## General

**Q: What is AWS Systems Manager?**
AWS Systems Manager allows you to centralize operational data from multiple AWS services and automate tasks across your AWS resources. You can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments. With 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. Systems Manager provides a central place to view and manage your AWS resources, so you can have complete visibility and control over your operations.

Show less

**Q: Who should use AWS Systems Manager?**
If you use multiple AWS services, AWS Systems Manager provides you with a centralized and consistent way to gather operational insights and carry out routine management tasks. You can use AWS Systems Manager to perform routine operations, track your development, test, and production environments, and proactively act on events or other operational incidents. AWS Systems Manager provides an operations complement to the more developer-focused tools you use, such as code editors and integrated development environments (IDEs). Similar to an IDE, AWS Systems Manager integrates a broad range of operations tools.

Show less

**Q: Does AWS Systems Manager manage instances running on-premises?**
Yes, AWS Systems Manager supports managing instances that are running in an on-premises data center. Refer to AWS Systems Manager prerequisites for more details.

Show less

**Q: How does AWS Systems Manager help manage Amazon EC2 instances and on-premises servers?**
AWS Systems Manager offers an agent to perform actions inside instances or servers. The agent is completely open-sourced and available on GitHub.

Show less

**Q: Can I privately access AWS Systems Manager APIs from my VPC without using public IP addresses?**
Yes, you can privately access AWS Systems Manager APIs from your VPC (created using Amazon Virtual Private Cloud) by creating VPC Endpoints. With VPC Endpoints, the routing between the VPC and AWS Systems Manager is handled by the AWS network without the need for an internet gateway, NAT gateway, or VPN connection. The latest generation of VPC Endpoints used by AWS Systems Manager are powered by AWS PrivateLink, a technology that enables private connectivity between AWS services using Elastic Network Interfaces (ENIs) with private IP addresses in your VPCs. To learn more about PrivateLink, visit the PrivateLink documentation.

**Q: What sorts of insights can I gather through AWS Systems Manager?**
AWS Systems Manager overlays information from multiple AWS services. These cross-service insights are surfaced through multiple native dashboards. AWS Systems Manager also embeds Amazon CloudWatch dashboards and lets you reuse your existing dashboards or build new ones.

Show less

**Q: What are built-in insights?**
AWS Systems Manager's built-in insights are dashboards that include recent API calls through AWS CloudTrail, recent configuration changes through AWS Config, Instance software inventory listings, instance patch compliance views, and instance configuration compliance views. You can filter these account-level insights to reflect the members of a particular resource group. These dashboards also show recent event logs through AWS Personal Health Dashboard and optimization recommendations through AWS Trusted Advisor.

Show less

**Q: What is a managed instance?**
A managed instance is any on-premises server or Amazon EC2 instance that can be managed using AWS Systems Manager. A managed instance can be a physical server or virtual machine in your on-premises data center or even another cloud provider.

Show less

**Q: What are AWS Systems Manager activations?**
AWS Systems Manager activations enable hybrid and cross-cloud management. Using AWS Systems Manager activations, you can easily register any server, whether physical or virtual to be managed by AWS Systems Manager.

Show less

**Q: How do I register an instance using AWS Systems Manager activation?**
You can create an AWS Systems Manager activation from the AWS Systems Manager console or API, which gives you an activation code and ID. Using this activation code and ID, you can run a command on your servers to register them to Systems Manager.

Show less

**Q: What is an AWS Systems Manager document?**
An AWS Systems Manager document enables configuration as code to manage resources at scale. An AWS Systems Manager document defines a series of actions that allows you to remotely manage instances, ensure desired state, and automate operations. An AWS Systems Manager document is cross-platform and can be used for Windows and Linux instances.

Show less

**Q: How do I create my own AWS Systems Manager document?**
You can author AWS Systems Manager documents in JSON or YAML to match the defined document schema, from the AWS Systems Manager console or the APIs.

Show less

## Resource Groups

**Q: What is the relationship between AWS Systems Manager and AWS Resource Groups?**
The AWS Systems Manager console integrates with AWS Resource Groups, and it offers grouping capabilities in addition to other native integrations.

Show less

**Q: Can I create resource groups through AWS Systems Manager?**
You can use the AWS Systems Manager console to create your own heterogeneous resource groups by using a tag query. This query will contain all of the AWS resources that are tagged that match a particular tag query. By creating your own resource groups, you can produce AWS Systems Manager views that reflect how you think about your resources. For instance, you might want to create resource groups by application component, application tier, or areas of operational ownership.

Show less

variety of example actions, such as restarting instances in a resource group after approval or patching Amazon EC2 instances, three at a time.

Show less

## CloudWatch Dashboards

**Q: What are Amazon CloudWatch Dashboards?**
With Amazon CloudWatch Dashboards, you can create reusable dashboards that allow you to monitor your AWS resources in one location. Metric data is kept for a period of fifteen months enabling you to view up-to-the-minute data and also historical data.

Show less

**Q: How are Amazon CloudWatch Dashboards integrated with AWS Systems Manager?**
Your existing CloudWatch Dashboards are now available directly through AWS Systems Manager. You can also create new CloudWatch Dashboards directly from Systems Manager. Using CloudWatch Dashboards, you can build your own custom operational dashboards to reflect the health of an application component, an application tier, or general areas of operational ownership.

Show less

**Q: Can I collect customized information from an Amazon EC2 instance or an on-premises instance?**

Yes, you can create custom inventory types to collect additional system properties, which can be gathered by the instance itself or recorded using the API. Some examples include JSON-formatted results from PowerShell or other applications, and information statically stored in JSON files such as rack-info.

Show less

**Q: How can I track changes to my configuration over time?**

Using AWS Config, you can monitor an instance's compliance with a desired configuration through AWS Config rules. This capability allows security experts and compliance auditors to have a complete audit trail of instance configuration changes, as well as receive proactive notifications in the event of non-compliance.

Show less

**Q: Can I view or query inventory data from across AWS accounts or Regions?**

Yes, you can sync inventory data from multiple accounts and Regions to the same Amazon S3 bucket. You can then use Amazon Athena, Amazon QuickSight, or your own business intelligence (BI) tools to query inventory data across accounts and Regions.

Show less

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.

Show less

**Q: Can I track changes to my configuration over time?**

Using an integration with AWS Config, you can monitor an instance's compliance with a desired configuration through AWS Config rules. This capability allows security experts and compliance auditors to have a complete audit trail of instance configuration changes, as well as receive proactive notifications in the event of non-compliance.

Show less

**Q: How do I view the compliance levels of my instances?**

With AWS Systems Manager you can view patch compliance information, which tells you the detailed results of the patching process. You can easily get aggregate compliance details per instance. In addition, you can drill in further and for each instance you can determine which patches are installed, missing, not applicable, and which failed to install.

Show less

**Q: Can I create my own compliance checks?**

Yes. You can create your own compliance types that can be recorded through the API. Based on

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.

Show less

**Q: What tasks can I automate?**

You can automate any task that involves interaction with AWS and on-premises resources. Built-in action types let you easily interact with Amazon EC2 instances, AWS CloudFormation stacks, and more. Action types are available to invoke AWS Systems Manager run command, PowerShell scripts, and AWS Lambda functions.

Show less

**Q: Are there predefined AWS Systems Manager automation documents?**

There are over 20 predefined AWS Systems Manager automation documents that you can click and execute to accomplish a wide range of tasks such as baking golden AMIs, patching Amazon EC2 instances, managing instance states, and more.

Show less

**Q: Can I execute AWS Systems Manager automation documents against an entire resource group?**
Yes. You can target resource groups and execute AWS Systems Manager automation documents against specific resource types. You can also specify safety controls to indicate the number of resources in the group that should be simultaneously executed against, and you can add error thresholds that will stop AWS Systems Manager automation document execution.

Show less

**Q: Can I execute AWS Systems Manager automation document steps one at a time?**
Yes. You can execute the entire AWS Systems Manager automation document in one action or choose to execute one step at a time.

Show less

**Q: Can I trigger AWS Systems Manager automation document execution on a schedule or based on other events?**
Yes. You can schedule AWS Systems Manager automation document execution to be triggered as an Amazon CloudWatch Events target, or you can use AWS Systems Manager maintenance windows to trigger AWS Systems Manager automation document execution on a schedule. You can also trigger AWS Systems Manager automation document execution based on changes to AWS resources through Amazon CloudWatch Events.

the actions users can perform on instances. All actions taken with Systems Manager are recorded by AWS CloudTrail, allowing you to audit changes throughout your environment.

Show less

**Q: Does AWS provide any predefined commands?**
Yes. There are predefined commands available which are designed to help with commonly used administrative tasks. For Windows you can run a PowerShell or Shell command or script, configure Windows Update settings, and deploy an MSI application and more. For Linux you run any Shell command or script, and remotely update an installed agent. You can also create custom commands to perform common tasks required for your environment.

Show less

**Q: Can I make bulk changes across my environments?**
Yes. You can act against large groups of instances by targeting using tag based queries. You can propagate changes safely across your environments by setting up rate control, which allows you to specify simultaneous execution batches with error thresholds.

Show less

**Q: Can I control who can execute a command?**
Yes. Using the published AWS Identity and Access Management (IAM) permissions and policies, you can use tag-based permissions to control who has access to execute commands or documents on specific instances. For example, you can specify an IAM user who can run PowerShell commands,

need to open inbound ports, maintain bastion hosts, and manage SSH keys. Session Manager helps to enable compliance with corporate policies that require controlled access to instances, increase security and auditability of instance access, while providing the simplicity and cross-platform instance access to end users.

Show less

**Q: What are the benefits of using Session Manager?**

Session Manager improves your security posture by not requiring you to open inbound ports, or to maintain SSH keys or certificates on your instances. It also centralizes access to instances using AWS Identity and Access Management (IAM). Once you enable Session Manager, you can connect to any Linux or Windows EC2 instance and track each user who started a session on each instance. You can audit which user accessed an instance and when using AWS CloudTrail, and log every command executed on an instance to Amazon S3 or Amazon CloudWatch Logs. Finally, with Session Manager you don't need up-front investments to operate and maintain bastion hosts.

Show less

**Q: Who should use Session Manager?**

Any AWS customer who wants to improve their security and audit posture, reduce operational overhead by centralizing access control on instances, and reduce inbound instance access will benefit from Session Manager. Information Security experts who want to monitor and track instance access and activity, and close down inbound ports on instances, or enable connecting to instances without a public IP will benefit from Session Manager. Administrators who want to grant and revoke access from a single place and want to provide one solution for Windows and Linux

**Q: How much does Session Manager cost?**
Session Manager is available at no additional cost to manage Amazon EC2 instances.

Show less

**Q: How do I get started?**
The quickest way to get started with Session Manager is to use the AWS Management Console. You can turn on Session Manager in a few clicks. For additional details, see the Getting Started documentation.

Show less

**Q: Does Session Manager require the use of the AWS Systems Manager Agent?**
Yes. Getting started with Session Manager requires the use of the latest version of the SSM Agent. The SSM Agent is open-sourced and on GitHub.

Show less

**Q: Can I turn on logging across an account?**
Yes. You can enforce logging across an account by setting up Session Manager preferences.

Show less

**Q: How do I specify when I want to patch an instance?**
You can use an AWS Systems Manager maintenance window to define when patching occurs. AWS Systems Manager provides you the ability to define one or more recurring windows of time during which it is acceptable for your own maintenance to occur. By defining these windows and associating your instances with them, it is easier for you to ensure that any maintenance activities you perform on your instances which may affect the availability of a workload is done so during a well-defined window of time.

Show less

**Q: How do I customize the patching process?**
AWS Systems Manager provides a fully automated patching process. You can easily customize the patching process by writing your own AWS Systems Manager command or automation document.

Show less

**Q: What types of patches can I install?**
AWS Systems Manager supports the patching of Windows- and Linux-based instances. Please visit our documentation to see the versions currently supported.

Show less

**Q: How do I pick the patches I want to install?**
Patch baselines define the set of patches you have approved or blocked for deployment to your

process. From the AWS Systems Manger console or APIs, you can easily get aggregate compliance details per instance. In addition, you drill in further and for each instance you can determine which patches are installed, missing, not applicable, and which failed to install.

Show less

## Maintenance Windows

**Q: What is an AWS Systems Manager maintenance window?**
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.

Show less

**Q: Why should I use AWS Systems Manager maintenance windows?**
AWS Systems Manager maintenance windows help improve availability and reliability of your workloads by automatically performing tasks in a well-defined window of time, significantly reducing the impact of any operational or infrastructure failures.

Show less

Show less

**Q: What types of tasks can I schedule in an AWS Systems Manager maintenance window?**
You can create and schedule any AWS Systems Manager run command execution, AWS Systems Manager automation document execution, AWS Step Functions, or AWS Lambda functions as tasks.

Show less

**Q: What are the types of schedules I can choose for my AWS Systems Manager maintenance windows?**
AWS Systems Manager maintenance windows can be scheduled for a recurring date (e.g., weekly on Tuesdays at 22:00:00 or first Sunday of every month at 22:00:00). You can define your schedule using cron or rate expression.

Show less

## State Manager

**Q: What is AWS Systems Manager state manager?**
AWS Systems Manager provides configuration management, which helps you maintain consistent configuration of your Amazon EC2 or on-premises instances. With Systems Manager, you can

drift, and monitor the status of your intended state.

Show less

**Q: How do I create my policies?**
Policies can be easily created through AWS Systems Manager documents. In addition, you also have predefined configurations that you can use for installing applications, joining instances to domain and so on.

Show less

**Q: What are the targets that can be configured?**
You have the flexibility to target instances or tags. This means you have the flexibility to have specific configurations for groups of instances such as web servers.

Show less

**Q: Can I use my existing configuration management tools with AWS Systems Manager state manager?**
Yes. AWS provides pre-defined AWS Systems Manager documents to run Ansible playbooks or Salt States, and you can use PowerShell DSC on your instances using AWS Systems Manager state manager to mitigate configuration drift. In addition, you can also directly run any configuration scripts from your public or private GitHub repository.

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

Show less

**Q: Why should I use AWS Systems Manager parameter store?**
It is a best practice to store configuration data and secrets separately from your code. You can use AWS Systems Manager parameter store to quickly store and reference configuration and sensitive information. Rather than storing data in config files or referencing them in plain text, you can store and obtain this information in your applications or scripts. Additionally, you control who has access to parameters so that only the right set of users has access to the appropriate information.

Show less

**Q: How do you store sensitive data?**
A secure string is any sensitive data that needs to be stored and referenced in a secure manner. If you have data that you do not want users to reference in clear text or have access to data that can be tampered with or misused, you should use secure strings in AWS Systems Manager parameter store. You can encrypt your sensitive data using your own AWS Key Management Service (KMS) key or your user account default key provided by AWS KMS.

Show less

Show less

**Q: Can I track changes to parameters?**
Yes, you can see history of parameter changes. You can also use versions that are automatically incremented upon change to look up specific parameter value bases on its version.

Show less

**Q: Can I store hierarchical data as parameters?**
Yes, you can use a hierarchical structure to store parameters. You can also control and audit access at every level of the hierarchy.

Show less

**Q: Can I receive notifications upon changes to parameter values?**
Yes, you can set up Amazon CloudWatch and Amazon Simple Notification Service (SNS) notifications for individual parameter values, and receive notifications upon change.

Show less

**Q: What is the difference between Secrets Manager and Parameter Store?**
AWS Secrets Manager is a service to manage the lifecycle for the secrets used in your organization centrally including rotation, audit, and access control. Secrets Manager helps you meet your

**Q: Should I use Parameter Store or Secrets Manager?**
If you want a single store for configuration and secrets, you can use Parameter Store. If you want a dedicated secrets store with lifecycle management, use Secrets Manager. Parameter Store is available at no additional charge with limit of 10,000 parameters. Refer to secrets manager pricing page for pricing details.

Show less

**Q: Is there a difference in the security model of Parameter Store and Secrets Manager?**
No. Both Secrets Manager and Parameter Store are equally secure. Both services support encryption at rest using customer-owned KMS keys. For more information on how Parameter Store uses KMS, please see the KMS Developer Guide on how Parameter Store uses AWS KMS.

Show less

**Q: Can I use Secrets Manager with Parameter Store?**
No. You cannot reference a Secrets Manager secret with Parameter Store at this time.

Show less

## Learn more about AWS Systems Manager partners

## AWS Systems Manager

- Overview
- Features
- Pricing
- Getting Started
- FAQs
- Partners

Twitter Facebook Podcast Twitch AWS Blog RSS News Feed
Email Updates

**AWS & Cloud Computing**

What is Cloud Computing?
What is Caching?
What is NoSQL?
What is DevOps?
What is Docker?
Products & Services
Customer Success
Economics Center
Architecture Center
Security Center
What's New
Whitepapers
AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal

**Solutions**

Websites & Website Hosting
Business Applications
Backup & Recovery

## AWS Systems Manager

- Overview
- Features
- Pricing
- Getting Started
- FAQs
- Partners

Power & Utilities
Oil & Gas
Automotive
Blockchain
Manufacturing

**Resources & Training**

Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS
SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Quick Starts

**Manage Your Account**

Management Console
Billing & Cost Management
Subscribe to Updates