Symantec Backup Exec Blueprints

Blueprint for Remote Office Protection

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; the purpose of these diagrams is 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.

Symantec Backup Exec Blueprints

How to use

- **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 BE 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

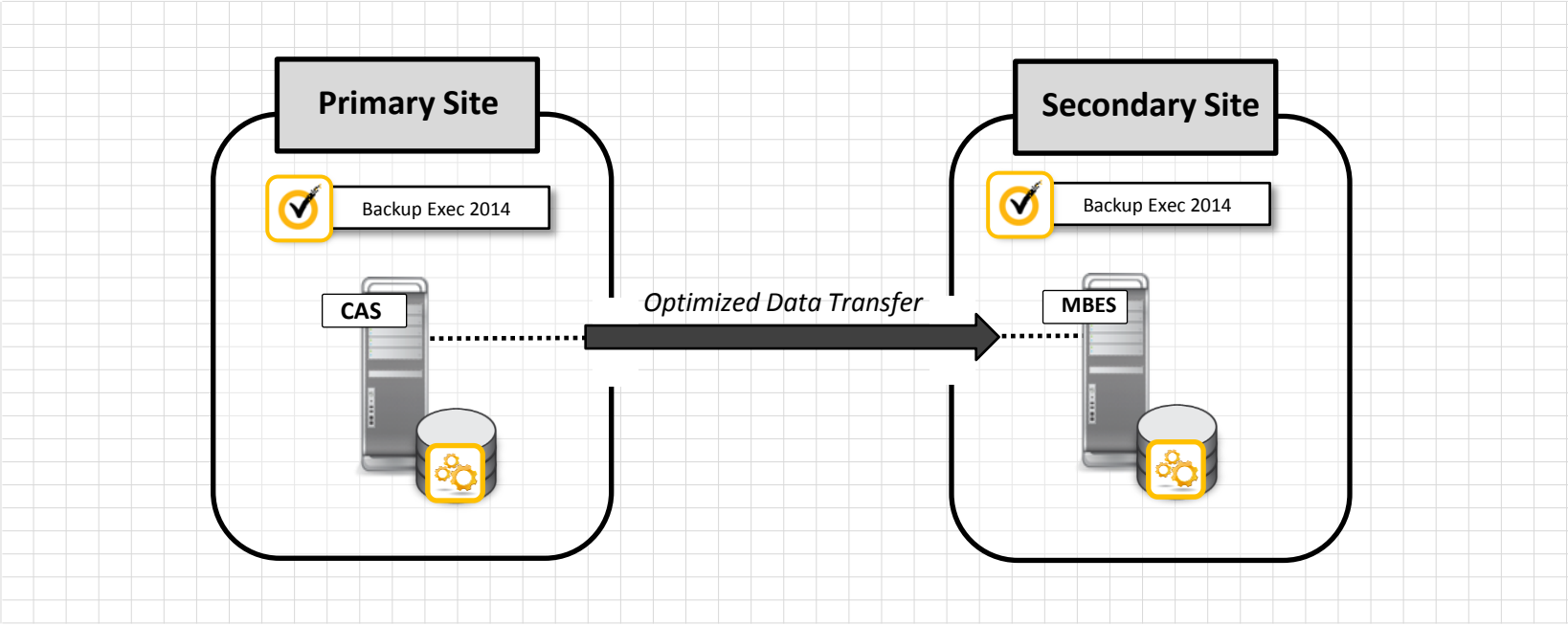
- Backup Exec Server Centrally Managed by a CAS
- Will Have Access to One or More Backup Devices
  - *Locally attached*
  - *Accessible via LAN/SAN*
  - *Shared from other MBES*
- Processes Backup and Restore Tasks
  - *Assigned from CAS*
  - *Assigned by local administrator*
- Can Be Configured in 'Pools'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

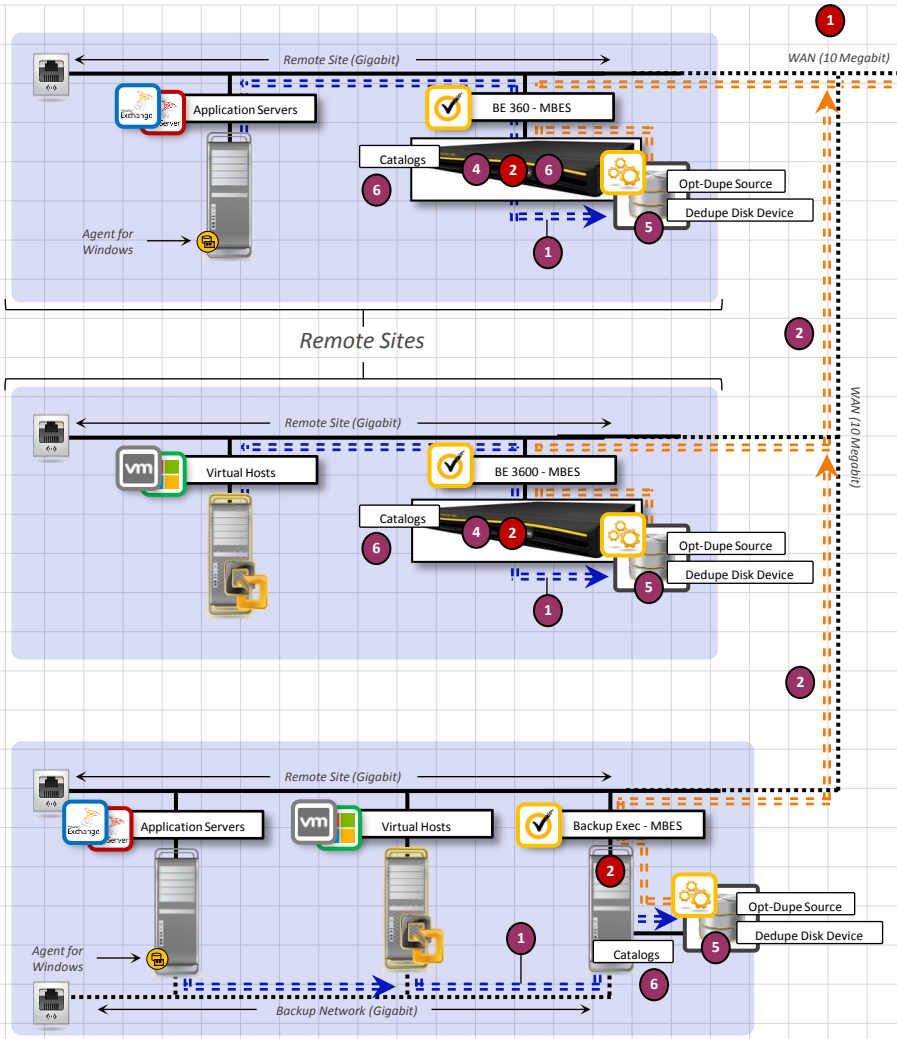


Example Diagrams and Life Preservers

Best practices for protecting remote sites

Example Diagram: Remote Office Protection

High-level best practices



Remote Sites

1. Local backups at remote sites
2. Optimized duplication to central site/office
3. Perform verify jobs at the central site/office
4. BE 3600 can be MBES at remote sites (fast/easy setup)
5. Backups at remote sites must target deduplication
6. Use distributed catalogs, especially if WAN connection is poor

Central Site/Office

1. Central Administration Server located at Central Site/Office
2. 'Tape out' at Central Site/Office (remove tape from remote sites)
3. Seed the Deduplication Disk Device at Central Site/Office

General Notes

1. WAN latency and reliability critical to optimized duplication
2. MBESs will halt backup operations if connection to CAS is lost

- Seed the 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 a Dedicated Volume for a 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 that the 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*

- Managed Backup Exec Server Memory Requirements
  - *MBES should have minimum of 8 GB of RAM*
  - *8 GB RAM = up to 5 TB of deduplicated data*
- Central Administration Server Minimum Recommendations
  - *http://www.symantec.com/docs/HOWTO73231*
  - *http://www.symantec.com/docs/HOWTO73627*
  - ***CAS sizing tool:*** *http://www.symantec.com/docs/TECH205843*
- Recovery Preparation
  - *Inventory and catalog media on destination server before you recover from the duplicated backup set*
- Exclude Deduplication Dsk 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*

- OST Licenses and Plug-ins
  - *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 domain controllers*
- 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 the disk where the deduplication disk storage device is located*
- Do Not Delete Files From Inside the Deduplication Disk Device
- Backup Exec Server Pools
  - *Do not use Backup Exec server pools as device targets in 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*
  - *Connection loss will halt backups at MBES(s) until connection is restored*
- Additional Best Practice Resources
  - *http://www.symantec.com/docs/HOWTO21788*
  - *http://www.symantec.com/docs/TECH60559*
  - *Additional Backup Exec best practice documents are located here.*

Job and Device Management

Managing backup jobs and devices in distributed 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
- 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 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