Corda Blockchain on the AWS Cloud

Quick Start Reference Deployment

Contents

This Quick Start was created by R3 in collaboration with Amazon Web Services (AWS).

Quick Starts are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying Corda on the Amazon Web Services (AWS) Cloud.

Corda Blockchain on AWS

Corda is a blockchain technology platform built to transform the way the world does business. Using smart contract and blockchain technology, Corda allows existing business networks to reduce transaction and record-keeping costs and to streamline business operations. Corda was designed to meet the highest standards of the most complex and highly regulated industries in the world. Specifically, Corda is designed to address the privacy and scalability concerns of traditional public blockchain systems while maintaining the global interoperability needed to power real world commerce.

Corda on AWS is a production-ready implementation of a Corda node, which offers built-in resilience and high availability and which can scale as the needs of the node operator change.

This Quick Start is for IT infrastructure architects, administrators, DevOps professionals, CorDapp developers, or business users who are planning to implement a Corda node deployment on the AWS Cloud.

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. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

This Quick Start includes a 60-day trial license that provides limited access to Corda features. The terms of the license can be found on the R3 website. To utilize the deployment created by this Quick Start after this trial, you will need to obtain a Corda license by contacting sales@r3.com.

Architecture

Deploying this Quick Start for a new virtual private cloud (VPC) with **default parameters** builds the following Corda environment in the AWS Cloud.
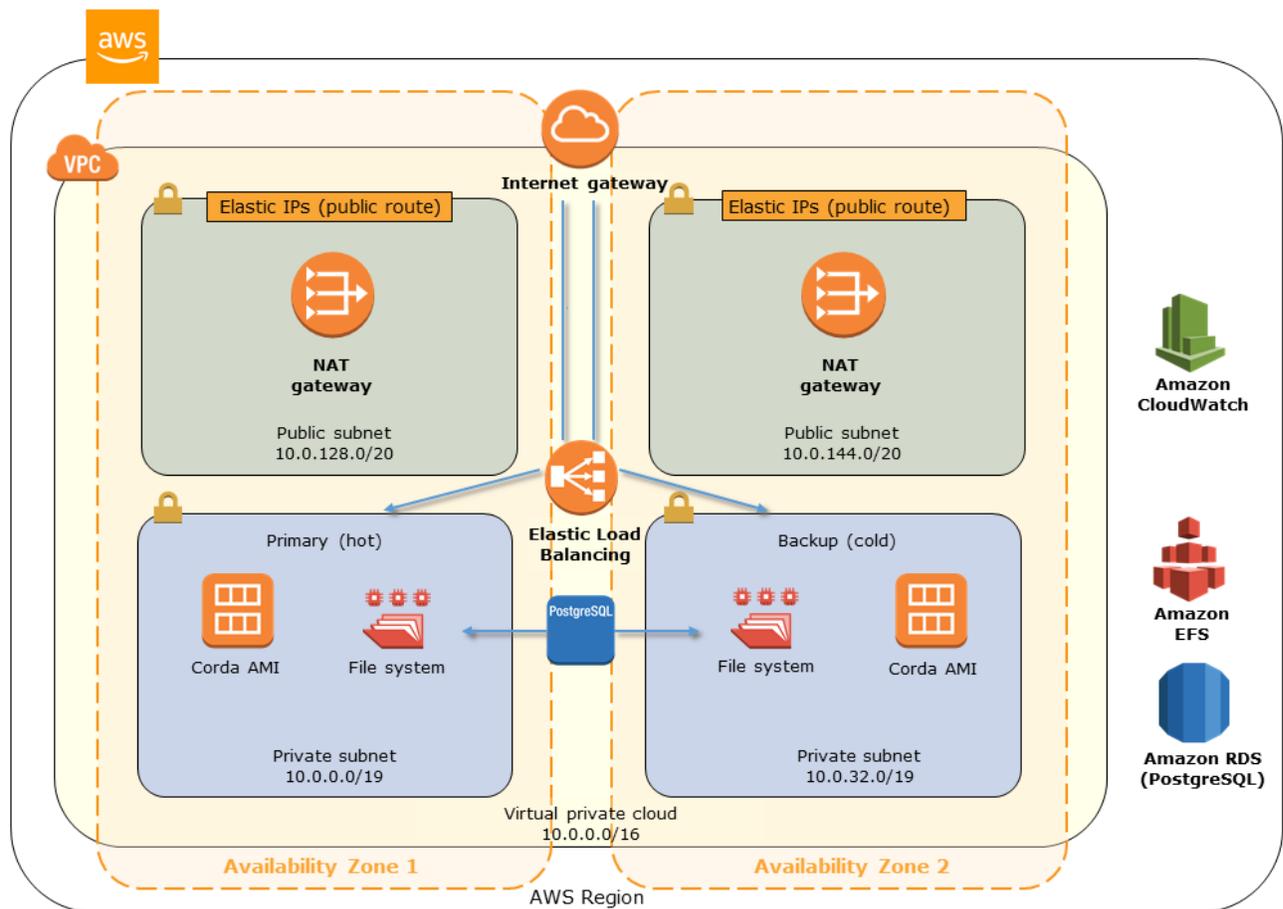
Figure 1: Quick Start architecture for Corda on AWS

The Quick Start sets up the following:

- A virtual private cloud (VPC) configured across two Availability Zones with public and private subnets according to AWS best practices.*

- An internet gateway to allow access to the internet.*

- Managed NAT gateways to allow outbound internet access for the Corda node instances.*

- A logical Corda node with hot-cold instances across the two Availability Zones.

- Security groups for each instance, which restrict access to only the necessary protocols and ports.

- Elastic Load Balancing (ELB) load balancers to load-balance remote procedure calls (RPCs), and P2P traffic over TCP to the highly available Corda node instances.

- An Amazon Relational Database Service (Amazon RDS) PostgreSQL managed database instance configured for the Corda Vault and pertinent node state, such as check-pointing and keeping track of identities.

- An Amazon Elastic File System (Amazon EFS) instance shared by the instances across Availability Zones.

- Amazon CloudWatch logging of resources and Corda node.

* The template that deploys the Quick Start into an existing VPC skips the tasks marked by asterisks and prompts you for your existing VPC configuration.

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 EC2
- Amazon EBS
- Amazon VPC
- AWS CloudFormation
- Amazon RDS for PostgreSQL
- Elastic Load Balancing
- Amazon Elastic File System
- Amazon CloudWatch

We recommend that you also become familiar with Corda key concepts including Corda nodes.

Technical Requirements: Corda Network

This Quick Start will create a deployment of a single logical Corda node. This Corda node will need to connect to a Corda network of other Corda nodes in order to transact. By default, the template is configured for connection to the Corda Testnet. To provision your AWS based node to this Testnet, you will need a ONE-TIME KEY, which you can obtain by signing up for the Corda Testnet at http://testnet.corda.network/ and creating a node (the key is valid for one hour). After you have obtained the key, paste it into the **One-time key** parameter field in the template (see the parameter tables in step 3). Your node will automatically provision and connect to Testnet when you run the template.

Deployment Options

This Quick Start provides two deployment options:

- **Deploy Corda into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, subnets, NAT gateways, security groups, and other infrastructure components, and then deploys Corda into this new VPC.

- **Deploy Corda into an existing VPC**. This option provisions Corda in your existing AWS infrastructure.

The Quick Start provides separate templates for these options. It also lets you configure CIDR blocks, instance types, and Corda settings, as discussed later in this guide.

Instance Selection

Minimum recommended specification for a Corda instance type is a t2.large, which is set as the default. (For more information on instance types, see the AWS Website.) If you want more performance—for example to make use of the multi-threading performance available with Corda—you can choose from a number of instance types in the Quick Start parameters. The Corda software will automatically scale the number of threads to the available virtual CPUs (vCPUs), with 4 threads per vCPU.

The following table gives an indication of the performance gain of adding vCPUs.

Instance throughput:

# vCPUs	Thread count	Transactions per second (Issue)	Transactions per second (Issue+Pay)
1	4	90	14
2	8	100	22
4	16	225	46

# vCPUs	Thread count	Transactions per second (Issue)	Transactions per second (Issue+Pay)
8	32	350	70
16	64	730	130
32	128	1001	205

For more information about Issue+Pay, see the Corda documentation.

Deployment Steps

Step 1. Prepare Your AWS Account

1. If you don't already have an AWS account, create one at https://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 Corda on AWS.
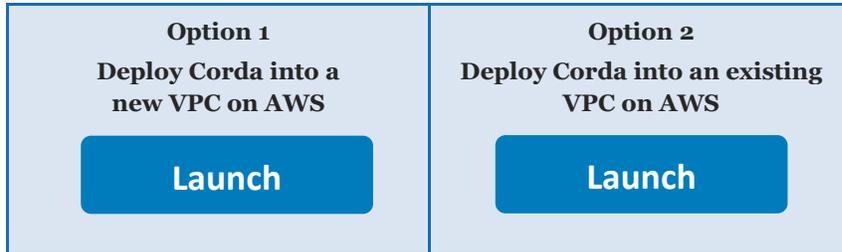
> **Note**   This Quick Start uses Amazon Elastic File System and can be deployed only in regions where it is available. For a list of supported regions for Amazon EFS, see the AWS Regions and Endpoints webpage.

3. Create a key pair in your preferred region.

4. If necessary, request a service limit increase for the Amazon EC2 instance type selected in the parameters (the default is t2.large). 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 deployment.

Step 2. Launch the Quick Start

> **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 full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see deployment options earlier in this guide.

Option 1 Deploy Corda into a new VPC on AWS	Option 2 Deploy Corda into an existing VPC on AWS
Launch	**Launch**

> **Important**   If you're deploying Corda into an existing VPC, make sure that your VPC has two private subnets in different Availability Zones for the database instances. These subnets require NAT gateways or NAT instances in their route tables, to allow the instances to download packages and software without exposing them to the internet. You will also need the domain name option configured in the DHCP options as explained in the Amazon VPC documentation. You will be prompted for your VPC settings when you launch the Quick Start.

Each deployment takes about 30 minutes to complete.

2. Check the 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 your Corda node will be built. The template is launched in the US East (Ohio) Region by default.

> **Note**   This Quick Start uses Amazon Elastic File System and can be deployed only in regions where it is available. For a list of supported regions for Amazon EFS, see the AWS Regions and Endpoints webpage.

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

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

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

   – Parameters for deploying a Corda node into a new VPC

– Parameters for deploying a Corda node into an existing VPC

- **Option 1: Parameters for deploying a Corda node into a new VPC**

View template

Network Configuration (new VPC):

Parameter label (name)	Default	Description
Availability Zones (AvailabilityZones)	*Requires input*	The list of Availability Zones to use for the subnets in the VPC. Only two Availability Zones are used for this deployment, and the logical order of your selections is preserved.
Number of used Availability Zones (NumberOfAZs)	2	The number of Availability Zones to use in the VPC.
Public Subnet 1 CIDR (PublicSubnet1CIDR)	10.0.128.0/20	CIDR block for the public (DMZ) subnet 1 located in Availability Zone 1.
Public Subnet 2 CIDR (PublicSubnet2CIDR)	10.0.144.0/20	CIDR block for the public (DMZ) subnet 2 located in Availability Zone 2.
VPC CIDR (VPCCIDR)	10.0.0.0/16	CIDR block for the VPC to create.

Corda Configuration:

Parameter label (name)	Default	Description
Allowed SSH access CIDR (RemoteAccessCIDR)	*Requires input*	Allowed CIDR block for external SSH access
Allowed Corda ports CIDR (CordaAccessCIDR)	*Requires input*	Allowed CIDR block for Corda access.
Allowed Corda RPC access CIDR (CordaRPCAccessCIDR)	*Requires input*	Allowed CIDR block for RPC access.
Corda instance type (InstanceType)	t2.large	Amazon EC2 instance type for the Corda node.
SSH key name (KeyPairName)	*Requires input*	The name of an existing public/private key pair, which allows you to securely connect to your instance after it launches.
City (Location)	*Requires input*	The city or location to which the node is associated. This does not need to be where the node is physically located.

Parameter label (name)	Default	Description
Country code (CountryCode)	*Requires input*	The ISO 3166-1 alpha 2 code of the country to which the node is associated. This does not need to be where the node is physically located.
One-time key (OneTimeKey)	*Requires input*	The one-time key that you received when you created a new node on Corda Testnet (the code is valid for 1 hour).
Corda Testnet endpoint (TestnetEndpoint)	https://testnet.corda. network	The base URL of Corda Testnet.

Corda RDS Configuration:

Parameter label (name)	Default	Description
Database storage size (in GiB) (DBAllocatedStorage)	16	The size of the database in gigabytes (GiB).
Automatic upgrade to new Amazon Aurora minor versions (DBAutoMinorVersionUpgrade)	true	Select true to set up Auto Minor Version upgrade.
Database backup retention period (DBBackupRetentionPeriod)	7	The number of days for which automatic database snapshots are retained.
Amazon Aurora database instance type (DBInstanceClass)	db.r4.large	The name of the compute and memory capacity class of the database instance.
Database IOPS (DBIops)	1000	The rate of database input/output operations per second. This parameter is used only when you specify io1 for the DBStorageType property.
Database master password (DBMasterUserPassword)	*Requires input*	The database admin account password. Must be at least 8 characters and contain letters, numbers, and symbols.
Database master user name (DBMasterUsername)	cordauser	The database admin account user name.
Enable Multi-AZ deployment for database instance (DBMultiAZ)	true	Specifies whether the database instance is a multiple Availability Zone deployment. This Quick Start deploys two Availability Zones, so this parameter should always be set to true.
Database name (DBName)	CordaQuickstartDB	The name of the Corda Quick Start database.
Database storage type (DBStorageType)	gp2	The storage type associated with this database instance.

aws

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	quickstart-reference	The S3 bucket you have 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)	quickstart-r3-corda/	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.

- **Option 2: Parameters for deploying a Corda node into an existing VPC**

   View template

   Network Configuration:

Parameter label (name)	Default	Description
Public Subnet 1 ID (PublicSubnet1ID)	*Requires input*	ID of the public subnet in Availability Zone 1.
Public Subnet 2 ID (PublicSubnet2ID)	*Requires input*	ID of the public subnet in Availability Zone 2.
Private Subnet 1 ID (PrivateSubnet1ID)	*Requires input*	ID of the private subnet in Availability Zone 1.
Private Subnet 2 ID (PrivateSubnet2ID)	*Requires input*	ID of the private subnet in Availability Zone 2.
VPC CIDR (VPCCIDR)	10.0.0.0/16	CIDR block for the existing VPC.
VPC ID (VPCID)	*Requires input*	ID of your existing VPC (e.g., vpc-0343606e).

Corda Configuration:

Parameter label (name)	Default	Description
City (Location)	*Requires input*	The city or location to which the node is associated. This does not need to be where the node is physically located.

Country code (CountryCode)	*Requires input*	The ISO 3166-1 alpha-2 code of the country to which the node is associated. This does not need to be where the node is physically located.
One-time key (OneTimeKey)	*Requires input*	The one-time key that you received when you created a new node on Corda Testnet (the code is valid for 1 hour).
Corda Testnet endpoint (TestnetEndpoint)	https://testnet.corda.network	The base URL of Corda Testnet.
SSH key name (KeyPairName)	*Requires input*	The name of an existing public/private key pair, which allows you to securely connect to your instance after it launches.
Allowed SSH access CIDR (RemoteAccessCIDR)	*Requires input*	Allowed CIDR block for external SSH access.
Allowed Corda access (CordaAccessCIDR)	*Requires input*	Allowed CIDR block for Corda access.
Allowed Corda RPC access CIDR (CordaRPCAccessCIDR)	*Requires input*	Allowed CIDR block for Corda RPC access.
Corda instance type (InstanceType)	t2.large	Amazon EC2 instance type for the Corda nodes.

Corda RDS Configuration:

Parameter label (name)	Default	Description
Database storage size (in GiB) (DBAllocatedStorage)	16	The size of the database in gigabytes (GiB).
Automatic upgrade to new Amazon Aurora minor versions (DBAutoMinorVersionUpgrade)	true	Select true to set up Auto Minor Version upgrade.
Database backup retention period (DBBackupRetentionPeriod)	7	The number of days for which automatic database snapshots are retained.
Amazon Aurora database instance type	db.r4.large	The name of the compute and memory capacity class of the database instance.
DB IOPS (DBIOPS)	1000	The rate of database input/output operations per second. This parameter is used only when you specify io1 for the DBStorageType property.
DB master password (DBMasterUserPassword)	*Requires input*	The database admin account password. Must be at least 8 characters and contain letters, numbers, and symbols.
DB master user name (DBMasterUsername)	cordauser	The database admin account user name.

Enable Multi-AZ deployment for database instance (DBMultiAZ)	true	Specifies whether the database instance is a multiple Availability Zone deployment. This Quick Start deploys two Availability Zones, so this parameter should always be set to true.
Database name (DBName)	CordaQuickstartDB	The name of the Corda Quick Start database.
Database storage type (DBStorageType)	gp2	The storage type associated with this database instance.

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	aws-quickstart	The S3 bucket you have 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)	quickstart-r3-corda/	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.

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 Corda node cluster is ready.

9. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.

Step 3. Test the Deployment

You can test the deployment of your Corda node by following the steps in the documentation for using the Node Explorer to test a Corda node on Corda Testnet.

Best Practices Using Corda on AWS

Corda nodes need to stay in sync with their network of peers and ordering services. There are 2 key stores of state in the Corda node, the Corda Vault which is a SQL database hosted by the Amazon RDS PostgreSQL service and the message queue which is based on Artemis and is hosted on the shared Amazon EFS. The Quick Start template sets these up to be both backed up and shared between the primary and the backup instances of Corda.

For details on the hot-cold deployment of Corda, see the [Corda documentation](#).

You can configure the default retention period of database snapshots in the database configuration parameters in the Quick Start.

Corda is also multi-threaded by default and will expand the number of workers to make use of the available vCPUs.

Security

Key Management

Corda utilizes public key infrastructure for transaction signing. Good key management process is important for the security of your applications and assets. By default, the node will connect to the Corda Testnet which auto generates keys and provisions these to your node. This is for convenience and demonstration purposes and must not be used for production use. Before running transactions with real assets, the node will need to [generate a secure key-pair](#) locally and [register](#) with a production Corda network.

Troubleshooting

Q. I encountered a CREATE_FAILED error when I launched the Quick Start.

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. (Look at the log files in CloudWatch.)

> **Important**   When you set **Rollback on failure** to **No**, you will continue to incur AWS charges for this stack. Please make sure 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 about AWS CloudFormation limits, see the AWS documentation.

Git Repository

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

Additional Resources

AWS services

- Amazon EBS
  https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html

- Amazon EC2
  https://aws.amazon.com/documentation/ec2/

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

- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/

Corda documentation

- Corda Documentation
  http://docs.corda.r3.com/

Quick Start reference deployments

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

Document Revisions

Date	Change	In sections
August 2018	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.

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.