Linux Bastion Hosts on the AWS Cloud

Quick Start Reference Deployment

Santiago Cardenas, Tony Vattathil, and Ian Hill
Solutions Architects, AWS Quick Start Reference Team

September 2016
Last update: April 2017 (revisions)

This guide is also available in HTML format at https://docs.aws.amazon.com/quickstart/latest/linux-bastion/.

Contents

About This Guide

This Quick Start deployment guide provides instructions for deploying Linux bastion hosts in an Amazon Virtual Private Cloud (Amazon VPC) environment on the Amazon Web Services (AWS) Cloud. The Quick Start also provides AWS CloudFormation templates that automate the deployment.

The guide is for IT infrastructure architects, DevOps engineers, and administrators who are building an AWS Cloud environment for their workloads and would like to securely deploy Linux bastion hosts to manage their deployments remotely.

Quick Starts are automated reference deployments for AWS Cloud infrastructure components and key enterprise workloads on the AWS Cloud. Each Quick Start launches, configures, and runs AWS compute, network, storage, and other services, using AWS best practices for security and availability.

Overview

This Quick Start provides a Linux bastion functionality for AWS Cloud infrastructures. It deploys a virtual private cloud (VPC) using the Quick Start reference deployment, sets up private and public subnets, and deploys Linux bastion instances into that VPC. You can also choose to deploy Linux bastion hosts into your existing AWS infrastructure.

The bastion hosts provide secure access to Linux instances located in the private and public subnets. The Quick Start architecture deploys Linux bastion host instances into every public subnet to provide readily available administrative access to the environment. The Quick Start sets up a Multi-AZ environment consisting of two Availability Zones. If highly available bastion access is not necessary, you can stop the instance in the second Availability Zone and start it up when needed.

You can use this Quick Start as a building block for your own Linux-based deployments. You can add other infrastructure components and software layers to complete your Linux environment in the AWS Cloud. To build an AWS Cloud infrastructure for accessing Microsoft Windows-based instances, see the Quick Start for Remote Desktop (RD) Gateway.

Quick Links

The links in this section are for your convenience. Before you launch the Quick Start, please review the architecture, configuration, and other considerations discussed in this guide.

- If you have an AWS account and you're already familiar with AWS services, you can launch the Quick Start to build the architecture shown in Figure 1 in a new or existing VPC in your AWS account. The deployment takes approximately 5 minutes. If you're new to AWS, please follow the step-by-step instructions provided later in this guide.

Launch Quick Start (for new VPC)

Launch Quick Start (for existing VPC)

- If you want to take a look under the covers, you can view the AWS CloudFormation templates that automate the deployment. The templates include default settings that you can customize by following the instructions in this guide.

View template (for new VPC)

View template (for existing VPC)

Cost

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 the settings, such as the instance type, will determine the cost of deployment. For pricing details, see the Amazon EC2 pricing page.

Architecture

Deploying this Quick Start with the **default parameters** builds the following virtual networking environment in the AWS Cloud. (Note that the diagram doesn't show all the components of the VPC architecture. For details about that architecture, see the Amazon VPC Quick Start.)

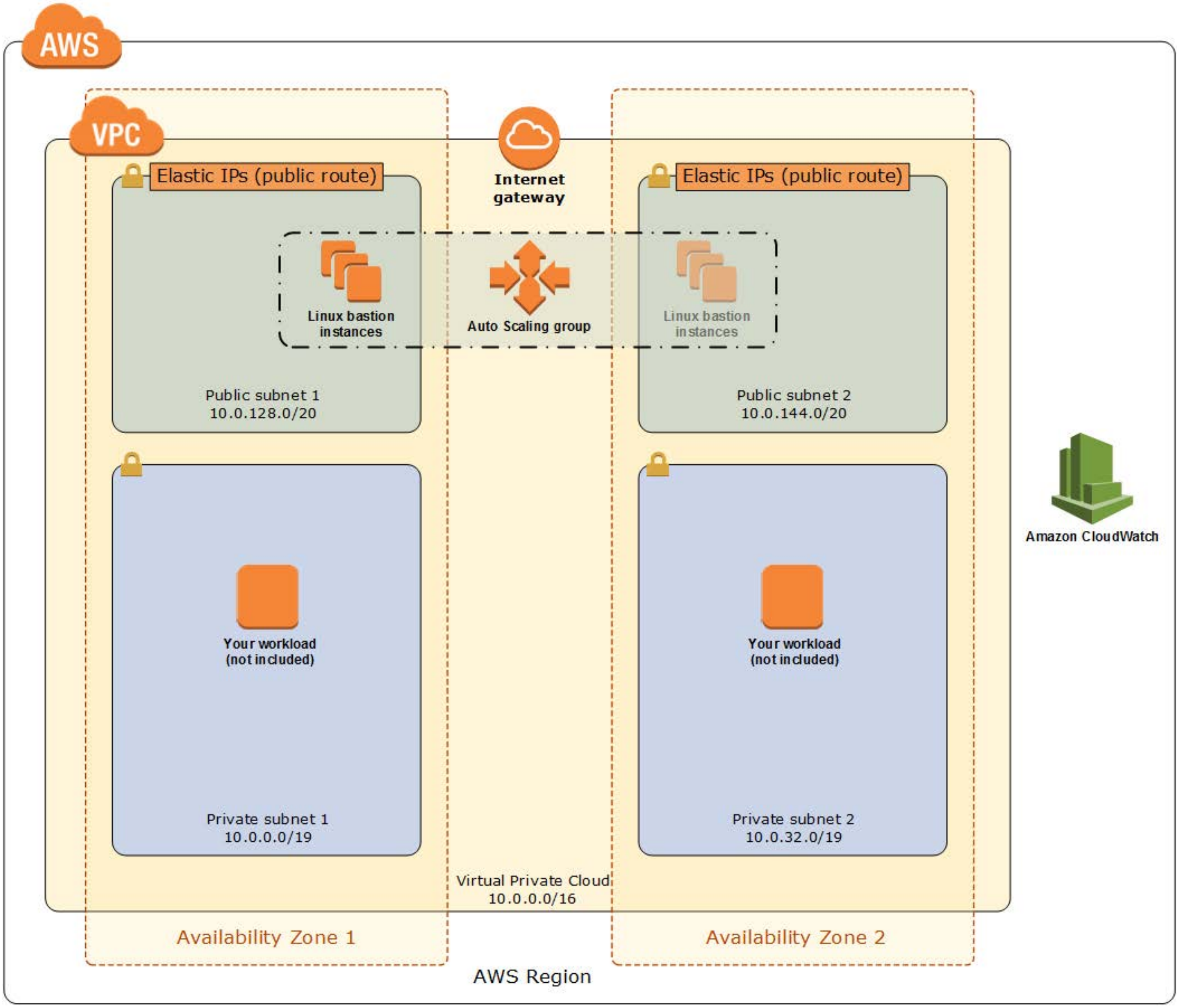


Figure 1: Linux bastion host architecture on AWS

The Quick Start builds a networking environment that includes the following components. If you already have an AWS infrastructure, the Quick Start also provides an option for deploying Linux bastion hosts into your existing VPC. (The template that deploys the Quick Start into an existing VPC skips the tasks marked by asterisks.)

- A highly available architecture that spans two Availability Zones.*
- A VPC configured with public and private subnets according to AWS best practices, to provide you with your own virtual network on AWS.*

- An Internet gateway to allow access to the Internet. This gateway is used by the bastion hosts to send and receive traffic.*
- Managed NAT gateways to allow outbound Internet access for resources in the private subnets.*
- A Linux bastion host in each public subnet with an Elastic IP address to allow inbound Secure Shell (SSH) access to EC2 instances in public and private subnets.
- A security group for fine-grained inbound access control.
- An Amazon EC2 Auto Scaling group with a configurable number of instances.
- A set of Elastic IP addresses that match the number of bastion host instances. If the Auto Scaling group relaunches any instances, these addresses are reassociated with the new instances.
- An Amazon CloudWatch Logs log group to hold the Linux bastion host shell history logs.

AWS Services

The core AWS components used by this Quick Start include the following AWS services. (If you are new to AWS, see the Getting Started section of the AWS documentation.)

- Amazon VPC – The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of an IP address range, creation of subnets, and configuration of route tables and network gateways.
- Amazon EC2 – The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing Amazon Machine Images (AMIs) or import your own virtual machine images.
- Amazon EBS – Amazon Elastic Block Store (Amazon EBS) provides persistent block-level storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. Amazon EBS volumes provide consistent and low-latency performance to run your workloads.
- NAT Gateway – NAT gateways are network address translation (NAT) devices, which provide outbound Internet access to instances in a private subnets, but prevent the Internet from accessing those instances. NAT gateways provide better availability and

bandwidth than NAT instances. The NAT Gateway service is a managed service that takes care of administering NAT gateways for you.

- Auto Scaling– Auto Scaling helps you ensure that you have the desired number of EC2 instances available to handle the load for your application. You create collections of EC2 instances, called *Auto Scaling groups*. When you deploy the Quick Start, you can specify the desired number of instances in each Auto Scaling group, and Auto Scaling ensures that your group has this number of instances at all times.
- Amazon CloudWatch Logs – You can use Amazon CloudWatch Logs to monitor, store, and access your log files from EC2 instances, AWS CloudTrail, and other sources. You can retrieve the log data from CloudWatch Logs, and monitor your EC2 instances in real time.

Bastion Hosts

Including bastion hosts in your VPC environment enables you to securely connect to your Linux instances without exposing your environment to the Internet. After you set up your bastion hosts, you can access the other instances in your VPC through Secure Shell (SSH) connections on Linux. Bastion hosts are also configured with security groups to provide fine-grained ingress control.

Best Practices

The architecture built by this Quick Start supports AWS best practices for high availability and security:

- Linux bastion hosts are deployed in two Availability Zones to support immediate access across the VPC. You can configure the number of bastion host instances at launch.
- An Auto Scaling group ensures that the number of bastion host instances always matches the desired capacity you specify during launch.
- Bastion hosts are deployed in the public (DMZ) subnets of the VPC.
- Elastic IP addresses are associated with the bastion instances to make it easier to remember and allow these IP addresses from on-premises firewalls. If an instance is terminated and the Auto Scaling group launches a new instance in its place, the existing Elastic IP addresses are reassociated with the new instances. This ensures that the same trusted Elastic IP addresses are used at all times.
- Access to the bastion hosts are locked down to known CIDR scopes for ingress. This is achieved by associating the bastion instances with a security group. The Quick Start creates a `BastionSecurityGroup` resource for this purpose.

- Ports are limited to allow only the necessary access to the bastion hosts. For Linux bastion hosts, TCP port 22 for SSH connections is typically the only port allowed.

We recommend that you follow these best practices when you're using the architecture built by the Quick Start:

- When you add new instances to the VPC that require management access from the bastion host, make sure to associate a security group ingress rule, which references the bastion security group as the source, with each instance. It is also important to limit this access to the required ports for administration.
- During deployment, the public key from the selected Amazon EC2 key pair is associated with the user `ec2-user` in the Linux instance. For additional users, you should create users with the required permissions and associate them with their individual authorized public keys for SSH connectivity.
- For the bastion host instances, you should select the number and type of instances according to the number of users and operations to be performed. The Quick Start creates one bastion host instance and uses the t2.micro instance type by default, but you can change these settings during deployment.

Note You can also change the number and type of bastion host instances after deployment, by updating the AWS CloudFormation stack and changing the parameters. Reconfiguring the bastion host instances updates the related Elastic IP addresses and changes the bootstrapping logic in the launch configuration and Auto Scaling group. However, before you update the stack, you must terminate the instances you want to replace while keeping the Elastic IP addresses. When you update the stack, Auto Scaling will launch the new instances with the updated instance type, and bootstrapping will assign the Elastic IP addresses from the existing pool of IP addresses that were provisioned during the initial deployment.

- Set your desired expiration time directly in the CloudWatch Logs log group for the logs collected from each bastion instance. This ensures that bastion log history is retained only for the amount of time you need.
- Keep your CloudWatch log files separated for each bastion host instance so that you can filter and isolate logs messages from individual bastion hosts more easily. Every instance that is launched by the bastion Auto Scaling group will create its own log stream based on the instance ID.

Deployment Scenarios

This Quick Start provides separate AWS CloudFormation templates for the following two deployment scenarios:

- **Deployment into a new VPC**. This template creates the VPC, subnets, NAT gateways, and security groups in your AWS account, and deploys Linux bastion hosts into that new infrastructure.
- **Deployment into an existing VPC**. This template provisions Linux bastion hosts in your existing VPC infrastructure. This option requires a VPC environment set up with at least two public subnets.

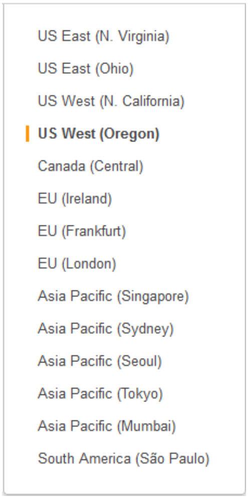
In the next section, you can choose one of these templates for your deployment.

Deployment Steps

Follow the step-by-step instructions in this section to build the virtual network environment illustrated in Figure 1 in your AWS account.

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. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.
2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy the Quick Start on AWS.



US East (N. Virginia)
US East (Ohio)
US West (N. California)
US West (Oregon)
Canada (Central)
EU (Ireland)
EU (Frankfurt)
EU (London)
Asia Pacific (Singapore)
Asia Pacific (Sydney)
Asia Pacific (Seoul)
Asia Pacific (Tokyo)
Asia Pacific (Mumbai)
South America (São Paulo)

Figure 2: Choosing an AWS Region

> **Tip** Consider choosing a region closest to your data center or corporate network to reduce network latency between systems running on AWS and the systems and users on your corporate network.

3. Create a key pair in your preferred region. To do this, in the navigation pane of the Amazon EC2 console, choose **Key Pairs**, **Create Key Pair**, type a name, and then choose **Create**.

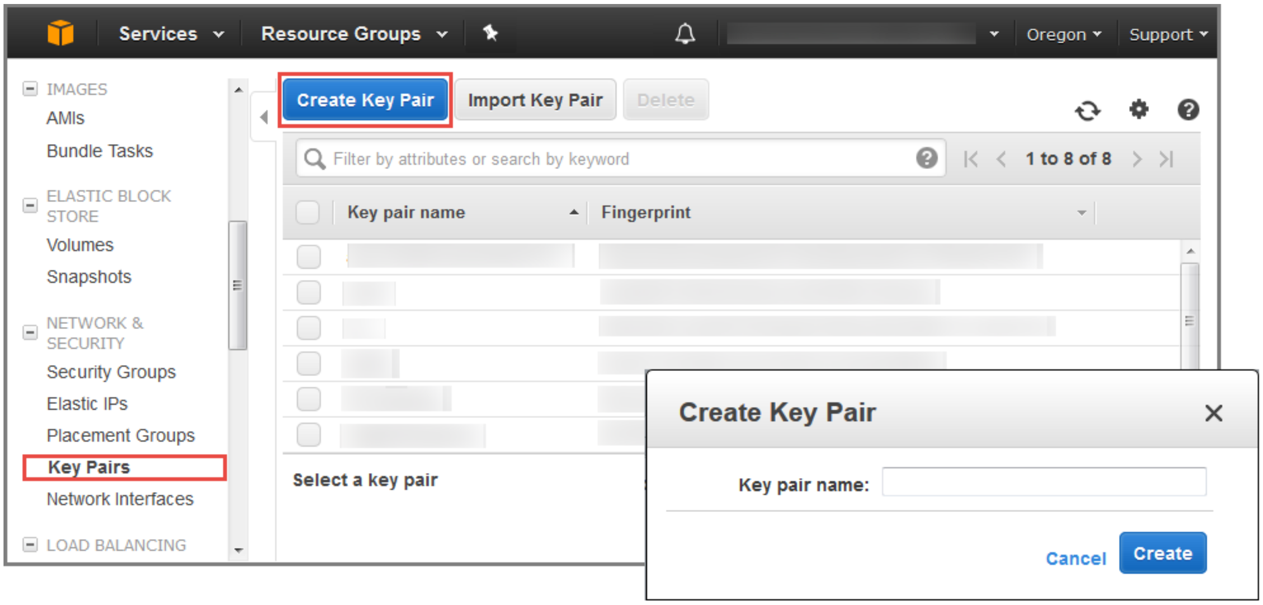


Figure 3: Creating a key pair

Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. To be able to log in to your instances, you must create a key pair. On Linux, the key pair is used to authenticate SSH login.

Step 2. Launch the Stack

1. If you are using the CentOS operating system, subscribe to the CentOS AMI in AWS Marketplace.

2. Use one of the following options to launch the Quick Start into your AWS account. (For more information about these options, see Deployment Scenarios.)

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

   Launch Quick Start (for new VPC)

   Launch Quick Start (for existing VPC)

   Each stack takes approximately 5 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. For cost estimates, see the pricing pages for each AWS service you will be using in this Quick Start.

3. On the **Select Template** page, keep the default setting for the Amazon S3 template URL, and then choose **Next**.

4. On the **Specify Details** page, review the parameters for the template, provide values for parameters that require your input, and customize the default settings as necessary. For example, you can change the instance types or IP addresses for the bastion host instances, or choose a banner that is displayed when you connect to the bastion host.

   In the following tables, parameters are listed and described separately for deploying the bastion host 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 public 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.

- **Option 1: Parameters for deploying Linux bastion hosts into a new VPC**

  View the template for new VPC

  Network Configuration:

Parameter label (name)	Default	Description
Availability Zones (AvailabilityZones)	*Requires input*	The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and 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.
Public Subnet 1 CIDR (PublicSubnet1CIDR)	10.0.128.0/20	CIDR block for the public subnet located in Availability Zone 1.
Public Subnet 2 CIDR (PublicSubnet2CIDR)	10.0.144.0/20	CIDR block for the public subnet located in Availability Zone 2.
Allowed Bastion External Access CIDR (RemoteAccessCIDR)	*Requires input*	CIDR block that's allowed SSH external access to the bastion hosts. We recommend that you set this value to a trusted CIDR block. For example, you might want to restrict access to your corporate network.

  Amazon EC2 Configuration:

Parameter label (name)	Default	Description
Key Pair Name (KeyPairName)	*Requires input*	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.
Bastion AMI Operating System (BastionAMIOS)	Amazon-Linux-HVM	The Linux distribution for the AMI to be used for the bastion host instances. If you choose CentOS, make sure that you have a subscription to the CentOS AMI in AWS Marketplace.
Bastion Instance Type (BastionInstanceType)	t2.micro	EC2 instance type for the bastion host instances.

Linux Bastion Configuration:

Parameter label (name)	Default	Description
Number of Bastion Hosts (NumBastionHosts)	1	The number of Linux bastion hosts to run. Auto Scaling will ensure that you always have this number of bastion hosts running. The maximum is 4 bastion hosts.
Enable Banner (EnableBanner)	false	Includes or suppresses the banner that is displayed when you connect to the bastion host via SSH. To display the banner, set this parameter to **true**. (See section on customizing the banner.)
Bastion Banner (BastionBanner)	*default URL*	URL for the ASCII text file that contains the banner text to display upon login. (See section on customizing the banner.)
Enable TCP Forwarding (EnableTCPForwarding)	false	Setting this value to **true** will enable TCP forwarding (SSH tunneling). This can be very useful but it is also a security risk, so we recommend that you keep the default (disabled) setting unless required.
Enable X11 Forwarding (EnableX11Forwarding)	false	Setting this value to **true** will enable X Windows over SSH. X11 forwarding can be a useful tool but it is also a security risk, so we recommend that you keep the default (disabled) setting unless required.

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	quickstart-reference	S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you've created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.
Quick Start S3 Key Prefix (QSS3KeyPrefix)	linux/bastion/ latest	The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. 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).

- ## Option 2: Parameters for deploying Linux bastion hosts into an existing VPC

View the template for existing VPC

Network Configuration:

Parameter label (name)	Default	Description
VPC ID (VPCID)	*Requires input*	ID of your existing VPC (e.g., vpc-0343606e).
Public Subnet 1 ID (PublicSubnet1ID)	*Requires input*	ID of the public subnet you want to provision the first bastion host into (e.g., subnet-a0246dcd).
Public Subnet 2 ID (PublicSubnet2ID)	*Requires input*	ID of the public subnet you want to provision the second bastion host into (e.g., subnet-e3246d8e).
Allowed Bastion External Access CIDR (RemoteAccessCIDR)	*Requires input*	CIDR block that's allowed SSH external access to the bastion hosts. We recommend that you set this value to a trusted CIDR block. For example, you might want to restrict access to your corporate network.

Amazon EC2 Configuration:

Parameter label (name)	Default	Description
Key Pair Name (KeyPairName)	*Requires input*	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.
Bastion AMI Operating System (BastionAMIOS)	Amazon-Linux-HVM	The Linux distribution for the AMI to be used for the bastion host instances. If you choose CentOS, make sure that you have a subscription to the CentOS AMI in AWS Marketplace.
Bastion Instance Type (BastionInstanceType)	t2.micro	EC2 instance type for the bastion host instances.

Linux Bastion Configuration:

Parameter label (name)	Default	Description
Number of Bastion Hosts (NumBastionHosts)	1	The number of Linux bastion hosts to run. Auto Scaling will ensure that you always have this number of bastion hosts running. The maximum is 4 bastion hosts.
Enable Banner (EnableBanner)	false	Includes or suppresses the banner that is displayed when you connect to the bastion host via SSH. To display the banner, set this parameter to **true**. (See section on customizing the banner.)

Parameter label (name)	Default	Description
Bastion Banner (BastionBanner)	*default URL*	URL for the ASCII text file that contains the banner text to display upon login. (See section on customizing the banner.)
Enable TCP Forwarding (EnableTCPForwarding)	false	Setting this value to **true** will enable TCP forwarding (SSH tunneling). This can be very useful but it is also a security risk, so we recommend that you keep the default (disabled) setting unless it's required.
Enable X11 Forwarding (EnableX11Forwarding)	false	Setting this value to **true** will enable X Windows over SSH. X11 forwarding can be a useful tool but it is also a security risk, so we recommend that you keep the default (disabled) setting unless it's required.

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	quickstart-reference	S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you've created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.
Quick Start S3 Key Prefix (QSS3KeyPrefix)	linux/bastion/ latest	The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. 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).

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

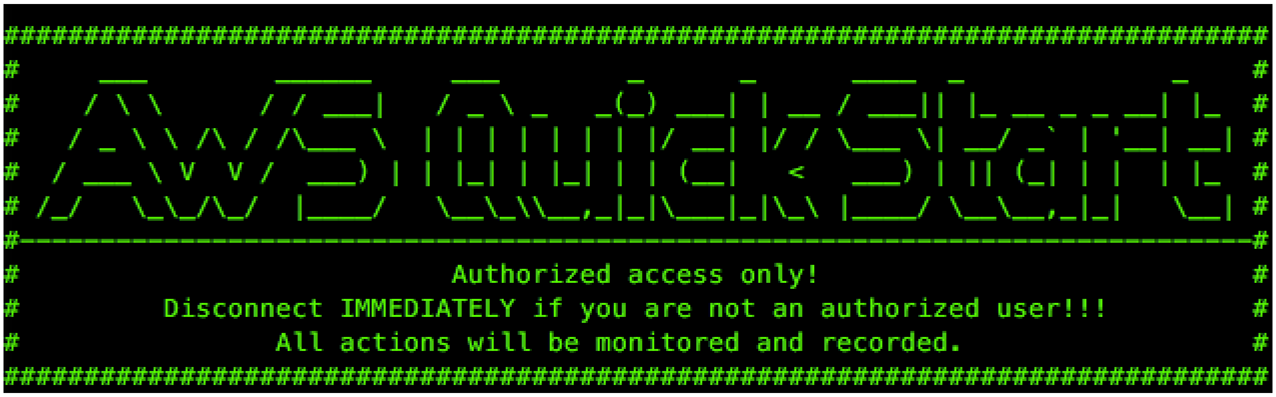
5. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you're done, choose **Next**.
6. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.
7. Choose **Create** to deploy the stack.
8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the stack is ready.

Step 3. Add AWS Services or Other Applications

After you use this Quick Start to build your VPC environment with Linux bastion hosts, you can deploy additional Quick Starts or deploy your own applications on top of this AWS infrastructure. If you decide to extend your AWS environment with additional Quick Starts for trial or production use, we recommend that you choose the option to deploy the Quick Start into an existing VPC, where that option is available.

Customizing the Linux Bastion Host Banner

This Quick Start provides the default banner illustrated in Figure 4 for the Linux bastion hosts. The banner is suppressed by default, but you can enable it by setting the **EnableBanner** parameter to **true** during deployment.



```
###########################################################################
#                                                                         #
#     ___        ______     ___        _      _     ____  _             _ #
#    / \ \      / / ___|   / _ \ _   _(_) ___| | __/ ___|| |_ __ _ _ __| |_ #
#   / _ \ \ /\ / /\___ \  | | | | | | | |/ __| |/ /\___ \| __/ _` | '__| __| #
#  / ___ \ V  V /  ___) | | |_| | |_| | | (__|   <  ___) | || (_| | |  | |_ #
# /_/   \_\_/\_/  |____/   \__\_\\__,_|_|\___|_|\_\|____/ \__\__,_|_|   \__| #
#-------------------------------------------------------------------------#
#                        Authorized access only!                          #
#          Disconnect IMMEDIATELY if you are not an authorized user!!!    #
#                 All actions will be monitored and recorded.             #
###########################################################################
```

Figure 4. Default banner for Linux bastion hosts

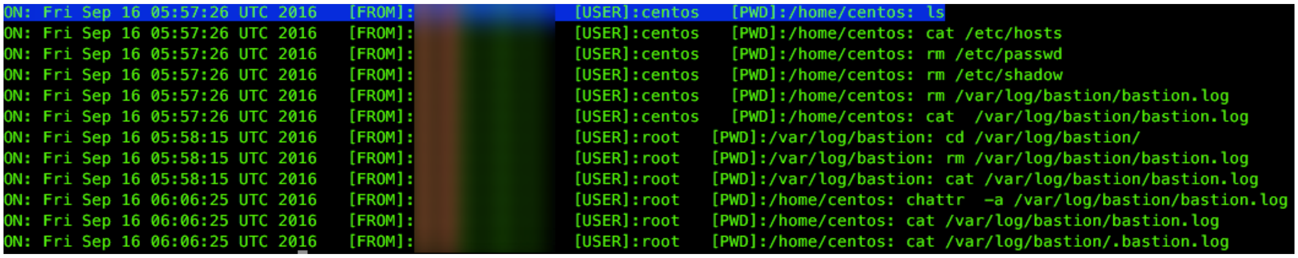
To customize the banner, you can create a ASCII text file with your own banner content, upload it to an S3 bucket or other publicly accessible location, and make sure that it is accessible from the host.

Bastion Logging

The bastion hosts deployed by this Quick Start provide a command logger in the `/var/log/bastion/bastion.log` file. This log file contains the following information: the date, the SSH client connection IP address, the user name, the working directory, and the commands issued.

For added security, the contents of the `/var/log/bastion/bastion.log` file is also stored in a CloudWatch Logs log group in the AWS Cloud, and will remain available in case the bastion hosts fail.

The log includes a history of all the commands that are executed when a user logs in. For example, Figure 5 shows a log that recorded that a user logged in through a specific IP address and attempted to remove the password file as a standard user, and then escalated to root access and tried to remove the bastion log.



```
ON: Fri Sep 16 05:57:26 UTC 2016    [FROM]:[redacted]   [USER]:centos    [PWD]:/home/centos: ls
ON: Fri Sep 16 05:57:26 UTC 2016    [FROM]:[redacted]   [USER]:centos    [PWD]:/home/centos: cat /etc/hosts
ON: Fri Sep 16 05:57:26 UTC 2016    [FROM]:[redacted]   [USER]:centos    [PWD]:/home/centos: rm /etc/passwd
ON: Fri Sep 16 05:57:26 UTC 2016    [FROM]:[redacted]   [USER]:centos    [PWD]:/home/centos: rm /etc/shadow
ON: Fri Sep 16 05:57:26 UTC 2016    [FROM]:[redacted]   [USER]:centos    [PWD]:/home/centos: rm /var/log/bastion/bastion.log
ON: Fri Sep 16 05:57:26 UTC 2016    [FROM]:[redacted]   [USER]:centos    [PWD]:/home/centos: cat  /var/log/bastion/bastion.log
ON: Fri Sep 16 05:58:15 UTC 2016    [FROM]:[redacted]   [USER]:root   [PWD]:/var/log/bastion: cd /var/log/bastion/
ON: Fri Sep 16 05:58:15 UTC 2016    [FROM]:[redacted]   [USER]:root   [PWD]:/var/log/bastion: rm /var/log/bastion/bastion.log
ON: Fri Sep 16 05:58:15 UTC 2016    [FROM]:[redacted]   [USER]:root   [PWD]:/var/log/bastion: cat /var/log/bastion/bastion.log
ON: Fri Sep 16 06:06:25 UTC 2016    [FROM]:[redacted]   [USER]:root   [PWD]:/home/centos: chattr  -a /var/log/bastion/bastion.log
ON: Fri Sep 16 06:06:25 UTC 2016    [FROM]:[redacted]   [USER]:root   [PWD]:/home/centos: cat /var/log/bastion/bastion.log
ON: Fri Sep 16 06:06:25 UTC 2016    [FROM]:[redacted]   [USER]:root   [PWD]:/home/centos: cat /var/log/bastion/.bastion.log
```

Figure 5. Command logger for bastion hosts

If you'd like to notify your users that all their commands will be monitored and logged, we recommend that you enable the bastion host banner, as described in the previous section. The default banner text includes the alert shown in Figure 4, and you can customize the wording as necessary.

The bastion.log file has the immutable bit set, so it cannot be easily removed or tampered with. If a malicious user does find the bastion.log file, somehow gains root privileges, removes the protections, and deletes the log file, there is a shadow file that contains a copy of the log. The shadow file is located in `/var/log/bastion/.bastion.log`. The shadow file is just a copy—an attacker can find and delete it. For this reason, the Quick Start also stores the contents of the bastion.log file remotely using the CloudWatch Logs service. The log files can be found under CloudWatch Logs using the instance ID as the log stream name.

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 in the `C:\cfn\log` folder.)

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.

The following table lists specific **CREATE_FAILED** error messages you might encounter.

Error message	Possible cause	What to do
API: ec2: RunInstances Not authorized for images: *ami-ID*	The template is referencing an AMI that has expired.	We refresh AMIs on a regular basis, but our schedule isn't always synchronized with AWS AMI updates. If you get this error message, notify us, and we'll update the template with the new AMI ID. If you'd like to fix the template yourself, you can download it and update the `Mappings` section with the latest AMI ID for your region.
We currently do not have sufficient *instance-type* capacity in the AZ you requested	Your resources require a larger or different instance type.	Switch to an instance type that supports higher capacity. If a higher-capacity instance type isn't available, try a different Availability Zone or region. Or you can complete the request form in the AWS Support Center to increase the Amazon EC2 limit for the instance type or region. Limit increases are tied to the region they were requested for.
Instance *ID* did not stabilize	You have exceeded your IOPS for the region.	Request a limit increase by completing the request form in the AWS Support Center.
In order to use this AWS Marketplace product you need to accept terms and subscribe. To do so please visit *URL*.	You've changed the **BastionAMIOS** parameter setting to CentOS, but you don't have a subscription to the CentOS operating system.	Subscribe to the CentOS AMI in AWS Marketplace, and then redeploy the Quick Start.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website. If the problem you encounter isn't covered on that page or in the table, please visit the AWS Support Center. If you're filing a support ticket, please attach the install.log file from the master instance (this is the log file that is located in the `/root/install` folder) to the ticket.

Q. I changed the instance type parameter after deployment and updated the stack, but the instance types didn't change or the Elastic IP addresses weren't reassociated after the stack update.

A. Terminate your bastion host instances. They will be replaced by Auto Scaling. The new instances will undergo bootstrapping, which configures the security settings and CloudWatch logs, and associates Elastic IP addresses from the pool of IPs created as part of the stack.

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.

Security

This Quick Start provisions one Linux bastion host in each Availability Zone with a single security group as a virtual firewall. This security group is required for remote access from the Internet. The security group is configured as follows:

Inbound:

Source	Protocol	Ports
Remote access CIDR	TCP	22
Remote access CIDR	ICMP	N/A

Outbound:

Destination	Protocol	Ports
0.0.0.0/0	All	All

For additional details, see Security in Your VPC in the Amazon VPC documentation.

Additional Resources

AWS services

- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/
- Amazon EC2
  – User guide for Linux:
    https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/

  - Elastic IPs
    https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

- Amazon VPC
  https://aws.amazon.com/documentation/vpc/

  - Security groups
    https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

  - Bastion host servers
    https://blogs.aws.amazon.com/security/post/Tx3N8GFK85UN1G6/Securely-connect-to-Linux-instances-running-in-a-private-Amazon-VPC

Quick Start reference deployments

- AWS Quick Start home page
  https://aws.amazon.com/quickstart/

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 Auto Scaling group, CloudWatch Logs, and additional configuration options	Changes in templates and throughout guide
September 2016	Initial publication	—

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.