Symantec Backup Exec Blueprints

Blueprint for Large Installations

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

Introduction

Key terms and principles

- Central Admin Server Option (CASO)

Management of large/distributed Backup Exec environments

  - *Centralized management and monitoring*
  - *Load balancing of backup operations*
  - *Centralization of backup data*

Offsite disaster recovery management

- Advanced Disk Backup Option (ADBO)
  - *Synthetic backups*
  - *True Image Restore*
  - *Off host backups*

- Centralization of Information
  - *Monitor the status of managed Backup Exec servers (MBES)*
  - *Ensure backup devices are online and operational*
- Active Alerts
  - *Enables administrators to quickly identify and drill-down to problems*
  - *Focus on high priority tasks and resolve problems quickly*
- Server Grouping
  - *Group servers by any desired attribute*
  - *Quickly filter views to specific servers rather than sort through long list*
- Compliance and Auditing

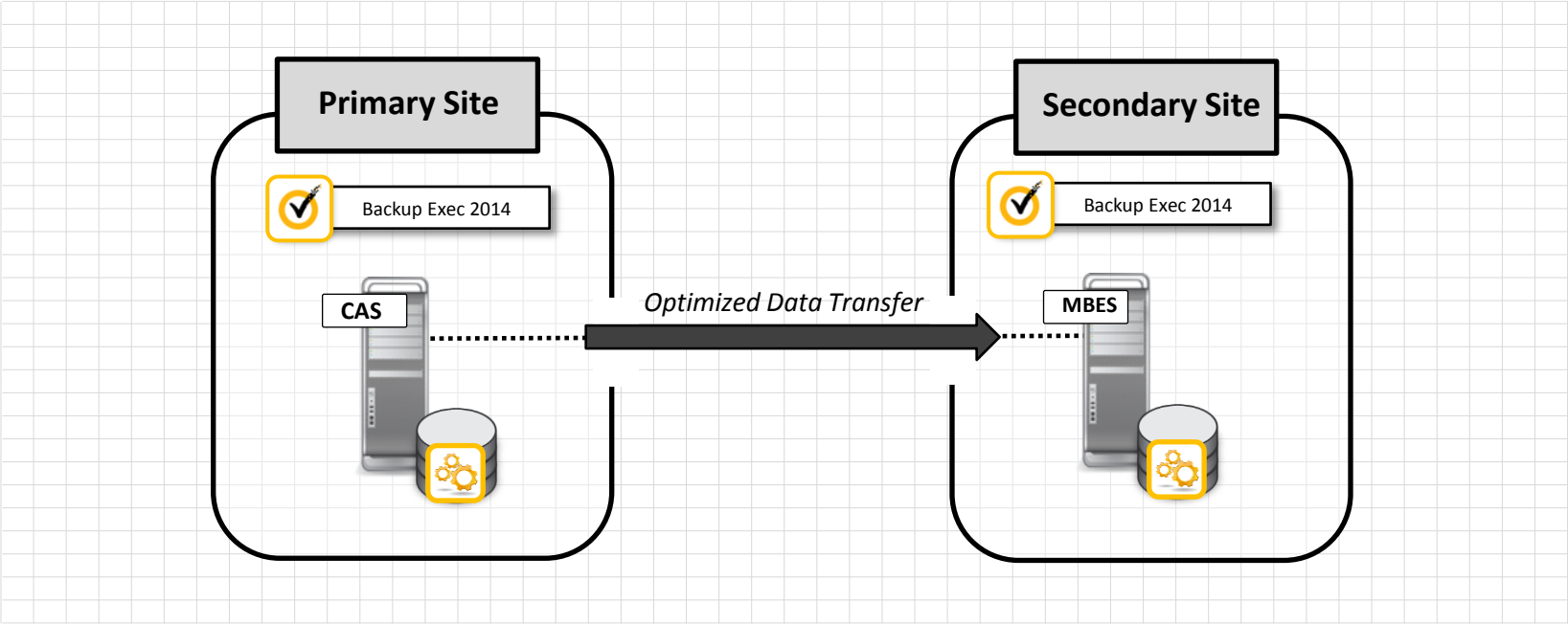
- Backup Exec Server Centrally Managed by a CAS
- Will Have Access to One or More Backup Devices
  - *Locally attached*
  - *Accessible via LAN/SAN*
  - *Shared from other MBES*
- Processes Backup and Restore Tasks
  - *Assigned from CAS*
  - *Assigned by local administrator*
- Can Be Configured in 'Pools' for Load Balancing

- Relates to Management of Backup Devices Attached to an MBES
- Can Be Managed Centrally by CAS or Locally by MBES
- Configuration Has Direct Impact on CAS/MBES Bandwidth Requirements
  - *Whether connection must be persistent*
  - *Whether connection must be low-latency*

Device and Media Local to the MBES (Remote Site Configuration)	
Persistent network connection required	-
Low latency connection required	-
Backup devices centrally managed by the CAS	-
MBES can be centrally monitored from the CAS	✓
Backup and restore tasks can be copied to the MBES from the CAS	✓
Backup and restore tasks can be dispatched centrally from CAS	-
Backup and restore tasks can be configured locally on MBES	✓

Device and Media Local Centralized on the CAS (Same Site Configuration)	
Persistent network connection required	✓
Low latency connection required	✓
Backup devices centrally managed by the CAS	✓
MBES can be centrally monitored from the CAS	✓
Backup and restore tasks can be copied to the MBES from the CAS	✓
Backup and restore tasks can be dispatched centrally from CAS	✓
Backup and restore tasks can be configured locally on MBES	✓

- Copying of Data between OpenStorage (OST) Devices
- Transfer is Optimized; Only Unique Blocks Transferred
- Enables Offsite Disaster Recovery and Other Use Cases
- Requires a Central Administration Server (CAS)

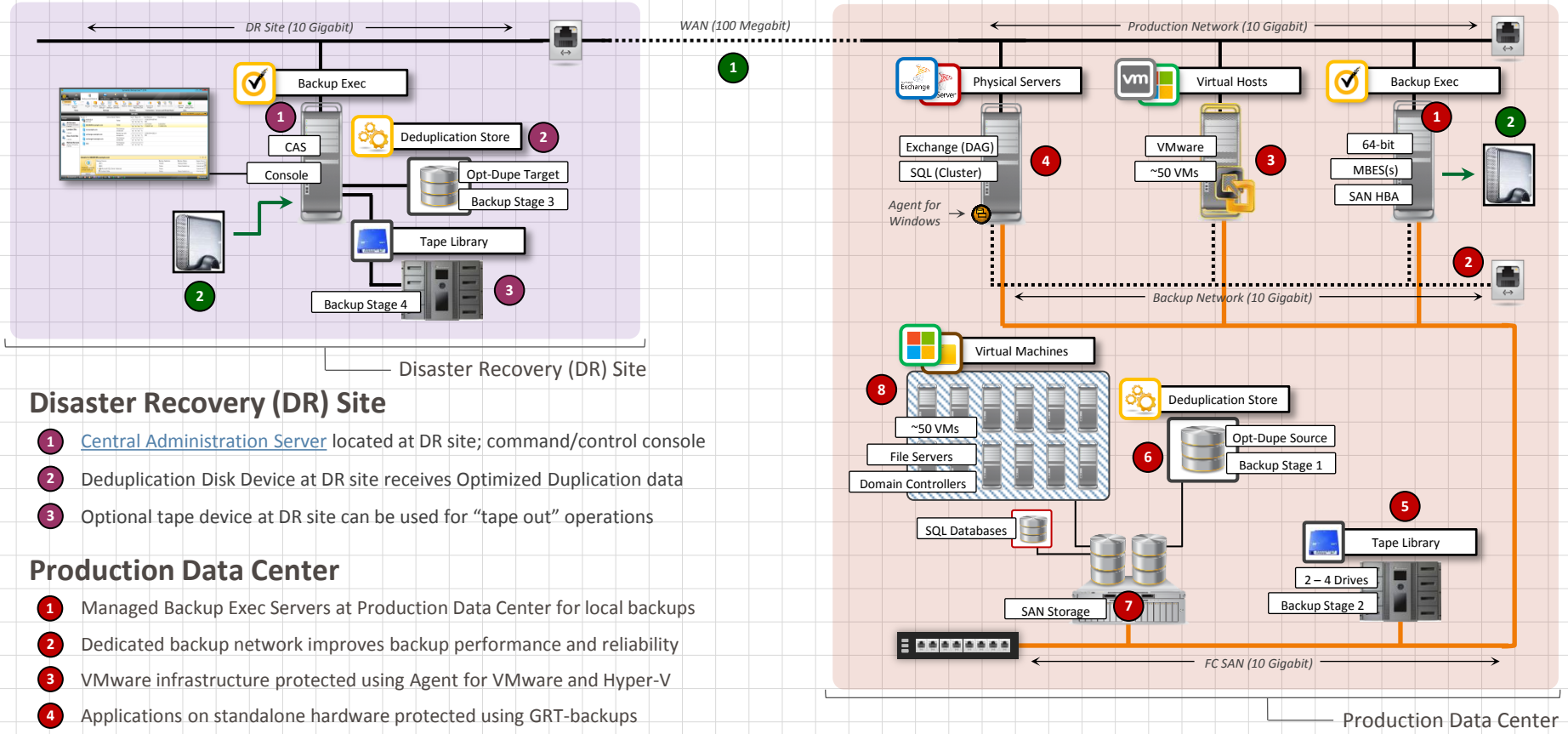


Example Diagrams and Life Preservers

Getting the most out of Backup Exec in large environments

Example Diagram: Large Installation

High-level best practices



Disaster Recovery (DR) Site

1. Central Administration Server located at DR site; command/control console
2. Deduplication Disk Device at DR site receives Optimized Duplication data
3. Optional tape device at DR site can be used for "tape out" operations

Production Data Center

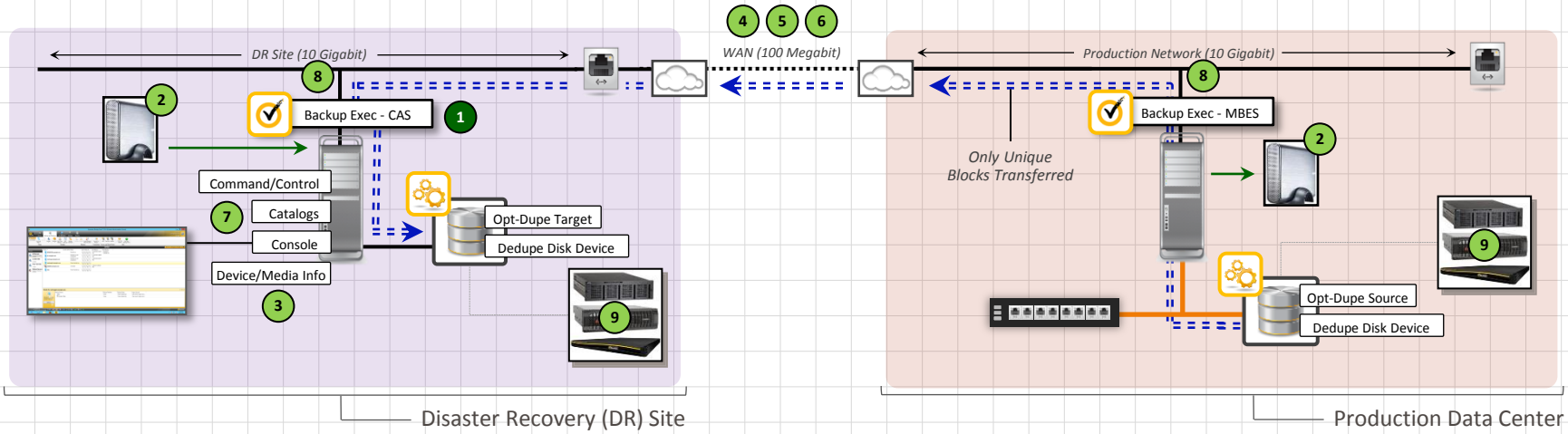
1. Managed Backup Exec Servers at Production Data Center for local backups
2. Dedicated backup network improves backup performance and reliability
3. VMware infrastructure protected using Agent for VMware and Hyper-V
4. Applications on standalone hardware protected using GRT-backups
5. Optional tape device at Data Center can be used for "tape out" operations
6. SAN storage used by Backup Exec for Deduplication Disk Device location
7. SAN fabric leveraged for VMware virtual machine backups
8. Virtual machine data store located on SAN storage

Other Notes

1. WAN latency and reliability critical to Optimized Duplication
2. Transfer drives for seeding of Optimized Duplication data at DR site

Example Diagram: Optimized Duplication

High-level best practices



Optimized Duplication High-level Best Practices

1. Place the Central Administration Server (CAS) at the Disaster Recovery (DR) site
2. Seed the Deduplication Disk Device attached to the CAS at the DR site
3. Configure Device and Media Information to be managed centrally at the CAS
4. Connection between sites can optionally be secured using a VPN solution (enables "in flight" security)
5. Ensure a "round trip" latency of 250ms (preferably much better) is achievable between sites
6. Minimize packet loss and other networking issues as much as possible
7. For larger environments, use of distributed catalogs is generally recommended
8. Use of static IP addresses for the CAS and MBESs in the environment can help overcome DNS issues
9. OST-compliant appliances can be used for Optimized Duplication (source and/or target)

- Seed Deduplication Disk Device on the CAS (DR site)
  - *Option 1: Transfer drive (PCS Planning and Deployment Guide p. 29)*
  - *Option 2: Seed OS files (PCS Planning and Deployment Guide p. 28)*
- Use Dedicated Volume for Deduplication Disk Storage Device
- Catalog and SQL Database Recommendations
  - *Catalog and SQL file locations should be distributed (separate disks/LUNs)*
  - *In very large environments, use full SQL 2008*
- Verify CAS Server Can Ping the MBES
- Site-to-site Optimized Duplication Jobs Can Impact WAN Links
  - *Modifying config file can reduce bandwidth used by Optimized Duplication*
  - *http://www.symantec.com/docs/TECH165599*

- MBES Should Have Minimum of 8 GB of RAM
  - *8 GB RAM = up to 5 TB of deduplicated data*
- CAS Minimum Recommendations
  - *http://www.symantec.com/docs/HOWTO73231*
  - *http://www.symantec.com/docs/HOWTO73627*
  - ***CAS sizing tool:*** *http://www.symantec.com/docs/TECH205843*
- Before Recovery from Deduplicated Backup Set
  - Inventory/catalog media on destination server before recovery from duplicated backup set
- Exclude Deduplication Disk Storage Device from Antivirus Scans
  - *If an antivirus scanner deletes/quarantines files from the deduplication disk storage device, access to the device may be disabled*
  - *Schedule BE processes and antivirus scans to avoid conflicts*

Life Preservers: Large Installations

Optimized duplication

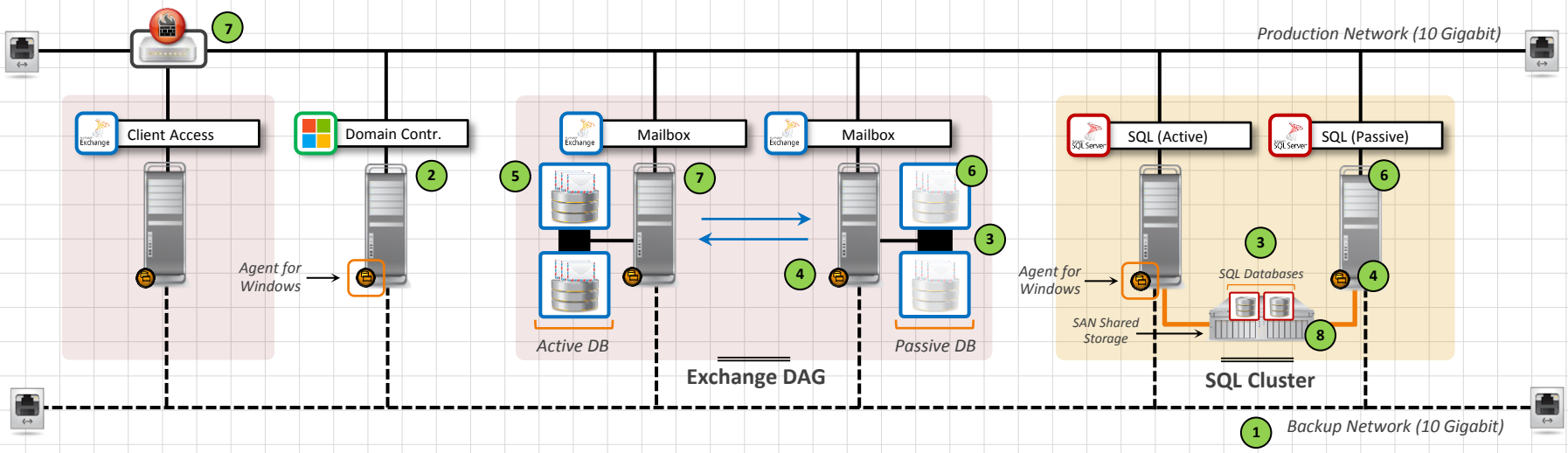
- OST Plug-in
  - Install vendor-provided OST license when using third party appliance with Backup Exec
- Domain Considerations
  - Have all Backup Exec servers in same domain or ensure trust between domains
- Backup Exec Tuning and Performance Guide
  - *http://www.symantec.com/docs/DOC5481*
- Backup Exec Device Limits/CAS Requirements Calculator
  - *http://www.symantec.com/docs/TECH205843*
- Cloud Backup Time Calculator:
  - *http://www.symantec.com/docs/TECH172473*
- Private Cloud Services Planning and Deployment Guide
  - *http://www.symantec.com/docs/TECH172464*

- RAID Caching
  - Do not enable RAID caching on disk hosting deduplication disk storage device
- Do Not Delete Files from Inside Deduplication Disk Storage Device
- Do Not Use Backup Exec Server Pools with Standalone Backups
  - *Prevents duplicate data from being hosted on multiple backup servers*
  - *See article: http://www.symantec.com/docs/HOWTO74447*
- Direct Access Sharing
  - Limit number of remote computers enabled for direct access sharing with other Backup Exec servers
- Create separate backup and verify jobs and schedules
  - *Helps meet backup windows*

- Network Performance (Latency) Considerations
  - *Maintain persistent, high-bandwidth link between CAS and MBES(s)*
  - *Ensure less than one percent (1%) packet loss during transmissions*
  - *Ensure a destination "round trip" latency of 250ms or better*
  - *Connection problems can impact job success rates*
- Additional Best Practice Resources
  - *Ensure NIC and HBA drivers are up to date*
  - *http://www.symantec.com/docs/HOWTO21788*
  - *http://www.symantec.com/docs/TECH60559*
  - *Additional Backup Exec best practice documents are located here.*

Example Diagram: Applications

High-level best practices



Application Protection High-level Best Practices

1. Leverage a separate network for backups (prevents saturation, improves performance)
2. Protect the Active Directory infrastructure in addition to application components
3. Enable Granular Recovery Technology for optimal recovery flexibility
4. Ensure all required Backup Exec logon account permissions are configured properly
5. Uniquely named mailbox required for Exchange Granular Recovery
6. For high-availability configurations, protect the passive copy of servers/databases
7. When firewall access is required, ensure ports are configured properly
8. Do not store backups to the same disk that contains databases/logs

- Place Transaction Logs on Separate Physical Disk from Database
  - *If database is damaged, transaction logs will be a recovery resource*
- Avoid Making Exchange Server a Domain Controller
  - *Simplifies recovery; Active Directory won't need to be recovered first*
- For Exchange 2010/2013, Use a DAG With At Least One Passive Database Copy for Each Database
  - *For more than one passive copy, second passive copy should use log replay delay of 24 hours*
- For Exchange 2010/2013, 64-bit Backup Exec Server Required
  - *Exchange 2010/2013 Management tools must be installed on Backup Exec server*

- Physical Exchange Servers
  - *Agent for Windows should be installed on the Exchange server*
- Exchange 2010/2013 Database Availability Groups (DAGs)
  - *Agent for Windows should be installed on each mailbox server*
- Agent for Windows
  - *Must be run under 'Local System' account on the Exchange server as well as the Backup Exec server*
  - *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
  - *Allows granular object restore without requiring separate mailbox backup*
- For GRT-enabled Backup, Change Default Staging Location on the Backup Exec Server to a Non-system Volume
  - *This volume should possess the same disk sector size as the volume used for Exchange transaction log storage on the Exchange server*
- Ensure that Scheduled Maintenance for the Information Store Does Not Run at Same Time as the Database Backup

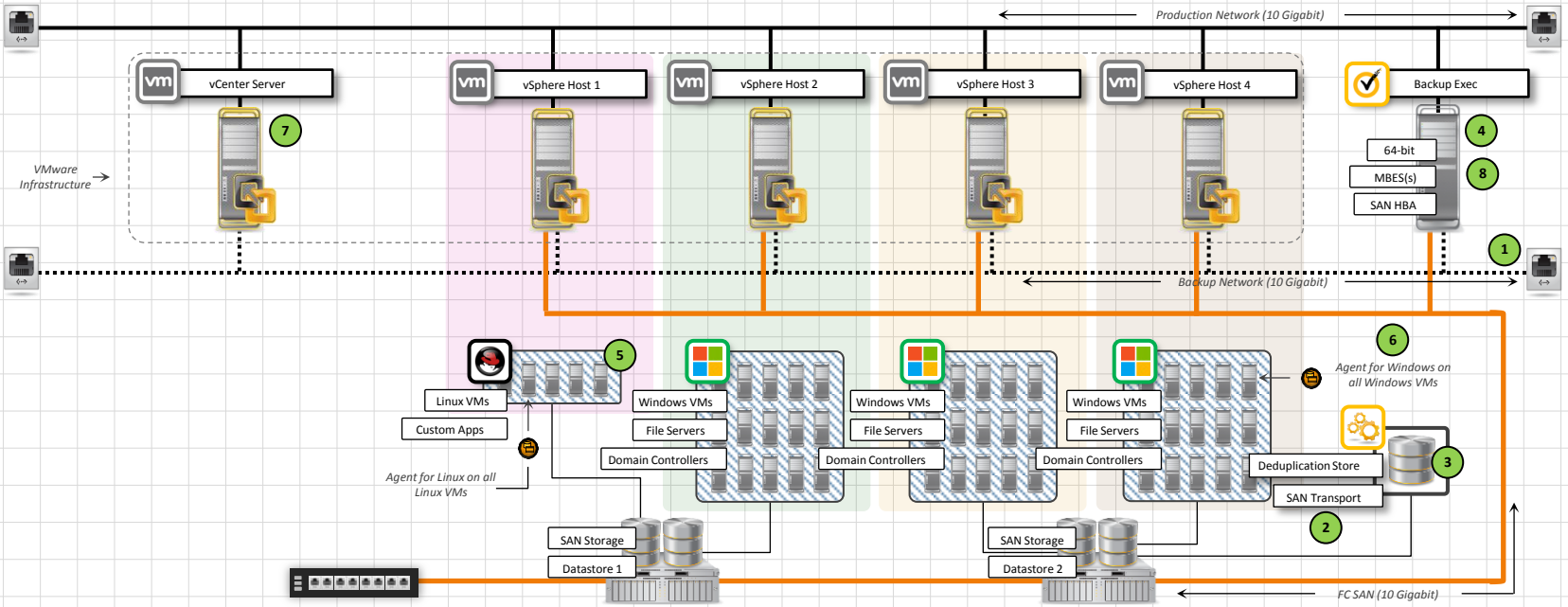
- Use a Separate Backup Network if Possible
  - *Optionally ensure backups occur during non-peak hours*
- Run Exchange Backup Jobs Separately from Other Backup Jobs
- Back Up Active Directory on a Regular Basis
- Run a Backup After Making Changes to System Settings or Application Settings
- For Exchange 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

- Backup Recommendations
  - *Use weekly full database backups, daily differential database backups, and transaction log backups as necessary*
- Use the Checksum Feature to Check Database Integrity
- Perform Test Restores Periodically
- Use the Copy Only Option for Unscheduled Backup Operations
- Use Encryption to Ensure Data Security
- SQL Native Compression and Deduplication
  - *Do not use SQL native compression if you are planning to use Backup Exec Deduplication technology*

- Schedule Backup Jobs when Database Activity is Low
- Avoid Full Database Backups During Peak Hours or when Database Activity on the Server is High
- Consider D2D2T (disk to disk to tape) Backup Strategies for Optimal Backup and Restore Performance
- Use Tape-based Devices for Long-term Retention
- Do Not Store Backups to the Same Disk that Holds Database Files or Log Files

Example Diagram: VMware

High-level best practices



VMware Protection High-level Best Practices

1. Leverage a separate network for NBD/LAN backups, if possible
2. Use SAN Transport for backups whenever possible
3. Store backups to deduplication to optimize backup storage
4. Use image-level agent-assisted backups for Windows VMs
5. Consider legacy agent-based backups for Linux VMs
6. Use the VSS Provider installed with Agent for Windows for Windows VMs
7. When available, discover and select VMs for backup via vCenter server
8. Connect Backup Exec server to SAN (access LUNs with VM datastores)

- Virtual Machines with RDM Physical Compatibility Mode Disks
  - *Agent for VMware/Hyper-V can't protect RDM Physical Compatibility Mode disks*
  - *Use the Agent for Windows/Linux to protect them using traditional backups*
- Virtual Machines Configured With GPT Disks
  - *Image-level backups supported, granular file/application recovery not supported*
  - *For granular recovery support, use the Agent for Windows or Agent for Linux to protect them using traditional backup methods*
- Virtual Machines Configured With Fault Tolerance
  - *Agent for VMware/Hyper-V cannot protect Fault Tolerant virtual machines*
  - *Fault Tolerance must be disabled first*

- General Backup Strategy Recommendations
  - *Seven-day rotation incremental and differential backups, where a full backup is run on the 7th day*
  - *Use the Deduplication Option to optimize backup storage*
- **Windows 2012/R2 Running as a VMware Virtual Machine**
  - Windows 2012/R2 Virtual Machines with ReFS Volumes

    Backup and recovery of virtual machines with ReFS volumes, including granular recovery, is supported. A Backup Exec server running on Windows 2012 or later is required.
  - Windows 2012/R2 Virtual Machines with Deduplication Volumes

    Backup and recovery of virtual machines with Deduplication volumes, including granular recovery, is supported. A Backup Exec server running on Windows 2012 or later is required.
  - Virtual Machines Using Dynamic Disks
    - Backup and recovery of virtual machines using GPT Dynamic Disks is supported; however, granular recovery is not.
    - Backup and recovery of virtual machines using MBR Dynamic Disks is supported; including granular recovery (except RAID 5)
  - Virtual Machines Using Storage Spaces

    Backup and recovery of virtual machines using Storage Spaces is supported; however, granular recovery is not.

- VADP Buffer Settings
  - *VADP buffer settings can be tuned to improve performance*
  - *See tech note: http://www.symantec.com/docs/TECH185691*
- General VMware Performance Guidelines and Expectations
  - *For SAN-based backups, install Backup Exec on a physical machine*
  - *Backup Exec server I/O performance is generally more important than CPU performance*
  - *See tech note: http://www.symantec.com/docs/TECH125455*

Job and Device Management

Managing backup jobs and devices in large environments

- Full, Differential, and Incremental Backups Supported for Physical and Virtual Backups
- Full Backups Offer a Restore Performance Advantage
  - *One backup to restore*
  - *If backup windows and storage are not an issue, use full backups*
- Incremental/Differential Backups Offer a Backup Performance Advantage
  - *Only delta changes captured*
  - *If backup windows and/or storage are a challenge, use differential or incremental backups*

- Consider Weekly Full Backups and Daily Incremental Backups as 'Standard' Protection Policy
- Schedule Disk-to-tape (D2T) to Occur Over the Weekend After Full Backup
- D2T Stage Can Happen Outside Standard Backup Window
  - *It's an operation that involves backup server and tape drive only*
  - *Can be done at any time; no required 'handle' to protected servers*
- Deduplication Can Greatly Optimize Secondary Disk Storage
  - *Additional processing overhead for deduplication calculations*
  - *Processing overhead can be handled by client or server*

- Disk-to-disk-to-tape (D2D2T) Commonly Used and Recommended Backup Methodology
  - *Disk-to-disk (D2D) stage represents open "handle" to protected server(s)*
  - *Disk-to-tape (D2T) stage is performed only by backup server + tape drive*
  - *D2D2T approach offers combination of speed and two-level protection*
- Disk as First Backup Stage Advantages:
  - *Can greatly increase backup performance*
  - *Can greatly increase non-DR restore performance*
  - *Local disk backup can be leveraged for restore in most cases*
  - *Offsite tape backup can be leveraged for disaster recovery cases*

- Infinite Setting For the Overwrite Protection Period For All Tape Media and Disk Cartridge Media:
  - *Backup data may consume tape and disk cartridge media capacity quickly*
  - *Tape and disk cartridge media do not become recyclable automatically*
    - *You must specify when to overwrite each media*
- Create New Media Sets With the Append and Overwrite Protection Periods that Accommodate Your Needs
  - *When overwrite protection periods expire, tape media and disk cartridge media are recyclable and Backup Exec has access to overwritable media*
- Overwrite Tape and Disk Cartridge Media Periodically to Keep the Media Family at a Manageable Size
  - *Allows Backup Exec to rebuild the catalog if necessary*
  - *You can use a media rotation strategy so that media is periodically overwritten, or select the option Overwrite media when you run a full backup*

- Leverage Backup Exec Server Pools to Load Balance Backup Operations Across Large Environments
  - *Server pools: see **admin guide p. 1143***
- Backup Server Pools:
  - *Prevent bottlenecks resulting from backup tasks waiting for a specific managed Backup Exec server to become available*
  - *Devices/device pools on included Backup Exec servers become available for task delegation*
  - *Central administration server itself can participate in backup server pools*
  - *Backup task can be processed by other managed Backup Exec servers in the pool allowing task processing to continue Storage device pools*

- Leverage Storage Device Pools to Load Balance Backup Operations Across Large Environments
  - *Storage device pools: see **admin guide p. 451***
- Storage Device Pools Prevent Bottlenecks Resulting From Tasks Waiting for a Specific Storage Device to Become Available
  - *If a specific storage device is unavailable or offline, the backup task can be processed by another storage device in the same pool*
  - *Allows task processing to continue and prevents operational bottlenecks*
- Backup Device Pools:
  - *Devices in a pool must be of the same type (all tape or all disk)*
  - *Storage device pools can be configured in standalone (unmanaged) configurations or in managed Backup Exec server configurations*
  - *Storage device pools can consist of devices attached to the same server or of devices attached to different servers*

- To Reclaim Disk Space Before Backup Sets Expire
  - *You can delete backup sets manually in Backup Exec*
  - *Do not use Windows Explorer or command prompt to delete backup files*
  - *By default, the data lifecycle management process runs every four hours*
- To Prevent a Backup Set From Expiring
  - *You can manually retain it*
  - *Backup Exec automatically retains all dependent backup sets as well*
  - *When you no longer want to retain a backup set, you must release it so that data lifecycle management can manage the retention period for it*
- Backup Scheduling
  - *Avoid adding too many incremental backups between full backups*
  - *The data lifecycle management process must search through each backup set to check dependencies*
  - *More incrementals = longer the DLM process*

Thank You!

Backup Exec Product Management