Respond

AWS Foundational and Layered Security Services

Identify

- AWS Security Hub
- AWS Organizations
- AWS Control Tower
- AWS Trusted Advisor
- AWS Service Catalog
- AWS Config
- AWS Well-Architected Tool
- AWS Systems Manager

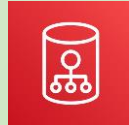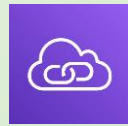**Protect**
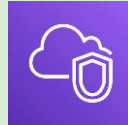
- AWS Transit Gateway
- Amazon VPC
- AWS IoT Device Defender
- Amazon Cloud Directory
- Amazon VPC PrivateLink
- AWS Direct Connect
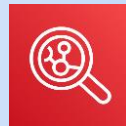- Resource Access manager
- AWS Directory Service
- AWS Shield
- IAM
- AWS Secrets Manager
- KMS
- Amazon Cognito
- AWS WAF
- AWS Firewall Manager
- AWS Certificate Manager
- AWS CloudHSM
- AWS IAM Identity Center

Detect

- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- AWS Security Hub

Respond

Automate

- Amazon CloudWatch
- AWS Step Functions
- AWS Systems Manager
- AWS Lambda

Investigate

- Amazon Detective
- Amazon CloudWatch
- AWS CloudTrail
- Personal Health Dashboard
- Amazon Route 53

- AWS OpsWorks
- AWS CloudFormation
- Amazon S3 Glacier
- Snapshot
- Archive

AWS Systems Manager

AWS Systems Manager

- AWS Systems Manager is the operations hub for your AWS applications and resources and a secure end-to-end management solution for hybrid and multicloud environments that enables secure operations at scale.

AWS Systems Manager

Capabilities

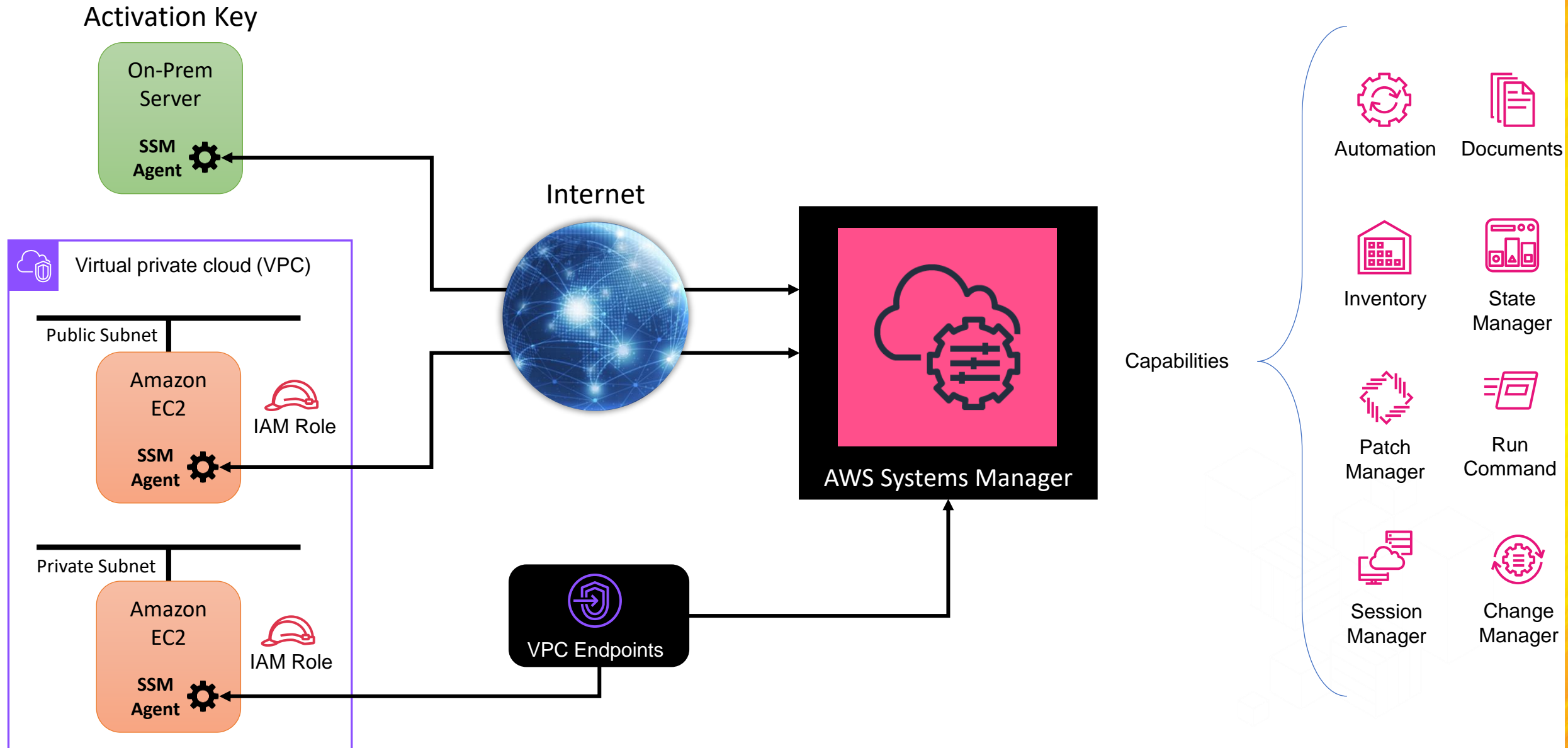|			
Automation	Documents	Patch Manager	Parameter Store
Inventory	State Manager	Run Command	Incident Manager
Change Calendar	Compliance	Application Manager	Distributor
Session Manager	Change Manager	OpsCenter	Maintenance Windows

Workshop

Managing nodes using the AWS Systems Manager agent

Session Manager

- Session Manager lets you manage your EC2 instances, on-premises servers, edge devices, and virtual machines (VMs), including VMs in other cloud environments, through an interactive one-click browser-based shell or through the AWS CLI.

- Session Manager provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.

Session Manager
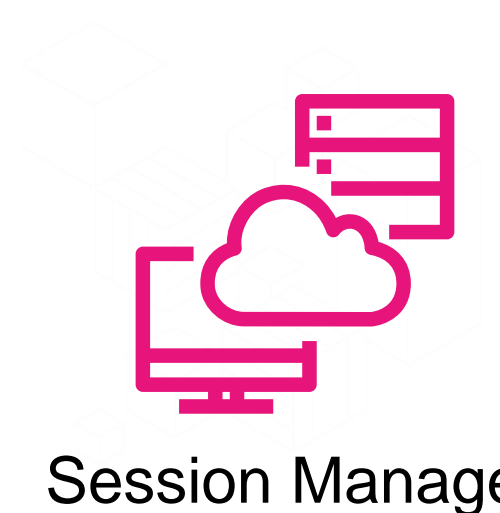
Documents

- An AWS Systems Manager document (SSM document) the configuration options, policies, and the actions that Systems Manager performs on your managed instances and other AWS resources.

- Documents use JavaScript Object Notation (JSON) or YAML, and they include steps and parameters that you specify.

- You can use pre-defined AWS managed documents or create your own depending on your use case.

Example

Documents

State Manager

- State Manager automates the process of keeping your managed nodes and other AWS resources in a state that you define.

- State Manager offers the following benefits for managing your nodes
  - Bootstrap nodes with specific software at start-up.
  - Download and update agents on a defined schedule, including the SSM Agent.
  - Join nodes to a Microsoft Active Directory domain.
  - Patch nodes with software updates throughout their lifecycle.
  - Run scripts on managed nodes throughout their lifecycle.

- An association includes three components and one optional set of components:
  - A Command or Automation document that defines the state.
  - Target(s), which can be managed nodes or other AWS resources.
  - A schedule for when or how often to apply the state.
  - (Optional) Runtime parameters specific to the document.

State Manager

Patch Manager

- You can patch Amazon EC2 instances, edge devices, and on-premises servers and virtual machines (VMs), including VMs in other cloud environments.

- You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

- You can target instances individually or in large groups by using resource tags or Resource Groups.

- Patch Manager doesn't support upgrading major versions of operating systems, such as Windows Server 2016 to Windows Server 2019, or SUSE Linux Enterprise Server (SLES) 12.0 to SLES 15.0.
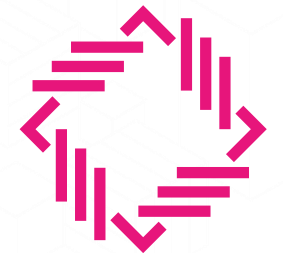
Patch Manager

Run Commands

- Run Command lets you remotely and securely manage the configuration of your managed instances. Run Command enables you to automate common administrative tasks and perform ad-hoc configuration changes at scale.

- You can use Run Command from the AWS Management Console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs.

- Administrators use Run Command to install or bootstrap applications, build a deployment pipeline, capture log files when an instance is removed from an Auto Scaling group, join instances to a Windows domain, and more.

Run Command

Change Manager

- Change Manager, a capability of AWS Systems Manager, is an enterprise change management framework for requesting, approving, implementing, and reporting on operational changes to your application configuration and infrastructure.

- With Change Manager, you can use preapproved change templates to help automate change processes for your resources and help avoid unintentional results when making operational changes.

- Change templates can be helpful during audits to show how standard changes are made.

Change Manager