AWS Systems Manager Overview

## AWS Systems Manager

* provides visibility and control of the infrastructure on AWS
* helps to view operational data from multiple AWS services and automate operational tasks across AWS resources.
* works with managed instances, which are configured for use with Systems Manager
* helps configure and maintain managed instances.
* helps maintain security and compliance by scanning the managed instances and reporting on (or taking corrective action on) any policy violations it detects.
* supports machine types include EC2 instances, on-premises servers, and virtual machines (VMs), including VMs in other cloud environments. Supported operating system types include Windows Server, multiple distributions of Linux, and Raspbian.

## Systems Manager Capabilities

### Operations Management

Capabilities that help manage the AWS resources

* [Trusted Advisor](https://jayendrapatil.com/aws-trusted-advisor-categories/) is an online tool that provides you real time guidance to help you provision your resources following AWS best practices
* AWS Personal Health Dashboard provides information about AWS Health events that can affect your account

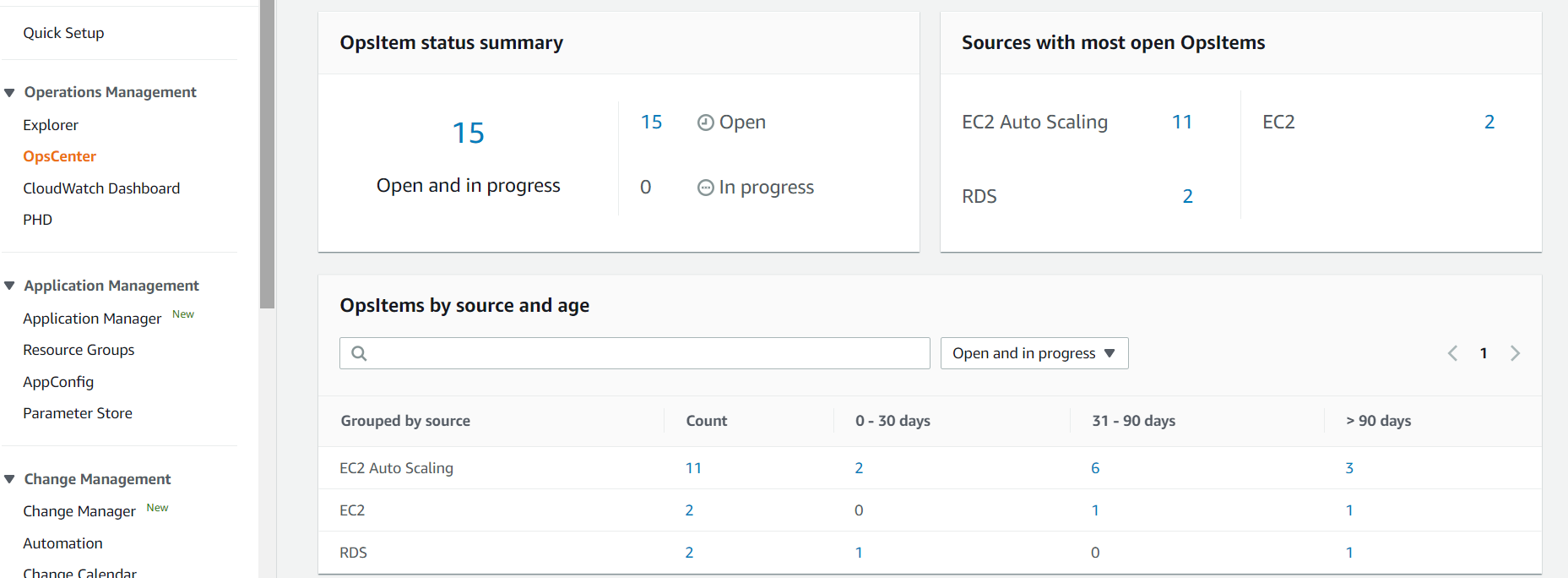
**AWS Systems Manager - Explorer**

* AWS Systems Manager Explorer is a customizable operations dashboard that reports information about your AWS resources.
* Explorer displays an aggregated view of operations data (OpsData) for your AWS accounts and across Regions.
* In Explorer, OpsData includes metadata about your EC2 instances, patch compliance details, and State Manager association compliance details. OpsData also includes information from supporting AWS services like AWS Trusted Advisor, AWS Compute Optimizer, and information about your AWS Support cases.
* Explorer helps users discover trends and patterns and, if necessary, quickly resolve issues using Systems Manager Automation runbooks.


            Explorer dashboard in AWS Systems Manager
        

**AWS Systems Manager - OpsCenter**

* [Systems Manager OpsCenter](https://docs.aws.amazon.com/systems-manager/latest/userguide/OpsCenter.html) provides a central location where operations engineers and IT professionals view, investigate, and resolve OpsItems related to AWS resources.
* Explorer is a report hub where DevOps managers view aggregated summaries of their operations data, including OpsItems, across AWS Regions and accounts.

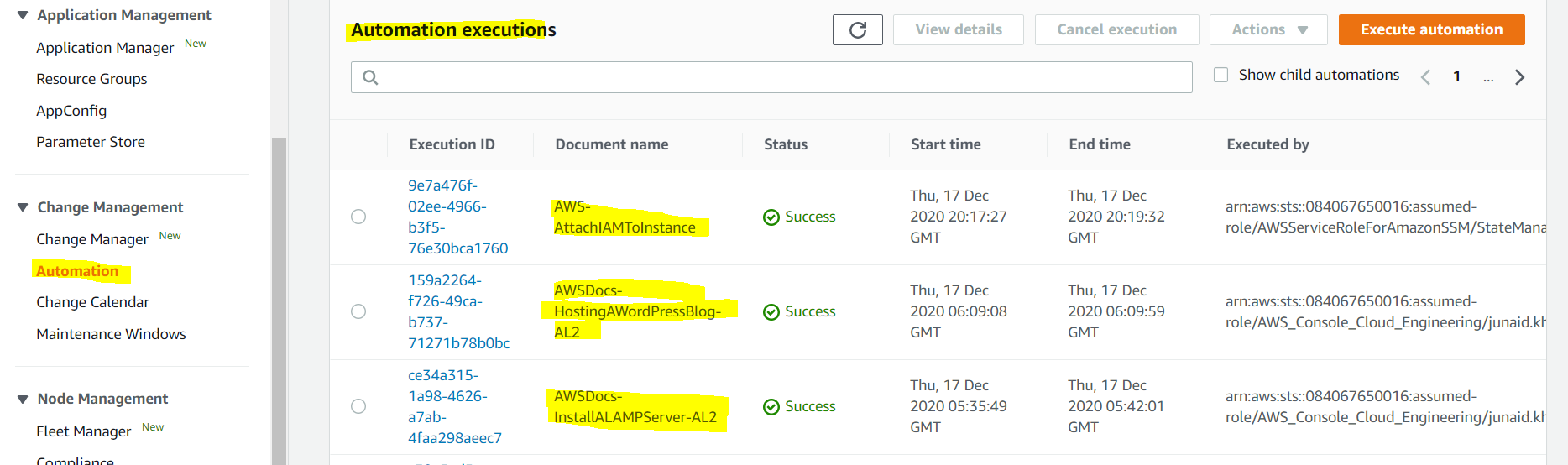


### Actions & Change

Capabilities for taking action against or changing the AWS resources

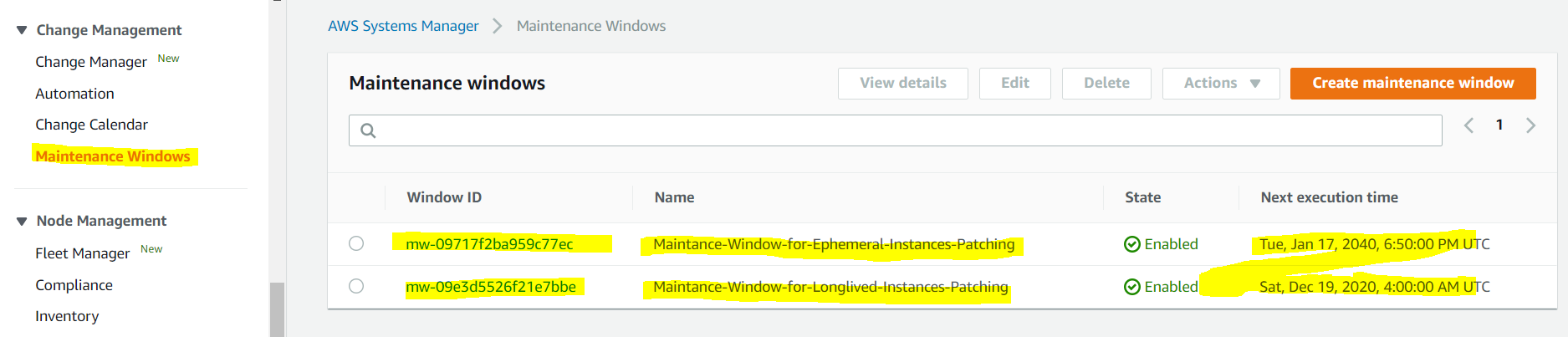
#### **Systems Manager Automation**

* helps automate common maintenance and deployment tasks for e.g. create and update AMIs, apply driver and agent updates, reset passwords on Windows instance, reset SSH keys on Linux instances, and apply OS patches or application updates.



#### **Maintenance Windows**

* helps set up recurring schedules for managed instances to run administrative tasks like installing patches and updates without interrupting business-critical operations.



### Instances & Nodes

Capabilities for managing the EC2 instances, on-premises servers and virtual machines (VMs) in the hybrid environment, and other types of AWS resources (nodes)

#### **Systems Manager Configuration Compliance**

* helps scan fleet of managed instances for patch compliance and configuration inconsistencies.
* helps collect and aggregate data from multiple AWS accounts and Regions, and then drill down into specific resources that aren’t compliant.
* provides, by default, displays compliance data about Patch Manager patching and State Manager associations, but can be customized

#### **Session Manager**

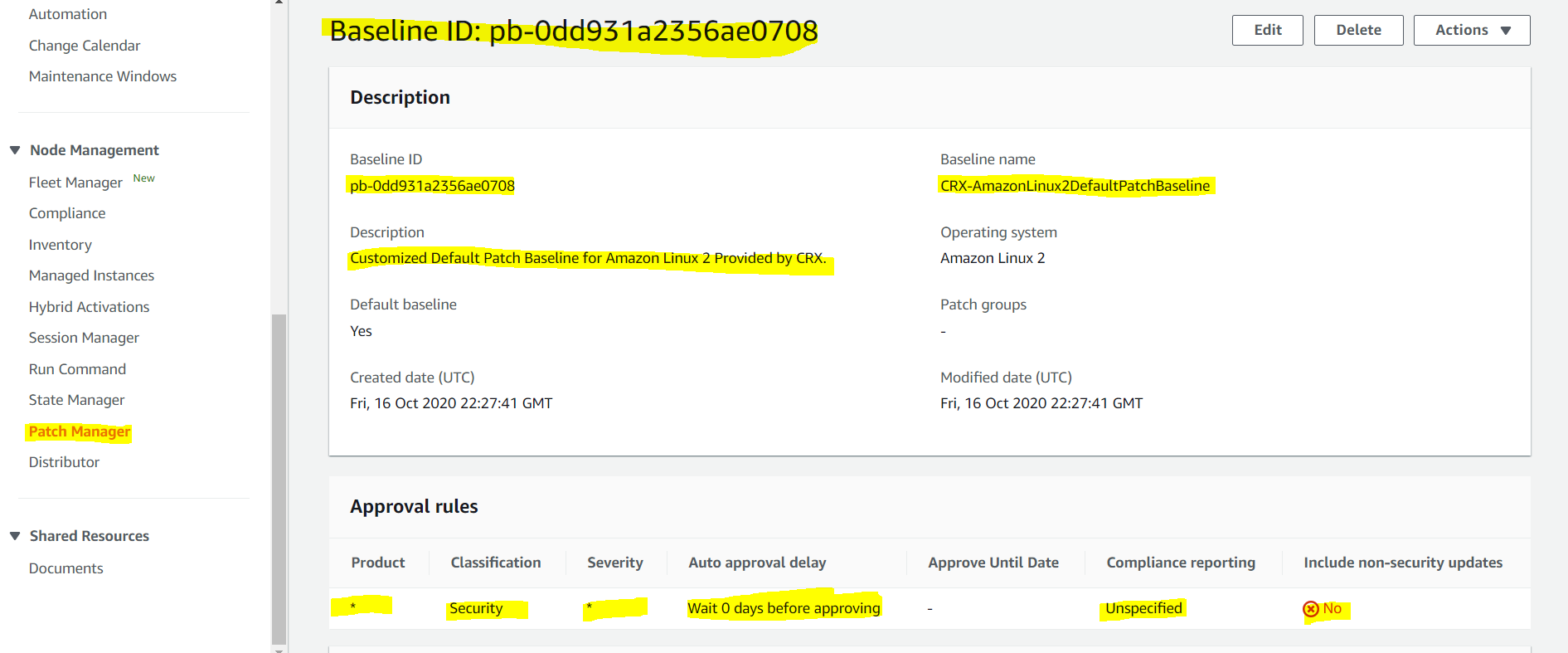
* helps manage EC2 instances through an interactive one-click browser-based shell or through the AWS CLI.
* **provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.**
* helps comply with corporate policies that require controlled access to instances, strict security practices, and fully auditable logs with instance access details, while still providing end users with simple one-click cross-platform access to the EC2 instances.

#### **Systems Manager Run Command**

* helps to remotely and securely manage the configuration of the managed instances at scale.
* helps perform on-demand changes like updating applications or running Linux shell scripts and Windows PowerShell commands on a target set of dozens or hundreds of instances.

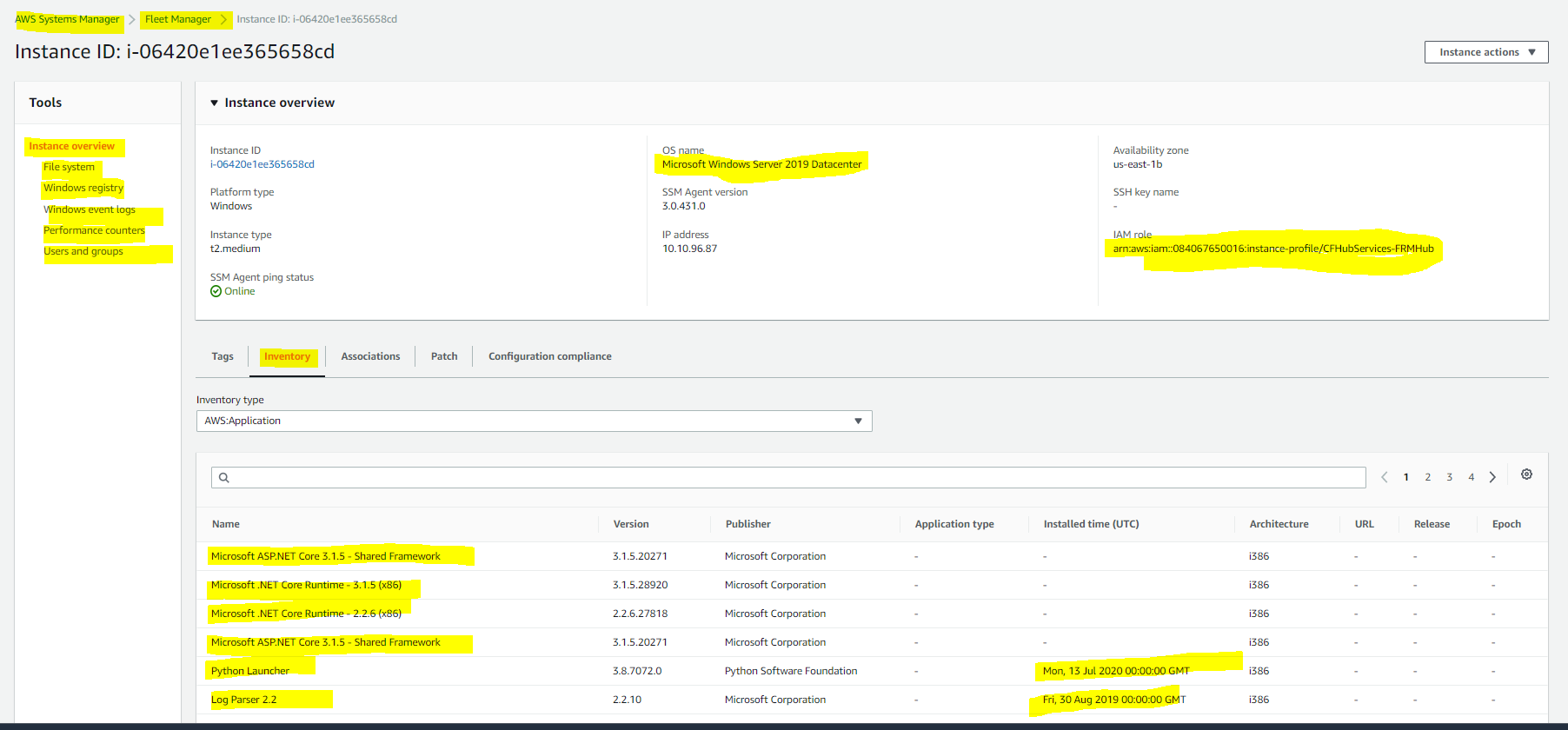
#### **Patch Manager**

* helps automate process of patching managed instances with both security related and other types of updates.
* helps apply patches for both operating systems and applications. **(On Windows Server, application support is limited to updates for Microsoft applications.)**
* enables scanning of instances for missing patches and applies them individually or to large groups of instances by using EC2 instance tags.
* uses patch baselines, which can include rules for auto-approving patches within days of their release, as well as a list of approved and rejected patches.
* helps install security patches on a regular basis by scheduling patching to run as a Systems Manager maintenance window task.



#### **Systems Manager Inventory**

* provides visibility into your Amazon EC2 and on-premises computing environment
* collect metadata from the managed instances about applications, files, components, patches, and more on your managed instances



#### **Systems Manager State Manager**

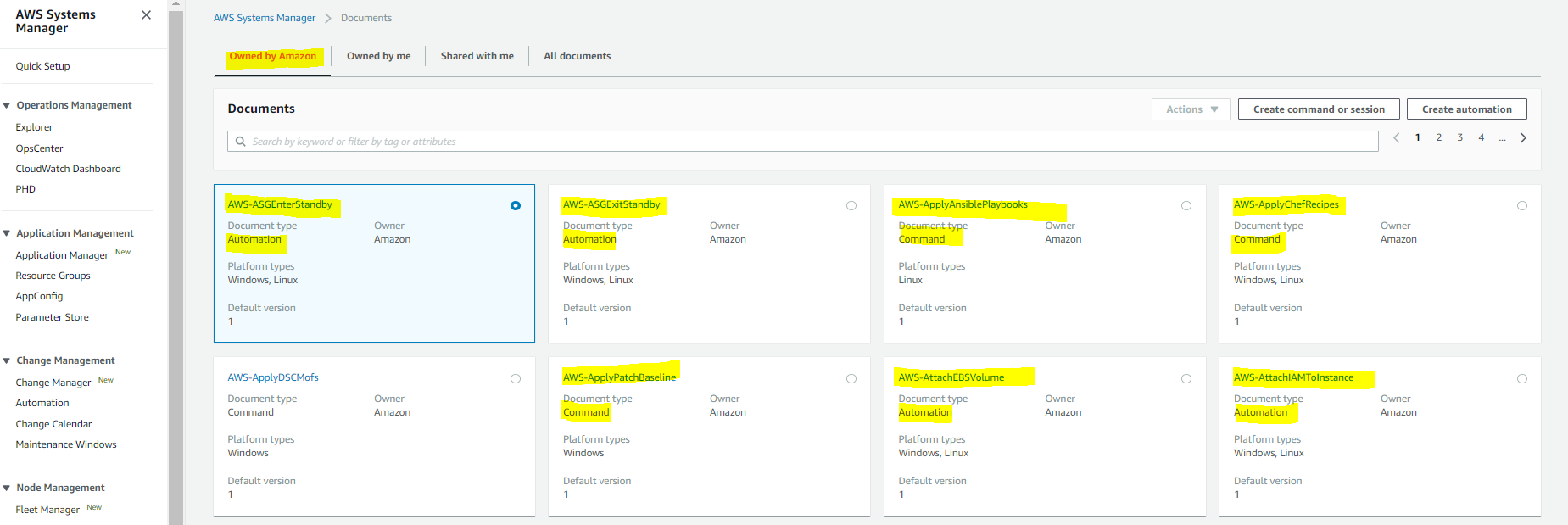
* helps automate the process of keeping the managed instances in a defined state.
* helps ensure that the instances are bootstrapped with specific software at startup, joined to a Windows domain (Windows instances only), or patched with specific software updates.

### Shared Resources

Capabilities for managing and configuring the AWS resources

#### **Systems Manager document (SSM document)**

* defines the actions that Systems Manager performs.
* SSM document types include
  + Command documents, which are used by State Manager and Run Command, and
  + Automation documents, which are used by Systems Manager Automation.



#### **Parameter Store**

* provides secure, hierarchical storage for configuration data and secrets management.
* can store data such as passwords, database strings, and license codes as parameter values.
* supports values as plain text or encrypted data, referenced by using the specified unique name

## Systems Manager Agent

* is software that can be installed and configured on an EC2 instance, an on-premises server, or a virtual machine (VM)
* makes it possible for Systems Manager to update, manage, and configure these resources
* must be installed on each instance to use with Systems Manager
* usually comes preinstalled with lot of Amazon Machine Images (AMIs), while it must be installed manually on other AMIs, and on on-premises servers and virtual machines for your hybrid environment

## AWS Certification Exam Practice Questions

1. Which of the following tools from AWS allows the automatic collection of software inventory from EC2 instances and helps apply OS patches?
   1. AWS Code Deploy
   2. **Systems Manager**
   3. EC2 AMI’s
   4. AWS Code Pipeline
2. A Developer is writing several Lambda functions that each access data in a common RDS DB instance. They must share a connection string that contains the database credentials, which are a secret. A company policy requires that all secrets be stored encrypted. Which solution will minimize the amount of code the Developer must write?
   1. Use common DynamoDB table to store settings
   2. Use AWS Lambda environment variables
   3. **Use Systems Manager Parameter Store secure strings**
   4. Use a table in a separate RDS database
3. A company has a fleet of EC2 instances and needs to remotely execute scripts for all of the instances. Which Amazon EC2 systems Manager feature allows this?
   1. Systems Manager Automation
   2. **Systems Manager Run Command**
   3. Systems Manager Parameter Store
   4. Systems Manager Inventory
4. As a part of compliance check it was found that EC2 instances launched by the deployment team were not in compliance to latest security patches. The team had all tagged the resources. Which AWS service can help make the instances complaint?
   1. AWS Inspector
   2. AWS GuardDuty
   3. **AWS Systems Manager**
   4. AWS Shield