Best Practices for Microsoft Exchange

https://campus.barracuda.com/doc/44436296/

> **Best Practice**
> Use these tips and recommendations to efficiently protect your Microsoft Exchange
> environment using Barracuda Backup.

Barracuda Backup provides two different types of Microsoft Exchange backups:

1. **Native Backup (Entire Exchange server and databases)** – To protect the entire Microsoft Exchange Server and the Exchange databases, install the Barracuda Backup Agent. Microsoft Exchange protection is achieved by leveraging Microsoft Volume Shadow Copy Service (VSS) and the Exchange VSS Writer. This level of protection is designed to rebuild your entire Microsoft Exchange Server or to provide the ability to restore an entire Exchange database either by overwriting an existing database or by restoring to a Recovery Database. This is the primary backup and recovery method for Microsoft Exchange.
2. **Message-Level Backup** – Message-level backup provides a quick way to restore individual email messages to the original location or to an alternate mailbox. Message-level backup is not intended to be a disaster recovery option for your Microsoft Exchange environment and is used in conjunction with Agent-level Microsoft Exchange environment backups. Message-level backups are configured as a separate data source from your agent-based Exchange Server backup. Message-level backups leverage Microsoft Exchange Web Services (EWS) and are configured on the Exchange Client Access Server (CAS).

Each backup method provides its own advantages and disadvantages. The best practices in this guide are designed to help you find the best level of protection for your Microsoft Exchange environment and to meet your recovery objectives.

Microsoft Exchange Server Protection

> **Best Practice**
> Document the Exchange Server configuration in detail and any subsequent changes including all applied hotfixes and service packs. Additionally, it is highly recommended that you familiarize yourself with the Microsoft documentation for Exchange database management, disaster plans, and recovery.

- The Barracuda Backup Agent must be installed on each Exchange server
- Microsoft Volume Shadow copy Service (VSS) and VSS Writer must be enabled
- Ensure that Exchange is not being backed up by more than one backup solution; using more than one backup solution can cause issues with Transaction Log backups and possibly result in

data corruption
- Circular logging must be disabled if you want to do the following:
  - Run incremental backups
  - Recover data up to the point of failure
- Allow sufficient disk space for maintenance and recovery procedures, e.g., allow additional disk space for a recovery database
- Attempt to keep moderate-sized Exchange databases; if databases are large, backup and recovery times will increase
- Perform test restores periodically to ensure that disaster recovery and data recovery scenarios produce the expected results
- Verify that backups have completed successfully before attempting any maintenance within the Exchange environment

With Barracuda Backup, you can:

- Select individual or multiple databases for backup

Protect Exchange database availability groups (DAGs)

- Install the Barracuda Backup Agent on each node
- By default, only the active database is backed up on each node
- Passive database backup can be optionally configured

  > For details on backing up Exchange DAGs, refer to the section *Microsoft Exchange Database Availability Groups* in the article [Protecting Microsoft Exchange](#).

Perform regular **Complete** Exchange database backups weekly through Backup Schedules:

- Set your Backup type to **Smart** mode to allow Barracuda Backup to automatically determine whether **Complete** or **Log** backup is appropriate
- Create two schedules for your Exchange server; create one schedule to back up once weekly using **Complete** backup mode, and create a second schedule to back up daily using **Log** backup mode

  Best Practice
  Transaction log truncation occurs after every backup, **Complete** or **Log**.

  Important
  In Exchange 2010 and later, log truncation occurs on both **Complete** and **Log** backups. However, if the Exchange 2010 or later database is part of a DAG, the logs are truncated only up to the earliest checkpoint of the database replica on any node.

Barracuda Backup provides the following Microsoft Exchange recovery options:

- Overwrite an existing database
- Restore to a Recovery Database

When restoring to an Exchange server that is *not* the source server, ensure the following:

- The recovery server is in a different Active Directory (AD) forest than the source server;
- The recovery server has the same Organization and Administrative Group names as the source server; and
- The database already exists on the recovery server and has the same name as the original database.

Message-Level Exchange Protection

- Restore individual email messages without having to restore or mount the Exchange database
- Email messages can be restored to the original mailbox or to an alternate mailbox
- Use Message-level backup in conjunction with agent-level protection of the Exchange environment only
- Message-level backup is not intended to recover corrupted or deleted user mailboxes, instead, use an Exchange Recovery Database in this scenario
- Message-level backups do not contain Exchange items such as Contacts, Calendars, and Tasks
- Configure message-level backups as a separate data source from your Agent-based Exchange Server backup
- Message-level backups leverage Microsoft EWS
- Message-level backups are configured from the Exchange CAS
- A service account with an Exchange mailbox and SMTP address is required

For more information on message-level backup, see the *Exchange Message-Level Backup* section in the article Protecting Microsoft Exchange.