AWS Systems Manager

is an AWS service that provides visibility and control of infrastructure on AWS.

AWS Systems Manager provides a unified interface through which you can view operational data from multiple AWS services.

AWS Systems Manager allows you to automate operational tasks across your AWS resources.

Formally known as SSM, AWS Systems Manager is a central hub to control and view your entire AWS infrastructure.

It can aid with security within your account and helps automate remedial tasks to ensure your environment is as compliant as possible.

AWS Systems manager is a powerful service which allows you to have a holistic view of all of the services you are using to view and control your infrastructure on AWS.

AWS Systems Manager provides a unified interface through which you can view operational data from multiple AWS services.

With AWS Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources.

With AWS Systems Manager, you can select a resource group and view its recent API activity, resource configuration changes, related notifications, operational alerts, software inventory, and patch compliance status.

You can also take action on each resource group depending on your operational needs.

AWS Systems Manager simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easy to operate and manage your infrastructure securely at scale.

## 

## **Systems Manager Components**

AWS Systems Manager Inventory Manager Automates the process of collecting software inventory from managed instances.

You can simply specify the types of metadata to be collected, the instances from which the metadata should be gathered, and the schedule for collecting metadata.

AWS Systems Manager collects information about your instances and the software installed on them, helping you to understand your system configurations and installed applications.

The gathered data enables you to manage application assets, track licences, monitor file integrity, discover applications not installed by a traditional installer, and more.

#### **Configuration Compliance**

AWS Systems Manager lets you scan your managed instances for patch compliance and configuration inconsistencies.

You can collect and aggregate data from multiple AWS accounts and Regions, and then drill down into specific resources that aren’t compliant.

By default, AWS Systems Manager displays data about patching and associations. You can also customize the service and create your own compliance types based on your requirements.

#### **AWS Systems Manager Automation**

AWS Systems Manager allows you to safely automate common and repetitive IT operations and management tasks across AWS resources.

With Systems Manager, you can create JSON/YAML documents that specify a specific list of tasks or use community published documents.

These documents can be executed directly through the AWS Management Console, CLIs, and SDKs, scheduled in a maintenance window, or triggered based on changes to AWS resources through Amazon CloudWatch Events.

You can track the execution of each step in the documents as well as require approvals for each step.

You can also incrementally roll out changes and automatically halt when errors occur.

#### 

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

By using Run Command, you can automate common administrative tasks and make one-time configuration changes in bulk, and at enterprise scale.

This essentially prevents you from having to jump into every one of your instances and run the same command hundreds of times.

It is all actively managed within the console and there is an easy to use console in which to administer your commands, as well as a CLI or through the AWS SDK.

Example tasks include: stopping, restarting, terminating, and resizing instances. Attaching and detaching EBS volumes, creating snapshots and you can install or bootstrap an application, build a deployment pipeline etc.

Commands can be applied to a group of systems based on AWS instance tags or manual selection.

The commands and parameters are defined in an AWS Systems Manager document.

Commands can be issued using the AWS Console, AWS CLI, AWS Tools for Windows PowerShell, the AWS Systems Manager API, or Amazon SDKs.

#### **AWS Systems Manager Session Manager**

AWS Systems Manager provides safe; secure and remote management of your instances at scale without logging into your servers, replacing the need for bastion hosts, SSH, or remote PowerShell.

It provides a simple way of automating common administrative tasks across groups of instances such as registry edits, user management, and software and patch installations.

Session Manager provides a command terminal for Linux instances and Windows PowerShell terminal for Windows instances.

Session Manager not only provides a fully auditable terminal environment, but you can administer access to SSH sessions without having to open any ports, strongly enhancing your security posture. You can simply enable the least privileged IAM permissions to the Session Manager console and allow your developers to maximise their efficiency and effectiveness.

All actions taken with AWS Systems Manager are recorded by AWS CloudTrail, allowing you to audit changes throughout your environment.

CloudTrail can intercept StartSession events using Session Manager.

Compared to SSH:

• Do not need to open port 22.

• Do not need bastion hosts for management.

• All commands are logged to S3 / CloudWatch.

• Secure shell access is authenticated using IAM user accounts, not key pairs.

#### **Incident Manager**

You can automate solutions in the Incident Manager console to help bring the appropriate internal resources to your attention.

AWS Chatbot links designated chat channels to AWS Incident Manager, and Automation runbooks are executed for AWS Systems Manager using the Incident Manager.

Responders are engaged via SMS and phone calls in predefined response plans.

By suggesting action items based on Amazon’s post-incident analysis template, Incident Manager helps you improve service reliability. For example, you can automate a runbook step or add a new alarm after an incident.

#### **Systems Manager Patch Manager**

Patch Manager enables the automated patching your EC2 instances. It includes security patches, as well as other patches for both your applications and your operating systems.

Patch Manager uses what are known as patch baselines, which involve the definition of rules for auto-approving patches, as well as declined patches. By scheduling patching as a maintenance window task in Systems Manager, you can easily install patches on a regular basis.

Understanding the state of your servers that are part of your Systems Manager fleet is paramount to enabling a compliant and secure workload of your applications and your servers.

The process from end-to-end consists of obtaining metadata about your managed Systems Manager nodes (on-premise, EC2 etc.) Regardless of if you are using Systems Manager in the cloud or Systems Manager on-premise you store this metadata in a centralized repository (an S3 Bucket). You can from there query the metadata using native tools to gain insights into trends across your nodes in a number of different categories.

This aggregation of metadata can include multiple regions and multiple accounts, all in one place, and permissions to this sub-service can be granularly assigned using IAM as well as Service Control Policies for AWS Organizations.

#### 

#### **AWS Systems Manager Parameter Store**

AWS Systems Manager provides a centralised store to manage your configuration data, whether plain-text data such as database strings or secrets such as passwords.

This allows you to separate your secrets and configuration data from your code. Parameters can be tagged and organised into hierarchies, helping you manage parameters more easily.

For example, you can use the same parameter name, “db-string”, with a different hierarchical path, “dev/db-string” or “prod/db-string”, to store different values.

AWS Systems Manager is integrated with AWS Key Management Service (KMS), allowing you to automatically encrypt the data you store.

You are able to store these secrets in a way in which you don’t have to manage any servers, making the entire process much easier.

If your data is also kept separate from your code, you will be in a much better position security wise, as you are enabling separation.

You can also control user and resource access to parameters using AWS Identity and Access Management (IAM).

Parameters can be referenced through other AWS services, such as Amazon Elastic Container Service, AWS Lambda, and AWS CloudFormation.

#### **AWS Systems Manager Distributor**

Distributor is an AWS Systems Manager feature that enables you to securely store and distribute software packages in your organization.

You can use Distributor with existing Systems Manager features like Run Command and State Manager to control the lifecycle of the packages running on your instances.

#### **AWS Systems Manager State manager**

If you need to manage the state of your AWS EC2 resources, AWS Systems Manager State Manager enables you to maintain your instances in whichever state you like.

There are three steps in using Systems Manager State Manager:

1. Decide which state to apply to your resources

2. You may be able to create the desired state for your AWS resources with a pre-configured SSM document – you need to figure this out.

3. You then create an association between your instance and the state you have defined.

You can query AWS Systems Manager at any time to view the status of your instance configurations, giving you on-demand visibility into your compliance status.

#### **AWS Systems Manager OpsCenter**

If you have any operational issues related to your AWS Resources – you can use OpsCenter to provide a central location where operations engineers and IT professionals can view, investigate, and resolve operational work items (OpsItems) related to AWS resources

#### **AWS Systems Manager Maintenance Windows**

AWS Systems Manager lets you schedule windows of time to run administrative and maintenance tasks across your instances.

This ensures that you can select a convenient and safe time to install patches and updates or make other configuration changes, improving the availability and reliability of your services and applications.

#### **AWS Systems Manager Resource Groups**

You can use resource groups to organize your AWS resources. Resource groups make it easier to manage, monitor, and automate tasks on large numbers of resources at one time.

AWS Resource Groups provides two general methods for defining a resource group. Both methods involve using a query to identify the members for a group.

The first method relies on tags applied to AWS resources to add resources to a group. Using this method, you apply the same key/value pair tags to resources of various types in your account and then use the AWS Resource Groups service to create a group based on that tag pair.

The second method is based on resources available in an individual AWS CloudFormation stack. Using this method, you choose an AWS CloudFormation stack, and then choose resource types in the stack that you want to be in the group.

AWS Systems Manager Resource Groups allows the creation of logical groups of resources that you can perform actions on (such as patching).

Resource groups are regional in scope.

#### **Systems Manager Document**

An AWS Systems Manager document (SSM document) defines the actions that Systems Manager performs on your managed instances.

Systems Manager includes more than a dozen pre-configured documents that you can use by specifying parameters at runtime.

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

## 

## **Monitoring and Reporting**

#### **Insights Dashboard**

AWS Systems Manager automatically aggregates and displays operational data for each resource group through a dashboard.

Systems Manager eliminates the need for you to navigate across multiple AWS consoles to view your operational data.

With Systems Manager you can view API call logs from AWS CloudTrail, resource configuration changes from AWS Config, software inventory, and patch compliance status by resource group.

You can also easily integrate your AWS CloudWatch Dashboards, AWS Trusted Advisor notifications, and AWS Personal Health Dashboard performance and availability alerts into your Systems Manager dashboard.

Systems Manager centralises all relevant operational data, so you can have a clear view of your infrastructure compliance and performance.

#### **Amazon CloudWatch**

You can configure and use the Amazon CloudWatch agent to collect metrics and logs from your instances instead of using SSM Agent for these tasks. The CloudWatch agent enables you to gather more metrics on EC2 instances than are available using SSM Agent. In addition, you can gather metrics from on-premises servers using the CloudWatch agent.

#### **Logging and Auditing**

Systems Manager is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Systems Manager. CloudTrail captures all API calls for Systems Manager as events, including calls from the Systems Manager console and from code calls to the Systems Manager APIs.

SSM Agent writes information about executions, commands, scheduled actions, errors, and health statuses to log files on each instance. You can view log files by manually connecting to an instance, or you can automatically send logs to Amazon CloudWatch Logs.

## 

## **Authorisation and Access Control**

AWS Systems Manager supports identity-based policies.

AWS Systems Manager does not support resource-based policies.

You can attach tags to Systems Manager resources or pass tags in a request to Systems Manager.

To control access based on tags, you provide tag information in the condition element of a policy using the ssm:resourceTag/key-name, aws:ResourceTag/key-name, aws:RequestTag/key-name, or aws:TagKeys condition keys.

## **AWS Systems Manager Pricing**

There is no charge for most components in Systems Manager, and you only pay for the resources that are managed as part of the systems manager service.

There are some exceptions however – OpsCenter and Parameter store cost a small amount of money.

The OpsCenter pricing is as follows:

| **OpsCenter Details** | **Pricing** |
| --- | --- |
| Number of OpsItems | $2.97 per 1,000 OpsItems |
| Get, Describe, Update, and GetOpsSummary API requests | $0.039 per 1,000 requests |
|  |  |

The Parameter store pricing is also as follows:

| **Parameter type** | **Pricing** |
| --- | --- |
| Standard | No additional charge |
| Advanced | $0.05 per advanced parameter per month (prorated hourly if the parameter is stored less than a month) |

## 

## **AWS Systems Manager FAQ**

• Who should use Systems Manager?

If you are using many different services across many different accounts, and you want to gain keen operational insight into your AWS Resources, you can use Systems Manager. If you are a SysOps administrator you can gain great benefits from using Systems Manager.

• Which operating system can Systems Manager support?

You can use Systems Manager with both Linux and Windows operating systems.

• Which Regions can I use Systems Manager in?

There is a Systems Manager Region table, linked here which you can use to check your region.

• How can I use a Systems Manager?

You can use AWS Systems Manager with the CLI, SDK and the AWS Console.

Thanks for reading our breakdown of Systems Manager, and exploring how useful it is as a service.

* What is a managed instance?

A managed instance is any on-premises server or any Amazon EC2 instance that can be managed using AWS Systems Manager.

### **Related posts:**

* ****