AWS Systems Manager

JJ Tech Inc
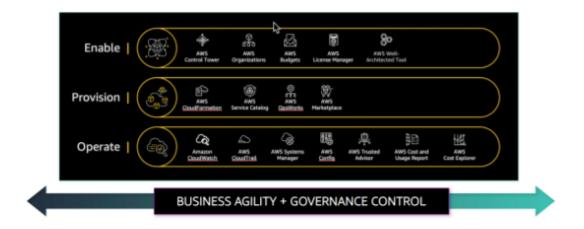
What is Systems Manager

- A set of fully managed AWS services and capabilities
- Automated configuration and ongoing management of systems at scale
- Acceleration of your cloud journey
- Flexible, easy-to-use, automation-focused approach

Key Benefits to AWS Systems Manager

1. Hybrid
2. Cross-platform support
3. Scalable
4. AWS optimized
5. No complex licensing models

What problems does it solve

1. Traditional IT toolsets are not designed or built for cloud scale.
2. Deploying and maintaining multiple management products is a significant operational overhead.
3. Licensing adds costs and complexity.

AWS Management and Governance Services

- Run Command
- State Manager
- Inventory
- Patch Manager
- Maintenance Window
- Automation
- Parameter Store
- Session Manager
- OpsCenter
- Explorer
- Change Calendar
- Distributor

Systems Manager capabilities

Systems Manager building blocks

- Simple Systems Manager (SSM) agent on Amazon Elastic Compute Cloud (Amazon EC2)
- Documents

Prerequisites

- Access control
  - Privileges to manage the service
  - Instance profile role
- SSM agent
- Connectivity to the Systems Manager service

SSM Agent

SSM agent is preinstalled, by default, on the following Amazon Machine Images (AMIs):
- Windows Server 2003–2012 R2 AMIs published in November 2016 or later
- Windows Server 2016 and 2019
- Amazon Linux
- Amazon Linux 2
- Ubuntu Server 16.04
- Ubuntu Server 18.04

Systems Manager Service Connectivity

- Internet connectivity
- Amazon Virtual Private Cloud (Amazon VPC) endpoints

Managed Instance Registrations

- Register new Amazon EC2 instances at launch
- Register existing, long-running instances
- Register on-premises servers to Systems Manager

AWS Systems Manager Quick Setup

- AWS Identity and Access Management (IAM) instance profile roles for Systems Manager
- A scheduled, biweekly update of SSM agent
- A scheduled collection of inventory metadata every 30 minutes
- A daily scan of your instances to identify missing patches
- A one-time installation and configuration of the Amazon CloudWatch agent
- A scheduled, monthly update of the CloudWatch agent

AWS Systems Manager: Run Command

- Remotely and securely run configuration actions at scale
  - Hybrid
  - No inbound network ports
  - Access control = authorization
  - Auditable
- Accessible via:
  - AWS Management Console
  - AWS Command Line Interface (AWS CLI)
  - Any of the AWS software development kits (SDKs)

What is Run Command?

How does run command work?

- Managed instance
- Document
- Command invocation

Run Command Use Cases

- Monitoring your systems
- Joining instances to a domain
- On-demand patching
- Deploying code to instances
- Process management
- Run bootstrap scripts on applications
- User and account management
- Countless other use cases

AWS Systems Manager: State Manager

What is state manager

- Secure and scalable configuration management service

State manager use cases

- Enabling or disabling a service
- Ensuring desired state is continuously applied, such as closing ports on a firewall
- Collecting inventory
- Running scripts on Windows or Linux managed instances throughout their lifecycle
- Running antivirus scans
- Countless other use cases

Example: Maintain Compliance with Ansible Playbooks

+ Maintain compliance by running ansible playbooks that define and enforce the desired state

AWS Systems Manager: Patch Manager

- Simplify operating system and application patching process
- Select patches to deploy
  - Whitelist or blacklist specific patches
- Specify timing to roll out
- Control instance reboots
- Report patching compliance
- Schedule automatic rollout with Maintenance Windows

Patch Manager Benefits

- Hybrid
- Operating system and application patching
- Supports for Windows Server, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), CentOS, Amazon Linux, and Amazon Linux 2
- Scan, or scan and install, missing patches
- No additional cost for patching Amazon EC2 instances
- No additional cost for OS patching of on-premises resources**

** limits may apply

How does patch manager work?

- Managed instance prerequisites
  - SSM agent installed
  - Permissions granted via IAM
  - Connectivity with Systems Manager endpoints
  - Patch Group tags added
- Configure patch baselines
  - Define approval rules
  - Whitelist/blacklist specific patches
  - Associate Patch Group tags
- Create a Maintenance Window
- Review patch compliance

AWS Systems Manager: Maintenance Windows

What is Maintenance Window?

- Capability to schedule tasks
  - Patching an OS
  - Updating drivers
  - Installing software
  - Creating AMIs

How does Maintenance Window work?

- Define a schedule
- Specify the duration
- Register a set of targets
- Register a set of tasks, including:
    - Run Command
    - Automation
    - Lambda function
    - Step Functions

AWS Systems Manager: Parameter Store

What is Parameter Store?

- Provides secure and hierarchical storage for:
  - Configuration data
  - Secrets data
- You can store:
  - Passwords, license codes, database strings, etc.
- Can be stored encrypted or in plaintext; can be accessed programmatically, from the AWS Console, or AWS CLI
- Highly scalable, available, and durable
- Auditable
- Native integration with IAM

AWS Systems Manager:
inventory

What is AWS Systems Manager Inventory?

- Collect instance details and OS details
  - Applications installed
  - Network configuration
  - Updates installed
  - Monitor file paths
  - Monitor Windows services and roles
  - Monitor Windows registry keys
  - Billing information
  - Custom inventory
- Aggregate data using Resource Data Sync
- Integrates with AWS Config

How does inventory work?

- Managed instance prerequisites:
  - SSM agent installed
  - Granted permissions via IAM
  - Connectivity with Systems Manager endpoints
- Setup inventory
  - Define targets
  - Specify schedule
  - Define type of data to gather
- Create Resource Data Sync
- Enable AWS Config recording

AWS Systems Manager: Automation

What AWS Systems Manager Automation?

- Platform to orchestrate operational playbooks
- Manage any AWS resource across accounts/Regions
- Orchestrate dynamic playbooks
- Standardize and share playbooks across organization
- Safe at-scale operations
- Integrates with AWS Config, AWS Service Catalog, and others

Automation Benefits

- Auditable service
- Native IAM integration
- Enhanced operations security
- Ability to share best practices via automation playbooks
- Enhanced integration
  - Ability to call and run AWS API actions, such as creating an AWS CloudFormation stack
  - Ability to run a script (PowerShell, Python)
  - AWS Service Catalog self-service actions like reboot RDS
- Automation at scale

Automation common use cases

- Automating the creation of golden AMIs
- Handling one-click configuration tasks, such as configuring Amazon S3 buckets
- Performing routine maintenance tasks, such as patching AutoScaling groups
- Automatically remediating resources through AWS Config
- Stopping Amazon EC2 instances with approvals
- Taking backups of resources, such as DynamoDB or RDS

How does Automation work?

- Assumes current user context by default
- Option to specify service role
- Leverage AWS playbooks
- Create custom Automation documents
    - Define actions to perform
    - Provide dynamic parameters
    - Conditionally branch based on step results
    - Configure approvals as part of workflow
- Run the Automation playbook
    - Multi-account and multi-Region
    - Register as a Maintenance Window task
    - Automatic remediation with AWS Config

AWS Systems Manager:
Distributor

What is distributor

- Securely store and distribute software packages
  - Software agents
  - Applications
  - Drivers
- Simplify and scale distribution
  - Central repository with version control
  - Share with other AWS accounts
  - Control access to packages using IAM
- Install on demand or on a schedule
- Install automatically on new instances

How does Distributor work?

- Managed Instance prerequisites:
  - SSM agent installed
  - Granted permissions via IAM
  - Connectivity with Systems Manager endpoints
- Create a package
  - Specify Amazon S3 bucket to store package
  - Provide software files (rpm, MSI, or deb)
  - Specify platform, version, and architecture
  - Validate install/uninstall/update scripts
- Install package
  - One time using Run Command
  - Scheduled install with State Manager associations

AWS Systems Manager:
Explorer

What is AWS Systems Manager Explorer?

- View operations data across AWS accounts/Regions
- Gain insight into operations issues
  - Sort by category
  - Monitor issue trends over time
- Provides summary of Amazon EC2 instances
  - Amazon Machine Image (AMI) used to launch
  - Patch compliance state
- Integrates with AWS Organizations
- Create customized reports

How does Explorer work?

- Aggregated and customizable view of OpsData
- Configure OpsCenter rules
- Configure OpsData sources
  - Systems Manager patch compliance
  - Amazon EC2 metadata via AWS Config
  - OpsCenter OpsItems
- Synchronize OpsData in AWS Organizations
- Export OpsData to Amazon S3

AWS Systems Manager: Change Calendar

What is AWS Systems Manager Change Calendar?

- Create calendars
  - Open or closed by default
- Define important business events
  - Prevent potentially disruptive actions
  - Whitelist or blacklist specific times or days
- Share calendars across AWS accounts

How does change calendar work?

- Create calendar
- Add scheduled events
- Query calendar state using Automation
  - If open, continue
  - If closed, block actions
- Include approval-based override actions

Thank you!