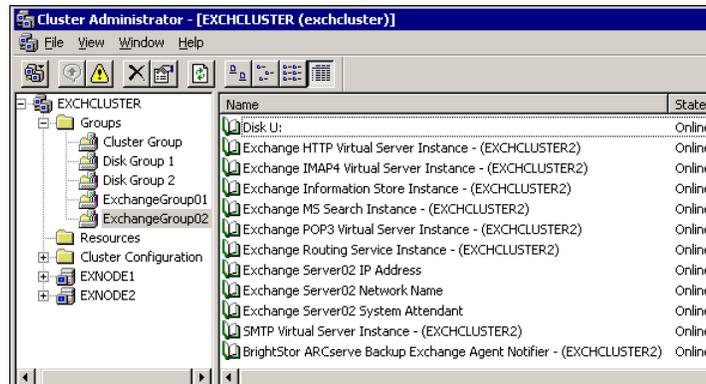
8. Right-click the BrightStor ARCserve Backup Exchange Agent Notifier resource to verify options. The options should appear similar to the following.

    On the General tab:
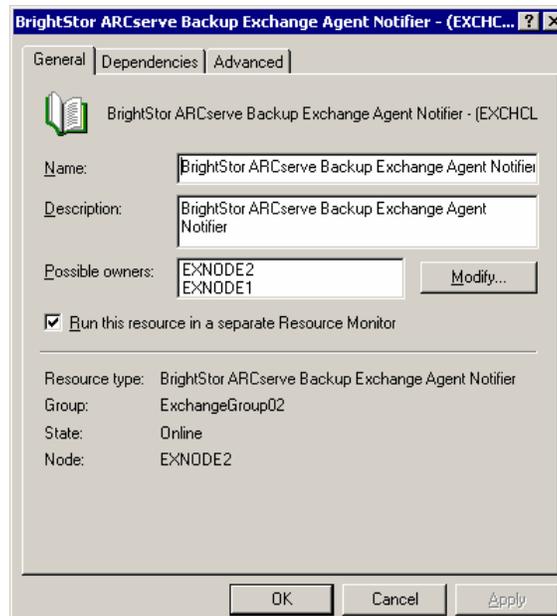
On the Dependencies tab:
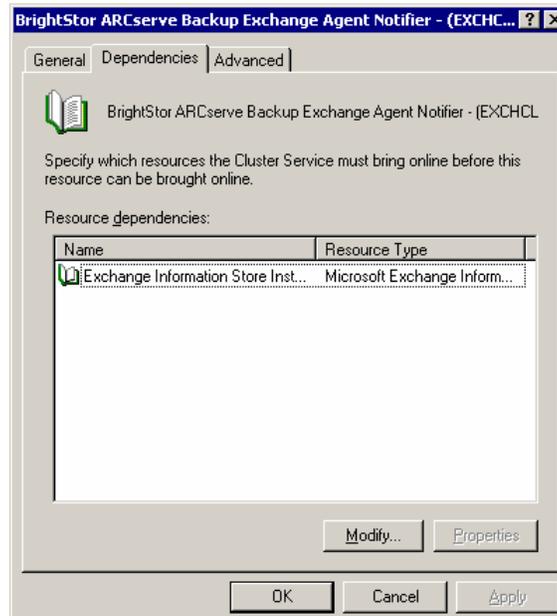
On the Advanced tab:
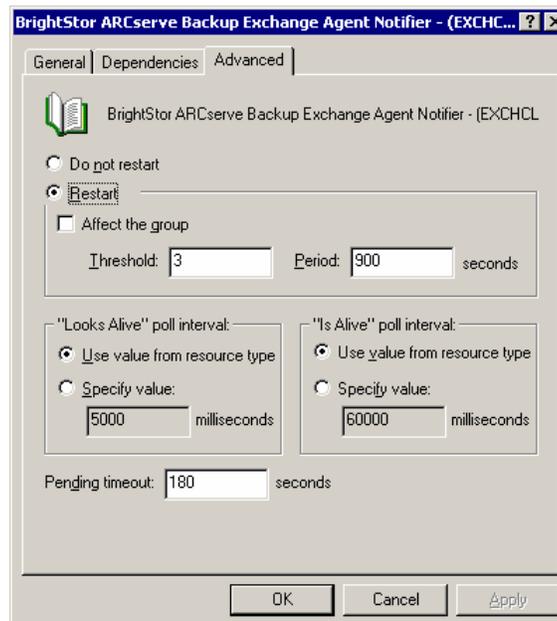
Note: On the Advanced tab, make sure the **Affect the group** checkbox is **not** selected. This ensures that the state of the resource does not affect the Exchange Server virtual group.

9. Repeat steps 2 to 6 on each node that has an Exchange Server virtual group where you need to create the resource.

Post-installation Tasks

If you did not configure the agent during the installation process, you must configure it now. The following sections explain how to perform these post-installation tasks.

Configure Database Level and Brick Level Backup and Restore

The Exchange Agent Configuration Utility lets you configure Database Level and Brick Level backup. Database Level configuration includes selecting a TCP/IP port number and selecting the number of 64 KB blocks of data that are sent per data transfer. Brick Level configuration includes creating or verifying the mandatory backup agent service account.

Note: We strongly encourage you to use the Exchange Agent Configuration Utility to create a backup agent service account for Brick Level backup and restore. However, if because of the setup of your environment it is better for you to manually create a backup agent service account, see the appendix "Configuring the Backup Agent Service Account Manually" for information on how to do so.

To configure Database Level and Brick Level backup and restore:

1. Log on to the Windows server where the Exchange Server is installed and verify that the Exchange Server database containing the service account mailbox is mounted.

   Note: If you are configuring the agent on a cluster node, make sure that the virtual server containing the service account mailbox is online on the local cluster node.

2. Choose Start, All Programs, Computer Associates, BrightStor, ARCserve, Backup Agents, Exchange Agent Configuration.

3. When the Configuration dialog opens, you can set up Database Level configuration and Brick Level configuration.
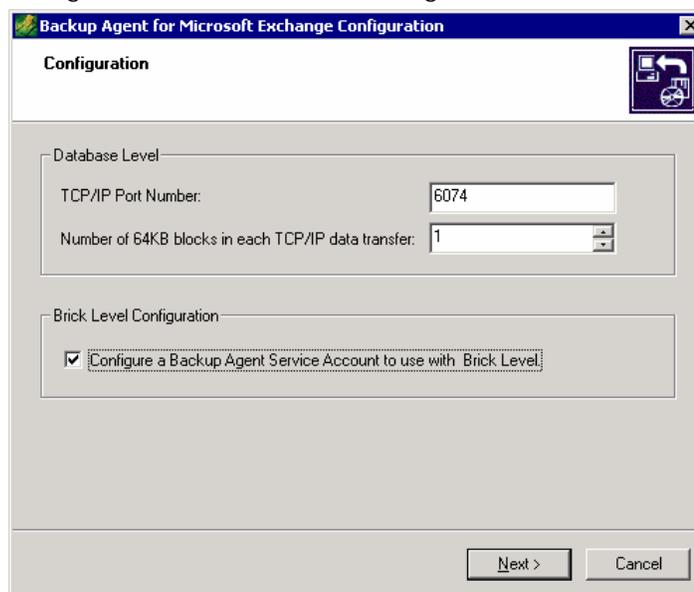
Database Level—These options apply only to Exchange Server Database Level backups. The TCP/IP port number and number of 64 KB blocks in each TCP/IP data transfer field apply to the DBAEXCHR.EXE process that is launched by the CA BrightStor ARCserve Backup RPC service when you perform a remote Database Level backup using the TCP socket protocol. Although you can configure this information, you should use the defaults:

■ **TCP/IP Port Number**—The default is 6074. To change this, you must enter a new port number. You must also modify the PortsConfig.cfg file on each Backup Manager you will be using to back up your Exchange Server. For more information on how to modify the PortsConfig.cfg file and configuring ports for firewalls, see the *Administrator Guide*.

■ **Number of 64 KB blocks in each TCP/IP data transfer**- Specifies the number of 64 KB blocks of data that are sent per data transfer. The default is 1. Other recommended numbers are 2, 4, 8, and 16.

Brick Level Configuration-If you want to configure for Brick Level backup and restore, check the Configure Exchange Agent to do a Brick Level Backup box.

4. After you finish configuring, click Next.

5. When the Brick Level Configuration dialog opens, either create a new account or verify an existing account to ensure that it meets the backup agent service account requirements, and then click Finish. For more information, see the following procedures for creating a new Brick Level account and verifying an existing Brick Level account.

6. When the dialog opens confirming that you successfully created your account, click OK.

    Note: If you have problems verifying an existing account or creating a new account, see the appendix "Configuring the Backup Agent Service Account Manually."

Create a Brick Level Account

To create a new Brick Level account:

1. In the Mailbox field, enter a unique name for your mailbox. A unique name is a name that does not exist in the organization as a subset of characters in another mailbox name. For example, you cannot use the name Admin, if there is a mailbox named Administrator in your organization.

2. In the Service Account field, enter a unique name for your Service Account.

3. In the Password field, enter a password. When entering the password, ensure that it meets the length, complexity, and history requirements of the domain and server you are restoring to.

4. In the Confirm Password field, reenter your password.

5. In the Domain of Account field, confirm your local domain name.

6. Place a check mark in the Create a new account box.

7. Click Finish to create and verify the account.

   Note: For Exchange Server 2000 and 2003, the mailbox is automatically created in the first database of the first storage group on the local machine. You can move this mailbox to any mailbox database on the local server.

8. For Exchange Server 2000 and 2003, when the dialog opens confirming that your account has been added as a member to the Administrators, Backup Operators, and Domain Admins groups, click Yes, and then click OK.

   Note: For Exchange Server 5.5, your account is added, as a member, to the Administrators Group and Backup Operators Group.

Verify a Brick Level Account

To verify an existing Brick Level account:

1. In the Mailbox field, enter the name of your mailbox.

2. In the Service Account field, enter the name of your Service Account.

3. In the Password field, enter your password.

4. In the Confirm Password field, reenter your password.

5. In the Domain of Account field, confirm your local domain name.

6. Click Finish.

Configure the Add-on

After you upgrade to the BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on, you must configure performance and file location settings.

To configure the add-on:

1. Choose Start, All Programs, Computer Associates, BrightStor, ARCserve Backup Agents, Backup Agent Admin.

2. When the BrightStor Backup Agent Admin dialog opens, select **CA BrightStor ARCserve Backup Agent for Exchange-Premium** in the drop-down list and click the Configuration button.
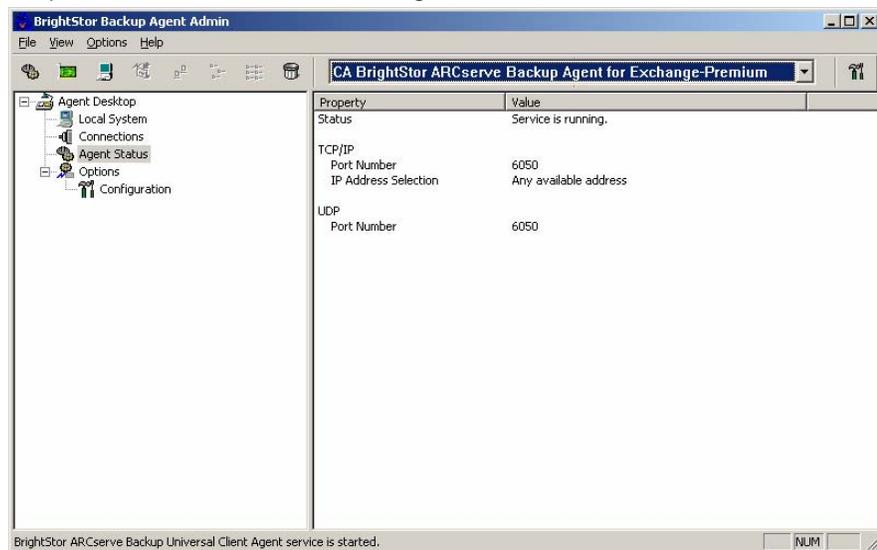
3. When the Configuration dialog opens, select the following settings:

- **Complete Messaging Single Instance Storage**—This option checks to see if attachments and messages have already been backed up and then backs up only one copy. This eliminates the need to back up each time the attachment and message are referenced. This can significantly decrease the size of your backups.

- **Backup Only Local Public Folder Documents**—In Exchange Server, public folders can include multiple public folder stores on many servers across the organization. As a result, when you select to back up a public folder, you could be backing up many public folder stores. To save time and maximize performance, this option lets you exclude remote public folder documents during public folder backups.

- **Number of Threads—**This is the number of threads you want to use to connect to MAPI per session. If you increase this number, it increases performance, but also increases CPU utilization. The default Number of threads value is 1.5 multiplied by the number of CPUs rounded down and the supported range is between 1 and 64.

- **Thread Priority—**This is the priority you want to set for your threads: low, medium, or high. If you increase the priority, the operating system increases the CPU cycles to the thread. If you increase the number of threads in the Number of threads field, you should decrease the thread priority to lessen the impact on your server.

- **Maximum Backup Size—**To allow an efficient flow of information during backup, data is stored in a transition queue. This setting lets you configure the size of this queue. The default Max queue depth value is 256 items and the supported range is between 32 and 1024.

- **Maximum Restore Size**—This sets the threshold for memory that SIS restores will use before saving objects to the temporary location you specify. If the amount of cached SIS data exceeds this value, you can increase the value to gain better performance. If the amount of cached SIS data exceeds the value you select, the restore is not affected, but a notification message appears in the activity log. The default Max Restore memory value is half of your system RAM and the supported range is between 32 and 1024.

- **Retry Counter—** If a MAPI error or time out occurs while trying to retrieve an object from Exchange Server, this setting lets you control the number of times you want to retry. This is useful for when your backups are competing with third-party applications or during periods of high volume activity. If a MAPI error or time out occurs, the object is skipped, but the backup continues and a notification message is displayed in the log location you specify. The default Retry counter value is 1 and the supported range is between 0 and 10.

- **Retry Delay—**If a MAPI error or time out occurs while trying to retrieve an object from Exchange Server, this setting lets you control the delay between retries. This is useful when your backups are competing with third-party applications or during periods of high volume activity. If a MAPI error or time out occurs, the object is skipped, but the backup continues and a notification message is displayed in the Log location you specify. The default Retry Delay value is 0 and the supported range is between 0 and 10.

- **Log Detail Level**—Do not change this value unless directed by a trained Computer Associates Customer Support technician. This sets the level of detail on the debug trace and log in the log location you specify. The default Debug Level value is 1 and the supported range is between 0 and 5.

- **Job Continuation Level**—If a job fails to complete, this setting lets you skip mailboxes and root public folders that already have been backed up and continue the job from the point of interruption. This is especially useful for continuing jobs in the case of a cluster failover. The default Job Continuation Level value is 1 and the supported range is between 0 and 2. 0 disables job continuation, 1 continues makeup jobs only, 2 continues any interrupted jobs.

  Note: Because job continuation begins the job at the point of interruption and skips items that were already backed up in the original job, you should ensure that the skipped items were backed up properly in the original job and that they can be browsed from a restore view.

- **Skip Log Setting**—At the end of each backup job, a summary of each session is displayed in the Activity Log. If individual folders, messages, and attachments are not backed up, by default, the details will be listed in the skip log in the agent log directory. If you would rather view the skip log information in the Activity Log or if you want to view it in the Activity Log in addition to the skip log, this setting lets you configure the location. The default Skip Log Setting value is 0 and the supported range is between 0 and 2. 0 logs information to the skip log only, 1 logs information to the Activity Log only, 2 logs information to both the skip log and Activity Log.

  Note: This skip log is also useful for tracking corrupt messages in an Exchange Server.

- **Backup Additional User Properties—**If you are using Exchange Server 2000 or 2003, this setting lets you back up a greater level of user properties detail and determines what is restored when using the **Create user if not existing** restore option. For more information on restore options, see Document Level Restore Options in the chapter "Performing Document Level Backups and Restores." If you do not enable this option, only the display name that is associated with the mailbox is backed up. This is useful if you will be using this user as a placeholder to perform an audit or test restore. If you do enable this option, most additional properties, such as first name, last name, fax number, and address information are backed up. This is useful for migration, but will increase the backup time.

- **Disable Purge Option—**When a backup job is created using the time-based backup method, the **Purge documents after backup** option can be enabled so that documents are automatically deleted after they are backed up. However, since this option should be used with caution, you can enable the Disable Purge Option as a safety feature to override the purge and prevent an agent from pruning an Exchange Server.

- **Show Brick Level—**This option displays Brick Level in the Backup Manager and Restore Manager.

  Note: If you previously used Brick Level and want to restore a Brick Level backup to an alternative location, enable this option so you can select the correct location on the Destination tab in the Backup Manager.

- **Append To Restored Mailbox—**During restore, if you want to create duplicates of existing users and mailboxes in the same organization, you must append a string to the user and mailbox names. Enter the string you want to append in this field. Since the maximum character limit for user and mailbox names on some systems is 20 characters, try to keep the string short. If you do not want to create duplicates, leave this field blank.

- **Log Location—**If you want to change your log location from the default, click Browse and select a new location.

- **Temp Location—**If you want to change your temp location from the default, click Browse and select a new location.
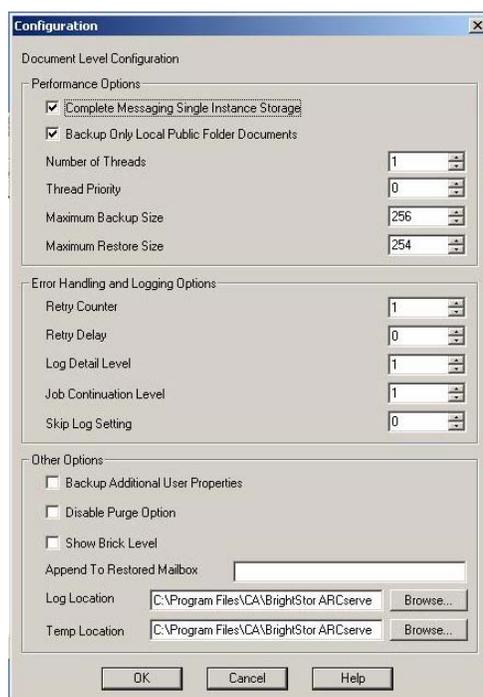
4. Click OK.

Remote Server Views in the Backup Manager

Depending on the configuration of the server on which BrightStor ARCserve Backup is installed, you can view remote Exchange servers from:

- The Exchange Organization View

- The Windows NT/2000/XP/2003 Systems object

- The Preferred Shares/Machine object

Exchange Organization View

The Exchange Organization View provides a central display of your entire Exchange Organization. This lets you quickly find all the remote Exchange servers in your environment rather than having to enter each of them manually under the Windows NT/2000/XP/2003 Systems object or Preferred Shares/Machines object.
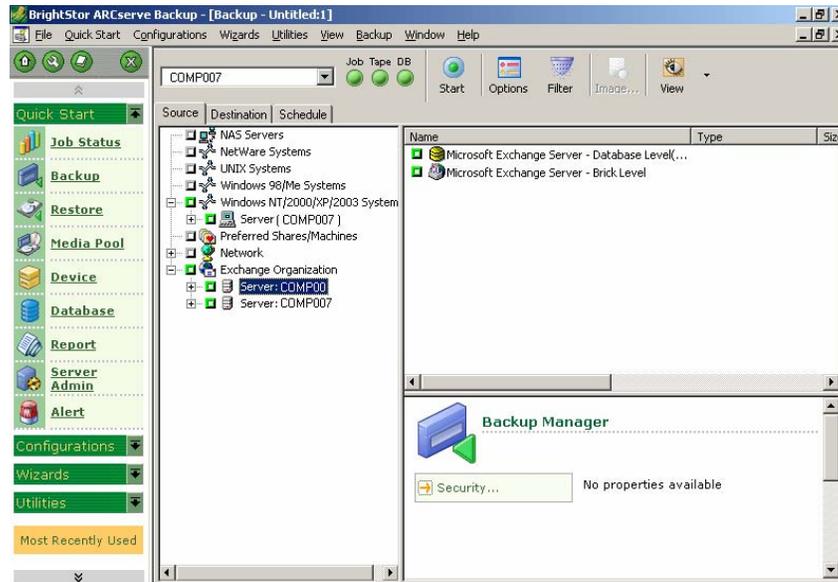
To use the Exchange Organization View, the BrightStor ARCserve Backup Manager must be installed on the same machine as your Exchange Server.

In the Exchange Organization View, the Exchange Server database objects are organized in a hierarchy similar to the Exchange Server Manager.

Note: The Exchange Organization is always explicitly packaged. You must repackage jobs if Exchange servers are added or removed from your organization. For more information on packaging your jobs, see *Getting Started*.

Add Remote Server to the Systems Object

If you installed the BrightStor ARCserve Backup Agent for Windows or the BrightStor ARCserve Backup Agent for Microsoft Exchange Premium Add-on components, to view remote Exchange Servers, you must add them to the Windows NT/2000/XP/2003 Systems object in the Backup Manager.

To add a remote server to the Windows NT/2000/XP/2003 Systems object:

1. From the Quick Start menu on the BrightStor ARCserve Backup Home Page, click Backup Manager.

2. When the BrightStor ARCserve Backup Manager opens, right-click the Windows NT/2000/XP/2003 Systems object and select **Add Machine/Object**.
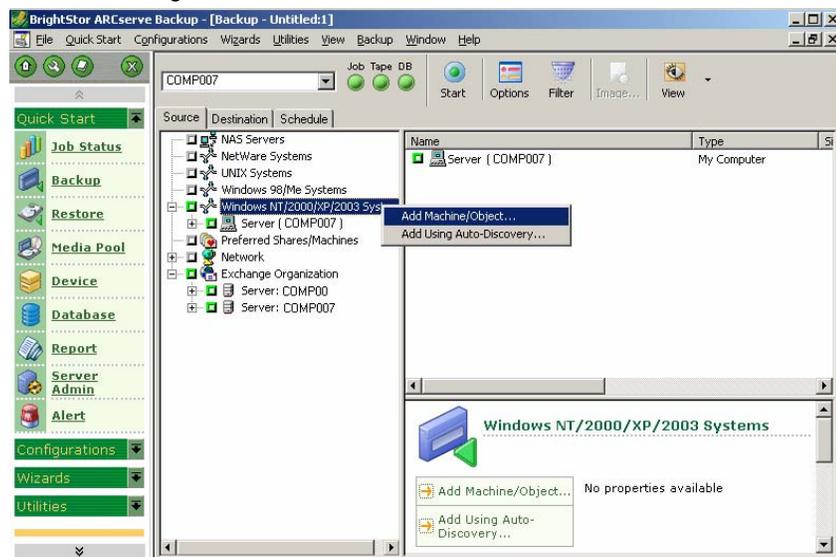
3. When the Add Agent dialog opens, enter the Host Name for the machine and either enable the **Use Computer Name Resolution** option to automatically search for the correct IP address each time you connect to this computer, or enter an IP address.

   Note: The machine you are adding must be running and have the Universal Agent started.

4. Click Add. The machine is added to the Windows NT/2000/XP/2003 Systems object.

5. Repeat Steps 3 and 4 for each remote Exchange Server in your environment.

6. Click Close.

Add Remote Server to the Preferred Shares/Machines Object

You must add remote Exchange Servers to the object Preferred Shares/Machines in the Backup Manager if you did not install the following software:

- BrightStor ARCserve Backup Agent for Windows

- BrightStor ARCserve Backup Agent for Microsoft Exchange Premium Add-on

To add a remote server to the Preferred Shares/Machines Object:

1. From the Quick Start menu on the BrightStor ARCserve Backup Home Page, click Backup Manager.

2. When the BrightStor ARCserve Backup Manager opens, right-click the Preferred Shares/Machines Object select **Add Machine/Object**.
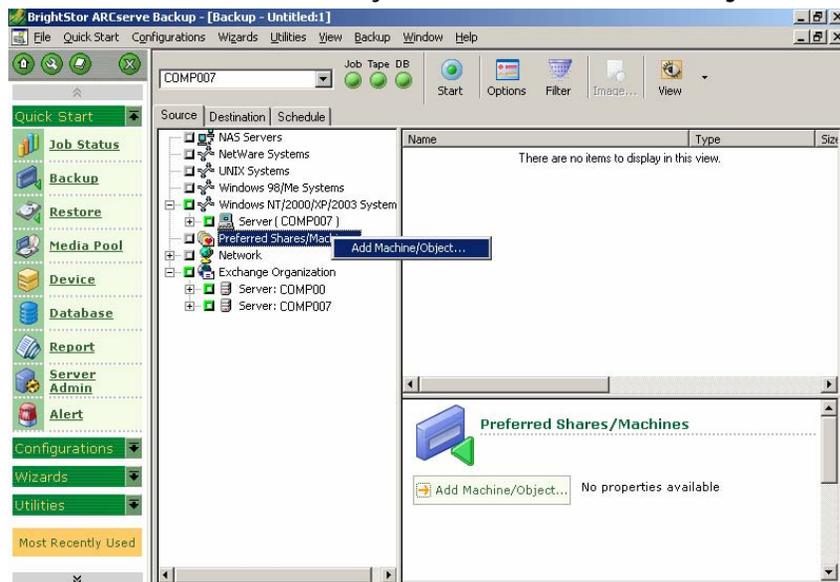
3.   When the Add Object dialog opens, ensure Microsoft Windows Network is selected in the Network Provider field and enter a share name using Uniform Naming Convention (UNC) format (for example, \\MACHINE\SHARE) or enter a machine name in UNC format (for example, \\MACHINE).
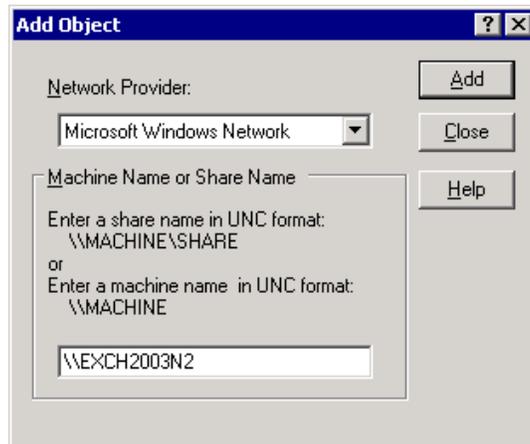
3.   Click Add. The machine is added the Preferred Shares/Machines object.

4.   Repeat Steps 3 and 4 for each machine or share you want to add.

5.   Click Close.

Chapter 3: Performing Database Level Backups and Restores

Database Level backup and restore protects the Exchange Server database files and logs. It is the fundamental backup for your Exchange Server, and you should always use it regardless of whether you use one of the other granular backup types. You can use Database Level backups to restore Exchange Server in the event of a system failure, database corruption, or disaster recovery scenario.

Using the Database Level backup, you can back up several types of databases, depending on the version of Exchange Server you are using:

- Exchange Server 2003
    - Information Store (IS)
    - Site Replication Service (SRS)
- Exchange Server 2000
    - Information Store (IS)
    - Key Management Service (KMS)
    - Site Replication Service (SRS)
- Exchange Server 5.5:
    - Information Store
    - Directory

The following sections describe how to use Database Level backups to protect these databases.

Database Level Backup and Restore for Exchange Server 2000 and 2003

The following sections describe how to use Database Level backup and restore for Exchange Server 2003 and 2000.

Database Level Views in the Backup Manager

Depending on your configuration, Microsoft Exchange Server – Database Level(IS) appears in the Backup Manager under the following objects:

- Windows NT/2000/XP/2003 Systems

- Preferred Shares/Machines

- Exchange Organization

When you expand the Microsoft Exchange Server – Database Level(IS) object, you can view your local and remote Exchange servers. When you expand a server, you can view the databases and their components that you can protect using Database Level backup and restore:

Note: Microsoft Key Management Service (Exchange Server 2000 only) and Microsoft Site Replication Service are optional and appear in the Backup Manager only if you have them installed.

In BrightStor ARCserve Backup, the Microsoft Exchange Server – Database Level (IS) object, Microsoft Site Replication Service object, and Microsoft Key Management Service object includes up to four storages groups. Each storage group includes up to five database stores.

Note: In a cluster environment, Exchange servers appear under the Exchange virtual server objects.

Backup Agent Service Account Requirements for Database Level Backup and Restore

To perform a Database Level backup and restore job, your backup agent service account must be a member of the following groups on the Exchange Server:

- Administrators

- Backup Operators

Database Level Backup Features

The following sections include information on the features that the BrightStor ARCserve Backup Agent for Microsoft Exchange and the optional BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on offer when backing up using Database Level and the procedure for how to perform a backup using Database Level.

Database Level Backup Methods

When you submit a backup job, you must select a backup method. The backup method tells BrightStor ARCserve Backup how you want your data to be backed up. When you use the agent, you can select a backup method for your Database Level backup job at the storage group level or you can use a globally scheduled backup method.

Important! *If you select to back up only a mailbox store or public folder store without dynamically selecting the entire storage group, the copy backup method is automatically used so that the storage group's logs are not affected.*

To select a backup method at the storage group level, explicitly select the storage group's parent database object (Microsoft Exchange Server – Database Level (IS), Microsoft Site Replication Service, or Microsoft Key Management Service object), right-click the storage group, and select **Agent Option**:

Note: For more information on explicit job packaging, see *Getting Started*.

The following dialog opens:
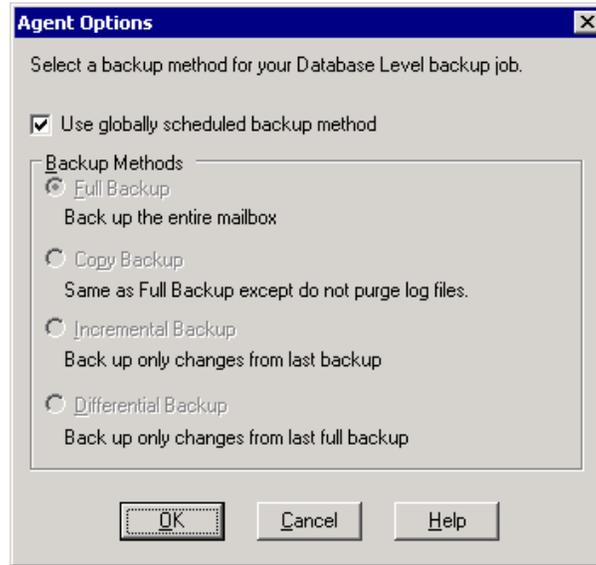
The advantage of selecting a backup method at the storage group level is that it gives you the flexibility to use a different method for different storage groups. You can select from the following backup methods:

- **Use globally scheduled backup method**—Enabled by default. You must disable this option if you want to set a backup method at the storage group level. If you do not disable this, you must select a backup method on the Schedule tab.

  Note: If you do not disable this and select Custom Schedule on the Schedule tab, there is no difference between the full (Keep Archive Bit) and full (Clear Archive Bit) backup methods; they both function as full.

- **Full Backup**—This is the default. It backs up the entire database, including the log files, and marks all of the files that have been backed up in preparation for a subsequent incremental or differential backup. The log files are also truncated during a full backup. The backup operation then purges, from the Exchange Server, the committed log files it no longer needs. While the backup is taking place, new database changes can occur, so a patch file (.pat) is created to log these late changes. The patch file is backed up at the end of the process along with the log files. These backed up .pat files are restored automatically with the log files.

  Note: Always perform a full backup when running the agent for the first time, after upgrading to a Service Pack, and after performing a restore.

- **Copy Backup**—Backs up the entire database, including the log files, but does not mark the files as having been backed up. Use a copy backup if you want to make a full backup of your data but do not want to disrupt any existing incremental or differential backups.

  Note: The log files are not truncated during a copy backup.

- **Incremental Backup**—Backs up the log files that have changed since the last full or incremental backup and marks them as backed up. The log files are also truncated. When restored, the log files are applied to recreate the database at the time of backup.

  Note: Microsoft does not support incremental backups when the Circular Logging feature is enabled. If you do not disable Circular Logging and submit an incremental backup, the agent automatically converts the backup to full.

- **Differential Backup**—Backs up the log files that have changed since the last backup. The log files are not truncated. It does not, however, mark them as backed up. When restored, the log files are applied to recreate the database at the time of backup.

  Note: Microsoft does not support differential backups when the Circular Logging feature is enabled. If you do not disable Circular Logging and submit a differential backup, the agent automatically converts the backup to full.

Multiplexing During Database Level Backups

Multiplexing is a process in which data from multiple sources are written to the same media simultaneously. When a job that has multiple sources is submitted with the multiplexing option enabled, it is broken into child jobs— one for each remote node and additional streams for each local Exchange Server storage groups. These child jobs write data to the same media simultaneously.

For more information on multiplexing, see the *Administrator Guide*.

Multi Stream Option

If your BrightStor ARCserve Backup server is equipped with multiple devices in two or more groups, or multiple devices in one or more groups with the BrightStor® ARCserve® Backup Enterprise Module and BrightStor® ARCserve® Backup Tape Library Option installed, you can take advantage of the Multi Stream option.

This option divides your backup jobs into several sub-jobs that run simultaneously to different devices. You can have as many jobs running simultaneously as you have devices or groups on your system.

Database Level backup provides one stream per storage group for simultaneous backup. The number of available tapes, drives, and storage groups determines the number of streams that are run simultaneously during backup. You can enable the Multi Stream option on the Destination tab in the Backup Manager:
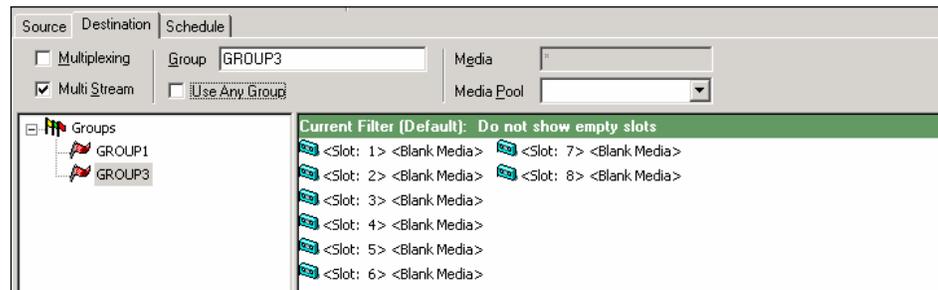
If you enable the Multi Stream option when you submit a Database Level backup job, the data is multi-streamed at the **storage group level** in two circumstances:

■ If you submit a local job under the Windows NT/2000/XP object:
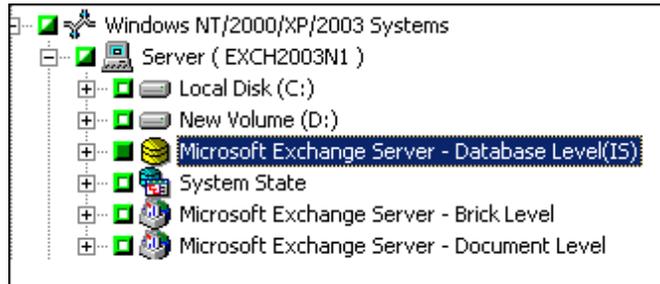
■ If you submit a local job under the Exchange Organization object:

In all other circumstances, data is multi-streamed at the server level.

For more information on the Multi Stream option, see the *Administrator Guide*.

Perform a Database Level Backup

Before you submit a Database Level backup job, make sure that the Exchange Server databases are mounted on your server and that the Microsoft Exchange Information Store and the CA BrightStor Backup Agent RPC Server service are running on your server.

To back up an Exchange Server database:

1. From the BrightStor ARCserve Backup Home Page, select the Backup Manager from the Quick Start menu.

2. When the Backup Manager opens, select the Database Level objects you want to back up (Microsoft Exchange Server – Database Level (IS), Microsoft Site Replication Service, and Microsoft Key Management Service). If you want to back up only certain storage groups or database stores within certain storage groups, expand a database object and select specific groups and database stores.

   Note: You should back up an entire storage group rather than individual database stores. Individual database stores can be restored from a backup of an entire storage group.

3. Right-click the Database Level object you selected to back up and select **Remote Protocol**.

4. When the Remote Protocol dialog opens, select one of the following remote protocols to use for the job, and then click OK:

   ■ **TCP/IP**—The default. Establishes a connection using sockets over TCP/IP. To configure what port the socket uses, see Configure Database Level and Brick Level Backup and Restore in the chapter "Installing the Agent."

   ■ **VI (Virtual Interfaces)**—Works with specific VI hardware environments.

   ■ **Named Pipes**—An alternative transport protocol used for legacy support.

   Note: By default, the agent uses the TCP/IP protocol when performing backups. If a problem occurs with this protocol, it automatically fails over to the Named Pipes protocol.

5. If you are not planning to schedule your job to use a rotation scheme, right-click each storage group object you are including in this job and select **Agent Option** to select a backup method to use. If you do this, the storage group's database parent object must be explicitly selected. For more information, see Database Level Backup Methods.

   Note: Always perform a full backup when running the agent for the first time. This allows you to store a complete set of Exchange Server databases.

6. If you want to enable CRC checking so that you can verify the integrity of your data using the Scan utility after the backup job is performed, click the Options button, click the Operation tab, enable the **Calculate and Store CRC Value on Backup Media** option, and then click OK.

    Note: For more information on CRC checking and using the Scan utility, see Database Level Scan Media Options.

7. Click the Destination tab and select a backup destination.

8. Click the Schedule tab. If you want to use a Custom Schedule, select a Repeat Method. If you want to use a rotation scheme, select the **Use Rotation Scheme** option and set up your scheme. For more information on scheduling jobs and rotation schemes, see the online help and the *Administrator Guide*.

    Note: If you use a Custom Schedule, the Backup Method section on the Schedule tab does not apply. For more information, see Database Level Backup Methods.

9. Click Start.

10. When the Security and Agent Information dialog opens, make sure that the correct user name and password are filled in for each object. If you need to enter or modify a user name or password, click the Security button, make your changes, and then click OK.

    Note: The security for a Database Level backup is determined from the security supplied for the server listed in the Object column. The security on that server must be a part of the Administrators and Backup Operators groups.

11. Click OK.

12. When the Submit Job dialog opens, select **Run Now** to run the job immediately, or select **Run On** and select a future date and time when you want the job to run.

13. Enter a description for your job.

14. If you selected multiple sources to back up and want to set the priority in which the job sessions initiate, click Source Priority. Use the Top, Up, Down, and Bottom buttons to change the order in which the jobs are processed. When you finish setting priorities, click OK.

15. On the Submit Job page, click OK to submit your job.

Database Level Backup Scan Utility

After you back up your Exchange Server database, you can use the BrightStor ARCserve Backup Scan utility to find out what is on your media, to view information about your media backup sessions, and, if you enabled **CRC checking during backup**, to verify the integrity of the data that was written to the media.

Note: For more information on how to enable CRC checking during backup, see Perform a Database Level Backup.

Each source that you select to back up is saved on media as an individual session. You can scan a single session or an entire media. To view the results of the Scan job in the Job Queue, click the Log tab.

Use the Log tab in the Options dialog to select the level of detail you see in the Job Queue Log. You can select to see just summary information and any errors that occurred during the scan or you can select to see each file that was backed up, summary information, and any errors that may have occurred.

Database Level Scan Media Options

If you enable CRC checking during backup, the following scan media options apply to your Exchange Server backup job.

On the Operation tab, enable **Calculate and Store CRC Value on Backup Media** if you want to scan files with a CRC check to verify the integrity of the data that was written to the media.

On the Job Log tab, select the level of detail you want to include in the log report:

- **Log All Activity—**Record all of the activity that occurs while the job is running in the Job Log.

- **Log Summary Only—**Record summary information of the job (including source, destination, session number, and totals) and errors.

- **Log Disabled—**Do not record any information about this job in the Job Log.

Note: You can view the log report in the Job Queue or Database Manager (Job Records).

Perform Media Scan

To scan media:

1. Open the Scan utility.

2. Select the media you want to scan. If the media you want to scan is not currently in a storage device, you must enter the information into the Group and Media fields.

3. Enter a specific session to scan or select to scan all sessions on the media.

4. Click Options to specify scan options for the job.

   Note: If you enabled **CRC checking during backup**, you must enable the **Calculate and Store CRC Value on Backup Media** option if you want to verify the integrity of the data.

5. Click Filter to specify filters for the job.

6. Click Start to submit the job.

Database Level Data Restore

The following sections include information on the prerequisites you must meet before you perform a restore, the features that the agent offers when restoring from a Database Level backup, and the procedure for how to perform a restore.

Database Level Restore Prerequisites

Before you restore, to prepare your Exchange Server, you must dismount the database stores within all storage groups you want to restore. To do this, open the Exchange System Manager, navigate to, and expand, the storage group you want to restore, right-click each database store and select **Dismount Store**:
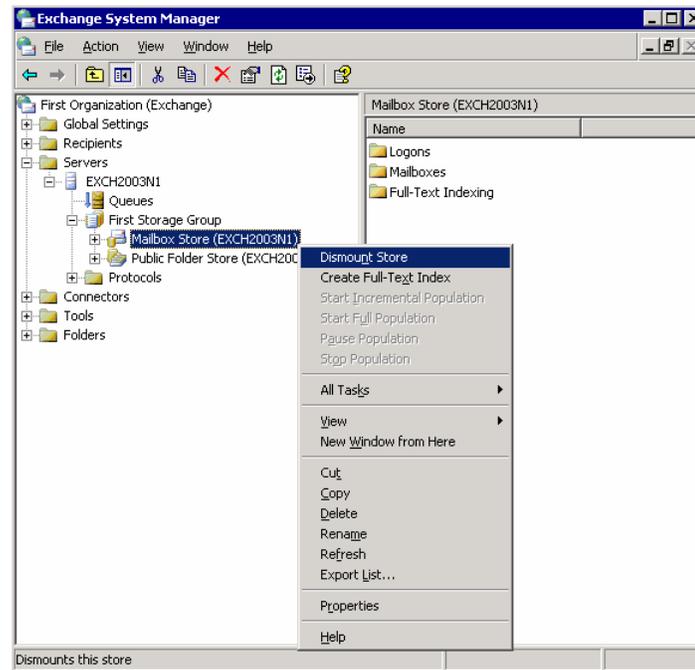
Note: You can also dismount databases automatically using the option **Automatically dismount database before restore**. For more information on this option, see Database Level Restore Options.

Enable the feature **This database can be overwritten by a restore** for each of the database stores in the Storage Groups you want to restore. To do this, open the Exchange System Manager, navigate to, and expand, the Storage Group you want to restore, right-click each database store and select Properties, click the Database tab, enable the feature **This database can be overwritten by a restore**, and then click OK.

Note: You can also automatically allow databases to be overwritten using the option **Allow database to be overwritten by restore**. For more information on this option, see Database Level Restore Options.
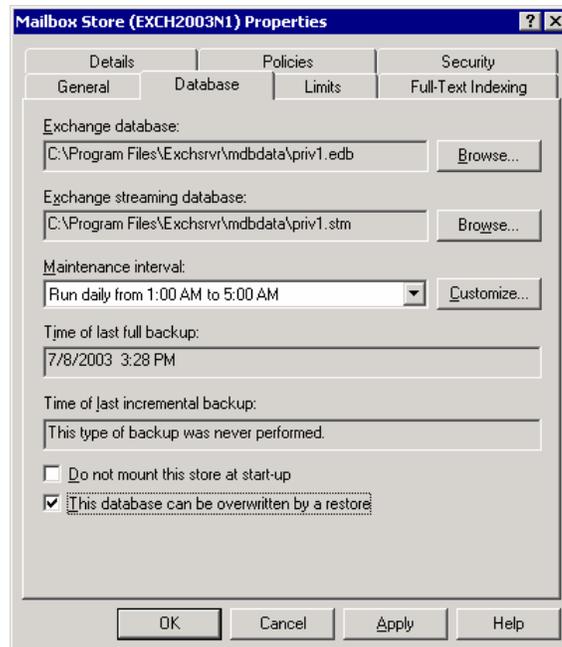
- Ensure that all of your necessary Exchange Server services are running.

- Ensure that the agent is installed on the same machine that has the Exchange Server installed and that the Backup Agent RPC Server service is running.

- Ensure that the server you are restoring to is configured exactly the same as the original server you backed up from. If you are restoring to the original location, the configuration is typically the same. Otherwise, use the worksheet in the appendix "Server Configuration Worksheet" to determine what needs to be identical. All fields in the worksheet except the Server Name field must be the same when restoring to an alternate location.

Database Level Restore Sets

When you back up an Exchange Server, each storage group that you select to back up is saved on media as an individual session. To restore an Exchange Server, you must restore all of the sessions that, when combined, completely restore the storage group. These sessions are called your restore set.

The number of sessions in your restore set depends on the backup methods you used:

- If you backed up your storage group using only the full backup method, your restore set includes only this full session.

- If you backed up your storage group using both full and incremental backups, your restore set includes your full session and at least one, but up to as many incremental sessions as you want to include. For example, in the following backup scenario, your restore set can be full and incremental 1, full and incremental 1 and 2, full and incremental 1, 2, and 3, or full and incremental 1, 2, 3, and 4:

Full	Incremental 1	Incremental 2	Incremental 3	Incremental 4

- If you backed up your storage group using both full and differential backups, your restore set includes your full session and one differential session. For example, in the following backup scenario, your restore set can be full and differential 1, full and differential 2, full and differential 3, or full and differential 4:

Full	Differential 1	Differential 2	Differential 3	Differential 4

After you determine your restore set, you must make sure that you select the entire set when submitting your restore job. If you use the Restore by Tree method when scheduling your restore job, the agent simplifies this task for you. When using Restore by Tree, all you must do is select the last incremental or differential session in your restore set and the agent will automatically include the full session for you.

To select your restore set in the Restore Manager:

1. From the BrightStor ARCserve Backup Home Page, select the Restore Manager from the Quick Start menu.

2. When the Restore Manager opens, select **Restore by Tree** in the drop-down box underneath the Source tab.

3. Expand the server that has the storage group you backed up and select the storage group object.

4. Click Version History.
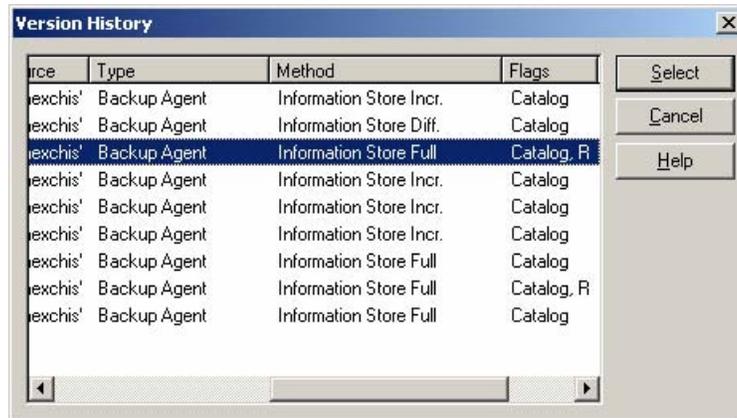
5. When the Version History dialog opens, highlight a session in your restore set and click Select. If your restore set includes incrementals and differentials, simply select the last incremental or differential in the set and the agent will automatically include the full backup for you (applies to Restore by Tree only).

    Note: The most recent backups are displayed at the top of the Version History dialog.

6. Set your restore options, select a destination, and submit the job.

    Note: If you use Restore by Session rather than Restore by Tree, you must repeat steps 1 to 6 for each session in your restore set.

Database Level Restore Options

When you create a restore job, you can choose restore options to customize the job:
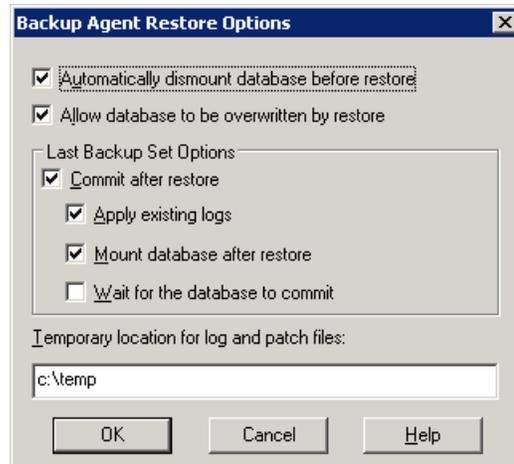
The following list describes each of the restore options. When to use these options depends on your restore set. To determine when to use each option, see Database Level Restore Options Selection.

- **Automatically dismount database before restore—**To prepare your Exchange Server before you restore, you must dismount the database stores within all storage groups that you want to restore. To do this automatically, enable this option. For information on how to dismount databases manually, see Database Level Restore Prerequisites.

- **Allow database to be overwritten by restore**—Before you restore, to prepare your Exchange Server, you must allow each database store in the Storage Groups you want to restore to be overwritten. To do this automatically, enable this option. For information on how to do this manually, see Database Level Restore Prerequisites.

- **Commit after restore**—Commits the database after the restore is completed. If you are restoring a set, use this option only when you are restoring the last backup in the set. If this option is not selected, the database is left in an intermediate state and is not yet usable but is ready for subsequent differential or incremental restores.

  - **Apply existing logs**—If you enable this, both the existing logs and any new logs that will be restored are applied together in sequential order when the database is committed. If you do not select this, only the new logs will be applied (existing logs are not applied).

    Important! *Do not use Apply existing logs if the Exchange Server you are restoring to is not the Exchange Server you backed up from, if the existing database is corrupt, or if the new logs that will be restored are out of sequence with the existing logs. If you enable this option and the agent detects that logs are out of sequence, the agent automatically disables the option so that the job does not fail.*

  - **Mount database after restore**—Instructs the Exchange Server to mount the database after the restore is completed. If you would rather manually mount your database, disable this option.

    Note: If the Exchange Server fails to mount the database, check the event log for details. If you think the Exchange Server failed to mount because of existing logs on the server, repackage and run the restore without the Apply existing logs option enabled.

  - **Wait for the database to commit**—If you enable this, the agent waits for the Exchange Server to return the commit result before finishing the restore. This may take a long time depending on the number of logs the Exchange Server is attempting to commit.

- **Temporary location for log and patch files**—Sets a temporary location on the Exchange Server machine to restore logs and patch files during the restore process. The temporary location you select must be empty before you restore and must have enough space for all the log files being restored. After the database commits the logs and patch files, they are deleted.

  Note: If you are restoring a series of full backups, incremental backups, or differential backups, you **must** use the same temporary location for all restore jobs.

Database Level Restore Options Selection

When to use these options depends on your restore set. The following tables describe when to use each restore option. If you restore using the Restore by Tree method, correct restore options are automatically applied for you. If you restore using Restore by Session, use the following information to determine when to use each option.

If your restore set contains incremental backups:

	Full	Intermediate Incrementals	Last Incremental
Apply	N	N	Y/N
Commit	N	N	Y
Mount	N	N	Y/N

If your restore set contains differential backups:

	Full	Differential
Apply	N	Y/N
Commit	N	Y
Mount	N	Y/N

If your restore set is a full backup:

	Full
Apply	Y/N
Commit	Y
Mount	Y/N

Perform a Database Level Restore

To restore an Exchange Server database:

1. From the BrightStor ARCserve Backup Home Page, select the Restore Manager from the Quick Start menu.

2. When the Restore Manager opens, select **Restore by Tree** in the drop-down box underneath the Source tab.

   Note: Both Restore by Tree and Restore by Session are supported for Database Level restore.

3. If the backup you want to restore is local, expand the Server object, expand the server that has the database you backed up, and select the database object. If the backup you want to restore is remote, expand the Microsoft Windows Network object, expand the server that has the database you backed up, and select the database object.

4. If the most recent backup is not the backup you want to restore, click Version History, select the version you want to restore, and click Select.

   Note: If you are using a restore set, you must restore the entire set in the order that it was backed up. If your restore set includes incrementals and differentials, simply select the last incremental or differential in the set and the agent will automatically include the full backup for you (applies to Restore by Tree only). For more information on restore sets, see Database Level Restore Sets.

5. Right-click each storage group object you are including in this job and select **Agent Option** to select backup options. For more information about restore options, see Database Level Restore Options.

6. Click the Destination tab. You can restore the database objects to their original location (default) or you can restore the database objects to an alternative location.

   Note: For Exchange Server 2003, you can select to restore to the Recovery Storage Group, a specialized storage group you can use in addition to the regular storage groups in Exchange Server. For more information on the Recovery Storage Group, see your Exchange Server documentation.

7. If you want to restore to an alternative location and have the BrightStor ARCserve Backup Agent for Windows installed, clear the **Restore files to their original locations** check box, expand the Windows NT/2000/XP Systems object, expand the server you want to restore to, and select the Microsoft Exchange Server – Database Level (IS) object. If you want to restore to an alternative location and do not have the BrightStor ARCserve Backup Agent for Windows installed, clear the **Restore files to their original locations** check box, expand the Microsoft Windows Network object, expand the appropriate domain, expand the server you want to restore to, and select the Microsoft Exchange Server – Database Level (IS) object.

   Note: For information about restoring to an alternative location, see the *Disaster Recovery for Microsoft Exchange 2000 Server* and *Disaster Recovery for Microsoft Exchange 2003 Server* white papers on the Microsoft web site.

8. Click Start.

9. If you are restoring to an alternative location, when the Security dialog appears, enter the user name and password for the destination server and click OK.

10. When the Session User Name and Password dialog opens, verify or change the user name and password for the destination Exchange Server. To change the user name or password, select the session, click Edit, make your changes, and then click OK.

    Note: The user name must be entered in the following format:

    `DOMAIN\USERNAME`

11. Click OK.

12. When the Submit Job dialog opens, select **Run Now** to run the job immediately, or select **Run On** and select a future date and time when you want the job to run.

13. Enter a description for your job and click OK.

Perform a Database Level Test Restore to an Alternative Location

You should perform a test restore to a backup server at least **once a month** and make sure the restored database is functioning properly. This lets you test your backup and restore strategies to assess whether you are backing up your system accurately and to prepare for a possible disaster.

Before you can restore an Exchange Server database backup to an alternative location, you must ensure that the server you are restoring to is configured exactly the same as the original server you backed up from. To determine what needs to be identical, use the worksheet in the appendix "Server Configuration Worksheet." Information in all fields in this worksheet except the Server Name field must be the same on the server you are restoring to.

To perform a test restore to an alternative location:

1. Ensure that the test server you are restoring to meets the following criteria:

   ■ Microsoft Exchange is installed and is configured exactly the same as the original server you backed up from.

   ■ BrightStor ARCserve Backup and the agent are installed.

   ■ The server is in a different domain than the domain of the server you backed up from and it has its own Active Directory.

2. Open the Restore Manager, right-click the session you want to restore and click OK.

3. Click the Destination tab and disable the Restore files to their original location(s) option.

4. Expand the server object for your test server and select the Microsoft Exchange Server – Database Level(IS) object.

5. Click Start.

Note: For information about restoring to an alternative location, see the *Disaster Recovery for Microsoft Exchange 2000 Server* or *Microsoft Exchange 2003 Server Disaster Recovery* white paper on the Microsoft web site.

Access an Individual Mailbox from a Database Level Test Restore

If you do not perform a Document Level or Brick Level backup in addition to your Database Level backup and need to restore an individual mailbox, do the following:

1. Follow the above procedure for performing a test restore to an alternative location.

2. Open the Exchange System Manager, expand the Mailbox Store, right-click the Mailboxes object and select Run Cleanup Agent. Because the new domain's Active Directory does not contain the same users as the original domain, mailboxes appear as disconnected.

3. Open the Active Directory Users and Computers dialog and create a new account to attach the mailbox to. While creating the new account, disable the Create an Exchange mailbox option because you must connect the user to the restored mailbox rather than a new mailbox.

4. In the Exchange System Manager, right-click the name of the disabled mailbox, select Reconnect, and then select the appropriate domain account to link with the mailbox. This connects the mailbox to the user.

5. When the Reconnect dialog opens, click OK.

6. When the warning replication message appears, click OK.

After you connect the mailbox to the user, the information replicates and the restore mailbox is available in the new domain.

Database Level Disaster Recovery

If a disaster occurs, you must perform the following steps to restore the Exchange Server:

■ For information about disaster recovery, see the *Disaster Recovery for Microsoft Exchange 2000 Server* and *Disaster Recovery for Microsoft Exchange 2003 Server* white papers on the Microsoft web site.

■ Restore the operating system on your Exchange Server and your domain controller and ensure that the System State with Active Directory is in a consistent state with the backup you intend to restore. The BrightStor ARCserve Backup Disaster Recovery Option provides an automated and efficient way for you to complete these tasks. For more information, see the *Disaster Recovery Option Guide*.

■ Ensure that the Exchange Server application is operational and that you have the same Service Pack you had prior to the disaster.

■ Restore the databases to the Exchange Server. For instructions on how to restore the databases to the Exchange Server, see Perform a Database Level Restore.

Database Level Backup and Restore for Exchange Server 5.5

The following sections describe how to use Database Level backup and restore for Exchange Server 5.5.

Database Level Views in the Backup Manager

Depending on your configuration, Microsoft Exchange Server – Database Level appears in the Backup Manager under the following objects:

- Windows NT/2000/XP/2003 Systems

- Preferred Shares/Machines

- Exchange Organization

When you expand the Database Level(IS) object, you can view your local and remote Exchange servers. When you expand a server, you can view the databases and their components that you can protect using Database Level backup and restore:

When you select Directory and Information Store, the following files are backed up:

Exchange Server Database	Online files	Directory
DIR.EDB, DIR.PAT, EDBXXXXX.LOG	Information Store	PRIV.EDB, PRIV.PAT, PUB.EDB, PUB.PAT, EDBXXXXX.LOG

Note: The actual files that are backed up depend on the type of backup option you select. For more information, see the Database Level Backup Methods.

Backup Agent Service Account Requirements for Database Level Backup and Restore

To perform a Database Level backup and restore job, your backup agent service account must be a member of the following groups on the Exchange Server:

- Administrators
- Backup Operators

Database Level Backup Features

The following sections include information on the features that the agent offers when backing up using Database Level and the procedure for how to perform a backup using Database Level.

Database Level Backup Methods

When you submit a backup job, you must select a backup method. The backup method tells BrightStor ARCserve Backup how you want your data to be backed up. When you use the agent, you can select a backup method for your Database Level backup job at the Directory and Information Store level or you can use a globally scheduled backup method.

To select a backup method at the Directory and Information Store level, explicitly select the Directory or Information Store's parent database object, right-click the Directory or Information Store object, and select **Agent Option**:

For more information on explicit job packaging, see *Getting Started*.

The following dialog opens:
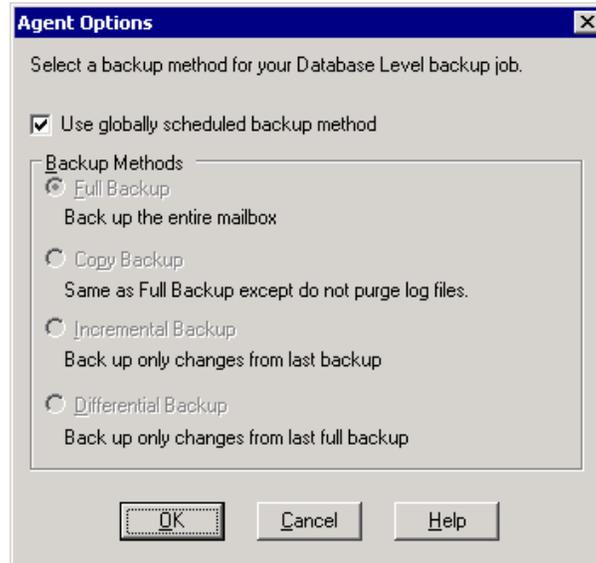
The advantage of selecting a backup method at the Directory and Information Store level is that it gives you the flexibility to use a different method for each database. You can select from the following backup methods:

- **Use globally scheduled backup method**—Enabled by default. You must disable this option if you want to set a backup method at the storage group level. If you do not disable this, you must select a backup method on the Schedule tab.

  Note: If you do not disable this and select Custom Schedule on the Schedule tab, there is no difference between the full (Keep Archive Bit) and full (Clear Archive Bit) backup methods; they both function as full.

- **Full Backup**—This is the default. It backs up the entire database, including the log files, and marks all of the files that have been backed up in preparation for a subsequent incremental or differential backup. The log files are also truncated during a full backup. The backup operation then purges the committed log files it no longer needs from the Exchange Server. While the backup is taking place, new database changes can occur, so a patch file (.*pat*) is created to log these late changes. The patch file is backed up at the end of the process along with the log files. These backed up .pat files are restored automatically with the log files.

  Note: Always perform a full backup when running the agent for the first time, after upgrading to a Service Pack, and after performing a restore.

- **Copy Backup**—Backs up the entire database, including the log files, but does not mark the files as having been backed up. Use a copy backup if you want to make a full Backup of your data but do not want to disrupt any existing incremental or differential backups.

  Note: The log files are not truncated during a copy backup.

■ **Incremental Backup**—Backs up the log files that have changed since the last full or incremental Backup and marks them as backed up. The log files are also truncated. When restored, the log files are applied to recreate the database at the time of backup.

Note: Microsoft does not support incremental backups when the Circular Logging feature is enabled. If you do not disable Circular Logging and submit an incremental backup, the agent automatically converts the backup to full.

■ **Differential Backup**—Backs up the log files that have changed since the last backup. The log files are not truncated. It does not however mark them as backed up. When restored, the log files are applied to recreate the database at the time of backup.

Note: Microsoft does not support differential backups when the Circular Logging feature is enabled. If you do not disable Circular Logging and submit a differential backup, the agent automatically converts the backup to full.

Perform a Database Level Backup

Before you submit a Database Level backup job, make sure that the Exchange Server databases are mounted on your server and that the Backup Agent RPC service is started.

To back up an Exchange Server database:

1. From the BrightStor ARCserve Backup Home Page, select the Backup Manager from the Quick Start menu.

2. When the Backup Manager appears, select the Database Level objects you want to back up.

   Note: You should back up the Directory and Information Store of a database at the same time. However, even though you are backing up all components at the same time, you can restore each component separately.

3. Right-click the Database Level object you selected to back up and select **Remote Protocol**.

4. When the Remote Protocol dialog appears, select one of the following remote protocols to use for the job, and then click OK:

   ■ **TCP/IP**—The default. Establishes a connection using sockets over TCP/IP. To configure what port socket uses, see Configure Database Level and Brick Level Backup and Restore in the chapter "Installing the Agent."

   ■ **VI (Virtual Interfaces)**—Works with specific VI hardware environments.

   ■ **Named Pipes**—An alternative transport protocol used for legacy support.

   Note: By default, the BrightStor ARCserve Backup Agent for Microsoft Exchange uses the TCP/IP protocol when performing backups. If a problem occurs with this protocol, it automatically fails over to the Named Pipes protocol.

5. If you are not planning to schedule your job to use a rotation scheme, right-click Directory and Information Store and select **Agent Option** to select a backup method to use. If you do this, the database parent object must be explicitly selected. For more information, see Database Level Backup Methods.

   Note: Always perform a full backup when running the BrightStor ARCserve Backup Agent for Microsoft Exchange for the first time. This allows you to store a complete set of Exchange Server databases.

6. If you want to enable CRC checking so that you can verify the integrity of your data using the Scan utility after the backup job is performed, click the Options button, click the Operation tab, enable the **Calculate and Store CRC Value on Backup Media** option, and then click OK.

   Note: For more information on CRC checking and using the Scan utility, see Database Level Scan Media Options.

7. Click the Destination tab and select a backup destination.

8. Click the Schedule tab. If you want to use a Custom Schedule, select a Repeat Method. If you want to use a rotation scheme, select the **Use Rotation Scheme** option and set up your scheme. For more information on scheduling jobs and rotation schemes, see the online help and *Administrator Guide*.

   Note: If you use a Custom Schedule, the Backup Method section on the Schedule tab does not apply. For more information, see Database Level Backup Methods.

9. Click Start.

10. When the Security and Agent Information dialog appears, make sure that the correct User Name and Password are filled in for each object. If you need to enter or modify a User Name or Password, click the Security button, make your changes, and then click OK.

    Note: The security for a Database Level backup is determined from the security supplied for the server listed in the Object column. The security on that server must be a part of the Administrators and Backup Operators groups.

11. Click OK.

12. When the Submit Job dialog opens, select **Run Now** to run the job immediately, or select **Run On** and select a future date and time when you want the job to run.

13. Enter a description for your job.

14. If you selected multiple sources to back up and want to set the priority in which the job sessions initiate, click Source Priority. Use the Top, Up, Down, and Bottom buttons to change the order in which the jobs are processed. When you finish setting priorities, click OK.

15. On the Submit Job page, click OK to submit your job.

Database Level Backup Scan Utility

After you back up your Exchange Server database, you can use the BrightStor ARCserve Backup Scan utility to find out what is on your media, to view information about your media backup sessions, and, if you enabled **CRC checking during backup**, to verify the integrity of the data that was written to the media.

Note: For more information on how to enable CRC checking during backup, see Perform a Database Level Backup.

Each source that you select to back up is saved on media as an individual session. You can scan a single session or an entire media. To view the results of the Scan job in the Job Queue, click the Log tab.

Use the Log tab in the Options dialog to select the level of detail you see in the Job Queue Log. You can select to see just summary information and any errors that occurred during the scan or you can select to see each file that was backed up, summary information, and any errors that may have occurred.

Database Level Scan Media Options

If you enable CRC checking during backup, the following scan media options apply to your Exchange Server backup job.

On the Operation tab, enable **Calculate and Store CRC Value on Backup Media** if you want to scan files with a CRC check to verify the integrity of the data that was written to the media.

On the Job Log tab, select the level of detail you want to include in the log report:

- **Log All Activity—**Record all of the activity that occurs while the job is running in the Job Log.

- **Log Summary Only—**Record summary information of the job (including source, destination, session number, and totals) and errors.

- **Log Disabled—**Do not record any information about this job in the Job Log.

Note: You can view the log report in the Job Queue or Database Manager (Job Records).

Perform Media Scan

To scan media:

1. Open the Scan utility.

2. Select the media you want to scan. If the media you want to scan is not currently in a storage device, you must enter the information into the Group and Media fields.

3. Enter a specific session to scan or select to scan all sessions on the media.

4. Click Options to specify scan options for the job.

   Note: If you enabled **CRC checking during backup**, you must enable the **Calculate and Store CRC Value on Backup Media** option if you want to verify the integrity of the data.

5. Click Filter to specify filters for the job.

6. Click Start to submit the job.

Database Level Data Restore

The following sections include information on the prerequisites you must meet before you perform a restore, the features that the BrightStor ARCserve Backup Agent for Microsoft Exchange offers when restoring from a Database Level backup, and the procedure for how to perform a restore.

Database Level Restore Prerequisites

Before you restore, you must satisfy the following prerequisites:

- Ensure that the agent is installed on the same machine that has the Exchange Server installed and that the Backup Agent RPC Server service is running.

- Ensure that the server you are restoring to is configured exactly the same as the configuration of the original server you backed up from. If you are restoring to the original location, the configuration is typically the same. Otherwise, for more information on restoring to an alterative location, see the *Microsoft Exchange 5.5 Disaster Recovery* white paper on the Microsoft web site.

Database Level Restore Sets

When you back up an Exchange Server, the Directory and Information Store that you select to back up are saved on media as an individual session. To restore an Exchange Server, you must restore all of the sessions that, when combined, completely restore the Directory and Information Store. These sessions are called your restore set.

The number of sessions in your restore set depends on the backup methods you used:

- If you backed up your Directory or Information Store using only the full backup method, your restore set includes only this full session.

- If you backed up your Directory or Information Store using both full and incremental backups, your restore set includes your full session and at least one, but up to as many incremental sessions as you want to include. For example, in the following backup scenario, your restore set can be full and incremental 1, full and incremental 1 and 2, full and incremental 1, 2, and 3, or full and incremental 1, 2, 3, and 4:

Full	Incremental 1	Incremental 2	Incremental 3	Incremental 4

- If you backed up your Directory or Information Store using both full and differential backups, your restore set includes your full session and one differential session. For example, in the following backup scenario, your restore set can be full and differential 1, full and differential 2, full and differential 3, or full and differential 4:

Full	Differential 1	Differential 2	Differential 3	Differential 4

After you determine your restore set, you must make sure that you select the entire set when submitting your restore job. If you use the Restore by Tree method when scheduling your restore job, the agent simplifies this task for you. When using Restore by Tree, all you must do is select the last incremental or differential session in your restore set and the agent will automatically include the full session for you.

To select your restore set in the Restore Manager:

1. From the BrightStor ARCserve Backup Home Page, select the Restore Manager from the Quick Start menu.

2. When the Restore Manager opens, select **Restore by Tree** in the drop-down box underneath the Source tab.

3. Expand the server that has the Directory or Information Store you backed up and select the Directory or Information Store object.

4. Click Version History.
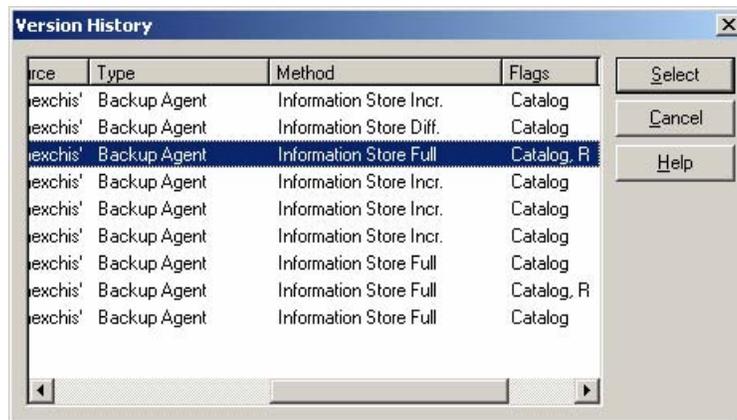
5. When the Version History dialog opens, highlight a session in your restore set and click Select. If your restore set includes incrementals and differentials, simply select the last incremental or differential in the set and the agent will automatically include the full backup for you (applies to Restore by Tree only).

6. The most recent backups are displayed at the top of the Version History dialog.

7. Set your restore options, select a destination, and submit the job.

   Note: If you use Restore by Session rather than Restore by Tree, you must repeat steps 1 to 6 for each session in your restore set.

Database Level Restore Options

When you create a restore job, you can choose restore options to customize the job:
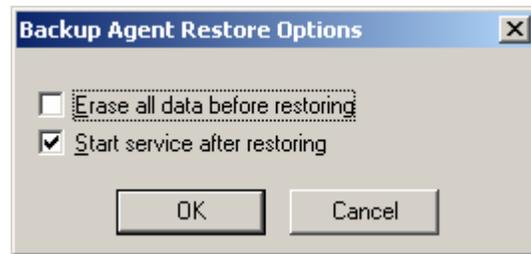
The agent offers the following options for restoring Exchange Server databases:

- **Erase all data before restoring**—Erases all the data in the database. Use this option when you are restoring to an alternative location or when you want to delete database information on the hard disk. This is useful if you are low on hard disk space or if your database was corrupted.

  Note: This option does not apply if you are restoring only the Private Information Store or only the Public Information Store.

- **Start service after restoring**—Use this to automatically start the Information Store or Directory Services after the restore job finishes. When restoring a restore set, use this option only on the last session in the set. For more information on restore sets, see Database Level Restore Sets.

Perform a Database Level Restore

To restore an Exchange Server database:

1. From the BrightStor ARCserve Backup Home Page, select the Restore Manager from the Quick Start menu.

2. When the Restore Manager opens, select **Restore by Tree** in the drop-down box underneath the Source tab.

   Note: Both Restore by Tree and Restore by Session are supported for Database Level restore.

3. If the backup you want to restore is local, expand the Server object, expand the server that has the database you backed up, and select the database object. If the backup you want to restore is remote, expand the Microsoft Windows Network object, expand the server that has the database you backed up, and select Directory, Information Store, or both. If you select Information Store, you can select the Public Information Store, Private Information Store, or both in the right-hand pane.

   Note: You can see Private and Public folders only if you are restoring from a backup session that used the full or copy backup method for the Information Store.

4. If the most recent backup is not the backup you want to restore, click Version History, select the version you want to restore, and click Select.

   Note: If you are using a restore set, you must restore the entire set in the order that it was backed up. If your restore set includes incrementals and differentials, simply select the last incremental or differential in the set and the agent will automatically include the full backup for you (applies to Restore by Tree only). For more information on restore sets, see Database Level Restore Sets.

5. Right-click the Directory and Information Store objects you are including in this job and select **Agent Option** to select backup options. For more information or restore options, see Database Level Restore Options.

6. Click the Destination tab. You can restore the database objects to their original location (default) or you can restore the database objects to an alternative location.

7. If you want to restore to an alternative location and have the BrightStor ARCserve Backup Agent for Windows installed, clear the **Restore files to their original locations** check box, expand the Windows NT/2000/XP Systems object, expand the server you want to restore to, and select the Microsoft Exchange Server – Database Level (IS) object. If you want to restore to an alternative location and do not have the BrightStor ARCserve Backup Agent for Windows installed, clear the **Restore files to their original locations** check box, expand the Microsoft Windows Network object, expand the appropriate domain, expand the server you want to restore to, and select the Microsoft Exchange Server – Database Level (IS) object.

   Note: For information on restoring to an alternative location, see the *Microsoft Exchange 5.5 Disaster Recovery* white paper on the Microsoft web site.

8. Click Start.

9. If you are restoring to an alternative location, when the Security dialog appears, enter the user name and password for the destination server and click OK

10. When the Session User Name and Password dialog appears, verify or change the user name and password for the destination Exchange Server. To change the user name or password, select the session, click Edit, make your changes, and then click OK.

    Note: The user name must be entered in the following format:

    `DOMAIN\USERNAME`

11. Click OK.

12. When the Submit Job dialog opens, select **Run Now** to run the job immediately, or select **Run On** and select a future date and time when you want the job to run.

13. Enter a description for your job and click OK.

    Note: The agent automatically stops the appropriate Exchange Server Services before the restore job begins. If you did not enable the **Start Service After Restore** backup option, you must manually restart services after your restore job completes.

Database Level Disaster Recovery

If a disaster occurs, you must perform the following steps to restore the Exchange Server:

- Read the *Microsoft Exchange 5.5 Disaster Recovery* white paper on the Microsoft web site.

- Ensure that the your operating system and Exchange Server application is operational and that you have the same Service Pack you had prior to the disaster. The BrightStor ARCserve Backup Disaster Recovery Option provides an automated and efficient way for you to complete these tasks. For more information, see the *Disaster Recovery Option Guide*.

■ Restore the databases to the Exchange Server. For instructions on how to restore the database to the Exchange Server, see Perform a Database Level Restore.

Note: After restoring an Exchange Server 5.5 database, you may need to perform a Directory or Information Store consistency adjustment to completely restore your database information. The Directory or Information Store consistency adjuster is used in disaster recovery scenarios where you cannot restore the directory to the recovery computer, or where the Information Store is copied to a recovery computer with a name that is different from that of the original server. For information on performing a consistency adjustment, see the white papers on the Microsoft web site.

Chapter 4: Performing Document Level Backups and Restores

Document Level backup and restore is available only if you install the BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on and should be used in place of Brick Level backup and restore.

Document Level backup is the most powerful and flexible backup type. It offers advanced configuration options, performs folder level backups and message level restores, and supports advanced filtering during backup. It also maximizes performance and flexibility by supporting complete messaging single instance storage (SIS), multi-threading, and by offering the most granular level of restore. You should use Document Level backup and restore when you want the flexibility to restore individual objects, such as a mailbox, folder, or even a single message. Document Level backup and restore can also be used to simplify many administrative tasks, such as auditing, migration, pruning, and aging. Using Document Level backup and restore, you can back up many messaging objects including posts, tasks, notes, journal entries, mail messages, events, appointments, meeting requests, and contacts.

Document Level Backup and Restore Benefits

Document Level backup and restore offers many benefits, including:

- **Complete Messaging Single Instance Storage**—Traditional Brick Level backups scan an Exchange Server mailbox-by-mailbox. They back up copies of individual message bodies and attachments as they arrive, without any regard for data that may have been backed up already and without accounting for the Exchange Server's ability to store only one copy of an attachment when it is sent to multiple people. This results in decreased speed and performance.

  Document Level backup and restore solves this problem by providing **complete** single instance storage backups of attachments and message bodies. Document level backup checks to see whether each attachment and message body has already been backed up and backs up only one copy.

- **Push Agent Technology**—Document Level backup uses push agent technology to increase the efficiency of your backup jobs by processing the data at the remote client workstations rather than processing it all from the BrightStor ARCserve Backup host server. This off loads the system resources from the BrightStor ARCserve Backup host server and minimizes network traffic.

  Push agent technology operates on a "per job" request, which means the host server sends an entire list of files to the remote client at one time. The push agent then enables the remote client to take an active role in the process by pushing all of the requested files to the host server. (Without push agent technology, backup jobs for remote clients operate on a series of "per file" requests—the host server has to request files from the remote client one file at a time.)

- **Multi-threading—**Document Level backup lets you take advantage of the full capacity of multi CPU machines capable of concurrent operations. It does this by supporting up to 64 threads per storage group and an additional 64 threads in the public folder store for a maximum of 320 threads. This lets you make the most of your resources and increases performance. For information on how to configure the multi-threading settings number of threads and thread priority, see Configure the Add-on in the chapter "Installing the Agent."

- **Multi-streaming Support—**Document Level backup lets you take advantage of the full capacity of multiple drives and high-speed RAID arrays capable of fast concurrent backups to multiple tapes. It does this by partitioning information into concurrent streams for parallel backups.

- **Document Level Restore—**Document Level restore lets you select a storage group, mailbox, folder, or even a particular document for restore.

- **Migration Support—**Document Level backup lets you seamlessly back up and restore documents, folders, and mailboxes between different versions of Exchange Server, including Exchange Server 5.5, 2000, and 2003. For more information about the guidelines on how you can restore from different versions of Exchange Server, see Document Level Restore Locations in this chapter.

- **Enhanced Cluster Support—** Document Level backup offers Active/Active and Active/Passive cluster support with cross cluster node failover. For more information about installing the add-on on a cluster, see Install the Add-on on a Cluster in the chapter "Installing the Agent."

- **Job Continuation—**If a job fails to complete, under certain circumstances, Document Level backup can automatically continue where the first job left off. For information on how to configure job continuation, see Configure the Add-on in the chapter "Installing the Agent."

Document Level Views in the Backup Manager

For Exchange Server 2000 and 2003, depending on your configuration, Microsoft Exchange Server – Document Level appears in the Backup Manager under the following objects:

- Windows NT/2000/XP/2003 Systems

- Exchange Organization

When you expand the Document Level object, you can view its storage groups. Each server includes up to five storage groups. For Document Level backup and restore, Public Folders is treated as a storage group.

When you expand a storage group you can view its containing folders:
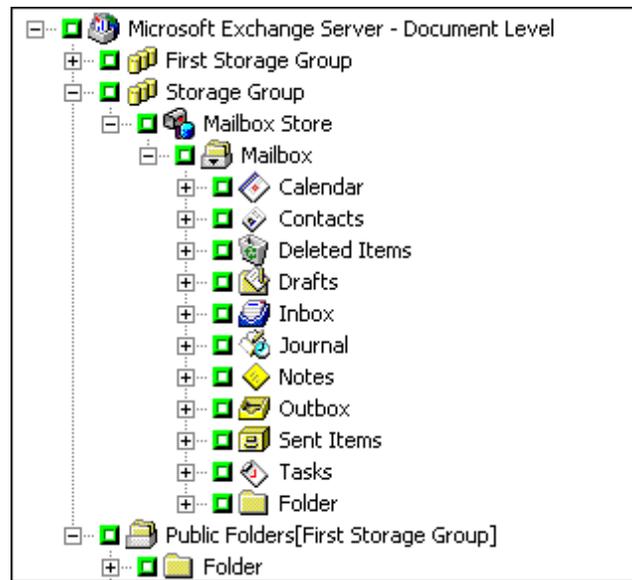
Note: If a mailbox or folder has the character "\" in its name, the character is substituted with another character in the Backup Manager for display purposes only (restored data will have the "\" character). For example, a folder named a\b\c is displayed as follows:

For Exchange Server 5.5, Microsoft Exchange Server – Document Level appears in the Backup Manager under the Windows NT/2000/XP/2003 Systems object and Exchange Organization object, depending on your configuration. When you expand the Document Level object, you can view Individual Mailboxes and Public Folders. When you expand a mailbox or a public folder, you can view its containing folders:
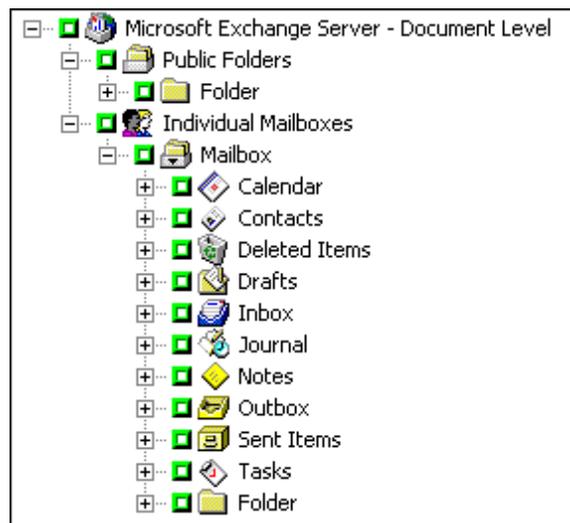
Note: In a cluster environment, Exchange servers appear under the Exchange virtual server objects.

Backup Agent Service Account Requirements for Document Level Backup and Restore

To perform a Document Level backup and restore job, your backup agent service account must meet the following criteria on the Exchange Server:

- It must be a domain account.

- There must be a mailbox on the Exchange Server to which you plan to back up or restore to. This mailbox must be operational, initialized, and must have the same name as the backup agent service account.

  Note: For Exchange Server 5.5, ensure that the Windows account name is the same name as the mailbox display name

- It must be a member of the Administrator group.

- It must be a member of the Backup Operators group.

- It must be assigned the Exchange Full Administrator Role.

- It must be assigned the Exchange Server MAPI Owner role on every public folder you intend to back up and restore because permissions for public folders can vary. If a lower permission level is assigned, back up or restore may fail or duplicate items may be restored because the backup agent service account does not have the permission to delete original documents. To assign this role, open the Exchange System Manager, right-click the public folder you want to back up or restore, and select Properties. When the Properties dialog opens, click the Permissions tab, click the Client permissions button, either add a new client with the Owner role or modify an existing client to assign the Owner role, and then click OK.

Document Level Backup Features

The following sections describe the features that are available when using Document Level backup and restore and describes how to perform a Document Level backup and restore.

Complete Messaging Single Instance Storage

To maximize performance during backup, enable the option: **Complete Messaging Single Instance Storage**. If you enable this, the add-on checks to see if attachments and messages have already been backed up and then backs up only one copy. This eliminates the need to back up each time the attachment and message are referenced and can significantly decrease the size of your backups. For information on how to enable Complete Single Instance Storage, see Configure the Add-on in the chapter "Installing the Agent."

Browsing Filter

To minimize the amount of time it may take and the impact on system resources when browsing extremely large amounts of data, Document Level backup includes a browsing filter that lets you reduce the number of items you want to search through.

Filter Criteria

The criteria you enter can be any combination of letters and numbers, with or without a wildcard at the end. If you do not enter a wildcard, the add-on performs a substring search and finds all folders that have the criteria you entered somewhere in the file name. For example, if you enter "min", all folders that contain the letters "min" somewhere in the file name are displayed, such as "Minutes", "Administrator", and "Admin". If you enter a wildcard at the end of your criteria, the add-on performs a prefix string search and finds only the folders that have the criteria you entered as the prefix of the file name. For example, if you enter "Admin*", only the files that begin with "Admin" are displayed, such as "Administrator" and "Admin26".
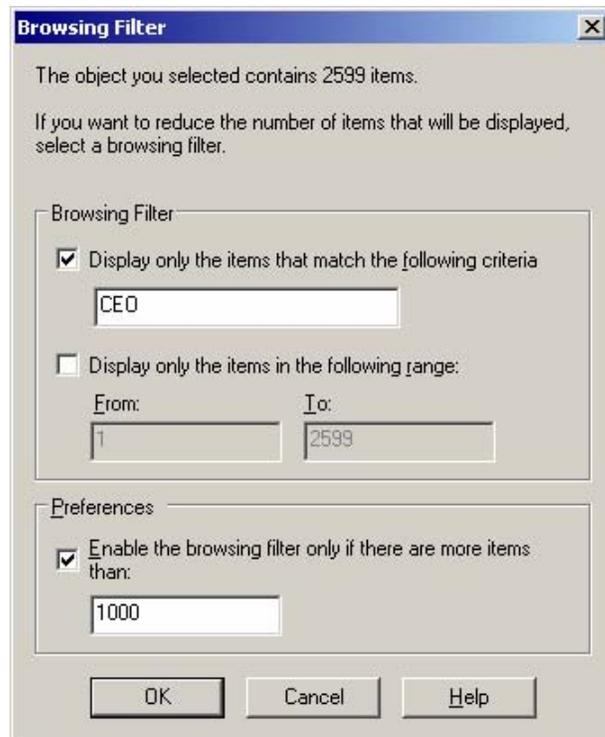
You can select from the following filters:

- **Display the items that match the following pattern—**Enable this to only display the items that match the criteria you specify.

- **Display the items in the following range—**Enable this to select a numeric range of items to be returned.

- **Enable the browsing filter only if there are more items than—**The browsing filter is automatically displayed when there are more than 500 items. Enter a new number in this field if you want to adjust this numeric threshold.

   Note: You can also adjust the numeric threshold by creating a value under the following registry key:

```
HKEY_CURRENT_USER\Software\ComputerAssociates\BrightStor ARCserve
Backup\Base\ASMgr\DBAEXSIS
Value Name:        MaxItemsDisplayed
Value Type:REG_DWORD
Value Data (Base Decimal):Desired threshold
```

Document Level Backup Methods

When you submit a backup job, you must select a backup method. The backup method tells BrightStor ARCserve Backup how you want your data to be backed up. When you use the add-on, you can select a backup method for your Document Level backup job at the Microsoft Exchange Server – Document Level or you can use a globally scheduled backup method.

Note: If you want to perform a Document Level backup job and include disaster recovery information, you must submit both a whole node backup job to generate the disaster recovery information and a separate Document Level backup job.

To select a backup method at the Document Level, right-click Microsoft Exchange Server – Document Level and select **Agent Options**:
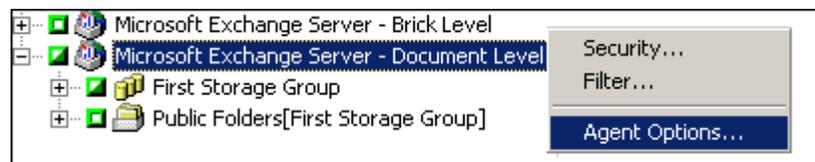
The following dialog opens:
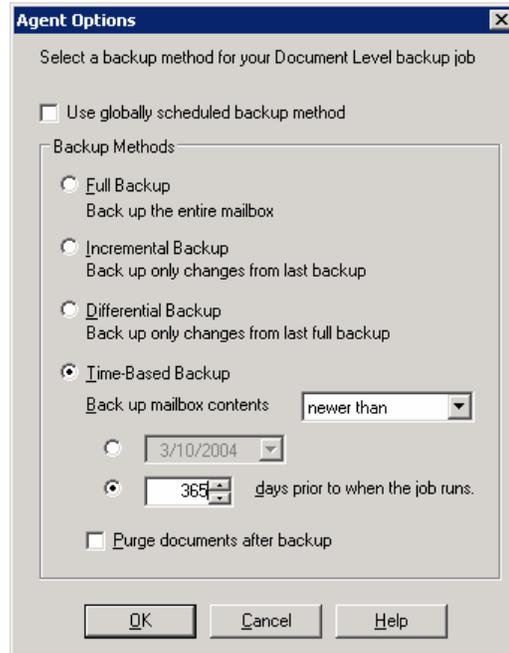
The advantage of selecting a backup method at the Document Level is that it gives you the flexibility to use a separate method for the Document Level backup portion of your job. You can select from the following backup methods:

■ **Use globally scheduled backup method**—Enabled by default. You must disable this option if you want to set a backup method at the Document Level. If you do not disable this, you must select a backup method on the Schedule tab.

Note: If you do not disable this and select Custom Schedule on the Schedule tab, there is no difference between the full (Keep Archive Bit) and full (Clear Archive Bit) backup methods, they both function as full.

■ **Full Backup**—Backs up all documents.

■ **Incremental Backup**—Backs up all documents created or modified since the last full or incremental backup. If no full backup has been performed, all documents are backed up.

■ **Differential Backup**— Backs up all documents created or modified since the last full backup. If no full backup has been performed, all documents are backed up.

■ **Time-Based Backup**— Backs up all documents newer than or older than a certain point in time. This point in time can either be a specific date or a number of days prior to when the job runs. If you select a number of days prior to when the job runs, the backup period is a moving window that stays relative to the time at which the job runs.

Note: If you select a specific date, 12:00 AM is the default time used and BrightStor ARCserve Backup automatically adjusts for daylight savings and if there is a time zone difference between the server that is running the BrightStor ARCserve Backup Manager and the server that has the add on installed. If you select the number of days prior to when the job runs, the exact time the job runs is the default time used.

– **Purge documents after backup—**Automatically deletes documents after they are backed up. This is useful for pruning and aging an Exchange Server. For example, you can use this option to back up and delete documents older than three years, thus reducing the size of your Exchange Server.

Important! *This option should be used with caution since it will delete all documents that were backed up.*

As an additional safety feature, you can prevent an agent from pruning an Exchange Server by enabling the Disable Purge Option. For more information on this option, see Configure the Add-on in the chapter "Installing the Agent."

Document Level Backup Filters

Document Level backup includes backup filters that give you the flexibility to exclude specific mailboxes, folders, or attachments from your backup job. In addition, you can set default filters, which is useful if you consistently use the same filters and do not want to have to set them every time you run a Document Level backup job.

To select a backup filter, right-click Microsoft Exchange Server – Document Level and select **Filter**:
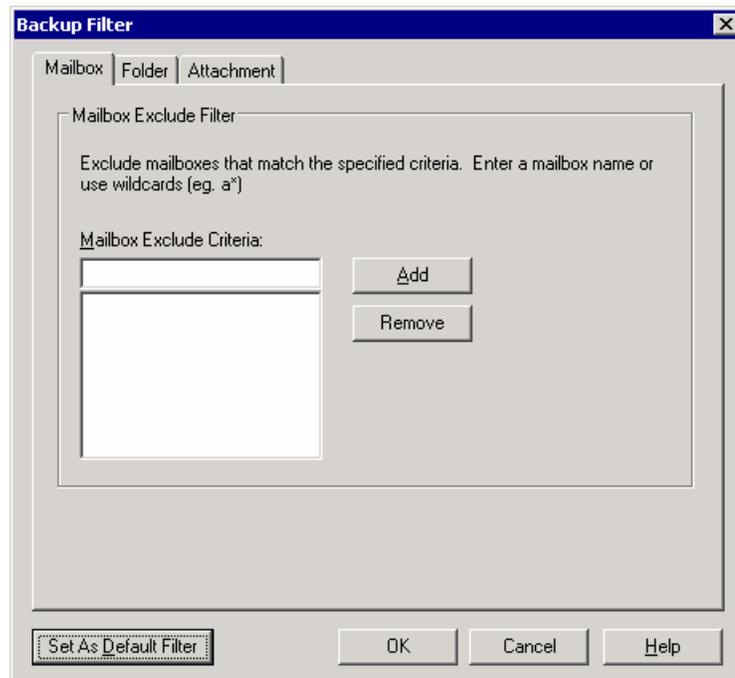
■ **On the Mailbox tab**—In the Mailbox Exclude Criteria field, enter the name of the mailbox that you want to exclude or the criteria that you want the add-on to use to exclude certain mailboxes, and then click Add. For information about filtering criteria, see Filter Criteria.
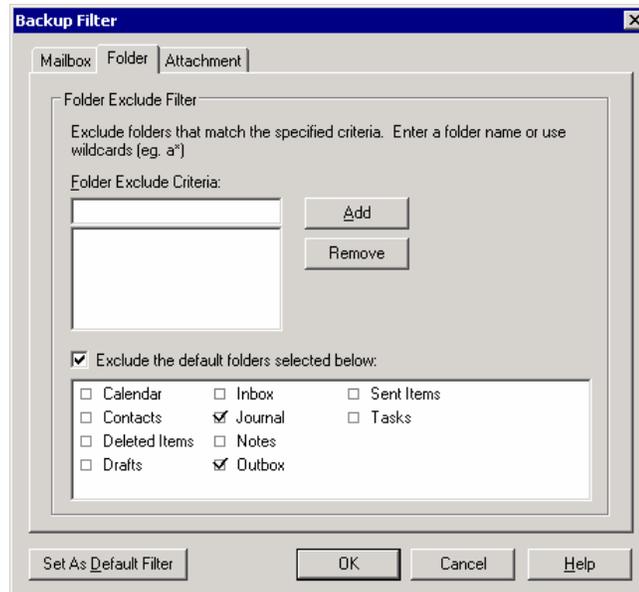
- **On the Folder tab**—In the Folder Exclude Criteria field, enter the name of the folder that you want to exclude or the criteria that you want the add-on to use to exclude certain folders, and then click Add. For information about filtering criteria, see Filter Criteria.

  If you want to exclude default folders, enable the Exclude the Default Folders selected below option and place a check mark next to the particular folder you want to exclude.
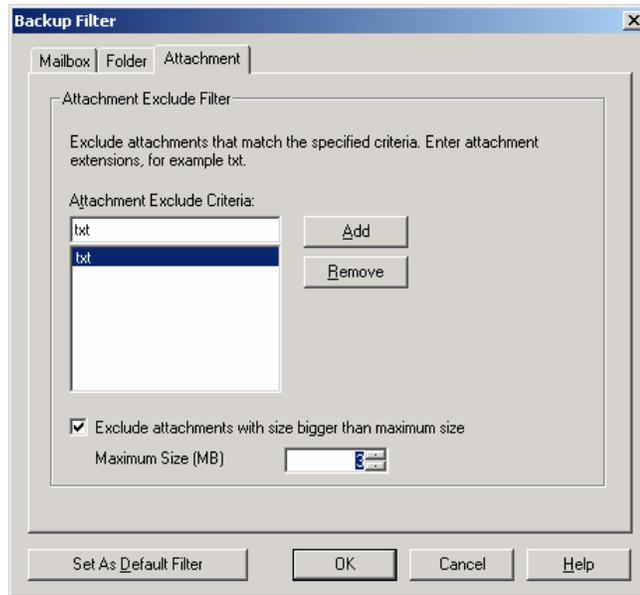
- **On the Attachment tab**—In the Attachment Exclude Criteria field, enter the extension type of the attachments that you want to exclude, and then click Add. For example, if you want to exclude text file attachments, enter **txt** and click Add.

  If you want to exclude attachments that exceed a certain size limit, enable the Exclude attachments with size bigger than maximum size option and select the maximum size. When selecting the maximum size, allow a small margin of leeway since the size displayed by some email clients may slightly differ from the size read from the Exchange Server.

  Note: The settings on the Attachment tab do not apply to embedded messages.

Document Level Compression and Encryption Options

To increase data speed and the effectiveness of your media, and to enhance network security, document level backup supports the BrightStor ARCserve Backup compression and encryption global options.

If you want your document level data to be compressed or encrypted before sending it to the backup server, enable the **Compress Files Before Backup** and **Encrypt File Before Backup** options, and then enter the password for the encryption in the Session/Encryption Password field.
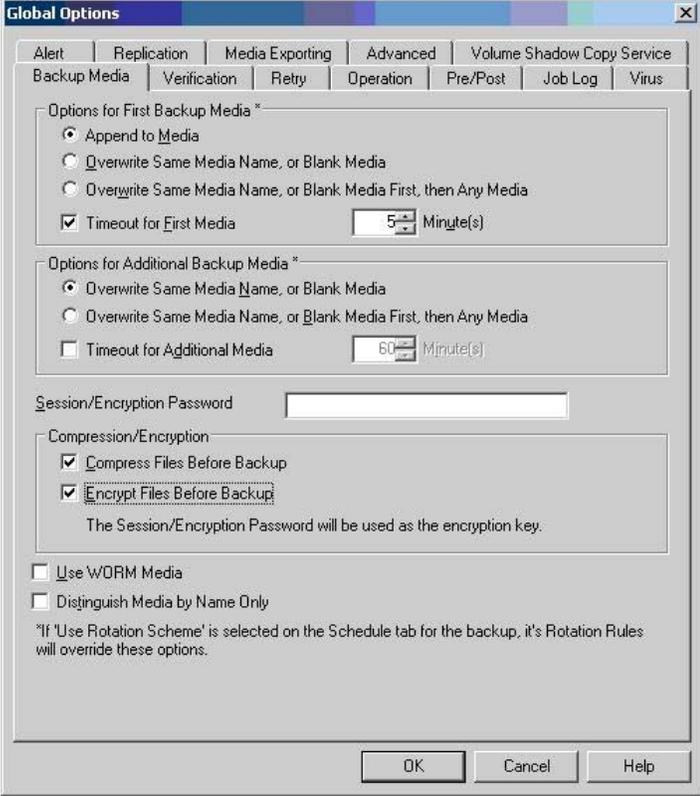
Multiplexing During Document Level Backups

Multiplexing is a process in which data from multiple sources is written to the same media simultaneously. When a job that has multiple sources is submitted with the multiplexing option enabled, it is broken into child jobs—one for each storage group. These child jobs write data to the same media simultaneously. If you enable multiplexing, Document Level backups from one or more storage groups on one or more machines can be backed up simultaneously in a single job to one device.

For more information on multiplexing, see the *Administrator Guide*.

Multi Stream Option

If your BrightStor ARCserve Backup server is equipped with multiple devices in two or more groups or multiple devices in one or more groups with the BrightStor ARCserve Backup Enterprise Module and BrightStor ARCserve Backup Tape Library Option installed, you can take advantage of the Multi Stream option. This option divides your backup jobs into several sub-jobs that run simultaneously to different devices. You can have as many jobs running simultaneously as you have devices or groups on your system. Document Level backup provides one to five streams for simultaneous backup (for Exchange Server 5.5, only two streams are supported). The available number of tapes, drives, and storage groups determines the number of streams that are run simultaneously during backup. You can enable the Multi Stream option on the Destination tab in the Backup Manager:
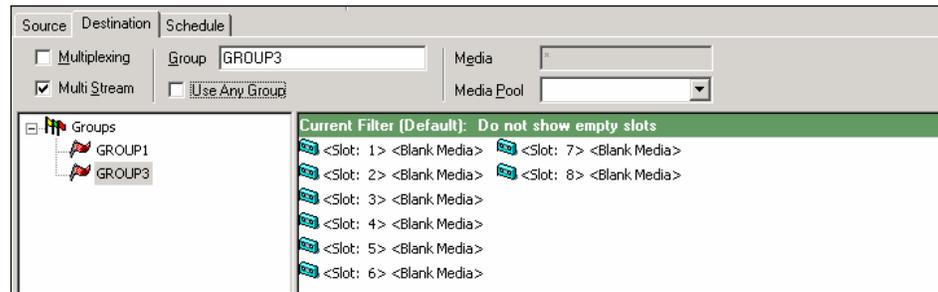
For more information on the Multi Stream option, see the *Administrator Guide*.

Note: If you enable the Multi Stream option when you submit a local or remote Document Level backup job, the data is multi-streamed at the storage group level. For example, if your Exchange Server has two storage groups and you enable the Multi Stream option during backup, one subjob is created for each storage group.

Perform a Document Level Backup

Before you submit a Document Level backup job, make sure that the Exchange Server services are started on your server and that the CA BrightStor Universal Agent is started.

To back up an Exchange Server using Document Level backup:

1. From the BrightStor ARCserve Backup Home Page, select the Backup Manager from the Quick Start menu.

2. When the Backup Manager opens, expand the Microsoft Exchange Server Document Level object to select the items that you want to back up.

   Note: Special mailboxes, such as Mail Connectors, System Attendant, Internet Mail Service, and MS Schedule+, cannot be selected for backup. These are special system mailboxes and should not be backed up. Hidden mailboxes also cannot be backed up.

3. If the Browsing Filter opens (the browsing filter is automatically displayed when there are more than 500 items), set filters to specify the items you want to search through and click OK. For more information on the browsing filters, see Browsing Filter.

4. Select the items that want to back up.

5. To select a backup method at the Document Level, right-click Microsoft Exchange Server – Document Level, select **Agent Option**, select a backup method, and then click OK. For more information about backup methods, see Document Level Backup Methods.

6. If you want to exclude mailboxes, folders, or attachments from your backup job, right-click Microsoft Exchange Server -Document Level, select Filter, set up your filters, and then click OK. For more information on filters, see Document Level Backup Filters.

7. If you want to enable CRC checking so that you can verify the integrity of your data by using the Scan utility after the backup job is performed, click the Options button, click the Operation tab, enable the **Calculate and Store CRC Value on Backup Media** option, and then click OK.

   Note: For more information on CRC checking and using the Scan utility, see Document Level Scan Media Options.

8. If you want to enable compression and encryption, click the Options button, click the Backup Media tab, enable the Compress Files Before Backup and the Encrypt Files Before Backup options, enter the password for the encryption in the Session/Encryption Password field, and then click OK.

9. Click the Destination tab and select a backup destination.

10. Click the Schedule tab. If you want to use a Custom Schedule, select a Repeat Method and, if you did not select a backup method at the Document Level, select a backup method. If you want to use a rotation scheme, select the **Use Rotation Scheme** option and set up your scheme. For more information on scheduling jobs and rotation schemes, see the online help and the *Administrator Guide*.

11. Click Start.

12. When the Security and Agent Information dialog opens, make sure that the correct user name and password are filled in for each object. If you need to enter or modify a user name or password, click the Security button, make your changes, and then click OK.

13. Click OK.

14. When the Submit Job dialog opens, select **Run Now** to run the job immediately, or select **Run On** and select a future date and time when you want the job to run.

15. Enter a description for your job.

16. If you selected multiple sources to back up and want to set the priority in which the job sessions initiate, click Source Priority. Use the Top, Up, Down, and Bottom buttons to change the order in which the jobs are processed. When you finish setting priorities, click OK.

17. On the Submit Job page, click OK to submit your job.

After you submit your backup job, you can go to the Job Status Manager and double-click the active job to view real-time job properties. If you have Complete Messaging Single Instance Storage enabled, all of the fields related to size will reflect the size prior to single instance storage optimization. The actual size of the backup after single instance storage optimization opens in the Activity Log and is labeled "(xx)MB Written to Media".

Activity Log Messages

At the end of each backup job, a summary of each session is displayed in the Activity Log. Depending on what occurs during backup, the summary includes messages with the following information:

- The status of the job. Depending on what you selected to back up and what occurred during the backup job, you will receive one of three statuses:

  - **Successful**—All selected mailboxes and root public folders were backed up.

  - **Incomplete**—One or more of the selected mailboxes and root public folders were backed up. At least one mailbox or root public folder failed to back up.

  - **Failed**—No selected mailboxes and root public folders were backed up.

  Note: Individual folders, messages, and attachments do not affect the status of the job. If these items are not backed up, the details will be listed in the skip log in the agent log directory. If you would rather view the skip log information in the Activity Log or if you want to view it in the Activity Log in addition to the skip log, you can change the value of the Skip Log Setting. For more information on the Skip Log Setting, see Configure the Add-on in the chapter "Installing the Agent." This skip log is also useful for tracking corrupt messages in an Exchange Server.

- The number of root public folders, mailboxes, folders, and documents that were backed up successfully

- The amount of data that was backed up

- The amount of data that was written to media

- The amount of size reduction achieved through Complete Messaging Single Instance

- The number of items that were skipped

- The number of mailboxes that failed to back up

- The number of root public folders that failed to back up

- The status of the session has changed

- Instructions on how to resolve an issue

Document Level Backup Scan Utility

After you back up your Exchange Server database, you can use the BrightStor ARCserve Backup Scan utility to find out what is on your media, to view information about your media backup sessions, and, if you enabled CRC checking during backup, to verify the integrity of the data that was written to the media.

Note: For more information on how to enable CRC checking during backup, see Perform a Document Level Backup.

Each source that you select to back up is saved on media as an individual session. You can scan a single session or an entire media. You can view the results of the Scan job in the Job Queue by clicking the Log tab.

Use the Log tab in the Options dialog to select the level of detail you see in the Job Queue Log. You can choose to see just summary information and any errors that occurred during the scan or you can choose to see each file that was backed up, summary information, and any errors that may have occurred.

Document Level Scan Media Options

If you enable CRC checking during backup, the following scan media options apply to your Exchange Server backup job:

On the Operation tab, enable **Calculate and Store CRC Value on Backup Media** if you want to scan files with a CRC check to verify the integrity of the data that was written to the media.

On the Job Log tab, select the level of detail you want to include in the log report:

- **Log All Activity—**Record all of the activity that occurs while the job is running in the Job Log.

- **Log Summary Only—**Record summary information of the job (including source, destination, session number, and totals) and errors.

- **Log Disabled—**Do not record any information about this job in the Job Log.

Note: You can view the log report in the Job Queue or Database Manager (Job Records).

Perform Media Scan

To scan media:

1. Open the Scan utility.

2. Select the media you want to scan. If the media you want to scan is not currently in a storage device, you must enter the information into the Group and Media fields.

3. Enter a specific session to scan or select to scan all sessions on the media.

4. Click Options to specify scan options for the job.

   Note: If you enabled **CRC checking during backup**, you must enable the **Calculate and Store CRC Value on Backup Media** option if you want to verify the integrity of the data.

5. Click Filter to specify filters for the job.

6. Click Start to submit the job.

Document Level Data Restore

The following sections include information about the prerequisites you must meet before you perform a restore, the features that the add-on offers when restoring from a Document Level backup, and the procedure for how to perform a restore.

Document Level Restore Prerequisites

Before you restore, you must satisfy the following prerequisites:

- The Exchange Server must be running and the storage groups and mailbox stores that you are restoring to must already exist (they are not created at restore time).

- The account you are using to restore must meet the backup agent service account requirements for the machine you are restoring to. For information on these requirements, see Backup Agent Service Account Requirements for Document Level Backup and Restore.

Document Level Restore Sets

When you back up an Exchange Server, each storage group that you select to back up is saved on media as an individual session. To restore an object, you should restore all of the sessions that, when combined, give you the most up-to-date version. These sessions are called your restore set.

The number of sessions in your restore set depends on the backup methods you used:

- If you backed up your storage group using only the full backup method, your restore set includes only this session.

- If you backed up your storage group using both full and incremental backups, your restore set includes the session from the full backup and at least one, but up to as many sessions from the incremental backup as you want to include. For example, in the following backup scenario, your restore set can be full and incremental 1, full and incremental 1 and 2, full and incremental 1, 2, and 3, or full and incremental 1, 2, 3, and 4:

Full	Incremental 1	Incremental 2	Incremental 3	Incremental 4

- If you backed up your storage group using both full and differential backups, your restore set includes the session from the full backup and one differential backup session. For example, in the following backup scenario, your restore set can be full and differential 1, full and differential 2, full and differential 3, or full and differential 4:

Full	Differential 1	Differential 2	Differential 3	Differential 4

After you determine your restore set, you must make sure that you select the entire set when submitting your restore job.

Note: Since Document Level backups are independent, you can restore an incremental backup or differential backup by itself (you do not have to restore it along with a full backup). As a result, if you want to restore your entire restore set, make sure you select the full backup because it is not automatically selected for you.

Document Level Restore Options

When you create a restore job, you can choose restore options to customize the job. To select restore options, right-click a storage group and select **Agent Option**:
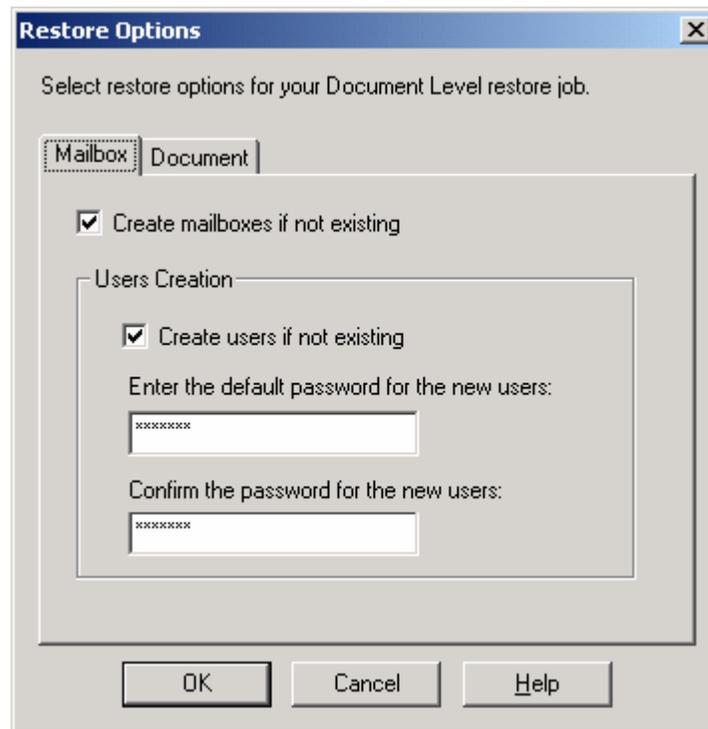
On the Mailbox tab, you can select the following:

■ **Create mailbox if not existing—**Use this option if you want to restore your data to a different Exchange Organization or if you want to restore to the same server you backed up from, but the mailbox you want to restore has been deleted.

Important! *If the mailbox you want to restore has been deleted but the user associated with this mailbox still exists and has the same properties, associate this user with the new mailbox. If both the mailbox you want to restore and the user associated with the mailbox have been deleted, you must create a new user.*

If you use this option, an email is sent to the new mailbox to finalize it and notify you that the mailbox is ready for use. If you want to customize the contents of this email, you can create a new message and save it as an RTF file in the BrightStor ARCserve Backup Agent for Exchange directory to replace the default MailboxInitialize.rtf. In addition, you can also customize the subject line of this email by using the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\BrightStor ARCserve
Backup\ExchangeDocumentAgent\Parameters
```

```
Value Name:FirstMailSubject
Value Type: REG_SZ
Value Data:The desired subject line
```

■ **Create user if not existing—**If you selected the **Create mailbox if not existing** option and do not have an existing user to associate with the mailbox, you must use this option and enter a password because every mailbox must have a user associated with it. When entering the password, ensure that it meets the length, complexity, and history requirements of the domain and server you are restoring to.

This option useful if you want to perform a test restore of a mailbox to backup server, if you want to audit a mailbox, or if you need a placeholder user because you plan on connecting the mailbox to a different user. When you use this option, the amount of properties that are assigned to the user during restore is determined by what setting you used for the **Backup Additional User Properties** configuration option during your backup job. For more information on the Backup Additional User Properties configuration option, see Configure the Add-on in the chapter "Installing the Agent."

Notes:

■ After the user is created, regardless of what you selected for the **Backup Additional User Properties** configuration option, you should still adjust the properties to set group memberships, to set up rights, and to reflect organizational policies.

- If you want to create duplicates of existing users and mailboxes in the same organization, you must append a string to the user and mailbox names. For information on how to configure this, see the section Configure the Add-on in the chapter "Installing the Agent."

If you have trouble with mailbox or user creation, see the section on failing to create the user account, to create the mailbox, or to finalize the mailbox in the appendix "Troubleshooting."
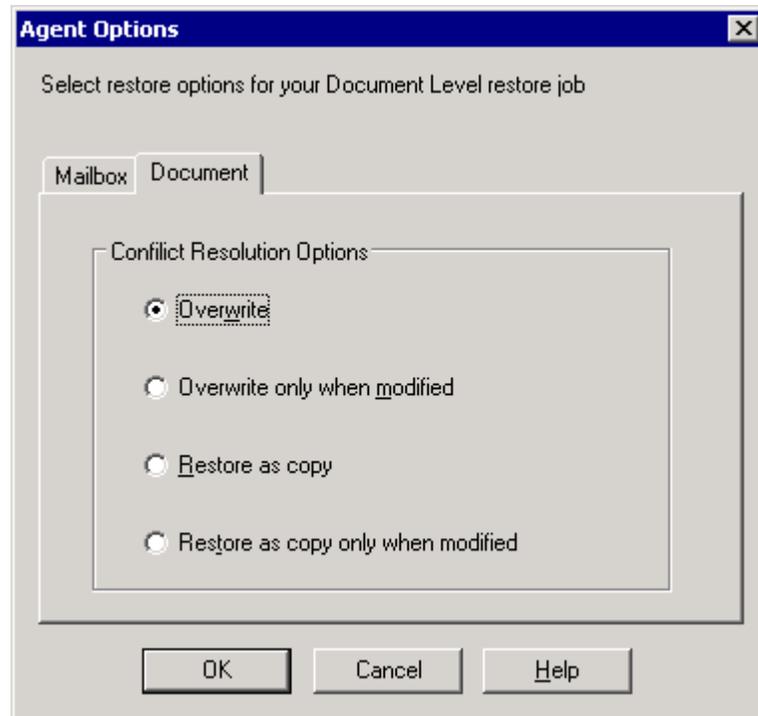
When restoring documents, a conflict may occur if a version of what you are restoring already exists on your destination. To prepare for this situation, select one of the following conflict resolution options:

- **Overwrite—**Delete original documents.

- **Overwrite only when Modified —**Delete only the original documents that have been modified since they were backed up. Because documents that have not been modified are skipped, this option is faster than the Overwrite option.

- **Restore as Copy—**Do not delete original documents and restore as copies. Use this option if you are restoring to an empty folder in the original location or an alternative location.

- **Restore as Copy only when Modified—**Do not delete original documents and restore as copies for documents that have been modified since they were backed up. Because documents that have not been modified are skipped, this option is faster than the Restore as Copy option.

Note: When a message is restored, a new message ID is created and assigned to it. Consequently, if you restore from one backup multiple times, you will see message duplicates even if you selected to overwrite the original.

Document Level Restore Locations

When restoring a Document Level backup, you can restore the files to their original location (default) or you can restore the files to an alternative location. Use the Restore files to their original location option only when you want to restore the exact location you backed up from and the hierarchy of the server has not changed. For all other scenarios, you must restore files to an alternative location.

Some examples of when to restore to an alternative location include:

- If you want to restore a document to a different folder or mailbox on the same server that you backed up from

- If you want to restore a document to a different folder or mailbox on a different server than the server you backed up from

- If you want to merge a mailbox

- If you want to migrate a mailbox

- If you renamed storage groups or mailbox stores

Alternate Restore Locations

When you restore to an alternative location, there are certain rules that apply when selecting your source and destination:

- **Source**—When you select your source, you can either select to restore it as a new object inside your destination or to merge it into your destination.

- **Destination**—When you select your destination, you must consider what you selected to restore and what version of Exchange Server you are restoring to.

The following sections include more information on selecting a source and destination.

Source Selection Considerations

When you restore to an alternative location, the objects you restore are either restored as new objects inside or merged into, the destination you select, depending on how you select your source. For example:

- Restoring inside your destination—This means that if you select Mailbox_A as your source and Mailbox_ B as your destination, Mailbox_A is restored as a new object within Mailbox_B.

- Merging into your destination—This means that if you select Mailbox_A as your source and Mailbox_B as your destination, the contents of Mailbox_A will be merged into the existing contents of Mailbox_B.
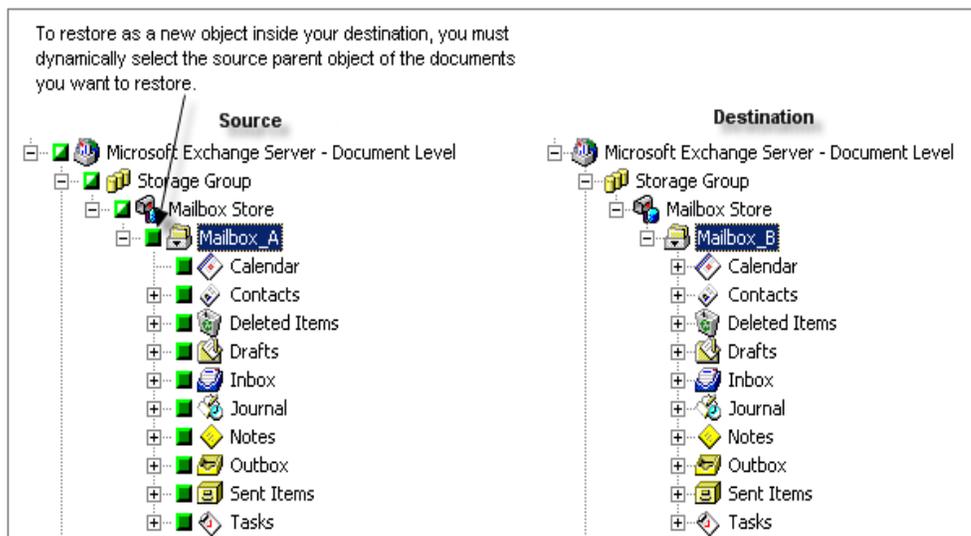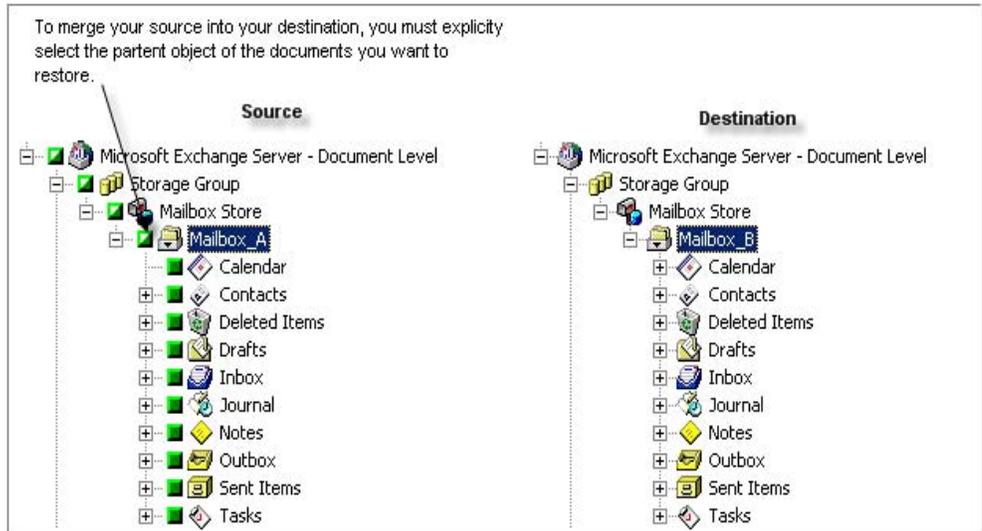
For more information on dynamic and explicit job packaging, see *Getting Started*.

Destination Selection Considerations

When restoring to an alternative location, there are certain rules that apply to the destination you select, depending on what you selected to restore and what version of Exchange Server you are restoring to.

Note: If you select multiple sources to restore, you must select a destination that supports all sources.

Because the destination you select depends on the source you select, the following diagrams display the BrightStor ARCserve Backup source view for each version of Exchange Server. The charts that follow each diagram include information about each destination that is supported, depending on the source and version of Exchange Server.

Source View for Exchange Server 2000 and 2003 Objects

The following diagram displays the source objects you can restore for Exchange Server 2000 and 2003 using the BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on:
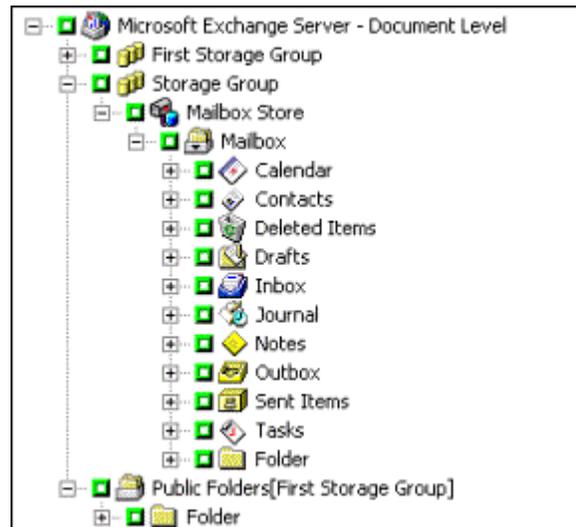
Source View for Exchange Server 5.5 Objects

The following diagram displays the source objects you can restore for Exchange Server 5.5 using the BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on:
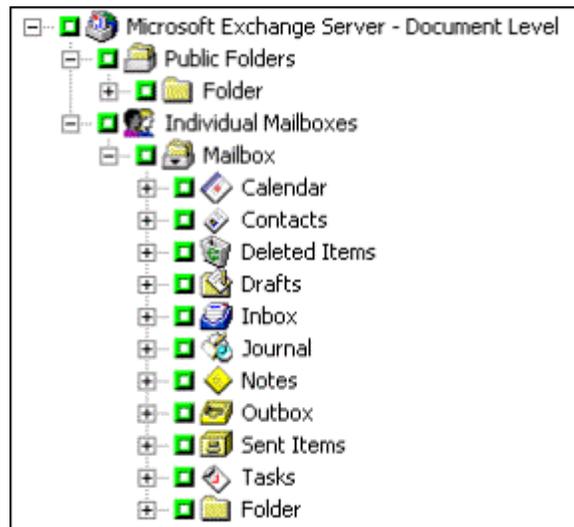
Source View of Document Objects for all Versions of Exchange Server

The following diagram displays the source document objects you can restore for all versions of Exchange Server using the BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on:

Subject	From	Received
□ ✉ Document	Administrator	6/25/03 12:28 PM
□ ✉ Document With Attachment	Administrator	6/25/03 12:27 PM

Supported Destinations when Restoring Exchange Server 2000 or 2003 to Exchange Server 2000 or 2003

The following chart lists the source objects you can select, and their supported destinations, when restoring Exchange Server 2000 or 2003 to Exchange Server 2000 or 2003 using the BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on:

Source Objects	Supported Destinations
Storage Group	Microsoft Exchange Server - Document Level
Public Folders [Storage Group]	Microsoft Exchange Server - Document Level
Mailbox Store	Storage Group
Mailbox*	Public Folders [Storage Group], Mailbox Store, Mailbox, Folder
Folder	Public Folders [Storage Group], Mailbox, Folder
Document	Folder

*Mailbox is converted into a folder if it is not restored to a Mailbox Store.

Supported Destinations when Restoring Exchange Server 5.5 to Exchange Server 2000 or 2003

The following chart lists the source objects you can select, and their supported destinations, when restoring Exchange Server 5.5 to Exchange Server 2000 or 2003 using the BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on:

Source Objects	Supported Destinations
Public Folders	Microsoft Exchange Server - Document Level
Mailbox*	Public Folders [Storage Group], Mailbox Store, Mailbox, Folder
Folder	Public Folders [Storage Group], Mailbox, Folder
Document	Folder

*Mailbox is converted into a folder if it is not restored to a Mailbox Store.

Note: When restoring from Exchange Server 5.5 to Exchange Server 2000 or 2003, you cannot select the Individual Mailboxes parent object as a source because of the ambiguity of the child mailbox locations. You can, however, select a child mailbox as a source or the mailbox store (and select the option Create mailbox if not existing) if you need to migrate or restore mailboxes.

Supported Destinations when Restoring Exchange Server 5.5 to Exchange Server 5.5

The following chart lists the source objects you can select, and their supported destinations, when restoring Exchange Server 5.5 to Exchange Server 5.5 using the BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on:

Source Objects	Supported Destinations
Individual Mailboxes	Microsoft Exchange Server - Document Level
Public Folders	Microsoft Exchange Server - Document Level
Mailbox*	Individual Mailboxes, Public Folders, Mailbox, Folder
Folder	Public Folders, Mailbox, Folder
Document	Folder

*Mailbox is converted into a folder if it is not restored to Individual Mailboxes.

Supported Destinations when Restoring Exchange Server 2000 or 2003 to Exchange Server 5.5

The following chart lists the source objects you can select, and their supported destinations, when restoring Exchange Server 2000 or 2003 to Exchange Server 5.5 using the BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on.

Source Objects	Supported Destinations
Storage Group	Microsoft Exchange Server - Document Level
Public Folders [Storage Group]	Microsoft Exchange Server - Document Level
Mailbox Store	Microsoft Exchange Server - Document Level
Mailbox*	Individual Mailboxes, Public Folders, Mailbox, Folder
Folder	Public Folders, Mailbox, Folder
Document	Folder

*Mailbox is converted into a folder if it is not restored to Individual Mailboxes.

Manually Extending your Destination Path to Create a New Folder

If you want to create a new folder to restore to within the mailbox or folder you selected as your destination, you can manually extend the destination path on the Destination tab in the Restore Manager. For example, if you select Mailbox_A as your destination and want to add a new folder within Mailbox_A to restore to, add the name of your new folder at the end of the destination path at the top of the page:

Note: Do not enter a backslash (\) at the end of your new folder name.
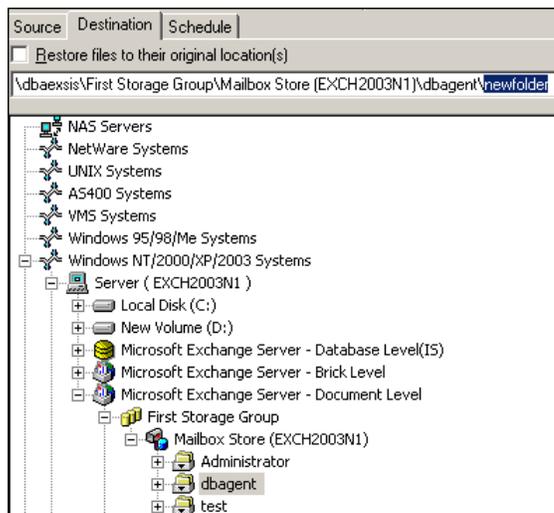
Note: Because Document Level restore uses push agent technology, you must always have Windows NT/2000/XP/2003 Systems selected in the Destination field next to the destination path:
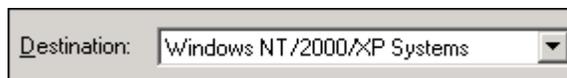
Perform a Document Level Restore

To restore using Document Level restore:

1. From the BrightStor ARCserve Backup Home Page, select the Restore Manager from the Quick Start menu.

2. When the Restore Manager opens, select **Restore by Tree** in the drop-down box underneath the Source tab.

   Note: Both Restore by Tree and Restore by Session are supported for Document Level restore.

3. Expand the **Windows NT/2000/XP/2003 Systems** object, expand the server you are restoring from, and then expand the server object to select the documents you want to restore—storage groups, mailbox stores, public folder stores, public folders, folders, or even individual documents.

   Note: Special mailboxes, such as Mail Connectors, System Attendant, Internet Mail Service, and MS Schedule+, cannot be selected for restore. These are special system mailboxes and should not be restored.

4. Click Version History, select a backup version for this session, and click Select.

   Note: Version History is supported at the storage group level only.

5. To select restore options, right-click a storage group, select **Agent Option**, select restore options, and then click OK. For more information about restore options, see Document Level Restore Options.

6. Click the Destination tab. You can restore the database objects to their original location (default) or you can restore the database objects to an alternative location.

7. If you want to restore to an alternative location, clear the **Restore files to their original locations** check box, expand the Windows NT/2000/XP/2003 Systems object, expand the server you want to restore to, expand the Microsoft Exchange Server – Document Level object, and select where you want to restore to.

   Note: When restoring to an alternative location, there are certain rules that apply to the destination you select, depending on what you selected to restore and what version of Exchange Server you are restoring to. For more information, see Alternate Restore Locations.

8. Click Start.

9. If you are restoring to an alternative location, when the Security dialog opens, enter the user name and password for the destination server and click OK.

10. When the Session User Name and Password dialog opens, on the Machine tab, verify or change the user name and password for the destination Exchange Server. To change the user name or password, select the session, click Edit, make your changes, and then click OK.

11. Click the DBAgent tab and verify or change the user name and password for the backup agent service account. This account must meet the requirements for the Exchange Server you are restoring to. For information on these requirements, see Backup Agent Service Account Requirements for Document Level Backup and Restore.

12. Click OK.

13. When the Submit Job dialog appears, select **Run Now** to run the job immediately, or select **Run On** and select a future date and time when you want the job to run.

14. Enter a description for your job and click OK.

Chapter 5: Performing Brick Level Backups and Restores

Brick Level backup and restore uses Messaging Application Programming Interface (MAPI) to access messages. This type of backup and restore is useful for recovering mailboxes and folders to original or alternative locations. It is not a single instance storage agent so when you use Brick Level backup your backups can be equal to or larger than the original database size.

Brick Level Views in the Backup Manager

Depending on your configuration, Microsoft Exchange Server – Brick Level is displayed in the Backup Manager under the following objects:

- Windows NT/2000/XP/2003 Systems

- Exchange Organization

Note: If you installed the add-on, Brick Level does not display in the Backup and Restore Managers automatically. To display Brick Level, you must enable the configuration option Show Brick Level. For more information on this option, see Configure the Add-on in the chapter "Installing the Agent."

When you expand the Brick Level object, you can view Individual Mailboxes and Public Folders. When you expand a mailbox or a public folder, you can view its containing folders:
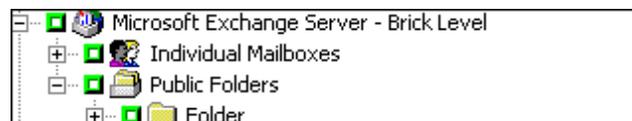
Note: In a cluster environment, Exchange servers appear under the Exchange virtual server objects.

Backup Agent Service Account Requirements for Brick Level Backup and Restore

To perform a Brick Level backup and restore job, your backup agent service account must meet the following criteria on the Exchange Server.

For Exchange Server 2000 and 2003:

- The account must have a domain user with a mailbox.

- The account must be added to the Domain Admins group on your domain controllers and to the Administrators group and Backup Operators group on your Exchange Server.

  Note: If your Exchange Server is your domain controller, you must add all three groups to your backup agent service account only on your domain controller.

- The account must be assigned the following rights:

  – Act as part of the operating system

  – Log on locally

  – Log on as service

- The account must be assigned roles at the Organization, Site, and Configuration levels of the organization tree.

- The account must be assigned the Owner permission level on every public folder you intend to back up and restore because permissions for public folders can vary. If a lower permission level is assigned, back up or restore may fail or duplicate items may be restored because the backup agent service account does not have the permission to delete original documents.

For Exchange Server 5.5:

- The account must have a domain user with a mailbox.

- If your Exchange Server is on a member server, the account must be added to the Administrators group and the Backup Operators group. If your Exchange Server is on a domain controller, the account must be added to the Domain Admins, Administrators, and Backup Operators groups.

  Note: If your Exchange Server is your domain controller, you must add all three groups to your backup agent service account only on your domain controller.

- The account must be assigned the following rights:
  - Act as part of the operating system
  - Log on locally
  - Log on as service

  Note: If you have a multi-domain environment or you are installing on a member server, you must add these rights on the domain controllers.

- The account must be assigned roles at the Organization, Site, and Configuration levels of the organization tree.

- The account must be assigned the Owner permission level on every public folder you intend to back up and restore because permissions for public folders can vary. If a lower permission level is assigned, back up or restore may fail or duplicate items may be restored because the backup agent service account does not have the permission to delete original documents.

The Exchange Agent Configuration Utility is the most efficient tool for creating your backup agent service account and ensuring it is set up correctly. For information on how to use this utility, see Configure Database Level and Brick Level Backup and Restore in the chapter "Installing the Agent." However, if because of the setup of your environment it is better for you to manually create a backup agent service account, see the appendix "Configuring the Backup Agent Service Account Manually" for instructions on how to do so.

Brick Level Backup Features

The following sections describe the features that are available when using Brick Level backup and restore and describe how to perform a Brick Level backup and restore.

Brick Level Backup Methods

When you submit a backup job, you must select a backup method. The backup method tells BrightStor ARCserve Backup how you want your data to be backed up. When you use the BrightStor ARCserve Backup Agent for Microsoft Exchange, you must select a backup method for your Brick Level backup job at the Microsoft Exchange Server – Brick Level.

Note: If you want to perform a Brick Level backup job and include disaster recovery information, you must submit both a whole node backup job to generate the disaster recovery information and a separate Brick Level backup job.

To select a backup method at the Brick Level, right-click Microsoft Exchange Server – Brick Level and select **Agent Options**:

The following dialog opens:
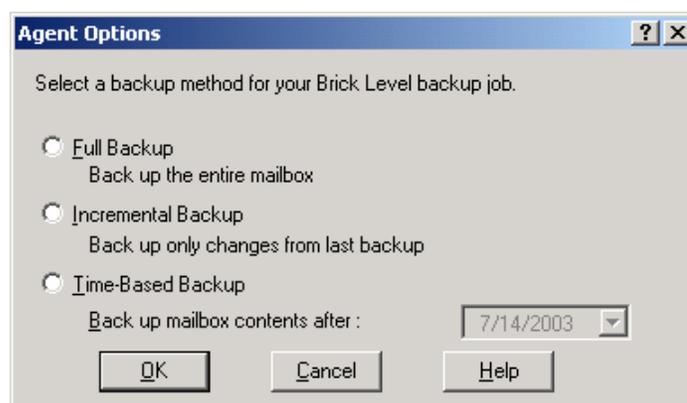
You can select from the following backup methods:

- **Full Backup**—Backs up all documents.

- **Incremental Backup**—Backs up all documents created or modified since the last full or incremental backup of the entire mailbox. If no full backup has been performed, all documents are backed up.

- **Time-Based Backup**—Backs up all documents created or modified since 12:00 AM on the date you specify. The BrightStor ARCserve Backup automatically adjusts for daylight savings and if there is a time zone difference between the server that is running the BrightStor ARCserve Backup Manager and the server that has the agent installed.

Perform a Brick Level Backup

Before you submit a Brick Level backup job, make sure that the Microsoft Exchange Information Store and the CA BrightStor Backup Agent RPC Server service are running on your server.

To back up an Exchange Server using Brick Level backup:

1. From the BrightStor ARCserve Backup Home Page, select the Backup Manager from the Quick Start menu.

2. When the Backup Manager opens, expand the Microsoft Exchange Server -Brick Level object.

3.   Select the items that you want to back up.

    Note: Special mailboxes, such as Mail Connectors, System Attendant, Internet Mail Service, and MS Schedule+, cannot be selected for backup. These are special system mailboxes and should not be backed up. Also, folders that have the character "\" in their names are skipped and will not be backed up.

4. Select a backup method. To do this, right-click Microsoft Exchange Server – Brick Level, select **Agent Option**, select a backup method, and then click OK. For more information about backup methods, see Brick Level Backup Methods.

5. Click the Destination tab and select a backup destination.

6. Click Start.

7. When the Security and Agent Information dialog opens, make sure that the correct user name and password are filled in for each object. If you need to enter or modify a user name or password, click the Security button, make your changes, and then click OK.

8. Click OK.

9. When the Submit Job dialog opens, select **Run Now** to run the job immediately, or select **Run On** and select a future date and time when you want the job to run.

10. Enter a description for your job.

11. If you selected multiple sources to back up and want to set the priority in which the job sessions initiate, click Source Priority. Use the Top, Up, Down, and Bottom buttons to change the order in which the jobs are processed. When you finish setting priorities, click OK.

12. On the Submit Job page, click OK to submit your job.

After you submit your restore job, you can go to the Job Status Manager and double-click the active job to view real-time job properties.

Brick Level Data Restore

The following sections include information about the prerequisites you must meet before you perform a restore, the features that the agent offers when restoring from a Brick Level backup, and the procedure for how to perform a restore.

Brick Level Restore Prerequisites

To perform a Brick Level restore, you must first meet the following prerequisites:

- The Exchange Server must be running and the storage groups, mailbox stores, and mailboxes that you are restoring to must already exist (they are not created during the restore process).

- If you are restoring to a mailbox, it cannot be disabled

- The account you are using to restore must meet the backup agent service account requirements for the machine you are restoring to. For information on these requirements, see Backup Agent Service Account Requirements for Brick Level Backup and Restore.

Brick Level Restore Sets

To restore a folder or mailbox, you must select the object you want to restore in all of the sessions that, when combined, completely restore the folder or mailbox. These sessions are called your restore set.

The number of sessions in your restore set depends on the backup methods you used:

- If you backed up your folder or mailbox using only the full backup method, your restore set includes only this full session.

- If you backed up your folder or mailbox using both full and incremental backups, your restore set includes your full session and at least one, but up to as many incremental sessions as you want to include. For example, in the following backup scenario, your restore set can be full and incremental 1, full and incremental 1 and 2, full and incremental 1, 2, and 3, or full and incremental 1, 2, 3, and 4:

Full	Incremental 1	Incremental 2	Incremental 3	Incremental 4

- If you backed up your folder or mailbox using both full and differential backups, your restore set includes your full session and one differential session. For example, in the following backup scenario, your restore set can be full and differential 1, full and differential 2, full and differential 3, or full and differential 4:

Full	Differential 1	Differential 2	Differential 3	Differential 4

Brick Level Restore Options

When you create a restore job, a conflict may occur if a version of what you are restoring already exists on your destination server. To prepare for this situation, you can choose a conflict resolution restore option. To select a restore option, right-click Microsoft Exchange Server-Brick Level and select **Agent Option**.
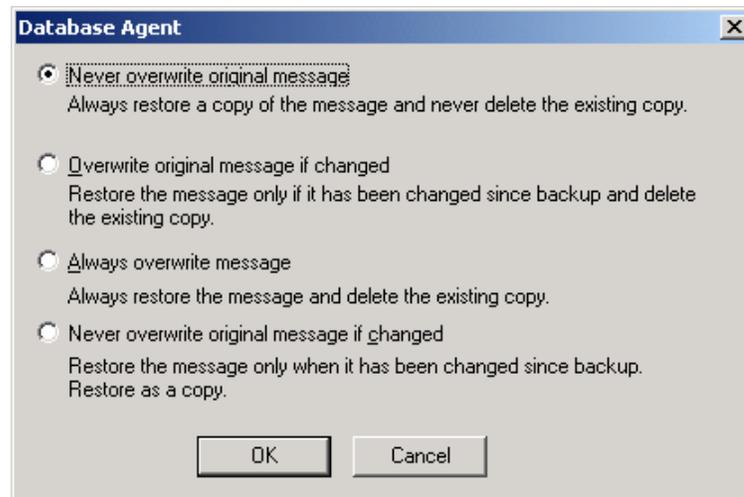
Select one of the following conflict resolution options:

- **Never overwrite original message—**Do not delete original messages and always restore as copies. Use this option if you are restoring to an empty folder in the original location or an alternative location.

- **Overwrite original message if changed**—Delete only the original messages that have been modified since they were backed up. Do not delete original messages and always restore as copies. Use this option if you are restoring to an empty folder in the original location or an alternative location.

- **Always overwrite message**—Delete original messages.

- **Never overwrite original message if changed**—Do not delete original messages and always restore as copies those messages that have been modified since they were backed up. Because messages that have not been modified are skipped, this option is faster than the Restore as Copy option.

  Note: When a message is restored, a new message ID is created and assigned to it. Consequently, if you restore from one backup multiple times, you will see duplicated messages even if you selected to overwrite the original.

Perform a Brick Level Restore

To restore using Brick Level restore:

1. From the BrightStor ARCserve Backup Home Page, select the Restore Manager from the Quick Start menu.

2. When the Restore Manager opens, select **Restore by Tree** in the drop-down box underneath the Source tab.

3. Expand the server you are restoring from, expand the Microsoft Exchange Server – Brick Level object, and select the folders that you want to restore.

    Notes:

    -   When you select a folder, an object is displayed in the top right-pane. This represents the folder you selected to restore and all of its contents. You do not need to select this object because it is automatically selected for you.

    -   Special mailboxes, such as Mail Connectors, System Attendant, Internet Mail Service, and MS Schedule+, cannot be selected for restore. These are special system mailboxes and should not be restored.

4. Click Version History, select a backup version for this session, and click Select.

5. Choose a restore option. To do this, right-click Microsoft Exchange - Brick Level, select **Agent Option**, select a restore option, and click OK. For more information about restore options, see Brick Level Restore Options.

6. Click the Destination tab. You can restore folders to their original location (default) or you can restore the folders to an alternative location (includes restoring a folder to a different mailbox on the same or different server).

7. If you want to restore to an alternative location, remove the check mark from the **Restore files to their original locations** check box, verify MS Windows System is selected in the Destination field, expand the Windows NT/2000/XP/2003 Systems object (if you do not have the Universal Agent installed, expand the Network object), expand the server you want to restore to, expand the Microsoft Exchange Server – Brick Level object, and select where you want to restore to.

8. Click Start.

9. When the Session User Name and Password dialog opens, verify or change the user name and password for the destination Exchange Server. To change the user name or password, select the session, click Edit, make your changes, and then click OK.

    Note: The user name must be entered in the following format:

    `Domain\Username`

10. Click the DBAgent tab and verify or change the user name and password for the backup agent service account. This account must meet the requirements for the Exchange Server you are restoring to. For information on these requirements, see Backup Agent Service Account Requirements for Brick Level Backup and Restore.

    Note: The user name must be entered in the following format:

    `Domain\Username`

11. Click OK.

12. When the Submit Job dialog opens, select **Run Now** to run the job immediately, or select **Run On** and select a future date and time when you want the job to run.

13. Enter a description for your job and click OK.

Chapter 6: Using Best Practices

This chapter recommends best practices for using BrightStor ARCserve Backup Agent for Microsoft Exchange and the BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on so that you can take full advantage of the powerful features these products offer.

General Recommendations

Consider the following best practices when using the agent.

Technical Resources

The Microsoft web site offers numerous technical resources for Exchange Server, including books, downloadable Help files, and software development kits. You should read these documents, especially the white papers *Disaster Recovery for Microsoft Exchange 2000 Server* and *Microsoft Exchange 5.5 Disaster Recovery*. The more informed you are about Exchange Server, the more you can apply your knowledge to maximize data protection when using the agent.

Logs in the Event Viewer

In addition to monitoring the BrightStor ARCserve Backup Activity Log for events that may occur when using the agent, you should also monitor the logs in your Windows Event Viewer, especially the Application Log and System Log. The Application Log includes internal Exchange Server events and the System Log includes Windows events.

Installation Recommendations

Consider the following best practices when installing the agent:

Product Recommendations

BrightStor ARCserve Backup offers agents and options that let you protect all of the servers in your Exchange Organization. These servers include your Exchange Servers and domain controllers.

Note: It is important to protect your domain controllers since they include the Active Directory containers, which hold user, mailbox, and public folder information.

To maximize your Exchange Server protection, use all of the following solutions on each of your Exchange Servers:

- **BrightStor ARCserve Backup Agent for Microsoft Exchange—** Includes Database and Brick Level backup and restore. Database Level backup and restore protects the Exchange Server database and logs. Brick Level backup and restore lets you perform folder-level backup and restore.

- **BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on—**Includes Database Level and Document Level backup and restore. Database Level backup and restore protects the Exchange Server database and logs. Document Level backup and restore, which is only available with this add-on, eases and expedites many administrative tasks and maximizes flexibility by offering the most granular level of restore.

- **BrightStor ARCserve Backup Agent for Windows**—Protects files and system state, including Active Directory. It is important to protect Active Directory when using Exchange Server 2000 and 2003 because it stores mailbox and user information.

  Note: In addition to using the BrightStor ARCserve Backup Agent for Windows on all of your Exchange Servers, also use it to protect all of your domain controllers.

- **BrightStor ARCserve Backup Disaster Recovery Option**—In the event of a disaster, the BrightStor ARCserve Backup Disaster Recovery Option recovers the machine to the last full backup state. Install the BrightStor ARCserve Backup Disaster Recovery Option on all Backup Managers you will use to back up your Exchange Servers and domain controllers.

Load Reduction

If you have the network infrastructure to support high performance remote backups, install the Backup Manager on a different server than your Exchange Server. This reduces the load on the Exchange Server.

Exchange Server Configuration Recommendations

Consider the following best practices for configuring your Exchange Server.

Circular Logging

Circular Logging must be disabled to take advantage of incremental and differential backups. If Circular Logging is not disabled and you submit an incremental or differential backup, the agent automatically converts the backup to full.

Although Circular Logging decreases the amount of disk space you use, it does not let you recover all changes since your last backup because it only maintains a small number of log files. Consequently, you cannot take advantage of the benefits of using a transaction-based system and you cannot completely recover if something goes wrong with the system. If you want to conserve disk space, perform regular backups rather than using Circular Logging because backups automatically remove transaction log files.

Transaction Log Space

Make sure that you have enough space on your Exchange Server in case you want to restore transaction logs. Leave at least twice the amount of space that you expect your transaction logs to use. In addition, if you intend to restore Brick or Document Level backups, you should leave enough space to accommodate the size of the backups because the size of the database file may increase during the restore.

Backup Recommendations

Consider the following best practices for backing up Exchange Server.

Online Backup Use

Always perform online backups. This lets you back up Exchange Server databases without shutting them down and losing work time. If you do not perform online backups, not only do you lose valuable work time, but you also run the risk of making costly errors since offline backups are detailed and labor-intensive. When you perform online backups, the agent manages files for you. When you perform offline backups, you must do all of the work yourself. In addition, if you perform offline backups, there is no process for validating the checksum on each page of the database so you cannot detect corruptions and check the integrity of the database.

Media Integrity

Use the global option Calculate and Store CRC Value on Backup Media when creating your backup job. Afterwards, scan your media with CRC verification to ensure the media integrity.

Database Level Backup Strategies

There are many factors that contribute to your backup strategy— backup window size, restore window size, server and storage hardware, the amount of available media, media retention time, network bandwidth, server load, and the size of your databases. Consequently, the backup strategy that you should use depends on your environment and physical hardware.

When determining a backup strategy, you must first assess the amount of time your organization has available each week for backing up your Exchange Server. When doing so, remember that the most time-consuming aspect of performing a restore is replaying the log files. Depending on how often you perform full backups, it can take several hours to replay log files on large servers during a restore because every transaction that has occurred since the last backup must be scanned. In addition, the speed at which transaction log replay occurs varies, depending on the type of transactions that must be replayed. Perform a test restore of your log files to get a more accurate estimate of how long it will take.

After you determine the size of your restore window, you must consider the affect that your environment and resources will have on your backup strategy:

- In an environment that has mission-critical data with minimal restore windows, you should perform full backups nightly (or during the hours your server is least active) and incremental backups at mid-day (or during a low production period during the day that is evenly spaced from your full backups).

- If media usage is major factor in your backup strategy, either perform full backups daily or full alternating with differential backups daily.

- In an environment that has non mission-critical data with less aggressive restore windows, you should perform a full backup at least once a week and perform incremental or differential backups on the other days.

The following chart includes examples of a few backup strategies and their advantages and disadvantages. Although, for maximum protection, you should perform daily full and incremental backups, for maximum protection, you can customize your backup strategy to suit your organization's needs. The only requirement is that you minimally perform daily backups on work days with a full backup once a week.

Backup Strategy	Advantages	Disadvantages
Daily full and incremental backups*	High frequency of protection	High media usage
	Short restore window	
Daily full backups	Good frequency of protection	High media usage
	Short restore window	
Daily backups with a full at least once a week	Good frequency of protection	Varying restore window
	Less media usage	

* Schedule full and incremental backups approximately 12 hours apart.

Document Level Backup Strategies

There are many factors that contribute to your backup strategy—backup window size, restore window size, server and storage hardware, the amount of available media, media retention time, network bandwidth, server load, and the size of your databases. Although it is important to consider all of these factors, for Document Level backups, the two most important factors are typically tape usage and the amount of time available for your backups. The following recommendations are based on these two factors. If other factors are more important in your environment, adjust your backup strategy accordingly.

The first task you must perform when determining a backup strategy is to assess the amount of time your organization has available each week for backing up your Exchange Server. Next, perform a backup of your Exchange Server using Document Level backup to ascertain how long the backup job will take. Finally, use this information to determine the most efficient way of backing up your Exchange Server within the time available to you.

If your organization's backup schedule allows you to perform a full backup at least one day a week, perform daily differential backups with one full backup a week.

If you want to distribute the full backup throughout the week, perform a full backup of only one storage group per day and rotate which storage group gets the full backup. Back up all other storage groups using differential backups.

Database Management Strategies for Document Level Backup Jobs

By default, BrightStor ARCserve Backup merges all job, session, and detail information into the database from the catalog file at the end backup jobs, which can quickly increase the size of the database. To reduce the size and increase the performance of the database when performing Document Level backups, you can use the following features:

- **Record Job and Session Information Only**—You can enable this feature from the Backup Manager while creating your backup job. To do this, click the Options button and select the Operation tab.

  When you use this feature, only job and session information is logged in the database, thereby reducing the size of the database.

  Note: This feature does **not** automatically merge details after a backup job, so you must manually merge the details. When you merge the details, BrightStor ARCserve Backup checks to see if the CATALOG.DB exists. If it does not exist, a request is sent to merge from tape.

- **Enable Catalog Database**—You can enable this feature from the Server Admin Manager. To do this, click the Config button and select the Database Engine tab.

  When you use this feature, BrightStor ARCserve Backup automatically provides transparent catalog database management functions (gets catalog file names, deletes catalog files, prunes catalog files using the preset database pruning cutoff date, purges catalog files, copies catalog files, and renames catalog files), and stores a copy of the catalog locally in a CATALOG.DB folder so that, if needed, it can be merged directly from this location rather from tape.

When to use these features depends on your environment. Use the following scenarios to determine when to use them:

- If you require the fastest merge performance, do not use either of the Enable Catalog Database or Record Job and Session Information Only features and let all of the information merge all of the time.

- If merging is a problem because of time or disk space, use **both** the Enable Catalog Database and Record Job and Session Information Only features. This reduces the size of the data, and reduces the merge time because of the cached local copy of the catalog.

- If you have very little disk space available, use only the Record Job and Session Information Only feature and do **not** use the Enable Catalog Database feature.

- Under no circumstances should you use **only** the Enable Catalog Database feature. Instead, use the Enable Catalog database feature only if you also enabled the Record Job and Session Information Only feature. Otherwise, there is no benefit in creating a catalog file on disk because all information is merged into the database.

Document Level Backup and Restore Performance Tuning

To maximize performance when using Document Level backup and restore:

- Increase the value of the Number of Threads configuration setting and decrease the value of the Thread Priority configuration setting. This combination increases performance and minimizes the impact on your server.

- Enable multiplexing to take advantage of high performance devices. Because destination devices are faster than a single Document Level backup stream, multiplexing decreases backup time by dividing your backup jobs into several sub-jobs that run simultaneously to the same device.

  If you enable multiplexing and also want to increase the value of the Number of Threads configuration setting, keep in mind that the Number of Threads value is per each backup stream. Therefore, the actual number of threads running on a system is the number of streams multiplied by the number of threads. As a result, leveraging multiplexing before leveraging the Number of Threads is optimal. For example, on a four processor machine with four storage groups, a total of six to eight threads is recommended. These threads should be configured as two threads per each storage group, resulting in four multiplexing streams. Because storage groups are independent resources, it is better to increase the level of streams with multiplexing than to increase the Number of Threads and sequentially back up one storage group at a time.

- Enable the Complete Messaging Single Instance Storage configuration option. This option checks to see if attachments and messages have already been backed up and backs up only one copy, eliminating the need to back up an attachment or message each time it is referenced. This can significantly decrease the size of your backups.

- If you are creating a short backup job or do not need an estimate of how long the job will take, enable the Disable File Estimate global option to save time.

- Use incremental and differential backup methods to back up only the data that has changed since your last full or incremental backup. This saves time by backing up only changed data rather than backing up all of your data.

- Use backup filters. This lets you exclude unwanted and large amounts of data from your backup jobs.

- If you want to reduce the disk space usage on your backup server, enable the Disable Database Recording global option when creating your backup job so that detail logs of every document are not recorded in the BrightStor ARCserve Backup database. If you use this option and later want to restore, you must first submit a Merge Media operation.

- If media usage is a major factor in your backup strategy, either perform full backups daily or full alternating with differential backups daily.

- In an environment that has non mission-critical data with less aggressive restore schedules, you should perform a full backup at least once a week and perform incremental or differential backups on the other days.

Restore Recommendations

Consider the following best practices for restoring the Exchange Server.

General Restore Strategies

Perform a test restore to a backup server **at least once a month** and make sure the restored database is functioning properly. For more information on how to perform a test restore, see Perform a Database Level Test Restore to an Alternative Location in the chapter "Performing Database Level Backups and Restores."

Document Level Restore Strategies

If you are restoring to an original location that contains existing data, select the conflict resolution option, **Overwrite only when modified**. If you are restoring to an original location in an empty folder or an alternative location, select the conflict resolution option, **Restore as copy**.

Backup and Restore Test Strategies

After you have developed backup and restore strategies, you need to test them to ensure that they work satisfactorily. You can perform backup tests on a production system; however, you should perform recovery tests on a test system that closely mimics the production system before applying your backup and restore strategies to the product system.

You should perform a test restore to a backup server at least **once a month** and make sure the restored database is functioning properly. This lets you test your backup and restore strategies to assess whether you are backing up your system accurately and to prepare for a possible disaster. For more information on how to perform a test restore, see Perform a Database Level Test Restore to an Alternative Location in the chapter "Performing Database Level Backups and Restores."

Note: Exchange Server 2003 has a recovery storage group, which can be used to test restores of a particular storage group. However, you should still practice restoring your entire Exchange Server to a test server.

Appendix A: Troubleshooting

This appendix provides troubleshooting information to help you identify and resolve problems that you may encounter when using the BrightStor ARCserve Backup Agent for Microsoft Exchange and BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on. To help you quickly find the information you need, this appendix lists some error messages and possible reasons and solution for these messages.

Activity Log

Many of the actions to resolve error conditions advise you to check the BrightStor ARCserve Backup Activity log. The Activity log contains comprehensive information about the operations performed by BrightStor ARCserve Backup. It provides an audit trail of all BrightStor ARCserve Backup activity for every job that is run. You can scan this log whenever necessary to see if any errors have occurred. The log is available from the Job Status Manager. For more information about using the Activity log, see the *Administrator Guide*.

Exchange Server Errors

For additional information on any Exchange Server error, check the Event Log on the Exchange Server or see the Microsoft web site.

Failed to Configure your Server or Authentication Failure

There are several reasons why these errors may occur. Each reason, and the action you can take to resolve the error, is described below:

Reason 1:

The account you are trying to verify does not have all of the necessary privileges, groups, and rights.

Action 1:

Use the Exchange Agent Configuration utility to create the backup agent service account and mailbox account automatically by enabling the Create a new account feature. When you use this utility, all of the necessary privileges, groups, and rights are applied.

Reason 2:

The account you are trying to verify does not have a mailbox on the Exchange Server you trying to configure.

Action 2:

Create a new account and specify the mailbox location as the local Exchange Server. Use the Exchange Agent Configuration utility to create this account automatically by enabling the Create a new account feature.

Reason 3:

Your mailbox name is not unique. A unique name is a name that does not exist in the organization as a subset of characters in another mailbox name. For example, you cannot use the name Admin, if there is a mailbox named Administrator in your organization.

Action 3:

Create a new user with a unique mailbox name.

Reason 4:

The Windows API that is called during verification requires that the account used to run the Exchange Agent Configuration has the "act as part of the operating system" privilege assigned to it.

Action 4:

Log on to the machine as the account you want to verify and run the configuration.

Reason 5:

The Windows Active Directory and Exchange Server caches may not have propagated a newly created user.

Action 5:

Propagating a newly created user can take minutes or hours depending on your domain configuration and traffic.

Reason 6:

The mailbox is not finalized and ready for use. On Exchange Server 2000, this may be because the Recipient Update Service (RUS) has not completed the mailbox. On Exchange Server 5.5, the mailbox has not yet been initialized.

Action 6:

Log into the mailbox or send mail to it to complete a newly created mailbox. On Exchange Server 2000, you can force the RUS to update the mailbox so it can be used immediately. To do this, open the Microsoft Exchange System Manager, expand the Recipients object in the left pane, and select Recipient Update Services. When you select this, your organization's recipient update services are displayed in the right pane. Right-click each service and select **Update Now**.

Reason 7:

The user or mailbox information that you entered is incorrect.

Action 7:

Make sure that you enter the correct user name, password, and alias name for your mailbox.

Reason 8:

A conflicting or incomplete Mapisvc.inf exists on the Exchange Server. This can occur if you have a messaging client installed that is creating its own version of Mapisvc.inf.

Action 8:

Find all copies of Mapisvc.inf on your Exchange Server and ensure that the most complete and accurate version is in the winnt\Systerm32 folder. If you need to make changes to Mapisvc.inf, first back up all copies of the file and see the Microsoft Q Article 294470 on the Microsoft web site for information on adding entries for Exchange Services.

Failed to create the user account '<MAILBOX ALIAS>', Failed to create the mailbox '<MAILBOX ALIAS>', or Failed to finalized the mailbox '<MAILBOX ALIAS>'

When performing a Document Level restore with new user and mailbox creation, the add-on:

- creates a basic user with minimal rights in the Users container of Active Directory.

- creates a mailbox for the user.

- sends a request to the recipient update service and sends a message to the mailbox to finalize it.

If all three of these steps are successful, you can view the mailbox in the Exchange System Manager. If any of these steps fail, the mailbox will not restore. There are several reasons why these steps may fail. Each reason, and the action you can take to resolve the error, is described below.

Reason 1:

The user account creation failed because the backup agent service account does not have enough rights to create a new account.

Action 1:

Ensure that your backup agent service account has the appropriate rights assigned to it. For information on these requirements, see Backup Agent Service Account Requirements for Document Level Backup and Restore in the chapter, "Performing Document Level Backups and Restores." Also, make sure that the backup agent service account is assigned membership to a group that has permissions over the Users container in Active Directory. For example the Account Operators group has these permissions by default.

Reason 2:

The user account or mailbox creation failed because the global catalog server could not be contacted or a Windows application or system error occurred.

Action 2:

Check the Event Viewer Application Log and System Log for recent errors. Also, check the agent logs DBAEXCUserSummary.log and WinUserUpd.log.

Reason 3:

The mailbox creation failed because a disabled mailbox with the same name already exists.

Action 3:

Check the Exchange System Manager to determine if there is a disabled mailbox with the same name. If you recently deleted a user account associated with the mailbox you are trying to restore, use the Run Cleanup Agent feature in the Exchange System Manager and purge the mailbox.

Reason 4:

The mailbox finalization failed because the Recipient Update Service failed to update the mailbox.

Action 4:

Make sure that the Recipient Update Service is able to finalize mailboxes when an update is called. You may have to rebuild the Recipient Update Service if it is not performing properly. For more information on the Recipient Update Service, see the Microsoft documentation.

Reason 5:

The mailbox finalization failed because of Active Directory replication delays or Exchange Server cache delays. This failure can occur even if the user or mailbox was successfully created.

Action 5:

In multi-domain controller environments or large Exchange Organizations, there may be delays before you can use the mailbox. If mailbox finalization fails, verify that the account appears in the Global Address List. If it appears in this list, repackage the failed mailbox with user and mailbox creation selected and run the job when the mailbox appears in the Exchange System Manager.

E8601 Failed to connect agent. (AGENT=agent name, EC=error message/code)

Reason 1:

The Backup Agent RPC Server service is not running on the target server.

Action 1:

Verify that the Backup Agent RPC Server service is running on the target server.

Reason 2:

The target database server may be stopped or inaccessible.

Action 2:

Verify that the target database server is running on the target server.

Reason 3:

The target server may be unreachable over the network.

Action 3:

Check network connections.

Reason 4:

(Windows error 1326) Machine authentication failure may have occurred because an incorrect user name or password was entered, or the user name was specified without a domain or machine name qualifier, and this qualifier is needed for this particular user on the target machine.

Actions 4:

- Check user name and password for machine login.
- Specify a domain qualifier for the user name used to log in to the database.

For a domain user, use this format:

```
Domain\User name
```

Reason 5:

(Windows error 1385) Machine authentication failure may have occurred because the specified user does not have sufficient rights to perform a backup.

Action 5:

Check that the user either has the "Backup files & Directories" right in the Local Security Policies of the database server machine or is a member of a group that has this right. This right is typically held by the Administrators group and the Backup Operators group.

Reason 6:

(Windows error 1387) Machine authentication failure may have occurred because the user name or password is missing.

Actions 6:

- Check user name and password for machine login.

- Specify a domain qualifier for the user name used to log in to the database.

For a domain user, use this format:

```
Domain\User name
```

Reason 7:

(Windows error 1314) Machine authentication failure may have occurred because the Backup Agent RPC Server service is running as a user who does not have sufficient privileges to log in to Windows.

Actions 7:

In the control panel, under Services (Windows NT) or Administrative Tools, Services (Windows 2000, XP, or 2003), check that the Backup Agent RPC Server is running as LocalSystem, or as a user that is a member of the Backup Operators group.

If the Backup Agent RPC Server is running as a user that is a member of the Backup Operators group, make sure that the Backup Operators group has the "Act as part of the Operating System" right in the Local Security Policies of the database server computer.

Reason 8:

A failure to load the agent DLL into memory may have occurred because there is insufficient memory available, the agent DLL does not exist in the agent home directory, or the DLL path is incorrect in the registry.

Action 8:

Verify that the target server has sufficient free memory available.

Reason 9:

The user ID or password that you entered does not match the user ID or password that you used to configure the backup agent service account for Brick Level backups.

Actions 9:

- Verify that the job package has the correct security.

- Use the Account Configuration dialog in the Exchange Agent Configuration utility to verify whether the account you are currently using is the same account that you used to configure for Brick Level backup and restore.

- If you changed your user password or mailbox name, reconfigure the agent.

- If you are trying to connect to a virtual server on a cluster, verify that the virtual server is running on a physical node where the account is configured for Brick Level backup and restore.

Reason 10:

When configuring the backup agent service account for Brick Level backups, the specified mailbox was hidden in Exchange Server.

Action 10:

Do not hide the backup agent service account mailbox.

E8602 Failed to read from database. (DBNAME=object name, EC=error message/code)

Reason 1:

An internal or communication error occurred when the agent attempted to read a backup object from the Database server or from the Database server to BrightStor ARCserve Backup.

Action 1:

Perform the following steps on the server that is running the agent:

1. Confirm that the database agent is running.
2. Confirm that the database is running.
3. Make certain no other backup or restore jobs are running on the database you are attempting to back up.
4. Restart the Backup Agent RPC Server service.
5. Resubmit the backup job.

If the problem reoccurs, check the network connections. If the problem persists, contact Computer Associates Customer Support.

Reason 2:

A network error has occurred.

Action 2:

Check all possible network related issues, such as inconsistent communication, time-outs, drivers, and settings on all networking related hardware.

Reason 3:

Two BrightStor ARCserve Backup Managers are attempting to back up the same Exchange Server database simultaneously.

Action 3:

Reschedule one of the backup jobs to avoid the conflict.

Reason 4:

A transaction log file for an Exchange Server 5.5 Database Level backup is either missing or corrupt.

Action: 4

For information on how to resolve this issue, see the following Microsoft related article:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q178934

Reason 5:

There is insufficient space on the hard disk on which the agent is installed for your Database Level backup.

Action 5:

Increase the free disk space on the drive where the agent is installed or reinstall the agent to a drive that has more space.

Reason 6:

(EC=69 READ/WRITE ERROR IN NAMED PIPES) Antivirus software on your server may be interfering with the Brick Level MAPI calls.

Action 6:

Check your Antivirus settings on the Exchange Server. If they are scanning incoming and outgoing, change it to Incoming Only or test your Brick Level backup with the Antivirus software turned off. In some cases, Antivirus software drivers can cause a problem even if they are not active. For more information on MAPI-AVAPI issues, see Microsoft Q Articles Q263949 and Q267431 on the Microsoft web site.

Reason 7:

There are corrupt objects in a mailbox that you included in a Brick Level backup job.

Action 7:

Check the job log associated with your failed Brick Level backup. If you find the backup failing on the same mailbox, exclude the mailbox and perform a test job to see if it runs properly. Also, clean out the mailbox that is causing the failure.

Reason 8:

A Brick Level backup failed because of a corrupt database.

Action 8:

Consult Microsoft about running the isinteg or eseutil utilities to check the integrity of the Exchange Server database and mailboxes.

Reason 9:

A specific folder failed to open during a Brick Level backup of public folders. This error usually indicates access is denied to that particular folder.

Action 9:

Check the permissions on the respective public folder and make sure there are no restrictive rights on the folder to the backup agent service account.

E8603 Failed to write to database. (DBNAME=object name, EC=error message/code)

Reason 1:

This error occurs when the agent writes data streams from BrightStor ARCserve Backup to a target object (DBNAME=object name) in the Database server.

Action 1:

Check the agent log file for details.

Reason 2:

An Exchange Server Database Level incremental or differential backup failed to restore.

Action 2:

Restore the latest full backup or copy session before you restore an incremental or differential backup.

Reason 3:

An Exchange Server Database Level restore is missing a log or a log is corrupt.

Action 3:

Restore an incremental or differential backup that includes the missing logs if they are available. If there are logs missing from the server, do not select the Commit existing logs option when restoring. For more information on how to manually restore partial log sequences, see the Microsoft web site.

Reason 4:

An attempt was made to restore the Exchange Server Directory or Information Store to an alternative server that has different organization and site names. When restoring to an alternative server, organization and site names must be identical to the server that you are restoring from.

Actions 4:

- When restoring to an alternative location, make sure you meet all of the requirements documented in the *Microsoft Exchange 5.5 Disaster Recovery* white paper, available at the Microsoft web site.

- If you filled out your server configuration worksheet in this guide for each of your Exchange Servers, use the worksheets to determine organization and site names. You also may be able to verify organization and site names by checking the Exchange Server agent log (dbaexch.log).

E8604 Failed to start backup. (DBNAME=object name, EC=error message/code)

Reason 1:

(Windows error 1326) Machine authentication failure may have occurred because an incorrect user name or password was entered, or the user name was specified without a domain or machine name qualifier and this qualifier is needed for this particular user on the target machine.

Actions 1:

- Check user name and password for machine login.

- Specify a domain qualifier for the user name used to log in to the database.

For a domain user, use this format:

```
Domain\User name
```

Reason 2:

(Windows error 1385) Machine authentication failure may have occurred because the specified user does not have sufficient rights to perform a backup.

Action 2:

Check that the user either has the "Backup files & Directories" right in the Local Security Policies of the database server machine, or is a member of a group that has this right. This right is typically held by the Administrators group and the Backup Operators group.

Reason 3:

(Windows error 1387) Machine authentication failure may have occurred because the user name or password is missing.

Actions 3:

- Check user name and password for machine login.

- Specify a domain qualifier for the user name used to log in to the database.

For a domain user, use this format:

```
Domain\User name
```

Reason 4:

(Windows error 1314) Machine authentication failure may have occurred because the Backup Agent RPC Server service is running as a user that does not have sufficient privileges to perform a Windows login.

Actions 4:

- In the control panel, under Services (Windows NT) or Administrative Tools, Services (Windows 2000, XP, or 2003), check that the Backup Agent RPC Server is running as "LocalSystem", or as a user that is a member of the Backup Operators group.

- If the Backup Agent RPC Server is running as a user that is a member of the Backup Operators group, make sure that the Backup Operators group has the "Act as part of the Operating System" right in the Local Security Policies of the database server computer.

Reason 5:

Database authentication failure may have occurred because an incorrect user name or password was entered, or the user name was specified without a domain or machine name qualifier and this qualifier is needed for this particular user on the target machine.

Actions 5:

- Check user name and password for machine login.

- Specify a domain qualifier for the user name used to log in to the database.

For a domain user, use this format:

```
Domain\User name
```

Reason 6:

Database authentication failure may have occurred because the necessary database services are not started.

Actions 6:

- Verify that the database you are trying to back up is mounted and the necessary services are running.

- Verify that the Backup Agent RPC Server service is started.

Reason 7:

The agent was unable to establish a named pipe connection to the BrightStor ARCserve Backup Manager.

Action 7:

Perform the following steps on the server that is running the agent:

1. Restart the Backup Agent RPC server service.

2. If possible, disable your Antivirus software to determine if it is conflicting. Disable named pipe scanning to prevent possible conflicts.

3. Disconnect all open shares to the agent machine (by name or IP) and run the backup again. To disconnect open shares from the machine where the BrightStor ARCserve Backup Manager is installed, right-click My Computer and select **Disconnect Network Drive** or use the **net use** command at the command prompt.

Reason 8:

The mailbox used to configure the backup agent service account for Brick Level backups has been disabled or deleted.

Action 8:

Open the Exchange System Manager and see if the mailbox exists. If it exists but is disabled, associate the mailbox with another user.

Reason 9:

(Backup Agent Error 116) The versions of the agent and add on that are installed are newer than the version of the BrightStor ARCserve Backup that is installed.

Action 9:

Install the latest version of BrightStor ARCserve Backup.

E8605 Failed to start restore. (DBNAME=object name, EC=error message/code)

Reason 1:

(Windows error 1326) Machine authentication failure may have occurred because an incorrect user name or password was entered, or the user name was specified without a domain or machine name qualifier and this qualifier is needed for this particular user on the target machine.

Actions 1:

- Check user name and password for machine login.
- Specify a domain qualifier for the user name used to log in to the database.

For a domain user, use this format:

```
Domain\User name
```

Reason 2:

(Windows error 1385) Machine authentication failure may have occurred because the specified user does not have sufficient rights to perform a backup.

Action 2:

Check that the user either has the "Backup files & Directories" right in the Local Security Policies of the database server machine, or is a member of a group which has this right. This right is typically held by the Administrators and Backup Operators groups.

Reason 3:

(Windows error 1387) Machine authentication failure may have occurred because the user name or password is missing.

Actions 3:

- Check user name and password for machine login.
- Specify a domain qualifier for the user name used to log in to the database.

For a domain user, use this format:

```
Domain\User name
```

Reason 4:

(Windows error 1314) Machine authentication failure may have occurred because the Backup Agent RPC Server service is running as a user that does not have sufficient privileges to perform a Windows login.

Actions 4:

■ In the control panel, under Services (Windows NT) or Administrative Tools, Services (Windows 2000, XP, or 2003), check that the Backup Agent RPC Server is running as LocalSystem, or as a user that is a member of the Backup Operators group.

■ If the Backup Agent RPC Server is running as a user that is a member of the Backup Operators group, make sure that the Backup Operators group has the "Act as part of the Operating System" right in the Local Security Policies of the database server computer.

Reason 5:

Database authentication failure may have occurred because an incorrect user name or password was entered, or the user name was specified without a domain or machine name qualifier and this qualifier is needed for this particular user on the target machine.

Actions 5:

■ Check user name and password for machine login.

■ Specify a domain qualifier for the user name used to log in to the database.

For a domain user, use this format:

```
Domain\User name
```

Reason 6:

Database authentication failure may have occurred because the necessary database services are not started.

Actions 6:

■ Verify that the database you are trying to back up is mounted and the necessary services are running.

■ Verify that the Backup Agent RPC Server service is started.

Reason 7:

When restoring a Database Level backup, the Erase All Data Before Restoring option was selected together with either the Public **or** the Private Information Store.

Action 7:

When using the Erase All Data Before Restoring option, select the Public **and** the Private Information Store.

Reason 8:

The mailbox used to configure the backup agent service account for Brick Level backups has been disabled or deleted.

Action 8:

Open the Exchange System Manager and see if the mailbox exists. If it exists but is disabled, associate the mailbox with another user.

Reason 9:

You have submitted a Brick Level restore of a mailbox to a non-existent or an uninitialized mailbox.

Action 9:

Make sure that the mailbox name selected for the destination exists, is not disabled, and has been initialized before performing the restore.

Reason 10:

For Exchange Server 2000 and 2003. The Information Store service is not running, or the database you want to restore does not exist or is not dismounted.

Actions 10:

- Verify that the database you intend to restore exists.
- Dismount the database you intend to restore.
- Enable the database to be overwritten by a restore.

Reason 11:

An invalid target was specified for your Database Level restore.

Action 11:

If you filled out your server configuration worksheet in this guide for each of your Exchange Servers, use the worksheets to verify the destination server parameters and make sure they match the parameters on the sever that you are restoring from.

E8617 Failed to end restore. (DBNAME=object name, EC=error message/code)

Reason 1:

The agent failed to recover the Database server after a restore job. An internal error occurred in either the agent or the Database server.

Action 1:

Check agent log file for details.

Reason 2:

An Exchange Service did not start in a specific time interval after the restore or an Exchange Service failed to start because of an invalid restore sequence.

Action 2:

Try to start the service manually. For additional information on this error, check the Event Log on the Exchange Server or see the Microsoft web site.

Information for Customer Support

If you need to contact Computer Associates Computer Support for additional assistance, use the following registry keys to gather the information Customer Support will need to help resolve your issues:

For Database Level backup and restore:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\BrightStor ARCserve
Backup\DSAgent\CurrentVersion\agent\dbaexch
Value Name:    Debug
Value Type:    REG_DWORD
Value Data:    0(off) or 1(on)
Results:       Dbaexch.log & dbaexch*.trc, in Exchange agent directory
```

Note: Restart the Backup Agent RPC Server service.

For Brick Level backup and restore:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\BrightStor ARCserve
Backup\DSAgent\CurrentVersion\agent\dbaxchg2
Value Name:    Debug
Value Type:    REG_DWORD
Value Data:    0(off, default)-3(on,verbose)
Results:       Dbaxchg2.log & dbaxchg2*.trc, in Exchange agent directory
```

Note: Restart the Backup Agent RPC Server service.

For Document Level backup and restore:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\BrightStor ARCserve
Backup\ExchangeDocumentAgent\Parameters
Value Name:     Debug
Value Type:     REG_DWORD
Value Data:     0(off), 1(default), 4(verbose)
Results:        Expaadp*.log & expaadp*.trc, in Exchange agent LOG
directory
```

Note: You do not need to restart the Universal Agent service.

If the trace files grow too large, you can use the following registry values to reduce the size:

```
Value Name:     MaxLogSize
Value Type:     REG_DWORD
Value Data:     size of each trace file in MB
Result: As soon as the size is reached, a new trace file will
                be generated.



Value Name:     DeleteLogFile

Value Type:     REG_DWORD
Value Data:     0, 1
Results:        0: When a new trace file is generated, the previous trace
file            will NOT be deleted. 1: When a new trace file is generated,
                    the previous trace file will be deleted.
```

Appendix B: Frequently Asked Questions

This appendix includes frequently asked questions to help you resolve issues that may arise when using the BrightStor ARCserve Backup Agent for Microsoft Exchange and BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on. To help you quickly find the information you need, this appendix is divided into the following categories:

- General

- Database Level Backup and Restore

- Document Level Backup and Restore

- Brick Level Backup and Restore

General Questions

The following questions are general questions.

Question:

What BrightStor ARCserve Backup agents and options do I need to protect my Exchange Server?

Answer:

The following agents and options can be used to protect different parts of your Exchange Organization:

- **BrightStor ARCserve Backup Agent for Microsoft Exchange—** Includes Database and Brick Level backup and restore. Database Level backup and restore protects the Exchange Server database and logs. Brick Level backup and restore lets you perform folder-level backup and restore.

- **BrightStor ARCserve Backup Agent for Microsoft Exchange-Premium Add-on—**Includes Database Level and Document Level backup and restore. Database Level backup and restore protects the Exchange Server database and logs. Document Level backup and restore, which is only available with this add-on, eases and expedites many administrative tasks and maximizes flexibility by offering the most granular level of restore.

- **BrightStor ARCserve Backup Agent for Windows**—Protects files and system state, including Active Directory. It is important to protect Active Directory when using Exchange Server 2000 and 2003 because it stores mailbox and user information. BrightStor ARCserve Backup Agent for Windows also protects your domain controllers, which are equally as important to protect as your Exchange Server.

- **BrightStor ARCserve Backup Disaster Recovery Option**—In the event of a disaster, the BrightStor ARCserve Backup Disaster Recovery Option recovers the machine to the last full backup state.

Question:

Do I need BrightStor® ARCserve® Backup Agent for Open Files to protect my Exchange Server if I am using the BrightStor ARCserve Backup Agent for Microsoft Exchange?

Answer:

No. BrightStor ARCserve Backup Agent for Open Files is beneficial when you want to protect files that are open or in use by active applications. Because the BrightStor ARCserve Backup Agent for Microsoft Exchange is an application-specific agent, dedicated to protecting Microsoft Exchange, it offers a complete and robust solution that encompasses all the features offered by BrightStor ARCserve Backup Agent for Open Files.

Question:

Do I need an email client like Microsoft Outlook installed on the Exchange Server I am backing up?

Answer:

No, it is not a requirement that you have an email client on the Exchange Server you are backing up.

Question:

If I add new objects that I want to back up, like a mailbox, to my Exchange Organization after I submit a backup job, do I need to resubmit the job to include the new objects?

Answer:

It depends on how you originally packaged the job. If you used dynamic job packaging, your new objects will be included because the contents of what you selected are determined when the job runs. If you used explicit job packaging, you must resubmit the job to include your new objects because the contents of what you selected are determined at the time the job is packaged. For more information on dynamic and explicit job packaging, see the *Getting Started*.

Question:

What is the M drive (ExIFS) and do I need to back it up?

Answer:

The M drive is a virtual drive that exposes Exchange Server 2000 mailboxes and public folders. It is simply a view of Exchange Server 2000 and not a physical drive, so you do **not** need to back it up, which is why it is skipped when you perform a backup job using the Client Agent for Windows.

Question:

Why are the names of the standard folders in my mailbox displayed in a different language?

Answer:

Most standard folders are created and named using the language of the first client to access them. For example, if the first client you use to access a new mailbox is a French client, standard folders like the Inbox or Sent Items are given French names. For more information, see the Microsoft Q Article 188856 on the Microsoft web site. For more information about controlling the language that is used, see the **Create mailbox if not existing** option under the Document Level Restore Options section in the chapter "Performing Document Level Backups and Restores."

Database Level Backup and Restore Questions

The following questions relate to database backup and restore.

Question:

When performing a Database Level restore, when should I use the Apply existing logs option?

Answer:

You should use the Apply existing logs option if you are restoring to the original server you backed up from and you believe the transaction logs are all sequentially present and not corrupt. Do not use this option if you are restoring to a different server or if have a reason to believe that any of the existing transaction logs on the server you are restoring to are missing or corrupt. If you enable this option and the agent detects that logs are out of sequence, the agent automatically disables it so that the job does not fail.

Question:

If I perform a Document Level backup or Brick Level backup, do I still need to perform a Database Level backup?

Answer:

Yes. Database Level backup is the fundamental backup for your Exchange Server, and you should always use it regardless of whether you use one of the other granular backup types. You can use Database Level backups to restore Exchange Server in the event of a system failure, database corruption, or disaster recovery situation.

Question:

When should I perform full database backups?

Answer:

In addition to the full database backups you perform during your weekly backup strategy, perform full database backups after installing service packs, after performing restores, and after changing the Circular Logging setting on your Exchange Server.

Question:

Can I restore to the Recovery Storage Group?

Answer:

Yes, but only when using Database Level Restore with Exchange Server 2003. For more information on the Recovery Storage Group, see your Exchange Server documentation

Document Level Backup and Restore Questions

The following questions relate to document level backup and restore.

Question:

What is Single Instance Storage?

Answer:

Single Instance Storage is the method Exchange Server uses to process messages. This method stores only one copy of a message, links it to multiple recipients in the Information Store, and uses references to the message in each recipient's mailbox. Single Instance Storage applies to individual attachments and other message components.

The backup and restore products that you can use to protect your Exchange Server support varying levels of Exchange Server's Single Instance Storage:

- **No Single Instance Storage**—Without Single Instance Storage, an Exchange Server is scanned mailbox-by-mailbox and copies of individual message bodies and attachments are backed up as they arrive, without any regard for data that may have been backed up already.

- **Partial Single Instance Storage**—Partial Single Instance Storage support backs up attachments only once, but continues to back up other message components, like message bodies, every time they are referenced. This translates into large amounts of unnecessary backup duplication because most messages do not include attachments, but all messages include message bodies and other message components.

- **Complete Single Instance Storage**—Complete Single Instance Storage checks to see whether each attachment, message body, and other single instance components of a message have been backed up already, and backs up only one copy. This is the fastest and most efficient solution because it removes unnecessary backup duplication and maximizes performance.

Document Level backup and restore supports Complete Single Instance Storage. Brick Level backup and restore does not support Single Instance Storage.

Question:

What setting should I select for the log level detail when I am configuring for Document Level backup and restore?

Answer:

The log detail level determines the level of detail in the debug trace and log. This does not affect the level of detail in the Activity Log in the BrightStor ARCserve Backup Manager. The default log detail level value is 1 and the supported range is between 0 and 4. If you want to disable agent side logging, use 0. Otherwise, you should always use level 1 unless you are instructed to raise the level by a trained Computer Associates Customer Support technician for troubleshooting purposes.

Question:

When I restore a document to the same location using the **Overwrite conflict** resolution option, why do I sometimes see duplicated messages?

Answer:

When a message is restored, a new message ID is created and assigned to it. Consequently, if you restore from one backup multiple times, you will see duplicated messages.

Question:

Can I perform a Database Level backup at the same time as a Document Level backup?

Answer:

Yes, you can perform a Database Level and Document Level backup at the same time. You can also perform multiple Document Level backups at the same time, and you can perform multiple Database Level backups at the same time by running up to one job for each storage group.

Question:

If I perform a Document Level backup, is there any benefit in also performing Brick Level backup?

Answer:

No.

Question:

How can I tell how much space is saved by backing up with Complete Single Instance Storage enabled?

Answer:

After you submit your backup job, you can go to the Job Status Manager and double-click the active job to view real-time job properties. If you have Complete Messaging Single Instance Storage enabled, all of the fields related to size will reflect the size prior to single instance storage optimization. The actual size of the backup after single instance storage optimization opens in the Activity Log and is labeled "(*xx*)MB Written to Media".

Brick Level Backup and Restore Questions

The following questions relate to brick level backup and restore.

Question:

How does antivirus software affect my Brick Level backup?

Answer:

There are several different types of antivirus software file systems and email virus scanners that integrate with Microsoft Exchange Server. Only one of these types may impact your Brick Level backups—AVAPI-based scanning. AVAPI-based scanners scan each message as it arrives. Consequently, your scanners may slow down your backups because the agent must wait for messages to be scanned before it can perform the backup.

Question:

Can I manually configure the backup agent service account that is required for Brick Level backup and restores?

Answer:

Yes. For instructions on how to manually configure the backup agent service account, see the appendix "Configuring the Backup Agent Service Account Manually."

Question:

What is MAPI and how does it relates to Brick Level backup and restore?

Answer:

Brick Level backups rely upon the Messaging Application Programming Interface (MAPI) to access the items in the mailbox for backup.

Question:

What hardware should I use on my Exchange Server to maximize the performance of my backups?

Answer:

For Database Level backups, use faster disk drives. For Document Level backups, use faster CPU speed, more memory, and more processors. For Brick Level backups, use faster CPU and more memory. If you are performing remote backups of your Exchange Server, network speeds may also play a significant role in the maximum throughput.

Question:

What impacts the speed of Brick Level backups?

Answer:

The most time-consuming part of a Brick Level backup is extracting the data from the Exchange Server through MAPI, which is a CPU-intensive operation.

Question:

How can I tell which backup agent service account is configured for Brick Level backup and restores?

Answer:

Run the Exchange Agent Configuration Utility. The fields will be populated with the configured backup agent service account information. If the fields are empty, no account is configured.

Appendix C: Configuring Your Backup Agent Service Account Manually

After you install the BrightStor ARCserve Backup Agent for Microsoft Exchange, you must set up a backup agent service account on your Exchange Server. The backup agent service account grants the agent the authority to communicate with the Exchange Server.

Set Up your Backup Agent Service Account Manually

To set up your backup agent service account manually, you must perform the following steps:

1. Determine your backup agent service account requirements.

2. Determine your tasks.

3. Determine your environment.

4. Use the procedures in this appendix to set up your account.

Backup Agent Service Account Requirements Overview

The requirements for your backup agent service account depend on the type of backup and restore (Database Level backup and restore, Document Level backup and restore, or Brick Level backup and restore) you will be using. To determine these requirements, see information about backup agent service account requirements in the chapters "Performing Database Level Backups and Restores, " "Performing Document Level Backups and Restores, " or "Performing Brick Level Backups and Restores."

Note: If you plan on using more than one type of backup and restore (for example, both Database Level and Document Level), your backup agent service account must meet the requirements for all types. Brick Level backup and restore requirements include all of the requirements for Document Level backup and restore and Database Level backup and restore. Document Level backup and restore requirements include all of the requirements for Database Level backup and restore.

Task Requirements

After you decide on your backup agent service account requirements, you must determine your tasks. Depending on your requirements, you must perform one or more of the following tasks:

- Create a user
- Create a mailbox
- Add groups
- Add rights
- Delegate roles

Environment Requirements

Each task you must perform to manually set up your backup agent service account is dependant on one or more of the following factors:

- The version of Exchange Server you are using:
  - Exchange Server 5.5
  - Exchange Server 2000 or 2003
- The version of Windows you are using:
  - Windows NT
  - Windows 2000 or 2003
- The type of server you are using:
  - Domain controller
  - Member server

How Account Setup Works

The following sections are divided into tasks. Each task includes different procedures based on the environment. Select the tasks and environments that match your needs and use the corresponding procedures to manually set up your backup agent service account. Also, for additional configuration considerations, see Additional Configuration Considerations.

User Setup

Use one of the following procedures to set up a user.

Important! *If you already have a domain account, you do not have to create a user. You can use the domain account as your backup agent service account. To do this, simply use your domain account to set up a mailbox, add groups, add rights, and delegate roles.*

Create a User for all Versions of Exchange Server on a Windows 2000 or 2003 Domain Controller

To create the backup agent service account:

1. On your domain controller, from the Start menu, select All Programs, Administrative Tools, and select Active Directory Users and Computers.

2. When the Active Directory dialog opens, expand the Active Directory Users and Computer tree and click Users.

3. From the Action menu, select New, User.

4. When the New Object - User dialog opens, in the First name field, enter a name for your backup agent service account, enter a User logon name, and then click Next.

5. Enter a password, confirm the password, enable the **Password never expires** option, and then click Next.

6. Click Finish.

Create a User for all Versions of Exchange Server on Windows NT Domain Controller

To create the backup agent service account:

1. On your Exchange Server, from the Start menu, select All Programs, Administrative Tools (Common), User Manager for Domains.

2. From the User menu, select New User.
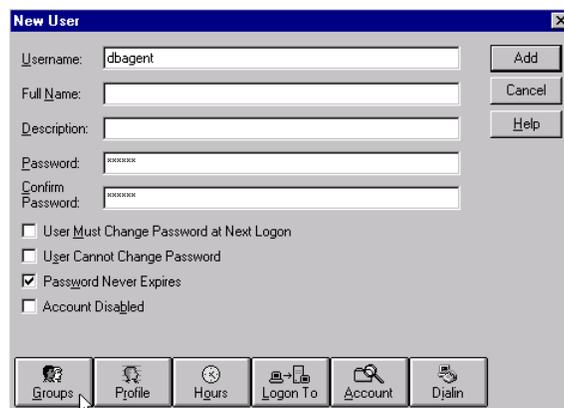
3. Enter a user name, password, confirm your password, disable the User Must Change Password at Next Logon option, and enable the **Password Never Expires** option.

Mailbox Setup

Use one of the following procedures to set up a mailbox.

Create a Mailbox for Exchange Server 2000 or 2003 on a Windows 2000 or 2003 Domain Controller

To create an Exchange Server mailbox for the backup agent service account:

1. On your domain controller, from the Start menu, select All Programs, Administrative Tools, and select Active Directory Users and Computers.

2. When the Active Directory dialog opens, expand the Active Directory Users and Computer tree and click Users.

3. From the Action menu, select New, User.

4. When the New Object - User dialog opens, in the First name field, enter a name for your backup agent service account, enter a User logon name, and then click Next.

5. Enter a password, confirm the password, enable the Password never expires option, and then click Next. If you have Exchange Server installed, the following dialog opens.
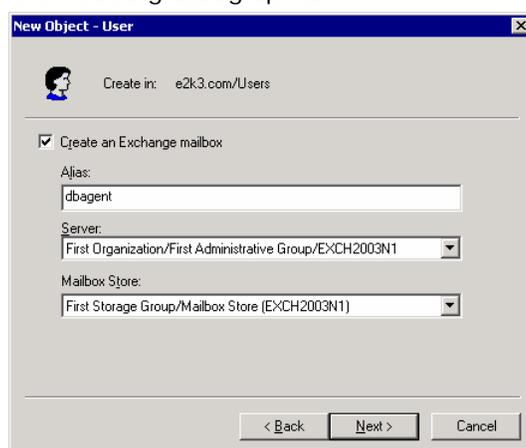
6. Make sure the **Create an Exchange mailbox** option is enabled. In the Alias field, the User Logon name is automatically displayed. If you want to change it, enter a new name. In the Server field, select the server you are going to install on. In the Mailbox Store field, select a mailbox store. Click Next.
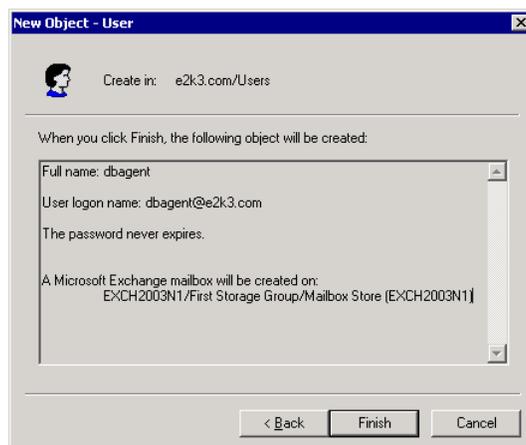
7. Confirm your selections and click Finish.

Note: After you finish creating your backup agent service account and mailbox, you should log into this account by using Outlook or by sending an email to the account to finalize the mailbox.

Create a Mailbox for Exchange Server 5.5 on any Windows Domain Controller or Member Server

To create an Exchange Server mailbox for the backup agent service account:

1. From the Start menu, select Programs, Microsoft Exchange, Microsoft Exchange Administrator.

2. When the Microsoft Exchange Administrator dialog opens, in the left pane, select Recipients and, from the File menu, select New Mailbox.

3. When the Properties dialog opens, enter a unique name for the mailbox in the First field. This name auto populates the Alias field. The alias name must not be a subset of any other mailbox alias. Click Primary Windows NT Account.

4. When the Primary Windows NT Account dialog opens, make sure Select an existing Windows NT account is selected, and then click OK.

5. When the Add Users and Groups dialog opens, in the List Names From field, select the appropriate domain. In the Names list, select the name of your backup agent service account, click Add, and then click OK.

6. Click OK.

Note: After you finish creating your backup agent service account and mailbox, you should log into this account by using Outlook or by sending an email to the account to finalize the mailbox. Enter information in all fields in the Name section, and then click the Primary Windows NT Account button.

Group Setup

Use one of the following procedures to add groups.

Add Groups for all Versions of Exchange Server on a Windows 2000 or 2003 Domain Controller

To add groups:

1. On your domain controller, from the Start menu, select All Programs, Administrative Tools, and select Active Directory Users and Computers. From the Active Directory Users and Computers dialog, in the right pane, right-click your new account name and select **Properties**.
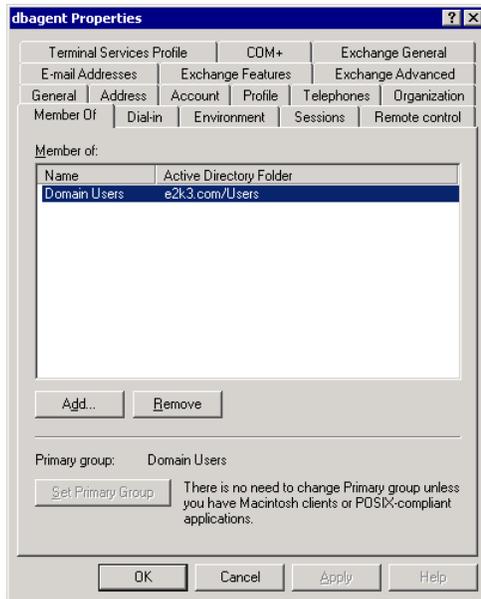
2. When the Properties dialog opens, click the Member Of tab and click Add.
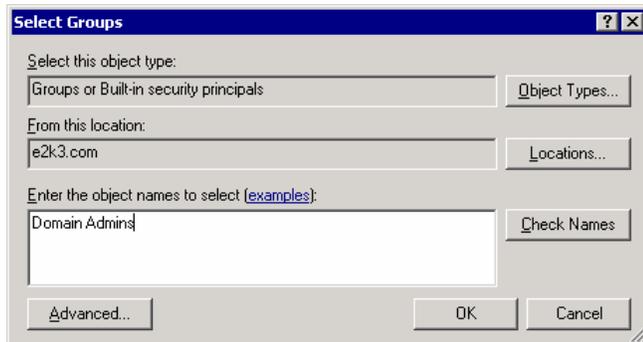
3. When the Select Groups dialog opens, type **Domain Admins** in the "Enter the object names to select" field and click OK.

   Note: If your Exchange Server is your domain controller, you must also select Administrators and Backup Operators.
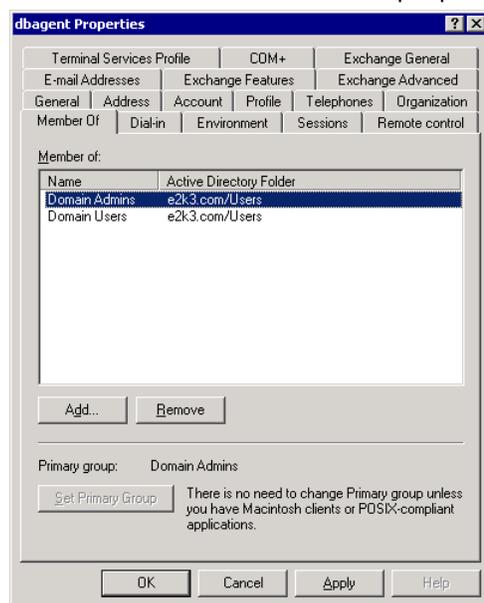
4. When the Properties dialog reappears, select **Domain Admins** and click Set Primary Group. Next, select Domain Users, click Remove, click Yes, and then click OK.

Add Groups for all Versions of Exchange Server on a Windows 2000 or 2003 Member Server

To add groups:

1. Right-click My Computer and select **Manage**.
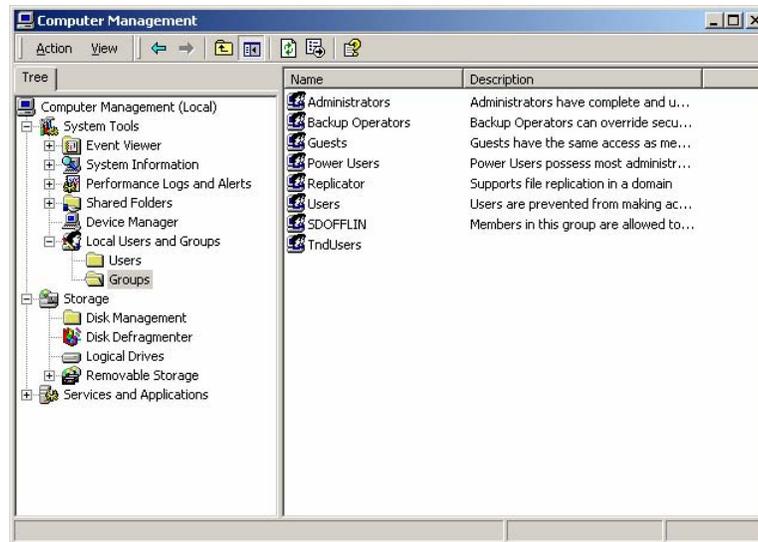
2. When the Computer Management dialog opens, expand the Local Users and Groups object and click Groups.

3. In the right-pane, double-click Administrators.

4. When the properties dialog opens, click Add.

5. When the Select Users or Groups dialog opens, in the Look in field, select the appropriate domain. Next, in the Name column, select the name of your backup agent service account, click Add, and then click OK.

6. When the Properties dialog reopens, the name of your backup agent service account is displayed in the Members list. Click OK.

7. When the Computer Management dialog reopens, in the right-pane, double-click Backup Operators and repeat steps 4 through 6.

Add Groups for Exchange Server 5.5 on a Windows NT Domain Controller or Member Server

To add groups:

1. From the User Manager, double click your backup agent service account from the Username list and, when the User Properties dialog opens, click Groups to specify the group assignments for the new account. Select Administrators, Backup Operators, and Domain Admins from the list at the right, and click Add. Select **Domain Admins** and click Set. Select Domain Users, click Remove, and then click OK.

    Note: If this Exchange Server is a member server, you do not have to add group membership to the Domain Admins. Set the Primary Group to Administrators.
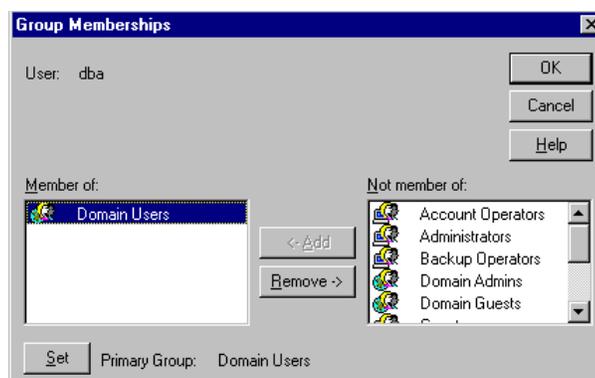
2. In the New User dialog, click Add.

3. When the properties dialog opens, click OK.

4. When the New User dialog reopens, click Close.

When the User Manager dialog opens, your new account is listed in the Username column.

Rights Setup

Use one of the following procedures to add rights.

Add Rights for all Versions of Exchange Server on a Windows 2000 or 2003 Domain Controller or Member Server

1. On your Exchange Server, select Start, Programs, Administrative Tools, Domain Security Policy.

   Note: If your Exchange Server is a member server, select Local Security Policy rather than Domain Security Policy.

2. When the security settings dialog opens, in the left pane, expand Local Policies and select User Rights Assignment.

3. In the right pane, double-click Act as part of the operating system.

4. When the security policy setting opens, click Add.

5. When the Select Users or Groups dialog opens, in the Look in field, select the appropriate domain. Next, in the Name column, select the name of your backup agent service account, click Add, and then click OK.
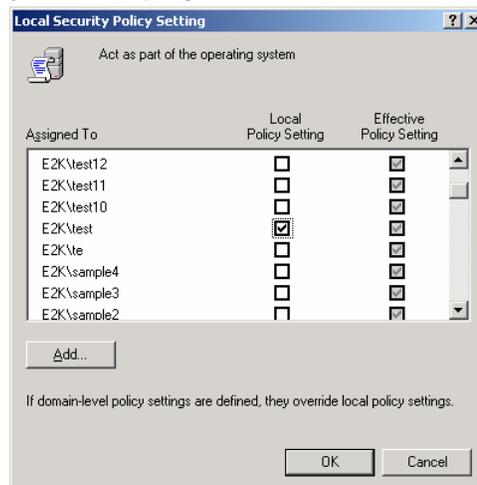
6. When the security policy setting dialog reopens, in the Assigned To field, locate the name of your backup agent service account, place a check mark next to it in the Local Policy Setting column, and then click OK.

   Notes:

   ■ If you are modifying a Local Security Policy, effective Policy settings are updated when you log in to the server. To update your Effective Policy setting, log out and log back in.

   ■ If you are modifying a Local Security Policy, the current Effective Policy setting may have been inherited from policies within the domain. If this is the case, those domain policies have to be changed.

7. Repeat steps 3 through 6 for the Log on Locally and Log on as Service rights.

Add Rights for Exchange Server 5.5 on a Windows NT Domain Controller or Member Server

1. From the User Manager, highlight your new account name and, from the Policies menu, select User Rights.
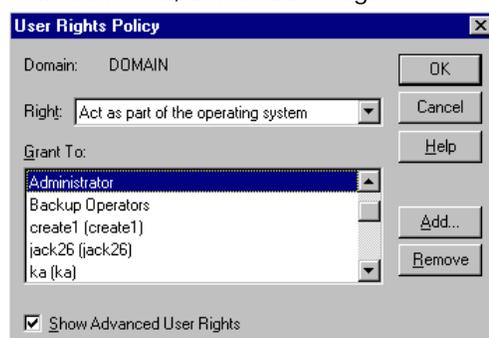
2. When the User Rights Policy dialog opens, enable the **Show Advanced User Rights** option and, in the Right field, select **Act As Part of the Operating System**, and then click Add.
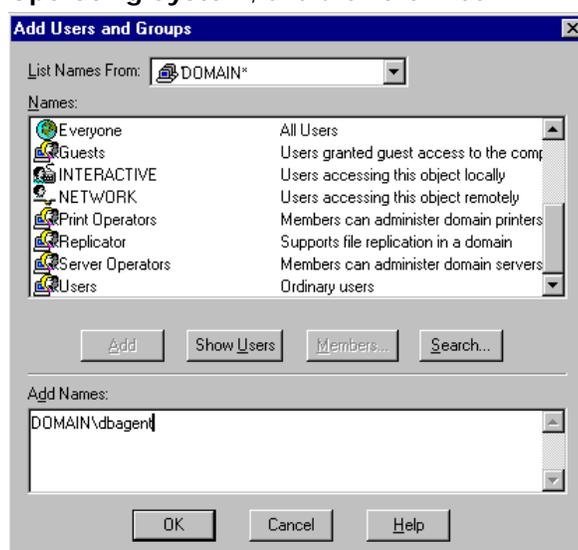
3. When the Add Users and Groups dialog opens, in the List Names From field, select the appropriate domain and click Show Users. In the Names list, select the name of your backup agent service account, click Add, and then click OK.

4. When the User Rights Policy dialog reopens, repeat steps 9 and 10 for the Log on Locally and Log on as Service rights.

Role Setup

Use one of the following procedures to delegate roles.

Delegate Roles for Exchange Server 2000 or 2003 on a Windows 2000 or 2003 Domain Controller or Member Server

To assign permissions for the backup agent service account:

1. On the Exchange Server, from the Start menu, select All Programs, Microsoft Exchange, System Manager.

2. When the Exchange System Manager dialog opens, right-click the name of your organization and select **Delegate control**.
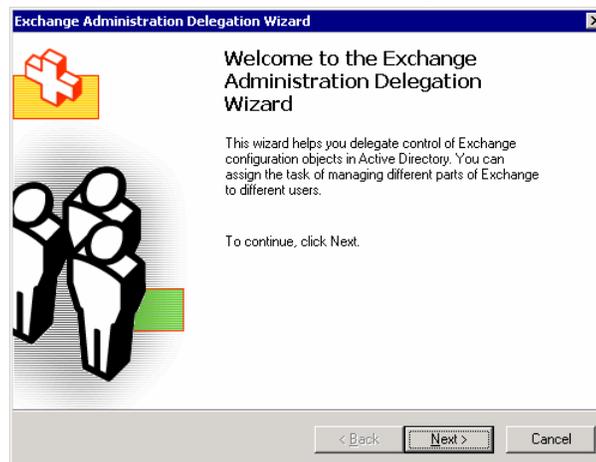
3. When the Exchange Administration Delegation Wizard opens, click Next.
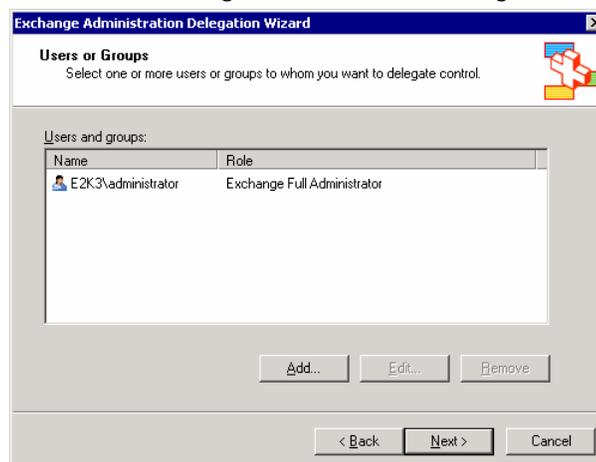
4. When the Users or Groups dialog opens, click Add.
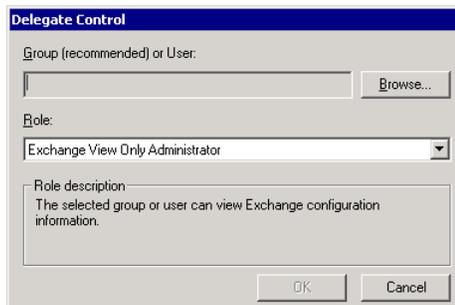
5. When the Delegate Control dialog opens, in the Group filed, click Browse.
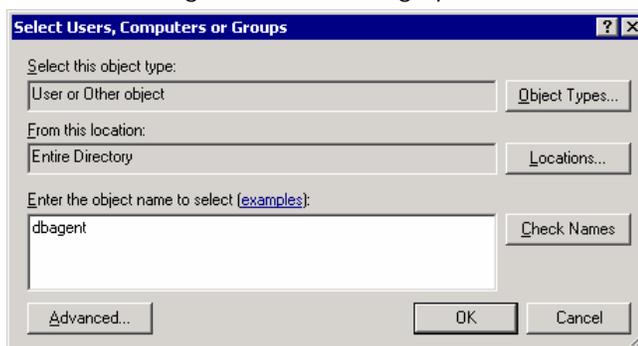
6. Enter the name of your Backup Agent System Account and click OK.
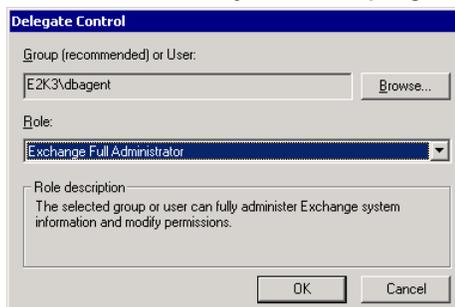
7. When the Delegate Control dialog reopens, in the Role field, select **Exchange Full Administrator** and click OK.

    The name of your account opens in the Users and groups field.
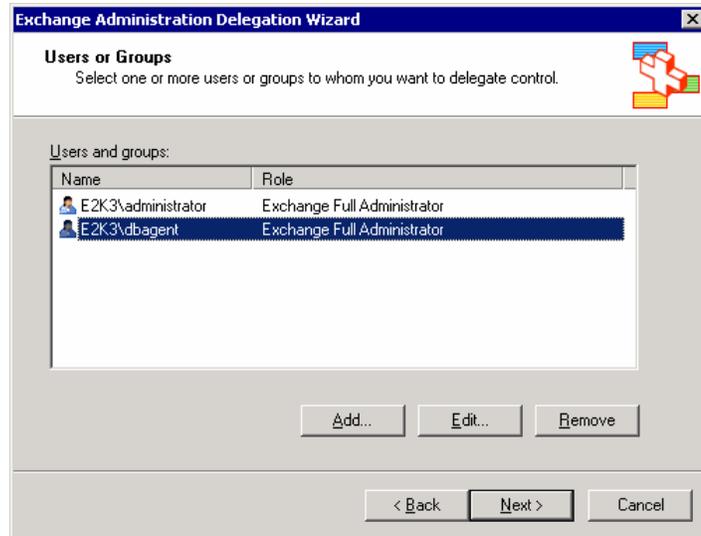
8. Click Next.

9. Click Finish.

Delegate Roles for Exchange Server 5.5 on any version of Windows Domain Controller or Member Server

After you create your backup agent service account and mailbox, you must assign permissions to this account so that it has control over the mailboxes in Exchange Server. You must assign permissions at the following levels of the organization tree:

	Organization
	Site
	Configuration

To assign permissions for the backup agent service account:

1. From the Start menu, select Programs, Microsoft Exchange, and Microsoft Exchange Administrator.

2. When the Microsoft Exchange Administrator dialog opens, select the Organization name in the left pane and, from the File menu, select **Properties**.

3. When the properties dialog opens, click the Permissions tab, and then click Add.

4. When the Add User or Group dialog opens, in the List Names From field, select the appropriate domain. In the Names list, select the name of your backup agent service account, click Add, and then click OK.
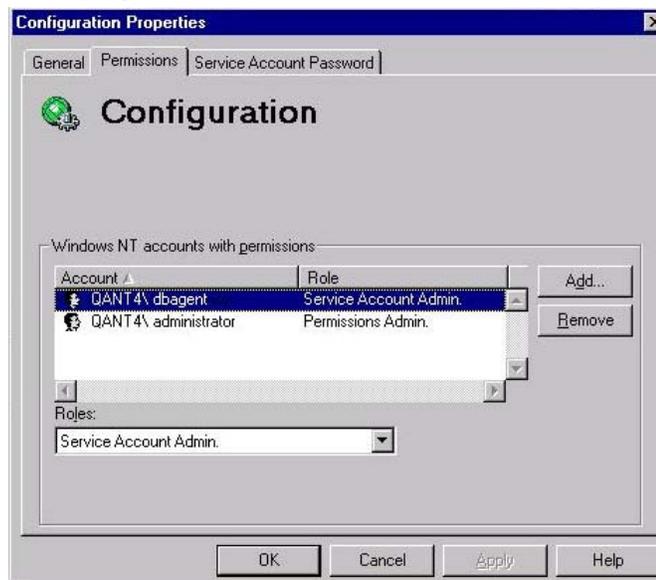
5. When the properties dialog reopens, in the Account list, select the name of your backup agent service account. Next, in the Roles field, select Service Account Admin, and then click OK.

6. When the Microsoft Exchange Administrator dialog opens, repeat steps 2 to 5 for the Site and Configuration levels of the organization tree.

Additional Configuration Considerations

The following sections include additional configuration considerations, depending on your environment.

Member Server Considerations

If your Exchange Server is on a member server, you may need to add the backup agent service account to the same groups and rights on the domain controller, depending on the domain controller security policies and the OU security settings.

Multiple Domain Considerations

If your Exchange Server is running on a network that has multiple domains and you want to create the backup agent service account in a different domain than the domain where your Exchange Server is located, add the groups and rights in both domains.

Grant Additional Rights in Exchange Server 2000

Exchange Server 5.5 included a Service Account that allowed unrestricted access to all mailboxes. To enhance security, Exchange Server 2000 did not include this Service Account. As a result, if you need unrestricted access to all mailboxes in Exchange Server 2000, your account is a member of Domain Admins, and your other security settings do not give you this access, use the following procedure:

Note: If your account is not a member of Domain Admins, see the Microsoft web site for Microsoft Knowledge Base Article 262054, XADM: *How to Get Service Account Access to All Mailboxes in Exchange* 2000.

1. Go to Start, All Programs, Microsoft Exchange, System Manager, and select **System Manager**.

2. When the Exchange System Manager dialog opens, in the left pane, expand Administrative Groups until you find the mailbox store or public folder store for which you want to have full mailbox access.

3. Right-click mailbox store or public store, select **Properties**. When the properties dialog opens, click the Security tab.

   Note: If you do not see the Security tab, see the Microsoft web site for Microsoft Knowledge Base Article 259221, XADM: *Security Tab Not Available on All Objects in System Manager*.
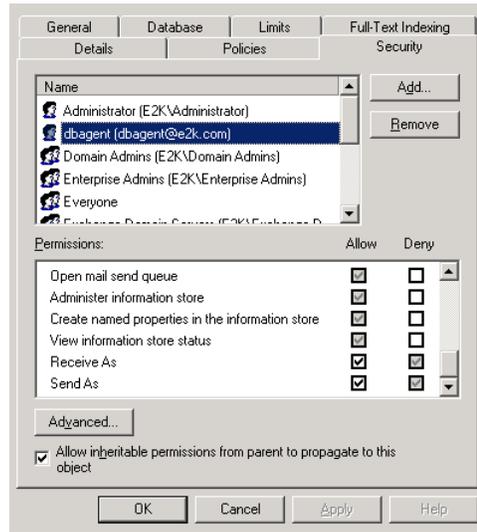
4. In the Name column, select the name of your backup agent service account. Next, in the Permissions box, place a check mark in the Allow box next to the Receive As and Send As permissions, and then click OK.

   Note: When you place a check mark in the Allow box, it overrides the Deny box, but only at the level where you are granting permission. For example, if you are granting permission for a mailbox store, the permission applies only to the mailbox store and not to its parent or children objects.

5. Repeat steps 2 through 4 for each database object you want to have full mailbox access to.

Use Alternate Domain Configuration for Exchange Server 2000 and 2003

If you plan on using Document Level backup and restore or Brick Level backup and restore, and you are using Exchange Server 2000 and 2003 and do not want to assign your backup agent service account to the Domain Admins group, use the following procedure:

1. Create a domain account on the domain controller.

2. Create a mailbox on the server you want to install the agent on.

3. Add the backup agent service account to the Administrators group on the Exchange Server.

4. Add the backup agent service account to the Exchange Services or Exchange Domain Servers groups.

5. Delegate Control in the Exchange Organization.

6. (Only for Brick Level backup and restore) Grant the Log on Locally right.

7. (Only for Brick Level backup and restore) Grant the Log on as a service right.

8. (Only for Brick Level backup and restore) Grant the Act as part of operating system right.

Appendix D: Server Configuration Worksheet

To limit the amount of time you spend troubleshooting restore issues during a disaster recovery, consult the Exchange System Manager to gather information and complete the following worksheet for each Exchange Server 2000 and 2003 server in your Exchange organization.

Note: The information you enter into the worksheet is case sensitive.

When restoring to an alternative location, information in all fields in this worksheet except the Server Name field must be the same on the server you are restoring to.

Server Name:

Exchange Server Version,
Service Pack, and Patches:

Exchange Organization Name:

Administrative Group Name:

Storage Group Name:	Database Store Names:

Storage Group Name:	Database Store Names:

Storage Group Name:	Database Store Names:

Storage Group Name:	Database Store Names:

LegacyExchangeDN Value:

Note: See the Microsoft web site for information on how to determine the LegacyExchangeDN value.

Index