Best Practices for Managing Storage Capacity

https://campus.barracuda.com/doc/96771692/

Article Highlights:

- Running out of disk space on your Barracuda Backup appliance can put your organization's data at risk.
- Barracuda Backup provides several methods for reducing the amount of storage on your appliance.
- Barracuda Professional Services can perform a health check of all appliances on your account, make configuration recommendations, and ensure that your backup appliances are properly sized for your environment.

Barracuda Backup has a number of appliance models to fit most environments, most often sized by the amount of raw data needing protection in an environment and the amount of backup data storage. For a variety of reasons, backup storage grows to a point where storage space on an appliance becomes limited or fills the capacity of the appliance altogether. While running out of available storage can be problematic, there are options to help reduce the amount of backup storage, while extending the life of your Barracuda Backup appliance.

Before getting into some of the ways to reduce backup storage, it is important to understand the risks associated with filling an appliance to capacity.

Running Out of Storage Capacity

When a Barracuda Backup appliance completely runs out of disk space, a number of core services can fail. Backups will fail instantly as there is not enough space to store the new data. In some cases, offsite replication, data purging, and some recovery operations will fail due to the limited amount of disk space.

When a Barracuda Backup appliance reaches 80% of capacity, an email notification is sent out to subscribed recipients. The appliance health status in the cloud user interface and dashboards will also show a yellow warning light and/or icon. When capacity reaches 90%, the alerts become more critical and the health indicators turn red.

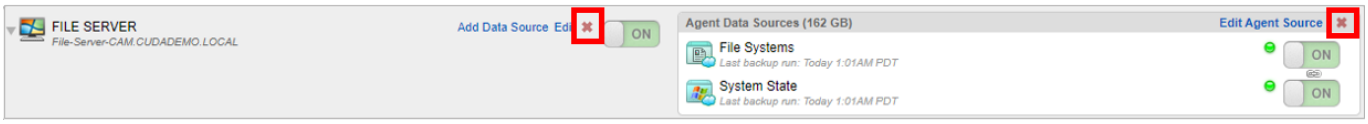
To avoid a lapse in backup functionality, it is critical to act as soon as possible when receiving these alerts. Here are some best practices for reducing the amount of storage on your Barracuda Backup appliance.

Revisiting the Backup Strategy and Configuration

The recommended method for reducing the amount of backup storage is to revisit or rethink the backup strategy and configuration altogether. In some cases, backups were configured long ago or by someone else within the organization. To help assess the current strategy or to build a new one, here are some questions to consider:

What data sources are backed up and do we still need these data sources backed up?

You may find that there are data sources that no longer need to be backed up or have been disabled and no longer need to be kept. To remove data sources from the **Backup -> Sources** page, click the red **X** for that server/source. Note that deleting a source will purge all data associated with it.



Do we have the right backup approach?

There are several ways to protect data in Barracuda Backup. VMware vSphere and Microsoft Hyper-V virtual machines can be protected without the use of a backup agent. This type of backup takes an image of the virtual machine and its disks and is ideal for full system recovery. The Barracuda Backup Agent protects file-level data. The agent can be installed on any physical or virtual Windows, Linux, or MacOS system. The agent backups are ideal for backing up the contents (files, directories, databases) within a system and performing granular recovery.

When deciding which approach to take, it is best to think about the type of recovery that typically needs to be performed. For virtual machines where you need to recover the entire system quickly and granular recovery is not likely, the agentless backup approach can work best. For virtual machines where granular recovery is frequent, like with a file server, the agent backup can work best. You could also take a hybrid approach for this type of system and data by using the agent to back up the file share(s) and scheduling a daily or weekly virtual/image backup in case of a full system failure or disaster.

For more information, see the following articles:

- How Backup Works
- Best Practices for VMware
- Best Practices for Microsoft Hyper-V
- Best Practices for Microsoft Exchange
- Best Practices for Microsoft SQL Server

How frequently is data backed up?

Typically, the more frequently data is backed up, the more backup revisions are created and more storage is consumed. There are no limits to the number of backup schedules that can be configured. You have the flexibility to configure a backup schedule for each data source that provides the desired recovery point objective (RPO).

To learn more about backup scheduling in Barracuda Backup, see Backup Scheduling.

Do I have retention policies configured for each of my data sources and do they fit the organization's needs?

In Barracuda Backup, if a data source does not have a defined retention policy, all backup data will be kept indefinitely. When viewing the **Backup -> Retention Policies** page, there will be a warning message at the top if a data source has no defined retention policy or is included in multiple policies.

Like backup schedules, there are no limits to the number of retention policies that can be configured. For organizations with a defined data retention policy, we recommend following that when configuring retention policies within Barracuda Backup.

For organizations without a defined data retention policy, it is helpful to anticipate the various recovery scenarios you might need to protect against for each data source. You might need to retain data on a file server for a longer period if users do not discover missing items for periods of time. For other types of systems or data where recovery from long ago revisions do not make sense, you can configure a shorter retention policy to protect against system failures or disasters where recovery is typically done on the most recent backup copy.

To learn more about how retention policies work in Barracuda Backup, see Data Retention.

> Need assistance? Barracuda Professional Services can ensure that your Barracuda Backup solution is properly deployed and configured, help you with firmware or hardware upgrades, and review your environment to identify any recommended changes.

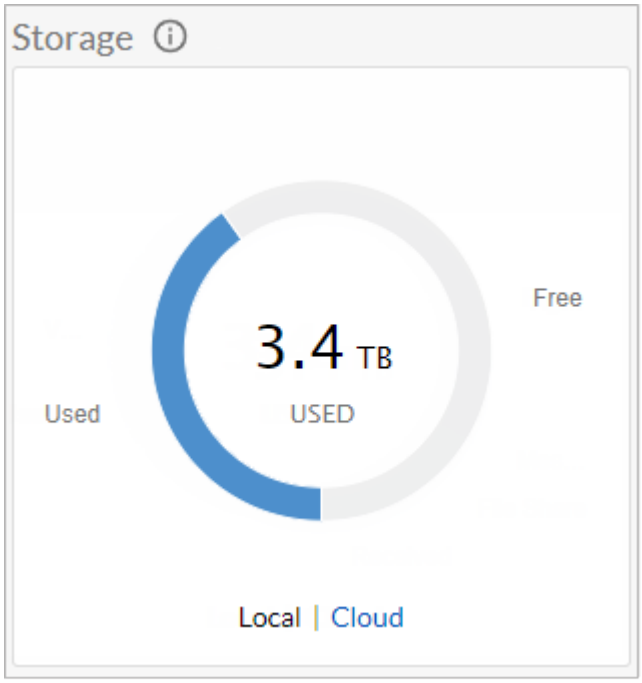
Understanding Storage Consumption

Prior to making any changes to your backup configuration, you need to understand what is consuming the most backup storage on your Barracuda Backup appliance.

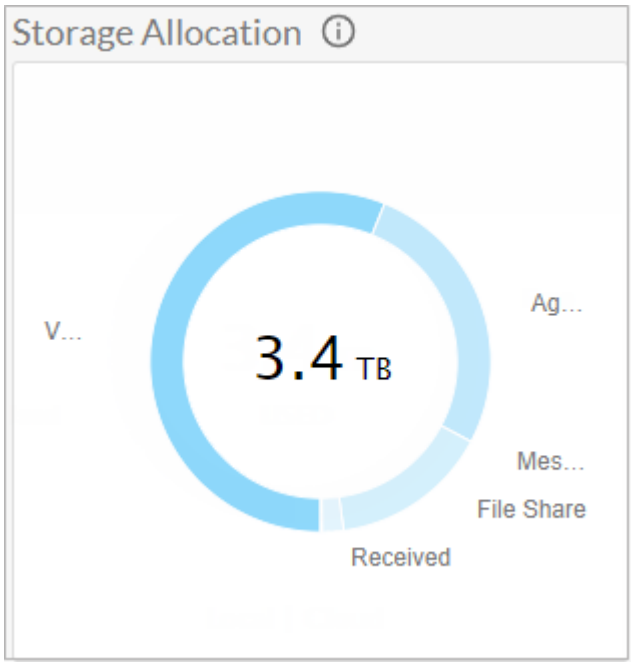
Backup Storage Dashboard

From the **Dashboard**, the **Storage** graph shows the used and free amounts of storage on your

Barracuda Backup appliance.



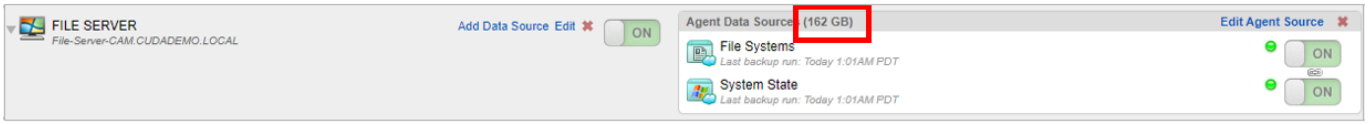
The **Storage Allocation** graph shows the types of backup storage: Agent, VMware, File Share, and Exchange Message-Level.



Sources

From the **Backup -> Sources** page, you can see how large the source was as of the last backup. This

number does not represent the total amount of backup storage for the source.



Large Items

From the **Reports -> Large Items** page, generate a list of the largest items backed up and stored on your appliance. The report shows the backup storage items sorted from largest to smallest and the number of revisions retained.

To learn more about the Large Items report in Barracuda Backup, see Large Items Reports.

Backup Reports

From the **Reports -> Backup** page, view the size of each backup. While this is not the actual amount of data stored on the appliance, it will help show which sources or backup schedules are backing up the most data.

Advanced Backup Storage Usage

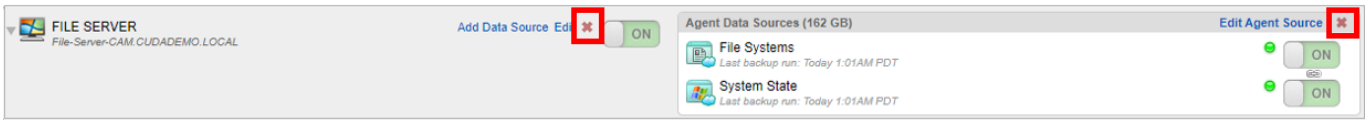
View the report with details on the amount of storage consumed by each data source on the Barracuda Backup appliance. **Note** that this feature is not yet available in the product interface. Currently, the report can be obtained by contacting Barracuda Networks Technical Support and requesting the Barracuda Backup storage usage report.

Reducing Backup Storage

There are several options available to reduce the amount of backup data stored on your Barracuda Backup appliance.

Delete Data Source(s)

To remove data sources from the **Backup -> Sources** page, click the red **X** for that server/source. Deleting a source will purge all data associated with it.



Reduce Retention

From the **Backup -> Retention Policies** page, edit the retention policy and reduce the length of time data is stored.

Remove Schedules or Modify Data Selected in the Schedule

From the **Backup -> Schedules** page, edit or remove the backup schedule. When removing the backup schedule, you will be prompted to retain the data per the configured retention policy or purge the data immediately.

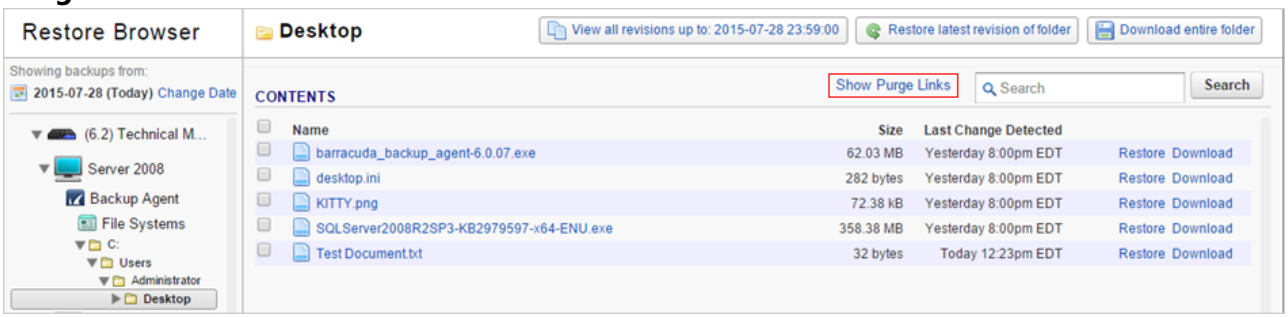
You can edit the schedule and choose to deselect data that was previously selected for backup. To save the schedule, you will be prompted to retain the data per the configured retention policy or purge the data immediately.

On-Demand Purging

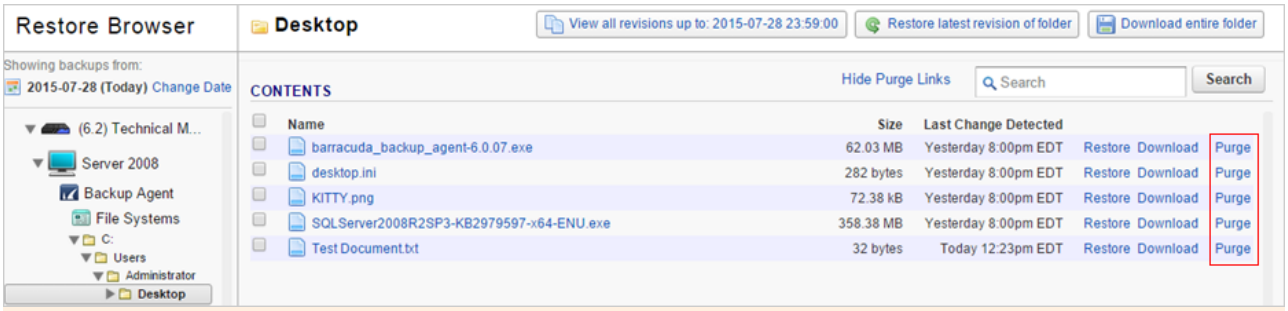
The purging of individual objects (VMs, files, directories) can be done from the **Large Items** report and the **Restore Browser**. To manually purge an item from the Restore Browser:

1. Log into Barracuda Backup at login.barracuda.com.
2. Go to **Restore > Restore Browser**.
3. In the Restore Browser, select the source from which you want to manually purge a file:

4. Drill down into the source until you reach the location of the desired file, and then click **Show Purge Links**:

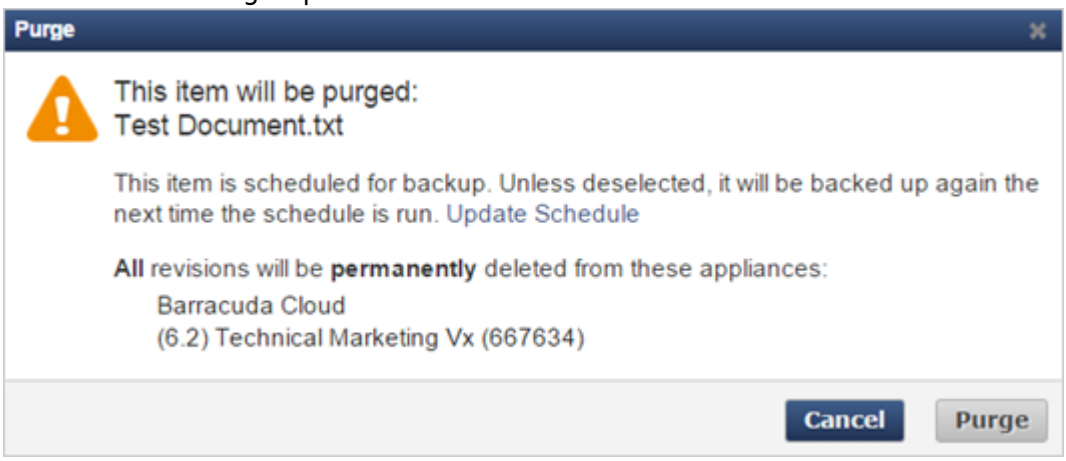


5. The **Purge** links display next to the files:

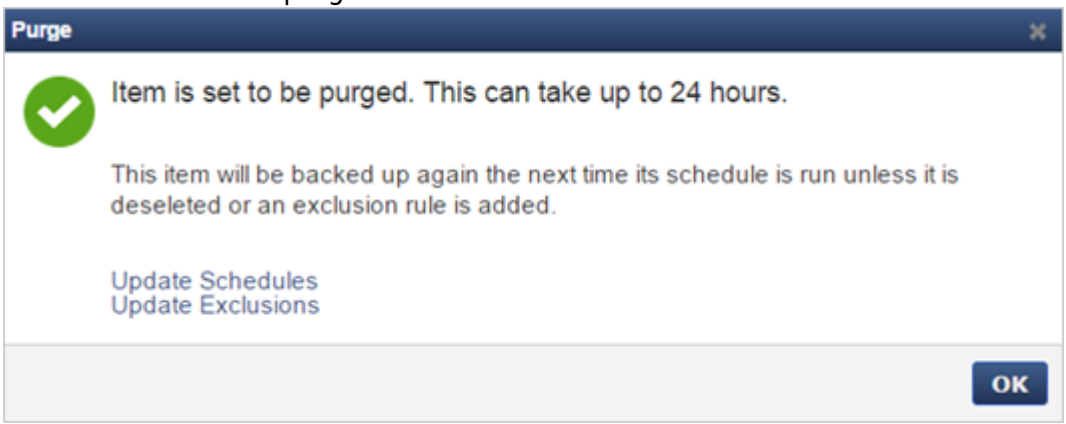


When you click Purge, an item and all of its historical revisions are purged from Barracuda Backup.

6. Click **Purge** next to the file you wish to remove from Barracuda Backup. Click **Purge** in the confirmation dialog to proceed:



7. The item is set to be purged:



8. Click **OK** to close the confirmation window.

Note that purging data does not remove the data source from Barracuda Backup . If you no longer want to back up data for a particular server, go to the **Backup > Source** page, and click the **Delete** icon for that particular server:

Once the data source is deleted, you can purge the files from Barracuda Backup. If you do not delete the data source, items will display in the **Large Items** report.

Offsite Vaulting

Offsite vaulting is a feature in Barracuda Backup that enables customers to archive data up to 12 monthly and 7 yearly historical revisions to a supported offsite destination while also deleting portions of these revisions no longer needed from the local appliance. This allows organizations to meet compliance objectives by retaining data for longer periods of time while freeing up 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.

Operational data that needs to be recovered quickly and/or frequently should never be vaulted offsite. 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.

To learn more about the offsite vaulting feature in Barracuda Backup, see Offsite Vaulting.

Conclusion

As data continues to grow over time and all attempts to reduce the amount of backup storage have been exhausted, it is beneficial to consider upgrading to a larger Barracuda Backup appliance with more backup storage capacity to fit your organization's needs. Barracuda Backup has 11 different appliance models with usable backup storage capacity from 1TB up to 112TB.

To learn more about the Barracuda Backup appliance models, see Barracuda Backup Appliance Hardware Specifications.

To upgrade to a larger Barracuda Backup appliance model, contact your Barracuda Networks sales representative, Barracuda Networks partner, or send an email to LeadDevelopment_Team@barracuda.com.

Figures