

Backup Daemon

<https://campus.barracuda.com/doc/98210928/>

The Backup Daemon is a new feature that adds to the existing options for creating and restoring backups for and from stand-alone and managed firewalls. Unlike backups stored in PAR files at a user's request, the backup daemon can be configured to operate autonomously at a scheduled time without any further interference. The backup daemon operates on the box level of an unmanaged box, a CC-managed box, and a Control Center, and must always be configured on the box level.

The backup daemon can create backups of the firewall configurations on the box level, on the CC level, and on the box & CC levels.

Creating Backup Storages and Backups

Local and Remote Storage

After enabling the backup daemon, you must register a certain type of storage that is identified by a unique ID. The back-end storage can be one of three types:

- Local Storage: Local back end in the file system of the firewall
- Remote Storage: An AWS S3 bucket
- Remote Storage: An Azure blob

Although the size of local storage is limited by the size of the firewall's internal hard disk/SSD, remote cloud storage is limited only by the licensing model you chose. However, if local control, availability, and speed are paramount to you, operating local storage can be the better choice.

Connecting to storage is provided by configuring a 'path' that lets the backup daemon send data to the configured storage. The format for the 'path' depends on the type of storage you chose:

- Local storage: /myPath
Example: /myLocalStorage
- AWS S3 bucket: server:port/bucket_name
Example: https://s3.amazonaws.com/bucket-backups
- Azure blob: container_name:/path
Example: containerbackup:/folder-backups

For more information on how to use cloud storage, see the user guides of the corresponding cloud provider and search for methods for accessing a bucket/blob.

Backup Encryption, Authorization, and Backup Jobs

Every back-end storage requires information for permitting a specific user to write to its file system. Also, the backup daemon requires information on whether to encrypt the data before backing it up. Encryption, however, is not mandatory. For accessing the back-end storage, you can select to either use an explicit password or to use your firewall credentials. If you configure the second password, it will be used to encrypt the backup. After entering the URL for the back end, you can add one or multiple backup jobs by configuring repeating trigger events.

A backup job is identified by a unique ID that relates exclusively to the firewall it is created on. The backup job can be configured to compress the data before sending it to the storage. You must create an execution trigger, which is the time to start the backup, supplied in Unix-like cronjob format. This cronjob format requires you to enter the time in the following template: 'Minute - Hour - Day of Month - Month - Day of the Week'.

Note: The minimal supported interval is daily!

The following table shows some examples of different possible entries:

| Minute | Hour | Day of the Month | Month | Day of the Week | Meaning |
|--------|------|------------------|-------|-----------------|--|
| 0 | 0 | * | * | * | Daily 00:00 |
| 20,40 | 3 | * | * | 5-6 | Every Friday and Saturday, always at 03:20 (AM) and 03:40 (AM). Note: using 7 as Sunday on the Campus page is non-standard and not supported by us. |
| 0 | 23 | */2 | * | * | Every second day at 23:00 |
| 20, 40 | 3 | * | * | 6-7 | Every Saturday and Sunday, always at 03:20 (AM) and 03:40 (AM) |
| 0 | 18 | 31 | 12 | * | Every 31st of December at 18:00 |
| 30 | 23 | 1,28 | */2 | * | On the first and 28th of every second month at 23:30 |

Backup Retention, Backup Removal

If you are configuring backup jobs that are executed on a regular basis, you must be aware that the increasing number of backups will also increase the amount of consumed space on your configured storage!

IMPORTANT


When selecting the option 'Local' for creating the back-end storage on your firewall or Control Center, you must consider that the total amount of consumed storage space can quickly grow to several gigabytes. This applies especially to Control Centers when configuring repeated







backups of 'Box and CC' configuration trees for a large number of managed firewalls. It is therefore essential to keep track of the amount of consumed space used!

Also, it is generally recommended that your backup strategy should keep the amount of used space to a minimum.

Because each configured backup can perform multiple backup jobs at either a single timestamp or at recurring time stamps, due to different execution triggers, the number of backups in the list will increase. However, you may not wish to keep all created backups. In order to more easily differentiate the importance of your backups, you can assign individual user tags to add meaningful information to your backups.

To protect your firewall/CC from consuming too much backup storage space, the edit field **Retain last** is preset with the value '5', and all other fields are left empty. An empty field has the intrinsic default value of '0'. This preset will ensure that the last 5 backups will be kept.

 *When setting no retention policy entry or when setting all entries to 0, then all backups will be kept*

| | | |
|----------------|--------------------------------|---|
| Retain last | <input type="text" value="5"/> |  |
| Retain hourly | <input type="text"/> |  |
| Retain daily | <input type="text"/> |  |
| Retain weekly | <input type="text"/> |  |
| Retain monthly | <input type="text"/> |  |
| Retain yearly | <input type="text"/> |  |

If you want to keep all backups indefinitely, set all Retain fields (e.g., last, hourly, daily, weekly, monthly, yearly) to '0'. Modify any of these fields to meet your individual retention requirements. As soon as one of these limits is exceeded, all backups that surpass the limit will be deleted automatically.

However, if you want to keep certain backups indefinitely, you can make use of your individually configured user tags. By configuring a retain tag, all backups having the same value in a user tag will be exempted from automatic deletion.

NOTE

Before a new backup job is triggered, the time stamp of all existing backup files is checked and compared to the current retain-time-related configuration settings. Before the new backup is created, all existing backups that no longer match the given limits of the time-related retain fields will immediately be deleted.

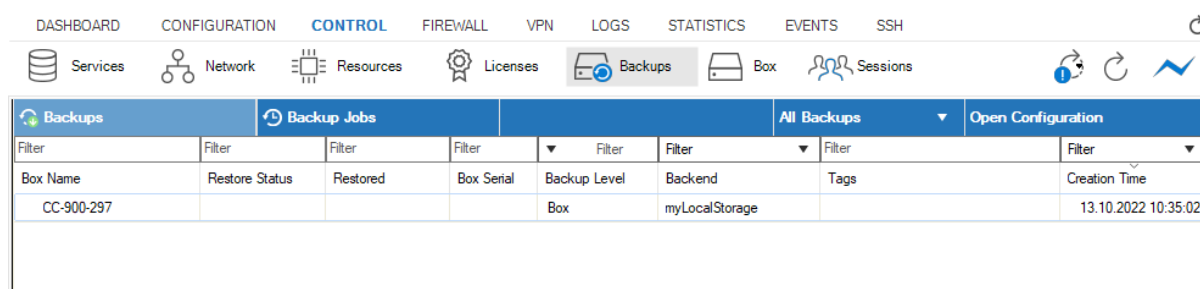
Keep this in mind, especially when decreasing one of the configured retain-time-related values.

Monitoring and Restoring Backups

You can monitor your backups and their state at **CONTROL > Backups**. There are two views that provide all relevant information on all backup files and on the result of an action that was executed on each triggered backup:

Backup Overview

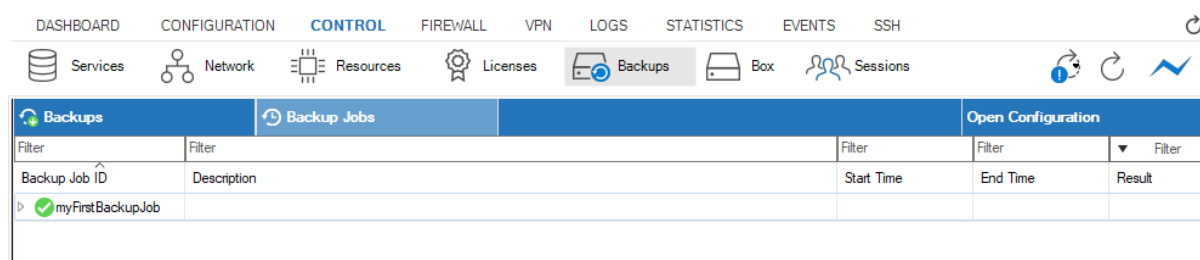
The **Backups** view displays a list of all configured back ends, their names, the levels of the configured backups (e.g., Box, Control Center, Box & Control Center), the tags that can attribute a backup, and the creation time.



| Backups | | | | | | | | |
|------------|----------------|----------|------------|--------------|----------------|--------|---------------------|--------|
| Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter |
| Box Name | Restore Status | Restored | Box Serial | Backup Level | Backend | Tags | Creation Time | |
| CC-900-297 | | | | Box | myLocalStorage | | 13.10.2022 10:35:02 | |

Backup Jobs

The **Backup Jobs** view displays a list of all processed backups grouped by the **Backup Job ID**.



| Backup Jobs | | | | | |
|------------------|-------------|------------|----------|--------|--------|
| Filter | Filter | Filter | Filter | Filter | Filter |
| Backup Job ID | Description | Start Time | End Time | Result | |
| myFirstBackupJob | | | | | |

By expanding the entry for a **Backup Job ID** entry, the list displays all associated backup jobs that have been triggered by the configured execution trigger. The time-related columns show the beginning and end time stamps and the **Result** column shows the current state of a triggered backup job.

| | | | | | | | | | |
|-----------|---------------|-----------|----------|---------|------|------------|--------|-----|--|
| DASHBOARD | CONFIGURATION | CONTROL | FIREWALL | VPN | LOGS | STATISTICS | EVENTS | SSH | |
| Services | Network | Resources | Licenses | Backups | Box | Sessions | | | |

| Backups | Backup Jobs | Open Configuration | | |
|------------------|---|---------------------|---------------------|---------|
| Filter | Filter | Filter | Filter | Filter |
| Backup Job ID | Description | Start Time | End Time | Result |
| myFirstBackupJob | Finished sync of config backup with backend. Retention policy successfully applied. | 13.10.2022 10:35:01 | 13.10.2022 10:35:04 | Success |
| | Finished sync of config backup with backend. Sync failed. Retention policy could not be applied, result code: 1 | 13.10.2022 09:43:01 | 13.10.2022 09:43:02 | Failed |
| | Finished sync of config backup with backend. Sync failed. Retention policy could not be applied, result code: 1 | 12.10.2022 15:35:02 | 12.10.2022 15:35:02 | Failed |

A backup job can be attributed to the following states:

- **Success** – A backup job has been successfully completed.
- **Pending** – A backup job is scheduled for execution.
- **Failed** – A backup job has failed.

The **Description** column provides further details that refer to the signal state of the entry in a row. These details should be informative enough in most cases. At times, however, you may want to know more about what happened during a certain phase. In such cases, even further details can be found in the log `box_Config_backup.log`.

For more information on how to create scheduled backups, see [How to Create and Monitor Backups Using the Backup Daemon](#).

Restoring Backus

Restoring a backup is done by locating the required backup and triggering the process for restoring it onto the related firewall.

For more information on how to configure the backup daemon and how to restore backups, see [How to Restore/Delete Backups Using the Backup Daemon](#).

Figures

1. backup_daemon_retain_time_related_fields.png
2. backup_daemon_view_list_of_backups.png
3. backup_daemon_view_list_of_backup_jobs_collapsed.png
4. backup_daemon_view_list_of_backup_jobs.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.