



# Symantec Backup Exec Blueprints

## Blueprint for Exchange

**Backup Exec Technical Services**

Backup & Recovery Technical Education Services



## Notice



This Backup Exec Blueprint presentation includes example diagrams that contain objects that represent applications and platforms from other companies such as Microsoft and VMware. These diagrams may or may not match or resemble actual implementations found in end user environments. Any likeness or similarity to actual end user environments is completely by coincidence.

The goal of the diagrams included in this blueprint presentation is not to recommend specific ways in which to implement applications and platforms from other companies such as Microsoft and VMware, but rather to illustrate Backup Exec best practices only.

For guidelines and best practices on installing and configuring applications and platforms from other companies, please refer to best practice documentation and other resources provided by those companies.

- **Blueprints** Help Customers Avoid Common Challenges/Pitfalls
- Each **Blueprint** Contains:
  - **Recommended Configuration:** Best-practice implementation example
  - **Life Preservers:** Best practices and pitfalls to avoid
- Use **Blueprints** to:
  - Present the Backup Exec best practice implementation example
  - Highlight key “life preserver” guidelines to avoid problems

# Example Diagram: Microsoft Exchange

## High-level best practices



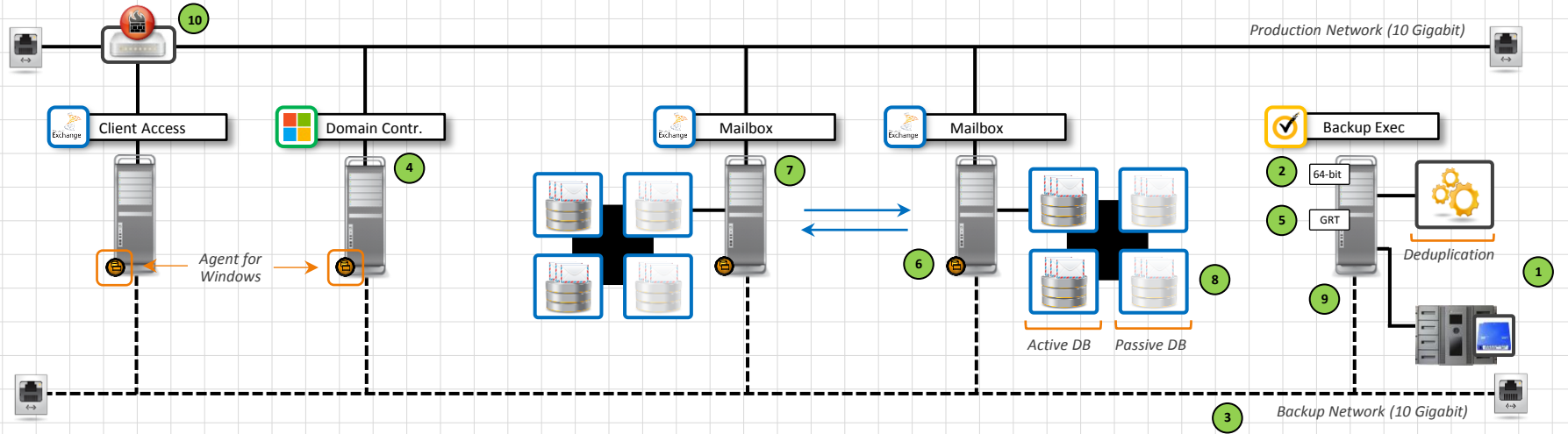
Start

Preface

How to Use

Example Diagram

Life Preservers



### High-level Best Practices

- 1 Backup Exchange data to disk first and then copy to tape (D2D2T) for optimal performance
- 2 Use a [64-bit Backup Exec server](#) (hardware and operating system) for Exchange 2010/2013
- 3 Leverage a separate network for backups (prevents saturation, improves performance)
- 4 [Protect the Active Directory infrastructure](#) in addition to Exchange components
- 5 Enable [Granular Recovery Technology](#) for optimal recovery flexibility
- 6 Ensure all required Backup Exec logon account permissions are configured properly
- 7 [Uniquely named mailbox](#) required for Exchange Granular Recovery
- 8 For high-availability configurations, protect the passive copy of mailbox servers/databases
- 9 [Exchange Management Tools](#) may be required on the Backup Exec server
- 10 When firewall access is required, [ensure ports are configured properly](#)



- Place Exchange transaction logs on separate disk from database
  - *If the disk with database is damaged, transaction logs remain available as recovery resource*
- Avoid making the Exchange server a domain controller
  - *Active Directory won't need to be recovered first during restore*
- Install Exchange into a domain with 2+ domain controllers
  - *Databases on a failed domain controller can be updated with replication*
- For Exchange 2010/2013 use a Database Availability Group with at least one passive database copy for each database
  - *If you can make more than one passive copy, the second passive copy should use a log replay delay of 24 hours*
- For Exchange 2010/2013 a 64-bit Backup Exec server is required



- For physical Exchange servers, the Agent for Windows should be installed on the Exchange server
- For Exchange 2010/2013 Database Availability Group (DAG) configurations, the Agent for Windows should be installed on each mailbox server
- To enable Granular Recovery, the Agent for Windows must be installed on Client Access Servers

**Note:** As this is a Backup Exec granular recovery technology specific requirement for Exchange we do not require the purchase of the Agent for Windows (AWS) for the CAS servers, just simply install AWS to each one

- The Agent for Windows must be running under the 'Local System' account on the Exchange server as well as the Backup Exec server
- The file versions of the Agent for Windows on the Backup Exec server and on the Exchange server should match



- Minimal Permissions required for Backing Up Exchange 2010 and Microsoft Exchange 2013: <http://www.symantec.com/docs/TECH212113>
- Backup Exec must have access to a uniquely named mailbox
- Unique mailbox must be activated
  - <http://www.symantec.com/docs/TECH24691>
- Backup Exec Logon Account:
  - For Exchange 2007, needs to be a member of '*Organization Administrator*' group
  - For Exchange 2010 and 2013, needs to have the '*Organization Management*' role
  - Needs to be member of the local computers Administration group on the Exchange servers



- For full backups, enable Granular Recovery Technology
  - *Enables granular object restore without requiring separate mailbox backup*
- For GRT backups, change default staging location on Backup Exec server to a volume that is not the system volume
  - *This volume should possess the same disk sector size as the volume used for Exchange transaction log storage on the Exchange server*
  - *See technote: <http://www.symantec.com/docs/TECH164166>*
- Ensure scheduled maintenance for the Information Store does not run at the same time as the database backup



- Run Exchange backup jobs separately from other backup jobs
- Back up the Active Directory on a regular basis
- Run a backup after you make any changes to system settings or application settings
- For Exchange 2007, select individual storage groups for backup rather than individual databases
- To perform incremental and differential backups of storage groups, ensure that circular logging is not enabled

# Thank You!

## Backup Exec Product Management