# MANAGEMENT TOOLS

## AWS ORGANIZATIONS

### AWS ORGANIZATIONS FEATURES

AWS Organizations le ayuda a administrar y gobernar su entorno de forma centralizada a medida que crece y escala sus recursos de AWS.

Las cuentas de AWS son límites naturales para los permisos, la seguridad, los costos y las cargas de trabajo.

El uso de un entorno de varias cuentas es una práctica recomendada al escalar su entorno de nube.

AWS Organizations proporciona muchas características para administrar entornos de varias cuentas, entre las que se incluyen:

* Simplifique la creación de cuentas mediante la creación mediante programación de nuevas cuentas mediante la awsa,dirección de comandos (CLI), SDK o API.
* Agrupar cuentas en unidades organizativas (OU) o grupos de cuentas que sirven a una sola aplicación o servicio.
* Aplicar directivas de etiquetas para clasificar o realizar un seguimiento de los recursos de la organización y proporcionar un control de acceso basado en atributos para usuarios o aplicaciones.
* Delegue la responsabilidad de los servicios de AWS admitidos a las cuentas para que los usuarios puedan administrarlos en nombre de su organización.
* Proporcione de forma centralizada herramientas y acceso para que su equipo de seguridad administre las necesidades de seguridad en nombre de la organización.
* Configurar el inicio de sesión único (SSO) de Amazon para proporcionar acceso a las cuentas y los recursos de AWS mediante active Directory, y personalizar los permisos en función de roles de trabajo independientes.
* Aplique políticas de control de servicios (SCP) a usuarios, cuentas o unidades organizativas para controlar el acceso a los recursos, servicios y regiones de AWS dentro de su organización.
* Comparta recursos de AWS dentro de su organización mediante AWS Resource Allocation Management (RAM).
* Active AWS CloudTrail en todas las cuentas, que crea un registro de toda la actividad en su entorno de nube que las cuentas de miembro no pueden desactivar ni modificar.
* Organizaciones le proporciona una sola factura consolidada.
* Además, puede ver el uso de los recursos en todas las cuentas y realizar un seguimiento de los costos con AWS Cost Explorer y optimizar el uso de los recursos informáticos con AWS Compute Optimizer.

AWS Organizations está disponible para todos los clientes de AWS sin cargo adicional.

La  [API](https://docs.aws.amazon.com/organizations/latest/APIReference/Welcome.html) de [AWS Organizations](https://docs.aws.amazon.com/organizations/latest/APIReference/Welcome.html) permite la automatización para la creación y administración de cuentas. AWS Organizations está disponible en dos conjuntos de características:

* Facturación consolidada.
* Todas las características.

De forma predeterminada, las organizaciones admiten funciones de facturación consolidada. La facturación consolidada separa las cuentas de pago y las cuentas vinculadas.

Puede utilizar AWS Organizations para configurar un único método de pago para todas las cuentas de AWS de su organización mediante facturación consolidada.

Con la facturación consolidada, puede ver una vista combinada de los cargos incurridos por todas sus cuentas.

También puede aprovechar los beneficios de precios del uso agregado, como los descuentos por volumen para Amazon EC2 y Amazon S3.

Límite de 20 cuentas vinculadas para la facturación consolidada (predeterminado). Las directivas se pueden asignar en diferentes puntos de la jerarquía. Puede ayudar con el control de costos a través de descuentos por volumen.

Las instancias EC2 reservadas no utilizadas se aplican en todo el grupo. Las cuentas de pago deben usarse solo para fines de facturación.

Las alertas de facturación se pueden configurar en la cuenta de pago, que muestra la facturación de todas las cuentas vinculadas.

### KEY CONCEPTS

Algunos de los conceptos clave que debe comprender se enumeran aquí:

AWS **Organization:** una organización es una colección de cuentas de AWS que puede organizar en una jerarquía y administrar de forma centralizada.

**Cuenta de** AWS: una cuenta de AWS es un contenedor para sus recursos de AWS.

**Cuenta** de administración: una cuenta de administración es la cuenta de AWS que utiliza para crear su organización.

**Cuenta de** miembro: una cuenta de miembro es una cuenta de AWS, distinta de la cuenta de administración, que forma parte de una organización.

**Raíz administrativa:** una raíz administrativa es el punto de partida para organizar sus cuentas de AWS. La raíz administrativa es el contenedor más alto de la jerarquía de la organización.

**Unidad** organizativa **(OU): una** unidad organizativa (OU) es un grupo de cuentas de AWS dentro de una organización. Una unidad organizativa también puede contener otras unidades organizativas que le permiten crear una jerarquía.

**Política:** una política es un "documento" con una o más instrucciones que definen los controles que desea aplicar a un grupo de cuentas de AWS. AWS Organizations admite un tipo específico de política denominada Política de control de servicios (SCP). Un SCP define las acciones de servicio de AWS, como Amazon EC2 RunInstances, que están disponibles para su uso en diferentes cuentas dentro de una organización.

Prácticas recomendadas para la cuenta de administración:

* [Use the management account only for tasks that require the management account.](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-use)
* [Use a group email address for the management account’s root user.](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_email-address)
* [Use a complex password for the management account’s root user.](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_complex-password)
* [Enable MFA for your root user credentials.](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_mfa)
* [Add a phone number to the account contact information.](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_phone-number)
* [Review and keep track of who has access.](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_review-access)
* [Document the processes for using the root user credentials.](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_document-processes)
* [Apply controls to monitor access to the root user credentials.](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_monitor-access)

### MIGRATING ACCOUNTS BETWEEN ORGANIZATIONS

Las cuentas se pueden migrar entre organizaciones.

Debe tener acceso raíz o de IAM tanto a las cuentas de miembro como a las de administración. Utilice la consola de AWS Organizations para unas pocas cuentas.

Utilice la API de AWS Organizations o la AWS Command Line Interface (AWS CLI) si hay muchas cuentas que migrar.

El historial de facturación y los informes de facturación de todas las cuentas permanecen con la cuenta de administración en un

organización.

Antes de la migración, descargue cualquier historial de facturación o informe de cualquier cuenta de miembro que desee conservar.

Cuando una cuenta de miembro abandona una organización, todos los cargos incurridos por la cuenta se cargan directamente a la cuenta independiente.

Incluso si el movimiento de la cuenta solo tarda un minuto en procesarse, es probable que la cuenta de miembro incurra en algunos cargos.

### SERVICE CONTROL POLICIES (SCPS)

Las directivas de control de servicios (SCP) son un tipo de directiva de organización que puede usar para administrar permisos en su organización.

Los SCP ofrecen un control central sobre el máximo de permisos disponibles para todas las cuentas de su organización. Los SCP le ayudan a garantizar que sus cuentas se mantengan dentro de las directrices de control de acceso de su organización.

Los SCP solo están disponibles en una organización que tiene todas las características habilitadas.

Los SCP no están disponibles si su organización solo ha habilitado las características de facturación consolidada. Los SCP por sí solos no son suficientes para conceder permisos a las cuentas de la organización.

Un SCP no concede permisos. Un SCP define una barandilla, o establece límites, en las acciones que

el administrador de la cuenta puede delegar en los usuarios y roles de IAM en las cuentas afectadas.

El administrador aún debe adjuntar políticas basadas en identidades o en recursos a los usuarios o roles de IAM, o a los recursos de sus cuentas para conceder permisos.

Los permisos efectivos son la intersección lógica entre lo que permite el SCP y lo que permiten las políticas basadas en recursos y IAM.

Herencia SCP:

* Los SCP ***solo afectan a los usuarios y roles de IAM*** administrados por cuentas que forman parte de la organización. Los SCP no afectan directamente a las políticas basadas en recursos. Tampoco afectan a los usuarios o roles de cuentas externas a la organización.
* Un SCP restringe los permisos para los usuarios y roles de IAM en las cuentas de miembro, incluido el usuario raíz de la cuenta de miembro.
* Cualquier cuenta tiene solo los permisos permitidos por ***todos los*** padres por encima de ella.
* Si un permiso está bloqueado en cualquier nivel por encima de la cuenta, ya sea implícitamente (al no estar incluido en una declaración de política Permitir) o explícitamente (al incluirse en una instrucción de política Denegar), un usuario o rol de la cuenta afectada no puede usar ese permiso, incluso si el administrador de la cuenta adjunta la política de IAM AdministratorAccess con permisos \*/\* al usuario.
* Los SCP solo afectan a las cuentas ***de miembros*** de la organización. No tienen ningún efecto sobre los usuarios o roles en la cuenta de administración.
* A los usuarios y roles se les deben seguir concediendo permisos con las políticas de permisos de IAM adecuadas. Un usuario sin políticas de permisos de IAM no tiene acceso, incluso si los SCP aplicables permiten todos los servicios y todas las acciones.
* Si un usuario o rol tiene una política de permisos de IAM que concede acceso a una acción que también permiten los SCP aplicables, el usuario o rol puede realizar esa acción.
* Si un usuario o rol tiene una política de permisos de IAM que concede acceso a una acción que no está permitida o denegada explícitamente por los SCP aplicables, el usuario o rol no puede realizar esa acción.
* Los SCP afectan a todos los usuarios y roles de las cuentas ***adjuntas, incluido el usuario raíz***. Las únicas excepciones son las descritas en [Tareas y entidades no restringidas por SCP.](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html#not-restricted-by-scp)
* Los SCP ***no*** afectan a ningún rol vinculado al servicio. Los roles vinculados a servicios permiten que otros servicios de AWS se integren con AWS Organizations y los SCP no pueden restringirlos.
* Cuando deshabilita el tipo de política SCP en una raíz, todos los SCP se separan automáticamente de todas las entidades de AWS Organizations en esa raíz. Las entidades de AWS Organizations incluyen unidades organizativas, organizaciones y cuentas.
* Si vuelve a habilitar SCP en una raíz, esa raíz se revierte solo a la directiva FullAWSAccess predeterminada que se adjunta automáticamente a todas las entidades de la raíz.
* Los archivos adjuntos de SCP a entidades de AWS Organizations anteriores a que se deshabilitaran los SCP se pierden y no se pueden recuperar automáticamente, aunque puede volver a adjuntarlos manualmente.
* Si hay un límite de permisos (una característica avanzada de IAM) y un SCP, el límite, el SCP y la política basada en identidad deben permitir la acción.

***No puede*** usar SCP para restringir las siguientes tareas:

* Cualquier acción realizada por la cuenta de administración.
* Cualquier acción realizada con permisos asociados a un rol vinculado al servicio.
* Regístrese en el plan de soporte Enterprise como usuario raíz.
* Cambiar el nivel de soporte de AWS como usuario raíz.
* Proporcionar funcionalidad de firmante de confianza para el contenido privado de CloudFront.
* Configurar DNS inverso para un servidor de correo electrónico de Amazon Lightsail como usuario raíz.
* Tareas en algunos servicios relacionados con AWS:
  + Los mejores sitios de Alexa.
  + Servicio de información web de Alexa.
  + Amazon Mechanical Turk.
  + API de marketing de productos de Amazon.

### RESOURCE GROUPS

Puede utilizar grupos de recursos para organizar sus recursos de AWS. En AWS, un recurso es una entidad con la que puede trabajar.

Los grupos de recursos facilitan la administración y automatización de tareas en un gran número de recursos a la vez.

Los grupos de recursos le permiten agrupar recursos y, a continuación, etiquetarlos. El Editor de etiquetas ayuda a encontrar recursos y agregar etiquetas.

###### Puede acceder a los grupos de recursos a través de cualquiera de los siguientes puntos de entrada:

* En la barra de navegación de la consola de administración de AWS.
* En la consola de AWS Systems Manager, en la entrada del panel de navegación izquierdo para grupos de recursos.
* Mediante el uso de la API de grupos de recursos, en comandos de la AWS CLI o lenguajes de programación de AWS SDK.

Un grupo de recursos es una colección de recursos de AWS que se encuentran todos en la misma región de AWS y que coinciden con los criterios proporcionados en una consulta.

En grupos de recursos, hay dos tipos de consultas en las que puede crear un grupo.

Ambos tipos de consulta incluyen recursos que se especifican en el formato AWS::service::resource.

* **Basado en etiquetas:** las consultas basadas en etiquetas incluyen listas de recursos y etiquetas. Las etiquetas son claves que ayudan

identificar y ordenar los recursos dentro de la organización. Opcionalmente, las etiquetas incluyen valores para las claves.

* **Basado en la pila de AWS CloudFormation:** en una consulta basada en la pila de AWS CloudFormation, elija una pila de AWS CloudFormation en su cuenta en la región actual y, a continuación, elija los tipos de recursos dentro de la pila que desea que estén en el grupo. Puede basar su consulta en una sola pila de AWS CloudFormation.

Los grupos de recursos se pueden anidar; Un grupo de recursos puede contener grupos de recursos existentes en la misma región.

## AMAZON CLOUDWATCH

### AMAZON CLOUDWATCH FEATURES

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS.

CloudWatch se utiliza para recopilar y realizar un seguimiento de las métricas, recopilar y supervisar archivos de registro y establecer alarmas. Con CloudWatch puede:

* Obtenga visibilidad en todo el sistema sobre la utilización de recursos.
* Supervisar el rendimiento de las aplicaciones.
* Supervisar el estado operativo.

Las alarmas de CloudWatch supervisan las métricas y se pueden configurar para iniciar acciones automáticamente. CloudWatch Logs centraliza los registros de sistemas, aplicaciones y servicios de AWS.

CloudWatch Events ofrece un flujo de eventos del sistema que describen los cambios en los recursos de AWS.

Diagrama

Descripción generada automáticamente

Se accede a CloudWatch a través de la API, la interfaz de línea de comandos, los SDK de AWS y la consola de administración de AWS.

CloudWatch se integra con AWS IAM.

CloudWatch puede reaccionar automáticamente a los cambios en sus recursos de AWS. Con CloudWatch puede supervisar recursos como:

* EC2 instances.
* DynamoDB tables.
* RDS DB instances.
* Custom metrics generated by applications and services.
* Any log files generated by your applications. CloudWatch conserva los datos de métricas de la siguiente manera:
* Los puntos de datos con un período de menos de 60 segundos están disponibles durante 3 horas. Estos puntos de datos son métricas personalizadas de alta resolución.
* Los puntos de datos con un período de 60 segundos (1 minuto) están disponibles durante 15 días.
* Los puntos de datos con un período de 300 segundos (5 minutos) están disponibles durante 63 días.
* Los puntos de datos con un período de 3600 segundos (1 hora) están disponibles durante 455 días (15 meses).

### AMAZON CLOUDWATCH VS AWS CLOUDTRAIL:

|  |  |
| --- | --- |
| **CloudWatch** | **CloudTrail** |
| Supervisión del rendimiento | Auditoría |
| Registrar eventos en todos los servicios de AWS: piense en las operaciones | Log Actividad de API en todos los servicios de AWS: piense en las actividades o a quién culpar |
| Supervisión integral de alto nivel y servicio de eventos | Más granular de bajo nivel |
| Iniciar sesión desde varias cuentas | Iniciar sesión desde varias cuentas |
| Registros almacenados indefinidamente | Registros almacenados en S3 o CloudWatch indefinidamente |
| Historial de alarmas durante 14 días | Ningún nativo alarmante; puede utilizar alarmas de CloudWatch |

### METRICS

Las métricas son el concepto fundamental en CloudWatch.

Una métrica representa un conjunto de puntos de datos ordenados en el tiempo que se publican en CloudWatch. Los servicios de AWS envían métricas a CloudWatch.

También puede enviar sus propias métricas personalizadas a CloudWatch. Las métricas existen dentro de una región.

Las métricas no se pueden eliminar, pero caducan automáticamente después de 15 meses.

Las métricas se definen de forma única mediante un nombre, un espacio de nombres y cero o más dimensiones.

CloudWatch conserva los datos de métricas de la siguiente manera:

* Los puntos de datos con un período de menos de 60 segundos están disponibles durante 3 horas. Estos puntos de datos son métricas personalizadas de alta resolución.
* Los puntos de datos con un período de 60 segundos (1 minuto) están disponibles durante 15 días.
* Los puntos de datos con un período de 300 segundos (5 minutos) están disponibles durante 63 días.
* Los puntos de datos con un período de 3600 segundos (1 hora) están disponibles durante 455 días (15 meses).

### CUSTOM METRICS

Puede publicar sus propias métricas en CloudWatch mediante la AWS CLI o una API.

Puede ver gráficos estadísticos de las métricas publicadas con la consola de administración de AWS. CloudWatch almacena datos sobre una métrica como una serie de puntos de datos.

Cada punto de datos tiene una marca de tiempo asociada.

Incluso puede publicar un conjunto agregado de puntos de datos llamado conjunto estadístico.

### HIGH-RESOLUTION METRICS

Cada métrica es una de las siguientes:

* Resolución estándar, con datos que tienen una granularidad de un minuto
* Alta resolución, con datos a una granularidad de un segundo Las métricas producidas por los servicios de AWS se resuelven de forma predeterminada de forma estándar.

Al publicar una métrica personalizada, puede definirla como resolución estándar o alta resolución.

Cuando publica una métrica de alta resolución, CloudWatch la almacena con una resolución de 1 segundo y puede leerla y recuperarla con un período de 1 segundo, 5 segundos, 10 segundos, 30 segundos o cualquier múltiplo de 60 segundos.

Las métricas de alta resolución pueden brindarle información más inmediata sobre la actividad de menos de un minuto de su aplicación.

Tenga en cuenta que cada llamada de PutMetricData para una métrica personalizada se cobra, por lo que llamar a PutMetricData con más frecuencia en una métrica de alta resolución puede generar cargos más altos.

Si configura una alarma en una métrica de alta resolución, puede especificar una alarma de alta resolución con un período de 10 segundos o 30 segundos, o puede configurar una alarma regular con un período de cualquier múltiplo de 60 segundos.

Hay una carga más alta para alarmas de alta resolución con un período de 10 o 30 segundos.

### NAMESPACE

Un espacio de nombres es un contenedor para las métricas de CloudWatch.

Las métricas de diferentes espacios de nombres están aisladas entre sí, de modo que las métricas de diferentes aplicaciones no se agregan erróneamente en las mismas estadísticas.

En la tabla siguiente se proporcionan algunos ejemplos de espacios de nombres para varios servicios de AWS:

|  |  |
| --- | --- |
| **Service** | **Namespace** |
| Amazon API Gateway | AWS/ApiGateway |
| Amazon CloudFront | AWS/CloudFront |
| AWS CloudHSM | AWS/CloudHSM |
| Amazon CloudWatch Logs | AWS/Logs |
| AWS CodeBuild | AWS/CodeBuild |
| Amazon Cognito | AWS/Cognito |
| Amazon DynamoDB | AWS/DynamoDB |
| Amazon EC2 | AWS/EC2 |
| AWS Elastic Beanstalk | AWS/ElasticBeanstalk |

### DIMENSIONS

En las métricas personalizadas, el parámetro –dimensions es común.

Una dimensión aclara aún más qué es la métrica y qué datos almacena.

Puede tener hasta 10 dimensiones en una métrica, y cada dimensión está definida por un par de nombres y valores.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

La forma de especificar una dimensión es diferente cuando se utilizan comandos diferentes.

Con [put-metric-data,](https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/put-metric-data.html) se especifica cada dimensión como MyName=MyValue, y con [get-metric-statistics](https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/get-metric-statistics.html)  o [put-metric-alarm](https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/put-metric-alarm.html) se utiliza el formato Name=MyName, Value=MyValue.

Por ejemplo, el siguiente comando publica una métrica Buffers con dos dimensiones denominada InstanceId e InstanceType.

aws cloudwatch put-metric-data --metric-name Buffers --namespace MyNameSpace --unit Bytes -- value 231434333 --dimensions InstanceId=1-23456789,InstanceType=m1.small

Este comando recupera estadísticas para esa misma métrica. Separe las partes Nombre y Valor de una sola dimensión con comas, pero si tiene varias dimensiones, utilice un espacio entre una dimensión y la siguiente.

aws cloudwatch get-metric-statistics --metric-name Buffers --namespace MyNameSpace -- dimensions Name=InstanceId,Value=1-23456789 Name=InstanceType,Value=m1.small --start-time 2016-10-15T04:00:00Z --end-time 2016-10-19T07:00:00Z --statistics Average --period 60

Si una sola métrica incluye varias dimensiones, debe especificar un valor para cada dimensión definida cuando utilice [get-metric-statistics.](https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/get-metric-statistics.html) Por ejemplo, la métrica de Amazon S3 BucketSizeBytes incluye las dimensiones BucketName y StorageType, por lo que debe especificar ambas dimensiones con [get-metric-statistics.](https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/get-metric-statistics.html)

aws cloudwatch get-metric-statistics --metric-name BucketSizeBytes --start-time 2017-01- 23T14:23:00Z --end-time 2017-01-26T19:30:00Z --period 3600 --namespace AWS/S3 --statistics Maximum --dimensions Name=BucketName,Value=MyBucketName Name=StorageType,Value=StandardStorage --output table

#### Publishing Single Data Points

Para publicar un único punto de datos para una métrica nueva o existente, utilice el comando [put-metric-data](https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/put-metric-data.html) con un valor y una marca de tiempo.

Por ejemplo, las siguientes acciones publican cada una un punto de datos.

aws cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService --value 2 -- timestamp 2016-10-20T12:00:00.000Z

aws cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService --value 4 -- timestamp 2016-10-20T12:00:01.000Z

aws cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService --value 5 -- timestamp 2016-10-20T12:00:02.000Z

### STATISTICS

Las estadísticas son agregaciones de datos métricos durante períodos de tiempo específicos.

CloudWatch proporciona estadísticas basadas en los puntos de datos de métrica proporcionados por sus datos personalizados o proporcionados por otros servicios de AWS a CloudWatch.

|  |  |
| --- | --- |
| Statistic | **Description** |
| Mínimo | El valor más bajo observado durante el período especificado. Puede usar este valor para determinar los bajos volúmenes de actividad de la aplicación. |
| Máximo | El valor más alto observado durante el período especificado. Puede utilizar este valor para determinar grandes volúmenes de actividad para la aplicación. |
| Suma | All values submitted for the matching metric added together. This statistic can be useful for determining the total volume of a metric. |
| Average | El valor Sum/SampleCount durante el período específico. Al comparar esta estadística con el Mínimo y el Máximo, puede determinar el alcance completo de una métrica y qué tan cerca está el promedio del Mínimo y el Máximo. Esta comparación le ayuda a saber cuándo aumentar o disminuir sus recursos según sea necesario. |
| SampleCount | El recuento (número) de puntos de datos utilizados para el cálculo estadístico. |
| pNN.NN | Valor del percentil especificado. Puede especificar un percentil utilizando hasta dos decimales (por ejemplo, p45.45). Las estadísticas de percentiles no están disponibles para las métricas que incluyen valores negativos. Para obtener más información, consulte [Percentiles.](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_concepts.html#Percentiles) |

### CLOUDWATCH ALARMS

Puede usar una alarma para iniciar automáticamente acciones en su nombre.

Una alarma observa una sola métrica durante un período de tiempo especificado y realiza una o más acciones especificadas, en función del valor de la métrica en relación con un umbral a lo largo del tiempo.

La acción es una notificación enviada a un tema de Amazon SNS o a una política de Auto Scaling. También puede agregar alarmas a los paneles.

Las alarmas invocan acciones solo para cambios de estado sostenidos.

Las alarmas de CloudWatch no invocan acciones simplemente porque se encuentran en un estado determinado. El estado debe haber cambiado y mantenido durante un número específico de períodos.

### CLOUDWATCH LOGS

Amazon CloudWatch Logs le permite supervisar y solucionar problemas de sus sistemas y aplicaciones utilizando su sistema, aplicación y archivos de registro personalizados existentes.

Puede utilizar Amazon CloudWatch Logs para supervisar, almacenar y obtener acceso a sus archivos de registro desde instancias de Amazon Elastic Compute Cloud (Amazon EC2), AWS CloudTrail, Route 53 y otros orígenes.

Funciones:

* **Monitoree los registros de las instancias Amazon EC2:** supervisa los registros de aplicaciones y sistemas y puede activar notificaciones.
* **Supervisar los eventos registrados de CloudTrail**: se pueden crear alarmas en CloudWatch en función de la actividad de la API capturada por CloudTrail.
* **Retención de** registros: de forma predeterminada, los registros se conservan indefinidamente. Configurable por grupo de registros de 1 día a 10 años.

CloudWatch Logs se puede utilizar para la supervisión de aplicaciones y sistemas en tiempo real, así como para la retención de registros a largo plazo.

Los registros de CloudTrail se pueden enviar a CloudWatch Logs para su supervisión en tiempo real.

Los filtros de métricas de CloudWatch Logs pueden evaluar los registros de CloudTrail para términos, frases o valores específicos.

### CLOUDWATCH LOGS AGENT

El agente de CloudWatch Logs proporciona una forma automatizada de enviar datos de registro a CloudWatch Logs desde instancias Amazon EC2.

Ahora hay un agente de CloudWatch unificado que recopila registros y métricas.

El agente unificado de CloudWatch incluye métricas como la utilización de la memoria y el disco. El agente unificado de CloudWatch le permite hacer lo siguiente:

* Recopile más métricas a nivel de sistema de instancias Amazon EC2 en todos los sistemas operativos. Las métricas pueden incluir métricas in-guest, además de las métricas para instancias EC2.
* Recopile métricas de nivel de sistema de servidores locales. Estos pueden incluir servidores en un entorno híbrido, así como servidores no administrados por AWS.
* Recupere métricas personalizadas de sus aplicaciones o servicios mediante StatsD y los protocolos recopilados.

Diagrama

Descripción generada automáticamente

### CLOUDWATCH EVENTS

Amazon CloudWatch Events ofrece un flujo casi en tiempo real de eventos del sistema que describen los cambios en los recursos de AWS.

Puede utilizar CloudWatch Events para programar acciones automatizadas que se autoactivan en determinados momentos mediante expresiones cron o de velocidad

Puede hacer coincidir eventos y enrutarlos a una o más funciones o secuencias de destino. Los objetivos incluyen:

* Instancias Amazon EC2.
* Funciones de AWS Lambda.
* Transmisiones en Amazon Kinesis Data Streams.
* Flujos de entrega en Amazon Kinesis Data Firehose.
* Grupos de registros en Amazon CloudWatch Logs.
* Amazon ECS tasks.
* Comando de ejecución de Systems Manager.
* Systems Manager Automation.
* AWS Batch jobs.
* Step Functions state machines.
* Pipelines in CodePipeline.
* CodeBuild projects.
* Plantillas de evaluación de Amazon Inspector.
* Amazon SNS topics.
* Amazon SQS queues.

En el ejemplo siguiente, una instancia EC2 cambia de estado (terminada) y el evento se envía a CloudWatch Events, que reenvía el evento al destino (cola SQS).

Interfaz de usuario gráfica

Descripción generada automáticamente

#### Useful API Actions

Es útil comprender las siguientes acciones de la API para el examen Developer Associate. También debe consultar estas y otras acciones de la API en el sitio web de AWS antes de su examen.

GetMetricData

* Recupere hasta 500 métricas diferentes en una sola solicitud. PutMetricData
* Publica puntos de datos de métricas en Amazon CloudWatch.
* CloudWatch asocia los puntos de datos con la métrica especificada.
* Si la métrica especificada no existe, CloudWatch la crea. GetMetricStatistics
* Obtiene estadísticas para la métrica especificada.
* CloudWatch agrega puntos de datos en función de la duración del período que especifique.
* El número máximo de puntos de datos devueltos por una sola llamada es de 1.440. PutMetricAlarm
* Crea o actualiza una alarma y la asocia con la métrica especificada, la expresión matemática métrica o el modelo de detección de anomalías.
* Las alarmas basadas en modelos de detección de anomalías no pueden tener acciones de Auto Scaling.

## AWS CLOUDTRAIL

### AWS CLOUDTRAIL FEATURES

AWS CloudTrail es un servicio web que registra la actividad realizada en su cuenta.

Se puede crear un registro de seguimiento de CloudTrail que entrega archivos de registro a un bucket de Amazon S3. CloudTrail se trata de registrar y guarda un historial de llamadas a la API para su cuenta de AWS.

CloudTrail permite la gobernanza, la conformidad y la auditoría operativa y de riesgos de su cuenta de AWS.

Los eventos incluyen las acciones realizadas en la consola de administración de AWS, la interfaz de línea de comandos de AWS y los SDK y las API de AWS.

CloudTrail proporciona visibilidad de la actividad del usuario mediante el registro de las acciones realizadas en su cuenta. El historial de API permite el análisis de seguridad, el seguimiento de cambios de recursos y la auditoría de cumplimiento. Registra las llamadas a la API realizadas a través de:

* Consola de administración de AWS.
* AWS SDKs.
* Herramientas de línea de comandos.
* Servicios de AWS de nivel superior (como CloudFormation).

CloudTrail registra la actividad de la cuenta y los eventos de servicio de la mayoría de los servicios de AWS y registra los siguientes registros:

* La identidad del llamador de la API.
* La hora de la llamada a la API.
* La dirección IP de origen del llamador de la API.
* Los parámetros de solicitud.
* Los elementos de respuesta devueltos por el servicio de AWS.

CloudTrail está habilitado en su cuenta de AWS cuando lo crea. CloudTrail es por cuenta de AWS.

Puede crear dos tipos de registros de seguimiento para una cuenta de AWS:

* Un registro de seguimiento que se aplica a todas las regiones: registra eventos en todas las regiones y se entrega a un bucket de S3.
* Un registro de seguimiento que se aplica a una sola región: registra eventos en una sola región y se entrega a un bucket de S3. Los rastros individuales adicionales pueden usar el mismo cubo de S3 o uno diferente.

Los registros de seguimiento se pueden configurar para registrar eventos de datos y eventos de administración:

* **Eventos de datos:** estos eventos proporcionan información sobre las operaciones de recursos realizadas en o dentro de un recurso. Estas también se conocen como operaciones de plano de datos.
* **Eventos de** administración: los eventos de administración proporcionan información sobre las operaciones de administración que se realizan en los recursos de su cuenta de AWS. Estas también se conocen como operaciones de plano de control. Los eventos de administración también pueden incluir eventos que no son de API que se producen en su cuenta.

Los eventos de datos de ejemplo incluyen:

* Actividad de API de nivel de objeto de Amazon S3 (por ejemplo, operaciones de API GetObject, DeleteObject y PutObject).
* Actividad de ejecución de funciones de AWS Lambda (la API Invoke).

Ejemplos de eventos de administración incluyen:

* Configuración de la seguridad (por ejemplo, operaciones de la API AttachRolePolicy de IAM).
* Registro de dispositivos (por ejemplo, operaciones de api de Amazon EC2 CreateDefaultVpc).
* Configuración de reglas para el enrutamiento de datos (por ejemplo, operaciones de la API CreateSubnet de Amazon EC2).
* Configuración del registro (por ejemplo, operaciones de la API CreateTrail de AWS CloudTrail).
* Los archivos de registro de CloudTrail se cifran mediante S3 Server Side Encryption (SSE).

También puede habilitar el cifrado mediante SSE KMS para mayor seguridad.

Se puede usar una sola clave KMS para cifrar los archivos de registro de los registros de seguimiento aplicados a todas las regiones. Puede consolidar registros de varias cuentas mediante un bucket de S3:

* 1. Activar CloudTrail en la cuenta de pago.
  2. Crear una política de bucket que permita el acceso entre cuentas.
  3. Active CloudTrail en las otras cuentas y use el bucket en la cuenta de pago.

Puede integrar CloudTrail con CloudWatch Logs para entregar eventos de datos capturados por CloudTrail a un flujo de registros de CloudWatch Logs.

La característica de validación de integridad del archivo de registro de CloudTrail le permite determinar si un archivo de registro de CloudTrail se ha modificado, eliminado o modificado desde que CloudTrail lo entregó al bucket de Amazon S3 especificado.

CloudWatch vs CloudTrail:

|  |  |
| --- | --- |
| **CloudWatch** | **CloudTrail** |
| Performance monitoring | Auditing |
| Log events across AWS services –  think operations | Log API activity across AWS services –  think activities |
| Higher-level comprehensive monitoring and events | More low-level granular |
| Log from multiple accounts | Log from multiple accounts |
| Logs stored indefinitely | Logs stored to S3 or CloudWatch indefinitely |
| Alarms history for 14 days | No native alarming; can use CloudWatch alarms |

## AWS OPSWORKS

### AWS OPSWORKS FEATURES

AWS OpsWorks es un servicio de administración de configuración que proporciona instancias administradas de Chef y Puppet, dos plataformas de automatización muy populares.

Automatiza la forma en que se configuran, implementan y administran las aplicaciones.

Proporcione administración de configuración para implementar código, automatizar tareas, configurar instancias, realizar actualizaciones, etc.

OpsWorks le permite utilizar Chef y Puppet para automatizar la forma en que se configuran, implementan y administran los servidores en sus instancias Amazon EC2 o entornos informáticos locales.

OpsWorks es una plataforma de automatización que transforma la infraestructura en código. OpsWorks consta de pilas y capas:

* Las pilas son colecciones de recursos necesarios para admitir un servicio o aplicación.
* Las pilas son contenedores de recursos (EC2, RDS, etc.) que desea gestionar colectivamente.
* Cada pila contiene una o más capas y las capas automatizan la implementación de paquetes.
* Las pilas se pueden clonar, pero solo dentro de la misma región.
* Las capas representan diferentes componentes de la jerarquía de entrega de aplicaciones.
* Las instancias EC2, las instancias RDS y ELBS son ejemplos de capas.

OpsWorks es un servicio global. Pero cuando crea una pila, debe especificar una región y esa pila solo puede controlar los recursos de esa región.

Hay tres ofertas: OpsWorks para Chef Automate, OpsWorks para Puppet Enterprise y OpsWorks Stacks.

### AWS OPSWORKS FOR CHEF AUTOMATE

* Un servicio de administración de configuración totalmente administrado que aloja Chef Automate, un conjunto de herramientas de automatización de Chef para la administración de la configuración, el cumplimiento y la seguridad, y la implementación continua.
* Completamente compatible con herramientas y libros de cocina de la comunidad de Chef y registra automáticamente nuevos nodos con su servidor de Chef.
* El servidor de Chef almacena recetas y datos de configuración.
* El cliente (nodo) de Chef está instalado en cada servidor.

### AWS OPSWORKS FOR PUPPET ENTERPRISE

* Un servicio de administración de configuración totalmente administrado que aloja Puppet Enterprise, un conjunto de herramientas de automatización de Puppet para **la administración** de **infraestructura y aplicaciones.**

### AWS OPSWORKS STACKS

* Un servicio de administración de aplicaciones y servidores que le permite modelar la aplicación como una pila que contiene diferentes capas, como el equilibrio de carga, la base de datos y el servidor de aplicaciones.
* OpsWorks Stacks es un cliente de creación y uso de AWS y Chef Solo integrado instalado en instancias EC2 para ejecutar recetas de Chef.

OpsWorks Stacks admite instancias EC2 y servidores locales, así como un agente.

## AWS CLOUDFORMATION

### AWS CLOUDFORMATION FEATURES

AWS CloudFormation es un servicio que le permite administrar, configurar y aprovisionar su infraestructura de AWS como código.

AWS CloudFormation proporciona un lenguaje común para que pueda describir y aprovisionar todos los recursos de infraestructura en su entorno de nube.

Los recursos se definen mediante una plantilla de CloudFormation.

CloudFormation interpreta la plantilla y realiza las llamadas a la API adecuadas para crear los recursos que ha definido.

Soporta YAML o JSON.

CloudFormation se puede utilizar para aprovisionar una amplia gama de recursos de AWS. Piense en CloudFormation como la implementación de infraestructura como código.

CloudFormation tiene algunas similitudes con AWS Elastic Beanstalk, aunque también son bastante diferentes, como se detalla en la tabla a continuación.:

|  |  |
| --- | --- |
| **CloudFormation** | **Elastic Beanstalk** |
| “Aprovisionamiento basado en plantillas” | “Aplicaciones web simplificadas" |
| Implementa la infraestructura mediante código | Implementa aplicaciones en EC2(PaaS) |
| Se puede utilizar para implementar casi cualquier servicio de AWS | Implementa aplicaciones web basadas en Java, .NET, PHP, Node.js, Python, Ruby, Go y Docker |
| Utiliza archivos de plantilla JSON o YAML | Utiliza archivos ZIP o WAR |
| Similar a Terraform | Similar a Google App Engine |

### KEY BENEFITS

La infraestructura se aprovisiona de manera consistente, con menos errores (error humano). Menos tiempo y esfuerzo que configurar los recursos manualmente.

Puede utilizar el control de versiones y la revisión por pares para las plantillas de CloudFormation.

Uso gratuito (solo se le cobra por los recursos aprovisionados).

Se puede utilizar para administrar actualizaciones y dependencias.

También se puede usar para revertir y eliminar toda la pila.

### KEY CONCEPTS

En la tabla siguiente se describen los conceptos clave asociados con AWS CloudFormation:

|  |  |
| --- | --- |
| **Component** | **Description** |
| Plantillas | El archivo de texto JSON o YAML que contiene las instrucciones para crear el entorno de AWS |
| Stacks | Todo el entorno descrito por la plantilla y creado, actualizado y eliminado como una sola unidad |
| StackSets | AWS CloudFormation StackSets amplía la funcionalidad de las pilas al permitirle crear, actualizar o eliminar pilas en varias cuentas y regiones con una sola operación. |
| Change Sets | Un resumen de los cambios propuestos en su pila que le permitirá ver cómo esos cambios podrían afectar a sus recursos existentes antes de implementarlos. |
| Templates | El archivo de texto JSON o YAML que contiene las instrucciones para crear el entorno de AWS |

### TEMPLATES

Una plantilla es una plantilla YAML o JSON que se utiliza para describir el estado final de la infraestructura que está aprovisionando o cambiando.

Después de crear la plantilla, debe cargarla en CloudFormation directamente o mediante Amazon S3. CloudFormation lee la plantilla y realiza las llamadas a la API en su nombre.

Los recursos resultantes se denominan "Stack".

Los identificadores lógicos se utilizan para hacer referencia a los recursos dentro de la plantilla.

Los identificadores físicos identifican recursos fuera de las plantillas de AWS CloudFormation, pero solo después de que se hayan creado los recursos.

### STACKS AND STACK SETS

#### Stacks

Recursos implementados basados en plantillas.

Cree, actualice y elimine pilas mediante plantillas. Implementado a través de la consola de administración, la CLI o las API. Errores de creación de pilas:

* La reversión automática del error está habilitada de forma predeterminada.
* Se le cobrará por los recursos aprovisionados incluso si hay un error. Actualización de pilas:
* AWS CloudFormation proporciona dos métodos para actualizar pilas: actualización directa o creación y ejecución de conjuntos de cambios.
* Cuando actualiza directamente una pila, envía los cambios y AWS CloudFormation los implementa inmediatamente.
* Usar actualizaciones directas cuando desee implementar rápidamente las actualizaciones.
* Con los conjuntos de cambios, puede obtener una vista previa de los cambios que AWS CloudFormation realizará en su pila y, a continuación, decidir si desea aplicar esos cambios.

#### Stack Sets

AWS CloudFormation StackSets amplía la funcionalidad de las pilas al permitirle crear, actualizar o eliminar pilas en varias cuentas y regiones con una sola operación.

Con una cuenta de administrador, puede definir y administrar una plantilla de AWS CloudFormation y utilizar la plantilla como base para aprovisionar pilas en cuentas de destino seleccionadas en regiones especificadas.

Una cuenta de administrador es la cuenta de AWS en la que se crean conjuntos de pilas.

Un conjunto de pilas se administra iniciando sesión en la cuenta de administrador de AWS en la que se creó.

Una cuenta de destino es la cuenta en la que crea, actualiza o elimina una o más pilas en su conjunto de pilas.

Antes de poder usar un conjunto de pilas para crear pilas en una cuenta de destino, debe configurar una relación de confianza entre el administrador y las cuentas de destino.

#### Nested Stacks

Las pilas anidadas permiten la reutilización del código de CloudFormation para casos de uso comunes.

Por ejemplo, configuración estándar para un equilibrador de carga, servidor web, servidor de aplicaciones, etc.

En lugar de copiar el código cada vez, cree una plantilla estándar para cada caso de uso común y referencia desde la plantilla de CloudFormation.

### BEST PRACTICES

AWS proporciona "scripts auxiliares" de Python que pueden ayudarle a instalar software e iniciar servicios en sus instancias EC2.

* Utilice CloudFormation para realizar cambios en su entorno en lugar de ir directamente a los recursos.
* Utilice los conjuntos de cambios para identificar posibles puntos problemáticos en sus actualizaciones.
* Usar directivas de pila para proteger explícitamente partes confidenciales de la pila.
* Usa un sistema de control de versiones como CodeCommit o GitHub para realizar un seguimiento de los cambios en las plantillas.

### CHARGES

AWS CloudFormation no tiene ningún cargo adicional.

Usted paga por los recursos de AWS (como instancias Amazon EC2, balanceadores de carga de Elastic Load Balancing, etc.) creados con AWS CloudFormation de la misma manera que si los creara manualmente.

Solo paga por lo que usa, a medida que lo usa; no hay tarifas mínimas ni compromisos iniciales requeridos.

## AWS CONFIG

### AWS CONFIG FEATURES

AWS Config es un servicio totalmente administrado que le proporciona un inventario de recursos de AWS, un historial de configuración y notificaciones de cambios de configuración para habilitar la seguridad y la gobernanza.

Con AWS Config puede descubrir los recursos de AWS existentes, exportar un inventario completo de sus recursos de AWS con todos los detalles de configuración y determinar cómo se configuró un recurso en cualquier momento.

Estas capacidades permiten la auditoría de cumplimiento, el análisis de seguridad, el seguimiento de cambios de recursos y la solución de problemas.

Le permite evaluar, auditar y evaluar las configuraciones de sus recursos de AWS. Muy útil para la gestión de la configuración como parte de un programa ITIL.

Crea una línea base de varios valores de configuración y archivos y, a continuación, puede realizar un seguimiento de las variaciones en relación con

esa línea de base.

### AWS CONFIG VS CLOUDTRAIL

[AWS CloudTrail](https://digitalcloud.training/aws-cloudtrail/) registra la actividad de la API del usuario en su cuenta y le permite obtener acceso a la información sobre esta actividad.

AWS Config registra los detalles de configuración puntuales de sus recursos de AWS como elementos de configuración (CI).

Puede utilizar un CI de AWS Config para responder: "¿Cómo era mi recurso de AWS?" en un momento dado. Puede utilizar AWS CloudTrail para responder: "¿Quién realizó una llamada a la API para modificar este recurso?".

### AWS CONFIG RULES

Una regla de configuración representa las configuraciones deseadas para un recurso y se evalúa con respecto a los cambios de configuración en los recursos relevantes, según lo registrado por AWS Config.

[Las reglas de](https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html) AWS [Config](https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html) pueden comprobar los recursos para determinadas condiciones deseadas y, si se encuentran infracciones, el

los recursos se marcan como "no conformes".

Ejemplos de reglas de configuración:

* Está habilitada la copia de seguridad en [Amazon RDS](https://digitalcloud.training/amazon-rds/)?
* ¿CloudTrail está habilitado en la cuenta de AWS??
* ¿Los volúmenes de [Amazon EBS](https://digitalcloud.training/amazon-ebs/) están cifrados?.

### 

### CONFIGURATION ITEMS

Un [elemento de configuración (CI)](https://docs.aws.amazon.com/config/latest/developerguide/config-item-table.html) es la configuración de un recurso en un momento dado. Un IC consta de 5 secciones:

1. Información básica sobre el recurso que es común en diferentes tipos de recursos (por ejemplo, nombres de recursos de Amazon, etiquetas).
2. Datos de configuración específicos del recurso (por ejemplo, tipo de instancia [Amazon EC2](https://digitalcloud.training/amazon-ec2/)).
3. Mapa de relaciones con otros recursos (por ejemplo, EC2::Volume vol-3434df43 is "attached to instance" EC2 Instance i-3432ee3a).
4. Identificadores de eventos de AWS CloudTrail relacionados con este estado.
5. Metadatos que le ayudan a identificar información sobre el CI, como la versión de este CI, y cuándo se capturó este CI.

### CHARGES

Con AWS Config, se le cobrará en función del número de elementos de configuración (CI) registrados para los recursos admitidos en su cuenta de AWS.

AWS Config crea un elemento de configuración cada vez que detecta un cambio en un tipo de recurso que está grabando.

## AWS SYSTEMS MANAGER

### AWS SYSTEMS MANAGER FEATURES

AWS Systems Manager es un servicio de AWS que proporciona visibilidad y control de la infraestructura en AWS.

AWS Systems Manager proporciona una interfaz unificada a través de la cual puede ver los datos operativos

de varios servicios de AWS.

AWS Systems Manager le permite automatizar las tareas operativas en todos sus recursos de AWS.

Con Systems Manager, puede agrupar recursos, como instancias [amazon EC2](https://digitalcloud.training/amazon-ec2/), buckets de Amazon S3 o instancias de Amazon RDS, por aplicación, ver datos operativos para monitoreo y solución de problemas, y tomar medidas en sus grupos de recursos.

Puede crear grupos lógicos de recursos, como aplicaciones, diferentes capas de una pila de aplicaciones o entornos de producción frente a entornos de desarrollo.

Con Systems Manager, puede seleccionar un grupo de recursos y ver su actividad reciente de API, los cambios en la configuración de recursos, las notificaciones relacionadas, las alertas operativas, el inventario de software y el estado de cumplimiento de parches.

También puede tomar medidas en cada grupo de recursos en función de sus necesidades operativas.

Systems Manager simplifica la administración de recursos y aplicaciones, acorta el tiempo para detectar y resolver problemas operativos y facilita la operación y administración segura de su infraestructura a escala.

### SYSTEMS MANAGER COMPONENTS

#### Systems Manager Inventory

AWS Systems Manager recopila información sobre sus instancias y el software instalado en ellas, lo que le ayuda a comprender las configuraciones del sistema y las aplicaciones instaladas.

Puede recopilar datos sobre aplicaciones, archivos, configuraciones de red, servicios de Windows, registros, roles de servidor, actualizaciones y cualquier otra propiedad del sistema.

Los datos recopilados le permiten administrar los activos de las aplicaciones, realizar un seguimiento de las licencias, supervisar la integridad de los archivos, descubrir aplicaciones no instaladas por un instalador tradicional y mucho más.

#### Configuration Compliance

AWS Systems Manager le permite analizar sus instancias administradas en busca de incoherencias de configuración y conformidad con los parches.

Puede recopilar y agregar datos de varias cuentas y regiones de AWS y, a continuación, profundizar

en recursos específicos que no son compatibles.

De forma predeterminada, AWS Systems Manager muestra datos sobre parches y asociaciones. También puede personalizar el servicio y crear sus propios tipos de cumplimiento en función de sus requisitos.

#### Systems Manager Automation

AWS Systems Manager le permite automatizar de forma segura las operaciones de TI comunes y repetitivas y las tareas de administración en todos los recursos de AWS.

Con Systems Manager, puede crear documentos JSON/YAML que especifiquen una lista específica de tareas o utilizar documentos publicados por la comunidad.

Estos documentos se pueden ejecutar directamente a través de la consola de administración de AWS, las CLI y los SDK, programarse en una ventana de mantenimiento o activarse en función de los cambios en los recursos de AWS.

a través de Amazon CloudWatch Events.

Puede realizar un seguimiento de la ejecución de cada paso en los documentos, así como requerir aprobaciones para cada paso.

También puede implementar cambios de forma incremental y detener automáticamente cuando se producen errores.

#### Systems Manager Run Command

Utilice Systems Manager Run Command para administrar de forma remota y segura la configuración de las instancias administradas a escala. Use Run Command para realizar cambios bajo demanda, como actualizar aplicaciones o ejecutar scripts de shell de Linux y comandos de Windows PowerShell en un conjunto de destino de docenas o cientos de instancias.

El comando Run requiere que el agente de SSM esté instalado en todas las instancias administradas.

Las tareas de ejemplo incluyen: detener, reiniciar, finalizar y cambiar el tamaño de las instancias. Conexión y separación de volúmenes de EBS, creación de instantáneas, etc.

A menudo se utiliza para aplicar parches y actualizaciones.

Los comandos se pueden aplicar a un grupo de sistemas basados en etiquetas de instancia de AWS o selección manual. Los comandos y parámetros se definen en un documento de Systems Manager.

Los comandos se pueden emitir mediante la consola de AWS, la AWS CLI, las herramientas de AWS para Windows PowerShell, la API de Systems Manager o los SDK de Amazon.

#### Systems Manager Session Manager

AWS Systems Manager le proporciona una administración remota segura de sus instancias a escala sin iniciar sesión en sus servidores, lo que reemplaza la necesidad de hosts bastión, SSH o PowerShell remoto.

Proporciona una forma sencilla de automatizar tareas administrativas comunes en grupos de instancias, como ediciones del Registro, administración de usuarios e instalaciones de software y parches.

Proporciona un terminal de comandos para instancias de Linux y un terminal de Windows PowerShell para instancias de Windows.

Mediante la integración con AWS Identity and Access Management (IAM), puede aplicar permisos granulares para controlar las acciones que los usuarios pueden realizar en las instancias.

AWS CloudTrail registra todas las acciones realizadas con Systems Manager, lo que le permite auditar los cambios en todo su entorno.

Requiere permisos de IAM para que la instancia EC2 acceda a SSM, S3 y CloudWatch Logs. CloudTrail puede interceptar eventos StartSession mediante Session Manager.

En comparación con SSH:

* No es necesario abrir el puerto 22.
* No necesita hosts bastión para la administración.
* Todos los comandos se registran en S3 / CloudWatch.
* El acceso seguro al shell se autentica mediante cuentas de usuario de IAM, no con pares de claves.

#### Systems Manager Patch Manager

AWS Systems Manager le ayuda a seleccionar e implementar parches de software y sistemas operativos automáticamente en grandes grupos de instancias amazon ec2 o locales.

A través de las líneas base de parches, puede establecer reglas para aprobar automáticamente determinadas categorías de revisiones que se instalarán, como el sistema operativo o las revisiones de alta gravedad, y puede especificar una lista de revisiones que anulan estas reglas y se aprueban automáticamente. o rechazado.

También puede programar ventanas de mantenimiento para sus parches para que solo se apliquen durante los tiempos preestablecidos.

Systems Manager ayuda a garantizar que su software esté actualizado y cumpla con sus políticas de cumplimiento.

#### Systems Manager Parameter Store

AWS Systems Manager proporciona un almacén centralizado para administrar los datos de configuración, ya sean datos de texto sin formato, como cadenas de bases de datos, o secretos como contraseñas.

Esto le permite separar sus secretos y datos de configuración de su código. Los parámetros se pueden etiquetar y organizar en jerarquías, lo que le ayuda a administrar los parámetros más fácilmente.

Por ejemplo, puede utilizar el mismo nombre de parámetro, "db-string", con una ruta jerárquica diferente, "dev/db-string" o "prod/db-string", para almacenar diferentes valores.

Systems Manager está integrado con AWS Key Management Service (KMS), lo que le permite cifrar automáticamente los datos que almacena.

También puede controlar el acceso de usuarios y recursos a los parámetros mediante AWS Identity and Access Management (IAM). Se puede hacer referencia a los parámetros a través de otros servicios de AWS, como Amazon Elastic Container Service, AWS Lambda y AWS CloudFormation.

#### Distributor

Distribuidor es una característica de AWS Systems Manager que le permite almacenar y distribuir de forma segura paquetes de software en su organización.

Puede utilizar Distributor con características existentes de Systems Manager, como Run Command y State Manager, para controlar el ciclo de vida de los paquetes que se ejecutan en las instancias.

#### State Manager

AWS Systems Manager proporciona administración de la configuración, lo que le ayuda a mantener una configuración coherente de sus instancias Amazon EC2 o locales.

Con Systems Manager, puede controlar los detalles de configuración, como las configuraciones del servidor, las definiciones de antivirus, la configuración del firewall y mucho más.

Puede definir políticas de configuración para sus servidores a través de la consola de administración de AWS o utilizar scripts, módulos de PowerShell o libros de estrategias de Ansible existentes directamente desde los buckets de GitHub o Amazon S3.

Systems Manager aplica automáticamente las configuraciones en todas las instancias en el momento y la frecuencia que defina.

Puede consultar Systems Manager en cualquier momento para ver el estado de las configuraciones de instancia, lo que le proporciona visibilidad bajo demanda de su estado de cumplimiento.

### MAINTENANCE WINDOWS

AWS Systems Manager le permite programar ventanas de tiempo para ejecutar tareas administrativas y de mantenimiento en todas sus instancias.

Esto garantiza que pueda seleccionar un momento conveniente y seguro para instalar parches y actualizaciones o realizar otros cambios de configuración, mejorando la disponibilidad y confiabilidad de sus servicios y aplicaciones.

### 

### DEPLOYMENT AND PROVISIONING

#### Resource Groups

Puede utilizar *grupos de recursos* para organizar sus recursos de AWS. Los grupos de recursos facilitan la administración, supervisión y automatización de tareas en un gran número de recursos a la vez.

Grupos de recursos de AWS proporciona dos métodos generales para definir un grupo de recursos. Ambos métodos implican el uso de una consulta para identificar a los miembros de un grupo.

El primer método se basa en etiquetas aplicadas a los recursos de AWS para agregar recursos a un grupo. Con este método, puede aplicar las mismas etiquetas de par clave/valor a los recursos de varios tipos de su cuenta y, a continuación, utilizar el servicio Grupos de recursos de AWS para crear un grupo basado en ese par de etiquetas.

El segundo método se basa en los recursos disponibles en una pila individual de AWS CloudFormation. Con este método, elija una pila de AWS CloudFormation y, a continuación, elija los tipos de recursos en la pila que desea que estén en el grupo.

Permite la creación de grupos lógicos de recursos en los que se pueden realizar acciones (como la aplicación de revisiones).

Los grupos de recursos tienen un alcance regional.

#### Systems Manager Document

Un documento de AWS Systems Manager (documento de SSM) define las acciones que Systems Manager realiza en las instancias administradas.

Systems Manager incluye más de una docena de documentos preconfigurados que puede utilizar especificando parámetros en tiempo de ejecución.

Los documentos utilizan JavaScript Object Notation (JSON) o YAML, e incluyen pasos y parámetros que especifique.

### MONITORING AND REPORTING

#### Insights Dashboard

AWS Systems Manager agrega y muestra automáticamente los datos operativos de cada grupo de recursos a través de un panel.

Systems Manager elimina la necesidad de navegar a través de varias consolas de AWS para ver sus datos operativos.

Con Systems Manager puede ver los registros de llamadas a la API de [AWS CloudTrail,](https://aws.amazon.com/cloudtrail/)  los cambios en la configuración de recursos de  [AWS Config,](https://aws.amazon.com/config/) el inventario de software y el estado de conformidad de parches por grupo de recursos.

También puede integrar fácilmente sus paneles [de AWS CloudWatch](https://aws.amazon.com/cloudwatch/), [AWS Trusted](https://aws.amazon.com/premiumsupport/trustedadvisor/)

Notificaciones de advisor y alertas de disponibilidad y rendimiento de  [AWS Personal Health Dashboard](https://aws.amazon.com/premiumsupport/phd/) en el panel de Systems Manager.

Systems Manager centraliza todos los datos operativos relevantes, para que pueda tener una visión clara del cumplimiento y el rendimiento de su infraestructura.

#### Amazon CloudWatch

Puede configurar y utilizar el agente de Amazon CloudWatch para recopilar métricas y registros de sus instancias en lugar de utilizar el Agente de SSM para estas tareas. El agente de CloudWatch le permite recopilar más métricas en instancias EC2 de las que están disponibles con el Agente de SSM. Además, puede recopilar métricas de servidores locales mediante el agente de CloudWatch.

### LOGGING AND AUDITING

Systems Manager está integrado con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en Systems Manager. CloudTrail captura todas las llamadas a la API de Systems Manager como eventos, incluidas las llamadas desde la consola de Systems Manager y desde las llamadas de código a las API de Systems Manager.

El Agente de SSM escribe información sobre ejecuciones, comandos, acciones programadas, errores y estados de mantenimiento en los archivos de registro de cada instancia. Puede ver los archivos de registro conectándose manualmente a una instancia o puede enviar registros automáticamente a Amazon CloudWatch Logs.

### AUTHORIZATION AND ACCESS CONTROL

AWS Systems Manager admite [políticas basadas en identidad.](https://docs.aws.amazon.com/systems-manager/latest/userguide/security_iam_service-with-iam.html)

AWS Systems Manager no admite  [políticas basadas en recursos](https://docs.aws.amazon.com/systems-manager/latest/userguide/security-iam.html).

Puede adjuntar etiquetas a los recursos de Systems Manager o pasar etiquetas en una solicitud a Systems Manager.

Para controlar el acceso en función de las etiquetas, proporcione información de la etiqueta en el elemento condition de una política mediante las claves de condición ssm:resourceTag/key-name, aws:ResourceTag/key-name, aws:RequestTag/key-name o aws:TagKeys.

## AWS COST MANAGEMENT SERVICES

### AWS COST EXPLORER

AWS Cost Explorer es una herramienta gratuita que le permite ver gráficos de sus costos.

Puede ver los datos de costos de los últimos 13 meses y pronosticar cuánto es probable que gaste en los próximos tres meses.

El Explorador de costos se puede utilizar para descubrir patrones en cuánto gasta en recursos de AWS a lo largo del tiempo e identificar áreas problemáticas de costos.

Cost Explorer puede ayudarle a identificar estadísticas de uso del servicio, como:

* Qué servicios utilizas más.
* Ver métricas para las que AZ tiene más tráfico.
* Qué cuenta vinculada se utiliza más.

### AWS COST & USAGE REPORT

Publique informes de facturación de AWS en un bucket de Amazon S3.

Los informes desglosan los costos por:

* Hora, día, mes, producto, recurso del producto, etiquetas.

Puede actualizar el informe hasta tres veces al día.

Cree, recupere y elimine sus informes mediante la AWS CUR API Reference.

### AWS PRICE LIST API

Consulte los precios de los servicios de AWS.

API de servicio de lista de precios (también conocida como API de consulta): consulta con JSON. API de lista de precios de AWS (también conocida como API masiva): consulta con HTML. Alertas a través de Amazon SNS cuando cambian los precios.

### AWS BUDGETS

Se utiliza para realizar un seguimiento del costo, el uso o la cobertura y utilización de sus instancias reservadas y planes de ahorro, en múltiples dimensiones, como el servicio o las categorías de costos.

Alertas a través de notificaciones de alertas basadas en eventos para saber cuándo se encuentra el costo o el uso real o previsto

exceda su límite de presupuesto, o cuando la cobertura o utilización de su RI y Planes de Ahorro caiga por debajo

su umbral.

Cree presupuestos anuales, trimestrales, mensuales o incluso diarios dependiendo de las necesidades de su negocio.

## AWS BACKUP

### AWS BACKUP FEATURES

AWS Backup proporciona protección de datos centralizada y automatizada. Funciona en todos los servicios de AWS y cargas de trabajo híbridas.

Ayuda a respaldar el cumplimiento normativo y las políticas empresariales para la protección de datos. Se integra con AWS Organizations para la implementación centralizada de políticas de protección de datos. Configure, administre y controle las actividades de copia de seguridad en todas las cuentas y recursos de AWS. AWS Backup puede proteger muchos recursos de AWS, incluidos:

* Amazon EC2 instances.
* Amazon EBS volumes.
* Amazon RDS databases.
* Amazon DynamoDB tables.
* Amazon Neptune databases.
* Amazon DocumentDB databases.
* Amazon EFS file systems.
* Amazon FSx for Lustre and Windows File Server file systems.
* AWS Storage Gateway volumes.
* VMware workloads on-premises and in VMware Cloud on AWS.
* Amazon S3 buckets.

AWS Backup se puede utilizar para copiar copias de seguridad en varios servicios de AWS en diferentes regiones. Las copias de seguridad entre regiones se pueden implementar de forma manual o automática mediante la programación.

La copia de seguridad entre cuentas también se puede configurar para cuentas dentro de una organización de AWS.

### POLICY-BASED BACKUP

Con AWS Backup, puede crear políticas de copia de seguridad denominadas planes de copia de seguridad. Los planes de copia de seguridad se utilizan para definir los requisitos de copia de seguridad.

A continuación, los planes de copia de seguridad se aplican a los recursos de AWS de los que desea realizar una copia de seguridad.

Puede crear planes de copia de seguridad independientes que cumplan con los requisitos específicos de cumplimiento normativo y empresarial.

Los planes de copia de seguridad facilitan la implementación de su estrategia de copia de seguridad en toda la organización y en todas sus aplicaciones.

### TAG-BASED BACKUP POLICIES

AWS Backup le permite aplicar planes de copia de seguridad a sus recursos de AWS simplemente etiquetándolos. Asegúrese de que todos sus recursos de AWS estén respaldados y protegidos de acuerdo con su estrategia. Las etiquetas de AWS son una excelente manera de organizar y clasificar sus recursos de AWS.

La integración con las etiquetas de AWS le permite aplicar rápidamente un plan de copia de seguridad a un grupo de recursos de AWS para que se realice una copia de seguridad de manera coherente y conforme.

### AUTOMATED BACKUP SCHEDULING

AWS Backup le permite crear programaciones de copia de seguridad que puede personalizar para cumplir con los requisitos de copia de seguridad normativos y empresariales.

También puede elegir entre programaciones de copia de seguridad predefinidas basadas en prácticas recomendadas comunes.

AWS Backup realizará automáticamente una copia de seguridad de sus recursos de AWS de acuerdo con las políticas y programaciones que defina.

Una programación de copia de seguridad incluye la hora de inicio de la copia de seguridad, la frecuencia de la copia de seguridad y la ventana de copia de seguridad.

### AUTOMATED RETENTION MANAGEMENT

Puede configurar políticas de retención de copias de seguridad que retengan y expiren automáticamente las copias de seguridad de acuerdo con los requisitos de cumplimiento normativo y empresarial.

La administración automatizada de la retención de backup minimiza los costos de almacenamiento de backup al retener los backups solo si son necesarios.

### AWS BACKUP VAULT LOCK

AWS Backup Vault Lock le permite proteger sus copias de seguridad de la eliminación o los cambios en su ciclo de vida mediante cambios inadvertidos o malintencionados.

Puede utilizar la AWS CLI, la API de AWS Backup o el SDK de AWS Backup para aplicar la protección aws Backup Vault Lock a un almacén existente o a uno nuevo.

## MANAGEMENT TOOLS QUIZ QUESTIONS

Answers and explanations are provided below after the last question in this section.

###### Question 1:

You are a Solutions Architect at Digital Cloud Training. A client from a large multinational corporation is working on a deployment of a significant amount of resources into AWS. The client would like to be able to deploy resources across multiple AWS accounts and regions using a single toolset and template. You have been asked to suggest a toolset that can provide this functionality?

1. Use a CloudFormation template that creates a stack and specify the logical IDs of each account and region
2. Use a CloudFormation StackSet and specify the target accounts and regions in which the stacks will be created
3. Use a third-party product such as Terraform that has support for multiple AWS accounts and regions
4. This cannot be done, use separate CloudFormation templates per AWS account and region

###### Question 2:

A Solutions Architect needs to monitor application logs and receive a notification whenever a specific number of occurrences of certain HTTP status code errors occur. Which tool should the Architect use?

1. CloudWatch Events
2. CloudWatch Logs
3. CloudTrail Trails
4. CloudWatch Metrics

###### Question 3:

A Solutions Architect is designing the system monitoring and deployment layers of a serverless application. The system monitoring layer will manage system visibility through recording logs and metrics and the deployment layer will deploy the application stack and manage workload changes through a release management process.

The Architect needs to select the most appropriate AWS services for these functions. Which services and frameworks should be used for the system monitoring and deployment layers? (choose 2)

1. Use AWS X-Ray to package, test, and deploy the serverless application stack
2. Use Amazon CloudTrail for consolidating system and application logs and monitoring custom metrics
3. Use AWS Lambda to package, test, and deploy the serverless application stack
4. Use AWS SAM to package, test, and deploy the serverless application stack
5. Use Amazon CloudWatch for consolidating system and application logs and monitoring custom metrics

###### Question 4:

A systems integration consultancy regularly deploys and manages multi-tiered web services for customers on AWS. The SysOps team are facing challenges in tracking changes that are made to the web services and rolling back when problems occur.

Which of the approaches below would BEST assist the SysOps team?

1. Use AWS Systems Manager to manage all updates to the web services
2. Use CodeDeploy to manage version control for the web services
3. Use Trusted Advisor to record updates made to the web services
4. Use CloudFormation templates to deploy and manage the web services

###### Question 5:

An event in CloudTrail is the record of an activity in an AWS account. What are the two types of events that can be logged in CloudTrail? (choose 2)

1. System Events which are also known as instance level operations
2. Management Events which are also known as control plane operations
3. Platform Events which are also known as hardware level operations
4. Data Events which are also known as data plane operations
5. API events which are also known as CloudWatch events

###### Question 6:

Your company currently uses Puppet Enterprise for infrastructure and application management. You are looking to move some of your infrastructure onto AWS and would like to continue to use the same tools in the cloud. What AWS service provides a fully managed configuration management service that is compatible with Puppet Enterprise?

1. Elastic Beanstalk
2. CloudFormation
3. OpsWorks
4. CloudTrail

###### Question 7:

The operations team in your company are looking for a method to automatically respond to failed system status check alarms that are being received from an EC2 instance. The system in question is experiencing intermittent problems with its operating system software.

Which two steps will help you to automate the resolution of the operating system software issues? (choose 2)

1. Create a CloudWatch alarm that monitors the “StatusCheckFailed\_System” metric
2. Create a CloudWatch alarm that monitors the “StatusCheckFailed\_Instance” metric
3. Configure an EC2 action that recovers the instance
4. Configure an EC2 action that terminates the instance
5. Configure an EC2 action that reboots the instance

### MANAGEMENT TOOLS - ANSWERS

###### Question 1 answer: B

Explanation:

AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation.

Using an administrator account, you define and manage an AWS CloudFormation template, and use the template as the basis for provisioning stacks into selected target accounts across specified regions. An administrator account is the AWS account in which you create stack sets.

A stack set is managed by signing in to the AWS administrator account in which it was created. A target account is the account into which you create, update, or delete one or more stacks in your stack set.

Before you can use a stack set to create stacks in a target account, you must set up a trust relationship between the administrator and target accounts.

A regular CloudFormation template cannot be used across regions and accounts. You would need to create copies of the template and then manage updates.

You do not need to use a third-party product such as Terraform as this functionality can be delivered through native AWS technology.

###### Question 2 answer: B

Explanation:

You can use **CloudWatch Logs** to monitor applications and systems using log data. For example, CloudWatch Logs can track the number of errors that occur in your application logs and send you a notification whenever the rate of errors exceeds a threshold you specify. This is the best tool for this requirement.

**Amazon CloudWatch Events** delivers a near real-time stream of system events that describe changes in Amazon Web Services (AWS) resources. Though you can generate custom application-level events and publish them to CloudWatch Events this is not the best tool for monitoring application logs.

**CloudTrail** is used for monitoring API activity on your account, not for monitoring application logs.

**CloudWatch Metrics** are the fundamental concept in CloudWatch. A metric represents a time- ordered set of data points that are published to CloudWatch. You cannot use a metric alone; it is used when setting up monitoring for any service in CloudWatch.

###### Question 3 answer: D,E

Explanation:

AWS Serverless Application Model (AWS SAM) is an extension of AWS CloudFormation that is used to package, test, and deploy serverless applications.

With Amazon CloudWatch, you can access system metrics on all the AWS services you use, consolidate system and application level logs, and create business key performance indicators (KPIs) as custom metrics for your specific needs.

AWS Lambda is used for executing your code as functions, it is not used for packaging, testing and deployment. AWS Lambda is used with AWS SAM.

AWS X-Ray lets you analyze and debug serverless applications by providing distributed tracing and service maps to easily identify performance bottlenecks by visualizing a request end-to-end.

###### Question 4 answer: D

Explanation:

When you provision your infrastructure with AWS CloudFormation, the AWS CloudFormation template describes exactly what resources are provisioned and their settings. Because these templates are text files, you simply track differences in your templates to track changes to your infrastructure, similar to the way developers control revisions to source code. For example, you can use a version control system with your templates so that you know exactly what changes were made, who made them, and when. If at any point you need to reverse changes to your infrastructure, you can use a previous version of your template.

AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. However, CloudFormation would be the preferred method of maintaining the state of the overall architecture.

AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, or serverless Lambda function.

AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.

###### Question 5 answer: B,D

Explanation:

Trails can be configured to log Data events and Management events:

* **Data events:** These events provide insight into the resource operations performed on or within a resource. These are also known as data plane operations
* **Management events:** Management events provide insight into management operations that are performed on resources in your AWS account. These are also known as control plane operations. Management events can also include non-API events that occur in your account

###### Question 6 answer: C

Explanation:

The only service that would allow you to continue to use the same tools is OpsWorks. AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.

###### Question 7 answer: B,E

Explanation:

EC2 status checks are performed every minute and each returns a pass or a fail status. If all checks pass, the overall status of the instance is OK. If one or more checks fail, the overall status is impaired.

**System status checks** detect (StatusCheckFailed\_System) problems with your instance that require AWS involvement to repair whereas **Instance status checks** (StatusCheckFailed\_Instance) detect problems that require your involvement to repair.

The action to *recover* the instance is only supported on specific instance types and can be used

only with StatusCheckFailed\_System.

Configuring an action to terminate the instance would not help resolve system software issues as the instance would be terminated.