# Foundations

These apps are more or less essential. You need Traefik for many other apps to run properly; you should also seriously think about backup if you do anything mission critical with this server or store data on it.

# 3: Setting Up Your Foundation

Before you can install your first application, we need to set up the basic infrastructure that Infinity Tools needs to work properly. Don't worry - Infinity Tools will handle most of this automatically!

This chapter also covers **foundational apps** that most Infinity Tools require—the most essential of them is Traefik, on which many other apps rely. You do not strictly *need* the back-tool Borgmatic, however, we **highly recommend** that you install it to automatically create **backups** of your data. And to use Borgmatic, you have to install Apprise, a notification system, which is why we also cover it in this chapter.

# What We'll Set Up

In this chapter, we'll prepare:

- **Docker** - The system that runs all your applications
- **Docker Network** - How applications talk to each other
- **System Requirements** - Making sure everything is ready
- **Basic Security** - Simple firewall setup (optional)

**Time needed:** About 10-15 minutes

# What is Docker? (Simple Explanation)

**Docker** is like a shipping container system for software. Just like how shipping containers make it easy to move goods around the world, Docker makes it easy to run applications on any computer.

**Why we need it:**

- Applications run in isolated "containers" - they can't interfere with each other
- Everything is pre-configured and ready to go
- If something goes wrong, you can easily restart or replace just that application
- It's the standard way modern applications are deployed

**Think of it like this:** Instead of installing WordPress directly on your server (which can be complicated), Docker runs WordPress in a container that has everything it needs already set up. If you install Portainer, you get a convenient web app to see what's going on with your Docker containers and administrate them.

# Step 1: Run the Readiness Check

Infinity Tools has a built-in system that checks if everything is ready and installs what's missing. Let's run it!

# Start Infinity Tools

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

```
sudo infinity-tools
```

# What You'll See in the GUI

When you start Infinity Tools, you'll see a beautiful, modern interface with:

- **Colorful headers** - Easy to identify different sections
- **Progress indicators** - Shows what's happening during installation
- **Status messages** - Tells you if things are working or if there are problems
- **Interactive prompts** - Asks you questions when needed

**Don't worry if it looks complex!** The GUI is designed to guide you through everything step by step.

# What Happens Next

Infinity Tools will automatically run a "readiness check" that:

- Checks if Docker is installed
- Installs Docker if it's missing
- Sets up the Docker network
- Installs other required tools
- Verifies everything is working

**You'll see messages like:**

```
∞  INFINITY TOOLS READINESS CHECK

Ensuring all prerequisites are met...

This will check and install:
• Docker & Docker Compose
```

- Docker Network for services
- GUM for modern UI
- Dialog for compatibility
- System requirements

# If Docker Needs to be Installed

If Docker isn't installed yet, you'll see a message asking if you want to install it:

```
□□DOCKER INSTALLATION REQUIRED

Infinity Tools requires Docker to run containerized services.

Docker will be installed and configured automatically.
This includes Docker Engine and Docker Compose.

⚠□  This requires internet connection and may take a few minutes.

Install Docker now?
```

**Answer "Yes"** to continue. The installation will take a few minutes.

# Docker Network Setup

After Docker is installed, you'll be asked about setting up a network:

```
□□DOCKER NETWORK SETUP

Infinity Tools services need a Docker network to communicate.

This network allows containers to find each other by name
and enables features like Traefik reverse proxy.

Default network name: proxy
```

**Press Enter** to use the default network name "proxy" (recommended).

# Step 2: Verify Everything is Working

After the readiness check completes, you should see:

```
 READINESS CHECK COMPLETE


All prerequisites are satisfied!
Infinity Tools is ready to use.
```

# What Was Installed

If everything went well, you now have:

- **Docker Engine** - The main Docker system
- **Docker Compose** - Tool for managing multiple containers
- **Docker Network** - A network called "proxy" for your services
- **GUM** - The modern interface you're using
- **Dialog** - Backup interface (just in case)

# Step 3: Understanding What Happened

# Docker Installation

Docker was installed and configured to:

- Start automatically when your server boots
- Run containers securely
- Manage storage for your applications
- Handle networking between containers

# Docker Network

The "proxy" network was created to:

- Allow applications to find each other by name
- Enable Traefik (our reverse proxy) to route traffic
- Keep your applications isolated from the internet
- Make it easy to add new services later

# Step 4: Optional - Basic Security Setup

Now that the basics are ready, you can optionally set up basic security. This is recommended but not required to get started.

# What is a Firewall?

A **firewall** is like a security guard for your server. It controls which connections are allowed in and out.

**Why it's important:** Without a firewall, your server is like a house with all doors unlocked - anyone can try to access it.

# Setting Up the Firewall

In the Infinity Tools menu, you'll see a "Security & Networking" section. You can set up the firewall later, but here's what it does:

- Allows SSH connections (so you can still connect)
- Allows HTTP and HTTPS traffic (for websites)
- Blocks other unwanted connections
- Protects against common attacks

**For now:** You can skip this and set it up later. Your server is reasonably safe as long as you keep your passwords strong.

# Step 5: Understanding Your System

# What's Running Now

Right now, your server has:

- **Infinity Tools** - The management system
- **Docker** - Ready to run applications
- **Docker Network** - Ready for services
- **No Applications Yet** - This is what we'll install next!

# What's Next

You're now ready to install your first application! The most important one to install first is **Traefik** - it handles secure connections and routing for all your other applications.

# Troubleshooting

## Docker Installation Failed

If Docker installation fails:

- Check your internet connection
- Make sure you have enough disk space (at least 1GB free)
- Try running the readiness check again
- If it keeps failing, contact support with the error message

## Network Creation Failed

If the Docker network creation fails:

- Make sure Docker is running: `sudo systemctl status docker`
- Try restarting Docker: `sudo systemctl restart docker`
- Run the readiness check again

## Can't Connect to Server

If you lose connection during setup:

- Reconnect via SSH
- Run `sudo infinity-tools` again
- The readiness check will continue where it left off

# Quick Reference

**Check if Docker is running:**

```
sudo systemctl status docker
```

**Check Docker networks:**

```
docker network ls
```

**View Docker containers:**

```
docker ps
```

**Restart Docker if needed:**

```
sudo systemctl restart docker
```

# You're Ready!

Congratulations! You now have:

- A working Docker system
- A network for your applications
- All the tools Infinity Tools needs
- A solid foundation for your applications

**Next step:** Install Traefik - the reverse proxy that will handle secure connections and routing for all your applications.

# What You Learned

- **Docker** - A system for running applications in containers
- **Docker Network** - How applications communicate with each other
- **Readiness Check** - Infinity Tools' automatic setup system
- **Infrastructure** - The foundation that makes everything else possible

You're now ready to install your first application! In the next chapter, we'll install Traefik, which is essential for running other applications securely.

---

*Next: Installing Traefik - Your Reverse Proxy (Chapter 4)*

# 4: Traefik - Reverse Proxy (essential)

Now that your infrastructure is ready, it's time to install Traefik - the most important service you'll set up. Traefik handles secure connections and routing for all your other applications.

# What is Traefik? (Simple Explanation)

**Traefik** is like a smart traffic director for your server. Think of it as a receptionist at a large office building who:

- Greets visitors (web traffic) at the front door
- Checks their ID (verifies security certificates)
- Directs them to the right office (routes traffic to the correct application)
- Makes sure they use the secure elevator (forces HTTPS)

**Why Traefik is essential:**

- **Automatic SSL certificates** - Makes your websites secure (HTTPS)
- **Domain routing** - Directs traffic to the right application
- **Security** - Protects your applications from direct internet access
- **Required by other apps** - Most Infinity Tools applications need Traefik

# Why Install Traefik First?

Traefik should be installed before any other application because:

- **Other apps depend on it** - Many applications will ask if you want to use Traefik
- **SSL certificates** - It handles secure connections for all your services
- **Domain management** - It routes traffic based on your domain names
- **Security foundation** - It provides a secure gateway to your applications

**Without Traefik:** You'd have to manually configure SSL certificates and routing for each application - a complex and time-consuming process.

# What You'll Need

Before installing Traefik, make sure you have:

- ✅ **Docker installed** (from Chapter 3)
- ✅ **Docker network set up** (from Chapter 3)
- ✅ **A domain name** (optional but recommended)
- ✅ **An email address** (for SSL certificate notifications)

# About Domain Names

**What is a domain name?** It's like your website's address (e.g., `mywebsite.com`).

**Why you need one:** Traefik uses your domain name to create SSL certificates and route traffic. Without one, you can still use Traefik, but you'll get security warnings in your browser.

**Examples of domain names:**

- `myinfinitytools.com`
- `myserver.example.com`
- `home.mydomain.net`

**Don't have a domain?** That's okay! You can still install Traefik and add a domain later, or use your server's IP address directly.

# Step 1: Start Infinity Tools

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

```
sudo infinity-tools
```

# Step 2: Navigate to Traefik Installation

In the Infinity Tools menu, you'll see several sections. Look for:

- 🛡️ **SECURITY & NETWORKING** - This is where Traefik is located

Use your arrow keys to navigate to this section and press Enter.

# Using the Infinity Tools GUI

The Infinity Tools interface makes everything easy to find and use:

- **Color-coded sections** - Each category has its own color
- **Clear descriptions** - Hover over options to see what they do
- **Status indicators** - Shows if services are running or stopped
- **Progress bars** - Shows installation progress in real-time

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

# Step 3: Install Traefik

In the Security & Networking menu, you'll see:

- **Install Traefik** - This is what you want

Select "Install Traefik" and press Enter.

## What Happens During Installation

Traefik installation will:

- Create a configuration file
- Set up SSL certificate management
- Create a Docker container
- Configure the reverse proxy
- Start the service

**This usually takes 1-2 minutes.**

# Step 4: Configure Traefik

During installation, you'll be asked a few questions:

## Email Address for SSL Certificates

You'll see a prompt like:

```
Enter email address for SSL certificates:
[admin@example.com]
```

**What to enter:** Use a valid email address you check regularly. This is used for SSL certificate notifications and warnings.

**Examples:**

- `admin@myinfinitytools.com`
- `your-email@gmail.com`
- `notifications@yourdomain.com`

# Domain Name (Optional)

If you have a domain name, you'll be asked:

```
Enter your domain name (or press Enter to skip):
[myinfinitytools.com]
```

**If you have a domain:** Enter it here (e.g., `myinfinitytools.com`)

**If you don't have a domain:** Press Enter to skip - you can add this later

# IPv6 Configuration

You might be asked about IPv6 support:

```
Do you want to enable IPv6 support?
Y) Yes - Enable both IPv4 and IPv6
N) No - IPv4 only (recommended for beginners)
```

**For beginners:** Choose "N" (No) - IPv4 only is simpler and works fine for most use cases.

# Step 5: Wait for Installation

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

```
□□Installing Traefik...
□□Creating configuration...
□□Starting Traefik container...
□ Traefik installed successfully!
```

# Step 6: Verify Traefik is Working

After installation completes, let's make sure Traefik is running properly.

# Check Traefik Status

In the Infinity Tools menu, go to:

- **STATUS & HEALTH → STATUS**

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

# Using the Status Dashboard

The Status & Health section gives you a complete overview of your system:

- **Service Status** - Shows which applications are running
- **System Health** - CPU, memory, and disk usage
- **Docker Info** - All your containers and their status
- **Network Status** - Shows your Docker networks

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

# Check Docker Containers

You can also check by going to:

- **STATUS & HEALTH → DOCKER INFO**

Look for a container named "traefik" - it should be running.

# Understanding the Docker Info Screen

The Docker Info section shows you:

- **Container Name** - What the container is called
- **Status** - Running, stopped, or restarting
- **Ports** - Which ports the container is using
- **Memory Usage** - How much RAM it's using

**Green status means everything is working!** Red or yellow means there might be an issue.

# Step 7: Understanding What Was Created

Traefik installation creates several important files and configurations:

# Configuration Files

Traefik stores its configuration in:

- `/opt/speedbits/traefik/traefik.yml` - Main configuration
- `/opt/speedbits/traefik/docker-compose.yml` - Docker setup

# SSL Certificates

SSL certificates are stored in:

- `/opt/speedbits/traefik/letsencrypt/` - Let's Encrypt certificates

# Docker Container

Traefik runs as a Docker container that:

- Listens on ports 80 (HTTP) and 443 (HTTPS)
- Automatically redirects HTTP to HTTPS
- Manages SSL certificates
- Routes traffic to your applications

# Step 8: Test Traefik (If You Have a Domain)

If you configured a domain name, you can test Traefik by visiting your domain in a web browser.

# What You Should See

When you visit your domain, you should see:

- A secure connection (HTTPS) - look for the lock icon in your browser
- Either a "404 Not Found" page (normal - no apps installed yet) or a Traefik dashboard

# If You Don't Have a Domain

You can still test Traefik by visiting your server's IP address:

- Visit `http://YOUR_SERVER_IP` in your browser
- It should redirect to `https://YOUR_SERVER_IP`
- You'll see a security warning (normal without a domain)

# What's Next?

Congratulations! You now have Traefik installed and running. This means:

- **SSL certificates** are automatically managed
- **Secure connections** are enforced
- **Domain routing** is ready
- **Other applications** can now be installed

# Ready for Applications

Now you can install any of the applications in Infinity Tools:

- **WordPress** - For websites and blogs
- **Vaultwarden** - For password management
- **Nextcloud** - For file storage and sharing
- **And many more!**

When you install these applications, they'll automatically work with Traefik to provide secure, domain-based access.

# Troubleshooting

## Traefik Won't Start

If Traefik fails to start:

- Check that Docker is running: `sudo systemctl status docker`
- Check Docker logs: `docker logs traefik`
- Verify the configuration: `cat /opt/speedbits/traefik/traefik.yml`
- Try restarting: `docker restart traefik`

## SSL Certificate Issues

If SSL certificates aren't working:

- Make sure your domain points to your server's IP address
- Check that ports 80 and 443 are open
- Wait a few minutes for certificates to be issued
- Check Traefik logs: `docker logs traefik | grep -i acme`

# Can't Access Traefik

If you can't access Traefik:

- Check that Traefik is running: `docker ps | grep traefik`
- Verify ports are open: `sudo ss -tulnp | grep :80`
- Check firewall settings
- Try accessing via IP address instead of domain

# Quick Reference

**Check Traefik status:**

```
docker ps | grep traefik
```

**View Traefik logs:**

```
docker logs traefik
```

**Restart Traefik:**

```
docker restart traefik
```

**Check SSL certificates:**

```
ls -la /opt/speedbits/traefik/letsencrypt/
```

# You're Ready!

Traefik is now installed and running! This is the foundation that makes all your other applications work securely and efficiently.

**What you accomplished:**

- ✅ Installed and configured Traefik
- ✅ Set up automatic SSL certificate management

- Created a secure gateway for your applications
- Prepared your system for other applications

**Next step:** You can now install any application from the Infinity Tools menu. Each application will automatically work with Traefik to provide secure, domain-based access.

# What You Learned

- **Traefik** - A reverse proxy that handles SSL and routing
- **SSL Certificates** - Automatic security certificates for your domains
- **Domain Routing** - How traffic is directed to the right application
- **Infrastructure Foundation** - The base layer that supports all other services

You now have a solid foundation for running secure, professional applications on your server!

---

*Next: Installing Your First Application (Coming Soon)*

# 5 Apprise - Notifications (optional, but essential for backups with Borgmatic)

Apprise sends notifications about your server and applications (e.g., backup success/failure). It supports email, Slack, Telegram, and 90+ providers. For detailed provider setup, see the official Apprise documentation.

# Why Apprise?

- **Essential for backups** - Borgmatic uses Apprise for alerts
- **Many providers** - Email, Slack, Discord, Telegram, etc.
- **Simple** - One container, easy configuration

# Prerequisites

- Traefik installed (Chapter 4)
- Docker running (Chapter 3)
- Optional: Subdomain (Chapter 4.5), e.g., `notify.yourdomain.com`

# Step 1: Start Infinity Tools

```
sudo infinity-tools
```

# Step 2: Install Apprise

1. Go to **APPLICATIONS**
2. Select **Apprise**
3. Choose **Install Apprise**

# Using the Infinity Tools GUI

- Use ↑/↓ to move, **Enter** to select, **Esc** to go back
- Look for the **turquoise cursor** indicating the current selection
- Each screen shows a short description at the top explaining what's needed

# Step 2.1: Choose SSL Mode

You'll see three options. Here's what each means and when to use it:

- **Traefik (recommended)**
  - **What it is:** Uses your domain name with a trusted HTTPS certificate from Let's Encrypt
  - **What you need:** A subdomain (e.g., `notify.yourdomain.com`) pointing to your server (see Chapter 4.5)
  - **What you get:** No browser warnings, a clean URL like `https://notify.yourdomain.com/notify`
  - **Pick this if:** You plan to use Apprise over the internet or want the simplest, secure setup
- **Standalone HTTPS (self-signed)**
  - **What it is:** Uses HTTPS with a self-signed certificate (your browser will warn it's not trusted)
  - **What you need:** Just a free port (e.g., 8099)
  - **What you get:** URL like `https://SERVER_IP:8099/notify` with a warning you must accept once
  - **Pick this if:** You only use Apprise inside your own network and don't want to set up a domain yet
- **Standalone HTTP (not encrypted)**
  - **What it is:** No encryption. Data is sent in plain text
  - **What you need:** A free port (e.g., 8098)
  - **What you get:** URL like `http://SERVER_IP:8098/notify`
  - **Pick this only if:** You're testing temporarily on a private network and never expose it to the internet

**Simple rule of thumb:** Use **Traefik** if you have a domain; use **Standalone HTTPS** for quick local use; avoid **HTTP** on the internet.

# Step 2.2: If You Choose Traefik

1. Enter your subdomain, e.g., `notify.yourdomain.com`
2. Ensure the subdomain's DNS A record points to your server (see Chapter 4.5)
3. Infinity Tools will configure HTTPS automatically via Let's Encrypt

**After install:** Your endpoint will be `https://notify.yourdomain.com/notify`

# Step 2.3: If You Choose Standalone

1. Pick a port (suggested defaults appear on screen)
   - HTTPS (self-signed): e.g., `8099` → `https://SERVER_IP:8099/notify`
   - HTTP: e.g., `8098` → `http://SERVER_IP:8098/notify`
2. Accept the browser warning if using self-signed HTTPS

# Where to Find the URL After Install

- On the finish screen, Infinity Tools prints the access URL
- You can also see it in □□ **STATUS & HEALTH → STATUS**

# What Happens

- Apprise container is created
- Optional domain + Traefik HTTPS routing
- Service is exposed for local HTTP API calls

# Step 3: Configure a Notification

Set your first notification target (example: email). You can add more later.

# Example: Email (SMTP)

Collect: SMTP host, username, password, from address.

- Provider URL example:
  `mailtos://USERNAME:PASSWORD@SMTP_HOST:587/?from=from@yourdomain.com&to=you@example.com`
- Store this URL safely; you'll paste it where notifications are configured (e.g., Borgmatic)

# Test a Notification

1. Find your Apprise endpoint (e.g., `http://apprise:8000/notify` or your domain)
2. Send a test:

```
curl -X POST "http://apprise:8000/notify" \
  -d "title=Test" \
  -d "body=Hello from Apprise" \
  -d "url=YOUR_PROVIDER_URL"
```

3. Confirm you received the notification

# Where It’s Used

- **Borgmatic:** Backup success/failure/security alerts
- **Other tools:** Can post to the same endpoint

# Troubleshooting

- Check container logs: `docker logs apprise`
- Verify provider URL syntax (see official docs)
- Confirm network access to your SMTP/notification provider

# You're Ready

Apprise is now running. Next, install Borgmatic (Chapter 6) so your backups can send notifications.

# 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)*

# 7: Portainer – Docker Management Made Easy (optional but convenient)

Portainer gives you a friendly web interface to manage your Docker containers, images, volumes, and networks. Instead of typing commands in the terminal, you can click buttons and see everything visually. Think of it as a control panel for all your Docker applications.

For advanced features, team management, and detailed documentation, see the official Portainer documentation.

# Why Portainer?

- **Visual management** - See all your containers at a glance
- **Easy operations** - Start, stop, restart containers with clicks
- **View logs** - See what's happening inside containers
- **Deploy stacks** - Install applications using docker-compose files via web UI
- **Monitor resources** - See CPU, memory, and network usage
- **No terminal needed** - Manage everything from your browser

# Prerequisites

- **Docker running** (from Chapter 3)
- **Optional: Traefik installed** (from Chapter 4) for HTTPS access with a domain
- **Optional: Subdomain** (from Chapter 4.5), e.g., `portainer.yourdomain.com`

**Note:** Portainer works fine without Traefik - you can access it directly via IP address and port. Traefik just makes it more secure and easier to access with a friendly domain name.

# Step 1: Start Infinity Tools

```
sudo infinity-tools
```

# Step 2: Install Portainer

1. Go to □□ **APPLICATIONS**
2. Select **Portainer**
3. Choose **Install Portainer**

# Using the Infinity Tools GUI

- Use ↑/↓ to move, **Enter** to select, **Esc** to go back
- Look for the **turquoise cursor** indicating the current selection
- Each screen shows a short description at the top explaining what's needed

# Step 2.1: Choose SSL Mode

You'll see two options. Here's what each means:

- **Traefik (recommended)**
  - **What it is:** Uses your domain name with a trusted HTTPS certificate from Let's Encrypt
  - **What you need:** A subdomain (e.g., `portainer.yourdomain.com`) pointing to your server (see Chapter 4.5)
  - **What you get:** No browser warnings, a clean URL like `https://portainer.yourdomain.com`
  - **Pick this if:** You want secure, easy access with a domain name
- **Standalone HTTPS (self-signed)**
  - **What it is:** Uses HTTPS with a self-signed certificate (your browser will warn it's not trusted)
  - **What you need:** Just a free port (default: 9443)
  - **What you get:** URL like `https://SERVER_IP:9443` with a warning you must accept once
  - **Pick this if:** You don't have a domain yet or only use Portainer on your local network

**Simple rule of thumb:** Use **Traefik** if you have a domain and want the best experience; use **Standalone HTTPS** if you're just getting started or don't have a domain yet.

# Step 2.2: If You Choose Traefik

1. Enter your subdomain, e.g., `portainer.yourdomain.com`
2. Ensure the subdomain's DNS A record points to your server (see Chapter 4.5)
3. Infinity Tools will configure HTTPS automatically via Let's Encrypt

**After install:** Your Portainer will be available at `https://portainer.yourdomain.com`

# Step 2.3: If You Choose Standalone

1. Pick a port (default: 9443)
2. Your Portainer will be available at `https://SERVER_IP:9443`
3. When you first visit, accept the browser security warning (click "Advanced" → "Proceed")

# What Happens During Installation

- Portainer container is created
- Data directory is set up at `/opt/speedbits/portainer`
- Optional domain + Traefik HTTPS routing (if using Traefik)
- Service starts and becomes accessible

# Step 3: First-Time Setup (IMPORTANT!)

⚠ **CRITICAL:** Portainer requires you to create admin credentials on your FIRST login. There is no default password!

# Step 3.1: Open Portainer

1. Open the access URL shown after installation in your browser
2. If using Traefik: Wait 30-60 seconds for SSL certificate generation
3. If using Standalone: Accept the browser security warning

# Step 3.2: Create Admin Account

You'll see a screen: **"Create the first administrator user"**

1. **Username:** Choose any username (many people use "admin")
2. **Password:** Enter a STRONG password (minimum 12 characters)
    - □□ **Tip:** Use a password manager (like Vaultwarden from Chapter 7!) to generate and store a strong password (20+ characters)
3. Click **"Create user"**

**⚠ WRITE DOWN YOUR CREDENTIALS IMMEDIATELY!**

This is your ONLY chance to set the initial password. There is NO "forgot password" option on first setup. If you forget it, you'll need to reset Portainer completely (see Troubleshooting below).

# Step 3.3: Connect to Docker

1. After creating your account, you'll see: **"Get Started"**
2. Click **"Get Started"**
3. Select **"Docker"** environment
4. Click **"Connect"**

 **Done!** You'll immediately see all your Docker containers, images, volumes, and networks.

# What You Can Do in Portainer

## Container Management

- **View all containers** - See running, stopped, and all containers
- ▶ **Start/Stop/Restart** - Control containers with buttons
- **View logs** - See what's happening inside containers in real-time
- ⚙ **Inspect settings** - See environment variables, volumes, networks
- **Execute commands** - Run commands inside containers (like opening a terminal)

## Image Management

- **Browse images** - See all Docker images on your server
- **Remove unused images** - Free up disk space
- **Pull new images** - Download images from Docker Hub

## Stack Deployment

- **Deploy stacks** - Install applications using docker-compose files via web UI
- **Edit stacks** - Modify docker-compose configurations visually
- **Update stacks** - Update applications with new configurations

## Monitoring

- **Resource usage** - See CPU, memory, and network usage for each container
- **Statistics** - View historical performance data
- **Health checks** - See container health status

## Volume and Network Management

- □□ **Manage volumes** - View, create, and delete data volumes
- □□ **Manage networks** - View and configure Docker networks

# Security Recommendations

Portainer has FULL access to your Docker system, so it's important to protect it:

- □ **Use a strong password** - Minimum 12 characters, preferably 20+
- □ **Store credentials securely** - Use a password manager (Vaultwarden recommended!)
- □ **Enable 2FA** - Go to Settings → Users → Two-Factor Authentication (after first login)
- □ **Create separate users** - If sharing access, create individual accounts (don't share admin)
- □ **Regular backups** - Go to Settings → Backup Configuration to export your Portainer settings
- ⚠ **Protect access** - Portainer can control all your containers - keep it secure!

# Troubleshooting

## Forgot Your Password?

If you forgot your Portainer admin password, you'll need to reset it completely:

1. Stop Portainer:
   ```
   cd /opt/speedbits/portainer
   docker compose down
   ```
2. Delete the Portainer database:
   ```
   rm -rf /opt/speedbits/portainer/data
   ```
3. Restart Portainer:
   ```
   cd /opt/speedbits/portainer
   docker compose up -d
   ```
4. Open Portainer again and create a new admin account

⚠ **WARNING:** This deletes ALL Portainer settings (users, preferences, etc.), but your Docker containers are NOT affected.

## Can't Access Portainer

- **Traefik mode:** Wait 30-60 seconds after installation for SSL certificate generation
- **Standalone mode:** Make sure you're using `https://` (not `http://`)
- **Check container status:** Run `docker ps | grep portainer` to see if it's running
- **Check logs:** Run `docker logs portainer` to see error messages

## Portainer Shows No Containers

- Make sure you selected "Docker" environment during first-time setup
- Check that Docker is running: `docker ps`
- Refresh the Portainer page

# Where to Find Portainer After Install

- On the finish screen, Infinity Tools prints the access URL
- You can also see it in ◫ **STATUS & HEALTH → STATUS**
- Check the installation directory: `/opt/speedbits/portainer`

# You're Ready!

Portainer is now installed and ready to use. You can manage all your Docker containers visually from your browser. This makes it much easier to work with your Infinity Tools applications!

**Next steps:** Use Portainer to monitor your containers, view logs, and manage your Docker environment. You can continue installing other Infinity Tools applications - Portainer will help you keep track of everything.