

HashiCorp Consul on the AWS Cloud

Quick Start Reference Deployment

November 2016

Last update: April 2017 ([revisions](#))

Cameron Stokes, HashiCorp, Inc.

Tony Vattathil and Brandon Chavis, Amazon Web Services

Contents

Overview.....	2
Costs and Licenses.....	3
Architecture.....	3
Prerequisites	4
Specialized Knowledge	4
Deployment Steps	5
Step 1. Prepare an AWS Account.....	5
Step 2. Launch the Quick Start	5
Step 3. Access Consul via SSH	9
Step 4. Access the Consul Web UI.....	12
Step 5. Get Started with Consul	13
Troubleshooting.....	13
Additional Resources	14
Send Us Feedback.....	15
Document Revisions	15

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

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying [HashiCorp](#) Consul on the Amazon Web Services (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.

Consul is a tool for discovering and configuring services in your infrastructure. It includes multiple components and provides several key features:

- **Service discovery:** Consul clients can provide a service, such as an API or MySQL, and other clients can use Consul to discover the providers of a specific service. Using either DNS or HTTP, applications can easily find the services they depend upon.
- **Health checking:** Consul clients can provide any number of health checks either associated with a given service (for example, to answer a question such as “is the web server returning 200 OK?”), or with the local node (for example, “is memory utilization below 90%?”). This information can be used by an operator to monitor cluster health, and by the service discovery components to route traffic away from unhealthy hosts.
- **Key/value store:** Applications can use Consul’s hierarchical key/value store for any number of purposes, including dynamic configuration, feature flagging, coordination, leader election, and more. The simple HTTP API makes it easy to use.
- **Multiple data centers:** Consul supports multiple data centers out of the box. This means that users of Consul do not have to worry about building additional layers of abstraction to expand their reach into multiple regions.

Consul is designed to be friendly to both the DevOps community and application developers, making it perfect for modern, elastic infrastructures.

This Quick Start is for users who are looking for a solution for service discovery, monitoring, or a key/value store. The Quick Start is built using the open-source version of Consul, but is also compatible with Consul Enterprise.

An expanded version of this deployment guide with detailed instructions and screen illustrations is available on the HashiCorp [Consul](#) and [Consul Enterprise](#) websites.

For other solutions from HashiCorp and AWS, see the [AWS Quick Start for HashiCorp Vault](#).

Costs 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, will affect the cost of deployment. See the pricing pages for each AWS service you will be using for cost estimates.

This Quick Start uses the open-source version of HashiCorp Consul, which doesn't require a license.

Architecture

Deploying this Quick Start with the **default parameters** builds the following Consul environment in its own virtual private cloud (VPC) in the AWS Cloud. For details about the VPC architecture, see the [Amazon VPC Quick Start Guide](#).)

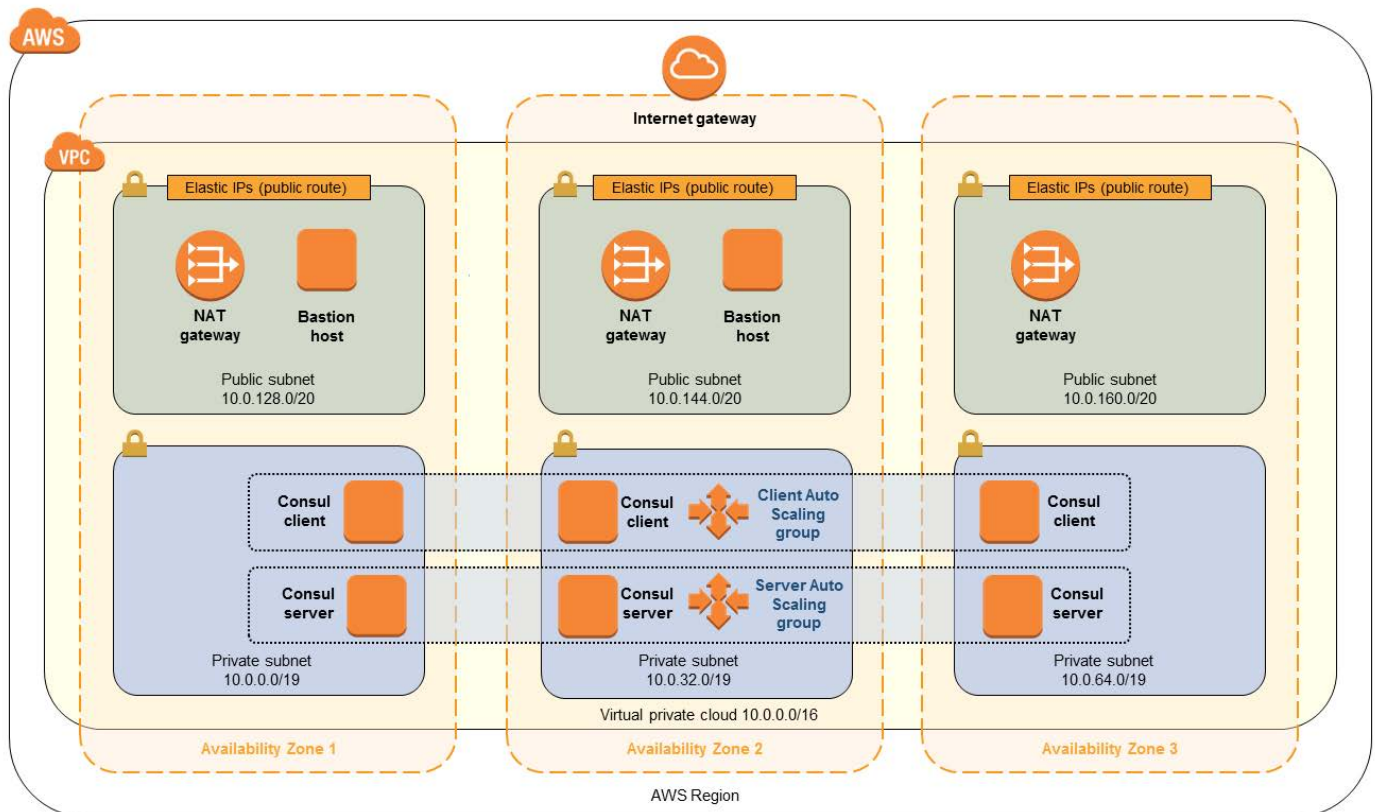


Figure 1: Quick Start architecture for HashiCorp Consul on AWS

The Quick Start provides two deployment options:

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

If you use the deployment option to create a new VPC, the AWS CloudFormation template included with the Quick Start will create the following components:

- A VPC with public and private subnets across three Availability Zones.
- Linux bastion hosts in the public subnets to allow inbound Secure Shell (SSH) access to EC2 instances in the private subnets.
- An Auto Scaling group for a Consul server cluster in the private subnets. You can choose to create 3, 5, or 7 servers.
- An Auto Scaling group for Consul clients in the private subnets. The number of clients is set to 3 by default, but is user-configurable.
- Consul Template (the `consul-template` daemon) installed on all nodes for integrating applications with Consul's service catalog and key/value store.
- **Dnsmasq** installed on all nodes for integrating applications with Consul's DNS interface for service discovery.

Prerequisites

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](#)

Deployment Steps

Step 1. Prepare an 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 Consul on AWS.
3. Create a [key pair](#) in your preferred region.
4. If necessary, [request a service limit increase](#) for the Amazon EC2 **t2.medium** instance type. You might need to do this if you already have an existing deployment that uses this instance type, and you think you might exceed the [default limit](#) with this reference deployment.

Step 2. Launch the Quick Start

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

Launch Quick Start
(for new VPC)

Launch Quick Start
(for existing VPC)

The templates are launched in the US West (Oregon) region by default. You can change the region by using the region selector in the navigation bar.

Each stack takes approximately 10 minutes to create.

Note 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 this Quick Start. See the pricing pages for each AWS service you will be using for full details.

2. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
3. On the **Specify Details** page, review the parameters for the template. Enter values for the parameters that require your input. For all other parameters, you can customize the default settings provided by the template.

In the following tables, parameters are listed and described separately for deploying HashiCorp Consul into a [new VPC](#) or an [existing VPC](#).

Note The templates for the two scenarios share most, but not all, of the same parameters. For example, the template for an existing VPC prompts you for the VPC and private subnet IDs in your existing VPC environment. You can also download the templates and edit them to create your own parameters based on your specific deployment scenario.

- **Parameters for deployment into a new VPC**

[View template](#)

VPC Network Configuration:

Parameter (name)	Default	Description
Availability Zones (AvailabilityZones)	<i>Requires input</i>	Choose three Availability Zones that will be used to deploy the components for HashiCorp Consul. The Quick Start preserves the logical order you specify.
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 the private subnet located in Availability Zone 1.
Private Subnet 2 CIDR (PrivateSubnet2CIDR)	10.0.32.0/19	CIDR block for the private subnet located in Availability Zone 2.
Private Subnet 3 CIDR (PrivateSubnet3CIDR)	10.0.64.0/19	CIDR block for the private subnet located in Availability Zone 3.
Public Subnet 1 CIDR (PublicSubnet1CIDR)	10.0.128.0/20	CIDR block for the public (DMZ) subnet located in Availability Zone 1.
Public Subnet 2 CIDR (PublicSubnet2CIDR)	10.0.144.0/20	CIDR block for the public (DMZ) subnet located in Availability Zone 2.
Public Subnet 3 CIDR (PublicSubnet3CIDR)	10.0.160.0/20	CIDR block for the public (DMZ) subnet located in Availability Zone 3.
Permitted IP range (AccessCIDR)	<i>Requires input</i>	The CIDR IP range that is permitted to access the Consul environment. We recommend that you use a constrained CIDR range to reduce the potential of inbound attacks from unknown IP addresses.

Consul Setup:

Parameter	Default	Description
Consul cluster node instance type (ConsulInstanceType)	t2.medium	The EC2 instance type for the Consul instance.
ConsulServerNodes (ConsulServerNodes)	3	The number of Consul server nodes that will be created. You can choose 3, 5, or 7 nodes.
ConsulClientNodes (ConsulClientNodes)	3	The number of Consul client nodes that will be created.
Key Name (KeyPairName)	<i>Requires input</i>	Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.

AWS Quick Start Configuration:

Parameter	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	aws-quickstart	S3 bucket name for the Quick Start assets. This bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-), but should not start or end with a hyphen. You can specify your own bucket if you copy all of the assets and submodules into it, if you want to override the Quick Start behavior for your specific implementation.
Quick Start S3 Key Prefix (QSS3KeyPrefix)	quickstart-hashicorp-consul/	S3 key prefix for the Quick Start assets. This prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slashes (/), but should not start or end with a forward slash (which is automatically added). This parameter enables you to override the Quick Start behavior for your specific implementation.

- Parameters for deployment into an existing VPC**

[View template](#)

Parameter name	Default	Description
AccessCIDR	<i>Requires input</i>	The CIDR IP range that is permitted to access the Consul environment. We recommend that you set this value to a trusted CIDR block. For example, you might want to restrict access to your corporate network. A value of 0.0.0.0/0 will allow access from any IP address.

Parameter name	Default	Description
AvailabilityZones	<i>Requires input</i>	Choose three Availability Zones that will be used to deploy the components for HashiCorp Consul. The Quick Start preserves the logical order you specify.
ConsulClientNodes	3	The number of Consul client nodes that will be created.
ConsulInstanceType	t2.medium	The EC2 instance type for the Consul instance.
ConsulServerNodes	3	The number of Consul server nodes that will be created. You can choose 3, 5, or 7 nodes.
KeyPair	<i>Requires input</i>	Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.
PrivateSubnet1CIDR	<i>Requires input</i>	CIDR block for the private subnet in Availability Zone 1.
PrivateSubnet1ID	<i>Requires input</i>	ID of the private subnet in Availability Zone 1 (e.g., subnet-a0246dcd).
PrivateSubnet2CIDR	<i>Requires input</i>	CIDR block for the private subnet in Availability Zone 2.
PrivateSubnet2ID	<i>Requires input</i>	ID of the private subnet in Availability Zone 2 (e.g., subnet-e3246d8e).
PrivateSubnet3CIDR	<i>Requires input</i>	CIDR block for the private subnet in Availability Zone 3.
PrivateSubnet3ID	<i>Requires input</i>	ID of the private subnet in Availability Zone 3.
PublicSubnet1CIDR	<i>Requires input</i>	CIDR block for the public subnet in Availability Zone 1.
PublicSubnet1ID	<i>Requires input</i>	ID of the public subnet in Availability Zone 1.
PublicSubnet2CIDR	<i>Requires input</i>	CIDR block for the public subnet in Availability Zone 2.
PublicSubnet2ID	<i>Requires input</i>	ID of the public subnet in Availability Zone 2.
PublicSubnet3CIDR	<i>Requires input</i>	CIDR block for the public subnet in Availability Zone 3.
PublicSubnet3ID	<i>Requires input</i>	ID of the public subnet in Availability Zone 3.
QSS3BucketName	aws-quickstart	S3 bucket name for the Quick Start assets. This bucket name can include numbers, lowercase

Parameter name	Default	Description
		letters, uppercase letters, and hyphens (-), but should not start or end with a hyphen. You can specify your own bucket if you copy all of the assets and submodules into it, if you want to override the Quick Start behavior for your specific implementation.
QSS3KeyPrefix	quickstart-hashicorp-consul/	S3 key prefix for the Quick Start assets. This prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slashes (/), but should not start or end with a forward slash (which is automatically added). This parameter enables you to override the Quick Start behavior for your specific implementation.
QuickStartS3URL	https://s3.amazonaws.com	Used to dynamically generate URLs for sub-templates.
VPCCIDR	<i>Requires input</i>	CIDR block for your existing VPC.
VPCID	<i>Requires input</i>	ID of your existing VPC (e.g., vpc-0343606e).

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

- 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**.
- On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.
- Choose **Create** to deploy the stack.
- Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the deployment is complete.
- You can use the URL displayed in the **Outputs** tab for the stack to view the resources that were created.

Step 3. Access Consul via SSH

To access the Consul environment, first connect to one of the bastion hosts. Use an SSH agent to forward your private key on connection.

Important Do not copy your private key to the bastion host.

For more information on SSH agents, see the [GitHub documentation](#).

To use an SSH agent to access the Consul environment on Mac or Linux:

1. Use the command:

```
ssh-add ~/.ssh/id_rsa
```

2. At the prompt, type your passphrase or press **Enter** for no passphrase.

```
Enter passphrase (empty for no passphrase): [Hit Enter Again or
Enter passphrase]
Enter same passphrase again: [Hit Enter Again or Enter passphrase]
```

3. In the Amazon EC2 console, select one of the two bastion hosts and note its Elastic IP address.

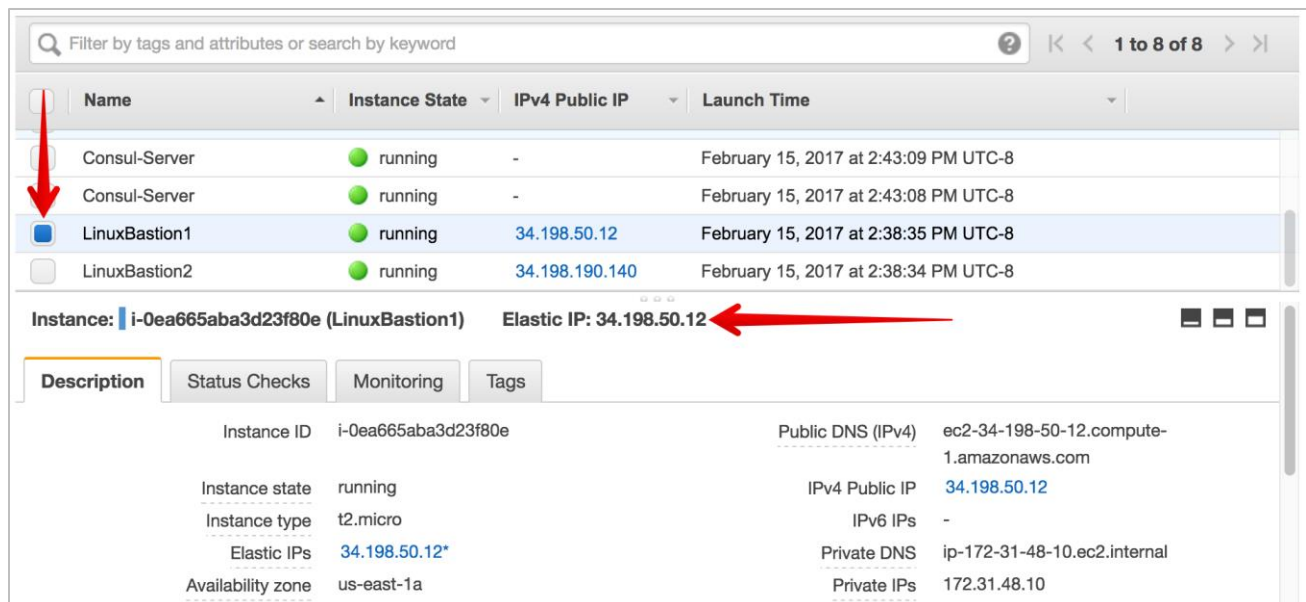


Figure 2: Finding the Elastic IP address for the bastion host instance

In the example in Figure 2, the Elastic IP for LinuxBastion1 is **34.198.50.12**.

4. Log in, and type **yes** when prompted to continue connecting:

```
ssh -A ubuntu@34.198.50.12
```



```

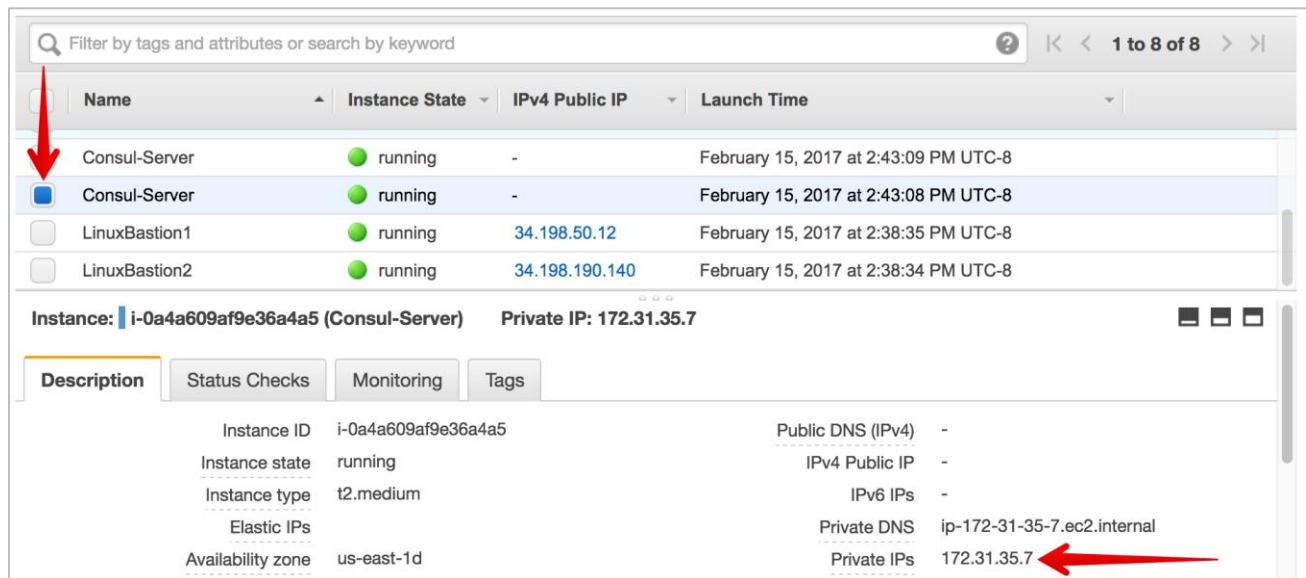
1. ec2-user@ip-172-31-48-10:~ (ssh)
~ $ ssh -A ec2-user@34.198.50.12
The authenticity of host '34.198.50.12 (34.198.50.12)' can't be established.
ECDSA key fingerprint is SHA256:WCx3LrBZLCicwKKGqpwv/C/hkjp1cXjNEJYngXUaR1o.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '34.198.50.12' (ECDSA) to the list of known hosts.
Last login: Thu Feb 16 01:47:36 2017 from c-71-231-52-72.hsd1.wa.comcast.net

  _ _ _ _ _
 _ _ _ _ _ /   Amazon Linux AMI
 _ _ _ _ _

https://aws.amazon.com/amazon-linux-ami/2016.09-release-notes/
4 package(s) needed for security, out of 7 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-48-10 ~]$

```

5. In the Amazon EC2 console, select one of the Consul-Server or Consul-Client hosts and note its private IP address.



Name	Instance State	IPv4 Public IP	Launch Time
Consul-Server	running	-	February 15, 2017 at 2:43:09 PM UTC-8
Consul-Server	running	-	February 15, 2017 at 2:43:08 PM UTC-8
LinuxBastion1	running	34.198.50.12	February 15, 2017 at 2:38:35 PM UTC-8
LinuxBastion2	running	34.198.190.140	February 15, 2017 at 2:38:34 PM UTC-8

Instance: **i-0a4a609af9e36a4a5 (Consul-Server)** Private IP: 172.31.35.7

Description	
Instance ID	i-0a4a609af9e36a4a5
Instance state	running
Instance type	t2.medium
Elastic IPs	-
Availability zone	us-east-1d
Public DNS (IPv4)	-
IPv4 Public IP	-
IPv6 IPs	-
Private DNS	ip-172-31-35-7.ec2.internal
Private IPs	172.31.35.7

Figure 3: Finding the private IP address for Consul-Server

In the example in Figure 2, the private IP for Consul-Server is **172.31.35.7**.

6. From the bastion host, connect to the Consul-Server or Consul-Client host, using Ubuntu as the user:

```

1. ubuntu@ip-172-31-35-7: ~ (ssh)
[ec2-user@ip-172-31-48-10 ~]$ ssh ubuntu@172.31.35.7
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-57-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

90 packages can be updated.
24 updates are security updates.

Last login: Thu Feb 16 01:54:05 2017 from 172.31.48.10
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-35-7:~$

```

7. View Consul members:

```
consul members
```

```

1. ubuntu@ip-172-31-35-7: ~ (ssh)
ubuntu@ip-172-31-35-7:~$ consul members
Node           Address          Status  Type    Build  Protocol  DC
ip-172-31-13-9  172.31.13.9:8301 alive   client  0.7.4   2         dc1
ip-172-31-19-251 172.31.19.251:8301 alive   client  0.7.4   2         dc1
ip-172-31-24-191 172.31.24.191:8301 alive   server  0.7.4   2         dc1
ip-172-31-35-7   172.31.35.7:8301 alive   server  0.7.4   2         dc1
ip-172-31-43-234 172.31.43.234:8301 alive   client  0.7.4   2         dc1
ip-172-31-9-125  172.31.9.125:8301 alive   server  0.7.4   2         dc1
ubuntu@ip-172-31-35-7:~$

```

Step 4. Access the Consul Web UI

1. Open an SSH tunnel from your local workstation and Linux bastion host:

```
ssh -L 8500:172.31.35.7:8500 ec2-user@34.198.50.12
```

2. Open a browser window to <http://localhost:8500/>. You'll see the Consul web screen illustrated in Figure 4.

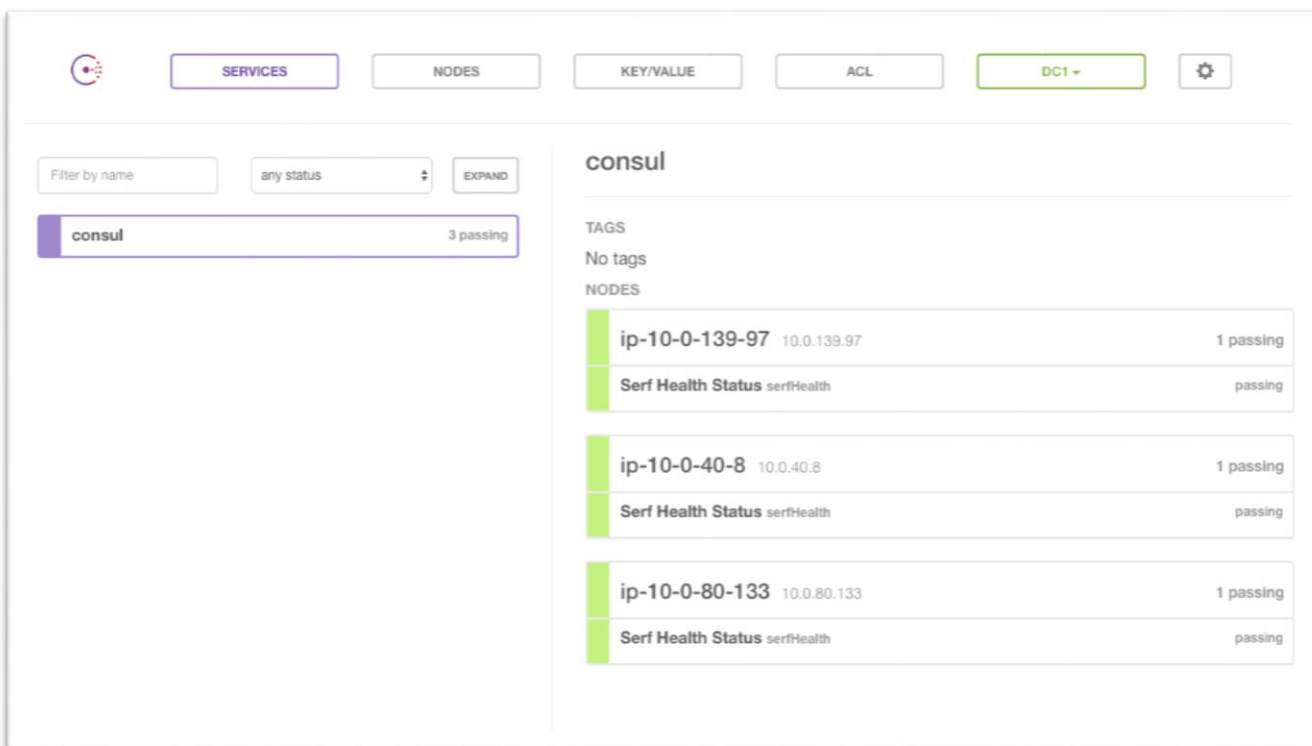


Figure 4: Consul web UI

Step 5. Get Started with Consul

To integrate Consul with your environment and get started with Consul services, see the [Getting Started](#) section of the HashiCorp Consul website.

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 **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state will be retained and the instance will be left running, so you can troubleshoot the issue. (You'll want to look at the log files in `%ProgramFiles%\Amazon\EC2ConfigService` and `C:\cfn\log`.)

Important When you set **Rollback on failure** to **No**, you'll continue to incur AWS charges for this stack. Please make sure to delete the stack when you've finished troubleshooting.

For additional information, see [Troubleshooting AWS CloudFormation](#) on the AWS website or contact us on the [AWS Quick Start Discussion Forum](#).

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 about AWS CloudFormation limits, see the [AWS documentation](#).

Additional Resources

AWS services

- Amazon EC2
<http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/>
- Amazon VPC
<http://aws.amazon.com/documentation/vpc/>

HashiCorp Consul

- Consul
<https://www.consul.io>
- Consul Enterprise
<https://www.hashicorp.com/consul.html>

Quick Start reference deployments

- AWS Quick Start home page
<https://aws.amazon.com/quickstart/>
- AWS Quick Start for HashiCorp Vault
<https://s3.amazonaws.com/quickstart-reference/hashicorp/vault/latest/doc/hashicorp-vault-on-the-aws-cloud.pdf>

Send Us Feedback

We welcome your questions and comments. Please post your feedback on the [AWS Quick Start Discussion Forum](#).

You can visit our [GitHub repository](#) to download the templates and scripts for this Quick Start, and to share your customizations with others.

Document Revisions

Date	Change	In sections
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	—

© 2017, Amazon Web Services, Inc. or its affiliates, and HashiCorp, Inc. All rights reserved.

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.