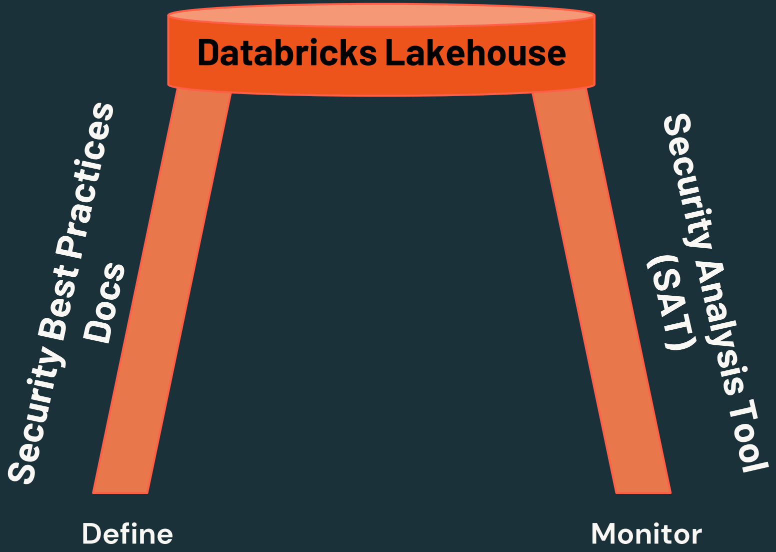
DATA+AI SUMMIT
BY databricks

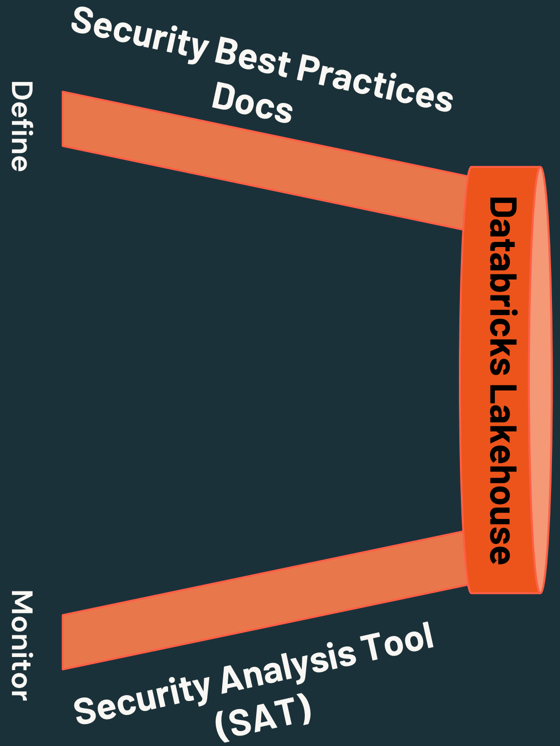
TERRAFORM TEMPLATES FOR SECURE DATABRICKS DEPLOYMENTS FROM DAY ZERO

JD BRAUN

Two Legs of Lakehouse Security



Two Legs of Lakehouse Security



Define

Security Best Practices Docs

Databricks Lakehouse

Monitor

Security Analysis Tool (SAT)

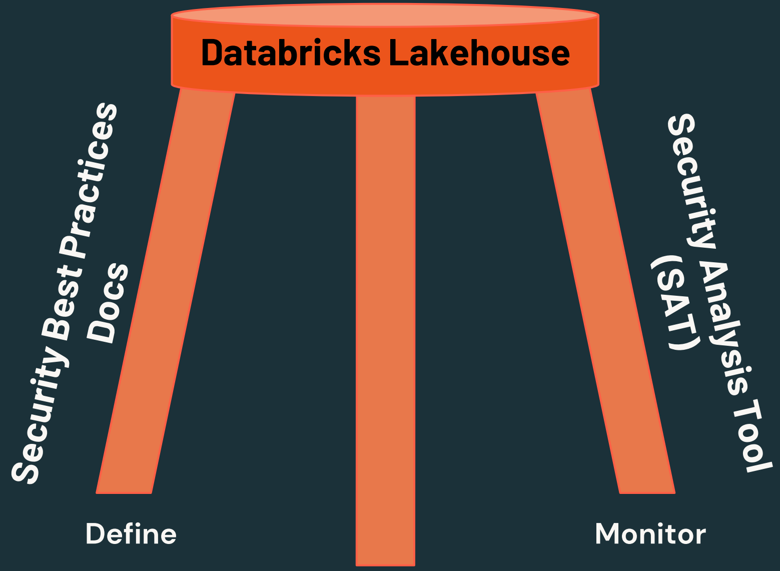
Our customer's ask:

> *How do I know how I can deploy workspaces with Databricks security best practices?*

Our answer:

The 🛡 Security Reference Architecture with Terraform Templates makes deploying workspaces with Security Best Practices easy for customers.

~~Two~~ Three Legs of Lakehouse Security



Databricks Lakehouse

Security Best Practices Docs

Security Analysis Tool (SAT)

Define

Monitor

Deplo
y

Security Reference Arch (SRA) Terraform Templates

Security Reference Architectures

Overview

- **Security Reference Architecture (SRA)**: Terraform templates makes deploying workspaces with Security Best Practices easy.
- **Opinionated perspective**: deployment model, security best practices, and ergonomics provide a definitive baseline for customers to adopt.
- **Programmatically deploy**: workspaces and the required cloud infrastructure using the official Databricks Terraform provider.
- **Pre-configured**: unified Terraform templates with hardened security settings similar to our most security-conscious customers.

Security Reference Architectures

What's included?

- **Cloud Infrastructure**
  - The SRA Terraform Templates focus on deploying infrastructure in a secure and scalable way. This includes customer managed network objects, back-end private connectivity, utilizing cloud resource endpoints whenever possible, and integrating Unity Catalog as a priority
- **Databricks Resources**
  - Following the deployment of the workspace, SRA Terraform Templates include commonly asked for features like audit and billing logs, creating service principals, setting token maximum lifetimes, and configuring admin configurations

SRA Across Clouds

Striving for parity

AWS

- Customer-managed VPC
- PrivateLink enabled
- Unity Catalog
- Customer-managed keys
- Scoped down IAM role
- VPC interface and gateway endpoints (STS, Kinesis, S3 etc.)

Azure

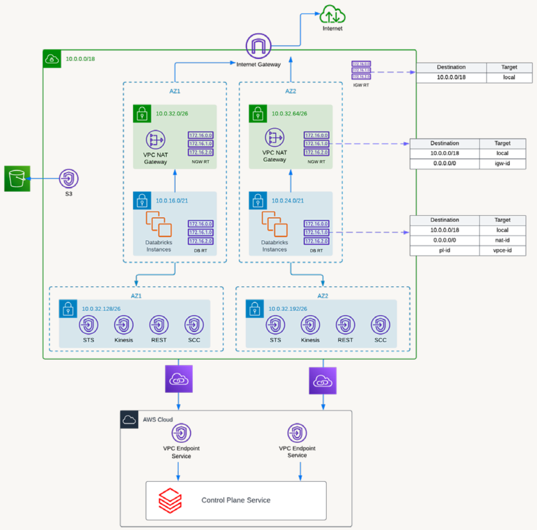
- Customer-managed VNet
- PrivateLink enabled
- Unity Catalog
- Customer-managed keys
- Firewall and configuration for exfiltration protection

GCP

- Customer managed VPC
- Private Service Connect enabled
- Unity Catalog
- Service account creation for workspace resource creation

SRA – AWS Network Architectures

Sandbox

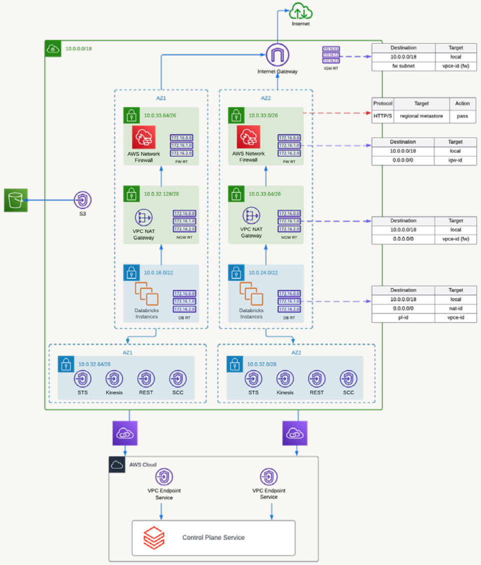


Destination	Target
10.0.0.0/18	local

Destination	Target
10.0.0.0/18	local
0.0.0.0/0	igw-id

Destination	Target
10.0.0.0/18	local
0.0.0.0/0	nat-id
pl-id	vpce-id

Egress Firewall



Destination	Target
10.0.0.0/18	local
fw subnet	vpce-id (fw)

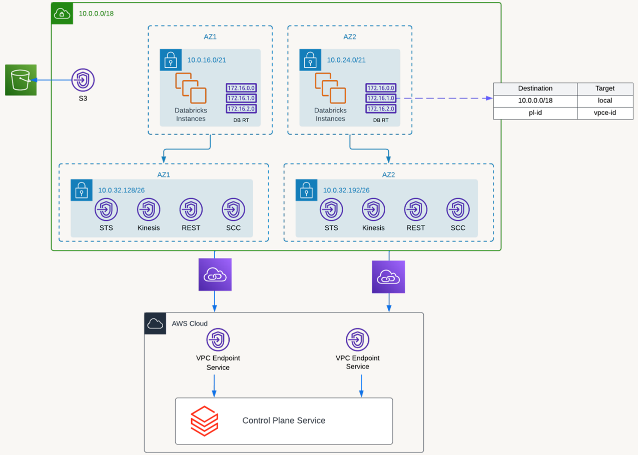
Protocol	Target	Action
HTTP/S	regional metastore	pass

Destination	Target
10.0.0.0/18	local
0.0.0.0/0	igw-id

Destination	Target
10.0.0.0/18	local
0.0.0.0/0	vpce-id (fw)

Destination	Target
10.0.0.0/18	local
0.0.0.0/0	nat-id
pl-id	vpce-id

Network Isolation



Destination	Target
10.0.0.0/18	local
pl-id	vpce-id

DEMO

DATA+AI SUMMIT