

TrueNAS - Backup Config to S3

Last verified: October 2026 against the TrueNAS Community Edition 25.10 documentation and AWS IAM/S3 documentation. See Sources.

This guide sets up two off-site backups from TrueNAS to Amazon S3: a daily archive of the **TrueNAS system configuration**, and the **app data / Docker stacks** folder. Both are uploaded with TrueNAS **Cloud Sync Tasks**. Use it so you can rebuild the NAS configuration and apps if the boot device or the system fails.

The configuration archive contains the **password secret seed** (`pwenc_secret`) and the config database. Together they decrypt stored credentials (cloud credentials, SSH keys, certificates, SMB hashes and so on). Keep the backups in a **private bucket**, enable **Remote Encryption** on the Cloud Sync task (step 5), and restrict the local folder to root.

Prerequisites

- TrueNAS Community Edition (formerly SCALE). UI paths below match 25.10.
- An AWS account with a private S3 bucket per backup (`<CONFIG_BUCKET>` , `<APPS_BUCKET>`), or one bucket with separate folders. Block Public Access stays on.
- A dataset for local archives, for example `/mnt/<POOL>/system-backups` , and the app data folder, for example `/mnt/<POOL>/<APPS_DATASET>` .
- Admin access to the TrueNAS web UI.

1) Create an IAM user for TrueNAS

In AWS IAM, create a dedicated user (for example `<IAM_USER>`) with an access key. Give it access only to the backup bucket(s). Repeat the bucket lines for each bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Effect": "Allow",
    "Action": ["s3:ListBucket", "s3:GetBucketLocation"],
    "Resource": "arn:aws:s3:::<BUCKET>"
  },
  {
    "Effect": "Allow",
    "Action": ["s3:GetObject", "s3:PutObject", "s3:DeleteObject"],
    "Resource": "arn:aws:s3:::<BUCKET>/*"
  }
]
}

```

Store the Access Key ID and Secret Access Key in a password manager. Do not put them in scripts or documentation.

2) Add the S3 cloud credential in TrueNAS

1. Go to **Credentials > Backup Credentials**. On **Cloud Credentials**, click **Add**.
2. **Provider:** Amazon S3. **Name:** for example `AWS S3 Backup`.
3. **Access Key ID:** `<ACCESS_KEY>`. **Secret Access Key:** `<SECRET_KEY>`.
4. Leave **Endpoint URL** empty for AWS. Set **Region** to the bucket region (for example `<REGION>`).
5. Click **Verify Credentials**, then **Save**.

3) Create the config backup script

Save this as `/mnt/<POOL>/system-backups/backup_config.sh`:

```

#!/bin/bash
# Save the TrueNAS config database and secret seed to a dated archive.
BACKUP_DIR="/mnt/<POOL>/system-backups"
DATE=$(date +%Y%m%d-%H%M%S)
FILENAME="truenas-config-${DATE}.tar"
tar -cf "${BACKUP_DIR}/${FILENAME}" -C /data freenas-v1.db pwenc_secret
if [ ! -s "${BACKUP_DIR}/${FILENAME}" ]; then
    echo "ERROR: backup file is empty or missing" >&2
    exit 1
fi
chmod 600 "${BACKUP_DIR}/${FILENAME}"
# Keep 30 days of local archives

```

```
find "${BACKUP_DIR}" -name "truenas-config-*.tar" -type f -mtime +30 -delete
```

```
chmod 700 /mnt/<POOL>/system-backups/backup_config.sh
```

4) Schedule the script with a cron job

1. Go to **System > Advanced Settings**. On **Cron Jobs**, click **Add**.
2. **Description:** `Daily config backup archive`. **Command:** `/mnt/<POOL>/system-backups/backup_config.sh`.
3. **Run As User:** `root`. **Schedule:** daily, for example `0 2 * * *` (02:00).
4. Leave **Hide Standard Error** cleared so failures are reported. Check **Enabled** and click **Save**.

5) Create the Cloud Sync tasks

Go to **Data Protection > Cloud Sync Tasks** and click **Add**. Create one task per source:

Setting	Config backup	App data / stacks
Credential	The S3 credential from step 2	Same
Direction / Transfer Mode	PUSH / SYNC (or COPY, see notes)	PUSH / SYNC
Directory/Files	<code>/mnt/<POOL>/system-backups</code>	<code>/mnt/<POOL>/<APPS_DATASET></code>
Bucket / Folder	<code><CONFIG_BUCKET></code> / <code>/system-backups</code>	<code><APPS_BUCKET></code> / <code>/</code>
Schedule	After the cron job, for example 02:15 daily	Daily, for example 00:00
Advanced Options	Remote Encryption on (Encryption Password + Salt)	Remote Encryption recommended. Follow Symlinks only if the stacks use them.

Save the Remote Encryption password and salt in your password manager. Without them the uploaded files cannot be restored.

6) Verify

1. Run the script once in **System > Shell** and check that a new archive appears:

```
sudo /mnt/<POOL>/system-backups/backup_config.sh
ls -lh /mnt/<POOL>/system-backups/
```

2. On **Data Protection > Cloud Sync Tasks**, click **Run Now** on each task (you can use **Dry Run** first). The state should show **SUCCESS**.
3. In the AWS S3 console, confirm the objects exist in each bucket and folder.

Troubleshooting / notes

- **SYNC vs COPY:** SYNC makes the bucket match the source, so archives the script deletes after 30 days are deleted in S3 too. Use COPY plus an S3 lifecycle rule if you want longer retention in S3.
- **Official config export:** the supported manual method is **System > Advanced Settings > Manage Configuration > Download File** with **Export Password Secret Seed** selected. Do this before upgrades. The script automates a similar archive. Restore with **Manage Configuration > Upload File**.
- **Credential errors:** check the IAM policy bucket names and the Region, then click **Verify Credentials** again.
- **Glacier:** Cloud Sync cannot delete objects that were moved to S3 Glacier / Deep Archive.
- **Stopped apps:** stop or quiesce apps with databases before backup, or use **Use Snapshot** on the task, to get consistent copies.

Sources

- [TrueNAS docs: Managing the System Configuration \(25.10\)](#)
- [TrueNAS docs: Advanced Settings Screen, Cron Jobs and Manage Configuration \(25.10\)](#)
- [TrueNAS docs: Adding Cloud Credentials \(25.10\)](#)
- [TrueNAS docs: Cloud Sync Tasks, incl. Remote Encryption \(25.10\)](#)
- [AWS: Amazon S3 policy examples](#)
- [AWS: Blocking public access to S3 storage](#)

Revision #2

Created 12 October 2026 12:19:37 by Admin

Updated 12 October 2026 12:45:54 by Admin