ECHOplatform Best Practices Partner Guide

Version 2.5

Barracuda
MSP

Revision History

Status	**Changes**	**Date**
Final.	• Added *Credential Security Best Practices for your MSP* chapter. • Added *Whitelisting the Backup Agent* section. • Removed Exchange 2007 references. • Updated hyperlinks.	June 2019.

Table of Contents

Table of Figures

Introduction

This section includes the following topics:

- Audience
- About This Guide
- Related Documentation
- Barracuda Partner Support

Audience

The audience for this document is IT professionals and partners who provide clients with Barracuda data backup and security services.

About This Guide

This Best Practices Partner Guide includes the following topics:

- Developing a disaster recovery (DR) plan
- Credential security best practices for your MSP
- Backup type considerations and recommendations
- Local vault backup
- Local only backup
- Restore considerations and recommendations
- Managing additional usage
- Avoiding common problems

Related Documentation

The following documentation is available from Barracuda MSP:

- *ECHOplatform Backup and Restore Reference Guide* – provides details on how to create backups and restores for each backup type.
- *ECHOplatform Quick Start Guide* - provides information about setting your preferences, creating templates, and installing the software.
- *ECHOplatform - Autotask Integration Guide* - provides information about setting up Autotask integration with ECHOplatform.
- *ECHOplatform - Connectwise Manage Integration Guide* - provides information about setting up Connectwise Manage integration with ECHOplatform.

Barracuda Partner Support

Barracuda Partner Support is available 8 AM to 9 PM (EST).

Phone: 800.569.0155 (Option 1) or 617.948.5300

Email: support@barracudamsp.com

Click the following link for Barracuda live chat service 8 AM to 6 PM (EST):

http://www.barracudamsp.com/support/contact.php

Chapter 1. **Developing a Disaster Recovery Plan**

This chapter includes the following topics:

- Overview
- Conduct a Data Assessment
- Saving Your Data
- Scheduling the Backup
- Running a Test Backup
- Running a Test Restore

Overview

Many small-to-medium sized business (SMB) owners genuinely question the need for any kind of disaster recovery plan (DRP), particularly a data disaster recovery plan. 'I'm just a small business. How much can I really lose?'

Statistics from the National Archives & Records Administration in Washington are reported in the following table.

After the disaster, Companies that lost their data...	Statistic
that never reopen.	25%
that close within 6 months.	60%
for 10 days or more filed for bankruptcy within one year.	93%
for 10 days or more filed for bankruptcy immediately.	50%

In addition, 31 % of PC users have lost all their files because of events beyond their control.

Recognizing the difference between a minor data disaster and a major business disaster is important. A minor data disaster refers to the loss of data due to a server crash, or hard drive crash, or some other small accident that deprives a business of data without affecting other assets. Developing a recovery plan for the loss of data is relatively easy.

However, what happens when a major disaster strikes? What happens to your customer's business when they lose all their assets, or there is no place to work? Being able to restore data is certainly part of a major disaster recovery plan, but not all the data in the world can help a business that has no place for employees to work, or tools, or systems to work with.

As an MSP, you can add value to your service by convincing your customers to develop comprehensive disaster recovery plans. Helping your customers develop plans that define where employees work, what they work with, and how they work following a major disaster establishes trustworthy relationships.

You do not have to provide all the answers. You only need to ask the right questions so your customers can develop the answers on their own. While you may not be able to offer more than support in recovering data or providing IT infrastructure after a disaster, convincing a customer to develop a comprehensive disaster recovery plan is the best thing you could ever do for them.

The good news is that disaster recovery planning does not require a lot of time or money. DRP requires the will and commitment to get the plan done. The effort put into the DRP is time and money well spent. The following suggestions are provided to help you and your customers get started.

- Establish a planning group.
- Perform a risk assessment.
    - Realistically, what disasters could occur?
        - Fire
        - Flood
        - Storms
        - Unique equipment failures
        - Total systems failures
        - Others
    - How would each one affect the business?
- Establish priorities by identifying systems/assets that are mission critical.
- Develop recovery strategies.
    - Where shall employees work?
    - What equipment/tools shall they need?
    - Where shall you get the equipment/tools?
    - What data is essential for the business to operate?
- Document the plan (include an inventory of all systems and safeguards).
- **Important**: Test the plan by conducting a disaster drill on those elements that are practical to test, like data recovery.
- Implement safeguards to reduce risk.
- Conduct an annual review and drill of the plan to ensure the plan works.

The following links provide more information.

https://barracudamsp.com/msp-resources/disaster-recovery-plan/
https://barracudamsp.com/resources/pdf/how-to-guide/Recipe-BDR-Final-for-web.pdf

Conducting a Data Assessment

The first and most important step in successfully protecting your customer is determining the data they need to safeguard. A surprising number of partners miss important files and folders, because they do not know the data exists, or that the data is important to the customer. The best rule to follow with every customer is never assume anything about what should or should not be backed up.

Do not leave yourself or your customers vulnerable. Know what you need to protect!

Conducting a data assessment with every customer may take a little time, but the avoidance of potential problems is worth the effort. A data assessment also helps establish rapport with your customer by demonstrating your genuine interest in their business success!

Data Assessment Tasks

The followings tasks are recommended for conducting the data assessment.

1. Develop a standard customer questionnaire.

   Ask the following suggested questions.

   - What applications do you use to run your business?
   - Who uses them, when, and how often?
   - Where does the data reside?
   - What are your data retention requirements (how long do you need to keep files)?
   - Which copies are kept onsite or offsite?
   - What is the impact on the business if the data is lost?
   - What is your recovery point objective (RPO); what is the minimum required to run the business?
   - What is your recovery time objective (RTO); how quickly must the RPO be achieved?

   The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down because of a hardware, program, or communications failure.
   The recovery time objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) to avoid a break in business continuity.

2. Email the questionnaire to the customer and schedule a face-to-face meeting.
3. Review the answers.
4. Ask for a tour of the facility, that includes:

   - Talking to end users.
   - Seeing the environment.
   - Understanding your customer’s needs and objectives.

5. Discuss the pros and cons of various protection options with the customer and agree on a plan.
6. Document the plan for the benefit of all parties and update the plan at least every 6 months (sooner is usually better).
7. After you know what to back up, create the backup set or sets.

Saving Your Data

Part of the data assessment is determining how long to retain the data. In some cases, as with medical records or tax records, legal requirements determine the length of retention. When there are no legal requirements, the length of retention is a customer decision based on several considerations. Some of these include:

- What data is mission critical?
  Data like client information (for law offices) may need to be kept longer than customer information (for businesses).
- What data is time sensitive?
  Financial information (revenue and expenses) for purposes of tax reporting or securities reporting needs to be kept longer than say, comparative analysis of two different sales/marketing campaigns.
- What data is nice to have?
  Customers want to save some data for various reasons. However, when data starts to push storage limits, costs should be understood.

Setting criteria for retaining data is highly important when discussing backups. Because deleting data from storage is different from deleting data on a Windows-based computer. If a file or folder is inadvertently deleted from Windows, data can be recovered with certain software. If data is deleted from backup storage, then that data is permanently gone.

Use delete with caution. Do not:

- Assume the next backup restores the data.
- Assume the data can be retrieved after deletion.
- Take any unnecessary risks.

> *If there is a chance you might need the data, do not delete the data!*

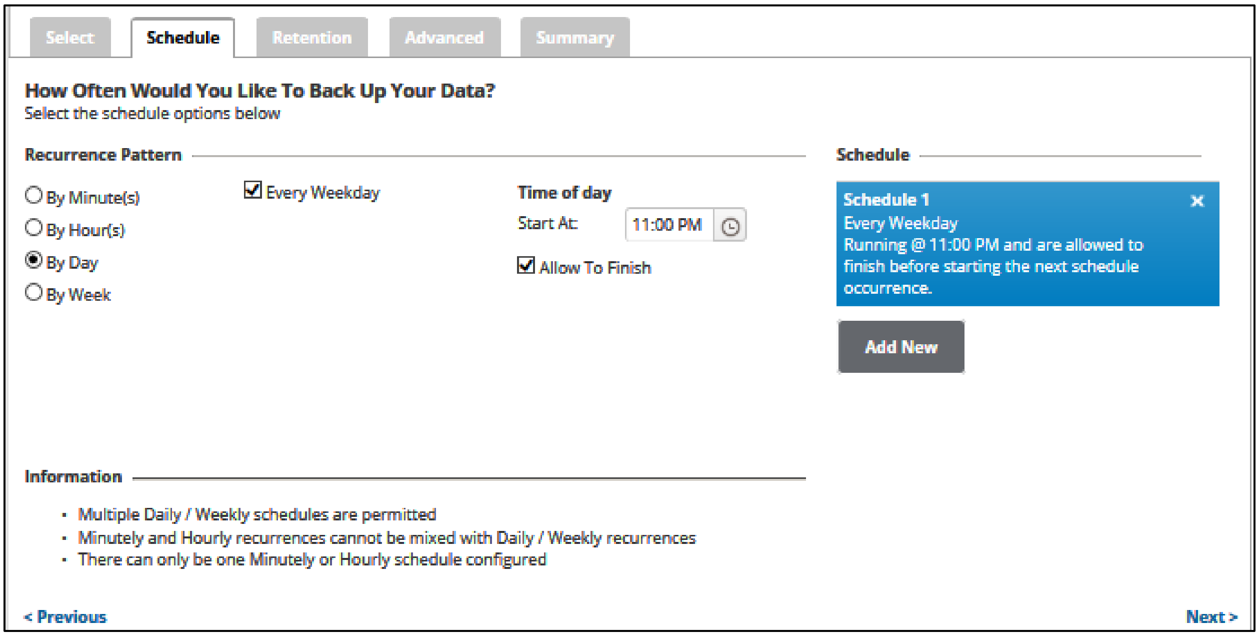
Scheduling the Backup

Schedule the Backup is in the list of best practices because, with Barracuda ECHOplatform, backups can be managed manually. Some customers prefer doing backups manually. The risk of setting a backup to manual mode means the backup does not run unless someone runs it. What if the person responsible gets busy and forgets? What if at the time they try to run the backup, they cannot access the server?

> *The data is not protected if the backup does not run!*

Backups can be scheduled for any day, at any time. Backups can be scheduled to run within fixed periods or run until completion. Multiple backups can be scheduled on the same day for customers who generate important changes in their data throughout the day.

Figure 1 shows an example of a schedule that displays when you run the backup for Files and Folders.



How Often Would You Like To Back Up Your Data?
Select the schedule options below

Recurrence Pattern

○ By Minute(s)
○ By Hour(s)
● By Day
○ By Week

☑ Every Weekday

Time of day
Start At: 11:00 PM
☑ Allow To Finish

Schedule

Schedule 1
Every Weekday
Running @ 11:00 PM and are allowed to finish before starting the next schedule occurrence.

Information

- Multiple Daily / Weekly schedules are permitted
- Minutely and Hourly recurrences cannot be mixed with Daily / Weekly recurrences
- There can only be one Minutely or Hourly schedule configured

Figure 1. Backup Schedule.

Running a Test Backup

As reliable as the backup and recovery solution you now are offering your customers is, problems can occur. Human involvement makes mistakes inevitable, as follows:

- Permissions may not be set correctly.
- Required software may not be installed.
- Remote drives may not be accessible.

Potential environmental pitfalls also can prevent a backup from running.

Performing a quick test can identify environmental issues with software or hardware that could prevent the backup from running successfully.

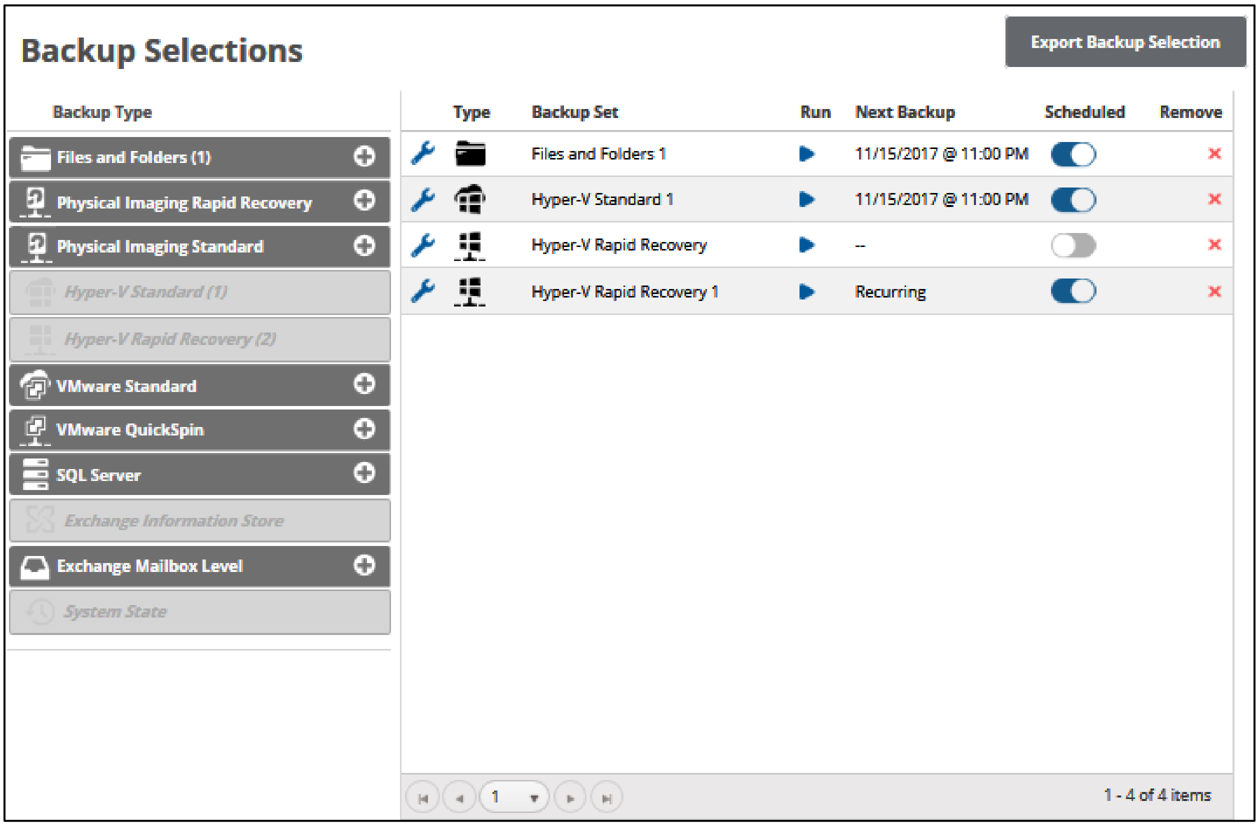
Ensure you perform the following checks after a backup:

- Review the logs after the backup has run.
- Look for any warnings or errors to ensure the backup has run successfully.

Knowing that everything is working correctly from the start can give both you and your customer peace of mind for the effectiveness and simplicity of the solution you have just sold them.

You can also use the results from a successful test as an additional sales point or as a teaching point for your customer. A successful backup test demonstrates to your customer that they made a good decision. Use the opportunity to review what is contained in the reports generated from backups.

Figure 2 shows the Backup Selections page where you can select a backup to run.



Type	Backup Set	Run	Next Backup	Scheduled	Remove
	Files and Folders 1	▶	11/15/2017 @ 11:00 PM	●	×
	Hyper-V Standard 1	▶	11/15/2017 @ 11:00 PM	●	×
	Hyper-V Rapid Recovery	▶	--	○	×
	Hyper-V Rapid Recovery 1	▶	Recurring	●	×

Figure 2. Backup Selections Page.

Running a Test Restore

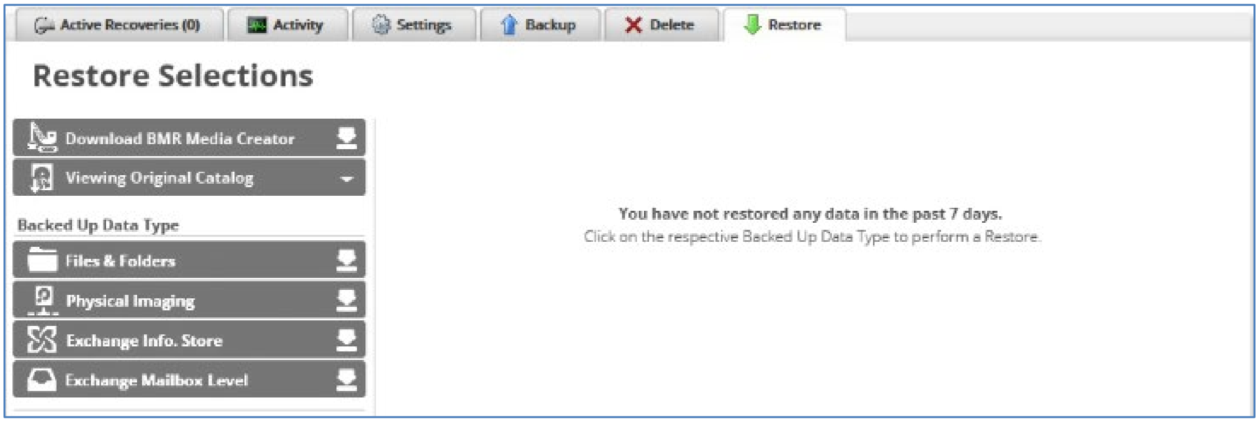
After you have demonstrated a successful backup, run a test restore to an alternative location. After all, recovery, or restoring data, is the reason you offer a cloud backup and recovery solution to your customers. The temporary folder should have at least twice the capacity of the amount of data being restored.

Select a location for the restore other than the backed-up computer.

After the restoration is complete, make sure that the:

- Results match the backup set you created.
- Restored data is complete and usable.

Figure 3 shows the Restore Selections page that displays where you can select a restore to run.



You have not restored any data in the past 7 days.
Click on the respective Backed Up Data Type to perform a Restore.

Figure 3. Restore Selections Page.

[This page left intentionally blank.]

]

Chapter 2. **Credential Security Best Practices for Your MSP**

This chapter provides the best practices for credential security.

In today's environment, end-customers are being targeted and infected with ransomware through their MSPs. As MSPs often hold the keys to their customers' environment, MSPs have an enormous responsibility to be vigilant about securing their credentials to ensure attackers cannot exploit customers through this type of access.

To help you strengthen your credential security, Barracuda MSP encourage you to adhere to the following best practices:

- Review access to MSP tools
- Enforce a strong password policy
- Use two-factor authentication
- Store passwords securely
- Review user roles

Review Access to MSP Tools

When users leave or personnel changes take place in your organization, ensure that only individuals who currently need access to your tools have that access. Any employees who have left the company or no longer need that access should have their access revoked so attackers cannot use these inactive accounts to gain entry to your customers' environments.

Enforce a Strong Password Policy

Implementing and enforcing a strong password policy is crucial to security. A strong password policy includes the following:

- Requiring passwords that cannot be easily guessed or vulnerable to brute-force/dictionary attacks
- Instituting a frequent password change policy
- Requiring unique passwords for different customer sites

Ensure the password change policy is enforced throughout your organization and for your entire portfolio of tools. Use a password generator to generate credentials such as GRC Passwords, which generates long, high-quality, random passwords.

Use Two-factor Authentication

Two-factor authentication in software has become a requirement in today's cyberthreat landscape. Barracuda MSP strongly recommends using two-factor authentication, configured in conjunction with Barracuda Cloud Control.

Store Passwords Securely

Using complicated passwords has disadvantages. Many users may start storing these passwords in commonly used but unsecure applications such as Notes or Notepad making the information easy for cybercriminals to steal. Employ the use of a password manager for your users to ensure passwords are securely stored.

Review User Roles

MSPs should review the roles assigned to users as well as the permissions associated with different roles. This review should be done regularly to ensure each user is not given more permissions than needed to do the job.

Security is of utmost importance at every business, including here at Barracuda MSP. Please review your security settings for your Barracuda products, as well as the rest of the solutions you manage to ensure you are complying with security best practices.

For more information about how to configure your security settings with Barracuda MSP products, please visit the Barracuda MSP products security considerations.

Chapter 3. **Backup Types Considerations and Recommendations**

This chapter provides an overview for each backup type with recommendations and general considerations. The backup types include:

- Files and folders backups
- Physical imaging Standard and Physical imaging Rapid Recovery backups
- VMware Standard and VMware QuickSpin backups
- Hyper-V Standard and Hyper-V Rapid Recovery backups
- Exchange Information Store backup
- Exchange Mailbox Level backup
- SQL backup
- System State backup

See the *ECHOplatform Backup and Restore Reference Guide* for details on how to create backups and restores for each backup type.

Files and Folders Backup

This section includes the following topics:

- General Considerations
- Specific Restrictions and Recommendations

General Considerations

Backing up files and folders that are shared from another computer may not work with the ECHOplatform agent software unless you take certain steps to ensure the backup. This issue is based on communication between the computer on which the Backup Agent is installed, and the computer that houses the shared files and folders.

Backups of shared files and folders:

- Are slower.
- Use more system resources.
- Do not let you back up open and locked files (VSS).

The best practice to ensure back up of shared files and folders is to copy them directly onto the machine that has the Backup Agent installed whenever possible.

If you cannot install the files and folders on the computer being backed up, and you need to back them up from the computer that is sharing them, use the Share Manager feature in the software to add access credentials.

The ECHOplatform agent does not support encrypted file systems. Decrypt encrypted files or encrypted folders for back up.

Make sure the backup agent user has access to all the data you have selected so there are no access issues.

The ECHOplatform agent leverages the built in VSS functionality within Windows to perform a snapshot of the data allowing backup of open or locked files. As a result, you must have the agent software running on each machine being used as a source for data (Windows only).

Process for File Backups

The ECHOplatform agent uses the following process to ensure successful backups.

Stage	What Happens
1	The ECHOplatform agent uses Volume Shadow Service (VSS) to create a snapshot of the volume to back up open and locked files.
2	To determine which files and folders are backed up the ECHOplatform agent uses these sources in the following order: a. the USN Journal b. name changes, path changes, and date modified changes
3	The ECHOplatform agent copies files and folders to a temporary location.
4	The ECHOplatform agent encrypts, zips, and breaks files over 100 Mb into 100 Mb chunks for transit.
5	Intelliblox uploads only the changed parts.

Note: File overhead contributes to processing time (number of files, type, and backing up from local or remote location).

Specific Restrictions and Recommendations

- If you want to run an image backup, use Image Rapid Recovery or Standard.
- If you use Stray File removal to clean up after backing up dumped files, do not overlap the start time of a backup with other VSS utilities like Shadow Protect.

  Note: Files with different names qualify as different files.

- If you run backup sets first that contain less data, and schedule ones that contain more data to run later, do not start all your backup sets at the same exact time. While you can overlap jobs (since a persistent snapshot is created using MS provider), stagger backup start times by at least a half hour.
- Verify in the Management Portal that the archiving settings are accurate.

  Note: You can configure different archiving rules for each backup set to store what the client needs.

Physical Imaging Backups

Barracuda provides image-based backup solutions that protect server applications on physical machines. Barracuda physical image backup lets you back up physical machines as volume-level images.

You have the options of backing up volumes and revisions with:

- Physical Imaging Standard backup
- Physical Imaging Rapid Recovery backup

Physical Imaging Standard Backup

Physical Imaging Standard backup allows you to:

- Create virtual machines from restored VHDs for physical-to-virtual recovery.
- Recover from image backups on local storage and bare metal restore (BMR) in minutes.

Physical Imaging Standard backups use the Changed Block Tracking (CBT) driver to keep track of the changes made on the VMs over time.

CBT reduces the time needed to identify changes that need to be backed up. The entirety of a VM's disks no longer need to be scanned to find what has changed. All changes are tracked and served to the agent as soon as the backup starts.

Subsequent backups are incremental containing only the changes detected by the CBT driver.

Note that full backups are performed by default at every 21st successful backup.

Any Physical Imaging Standard backups taken in previous versions of the Agent, before the introduction of the CBT driver, can be restored.

CBT makes Physical Imaging Standard more consistent with Hyper-V Standard, Hyper-V Rapid Recovery and VMware, which also use CBT.

Physical Imaging Standard provides the following restore options:

- Restore to VHD/X Files
- Restore to Hyper-V Virtual Machine
- Restore via Bare Metal Recovery

Physical Imaging Rapid Recovery Backup

Barracuda Physical Imaging Rapid Recovery backup and recovery options allow partners to address the specific restore requirements of each client with the same features as Physical Imaging Standard, with one unique addition: Object-level restore.

Object-level restore allows you to explore and to extract specific files and folders quickly and easily, with no need to mount VHDs.

At the Object-level, you can browse all the files of the volumes that you backed up and select individual files from those volumes to restore. This feature allows you to recover individual files and folders from a local Physical Imaging backup directly through the management portal. This granular restore of data is performed without having to explicitly mount the disks and display their contents with Windows explorer.

General Considerations

- Physical Imaging supports volumes up to 64 TB.

- Images can be backed up locally and to the cloud.
- Imaging backup sets store the last seven versions as the default.
- Imaging backups need high-performance backup destination:

If backing up to…	**Then use…**
an external hard disk,	USB 3.0
network-attached storage	at least 1 Gigabit Ethernet bandwidth. Your local network should have enough bandwidth to support transferring image backups to a NAS device.

Physical Imaging Standard backup and Physical Imaging Rapid Recovery are different pieces of a complete data protection strategy for Physical Imaging environments. Both can be used in your environment to provide multiple levels of protection.

Standard provides offsite, secure, and fewer backups.

Rapid Recovery provides onsite, rapid failover, and frequent replication. Rapid Recovery backups can be set to run every 15 minutes, and a default 96 revisions provides 24 hours of recoverable data.

Depending on customer needs, both can be used to provide coverage and redundancy in virtual machine protection.

Use Standard when:

- You would like to save a full image copy of your volumes and revisions offsite in case of a disaster.
- You are in a single-host environment.
- Data encryption (both in the cloud and locally) is a requirement.
- The customer is sensitive to recovery time objective (RTO) and has standby hardware.
- You are backing up locally and off-site (off-site only is fine if using Rapid Recovery) for DR scenarios.

Use Rapid Recovery when:

- You have multiple hosts (you have a second host to be used for recovery volumes and revisions).
- You have tighter recovery point objective (RPO) requirements and need to back up your volumes and revisions more frequently.
- You need to have your volumes and revisions running and accessible quickly after VM or host failure locally.
- Partners cannot afford high availability because of the hardware or software expense. The expense of a Rapid Recovery server is far less than for a high-availability server.

Specific Restrictions and Recommendations

The following list provides restrictions and recommendations for imaging configurations.

- Do not back up to a disk local to the machine you are protecting because it does not provide adequate protection in the event of hardware failure.
- Review Barracuda' restore options. One restore type may be preferable over another depending on:

- The environment to which you need to restore.
- Your customers' recovery time objectives.

- To ensure incremental backups run quickly, disable any scheduled Disk Defragmenter tasks. A defragmented disk negatively affects backup performance. The disk defragmenter processes:
    - Cause the ECHOplatform agent to detect more changes to a disk than have occurred.
    - Increase the amount of time required to determine changed blocks.
    - Cause incremental backups to run longer than expected.
- Running disk defragmenter prior to running an image backup can greatly improve the performance of your first and subsequent image backups. Run the disk defragmenter on any disk containing volumes selected to be backed up *before* running your first image backup. Do not schedule disk defragmenter jobs for these disks.
- If you have a system running either SQL or Exchange then do the following:
    - Use the Exchange and SQL plugins so that the logs truncate.
    - Enable processes to enable the applications to manage logs, such as circular logging in Exchange.

VMware Standard and VMware QuickSpin Backups

Barracuda offers a native VMware backup solution as part of the Barracuda MSP ECHOplatform that protects virtual machines using the same, centrally managed platform you use to back up all the rest of your data. Both Standard and QS require a VMware Essentials license or higher.

By managing VMware Standard and VMware QuickSpin services alongside other backup services in the central Barracuda Partner Portal, you can provide real-time client assessments for review and resolution.

With VMware QuickSpin, VMware data can be quickly restored from local storage without the need for an on-site visit or extra software.

General Considerations

VMware Standard backup and VMware QuickSpin replication are both different pieces of a complete data protection strategy for VMware environments. Both can be used in your environment to provide multiple levels of protection.

Standard provides offsite, secure, and fewer backups.

VMware QuickSpin provides onsite, rapid failover, and frequent replication. VMware QuickSpin backups can be set to run every 15 minutes, and a default 96 revisions provides 24 hours of recoverable data.

Depending on customer needs, both can be used to provide coverage and redundancy in virtual machine protection.

Use Standard when:

- You would like to save a full image copy of your VMs offsite in case of a disaster.
- You are in a single-host environment.
- Data encryption (both in the cloud and locally) is a requirement.
- The customer is sensitive to recovery time objective (RTO) and has standby hardware.
- You are backing up locally and off-site (off-site only is fine if using VMware QuickSpin) for DR scenarios.

Use VMware QuickSpin when:

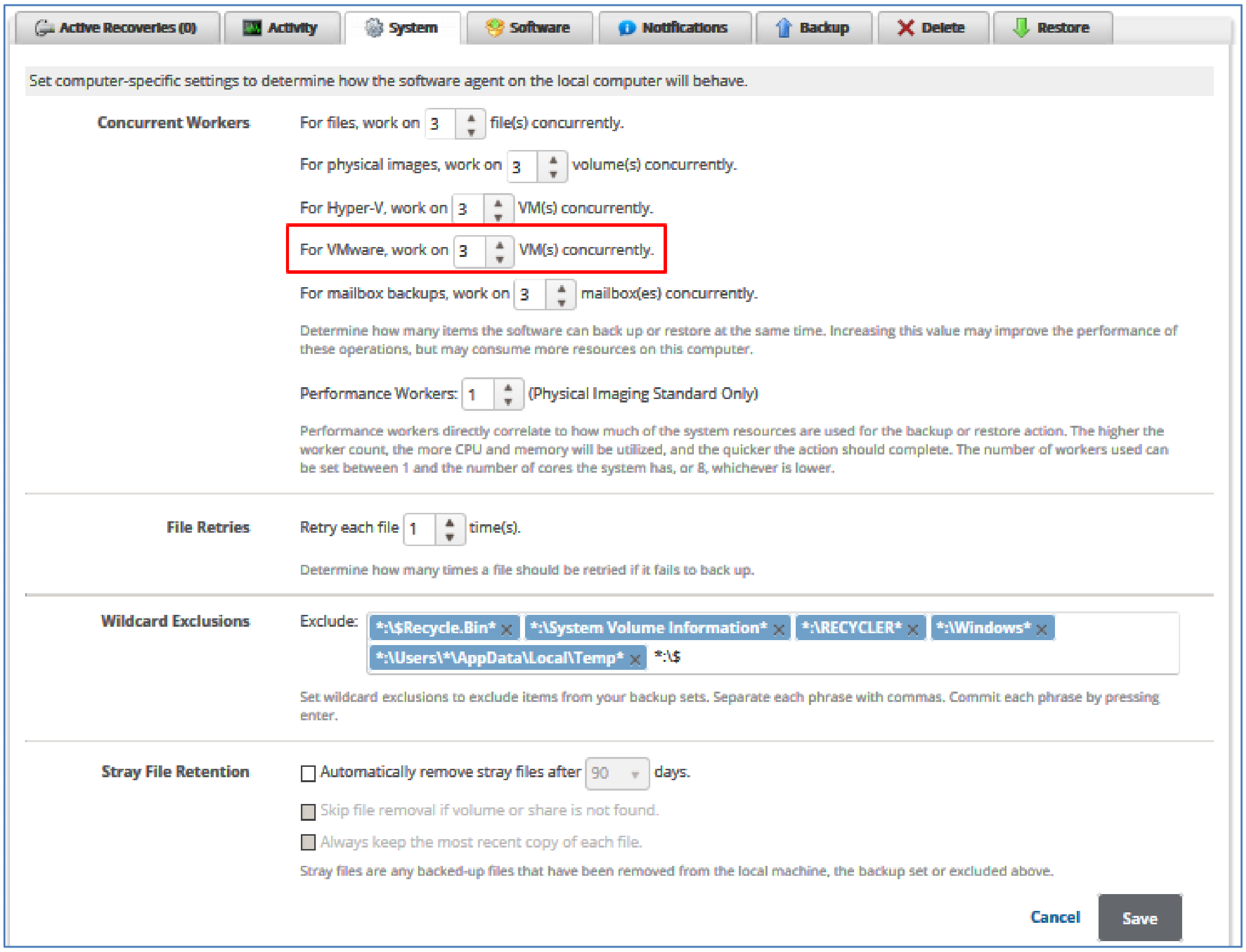
- You have multiple hosts (you have a second host to be used for recovery VMs).
- You have tighter recovery point objective (RPO) requirements and need to back up your VMs more frequently.
- You need to have your VMs running and accessible quickly after VM or host failure locally.
- Partners cannot afford high availability because of the hardware or software expense. The expense of a VMware QuickSpin server is far less than for a high-availability server.
- The server is running in a VMware environment and partners have multiple available hosts. Optionally, use the system state plugin locally to protect against application failure / administration error.

Recommended Number of VMware VMs to Back Up on a Single Host

Although any number of VMs can be selected for back up on a single host, the system resources of the host and the total number of VMs should be taken into consideration when choosing backup worker settings and creating backup sets.

Backup sets with large number of VMs take longer to back up, especially if the VMs' data changes frequently. Schedule your backups accordingly.

You can choose how many VMs are backed up at the same time by modifying the Concurrent Workers for VMware setting on the System Settings page, shown in Figure 4. For specific instructions, see the *ECHOplatform Backup and Restore Reference Guide.*



Set computer-specific settings to determine how the software agent on the local computer will behave.

Concurrent Workers

For files, work on 3 file(s) concurrently.

For physical images, work on 3 volume(s) concurrently.

For Hyper-V, work on 3 VM(s) concurrently.

For VMware, work on 3 VM(s) concurrently.

For mailbox backups, work on 3 mailbox(es) concurrently.

Determine how many items the software can back up or restore at the same time. Increasing this value may improve the performance of these operations, but may consume more resources on this computer.

Performance Workers: 1 (Physical Imaging Standard Only)

Performance workers directly correlate to how much of the system resources are used for the backup or restore action. The higher the worker count, the more CPU and memory will be utilized, and the quicker the action should complete. The number of workers used can be set between 1 and the number of cores the system has, or 8, whichever is lower.

File Retries

Retry each file 1 time(s).

Determine how many times a file should be retried if it fails to back up.

Wildcard Exclusions

Exclude: *:\$Recycle.Bin* × *:\System Volume Information* × *:\RECYCLER* × *:\Windows* × *:\Users\*\AppData\Local\Temp* × *:\$

Set wildcard exclusions to exclude items from your backup sets. Separate each phrase with commas. Commit each phrase by pressing enter.

Stray File Retention

□ Automatically remove stray files after 90 days.

□ Skip file removal if volume or share is not found.

□ Always keep the most recent copy of each file.

Stray files are any backed-up files that have been removed from the local machine, the backup set or excluded above.

Figure 4. Concurrent Workers Settings for VMware.

The default value for VMware is three workers; which means three VMs are backed up at a time. If the VMware host has adequate available resources (RAM and CPU), this value can be increased to back up to five VMs at the same time thereby improving backup speed.

Performance may degrade if backing up multiple VMs at once. Hosts with more robust specifications may be able to back up more VMs simultaneously.

Specific Restrictions and Recommendations

You cannot select the VM:

- On which the current agent is running.
- That is already part of another backup set. The names for these VMs are grayed out.

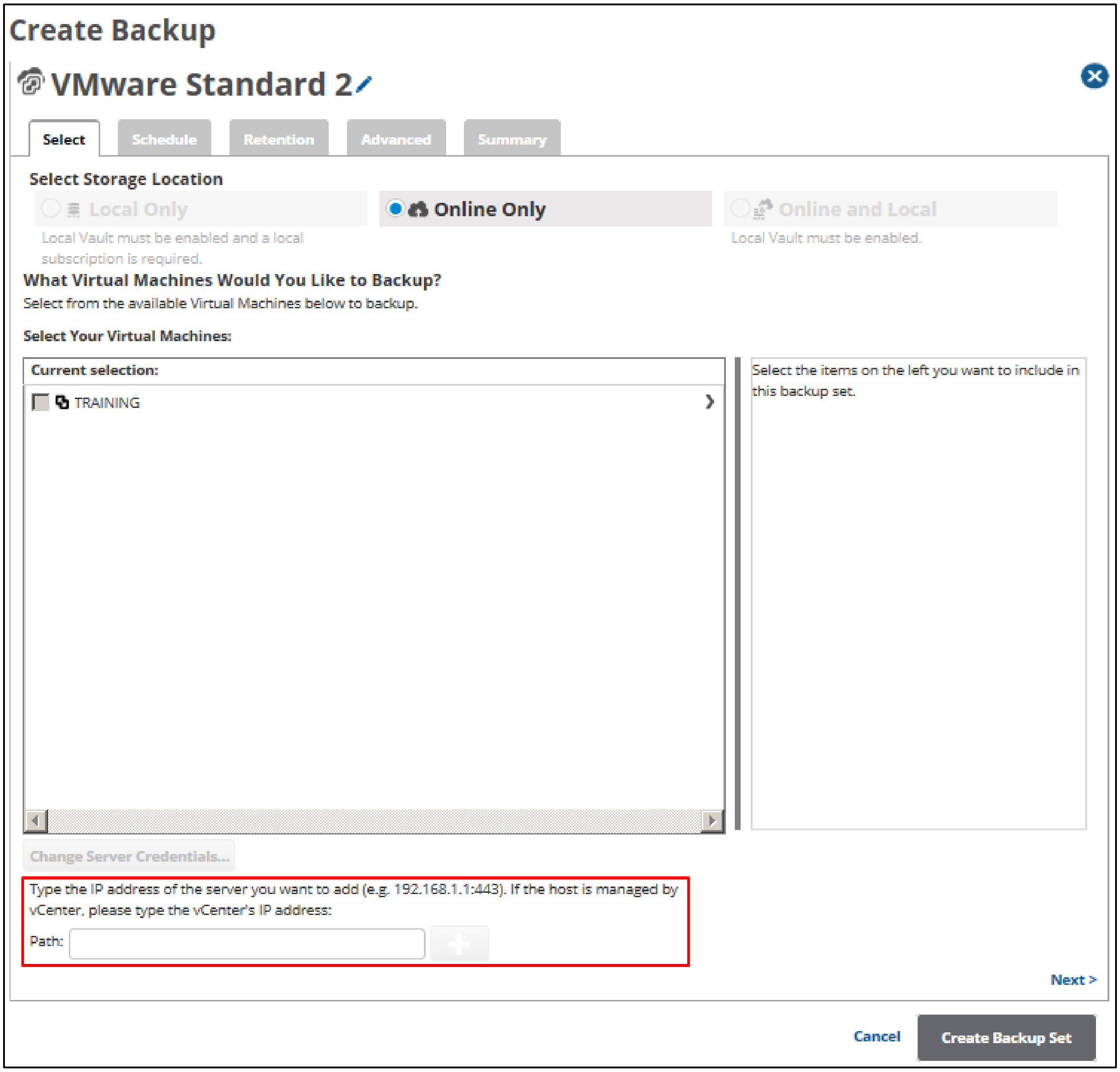
Do not choose a drive/volume/disk within a VM as a Local Vault location because if the VM goes down, all your local-only data could be gone, which defeats the purpose of the Local Vault.

If you try to back up a VM that no longer exists, the system displays an error message. This error must be resolved by editing the backup set. During the Backup Select step, a list of VMs that were selected for back up that no longer exist are displayed to let you know they must be removed from the backup set.

If you restore a VM and a new VM is created as a result, that VM is not automatically selected for back up. You must add this VM to a valid backup set after the restore is successful.

When creating a VM backup set consider the following information.

- Use a separate Backup Agent for VMs.
- Do not use the Agent being used for File and Folder, Exchange, SQL backups.
- The first time you create a backup set, you must manually enter the IP address of the server (ESXi host or vCenter) that hosts the VMs, as shown in Figure 5.



Create Backup

VMware Standard 2

Select Storage Location

○ Local Only — Local Vault must be enabled and a local subscription is required.

● Online Only

○ Online and Local — Local Vault must be enabled.

What Virtual Machines Would You Like to Backup?

Select from the available Virtual Machines below to backup.

Select Your Virtual Machines:

Current selection:

□ TRAINING

Select the items on the left you want to include in this backup set.

Type the IP address of the server you want to add (e.g. 192.168.1.1:443). If the host is managed by vCenter, please type the vCenter's IP address:

Path:

Figure 5. IP Address Field.

- If you enter a host IP that is managed by a vCenter, a message is displayed indicating that the vCenter is added.

- When adding a server, you must authenticate to the server. If the server is a vCenter using Active Directory (AD) credentials, the agent's credentials are used first.
  If AD credentials do not work, then you must enter credentials to the vCenter.
- Select any number of VMs under the selected server.
- Select VMs from multiple servers in the same backup set. A folder cannot be backed up but can be accessed to select multiple VMs. All selected and children-selected states are displayed.

Hyper-V Standard and Rapid Recovery Backups

Barracuda offers a native Hyper-V backup solution that allows you to protect virtual machines using the same web-based platform you use to back up the rest of your data.

General Considerations

This section includes the following:

- Rapid Recovery backups
- Standard backups
- Object-level recovery
- Maximum Size VM that Can Be Backed Up
- Recommended Number of Hyper-V VMs to Back Up on a Single Host
- Linux Running in a Hyper-V Virtual Machine

Rapid Recovery Backups

Rapid Recovery backups allow local backups of full VMs in a format that allows for fast RTO failover and object-level recovery.

Recover your VMs quickly (less than 15 minutes) and import the VMs into Hyper-V to run your recovered systems from the backup media. Use Rapid Recovery as a first line-of-defense against local failover and recovery solution to protect against host or VM issues or when:

- Your RTO are minutes, not hours or days.
- Protecting against user error and recovering individual files.
- Compliance standards do not require full encryption of all local backup media.

Standard Backups

Standard backups allow encrypted backups of full VMs to be stored in the Barracuda cloud or in a user's local storage.

You can restore VM VHD/VHDX files to a local or network location. Because this requires a copy operation, this restore has a longer RTO than Rapid Recovery. This restore can pull backup data from your local vault, or from the Barracuda cloud.

Use standard backups as a second line-of-defense against full-site disasters or downtime or when:

- A local backup is not available.
- A compliance standard requires fully encrypted and/or offsite backup of critical business data.

- Your RTO requirements are not as strict as Rapid Recovery.

Object-level Recovery

Object-level Recovery allows you to explore a VM backup from a point in time and restore individual files and folders.

Maximum Size VM that Can Be Backed Up

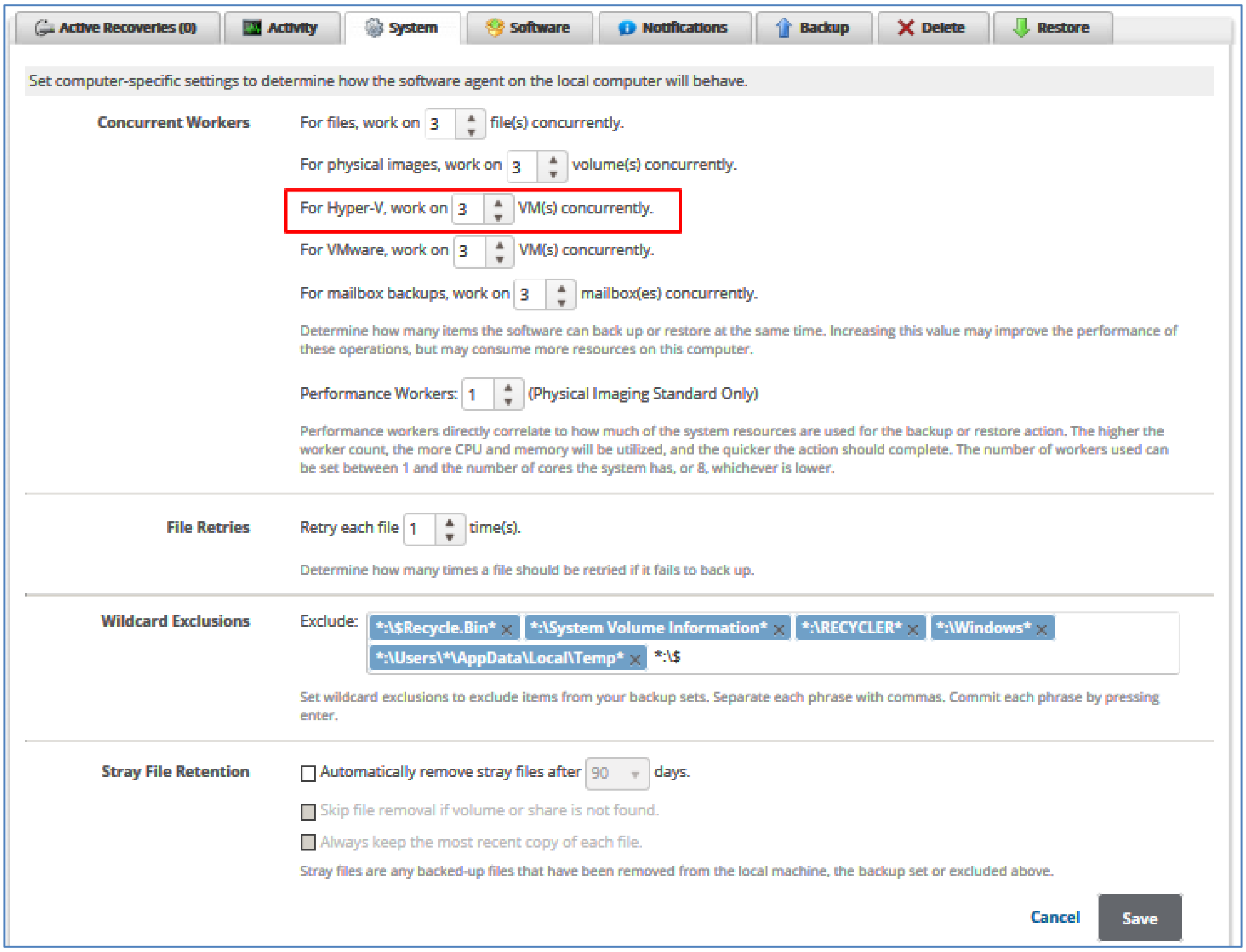
For Hyper-V or VMware Standard backups, there is no hard limit for backups. However, larger VMs may take longer to back up, especially if the VM contents change frequently.

Recommended Number of Hyper-V VMs to Back Up on a Single Host

Although any number of VMs can be selected for back up on a single host, the system resources of the host and the total number of VMs should be taken into consideration when choosing backup worker settings and creating backup sets.

Backup sets with large number of VMs take longer to back up, especially if the VMs’ data changes frequently. Schedule your backups accordingly.

You can choose how many VMs are backed up at the same time by modifying the Concurrent Workers setting on the System Settings page, shown in Figure 6.



Set computer-specific settings to determine how the software agent on the local computer will behave.

Concurrent Workers

For files, work on 3 file(s) concurrently.

For physical images, work on 3 volume(s) concurrently.

For Hyper-V, work on 3 VM(s) concurrently.

For VMware, work on 3 VM(s) concurrently.

For mailbox backups, work on 3 mailbox(es) concurrently.

Determine how many items the software can back up or restore at the same time. Increasing this value may improve the performance of these operations, but may consume more resources on this computer.

Performance Workers: 1 (Physical Imaging Standard Only)

Performance workers directly correlate to how much of the system resources are used for the backup or restore action. The higher the worker count, the more CPU and memory will be utilized, and the quicker the action should complete. The number of workers used can be set between 1 and the number of cores the system has, or 8, whichever is lower.

File Retries

Retry each file 1 time(s).

Determine how many times a file should be retried if it fails to back up.

Wildcard Exclusions

Exclude: *:\$Recycle.Bin* *:\System Volume Information* *:\RECYCLER* *:\Windows* *:\Users\*\AppData\Local\Temp* *:\$

Set wildcard exclusions to exclude items from your backup sets. Separate each phrase with commas. Commit each phrase by pressing enter.

Stray File Retention

□ Automatically remove stray files after 90 days.

□ Skip file removal if volume or share is not found.

□ Always keep the most recent copy of each file.

Stray files are any backed-up files that have been removed from the local machine, the backup set or excluded above.

Cancel Save

Figure 6. Concurrent Workers Settings for Hyper-V.

The default value for Hyper-V is three workers; which means three VMs are backed up at a time. If the Hyper-V host has adequate available resources (RAM and CPU), this value can be increased to back up to five VMs at the same time thereby improving backup speed.

Performance may degrade if backing up multiple VMs at once. Hosts with more robust specifications may be able to back up more VMs simultaneously.

Specific Restrictions and Recommendations

This section includes the following:

- Linux Running on a Hyper-V Virtual Machine Data Retention Settings
- Hyper-V Is Not Cluster Aware
- Do Not Use Image Option to Back Up a Host that is Running a Number of Virtual Machines

Linux Running on a Hyper-V Virtual Machine

In Hyper-V, Integration Services installed on the guest OS is required to back up Linux.

Integration Linux distributions that support or come with bundled Integration Services can be displayed at the following link:

https://technet.microsoft.com/en-us/library/Dn531030.aspx

Data Retention Settings

For maximum reliability and efficiency, the last 4 weeks of revisions, and no fewer than four revisions, is the recommended data retention settings for backup sets using:

- Hyper-V Standard
- VMware Standard
- SQL
- Exchange

Hyper-V Rapid Recovery backups run more frequently and allow you to choose a specific number of revisions to keep. Choose several revisions that keep data long enough to recognize any local failure (at least 24 hours, preferably a few days).

Hyper-V Is Not Cluster Aware

Currently, the Hyper-V plug-in is not cluster aware.

Backing up Hyper-V VMs from a clustered environment is not supported. Any Hyper-V backup sets that are in a clustered configuration fail all backup attempts.

Do Not Use Image Option to Back up a Host that is running a Number of Virtual Machines

For best recovery, use the Hyper-V backup set type to back up and restore individual VMs, and not the entire host.

Exchange Information Store Backup

Barracuda offers an Exchange Information Store backup solution that allows the MSP to select how much Exchange Information Store data to back up, protect, and recover.

Exchange Information Store backup has the following features:

- Back up database and log files, with flexible scheduling.
- Run automated backups in the background to avoid interruptions.
- Sort by date to restore full Exchange Information Stores.

General Considerations

Back up all Exchange databases to protect your customers' data in the event of a hardware failure or natural disaster. After you reinstall your operating system and Exchange Information Store, you can import the entire database from the last backup. This action minimizes the amount of downtime for the business.

Do not use the individual Mailbox Level backup for disaster recovery, since only one mailbox at a time is restored to Exchange, or to a .pst file that must be imported into Exchange.

Instead of selecting the Exchange database folder location in a file backup, create a new backup set in the Management Portal, and select **Exchange Information Stores.**

The ECHOplatform agent software must be installed directly on the Exchange server to display this backup set option.

The Barracuda Exchange plug-in backs up Exchange at the database level using Microsoft's best practices.

For Exchange 2010/2013/2016 the following process occurs:

Stage	What Happens
1	The ECHOplatform agent software uses Microsoft's Exchange Volume Shadow Service (VSS) copywriter. VSS takes a shadow copy of Exchange and backs up the files directly off the shadow copy.
2	Volume Shadow Copy can take a snapshot, from which the ECHOplatform agent software can back up directly, requiring less free Temporary Space. The ECHOplatform agent creates a persistent snapshot that is used for the duration of the backup. After the snapshot is taken, the Exchange VSS Writer is released, so that other utilities can back up Exchange.
3	During full backup, the ECHOplatform agent backs up the database files for Exchange, and then attempts to truncate the transaction logs on the machine after they are backed up. The Exchange database files are broken into 100 MB chunks that the ECHOplatform agent uploads individually to provide stability to the backup. Each chunk allows numerous retries in case the customer encounters connection issues. However, if the backup is canceled, or a chunk cannot be uploaded, the backup fails because not all chunks are present.

Specific Restrictions and Recommendations

When creating an Information Store level backup, the software requires you to pick which database you want to back up. You must configure a different backup job for each database being backed up.

Stagger the start times of the jobs if you have multiple Exchange backups, making sure that jobs do not start at the same time.

Schedule backup sets to run from smallest to largest.

Schedule the Public Folder database backup or smaller database backup first, so this backup is completed before the larger database backups run.

By default, the backup set schedule is configured according to Microsoft's best practice of one full backup per week with six daily incremental backups.

Your first backup of the database is a true full copy, and incremental backups afterwards contain only the transaction log changes to Exchange.

The next full weekly backup uses the ECHOplatform agent Intelliblox technology to take block-level differentials of the previous week's full backup.

Barracuda keeps a weekly retention of Exchange, and by default keeps four weeks of Exchange data. You can keep as little as one week of data.

To restore an incremental backup, the software must keep that week's differential, or full backup, and any other incremental backups from earlier in the week. This retention leads to increased usage but is essential to ensure that you can restore your data.

The two key settings in Exchange that need to change to ensure the most data efficient backups are:

- Circular logging
- Defragmentation

Circular Logging

Make sure that circular logging is disabled on each database you are backing up. Disabling circular logging prevents Exchange from overwriting Exchange transaction logs and allows the ECHOplatform agent software to perform normal incremental backups. Incremental backups are smaller, and complete faster during the week.

Defragmentation

Set Exchange maintenance such as defragmentation to once or twice per week. Exchange defragmentation shifts data around in your database files, which saves you space locally. However, frequent defragmentation shifts the blocks around in the files too much, forcing Intelliblox block-level technology to make more frequent full backups.

If you use another backup utility to back up Exchange such as NTBackup or Backup Exec, set that software to Copy Only Mode to copy the Exchange transaction logs, so that the ECHOplatform agent can back them up and truncate them. Using other software to truncate the Exchanges logs means that the ECHOplatform agent software receives logs that are out of order, forcing full backups and increasing overall data storage.

Exchange Forcing Full Backups

If Exchange backups take a long time and backs up too much information, view the logs from the ECHOplatform agent software under **Diagnostics > Browse Previous Actions** to see if backups are full.

If backups are full, check the following conditions:

- Circular logging
- Exchange logs not being in sequential order
- Too many changes to the .edb files

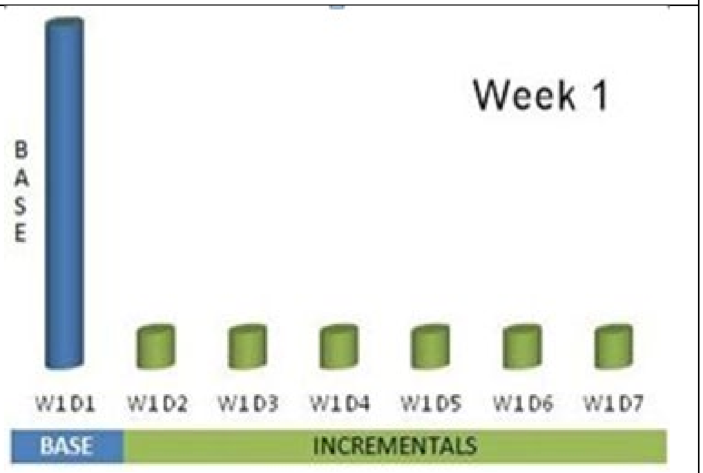
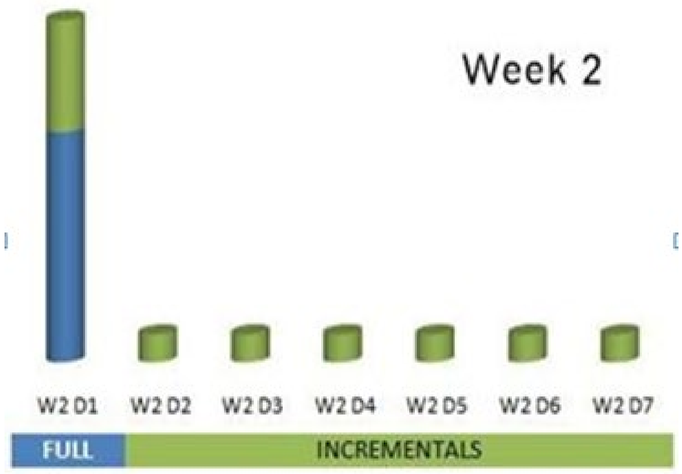
Exchange logs can get out of order from other backups truncating logs or from failed backups. In addition, defragmenting can disrupt Intelliblox block-level technology.

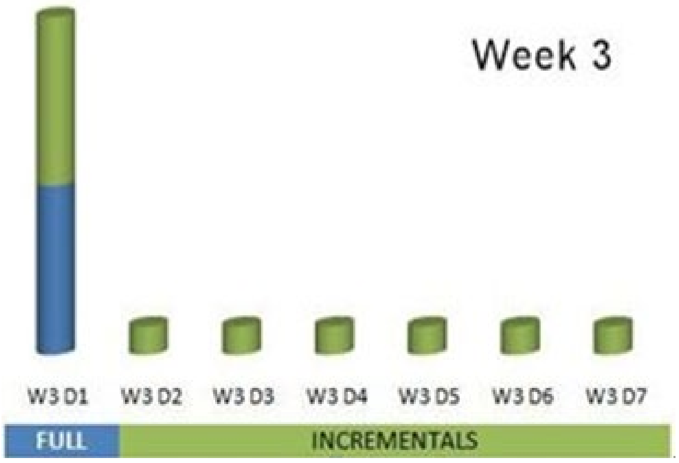
To resolve these issues, perform the following steps.

1. Disable circular logging.
2. Set other utilities like NTBackup or Backup Exec to **Copy Only** mode for the logs.
3. Set Exchange defragmentation to occur once or twice per week so as not to disrupt Intelliblox.

Exchange Information Store Usage Logic

The following table provides the decision-making stages followed by the ECHOplatform agent software as it manages Exchange Information Store content using the default 4-week retention rule policy.

Week	What Happens	Graphic
1	Exchange is called for a full (Base) backup. Exchange truncates all Log files into the .edb, and the Backup Agent backs up all the data in the edb.	
2	The Backup Agent calls Exchange to do log truncation, pulling all last week's transaction logs into the .edb. Intelliblox then processes the .edb and backs up only the new additions to the database. The blue portion represented in the graphic is not transferred or charged for, as it already exists in the week 1 full revision.	

Week	What Happens	Graphic
3	The same as Week 2. **Note**: To restore Week 3, day 4, you need Week 1 Day 1 and Week 3 Days 1, 2, 3, 4. Week 2 is not needed to restore data from Week 3.	
4	The same as week 2.	NA
5	Assuming a four-week retention policy, by the end of week 5, no data is needed from Week 1 days 2-6. These files are purged. Note that all current weeks are still dependent on Week 1 Day 1. This file is not purged.	NA
6	By the end of week 6, no files are needed from Week 2. These files are purged. Note that Week 1 Day 1 is retained.	NA

Exchange Mailbox Level Backup

Exchange Mailbox Level backups offer the ability to recover individual mail items in case of deletion or user error. Use this option to protect important employee mailboxes locally and to recover individual mail items. This option is best used when backed up local-only.

Barracuda does not recommend using Mailbox Level backups as a disaster recovery method since restoring an entire information store via a Mailbox Level backup is much slower than from an Information Store backup.

If an entire Exchange environment goes down, restoring the Information Store takes substantially less time than restoring individual mailboxes or mailbox items.

Mailbox Level backup sets are best used as a data-archiving utility to keep a record of the emails sent and received (as well as contacts and calendars) over a long period.

General Considerations

With the version 5.6 upgrade, Exchange Mailbox Level backups:

- Use Exchange Web Services (EWS) that allow multi-threading.
- Can be restored directly to a (.msg) file or to an Outlook Personal Storage Table (.pst) file.
- Can be run from any computer with web access so the ECHOplatform agent does not need to be installed on the Exchange server.

The following application settings are required for Exchange Mailbox Level backups.

Application	**Required Settings**
Exchange 2010/2013/2016	Create a Service Account with the following permissions: • Organization Management Role • Application Impersonation Role • Discovery Management Role (2013 & 2016 only) Disable EWS Throttling for all users.

The following server settings are required for Exchange Mailbox Level backups.

Server	**Required Settings**
Windows Server 2012	• Must use Internet Information Services (IIS). • IIS Basic Authentication for Powershell Remoting enabled
Windows Server 2008	• Windows PowerShell 2.0 • Powershell Remoting enabled • IIS Basic Authentication for Powershell Remoting enabled • Agent machine must belong to the same domain as the Exchange Server

The ECHOplatform agent software provides a series of validation steps to inform you if the user or the environment does not meet any of the necessary criteria.

Known Issues

The following table lists the known issues for Exchange Mailbox Level.

Exchange Object	**Issue**
Public folder	Public folder permission must be configured separately. Ensure you use the **Edit all** permission to avoid the following error message: `Access is denied. Check credentials and try again.`
Public folder item's property	EWS does not support directly setting the date and time stamp.
Email's, Meeting, Appointment, Task, Contact fields	Body and Note properties do not support RTF format, tables, WordArt, illustrations or images during restore to Exchange.
Meeting's properties	EWS does not support the following Meeting properties: Accepted, Declined Email, Tentative, Declined, New Time Proposed email, Current or Proposed.
Appointment's deleted occurrences	EWS does not support updates to the Deleted Occurrences field.
Attachment's size	The limitation to attachments is 100 MB.
Outlook display after a restore	• The first line in an email body aligns to the left. • Email's Subject, Location and When properties display a format that is different from the original.
Outlook	Does not support Attachments in attachments.
Contact's business card	Not supported for restore to file or PST.

Failing on GAL in Exchange 2010

If failing on GAL in Exchange 2010, perform the following steps.

1. Confirm the mailbox is not hidden in Exchange, and then verify that IPv6 is turned on.
2. With IPv6 turned on, modify your host file to contain an IPv4 address, so when you ping localhost you get IPv4 response back.

Backing Up Individual Mailboxes with the ECHOplatform Agent

To back up individual mailboxes and messages you must:

- Run the Backup Agent as a specific user that has a mailbox in Exchange.
- Provide the Backup Agent with domain administrator privileges.

The backup process works as follows:

1. The ECHOplatform agent user logs into Exchange.
2. The agent pulls the individual messages and items out of Exchange to a temporary folder that you designated in the software.
3. The folder contents are bundled into zip files.
4. The zip files are transferred to the Barracuda servers.

Specific Restrictions and Recommendations

After you validate all the necessary steps in the software to perform Mailbox Level backups, you can select specific mailboxes for back up and choose several other settings, including:

- Auto backup of new mailboxes
- Auto exclusion of deleted items
- Auto exclusion of junk mail
- Attempting to back up hidden mailboxes

Because Mailbox Level backups are intended for archival purposes, Barracuda continues to retain messages as part of the backup, even after they have been deleted in Exchange. Users frequently use mailbox backups to meet compliance standards, so Barracuda does not have revision rules to remove messages nor stray file rules that dominate mailbox backups. You can manually delete mailboxes from the backup that you do not want.

Exchange Mailbox Level backups can overlap with Exchange Information Store backups since they use different processes.

Message Level Backups outside one million messages can take a long time depending on connection speed and bandwidth availability.

You can create smaller message level jobs to increase efficiency.

You cannot have Outlook installed on the backup server.

SQL Backup

Barracuda offers native Microsoft SQL Server backup that enables MSPs to protect unlimited versions of their clients' SQL databases from business continuity and disaster recovery (BCDR) threats like user error or equipment failure.

Military-grade data encryption keeps your SQL backups safe in the Barracuda secure dual-coast data centers. The Barracuda central web-based platform allows you to back up SQL with the same tool you use to protect everything else.

General Considerations

Make sure the software has SQL admin credentials.

For any errors, check the SQL Management Studio.

When backing up Microsoft SQL databases, create a specific job using the Barracuda SQL plug-in. To do this, instead of selecting the SQL database folder location in a file backup, create a new backup set in the Management Portal, and select the SQL type.

The Barracuda SQL plug-in uses the same API calls that Microsoft makes when you select a database in SQL for back up.

The ECHOplatform agent creates .bak files of the databases in the temporary folder chosen in the software and then backs them up to Barracuda servers.

Barracuda allows you to back up both local and remote SQL servers using the ECHOplatform agent software.

Whenever possible, install the software directly on the SQL server (best practice).

To back up a remote SQL server, you must point the ECHOplatform agent software to a temporary directory on the remote SQL server, where the SQL .bak file is created. Make sure that the user (what the ECHOplatform agent service is running as) has permission to write to that directory and that the user (what your SQL service is running as) has permission to access that temporary directory.

Specific Restrictions and Recommendations

When you create a SQL backup set in the software you can search for SQL servers and instances that exist in your environment. You can then select the method with which to authenticate with that SQL server. You can choose Windows authentication or SQL authentication.

Windows authentication uses the credentials of the Backup Agent service (the ECHOplatform agent uses the Local System account by default) to connect to the SQL instance.

SQL authentication allows you to select a user, such as a SQL administrator account, and plug in the credentials of that user.

You can then refresh your list of databases to view all the databases on the instance you have selected to back up. You can select a single database, or you can select multiple ones. You can also de-select specific databases from the backup.

SQL backups are scheduled by default according to Microsoft best practice of having one full backup per week with six differential backups. Barracuda keeps SQL backups on a weekly basis, by default keeping four weeks of SQL data. You can configure the software to keep as little as one week of data.

Your first backup of the databases is a true full copy.

Day-to-day differentials back up the transactional changes since your most recent full backup. The weekly full backup uses the ECHOplatform agent Intelliblox technology to run a block-level differential on the previous full backup.

Configuring SQL Databases to be Backed Up by the ECHOplatform Agent

To back up a database successfully, the database mode in SQL needs to be set to Normal. SQL is not able to back up databases that are in Shutdown mode.

To add or subtract databases from the backup set in the Barracuda wizard, the databases must be set to Normal mode.

You can make the change to the database mode within SQL Management Studio.

In addition to having the database set to Normal mode, make sure that the AutoClose option is disabled for each database you want to back up. AutoClose shuts down a database when the last user logs out, that prevents the ECHOplatform agent software from accessing the data to back up.

Having databases set to full recovery mode in SQL forces the ECHOplatform agent software to make full backups instead of true differential ones.

Intelliblox technology allows block-level differentials on previous backups, but the ECHOplatform agent has to copy all the SQL transaction logs for every backup, creating larger files.

Full recovery mode specifies that all database transaction logs be saved so that you can restore to very specific transactions in the database history.

The recommended configuration is to set your databases to simple recovery mode in SQL.

This mode backs up and truncates the SQL transaction logs that make your daily differential backups much smaller. However, simple mode does not have the same level of granularity to restore specific points in database transaction history.

When backing up SQL Express data, point the software's temporary folder to the same folder where SQL Express generates backup files. SQL already has permission to write to this location when creating .bak files.

SQL Permissions

The ECHOplatform agent service needs to be installed on all computers/servers being backed up. The Backup Agent performs all:

- Backups
- Restores
- Deletes

The Backup Agent runs as a user (*Local System* by default) and takes the permissions of that account when conducting backups.

The Backup Agent user needs to have a log in for SQL and permissions to back up databases, or you need to set the job to use SQL authentication.

For best results, run the Backup Agent service as an administrator user.

Running the Backup Agent Service as a User

To run the Backup Agent service as a user, perform the following steps.

1. At the Windows Start menu, right-click **Computer**, and select **Manage**.
2. In the left-pane, expand **Services and Applications**, and select **Services**.

3. Right-click **Backup Agent**, and click **Stop**
4. Right-click **Backup Agent** again, and click **Properties**, and then click the **Log On** tab.
5. Select the **This account**: radio button, and then click the **Browse** button.
6. In the text box at the bottom, type in the name of the authorized user you want to run the service as, click **Check Names**, and then, click **OK**.
7. Type and confirm the user's password, and then click **OK**.
8. Right-click **Backup Agent**, and then click **Start**.

System State Backup

This option lets you back up the computer's system state data.

General Considerations

A System State Backup is a backup of operating system configuration files and is recommended as part of a server disaster recovery plan. System State Backups include the:

- System Registry
- Active Directory; backs up only if you have the specified services installed
- COM + Database
- SysVol
- Certificate Services; backs up only if you have the specified services installed
- IIS Metabase; backs up only if you have the specified services installed

System State Backups are meant only for recovery to the same server, or to another server with the identical operating system and hardware. Microsoft does not support restoring System State to different hardware as referenced in the Knowledge Base article, *http://support.microsoft.com/kb/249694*.

How the ECHOplatform Agent System State Backup Works

The Barracuda System State plug-in leverages the built-in Windows backup tools to create a System State Backup.

Windows 2008 however requires the Windows Backup utility to be installed, that does not come natively with the operating system.

You must add the Windows Server Backup utility through the Programs and Features section of the Control Panel.

If you are on a Server 2008 installation and System State is not displayed as an option in the ECHOplatform agent software, then you do not have Windows Backup installed.

With the above Windows utilities installed, set the schedule in the ECHOplatform agent software and the number of weeks of backup you would like to keep. The ECHOplatform agent software calls these utilities to create the backup file on the system before the ECHOplatform agent backs up the file to Barracuda servers.

In accordance with Microsoft best practices, System State is scheduled by default to run once weekly. However, you can run the System State Backup every day if you desire.

NTBackup generates a .bak file that the ECHOplatform agent software backs up to the remote servers. To restore the information, select the file with the ECHOplatform agent software to restore the file to your computer.

Windows Server Backup creates several small files that the ECHOplatform agent packages and bundles into a .tar file. After you restore the .tar file using the ECHOplatform agent software, you can unzip the files, and point Windows Backup to the directory to restore the files.

The ECHOplatform agent Intelliblox technology saves block-level differentials from backup to backup, frequently however there are too many changes between the files to save. Allot more space in your backup plan based on the number of System State Backups you are planning to keep.

Specific Restrictions and Recommendations

System state backups for Server 2008 are done with the Windows Server Backup program that does not come pre-packaged with Windows.

In Server 2008, Microsoft requires that you perform the System State Backup on a non-critical volume. A critical volume is a drive that contains files and programs that the operating system uses. The Windows Backup utility creates the backup file on this non-critical volume and then Barracuda backs up the file using the ECHOplatform agent software. One option with Server 2008 is to create a new partition with 15 – 20 Gbs free and use that for the System State Backup.

Microsoft uses its own criteria to determine what a critical drive is, so the ECHOplatform agent does not have the ability to create the backup file on a drive that is marked as critical by the operating system. If you only have one hard drive, use a portable hard drive to create the backup file. This portable drive can be used as temporary space for other backup sets or as your local vault.

If you do not have another drive or the ability to use a portable drive, Microsoft does have a work around in this Knowledge Base article, *http://support.microsoft.com/kb/944530*. The article details making modifications to the registry to use a critical drive to create the backup file and works for local system state backups but not ones run with the ECHOplatform agent software.

Windows 2008 system state backups do not adequately function as disaster recovery. The backups are designed for snapshot reversion only. Because of limitations in the Windows Backup feature, you may only recover to the exact same installation of Windows on the exact same hardware. If you try to restore to a different installation of Windows, even if it has identical hardware, the restore fails. See http://support.microsoft.com/default/kb/249694 for more detail.

System State Backups for Server 2008 can be up to five or more Gbs in size. These sizes are dependent on the machine backing up and are determined by the Windows backup utility.

> *System State backups can only recover to the same server or to another server with the identical operating system and hardware. Microsoft does not support restoring System State to different hardware.*

System State Backup Failing on Server 2008

The ECHOplatform agent calls the Windows Server Backup utility to create the backup, and then bundle the files into a single zip file for upload.

Windows Server Backup needs to be installed. You need 7 to 10 GB of free space on a local drive.

Backups must be written to a non-critical drive (Microsoft requirement), and this drive cannot not contain operating system files or registry entries in the backup set.

If your temporary folder is also on this non-critical drive, you need free space at least two times the size of the system state backup file to back up the file successfully.

Resolution

- Use ECHOplatform logs to view errors: **Activity > Browse Previous Actions**. Double-click a job to view logs.
- Search the Barracuda Knowledge Base for one of the common exit codes (2 & 3)
- Check Windows Event Viewer Application Logs for more information.
- When in doubt, run a command line backup in Windows using the Wbadmin. If the command runs, the issue is isolated to the ECHOplatform agent software: *wbadmin start systemstatebackup -backuptarget:G:* (Where G is target drive)

[This page left intentionally blank.]

Chapter 4. **Local Vault Backup**

This chapter provides the following topics:

- Overview
- General Considerations
- Specific Restrictions and Recommendations

Overview

Local Vault is an option that keeps a copy of the data stored off-site, locally on a USB drive, or NAS device. The following Barracuda MSP backup types provide a local vault backup option.

- File and Folder
- Physical Imaging Standard
- Hyper-V Standard
- VMware Standard
- Exchange Info Store
- Exchange Mailbox
- SQL
- System State

General Considerations

Local Vault sync writes data simultaneously to both places. *Local Vault async* writes to the local drive first and then copies completed backups to the off-site location.

Local Vault sync synchronizes the data back to the Local Vault if the data on Barracuda servers does not match the data on the Local Vault. For example, if a backup runs when the Local Vault is disconnected, *Local Vault sync* puts the Local Vault back in sync with the server when the Local Vault is reconnected.

Do Not Swap Local Vault Drives

If you change the Local Vault, the original drive no longer receives updates.

Barracuda conserves storage space and bandwidth by backing up only the files that change, and then only the parts of the file that change (delta blocks) with Intelliblox technology. A Local Vault is an exact copy of the data stored in Barracuda cloud, receiving the same initial and incremental backup sets. Swapping a Local Vault with another drive disrupts that sequence. The new drive does not have the initial seed or previous incremental backups.

Resolution

You can copy Local Vault drives. Connect a second drive to a USB and perform a copy. You can then take the copy offsite, keeping the original Local Vault in place. Just remember to take the copy.

Specific Restrictions and Recommendations

The following are restrictions and recommendations for Local Vault.

- Use regular sync for most situations.

- Do not put the Local Vault and Temporary Folder in same folder.
- Create different folders for each computer on a NAS or shared drive.
- Avoid using async unless the client has a very poor network connection (sub 1 Mb upload speed).
- Monitor async from the View Current Activity section of the software.
- Cancel async from the View Current Activity section of the software, if necessary.
- Do not swap out the location (drive) that is used as the local vault.
- If the local vault is damaged/removed/hardware failure, you need to copy the old vault to the new location. If you are unable to do so, contact the Partner Support Team.
- To use a network device as the local vault, you first need to enter the credentials for the destination into the share manager.
- Make sure that the backup agent service is running as a user account that has no access issues reaching the local vault destination.

Chapter 5. **Local Only Backup**

This chapter provides the following topics:

- Overview
- General Considerations
- Specific Restrictions and Recommendations

Overview

The Local Only Backup feature allows you to create backups that are only stored on the Local Vault. These backups are not stored on Barracuda servers and do not count toward your remote storage.

The following Barracuda MSP backup types provide a local only backup option:

- File and Folder
- Physical Imaging Standard
- Hyper-V Standard
- VMware Standard
- Exchange Info Store
- Exchange Mailbox
- SQL
- System State

General Considerations

The Local Only Backup feature allows you to create backups that are only stored on the Local Vault. These backups are not stored on Barracuda servers and do not count toward your remote storage.

Barracuda only supports using a single device for local only backups.

Barracuda does not support hard drive swapping and has not designed the local only feature to be a tape solution. Barracuda does not support swapping drives because the software writes the base copies of files on the initial backup to your local location, and then uses Intelliblox technology to write just the block changes to the drive. If you are swapping drives, you could have the base copies on one drive, and the changes on others, that creates problems on restore because pieces of files could be on different drives

Local Only Backup allows Barracuda partners to back up non-critical data exclusively to a local storage device on the customer's site. This feature allows partners to take a hybrid approach when backing up customer's information.

Local Only backup sets are managed exactly like Barracuda online backup sets, so partners do not need to utilize a different reporting system for remote and local backups and need to train technicians on only one solution, thus saving time and money.

Local Only Backup sets allow partners to separate critical data from non-critical data. Non-critical data can be stored to a device on the customer premise in an encrypted format. Critical data can also be stored on the same device, in addition to the Barracuda Cloud, to speed up restores.

For the procedure to run a local only backup, see the *ECHOplatform Quick Start Guide*.

Specific Restrictions and Recommendations

Files that are part of the remote backup cannot be included as Local Only Backup sets.

If you wish to convert data in the remote backup into a Local Only Backup, you must delete the remote data first, and create a new backup set designated as Local Only.

Local Only Backups are not available to back up accounts that do business directly with Barracuda. Only partners can enable this feature for their customers. Master partners also can assign their subpartners Local Only Backup subscriptions.

Select a quality device with an estimated life span of 35 years. This device should be at least 4x your current backup size to accommodate data growth over the life span of the device. Do not utilize the same physical disk or array that contains the data being backed up.

Utilize Local Only Backup for only non-critical information. Always store critical customer data in the Barracuda cloud.

Mailbox backup sets are a great candidate for local exclusive backups. Back up the entire Exchange databases to the Barracuda cloud to restore the entire mail system if a disaster strikes. Setting Mailbox Level backups to be a local exclusive backup set allows you to restore individual emails back if a customer deletes them or suffers a localized disaster. You can also avoid the expense of storing duplicate information in the Barracuda Cloud.

For the procedure to change a cloud backup to a local only backup, see the *ECHOplatform Quick Start Guide*.

Chapter 6. **Restore Considerations and Recommendations**

Before restoring data, you must disable any backup sets that might run during the restore to prevent overwriting the production data that is being restored.

This requirement is especially relevant if you have previously restored the computer from an image backup containing an older version of the file catalog than when you last backed up. Running a backup using the older catalog replaces the one that exists on Barracuda servers, thereby removing files more recently backed up.

If a machine is restored to a previous time with an Image, you need to create a new subaccount.

For procedures to restore backup sets, see the *ECHOplatform Backup and Restore Reference Guide*.

[This page left intentionally blank.]

Chapter 7. **Managing Additional Usage**

This chapter provides the following topics:

- Overview
- Setting Archiving Rules
- Deleting Backup Set Files
- Deleting Stray Files
- Replacing Computers

Overview

Users may find that over time, the usage on their account continues to increase. As data is added to a machine, any data that is added to a folder already being backed up is also backed up. Files that are updated also increase usage on the account. The following considerations may help you manage and lower usage and prevent usage from rising sharply.

Setting Archiving Rules

Archiving rules are specific to each type of backup set and must be configured while creating or editing the backup set.

You can set the number of days that the backup sets are kept and set the number of versions that are kept.

The more versions that you keep can cause higher storage usage.

If changed, the Archiving Rule applies to the data you back up when the next backup runs. Previous backup sets are not affected.

See the *ECHOplatform Backup and Restore Reference Guide* on how to adjust the archiving rules for a backup set.

Deleting Backup Set Files

See the *ECHOplatform Backup and Restore Reference Guide* for more information on deleting backup set files.

Deleting Stray Files

Stray files are flagged files on Barracuda servers that used to be scheduled for back up, but currently have been excluded from a backup set or deleted locally.

With the Annual Package Pricing option, Barracuda manages the deletion of stray files. Otherwise, Barracuda keeps these files in case a client mistakenly excludes or deletes them but still wants to restore them.

You can run a Stray File Delete to clear all data fitting this description.

CAUTION! Do not perform a Stray File Delete if you accidentally have deleted any files from the local computer because Stray File Delete deletes strays from both the cloud and the local vault. After files are deleted from both, they cannot be restored.

Figure 7 provides a display of the Stray File Delete option on the Files and Folders Delete page.

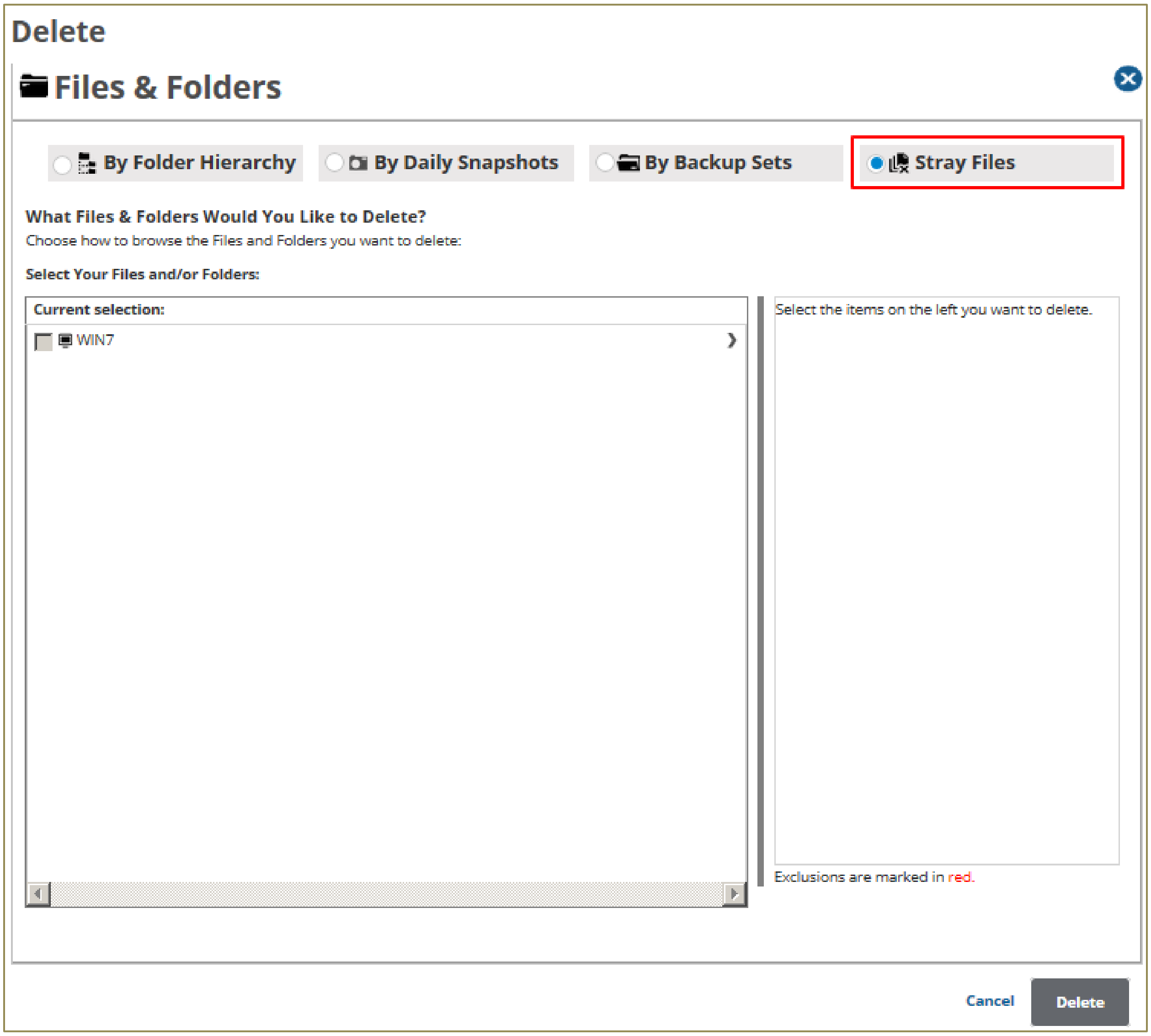

Delete
Files & Folders
○ By Folder Hierarchy
○ By Daily Snapshots
○ By Backup Sets
● Stray Files
What Files & Folders Would You Like to Delete?
Choose how to browse the Files and Folders you want to delete:
Select Your Files and/or Folders:
Current selection:
□ WIN7
Select the items on the left you want to delete.
Exclusions are marked in red.
Cancel
Delete

Figure 7. Stray Files Delete Option.

The Automatic Stray File Delete option deletes stray files after they reach a specified age.

Automatic Stray File Delete functions on a computer-basis but can be configured in a template (see the *ECHOplatform Quick Start Guide*) and then applied to individual computers or groups.

Barracuda recommends the default of 90 days unless you need to increase or decrease the length of retention.

Barracuda also recommends you leave the **Skip file removal if the volume or share cannot be found** check box selected to save storage space.

See the *ECHOplatform Backup and Restore Reference Guide* for more information on stray file management.

Replacing Computers

A common reason for unplanned increased usage is the replacement of old computers with new computers. Typically, all the data from the old computer is transferred to the new computer and a new Backup set is created for the new computer.

Delete unnecessary data held by the old computer from the server because duplication and increased usage results.

[This page left intentionally blank.]

Chapter 8. **Avoiding Common Problems**

This chapter provides the following topics:

- Open and locked files
- Unable to connect to servers
- Reboot stops Backup Agent
- Backup Agent does not start
- Anti-virus exclusions
- Keep your private key safe
- Proper procedure for switching between local and online
- Keep Local Storage and Local Vault protected from crypto-type viruses

The following best practices help avoid common problems. These problems are typically caused by mistakes in setting preferences, notifications, or other configurations of the software.

Open and Locked Files

Barracuda can back up open and locked files because the Windows Volume Shadow Service is used to copy the files to a temporary location, as they are encrypted and sent to the Barracuda servers. For instance, if you choose to back up your Outlook.pst file, and you have Outlook open when the backup runs, Barracuda can back up that file properly.

Note: You can configure ECHOplatform to back up files across a network to another server or computer. However, VSS does not allow the ECHOplatform agent to back up open and locked files across the network.

Whitelisting the Backup Agent

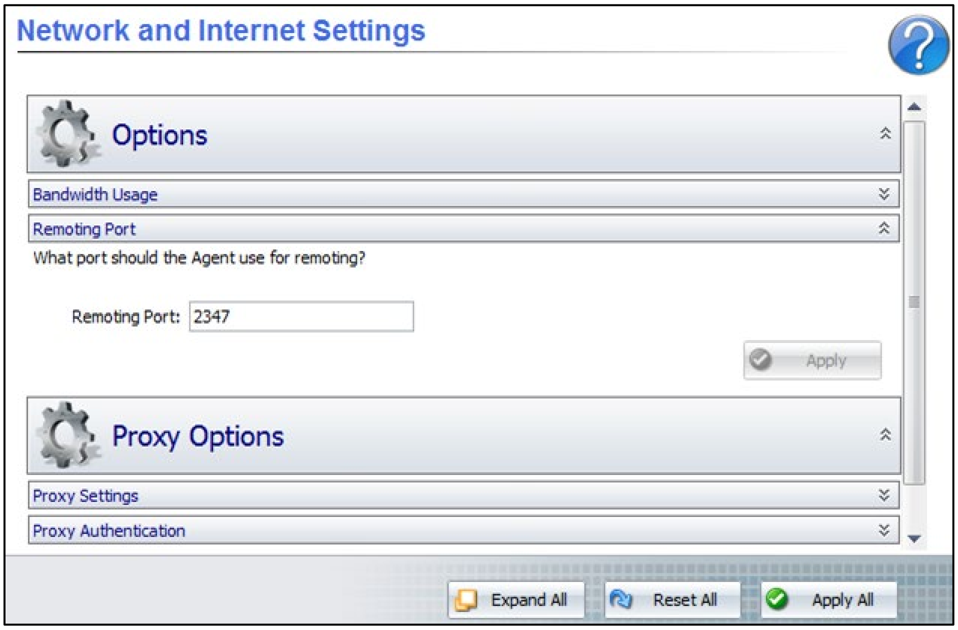
To ensure communications between the Backup Agent and Barracuda MSP servers are not impeded, you may need to whitelist some specific IP addresses, ports, and services. The following table provides the recommended whitelist items.

Country	**Host Name**	**IP Address**	**Ports**	**Services**
US + CA	mail4.intronis.com	38.97.76.85	443 2347* (both inbound and outbound)	BackupAgent.exe BackupExtender.exe BackupUpdater.exe BackupCLI.exe BackupStatusIcon.exe
	installer-api.intronis.com	38.97.76.69		
	relay.intronis.com	38.97.76.77		
	relay02.intronis.com	38.97.76.79		
	relay03.intronis.com	209.66.81.238		
	relay04.intronis.com	209.66.81.235		

Country	Host Name	IP Address	Ports	Services
	esureit.intronis.net	209.66.81.228		
	bk1.onlinebackupsolution.com	38.97.76.70		
	bk1-ca.onlinebackupsolution.com	38.103.154.100		
UK	mail1.echo.intronis.com	64.235.158.231		
	installer-api.echo.intronis.com	64.235.158.228		
	bk1.echo.onlinebackupsolution.com	64.235.158.227		
	relay01.echo.intronis.com	64.235.158.232		
	relay02.echo.intronis.com	64.235.158.233		

*Your specific Backup Agent may be configured to use a different port. To verify which port it is using, check the "Remoting Port" option in the "Network Settings" section of "Preferences" (in the Backup Monitor, not the management portal).

The following graphic is an example view of the remote port setting.


Network and Internet Settings

Options

Bandwidth Usage

Remoting Port

What port should the Agent use for remoting?

Remoting Port: 2347

Reboot Stops Backup Agent

Because the Backup Agent service performs all backups, restores, and deletes, if the service is restarted during an action, or the computer is rebooted, the action fails. The failure is happening if the following occurs:

- The logs for a backup job halt abruptly without the normal cleanup actions.

- The Exchange or SQL job immediately switches to cleaning up the information that was just uploading.

To display computer shutdowns and Backup Agent restarts, open **Activity**, **View Detailed History** that displays the software's general logs. Also, the application logs in Windows Event Viewer typically provide information.

Resolution

Cancel a job in the software before you reboot the computer or restart the Backup Agent.

Wait until the action has completed before rebooting.

If the status icon at the bottom right of the screen displays a red arrow, the backup agent service must be restarted.

There are two ways to restart the Backup Agent service:

- Through the services panel
- From the system tray

Restart Backup Agent through the Services Panel

To restart Backup Agent through the services panel, perform the following steps.

1. Select **Start**, right-click **My Computer** and click **Manage**.
2. Under Computer Management, select **Services and Applications** and then **Services**.
3. Locate the ECHO platform Backup Agent, right-click and select **Restart**.

Restart Backup Agent from the System Tray

To restart Backup Agent from the system tray, perform the following steps.

At bottom right of your screen, the Backup Agent status icon is displayed.

1. Right-click the icon, and then select **Restart Backup Agent**.

   After the arrow turns yellow, the backup agent is restarted.

2. Double-click the icon to open the Backup Agent monitor.

Backup Agent Does Not Start

If the Backup Agent fails to start on a computer, perform a clean re-install of the software to create a new version of the catalog.

1. Uninstall the software through Add/Remove Programs or Programs and Features in the Windows Control Panel.
2. Find the installation folder (usually located in *C:\Program Files or C:\Program Files (x86)*) and rename the folder to indicate that the folder is an old installation directory.
3. Re-install the software using the normal process.

Anti-Virus Exclusions

Some client's machines may stop running backups properly or cannot keep the Backup Agent service started. Or, when running the software installer package, the software hangs up or does not properly install Barracuda services.

Antivirus software installed on the client may prevent backups from running or even the Backup Agent service from running.

When encountering issues installing the ECHOplatform agent software, temporarily disable antivirus or firewall software on the machine. In addition, many antivirus suites have local and administrative interfaces. From time to time, adding exclusions in the local interface is insufficient.

If the antivirus suite comes with an administrative agent, you need to add the suite to exclusions.

Disable the real time protection and/or temporarily disable the associated services, if the ECHOplatform agent software installation has been blocked with the following applications:

- Microsoft Security Essentials
- Sophos
- Symantec Endpoint Protection
- Spyware Doctor
- Trend Micro
- AVG

After the ECHOplatform agent software is installed, add the ECHOplatform agent software's installation folder to exceptions from real-time scans, network filtering, firewall, etc.

Example*: C\Program Files\Barracuda MSP\eSureIT*. In addition, add these five executable files to the exclusion list:

- BackupAgent.exe
- BackupCLI.exe
- BackupStatusIcon.exe
- BackupUpdater.exe
- BackupMonitor.exe

You also may need to enable outbound connections on port 443 or 2347, which is the port the ECHOplatform agent uses to communicate to the Backup Monitor (the interface).

Exclude any Local Vault/Temporary directories within antivirus suites. Some antivirus programs (AVG, for example) either block transference of data to these directories or flash notices about BackupAgent.exe's attempt to work within these directories.

Keep Your Private Key Safe

The encryption key is the key to restoring your data. When using the Backup Agent, data is encrypted with AES 256 bit military-level encryption before being sent to Barracuda servers for storage. Your encryption key allows you to decrypt the data when performing restores and makes your data readable on your computer. The key is 48 characters in length and can be chosen as a private key or managed key.

A **private key** is completely user defined, meaning you decide exactly what 48 characters comprise your encryption. Since you define what the key is, you are responsible for keeping that key in a safe location that can be accessed in the event of a computer crash. Unfortunately, if you do not have your private key when you need to restore files, you are unable to restore them.

Using private keys are not supported for remotely installing via RMMs.

A **managed key** is an encryption key tied to your username and password and is generated by the ECHOplatform agent. You do not need to keep a copy of your managed key. The ECHOplatform agent system remembers the key for you.

If you have one type of encryption and would like to switch to another, the ECHOplatform agent needs to perform a full account reset from the ECHOplatform agent side. This reset, purges the data for an account from the ECHOplatform agent side, and makes the account as if you had never backed up with us, allowing you to pick the type of encryption key you would like when you re-install the software.

The encryption key is needed in case you need to restore your data. If you do not choose a managed key or have upgraded from an earlier version of the Backup Agent, you need to export and save your encryption key in a safe place.

Creating an Encryption Key

To create an encryption key, perform the following g steps.

1. Open the Backup Agent Monitor by selecting *Start->All Programs->Barracuda MSP->ESureIT Monitor*. You can also double-click the status icon in the System Tray.
2. Select **Preferences**.
3. In the General Settings, expand the **Encryption Key** section.
4. Click **Save** and select the desired location, such as a USB Thumb Drive.
5. Select **Print** to print the key.

Notes: Preserve the encryption key in a safe place that you can access in the event of any damage to your computer backing up with the ECHOplatform agent or any environmental disaster that may happen to your home or office.

If you lose your private encryption key, Barracuda is unable to recover your data because the key is encrypted on Barracuda servers.

When you choose the private key option, each account gets a unique private key. Do not assume the same key applies to all accounts.

Switching between Local and Online Procedure

From time to time, partners back up data to the cloud, or to a Local Vault, and later need to change the backup location from one to the other.

If the Local Vault backup has been done with the Local Only Backup option, perform the following steps to change the location of this backed up data.

1. Delete the data from the specified location by using the **Delete** tab in either the installed software or the web portal.
2. Delete the desired backup set.
3. Create a new backup set and specify Online/In Local vault or Local Only.

Backed up data must be deleted from the original location before being sent to a new destination because the file catalog (catalog.fdb) records when a file is backed up and retains the file in the original location.

Therefore, if you were to create a new backup set with a different destination without first deleting the backed-up data, only new files and changes to existing files would be written to your new destination. The original data would remain at the location where previously backed up.

Note: Perform the *Switching between Local and Online* procedure with the guidance of Barracuda Partner Support.

Keep Local Storage and Local Vault Protected from Crypto-type Viruses

It is good practice to create a backup user account that has access to Local Storage and Local Vault.

Do not give other user accounts permissions to these drives.

Glossary

The following table provides definitions for some of the terms used in this guide for cloud computing restore and backup functions.

Term	Definition
4k Sector	A 4k sector size rather than the traditional 512-byte sector used on legacy disk drives is larger and allows for higher capacity storage as well as the potential for improved performance.
Archive Rules	Controls the number of revisions stored, by removing unneeded revisions indicated in the rule. When the backup set is run, each rule is applied in the order listed within the set's revision rule list. The standard rules types are: • Disk Usage • Number of Revisions • Disk Usage • Date Range
Asynchronous	An attribute of a before and after action. If designated for a before action, the action starts at the start of a backup set but may not finish before the backup set begins. If designated for an after action, the backup set may not finish before the action is run.
Backup Set	A selected set of data and folders that are backed up when run, either manually, or automatically based on an associated schedule. Backup sets can include files and folders, VMware and Hyper-V virtual machines (VMs), an image of one or more physical drives, or SQL and Exchange data.
Checkpoint	A snapshot of a Hyper-V virtual machine. Differs from a VSS Snapshot.
Cloud Archive	Data that no longer needs to be accessed on a regular basis is maintained and backed up remotely by a cloud storage service provider.
Cloud Application	A software application that never is installed on a local machine and always accessed over the Internet.
Cloud Provider	A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations and/or individuals.
Computer ID	A unique four-digit code used to keep track of multiple subaccounts that are associated with a single main account. The first computer you install Online Backup Solution.com on has the computer ID 0000. Subsequent subaccounts have the next sequential computer ID of 0001, 0002, and so on.
Cluster	A group of hosts that are linked for providing high availability.
Differencing Disk	A virtual hard disk (VHD) that stores changes made to another VHD or to the guest operating system. The purpose of differencing disks is to maintain information about any changes made so changes can be reversed.
Differential Backup	A type of backup associated with SQL Server, for File and Folder backup sets. After the initial full backup is completed, a differential backup backups only data that has changed since the prior full backup.
FAT	File allocation table. A file system developed mostly for hard drives.

Term	Definition
File Catalog	A list of all of data, and revisions that are contained within backup set. The catalog is transmitted to the backup servers with every backup.
GPT	Globally unique identifier (GUID) partition table. A standard for the layout of the partition table on a physical hard disk using globally unique identifiers.
Hypervisor	A platform that allows multiple operating systems to run on a host computer at the same time.
Hyper-V	A Microsoft virtualization solution. Formerly known as Windows Server Virtualization, it can create virtual machines on x86-64 systems.
Hyper-V Manager	The primary GUI for Microsoft's Hyper-V through which virtual machines are managed.
Image-level (volume-level) Backup	A process that backs up an entire storage volume.
Incremental Backup	Backs up only the data changed since the last backup.
IntelliBlox	A proprietary technology that uploads only the changed blocks of a file. At your next backup, the data is scanned and any changes at the block level are detected; only these changes are uploaded.
Local Backup	Any backup where the storage medium is kept nearby.
Local Storage	The on-site destination for Image and Hyper-V Rapid Recovery backups. This location should be directly attached or network storage. The data stored for these backups in local storage is unencrypted and stored in reverse-incremental format.
Local Vault	Keeps a mirror copy of backup data stored on Barracuda and local servers.
MBR	Master boot record. The first sector on a hard drive occupied by code necessary to start the operating system startup process.
MSP	Managed Service Provider. Provides delivery and management of a variety of services that include but are not limited to network-based services (online backup), applications, and equipment.
NTFS	New technology file system. The standard file system of all supported Microsoft operating systems.
Object-level Recovery	A method of recovery that allows recovery of individual files and folders from an image backup. This option is available for Imaging and Hyper-V Rapid Recovery backups.
Quiescing	A process of bringing the data on a disk of a physical or virtual computer into a state suitable for backups.
Rapid Recovery	A recovery option for Hyper-V Rapid Recovery and Imaging that allows a VM to be created and/or run directly from the backup data in local storage. Because this option does not require a network copy it is very fast to complete, especially for the most recent revision of a protected machine.
Restore	The process of retrieving backed up data. You can restore your data to their original locations, or to a different folder.
Revision	The state of data at a particular point of time.
Revision Rules	See *Archive Rules*.

Term	Definition
Snapshot	A reproduction of the virtual machine as it was when you took the snapshot, including the state of the data on all the virtual machine’s disks and the virtual machine’s power state (on, off, or suspended).
Synchronous	An attribute of a Before and After action. If designated for a Before action, the action finishes before the backup set begins. If designated for an After action, the backup set finishes, before the action is run.
UNC	Uniform Naming Convention. Specifies a well-formed syntax to describe the location of a network resource, such as a shared file, directory, or printer.
vCenter Server	The management tool used to administer the various available servers in the enterprise. These servers can be ESXi, each tied to a physical server and able to host several virtual machines.
vCenter Server Database	A persistent storage area for maintaining the status of each virtual machine and user that is managed in the vCenter Server environment. Located on the same machine as vCenter Server.
vMotion	The live migration of VMs across hosts in a cluster without having to power them down.
Volume Shadow Copy	A copy of a volume (VHD/VHDX file) created by a VSS writer that enables files to be backed up even if they re-opened by another process.
VMware ESXi	VMware hypervisors that are installed on bare metal and run on the host computer.
VMware vSphere	The name of the VMware virtualization system.
VMware Virtual Machine Console	An interface that provides access to one or more virtual machines on the local host or on a remote host running vCenter Server.
VSS	Volume Shadow Copy Service. A Windows service for capturing and creating snapshots called shadow copies.
VSS Snapshot	See *Volume Shadow Copy*.