**AWS Systems Manager FAQs**

## **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.

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.

Q: How do I get started?  
Getting started with AWS Systems Manager is easy. Using the AWS Management Console, navigate to the AWS Systems Manager console. You can create a resource group by using a simple tag query, then begin exploring the integrated set of operational tools that AWS Systems Manager provides.

Q: Which operating systems does AWS Systems Manager support?  
AWS Systems Manager is optimized to manage both Windows and Linux platforms from a single unified experience. Refer to the [documentation](http://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-managedinstances.html) for more details on managing on-premises systems.

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](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/systems-manager-prereqs.html) for more details.

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](https://github.com/aws/amazon-ssm-agent).

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](http://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-setting-up-vpc.html), 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](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html#what-is-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](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html#what-is-privatelink).

Q: In what Regions is AWS Systems Manager available?  
See the [AWS Regions Table](https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/) for AWS Systems Manager Region availability.

Q: Can I still use Amazon EC2 Systems Manager through the EC2 console?  
Yes. Users who are accustomed to using EC2 Systems Manager in the EC2 console will find a link to AWS Systems Manager. Amazon EC2 Systems Manager services are still easy to discover and use. AWS Systems Manager offers a new user experience for these tools.

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](https://aws.amazon.com/cloudwatch/) dashboards and lets you reuse your existing dashboards or build new ones.

Q: What are built-in insights?  
AWS Systems Manager’s built-in insights are dashboards that include recent API calls through [AWS CloudTrail](https://aws.amazon.com/cloudtrail/), recent configuration changes through [AWS Config](https://aws.amazon.com/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](https://aws.amazon.com/premiumsupport/phd/) and optimization recommendations through [AWS Trusted Advisor](https://aws.amazon.com/premiumsupport/trustedadvisor/).

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.

Q: How do I set up a managed instance?  
You can set up an EC2 instance as a managed instance by installing the Systems Manager agent and attaching an [AWS Identity and Access Management (IAM)](https://aws.amazon.com/iam/) instance profile to the instance, which gives Systems Manager permission to perform actions on your instance. To register servers or virtual machines outside of Amazon EC2, you can create an activation.

Q: Do some operating systems already include the Systems Manager agent?  
The Systems Manager agent is installed by default on the AWS Windows AMIs, on the Amazon Linux AMI, and available on the Amazon Linux repo. You can also install the agent on other supported operating systems.

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.

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.

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.

Q: Where can I use AWS Systems Manager documents?  
You can use Systems Manager documents with run command, state manager, or automation features.

Q: Are there pre-defined AWS Systems Manager documents?  
Yes. You can choose from a variety of pre-defined AWS Systems Manager documents that automate common tasks including collecting inventory, installing applications, joining instances to a domain, instance operations, collecting metrics, and more.

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.

## **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.

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.

Q: What are resource group insights in AWS Systems Manager?  
AWS Systems Manager offers a collection of resource-group-specific insights. These insights include recent API calls through [AWS CloudTrail](https://aws.amazon.com/cloudtrail/), recent configuration changes through [AWS Config](https://aws.amazon.com/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.

Q: What are resource group actions in AWS Systems Manager?  
AWS Systems Manager lets you execute AWS Systems Manager automation documents directly on a resource group. The members of the resource group itself will be passed to the AWS Systems Manager automation document as an input. AWS Systems Manager automation documents offer a variety of example actions, such as restarting instances in a resource group after approval or patching Amazon EC2 instances, three at a time.

## **CloudWatch Dashboards**

Q: What are Amazon CloudWatch Dashboards?  
With [Amazon CloudWatch Dashboards](https://aws.amazon.com/cloudwatch/), 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.

Q: How are Amazon CloudWatch Dashboards integrated with AWS Systems Manager?  
Your existing [CloudWatch Dashboards](https://aws.amazon.com/cloudwatch/) are now available directly through AWS Systems Manager. You can also create new [CloudWatch Dashboards](https://aws.amazon.com/cloudwatch/) directly from Systems Manager. Using [CloudWatch Dashboards](https://aws.amazon.com/cloudwatch/), 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.

## **Inventory**

Q: What is AWS Systems Manager inventory?  
AWS Systems Manager collects information about your instances and the software installed on them, helping you to understand your system configurations and installed applications. You can collect data about applications, files, network configurations, Windows services, registries, server roles, updates, and any other system properties. The gathered data enables you to manage application assets, track licenses, monitor file integrity, discover applications not installed by a traditional installer, and more.

Q: Can I collect customized information from an Amazon EC2 instance or an on-premises instance?  
Yes, you can create [custom inventory](http://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-inventory-about.html#sysman-inventory-custom) 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.

Q: How can I track changes to my configuration over time?  
Using [AWS Config](https://aws.amazon.com/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.

Q: Can I view or query inventory data from across AWS accounts or Regions?   
Yes, you can [sync inventory data](http://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-inventory-datasync.html) from multiple accounts and Regions to the same [Amazon S3](https://aws.amazon.com/s3/) bucket. You can then use [Amazon Athena](https://aws.amazon.com/athena/), [Amazon QuickSight](https://aws.amazon.com/quicksight/), or your own business intelligence (BI) tools to query inventory data across accounts and Regions.

Q: Can I perform analytics and visualization on inventory data?  
Yes, in addition to a built-in inventory dashboard, you can build advanced analytics and visualizations on inventory data with [Amazon Athena](https://aws.amazon.com/athena/) and [Amazon QuickSight](https://aws.amazon.com/quicksight/).

## **Configuration Compliance**

Q: What is AWS Systems Manager 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](http://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-state-about.html#sysman-state-assoc). You can also customize the service and create your own compliance types based on your requirements.

Q: Can I track changes to my configuration over time?  
Using an integration with [AWS Config](https://aws.amazon.com/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.

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.

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 your business requirements, you can create your own checks and then record the compliance through AWS Systems Manager to track non-compliant instances. You can also view this compliance information across accounts and Regions by creating a [resource data sync](http://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-inventory-datasync.html).

## **Automation**

Q: What is 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 documents that specify a specific list of tasks or use community published documents. These documents can be executed directly through the [AWS Management Console](https://aws.amazon.com/console/), [CLIs](https://aws.amazon.com/cli/), and [SDKs](https://aws.amazon.com/tools/), scheduled in a maintenance window, or triggered based on changes to AWS resources through [Amazon CloudWatch](https://aws.amazon.com/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.

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](https://aws.amazon.com/ec2/) instances, [AWS CloudFormation](https://aws.amazon.com/cloudformation/) stacks, and more. Action types are available to invoke AWS Systems Manager run command, PowerShell scripts, and [AWS Lambda](https://aws.amazon.com/lambda/) functions.

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.

Q: Can I create my own AWS Systems Manager automation documents?  
You can customize existing AWS Systems Manager automation documents or create your own using JSON or YAML. You can also use AWS Systems Manager automation documents shared by another account and share your document with others.

Q: Can AWS Systems Manager automation help with the approval process?  
Yes. Built-in approval action types can be included in your AWS Systems Manager automation documents. The approver can be one or more [AWS Identity and Access Management (IAM)](https://aws.amazon.com/iam/) users. AWS Systems Manager automation document execution will wait until the minimum number of required approvals are received or denied and proceed appropriately.

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.

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.

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](https://aws.amazon.com/cloudwatch/) 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.

## **Run Command**

Q: What is AWS Systems Manager run command?  
AWS Systems Manager provides you safe, secure 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. Through integration with [AWS Identity and Access Management (IAM)](https://aws.amazon.com/iam/), you can apply granular permissions to control the actions users can perform on instances. All actions taken with Systems Manager are recorded by [AWS CloudTrail](https://aws.amazon.com/cloudtrail/), allowing you to audit changes throughout your environment.

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.

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.

Q: Can I control who can execute a command?  
Yes. Using the published [AWS Identity and Access Management (IAM)](https://aws.amazon.com/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, but not join an instance to a domain. Another IAM user can only be given access to run a very specific command, like restarting services, giving you the flexibility to specify how much access any given user can have.

## **Patch Manager**

Q: What is AWS Systems Manager patch manager?  
AWS Systems Manager helps you select and deploy operating system and software patches automatically across large groups of Amazon EC2 or on-premises instances. Through patch baselines, you can set rules to auto-approve select categories of patches to be installed, such as operating system or high severity patches, and you can specify a list of patches that override these rules and are automatically approved or rejected. You can also schedule maintenance windows for your patches so that they are only applied during preset times. Systems Manager helps ensure that your software is up-to-date and meets your compliance policies.

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.

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.

Q: What types of patches can I install?  
AWS Systems Manager supports the patching of Windows- and Linux-based instances. Please visit our [documentation](http://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html)to see the versions currently supported.

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 instances. In a patch baseline, you can select patches by the products (e.g., Windows Server 2008, Windows Server 2012, etc.), categories (e.g., critical updates, security updates, etc.), and severities for which you want to review patches for deployment. For each category selected, you can then define a schedule on which the contained patches will be automatically approved for deployment. In addition to the rules, you can also specify a whitelist and blacklist of patches that indicate patches that are to be installed or blocked respectively. At the time of patching, AWS Systems Manager will assess targeted instances for only the patches that have been approved prior to that point in time.

Q: How do I view the compliance levels of my instances?  
You can view patch compliance information, which tells you the detailed results of the patching 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.

## **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.

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.

Q: What tasks can I perform using an AWS Systems Manager maintenance window?  
You can perform tasks like the following:

* Installing applications, updating patches, installing or updating AWS Systems Manager agents, or executing PowerShell commands and Linux shell scripts.
* Building Amazon Machine Images (AMIs), boot-strapping software, and configuring instances.
* Executing [AWS Lambda](https://aws.amazon.com/lambda/) functions that trigger additional actions such as scanning your instances for patch updates.
* Running [AWS Step Function](https://aws.amazon.com/step-functions/) state machines to perform tasks such as removing an instance from an Elastic Load Balancing environment, patching the instance, and then adding the instance back to the Elastic Load Balancing environment.

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](https://aws.amazon.com/step-functions/), or [AWS Lambda](https://aws.amazon.com/lambda/) functions as tasks.

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.

## **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](https://aws.amazon.com/ec2/) or on-premises instances. With Systems Manager, you can control configuration details such as server configurations, anti-virus definitions, firewall settings, and more. You can define configuration policies for your servers through the [AWS Management Console](https://aws.amazon.com/console/) or use existing scripts, PowerShell modules, or Ansible playbooks directly from GitHub or [Amazon S3](https://aws.amazon.com/s3/) buckets. Systems Manager automatically applies your configurations across your instances at a time and frequency that you define. You can query Systems Manager at any time to view the status of your instance configurations, giving you on-demand visibility into your compliance status.

Q: Why should I use AWS Systems Manager state manager?  
Ensuring that the infrastructure that is powering your applications is consistent is a challenge. AWS Systems Manager allows you to create policies, reapply these policies to prevent configuration drift, and monitor the status of your intended state.

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.

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.

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.

## **Parameter Store**

Q: What is AWS Systems Manager parameter store?  
AWS Systems Manager provides a centralized 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 organized 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. Systems Manager is integrated with [AWS Key Management Service (KMS)](https://aws.amazon.com/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)](https://aws.amazon.com/iam/). Parameters can be referenced through other AWS services, such as [Amazon Elastic Container Service](https://aws.amazon.com/ecs/), [AWS Lambda](https://aws.amazon.com/lambda/), and [AWS CloudFormation](https://aws.amazon.com/cloudformation/).

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.

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)](https://aws.amazon.com/kms/) key or your user account default key provided by AWS KMS.

Q: What services can I reference my parameters?  
You can easily reference your parameters across AWS services such as [Amazon Elastic Container Service](https://aws.amazon.com/ecs/), [AWS Lambda](https://aws.amazon.com/lambda/), and AWS Systems Manager, or any service through which you can use the AWS Systems Manager parameter store APIs.

Q: Can I track usage and provide access control to specific parameters?  
Yes. You can provide granular access control through customized permissions to users and resources (such as instances) for parameters access using [AWS Identity and Access Management (IAM)](https://aws.amazon.com/iam/). This means you can control who can access which parameter on what resource. You can also set up [Amazon CloudWatch](https://aws.amazon.com/cloudwatch/) Events rules based on parameter change events. Additionally, you can also track and audit parameter API calls using [AWS CloudTrail](https://aws.amazon.com/cloudtrail/).

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.

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.

Q: Can I receive notifications upon changes to parameter values?  
Yes, you can set up [Amazon CloudWatch](https://aws.amazon.com/cloudwatch/) and [Amazon Simple Notification Service (SNS)](https://aws.amazon.com/sns/) notifications for individual parameter values, and receive notifications upon change.

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 security and compliance requirements by enabling you to rotate secrets automatically. Secrets Manager offers built-in integration for MySQL, PostgreSQL, and Amazon Aurora on Amazon RDS that's extensible to other types of secrets by customizing Lambda functions.

AWS Systems Manager Parameter Store provides secure, hierarchical storage for configuration data management, which can include secrets. Data such as database connection strings, passwords, and license codes can be stored as parameter values and can be audited and access controlled. Values stored can be either plain text or encrypted data. You can then reference values by using the unique name of the parameter. You can reference Systems Manager parameters to build generic configuration and automation scripts for use across AWS services such as Amazon ECS and AWS CloudFormation.

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](https://aws.amazon.com/secrets-manager/pricing/) for pricing details.

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](https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html) on how Parameter Store uses AWS KMS.

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