Best Practices for Microsoft Hyper-V

Use these tips and recommendations to efficiently protect your Microsoft Hyper-V environment using Barracuda Backup.

Barracuda Cloud LiveBoot

Use Barracuda Cloud LiveBoot to boot Microsoft Hyper-V VMs in the Barracuda Cloud. Cloud LiveBoot is useful as a sandbox for testing purposes. For more information, see Cloud LiveBoot Virtual Machine Recovery.

Best Practice
Document the Microsoft Hyper-V 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 Hyper-V documentation for management, disaster plans, and recovery.

Barracuda Backup provides three methods to protect your virtual environment:

1. Host-based (Agentless) protection;
2. Guest-level (Agent) protection; and
3. Hybrid host- and guest-level protection.

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 virtual environment and to meet your recovery objectives.

Host-Based (Agentless) Protection

- The Barracuda Backup Agent must be installed on each Hyper-V host machine
- Provides image-based agentless protection of guest VMs
- Barracuda Backup Agent provides source-based deduplication and incremental forever backups of guest VMs
- Quick and easy to configure, no need to add VMs as individual sources
- Automatically detects new and removed VMs
- Provides granular file/directory recovery via VHD Browsing
- Preferred method of protection for quick disaster recovery and to meet stringent recovery time objectives
    - Use Cloud LiveBoot to spin up a VM in Barracuda Cloud Storage
- Provides recovery of entire VM to original or rebuilt Hyper-V host
- Download individual virtual disks
- You cannot exclude individual files or directories from backup
- Can cause an increased storage footprint due to image-based backup method, better for short-term retention
- Protect Microsoft applications running on VMs using the Barracuda Backup Agent as separate sources in conjunction with host-based backups, including:
    - **Microsoft Exchange Server** – Only databases must be protected using the Barracuda Backup Agent. If you are using host-based VM backup in conjunction with Agent backup, you do not need to include the File System and System State with the Agent backup.
    - **Microsoft SQL Server** – Only databases must be protected using the Barracuda Backup Agent. If you are using host-based VM backup in conjunction with Agent backup, you do not need to include the File System and System State with the Agent backup.

- **Microsoft Active Directory** – Databases and System State must be protected using the Barracuda Backup Agent.

Guest-Level (Agent) Protection

- Provides incremental forever file-level protection of guest VMs using the Barracuda Backup Agent
- Backups treat each VM like a physical client
- Application-consistent protection for Microsoft applications, including:
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - Microsoft Active Directory
- Exclude any file, file type, or directory
- Run pre- and post-backup scripts
- Provides more granular recovery options including:
  - Restore files and directories to any client running the Barracuda Backup Agent
  - Designate the path where files are restored
  - Download individual files and directories (locally and cloud)
- Complete system restore through:
  - Bare metal restoration to a new computer without a pre-installed operating system
  - Restore the entire file system or individual volumes to a target system with a pre-installed operating system
- Provides a smaller storage footprint due to file-level backup and deduplication; this is potentially a better option for servers needing to adhere to longer retention policies, such as a file server needing to retain historical revisions for several years