Barracuda

Solution Brief

Understanding Data Verification and Disaster Recovery Using Barracuda Cloud LiveBoot Recovery

The amount of time it takes to get your organization up and running after a disaster is the key difference between backup and disaster recovery. Restoring terabytes worth of your organization's backups can take days, possibly even weeks without a disaster recovery procedure. With documented processes and disaster recovery preparedness, you could reduce this time to a few hours or maybe even minutes. The problem is that disaster recovery testing can be quite expensive. Smaller organizations often do not have the resources to properly test their backups, or afford redundant hardware or disaster recovery services. Backup is only one phase of your overall disaster recovery strategy. And, unfortunately, traditional backups have the potential to fail. A study done by National Archives & Records Administration in Washington concluded that "93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster."[1] Without proper testing of your backup set, results can be devastating for your organization should a disaster occur.

Barracuda Backup with VMware vSphere integration protects your entire VMware environment at the host level, while replication to the Barracuda Cloud ensures that your data is stored safely offsite in the event of a disaster. Add Barracuda Cloud LiveBoot Recovery, which can provide disaster recovery, data verification, and a virtual testing environment, and you have a complete, all-in-one solution for your backup and disaster recovery needs.

According to Gartner and Storage magazine, "Companies using antiquated backup methods (such as tapes) found that in over 77% of cases, the data exhibited discrepancies or failures that could not be fixed, rendering the backup useless." Additionally 34% companies protecting their data to tape do not test their backups.[2] Some data protection companies make data verification an optional feature by offering add-on solutions that increase cost or increase backup windows through a resource intensive verification process. Post-process data verification solutions add additional risk in the event of a disaster. They further hamper your recovery time and recovery point objectives, by increasing the time to disaster recovery readiness. A common, often optional, legacy verification process is to generate checksums for all data written to tape or disk, and then read the data from the tape or disks and compare the checksums to verify the integrity of the data and media. This multi-process verification procedure can degrade backup performance, as shown in Figure 1.

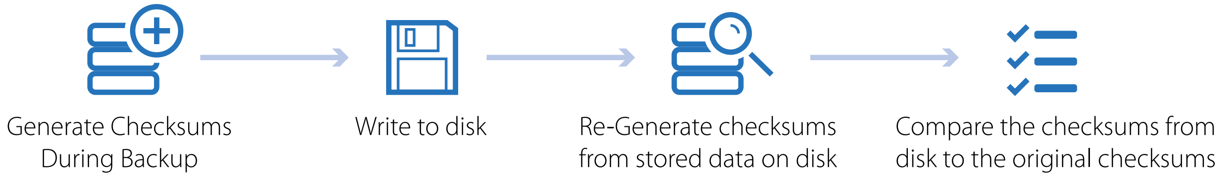
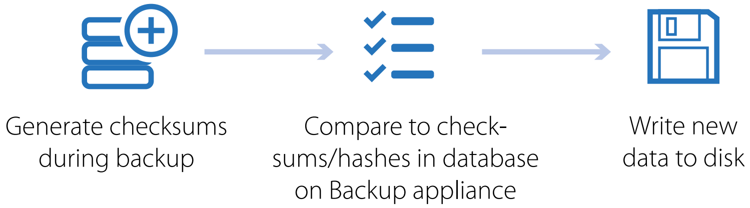

Generate Checksums During Backup
Write to disk
Re-Generate checksums from stored data on disk
Compare the checksums from disk to the original checksums

Figure 1

[1] National Archives & Records Administration in Washington
[2] Boston Computing Network Data Loss Statistics

Barracuda Backup contains built-in inline data verification that performs checks multiple times throughout the backup and replication process to ensure that data is never corrupted or missing. Each block of data is assigned a unique hash (digital fingerprint) using MD5 and SHA1 checksums. Each hash is stored in a database on the local appliance. As the backup process runs, each calculated hash value is compared to the values of blocks that are already processed. If the value is unique, the block is stored on the appliance. For duplicate hash values, only a small pointer is sent to the appliance. This ensures that data is already deduplicated when it is written to disk and that the integrity of the data has been verified. If an inconsistent or corrupted block is found during the backup, the job fails and you are notified in the backup report. The same method is used again when replicating to another Barracuda Backup appliance or Barracuda Cloud storage. Each hash is stored in a queue to be sent offsite. When the hash is sent, it is compared to what is already stored in the cloud. If a discrepancy occurs during the replication process, the block of data fails, and a new part is queued and replicated as shown in figure 2.


Generate checksums during backup

Compare to check-sums/hashes in database on Backup appliance

Write new data to disk

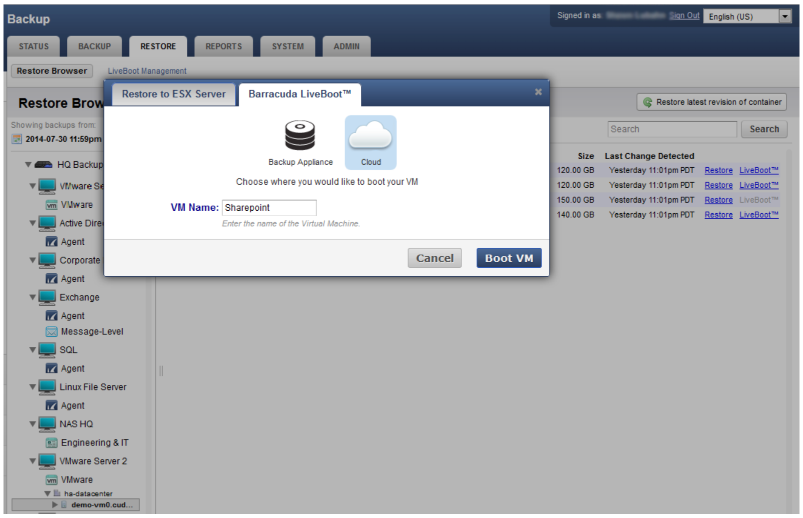
Figure 2

Even with the Barracuda Backup's built-in backup verification technology, performing your own disaster recovery testing and data verification is still a recommended best practice. You can achieve several goals through disaster recovery testing and planning:

- Minimize recovery time objective
- Guarantee reliability of standby systems
- Create a standard for testing
- Minimize decision-making during a disaster
- Reduce potential legal liabilities
- Provide a sense of security

Many organizations are forced to implement a piecemeal solution that uses many different vendors to meet these goals. Backup software, storage for backups, disaster recovery services, and redundant hardware for testing are often segregated from one another—creating a complex, multi-vendor environment. These environments create a cost structure that can be quite expensive as well as difficult to support.

In addition to providing renowned enterprise cloud storage for disaster recovery, Barracuda provides Cloud LiveBoot Recovery, an industry-first solution that brings enterprise grade technology to the mid-market. Barracuda Backup with Cloud LiveBoot Recovery provides an easy-to-use, all-in-one solution for backup and disaster recovery. You can boot a VMware virtual machine in the Barracuda Cloud with only a few clicks of the mouse, as shown in Figure 3. Barracuda stores the virtual machine configurations, so that when the virtual machine is booted in the Barracuda Cloud, the hardware configuration is the same as the original at the time of backup. You can choose to assign a public IP address to the virtual machine so that the machine is accessible externally and has Internet access. After you boot and assign a public IP address to a machine, you can retrieve files and directories on that machine and make them available to others. You can install and configure VPN software to let clients connect to the virtual machine. With Copy, a Barracuda file sync and share solution, you can easily make copies of your files and directories accessible to employees from anywhere over the Internet. When files are modified, the revisions are stored in the Barracuda Cloud where they can be downloaded back to your production environment when it is restored.



Choose where you would like to boot your VM

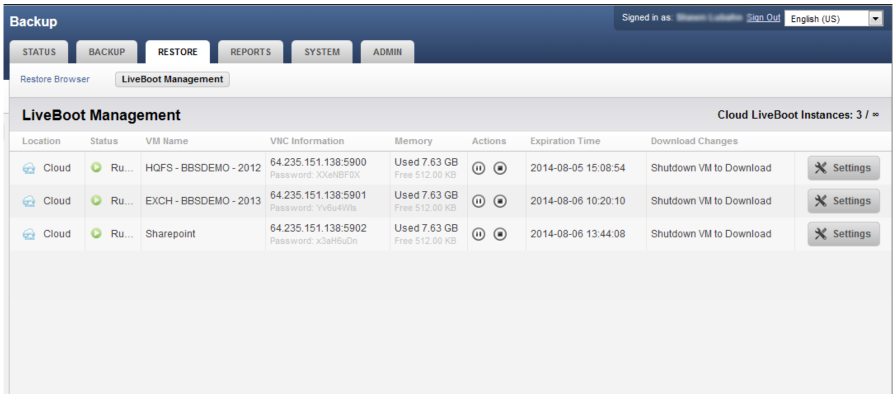
VM Name: Sharepoint

Enter the name of the Virtual Machine.

Size	Last Change Detected		
120.00 GB	Yesterday 11:01pm PDT	Restore	LiveBoot™
120.00 GB	Yesterday 11:01pm PDT	Restore	LiveBoot™
150.00 GB	Yesterday 11:01pm PDT	Restore	LiveBoot™
140.00 GB	Yesterday 11:01pm PDT	Restore	LiveBoot™

Figure 3: LiveBoot to the cloud

Barracuda Cloud LiveBoot provides you with the virtual hardware to perform disaster recovery and backup data testing without any extra fees, hardware costs, or third-party vendors. Barracuda Cloud LiveBoot also lets you prepare for disaster and get the best plan in place without affecting your production environment or having to perform complex restores that require time and resources. It takes just minutes to boot a virtual machine in the Barracuda Cloud. Doing this periodically, you can verify the state of your backups. Connect to your machines securely with a VNC client, while using a unique IP address and password that are provided by Barracuda, to verify that your files and applications are backed up and functioning properly. There are no restrictions on how many times you can LiveBoot a machine and no interaction from Barracuda is necessary.



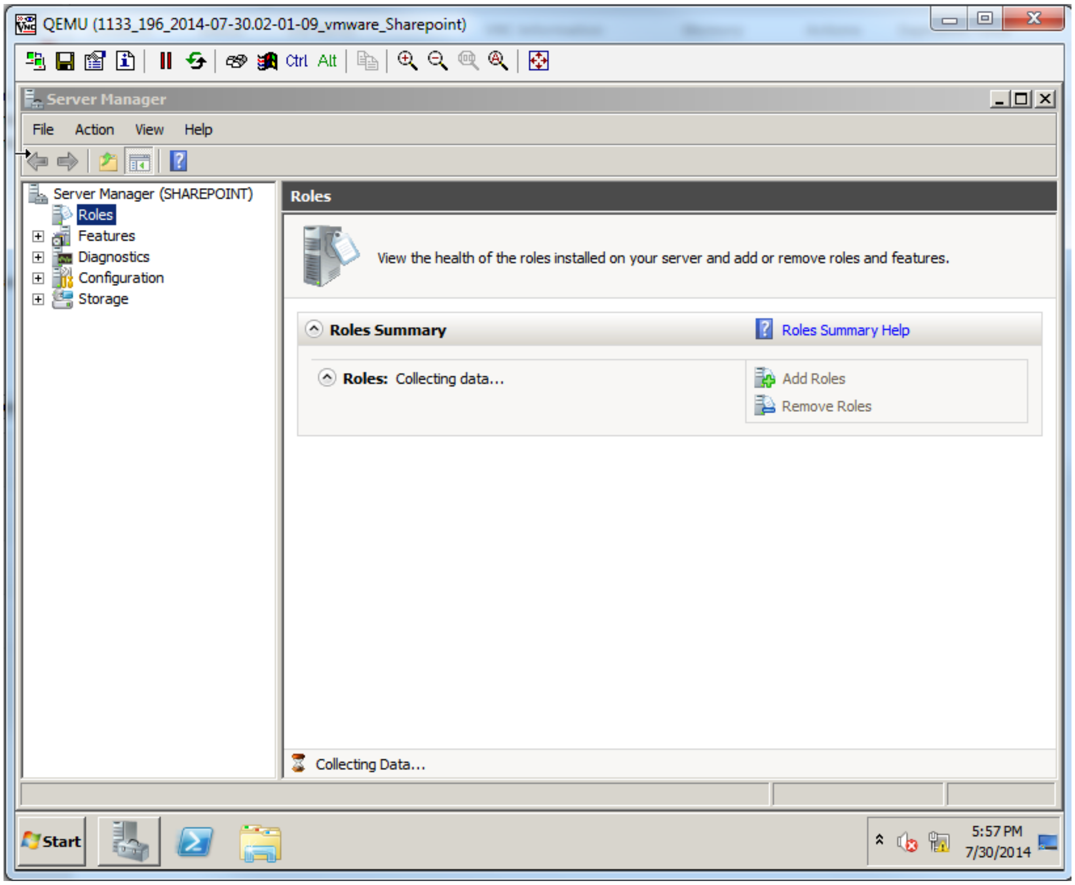
LiveBoot Management

Cloud LiveBoot Instances: 3 / ∞

Location	Status	VM Name	VNC Information	Memory	Actions	Expiration Time	Download Changes	
Cloud	Ru...	HQFS - BBSDEMO - 2012	64.235.151.138:5900 Password: XXeNBF0X	Used 7.63 GB Free 512.00 KB	⏸ ⏹	2014-08-05 15:08:54	Shutdown VM to Download	Settings
Cloud	Ru...	EXCH - BBSDEMO - 2013	64.235.151.138:5901 Password: Yv6u4Wls	Used 7.63 GB Free 512.00 KB	⏸ ⏹	2014-08-06 10:20:10	Shutdown VM to Download	Settings
Cloud	Ru...	Sharepoint	64.235.151.138:5902 Password: x3aH6uDn	Used 7.63 GB Free 512.00 KB	⏸ ⏹	2014-08-06 13:44:08	Shutdown VM to Download	Settings

Figure 4: Connect to and manage your virtual machines

Another important benefit of Barracuda Cloud LiveBoot is aiding business continuity through sandbox testing. Patching your operating systems and applications can be extremely risky without knowing the effects on your environment. By using Barracuda Cloud LiveBoot, you put a copy of your virtual machine in a safe, non-production environment. If a patch or upgrade causes a failure, you can power off the machine and start over. By booting several machines at once, on the same VLAN, you can re-create your own private network in the cloud.



View the health of the roles installed on your server and add or remove roles and features.

Roles: Collecting data...

Collecting Data...

Figure 5: Use a VNC utility to access your virtual machine

Barracuda Backup with Cloud LiveBoot offers organizations multiple layers of backup verification, while providing an affordable and easy-to-use solution. Backup times are reduced with Barracuda's advanced part verification, which executes while new data reaches the Barracuda Backup.

Conclusion

You can rest easier, knowing that your organization will stay up and running if a disaster occurs. Implementing Barracuda's comprehensive solutions for disaster recovery and data verification, powered by Cloud LiveBoot, safeguards your data across all fronts, whether your data is stored on-premises or off. This first of its kind, all-in-one, integrated solution, is easy to use, and is always performing to safeguard your data. Gain best-of-breed solutions to ensure that your data is always backed up, no matter what tomorrow may bring.

Find out more