Private Secrets Management Server with Infisical by Code Creator

Quick start: Launch the EC2 instance, wait a few minutes, SSH as ubuntu as user name, run codecreator-infisical-setup, then open the HTTPS URL shown by the server and create the first Infisical administrator.

1. Launch the EC2 Instance

Launch the AMI from AWS Marketplace or the EC2 console. Use an EC2 key pair that you control and make sure the instance receives a public IPv4 address.

Recommended starting sizes:

- t3.large for light use
- t3.xlarge for the recommended starting configuration
- 50 GB gp3 root volume

Recommended inbound security group rules:

Port	Source	Purpose
22 TCP	Your administrator IP only	SSH administration
80 TCP	Internet	Automatic HTTPS certificate issue and renewal
443 TCP	Intended users	Secure Infisical web access

Do not expose TCP 8080, 5432, or 6379. Infisical, PostgreSQL, and Redis are already isolated by the AMI.

2. Wait for First Boot

Allow about 3 to 5 minutes after the instance first starts. The AMI automatically generates unique application encryption and authentication secrets, creates new PostgreSQL and Redis credentials, starts the containers, detects the instance public IPv4 address, and requests a trusted HTTPS certificate.

If you browse to the server before authorizing your browser IP, a 403 Forbidden page is expected. This is a security feature.

3. Connect by SSH

Connect using the SSH username ubuntu and the EC2 key pair selected when you launched the instance.

```
ssh -i /path/to/your-key.pem ubuntu@PUBLIC_IP
```

After login, you can read the first login information, run:

```
cat /home/ubuntu/FIRST_LOGIN.txt
```

4. Authorize Your Browser and Create the First Administrator

From the SSH session, run the setup helper without sudo:

codecreator-infisical-setup

The helper authorizes the public IP from your current SSH connection and displays the secure Infisical URL.

Open the displayed URL in your browser:

https://Your_PUBLIC_IP

Create the first Infisical account. The first account created on a new self hosted Infisical instance becomes the server administrator.

After the first administrator is created, sign out and confirm that the normal sign in page appears.

If you later administer the server from a different public IP, SSH from that location and run codecreator-infisical-setup again. The helper updates the allowed browser IP.

5. Create Your First Project and Secret

1. Sign in to Infisical.
2. Create a Secret Management project.
3. Open the Development environment.
4. Add a test secret such as MY_TEST_SECRET with a harmless test value.
5. Save the secret and confirm that you can reveal it in the web interface.

Do not use real production credentials until you have confirmed your access controls and backup plan.

6. Useful Code Creator Commands

Command	Purpose
codecreator-infisical-url	Display the current secure Infisical URL.
codecreator-infisical-status	Show container status and application health.
codecreator-infisical-restart	Restart the Infisical application stack.
codecreator-infisical-backup	Create a protected local backup.
codecreator-infisical-help	Display the installed helper commands.
codecreator-infisical-refresh-ip	Manually refresh the public IP and HTTPS configuration if needed.
codecreator-infisical-setup	Authorize the current SSH source IP for browser access.

7. Backups and Recovery Material

Create a backup before upgrades or major configuration changes:

codecreator-infisical-backup

Backups are stored in:

/var/backups/codecreator-infisical

Each backup contains the PostgreSQL database, the Docker Compose configuration, and the instance specific Infisical application environment file. The environment file contains sensitive encryption and authentication material. Store backup archives securely and copy important backups off the instance.

The Infisical encryption key is required to decrypt restored secrets. Do not replace the generated encryption key during normal operation. A database restore must use the matching encryption key from the same backup set.

8. Security Notes

- SSH password authentication is disabled. Use your AWS EC2 key pair.
- Root SSH login is disabled.
- PostgreSQL port 5432 and Redis port 6379 are not exposed publicly.
- Infisical is proxied through Nginx using HTTPS.
- Unique Infisical encryption, authentication, PostgreSQL, and Redis secrets are generated on first boot.
- The HTTPS certificate is automatically renewed. If the EC2 public IPv4 address changes after stop and start, the server automatically refreshes the URL and certificate.
- Rotate the application secrets that you store in Infisical according to your organization policy. Infisical supports secret rotation for supported integrations.

9. Health and Troubleshooting

Start with the status helper:

```
codecreator-infisical-status
```

If the application needs a clean restart:

```
codecreator-infisical-restart
```

To view the Infisical container logs:

```
sudo docker logs --tail 100 cc-infisical
```

To view the first boot log:

```
sudo tail -100 /var/log/codecreator-infisical-firstboot.log
```

If the public IP changed and the URL does not update automatically:

```
codecreator-infisical-refresh-ip
```