

# 6: Borgmatic - Backup System (optional, but you should have backup)

Borgmatic is an automated backup system that keeps your data safe by creating encrypted, compressed backups of all your applications and databases. It's like having a digital safety net that automatically saves copies of everything important. For comprehensive configuration options and advanced features, please refer to the [official Borgmatic documentation](#).

## What is Borgmatic? (Simple Explanation)

**Borgmatic** is like a smart, automated filing system that makes copies of all your important data. Think of it as having a personal assistant who:

- Makes copies of all your files and databases
- Compresses them to save space
- Encrypts them for security
- Keeps multiple versions (daily, weekly, monthly)
- Runs automatically on a schedule

### Why Borgmatic is essential:

- **Data protection** - Your data is safe if something goes wrong
- **Automatic backups** - Runs without you remembering
- **Space efficient** - Only stores changes, not duplicates
- **Encrypted storage** - Your backups are secure
- **Easy recovery** - Restore files when you need them

**Think of it like this:** If your server was a house, Borgmatic would be like having a professional photographer who takes a complete photo of every room every day, stores the photos safely, and can help you rebuild the house exactly as it was if something happens.

## Interdependencies

**Required:** Borgmatic uses **Apprise** for notifications (success/failure/security alerts). Install Apprise first via `❏ APPLICATIONS → Apprise → Install`.

# Prerequisites

Before installing Borgmatic, make sure you have:

- `❏` **Infinity Tools installed** (from Chapter 2)
- `❏` **Docker running** (from Chapter 3)
- `❏` **Traefik installed** (from Chapter 4)
- `❏` **Apprise installed** (notifications dependency)
- `❏` **Storage space** - At least 2-3 times your data size

## Why These Prerequisites Matter

**Infinity Tools:** Provides the management interface for Borgmatic

**Docker:** Runs Borgmatic in a secure container

**Traefik:** Provides secure access to backup management

**Storage space:** Backups need somewhere to be stored

## Step 1: Start Infinity Tools

Make sure you're connected to your server via SSH, then start Infinity Tools:

```
sudo infinity-tools
```

## Using the Infinity Tools GUI

When you start Infinity Tools, you'll see the main menu. Look for the `❏` **BACKUP MANAGEMENT** section - this is where Borgmatic is located.

- `❏` **Color-coded sections** - Backup tools have their own section
- `❏` **Clear descriptions** - Each tool shows what it does
- `❏` **Status indicators** - Shows if backup systems are running
- `❏` **Easy navigation** - Use arrow keys to move around

# Step 2: Navigate to Borgmatic

In the Infinity Tools menu:

1. Use your arrow keys to navigate to **BACKUP MANAGEMENT**
2. Press **Enter** to open the Backup Management menu
3. Look for **Borgmatic** in the list
4. Select it and press **Enter**

## Understanding the Backup Management Section

The Backup Management section contains tools for protecting your data:

- **Borgmatic** - Automated backup system
- **Backup Status** - Check what's being backed up
- **Backup Settings** - Configure backup options
- **Restore Data** - Recover files when needed

**Look for the turquoise cursor** - it shows what you're about to select!

## Step 3: Install Borgmatic

When you select Borgmatic, you'll see installation options. Choose **Install Borgmatic**.

## What Happens During Installation

Borgmatic installation will:

- Create a backup container
- Set up two backup schedules (files and databases)
- Configure encryption for security
- Set up automatic notifications
- Create security monitoring (canary files)

**This usually takes 3-5 minutes.**

## Step 4: Configure Borgmatic

During installation, you'll be asked several questions:

# Backup Schedule

You'll see a prompt like:

```
Backup Schedule Configuration
=====
How often should files be backed up?

1) Daily (default) - Once per day at 2:00 AM
2) Twice daily - Every 12 hours
3) Weekly - Once per week on Sunday
```

**For beginners:** Choose "1" (Daily) - This provides good protection without using too much storage.

# Retention Policy

You'll be asked how long to keep backups:

```
Retention Policy
=====
How long should backups be kept?

1) Conservative (default) - 7 daily, 4 weekly, 6 monthly
2) Aggressive - 14 daily, 8 weekly, 12 monthly
3) Minimal - 3 daily, 2 weekly, 3 monthly
```

**For beginners:** Choose "1" (Conservative) - This keeps enough backups for recovery without using too much space.

# Compression Settings

You'll be asked about compression:

```
Compression Configuration
=====
Choose compression algorithm:

1) zstd (default) - Best balance of speed and compression
2) lz4 - Fastest compression, larger files
```

- 3) zlib - Good compression, moderate speed
- 4) lzma - Best compression, slower

**For beginners:** Choose "1" (zstd) - This provides good compression without being too slow.

## Security Passphrase

You'll be asked to create a passphrase for your backups:

```
██ Security Configuration
=====
Enter a strong passphrase for backup encryption:
[Enter your passphrase]
```

**Important:** This passphrase encrypts your backups. Choose something strong and save it safely!

### Passphrase tips:

- At least 12 characters long
- Mix of letters, numbers, and symbols
- Easy for you to remember
- Unique (don't use it anywhere else)

**Example:** `MyBackup@2024!Secure#Data`

## Step 5: Wait for Installation

After answering the questions, Borgmatic will install and start. You'll see messages like:

```
██ Installing Borgmatic...
██ Creating backup configurations...
██ Setting up encryption...
██ Creating security monitoring...
██ Setting up schedules...
█ Borgmatic installed successfully!
```

## Step 6: Understanding What Was Created

Borgmatic installation creates a sophisticated backup system with two types of backups:

## File Backups

These backup all your application files:

- **What's backed up:** All files in `/opt/speedbits/`
- **Schedule:** Daily (or your chosen frequency)
- **Retention:** 7 daily, 4 weekly, 6 monthly
- **Purpose:** Recover application configurations and data

## Database Backups

These backup all your databases:

- **What's backed up:** MariaDB, PostgreSQL, SQLite, MongoDB databases
- **Schedule:** Every 6 hours
- **Retention:** 48 hourly, 7 daily
- **Purpose:** Recover database data quickly

## Security Features

Borgmatic includes advanced security:

- **Encryption** - All backups are encrypted
- **Canary files** - Detects if your system is compromised
- **Notifications** - Alerts you about backup status
- **Deduplication** - Only stores changes, saving space

## Step 7: Verify Borgmatic is Working

Let's make sure Borgmatic is running properly.

### Check Status in Infinity Tools

In the Infinity Tools menu, go to:

- **STATUS & HEALTH → STATUS**

You should see Borgmatic listed as "RUNNING" or "ACTIVE".

# Using the Status Dashboard

The Status & Health section shows you:

- **Service Status** - Which applications are running
- **System Health** - CPU, memory, and disk usage
- **Docker Info** - All your containers and their status
- **Backup Status** - When backups last ran

**Look for the green checkmarks** - they indicate everything is working properly!

## Check Backup Status

You can also check by going to:

- **BACKUP MANAGEMENT** → **Backup Status**

This will show you:

- **Last Backup** - When backups last ran
- **Backup Size** - How much space backups use
- **Encryption Status** - Whether backups are encrypted
- **Backup History** - Recent backup activity

## Step 8: Understanding Backup Storage

Borgmatic stores your backups in a special location:

### Backup Location

Your backups are stored in:

- `/opt/speedbits-backup/borgmatic-repo/` - Main backup repository
- This contains all your encrypted, compressed backups
- Each backup is stored as an "archive" with a timestamp

### Backup Structure

Your backup repository contains:

- **File Archives** - `speedbits-files-server-2024-01-15-020000`

- **Database Archives** - `speedbits-databases-server-2024-01-15-060000`
- **Encryption Keys** - Secure keys for accessing backups
- **Metadata** - Information about each backup

## Step 9: Test Your First Backup

Let's run a test backup to make sure everything works:

### Manual Backup Test

In the Infinity Tools menu, go to:

- **BACKUP MANAGEMENT** → **Run Manual Backup**

This will start a backup immediately and show you the progress.

### What You'll See

During the backup, you'll see messages like:

```
Starting SpeedBits file backup...
Creating archive speedbits-files-server-2024-01-15-143000...
Backing up /opt/speedbits/vaultwarden...
Backing up /opt/speedbits/traefik...
File backup completed successfully
```

### Understanding Backup Progress

The backup process shows:

- **Files being backed up** - What's currently being processed
- **Progress indicators** - How much is complete
- **Time estimates** - How long it will take
- **Completion status** - When it's finished

### What's Next?

Congratulations! You now have an automated backup system protecting all your data.

# What You've Accomplished

- **Installed Borgmatic** - Automated backup system
- **Configured encryption** - Your backups are secure
- **Set up schedules** - Backups run automatically
- **Enabled monitoring** - You'll know if something goes wrong
- **Protected your data** - Everything is safely backed up

## Next Steps

Now you can:

- Install more applications - They'll be automatically backed up
- Monitor backup status - Check that backups are running
- Test recovery - Practice restoring files when needed
- Set up notifications - Get alerts about backup status

## Troubleshooting

### Backup Not Running

If backups aren't running:

- Check that Borgmatic container is running: `docker ps | grep borgmatic`
- Check backup logs: `docker logs borgmatic`
- Verify there's enough disk space
- Check that applications are installed to backup

### Backup Fails

If backups fail:

- Check disk space - Backups need free space
- Verify passphrase is correct
- Check file permissions
- Look at error messages in the logs

### Can't Access Backups

If you can't access your backups:

- Make sure you have the correct passphrase
- Check that the backup repository exists
- Verify file permissions on backup directory
- Try running a manual backup to test

## Quick Reference

### Check Borgmatic status:

```
docker ps | grep borgmatic
```

### View backup logs:

```
docker logs borgmatic
```

### Run manual backup:

```
docker exec borgmatic borgmatic --config /etc/borgmatic/borgmatic-files.yml create
```

### List all backups:

```
docker exec borgmatic borg list /backups/borgmatic-repo
```

## You're Ready!

Borgmatic is now installed and protecting your data! You have a professional-grade backup system that runs automatically and keeps your data safe.

### What you accomplished:

- Installed and configured Borgmatic
- Set up encrypted, automated backups
- Protected all your applications and data
- Enabled monitoring and notifications

**Next step:** You can now install your first application (Vaultwarden) knowing it will be automatically backed up and protected!

## What You Learned

- **Borgmatic** - An automated backup system for data protection
- **Backup Strategies** - How to protect files and databases
- **Encryption** - How to keep backups secure
- **Automation** - How to set up hands-off data protection
- **Monitoring** - How to ensure backups are working

You now have enterprise-grade data protection running on your server!

---

*Next: Installing Vaultwarden - Your Password Manager (Chapter 7)*

---

Revision #6

Created 30 October 2025 13:07:09 by bjoern

Updated 17 November 2025 16:27:25 by bjoern