Secure Cloud Foundation (SCF) –

Powered by Velocity

Change is everywhere

Table of Contents

AWS Service Usage Descriptions

Tower Post Processor (TPP)

- **Serverless Application:** Serverless Functions for performing automated actions
  - AWS Lambda Functions, Python Env 3.9 and later

- **Organization Management:** Service for managing Accounts and Organizational Units
  - AWS Organizations
  - AWS Control Tower
  - Customizations for Control Tower (CfCT)

- **DevOps:** Development Operations Services for Continuous Integration, Deployment/Delivery
  - CodeCommit Repository
  - CodeBuild Jobs
  - CodePipeline Pipelines

- **Cloud Development Kit Pipelines** (for use with CDK Applications)

Central Network (with PaloAlto)

- **Infrastructure Product Management**: Resources for managing infrastructure products for standard network architecture
  - Service Catalog Products – VPCs

- **Network:** Resources for managing network infrastructure and traffic
  - VPCs
  - Security Groups
  - VPC Endpoints
  - Palo Alto VM Series (using EC2 Infrastructure)
  - Route 53 – Public and Private Hosted Zones
  - Transit Gateway Attachments
  - Transit Gateway Route Tables
  - AWS Elastic Load Balancer – Gateway Load Balancer

- **Resiliency:** Services for maintaining resilience of network infrastructure
  - EC2 Autoscaling -> Palo Alto Firewall AutoScaling

- **Serverless Automation:** Resources for performing automating actions during deployment and management of network infrastructure
  - AWS Lambda Functions – Python Env 3.9 and Later

- **DevOps:** Development Operations Services for Continuous Integration, Deployment/Delivery
  - CodeCommit Repository
  - CodeBuild Jobs
  - CodePipeline Pipelines
    - Cloud Development Kit Pipelines (for use with CDK Applications)

- **Access Management:** Resources used for managing access to and from network infrastructure
  - IAM Roles and Policies

Identity

- **Access Management:** Resources used for managing access for users
    - AWS Single Sign On (AWS SSO) Permission Sets (Optional)
    - IAM Roles
    - IAM Customer Managed Policies

- **DevOps:** Development Operations Services for Continuous Integration, Deployment/Delivery
    - CodeCommit Repository
    - CodeBuild Jobs
    - CodePipeline Pipelines
        - Cloud Development Kit Pipelines (for use with CDK Applications)

IAM Roles and Policies

Tower Post Processor (TPP)

- **TowerPostRole**
  - Description: Organization enumeration to identify target accounts and OUs for post processing activities
  - Principal: lambda.amazonaws.com

Central Network (with PaloAlto)

- **SSM-Network-Test-Role**
  - Description: SSM Role used for Network Testing from a Test EC2 Instance
  - Principal: ec2.amazonaws.com

- **Cloud-Connector-Instance-Role**
  - Description: Used by EC2 to access secrets from Secret Manager
  - Principal: ec2.amazonaws.com

- **Palo-FW-Instance-Role**
  - Description: Used by EC2 to access secrets from Secrets manager
  - Principal: ec2.amazonaws.com

- **Data-flow-log-role**
  - Description: used for writing vpc flow logs to appropriate target S3 buckets
  - Principal: vpc-flow-logs.amazonaws.com

- **Subscription-filter-flow-logs**
  - Description: Role required for subscribing VPC Flow logs to Kinesis service family
  - Principal: logs.amazonaws.com

- **Subscription-Filter-DNS**
  - Description: Role for subscribing Route53 DNS Logs to Kinesis Service Family
  - Principal: logs.amazonaws.com

- **Role5id432**
  - Description: Creates IAM Instance Profiles to be used by EC2 VMs
  - Principal: ec2.amazonaws.com

Identity

Default Roles Listed below are OPTIONAL for deployment when deploying the Identity Block. All roles are built to be used by IAM User or SSO User Principals.

- **IAMDeveloper**
  - **Description:** Read Only Access to IAM, and full access to S3 for uploading custom policies

- **IAMAdministrator**
    - **Description:** Default Role for Administering IAM Resources

- **IAMArchitect**
    - **Description:** Read only Access for review of custom policies created by IAM Developers

- **CloudOperations**
    - **Description:**

- **CloudEngineer**
    - **Description:** Permission to develop cloud applications using cloudformation

- **CloudDeveloper**
    - **Description:** role for enabling cloud development with defined set of aws services/resources

- **SecurityComplianceEngineer**
    - **Description:** Enumeration actions for performing Security Auditing

- **DatabaseEngineer**
    - **Description:** Full access to defined storage and database services/resources for database enginering

- **NetworkEngineer**
    - **Description:** AWS NetworkAdministrator managed policy for handling AWS Network rescources

- **DevSecOpsEngineer**
    - **Description:** Permissions for handling development operations of cloud infrastructure and resources

- **Billing**
    - **Description:** Billing Access including Cost Explorer and Billing Dashboards/events