The Extended AWS Security Ramp-Up Guide

Rami McCarthy

On November 25th, AWS released the Ramp-Up Learning Guide for AWS Cloud Security, Governance, and Compliance. The Security Ramp-Up is a curated list of educational AWS resources. The goal is “to teach in-demand cloud skills and real-world knowledge that you can rely on to keep up with cloud security, governance, and compliance developments and grow your career.” The Ramp-Up is an excellent document, that describes a logical progression in first-party training resources, from the official Overview of Amazon Web Services through the AWS Certified Specialty – Security exam, and beyond.

Clients, in the run up to or wake of an assessment, are frequently looking to broaden their understanding of AWS security. We’ve found the Ramp-up a useful reference to point people to, as it gives the high-level view of how to learn AWS Security. Its role as an official AWS document lends to the curation, credibility, and overall quality. However, as an AWS resource, it focuses exclusively on AWS’s first-party resources and services. In light of this, we’ve put together the following “Extended” AWS Security Ramp-Up Guide, compiling some of the public resources we’ve found most helpful. Centralizing these resources will serve the same purposes as the original, and it allows us to publicly document them in a place that we can point to in the future. We also hope this will be a reference for the general public, those learning AWS Security, and those responsible for AWS environments.

Before looking at this extension, we highly recommend taking a look at the Official Guide, which is broken down into the following five phases:

Phase 0 Learn the fundamentals of AWS Cloud

Phase 1 Learn cloud security fundamentals

Phase 2 Learn cloud security concepts and best practices

Phase 3 Prepare for and take the AWS Certified Security – Specialty certification exam

Phase 4 Explore additional resources

Let’s expand this guide, phase by phase – excluding the certification, for which AWS already covers all the bases.

▸ Expand if you just want the list of resources!

Phase 0: Learn the fundamentals of AWS Cloud

The fundamentals are definitely a domain in which first-party resources take priority. That being said, the following three resources focus on the broader AWS Cloud. They can both help explain the ecosystem, and also help keep you up to date on the endless changes (and improvements!) in AWS.

Amazon Web Services In Plain English

AWS is sometime the butt of jokes for its opaque service naming scheme (see Dear AWS, we need to talk about your service names and Corey Quinn's twitter (@QuinnyPig)).

"Amazon Web Services In Plain English" is a somewhat tongue-in-cheek attempt at a digestible glossary of the major AWS Services.

The Open Guide to Amazon Web Services

The Open Guide to Amazon Web Services is a community project that strives to collect "trustworthy and practical information and recommendations." The project is by and for AWS customers, and is a living document with over a thousand contributions over the last several years. This is an encyclopedic reference, broken down by AWS Service, and includes:

links to official AWS pages and docs,

Important or often overlooked tips

"Serious gotchas"

"Regular" gotchas, limitations, or quirks

Undocumented features ("folklore")

Performance discussions

Cost issues, discussion, and gotchas

The Good Parts of AWS

This recently published book is an opinionated guide to "which AWS features you'd be foolish not to use." It is a great resource for a beginner dipping their toes in the AWS waters.

Last Week In AWS

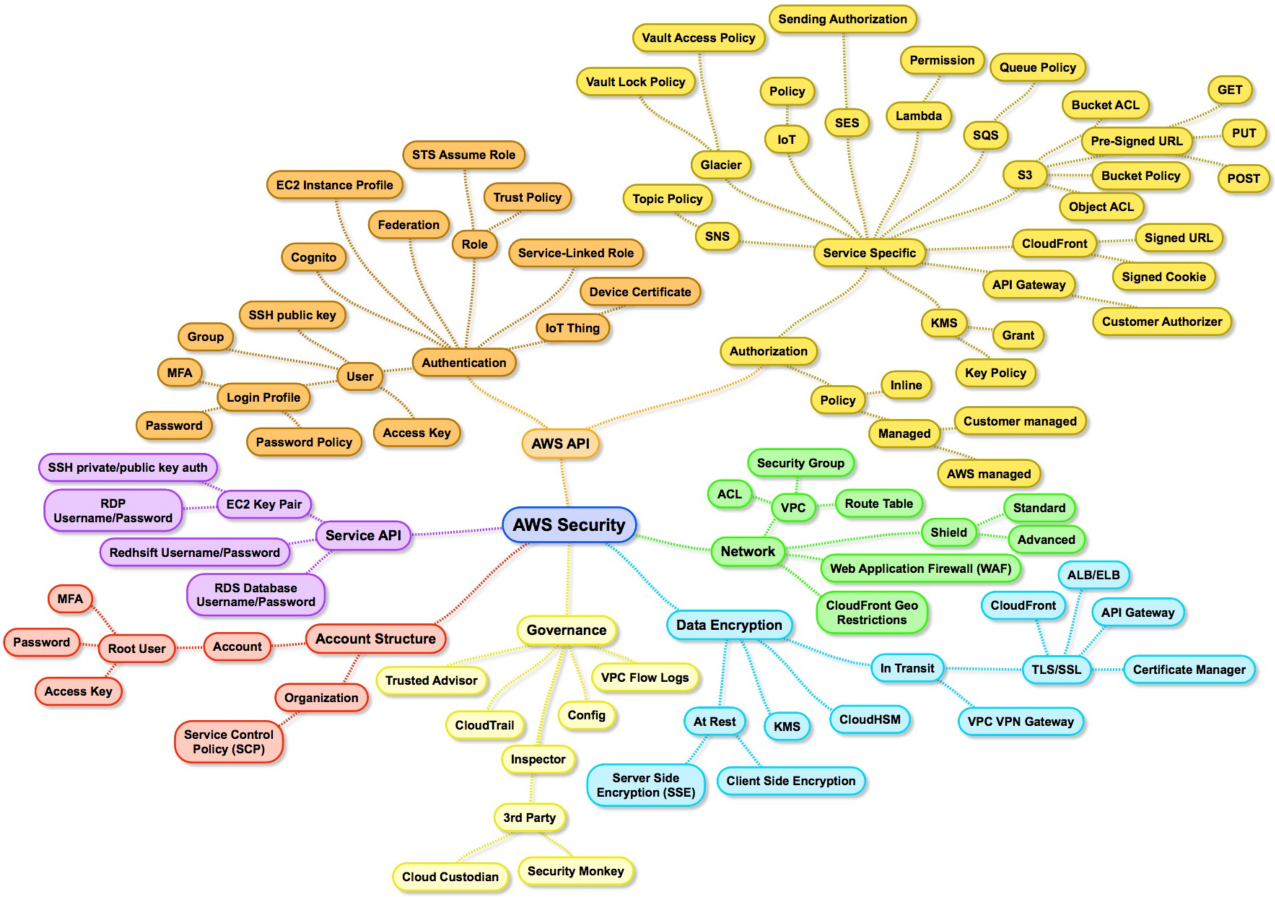
The "Last Week In AWS" newsletter is simultaneously home to dense information, and even denser snark. Corey Quinn is a "cloud economist," but this newsletter often goes well beyond billing to succeed in highlighting the biggest and most interesting news across the AWS ecosystem. AWS frequently has multiple feature announcements per day, and there is a seemingly endless system of open-source releases and blog posts on building in AWS. LWIA can help you cut through the cruft.

For a sample of the tone, check out Corey's twitter as well.

Phase 1 Learn cloud security fundamentals

AWS Security Primer

Although it is a little dated (mid-2017), this "Primer" does a great job surveying the AWS Security ecosystem in just a couple thousand words. The included mind map serves as a reasonable jumping-off point for a deeper dive.



https://research.nccgroup.com/wp-content/uploads/2023/04/aws-security-surface.png

Phase 2 Learn cloud security concepts and best practices

General

re:Inforce '19 – Leadership Session: Security Deep Dive (video)

Last year was the inaugural edition of AWS's security-focused re:Inforce conference. Spanning hundreds of sessions and thousands of attendees, the conference was recorded and broadly distributed. All of the talks are AWS vetted, and contain a gold-mine of security guidance, concepts, best practices, and case studies. There were four tracks to the conference, each with a "leadership session":

Security Deep Dive

Foundational Security

Governance, Risk Compliance

Aspirational Security

The Security Deep Dive leadership session with Bill Reid (Senior Manager of Security Solutions Architects) and Bill Shinn (Senior Principal in the Office of the CISO) is a broad ranging talk on the evolution of security leadership and best practices, and a must-see. In fact, consider checking out the whole security deep dive track!

NSA – Mitigating Cloud Vulnerabilities (PDF)

In January, the National Security Agency released an information sheet providing official guidance on cloud vulnerabilities. The document discusses threat actors, cloud-specific and general vulnerabilities, and common mitigation measures. It highlights four classes of cloud vulnerabilities:

misconfiguration

poor access control

shared tenancy vulnerabilities

supply chain vulnerabilities

The infosheet is a great resource for both business leadership, with its perspectives on cloud security principles, and for technical professionals, due to its concrete details on vulnerabilities and mitigations.

MITRE ATT CK Cloud Matrix

MITRE ATT CK is probably best known as a repository of global adversary TTPs (Tactics, Techniques and Procedures). The main matrix covers everything from Initial Access, through Privilege Escalation, to Exfiltration. In October 2019, MITRE updated the ATT CK matrix, and added cloud-focused techniques. The initial update included thirty-six techniques and updates for cloud, as well as all three major IaaS (infrastructure as a service) platforms. Based one-hundred percent on community contributions, the MITRE ATT CK Cloud Matrix is a great resource for the real world threats that will face your AWS environment.

Topic Deep Dives

re:Inforce '19 – Encrypting everything with AWS (video)

One of the major, complex security topics in AWS in Encryption. There are dozens of settings for encryption across various services, many of which are disabled by default. This talk from 2019's re:Inforce covers the whole stack of AWS encryption options, and suggests best practices.

Major Pitfalls to Avoid in Performing Incident Response in AWS (PDF)

Digital Forensics and Incident Response (DFIR) requires preparation, and is a frequent stumbling block for AWS denizens. Jonathon Poling put together this excellent survey of DFIR in AWS, because "Every organization is doing at least one thing inefficiently and/or ineffectively in performing DFIR in AWS." In the wake of an incident, the last thing you want is for it to be compounded by insufficient preparation.

Continuous Cloud Security Monitoring (PDF)

Michael Wylie gave a masterclass in Continuous Cloud Security Monitoring (CCSM) strategies, techniques, and best practices at AppSec Cali 2020. This wide ranging talk covers not just monitoring and logging, but also inventory control, vulnerability management, secure configuration, and least privilege. Almost anyone will walk away from this talk with a number of high fidelity action items, applicable directly to their environment(s).

Phase 4 Explore additional resources

AWS Security Maturity Roadmap (PDF)

Scott Piper's AWS Security Maturity Roadmap is chock-full of actionable guidance and best practices. It pairs a checklist for each of 10 stages, with a succinct description of the problem space. This guide might be the best bang-for-your-buck, period.

Toniblyx's Arsenal of AWS Security Tools

Likely already familiar to anyone working with AWS security, Toni de la Fuente's Github repo links off to almost all the key open-source AWS security tooling. This includes NCCGroup's own ScoutSuite, PMapper, sadcloud, and aws-inventory – and covers the spectrum of popularity from 2 Github stars to over 7000. If you have a problem you think would benefit from automation or tooling in AWS, this is the first stop to see if it already exists.

Blogs + Newsletters

The following blogs and newsletters are regularly updated, and cover a broad swath of AWS security. The authors compile information, and produce original research and open-source tooling.

Teri Radichel – 2nd Sight Lab – https://medium.com/@2ndsightlab

Andres Riancho – https://andresriancho.com/blog/

Rhino Security Labs – https://rhinosecuritylabs.com/blog/?category=aws

Scott Piper – Summit Route – https://summitroute.com/blog/

Chris Farris – https://www.chrisfarris.com/

Marco Lancini – CloudSecList – https://cloudseclist.com/

Community Slacks

When you're learning a skill, one of the most valuable resource you can have is a community of practitioners to bounce ideas and questions off of. Whether or not you have a physical group of cloud security practitioners, the OG-AWS and CloudSecurityForum community Slacks are a great place to gather and share.

OG-AWS Slack

CloudSecurityForum Slack

Hands-on AWS Security Labs

FlAWS + *FlAWS2*

Both FlAWS and its sequel are the products of Scott Piper of Summit Route, who has been mentioned already in this guide. The original is a linear game/CTF that aims to teach AWS security concepts. The sequel expands on the idea by allowing for play as both an "Attacker" and a "Defender." The "Defender" role especially is a excellent opportunity for simulated incident response, much better than waiting to try out your skills once your own environment has been breached.

sadcloud

Disclaimer: `sadcloud` is an NCCGroup open-source project
`sadcloud` uses Terraform templates to define a configurably insecure AWS environment. Effectively, sadcloud is a collection of Terraform configuration files. Broken down into modules by service, each service has a set of variables, mapped to ScoutSuite, Cloudmapper, and Prowler findings, that can be toggled to result in infrastructure that will fail the associated security audit check. Currently, sadcloud only supports AWS, however it would be possible to provide additional modules for other clouds, which will be a target of future development. `sadcloud` is useful for exploring common AWS misconfigurations, and as a testbed for open-source AWS auditing tools.

CloudGoat

CloudGoat is Rhino Security Labs' "Vulnerable by Design" AWS deployment tool, with a focus on specific scenarios. These include cloud_breach_s3, where you can exploit a misconfigured reverse-proxy server to query the v1 EC2 metadata service and acquire instance profile keys that allow excessive access to S3, sound familiar (spoilers)?

Conclusion

The AWS Ramp-Up Learning Guide for AWS Cloud Security, Governance, and Compliance is an excellent resource for learning about AWS security, but it is just the beginning. Similarly, while we hope this extension provides a wealth of knowledge, there is a massive landscape and undoubtedly some wonderful resources that we've missed.

Here are some related articles you may find interesting

From ERMAC to Hook: Investigating the technical differences between two Android malware variants

Authored by Joshua Kamp (main author) and Alberto Segura. Summary Hook and ERMAC are