



Terraform Enterprise Architecture Deep Dive

Stand Alone

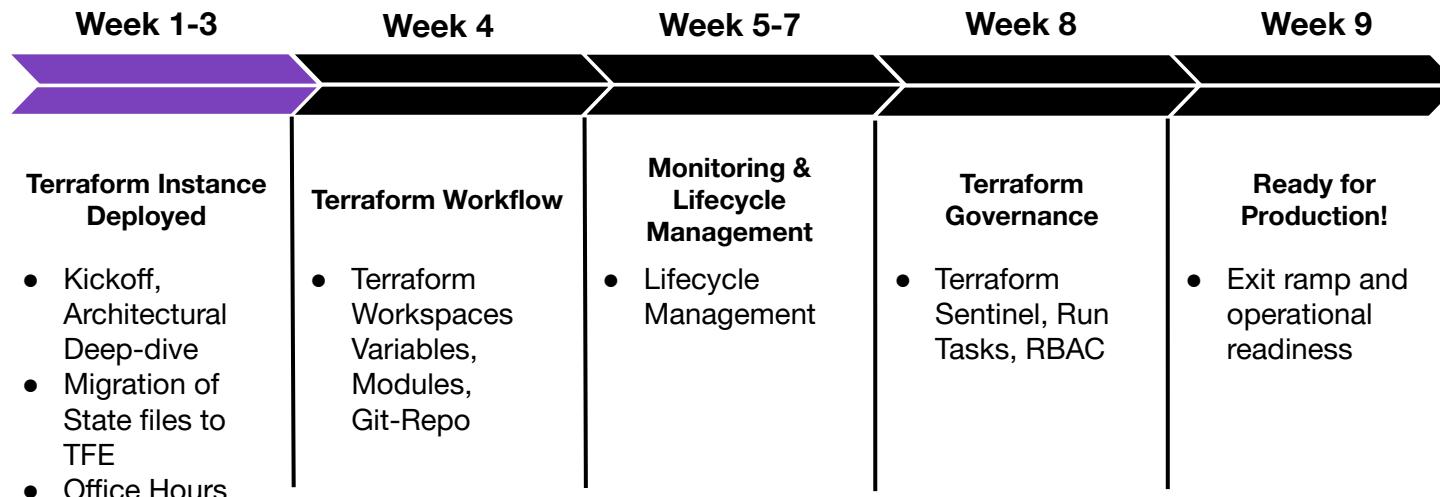
April 2022



Agenda

- **Architecture**
- **Deployment Patterns**
- **Configuration**
- **Next Steps**
- **Q & A**

Terraform Enterprise Path to Production



Reference Architecture



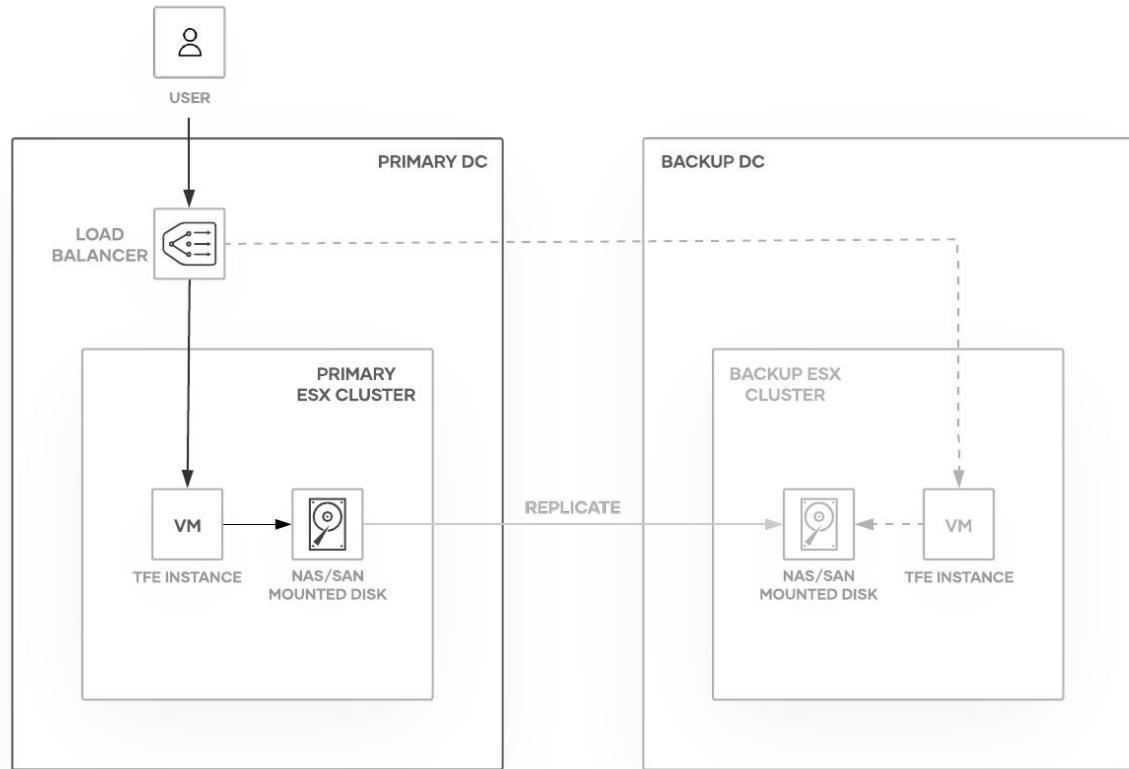


Architecture

- Terraform is an **Infrastructure as Code (IaC)** system that enables companies to define their cloud resources as **HashiCorp Configuration Language (HCL)**.
- HCL code can be stored in a Git repo to provide Version Control and **Auditing**. Git can also be used to **trigger automation**.
- **Terraform Enterprise (TFE)** is a self-managed service, unlike Terraform Cloud.
 - Includes remote runners called '**Cloud Agents**', that can be deployed both on-prem and across multiple cloud providers.
 - Uses **S3**-compatible storage, **Postgres** and **Replicated** for licensing.

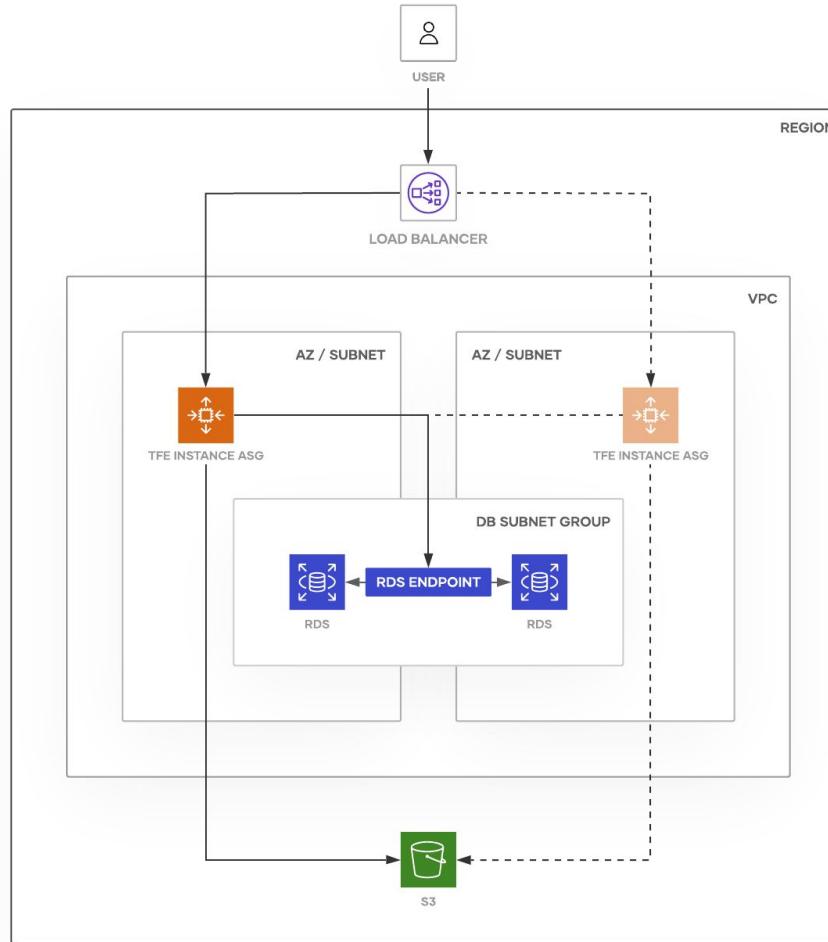


VMware Standalone, Reference Architecture (Recommended)





Cloud Provider Standalone, Reference Architecture (Recommended)



Pre-Deploy Requirements



OS & Software Requirements



Operating System	
Distro	Version
Ubuntu	20.04, 18.04
Debian	11, 10, 9
CentOS	8.x, 7.x
Oracle Linux	8.x, 7.x
Red Hat Enterprise Linux	8.x, 7.x
Amazon Linux	2.0

Software	
Name	Version
Docker CE*	20.x 19.x
containerd.io	containerd 1.4.9 (2021-07-29) containerd 1.5.5 (2021-07-29) or newer
runc	runc v1.0.0-rc93 (2021-02-03) or newer
PostgreSQL	10.x, 11.x, 12.x

Note: Docker CE is not vendor supported on Red Hat Enterprise Linux and Oracle Linux
<https://www.terraform.io/docs/enterprise/before-installing/rhel-requirements.html#install-requirements>

VMware Recommended Sizing



TFE Server (vSphere and vRealize)					
Type	CPU Sockets	CPU Cores	Memory	Storage	Storage (Mounted Disk Volume)
Minimum	2	4	16 GB RAM	40GB	200GB
Scaled	2	8	32 GB RAM	40GB	200GB
PostgreSQL Database (External Services)					
Type	CPU Sockets	CPU Cores	Memory	Storage	
Minimum	2	2 cores	8 GB RAM	50GB	
Scaled	2	4-8 cores	16-32 GB RAM	50GB	

Cloud Recommended Sizing



TFE Server						
Type	CPU	Memory	Storage	AWS	Azure	GCP
Minimum	4 core	16 GB RAM	50GB	m5.xlarge	Standard_D4_v4	N1-standard-4 (200GB Storage)
Scaled	8 core	32 GB RAM	50GB	m5.2xlarge	Standard_D8_v4	N1-standard-8 (200GB Storage)
PostgreSQL Database						
Type	CPU	Memory	Storage	AWS	Azure	GCP
Minimum	4 core	16 GB RAM	50GB	db.m4.xlarge	GP_Gen5_4	Custom PostgreSQL Production
Scaled	8 core	32 GB RAM	50GB	db.m4.2xlarge	GP_Gen5_8	Custom PostgreSQL Production

<https://www.terraform.io/docs/enterprise/before-installing/reference-architecture/aws.html>
<https://www.terraform.io/docs/enterprise/before-installing/reference-architecture/azure.html>
<https://www.terraform.io/docs/enterprise/before-installing/reference-architecture/gcp.html>



Network Requirements (Egress)

Online Installations

- *.replicated.com
- *.quay.io
- quay-registry.s3.amazonaws.com
- *.cloudfront.net
- *.docker.com
- *.docker.io
- *.terraform.io
- releases.hashicorp.com

TFE also needs Egress access to:

- Any VCS servers/services that will be utilized
- Login/authentication servers if SAML will be configured (ADFS, Okta, etc)
- The various cloud API endpoints that will be managed with Terraform
- Any other third party services that will either be integrated with the TFE server or managed with it.

Cost Estimation APIs

When Cost Estimation is enabled, it uses the respective cloud provider's APIs to get up-to-date pricing info.

- api.pricing.us-east-1.amazonaws.com
- cloudbilling.googleapis.com
- prices.azure.com



Network Requirements (Ingress)

Source - User/Client/VCS

- **80:** Terraform Enterprise application access (HTTP; redirects to HTTPS)
- **443:** Terraform Enterprise application access (HTTPS)
- VCS Web Hooks are inbound. If you intend to use VCS integration with a cloud hosted VCS, you'll need to expose TFE on the public internet.

Source - Administrators

- **22:** SSH access (administration and debugging)
- **8800:** Replicated (TFE setup dashboard, HTTPS)

Network Requirements (TLS Certificates)



Trusted

Prior to installation determine the hostname and generate a certificate that will be used during installation. Using an IP to access TFE is not supported.

- If using on prem VCS, then the cert could be signed by your own root authority.
- If using SaaS VCS, then you'll need a publicly trusted cert.

Self-signed

Don't do it! It will be more trouble in the long run.

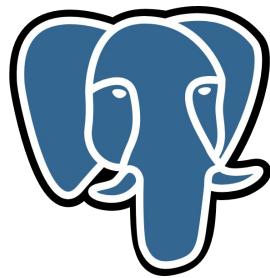
Load Balancer / WAF: TLS Offload / Inspection

Ensure you re-encrypt the traffic and still use a trusted cert on the origin servers.

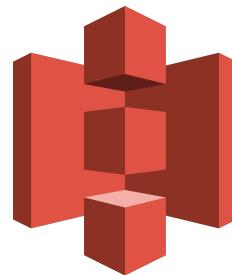
Components



External Services



Postgres



S3 Storage

Replicated



Replicated is an external vendor that HashiCorp uses to manage licensing of Terraform Enterprise, and as a scheduler to manage Docker containers.

Customers should not interact with Replicated directly unless directed by support.

Terraform - Services



- **ptfe_nginx** - Nginx reverse proxy, facilitates access to the Terraform Enterprise services
- **ptfe_atlas** - The API and Web UI. Terraform Enterprise used to be known as Atlas
- **ptfe_build_manager** - Manages the queue of Terraform runs
- **ptfe_build_worker** - Creates workers on-demand as required by the queue. Injects variables, secrets, and Terraform configuration to a temporary container, **ptfe_worker**
- **ptfe_worker** - Executes a Terraform **plan** or **apply**. This container can be replaced with a custom image. This ephemeral container may be created with a randomly generated name by Docker

Operational Modes





Operational Modes

- Demo Mode
- Mounted Disk **
- External Services
- Active/Active

*** Recommended Operational Mode*



Demo Mode

Not supported nor recommended for Production use

- Ephemeral
- Low Capacity
- Single Region
- Self-contained
- Easy to set up manually
- Good for Non-Production Local Testing
- Single Docker instance for Postgres, S3 Storage



Mounted Disk

Production supported
(Recommended for VMWare)

- Good for Production workloads
- Long-Lived
- Single Region
- Self-contained
- Easy to set up manually
- High Availability (HA) / Disaster Recovery (DR) with cold standby
- Single Docker instance for Postgres, S3 Storage



Standalone External Services

- Good for high Capacity Production Workloads
- Single Region
- Needs automation to set up quickly
- Uses externally running Postgres, S3 Storage
- High Availability (HA) / Disaster Recovery (DR) with cold standby



Active/Active

- High Availability (HA)
- Disaster Recovery (DR)
- Single Region
- Needs automation to set up quickly, with twice the hardware
- Good for Production Workloads with fast MTTR, RTO, RPO
- Uses externally running Postgres, S3 Storage, and Redis

Deployment Patterns





Deployment Patterns

- Online
- Airgapped



TERMINAL

```
$ echo "Installing with internet access"
$ curl -o install-TFE.sh
https://install.terraform.io/TFE/stable
$ sudo bash install-TFE.sh
[... time passes ...]

To continue the installation, visit the following URL
in your browser:

https://<this\_server\_address>:8800
```



Online Installation



Airgapped Installation

Running Terraform Enterprise within an Airgapped Environment includes a variety of manual configuration and management processes.

TERMINAL

```
$ echo "Installing with Airgap file"  
$ apt install docker -y  
$ wget  
https://install.terraform.io/airgap/latest.tar.gz  
$ echo "SCP the .airgap file onto the machine"  
$ tar xzf replicated.tar.gz  
$ sudo ./install.sh airgap  
[... time passes ...]  
To continue the installation, visit the following URL  
in your browser:  
https://<this\_server\_address>:8800
```

Automated Installation



Replicated Settings

The initial replicated configuration of the dashboard password, TLS certificates, license file, and application settings can be defined in `/etc/replicated.conf`.

Replicated automatically checks this location during execution of the installer.

Application Settings

The configuration of TFE can be completed by passing a JSON formatted settings file during the installation. This is supported for both online and airgapped installations.

Initial User Creation

After installation an initial admin user must be created to use TFE. This is normally created in the UI however we can leverage the API to create this user.



Automated Installation

Replicated Settings

TERMINAL

```
{  
    "DaemonAuthenticationType": "password",  
    "DaemonAuthenticationPassword": "your-password-here",  
    "TlsBootstrapType": "server-path",  
    "TlsBootstrapHostname": "server.company.com",  
    "TlsBootstrapCert": "/etc/server.crt",  
    "TlsBootstrapKey": "/etc/server.key",  
    "BypassPreflightChecks": true,  
    "ImportSettingsFrom":  
        "/path/to/application-settings.json",  
    "LicenseFileLocation": "/path/to/license.rli"  
}
```



A screenshot of a dark-themed code editor window titled "CODE EDITOR". The editor displays a single file containing Terraform configuration code. The code defines a resource block with several key-value pairs: "hostname", "installation_type", and "capacity_concurrency".

```
{  
  "hostname": {  
    "value": "terraform.example.com"  
  },  
  "installation_type": {  
    "value": "poc"  
  },  
  "capacity_concurrency": {  
    "value": "5"  
  }  
}
```



Automated Installation

Application Settings



Automated Installation

Initial admin user creation

```
$ replicated admin --no-tty retrieve-iact > iact.txt
$ curl payload.json
{
  "username": "admin",
  "email": "it@mycompany.com",
  "password": "thisisabadpassword"
}
$ curl --header "Content-Type: application/json" \
  --request POST --data @payload.json \
  https://TFE.company.com/admin/initial-admin-user?token=$(cat
  iact.txt)
{
  "status": "created",
  "token":
  "aabbcdd.v1.atlas.ddeeffgghhijjkllmmnnooppqqrrssttuuvvxyyzz"
}
```

TERMINAL

Configuration



The screenshot shows a web browser window with a title bar and a main content area. The content area has a heading 'HTTPS for admin console' and a paragraph explaining the current use of a self-signed TLS certificate. Below this is a section titled 'Provide Custom SSL Certificate' with fields for Hostname, Private Key, and Certificate, each with a 'Choose file' button. A note below the fields states that files will be uploaded directly to the management server. At the bottom are two buttons: 'Use Self-Signed Cert' (orange) and 'Upload & Continue' (green).

HTTPS for admin console

We're currently using a self-signed TLS certificate to secure the communication between your browser & the management console. If you don't upload your own TLS cert, you'll see a warning about this in your browser every time you access the management console.

Provide Custom SSL Certificate

Hostname (Ensure this domain name resolves to this server & is routable on your network)

Private Key

Certificate

Files will be uploaded directly to the management server & will never leave.
[If your private key and cert are already on this server, click here.](#)



HTTPS Config

Enter hostname and upload private key and certificate



TFE Licensing

Upload .rli file provided in your welcome email

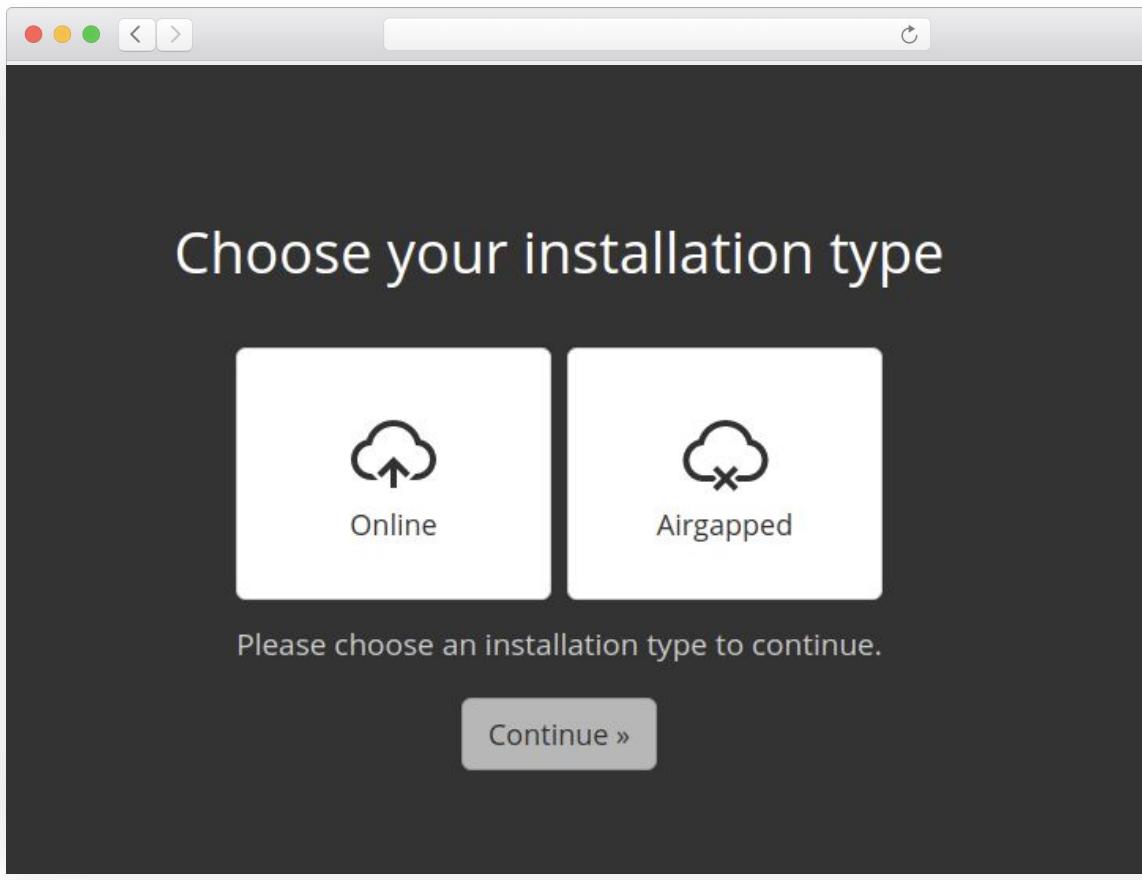
The screenshot shows a dark-themed web page with a header containing window control buttons (red, yellow, green) and back/forward navigation arrows. To the right of the header is a refresh/circular arrow icon. The main content area has a large, bold, white text "Upload your license". Below this, a smaller white text instructs the user to click a button to find and upload their license file, noting that it will have a ".rli" extension. A prominent white button with a folder icon and the text "Choose license" is centered. At the bottom of the page, there is a link labeled "Restore from a snapshot" in a smaller white font.

Upload your license

Click the button below to find and upload your license file.
The file will have a `.rli` extension.

Choose license

Restore from a snapshot



Select Installation Type

Select online or airgapped and the preflight check will begin



Admin Console Auth

Enter password or
configure LDAP.
Anonymous is not
recommended for use in
production deployment

The screenshot shows a window titled "Secure the Admin Console". The window has a standard OS X title bar with red, yellow, and green buttons, and a refresh icon. The main content area contains the title "Secure the Admin Console" and a sub-instruction: "Keeping this admin console secure is important. You can create a shared password that will be required to access the settings, or you can connect it to your existing directory based authentication system." Below this, there are three radio button options: "Anonymous", "Password" (which is selected), and "LDAP". Under each option is a text input field. The "Password" field contains a single character and has a key icon with a dropdown arrow. The "Confirm Password" field is empty. At the bottom is a large green "Continue" button.

Secure the Admin Console

Keeping this admin console secure is important.

You can create a shared password that will be required to access the settings, or you can connect it to your existing directory based authentication system.

Anonymous

Password

LDAP

Password

Confirm Password

Continue

The screenshot shows a Mac OS X-style window titled "Settings". On the left is a sidebar with the following options:

- Hostname
- Encryption Password
- Installation Type
- SSL/TLS Configuration
- Capacity
- Externally Managed Vault
- Terraform Build Worker image
- Backup API Token
- Log Forwarding
- Advanced Configuration

The main content area has three sections:

Hostname

Ensure this domain name is routable on your network.

Hostname:

[Check DNS](#)

Encryption Password

The password used to encrypt and decrypt the internally managed Vault unseal key and root token. Required only when using internally managed Vault.

NOTE: Please be sure to retain the value as it will be needed in the event of a re-installation.

Encryption Password (Required):

Installation Type

What kind of installation is this?

NOTE: You must not change the Installation Type after initial configuration. Doing so will result in data loss: data is not migrated between Installation Types!



Installer Settings

Specify installation type and operation mode.



Installer Settings

Specify installation type and operation mode.

How will you be storing the data generated by the install?

NOTE: You must not change the Production Type after initial configuration. Doing so will result in data loss: data is not migrated between Production Types!

External Services Mounted Disk

Mounted Disk Configuration

Terraform Enterprise will store all the critical state in a path on the host system.
The expectation is that this path is backed by a persistent disk (EBS, SAN, etc).

Path on Host (Required)

SSL/TLS Configuration

This allows you to add custom SSL/TLS data to the install. The most common usage is to add custom certificates to the system, to allow an internal certificate authority (CA) to be trusted.

This is done when you use certificates on your VCS provider and/or Terraform Enterprise installation and thus need Terraform Enterprise to trust services.

Custom Certificate Authority (CA) Bundle

The screenshot shows a web-based configuration interface for Terraform Enterprise. At the top, there's a header bar with a refresh icon and a logo for 'TERRAFORM ENTERPRISE'. Below the header, the main content area has several sections:

- Capacity**: A section for controlling how much work the instance can perform. It includes a note about setting it too high causing instability and two input fields: one for 'Total concurrent Terraform plans and applies' set to 10, and another for 'The maximum amount of memory' set to 256.
- Externally Managed Vault**: A section for configuring an external Vault cluster. It contains a note about documentation and a checkbox for 'Enable Externally Managed Vault'.
- Terraform Build Worker image**: A section for configuring the Docker image used for running Terraform plans and applies. It includes a note about standard vs. custom images and two radio button options: 'Use TFE's standard image' (selected) and 'Provide the location of a custom image'.



Installer Settings

Specify installation type and operation mode.



Installer Settings

Click save and the installer will configure deploy the TFE docker containers and start the app.

The screenshot shows a web-based configuration interface for a 'Terraform Build Worker image'. At the top, there are standard OS X window controls (red, yellow, green buttons, close, minimize, maximize) and a refresh icon. The main title is 'Terraform Build Worker image'. Below the title, a descriptive text states: 'Configure which docker image will be used when running terraform plans and applies. This can either be the standard image that ships with PTFE or a custom image that includes extra tools not present in the default one.' There are two radio button options: ' Use TFE's standard image' and ' Provide the location of a custom image'. A section titled 'Advanced Configuration' follows, with a note: 'These are advanced configuration options that should not be changed without the direction of HashiCorp support personnel.' Under this section, there is a checked checkbox labeled ' Enable Metrics Collection' with a explanatory text below it: 'Collected metrics are used by HashiCorp support to diagnose performance issues and help customers tune behavior.' Another section is labeled 'Initial Admin Creation Token Subnets' with a text input field. Below it, a note explains: 'To automate the creation of the initial admin user, customers can retrieve a special token (called the IACT) that can be exchanged with another API to create the admin user. By default no subnet list is defined and thusly this feature is disabled, but can be configured to allow access from a list of subnets (cidr masks separated by commas). For example: 10.0.1.0/24,172.16.4.0/24.' A final section is 'Initial Admin Creation Token Time Limit' with a text input field containing the value '60'. A note below it states: 'To prevent an unconfigured instance from being discovered and hijacked by a rogue operator, ips from the above subnet list are only allowed to access the retrieval API for a certain initial period of time. This setting defines that time period in minutes. Setting this to *unlimited* will disable the time limit.' At the bottom right is a blue 'Save' button.

Terraform Build Worker image

Configure which docker image will be used when running terraform plans and applies. This can either be the standard image that ships with PTFE or a custom image that includes extra tools not present in the default one.

Use TFE's standard image Provide the location of a custom image

Advanced Configuration

These are advanced configuration options that should not be changed without the direction of HashiCorp support personnel.

Enable Metrics Collection

Collected metrics are used by HashiCorp support to diagnose performance issues and help customers tune behavior.

Initial Admin Creation Token Subnets

To automate the creation of the initial admin user, customers can retrieve a special token (called the IACT) that can be exchanged with another API to create the admin user. By default no subnet list is defined and thusly this feature is disabled, but can be configured to allow access from a list of subnets (cidr masks separated by commas). For example: 10.0.1.0/24,172.16.4.0/24.

Initial Admin Creation Token Time Limit

60

To prevent an unconfigured instance from being discovered and hijacked by a rogue operator, ips from the above subnet list are only allowed to access the retrieval API for a certain initial period of time. This setting defines that time period in minutes. Setting this to *unlimited* will disable the time limit.

Save

Resources





Resources

- Reference Architecture
 - [AWS / Azure / GCP](#)
 - [VMware](#)
- Pre-deploy Requirements
 - [OS Requirements](#)
 - [Software Requirements](#)
 - [Network Requirements](#)
 - [Certificates](#)
- Components
 - [Services & Data Flow Diagram](#)
 - [Terraform Enterprise Containers](#)
- [Operational Modes](#)
- Deployment Patterns
 - Online
 - [Airgapped](#)
 - [Interactive Installation](#)

Next Steps



The screenshot shows a web browser window with the HashiCorp logo and "Discuss" tab selected. The main content area displays a list of topics under the "HashiCorp Cloud Platform (HCP)" category. Each topic card includes a thumbnail, title, author, replies, views, and activity date.

Topic	Replies	Views	Activity
About the HashiCorp Cloud Platform (HCP) category HashiCorp Cloud Platform (HCP)	1	387	May 24
HCP Vault "per-client" pricing HCP Vault	0	39	9d
Failing to use HCP Consul as my terraform backend HashiCorp Cloud Platform (HCP)	1	72	12d
Does HCP support Automation APIs in AWS HashiCorp Cloud Platform (HCP) vault	0	73	27d



Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers.

discuss.hashicorp.com

Learn



Step-by-step guides to accelerate deployment of Terraform

The screenshot shows a web browser window for HashiCorp Learn. The left sidebar lists several 'Enterprise Patterns' including 'Module Creation - Recommended Pattern', 'Terraform Enterprise Backup - Recommended Pattern' (which is currently selected), 'Forward Terraform Enterprise Logs to Datadog', and 'Use hcdiag with Terraform'. The main content area displays the 'Terraform Enterprise Backup - Recommended Pattern' tutorial. It features a '28 MIN' duration indicator, a 'PRODUCTS USED: Terraform' section, and a detailed description of the importance of reliable backups for business continuity. It also mentions the extension of the guide from the 'Backup & Restore documentation' and provides specific details about its relevance to single-region, multi-availability zone External Services mode deployments.

HashiCorp Learn

Browse tutorials ▾

Search

Sign in

Terraform

Enterprise Patterns

- Module Creation – Recommended Pattern
- Terraform Enterprise Backup – Recommended Pattern**
- Forward Terraform Enterprise Logs to Datadog
- Use hcdiag with Terraform

Jump to section ▾

Docs Forum Bookmark

ENTERPRISE

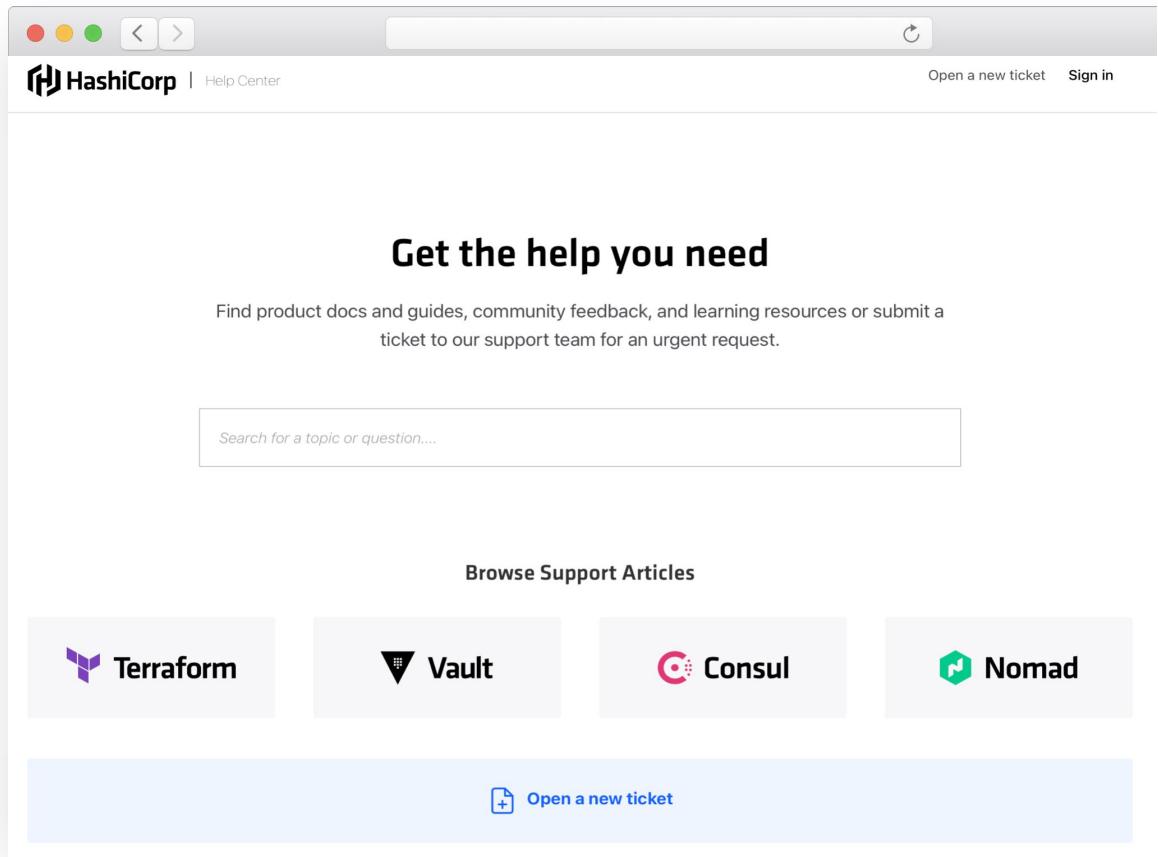
Terraform Enterprise Backup - Recommended Pattern

28 MIN PRODUCTS USED: Terraform

Many business verticals require business continuity management (BCM) for production services. A reliable backup of your Terraform Enterprise deployment is crucial to ensuring business continuity. The backup should include data held and processed by Terraform Enterprise's components so that operators can restore it within the organization's Recovery Time Objective (RTO) and to their Recovery Point Objective (RPO).

This guide extends the [Backup & Restore documentation](#), which contains more technical detail about the backup and restore process. This guide discusses the best practices, options, and considerations to back up Terraform Enterprise and increase its resiliency. It also recommends redundant, self-healing configurations using public and private cloud infrastructure, which add resilience to your deployment and reduce the chances of requiring backups.

Most of this guide is only relevant to single-region, multi-availability zone External Services mode deployments except where otherwise stated. Refer to [Backup a Mounted Disk Deployment](#) section below for specific details if you



A screenshot of a web browser showing the HashiCorp Support Center. The page has a light gray header with the HashiCorp logo and "Help Center" text. On the right, there are links for "Open a new ticket" and "Sign in". Below the header, a large section features the text "Get the help you need" and a subtext about finding product docs, guides, community feedback, and learning resources or submitting a ticket. A search bar is present with the placeholder "Search for a topic or question....". Below the search bar, there's a section titled "Browse Support Articles" with four categories: Terraform, Vault, Consul, and Nomad. At the bottom, a blue button says "Open a new ticket" with a plus sign icon.

HashiCorp | Help Center

Open a new ticket Sign in

Get the help you need

Find product docs and guides, community feedback, and learning resources or submit a ticket to our support team for an urgent request.

Search for a topic or question....

Browse Support Articles

Terraform

Vault

Consul

Nomad

Open a new ticket



Support

<https://support.hashicorp.com>

Need Additional Help?



Customer Success

Contact our Customer Success Management team with any questions. We will help coordinate the right resources for you to get your questions answered.

customer.success@hashicorp.com

Technical Support

Something not working quite right? Engage with HashiCorp Technical Support by opening a new ticket for your issue at support.hashicorp.com.

Q & A



Upcoming Onboarding Webinars



May 5, 2022

Importing Resources and State into Terraform Enterprise

Learn Best Practices for
importing resources into
Terraform State and moving
Terraform OSS into Enterprise.

May 10, 2022

Community Office Hours

An interactive open forum to
discuss specific questions about
your environment and Use
Cases. Please bring your
questions.

May 17, 2022

Lifecycle Management

Learn Best Practices for
monitoring, upgrades, and
backups in Terraform Enterprise.



Thank You

hello@hashicorp.com
www.hashicorp.com