AWS Systems Manager

Welcome to AWS Systems Manager.

What you will learn

At the core of the lesson

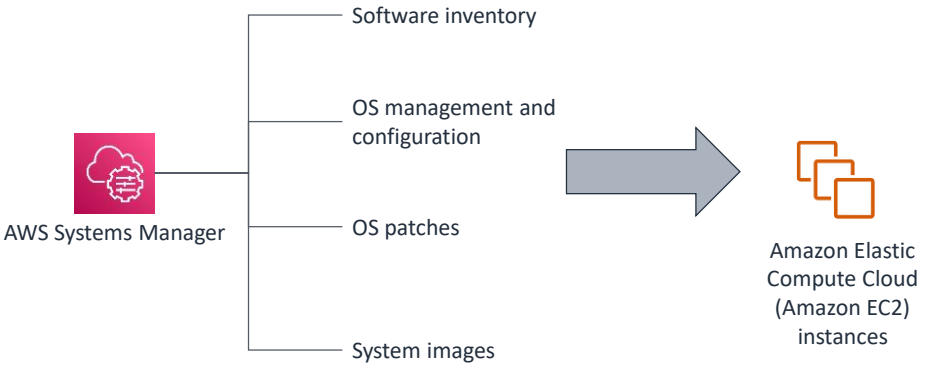
You will learn how to identify the capabilities of AWS Systems Manager.

aws re/start

At the end of this lesson, you will be able to identify the capabilities of AWS Systems Manager.

Systems Manager overview

Systems Manager is a collection of capabilities that help you manage your applications and infrastructure running in the AWS Cloud.



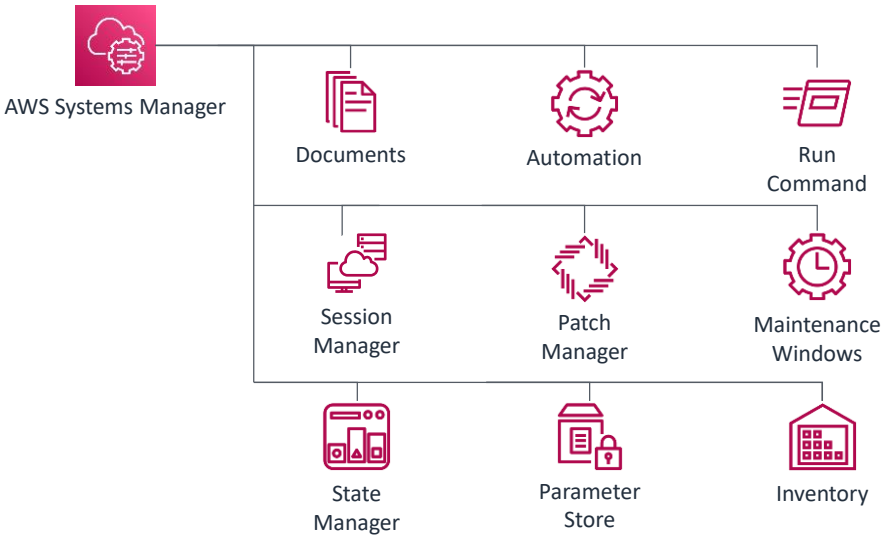
aws re/start

Systems Manager is a management service that helps a user perform and automate administration tasks, including the following:

- Collect software inventory.
- Configure Microsoft Windows and Linux operating systems.
- Apply operating system (OS) patches.
- Create system images.

Systems Manager automates the configuration and management of systems that run on premises and in the AWS Cloud. With Systems Manager, a user can select the instances that they want to manage and define the management tasks that they want to perform. Systems Manager also offers many capabilities and benefits that systems operations (SysOps) specialists find useful.

Capabilities overview

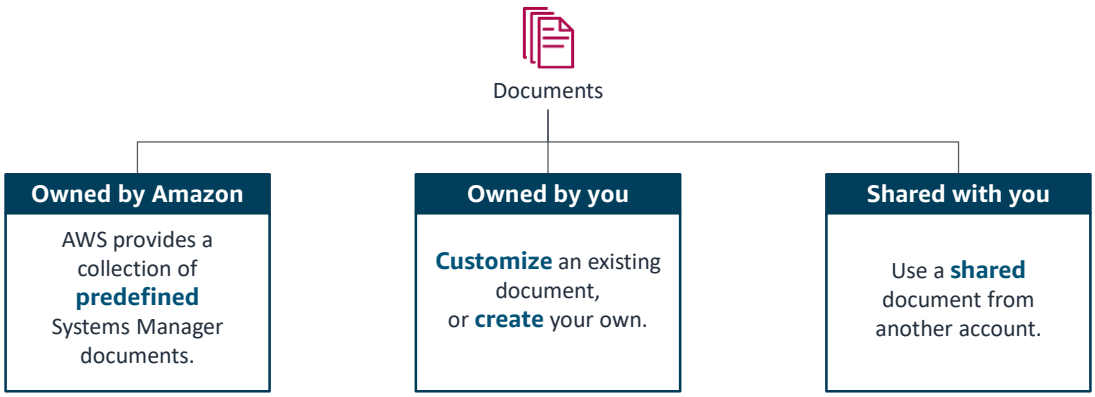


aws re/start

This slide shows the core capabilities of Systems Manager. You will learn more details about them in the subsequent slides.

Documents

A Systems Manager document defines the actions that Systems Manager performs on your managed instances.

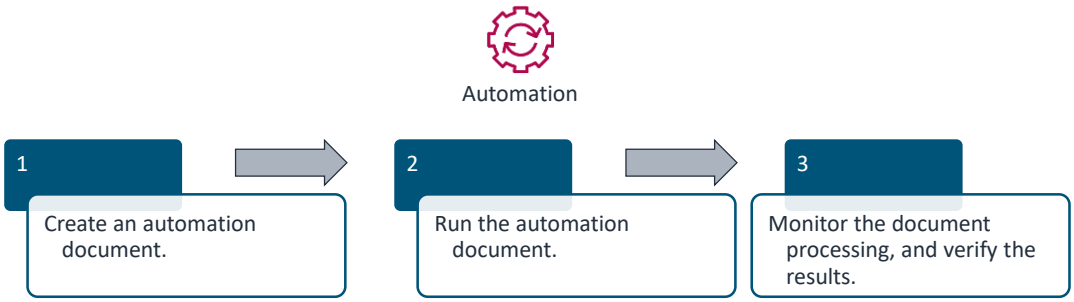


Documents are a core capability of many Systems Manager features. They define the steps and parameters of the actions that you want to perform on instances. Systems Manager document (SSM document) types include Command documents, which are used by State Manager and Run Command, and Automation runbooks, which are used by Systems Manager Automation.

Documents can be authored in JSON or YAML. You can use a predefined Systems Manager document, create your own custom document, or use a shared document.

Automation

Safely automate common and repetitive IT operations and management tasks across AWS resources.



aws re/start

The Automation capability in Systems Manager gives you the ability to define common IT tasks as a collection of steps in an SSM document. The Automation capability can then run all the document steps on an entire collection of AWS resources. For example, you can define an automation to remediate unreachable instances, create golden Amazon Machine Images (AMIs), or patch instances. Custom automations can also be authored in JSON. Amazon EventBridge can also be configured to initiate Systems Manager automations.

The following is a suggested approach to developing and testing a Systems Manager automation:

1. Create an automation document or use an existing automation template that includes sequential steps and parameters that Systems Manager runs.
2. Run the automation document. Depending on the actions requested in the document, Systems Manager will automatically perform certain steps, including the following:
    - Launch an instance.
    - Take a snapshot.
    - Tag an instance.
    - Delete old images.
    - Terminate an EC2 instance.
3. Monitor the automation workflow (for example, by using the AWS Management Console). After the automation finishes, confirm that the expected results were achieved. For example, you can launch a test instance from an AMI that was

updated by a Systems Manager automation to verify that it has the expected characteristics.

Run Command

The Systems Manager Run Command provides an automated way to run predefined commands against EC2 instances.

- Use predefined commands.
- Create your own.
- Choose instances or tags.
- Choose controls or schedules.
- Run a command immediately or on a specific schedule.

Run Command

Example command types

Command Name	Platform Types
AWS-InstallWindowsUpdates	Windows
AWS-RunPowerShellScript	Windows and Linux
AWS-RunShellScript	Linux and MacOS

aws re/start

Run Command gives you the ability to automate common administrative tasks and perform configuration changes at scale. You can use predefined Command documents or create your own. You can also choose the instances to administer manually or by using tags and can specify safety controls to indicate the number of instances that should be affected. Finally, you can run a command immediately or based on a specified schedule.

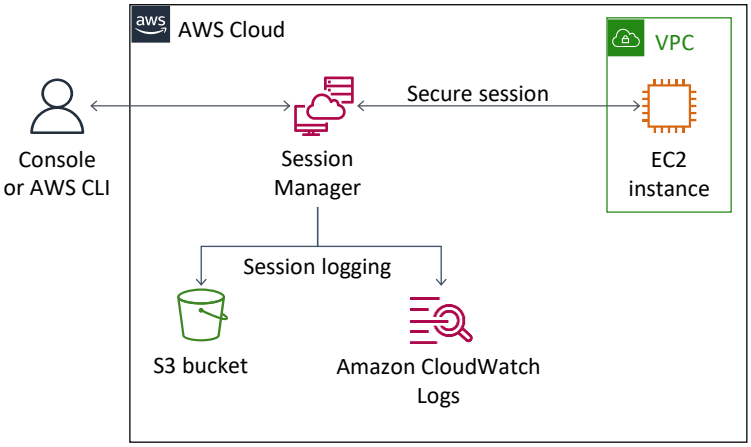
Run Command reduces management overhead because a user can manage instances without setting up bastion hosts or managing Secure Shell (SSH) keys and certificates. You can use Run Command from the AWS Management Console, the AWS Command Line Interface (AWS CLI), AWS Tools for Windows PowerShell, or the AWS SDKs.

Run Command provides a rich set of predefined commands. This slide lists examples of predefined commands and the OS platforms that they support. These commands include the following:

- AWS-InstallWindowsUpdates: This command scans for or installs missing updates on a Windows instance and optionally reboots the instance after the installation.
- AWS-RunPowerShellScript: This command runs a PowerShell script on a Windows or Linux instance.
- AWS-RunShellScript: This command runs a shell script on a Linux or macOS instance.

Session Manager

Securely connect to instances without opening inbound ports, using bastion hosts, or maintaining SSH keys.



aws re/start

With the Session Manager capability in Systems Manager, you can manage your EC2 instances through an interactive browser-based shell in the AWS Management Console. You can use also use the AWS CLI or SSH to start a session.

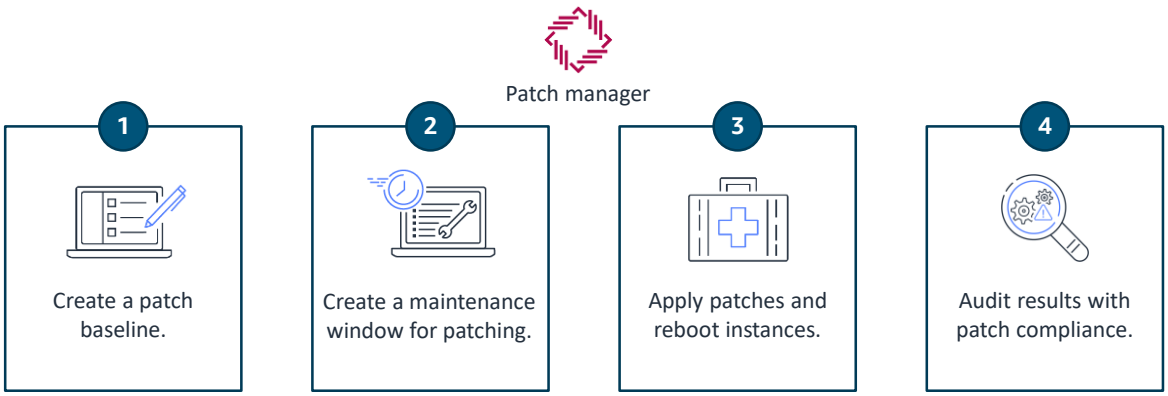
Session Manager provides secure and auditable instance management without the need to open inbound ports in the security groups, maintain bastion host instances in Amazon EC2 subnets, or manage SSH keys.

Session Manager also helps you comply with corporate policies that require controlled access to instances, strict security practices, and auditable logs that contain instance access details.

When you can connect to a Linux or Windows EC2 instance, Session Manager tracks each user who started a session on each instance. You can audit which user accessed an instance and when they accessed the instance using AWS CloudTrail. You can also configure Session Manager to log every command performed on an instance to Amazon Simple Storage Service (Amazon S3) or Amazon CloudWatch Logs.

Patch Manager

Deploy operating system and software patches automatically across large groups of EC2 instances or on-premises machines.



aws re/start

You might encounter several challenges when patching servers and instances, including the following:

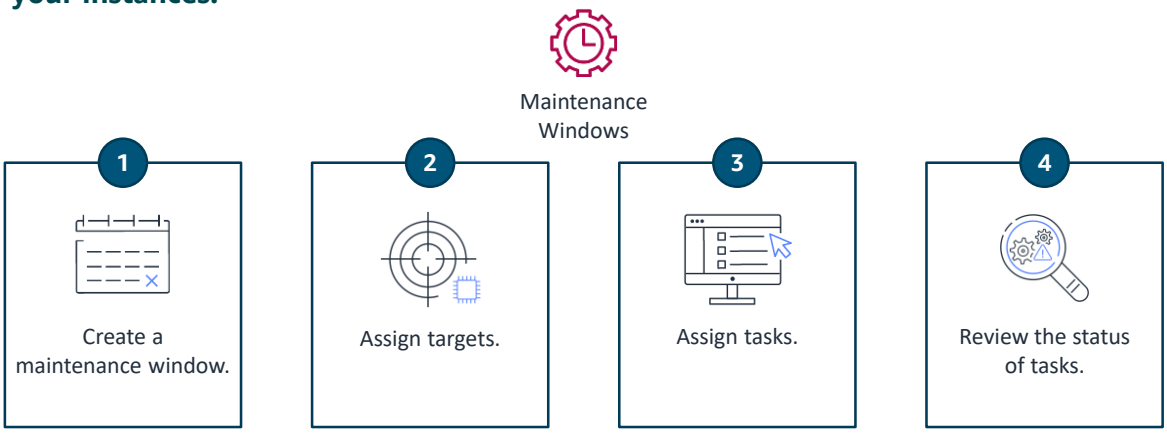
- The time that it takes to patch multiple EC2 instances or on-premises machines
- The repetitive nature of the task
- Errors that can result in downtime
- Compliance issues

You can use Patch Manager to automate patching by performing the following steps:

1. Create a patch baseline, which contains rules that automatically approve or reject released patches.
2. Define a maintenance window, and group instances together for patching.
3. Apply patches in the maintenance window, and reboot every instance in the patch group.
4. Review the results and the details of patch compliance.

Maintenance Windows

Schedule windows of time to run administrative and maintenance tasks across your instances.



aws re/start

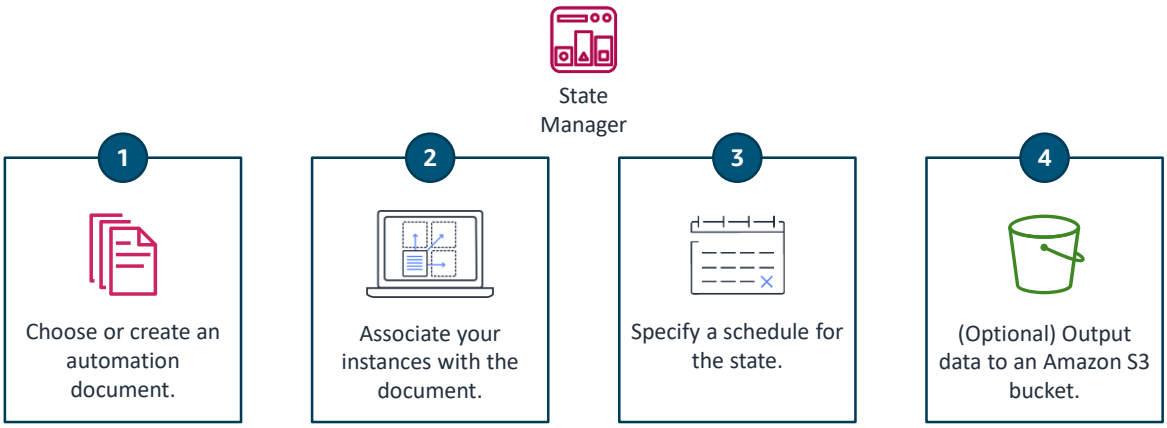
You can use Maintenance Windows to define a schedule for when to perform potentially disruptive actions on your instances. For example, these actions can include patching an operating system, updating drivers, or installing software or patches. The scheduled actions are run automatically, and the user can set limits for simultaneous task runs and allowable error rates.

The following are the steps to implement a Maintenance Window:

1. Create a maintenance window that specifies basic options, such as name, schedule, and duration.
2. Assign targets. These are the resources that the maintenance window tasks will update.
3. Assign tasks to be run on those targets. Types of tasks include the following:
    - Commands run by Systems Manager Run Command
    - Systems Manager Automation workflows
    - AWS Step Functions workflows
    - AWS Lambda functions
4. Review the status of the tasks after the tasks are completed.

State Manager

Maintain consistent configuration of Amazon EC2 or on-premises instances.



aws re/start

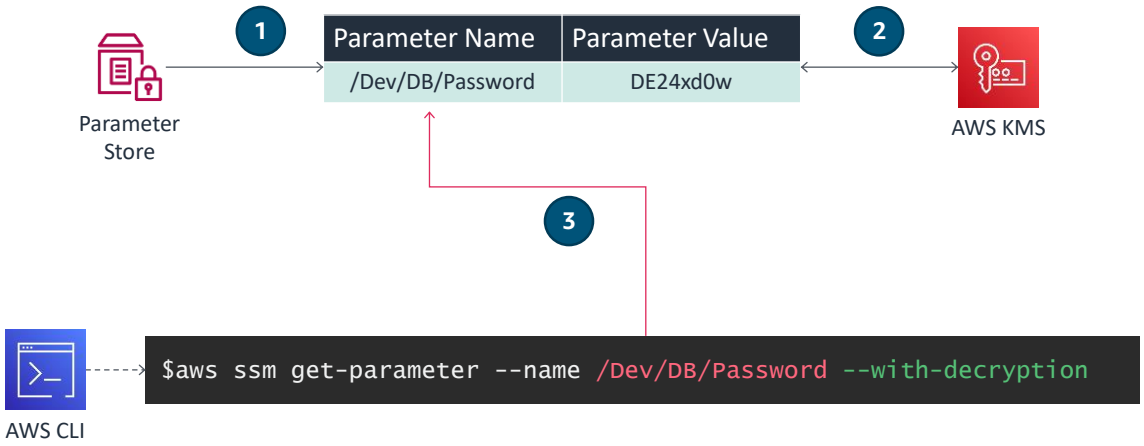
Systems Manager State Manager is a secure and scalable configuration management service that automates the process of keeping your Amazon EC2 and hybrid infrastructure in a state that you define. State Manager helps you prevent configuration drift and monitor the status of an instance's intended state.

Here is how State Manager works:

1. First, choose or create an SSM document or identify an existing one that defines the actions that State Manager will perform on your managed instances. The document defines the state that you want to apply.
2. Next, you associate instances with the document. This association identifies the individual or groups of instances that will be the target of the actions in the document that will configure the instance to the desired state.
3. When you create the association, you also define the schedule for how often to apply the configured state.
4. Finally, you can choose to write the output of the commands to an S3 bucket when you create the association.

Parameter Store

Parameter Store provides a centralized store to manage configuration data or secrets.



aws re/start

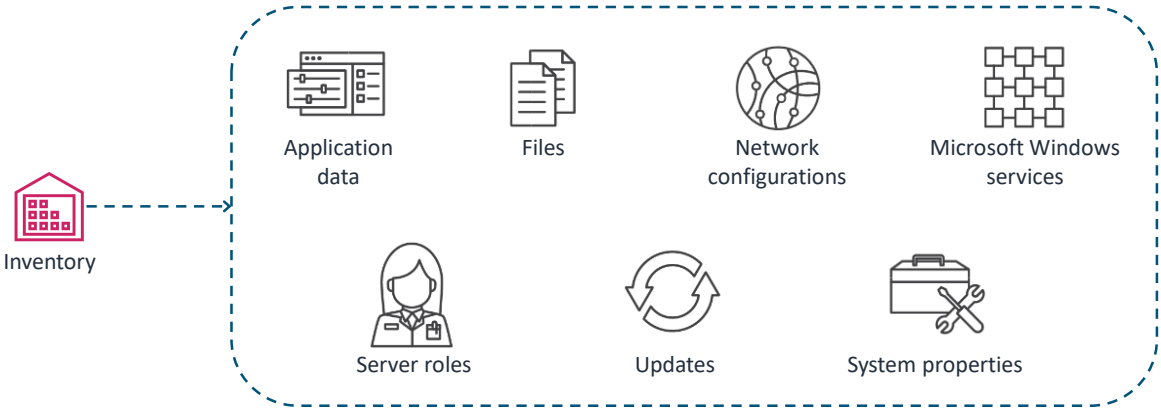
Parameter Store provides secure, hierarchical storage for configuration data management and secrets management. It stores data as name-value pairs and can store values as plain text or encrypted data. You can store data such as passwords, database strings, and AMI IDs as parameter values. You can then reference Systems Manager parameters in your scripts, commands, SSM documents, and configuration and automation workflows by using the parameter's unique name. If you choose to secure the parameter value when you create the parameter, Parameter Store uses the AWS Key Management Service (AWS KMS) service to encrypt the parameter value.

The following information describes this example:

1. You create a new parameter in Parameter Store to store a database password. The parameter has hierarchical path name of /Dev/DB/Password to indicate that it is a development environment password. You also indicate that the data is sensitive and must be encrypted.
2. Parameter Store uses the AWS KMS service to encrypt the parameter value and stores the encrypted value of DE24xd0w.
3. In the AWS CLI, when you need to retrieve the password, you can use the AWS SSM get-parameter command and pass it the name of the parameter, /Dev/DB/Password. You also include the --with-decryption option to get back the decrypted value of the parameter.

Inventory

The Inventory capability collects information about instances and the software that is installed on them.



aws re/start

The Systems Manager Inventory capability can collect inventory information about EC2 instances and the software installed on them, such as the following:

- Application data
- Files
- Network configurations
- Windows services
- Server roles
- Updates
- System properties

Inventory can provide a comprehensive understanding of the system configurations and installed applications across multiple instances, without the need to log in to each instance individually.

The gathered data supports managing application assets, tracking licenses, monitoring file integrity, discovering applications that were not installed by a traditional installer, and more.

Checkpoint questions

1. What are some ways that Systems Manager helps users?
2. Which Systems Manager capability defines the actions that Systems Manager performs on your managed instances?
3. Which Systems Manager capability can you use to manage your EC2 instances through an interactive browser-based shell in the AWS Management Console?

aws re/start

1. What are some ways that Systems Manager helps users?

   Systems Manager helps users perform and automate administration tasks, including the following:
   - Collect software inventory.
   - Configure operating systems.
   - Apply OS patches.
   - Create system images.

2. Which Systems Manager capability defines the actions that Systems Manager performs on your managed instances?

   Documents

3. Which Systems Manager capability can you use to manage your EC2 instances through an interactive browser-based shell in the AWS Management Console?

   Session Manager

Key ideas

- With Systems Manager, you can safely **automate common and repetitive IT operations and management tasks** across AWS resources.
- Systems Manager provides a suite of capabilities that help **automate** operational tasks across **AWS and on-premises resources**.
- You can use the **Patch Manager** and **Maintenance Windows** capabilities to **apply OS patches** based on a **predefined schedule**.

aws re/start

This lesson includes the following key takeaways:

- With Systems Manager, you can safely automate common and repetitive IT operations and management tasks across AWS resources.
- Systems Manager provides a suite of capabilities that help automate operational tasks across AWS and on-premises resources.
- You can use the Patch Manager and Maintenance Windows capabilities to apply OS patches based on a predefined schedule.

Thank you

Thank you for completing this lesson.