Guía del administrador

Amazon Nimble Studio

Amazon Nimble Studio: Guía del administrador

Table of Contents

¿Qué es Nimble Studio? 1
Características y ventajas 1
Aplicaciones relacionadas 2
Precio de Nimble Studio 2
Primeros pasos con Nimble Studio 3
Conceptos y terminología 4
Características principales 4
Conceptos y terminología clave 5
Configuración 8
Configurar IAM 8
Registro para obtener una Cuenta de AWS 8
Crear un usuario administrativo 9
Recursos relacionados 10
Introducción 11
Configuración rápida 11
Paso 1: configure la infraestructura del estudio 11
Paso 2: revise y cree su estudio. 12
Ajustes adicionales 13
Configure el rol de usuario del estudio 13
AWS IAM Identity Center 14
Configure la clave de cifrado AWS KMS 14
Configurar etiquetas 15
Eliminar un estudio 16
Seguridad 17
Más información 17
Seguridad de la cuenta 18
Elimine las claves de acceso de su cuenta 18
Habilite la autentificación multifactor 18
Habilitar CloudTrail en todos Regiones de AWS 19
Configurar Amazon GuardDuty y las notificaciones 19
Protección de datos 22
Cifrado en reposo 23
Cifrado en tránsito 24
Administración de claves para Amazon Nimble Studio 25

Medidas de seguridad de los datos ... 26
Datos y métricas de diagnóstico ... 26
Identity and Access Management ... 27
Público ... 27
Autenticación con identidades ... 28
Administración de acceso mediante políticas ... 31
Cómo funciona Amazon Nimble Studio con IAM ... 33
Ejemplo de políticas basadas en identidad ... 40
AWS políticas gestionadas ... 41
Prevención de la sustitución confusa entre servicios ... 51
Solución de problemas ... 53
Registro y monitorización ... 56
Registrar llamadas de Nimble Studio mediante AWS CloudTrail ... 56
Validación de conformidad ... 62
Seguridad de la infraestructura ... 63
Prácticas recomendadas de seguridad ... 64
Monitoreo ... 64
Protección de datos ... 64
Permisos ... 65
Soporte ... 66
Foro de Nimble Studio ... 66
Soporte para aplicaciones ... 66
AWSThinkboxDeadline ... 66
Nimble Studio File Transfer ... 66
AWS Support Center ... 66
AWS Support Plans ... 67
Historial de documentos ... 68
Glosario de AWS ... 69
... lxx

¿Qué es Amazon Nimble Studio?

Nimble Studio proporciona infraestructura y administración centralizada para un conjunto de aplicaciones y servicios que los artistas pueden usar para producir contenido de efectos visuales, animaciones y juegos en la nube.

Con Nimble Studio, dispondrá de las herramientas esenciales para la gestión de usuarios y grupos. También puede añadir y gestionar aplicaciones, incluida AWS Thinkbox y Nimble Studio File Transfer.

Nimble Studio presenta una interfaz unificada que coloca todos los recursos de su estudio en un solo lugar. Puede incorporar usuarios, asignar aplicaciones y adjuntar permisos específicos a su función laboral. Nimble Studio no requiere experiencia en AWS y puede configurarlo en unos cinco minutos.

Contenido

- Características y ventajas
- Aplicaciones relacionadas
- Precio de Nimble Studio
- Primeros pasos con Nimble Studio

Características y ventajas

Estas son algunas de las características y ventajas que ofrece Nimble Studio:

- Use Nimble Studio sin coste alguno; pague solo por los recursos de estudio que utilizan sus aplicaciones.
- Gestione su estudio de forma centralizada, compruebe su estado y obtenga información de alto nivel sobre su funcionamiento.
- Agregue y administre aplicaciones, usuarios y grupos de Nimble Studio, y adjunte permisos.
- Gestione de forma segura el acceso a los recursos del estudio con políticas y funciones AWS Identity and Access Management (IAM).
- Gestione la seguridad de inicio de sesión para los usuarios de Studio y los proveedores de identidad externos con AWS IAM Identity Center (IAM Identity Center).
- Organice y busque fácilmente los recursos del estudio con etiquetas para los recursos de su estudio.

Aplicaciones relacionadas

Nimble Studio ofrece aplicaciones para que los creadores de contenido digital gestionen un estudio basado en la nube para producir efectos visuales (VFX), animaciones y contenido interactivo.

Puede instalar estas aplicaciones en su ordenador local o en la nube con una instancia de Amazon Elastic Compute Cloud (Amazon EC2). También puede utilizar Amazon Simple Storage Service (Amazon S3) para transferir y almacenar activos multimedia digitales de forma segura. Esto significa que puede usar Nimble Studio para reducir los costos de infraestructura física, equipo y personal técnico.

Actualmente, Nimble Studio ofrece las siguientes aplicaciones:

- AWS Thinkbox: el software Thinkbox incluye la Thinkbox de administrador de granjas de renderizado Deadline y el complemento 3D, Krakatoa Thinkbox. Puede utilizar un software Thinkbox que le ayude a aumentar la producción creativa de su estudio en las instalaciones, en la nube con Amazon EC2 o una combinación de ambos. Para obtener más información, consulte Productos AWS Thinkbox.
- Nimble Studio File Transfer: File Transfer acelera las transferencias de activos multimedia de activos multimedia digitales desde y hacia Amazon S3. File Transfer proporciona una interfaz gráfica de usuario que puede utilizar para mover rápidamente miles de archivos multimedia de gran tamaño. Para obtener más información, consulte la página ¿Qué es Nimble Studio File Transfer?

Precio de Nimble Studio

Configurar Nimble Studio y usarlo para administrar la infraestructura, los usuarios, la seguridad y los servicios de su estudio es gratuito.

Sin embargo, si configura servicios y aplicaciones en su estudio, es posible que le cobren por el almacenamiento y otros recursos del estudio. Para obtener más información sobre los precios de las aplicaciones de Nimble Studio, consulte la página de precios de cada aplicación.

Para obtener información sobre los costo de admnistración de AWS, consulte AWS Cost Explorer Service y AWS Budgets.

Primeros pasos con Nimble Studio

La configuración y la implementación de Nimble Studio tardan unos cinco minutos.

Una vez que se haya familiarizado con los conceptos y la terminología de Nimble Studio, consulte Introducción a Amazon Nimble Studio. Allí encontrará instrucciones paso a paso para implementar su estudio.

Conceptos y terminología de Amazon Nimble Studio

Para ayudarle a empezar a utilizar Amazon Nimble Studio y a entender cómo funciona, puede consultar los conceptos y la terminología clave de esta guía.

Características principales

Amazon Nimble Studio

Amazon Nimble Studio es un Servicio de AWS que permite a los estudios creativos producir efectos visuales, animaciones y contenido interactivo completamente en la nube, desde el boceto del guion gráfico hasta la entrega final.

Consola Amazon Nimble Studio

La consola Nimble Studio es una parte de la AWS Management Console que está dedicada a nuestros clientes de TI administrativos. En esta consola, los administradores crean su estudio en la nube y administran muchos ajustes. Por ejemplo, la página del administrador de Studio le permite añadir o eliminar recursos, añadir aplicaciones y conceder permisos a usuarios y grupos.

Portal de Amazon Nimble Studio

El portal de Nimble Studio proporciona una interfaz de usuario para las interacciones diarias con las aplicaciones y los servicios de Nimble Studio. Los usuarios inician sesión directamente en el portal con su nombre de usuario y contraseña sin tener que interactuar con la AWS Management Console.

Nimble Studio File Transfer

File Transfer acelera las transferencias de activos multimedia de activos multimedia digitales desde y hacia Amazon Simple Storage Service (Amazon S3). File Transfer proporciona una interfaz gráfica de usuario que puede utilizar para mover rápidamente miles de archivos multimedia de gran tamaño. Para obtener más información, consulte la página ¿Qué es Nimble Studio File Transfer?

AWS Thinkbox

El software Thinkbox incluye el administrador de granjas de renderizado Thinkbox Deadline y el complemento 3D, Thinkbox Krakatoa. Puede utilizar un software Thinkbox que le ayude a aumentar la producción creativa de su estudio in situ, en la nube con Amazon EC2 o una combinación de ambos. Para obtener más información, consulte ProductosAWS Thinkbox.

Conceptos y terminología clave

Políticas administradas por AWS

Una política administrada por AWS es una política independiente creada y administrada por AWS. Política independiente significa que la política tiene su propio Nombre de recurso de Amazon (ARN) que incluye el nombre de la política. Por ejemplo, arn:aws:iam: :aws:policy/IAMReadOnlyAccess es una política administrada por AWS. Para obtener más información sobre los ARN, consulte ARN de IAM.

Las políticas gestionadas AWS se utilizan para conceder permisos a funciones laborales comunes. Las políticas de la función de trabajo es que se mantienen y actualizan por AWS como nuevos servicios y operaciones de la API. Por ejemplo, la función de trabajo AdministratorAccess proporciona acceso completo y delegación de permisos a cada servicio y recurso de AWS. Por el contrario, las políticas gestionadas AWS de acceso parcial, como AmazonMobileAnalyticsWriteOnlyAccess y AmazonEC2ReadOnlyAccess, pueden proporcionar niveles específicos de acceso sin permitir el acceso total Servicios de AWS. Para obtener más información sobre los niveles de acceso, consulte Descripción de los resúmenes de nivel de acceso en los resúmenes de políticas.

AWS Management Console

La AWS Management Console es una aplicación web que engloba y hace referencia a un amplio conjunto de consolas de servicios para la administración de Servicios de AWS.

Cada servicio también incluye su propia consola. Estas consolas ofrecen una amplia gama de herramientas para la computación en la nube. Incluso hay un servicio que ayuda a gestionar la facturación y los costes.

AWS IAM Identity Center (IAM Identity Center)

IAM Identity Center es un servicio AWS que facilita la administración centralizada del acceso a múltiples Cuentas de AWS y aplicaciones empresariales. Con IAM Identity Center, puede proporcionar a los usuarios un acceso de inicio de sesión único a todas sus cuentas y aplicaciones asignadas desde un solo lugar. También puede gestionar de forma centralizada el acceso a varias cuentas y los permisos de usuario a todas sus cuentas AWS Organizations. Para obtener más información, visite AWS IAM Identity Center FAQs.

AWSPrivateLink

AWSPrivateLink proporciona conectividad privada entre las VPC Servicios de AWS y las redes locales, sin exponer el tráfico a la Internet pública. AWS PrivateLink facilita la conexión de servicios entre diferentes cuentas y VPC. AWS PrivateLink está disponible por una cuota mensual que se facturará a su cuenta Cuenta de AWS.

Creación de contenido digital (DCC)

La creación de contenido digital (DCC) se refiere a la categoría de aplicaciones que se utilizan para producir contenido creativo, incluidas Blender, Nuke, Maya, y Houdini.

Regiones

Nimble Studio ofrece once Regiones de AWS entre las que elegir para implementar su estudio. Las regiones son donde existe la infraestructura de estudio esencial, como sus datos y aplicaciones.

La región debe estar ubicada más cerca de los usuarios de su estudio. Esto reduce el retraso y mejora las velocidades de transferencia de datos.

Estudio

Un estudio es el contenedor de nivel superior para otros recursos relacionados con Nimble Studio. Su estudio en la nube administra el portal web de Nimble Studio y las conexiones a los recursos esenciales que tiene en su Cuenta de AWS, como su VPC, su directorio de usuarios y las claves de cifrado de almacenamiento.

Aplicaciones de estudio

Los componentes de estudio son configuraciones del Nimble Studio de un cliente que indican al servicio cómo acceder a recursos como los sistemas de archivos, los servidores de licencias y las granjas de renderizado del cliente en su Cuenta de AWS.

Nimble Studio contiene varios subtipos de componentes de estudio, como un sistema de archivos compartidos, una granja de cómputos, Active Directory y un componente de licencia. Estos subtipos describen los recursos que le gustaría que usara su estudio.

Recursos de estudio

Recursos de estudio es un término que resume las cosas que un estudio necesita en sus operaciones diarias. Al describir cómo se integran los recursos en la infraestructura de un estudio en la nube, también se los puede denominar componentes de estudio.

Etiquetas

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional definido por usted.

Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras. Por ejemplo, podría definir un conjunto de etiquetas para las instancias Amazon Elastic Compute Cloud (Amazon EC2) de su cuenta que le ayude a realizar un seguimiento del propietario y el nivel de la pila de cada instancia. Las etiquetas también le permiten integrar los sistemas de archivos compartidos y las granjas de renderizado de su organización con Nimble Studio, para mantener sus flujos de trabajo ininterrumpidos mientras traslada sus empleados a la nube.

Con las etiquetas, puede clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Esto es útil cuando tiene muchos recursos del mismo tipo: puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado.

Configuración de Nimble Studio

Este tutorial es para usuarios administradores que desean configurar un Amazon Nimble Studio.

Las siguientes secciones le guiarán por los pasos que debe completar antes de implementar un estudio en Nimble Studio.

Contenido

- Configurar IAM
- Recursos relacionados

Configurar IAM

Revise la siguiente documentación AWS Identity and Access Management (IAM) antes de empezar.

- Security best practices in IAM (Prácticas recomendadas de seguridad en IAM)
- Inicie sesión en su Cuenta de AWS como usuario administrador para completar el resto de la configuración.

Registro para obtener una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Cómo registrarse en una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para realizar tareas que requieran acceso de usuario raíz.

AWS le enviará un correo electrónico de confirmación luego de completar el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Crear un usuario administrativo

Después de registrarse para obtener una Cuenta de AWS, proteja su Usuario raíz de la cuenta de AWS, habilite AWS IAM Identity Center y cree un usuario administrativo para no utilizar el usuario raíz en las tareas cotidianas.

Protección de su Usuario raíz de la cuenta de AWS

1. Inicie sesión en la AWS Management Console como propietario de cuenta, elija Usuario raíz e ingrese el email de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In.
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario raíz de la Cuenta de AWS (consola) en la Guía del usuario de IAM.

Crear un usuario administrativo

1. Activar IAM Identity Center

   Para ver las instrucciones, consulte Habilitación de AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.
2. En IAM Identity Center, conceda acceso administrativo a un usuario administrativo.

   Para ver un tutorial sobre el uso del Directorio de IAM Identity Center como origen de identidades, consulte Configuración del acceso de los usuarios con el Directorio de IAM Identity Center predeterminado en la Guía del usuario de AWS IAM Identity Center.

Cómo iniciar sesión como usuario administrativo

- Para iniciar sesión con el usuario del IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario del Centro de identidades de IAM.

Para obtener ayuda para iniciar sesión con un usuario del IAM Identity Center, consulte Iniciar sesión en el portal de acceso de AWS en la Guía del usuario de AWS Sign-In.

Recursos relacionados

- Prácticas recomendadas de seguridad en IAM
- Cuotas de Servicio de AWSReferencia general de AWS

Introducción a Amazon Nimble Studio

En este capítulo se muestra cómo usar la consola de Nimble Studio para crear la infraestructura de su estudio, confirmar la Región de AWS, revisar los ajustes y crear su estudio. También puede personalizar la configuración con ajustes adicionales.

Para los clientes primerizos de AWS, consulte los tutoriales Configuración de Nimble Studio.

Temas

- Configurar Nimble Studio
- Ajustes de estudio adicional

Configurar Nimble Studio

Esta guía le muestra cómo configurar su infraestructura, revisar los ajustes y crear su estudio. También puede personalizar su estudio con Ajustes de estudio adicional.

Paso 1: configure la infraestructura del estudio

La infraestructura de su estudio consta de los siguientes componentes:

- Nombre para mostrar del estudio: el nombre para mostrar del estudio es la forma en que puede identificar su estudio, por ejemplo, AnyCompany Studio. El nombre de su estudio también determina su URL del portal del estudio. Puede cambiar el Nombre para mostrar del estudio en cualquier momento una vez que haya completado la configuración.
- URL del portal del estudio: puede acceder a su estudio mediante la URL del portal del estudio. La URL se basa en el nombre para mostrar del estudio, por ejemplo, https://anycompanystudio.awsapps.com. Puede cambiar la URL del portal del estudio en cualquier momento una vez que haya completado la configuración.
- Región de AWS: La Región de AWS es la ubicación física de un conjunto de centros de datos AWS. Cuando configura su estudio, la región elige de forma predeterminada su ubicación más cercana. Debe cambiar la región para que esté más cerca de sus usuarios. Esto reduce el retraso y mejora las velocidades de transferencia de datos.

> **Important**
>
> No podrá cambiar su región una vez haya terminado de configurar Nimble Studio.

Complete las tareas de esta sección para configurar la infraestructura de su estudio.

Para configurar la infraestructura de su estudio

1. Inicie sesión en la AWS Management Console de Nimble Studio y ábrala.
2. Seleccione Configurar Nimble Studio y, a continuación, seleccione Siguiente.
3. Escriba el nombre para mostrar del estudio, por ejemplo**`AnyCompany Studio`**.
4. (Opcional) Para cambiar el nombre del portal del estudio, seleccione Editar URL.
5. (Opcional) Para cambiar la Región de AWS de forma que esté más cerca de los usuarios de su estudio, seleccione Cambiar región.
   a. Elija la región que esté más próxima a la mayoría de los usuarios.
   b. Elija Añadir región.
6. (Opcional) Para personalizar aún más la configuración del estudio, seleccione Ajustes de estudio adicional.
7. Para revisar la configuración antes de crear el estudio, seleccione Siguiente.

Paso 2: revise y cree su estudio.

Tras configurar la infraestructura del estudio, puede revisarla, realizar cambios y crear su estudio.

Para revisar y crear su estudio

1. En la página Revisar y crear, revise la infraestructura de su estudio.
2. Confirme que la Región de AWS es la más cercana a los usuarios de su estudio.
3. (Opcional) Seleccione Editar para realizar cambios en la configuración de su estudio.
4. Cuando haya terminado, elija Crear estudio.

Ajustes de estudio adicional

La configuración de Nimble Studio incluye ajustes de estudio adicionales. Con estos ajustes, puede ver todos los cambios que la configuración de Nimble Studio realiza en su Cuenta de AWS, configurar su rol de usuario en el estudio y cambiar el tipo de clave de cifrado. También puede añadir etiquetas opcionales a los recursos de su estudio.

Configure el rol de usuario del estudio

Un servicio AWS puede adoptar un rol de servicio para realizar acciones en su nombre. Nimble Studio requiere un rol de usuario de estudio para que los usuarios puedan acceder a los recursos de su estudio.

Puede adjuntar políticas gestionadas AWS Identity and Access Management (IAM) al rol de usuario del estudio. Las políticas permiten a los usuarios realizar determinadas acciones, como crear trabajos en una aplicación específica de Nimble Studio. Como las aplicaciones dependen de condiciones específicas de la política administrada, si no usa las políticas administradas, es posible que la aplicación no funcione como se espera.

Puede cambiar el rol de usuario del estudio en cualquier momento una vez que haya completado la configuración. Para obtener más información sobre los roles, consulte Roles de IAM.

Las siguientes pestañas contienen instrucciones para dos casos prácticos diferentes. Para crear y utilizar un nuevo rol de servicio, elija la pestaña New service rol (Nueva característica de servicio). Para usar un rol de servicio existente, seleccione la pestaña Existing service rol (Rol de servicio existente).

New service role

Para crear y usar un nuevo rol de servicio

1. Seleccione Create and use a new service role (Crear y usar un nuevo rol de servicio).
2. (Opcional) Escriba un nombre Service user role (Rol de servicio).
3. Seleccione View permission details (Ver detalles del permiso) para obtener más información sobre el rol.

Existing service role

Para usar un rol de servicio existente

1. Seleccione Use an existing service role (Usar un rol de servicio existente).
2. Abra la lista desplegable para elegir un rol de servicio existente.
3. (Opcional) Seleccione View in IAM console (Ver en la consola de IAM) para obtener más información sobre el rol.

AWS IAM Identity Center

AWS IAM Identity Center es un servicio de inicio de sesión único basado en la nube para administrar usuarios y grupos. El IAM Identity Center también se puede integrar con el proveedor de inicio de sesión único (SSO) empresarial para que los usuarios puedan iniciar sesión con la cuenta de su empresa.

Nimble Studio habilita el IAM Identity Center de forma predeterminada y es necesario para configurar y usar Nimble Studio. Para obtener más información, consulte ¿Qué es AWS IAM Identity Center?

Configure la clave de cifrado AWS KMS

Las claves AWS Key Management Service (AWS KMS) son el tipo principal de clave KMS que puede utilizar para cifrar, descifrar y volver a cifrar datos.

Nimble Studio incluye los siguientes tipos de claves de cifrado AWS KMS:

- Clave de propiedad AWS: las claves de propiedad AWS son claves KMS que el Servicio de AWS posee y administra para su uso en varias cuentas Cuentas de AWS. Las claves de propiedad AWS no están en su Cuenta de AWS, pero Nimble Studio puede usar una clave de propiedad AWS para proteger los recursos de su cuenta.

  Para usar AWS KMS, no es necesario crear ni mantener la clave ni su política de claves. El uso de claves de propiedad AWS es gratuito y no se descuenta de las cuotas AWS KMS que tenga para su Cuenta de AWS.
- AWS KMSClave administrada por el cliente: una clave administrada por el cliente es una clave KMS en su Cuenta de AWS que usted ha creado, posee y administra.

  Usted tiene el control total sobre estas claves KMS. Las claves administradas por el cliente conllevan una cuota mensual. También se les aplica una tarifa por cada solicitud de API para AWS KMS más allá del nivel gratuito. Para obtener más información acerca de los precios de AWS KMS, consulte Precios de AWS Key Management Service.

Una vez finalizada la configuración, el tipo de clave de cifrado no se puede cambiar. Para obtener más información sobre AWS KMS y los tipos de claves de cifrado, consulte la documentaciónAWS KMS.

Para elegir un tipo de clave de cifrado diferente

1. Seleccione Elegir una clave AWS KMS diferente (avanzada).
2. Seleccione una clave AWS KMS o escriba un número de recurso de Amazon (ARN).
3. Elija Crear clave AWS KMS.

Configurar etiquetas

Las etiquetas actúan como etiquetas para organizar los recursos de Nimble Studio. Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos.

Cada etiqueta consta de dos partes, que usted define: una clave de etiqueta y un valor de etiqueta opcional, por ejemplo, clave: `domain` y valor:`anycompanystudio.com`.

Puede agregar o eliminar etiquetas una vez que haya completado la configuración, en cualquier momento. Para obtener más información acerca de las etiquetas, consulte Etiquetar sus recursosAWS.

Para añadir etiquetas a los recursos de su estudio

1. Elija Add new tag (Agregar nueva etiqueta).
2. Ingrese la Key (Clave) de la etiqueta.
3. (Opcional) Ingrese el Value (Valor) de la etiqueta.

Eliminar un estudio

Si ya no necesita un estudio, puede eliminarlo. Al eliminar el estudio, solo se elimina la infraestructura del estudio. Los demás recursos AWS, como las funciones de los usuarios, las políticas y los datos de las aplicaciones, permanecen intactos.

> **Important**
>
> No puede recuperar un estudio después de eliminarlo.

Para eliminar su estudio

1. Inicie sesión en la consola AWS Management Console de Nimble Studio y ábrala.
2. Seleccione Descripción general de estudio.
3. Seleccione Acciones y, a continuación, elija Eliminar estudio.
4. Escriba **`delete`** y luego elija Eliminar.

Seguridad en Amazon Nimble Studio

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener información sobre los programas de conformidad que se aplican a Amazon Nimble Studio, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

> **Important**
>
> Se recomienda encarecidamente que lea y se familiarice con el pilar de seguridad: AWS Well-Architected Framework. Este artículo contiene los principios clave para proteger su infraestructura. AWS

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida a la hora de utilizar Nimble Studio. Los siguientes temas le mostrarán cómo configurar Nimble Studio para satisfacer sus objetivos de seguridad y de conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus Nimble Studio recursos.

Más información

- Pilar de seguridad: AWS Well-Architected Framework
- Seguridad para el AWS Cloud Development Kit (AWS CDK) (AWS CDK)

- Seguridad en Amazon Virtual Private Cloud
- Credenciales de seguridad de AWS
- Seguridad en Amazon EC2
  - Linux
  - Windows

Configure la seguridad Cuenta de AWS

Esta guía muestra cómo configurarlo Cuenta de AWS para recibir notificaciones cuando sus recursos se vean comprometidos y permitir que Cuenta de AWS usuarios específicos accedan a ellos. Para proteger tus recursos Cuenta de AWS y hacer un seguimiento de ellos, sigue estos pasos.

Contenido

- Elimine las claves de acceso de su cuenta
- Habilite la autentificación multifactor
- Habilitar CloudTrail en todos Regiones de AWS
- Configurar Amazon GuardDuty y las notificaciones

Elimine las claves de acceso de su cuenta

Puedes permitir el acceso programático a tus AWS recursos desde AWS Command Line Interface (AWS CLI) o mediante las AWS API. Sin embargo, te AWS recomienda no crear ni usar las claves de acceso asociadas a tu cuenta raíz para el acceso programático.

Si aún tiene claves de acceso, se recomienda eliminarlas y crear un usuario. A continuación, conceda a ese usuario solo los permisos necesarios para las API a las que piensa llamar. Puede usar a ese usuario para emitir claves de acceso.

Para obtener más información, consulte Administrar claves de acceso para su Cuenta de AWS en la Guía de usuario de Referencia general de AWS .

Habilite la autentificación multifactor

La autenticación multifactor (MFA) es una capacidad de seguridad que proporciona una capa de autenticación además del nombre de usuario y la contraseña.

La MFA funciona de la siguiente manera: después de iniciar sesión con su nombre de usuario y contraseña, también debe proporcionar información adicional a la que solo usted tiene acceso físico. Esta información puede provenir de un dispositivo de hardware MFA dedicado o de una aplicación de un teléfono.

Debe seleccionar el tipo de dispositivo MFA que desea usar de la lista de dispositivos MFA compatibles. En el caso de un dispositivo de hardware, mantenga el dispositivo MFA en un lugar seguro.

Si utiliza un dispositivo MFA virtual (como una aplicación de teléfono), piense en lo que podría suceder si su teléfono se pierde o se daña. Una opción consiste en mantener el dispositivo MFA virtual que utilice en un lugar seguro. Otra opción es activar más de un dispositivo al mismo tiempo o utilizar una opción de MFA virtual para recuperar la clave del dispositivo.

Para obtener más información, consulte Habilitación de un dispositivo de autenticación multifactor (MFA) virtual .

Recursos relacionados

- Cómo empezar con la autenticación multifactor
- Protección del acceso al AWS uso de MFA

Habilitar CloudTrail en todos Regiones de AWS

Puede realizar un seguimiento de toda la actividad de sus AWS recursos utilizando AWS CloudTrail. Te recomendamos que los enciendas CloudTrail ahora. Esto puede ayudar a AWS Support su arquitecto de AWS soluciones a solucionar un problema de seguridad o configuración más adelante.

Para activar todos los CloudTrail registros Regiones de AWS, consulta AWS CloudTrail Actualizar: activar en todas las regiones y utilizar varias rutas.

Para obtener más información CloudTrail, consulta Activar CloudTrail: registrar la actividad de la API en tu Cuenta de AWS. Para obtener información sobre cómo CloudTrail monitorea Nimble Studio, consultaRegistrar llamadas de Nimble Studio mediante AWS CloudTrail.

Configurar Amazon GuardDuty y las notificaciones

Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa lo siguiente:

- Origen de datos
- Registros de flujo de Amazon VPC
- AWS CloudTrail registros de eventos de administración
- CloudTrail registros de eventos de datos de S3
- Registros de DNS

Amazon GuardDuty identifica las actividades inesperadas, potencialmente no autorizadas y maliciosas en su AWS entorno. Esto puede incluir problemas como escalado de privilegios, uso de credenciales expuestas o la comunicación con direcciones IP, URL o dominios malintencionados. Para identificar estas actividades, GuardDuty utiliza fuentes de inteligencia sobre amenazas, como listas de direcciones IP y dominios maliciosos, y aprendizaje automático. Por ejemplo, GuardDuty puede detectar instancias de Amazon EC2 comprometidas que sirven malware o minan bitcoins.

GuardDuty también monitorea el comportamiento de Cuenta de AWS acceso en busca de señales de peligro. Esto incluye las implementaciones de infraestructura no autorizadas, como las instancias implementadas en una infraestructura Región de AWS que nunca se ha utilizado. También incluye llamadas a la API poco habituales, como un cambio en la política de contraseñas para reducir la seguridad de las contraseñas.

GuardDuty le informa del estado de su AWS entorno mediante la generación de datos de seguridad. Puedes ver estos resultados en la GuardDuty consola o a través de CloudWatch los eventos de Amazon.

Configuración de un punto de conexión y un tema de Amazon SNS

Siga las instrucciones del tutorial Configurar un tema de Amazon SNS y un punto de conexión.

Organiza un EventBridge evento para recopilar GuardDuty los resultados

Cree una regla para EventBridge enviar eventos para todos los hallazgos que se GuardDuty generen.

Para crear un EventBridge evento para los GuardDuty hallazgos

1. Inicia sesión en la EventBridge consola de Amazon: https://console.aws.amazon.com/events/
2. En el panel de navegación, seleccione Reglas. A continuación, elija Crear regla.
3. Escriba un Nombre y la Descripción de la nueva regla. A continuación, elija Next.

4. Deja AWS los eventos o eventos EventBridge asociados seleccionados en la fuente del evento.
5. En Patrón de eventos, elija los servicios AWS para la fuente del evento. A continuación, GuardDutypara los AWS servicios y GuardDuty Finding para el tipo de evento. Este es el tema que creó en Configuración de un punto de conexión y un tema de Amazon SNS.
6. Elija Siguiente.
7. Para Destino 1, seleccione el servicio de AWS . Elija el tema SNS en el menú desplegable Seleccione un destino. A continuación, elige tu tema de GuardDuty_to_email.
8. En la sección Ajustes adicionales, en Configurar entrada de destino, elija Transformador de entrada. Elija Configurar transformador de entrada.
9. Escriba el siguiente código en el campo Ruta de entrada de la sección Transformador de entrada de destino.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

10. Para formatear el correo electrónico, escriba el siguiente código en el campo Plantilla.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type <Finding_Type>
 in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id=<Finding_ID>"
```

11. Seleccione Crear. A continuación, elija Siguiente.
12. (Opcional) Añade etiquetas si las utilizas para hacer un seguimiento de tus recursos. AWS
13. Elija Siguiente.
14. Revise su regla. A continuación, elija Crear regla.

Ahora que has configurado tu Cuenta de AWS seguridad, puedes conceder acceso a usuarios específicos y recibir notificaciones cuando tus recursos se vean comprometidos.

Protección de los datos en Amazon Nimble Studio

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos enAmazon Nimble Studio. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja Nimble Studio o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o

diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

El modelo de responsabilidad AWS compartida se aplica a la protección de datos en Amazon Nimble Studio. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye las tareas de configuración y administración de la seguridad Servicios de AWS que utilice.

Para obtener más información sobre la privacidad de datos, consulte Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en la Unión Europea, visite el Centro del RGPD.

Cifrado en reposo

Nimble Studio protege los datos confidenciales del estudio cifrándolos en reposo mediante claves de cifrado almacenadas en AWS Key Management Service (AWS KMS). El cifrado en reposo está disponible en todos los Regiones de AWS lugares donde esté disponible Nimble Studio. Los datos de estudio que ciframos incluyen el nombre y las descripciones de todos los tipos de recursos, así como los scripts de los componentes del estudio, los parámetros de los scripts, los puntos de montaje, los nombres de los recursos compartidos y otros datos.

El cifrado de datos significa que ningún usuario o aplicación podrá leer los datos confidenciales guardados en los discos sin una clave válida. Los datos cifrados se pueden almacenar de forma segura en reposo y solo puede descifrarlos una persona con acceso autorizado a la clave gestionada.

Para obtener información sobre cómo utiliza Nimble Studio AWS KMS para cifrar los datos en reposo, consulte. Administración de claves para Amazon Nimble Studio

Uso de subvenciones con claves AWS KMS

Una subvención es un instrumento de política que permite a AWS los directores utilizar AWS KMS claves en operaciones criptográficas. También puede permitirles ver una clave KMS con el comando `DescribeKey`, y crear y administrar concesiones.

Las subvenciones suelen ser utilizadas por las personas Servicios de AWS que se integran con ellas AWS KMS para cifrar sus datos en reposo. El servicio crea una concesión en nombre de un usuario de la cuenta, utiliza sus permisos y retira la concesión tan pronto como finalice su tarea.

Cuando Nimble Studio crea su estudio, asignamos dos funciones a los usuarios del portal de Nimble Studio: funciones de usuario y de administrador. Nimble Studio crea concesiones en las claves administradas por los clientes para estos roles a fin de proporcionarles acceso a los datos cifrados del estudio.

> **Important**
>
> Si elimina una concesión, los usuarios no podrán utilizar el portal de Nimble Studio hasta que el administrador cree una nueva concesión.

Para obtener más información sobre cómo Servicios de AWS usar las subvenciones, consulta el tema Cómo Servicios de AWS usar AWS KMS o el cifrado en reposo en la guía del usuario o la guía para desarrolladores del servicio.

Cifrado en tránsito

En la siguiente tabla se proporciona información sobre cómo se cifran los datos en tránsito. Si corresponde, también se enumeran otros métodos de protección de datos para Nimble Studio.

Datos	Ruta de acceso a la red	Protección
Activos web, como imágenes y JavaScript archivos	La ruta de red es entre los usuarios de Nimble Studio y Nimble Studio.	El cifrado de datos utiliza TLS 1.2 o posterior.
Pixel y tráfico de streaming relacionado	La ruta de red es entre los usuarios de Nimble Studio y Nimble Studio.	Cifrado con el estándar de cifrado avanzado de 256 bits (AES-256) y se transporta con TLS 1.2 o posterior.
Tráfico de API	La ruta es entre los usuarios de Nimble Studio y Nimble Studio.	Cifrado mediante TLS 1.2 o posterior. Las solicitudes para crear una conexión se firman mediante SigV4

Administración de claves para Amazon Nimble Studio

Al crear un nuevo estudio, puede elegir una de las siguientes claves para cifrar sus datos de estudio:

- AWS clave KMS propia: tipo de cifrado predeterminado. La clave es propiedad de Nimble Studio (sin cargo adicional).
- Clave administrada por el cliente: la clave se almacena en la cuenta y usted la crea, posee y administra. Usted tiene el control total sobre la clave. AWS KMS se aplican cargos.

Eliminar una clave de KMS gestionada por el cliente en AWS Key Management Service (AWS KMS) es destructivo y potencialmente peligroso. Elimina el material de claves y todos los metadatos asociados con la clave. Esta acción es irreversible. Una vez que se elimina una clave KMS administrada por el cliente, ya no puede descifrar los datos que se habían cifrado con ella. Esto significa que los datos se vuelven irrecuperables.

Por eso, AWS KMS los clientes tienen un período de espera de hasta 30 días antes de eliminar la clave. El periodo de espera predeterminado es de 30 días.

Acerca del período de espera

Como la eliminación de una clave KMS administrada por el cliente es un proceso destructivo y potencialmente peligroso, le requerimos que establezca un período de espera de 7 a 30 días. El periodo de espera predeterminado es de 30 días.

Sin embargo, el período de espera real puede ser hasta 24 horas más largo que el programado. Para obtener la fecha y la hora reales en las que se eliminará la clave, utilice la DescribeKeyoperación. O en la consola AWS KMS, en la página de detalles para la clave, en la sección Configuración general, consulte la eliminación programada. Fíjese en la zona horaria.

Durante el periodo de espera, el estado de la clave administrada por el cliente y el estado de la clave es Pendiente de eliminación.

- Una clave KMS administrada por el cliente que está pendiente de eliminación no puede utilizarse en ninguna operación criptográfica.
- AWS KMS no rota las claves secundarias de las AWS KMS claves gestionadas por el cliente que están pendientes de ser eliminadas.

Para obtener más información sobre cómo eliminar una AWS KMS clave administrada por el cliente, consulte Eliminar las claves maestras del cliente.

Medidas de seguridad de los datos

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure cuentas individuales con AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Le recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, números de cuenta de sus clientes, en los campos de formato libre, como el campo Nombre. Esto incluye cuando trabaja con Amazon Nimble Studio u otro dispositivo Servicios de AWS mediante la consola, la API o los AWS SDK. AWS CLI Es posible que cualquier dato que ingrese en Amazon Nimble Studio o en otros servicios se incluya en los registros de diagnóstico. Cuando le proporcione una URL a un servidor externo, no incluya información sobre las credenciales en la URL para validar la solicitud en ese servidor.

Datos y métricas de diagnóstico

Durante la implementación y la eliminación de StudioBuilder, Amazon Nimble Studio recopila determinadas métricas que utilizamos para diagnosticar problemas y mejorar las funciones y la experiencia del usuario de Nimble Studio.

Tipos de métricas recopiladas

- Información de uso: los comandos y subcomandos genéricos que se ejecutan.

- Errores e información de diagnóstico: el estado y la duración de los comandos que se ejecutan, incluidos los códigos de salida, los nombres de las excepciones internas y los errores.
- Información del sistema y del entorno: la versión de Python, el sistema operativo (WindowsLinux, omacOS) y el entorno en el que StudioBuilder se ejecuta.

Identity and Access Management para Amazon Nimble Studio

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores controlan quién se puede autenticar (iniciar sesión) y autorizar (tener permisos) para utilizar los recursos de Amazon Nimble Studio. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona Amazon Nimble Studio con IAM
- Ejemplos de políticas basadas en identidades de Amazon Nimble Studio
- AWS políticas gestionadas para Amazon Nimble Studio
- Prevención de la sustitución confusa entre servicios
- Solución de problemas de identidad y acceso de Amazon Nimble Studio

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Nimble Studio.

Usuario de servicio: si utiliza el servicio Nimble Studio para realizar su trabajo, significa que es un usuario de servicio. En este caso, su administrador le proporcionará las credenciales y los permisos que necesite para obtener acceso a los recursos asignados. A medida que utilice más características de Nimble Studio para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica de Nimble Studio, consulte Solución de problemas de identidad y acceso de Amazon Nimble Studio.

Administrador de servicio: si está a cargo de los recursos de Nimble Studio en su empresa, probablemente tenga acceso completo a Nimble Studio. Su trabajo consiste en determinar a qué características y recursos de Nimble Studio deben acceder sus empleados. A continuación, debe enviar solicitudes a su administrador para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo puede su empresa utilizar IAM con Nimble Studio, consulte Cómo funciona Amazon Nimble Studio con IAM.

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Para obtener más información sobre cómo iniciar sesión con AWS Management Console, consulte Iniciar sesión AWS Management Console como usuario de IAM o usuario raíz en la Guía del usuario de IAM.

Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario Cuenta de AWS raíz, usuario o asumiendo una función de IAM. También puede utilizar la autenticación de inicio de sesión único de la empresa o incluso iniciar sesión con Google o Facebook. En estos casos, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS con credenciales de otra empresa, asumes un rol de forma indirecta.

Para iniciar sesión directamente en la AWS Management Console, utilice la contraseña con su dirección de correo electrónico de usuario raíz o con su nombre de usuario. Puede obtener acceso a AWS mediante programación a través de las claves de acceso del usuario o del usuario raíz.

AWS proporciona herramientas de línea de comandos y de SDK para firmar criptográficamente tu solicitud con tus credenciales. Si no utilizas AWS herramientas, firma la solicitud tú mismo. Para ello, utilice Signature Version 4, un protocolo para autenticar solicitudes de API de entrada. Para obtener más información sobre las solicitudes de autenticación, consulte Proceso de firma de Signature Version 4 en la Referencia general de AWS .

Independientemente del método de autenticación que utilice, es posible que también deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una por primera vez Cuenta de AWS, se comienza con una identidad de inicio de sesión única que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Se recomienda encarecidamente no utilizar el usuario raíz para las tareas cotidianas, ni siquiera para las tareas administrativas. En lugar de ello, es mejor ceñirse a la práctica recomendada de utilizar el usuario final exclusivamente para crear al primer usuario de IAM. A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas tan solo para algunas tareas de administración de cuentas y servicios.

Usuarios y grupos

Un usuario es una identidad dentro de ti Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Un usuario puede tener credenciales a largo plazo o un conjunto de claves de acceso. Para obtener información sobre cómo generar claves de acceso, consulte Administración de claves de acceso de los usuarios de IAM en la Guía del usuario de IAM. Al generar claves de acceso para un usuario de IAM, asegúrese de ver y guardar de forma segura el par de claves. No puede recuperar la clave de acceso secreta en el futuro. En su lugar, debe generar un nuevo par de claves de acceso.

Un Grupo de IAM es una identidad que especifica un conjunto de usuarios. No puede iniciar sesión como grupo. Puede usar grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario, pero no está asociado a una persona específica. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol

llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para obtener más información acerca de los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Permisos de usuario temporales: un usuario puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso de usuario federado: en lugar de crear un usuario, puede utilizar las identidades existentes de AWS Directory Service su directorio de usuarios empresarial o de un proveedor de identidades web. A estas identidades se les llama usuarios federados. AWS asigna una función a un usuario federado cuando se solicita acceso a través de un proveedor de identidad. Para obtener más información acerca de los usuarios federados, consulte Usuarios federados y roles en la Guía del usuario de IAM.
  - Membresía: Nimble Studio utiliza un concepto llamado "membresía" para proporcionar al usuario acceso a un perfil de lanzamiento concreto. La membresía permite a los administradores del estudio delegar el acceso a los recursos a los usuarios, sin tener que redactar ni comprender las políticas de IAM. Cuando un administrador de Nimble Studio crea una membresía para un usuario en un perfil de lanzamiento, el usuario está autorizado a realizar las acciones de IAM necesarias para usar un perfil de lanzamiento, como ver sus propiedades e iniciar una sesión de streaming con ese perfil de lanzamiento.
  - Rol de servicio: un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Los roles de servicio ofrecen acceso solo dentro de su cuenta y no se pueden utilizar para otorgar acceso a servicios en otras cuentas. Un administrador puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Nimble Studio no es compatible con roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para

conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM o usuarios, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla creando políticas y adjuntándolas a las identidades o los recursos de IAM. AWS AWS Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. Puede iniciar sesión como usuario raíz o usuario, o puede asumir un rol de IAM. A continuación, al realizar una solicitud, AWS evalúa las políticas relacionadas basadas en la identidad o en los recursos. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan como documentos JSON. AWS Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

Cada entidad de IAM (usuario o rol) comienza sin permisos. En otras palabras, de forma predeterminada, los usuarios no pueden hacer nada, ni siquiera cambiar sus propias contraseñas. Para conceder permiso a un usuario para hacer algo, el administrador debe adjuntarle una política de permisos. O bien el administrador puede agregar al usuario a un grupo que tenga los permisos necesarios. Cuando el administrador concede permisos a un grupo, todos los usuarios de ese grupo obtienen los permisos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y bajo qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información acerca de cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se adjunta la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL) en Nimble Studio

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de política JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límite de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una

entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en identidad de la entidad y los límites de sus permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicios (SCP): las SCP son políticas JSON que especifican los permisos máximos para una organización o unidad organizativa (OU) en Organizations. Organizations es un servicio que le permite agrupar y administrar de forma centralizada varias Cuentas de AWS que posee su negocio. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluido cada Cuenta de AWS usuario raíz. Para obtener más información sobre Organizations y los SCP, consulte Cómo funcionan los SCP en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección del usuario o de las políticas basadas en identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon Nimble Studio con IAM

Antes de utilizar IAM para administrar el acceso a Nimble Studio, conozca qué características de IAM se pueden utilizar con Nimble Studio.

Características de IAM que puede utilizar con Amazon Nimble Studio

Características de IAM	Soporte de Nimble Studio
Acciones de política de Nimble Studio	Sí
Recursos de políticas para Nimble Studio	Sí
Claves de condición de políticas de Amazon Nimble Studio	Sí
Listas de control de acceso (ACL) en Nimble Studio	No
Control de acceso basado en atributos (ABAC) con Nimble Studio	Sí
Uso de credenciales temporales con Nimble Studio	Sí
Permisos de entidades principales entre servicios de Nimble Studio	Sí
Funciones de servicio para Nimble Studio	Sí
Funciones de servicio para Nimble Studio	No

Para obtener una visión general de cómo Servicios de AWS funcionan Nimble Studio y otros dispositivos con la mayoría de las funciones de IAM, consulta Servicios de AWS cómo funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades para Nimble Studio

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario, un grupo de usuarios o un rol. Estas políticas controlan

qué acciones pueden realizar los usuarios y los roles, en qué recursos y bajo qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidad de IAM, puede especificar las acciones y recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociado. Para obtener más información acerca de los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades de Amazon Nimble Studio

Para ver ejemplos de políticas basadas en identidad de Nimble Studio, consulte Ejemplos de políticas basadas en identidades de Amazon Nimble Studio.

Políticas basadas en recursos de Nimble Studio

Compatibilidad con las políticas basadas en recursos	No

Nimble Studio no es compatible con políticas basadas en recursos ni acceso entre cuentas. Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se adjunta la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Acciones de política de Nimble Studio

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Nimble Studio, consulte Acciones definidas por Amazon Nimble Studio en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Nimble Studio utilizan el siguiente prefijo antes de la acción:

```
nimble
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "nimble:action1",
      "nimble:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidad de Nimble Studio, consulte Ejemplos de políticas basadas en identidades de Amazon Nimble Studio.

Recursos de políticas para Nimble Studio

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter asterísco (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver ejemplos de políticas basadas en identidad de Nimble Studio, consulte Ejemplos de políticas basadas en identidades de Amazon Nimble Studio.

Claves de condición de políticas de Amazon Nimble Studio

Admite claves de condición de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

El elemento `Condition` (o elemento `Condition`**`block`**`) lets you specify conditions in which a statement is in effect. The `Condition`) es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación `OR` lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario para acceder a un recurso solo si está etiquetado con su nombre de usuario. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS , consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Para ver ejemplos de políticas basadas en identidad de Nimble Studio, consulte Ejemplos de políticas basadas en identidades de Amazon Nimble Studio.

Listas de control de acceso (ACL) en Nimble Studio

Admite las ACL	No

Nimble Studio no es compatible con Listas de control de acceso (ACL). Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de política JSON.

Control de acceso basado en atributos (ABAC) con Nimble Studio

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Nimble Studio

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información acerca del cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios de Nimble Studio

Admite permisos de entidades principales	Sí

Funciones de servicio para Nimble Studio

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Los roles de servicio ofrecen acceso solo dentro de su cuenta y no se pueden utilizar para otorgar acceso a servicios en otras cuentas. Un administrador puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de ACM. Edite los roles de servicio solo cuando Nimble Studio proporcione orientación para hacerlo.

Funciones de servicio para Nimble Studio

Compatible con roles vinculados al servicio	No

Nimble Studio no es compatible con roles vinculados a servicios. Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información acerca de cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades de Amazon Nimble Studio

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Nimble Studio. Tampoco pueden realizar tareas mediante la API AWS Management Console AWS CLI, o AWS . Un administrador de IAM debe crear políticas de IAM que concedan a los usuarios y a los roles permiso para realizar acciones en los recursos que necesitan. El administrador debe asociar esas políticas a los usuarios o grupos que necesiten esos permisos.

Para obtener más información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas de JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

- Prácticas recomendadas relativas a políticas

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidad son muy eficaces. Determinan si alguien puede crear, acceder o eliminar los recursos de Nimble Studio de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience a utilizar las políticas AWS gestionadas: para empezar a utilizar Nimble Studio rápidamente, utilice las políticas AWS gestionadas para conceder a sus empleados los permisos que necesitan. Estas políticas ya están disponibles en su cuenta, y las mantiene y actualiza AWS. Para obtener más información, consulta Cómo empezar a usar permisos con políticas AWS administradas en la Guía del usuario de IAM.
- Conceder privilegios mínimos: al crear políticas personalizadas, conceda solo los permisos necesarios para llevar a cabo una tarea. Comience con un conjunto mínimo de permisos y conceda permisos adicionales según sea necesario. Por lo general, es más seguro que comenzar con permisos demasiado tolerantes e intentar hacerlos más estrictos más adelante. Para obtener más información, consulte Conceder privilegios mínimos en la Guía del usuario de IAM.
- Habilitar MFA para operaciones confidenciales: para mayor seguridad, obligue a los usuarios a utilizar la autenticación multifactor (MFA) para acceder a los recursos u operaciones confidenciales de la API. Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.
- Utilizar condiciones de política para mayor seguridad: en la medida en que sea práctico, defina las condiciones en las que las políticas basadas en identidad permitan el acceso a un recurso. Por ejemplo, puede escribir condiciones para especificar un rango de direcciones IP permitidas desde el que debe proceder una solicitud. También puede escribir condiciones para permitir solicitudes solo en un intervalo de hora o fecha especificado o para solicitar el uso de SSL o MFA. Para obtener más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.

AWS políticas gestionadas para Amazon Nimble Studio

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política.

Es más probable que los servicios actualicen una política administrada de AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripción de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

Sus usuarios finales accederán a Amazon Nimble Studio principalmente a través del portal Nimble Studio. Al crear tu estudio con StudioBuilder la consola de Nimble Studio, se crea un rol de IAM para cada persona del estudio: el administrador del estudio y el usuario del estudio. Cada uno de ellos incluye la política de gestión de IAM correspondiente. El portal Nimble Studio proporciona una experiencia en la que los usuarios solo pueden publicar y utilizar los recursos a los que tienen permiso de acceso.

El portal Nimble Studio ofrece una experiencia en la que los usuarios solo pueden publicar y utilizar los recursos a los que tienen acceso, y el portal depende del contenido de estas políticas para funcionar correctamente. Los usuarios finales de Nimble Studio utilizarán el portal para acceder a su estudio en la nube. Por lo tanto, cuando los administradores crean su estudio con él StudioBuilder, se crea un rol de IAM para cada persona que necesite acceder al estudio. Esto incluye al administrador y al usuario del estudio, cada uno con su política de gestión de IAM correspondiente adjunta.

Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas por AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: **`AmazonNimbleStudio-LaunchProfileWorker`**

Puede adjuntar la política de `AmazonNimbleStudio-LaunchProfileWorker` a las identidades de IAM.

Adjunta esta política a las instancias de EC2 creadas por Nimble Studio Builder para permitir el acceso a los recursos que necesitan los trabajadores del perfil de lanzamiento de Nimble Studio.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- ds: permite a LaunchProfile los trabajadores descubrir información de conexión sobre la AWS Managed Microsoft AD asociada a un LaunchProfile.
- ec2: permite a LaunchProfile los trabajadores descubrir información sobre grupos de seguridad y subredes para conectarse a un. LaunchProfile
- fsx: permite a LaunchProfile los trabajadores descubrir la información de conexión a los volúmenes de Amazon FSx asociados a un. LaunchProfile

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      },
      "Sid": "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version": "2012-10-17"
}
```

AWS política gestionada: **AmazonNimbleStudio-StudioAdmin**

Puede adjuntar la política de AmazonNimbleStudio-StudioAdmin a las identidades de IAM.

Adjunte esta política al rol de administrador asociado a su estudio para permitir el acceso a los recursos de Amazon Nimble Studio asociados al administrador del estudio y a los recursos del estudio relacionados en otros servicios.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- nimble: permite a los usuarios de Studio acceder a los recursos de Nimble que les han sido delegados por. StudioAdmins
- sso: permite a los usuarios de Studio ver los nombres de otros usuarios del estudio.
- sso: permite a los usuarios de Studio ver los nombres de otros usuarios del estudio.
- ds: permite a Nimble Studio añadir estaciones de trabajo virtuales a las asociadas al AWS Managed Microsoft AD estudio.
- ec2: permite a Nimble Studio conectar estaciones de trabajo virtuales a la VPC configurada.
- fsx: permite a Nimble Studio conectar estaciones de trabajo virtuales a los volúmenes de Amazon FSx configurados.
- cloudwatch: permite a Nimble Studio recuperar métricas. CloudWatch

```
{
  "Statement": [
    {
      "Sid": "StudioAdminFullAccess",
      "Effect": "Allow",
      "Action": [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
```

```
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:GetMetricData",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/NimbleStudio"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

AWS política gestionada: **AmazonNimbleStudio-StudioUser**

Puede adjuntar la política de AmazonNimbleStudio-StudioUser a las identidades de IAM.

Adjunte esta política al rol de usuario asociado a su estudio para permitir el acceso a los recursos de Amazon Nimble Studio asociados al usuario del estudio y a los recursos de estudio relacionados en otros servicios.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- nimble: permite a los usuarios de Studio acceder a los recursos de Nimble que les han sido delegados por. StudioAdmins
- sso: permite a los usuarios de Studio ver los nombres de otros usuarios del estudio.
- sso: permite a los usuarios de Studio ver los nombres de otros usuarios del estudio.
- ds: permite a Nimble Studio añadir estaciones de trabajo virtuales a las asociadas al AWS Managed Microsoft AD estudio.
- ec2: permite a Nimble Studio conectar estaciones de trabajo virtuales a la VPC configurada.
- fsx: permite a Nimble Studio conectar estaciones de trabajo virtuales a los volúmenes de Amazon FSx configurados.

```
{
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListLaunchProfiles"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```
          "nimble:requesterPrincipalId": "${nimble:principalId}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions"
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:ownedBy": "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

Nimble Studio actualiza las políticas administradas por AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas de Amazon Nimble Studio desde que este servicio comenzó a realizar el seguimiento de estos cambios.

Cambio	Descripción	Fecha
AWS política gestionada: `AmazonNimbleStudio-StudioUser` - Política actualizada	Amazon Nimble Studio actualizó una política para usar la versión más reciente del servicio Identity Store.	22 de septiembre de 2023
AWS política gestionada: `AmazonNimbleStudio-StudioAdmin`: política actualizada	Amazon Nimble Studio actualizó una política para usar la versión más reciente del servicio Identity Store.	22 de septiembre de 2023
AWS política gestionada: `AmazonNimbleStudio-StudioUser`: política actualizada	Amazon Nimble Studio actualizó una política para permitir a los usuarios del estudio ver las copias de seguridad de sus estaciones de trabajo.	20 de diciembre de 2022
AWS política gestionada: `AmazonNimbleStudio-StudioAdmin`: política actualizada	Amazon Nimble Studio actualizó la política para permitir a los administradores de los estudios ver las copias de seguridad de sus estacione s de trabajo.	20 de diciembre de 2022
AWS política gestionada: `AmazonNimbleStudio-StudioUser`: política actualizada	Amazon Nimble Studio actualizó una política para permitir a los administradores de los estudios recuperar CloudWatch las métricas.	11 de noviembre de 2021

Cambio	Descripción	Fecha
AWS política gestionada: `AmazonNimbleStudio-StudioUser` : política actualizada	Amazon Nimble Studio actualizó la política para permitir a los usuarios del estudio iniciar y detener sus estaciones de trabajo.	1 de noviembre de 2021
AWS política gestionada: `AmazonNimbleStudio-StudioAdmin` : política actualizada	Amazon Nimble Studio actualizó la política para permitir a los usuarios del estudio iniciar y detener sus estaciones de trabajo.	1 de noviembre de 2021
AWS política gestionada: `AmazonNimbleStudio-StudioUser` : política actualizada	Amazon Nimble Studio actualizó la política para permitir de forma condicion al el acceso a los recursos de las sesiones de streaming en función de `nimble:ownedBy` en lugar de `nimble:createdBy` .	16 de agosto de 2021
AWS política gestionada: `AmazonNimbleStudio-StudioUser` : política nueva	Amazon Nimble Studio es una política administrada que: otorga acceso a los recursos asociados al usuario del estudio y a los recursos del estudio relacionados en otros servicios.	28 de abril de 2021

Cambio	Descripción	Fecha
AWS política gestionada: `AmazonNimbleStudio-StudioAdmin`: política nueva	Amazon Nimble Studio es una política administrada que otorga acceso a los recursos asociados al usuario del estudio y a los recursos del estudio relacionados en otros servicios.	28 de abril de 2021
AWS política gestionada: `AmazonNimbleStudio-LaunchProfileWorker`: política nueva	Amazon Nimble Studio agregó una nueva política que permite el acceso a los recursos que necesitan los trabajadores del perfil de lanzamiento de Nimble Studio.	28 de abril de 2021
Amazon Nimble Studio comenzó a realizar el seguimiento de los cambios	Amazon Nimble Studio comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	28 de abril de 2021

Prevención de la sustitución confusa entre servicios

El problema del suplente confuso es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que le ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` en las políticas de recursos para limitar los permisos que Identity and Access

Management (IAM) concede a Amazon Nimble Studio para el acceso a sus recursos. Si se utilizan ambas claves de contexto de condición global, el valor `aws:SourceAccount` y la cuenta del valor `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilicen en la misma declaración de política.

El valor de `aws:SourceArn` debe ser el ARN del estudio y `aws:SourceAccount` debe ser el identificador de su cuenta. No sabrá cuál es el identificador del estudio hasta que lo haya creado, ya que lo genera Nimble Studio. Una vez creado su estudio, puede actualizar la política de confianza con el identificador final del estudio establecido como `aws:SourceArn`.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si especifica varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con el carácter asterisco (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:nimble::123456789012:*`.

Sus usuarios finales asumen su rol de estudio cuando inician sesión en el portal de Nimble Studio. Al crear su estudio, AWS configura el rol y evalúa la política. AWS evalúa la política cada vez que uno de tus usuarios inicie sesión en el portal de Nimble Studio. Al crear un estudio, no se puede modificar `aws:SourceArn`. Cuando termine de crear su estudio, puede usar su studioARN para `aws:SourceArn`.

El siguiente ejemplo muestra cómo se pueden utilizar las claves contextuales de condición global `aws:SourceArn` y `aws:SourceAccount` en Nimble Studio para evitar el problema del suplente confuso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "identity.nimble.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
```

```
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:nimble:us-west-2:123456789012:studio/*"
        }
      }
    }
  ]
}
```

Solución de problemas de identidad y acceso de Amazon Nimble Studio

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Nimble Studio e IAM.

Temas

- No tengo autorización para realizar una acción en Nimble Studio.
- No estoy autorizado a realizar iam:PassRole.
- Quiero ver mis claves de acceso
- Soy administrador y quiero permitir que otros obtengan acceso a Nimble Studio.
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Nimble Studio.

No tengo autorización para realizar una acción en Nimble Studio.

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `nimble:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 nimble:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `nimble:`*`GetWidget`*.

Si necesitas ayuda, ponte en contacto con tu administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar iam:PassRole.

Si recibe un error que indica que no está autorizado para llevar a cabo la acción `iam:PassRole`, debe ponerse en contacto con su administrador para recibir ayuda. Pida a la persona que actualice sus políticas de forma que pueda transferir un rol a Nimble Studio.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio, en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario denominado `johndoe` intenta utilizar la consola para realizar una acción en Nimble Studio. Sin embargo, la acción requiere que el servicio cuente con permisos otorgados por un rol de servicio. John no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/johndoe is not authorized to perform: iam:PassRole
```

En este caso, John pide a su administrador que actualice sus políticas para conceder permiso para realizar la acción `iam:PassRole`.

Quiero ver mis claves de acceso

Amazon Nimble Studio no proporciona claves de acceso. Para obtener información sobre cómo crear claves de acceso secretas, consulte Administración de las claves de acceso en la Guía de usuarios de IAM.

> **Important**
>
> No proporcione las claves de acceso a terceros, ni siquiera para que le ayuden a buscar el ID de usuario canónico. Si lo hace, podría conceder a otra persona acceso permanente a su cuenta.

Cuando crea un par de claves de acceso, se le pide que guarde el ID de clave de acceso y la clave de acceso secreta en un lugar seguro. La clave de acceso secreta solo está disponible en el momento de su creación. Si pierde la clave de acceso secreta, debe añadir nuevas claves de acceso a su usuario. Puede tener un máximo de dos claves de acceso. Si ya cuenta con dos, debe eliminar un par de claves antes de crear una nueva. Para consultar las instrucciones, consulte Administración de claves de acceso en la Guía del usuario de IAM.

Soy administrador y quiero permitir que otros obtengan acceso a Nimble Studio.

Para permitir que otros obtengan acceso a Nimble Studio, debe crear una entidad de IAM (usuario o rol) para la persona o la aplicación que necesita acceso. Esta persona utilizará las credenciales de la entidad para acceder a AWS. A continuación, debe asociar una política a la entidad que le conceda los permisos correctos.

Nimble Studio le proporciona el `AmazonNimbleStudio-StudioUser` en la AWS Management Console. El administrador de TI que administra la consola utiliza esta política para conceder acceso al estudio a otras personas.

Para ver un tutorial sobre el uso de la política de administración, consulte la guía Configuración de Nimble Studio. Para obtener información sobre cómo asociar las políticas existentes a los usuarios, como las políticas de usuario y de perfil de lanzamiento, consulte Creación de usuarios de IAM (consola).

Para obtener información sobre cómo importar políticas, consulte Creación del primer grupo y usuario delegado de IAM en la Guía del usuario de IAM.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Nimble Studio.

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si Nimble Studio admite estas características, consulte Cómo funciona Amazon Nimble Studio con IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a través de los Cuentas de AWS que eres propietario, consulta Cómo proporcionar acceso a un usuario de IAM a otro usuario de tu Cuenta de AWS propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Registro y supervisión de eventos de seguridad con Nimble Studio

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon Nimble Studio y sus AWS soluciones. Recopile datos de monitoreo de todas las partes de su AWS solución para poder depurar con mayor facilidad una falla multipunto en caso de que se produzca.

AWS y Nimble Studio proporcionan herramientas para supervisar sus recursos y responder a posibles incidentes, incluida Registrar llamadas de Nimble Studio mediante AWS CloudTrail una guía del usuario.AWS CloudFormation

Para obtener más información sobre cómo funciona Amazon Nimble Studio AWS CloudFormation, incluidos ejemplos de plantillas JSON y YAML, consulte la referencia de recursos y propiedades de Amazon Nimble Studio en la Guía del AWS CloudFormation usuario. Para entender cómo usar las CloudFormation plantillas, consulte los conceptos.AWS CloudFormation

Temas

- Registrar llamadas de Nimble Studio mediante AWS CloudTrail

Registrar llamadas de Nimble Studio mediante AWS CloudTrail

Amazon Nimble Studio está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o una persona Servicio de AWS en Nimble Studio. CloudTrail captura todas las llamadas a la API de Nimble Studio como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Nimble Studio y las llamadas desde el código a las operaciones de Amazon Nimble Studio.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Nimble Studio. Si no configuras una ruta, podrás ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted

CloudTrail, puede determinar la solicitud que se realizó a Nimble Studio, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Información de Nimble Studio en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Nimble Studio, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos del historial de eventos. Puedes ver, buscar y descargar eventos recientes en tu Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos de Nimble Studio, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en los CloudTrail registros y actúen en función de ellos.

Para más información, consulte los siguientes temas:

Introducción a la creación de registros de seguimiento

CloudTrail servicios e integraciones compatibles

Configuración de las notificaciones de Amazon SNS para CloudTrail

Recibir archivos de CloudTrail registro de varias regiones

Recibir archivos de CloudTrail registro de varias cuentas

Las acciones de Nimble Studio se registran CloudTrail y se documentan en la referencia de la API de Amazon Nimble Studio. Por ejemplo, las llamadas a GetStudio y DeleteStudio las acciones generan entradas en los archivos de CloudTrail registro. CreateStudio

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.

- Si la solicitud la realizó otro servicio de .

Para obtener más información, consulte el elemento de identidad CloudTrail del usuario.

Descripción de las entradas de archivos de registro de Nimble Studio

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un seguimiento ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En este ejemplo de JSON se muestran tres acciones:

- ACCIÓN_1: CreateStudio
- ACCIÓN_2: GetStudio
- ACCIÓN_3: DeleteStudio

```
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:25:49Z"
```

```
            }
        }
    },
    "eventTime": "2021-03-08T23:25:49Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "CreateStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "displayName": "Studio Name",
        "studioName": "EXAMPLE-studioName",
        "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User",
        "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin"
    },
    "responseElements": {},
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
```

```
                "creationDate": "2021-03-08T23:44:25Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:25Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "GetStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": null,
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:45:14Z"
            }
```

```
        }
    },
    "eventTime": "2021-03-08T23:44:14Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "DeleteStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": {
        "studio": {
            "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin",
            "displayName": "My New Studio Name",
            "homeRegion": "us-west-2",
            "ssoClientId": "EXAMPLE-ssoClientId",
            "state": "DELETING",
            "statusCode": "DELETING_STUDIO",
            "statusMessage": "Deleting studio",
            "studioEncryptionConfiguration": {
                "keyType": "AWS_OWNED_CMK"
            },
            "studioId": "us-west-2-EXAMPLE-studioId",
            "studioName": "EXAMPLE-studioName",
            "studioUrl": "https://sso111122223333.us-
west-2.portal.nimble.amazonaws.com",
            "tags": {},
            "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User"
        }
    },
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


En el ejemplo, observará que los eventos muestran la región, la dirección IP y otros «RequestParameters», como «» y adminRoleArn «userRoleArn», que le ayudarán a identificar el

evento. Puede ver la fecha y la hora en la "creationDate" y la fuente en la que se originó la solicitud, que está marcada como "eventSource": “nimble.amazonaws.com”.

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en IAM o AWS STS, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos del historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS.

AWS CloudTrail captura todas las llamadas a la API para IAM y AWS Security Token Service (AWS STS) como eventos, incluidas las llamadas desde la consola y las llamadas a la API. Para obtener más información sobre su uso CloudTrail con IAM AWS STS, consulte Registrar llamadas de IAM y AWS STS API con. AWS CloudTrail

Para obtener más información al respecto CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Para obtener información sobre otros servicios de monitoreo que ofrece Amazon, consulta la Guía del CloudWatch usuario de Amazon.

Validación de conformidad para Amazon Nimble Studio

Amazon Nimble Studio sigue el modelo de responsabilidad compartida y el cumplimiento es compartido entre nuestros clientes AWS y nosotros.

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.

- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Seguridad de la infraestructuras en Amazon Nimble Studio

Como servicio gestionado, Amazon Nimble Studio está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a Nimble Studio a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Prácticas recomendadas de seguridad para Nimble Studio

Amazon Nimble Studio proporciona una serie de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Monitoreo

La supervisión es una parte importante para mantener la fiabilidad, la disponibilidad y el rendimiento de Nimble Studio y sus AWS soluciones. Para obtener más información acerca del monitoreo y la respuesta a los eventos, consulte Registro y supervisión de eventos de seguridad con Nimble Studio.

Protección de datos

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure cuentas individuales con AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Recomendamos TLS 1.2 o una versión posterior.

- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que lo ayuden a detectar y proteger los datos personales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información acerca de los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Le recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, números de cuenta de sus clientes, en los campos de formato libre, como el campo Nombre. Esto incluye cuando trabaja con Amazon Nimble Studio u otro dispositivo Servicios de AWS mediante la consola, la API o los AWS SDK. AWS CLI Es posible que cualquier dato que ingrese en Amazon Nimble Studio o en otros servicios se incluya en los registros de diagnóstico. Cuando le proporcione una URL a un servidor externo, no incluya información sobre las credenciales en la URL para validar la solicitud en ese servidor.

Permisos

Administre el acceso a AWS los recursos mediante los usuarios, las funciones de IAM y concediendo el mínimo de privilegios a los usuarios. Establezca políticas y procedimientos de administración de credenciales para crear, distribuir, rotar y revocar las credenciales de acceso. AWS Para obtener más información, consulte la sección Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Soporte para Nimble Studio

Obtenga información sobre las distintas opciones de soporte para Nimble Studio, por ejemplo, cómo obtener ayuda para implementar o usar el servicio y sus aplicaciones relacionadas.

Contenido

- Foro de Nimble Studio
- Soporte para aplicaciones
- AWS Support Center
- AWS Support Plans

Foro de Nimble Studio

Si tiene preguntas sobre Nimble Studio, puede visitar el foro de Nimble Studio. Allí podrá obtener respuestas de la comunidad y de los moderadores del foro AWS sobre las funciones, los problemas técnicos y la ayuda para solucionar problemas de Nimble Studio.

Soporte para aplicaciones

Nimble Studio proporciona documentación adicional para las siguientes aplicaciones.

AWSThinkboxDeadline

Para obtener ayuda con su granja de renderizado o para aprender cómo funciona Deadline, consulte la documentaciónAWSThinkboxDeadline.

Nimble Studio File Transfer

Para saber cómo funciona File Transfer, consulte la Guía del usuario de transferencia de archivos de Nimble Studio.

AWS Support Center

AWS Support Center es un centro para crear y administrar sus casos de soporte. Proporciona acceso a una variedad de recursos, que incluyen soluciones técnicas y de facturación, un centro de

conocimiento, vídeos del centro de conocimiento, documentación AWS, además de capacitación y certificación.

AWS Support Plans

AWS Support Plans le ayuda a optimizar el rendimiento, mantener la seguridad, evitar el tiempo de inactividad y controlar los costes. Para obtener más información acerca de los diferentes planes de AWS Support, consulte Comparar AWS Support Plans.

Para obtener más información sobre cómo puede AWS ayudarlo, visite la página de Contacto.

Historial de documentos

- Versión de la API: la más reciente
- Última actualización de la documentación: 22 de septiembre de 2023

En la tabla siguiente, se describen los cambios importantes de cada versión de la Guía del administrador de Nimble Studio.

Cambio	Descripción	
Nuevo servicio y guía	Esta es la versión inicial Amazon Nimble Studio y de la Guía del administrador de Amazon Nimble Studio.	19 de junio de 2023
Actualizaciones de políticas administradas por AWS	Se actualizaron las políticas `AmazonNimbleStudio-StudioUser` y `AmazonNimbleStudio-StudioAdmin` para usar la versión más reciente del servicio AWS IAM Identity Center.	22 de septiembre de 2023

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.