
Offsite Vaulting

<https://campus.barracuda.com/doc/78157276/>

Barracuda Backup offsite vaulting 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

The Barracuda Backup offsite vaulting feature is 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, verify you understand the implications to data recoverability. Additionally, 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 is longer because parts or all of this data is only available offsite. 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. Offsite vaulted data recovery time expectations should be in hours or days rather than minutes, and it is largely based on the amount of data and available bandwidth between the local Barracuda Backup device and the offsite destination.

Data that has been offsite vaulted is visible in the Restore Browser and appears 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 takes an extended period of time to recover, as noted 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 backed up data sources. To achieve deduplication, all files and other backed-up data are broken down into chunks or blocks of data as it is ingested into the local Barracuda 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 not 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 is kept locally to rebuild daily or weekly historical revisions, the number of unique data blocks to 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.

Figure 1 illustrates 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. Data is Deduplicated and Replicated Offsite.

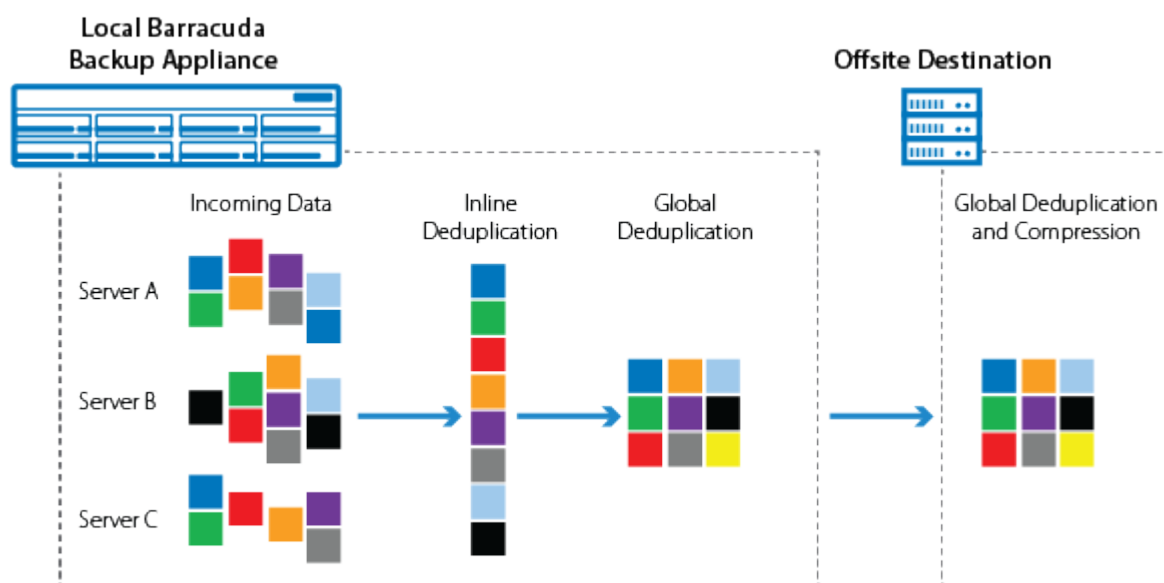
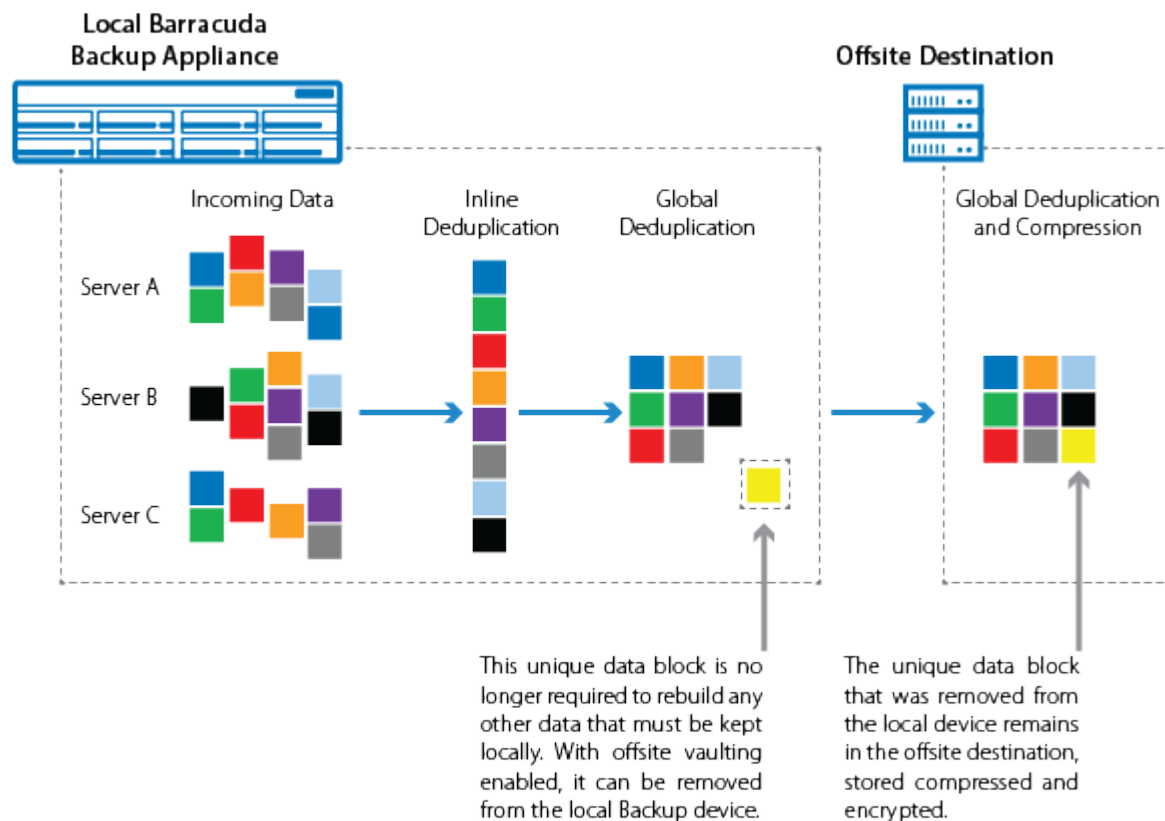


Figure 2 illustrates what happens to the same dataset when offsite vaulting is enabled. Only the blocks that are part of the monthly or yearly historical revision that are no longer needed on-premises for other datasets are removed from the local Barracuda Backup device.

Figure 2. Unique Data Blocks Removed Locally Due to Offsite Vaulting.



Configure Offsite Vaulting

Offsite vaulting only applies to data 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 is not purged from the local Barracuda Backup device. Once replication is enabled and the data is successfully transferred offsite, the offsite vaulted data is purged from the local Barracuda Backup device. Note that purging of offsite vaulted data from the local device may take between 24 and 72 hours.

Important

For VMware vSphere and Microsoft Hyper-V virtual machines, LiveBrowse (granular file recovery) and LiveBoot does not support historical backup revisions that have been offsite vaulted. Since the virtual machines no longer exist on the local Barracuda Backup device, they are unable to be mounted for granular recovery. If granular recovery is a requirement for older VMware and Hyper-V virtual machine revisions, Barracuda Networks recommends not configuring offsite vaulting for this data.

Once offsite vaulting is enabled, it cannot be undone. If the retention policy with offsite vaulting

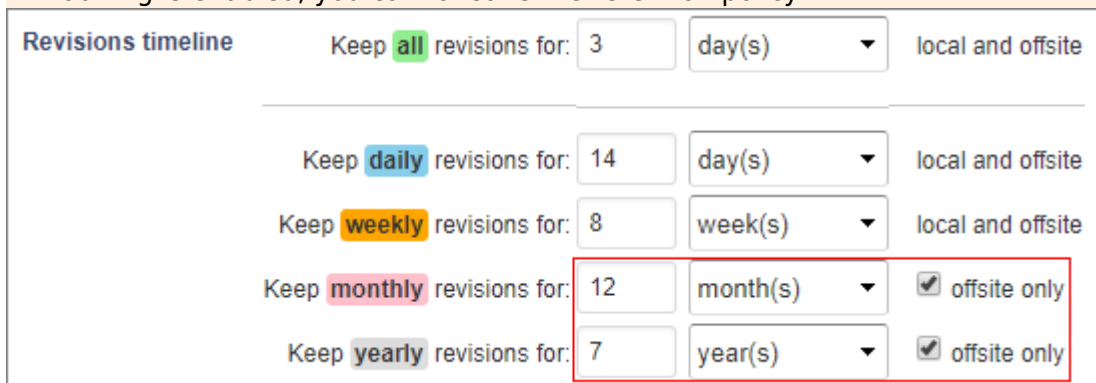
enabled is deleted for modified, the local Barracuda Backup device is not repopulated with the data that has already been vaulted.

Ensure that you have read the sections above and fully understand how offsite vaulting works and how best to use it.

Use the following steps to configure offsite vaulting:

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup appliance in the left pane.
2. Go to the **Backup > Retention Policies** page.
3. Click **Add a Retention Policy** to create a new retention policy, or click **Edit** to the right of an existing retention policy.
4. In the **Items to Retain** section, choose or verify the data sources to which the retention policy applies.
5. In the **Retention Timeline** section, specify how long the **all** (hourly), **daily**, **weekly**, **monthly**, and **yearly** historical revisions need to be kept.
6. If **monthly** revisions do not exceed 12 months, and **yearly** revisions do not exceed 7 years, select **offsite only**:

If monthly revisions exceed 12 months and/or yearly revisions exceed 7 years, and offsite vaulting is enabled, you cannot save the retention policy.



Revisions timeline	Keep	all	revisions for:			
		all	revisions for:	3	day(s)	local and offsite
		daily	revisions for:	14	day(s)	local and offsite
		weekly	revisions for:	8	week(s)	local and offsite
		monthly	revisions for:	12	month(s)	<input checked="" type="checkbox"/> offsite only
		yearly	revisions for:	7	year(s)	<input checked="" type="checkbox"/> offsite only

7. Click **Save** to apply your changes.

Figures

1. OffsiteVaultingDeduplication.png
2. RemoveUniqueDataBlock.png
3. RevisionTimeline.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.