Table of Contents

# My Big Company

# Server Engineering and Operations - Platform Admin Guide

## 1. Introduction

**Purpose:** Define administrative responsibilities in My Big Company’s AAP deployment.  
**Scope:** Covers Execution Environments (EEs), job templates, RBAC, security, and compliance for My Big Company.

## 2. Infrastructure Overview

### AAP Architecture Overview

* Control Nodes (Orchestration)
* Execution Nodes (Playbook Execution)
* Load Balancer: F5 Big-IP

### Networking Requirements

* Registry access for EE builds: quay.io/internal-registry
* RBAC via Okta

## 3. Execution Environment (EE) Management

### 3.1. Building a Custom EE

#### Define EE Build Configuration

* Base image
* Collections: ansible.windows, community.general
* Python dependencies (e.g., boto3, requests)
* System dependencies (e.g., RPM packages)

#### Steps

1. Build the EE
2. Push EE to Registry
3. Register EE in AAP

### 3.2. Automating EE Builds (CI/CD)

* Use AAP Job Templates to trigger EE builds on updates.
* Automate registry sync to avoid stale images.

## 4. Platform Security & Governance

### RBAC Enforcement

* Role-based access control via SailPoint
* No direct individual permissions

### Inventory & Credential Security

* Centralized credential storage: AAP (Future State: CyberArk)
* Role-based credential usage restrictions

### Job Execution Policies

* Execution only within predefined environments
* Approval workflow for sensitive automation

## 5. Maintenance & Troubleshooting

### EE Build Issues

* Debugging execution-environment.yml errors
* Checking build logs

### Registry Sync Failures

* Ensuring connectivity to quay.io/internal-registry
* Automating periodic sync jobs

### RBAC/Access Errors

* Validating Okta group memberships
* Ensuring correct role assignments

### Container Logs & Debugging

* Accessing logs from execution nodes
* Reviewing job failures in AAP logs

## 6. Roles & Responsibilities

### 6.1 Overview

To maintain the integrity, security, and efficiency of My Big Company’s AAP, clearly defined roles and responsibilities ensure structured governance, technical execution, and compliance.

### 6.2 Key Roles

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Responsibilities | Decision Authority | SME Area |
| **Principal Engineer & Architect (PEA)** | - Define AAP governance, policies, and architecture.- Approve all runbooks, procedures, and best practices.- Establish compliance, security, and operational standards.- Align AAP with broader IT and business strategy. | Final authority on governance, architecture, and operational procedures. | Governance, architecture, security, compliance |
| **AAP Engineer** | - Implement AAP configurations, execute technical builds.- Deploy and maintain Execution Environments (EEs).- Troubleshoot job execution issues.- Manage day-to-day platform operations. | Executes technical tasks within established governance. | Technical SME for AAP operations and configurations |
| **Platform Administrator** | - Manage platform-wide settings and user access.- Ensure AAP is operational and compliant.- Oversee inventory and credential security. | Administrative control over AAP infrastructure. | Platform maintenance, access control, security policies |
| **Platform Operator** | - Execute approved automation workflows.- Report issues and provide operational feedback. | Executes but does not modify workflows. | Job execution and automation workflows |
| **Platform Auditor** | - Monitor compliance, security adherence, and audit logs.- Ensure governance policies are being followed. | Read-only access for auditing and compliance. | Compliance, security adherence, reporting |

### 6.3 Governance and Decision-Making Authority

* Final approval on architecture, governance, and procedures resides with the Principal Engineer & Architect.
* Technical implementation of approved procedures and governance is the responsibility of the AAP Engineer.
* All changes, deployments, and modifications must follow the established approval workflow and security policies.

### 6.4 Approval Workflow

#### Significant Change Requests & New Implementations

* Changes impacting security, compliance, or architecture must be reviewed and approved by the Principal Engineer & Architect before execution.
* Examples include new governance frameworks, major RBAC modifications, or infrastructure-wide automation updates.

#### Minor Process or Workflow Modifications

* Updates that do not impact security, compliance, or architecture (e.g., minor optimizations, updates to non-governance job templates) may be reviewed and approved by the AAP Engineer or Platform Administrator.

#### Technical Deployments

* AAP Engineer executes approved tasks based on defined architecture and governance policies.

#### Compliance & Security Audits

* Conducted periodically by Platform Auditors to ensure adherence to security and operational guidelines.