AWS Security Blog

AWS Security Reference Architecture: A guide to designing with AWS security services

by Avik Mukherjee | on 30 JUN 2021 | in Advanced (300), Announcements, Security, Identity, & Compliance | Permalink | Comments | Share

Amazon Web Services (AWS) is happy to announce the publication of the AWS Security Reference Architecture (AWS SRA). This is a comprehensive set of examples, guides, and design considerations that you can use to deploy the full complement of AWS security services in a multi-account environment that you manage through AWS Organizations. The architecture and accompanying recommendations are based on our experience here at AWS with enterprise customers. The AWS SRA is built around a single-page architecture that depicts a simple three-tier web architecture, and shows you how the AWS security services help you achieve security objectives; where they are best deployed and managed in your AWS accounts; and, how they interact with other security services. The guidance aligns to AWS security foundations, including the AWS Cloud Adoption Framework (AWS CAF), AWS Well-Architected, and the AWS Shared Responsibility Model.

Security executives, architects, and engineers can use the AWS SRA to gain understanding of AWS security services and features, by seeing a more detailed explanation of the organization of the functional accounts within the architecture and the individual services within individual AWS accounts. The document and accompanying code repository can be used in two ways. First, you can use the AWS SRA as a practical guide to deploying AWS security services—beginning with foundational security guidance, discussing each service and its role in the architecture, and ending with a discussion of implementable code examples. Alternatively, the AWS SRA can serve as a starting point for defining a security architecture for your own multi-account environment. It’s designed to prompt you to consider your own security decisions. For example, you can think about how to leverage virtual private cloud (VPC) endpoints as a layer of security control, or consider which controls are managed in the application account, and how appropriate information can flow to the central security team.

The reference document is accompanied by a GitHub code repository that provides examples of how to deploy the services. The examples use common deployment platforms like Customizations for AWS Control Tower, AWS CloudFormation StackSets, and the AWS Landing Zone solution. All the example solutions are deployed with the recommended configurations and are deliberately very restrictive in order to demonstrate patterns in the AWS SRA guidance. AWS will continue to add additional example solutions for new and existing services on a regular basis.

The AWS SRA document and code repository are living artifacts and will be updated periodically, driven by new service and feature releases, customer feedback, and emerging best practices.

Preview

Here’s the core architecture diagram from the guide: the AWS SRA in its simplest form. The architecture is purposefully modular and provides a high-level abstracted view that represents a generic web application. The AWS organization and account structure follows the latest AWS guidance for using multiple AWS accounts.

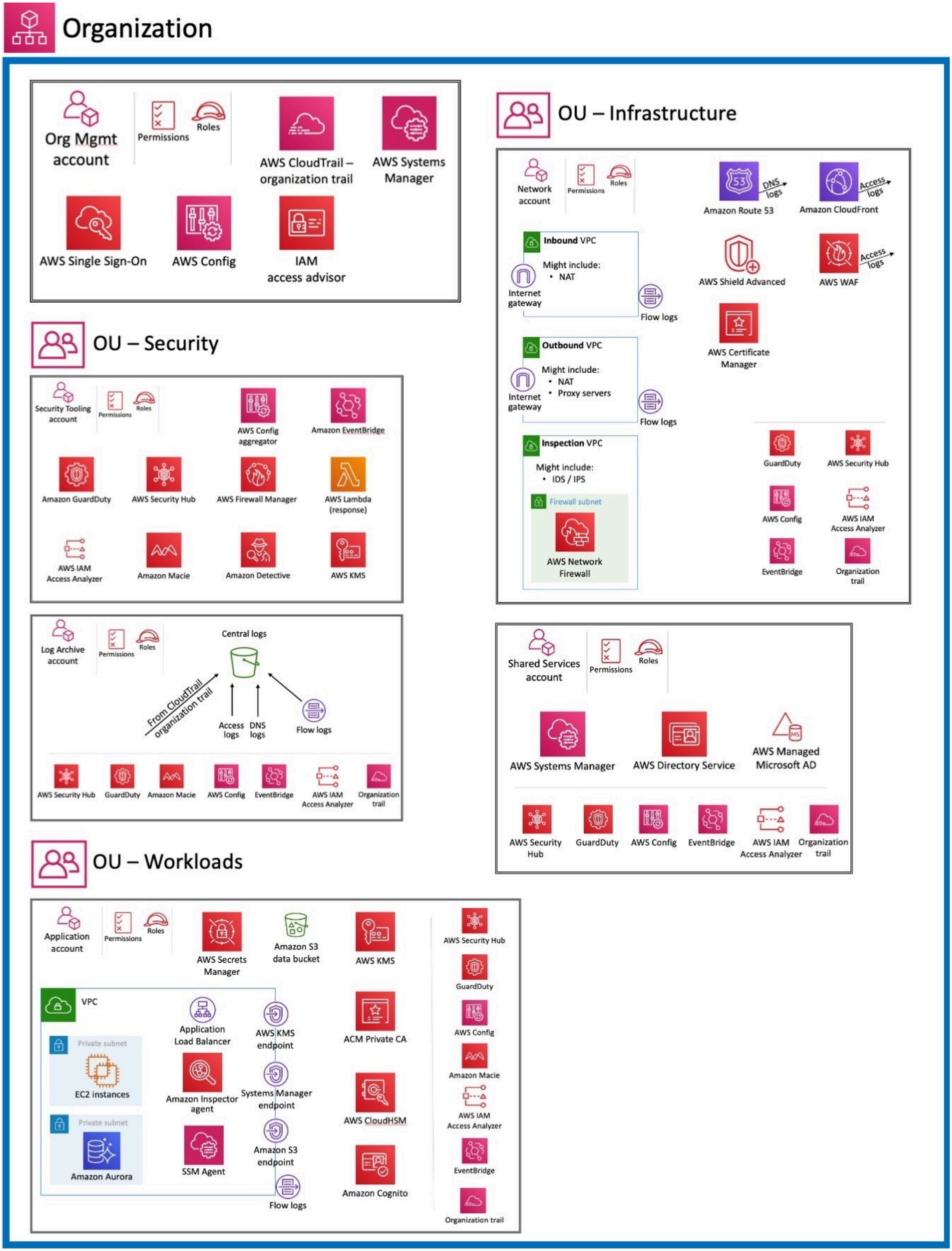
Organization
Org Mgmt account
Permissions
Roles
AWS CloudTrail – organization trail
AWS Systems Manager
AWS Single Sign-On
AWS Config
IAM access advisor
OU – Security
Security Tooling account
Permissions
Roles
AWS Config aggregator
Amazon EventBridge
Amazon GuardDuty
AWS Security Hub
AWS Firewall Manager
AWS Lambda (response)
AWS IAM Access Analyzer
Amazon Macie
Amazon Detective
AWS KMS
Log Archive account
Permissions
Roles
Central logs
From CloudTrail organization trail
Access logs
DNS logs
Flow logs
AWS Security Hub
GuardDuty
Amazon Macie
AWS Config
EventBridge
AWS IAM Access Analyzer
Organization trail
OU – Infrastructure
Network account
Permissions
Roles
Amazon Route 53
DNS logs
Amazon CloudFront
Access logs
Inbound VPC
Might include:
• NAT
Internet gateway
Flow logs
AWS Shield Advanced
AWS WAF
Access logs
AWS Certificate Manager
Outbound VPC
Might include:
• NAT
• Proxy servers
Internet gateway
Flow logs
Inspection VPC
Might include:
• IDS / IPS
Firewall subnet
AWS Network Firewall
GuardDuty
AWS Security Hub
AWS Config
AWS IAM Access Analyzer
EventBridge
Organization trail
Shared Services account
Permissions
Roles
AWS Systems Manager
AWS Directory Service
AWS Managed Microsoft AD
AWS Security Hub
GuardDuty
AWS Config
EventBridge
AWS IAM Access Analyzer
Organization trail
OU – Workloads
Application account
Permissions
Roles
AWS Secrets Manager
Amazon S3 data bucket
AWS KMS
VPC
Private subnet
EC2 instances
Private subnet
Amazon Aurora
Application Load Balancer
Amazon Inspector agent
SSM Agent
AWS KMS endpoint
Systems Manager endpoint
Amazon S3 endpoint
Flow logs
ACM Private CA
AWS CloudHSM
Amazon Cognito
AWS Security Hub
GuardDuty
AWS Config
Amazon Macie
AWS IAM Access Analyzer
EventBridge
Organization trail

Figure 1: The AWS Security Reference Architecture

How to use the AWS SRA

The AWS SRA guidance can be used as either a narrative or a reference. The topics are organized as a story, so you can read them from the beginning (foundational security guidance) to the end (discussion of implementable code examples). Alternatively, you can navigate the document to focus on the security principles, services, account types, guidance, and examples that are most relevant to your needs.

The AWS SRA documentation has five primary sections that guide you from AWS security fundamentals to the deployment of code examples:

- **Security foundations –** Reviews the AWS CAF, the AWS Well-Architected Framework, and the AWS Shared Responsibility Model and highlights elements that are especially relevant to the AWS SRA.
- **AWS Organizations and account strategy –** Introduces the AWS Organizations service, discusses its foundational security capabilities and guardrails, and gives an overview of our recommended multi-account strategy.
- **The AWS Security Reference Architecture –** A single-page architecture diagram that shows all AWS security services and features, including a detailed explanation of the functional accounts and the individual services within each account.
- **IAM resources –** Presents a summary and set of pointers for important AWS Identity and Access Management (IAM) recommendations.
- **Code repository for the AWS SRA examples –** Provides an overview of the associated public GitHub repo that contains example AWS CloudFormation templates and code for deploying some of the patterns discussed in the AWS SRA.

The AWS SRA provides a **Design Considerations** section for each element, which discusses optional features or configurations that might have important security implications or capture common variations in how you implement that element—typically as a result of alternate requirements or constraints.

When to use the AWS SRA

You can refer to the AWS SRA at various stages of your migration to the AWS Cloud. During the initial phase, you can use this document to architect your own multi-account AWS environment and weave in the various security services that AWS has to offer. If you've been using AWS for some time, you can use the AWS SRA to evaluate your current architecture and make adjustments to improve your security posture by using the full potential of various AWS security services. If you're in a mature stage of AWS Cloud adoption, you can use the AWS SRA to independently validate your security architecture against AWS recommended architecture.

Next steps

You can't host your workloads on paper, so the next step is to get started building out the reference architecture. You can consume the architecture and the associated code examples and combine these with your organization's best practices, in order to start building your production grade architecture. If you need assistance, you can reach out to AWS Professional Services, your AWS account team, or the AWS Partner Network, who can work with you to translate the reference architecture into a customized AWS environment that you can then operate.

If you have feedback about this post, submit comments in the **Comments** section below. If you need assistance with architecting or implementing a secure AWS environment, reach out to AWS Professional Services.

Want more AWS Security how-to content, news, and feature announcements? Follow us on Twitter.

TAGS: AWS Security Reference Architecture, Multi-account security, Security Blog

Comments

ALSO ON **AWS SECURITY BLOG**

How to access AWS resources from …

6 months ago • 1 comment

Use of long-term access keys for authentication between cloud resources increases …

How AWS tracks the cloud's biggest …

19 days ago • 1 comment

Threat intelligence that can fend off security threats before they happen …

How to enforce creation of roles in …

6 months ago • 1 comment

An AWS Identity and Access Management (IAM) role is an IAM identity that you …

Generate A insights for

7 months ago • 1

In part 1, we di to use Amazon Studio to analy

1 Comment

4 Prashanth ▾

Join the discussion…

♡ **Share**

Best **Newest** **Oldest**

W **webexcels**

3 years ago

Web excels is one of the growth-oriented software house in Sialkot. We provide leading class services to our clients and we proudly say our clients are really satisfied with our services. We provide an Ecommerce Platform to our clients where they can run businesses and earn huge profits. As we are the partner of alibaba global we offer alibaba account, alibaba stores, product listing, alibaba training, and lots of more. We provide social media marketing campaigns, social media business profile, domain and hosting registration, and seo packages as well.
Please visit our website and give us a chance to serve you: www.webexcels.com

0 0 Reply