# SECURITY, IDENTITY & COMPLIANCE

## AWS IAM

### AWS IAM FEATURES

IAM es el servicio de administración de acceso e identidad de AWS.

IAM se utiliza para controlar de forma segura el acceso individual y grupal a los recursos de AWS. IAM facilita el acceso seguro de varios usuarios a los recursos de AWS. IAM se puede utilizar para gestionar:

* Users.
* Groups.
* Access policies.
* Roles.
* User credentials.
* User password policies.
* Multi-factor authentication (MFA).

1. API keys for programmatic access (CLI). Proporciona un control centralizado de su cuenta de AWS. Habilita el acceso compartido a su cuenta de AWS.

De forma predeterminada, se crean nuevos usuarios sin acceso a ningún servicio de AWS: solo pueden iniciar sesión en la consola de AWS.

El permiso debe concederse explícitamente para permitir que un usuario obtenga acceso a un servicio de AWS. Los usuarios de IAM son personas a las que se les ha concedido acceso a una cuenta de AWS. Cada usuario de IAM tiene tres componentes principales:

* A username.
* A password.

1. Permissions to access various resources. Puede aplicar permisos granulares con IAM.

Puede asignar a los usuarios credenciales de seguridad individuales, como claves de acceso, contraseñas y dispositivos de autenticación multifactor.

IAM no se utiliza para la autenticación a nivel de aplicación.

Federación de identidad (incluyendo AD, Facebook, etc.). se puede configurar permitiendo el acceso seguro a los recursos de una cuenta de AWS sin necesidad de crear una cuenta de usuario de IAM.

La autenticación multifactor (MFA) se puede habilitar/aplicar para la cuenta de AWS y para los usuarios individuales de la cuenta.

MFA utiliza un dispositivo de autenticación que genera continuamente códigos de autenticación aleatorios, de seis dígitos y de un solo uso.

Puede autenticarse mediante un dispositivo MFA de las tres maneras siguientes:

* A través de la **consola de administración de AWS,** se solicita al usuario un nombre de usuario, una contraseña y un código de autenticación.
* Uso de la **API de AWS**: se agregan restricciones a las políticas de IAM y los desarrolladores pueden solicitar credenciales de seguridad temporales y pasar parámetros MFA en sus solicitudes de API de AWS STS.
* Uso de la **AWS CLI** mediante la obtención de credenciales de seguridad temporales de STS (aws sts get- session-token).

¿Quieres ver cómo configurar MFA? En el breve tutorial en vídeo de AWS Hands-on Labs que se muestra a continuación, aprenderá a activar una autenticación multifactor (MFA) virtual para su cuenta raíz de AWS. En menos de 5 minutos, cubrimos: Eliminación de la clave de acceso de la cuenta raíz y Activación de la autenticación multifactor.

Es una práctica recomendada usar MFA para todos los usuarios y usar dispositivos U2F o MFA de hardware para todos los usuarios privilegiados.

IAM es universal (global) y no se aplica a las regiones. IAM es eventualmente consistente.

IAM replica datos en varios centros de datos de todo el mundo.

La "cuenta raíz" es la cuenta creada al configurar la cuenta de AWS. Tiene completo

Acceso de administrador y es la única cuenta que tiene este acceso de forma predeterminada.

Es una práctica recomendada no usar la cuenta raíz para nada que no sea la facturación.

El acceso de usuario avanzado permite todos los permisos, excepto la administración de grupos y usuarios en IAM.

Las credenciales de seguridad temporales consisten en el ID de clave de acceso de AWS, la clave de acceso secreta y el token de seguridad.

IAM puede asignar credenciales de seguridad temporales para proporcionar a los usuarios acceso temporal a servicios o recursos.

Para iniciar sesión, debe proporcionar su ID de cuenta o alias de cuenta, además de un nombre de usuario y una contraseña.

La URL de inicio de sesión incluye el ID de cuenta o el alias de la cuenta, por ejemplo: https:// My\_AWS\_Account\_ID.signin.aws.amazon.com/console/.

Alternativamente, puede iniciar sesión en la siguiente URL e ingresar su ID de cuenta o alias manualmente: https://console.aws.amazon.com/.

IAM se integra con muchos servicios de AWS diferentes. IAM es compatible con el cumplimiento de PCI DSS.

AWS recomienda utilizar los SDK de AWS para realizar llamadas de API programáticas a IAM. Sin embargo, también puede utilizar la API de consulta de IAM para realizar llamadas directas al servicio web de IAM.

### IAM ELEMENTS

Principals:

* Una entidad que puede realizar una acción en un recurso de AWS.
* El usuario administrativo de IAM es su primer principal.
* Puede permitir que los usuarios y los servicios asuman un rol.
* IAM admite usuarios federados.
* IAM admite el acceso mediante programación para permitir que una aplicación obtenga acceso a su cuenta de AWS.
* Los usuarios, roles, usuarios federados y aplicaciones de IAM son todos entidades de seguridad de AWS. Requests:
* Los directores de seguridad envían solicitudes a través de la consola, la CLI, los SDK o las API.
* Las solicitudes son:
  + Acciones (u operaciones) que el principal desea realizar.
  + Recursos sobre los que se realizan las acciones.
  + Información principal, incluido el entorno desde el que se realizó la solicitud.
* Contexto de la solicitud: AWS recopila la información de la solicitud:
  + Principal (requester).
  + Agregar permisos asociados a la entidad de seguridad.
  + Datos del entorno, como la dirección IP, el agente de usuario, el estado SSL, etc.
  + Datos de recursos o datos relacionados con el recurso que se solicita Authentication:
* Una entidad de seguridad que envía una solicitud debe estar autenticada para enviar una solicitud a AWS.
* Para autenticarse desde la consola, debe iniciar sesión con su nombre de usuario y contraseña.
* Para autenticarse desde la API o la CLI, debe proporcionar la clave de acceso y la clave secreta.

Authorization:

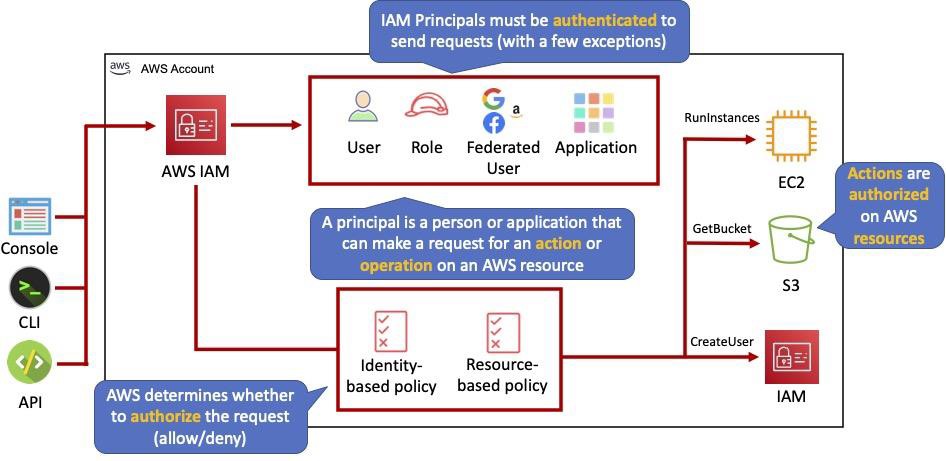
* IAM utiliza valores del contexto de la solicitud para comprobar si hay políticas coincidentes y determina si se debe permitir o denegar la solicitud.
* Las políticas de IAM se almacenan en IAM como documentos JSON y especifican los permisos permitidos o denegados.
* Las políticas de IAM pueden ser:
  + Directivas basadas en usuario (identidad).
  + Políticas basadas en recursos.
* IAM comprueba cada política que coincide con el contexto de su solicitud.
* Si una sola política tiene una acción de denegación, IAM deniega la solicitud y deja de evaluar (denegación explícita).
* Lógica de evaluación:
  + De forma predeterminada, todas las solicitudes se deniegan (denegación implícita).
  + Una autorización explícita anula la denegación implícita.
  + Una denegación explícita anula cualquier permiso explícito.
* Solo el usuario raíz tiene acceso a todos los recursos de la cuenta de forma predeterminada.

Acciones:

* Las acciones son definidas por un servicio.
* Las acciones son las cosas que puede hacer a un recurso, como ver, crear, editar, eliminar.
* Cualquier acción sobre recursos que no esté explícitamente permitida se deniega.
* Para permitir que una entidad de seguridad realice una acción, debe incluir las acciones necesarias en una directiva que se aplique a la entidad de seguridad o al recurso afectado.

Recursos:

* Un recurso es una entidad que existe dentro de un servicio.
* Por ejemplo, instancias EC2, buckets de S3, usuarios de IAM y tablas de DynamoDB.
* Cada servicio de AWS define un conjunto de acciones que se pueden realizar en el recurso.
* Después de que AWS apruebe las acciones de su solicitud, esas acciones se pueden realizar en los recursos relacionados de su cuenta.



### AUTHENTICATION METHODS

Contraseña de la consola:

* Una contraseña que el usuario puede introducir para iniciar sesión en sesiones interactivas, como la consola de administración de AWS.
* Puede permitir que los usuarios cambien sus propias contraseñas.
* Puede permitir que los usuarios de IAM seleccionados cambien sus contraseñas deshabilitando la opción para todos los usuarios y utilizando una política de IAM para conceder permisos a los usuarios seleccionados.

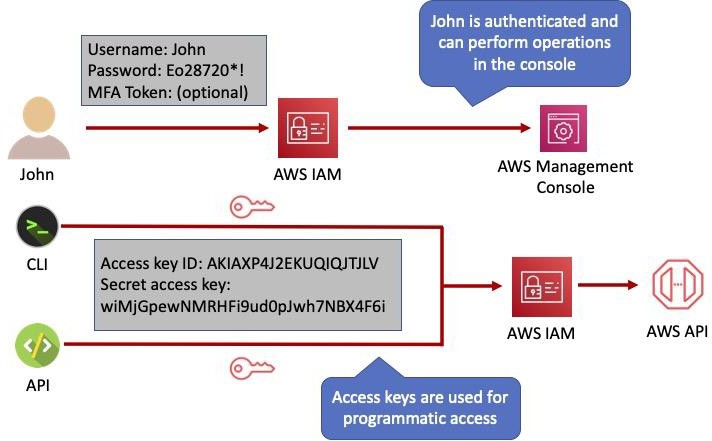
Access Keys:

* Una combinación de un ID de clave de acceso y una clave de acceso secreta.
* Puede asignar dos claves de acceso activas a un usuario a la vez.
* Estos se pueden utilizar para realizar llamadas programáticas a AWS cuando se utiliza la API en el código del programa o en un símbolo del sistema cuando se utiliza la AWS CLI o las herramientas de AWS PowerShell.
* Puede crear, modificar, ver o rotar claves de acceso.
* Cuando se crea, IAM devuelve el ID de clave de acceso y la clave de acceso secreta.
* The secret access is returned only at creation time and if lost a new key must be created.
* Asegúrese de que las claves de acceso y las claves de acceso secretas se almacenen de forma segura.
* Los usuarios pueden tener acceso para cambiar sus propias claves a través de la política de IAM (no desde la consola).
* Puede deshabilitar la clave de acceso de un usuario que impide que se use para llamadas a la API.

Certificados de servidor:

* Certificados SSL/TLS que puede utilizar para autenticarse con algunos servicios de AWS.
* AWS recomienda utilizar AWS Certificate Manager (ACM) para aprovisionar, administrar e implementar los certificados de servidor.
* Usar IAM solo cuando deba admitir conexiones HTTPS en una región que no sea compatible con ACM.

El siguiente diagrama muestra los diferentes métodos de autenticación disponibles con IAM:



### IAM USERS

Un usuario de IAM es una entidad que representa a una persona o servicio. Se puede asignar:

* Un ID de clave de acceso y una clave de acceso secreta para el acceso mediante programación a la API de AWS, la CLI, el SDK y otras herramientas de desarrollo.
* Una contraseña para acceder a la consola de administración.

De forma predeterminada, los usuarios no pueden acceder a nada de su cuenta.

Las credenciales de usuario raíz de la cuenta son la dirección de correo electrónico utilizada para crear la cuenta y una contraseña.

La cuenta raíz tiene permisos administrativos completos y estos no se pueden restringir. Prácticas recomendadas para cuentas raíz:

* No uses las credenciales de usuario raíz.
* No compartir las credenciales de usuario raíz.
* Crear un usuario de IAM y asignar permisos administrativos según sea necesario.
* Habilitar MFA.

Los usuarios de IAM se pueden crear para representar aplicaciones, y estas se conocen como "cuentas de servicio".

Puede tener hasta 5000 usuarios por cuenta de AWS.

Cada cuenta de usuario tiene un nombre descriptivo y un ARN que identifica de forma única al usuario en AWS.

También se crea un ID único que se devuelve solo cuando se crea el usuario mediante la API, Herramientas para Windows PowerShell o la AWS CLI.

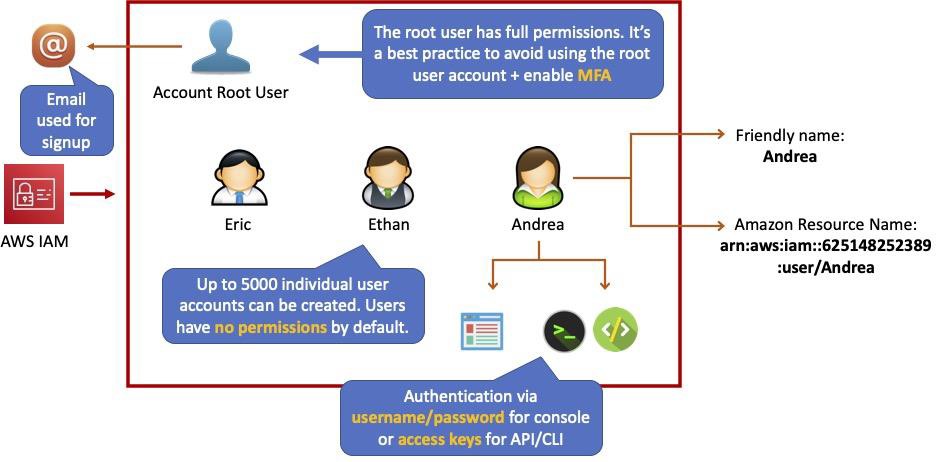
Debe crear cuentas de IAM individuales para los usuarios (práctica recomendada para no compartir cuentas).

El ID de clave de acceso y la clave de acceso secreta no son lo mismo que una contraseña y no se pueden utilizar para iniciar sesión en la consola de AWS.

El ID de clave de acceso y la clave de acceso secreta solo se pueden generar una vez y deben regenerarse si se pierden.

Se puede definir una política de contraseñas para hacer cumplir la longitud, la complejidad de la contraseña, etc. (se aplica a todos los usuarios).

Puede permitir o no permitir la posibilidad de cambiar contraseñas mediante una política de IAM. Las claves de acceso y las contraseñas deben cambiarse regularmente.

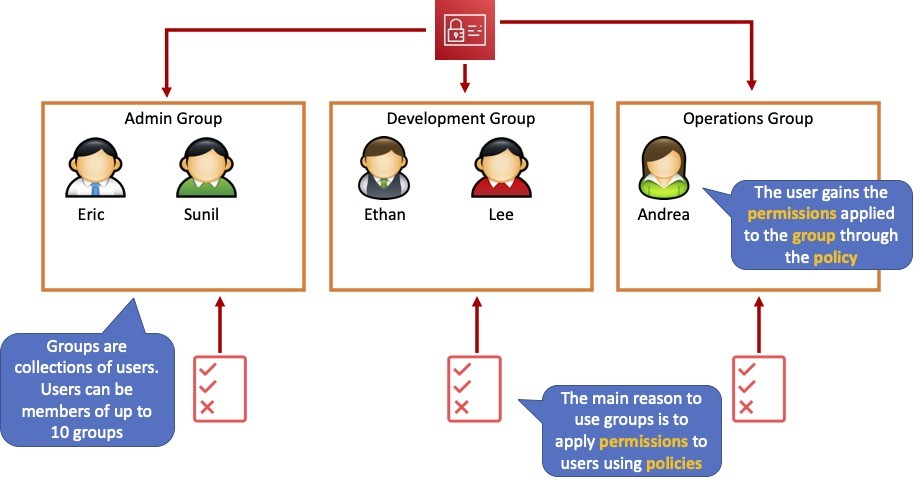


### GROUPS

Los grupos son colecciones de usuarios y tienen directivas adjuntas a ellos.

Un grupo no es una identidad y no se puede identificar como entidad de seguridad en una política de IAM. Utilice grupos para asignar permisos a los usuarios.

Utilice la entidad de seguridad con privilegios mínimos al asignar permisos. No se pueden anidar grupos (grupos dentro de grupos).



### ROLES

Los roles se crean y luego son "asumidos" por entidades de confianza y definen un conjunto de permisos para

realizar solicitudes de servicio de AWS.

Con IAM Roles puede delegar permisos a recursos para usuarios y servicios sin utilizar credenciales permanentes (por ejemplo, nombre de usuario y contraseña).

Los usuarios de IAM o los servicios de AWS pueden asumir un rol para obtener credenciales de seguridad temporales que se pueden utilizar para realizar llamadas a la API de AWS.

Puede delegar mediante roles.

No hay credenciales asociadas a un rol (contraseña o claves de acceso).

Los usuarios de IAM pueden asumir temporalmente un rol para asumir permisos para una tarea específica.

Se puede asignar un rol a un usuario federado que inicie sesión con un proveedor de identidades externo. Las credenciales temporales se utilizan principalmente con roles de IAM y caducan automáticamente.

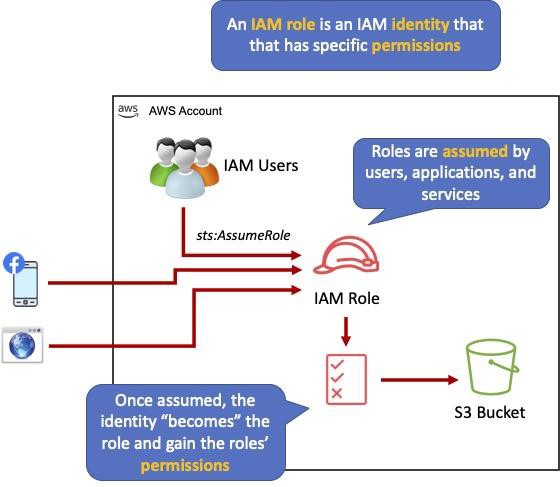
Los roles se pueden asumir temporalmente a través de la consola o mediante programación con la **AWS CLI**, **Las herramientas para Windows PowerShell** o **la API.**

Roles de IAM con instancias EC2:

* Los roles de IAM se pueden utilizar para conceder permisos a las aplicaciones que se ejecutan en instancias EC2 para las solicitudes de API de AWS mediante perfiles de instancia.
* Solo se puede asignar un rol a una instancia EC2 a la vez.
* Se puede asignar un rol en el momento decreación de la **instancia EC2** o **en cualquier momento posterior.**
* Al utilizar la AWS CLI o la instancia de API, los perfiles deben crearse manualmente (es automático y transparente a través de la consola).
* Las aplicaciones recuperan credenciales de seguridad temporales de los metadatos de la instancia.

Delegación de roles:

* Crear un rol de IAM con dos políticas:
  + Directiva de permisos: concede al usuario del rol los permisos necesarios en un recurso.
  + Directiva de confianza: especifica las cuentas de confianza a las que se les permite asumir el rol.
* Los caracteres comodín (\*) no se pueden especificar como entidad de seguridad.
* También se debe adjuntar una directiva de permisos al usuario de la cuenta de confianza.



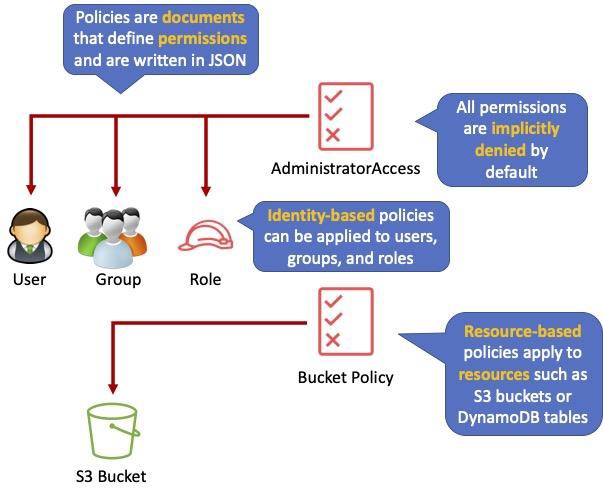
### POLICIES

Las directivas son documentos que definen permisos y se pueden aplicar a usuarios, grupos y roles. Los documentos de directiva se escriben en JSON (par de valores clave que consta de un atributo y un valor). Todos los permisos se deniegan implícitamente de forma predeterminada.

Se aplica la política más restrictiva.

El simulador de políticas de IAM es una herramienta que le ayuda a comprender, probar y validar los efectos de las políticas de control de acceso.

El elemento Condition se puede utilizar para aplicar más lógica condicional.



### INLINE POLICIES VS MANAGED POLICIES

Hay 3 tipos de políticas:

* Managed policies.
* Customer managed policies.
* Inline policies. Managed Policy:
* Creado y administrado por AWS.
* Se utiliza para casos de uso comunes basados en la función de trabajo.
* Ahorre tener que crear políticas usted mismo.
* Se pueden adjuntar a varios usuarios, grupos o roles dentro de las cuentas de AWS y entre ellas.
* No se pueden cambiar los permisos asignados.

Política gestionada por el cliente:

* Política independiente que cree y administre en su propia cuenta de AWS.
* Can be attached to multiple users, groups, and roles – but only within your own account.
* Se puede crear copiando una directiva administrada existente y, a continuación, personalizándola.

1. Recomendado para casos de uso en los que las políticas administradas de AWS existentes no cumplen con el

necesidades de su entorno.

Inline Policy:

* Las directivas en línea se incrustan en el usuario, grupo o rol al que se aplica.
* Relación estricta 1:1 entre la entidad y la política.
* Al eliminar el usuario, grupo o rol en el que está incrustada la directiva en línea, la directiva también se eliminará.
* En la mayoría de los casos, AWS recomienda utilizar políticas administradas en lugar de políticas en línea.
* Las directivas en línea son útiles cuando desea asegurarse de que los permisos de una directiva no se asignan inadvertidamente a ningún otro usuario, grupo o rol.

### AWS MANAGED AND CUSTOMER MANAGED POLICIES

Una política administrada de AWS es una política independiente creada y administrada por AWS.

La política independiente significa que la política tiene su propio nombre de recurso de Amazon (ARN) que incluye el nombre de la política.

Las políticas administradas de AWS están diseñadas para proporcionar permisos para muchos casos de uso comunes. No puede cambiar los permisos definidos en las políticas administradas de AWS.

Algunas políticas administradas de AWS están diseñadas para funciones de trabajo específicas. Las políticas administradas de AWS específicas del trabajo incluyen:

* Administrator.
* Billing.
* Database Administrator.
* Data Scientist.
* Developer Power User.
* Network Administrator.
* Security Auditor.
* Support User.
* System Administrator.
* View-Only User.

Puede crear políticas independientes que administre en su propia cuenta de AWS, a las que nos referimos como políticas administradas por el cliente.

A continuación, puede adjuntar las políticas a varias entidades principales de su cuenta de AWS.

Cuando se adjunta una directiva a una entidad principal, se conceden a la entidad los permisos definidos en la directiva.

### IAM POLICY EVALUATION LOGIC

De forma predeterminada, todas las solicitudes se deniegan implícitamente. (Alternativamente, de forma predeterminada, el usuario raíz de la cuenta de AWS tiene acceso completo).

Un permiso explícito en una directiva basada en identidad o en recursos anula este valor predeterminado.

Si hay un límite de permisos, un SCP de organizaciones o una directiva de sesión, es posible que invalide el permiso con una denegación implícita.

Una denegación explícita en cualquier directiva anula cualquier permiso.

Se deben conocer algunos conceptos para entender la lógica.:

* **Políticas basadas** en identidad: las políticas basadas en identidad se adjuntan a una identidad de IAM (usuario, grupo de usuarios o rol) y conceden permisos a las entidades de IAM (usuarios y roles).
* **Directivas basadas** en recursos: las directivas basadas en recursos conceden permisos a la entidad de seguridad (cuenta, usuario, rol o usuario federado) especificada como entidad de seguridad.
* **IAM permissions boundaries – Los límites de permisos son una característica avanzada que establece l**os permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol).
* **Políticas de control de servicios (SCP) de AWS** Organizations: los SCP de organizaciones especifican los permisos máximos para una organización o unidad organizativa (OU). Directivas de sesión: las directivas de sesión son directivas avanzadas que se pasan como parámetros cuando se crea mediante programación una sesión temporal para un rol o usuario federado.

El siguiente diagrama de flujo detalla la lógica de evaluación de políticas de IAM:

Diagrama

Descripción generada automáticamente

### IAM INSTANCE PROFILES

Un perfil de instancia es un contenedor para un rol de IAM que puede utilizar para pasar información de rol a una instancia EC2 cuando se inicia la instancia.

Un perfil de instancia solo puede contener un rol de IAM, aunque un rol se puede incluir en varios perfiles de instancia.

Diagrama

Descripción generada automáticamente

Puede utilizar los siguientes comandos de la AWS CLI para trabajar con perfiles de instancia en una cuenta de AWS:

* Crear un perfil de instancia: aws iam create-instance-profile
* Agregar un rol a un perfil de instancia: aws iam add-role-to-instance-profile
* Enumerar perfiles de instancia: aws iam list-instance-profiles, aws iam list-instance-profiles-for-role
* Obtener información sobre un perfil de instancia: aws iam get-instance-profile
* Quitar un rol de un perfil de instancia: aws iam remove-role-from-instance-profile
* Eliminar un perfil de instancia: aws iam delete-instance-profile

### AWS SECURITY TOKEN SERVICE

AWS Security Token Service (STS) es un servicio web que le permite solicitar credenciales temporales de privilegios limitados para los usuarios de IAM o para los usuarios que autentica (usuarios federados).

De forma predeterminada, AWS STS está disponible como un servicio global y todas las solicitudes de AWS STS van a un único punto de enlace en [https://sts.amazonaws.com](https://sts.amazonaws.com/)

Opcionalmente, puede enviar sus solicitudes de AWS STS a puntos de enlace en cualquier región (puede reducir la latencia). Las credenciales siempre funcionarán a nivel mundial.

STS es compatible con AWS CloudTrail, que registra las llamadas de AWS para su cuenta de AWS y entrega archivos de registro a un bucket de S3.

Las credenciales de seguridad temporales funcionan de manera casi idéntica a las credenciales de clave de acceso a largo plazo que pueden usar los usuarios de IAM, con las siguientes diferencias:

* Las credenciales de seguridad temporales son a corto plazo.
* Se pueden configurar para que duren desde unos pocos minutos hasta varias horas.
* Una vez que expiran las credenciales, AWS ya no las reconoce ni permite ningún tipo de acceso a las solicitudes de API realizadas con ellas.
* Las credenciales de seguridad temporales no se almacenan con el usuario, sino que se generan dinámicamente y se proporcionan al usuario cuando se solicitan.
* Cuando (o incluso antes) expiran las credenciales de seguridad temporales, el usuario puede solicitar nuevas credenciales, si el usuario que las solicita todavía tiene permiso para hacerlo.

Las ventajas de STS son:

* No es necesario distribuir ni incrustar credenciales de seguridad de AWS a largo plazo con una aplicación.
* Puede proporcionar acceso a sus recursos de AWS a los usuarios sin tener que definir una identidad de AWS para ellos (las credenciales de seguridad temporales son la base de los roles de IAM y la federación de ID).
* Las credenciales de seguridad temporales tienen una vida útil limitada, por lo que no tiene que rotar o revocarlos explícitamente cuando ya no sean necesarios.
* Después de que caduquen las credenciales de seguridad temporales, no se pueden reutilizar (puede especificar durante cuánto tiempo son válidas las credenciales, hasta un límite máximo).

La acción de la API de AWS STS devuelve credenciales de seguridad temporales que consisten en:

* Una clave de acceso que consta de un ID de clave de acceso y un ID secreto.
* Un token de sesión.
* Caducidad o duración de la validez.
* Los usuarios (o una aplicación que ejecute el usuario) pueden usar estas credenciales para tener acceso a los recursos.

Con STS puede solicitar un token de sesión mediante una de las siguientes API:

* AssumeRole – solo pueden utilizar los usuarios de IAM (se pueden utilizar para MFA).
* AssumeRoleWithSAML – puede ser utilizado por cualquier usuario que pase una respuesta de autenticación SAML que indique la autenticación de un proveedor de identidad conocido (de confianza).
* AssumeRoleWithWebIdentity – Puede ser utilizado por un usuario que pasa un token de identidad Web que indica la autenticación de un proveedor de identidad conocido (de confianza).
* GetSessionToken – puede ser utilizado por un usuario de IAM o un usuario raíz de cuenta de AWS (se puede utilizar para MFA).
* GetFederationToken – puede ser utilizado por un usuario de IAM o un usuario raíz de una cuenta de AWS.

AWS recomienda usar Cognito para la federación de identidades con proveedores de identidades de Internet. Los usuarios pueden provenir de tres fuentes.

###### Federation (typically AD):

* Uses SAML 2.0.
* Concede acceso temporal en función de las credenciales de AD de los usuarios.
* No es necesario ser usuario en IAM.
* El inicio de sesión único permite a los usuarios iniciar sesión en la consola de AWS sin asignar credenciales de IAM.

###### Federación con aplicaciones móviles:

* Utilice Facebook/Amazon/Google u otros proveedores de OpenID para iniciar sesión.

###### Cross Account Access:

* Permite a los usuarios de una cuenta de AWS acceder a los recursos de otra.
* Para realizar una solicitud en una cuenta diferente, el recurso de esa cuenta debe tener una directiva basada en recursos adjunta con los permisos que necesita.
* Or you must assume a role (identity-based policy) within that account with the permissions you need.

Hay un par de formas en que se puede usar STS.

Scenario 1:

* 1. Desarrollar un agente de identidades para comunicarse con LDAP y AWS STS.
  2. Identity Broker siempre se autentica primero con LDAP y luego con AWS STS.
  3. A continuación, la aplicación obtiene acceso temporal a los recursos de AWS.

Scenario 2:

1. Desarrollar un agente de identidades para comunicarse con LDAP y AWS STS.
2. Identity Broker se autentica primero con LDAP y, a continuación, obtiene un rol de IAM asociado al usuario.
3. A continuación, la aplicación se autentica con STS y asume ese rol de IAM.
4. La aplicación utiliza ese rol de IAM para interactuar con el servicio.

### CROSS ACCOUNT ACCESS

Útil para situaciones en las que un cliente de AWS tiene una cuenta de AWS independiente, por ejemplo, para recursos de desarrollo y producción.

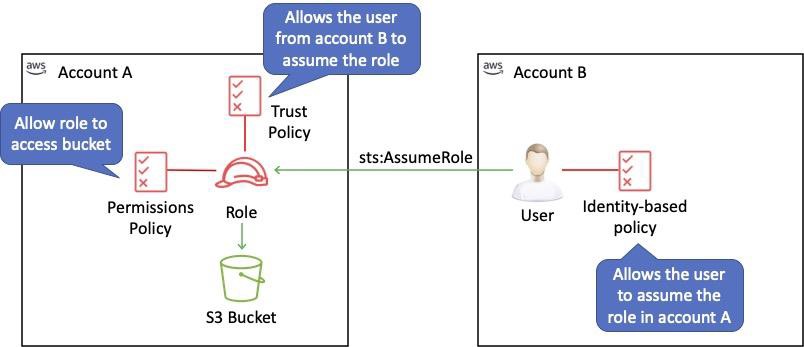
El acceso entre cuentas facilita el trabajo productivo dentro de un entorno de AWS de varias cuentas (o varios roles) al facilitar el cambio de roles dentro de la consola de administración de AWS.

Puede iniciar sesión en la consola con su nombre de usuario de IAM y, a continuación, cambiar la consola para administrar otra cuenta sin tener que introducir otro nombre de usuario y contraseña.

Permite a los usuarios de una cuenta de AWS acceder a los recursos de otra.

Para realizar una solicitud en una cuenta diferente, el recurso de esa cuenta debe tener una directiva basada en recursos adjunta con los permisos que necesita.

O bien, debe asumir un rol (directiva basada en identidad) dentro de esa cuenta con los permisos que necesita.



### IAM BEST PRACTICES

Para proteger los recursos de AWS, se recomienda que siga estas prácticas recomendadas:

* Bloquee las claves de acceso de usuario raíz de su cuenta de AWS.
* Usar roles para delegar permisos.
* Conceder el privilegio mínimo.
* Introducción al uso de permisos con políticas administradas de AWS.
* Validate your policies.
* Usar políticas administradas por el cliente en lugar de directivas en línea.
* Usar niveles de acceso para revisar los permisos de IAM.
* Configurar una directiva de contraseñas seguras para los usuarios.
* Habilitar MFA.
* Uso de roles para aplicaciones que se ejecutan en instancias Amazon EC2.
* No compartir claves de acceso.
* Rotar credenciales regularmente.
* Eliminar credenciales innecesarias.
* Condiciones de la política de uso para mayor seguridad.
* Monitoree la actividad en su cuenta de AWS.

## AWS DIRECTORY SERVICE

### AWS DIRECTORY SERVICE FEATURES

AWS proporciona varios tipos de directorios.

Los siguientes tres tipos se presentan actualmente en el examen y se cubrirán en esta página:

* Servicio de Active Directory para Microsoft Active Directory.
* Simple AD.
* AD Connector.

Como alternativa al servicio AWS Directory, puede crear sus propios controladores de dominio de Microsoft AD en la nube de AWS (on EC2).

* Cuando crea el suyo propio, puede unirse a un dominio de Active Directory local existente (modo de replicación).
* Debe establecer una VPN (además de Direct Connect si la tiene).
* El modo de replicación es menos seguro que establecer relaciones de confianza.

La siguiente tabla resume los servicios de directorio cubiertos en esta página, así como un par de otros, y proporciona algunos casos de uso típicos:

|  |  |  |
| --- | --- | --- |
| **Directory Service Option** | **Description** | **Use Case** |
| AWS Cloud Directory | Directorio nativo de la nube para compartir y controlar el acceso a datos jerárquicos entre aplicaciones | Aplicaciones en la nube que necesitan datos jerárquicos con relaciones complejas |
| Amazon Cognito | Funcionalidad de registro e inicio de sesión que se escala a millones de usuarios y se federa a servicios públicos de redes sociales | Desarrollar aplicaciones de consumo o SaaS |
| AWS Directory Service for Microsoft Active Directory | Microsoft AD completo administrado por AWS que se ejecuta en Windows Server 2012 R2 | Empresas que desean Microsoft AD hospedado o que necesitan LDAP para aplicaciones Linux |
| AD Connector | Allows on-premises users to log into AWS services with their existing AD credentials. Also allows EC2 instances to join AD domain | Single sign-on for on- premises employees and for adding EC2 instances to the domain |
| Simple AD | Implementación de AD a baja escala y bajo costo basada en Samba | Directorio de usuario simple, o necesita compatibilidad con LDAP |

### ACTIVE DIRECTORY SERVICE FOR MICROSOFT ACTIVE DIRECTORY

Servicios de AWS totalmente administrados en la infraestructura de AWS.

La mejor opción si tiene más de 5000 usuarios y / o necesita una relación de confianza configurada.

Incluye parches de software, replicación, copias de seguridad automatizadas, reemplazo de controladores de dominio fallidos y monitoreo. Se ejecuta en un servidor Windows.

Puede realizar extensiones de esquema.

Funciona con aplicaciones de SharePoint, Microsoft SQL Server y.Net.

Puede configurar relaciones de confianza para extender la autenticación desde los directorios activos locales a la nube de AWS.

Los usuarios y grupos locales pueden obtener acceso a los recursos de cualquiera de los dominios mediante SSO. Requiere una conexión VPN o Direct Connect.

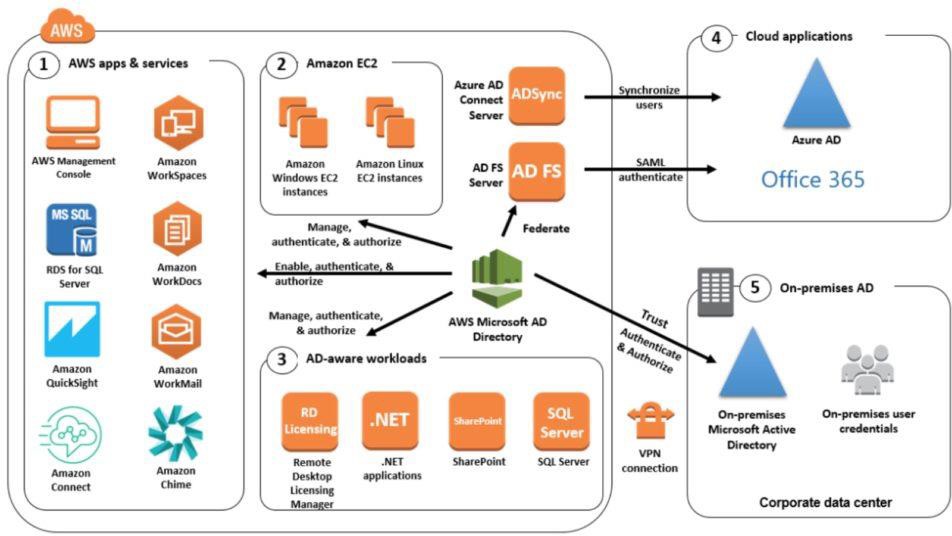
Se puede utilizar como un anuncio independiente en la nube de AWS.

Cuando se usa de forma independiente, los usuarios pueden acceder a aplicaciones de terceros como Microsoft O365 a través de la federación.

También puede utilizar las credenciales de Active Directory para autenticarse en la consola de administración de AWS sin tener que configurar la autenticación SAML.

AWS Microsoft AD admite aplicaciones de AWS, incluidas Workspaces, WorkDocs, QuickSight, Chime, Amazon Connect y RDS para Microsoft SQL Server.

El siguiente diagrama muestra algunos de los casos de uso para su directorio de AWS Microsoft AD, incluida la capacidad de conceder a sus usuarios acceso a aplicaciones en la nube externas y permitir que los usuarios de AD locales administren y tengan acceso a los recursos en la nube de AWS.



Incluye características de seguridad como:

* Administración detallada de políticas de contraseñas.
* Cifrado LDAP a través de SSL/TLS.
* Aprobado por HIPAA y PCI DSS.
* Autenticación multifactor a través de la integración con la infraestructura MFA basada en RADIUS existente.

Monitoreo proporcionado a través de CloudTrail, notificaciones a través de SNS, instantáneas automatizadas diarias. Servicio escalable que se escala mediante la adición de controladores de dominio.

Implementado en una configuración de alta disponibilidad en dos zonas de disponibilidad de la misma región.

AWS Microsoft AD no admite el modo de replicación en el que se realiza la replicación en un AD local.

Dos ediciones:

* Standard Edition está optimizado para ser un directorio principal para pequeñas y medianas empresas con hasta 5.000 empleados. Proporciona suficiente capacidad de almacenamiento para admitir hasta 30.000 objetos de directorio, como usuarios, grupos y equipos.
* Enterprise Edition está diseñado para admitir organizaciones empresariales con hasta 500.000 objetos de directorio.

Uso compartido de directorios:

* AWS Directory Service for Microsoft Active Directory le permite utilizar un directorio en una cuenta y compartirlo con varias cuentas y VPC.
* Hay un cargo por uso compartido por hora por cada cuenta adicional con la que comparte un directorio.
* No hay ningún cargo por uso compartido para las VPC adicionales en las que comparte un directorio o para la cuenta en la que instala el directorio.

### SIMPLE AD

Un servicio económico compatible con Active Directory con características de directorio comunes. Directorio independiente y totalmente administrado en la nube de AWS.

Simple AD es generalmente la opción menos costosa.

La mejor opción para menos de 5000 usuarios y no necesita funciones avanzadas de AD.

Desarrollado por SAMBA 4 servidor compatible con Active Directory. Puede crear usuarios y controlar el acceso a las aplicaciones en AWS. Proporciona un subconjunto de las características proporcionadas por AWS MS AD. Las características incluyen:

* Manage user accounts.
* Manage groups.
* Apply group policies.
* Securely connect to EC2 instances.
* Kerberos-based SSO.

1. Supports joining Linux or Windows based EC2 instances. AWS proporciona servicios de monitoreo, instantáneas diarias y recuperación. Posibilidad de instantáneas manuales.

Simple AD es compatible con WorkSpaces, WorkDocs, Workmail y QuickSight.

También puede iniciar sesión en la consola de administración de AWS con cuentas de usuario de Simple AD para administrar los recursos de AWS.

Disponible en dos edicioness:

* Small – soporta hasta 500 usuarios (aproximadamente 2000 objetos).
* Large – soporta hasta 5000 usuarios (aproximadamente 20.000 objetos).

AWS crea dos servidores de directorios y servidores DNS en dos subredes diferentes dentro de una zona de disponibilidad. Simple AD no es compatible:

* DNS dynamic updates.
* Schema extensions.
* Multi-factor authentication.
* Communication over LDAPS.
* PowerShell AD cmdlets.
* FSMO role transfer.

No es compatible con RDS SQL Server.

No admite relaciones de confianza con otros dominios (utilice AWS MS AD).

### AD CONNECTOR

AD Connector es una puerta de enlace de directorio para redirigir las solicitudes de directorio a su Active Directory local.

AD Connector elimina la necesidad de sincronización de directorios y el costo y la complejidad de hospedar una infraestructura de federación.

Conecta su AD local existente a AWS.

La mejor opción cuando desee utilizar un Active Directory existente con los servicios de AWS. AD Connector viene en dos tamaños:

* Small – diseñado para organizaciones de hasta 500 usuarios.
* Large – diseñado para organizaciones de hasta 5000 usuarios.

La VPC debe estar conectada a la red local a través de VPN o Direct Connect.

Cuando los usuarios inician sesión en AWS Applications AD Connector reenvía las solicitudes de inicio de sesión a los controladores de dominio de AD locales.

También puede unir instancias EC2 a su AD local a través de AD Connector.

También puede iniciar sesión en la consola de administración de AWS mediante los controladores de dominio de AD locales para la autenticación.

No es compatible con RDS SQL.

Puede usar AD Connector para la autenticación multifactor mediante la infraestructura MFA basada en RADIUS.

### AD CONNECTOR VS SIMPLE AD

En la tabla siguiente se describen algunas de las diferencias clave que se deben tener en cuenta al elegir AD Connector o Simple AD:

|  |  |
| --- | --- |
| **AD Connector** | **Simple AD** |
| Must have an existing AD | AD independiente basado en Samba |
| Existing AD users can access AWS assets via IAM roles | Admite cuentas de usuario, grupos, directivas de grupo y dominios |
| Supports MFA via existing RADIUS- based MFA infrastructure | Kerberos-based SSO |
|  | MFA no compatible |
|  | Relaciones de confianza no admitidas |

## AMAZON COGNITO

### AMAZON COGNITO FEATURES

Amazon Cognito le permite agregar el registro de usuarios, el inicio de sesión y el control de acceso a sus aplicaciones web y móviles de forma rápida y sencilla.

Amazon Cognito proporciona autenticación, autorización y administración de usuarios para sus aplicaciones web y móviles.

Sus usuarios pueden iniciar sesión directamente con un nombre de usuario y contraseña, o a través de un tercero como Facebook, Amazon o Google.

### WEB IDENTITY FEDERATION

AWS Cognito trabaja con proveedores de identidad externos que admiten SAML u OpenID Connect, proveedores de identidad social (como Facebook, Twitter, Amazon)

La federación permite a los usuarios autenticarse con un proveedor de identidad web (por ejemplo, Google, Facebook, Amazon).

El usuario se autentica primero con el proveedor de ID web y recibe un token de autenticación, que luego se intercambia por credenciales temporales de AWS que le permiten asumir un rol de IAM que permite el acceso a los recursos necesarios.

Cognito es un agente de identidad que gestiona la interacción entre sus aplicaciones y el ID web

proveedor (no necesita escribir su propio código para hacer esto).

Puede utilizar Amazon, Facebook, Twitter, Digits, Google y cualquier otro proveedor de identidad compatible con OpenID Connect.

También puede integrar su propio proveedor de identidades.

### USER POOLS AND IDENTITY POOLS

Los dos componentes principales de AWS Cognito son los grupos de usuarios y los grupos de identidades:

* Los grupos de usuarios son directorios de usuarios que proporcionan opciones de registro e inicio de sesión para los usuarios de la aplicación.
* Los grupos de identidades le permiten conceder a sus usuarios acceso a otros servicios de AWS.

Puede usar grupos de identidades y grupos de usuarios por separado o juntos.

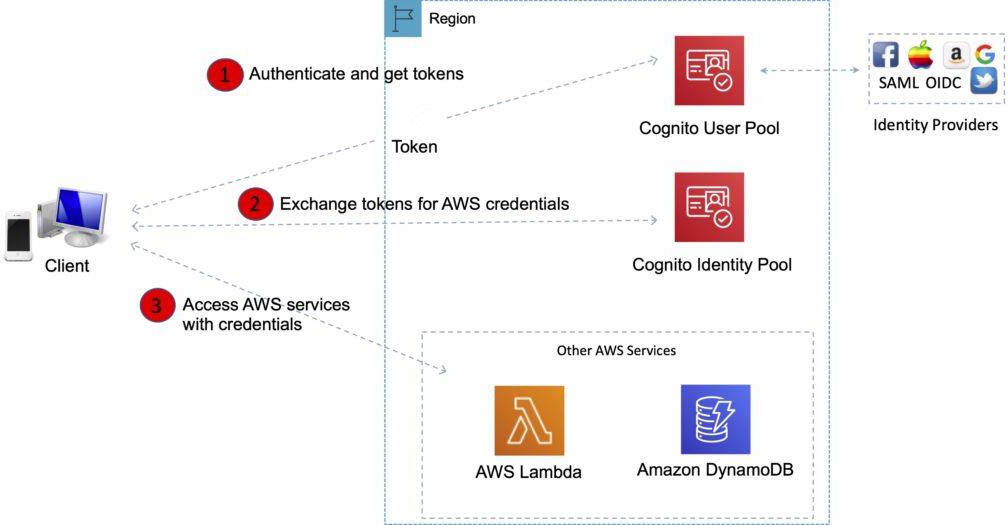
No es necesario que la aplicación incruste o almacene las credenciales de AWS localmente en el dispositivo y ofrece a los usuarios una experiencia perfecta en todos los dispositivos móviles.

Cognito Identity proporciona credenciales de seguridad temporales para acceder a los recursos back-end de la aplicación en

AWS o cualquier servicio detrás de Amazon API Gateway. Cognito expone las API del lado del servidor.

Los usuarios pueden registrarse e iniciar sesión utilizando el correo electrónico, el número de teléfono o el nombre de usuario. Los usuarios finales de una aplicación también pueden iniciar sesión con MFA basado en SMS.

Existe una herramienta de importación para migrar usuarios a un grupo de usuarios de Amazon Cognito.



### USER POOLS

Los grupos de usuarios de Cognito son directorios de usuarios que se utilizan para administrar la funcionalidad de registro e inicio de sesión para aplicaciones móviles y web.

Con un grupo de usuarios, los usuarios pueden iniciar sesión en su aplicación web o móvil a través de Amazon Cognito.

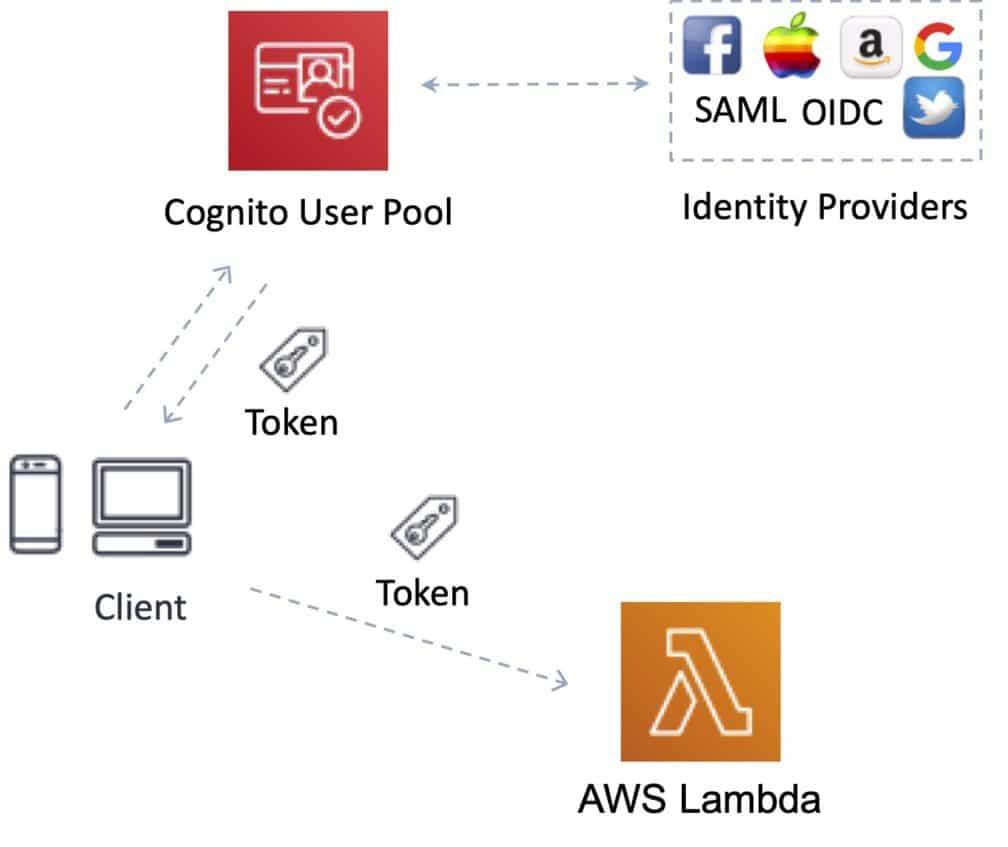
Los usuarios también pueden iniciar sesión a través de proveedores de identidad social como Facebook o Amazon, y a través de proveedores de identidad SAML.

Ya sea que los usuarios inicien sesión directamente o a través de un tercero, todos los miembros del grupo de usuarios tienen un perfil de directorio al que puede acceder a través de un SDK.

Cognito actúa como agente de identidad entre el proveedor de ID y AWS. Los grupos de usuarios proporcionan:

* Servicios de registro e inicio de sesión.
* Una interfaz de usuario web integrada y personalizable para iniciar sesión en los usuarios.
* Inicio de sesión social con Facebook, Google e inicio de sesión con Amazon, así como inicio de sesión con proveedores de identidad SAML de su grupo de usuarios.
* Administración de directorios de usuarios y perfiles de usuario.
* Características de seguridad como autenticación multifactor (MFA), comprobaciones de credenciales comprometidas, protección de adquisición de cuentas y verificación de teléfono y correo electrónico.
* Flujos de trabajo personalizados y migración de usuarios a través de desencadenadores de AWS Lambda.

Después de autenticar correctamente a un usuario, Amazon Cognito emite tokens web JSON (JWT) que puede utilizar para proteger y autorizar el acceso a sus propias API o intercambiar por credenciales de AWS.



### IDENTITY POOLS

Los grupos de identidades le permiten crear identidades únicas para los usuarios y autenticarlos con proveedores de identidades.

Con una identidad, puede obtener credenciales de AWS temporales con privilegios limitados para obtener acceso a otros servicios de AWS.

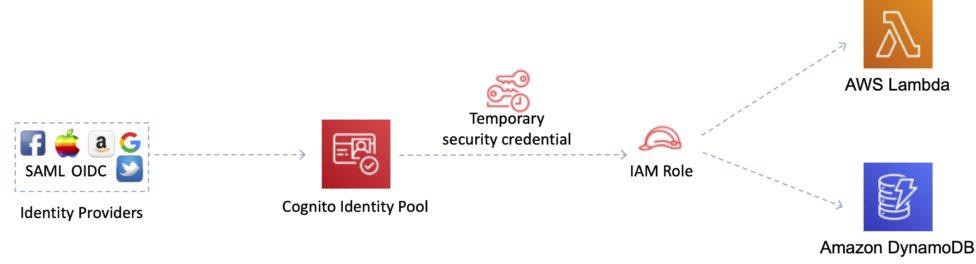
Cognito realiza un seguimiento de la asociación entre la identidad del usuario y los diferentes dispositivos desde los que inician sesión.

Con el fin de proporcionar una experiencia de usuario perfecta para su aplicación, Cognito utiliza la sincronización push para enviar actualizaciones y sincronizar los datos del usuario en varios dispositivos.

Amazon SNS se utiliza para enviar una notificación push silenciosa a todos los dispositivos cada vez que cambian los datos almacenados en la nube.

Los grupos de identidades de Amazon Cognito admiten los siguientes proveedores de identidades:

* Proveedores públicos: Iniciar sesión con Amazon (grupos de identidades), Facebook (grupos de identidades), Google (grupos de identidades).
* Amazon Cognito User Pools.
* Open ID Connect Providers (Identity Pools).
* SAML Identity Providers (Identity Pools).
* Developer Authenticated Identities (Identity Pools).



***Consejo para el examen:*** *Para que sea más fácil recordar la diferencia entre grupos de usuarios y grupos de identidades, piense en los grupos de usuarios como usuarios de IAM o Active Directory y en los grupos de identidades como un rol de IAM.*

## AMAZON INSPECTOR

### AMAZON INSPECTOR FEATURES

Amazon Inspector es un servicio automatizado de evaluación de seguridad que ayuda a mejorar la seguridad y la conformidad de las aplicaciones implementadas en AWS.

Amazon Inspector evalúa automáticamente las aplicaciones en busca de exposición, vulnerabilidades y desviaciones de las prácticas recomendadas.

Después de realizar una evaluación, Amazon Inspector produce una lista detallada de los hallazgos de seguridad priorizados por nivel de gravedad.

Amazon Inspector prueba la accesibilidad de red de las instancias Amazon EC2 y el estado de seguridad de las aplicaciones que se ejecutan en esas instancias.

Las evaluaciones de seguridad de Amazon Inspector le ayudan a comprobar la accesibilidad de red no deseada de sus instancias Amazon EC2 y las vulnerabilidades en esas instancias EC2.

Después de realizar una evaluación, Amazon Inspector produce una lista detallada de los hallazgos de seguridad que se organiza por nivel de gravedad.

Estos hallazgos se pueden revisar directamente o como parte de informes de evaluación detallados que están disponibles a través de la consola o API de Amazon Inspector.

Con Amazon Inspector, puede automatizar las evaluaciones de vulnerabilidades de seguridad en todas sus canalizaciones de desarrollo e implementación o para sistemas de producción estáticos.

Esto le permite hacer que las pruebas de seguridad sean una parte regular de las operaciones de desarrollo y TI.

### BENEFITS OF INSPECTOR

**Motor de análisis de** configuración **y monitoreo de actividad**: Amazon Inspector proporciona un agente que analiza la configuración del sistema y los recursos.

**Biblioteca de contenido integrada**: Amazon Inspector incluye una biblioteca integrada de reglas e informes.

**Automatización a través de una API**: Amazon Inspector se puede automatizar completamente a través de una API.

### AMAZON INSPECTOR AGENT

Amazon Inspector también ofrece software predefinido denominado agente que puede instalar opcionalmente en el sistema operativo de las instancias EC2 que desea evaluar.

El agente supervisa el comportamiento de las instancias EC2, incluida la actividad de red, sistema de archivos y procesos. También recopila un amplio conjunto de datos de comportamiento y configuración (telemetría).

### RULES AND PACKAGES

Puede utilizar Amazon Inspector para evaluar sus objetivos de evaluación (colecciones de recursos de AWS) en busca de posibles problemas de seguridad y vulnerabilidades.

Amazon Inspector compara el comportamiento y la configuración de seguridad de los objetivos de evaluación con los paquetes de reglas de seguridad seleccionados.

En el contexto de Amazon Inspector, una regla es una comprobación de seguridad que Amazon Inspector realiza durante la ejecución de la evaluación.

Las evaluaciones de Amazon Inspector se le ofrecen como paquetes de reglas predefinidas asignados a prácticas recomendadas de seguridad comunes y definiciones de vulnerabilidad.

Los ejemplos de reglas integradas incluyen la comprobación del acceso a las instancias EC2 desde Internet, la habilitación del inicio de sesión raíz remoto o la instalación de versiones de software vulnerables.

Los investigadores de seguridad de AWS actualizan periódicamente estas reglas.

Una evaluación de Amazon Inspector puede utilizar cualquier combinación de los siguientes paquetes de reglas:

#### Network assessments

**Accesibilidad de red**: las reglas del paquete Accesibilidad de red analizan las configuraciones de red para encontrar vulnerabilidades de seguridad de las instancias EC2. Los hallazgos que genera Amazon Inspector también proporcionan orientación sobre cómo restringir el acceso que no es seguro.

#### Host assessments

**Vulnerabilidades y exposiciones comunes**: las reglas de este paquete ayudan a verificar si las instancias EC2 de sus objetivos de evaluación están expuestas a vulnerabilidades y exposiciones comunes (CVE).

**Puntos de referencia del Centro de Seguridad en Internet (CIS**): el programa de Puntos de referencia de seguridad de CIS proporciona las mejores prácticas de la industria bien definidas, imparciales y basadas en el consenso para ayudar a las organizaciones a evaluar y mejorar su seguridad.

**Prácticas recomendadas de** seguridad **para Amazon Inspector**: utilice las reglas de Amazon Inspector para determinar si sus sistemas están configurados de forma segura.

## AWS TRUSTED ADVISOR

### AWS TRUSTED ADVISOR FEATURES

Trusted Advisor es un recurso en línea que ayuda a reducir costos, aumentar el rendimiento y mejorar la seguridad mediante la optimización de su entorno de AWS.

Trusted Advisor proporciona orientación en tiempo real para ayudarle a aprovisionar sus recursos siguiendo las prácticas recomendadas.

Advisor le asesorará sobre optimización de costos, rendimiento, seguridad y tolerancia a fallas.

Trusted Advisor analiza su infraestructura de AWS y la compara con las prácticas recomendadas de AWS en cinco categorías:

* Cost Optimization.
* Performance.
* Security.
* Fault Tolerance.
* Service Limits.

Trusted Advisor viene en dos versiones. Comprobaciones y recomendaciones básicas (gratis):

* Acceso a las 7 comprobaciones principales para ayudar a aumentar la seguridad y el rendimiento.
* Las comprobaciones incluyen permisos de bucket de S3, grupos de seguridad, uso de IAM, MFA en la cuenta raíz, instantáneas públicas de EBS, instantáneas públicas de RDS.

Beneficios completos de Trusted Advisor (planes de soporte empresarial y empresarial). Conjunto completo de comprobaciones para ayudar a optimizar toda su infraestructura de AWS.

Asesora sobre seguridad, rendimiento, costo, tolerancia a fallas y límites de servicio.

Las ventajas adicionales incluyen notificaciones de actualización semanales, alertas, acciones automatizadas con CloudWatch y acceso mediante programación mediante la API de AWS Support.

## AWS GUARDDUTY

### AWS GUARDDUTY FEATURES

Servicio inteligente de detección de amenazas.

Monitorea continuamente la actividad maliciosa y ofrece hallazgos de seguridad detallados para visibilidad y corrección.

Monitorea cuentas, cargas de trabajo y datos de AWS en Amazon S3.

Detecta el compromiso de la cuenta, el compromiso de la instancia, el reconocimiento malicioso y el compromiso del bucket.

Amazon GuardDuty le ofrece acceso a técnicas de detección integradas desarrolladas y optimizadas para la nube.

AWS Security mantiene y mejora continuamente estos algoritmos de detección. Las categorías de detección principales incluyen:

* **Reconocimiento:** Actividad que sugiere reconocimiento por parte de un atacante como:
  + Actividad inusual de la API.
  + Análisis de puertos dentro de la VPC.
  + Patrones de solicitud de inicio de sesión inusuales y fallidos.
  + Sondeo de puerto desbloqueado de una IP incorrecta conocida.
* **Compromiso de instancia:** actividad que indica un compromiso de instancia, como:
  + Minería de criptomonedas
  + Actividad de comando y control de puerta trasera (C&C).
  + Malware mediante algoritmos de generación de dominios (DGA).
  + Actividad de denegación de servicio saliente.
  + Volumen de tráfico de red inusualmente alto.
  + Protocolos de red inusuales.
  + Comunicación de instancia saliente con una IP maliciosa conocida.
  + Credenciales temporales de Amazon EC2 utilizadas por una dirección IP externa.
  + Exfiltración de datos mediante DNS.
* **Compromiso de cuenta:** Los patrones comunes indicativos de compromiso de cuenta incluyen:
  + Llamadas a la API desde una geolocalización inusual o un proxy anónimo.
  + Intentos de deshabilitar el registro de AWS CloudTrail.
  + Cambios que debilitan la directiva de contraseñas de la cuenta.
  + Lanzamientos inusuales de instancias o infraestructuras.
  + Implementaciones de infraestructura en una región inusual.
  + Llamadas a la API desde direcciones IP maliciosas conocidas.
* **Compromiso de bucket:** actividad que indica un compromiso de bucket, como:
  + Patrones de acceso a datos sospechosos que indican un uso indebido de credenciales.
  + Actividad inusual de la API de Amazon S3 desde un host remoto.
  + Acceso no autorizado a S3 desde direcciones IP maliciosas conocidas.
  + Llamadas a la API para recuperar datos en buckets de S3 de un usuario sin historial previo de acceso al bucket o invocado desde una ubicación inusual.

## AWS CERTIFICATE MANAGER

### AWS CERTIFICATE MANAGER FEATURES

Crear, almacenar y renovar certificados SSL/TLS X.509 Dominios individuales, varios nombres de dominio y comodines Se integra con varios servicios de AWS, incluidos:

* Elastic Load Balancing.
* Amazon CloudFront.
* AWS Elastic Beanstalk.
* AWS Nitro Enclaves.
* AWS CloudFormation.

**Los certificados públicos** están firmados por la autoridad de certificación pública de AWS. También puede crear una CA privada con ACM.

A continuación, puede emitir certificados privados.

También puede importar certificados de emisores externos.

## AWS KMS

### AWS KMS FEATURES

AWS Key Management Store (KMS) es un servicio administrado que le permite cifrar fácilmente sus datos.

AWS KMS proporciona una solución de almacenamiento, administración y auditoría de claves de alta disponibilidad para que pueda cifrar datos dentro de sus propias aplicaciones y controlar el cifrado de datos almacenados en todos los servicios de AWS.

AWS KMS le permite administrar y almacenar sus claves de forma centralizada y de forma segura. Estas se conocen como claves de AWS KMS (anteriormente conocidas como claves maestras de cliente (CMK).

### AWS KMS KEYS

Una clave KMS consta de:

* Alias.
* Creation date.
* Description.
* Key state.
* Material clave (proporcionado por el cliente o proporcionado por AWS). Las claves de KMS son los recursos principales de AWS KMS.

La clave KMS incluye metadatos, como el identificador de clave, la fecha de creación, la descripción y el estado de la clave. La clave KMS también contiene el material de clave utilizado para cifrar y descifrar datos.

AWS KMS admite claves KMS simétricas y asimétricas.

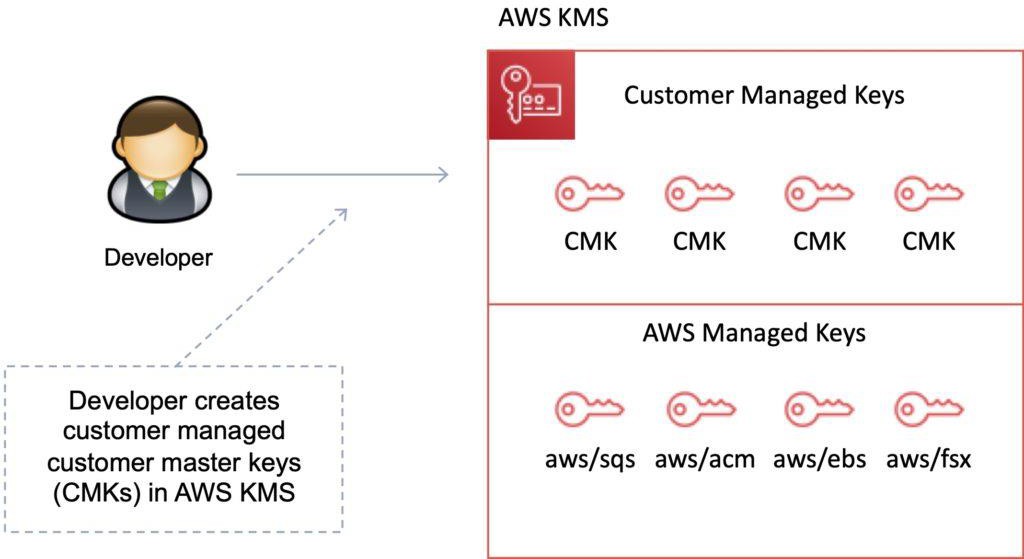
Las claves de KMS se crean en AWS KMS. Las claves KMS simétricas y las claves privadas de las claves KMS asimétricas nunca dejan AWS KMS sin cifrar.

De forma predeterminada, AWS KMS crea el material de clave para una clave de KMS. Una clave KMS puede cifrar datos de hasta 4 KB de tamaño.

Una clave KMS puede generar, cifrar y descifrar claves de cifrado de datos (DEK). Una clave KMS nunca se puede exportar desde KMS (CloudHSM lo permite).

Claves de KMS administrados por AWS:

* Las claves de KMS administradas por AWS son utilizadas por los servicios de AWS que interactúan con KMS para cifrar datos.
* Solo pueden ser utilizados por el servicio que los creó dentro de una región en particular.
* Se crean la primera vez que se implementa el cifrado mediante ese servicio. Claves KMS administradas por el cliente:
* Estos proporcionan la capacidad de implementar una mayor flexibilidad.
* Puede realizar la rotación, el control del acceso y la configuración de directivas clave.
* Puede habilitar y deshabilitar la clave cuando ya no sea necesaria.



### CUSTOMER MANAGED KMS KEYS

Las claves KMS administradas por el cliente son claves KMS de su cuenta de AWS que usted crea, posee y administra.

Tiene control total sobre estas claves de KMS, incluido el establecimiento y mantenimiento de sus directivas clave,

Políticas y concesiones de IAM, habilitándolas y deshabilitándolas, rotando su material criptográfico, agregando etiquetas, creando alias que hacen referencia a la clave KMS y programando las claves KMS para su eliminación.

Las claves KMS administradas por el cliente incurren en una tarifa mensual y una tarifa por uso que excede el nivel gratuito.

### AWS MANAGED KMS KEYS

Las claves de KMS administradas por AWS son claves de KMS de su cuenta que un servicio de AWS que está integrado con AWS KMS crea, administra y utiliza en su nombre.

No puede administrar estas claves KMS, rotarlas o cambiar sus directivas de claves.

Tampoco puede utilizar directamente las claves KMS administradas por AWS en operaciones criptográficas; el servicio que los crea los utiliza en su nombre.

No paga una tarifa mensual por las claves KMS administradas por AWS. Pueden estar sujetos a tarifas por su uso que excedan la capa gratuita, pero algunos servicios de AWS cubren estos costos por usted.

### AWS OWNED KMS KEYS

Las claves de KMS propiedad de AWS son una colección de claves de KMS que un servicio de AWS posee y administra para su uso en varias cuentas de AWS.

Aunque las claves KMS propiedad de AWS no están en su cuenta de AWS, un servicio de AWS puede utilizar sus claves KMS propiedad de AWS para proteger los recursos de su cuenta.

No es necesario crear ni administrar las claves de KMS propiedad de AWS. Sin embargo, no puede verlos, usarlos, rastrearlos o auditarlos.

No se le cobra una tarifa mensual ni una tarifa de uso por las claves de KMS propiedad de AWS y no cuentan para las cuotas de AWS KMS para su cuenta.

### DATA ENCRYPTION KEYS

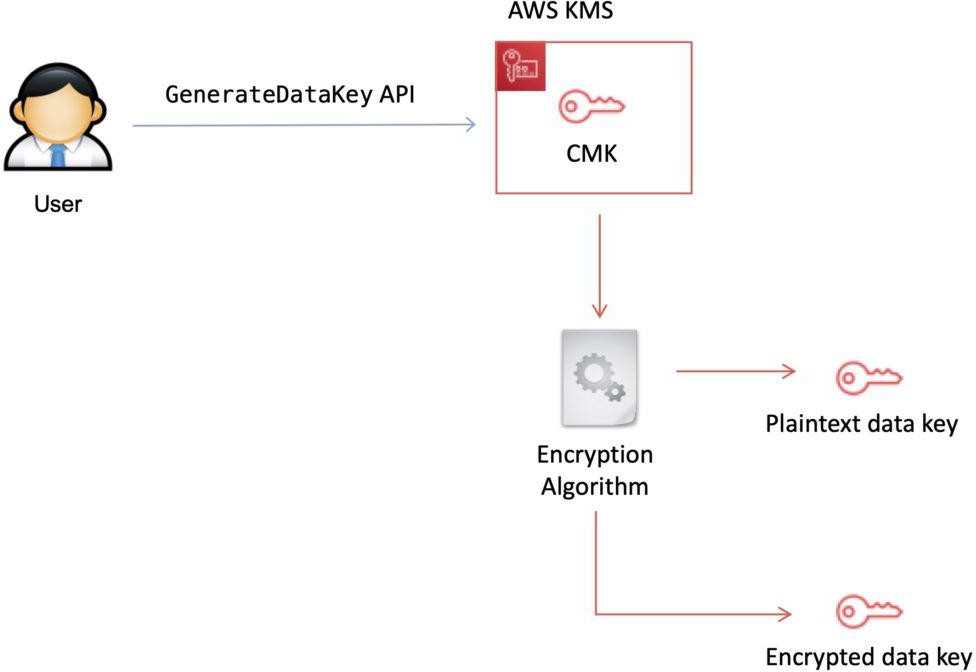
Las claves de datos son claves de cifrado que puede utilizar para cifrar datos, incluidas grandes cantidades de datos y otras claves de cifrado de datos.

Puede utilizar claves de AWS KMS para generar, cifrar y descifrar claves de datos.

AWS KMS no almacena, administra ni realiza un seguimiento de las claves de datos, ni realiza operaciones criptográficas con claves de datos.

Debe utilizar y administrar claves de datos fuera de AWS KMS.

La API GenerateDataKey se puede utilizar para crear una clave de cifrado de datos mediante una clave KMS:



### KMS DETAILS

Establezca directivas de uso en las claves que determinen qué usuarios pueden usarlas para cifrar y descifrar datos y en qué condiciones.

Opciones de materiales clave:

* KMS generated.
* Importa el tuyo propio.

Puede generar claves KMS en KMS, en un clúster de AWS CloudHSM, o importarlas desde su propia infraestructura de administración de claves.

Estas claves maestras están protegidas por módulos de seguridad de hardware (HSM) y solo se utilizan dentro de esos módulos.

Puede enviar datos directamente a KMS para cifrarlos o descifrarlos utilizando estas claves maestras. KMS ahora tiene la opción de teclas simétricas y asimétricas.

KMS es solo para cifrado en reposo (no en tránsito, use SSL).

KMS está estrechamente integrado en muchos servicios de AWS como Lambda, S3, EBS, EFS, DynamoDB, SQS, etc. KMS no conserva ni administra las claves de datos.

Los servicios de AWS cifran sus datos y almacenan una copia cifrada de la clave de datos junto con los datos que protege.

Cuando un servicio necesita descifrar sus datos, solicita a KMS que descifre la clave de datos utilizando su clave maestra.

Si el usuario que solicita datos del servicio de AWS está autorizado a descifrar bajo su política de clave maestra, el servicio recibirá la clave de datos descifrada de KMS con la que puede descifrar sus datos y devolverlos en texto sin formato.

Todas las solicitudes para utilizar sus claves maestras se registran en AWS CloudTrail para que pueda comprender quién utilizó qué clave en qué contexto y cuándo la utilizaron.

Puede controlar quién administra y accede a las claves a través de los usuarios y roles de IAM. Puede auditar el uso de claves a través de CloudTrail.

KMS difiere de Secrets Manager como su diseño específico para la administración de claves de cifrado. KMS está validado por muchos esquemas de cumplimiento (por ejemplo, PCI DSS Nivel 1, FIPS 140-2 Nivel 2). **Consejo para el examen: Las** claves de cifrado son regionales.

### KEY MANAGEMENT WITH KMS

Puede realizar las siguientes funciones de administración de claves en AWS KMS:

* Cree claves con un alias y una descripción únicos.
* Importa tu propio material clave.
* Defina qué usuarios y roles de IAM pueden administrar claves.
* Defina qué usuarios y roles de IAM pueden usar claves para cifrar y descifrar datos.
* Elija que AWS KMS gire automáticamente sus claves anualmente.
* Deshabilite temporalmente las claves para que no puedan ser utilizadas por nadie.
* Vuelva a habilitar las teclas deshabilitadas.
* Elimine las claves que ya no utiliza.
* Audite el uso de claves inspeccionando los registros en AWS CloudTrail.
* Crear almacenes de claves personalizados \*.
* Conecte y desconecte almacenes de claves personalizados\*.
* Eliminar almacenes de claves personalizados\*.

\* El uso de almacenes de claves personalizados requiere que los recursos de CloudHSM estén disponibles en su cuenta.

### LIMITS

Puede crear hasta 1000 claves KMS por cuenta y por región.

Dado que las claves KMS habilitadas y deshabilitadas cuentan para el límite, AWS recomienda eliminar las claves deshabilitadas que ya no utilice.

Las claves maestras administradas de AWS creadas en su nombre para su uso en los servicios de AWS compatibles no cuentan para este límite.

No hay límite para el número de claves de datos que se pueden derivar mediante una clave maestra y utilizar en la aplicación o en los servicios de AWS para cifrar los datos en su nombre.

## AWS CLOUDHSM

### AWS CLOUDHSM FEATURES

El servicio AWS CloudHSM le ayuda a cumplir los requisitos de conformidad corporativos, contractuales y normativos para la seguridad de los datos mediante el uso de instancias dedicadas del Módulo de seguridad de hardware (HSM) dentro de la nube de AWS.

AWS y los socios de AWS Marketplace ofrecen una variedad de soluciones para proteger datos confidenciales dentro de la plataforma de AWS, pero para algunas aplicaciones y datos sujetos a mandatos contractuales o reglamentarios para administrar claves criptográficas, la protección adicional puede ser necesario.

CloudHSM complementa las soluciones de protección de datos existentes y le permite proteger sus claves de cifrado dentro de HSM que están diseñadas y validadas según los estándares gubernamentales para su seguridad.

gestión de claves.

CloudHSM le permite generar, almacenar y administrar de forma segura las claves criptográficas utilizadas para el cifrado de datos de manera que solo usted pueda acceder a las claves.

Un módulo de seguridad de hardware (HSM) proporciona almacenamiento seguro de claves y operaciones criptográficas dentro de un dispositivo de hardware resistente a la manipulación.

Los HSM están diseñados para almacenar de forma segura el material de clave criptográfica y utilizar el material de clave sin exponerlo fuera del límite criptográfico del hardware.

Puede utilizar el servicio CloudHSM para admitir una variedad de casos de uso y aplicaciones, como el cifrado de bases de datos, la administración de derechos digitales (DRM), la infraestructura de clave pública (PKI), la autenticación y autorización, la firma de documentos y las transacciones. Tratamiento.

Se ejecuta en un dispositivo de hardware dedicado, con un solo inquilino.

Cuando utiliza el servicio AWS CloudHSM, crea un clúster de CloudHSM.

Los clústeres pueden contener varias instancias de HSM, repartidas en varias zonas de disponibilidad de una región. Las instancias de HSM en un clúster se sincronizan automáticamente y se equilibran la carga.

Recibirá acceso dedicado de un solo inquilino a cada instancia de HSM del clúster. Cada instancia de HSM aparece como un recurso de red en su Amazon Virtual Private Cloud (VPC).

Agregar y quitar HSM de su clúster es una sola llamada a la API de AWS CloudHSM (o en la línea de comandos mediante la AWS CLI).

Después de crear e inicializar un clúster de CloudHSM, puede configurar un cliente en la instancia EC2 que permita a las aplicaciones utilizar el clúster a través de una red segura y autenticada. conexión.

Debe estar dentro de una VPC y se puede acceder a través de VPC Peering.

Las aplicaciones no necesitan estar en la misma VPC, sino en el servidor o la instancia en la que se encuentra la aplicación

y el cliente HSM que se está ejecutando debe tener accesibilidad de red (IP) a todos los HSM del clúster.

No se integra de forma nativa con muchos servicios de AWS como KMS, sino que requiere secuencias de comandos de aplicaciones personalizadas.

### AWS CLOUDHSM USE CASES

Descargue el procesamiento SSL/TLS de los servidores web.

Proteja las claves privadas de una entidad emisora de certificados (CA). Almacene la clave maestra para Oracle DB Transparent Data Encryption.

Almacén de claves personalizado para AWS KMS: conserve el control del HSM que protege las claves maestras.

### CLOUDHSM VS AWS KMS

The table below compares CloudHSM against KMS:

|  |  |  |
| --- | --- | --- |
|  | **CloudHSM** | **AWS KMS** |
| Tenancy | Single-tenant HSM | Multi-tenant AWS service |
| Availability | Customer-managed durability and available | Highly available and durable key storage and management |
| Root of Trust | Customer managed root of trust | AWS managed root of trust |
| FIPS 140-2 | Level 3 | Level 2 / Level 3 |
| 3rd Party Support | Broad 3rd Party Support | Broad AWS service support |

## AWS SECRETS MANAGER

### AWS SECRETS MANAGER FEATURES

AWS Secrets Manager le ayuda a proteger los secretos necesarios para obtener acceso a sus aplicaciones, servicios y recursos de TI.

El servicio le permite rotar, administrar y recuperar fácilmente las credenciales de la base de datos, las claves de API y otros secretos a lo largo de su ciclo de vida.

Los usuarios y las aplicaciones recuperan secretos con una llamada a las API de Secrets Manager, lo que elimina la necesidad de codificar información confidencial en texto sin formato.

Secrets Manager ofrece rotación secreta con integración integrada para Amazon RDS, Amazon Redshift y Amazon DocumentDB.

Además, el servicio es extensible a otros tipos de secretos, incluidas las claves de API y los tokens OAuth. Además, Secrets Manager le permite controlar el acceso a los secretos mediante permisos detallados y auditar la rotación de secretos de forma centralizada para los recursos en la nube de AWS, los servicios de terceros y las instalaciones.

|  |  |  |
| --- | --- | --- |
|  | **Secrets Manager** | **SSM Parameter Store** |
| Automatic Key Rotation | Yes, built-in for some services, use Lambda for others | No native key rotation; can use custom Lambda |
| Key/Value Type | String or Binary (encrypted) | String, StringList, SecureString (encrypted) |
| Hierarchical Keys | No | Yes |
| Price | Charges apply per secret | Free for standard, charges for advanced |

AWS Secrets Manager cifra los secretos en reposo mediante claves de cifrado que usted posee y almacena en AWS Key Management Service (KMS).

Cuando recupera un secreto, Secrets Manager lo descifra y lo transmite de forma segura a través de TLS a su entorno local.

Secrets Manager no escribe ni almacena en caché el secreto en el almacenamiento persistente.

Puede controlar el acceso al secreto mediante políticas detalladas de AWS Identity and Access Management (IAM) y políticas basadas en recursos.

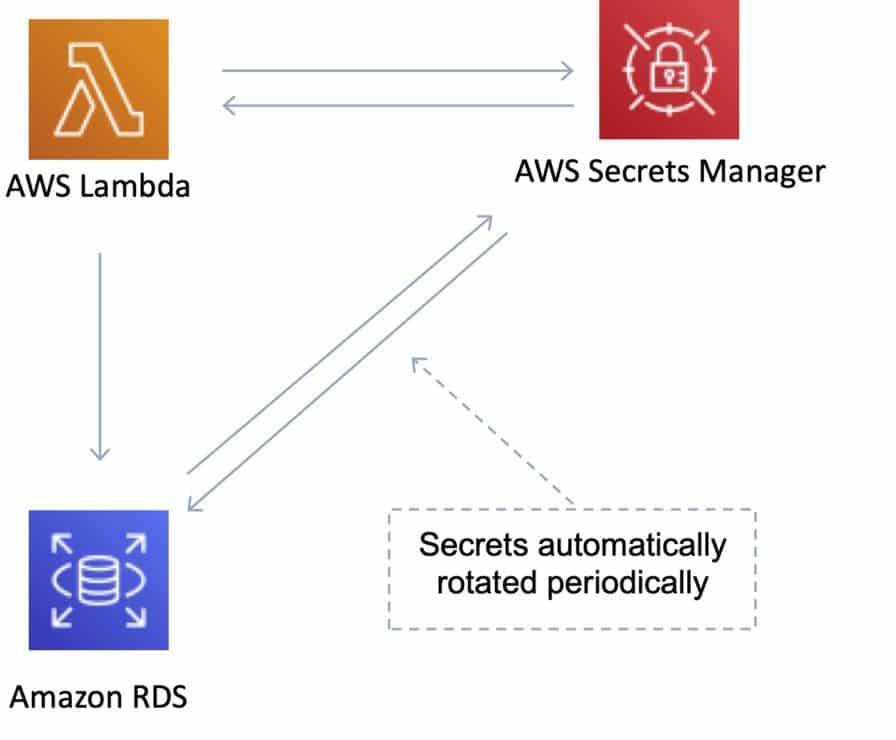
También puede etiquetar secretos individualmente y aplicar controles de acceso basados en etiquetas.

Con AWS Secrets Manager, puede rotar los secretos en una programación o bajo demanda mediante la consola de Secrets Manager, el SDK de AWS o la CLI de AWS.

Por ejemplo, para rotar una contraseña de base de datos, proporcione el tipo de base de datos, la frecuencia de rotación y las credenciales de la base de datos maestra al almacenar la contraseña en Secrets Manager.

Secrets Manager admite de forma nativa credenciales rotativas para bases de datos alojadas en Amazon RDS y Amazon DocumentDB y clústeres alojados en Amazon Redshift.

Puede ampliar Secrets Manager para rotar otros secretos modificando funciones de Lambda de ejemplo.



Puede almacenar y recuperar secretos mediante la consola de AWS Secrets Manager, AWS SDK, AWS CLI o AWS CloudFormation.

Para recuperar secretos, simplemente reemplace los secretos de texto sin formato en sus aplicaciones con código para extraer esos secretos mediante programación mediante las API de Secrets Manager. Secrets Manager proporciona ejemplos de código para llamar a las API de Secrets Manager, también disponibles en la página  [Recursos](https://aws.amazon.com/secrets-manager/resources/) de  [Secrets Manager](https://aws.amazon.com/secrets-manager/resources/).

Puede configurar puntos de enlace de Amazon Virtual Private Cloud (VPC) para mantener el tráfico entre su VPC y Secrets Manager dentro de la red de AWS.

También puede usar bibliotecas de almacenamiento en caché del lado cliente de Secrets Manager para mejorar la disponibilidad y reducir la latencia del uso de los secretos.

AWS Secrets Manager le permite auditar y supervisar secretos mediante la integración con AWS

servicios de registro, supervisión y notificación.

## AWS WAF AND SHIELD

### AWS WAF & SHIELD FEATURES

AWS WAF y AWS Shield ayudan a proteger sus recursos de AWS de exploits web y ataques DDoS.

AWS WAF es un servicio de firewall de aplicaciones web que ayuda a proteger sus aplicaciones web de vulnerabilidades comunes que podrían afectar a la disponibilidad de las aplicaciones, comprometer la seguridad o consumir recursos excesivos.

AWS Shield proporciona protección ampliada contra ataques DDoS para sus recursos de AWS. Obtenga soporte 24/7 de nuestro equipo de respuesta DDoS y visibilidad detallada de los eventos DDoS.

Ahora entraremos en más detalles sobre cada servicio.

### AWS WEB APPLICATION FIREWALL (WAF)

AWS WAF es un firewall de aplicaciones web que ayuda a proteger sus aplicaciones web de vulnerabilidades web comunes que podrían afectar a la disponibilidad de las aplicaciones, comprometer la seguridad o consumir recursos excesivos.

AWS WAF ayuda a proteger las aplicaciones web de los ataques al permitirle configurar reglas que permiten, bloquean o monitorean (cuentan) las solicitudes web en función de las condiciones que defina.

Estas condiciones incluyen direcciones IP, encabezados HTTP, cuerpo HTTP, cadenas URI, inyección SQL y secuencias de comandos entre sitios.

Puede permitir o bloquear solicitudes web basadas en cadenas que aparecen en las solicitudes mediante condiciones de coincidencia de cadenas.

Por ejemplo, AWS WAF puede hacer coincidir los valores de los siguientes elementos de solicitud:

* Encabezado: un encabezado de solicitud especificado, por ejemplo, el encabezado User-Agent o Referer.
* Método HTTP: el método HTTP, que indica el tipo de operación que la solicitud solicita al origen que realice. CloudFront admite lo siguiente
* métodos: DELETE, GET, HEAD, OPTIONS, PATCH, POST y PUT.
* Cadena de consulta: la parte de una dirección URL que aparece después de un carácter ?, si lo hay.
* URI: la ruta de acceso URI de la solicitud, que identifica el recurso, por ejemplo, /images/daily-ad.jpg.
* Cuerpo: la parte de una solicitud que contiene cualquier dato adicional que desee enviar al servidor web como cuerpo de la solicitud HTTP, como los datos de un formulario.
* Parámetro de consulta único (solo valor): cualquier parámetro que haya definido como parte de la cadena de consulta.
* Todos los parámetros de consulta (solo valores): como se mencionó anteriormente, buy inspecciona todos los parámetros dentro de la cadena de consulta.

Se pueden implementar nuevas reglas en cuestión de minutos, lo que le permite responder rápidamente a los patrones de tráfico cambiantes.

Cuando los servicios de AWS reciben solicitudes de sitios web, las solicitudes se reenvían a AWS WAF para su inspección con arreglo a reglas definidas.

Una vez que una solicitud cumple una condición definida en las reglas, AWS WAF indica al servicio subyacente que bloquee o permita la solicitud en función de la acción que defina.

Con AWS WAF solo paga por lo que utiliza.

Los precios de AWS WAF se basan en el número de reglas que implemente y en el número de solicitudes web que reciba la aplicación web.

No hay compromisos iniciales.

AWS WAF está estrechamente integrado con amazon CloudFront y los servicios application Load Balancer (ALB).

Cuando utiliza AWS WAF en Amazon CloudFront, las reglas se ejecutan en todas las ubicaciones de borde de AWS, ubicadas en todo el mundo cerca de los usuarios finales.

Esto significa que la seguridad no viene a expensas del rendimiento.

Las solicitudes bloqueadas se detienen antes de que lleguen a sus servidores web.

Cuando utiliza AWS WAF en un balanceador de carga de aplicaciones, las reglas se ejecutan en la región y se pueden utilizar para proteger los equilibradores de carga internos y orientados a Internet.

#### Web Traffic Filtering

AWS WAF le permite crear reglas para filtrar el tráfico web en función de condiciones que incluyen direcciones IP, encabezados HTTP y cuerpo, o URI personalizados.

Esto le brinda una capa adicional de protección contra ataques web que intentan explotar vulnerabilidades en aplicaciones web personalizadas o de terceros.

Además, AWS WAF facilita la creación de reglas que bloquean vulnerabilidades web comunes como la inyección SQL y las secuencias de comandos entre sitios.

AWS WAF le permite crear un conjunto centralizado de reglas que puede implementar en varios sitios web.

Esto significa que en un entorno con muchos sitios web y aplicaciones web, puede crear un único conjunto de reglas que puede reutilizar en todas las aplicaciones en lugar de volver a crear esa regla en cada aplicación que desee proteger.

#### Full feature API

AWS WAF se puede administrar completamente a través de API.

Esto proporciona a las organizaciones la capacidad de crear y mantener reglas automáticamente e incorporarlas en el proceso de desarrollo y diseño.

Por ejemplo, un desarrollador que tenga un conocimiento detallado de la aplicación web podría crear una regla de seguridad como parte del proceso de implementación.

Esta capacidad de incorporar la seguridad en su proceso de desarrollo evita la necesidad de transferencias complejas entre los equipos de aplicaciones y seguridad para asegurarse de que las reglas se mantengan actualizadas.

AWS WAF también se puede implementar y aprovisionar automáticamente con plantillas de muestra de AWS CloudFormation que le permiten describir todas las reglas de seguridad que desea implementar para sus aplicaciones web entregadas por Amazon CloudFront.

AWS WAF está integrado con Amazon CloudFront, que admite orígenes personalizados fuera de AWS:

esto significa que puede proteger los sitios web no alojados en AWS.

La compatibilidad con IPv6 permite a AWS WAF inspeccionar las solicitudes HTTP/S procedentes de direcciones IPv6 e IPv4.

#### Real-time visibility

AWS WAF proporciona métricas en tiempo real y captura solicitudes sin procesar que incluyen detalles sobre direcciones IP, ubicaciones geográficas, URI, agente de usuario y referentes.

AWS WAF está totalmente integrado con Amazon CloudWatch, lo que facilita la configuración de alarmas personalizadas cuando se superan los umbrales o se producen ataques.

Esta información proporciona información valiosa que se puede utilizar para crear nuevas reglas para proteger mejor las aplicaciones.

### AWS SHIELD

AWS Shield es un servicio de protección de denegación de servicio distribuido (DDoS) administrado que protege las aplicaciones que se ejecutan en AWS.

AWS Shield proporciona detección siempre activa y mitigaciones automáticas en línea que minimizan el tiempo de inactividad y la latencia de las aplicaciones, por lo que no es necesario contratar a AWS Support para beneficiarse de la protección DDoS.

Hay dos niveles de AWS Shield: Estándar y Avanzado.

#### AWS Shield Standard

Todos los clientes de AWS se benefician de las protecciones automáticas de AWS Shield Standard, sin cargo adicional.

AWS Shield Standard se defiende contra los ataques DDoS de capa de red y transporte más comunes y frecuentes que se dirigen a sitios web o aplicaciones.

Al utilizar AWS Shield Standard con Amazon CloudFront y Amazon Route 53, recibe una protección de disponibilidad completa contra todos los ataques de infraestructura conocidos (capa 3 y 4).

#### AWS Shield Advanced

Proporciona niveles más altos de protección contra ataques dirigidos a aplicaciones que se ejecutan en recursos de Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator y Amazon Route 53.

Además de las protecciones de la capa de red y transporte que vienen con Standard, AWS Shield Advanced proporciona detección y mitigación adicionales contra ataques DDoS grandes y sofisticados, visibilidad casi en tiempo real de los ataques e integración con AWS WAF, un firewall de aplicaciones web.

AWS Shield Advanced también le brinda acceso 24×7 a AWS DDoS Response Team (DRT) y protección contra picos relacionados con DDoS en Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator y Amazon Cargos de la ruta 53.

AWS Shield Advanced está disponible en todo el mundo en todas las ubicaciones de borde de Amazon CloudFront, AWS Global Accelerator y Amazon Route 53.

Los servidores de origen pueden ser Amazon S3, Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB) o un servidor personalizado fuera de AWS.

AWS Shield Advanced incluye protección de costos DDoS, una protección contra cargos de escalado debido a un ataque DDoS que causa picos de uso en Amazon EC2 protegido, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator o Amazon Route 53.

Si alguno de los recursos protegidos de AWS Shield Advanced se amplía en respuesta a un ataque DDoS, puede solicitar créditos a través del canal normal de AWS Support.

## AWS RESOURCE ACCESS MANAGER

### AWS RESOURCE ACCESS MANAGER FEATURES

AWS Resource Access Manager (RAM) es un servicio que le permite compartir recursos de AWS de forma fácil y segura con cualquier cuenta de AWS o dentro de su organización de AWS.

Puede compartir aws transit gateways, subredes, configuraciones de AWS License Manager y recursos de reglas de Amazon Route 53 Resolver con RAM.

La RAM elimina la necesidad de crear recursos duplicados en varias cuentas, lo que reduce la sobrecarga operativa de administrar esos recursos en cada cuenta que posee.

Puede crear recursos de forma centralizada en un entorno de varias cuentas y usar RAM para compartir esos recursos entre cuentas en tres sencillos pasos:

1. Crear un recurso compartido.
2. Especificar recursos.
3. Especificar cuentas.

La RAM está disponible sin cargo adicional.

###### Beneficios clave:

* **Reduzca la sobrecarga operativa: adquiera recursos de AWS de forma centralizada y utilice la RAM para compartir recursos como subredes o configuraciones de License Manager con otras cuentas. Esto elimina la necesidad de aprovisionar recursos duplicados en cada cuenta en un entorno de varias cuentas.**
* **Mejore la seguridad y la visibilidad: la RAM aprovecha las políticas y los permisos existentes establecidos en AWS Identity and Access Management (IAM) para controlar el consumo de recursos compartidos. La RAM también proporciona una visibilidad completa de los recursos compartidos para configurar alarmas y visualizar registros mediante la integración con Amazon CloudWatch y AWS CloudTrail.**
* **Optimizar costos: compartir recursos como configuraciones de AWS License Manager** entre cuentas le permite aprovechar las licencias en varias partes de su empresa para aumentar la utilización y optimizar los costos.

## SECURITY, IDENTITY & COMPLIANCE QUIZ QUESTIONS

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

###### Question 1:

A company needs to deploy virtual desktops for its customers in an AWS VPC, and would like to leverage their existing on-premise security principles. AWS Workspaces will be used as the virtual desktop solution.

Which set of AWS services and features will meet the company’s requirements?

1. A VPN connection. AWS Directory Services
2. A VPN connection, VPC NACLs and Security Groups
3. A VPN connection, VPC NACLs and Security Groups
4. Amazon EC2, and AWS IAM

###### Question 2:

To improve security in your AWS account you have decided to enable multi-factor authentication (MFA). You can authenticate using an MFA device in which two ways? (choose 2)

1. Locally to EC2 instances
2. Through the AWS Management Console
3. Using biometrics
4. Using a key pair
5. Using the AWS API

###### Question 3:

Your company would like to restrict the ability of most users to change their own passwords whilst continuing to allow a select group of users within specific user groups.

What is the best way to achieve this? (choose 2)

1. Under the IAM Password Policy deselect the option to allow users to change their own passwords
2. Create an IAM Policy that grants users the ability to change their own password and attach it to the groups that contain the users
3. Create an IAM Role that grants users the ability to change their own password and attach it to the groups that contain the users
4. Create an IAM Policy that grants users the ability to change their own password and attach it to the individual user accounts
5. Disable the ability for all users to change their own passwords using the AWS Security Token Service

###### Question 4:

Your company has started using the AWS CloudHSM for secure key storage. A recent administrative error resulted in the loss of credentials to access the CloudHSM. You need access to data that was encrypted using keys stored on the hardware security module.

How can you recover the keys that are no longer accessible?

1. There is no way to recover your keys if you lose your credentials
2. Log a case with AWS support and they will use MFA to recover the credentials
3. Restore a snapshot of the CloudHSM
4. Reset the CloudHSM device and create a new set of credentials

###### Question 5:

The AWS Acceptable Use Policy describes permitted and prohibited behavior on AWS and includes descriptions of prohibited security violations and network abuse. According to the policy, what is AWS's position on penetration testing?

1. AWS do not allow any form of penetration testing
2. AWS allow penetration testing by customers on their own VPC resources
3. AWS allow penetration for some resources with prior authorization
4. AWS allow penetration testing for all resources

###### Question 6:

You have been asked to come up with a solution for providing single sign-on to existing staff in your company who manage on-premise web applications and now need access to the AWS management console to manage resources in the AWS cloud.

Which product combinations provide the best solution to achieve this requirement?

1. Use your on-premise LDAP directory with IAM
2. Use IAM and MFA
3. Use the AWS Secure Token Service (STS) and SAML
4. Use IAM and Amazon Cognito

###### Question 7:

You are a Developer working for Digital Cloud Training. You are planning to write some code that creates a URL that lets users who sign in to your organization's network securely access the AWS Management Console. The URL will include a sign-in token that you get from AWS that authenticates the user to AWS. You are using Microsoft Active Directory Federation Services as your identity provider (IdP) which is compatible with SAML 2.0.

Which of the steps below will you need to include when developing your custom identity broker? (choose 2)

1. Generate a pre-signed URL programmatically using the AWS SDK for Java or the AWS SDK for.NET
2. Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user
3. Delegate access to the IdP through the "Configure Provider" wizard in the IAM console
4. Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token
5. Assume an IAM Role through the console or programmatically with the AWS CLI, Tools for Windows PowerShell or API

###### Question 8:

A health club is developing a mobile fitness app that allows customers to upload statistics and view their progress. Amazon Cognito is being used for authentication, authorization and user management and users will sign-in with Facebook IDs.

In order to securely store data in DynamoDB, the design should use temporary AWS credentials. What feature of Amazon Cognito is used to obtain temporary credentials to access AWS services?

1. User Pools
2. Identity Pools
3. SAML Identity Providers
4. Key Pairs

### SECURITY, IDENTITY & COMPLIANCE - ANSWERS

###### Question 1 answer: A

Explanation:

A security principle is an individual identity such as a user account within a directory. The AWS Directory service includes: Active Directory Service for Microsoft Active Directory, Simple AD, AD Connector. One of these services may be ideal depending on detailed requirements. The Active Directory Service for Microsoft AD and AD Connector both require a VPN or Direct Connect connection.

A VPN with NACLs and security groups will not deliver the required solution. AWS Directory Service with IAM or EC2 with IAM are also not sufficient for leveraging on-premise security principles. You must have a VPN.

###### Question 2 answer: A,E

Explanation:

You can authenticate using an MFA device in the following ways:

* Through the AWS Management Console – the user is prompted for a user name, password and authentication code
* Using the AWS API – restrictions are added to IAM policies and developers can request temporary security credentials and pass MFA parameters in their AWS STS API requests
* Using the AWS CLI by obtaining temporary security credentials from STS (aws sts get- session-token)

###### Question 3 answer: A,B

Explanation:

A password policy can be defined for enforcing password length, complexity etc. (applies to all users).

You can allow or disallow the ability to change passwords using an IAM policy and you should attach this to the group that contains the users, not to the individual users themselves.

You cannot use an IAM role to perform this function.

The AWS STS is not used for controlling password policies.

###### Question 4 answer: A

Explanation:

Amazon does not have access to your keys or credentials and therefore has no way to recover your keys if you lose your credentials.

###### Question 5 answer: C

Explanation:

Permission is required for all penetration tests.

You must complete and submit the AWS Vulnerability / Penetration Testing Request Form to request authorization for penetration testing to or originating from any AWS resources.

There is a limited set of resources on which penetration testing can be performed.

###### Question 6 answer: C

Explanation:

Single sign-on using federation allows users to login to the AWS console without assigning IAM

credentials.

The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (such as federated users from an on-premise directory).

Federation (typically Active Directory) uses SAML 2.0 for authentication and grants temporary access based on the users AD credentials. The user does not need to be a user in IAM.

You cannot use your on-premise LDAP directory with IAM, you must use federation. Enabling multi-factor authentication (MFA) for IAM is not a federation solution.

Amazon Cognito is used for authenticating users to web and mobile apps not for providing single sign-on between on-premises directories and the AWS management console.

###### Question 7 answer: B,D

Explanation:

The aim of this solution is to create a single sign-on solution that enables users signed in to the organization's Active Directory service to be able to connect to AWS resources. When developing a custom identity broker you use the AWS STS service.

The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users). The steps performed by the custom identity broker to sign users into the AWS management console are:

1. Verify that the user is authenticated by your local identity system
2. Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user
3. Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token
4. Construct a URL for the console that includes the token
5. Give the URL to the user or invoke the URL on the user's behalf

You cannot generate a pre-signed URL for this purpose using SDKs, delegate access through the IAM console or directly assume IAM roles.

###### Question 8 answer: B

Explanation:

With an identity pool, users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 and DynamoDB.

A user pool is a user directory in Amazon Cognito. With a user pool, users can sign in to web or mobile apps through Amazon Cognito, or federate through a third-party identity provider (IdP).

SAML Identity Providers are supported IDPs for identity pools but cannot be used for gaining temporary credentials for AWS services.

Key pairs are used in Amazon EC2 for access to instances.