ClassicLink Mirror on AWS

AWS Implementation Guide

Becky Weiss

September 2016

Contents

About This Guide

This implementation guide discusses architectural considerations and configuration steps for deploying the ClassicLink Mirror solution on the Amazon Web Services (AWS) cloud. It includes links to AWS CloudFormation templates that launch, configure, and run the AWS compute, network, storage, and other services required to deploy this solution on AWS, using AWS best practices for security and availability.

The guide is intended for IT infrastructure architects, administrators, and DevOps professionals who have practical experience architecting on the AWS Cloud.

Overview

ClassicLink Mirror is an AWS-provided, open-source solution for replicating (mirroring) EC2-Classic security groups to a new environment in Amazon Virtual Private Cloud (Amazon VPC). This solution is especially useful when performing complicated migrations between the two platforms because it mirrors network security settings in EC2 Classic to the corresponding (target) VPC network environment.

Background: Migrating from EC2-Classic to Amazon VPC

Two key challenges arise when planning for migration of an application from one network to another. One is maintaining connectivity, as it is common for cloud applications to consist of multiple services that require interconnectivity within the network, i.e. over private IP addresses. The other is maintaining proper access between applications while the migration is in progress.

One way to complete a migration is to replicate the old network structure in the new network, and then move the entire deployment from one network to the other. However, this requires application downtime and so, for availability reasons, many customers prefer to carry out migration in a more incremental manner.

In January 2015, AWS released a feature called *ClassicLink*[1] which allows customers to associate (link) EC2-Classic instances with Amazon VPC security groups in the same AWS Region, enabling private communication between the two platforms. This communication facilitates incremental migrations to Amazon VPC, allowing customers to migrate individual components while maintaining communication between older EC2-Classic instances and new EC2 instances running in a virtual private cloud (VPC).

In some cases, the migration is completed rapidly and this association is straightforward. However, over the course of a longer-term migration, the set of EC2-Classic instances might change due to manual capacity adjustments or Auto Scaling rules. Furthermore, EC2-Classic security group rules might be added or removed, and it will be necessary to mirror those changes to the corresponding VPC security groups as well.

The ClassicLink Mirror solution automates these tasks. It monitors appropriately tagged EC2-Classic security groups, and whenever there is change in their rules or instance memberships, it will replicate those changes in the associated VPC to help keep the networks consistent (mirrored) during migration. The mirroring actions are unidirectional: the user need only update the EC2-Classic security groups and ClassicLink Mirror will

[1] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-classiclink.html

overwrite/update the Amazon VPC side accordingly. See the Architecture Overview for detailed information.

Cost

You are responsible for the cost of the AWS services used while running this solution. There is no additional cost for deploying the automated solution. As of the date of publication, the cost for running this solution is negligible—for most customers the estimated cost will be less than a penny a month.

AWS Lambda pricing is based on invocation count and duration.[2] Therefore, the cost of running ClassicLink Mirror automation depends primarily on the frequency with which relevant Amazon EC2 APIs are called from your account (see the appendix for a complete list). For smaller deployments, each invocation of the Lambda function can be expected to complete in under five (5) seconds. Monitor your monthly AWS Lambda bill for a detailed breakdown of service costs incurred while running this solution.

Prices are subject to change. For full details, see the pricing webpage for each AWS service you will be using in this solution.

Architecture Overview

Deploying this solution with the **default parameters** builds the following environment in the AWS Cloud.

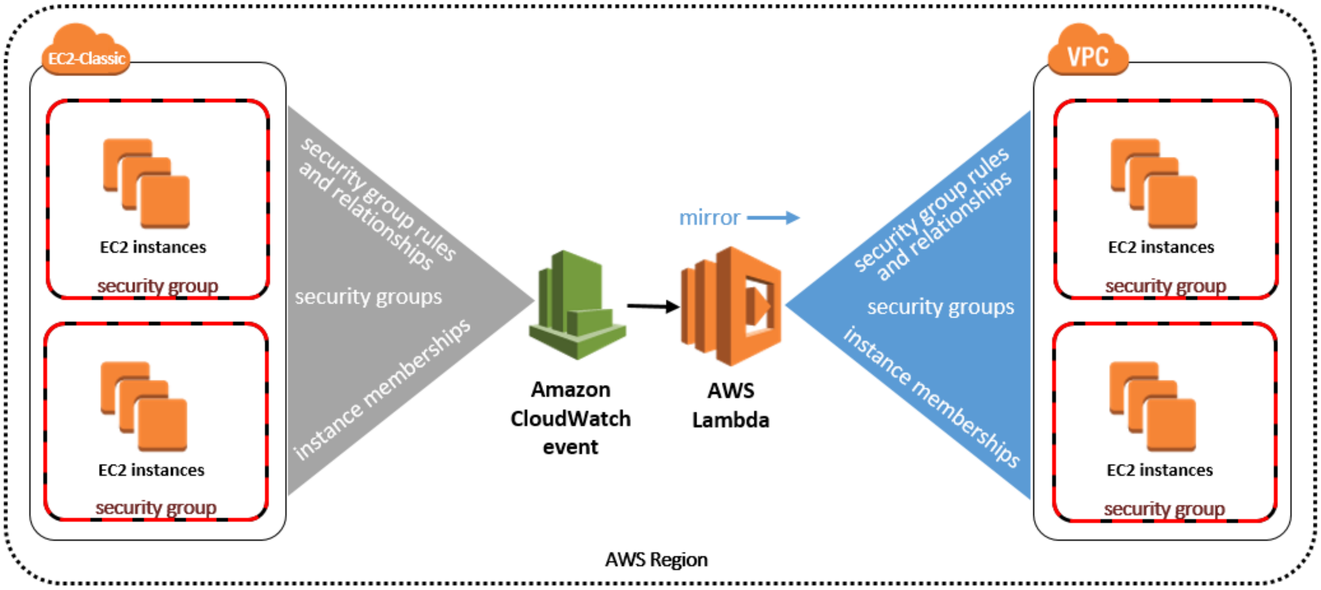

Figure 1: ClassicLink Mirror on AWS

[2] https://aws.amazon.com/lambda/pricing/

The AWS CloudFormation template creates an Amazon CloudWatch event rule, which invokes the solution's AWS Lambda function after a relevant EC2 API call is made (see the appendix).

> **Note:** AWS CloudTrail is necessary to emit a CloudWatch event after an API call, therefore you must manually enable AWS CloudTrail in your account before deploying this solution (see Prerequisites).

After launching the AWS CloudFormation template, the user must create the virtual private cloud (VPC) to migrate to, and enable ClassicLink on that VPC. The user must also identify the EC2-Classic security groups for ClassicLink Mirror to manage, and manually assign them tags that contain the VPC ID (see Step 3. Tag Your EC2-Classic Security Groups). Once ClassicLink Mirror is configured, it will create and manage a set of mirrored security groups in that VPC.

When invoked, the ClassicLink Mirror Lambda function audits the tagged EC2-Classic security groups for any changes (such as rule changes or new instance memberships), and completes the appropriate action to maintain a mirror in the VPC. This includes the following actions:

- **Create an analogous VPC security group** if one does not yet exist. ClassicLink Mirror will give the VPC security group the same name as the EC2-Classic security group, and add a tag (`classiclinkmirror:mirroredFromClassicSecurityGroupId`) that contains the associated EC2-Classic security group ID in the tag value. Likewise, ClassicLink Mirror will add a tag (`classiclinkmirror:mirroredToVpcSecurityGroupId`) to the original EC2-Classic security group that contains the associated VPC security group ID in the tag value. Thus, you will be able to see the relationships between your EC2-Classic security groups and those that ClassicLink Mirror is managing in your VPC.
- **Identify any differences in security group rules and sync them** (on the VPC side). For example, if you recently authorized SSH traffic from 55.55.55.55/32 to your EC2-Classic security group, ClassicLink Mirror will add the same rule to the VPC security group. Similarly, if you dropped that rule from the EC2-Classic security group, ClassicLink Mirror will revoke that rule on the corresponding VPC security group. If the new rule references another EC2-Classic security group that is also managed by ClassicLink Mirror, ClassicLink Mirror will find the source group's counterpart in your VPC and authorize a similar relationship in the VPC security group.

  See Implementation Considerations for information about exceptions to this actions (i.e., security group rules that ClassicLink Mirror will not revoke.)

- **Discover any new members of the EC2-Classic security group and link them to the VPC** using ClassicLink to make them members of the corresponding VPC security group. Most customers will include ClassicLink in their automatic deployment processes, such as an Auto Scaling group that uses a launch configuration to automatically link new EC2-Classic instances to a VPC at launch. But, we include this action in the solution to serve as a backup check for instances that were provisioned manually.

Implementation Considerations

- **ClassicLink Mirror fully manages the VPCs it creates**, specifically any security group with the tag:
  `classiclinkmirror:mirroredFromClassicSecurityGroupId`
  If you attempt to authorize or revoke rules on a VPC security group that ClassicLink Mirror manages, those changes will be undone the next time ClassicLink Mirror runs, in order to keep the VPC security group in sync with its corresponding EC2-Classic security group.

  The exception to this is references to VPC security groups that do not have equivalents in EC2-Classic. For example, in EC2 Classic, Elastic Load Balancing instances that are members of a special, shared Elastic Load Balancing security group. However, in Amazon VPC the Elastic Load Balancing network interface has its own customer-managed security group that is attached to a VPC. Therefore, because Elastic Load Balancing configuration is not parallel between the two platforms, ClassicLink Mirror will not revoke an Elastic Load Balancing security group rule on the VPC side.

- **You can create a ClassicLink association only between a single EC2-Classic instance and a single VPC**. Therefore, if you have an EC2-Classic instance that is a member of two EC2-Classic security groups, and the ClassicLink Mirror tags on those groups point to two different VPCs, there is no way for ClassicLink Mirror to link the instance to both VPCs, and thus it will not create a ClassicLink association for that instance at all.

- **ClassicLink Mirror deployments are regional:** If you have EC2-Classic instances in multiple AWS Regions, you must deploy ClassicLink Mirror independently in each region that has instances you want to automatically manage.

> **Note:** Do not deploy ClassicLink Mirror more than once per AWS Region, as you might incur unnecessary AWS Lambda charges. If you wish to link EC2-Classic instances in the same region to different VPCs, you need only identify a different VPC in the instance tag (see Step 3. Tag Your EC2-Classic Security Groups).

AWS CloudFormation Templates

This solution uses AWS CloudFormation to bootstrap AWS infrastructure and automate the deployment of ClassicLink Mirror on the AWS Cloud from scratch. It includes the following CloudFormation templates, which you can download before deployment:

View template

classiclink-mirror.template: This is the primary solution template you use to launch ClassicLink Mirror and all associated components. The default configuration automates common tasks during a migration from EC2-Classic to Amazon VPC, but you can also customize the template based on your specific needs.

Automated Deployment

Before you launch the automated deployment, please review the architecture, configuration, and other considerations discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy ClassicLink Mirror into your account.

Time to deploy: Approximately 5 minutes

Prerequisites

Enable AWS CloudTrail

ClassicLink Mirror requires AWS CloudTrail in order to use API calls to generate a CloudWatch event.[3] Therefore, you must turn on AWS CloudTrail before deploying this solution. For detailed instructions, refer to the AWS CloudTrail documentation.[4]

Configure a Test Environment

It is best practice to test an automated solution before deploying it to production resources. This solution includes an AWS CloudFormation template that creates a simple EC2-Classic stack for testing purposes (see Testing).

Alternatively, you can launch some EC2-Classic instances for a test deployment, and then configure and modify their security groups to verify the ClassicLink Mirror functionality.

[3] http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/WhatIsCloudWatchEvents.html

[4] http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.html

What We'll Cover

The procedure for deploying this architecture on AWS consists of the following steps. For detailed instructions, follow the links for each step.

Step 1. Launch the Stack

- Launch the AWS CloudFormation template into your AWS account.
- Enter values for the required parameter: **Stack Name**

Step 2. Create a VPC

- Create the VPC to mirror to, and enable ClassicLink on that VPC.

Step 3. Tag Your EC2-Classic Security Groups

- Apply the custom tag to applicable security groups in EC2 Classic.

Step 1. Launch the Stack

This automated AWS CloudFormation template deploys ClassicLink Mirror on the AWS Cloud.

> **Note**: You are responsible for the cost of the AWS services used while running this solution. See the Cost section for more details. For full details, see the pricing webpage for each AWS service you will be using in this solution.

1. Log in to the AWS Management Console and click the button to the right to launch the *classic-mirror* AWS CloudFormation template.

   Launch Solution

   You can also download the template as a starting point for your own implementation.

2. The template is launched in the US East (N. Virginia) Region by default. To launch the ClassicLink Mirror in a different AWS Region, use the region selector in the console navigation bar.

   > **Note**: This solution is for EC2-Classic customers and uses the AWS Lambda service. You must launch this solution in an AWS Region that supports both AWS Lambda[5] and EC2-Classic: ap-northeast-1, eu-west-1, us-east-1, us-west-2

3. On the **Select Template** page, verify that you selected the correct template and choose **Next**.

4. On the **Specify Details** page, assign a name to your ClassicLink Mirror stack.

[5] For the most current AWS Lambda availability by region, see https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/

5. On the **Options** page, choose **Next**.
6. On the **Review** page, review and confirm the settings. Be sure to check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
7. Choose **Create** to deploy the stack.

   You can view the status of the stack in the AWS CloudFormation Console in the **Status** column. You should see a status of CREATE_COMPLETE in roughly five (5) minutes.
8. To quickly test the ClassicLink Mirror AWS Lambda function, you can make a relevant API call (see the appendix), and then check the ClassicLink Mirror log files in CloudWatch Logs to confirm the Lambda function was invoked. Note that ClassicLink Mirror will not make changes to your resources at this point because you have not yet tagged any EC2-Classic security groups to be managed.

Step 2. Create a VPC

You must create the VPC that you will migrate your EC2-Classic resources to. After you create the VPC, there are no ongoing configuration tasks to complete because ClassicLink Mirror will fully manage it, ensuring that it mirrors your EC2-Classic environment throughout the duration of your migration.

1. Open the Amazon VPC console, make sure you are in the correct AWS Region, and in the left pane, choose **Your VPCs**.
2. Choose **Create VPC** and configure your network as necessary. (See Amazon VPC documentation for guidance.)
3. Enable ClassicLink on your new VPC. Select the VPC, right-click, and choose **Enable ClassicLink**.
4. Note the VPC ID (`vpc-xxxxxxxx`) to use in the next step of this deployment.

Step 3. Tag Your EC2-Classic Security Groups

You must assign tags to each EC2-Classic security group that you want ClassicLink Mirror to manage.

Use the following format:

- Tag name: `classicmirror:linkToVPC`
- Tag value: <The VPC ID noted in the previous procedure, e.g., `vpc-11112222`>

Within a few minutes, you will see that the AWS Lambda function was invoked and completed the following actions: created a VPC security group analogous to the EC2-Classic security group that you tagged; copied over its rules; and linked (via ClassicLink) any member EC2 instances to that VPC security group.

Testing

This solution includes an additional AWS CloudFormation template that you can use to quickly launch an EC2-Classic test environment in your AWS account.

1. Click the button to the right to launch the *classic-mirror-test* AWS CloudFormation template.
   You can also download the template.

   Launch Test Stack

2. On the **Specify Details** page, assign a name to your test stack.
3. Under **Parameters**, modify the following values (this is not required):

Parameter	Default	Description
AllowSSHFromRange	<Optional input>	If you want to connect to the backend instances using SSH, provide a CIDR range for inbound SSH traffic.
KeyName	<Optional input>	For SSH connection, provide the public/private EC2 key pair name.
ServiceInstanceCount	1	Modify the number of instances as necessary.
ServiceInstancePortNumber	8080	Modify this value if you want the backend instances to use a different service port.

   When the stack build completes, you will have a three-instance (t1.micro), Elastic Load Balancing load-balancer-fronted service in EC2-Classic. This includes two security groups: one that allows Elastic Load Balancing to talk to the backend instances; and one that allows SSH access to the backend instances from an IP range you provide.

4. Choose the **Outputs** tab. In the **Value** column, go to the public URL for this test service. The webpage will show a reply identifying one of the backend servers you launched.
5. Complete the procedures in the Automated Deployment section and verify that the security groups were correctly mirrored from this test environment to your new VPC. Modify the EC2-Classic security groups to verify that ClassicLink Mirror replicates those changes on the Amazon VPC side.

Additional Resources

AWS services documentation

- AWS CloudFormation
- ClassicLink in the Amazon VPC User Guide
- Amazon VPC

Appendix: Relevant EC2 API Calls

The following API calls will trigger the Amazon CloudWatch event that invokes the ClassicLink Mirror AWS Lambda function:

- `AuthorizeSecurityGroupIngress`
- `CreateTags`
- `DeleteSecurityGroup`
- `DeleteTags`
- `RevokeSecurityGroupIngress`

An Amazon CloudWatch event is also generated when the state of an EC2-Classic instance changes to **running**.

Send Us Feedback

We welcome your questions and comments. Please post your feedback on the AWS Solutions Discussion Forum.

Document Revisions

Date	Change	In sections
September 2016	Initial release	—

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.