Barracuda

Solution Brief
Understanding Offsite Vaulting

Introduction

The offsite vaulting feature of Barracuda Backup enables customers to archive up to 12 monthly and 7 yearly historical revisions to a supported offsite destination, while deleting unneeded portions of these revisions from the local appliance. This allows organizations to meet compliance objectives by retaining data for longer periods of time, while freeing up some amount of disk space to protect operational data. Supported data types include all file data, VMware vSphere and Microsoft Hyper-V virtual machines, and Microsoft Exchange and SQL Server application data.

When to Use Offsite Vaulting

Before enabling offsite vaulting, it is important to understand the use case where this feature works best. Think of offsite vaulting as a similar offering to Amazon's Glacier service, or an offsite tape service, where data is considered archived, and therefore quick recovery times are not expected. Recovery time of offsite-vaulted data will be longer because parts or all of this data will only be available off-site. To recover this data, it must first be transferred back to the local Barracuda Backup device.

Operational data, or data that needs to be recovered quickly and/or frequently, should never be offsite vaulted. Only data that needs to be kept for long periods of time to meet organizational or compliance objectives, and where recovery time is not a priority, is a candidate for this feature. The expectation for recovery time of offsite-vaulted data should be in hours or days instead of minutes, and it is largely based on the amount of data and available bandwidth between the local backup device and the offsite destination.

Data that has been offsite vaulted will be visible in the Restore Browser and will appear the same way as data that has not been offsite vaulted. Initiating a restore of offsite-vaulted data works the same way as data stored locally, but will take an extended period of time to recover as mentioned above.

How Offsite Vaulting Works

To understand how the offsite vaulting feature works, it is important to have a basic understanding of Barracuda's deduplication methodology. Barracuda Backup deduplicates data globally, across all data sources that have been backed up. To achieve deduplication, all files and other backed-up data is broken down into "chunks" or blocks of data as it is ingested into the local backup device. Redundant data blocks are replaced with a pointer to the unique data block.

When a restore is initiated, Barracuda uses the pointers to reassemble the data with the unique data blocks that were written to disk on the Barracuda Backup device. Data retention works in a similar manner, as the pointers tell Barracuda which unique data blocks are required to rebuild each recovery point.

By enabling offsite vaulting, only the unique data blocks that are no longer required to be on the local appliance to rebuild data that has not been vaulted are removed from the local Barracuda Backup device and kept offsite. Since data is deduplicated globally across all data sources, and most of the data will be kept locally to rebuild daily or weekly historical revisions, the number of unique data blocks that will be removed by offsite vaulting is usually low. Customers may experience the most benefit from offsite vaulting when the source data is frequently changing between backups. A high change rate creates a greater disparity between the data needed to rebuild a monthly or yearly historical revision and a more current revision, and, in turn, increases the number of unique data blocks that may be eligible for offsite vaulting.

The following image shows how data is deduplicated and replicated offsite. Without offsite vaulting, the retention of data is the same for the data stored both locally and at the offsite destination.
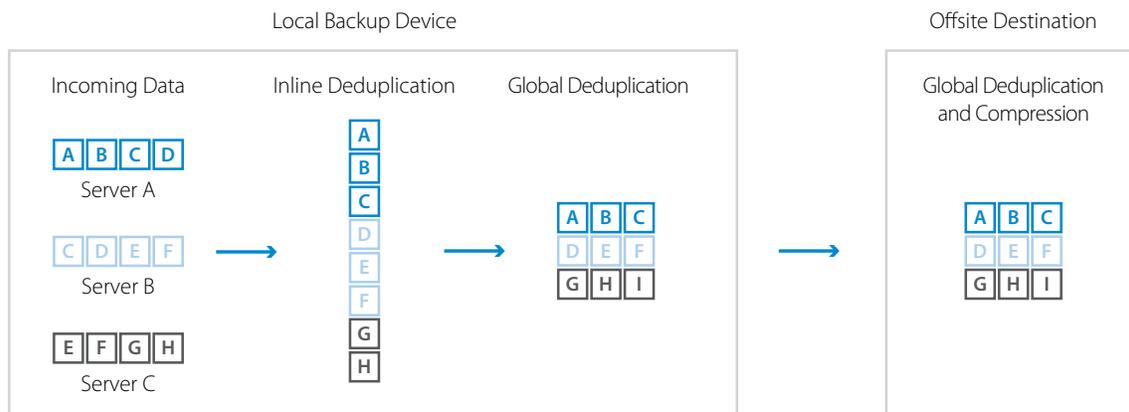

Figure 1: Local backup, deduplication, and offsite replication

The next image shows what happens to the same dataset when the Offsite Vaulting feature is enabled. Only the blocks that are part of the monthly or yearly historical revision that are no longer needed on-premises for other datasets are removed from the local backup device.
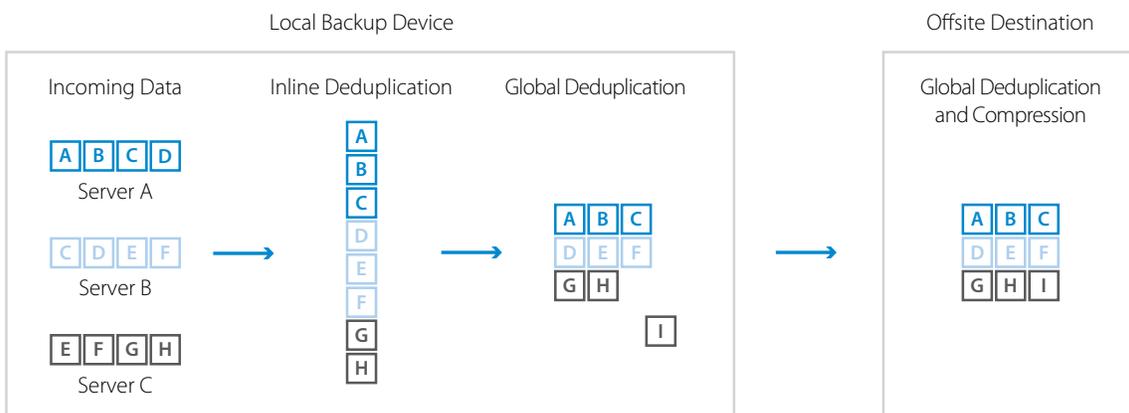

Figure 2: The removal of unique data blocks locally due to offsite vaulting

Configuring Offsite Vaulting

Offsite vaulting only applies to data that has been replicated offsite. If you are already replicating data offsite and you enable offsite vaulting, the data chunks to which offsite vaulting applies are purged from the local Barracuda Backup device; No data is transferred since it is already present in the offsite destination. If you are not replicating data offsite and you enable offsite vaulting, the data will not be purged from the local Barracuda Backup device. Once replication has been enabled and the data has been successfully transferred offsite, the offsite-vaulted data will be purged from the local Barracuda Backup device. Please be advised that the purging of offsite-vaulted data from the local device may take between 24 and 72 hours.

Note: Once offsite vaulting is enabled, it cannot be undone. If the feature is disabled, offsite vaulting of data will stop. However, the local Barracuda Backup device will not be repopulated with the data that has already been vaulted. Please ensure that you have read the sections above and fully understand how offsite vaulting works and how best to use it.

To configure offsite vaulting, follow the steps below.

1. Log in to Barracuda Cloud Control, then select your Barracuda Backup device.
2. Navigate to the Backup > Retention Policies page.
3. Create a new retention policy or edit an existing policy.
4. Choose or verify the data sources that the retention policy will apply to.
5. In the retention timeline section, specify how long the all (hourly), daily, weekly, monthly, and yearly historical revisions will need to be kept.
6. If monthly revisions do not exceed 12 months and yearly revisions do not exceed 7 years, check the "offsite only" boxes.

Note: If monthly revisions exceed 12 months and/or yearly revisions exceed 7 years, and offsite vaulting is enabled, you will be unable to successfully save the retention policy.

Figure 3: Configuring offsite vaulting

7. Click Save to apply your changes.

Summary

The offsite vaulting feature for Barracuda Backup can be a useful tool for retaining long-term archival data while reclaiming some amount of disk space on the Barracuda Backup appliance. Before enabling this feature, please make sure you understand the implications to data recoverability