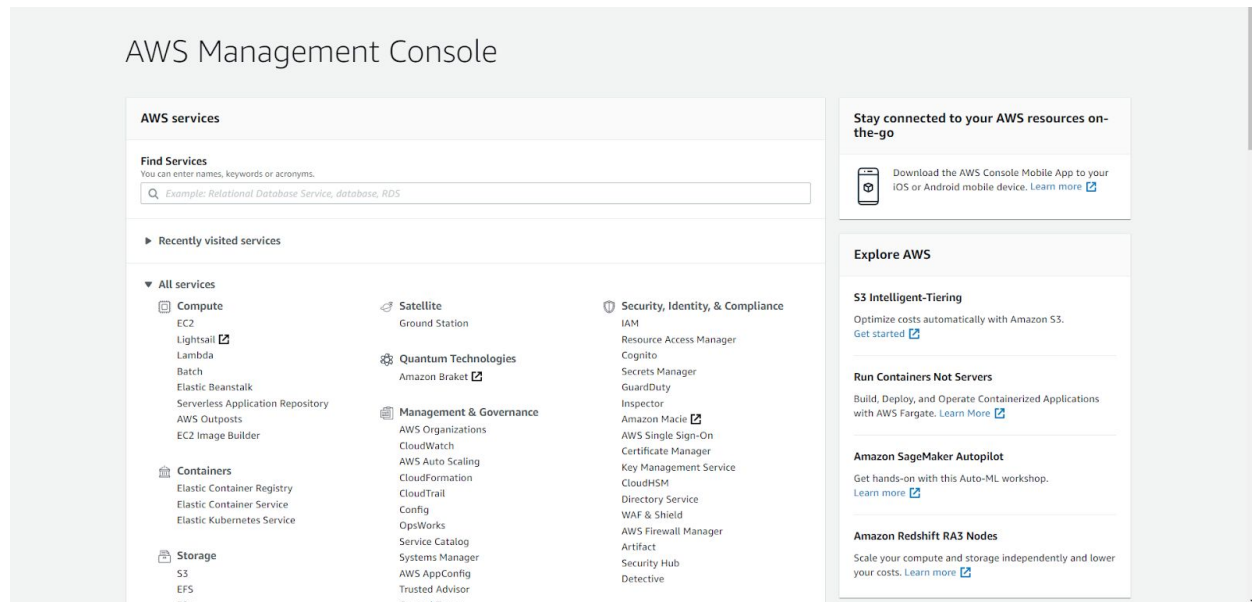


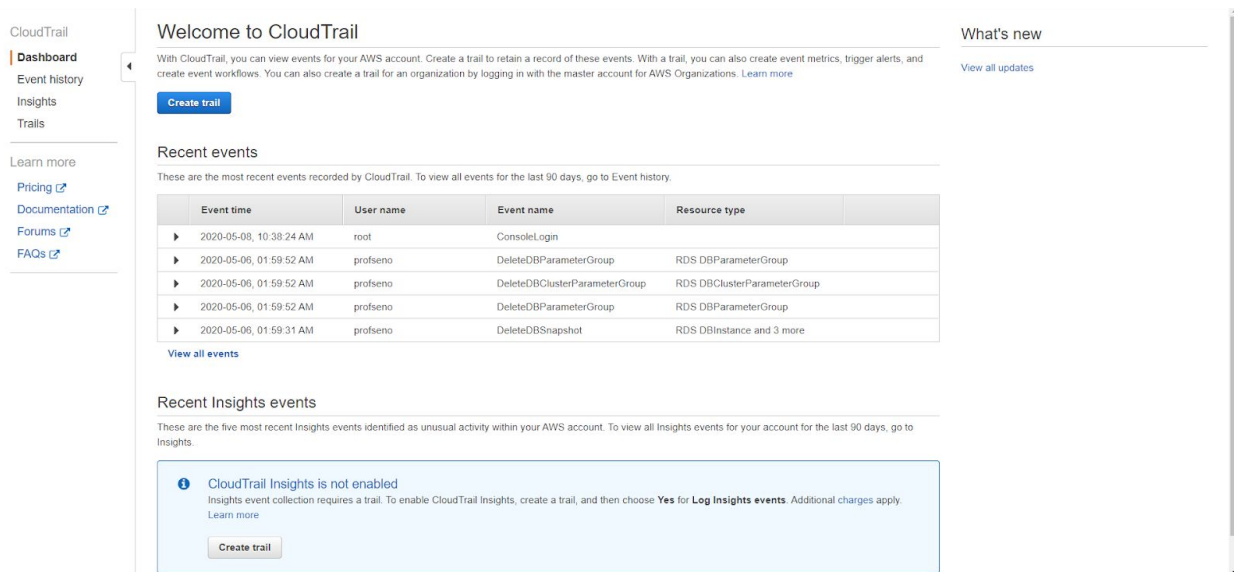
Module 4 Lab 1: CloudTrail Trail

AWS Management Console



Start with selecting CloudTrail.

CloudTrail - Create Trail



For longer term use, a trail needs S3 bucket access.

CloudTrail - Create Trail

CloudTrail
Dashboard
Event history
Insights
Trails

Learn more
Pricing [Pricing](#)
Documentation [Documentation](#)
Forums [Forums](#)
FAQs [FAQs](#)

Creating a trail might incur charges. For more information, see [AWS CloudTrail Pricing](#).

Create Trail

Trail name*

Apply trail to all regions ☒ Yes ☐ No
Creates the same trail in all regions and delivers log files for all regions

Management events

Management events are records of actions that are performed on or within resources in your AWS account. These are also known as control plane operations. [Learn more](#)

Read/Write events ☒ All ☐ Read-only ☐ Write-only ☐ None ⓘ

Log AWS KMS events ☒ Yes ☐ No ⓘ

Insights events

Insights events are records that capture an unusual call volume of **write management APIs** in your AWS account. Additional charges apply. [Learn more](#)

Log Insights events ☐ Yes ☒ No

Data events

Data events are records of resource operations performed on or within a resource. These are also known as data plane operations. Additional charges apply. [Learn more](#)

☒ S3 ☐ Lambda

You can record S3 object-level API activity (for example, GetObject and PutObject) for individual buckets, or for all current and future buckets in your AWS account. Additional charges apply. [Learn more](#)

A new S3 bucket to store the Trail log will be created.

Amazon S3

idtraillogs-spring20 > AWSLogs > 758287676861 > CloudTrail > us-west-1 > 2020 > 05 > 08

idtraillogs-spring20

Press Enter to search. Press ESC to clear.

Create folder Download Actions

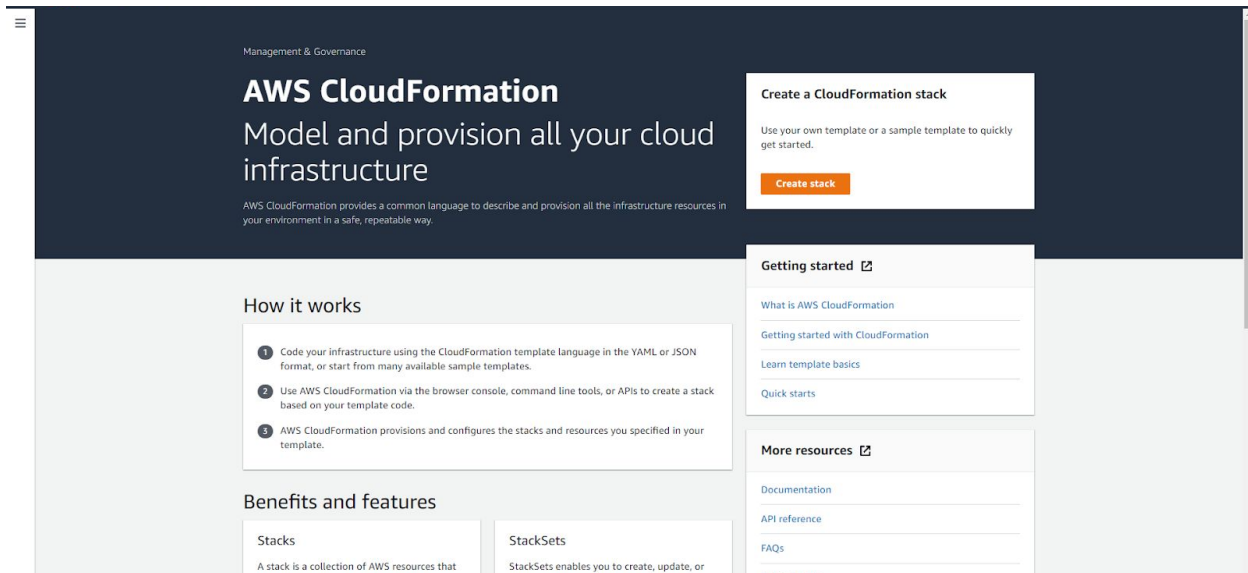
US West (N. California) ↻

Viewing 1 to 1

	Last modified ▼	Size ▼	Storage class ▼
l_CloudTrail_us-west-1_20200508T1810Z_hu9ejpmQVhRF5AI.json.gz	May 8, 2020 11:17:12 AM GMT-0700	1.2 KB	Standard

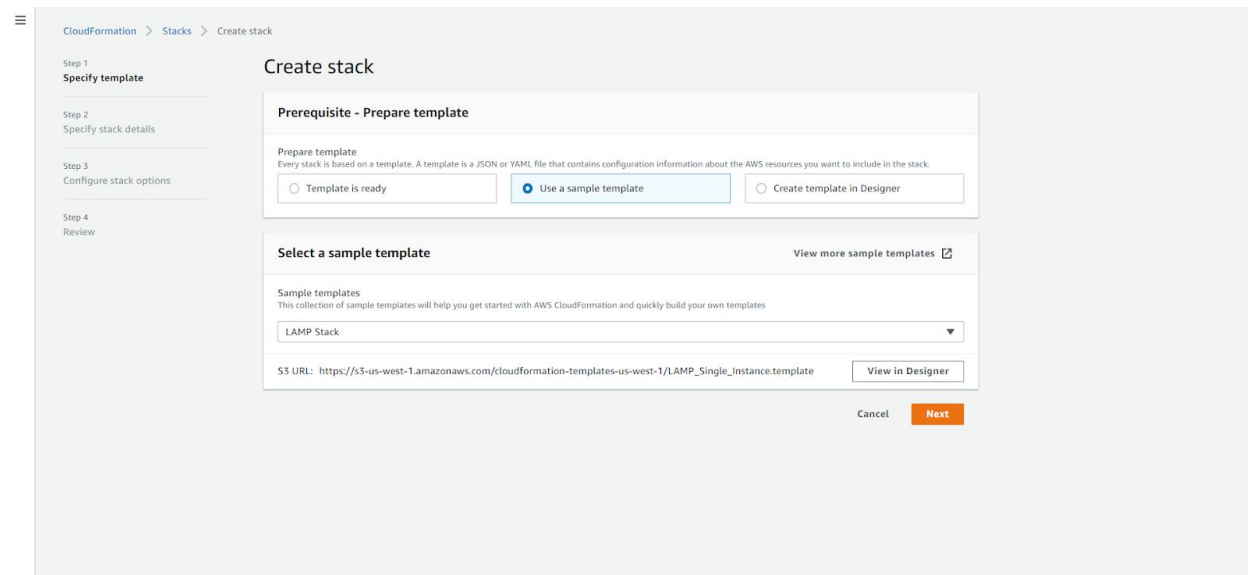
Viewing 1 to 1

The S3 bucket has been created and shows a Trail in the us-west-1 location.



In order to create a larger set of logs to view, AWS CloudFormation is used to create a stack.

CloudFormation - Create stack



The CloudFormation stack is created using a pre-existing sample LAMP Stack.

CloudFormation - Create stack

The screenshot shows the 'Specify stack details' step in the AWS CloudFormation console. On the left, a sidebar lists four steps: Step 1: Specify template, Step 2: Specify stack details (active), Step 3: Configure stack options, and Step 4: Review. The main content area is titled 'Specify stack details' and contains several input fields. The 'Stack name' field is filled with 'myLampStack'. Below it, a note states: 'Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-)'. The 'Parameters' section includes fields for 'DBName' (MyDatabase), 'DBPassword' (masked with asterisks), 'DBRootPassword' (masked with asterisks), 'DBUser' (masked with asterisks), and 'InstanceType' (t2.small). A 'KeyName' field is also present with a note: 'Name of an existing EC2 KeyPair to enable SSH access to the instance'.

The sample Lamp stack settings.

CloudFormation - Create stack

The screenshot shows the 'Configure stack options' step in the AWS CloudFormation console. The sidebar on the left shows Step 3: Configure stack options as the active step. The main content area is titled 'Configure stack options' and includes sections for 'Tags', 'Permissions', and 'Advanced options'. The 'Tags' section has two input fields: 'useCase' and 'LAMP demo', with an 'Add tag' button and a 'Remove' button. The 'Permissions' section has an 'IAM role - optional' dropdown menu set to 'Sample-role-name' and a 'Remove' button. The 'Advanced options' section includes a 'Stack policy' section with a 'Define the resources that you want to protect from unintentional updates during a stack update.' and a 'Rollback configuration' section with a 'Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back.' link.

The remaining CloudFormation Lamp stack settings.

CloudFormation - Create stack

Step 2: Specify stack details

Step 3: Configure stack options

Step 4: Review

Step 1: Specify template

Template

Template URL
https://s3-us-west-1.amazonaws.com/cloudformation-templates-us-west-1/LAMP_Single_Instance.template

Stack description
AWS CloudFormation Sample Template LAMP_Single_Instance: Create a LAMP stack using a single EC2 instance and a local MySQL database for storage. This template demonstrates using the AWS CloudFormation bootstrap scripts to install the packages and files necessary to deploy the Apache web server, PHP and MySQL at instance launch time. ****WARNING**** This template creates an Amazon EC2 instance. You will be billed for the AWS resources used if you create a stack from this template.

Estimate cost

Step 2: Specify stack details

Parameters (7)

Search parameters

Key	Value
DBName	MyDatabase
DBPassword	*****
DBRootPassword	*****
DBUser	*****
InstanceType	t2.small
KeyName	dockerLabKey
SSHLocation	0.0.0.0/0

Review page before stack creation.

CloudFormation - myLampStack

CloudFormation > Stacks > myLampStack

Stacks (1)

Filter by stack name

Active View nested

myLampStack
2020-05-08 11:35:56 UTC-0700
CREATE_COMPLETE

myLampStack

Delete Update Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change sets

Overview

Stack ID
arn:aws:cloudformation:us-west-1:758287676861:stack/myLampStack/c12H050-915a-11ea-9d0f-02e07b6ae9e9

Description
AWS CloudFormation Sample Template LAMP_Single_Instance: Create a LAMP stack using a single EC2 instance and a local MySQL database for storage. This template demonstrates using the AWS CloudFormation bootstrap scripts to install the packages and files necessary to deploy the Apache web server, PHP and MySQL at instance launch time. ****WARNING**** This template creates an Amazon EC2 instance. You will be billed for the AWS resources used if you create a stack from this template.

Status
CREATE_COMPLETE

Status reason
-

Root stack
-

Parent stack
-

Created time
2020-05-08 11:35:56 UTC-0700

Deleted time
-

Updated time
-

Drift status
NOT_CHECKED

Last drift check time
-

Termination protection
Disabled

IAM role
-

Tags (1)

Stack-level tags will apply to all supported resources in your stack. You can add up to 200 unique tags for each stack.

The stack has successfully been created.

Amazon S3 - us-west-1

awslogs-spring20 / AWSLogs / 702627070001 / CloudTrail / us-west-1 / 2020 / 05 / 08

spring20

Press Enter to search. Press ESC to clear.

Folder Download Actions

US West (N. California)

Viewing 1 to 12

	Last modified ▼	Size ▼	Storage class ▼
_CloudTrail_us-west-1_20200508T1805Z_Ult2ouDRyUJCGN8.json.gz	May 8, 2020 12:16:46 PM GMT-0700	2.3 KB	Standard
_CloudTrail_us-west-1_20200508T1810Z_hu9ejpmQVnRF5Al.json.gz	May 8, 2020 11:17:12 AM GMT-0700	1.2 KB	Standard
_CloudTrail_us-west-1_20200508T1820Z_pz645E3Nv4omhNbv.json.gz	May 8, 2020 11:27:14 AM GMT-0700	6.8 KB	Standard
_CloudTrail_us-west-1_20200508T1825Z_Hlu6PFzSpSuj3C6jy.json.gz	May 8, 2020 11:31:52 AM GMT-0700	8.1 KB	Standard
_CloudTrail_us-west-1_20200508T1830Z_AqYHbworjKtHj1xj.json.gz	May 8, 2020 11:37:03 AM GMT-0700	1.2 KB	Standard
_CloudTrail_us-west-1_20200508T1835Z_pok33Kq9d8pQND.json.gz	May 8, 2020 11:44:11 AM GMT-0700	1.2 KB	Standard
_CloudTrail_us-west-1_20200508T1840Z_jxyX01msLyEEcao.json.gz	May 8, 2020 11:50:26 AM GMT-0700	3.9 KB	Standard
_CloudTrail_us-west-1_20200508T1845Z_0fUHVm18x2o2mrHd.json.gz	May 8, 2020 11:54:04 AM GMT-0700	1.2 KB	Standard
_CloudTrail_us-west-1_20200508T1850Z_GQVKh96C2vekorCQ.json.gz	May 8, 2020 11:56:56 AM GMT-0700	1.4 KB	Standard
_CloudTrail_us-west-1_20200508T1855Z_idhmkv0t0EFEZk5.json.gz	May 8, 2020 12:16:11 PM GMT-0700	1.1 KB	Standard
_CloudTrail_us-west-1_20200508T1900Z_Bu2x6nOTmMG3gc9.json.gz	May 8, 2020 12:07:06 PM GMT-0700	904.0 B	Standard
_CloudTrail_us-west-1_20200508T1905Z_KBmcseU9gs5THN8.json.gz	May 8, 2020 12:13:06 PM GMT-0700	5.6 KB	Standard

Viewing 1 to 12

The Trail created from the CloudFormation stack.