

Realtime
publishers

The Essentials Series: Configuring
Microsoft Exchange for Fast Recovery

Backup Methods Available for Exchange

by Ron Barrett

Backup Methods Available for Exchange.....	1
Backup Methodology	1
Backing Up Domain Controllers	2
VSS vs. Streaming (Legacy) Backups	2
Backup Best Practices	3
Four Types of High-Availability Solutions in Exchange 2007	3
Local Continuous Replication	3
Cluster Continuous Replication	4
Standby Continuous Replication	4
Single Copy Cluster	5
High Availability for the Remaining Server Roles	5

Copyright Statement

© 2008 Realtime Publishers, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers, Inc or its web site sponsors. In no event shall Realtime Publishers, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

Backup Methods Available for Exchange

To be sure you have the ability to perform fast recoveries in Exchange Server, you need to be sure you have a good method of backup. The backup must be fast, complete, and, of course, recoverable. This article will look at different backup methodologies and consider some of the new features in Exchange 2007 that make fast recovery possible. We will then look at considerations for backing up the various server roles and domain controllers. Finally, we will finish up with backup best practices.

Backup Methodology

Estimates show that 80 percent of all corporate knowledge is stored in email. Gartner estimates that businesses lose \$25 per hour, per employee when email is down. Suppose your organization supports one database of 250 mailboxes, which is down for 1 hour; you are looking at a cost of \$6250 per hour.

Considering these numbers, you can see the importance of making sure that your Exchange backup plan includes not only database and logs but also the operating system (OS) and all volumes on the server. The first article in this series addresses recovery point objective (RPO); to reiterate, it is a determined acceptable data loss measured in time. To meet fast recovery objectives, you must also consider Recovery Time Objectives. RTOs are defined as the duration of time that the systems need to be restored.

RTO is tied to service level agreements (SLA), which are part of the business continuity plan. Thus, the RTO encompasses not only how fast the system needs to be back online but also the acceptable level of operation. Thinking along these lines, you need to consider a few factors: What media will you back up to? Will it be tape, SAN, NAS? How often will you back up? Will nightly backups be performed or do you need more frequent intra-day backups? Each of these decisions will affect the RPO and RTO and ultimately your plan for fast recovery.

In addition, each of these factors is crucial and comes with a pain threshold (how much you want to spend versus how much you're willing to lose). When you look at the potential costs associated with a critical data loss, fast recovery just makes sense.

Backing Up Domain Controllers

It is important to think about backing up domain controllers in an Exchange environment. Since Exchange Server 2003, the importance of Active Directory (AD) to Exchange makes it necessary to ensure you have at least one domain controller backed up for fast recovery. Performing a system state backup on a domain controller will back up the necessary AD files. Remember that domain controllers have circular logging enabled for AD; therefore, any data written to AD after a backup will be lost. Depending on the frequency of changes to your domain controllers, you should back up at least one domain controller nightly. Doing so will ensure that you can meet RPO and RTO levels and ensures that you will not run into trouble by having an “old” AD backup, which would be un-restorable.

VSS vs. Streaming (Legacy) Backups

Exchange Server offers two options for backing up data. Both support the four backup methods (full, incremental, differential, and copy). The options are the traditional streaming (legacy) backup, which utilizes the ESE API and has been the available option for backing up Exchange Server using NTBackup, Windows Server Backup, and many third-party backup solutions. Highlights of streaming (legacy) backup:

- Backup is taken from the active copy of the database
- Can perform backup at the database level
- Only one backup running against a single storage group
- Separate storage groups can be backed up concurrently

Warning

Windows Server 2008 does not support streaming backups and is not Exchange-aware. Therefore, a third-party solution that utilizes VSS is required for Exchange backup in Windows Server 2008.

The second method utilized is the Volume Shadow Copy Service (VSS), which provides a point in time “snapshot” of your data. In subsequent backups, it looks at the last snapshot and then backs up *only* the changes. VSS was introduced to Exchange 2003; although it provides the ability to take shadow copies, these copies were made at the file level and were not Exchange-aware. Snapshot backups in Exchange are fast and consistent due to the use of checksums to the database pages. Highlights of VSS:

- Backup can be taken from the active and passive copy of the database
- Can perform backup at the storage group level
- Separate storage groups can be backed up in parallel

Backup Best Practices

Shrinking the backup window in Exchange can be achieved with the use of multiple storage groups. Keeping databases to a manageable size will also shrink the time it takes to back up those databases. The high-availability solutions considered in the next section can help to shrink backup windows by requiring less need for full backups. Replication can be the primary fast recovery option with backup as the secondary option.

Microsoft has a great document titled "[What Needs to Be Protected](#)," which is a good gauge for how to setup your backup strategy.

Another best practice is to create reliability for backups. This can be done several ways. One way I like to emphasize is the use of disk backups for Exchange. After you have a disk backup of the Exchange Server, you can use tape backup to create redundancy.

Four Types of High-Availability Solutions in Exchange 2007

Exchange 2007 SP1 provides four high-availability solutions to ensure a percentage-based uptime to the Mailbox role in Exchange. First, let's look at a quick description of each replication type and then explore the pros and cons of each.

Local Continuous Replication

As the name suggests, Local Continuous Replication (LCR) creates a continuous local copy of the active storage group to a second set of disks using log shipping and replay.

Pros:

- Cheapest solution requiring only a disk or disks and secondary controller
- Can implement on a single server
- Can perform VSS backups on the passive side

Cons:

- Failover needs to be implemented manually
- Hardware failures could make data unavailable
- Only one database can be added to a storage group running LCR

Cluster Continuous Replication

Cluster Continuous Replication (CCR) creates a continuous copy of the data over to a second server, and uses log shipping to maintain a copy of a storage group onto non-shared storage. Clustering adds automation to replication.

Pros:

- Provides automatic failover
- Provides both disk and server redundancy
- Utilizes the transport dumpster to maintain data that has not been synchronized between clusters
- Can perform VSS backups on the passive side

Cons:

- Requires knowledge of clustering services
- Requires an additional server and software to implement (that is, additional cost)

Standby Continuous Replication

Introduced in SP1, Standby Continuous Replication (SCR) uses the same log shipping and replay technology as LCR employs. Replication is server to server, but it does not require clustering services to provide redundancy.

Pros:

- Provides both disk and server redundancy
- Can be used in conjunction with the other three replication methods
- Replay delay protects from database corruption to the SCR copy

Cons:

- Failover needs to be implemented manually as with LCR
- Management is done through the Exchange Management Shell (EMS)

Single Copy Cluster

Similar to Exchange Server 2003 clustering technology, Single Copy Cluster (SCC) uses a single copy of the storage group that is located on shared storage in a cluster.

Pros:

- Provides automatic failover
- Supports up to eight cluster nodes

Cons:

- Requires knowledge of clustering services
- Requires an additional server and software to implement

High Availability for the Remaining Server Roles

As replication is used for the Mailbox server role only, how do you ensure that the remaining roles are backed up properly? Let's talk about how to achieve high availability in the remaining server roles. Providing high availability for the Client Access, Hub Transport, Edge Transport, and Unified Messaging servers is for the most part similar:

- Client Access Server—Deploy multiple client access servers and use Network Load Balancing (NLB) to provide high availability.
- Hub Transport Server—Resilient by default due to the fact that all Hub Transport servers are registered within AD. You can achieve high availability by deploying multiple hub transport servers.
- Edge Transport Server—Deploy multiple edge transport servers and use DNS MX records to achieve high availability.
- Unified Messaging Server—Deploy multiple unified messaging servers and place them into the same dial plan so that the VoIP gateways can retrieve a list of servers within the dial plan. Configure VoIP gateways to round-robin calls to ensure high availability if a unified messaging server is down.

Once you have a reliable backup plan that meets your RPO, RTO, and SLA requirements, and you have the ability to test that backup to ensure reliability, you need to move on to the last part of the fast recovery plan—finding out both how to recover Exchange quickly and ensure you have what you need in your environment once Exchange is recovered. The next article will explore this topic and consider recommendations for recovery in Exchange Server.