



SUMMIT
ONLINE

2 8

Security best practices: The Well-Architected Framework

Martin Beeby

Principal Developer Advocate

AWS Developer Relations



AWS Well-Architected

<https://aws.amazon.com/well-architected>

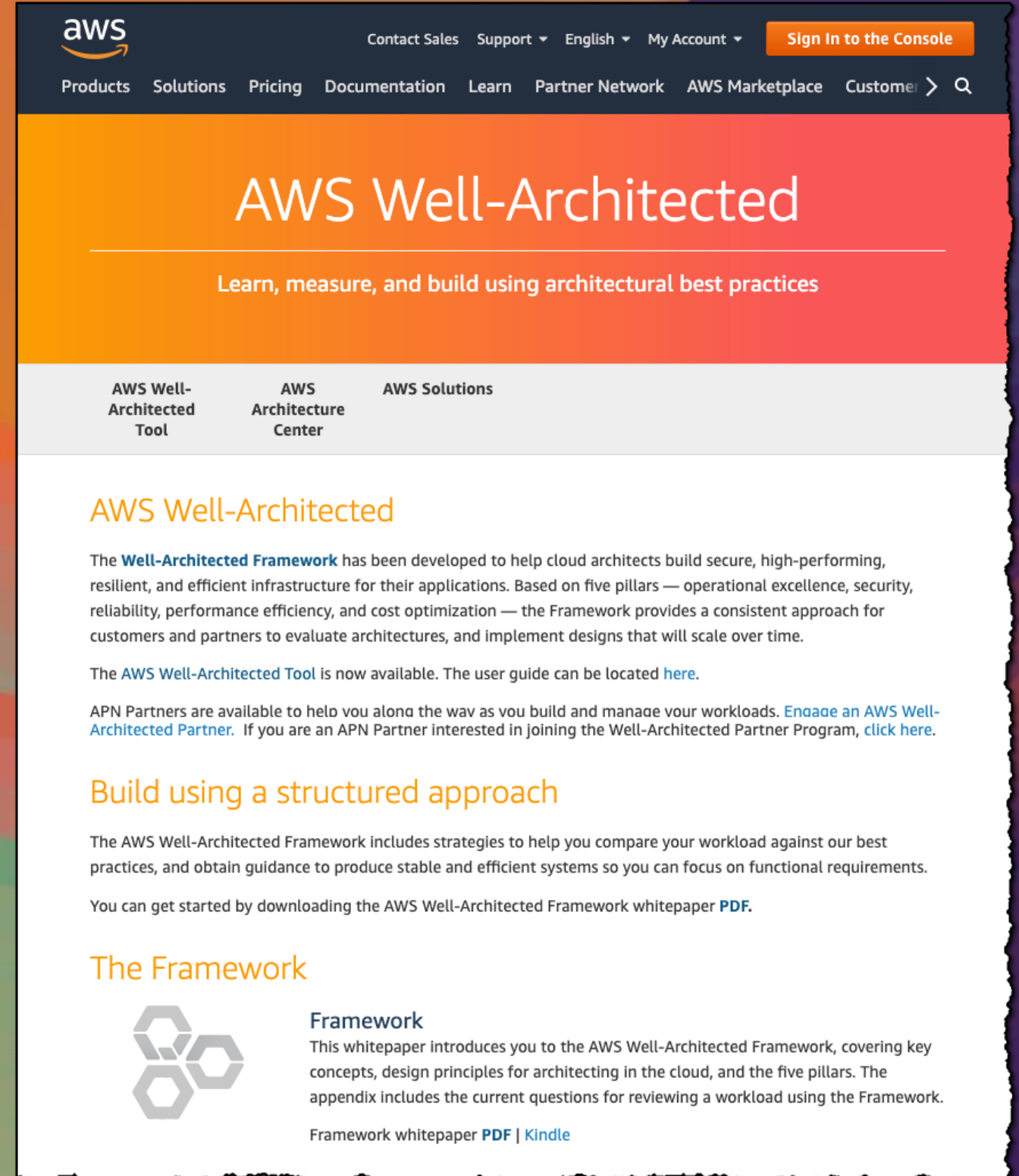
<https://wa.aws.amazon.com>

<https://wellarchitectedlabs.com>

The Well-Architected Framework

Developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications

<https://aws.amazon.com/well-architected>



The screenshot shows the AWS Well-Architected Framework landing page. At the top is the AWS logo and a navigation bar with links for Contact Sales, Support, English, My Account, and a Sign In to the Console button. Below the navigation bar is a header section with the title "AWS Well-Architected" and the subtitle "Learn, measure, and build using architectural best practices". A secondary navigation bar contains links for AWS Well-Architected Tool, AWS Architecture Center, and AWS Solutions. The main content area features a section titled "AWS Well-Architected" with a paragraph explaining the framework's purpose and five pillars. Below this is a section titled "Build using a structured approach" with a paragraph about the framework's strategies and a link to download the whitepaper. The final section is titled "The Framework" and includes a graphic of three interlocking hexagons, a sub-header "Framework", and a paragraph introducing the whitepaper. At the bottom of this section are links for the Framework whitepaper in PDF and Kindle formats.

aws

Contact Sales Support English My Account Sign In to the Console

Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer > Q

AWS Well-Architected

Learn, measure, and build using architectural best practices

AWS Well-Architected Tool AWS Architecture Center AWS Solutions

AWS Well-Architected

The **Well-Architected Framework** has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars — operational excellence, security, reliability, performance efficiency, and cost optimization — the Framework provides a consistent approach for customers and partners to evaluate architectures, and implement designs that will scale over time.

The **AWS Well-Architected Tool** is now available. The user guide can be located [here](#).


APN Partners are available to help you along the way as you build and manage your workloads. [Engage an AWS Well-Architected Partner](#). If you are an APN Partner interested in joining the Well-Architected Partner Program, [click here](#).

Build using a structured approach

The AWS Well-Architected Framework includes strategies to help you compare your workload against our best practices, and obtain guidance to produce stable and efficient systems so you can focus on functional requirements.

You can get started by downloading the AWS Well-Architected Framework whitepaper [PDF](#).

The Framework



Framework

This whitepaper introduces you to the AWS Well-Architected Framework, covering key concepts, design principles for architecting in the cloud, and the five pillars. The appendix includes the current questions for reviewing a workload using the Framework.

Framework whitepaper [PDF](#) | [Kindle](#)

What is the AWS Well-Architected Framework?



Pillars



Design principles



Questions



Build and deploy faster



Lower or mitigate risks



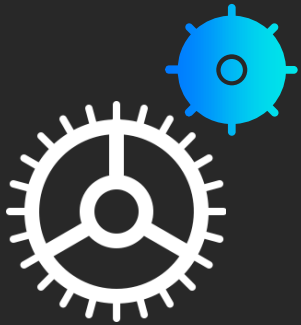
Make informed decisions



Learn AWS best practices

Why AWS Well-Architected Framework?

Are you Well-Architected?



Operational
excellence



Security



Reliability



Performance
efficiency



Cost
optimization

Design Principles for Security

Implement a strong identity foundation

Enable traceability

Apply security at all layers

Automate security best practices

Protect data in transit and at rest

Keep people away from data

Prepare for security events



Design Principles for Security

Implement a strong identity foundation

Enable traceability

Apply security at all layers

Automate security best practices

Protect data in transit and at rest

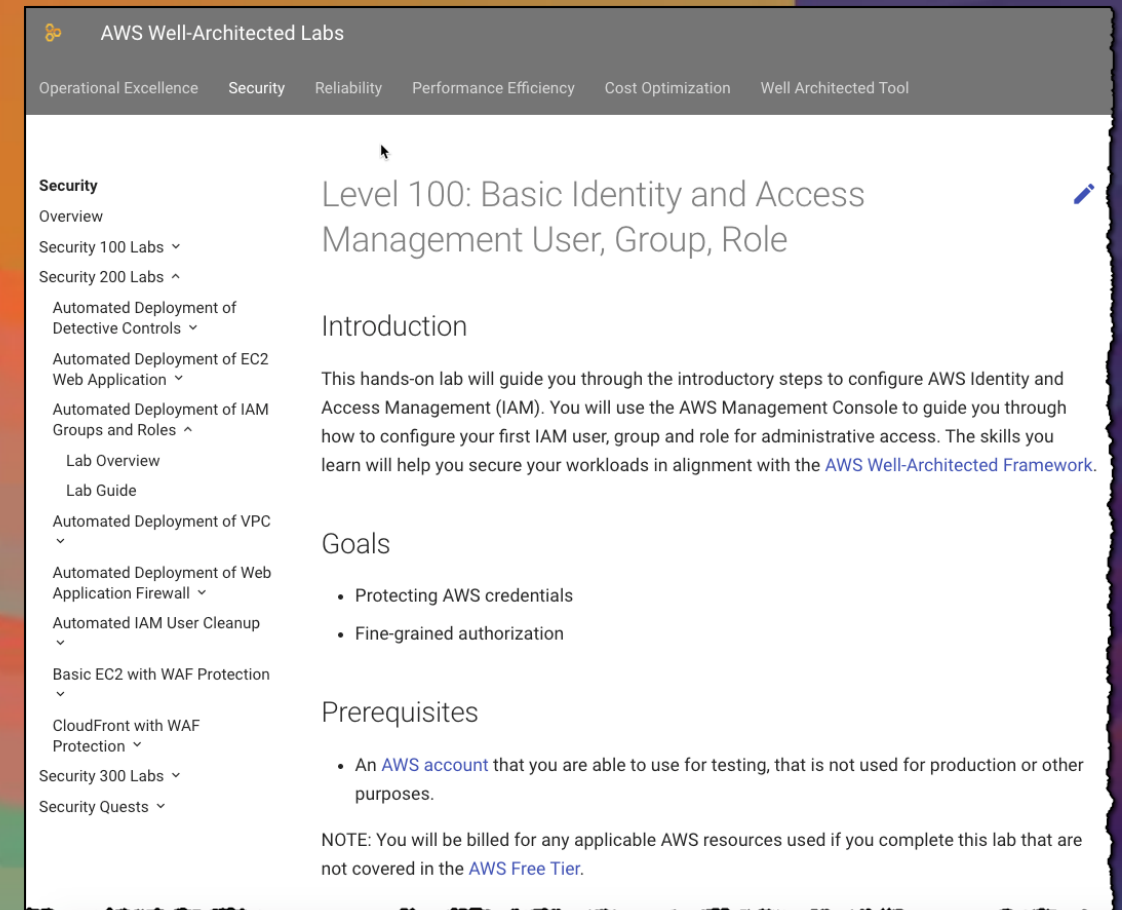
Keep people away from data

Prepare for security events



Labs

Basic Identity and Access Management



The screenshot shows the AWS Well-Architected Labs interface. The top navigation bar includes links for Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization, and Well Architected Tool. The left sidebar lists various lab categories under the 'Security' heading, including Overview, Security 100 Labs, Security 200 Labs, and several automated deployment labs. The main content area is titled 'Level 100: Basic Identity and Access Management User, Group, Role' and includes an edit icon. Below the title, there is an 'Introduction' section, a 'Goals' section with two bullet points, and a 'Prerequisites' section with one bullet point. A note at the bottom states that users will be billed for any applicable AWS resources used if they complete this lab that are not covered in the AWS Free Tier.

AWS Well-Architected Labs

Operational Excellence Security Reliability Performance Efficiency Cost Optimization Well Architected Tool

Security
Overview
Security 100 Labs ▾
Security 200 Labs ▲
Automated Deployment of Detective Controls ▾
Automated Deployment of EC2 Web Application ▾
Automated Deployment of IAM Groups and Roles ▲
Lab Overview
Lab Guide
Automated Deployment of VPC ▾
Automated Deployment of Web Application Firewall ▾
Automated IAM User Cleanup ▾
Basic EC2 with WAF Protection ▾
CloudFront with WAF Protection ▾
Security 300 Labs ▾
Security Quests ▾

Level 100: Basic Identity and Access Management User, Group, Role

Introduction

This hands-on lab will guide you through the introductory steps to configure AWS Identity and Access Management (IAM). You will use the AWS Management Console to guide you through how to configure your first IAM user, group and role for administrative access. The skills you learn will help you secure your workloads in alignment with the [AWS Well-Architected Framework](#).

Goals

- Protecting AWS credentials
- Fine-grained authorization


Prerequisites

- An [AWS account](#) that you are able to use for testing, that is not used for production or other purposes.

NOTE: You will be billed for any applicable AWS resources used if you complete this lab that are not covered in the [AWS Free Tier](#).

Labs

IAM based Access Control

 AWS Well-Architected Labs

Operational ExcellenceSecurityReliabilityPerformance EfficiencyCost OptimizationWell Architected Tool

Security

Overview

Security 100 Labs ▾

Security 200 Labs ▾

Security 300 Labs ▴

IAM Permission Boundaries Delegating Role Creation ▾

IAM Tag Based Access Control for EC2 ▴

Lab Overview

Lab Guide

Incident Response with AWS Console and CLI ▾

Lambda Cross Account IAM Role Assumption ▾

Lambda Cross Account Using Bucket Policy ▾

Incident Response Playbook with Jupyter ▾

Security Quests ▾

Level 300: IAM Tag Based Access Control for EC2

Introduction

This hands-on lab will guide you through the steps to configure example AWS Identity and Access Management (IAM) policies, and a AWS IAM role with associated permissions to use EC2 resource tags for access control. Using tags is powerful as it helps you scale your permission management, however you need to be careful about the management of the tags which you will learn in this lab.

In this lab you will create a series of policies attached to a role that can be assumed by an individual such as an EC2 administrator. This allows the EC2 administrator to create tags when creating resources only if they match the requirements, and control which existing resources and values they can tag.

The skills you learn will help you secure your workloads in alignment with the [AWS Well-Architected Framework](#).

Goals

Design Principles for Security

Implement a strong identity foundation

Enable traceability

Apply security at all layers

Automate security best practices

Protect data in transit and at rest

Keep people away from data

Prepare for security events

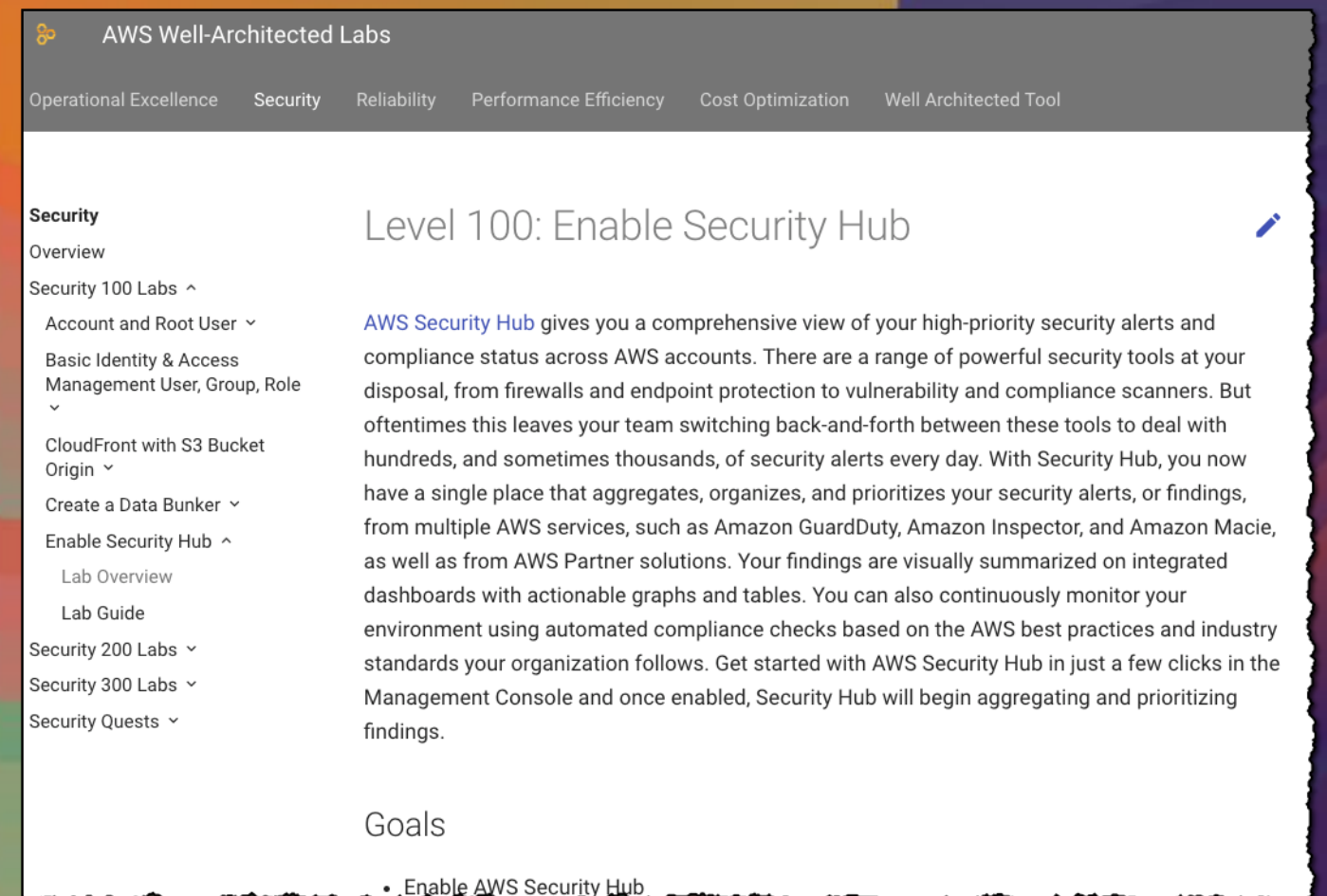


Enable traceability

- Monitor
- Alert
- Audit changes to your environment

Security Hub

AWS Security Hub gives you a comprehensive view of your high-priority security alerts and security posture across your AWS accounts.



Design Principles for Security

Implement a strong identity foundation

Enable traceability

Apply security at all layers

Automate security best practices

Protect data in transit and at rest

Keep people away from data

Prepare for security events



Design Principles for Security

Implement a strong identity foundation

Enable traceability

Apply security at all layers

Automate security best practices

Protect data in transit and at rest

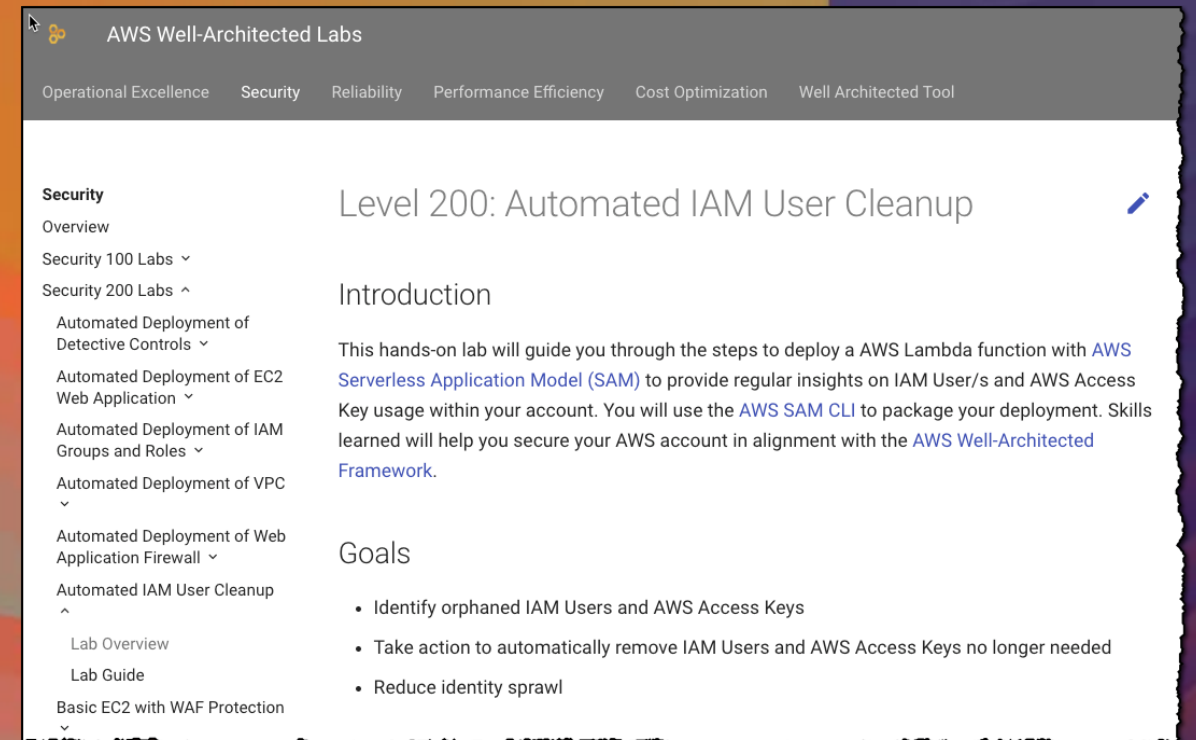
Keep people away from data

Prepare for security events



Labs

IAM automated cleanup



The screenshot shows the AWS Well-Architected Labs interface. The top navigation bar includes links for Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization, and Well Architected Tool. The left sidebar lists various labs under the 'Security' category, with 'Automated IAM User Cleanup' selected. The main content area displays the title 'Level 200: Automated IAM User Cleanup' with an edit icon, followed by an 'Introduction' section and a 'Goals' section with three bullet points.

AWS Well-Architected Labs

Operational Excellence Security Reliability Performance Efficiency Cost Optimization Well Architected Tool

Security

Overview

Security 100 Labs ▾

Security 200 Labs ▲

- Automated Deployment of Detective Controls ▾
- Automated Deployment of EC2 Web Application ▾
- Automated Deployment of IAM Groups and Roles ▾
- Automated Deployment of VPC ▾
- Automated Deployment of Web Application Firewall ▾
- Automated IAM User Cleanup ▲
- Lab Overview
- Lab Guide
- Basic EC2 with WAF Protection ▾

Level 200: Automated IAM User Cleanup

Introduction

This hands-on lab will guide you through the steps to deploy a AWS Lambda function with [AWS Serverless Application Model \(SAM\)](#) to provide regular insights on IAM User/s and AWS Access Key usage within your account. You will use the [AWS SAM CLI](#) to package your deployment. Skills learned will help you secure your AWS account in alignment with the [AWS Well-Architected Framework](#).

Goals

- Identify orphaned IAM Users and AWS Access Keys
- Take action to automatically remove IAM Users and AWS Access Keys no longer needed
- Reduce identity sprawl

Labs

Automated set up of AWS CloudTrail, AWS Config, and Amazon GuardDuty

The screenshot displays the AWS Well-Architected Labs interface. The top navigation bar includes the AWS Well-Architected Labs logo and a menu with categories: Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization, and Well Architected Tool. The left sidebar shows a tree view under the 'Security' section, with 'Level 200: Automated Deployment of Detective Controls' selected. The main content area displays the title 'Level 200: Automated Deployment of Detective Controls' with an edit icon, followed by an 'Introduction' section. The introduction text states: 'This hands-on lab will guide you through how to use AWS CloudFormation to automatically configure detective controls including AWS CloudTrail, AWS Config, and Amazon GuardDuty. You will use the AWS Management Console and AWS CloudFormation to guide you through how to automate the configuration of each service. The skills you learn will help you secure your workloads in alignment with the [AWS Well-Architected Framework](#).' Below the introduction is a 'Goals' section with two bullet points: 'Implement detective controls' and 'Automate security best practices'.

Security

- Overview
- Security 100 Labs ▾
- Security 200 Labs ▲
 - Automated Deployment of Detective Controls ▲
 - Lab Overview
 - Lab Guide
 - Automated Deployment of EC2 Web Application ▲
 - Lab Overview
 - Lab Guide
 - Automated Deployment of IAM Groups and Roles ▾
 - Automated Deployment of VPC ▾
 - Automated Deployment of Web Application Firewall ▾
 - Automated IAM User Cleanup ▾

Level 200: Automated Deployment of Detective Controls

Introduction

This hands-on lab will guide you through how to use AWS CloudFormation to automatically configure detective controls including AWS CloudTrail, AWS Config, and Amazon GuardDuty. You will use the AWS Management Console and AWS CloudFormation to guide you through how to automate the configuration of each service. The skills you learn will help you secure your workloads in alignment with the [AWS Well-Architected Framework](#).

Goals

- Implement detective controls
- Automate security best practices

Design Principles for Security

Implement a strong identity foundation

Enable traceability

Apply security at all layers

Automate security best practices

Protect data in transit and at rest

Keep people away from data

Prepare for security events



AWS KMS protects your data

AWS KMS helps protect your data

Customers use separate CMKs to partition access to data

CMK key policy defines access

CMK authorization ought to separate key administrators from encryption key users

AWS KMS improves the intentionality and discretion of data access



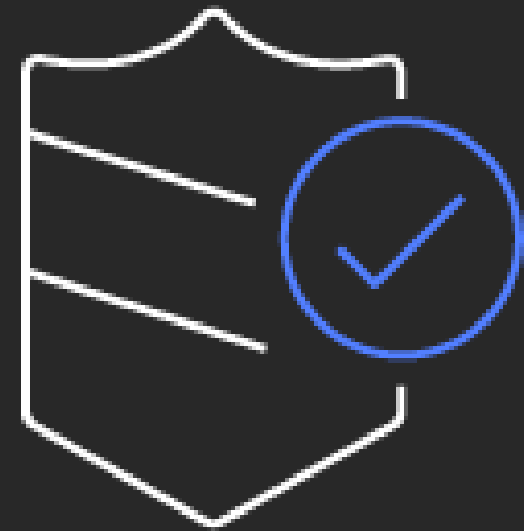
AWS KMS is an additional plane of access control

Resources protected by AWS KMS require additional authorization

Even with Amazon S3 full access, accessing objects backed by SSE-KMS requires authorization to use the AWS KMS CMK

Customers with teams managing sensitive data on Amazon EBS use separate CMKs with discrete authorization

Amazon RDS separation of duties – separate access to instances and snapshots from access to secrets and credentials



Design Principles for Security

Implement a strong identity foundation

Enable traceability

Apply security at all layers

Automate security best practices

Protect data in transit and at rest

Keep people away from data

Prepare for security events



Design Principles for Security

Implement a strong identity foundation

Enable traceability

Apply security at all layers

Automate security best practices

Protect data in transit and at rest

Keep people away from data

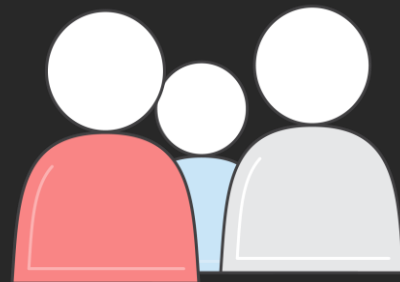
Prepare for security events



How to run a gameday



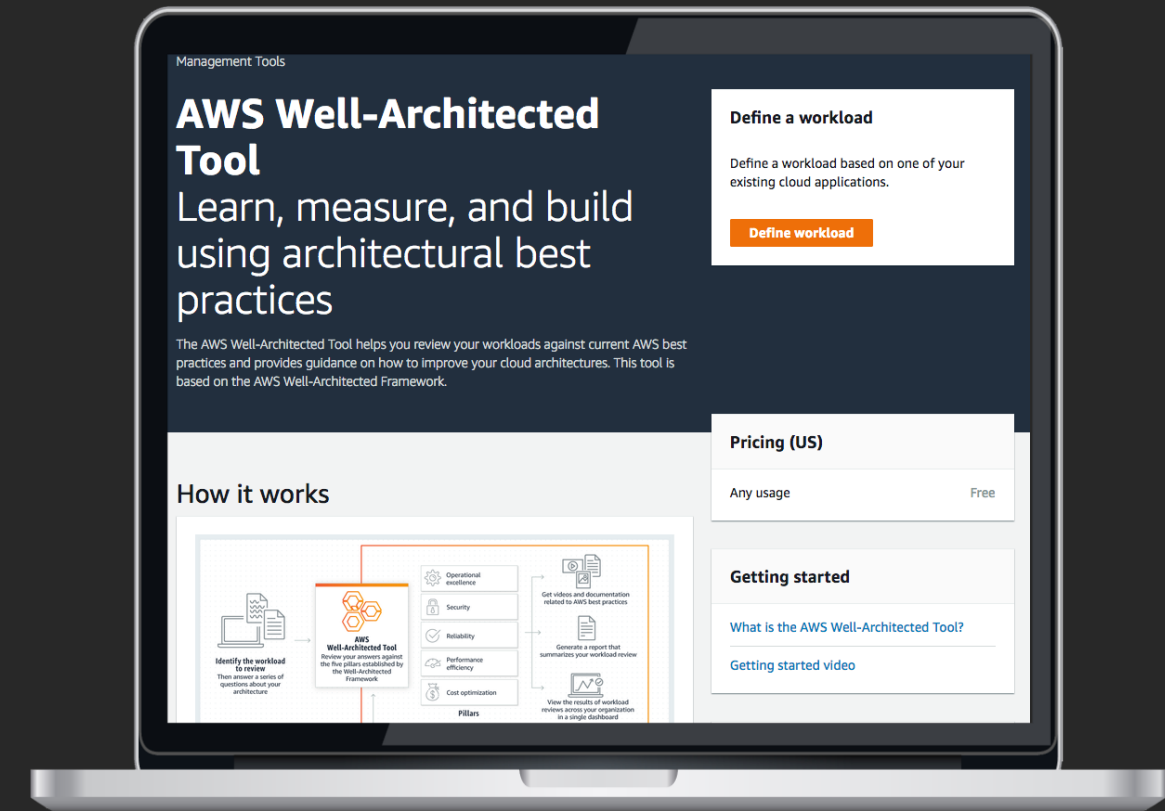
1. Schedule time block
2. Find a prize
3. Supply junk food and beverages
4. Pick relevant finding from: <https://amzn.to/2PetNro>
5. Create a playbook
6. Learn
7. Have fun!



How can Well-Architected enable your business?

AWS Well-Architected Tool

- It is in the console
- If its not in your region, use North Virginia
- Use it as a training/learning tool
- Create a dummy workload and start



Code Give Aways and Resources!

- Download the Well-Architected Framework Whitepaper.
- Check out YouTube for ReInvent Deep Dives on KMS and all the topics covered in today's session.
- <https://wellarchitectedlabs.com>
- <https://aws.amazon.com/partners/well-architected-program>

Thank you!

Martin Beeby
@thebeeb
thebeeb.net