HashiCorp Vault on the AWS Cloud

Quick Start Reference Deployment

November 2016
(last update: June 2020)

Daniel Callao, HashiCorp, Inc.
Andrew Gargan, Amazon Web Services

Visit our GitHub repository for source files and to post feedback, report bugs, or submit feature ideas for this Quick Start.

Contents

This Quick Start deployment guide was created by Amazon Web Services (AWS) in collaboration with HashiCorp, Inc.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying HashiCorp Vault on the AWS Cloud. Quick Starts are automated reference deployments that use AWS CloudFormation templates to launch, configure, and run the AWS compute, network, storage, and other services required to deploy a specific workload on AWS.

HashiCorp Vault on AWS

HashiCorp Vault is a product that centrally secures, stores and tightly controls access to tokens, passwords, certificates, encryption keys, protecting secrets and other sensitive data through a user interface (UI), a command line interface (CLI), or an HTTP application programming interface (API). Vault's core use cases include the following:

- Secrets management: Securely manage and deploy secrets across different environments, applications, and services.
- Encryption and data protection: Manage encryption and keys for developers and operators across different environments, applications, and services.
- Privileged-access management: Secure workloads for application-to-application and user-to-application credential management across different environments and services.

Vault is designed for DevOps professionals and application developers who want to manage their secrets, data, and key-value stores. It's built using the open-source version of Vault, but it's also compatible with Vault Enterprise.

Supplemental details, with instructions and screenshots, are available on the HashiCorp Vault and Vault Enterprise websites.

Please know that we may share who uses AWS Quick Starts with the AWS Partner Network (APN) Partner that collaborated with AWS on the content of the Quick Start.

Cost and licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, affects the cost of deployment. See the pricing pages for each AWS service you use.

This Quick Start uses the open-source version of HashiCorp Vault, which does not require a license.

Architecture

Deploying this Quick Start with the **default parameters** builds the following Vault environment in its own virtual private cloud (VPC). For more information, see Building a Modular and Scalable Virtual Network Architecture.

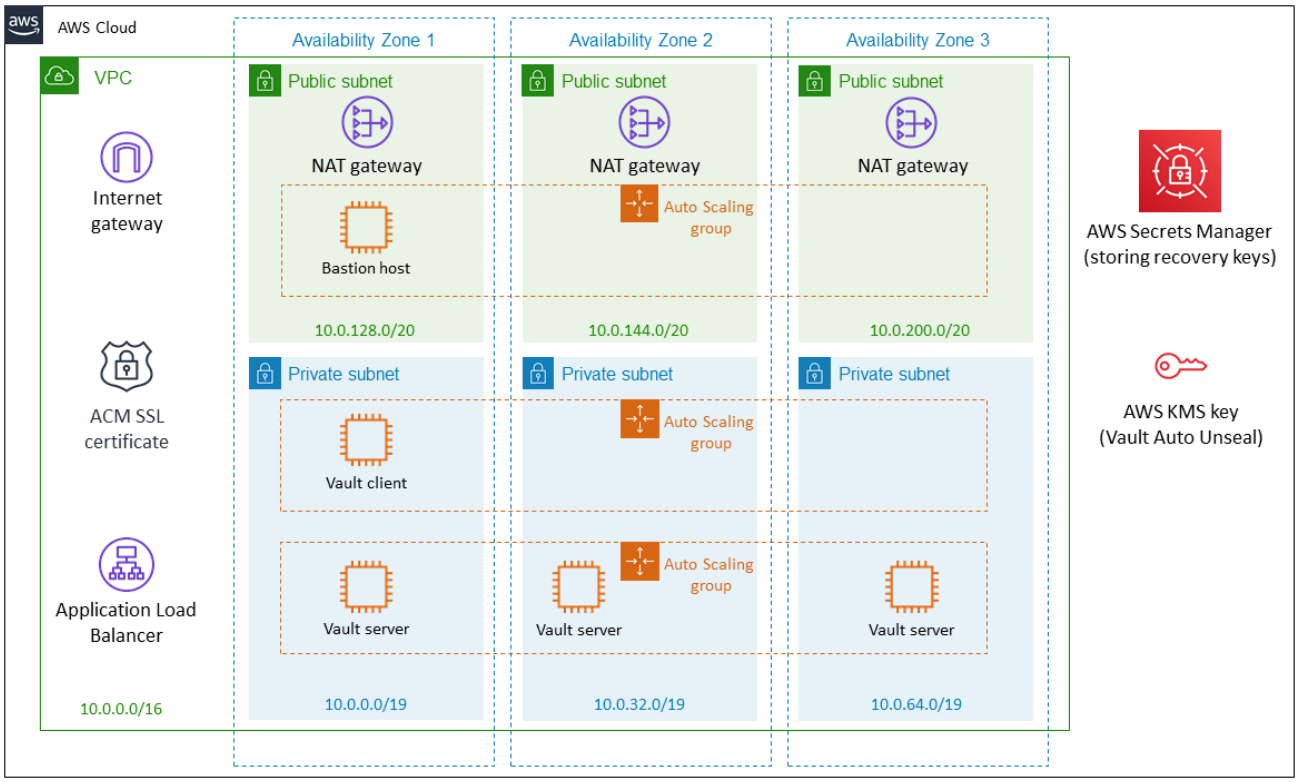


Figure 1: Quick Start architecture for HashiCorp Vault on AWS

As shown in figure 1, the Quick Start sets up the following:

- A VPC with public and private subnets across three Availability Zones.
- An internet gateway to provide access to the internet.*
- A certificate from the AWS Certificate Manager (ACM) Secure Sockets Layer (SSL), assuming that the supplied hosted-zone ID and DNS name are associated with the Application Load Balancer.
- An Application Load Balancer that can either be internal or external facing.
- In the public subnets:
  - Managed network address translation (NAT) gateways to allow outbound internet access for resources.
  - A Linux bastion host to allow inbound Secure Shell (SSH) access to Amazon Elastic Compute Cloud (Amazon EC2) instances.
- In the private subnets:
  - Auto Scaling groups that contain three, five, or seven HashiCorp Vault server instances across three Availability Zones.
  - A HashiCorp Vault environment with a Raft storage backend. Vault uses the Raft consensus algorithm to replicate data across the cluster.
- An AWS Secrets Manager secret that contains the root token and unseal keys created during the HashiCorp Vault cluster initialization.
- An AWS Key Management Service (AWS KMS) key that is used to auto-unseal HashiCorp Vault as well as encrypt the AWS Secrets Manager secret.

Planning the deployment

Specialized knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. If you are new to AWS, see Getting Started with AWS.

- Amazon VPC
- Amazon EC2
- Elastic Load Balancing
- Amazon EC2 Auto Scaling

Note: The Center for Internet Security (CIS) AMI for Ubuntu Linux 16.04 LTS is available as an optional, hardened AMI type. The image of Ubuntu Linux 16.04 LTS is preconfigured by CIS according to their benchmark recommendations. For more information, see CIS Ubuntu Linux 16.04 LTS Benchmark — Level 1.

AWS account

If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.

Your AWS account is automatically signed up for all AWS services. You are charged only for the services you use.

Technical requirements

Before you launch the Quick Start, your account must be configured as specified in the following table. Otherwise, deployment might fail.

Resources	If necessary, request service quota increases for the following resources. You might do this if an existing deployment uses these resources and you exceed the default quotas with this deployment. The Service Quotas console displays your usage and quotas for some aspects of some services. For more information, see the AWS documentation.

Resource	This deployment uses
VPCs	1
Elastic IP addresses	4
IAM security groups	4
IAM roles	4
Auto Scaling groups	3
Application Load Balancers	1
EC2 instances	4–9

Regions	This deployment includes AWS Systems Manager Parameter Store, which isn't currently supported in all AWS Regions. For a current list of supported Regions, see Service endpoints and quotas in the AWS documentation. This deployment also includes the CIS Ubuntu Linux 16.04 LTS Benchmark — Level 1 AMI. Please note that this AMI may not be available in all AWS Regions. See the AWS Market Place listing for more information.

Key pair	Ensure that at least one Amazon EC2 key pair exists in your AWS account in the Region where you plan to deploy the Quick Start. Make note of the key pair name. You need it during deployment. To create a key pair, follow the instructions in the AWS documentation. For testing or proof-of-concept purposes, we recommend creating a new key pair instead of using one that's already being used by a production instance.
IAM permissions	Before launching the Quick Start, you must log in to the AWS Management Console with IAM permissions for the resources and actions the templates deploy. The *AdministratorAccess* managed policy within IAM provides sufficient permissions, although your organization may choose to use a custom policy with more restrictions.

Deployment options

This Quick Start provides two deployment options:

- **Deployment of HashiCorp Vault into a new VPC** (end-to-end deployment) builds a new VPC with public and private subnets, and then deploys HashiCorp Vault into that infrastructure.
- **Deployment of HashiCorp Vault into an existing VPC** provisions HashiCorp Vault into your existing infrastructure.

The Quick Start provides separate templates for these options. It also lets you configure AWS IAM–based authentication as well as Kubernetes-integrated authentication within the HashiCorp Vault cluster, which this Quick Start creates.

Deployment steps

Step 1. Sign in to your AWS account

1. If you don't already have an AWS account, create one at http://aws.amazon.com by following the on-screen instructions.
2. Use the Region selector in the navigation bar to choose the AWS Region where you want to deploy HashiCorp Vault.
3. Create an Amazon EC2 key pair in your preferred AWS Region.
4. If necessary, request a service quota increase for the Amazon EC2 **t3.medium** and **m5.large** instance types. You might do this if you already have an existing deployment that uses these instance types and you exceed the default quota with this reference deployment.

Step 2. Subscribe to CIS Ubuntu Linux 16.04 LTS

This Quick Start recommends subscribing to the AMI for "CIS Ubuntu Linux 16.04 LTS Benchmark — Level 1" in AWS Marketplace.

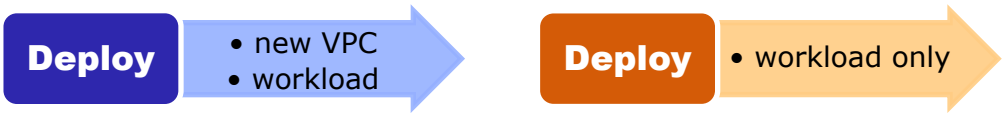
1. Sign in to your AWS account.
2. Open the page for the **CIS Ubuntu Linux 16.04 LTS Benchmark — Level 1** AMI in AWS Marketplace, and then choose **Continue to Subscribe**.
3. Review the terms and conditions for software usage, and then choose **Accept Terms**.

   A confirmation page loads, and an email confirmation is sent to the account owner. For detailed subscription instructions, see the AWS Marketplace documentation.
4. When the subscription process is complete, exit AWS Marketplace without further action.

> **Important:** Do not provision the software from AWS Marketplace—the Quick Start deploys the AMI for you.

Step 3. Launch the Quick Start

5. Choose one of the following options to deploy the AWS CloudFormation template into your AWS account.



Deploy HashiCorp Vault into a new VPC on AWS

Deploy HashiCorp Vault into an existing VPC on AWS

Each stack takes approximately 20 minutes to create.

> **Important:** If you deploy HashiCorp Vault into an existing VPC, ensure that your VPC has two private subnets in different Availability Zones for the workload instances, and that the subnets are not shared. This Quick Start does not support shared subnets. To enable the instances to download packages and software without exposing them to the internet, the subnets require NAT gateways in their route tables.

> Also ensure that the domain name in the DHCP options is configured as explained in the Amazon VPC documentation. Provide your VPC settings when you launch the Quick Start.

6. Check the AWS Region that's displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for HashiCorp Vault is built. The template is launched in the US East (Ohio) Region by default.

> **Note:** This deployment includes AWS Systems Manager Parameter Store, which isn't currently supported in all AWS Regions. For a current list of supported Regions, see the endpoints and quotas webpage.

7. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
8. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary.

   In the following tables, parameters are listed by category and described separately for the two deployment options:

   - Parameters for deploying HashiCorp Vault into a new VPC
   - Parameters for deploying HashiCorp Vault into an existing VPC

   When you finish reviewing and customizing the parameters, choose **Next**.

OPTION 1: PARAMETERS FOR DEPLOYING HASHICORP VAULT INTO A NEW VPC:

View template

VPC network configuration:

Parameter label (name)	Default	Description
Availability Zones (`AvailabilityZones`)	*Requires input*	List of Availability Zones to use for the VPC. Three Availability Zones are used for this deployment.
VPC CIDR (`VPCCIDR`)	10.0.0.0/16	CIDR block for the VPC.
Private subnet 1 CIDR (`PrivateSubnet1CIDR`)	10.0.0.0/19	CIDR block for private subnet 1 located in Availability Zone 1.

Parameter label (name)	Default	Description
Private subnet 2 CIDR (PrivateSubnet2CIDR)	10.0.32.0/19	CIDR block for private subnet 2 located in Availability Zone 2.
Private subnet 3 CIDR (PrivateSubnet3CIDR)	10.0.64.0/19	CIDR block for private subnet 3 located in Availability Zone 3.
Public subnet 1 CIDR (PublicSubnet1CIDR)	10.0.128.0/20	CIDR block for public DMZ subnet 1 located in Availability Zone 1.
Public subnet 2 CIDR (PublicSubnet2CIDR)	10.0.144.0/20	CIDR block for public DMZ subnet 2 located in Availability Zone 2.
Public subnet 3 CIDR (PublicSubnet3CIDR)	10.0.160.0/20	CIDR block for public DMZ subnet 3 located in Availability Zone 3.
Permitted IP range (AccessCIDR)	*Requires input*	CIDR IP range permitted to access Vault. A value of 0.0.0.0/0 allows access from any IP address.

Bastion configuration:

Parameter label (name)	Default	Description
Bastion hosts (NumBastionHosts)	1	Enter the number of bastion hosts to create.

HashiCorp Vault configuration:

Parameter label (name)	Default	Description
EC2 key pair (KeyPairName)	*Requires input*	Key pair to securely connect to your instance after it launches.
HashiCorp Vault version (VaultVersion)	1.4.0	Specify which version of HashiCorp Vault to install.
Vault cluster operating system (VaultAMIOS)	Ubuntu-1604-HVM	Linux distribution AMI for the Vault instances.
Vault server nodes (VaultServerNodes)	3	Set the desired capacity and maximum size of the Vault server Auto Scaling group.
Instance type (VaultInstanceType)	m5.large	HashiCorp Vault node instance type.
Unseal keys to create (VaultNumberOfKeys)	5	Number of unseal keys to create for HashiCorp Vault.

Parameter label (name)	Default	Description
Required unseal keys (`VaultNumberOfKeysForUnseal`)	3	Number of keys required to unseal HashiCorp Vault.
Vault AWS role name (`VaultClientRoleName`)	client-role-iam	HashiCorp Vault name for the AWS IAM role.
Vault client nodes (`VaultClientNodes`)	0	Sets the desired capacity and maximum size of the Vault client Auto Scaling group.
Enable Kubernetes authentication (`VaultKubernetesEnable`)	false	Enables Kubernetes authentication and creates a Kubernetes authentication role.
Kubernetes host URL (`VaultKubernetesHostURL`)	*Requires input*	URL of Kubernetes cluster (e.g., https://192.168.99.100:8443).
Kubernetes Vault role name (`VaultKubernetesRoleName`)	kube-auth-role	Internal Vault name for the Kubernetes Authentication role.
Kubernetes CA certificate (`VaultKubernetesCertificate`)	—	AWS SSM parameter that contains a base64-encoded PEM CA certificate for the Kubernetes cluster service account.
Kubernetes JWT token (`VaultKubernetesJWT`)	—	AWS SSM secure parameter that contains a base64-encoded JWT token for the Kubernetes cluster service account.
Kubernetes service account name (`VaultKubernetesServiceAccount`)	vault-auth	Name of the Kubernetes service account.
Kubernetes name space (`VaultKubernetesNameSpace`)	default	Vault name space of the Kubernetes service account.
Kubernetes Vault policies (`VaultKubernetesPolicies`)	default	Vault policies for the Kubernetes service account.

AWS Quick Start configuration:

Parameter label (name)	Default	Description
Quick Start S3 bucket name (`QSS3BucketName`)	aws-quickstart	S3 bucket name for the Quick Start assets. Quick Start bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Quick Start S3 key prefix (`QSS3KeyPrefix`)	quickstart-hashicorp-vault/	S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).
Quick Start S3 bucket Region (`QSS3BucketRegion`)	us-east-1	Region where the Quick Start S3 bucket (`QSS3BucketName`) is hosted. If you use your own bucket, specify this value.

Load balancer configuration:

Parameter label (name)	Default	Description
Internal/external load balancer (`LoadBalancerType`)	Internal	Specify if the load balancer for HashiCorp Vault is internal or external.
Load balancer DNS domain name (`DomainName`)	—	Fully qualified domain name for the HashiCorp Vault load balancer. If you don't provide a value for `ACMSSLCertificateArn`, use the `HostedZoneID`.
Hosted-zone ID (`HostedZoneID`)	—	Route 53-hosted zone ID of the domain name. If you don't provide an `ACMSSLCertificateArn` value, the Quick Start creates the ACM certificate for you using `HostedZoneID` in conjunction with `DomainName`.
SSL certificate ARN (`ACMSSLCertificateArn`)	—	Amazon Resource Name (ARN) of the load balancer's SSL certificate. If you don't provide values for `DomainName` and `HostedZoneID`, provide a value for `ACMSSLCertificateArn`.

OPTION 2: PARAMETERS FOR DEPLOYING HASHICORP VAULT INTO AN EXISTING VPC

View template

Network configuration:

Parameter label (name)	Default	Description
Permitted IP range (`AccessCIDR`)	*Requires input*	CIDR IP range that is permitted to access Vault. A value of 0.0.0.0/0 allows access from any IP address.

Parameter label (name)	Default	Description
VPC ID (VPCID)	*Requires input*	VPC ID.
VPC CIDR (VPCCIDR)	*Requires input*	CIDR block for the VPC.
Bastion host security group ID (BastionSecurityGroupID)	*Requires input*	ID of the bastion host security group to enable SSH connections (e.g., sg-7f16e910).
First subnet ID for Auto Scaling group (PrivateSubnet1ID)	*Requires input*	ID of private subnet 1 in Availability Zone 1 (e.g., subnet-xxxxxxxx).
Second subnet ID for Auto Scaling group (PrivateSubnet2ID)	*Requires input*	ID of private subnet 2 in Availability Zone 2 (e.g., subnet-xxxxxxxx).
Third subnet ID for Auto Scaling group (PrivateSubnet3ID)	*Requires input*	ID of private subnet 3 in Availability Zone 3 (e.g., subnet-xxxxxxxx).
First public subnet ID Auto Scaling group (PublicSubnet1ID)	*Requires input*	ID of public subnet 1 in Availability Zone 1 (e.g., subnet-xxxxxxxx).
Second public subnet ID for Auto Scaling group (PublicSubnet2ID)	*Requires input*	ID of public subnet 2 in Availability Zone 2 (e.g., subnet-xxxxxxxx).
Third public subnet ID for Auto Scaling group (PublicSubnet3ID)	*Requires input*	ID of public subnet 3 in Availability Zone 3 (e.g., subnet-xxxxxxxx).

HashiCorp Vault configuration:

Parameter label (name)	Default	Description
EC2 key pair (KeyPairName)	id_rsa_aws	Key pair to securely connect to your instance.
HashiCorp Vault version (VaultVersion)	1.4.0	Specify which version of HashiCorp Vault to install.
Vault cluster operating system (VaultAMIOS)	Ubuntu-1604-HVM	Linux distribution AMI for the Vault instances.

Parameter label (name)	Default	Description
Vault server nodes (`VaultServerNodes`)	5	Sets the desired capacity and maximum size for the Vault server Auto Scaling group.
Instance type (`VaultInstanceType`)	m5.large	HashiCorp Vault node instance type.
Unseal keys to create (`VaultNumberOfKeys`)	5	Number of unseal keys to create for HashiCorp Vault.
Unseal keys required (`VaultNumberOfKeysForUnseal`)	3	Number of keys required to unseal HashiCorp Vault.
Vault AWS role name (`VaultClientRoleName`)	quickstart-client-role-iam	HashiCorp Vault name for the AWS IAM role.
Vault client nodes (`VaultClientNodes`)	0	Sets the desired capacity and maximum size for the Vault client Auto Scaling group.
Enable Kubernetes authentication (`VaultKubernetesEnable`)	false	Enable Kubernetes authentication and create the Kubernetes authentication role.
Kubernetes host URL (`VaultKubernetesHostURL`)	*Requires input*	URL of the Kubernetes cluster (e.g., https://192.168.99.100:8443).
Kubernetes Vault role name (`VaultKubernetesRoleName`)	kube-auth-role	Internal HashiCorp Vault name for the Kubernetes Authentication role.
Kubernetes CA certificate (`VaultKubernetesCertificate`)	—	AWS SSM parameter that contains a base64-encoded PEM CA certificate of the Kubernetes cluster service account.
Kubernetes JWT token (`VaultKubernetesJWT`)	—	AWS SSM secure parameter that contains a base64-encoded JWT token of the Kubernetes cluster service account.
Kubernetes service account name (`VaultKubernetesServiceAccount`)	vault-auth	Name of the Kubernetes service account.
Kubernetes name space (`VaultKubernetesNameSpace`)	default	Vault name space of the Kubernetes service account.

Parameter label (name)	Default	Description
Kubernetes Vault policies (`VaultKubernetesPolicies`)	default	Vault policies for the Kubernetes service account.

AWS Quick Start configuration:

Parameter label (name)	Default	Description
Quick Start S3 bucket name (`QSS3BucketName`)	aws-quickstart	S3 bucket name for the Quick Start assets. Quick Start bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Quick Start S3 key prefix (`QSS3KeyPrefix`)	quickstart-hashicorp-vault/	S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).
Quick Start S3 bucket Region (`QSS3BucketRegion`)	us-east-1	AWS Region where the Quick Start S3 bucket (`QSS3BucketName`) is hosted. When using your own bucket, you must specify this value.

Load balancer configuration:

Parameter label (name)	Default	Description
Internal/external load balancer (`LoadBalancerType`)	Internal	Specify if the load balancer for HashiCorp Vault is internal or external.
Load balancer DNS name (`DomainName`)	—	Fully qualified domain name for the HashiCorp Vault load balancer. If you don't provide a value for `ACMSSLCertificateArn`, use the `HostedZoneID`.
Hosted-zone ID (`HostedZoneID`)	—	Route 53-hosted zone ID of the domain name. If you don't provide an `ACMSSLCertificateArn` value, the Quick Start creates the ACM certificate for you using `HostedZoneID` in conjunction with `DomainName`.
SSL certificate ARN (`ACMSSLCertificateArn`)	—	Amazon Resource Name (ARN) of the load balancer's SSL certificate. If you don't provide values for `DomainName` and `HostedZoneID`, provide a value for `ACMSSLCertificateArn`.

When you finish reviewing and customizing the parameters, choose **Next**.

9. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you're done, choose **Next**.
10. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template creates IAM resources.
11. Choose **Create** to deploy the stack.
12. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the deployment is complete.
13. You can use the URL displayed in the **Outputs** tab for the stack to view the resources that were created.

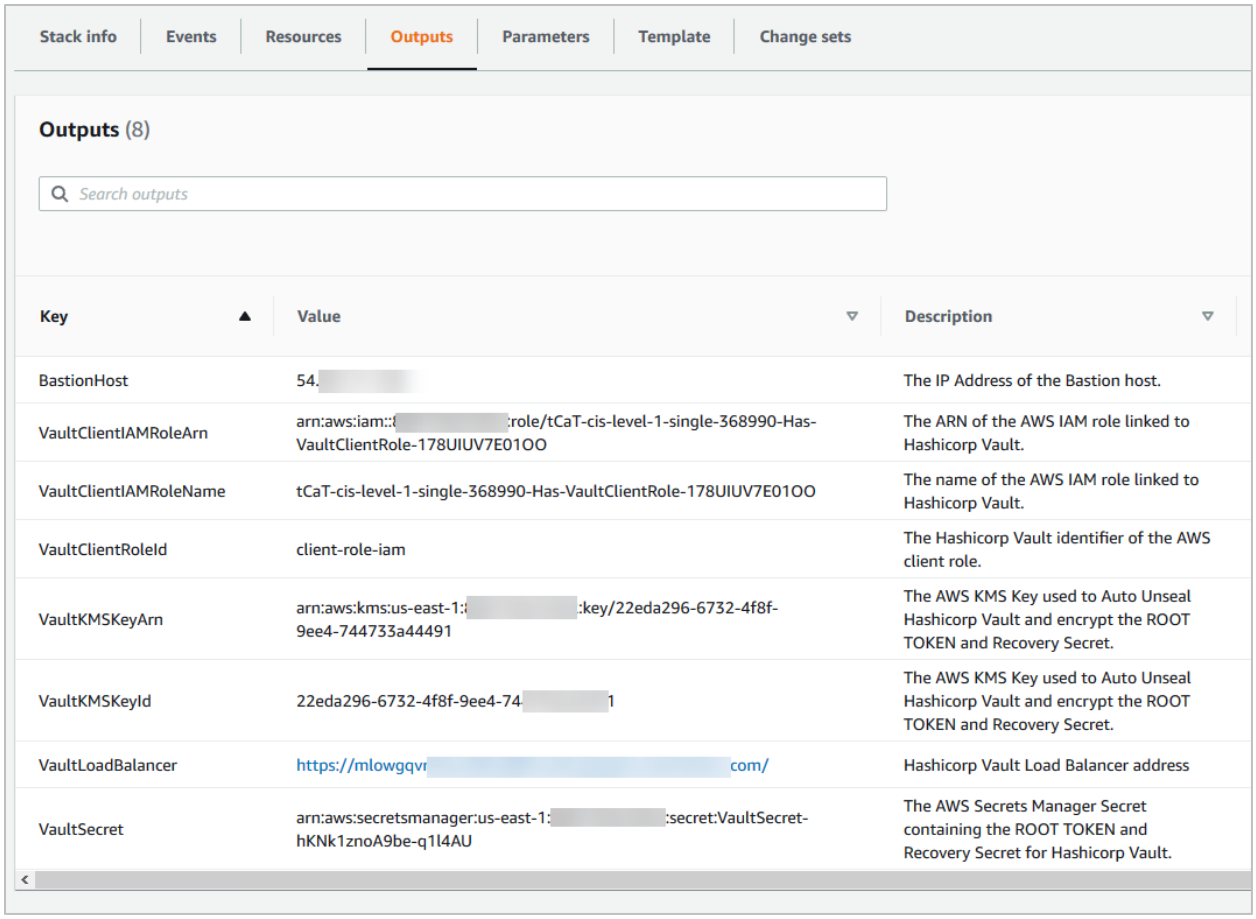


Figure 2: HashiCorp Vault outputs after successful deployment

Step 4. Review audit logs

14. This Quick Start is configured to ship Vault audit logs to Amazon CloudWatch. To see your logs, open the Amazon CloudWatch console. In the navigation pane, choose **Logs**,

and then select **Vault-Audit-Logs-XXXX** value from the **Outputs**. You will see a screen that is similar to figure 3.

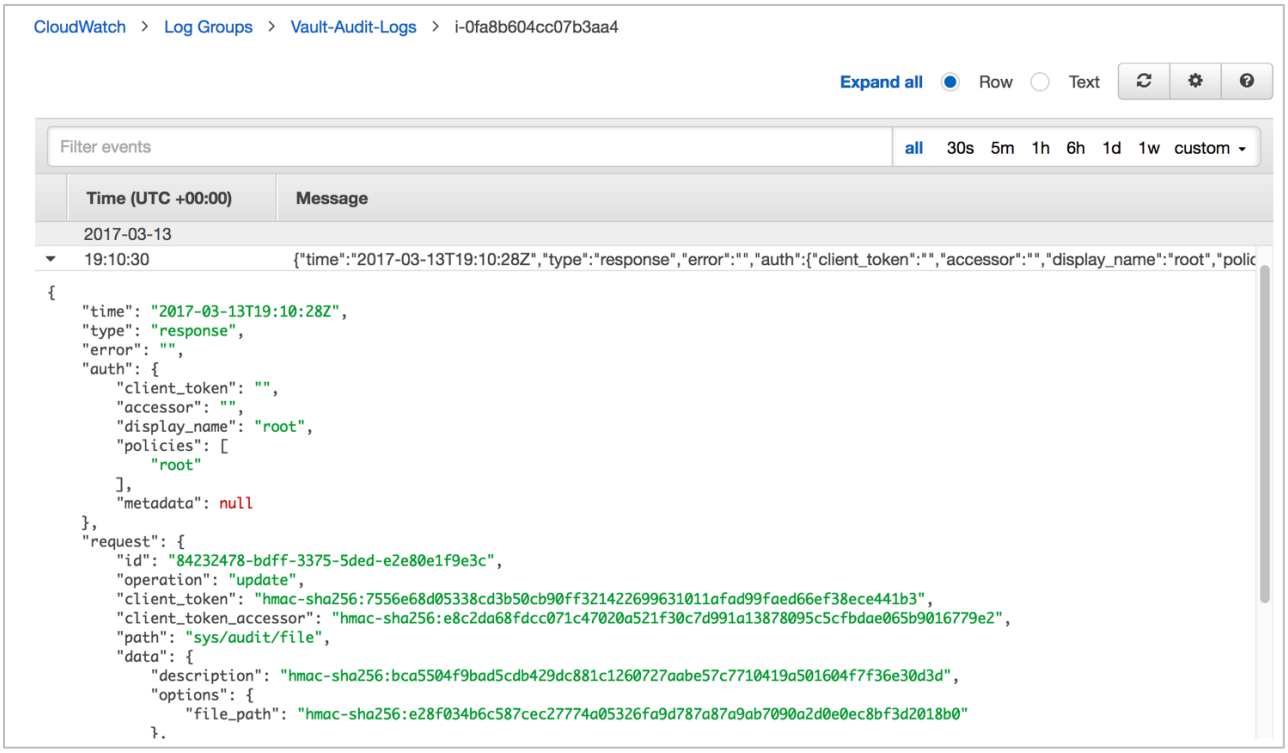


Figure 3: Viewing Vault audit logs

Step 5. Test the deployment

To access the Vault server cluster environment, access the Application Load Balancer (ALB) endpoint that was created during the deployment.

1. Locate the AWS Secrets Manager secret from the **Outputs** tab containing the Vault root token and recovery secrets for Vault.

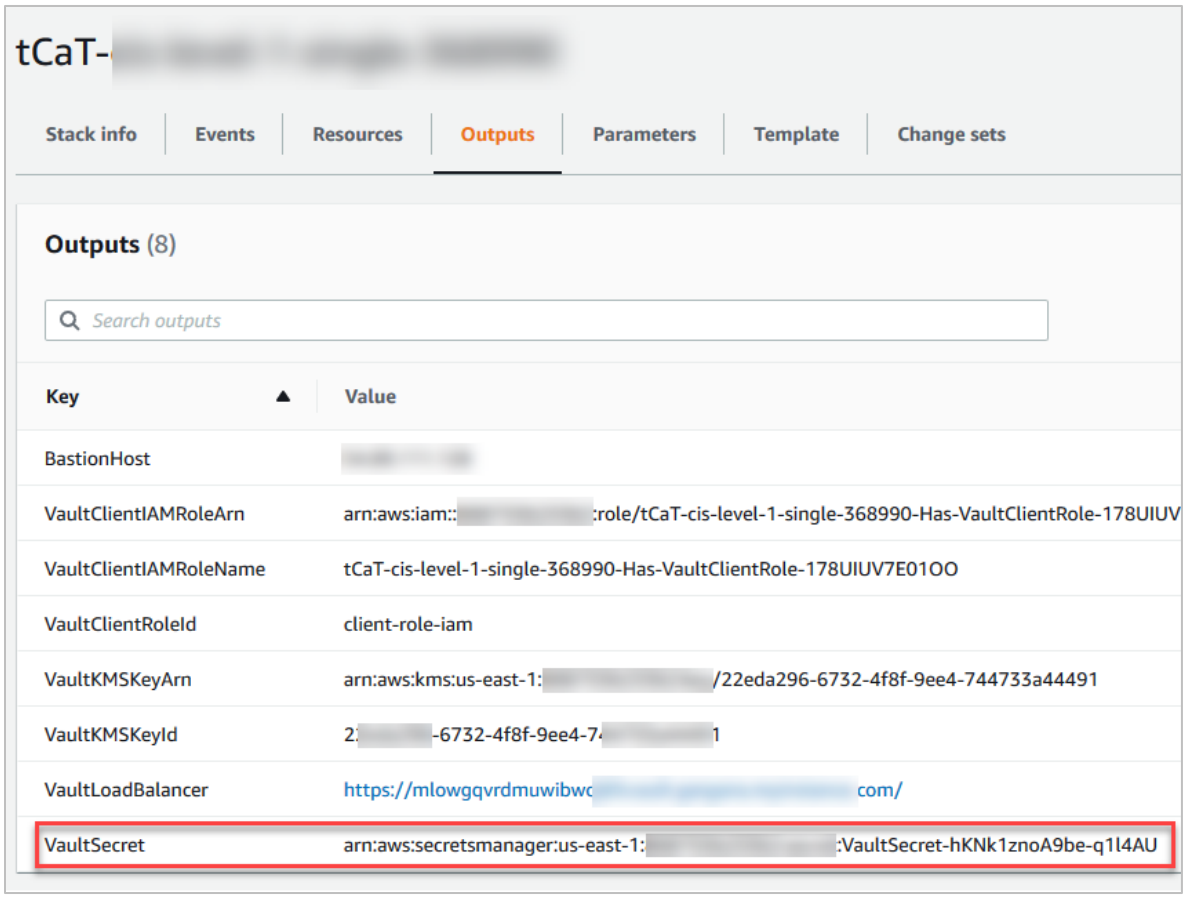


Figure 4: AWS Secrets Manager secret from the CloudFormation stack outputs

2. Locate the Application Load Balancer endpoint address from the **Outputs** tab of the AWS CloudFormation console.

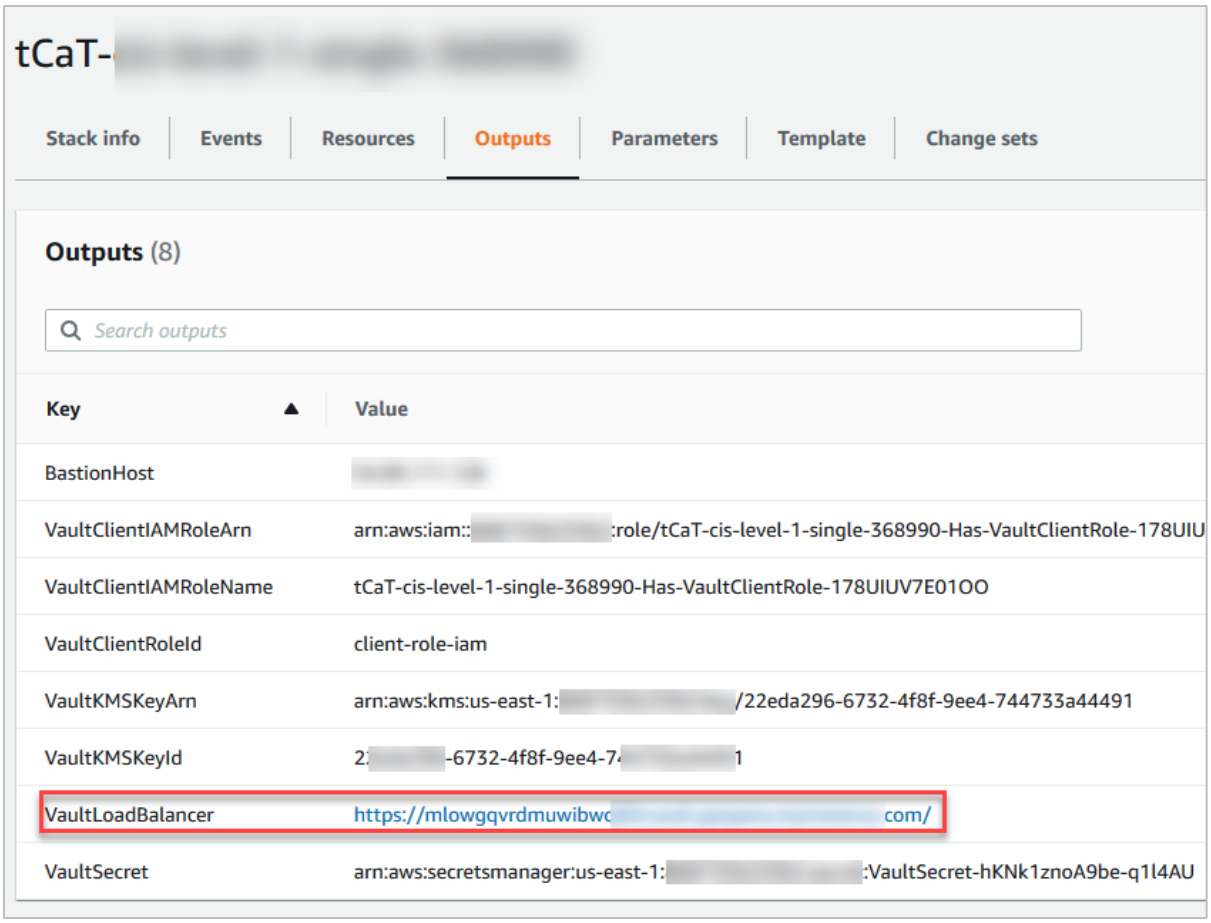


Figure 5: Vault load balancer from CloudFormation stack outputs

3. Use your preferred web browser to open the URL. On the Vault server login screen, use the root token from AWS Secrets Manager to log in to the Vault server cluster.

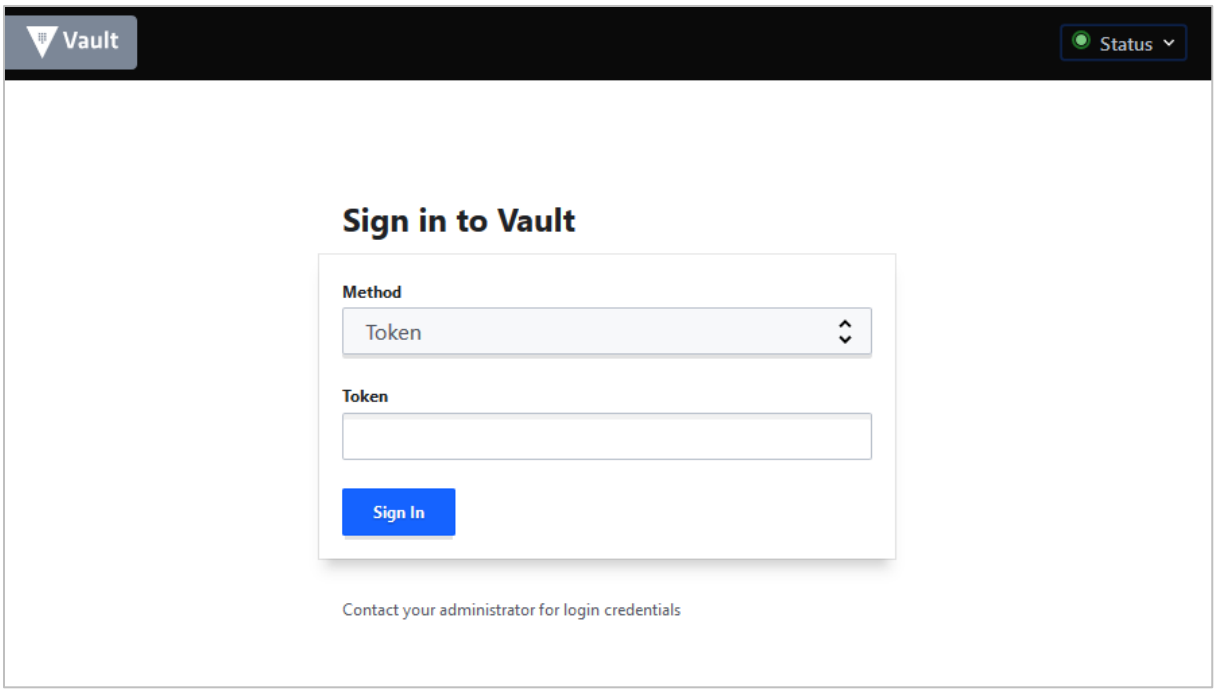


Figure 6: HashiCorp Vault cluster login screen

Note: Ensure that you have network access to this address. Specifically, for internal load balancers, you must configure the VPC to allow this.

Step 6. Get started with HashiCorp Vault

To integrate Vault with your environment and get started, see the Getting Started section of the HashiCorp Vault website.

How to deploy Vault with a CIS Ubuntu Linux 16.04 LTS–hardened AMI

The CIS AMI for Ubuntu Linux 16.04 LTS is available as an optional, hardened AMI type. The image of Ubuntu Linux 16.04 LTS is preconfigured by CIS according to their benchmark recommendations. For more information, see CIS Ubuntu Linux 16.04 LTS Benchmark — Level 1.

How to deploy Vault with Raft-integrated storage

Raft consensus algorithm is enabled by default. Using Raft as a storage backend eliminates reliance on any third-party systems, it implements high availability, supports enterprise-replication features, and provides backup/restore workflows. For more information, see the following HashiCorp pages.

- Vault with Integrated Storage Reference Architecture
- Vault HA Cluster with Integrated Storage on AWS
- Migrating to Integrated Storage

How to manage Vault Agent using AWS Auth method

AWS Auth method is available as an optional Auth method in the deployment wizard. The AWS Auth method provides an automated mechanism to retrieve a Vault token for IAM principals and Amazon EC2 instances. For more information, see Vault Agent with AWS.

How to manage Vault Agent using Kubernetes Auth method

Kubernetes Auth method is an option in the deployment wizard. The Kubernetes Auth method can be used to authenticate with Vault using a Kubernetes service account token. For more information, see Vault Agent with Kubernetes.

How to manage Vault Auto Unseal using AWS KMS

Vault Auto Unseal was developed to aid in reducing the operational complexity of keeping the master key secure. For more information, see Auto Unseal using AWS KMS.

Troubleshooting

Q. I encountered a **CREATE_FAILED** error when I launched the Quick Start. What should I do?

A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **Disabled**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state is retained and the instance is left running, so you can troubleshoot the issue. (Look at the log files in `%ProgramFiles%\Amazon\EC2ConfigService` and `C:\cfn\log`.)

> **Important:** When you set **Rollback on failure** to **Disabled**, you continue to incur AWS charges for the stack. Ensure to delete the stack when you finish troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

Q. I encountered a size limitation error when I deployed the AWS CloudFormation templates.

A. We recommend that you launch the Quick Start templates from the location we've provided or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information, see the AWS CloudFormation Limits.

Document revisions

Date	Change	In sections
June 2020	Upgraded to HashiCorp Vault 1.4, including best practices; updated AWS Architecture	Changes in templates and throughout guide
October 2019	Updated to reflect only one bastion host being deployed.	Architecture
April 2017	Added Linux bastion hosts; updated Consul to version 0.8.0; removed Seed server; added Amazon EC2 retry functionality	Changes in templates and throughout guide
November 2016	Initial publication	—

Additional resources

AWS services

- Amazon EC2
- Amazon VPC

HashiCorp Vault

- HashiCorp
- Vault
- Vault Enterprise

Quick Start reference deployments

- AWS Quick Start

Send us feedback

To post feedback, submit feature ideas, or report bugs, use the **Issues** section of the GitHub repository for this Quick Start. If you want to submit code, see the Quick Start Contributor's Guide.

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.