Terraform Enterprise Installation and As-Built Documentation

Contact:
Ryan Butler, Senior Solutions Architect
Jesse Adelman, Engineer
Jim Raymonds, Project Manager
April 20, 2020

AHEAD
401 North Michigan Ave., Suite 3400
Chicago, IL 60611
312.924.4492 (office)
800.294.5141 (fax)
www.ThinkAHEAD.com

Table of Contents

1. Document Overview 4
1.1. Assumptions 4
1.1.1. Scope 4

2. Firewall Rules 5

3. Infrastructure Services 6
3.1. Hosting Information 6
3.2. Load Balancer (Optional) 6

4. Virtual Machine Information 8
4.1. Appliance Configurations 8

5. Object Storage 9
5.1. Overview 9

6. PostgreSQL Database 10
6.1. Overview 10

7. Passwords 11

8. Terraform Environment Configuration 12
8.1. Overview 12
8.2. Enterprise Licensing 12
8.3. Logging and Reporting 13
8.4. Backup / Recovery 13
8.4.1. Snapshots 13
8.4.2. Azure Backup 13
8.5. Support 14

9. Coding Requirements 15
9.1. Modules Created (Prototypes) 15
9.2. Registry Modules Needed/Used 13
9.3. Sentinel Policy Rules (Prototypes) 15
9.4. Workspaces 16

10. Other Notes 15

11. Recommendations 17

Appendix 18
1. Terraform Enterprise Azure Architecture 18

Table of Tables

Table 1. Firewall Rules 5
Table 2. Infrastructure Hosting Information 6
Table 3. Load Balancer DNS and IP Addresses 6
Table 4. Load Balancer Setup 7
Table 5. VM Configurations 8
Table 6. Object Storage Overview 9
Table 7. PostgreSQL Database 10

Table 8. Passwords 11
Table 9. Terraform Infrastructure Services 13
Table 10. Logging and Reporting Tools and Configurations 13
Table 11. Azure Backup Configurations 13
Table 12. Support Contacts 14
Table 13. Custom Modules 15
Table 14. Registry Modules 15
Table 15. Sentinel Policy Rules (Prototypes) 15
Table 16. Dev Workspace Information 16
Table 17. Staging Workspace Information 16
Table 18. Production Workspace Information 16

Development Log

Version	Date	Description
v1	3/11/2020	Initial draft completed by Advantasure (Gunjan Pujara)
v2	4/17/2020	Updated with current deployment/configuraiton details

1. Document Overview

This document is produced by AHEAD as part of the *Terraform Enterprise Deployment* service and will be used to guide the deployment. Once the deployment is complete, this document will be updated with actual configurations and become the As-Built Documentation for this Service.

1.1. Assumptions

- There are no host or network firewall services (iptables, firewalls) configured that would impede communication between devices and services. Firewalld is disabled. SELINUX is in Permissive mode.
- A public DNS name has been created, pointing to a Public IP address.
- An appropriate TLS certificate is available, from a public Certificate Authority.
- A Git-based repository is available for Sentinel Policies, Workspaces, and CI/CD functions (Azure DevOps, GitHub, etc.).

1.1.1. Scope

Advantasure has engaged AHEAD to assist in developing Infrastructure as Code for their reference architecture. This is part of a business initiative to improve time to delivery and the lifecycle management of resources for the PaaS solution that runs on that reference architecture. AHEAD is proposing a design workshop followed by implementation services to help the Advantasure team to deploy and manage resources to Azure with Terraform Enterprise.

2. Firewall Rules

The following table details the firewall rules needed to interact with TFE.

More information: https://www.terraform.io/docs/enterprise/before-installing/network-requirements.html

Source	Destination	Port	Protocol
Internal	Instance	22	TCP
Internal	Instance (HTTP)	80	TCP
Internal	Instance (HTTPS)	443	TCP
Internal	TFE Load Balancer (HTTP)	80	TCP
Internal and External	TFE Load Balancer (HTTPS)	443	TCP
Internal	TFE Load Balancer (Cluster)	8800	TCP

Table 1. Firewall Rules

Note: The above requirements could change based on the architecture.

3. Infrastructure Services

This section describes the typical components that should already exist in the infrastructure that will be utilized.

Infrastructure Services	
Version of Terraform Enterprise	(Latest Stable Version)
SSL Cert Needed For Console:	Advantasure-provided (*.services.advantasure.com)
Installation Type:	Production
Production Type:	External Services
Automatic TFE Snapshots	Disabled
Update Check	5h
License Sync	10h

Table 9. Terraform Infrastructure Services

3.1. Hosting Information

The following table is used to set up the hosting information:

Infrastructure Services	
DNS Server(s)	10.120.18.5/.5/.7
Domain Name Suffix	services.advantasure.com
NTP Server(s)	(Via DHCP)
Load Balancer	Yes

Table 2. Infrastructure Hosting Information

3.2. Load Balancer (Optional)

The following table defines the Virtual IP addresses and DNS names for load balancers.

Note: The Azure load balancer currently does not support Active/Passive load balancing.

More Information: https://www.terraform.io/docs/enterprise/before-installing/reference-architecture/aws.html#ssl-tls-certificates-and-load-balancers

Load Balancer	DNS Name	IP Address
TFE	terraform.services.advantasure.com	<locally assigned>

Table 3. Load Balancer DNS and IP Addresses

Load Balancer Setup

The load balancer should be set up to manage each of the services and ensure they are healthy. The load balancer setup is typically a customer task. This means the agents can just use “terraform.example.com” for their server setup. This also means that to get to the console you can just go to https://terraform.services.advantasure.com and not have to remember different addresses. The load balancer must also be configured with the proper TLS certificates for the hostname.

The following table defines the load balancer setup, if it is chosen:

Service	Load Balancing Method	Health Check	HTTP Code
TFE	Active/Passive	/_health_check	200

Table 4. Load Balancer Setup

Note: These can all be directed to the “Terraform” address for consistency.

4. Virtual Machine Information

4.1. Appliance Configurations

AHEAD bases the following system configurations on HashiCorp's published recommendations and then update/adjust them based on the particular workloads. The following table lists the virtual machine information—the example values are the recommended settings for performance specs (processors/cores, memory, and disk space).

More Information: https://www.terraform.io/docs/enterprise/before-installing/index.html#linux-instance

Terraform (Primary)

Configuration Item	Value
Azure Subscription	VT_SHAREDSERVICES
Azure Resource Group	UNIV_SHARED
Azure Region	US East 2
Azure Virtual Network	Hub.east2.vt1
Azure Subnet	Hub.east2.vt1.univ.jenkins
FQDN	ZULUSHDTRF01C.entcorecloud.com
IP Address	10.120.20.41
Operating System	Red Hat Enterprise Linux 7.7
Host Firewall Enabled	NO, disabled firewalld and SELINUX
Selinux Enabled	NO, disabled SELINUX
Azure VM Size	Standard_D4s_v3
Processor Cores	4
Memory	16
Azure Disk Size	128 GB

Table 5. VM Configurations

5. Object Storage

5.1. Overview

Configuration Item	Value
Azure Storage Account Name	Svtssptrf01s
Azure Subscription	AHEAD
Azure Resource Group	UNIV_SHARED
Location	US East 2
Performance	Standard
Account Kind	StorageV2
Replication	Locally redundant storage (LRS)
Access Tier	Hot
Container Name	Terraform
Azure Type	General Purpose
Azure Processor Cores	4
Azure Storage	100 GB

Table 6. Object Storage Overview

6. PostgreSQL Database

6.1. Overview

Configuration Item	Value
Azure Subscription	AHEAD
Azure Resource Group	UNIV_SHARED
Azure Region	US East 2
Azure PostgreSQL Deployment Option	Single Server
Location	US East 2
PostgreSQL Connection String	(Provided after creation)
PostgreSQL Version	Latest Version 11.x
Azure Type	General Purpose
Azure Processor Cores	4
Azure Storage	100 GB
Azure Subscription	AHEAD

Table 7. PostgreSQL Database

7. Passwords

The following table lists the appliances and passwords used in the implementation. If the passwords are not stored here, then list where they can be found (Vault, CyberArk, etc.)

Account	Type	Username/Holder	Password to be used
Terraform VM's	root	root	Azure Key Vault
Terraform Enterprise Console	Admin	Gunjan Pujara	Azure Key Vault
PostgreSQL Database User	Admin	Gunjan Pujara	Azure Key Vault
VCS Provider	Token	Gunjan Pujara	<OAUTH Token>
Azure Storage Account Key	Key	Azure Key Vault	Azure Key Vault
Azure SPN Account Info	Client ID	Azure Key Vault	Azure Key Vault
Azure SPN Account Info	Client Secret	Azure Key Vault	Azure Key Vault
Azure SPN Account Info	Tenant ID	Azure Key Vault	Azure Key Vault
Azure SPN Account Info	Subscription ID	Azure Key Vault	Azure Key Vault

Table 8. Passwords

Note: If AHEAD is setting up the new VM/instance, **we would need access to the virtualization/console as well, depending on the environment**.

8. Terraform Environment Configuration

8.1. Overview

Terraform Enterprise Design Decisions

User Capacity Requirements:

- 3 workspaces per customer across multi-tiered environments
- Target of 20 customers to be transitioned to TFE after implementation in the next 1 year

Security Requirements:

- SSO
- Enhanced Audit Logging
- Self-Hosted
- Sentinel Policy to be enforced prior to Azure deployment

8.2. Enterprise Licensing

To meet the user workspace and customer capacity requirements, it has been decided that the Terraform Enterprise Essentials Tier will be the licensing model used. This will allow for multi-team collaboration and will support the planned user capacity.

During design conversations we verified that 3 workspaces per customer will likely be needed for different tiered environments, but this could include up to 5 or more workspaces for some customers. Assuming 20 customers may be transitioned to Terraform infrastructure as code over the next several months, we anticipate that the current plan of 100 workspaces will be sufficient for the foreseeable future.

The TFE Essentials Tier supports the following:

- 100 Terraform Workspaces (minimum buy-in)
- Sentinel Policy as Code
- SSO integration
- HashiCorp support

8.3. Logging and Reporting

This section documents what logging tools will be used and any configurations that might need to be set up.

More Information: https://www.terraform.io/docs/enterprise/admin/logging.html

Logging tools	TFE Monitoring
Reporting Destination	Local filesystem
Syslog Location	N/A
Syslog Endpoint	N/A
Implementation Details	Docker container logs: • tail -f /var/lib/docker/containers/*/*.log • docker logs <containername> # See output from 'docker ps' for <containername> Some application logs sent to: • /var/log/messages

Table 9. Logging and Reporting Tools and Configurations

8.4. Backup / Recovery

8.4.1. Snapshots

This section is about how the backup snapshots will be configured to safeguard the Terraform Enterprise Environment.

More Information: https://www.terraform.io/docs/enterprise/admin/automated-recovery.html

Backup Destination	N/A
Max Number Snapshots	N/A
Snapshot Timeout	N/A
Automatic Snapshots	N/A
Automatic Snapshot Interval	N/A

8.4.2. Azure Backup

This section covers the backup of the Azure VM Instances.

Recovery Services Vault	VTPSHRDSERVICES01
Azure Resource Group	UNIV_SHARED
Backup Policy	H1-D30-W26-M12-Y10
Backup Frequency	Daily at 1:00 AM EST
Backup Retention Days	Daily Backup – 30 Days Weekly Backup – 26 Weeks

Table 10. Azure Backup Configurations

8.5. Support

This table lists name and contact for people responsible for supporting the environment; AHEAD recommends at least two people be identified in case one is not available. AHEAD will work with these people to ensure they know how to open support calls/tickets and to ensure any pre-creation of accounts or access is taken care of.

Support Link: https://support.hashicorp.com/hc/en-us

Name	Email
Gunjen Pujara	Gunjan.Pujara@advantasure.com
Alan O'Connor	Alan.O'Connor@advantasure.com

Table 11. Support Contacts

9. Coding Requirements

9.1. Modules Created (Prototypes)

These are custom modules that AHEAD will develop for Advantasure based on their specific requirements.

More information: https://www.terraform.io/docs/modules/index.html

Module Name	Description
azure-linux-virtualmachine	Deploy Azure VM based on variable criteria
azure-virtualnetwork	Deploy Azure Virtual Network and reslated objects based on variable criteria

Table 12. Custom Modules

9.2. Sentinel Policy Rules (Prototypes)

Policies are used to determine the rights of users and what actions they can perform.

More information: https://www.terraform.io/docs/cloud/sentinel/index.html

Name	Description
enforce-mandatory-tags	Check for, and optionally require, the presence of specific tags on resources
restrict-vm-size	Check for, and optionally require, a subset of available Virtual Machine ‘size’s

Table 13. Sentinel Policy Rules (Prototypes)

9.3. Workspaces

Workspaces are how Terraform Enterprise organizes the modules for deployment. They contain things like the VCS info, any variables used for this particular environment/configuration, some persistent stored state, and historical run information.

More information:

Workspaces Overview: https://www.terraform.io/docs/cloud/workspaces/index.html

Workspaces Naming: https://www.terraform.io/docs/cloud/workspaces/naming.html

Dev Workspace	
Name	infrastructure-dev
Exec Mode	Remote
Apply Method	Automatic
TF Version	0.12.20
Working Directory	terraform/
Team Access Name	Owners
Team Access Privs	default
VCS Connection	Azure VCS

Table 14. Dev Workspace Information

Staging Workspace	
Name	infrastructure-staging
Exec Mode	Remote
Apply Method	Manual
TF Version	0.12.20
Working Directory	terraform/
Team Access Name	Owners
Team Access Privs	default
VCS Connection	Azure VCS

Table 15. Staging Workspace Information

Production Workspace	
Name	infrastructure-production
Exec Mode	Remote
Apply Method	Manual
TF Version	0.12.20
Working Directory	terraform/
Team Access Name	Owners
Team Access Privs	default
VCS Connection	Azure VCS

Table 16. Production Workspace Information

10. Recommendations

Any recommendations for after the engagement:

- Begin to involve all technical/engineering departments in Terraform Enterprise Workspaces and Sentinel policy development
- Ensure that development branches are valid representations of production environments
- Automate everything!
- Integrate security scans and security policy validations into Terraform workflows (most appropriately via Sentinel, but also via other mechanisms)
- Identify Terraform Public Module Registry modules that can be used and extended – don't reinvent the wheel
- Establish Service Level Objectives and Service Level Agreements, Error Budgets for services internally, and with Advantasure's customers/clients
- Hook up docker/application logs (and OS logs) to searchable log aggregation system
- Continue work to make true production-ready deployments from the prototype Terraform code here created

Appendix

1. Terraform Enterprise Azure Architecture

The following diagram depicts a typical logical architecture:

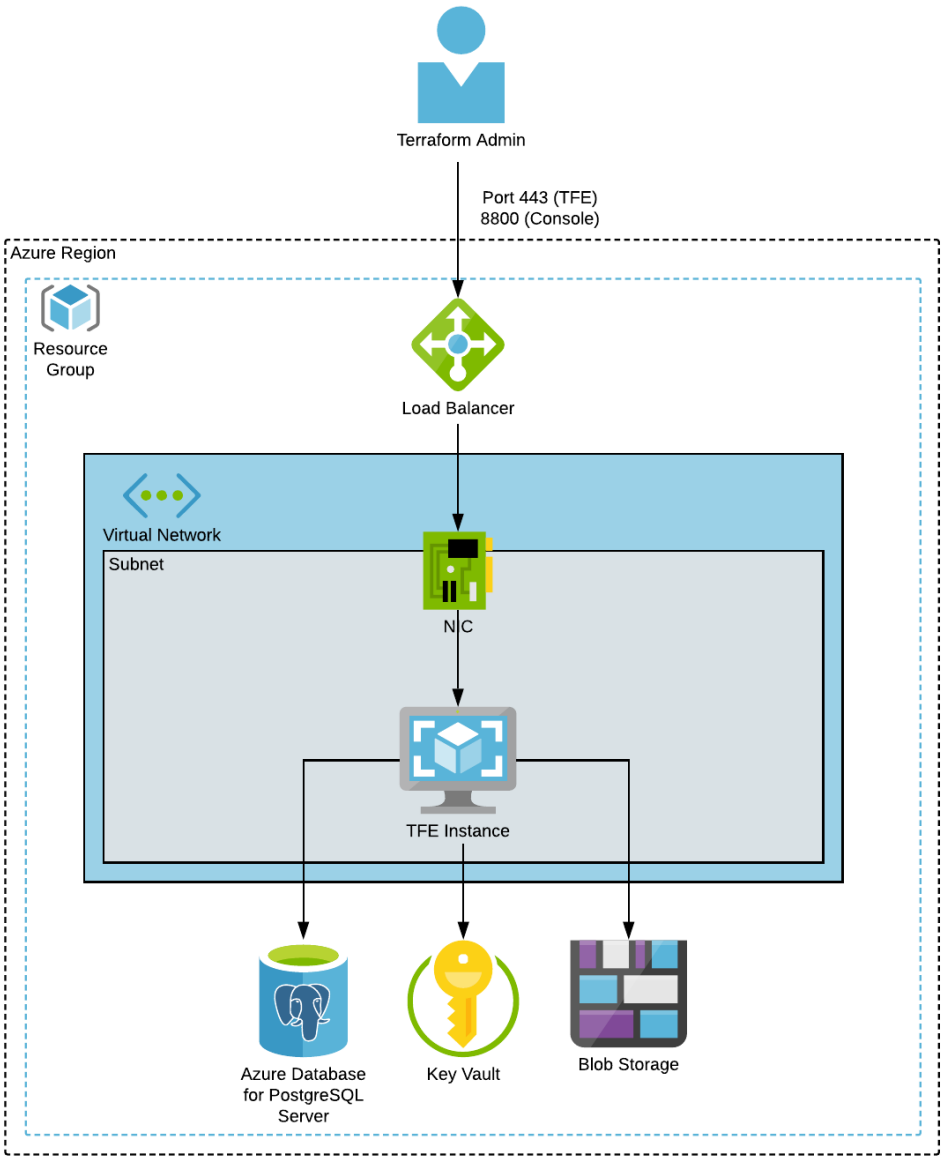

Figure 1. Typical Terraform Enterprise Logical Architecture

1.1. Example CI\CD Pipeline

The following diagram depicts a pipeline utilizing Terraform with separate repositories for application and infrastructure code.

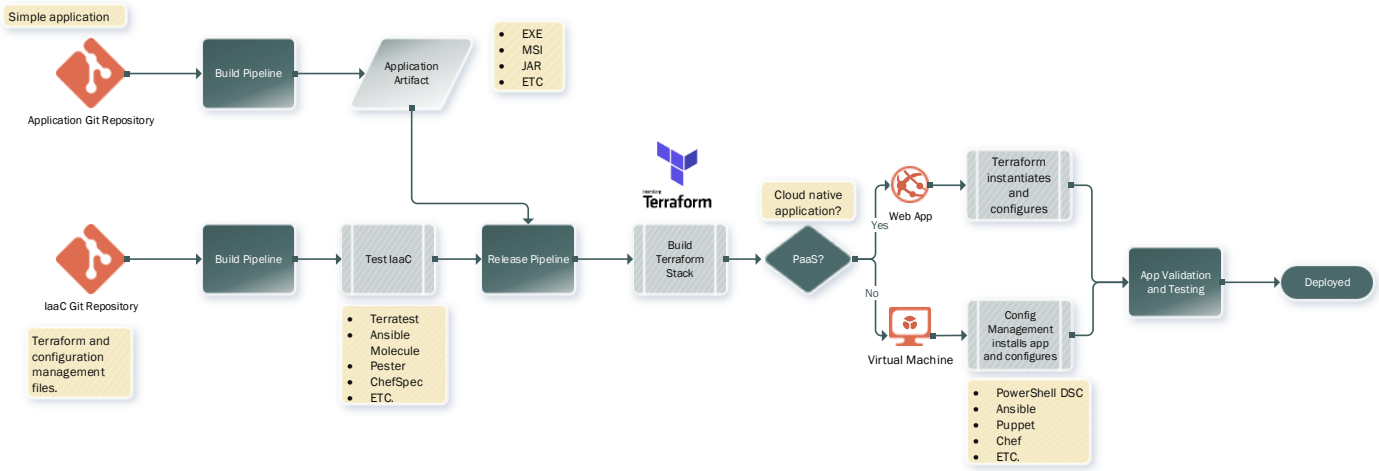

Figure 2. Example CI/CD Pipeline Using Terraform

1.2. Example DevOps Reference Architecture

The following diagram depicts a full CI\CD reference architecture and how Terraform fits in.

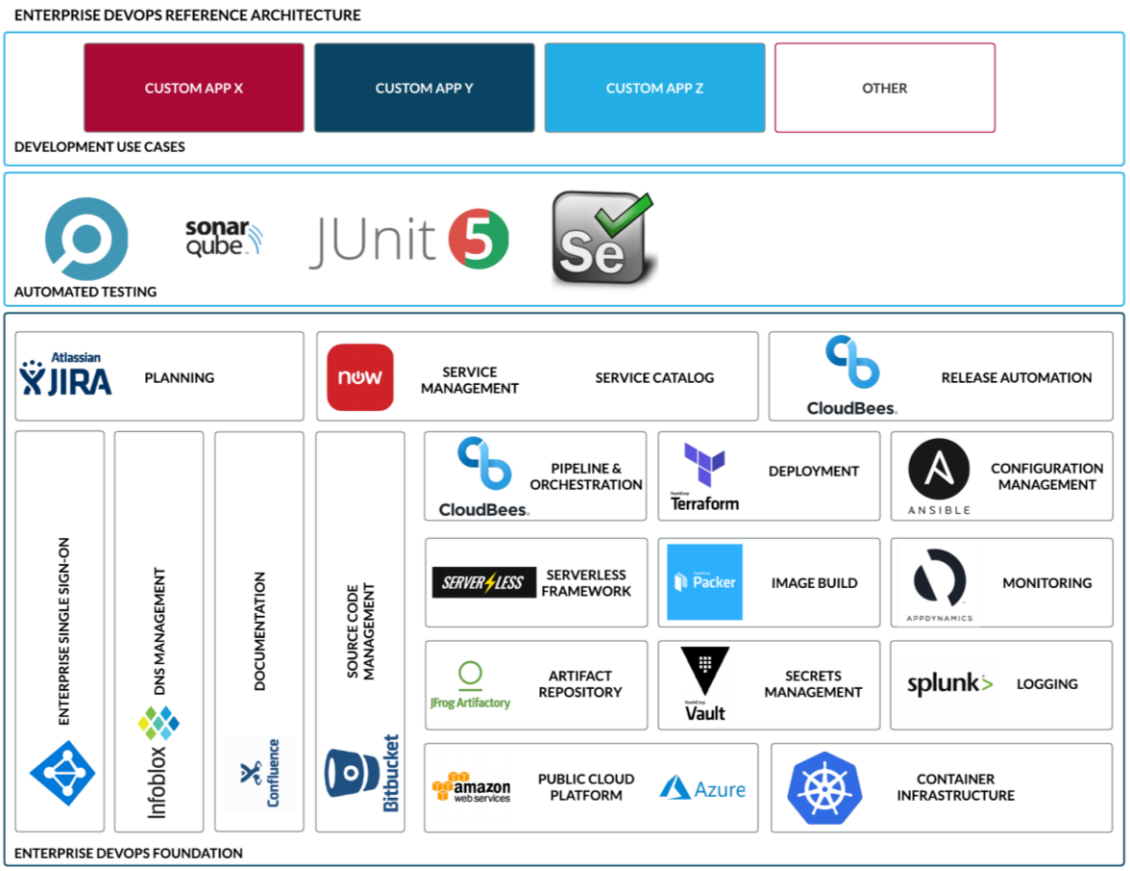

Figure 3. Enterprise Reference Architecture