# Terraform Enterprise Guided Documentation

HashiCorp

The HashiCorp Customer Success Team has created this document to augment the content presented in the Enterprise Onboarding Program and questions asked in the Production Readiness Checklist. This guide is a starting point for reviewing your installation and environment and creation of a Terraform runbook. This checklist is a collection of suggestions and best practices documents, please use it as a foundation to review your environment and adjust to your business needs, requirements and operating conditions. This document comes with no warranty.

| **Architecture and Infrastructure** |
| --- |
| Is the installation architecture aligned with the reference architecture?<br>• Reference Architecture<br>• Which Operational Mode did you decide on?<br>• Did you decide on an online deployment, or an airgapped one?<br>• If in Active/Active, are the nodes separated across AZs?<br>• Are the nodes sized appropriately in AWS, GCP, Azure, VMWare?<br>• Are you using a supported OS for your nodes? |
| If using External Services, does your Managed Postgres database and S3 storage scale? |
| Are the network ports that are opened aligned with the documentation for an online or airgapped deployment? |
| Are network, load balancer and certificate configurations and firewall openings understood, documented, and known not to change? Does the current documentation / runbook(s) include a topology diagram for all Terraform Enterprise instances & additional resources for External Services/Active Active? |
| Current setup<br>• Are you using any CICD tooling, do you wish to integrate this into TFE. Have you looked at our documentation for CLI based workflows?<br>• Do you intend to use VCS or UI based workflows? Or even API Driven workflows?<br>• How many environments do you intend to have a Terraform Enterprise installation in. We would always advise one smaller setup for testing DR, upgrades, features etc, then one or more instances for running terraform plans and applies on.<br>• What is the approach you will take for IAM, SAML, SSO, AzureAD, ADFS?<br>• Have you looked at the capacity & performance docs, we would advise profiling any large monolithic workspaces you use, breaking them down where possible, failing this |

| |
|---|
| attempting to upscale your workers. As a note, the worker will rarely match your local machines specs and therefore is likely to run slower.<br>• Do you have specific security or monitoring software that needs to be installed on the Terraform Enterprise nodes? Have you looked at the following monitoring guide<br>• Where do you intend to store the Terraform Enterprise Encryption password & database passwords? In a cloud KMS, HashiCorp Vault, other secret solution? |

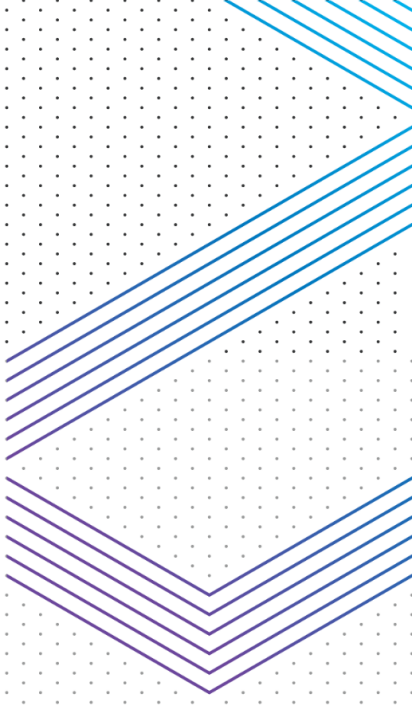
| **Day 2 + operations** |
|---|
| Depending on setup, are you taking:<br>• VM Snapshots<br>• Disk Replication<br>• Database Snapshots<br>• Multi region blob storage backups<br>What is the cadence for those that are relevant to you? Do these follow the RTO/RPO you have for Terraform Enterprise? A very detailed learn guide can be seen here |
| Have you read up on Audit Logging in TFE? Are you using any specific tools already such as Datadog, are you comfortable pushing logs to your own preferred solution? |
| Have you tested that in the event of a catastrophic failure of Terraform Enterprise, logs are still persisted for debugging purposes? |
| Does your company have a specific monitoring tool used across the company? Does your team make use of a specific stack for this? Have you implemented monitoring for the key metrics on the VM and Container? |
| Does the team managing Vault have runbooks and processes for all key operational tasks?<br>• Upgrading Terraform Enterprise<br>• Executing DR failovers in Terraform Enterprise<br>• In event of a failure, creating a new PostgresQL database using a snapshot<br>• In event of a failure, creating a new Terraform Enterprise instance using a snapshot<br>• Rotating any cloud credentials or other secrets needed by Terraform Enterprise workspaces<br>• Adding new users to SSO with correct RBAC permissions<br>• Adding new workspaces or other TFE resources with/without using the TFE terraform provider. |
| Has your team run disaster scenarios testing the above runbooks & processes? |
| More details on Recovery Procedures and Backups & Restores |

| |
|---|
| Have you implemented any cloud agents? |
| Have you connected all VCS systems you plan to? Are there any proposed VCS migrations in the near future which may affect Terraform Enterprise |
| Does your team have a regular cadence to check the Terraform Enterprise releases page? |
| Has your team looked at HCDiag for Terraform Enterprise? |

| **Workspaces & Functionality** |
|---|
| Are you leveraging auto-apply on any workspaces, if so, in which environments? |
| Do you run any terraform testing? Youtube on Snyk & Terraform |
| How do you intend to use modules within your workspaces? |
| Are you intending to pin all module versions, leaving none at “Latest” |
| Do you intend to make use of the private registry for modules or providers? |
| How do you intend to push module upgrades in a safe and secure manner, do you use a particular branching strategy, how many approvals are needed for certain modules, who has the RBAC needed to make these approvals? |
| Have you decided on a workspace naming strategy yet? {region}-{env}-{team}-{use-case} as an example |
| Have you implemented any Sentinel policies yet? |
| Do you want to follow an inner sourcing methodology such that developers outside of your team can contribute to:<br>• Terraform Configurations for resources<br>• Terraform Configurations for Terraform Enterprise Resources (workspaces, teams, permissions etc)<br>• Modules that are centrally managed<br>• Approvals on specific teams Terraform configurations pull requests<br>• Sentinel policy writing |

| **Service Consumption** |
|---|
| Do you intend to allow Developers to have access to your Terraform Enterprise Instance |

| |
|---|
| Are RBAC settings configured for least privilege? |
| Are there any additional teams, such as security or budget teams you intend to involve with the development of Sentinel code? |
| Have you defined standards for resources created in terraform enterprise, a specific tag/tags to be applied to infrastructure to let practitioners know it should not be amended manually |
| Have you discussed how to deal with cleaning up un-used Terraform Enterprise resources, if a workspace was created but never used, if resources were built for a PoC and never cleaned up etc. |
| Do you have a specific RPO/RTO you need to be following? Are your snapshot cadences and backup & recovery processes aligning to this? |
| Do you intend to provide an SLA for practitioners using your Terraform Enterprise instance? Expected uptimes and downtimes etc. |



USA Headquarters

101 Second St., Suite 700, San Francisco, CA, 94105
www.hashicorp.com