Guía de administración

AWS Wickr

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Wickr: Guía de administración

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Wickr? ... 1
Características de Wickr ... 1
Disponibilidad regional ... 3
Acceso a Wickr ... 3
Precios ... 3
Documentación para el usuario final de Wickr ... 3
Configuración ... 4
Inscríbase en AWS ... 4
Creación un usuario de IAM ... 4
Siguientes pasos ... 6
Introducción ... 7
Requisitos previos ... 7
Paso 1: crear una red ... 7
Paso 2: configurar su red ... 8
Paso 3: crear e invitar a usuarios ... 9
Pasos a seguir a continuación ... 11
Cómo administrar la red ... 12
Detalles de la red ... 12
Vea los detalles de la red ... 12
Editar el nombre de la red ... 13
Eliminar red ... 13
Grupos de seguridad ... 14
Cómo consultar los grupos de seguridad ... 14
Cree un grupo de seguridad ... 15
Editar el grupo de seguridad ... 16
Eliminar un grupo de seguridad ... 18
Configuración del SSO ... 19
Cómo ver la información del SSO ... 19
Cómo configurar el SSO ... 20
Periodo de gracia para la actualización del token ... 25
Etiquetas de red ... 26
Cómo administrar las etiquetas de red ... 26
Agregue una etiqueta de red ... 27
Editar una etiqueta de red ... 27

Eliminar una etiqueta de red ... 28
Lea los recibos ... 28
Administre el plan de red ... 29
Limitaciones de la prueba gratuita de Premium ... 29
Retención de datos ... 30
Vea la retención de datos ... 30
Cómo configurar la retención de datos ... 31
Cómo obtener los registros ... 43
Métricas y eventos de retención de datos ... 44
¿Qué es ATAK? ... 49
Cómo habilitar ATAK ... 50
Información adicional sobre ATAK ... 51
Instalar y emparejar ... 51
Desvincular ... 53
Marcar y recibir una llamada ... 53
Enviar un archivo ... 53
Envía un mensaje de voz seguro ... 54
Rueda de opciones ... 54
Navegación ... 55
Lista de puertos y dominios que deben ser permitidos ... 55
Lista de dominios y direcciones a permitir por región ... 56
GovCloud ... 66
Vista previa del archivo ... 67
Administración de usuarios ... 69
Directorio de equipos ... 69
Ver usuarios ... 69
Invite a un usuario ... 70
Cómo editar usuarios ... 70
Delete user (Eliminar usuario) ... 71
Cómo eliminar usuarios en bloque ... 71
Suspensión de usuarios en bloque ... 73
Usuarios invitados ... 74
Cómo habilitar o deshabilitar usuarios invitados ... 74
Cómo ver el número de usuarios invitados ... 75
Cómo ver el uso mensual ... 76
Cómo ver los usuarios invitados ... 76

Bloquee a un usuario invitado ... 76
Seguridad ... 78
Protección de los datos ... 79
Identity and Access Management ... 80
Público ... 80
Autenticación con identidades ... 81
Administración de acceso mediante políticas ... 85
Políticas administradas por AWS Wickr ... 87
Cómo funciona AWS Wickr con IAM ... 89
Ejemplos de políticas basadas en identidades ... 96
Solución de problemas ... 99
Validación de conformidad ... 100
Resiliencia ... 100
Seguridad de infraestructuras ... 101
Configuración y análisis de vulnerabilidades ... 101
Prácticas recomendadas de seguridad ... 101
Monitorización ... 103
CloudTrail registros ... 103
Información sobre Wickr en CloudTrail ... 103
Descripción de las entradas de los archivos de registro de Wickr ... 104
Panel de análisis ... 111
Historial de documentos ... 114
Notas de la versión ... 120
Mayo de 2025 ... 120
Marzo de 2025 ... 120
Octubre de 2024 ... 120
Septiembre de 2024 ... 120
Agosto de 2024 ... 120
Junio de 2024 ... 121
Abril de 2024 ... 121
Marzo de 2024 ... 121
Febrero de 2024 ... 121
Noviembre de 2023 ... 122
Octubre de 2023 ... 122
Septiembre de 2023 ... 122
Agosto de 2023 ... 122

Julio de 2023 123
Mayo de 2023 123
Marzo de 2023 123
Febrero de 2023 123
Enero de 2023 123
..... cxxiv

¿Qué es AWS Wickr?

AWS Wickr es un servicio end-to-end cifrado que ayuda a las organizaciones y agencias gubernamentales a comunicarse de forma segura a través one-to-one de mensajes grupales, llamadas de voz y vídeo, uso compartido de archivos, uso compartido de pantalla y mucho más. Wickr puede ayudar a los clientes a superar las obligaciones de retención de datos asociadas a las aplicaciones de mensajería del consumidor y a facilitar la colaboración de forma segura. Los controles administrativos y de seguridad avanzados ayudan a las organizaciones a cumplir los requisitos legales y reglamentarios y a crear soluciones personalizadas para los desafíos de seguridad de datos.

La información se puede registrar en un almacén de datos privado controlado por el cliente con fines de retención y auditoría. Los usuarios tienen un control administrativo exhaustivo sobre los datos, que incluye la configuración de permisos, la configuración de opciones de mensajería efímera y la definición de grupos de seguridad. Wickr se integra con servicios adicionales como Active Directory (AD), inicio de sesión único (SSO) con OpenID Connect (OIDC) y más. Puede crear y administrar rápidamente una red de Wickr a través de los AWS Management Console bots de Wickr y automatizarlos de forma segura. Para empezar, consulte Configuración de AWS Wickr.

Temas

- Características de Wickr
- Disponibilidad regional
- Acceso a Wickr
- Precios
- Documentación para el usuario final de Wickr

Características de Wickr

Seguridad y privacidad mejoradas

Wickr utiliza el cifrado AES (Advanced Encryption Standard) end-to-end de 256 bits para cada función. Las comunicaciones se cifran localmente en los dispositivos del usuario y permanecen indescifrables mientras están en tránsito hacia cualquier persona que no sea el remitente y el receptor. Todos los mensajes, llamadas y archivos se cifran con una nueva clave aleatoria, y solo los destinatarios (ni siquiera AWS) pueden descifrarlos. Ya sea que estén compartiendo datos

confidenciales y regulados, discutiendo asuntos legales o de recursos humanos, o incluso llevando a cabo operaciones militares tácticas, los clientes utilizan Wickr para comunicarse cuando la seguridad y la privacidad son primordiales.

Retención de datos

Las características administrativas flexibles están diseñadas no solo para proteger la información confidencial, sino también para retener los datos según sea necesario para cumplir con las obligaciones de cumplimiento, la retención legal y los fines de auditoría. Los mensajes y los archivos se pueden archivar en un almacén de datos seguro y controlado por el cliente.

Acceso flexible

Los usuarios tienen acceso a varios dispositivos (móviles, de escritorio) y pueden funcionar en entornos con poco ancho de banda, incluidos los de desconexión y de comunicación. out-of-band

Controles administrativos

Los usuarios tienen un control administrativo integral sobre los datos, lo que incluye configuración de permisos, configuración de opciones de mensajería efímera responsable y definición de grupos de seguridad.

Potentes integraciones y bots

Wickr se integra con servicios adicionales como Active Directory, inicio de sesión único (SSO) con OpenID Connect (OIDC) y más. Los clientes pueden crear y administrar rápidamente una red de Wickr a través de los AWS Management Console robots de Wickr y automatizarlos de forma segura.

A continuación se presenta un desglose de las ofertas de colaboración de Wickr:

- Mensajería individual y grupal: chatee de forma segura con su equipo en salas con hasta 500 miembros
- Llamadas de audio y vídeo: realice conferencias telefónicas con hasta 70 personas
- Transmisión y uso compartido de pantalla: preséntese con hasta 500 participantes
- Compartir y guardar archivos: transfiera hasta 5 archivos GBs con almacenamiento ilimitado
- Efímero: controle la caducidad y los temporizadores burn-on-read
- Federación global: conéctese con usuarios de Wickr fuera de su red

Disponibilidad regional

Wickr está disponible en EE. UU. Este (Virginia del Norte), Asia Pacífico (Malasia), Asia Pacífico (Singapur), Asia Pacífico (Sídney), Asia Pacífico (Tokio), Canadá (Central), Europa (Fráncfort), Europa (Londres), Europa (Estocolmo) y Europa (Zúrich). Regiones de AWS Wickr también está disponible en la región AWS GovCloud (EE. UU.-Oeste). Cada región contiene varias zonas de disponibilidad, que están separadas físicamente pero conectadas mediante conexiones de red privadas, de baja latencia, de gran ancho de banda y redundantes. Estas zonas de disponibilidad se utilizan para proporcionar una mayor disponibilidad, tolerancia a errores y una latencia minimizada.

Para obtener más información Regiones de AWS, consulte Especificar qué Regiones de AWS cuenta puede usar en el. Referencia general de AWS Para obtener más información sobre la cantidad de zonas de disponibilidad disponibles en cada región, consulte Infraestructura AWS global.

Acceso a Wickr

Los administradores acceden a AWS Management Console ellas para Wickr en https://console.aws.amazon.com/wickr/. Antes de empezar a usar Wickr, debe completar las guías Configuración de AWS Wickr y Introducción a AWS Wickr.

> **Note**
>
> El acceso a la API de Wickr solo está disponible para Wickr Enterprise (autohospedado) y no para AWS Wickr.

Los usuarios finales acceden a Wickr a través del cliente de Wickr. Para obtener más información, consulte la Guía del usuario de AWS Wickr.

Precios

Wickr está disponible en diferentes planes para individuos, equipos pequeños y grandes empresas. Para obtener más información, consulte Precios de AWS Wickr.

Documentación para el usuario final de Wickr

Si es un usuario final del cliente de Wickr y necesita acceder a su documentación, consulte la Guía del usuario de AWS Wickr.

Configuración de AWS Wickr

Si es un AWS cliente nuevo, complete los requisitos previos de configuración que se indican en esta página antes de empezar a usar AWS Wickr. Para estos procedimientos de configuración, utiliza el servicio AWS Identity and Access Management (IAM). Para obtener información completa sobre IAM, consulte la Guía del usuario de IAM.

Temas

- Inscríbase en AWS
- Creación un usuario de IAM
- Siguientes pasos

Inscríbase en AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

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

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

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. 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 y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Creación un usuario de IAM

Para crear un usuario administrador, elija una de las siguientes opciones.

Elegir una forma de administrar el administrador	Para	Haga esto	También puede
En IAM Identity Center (recomendado)	Usar credenciales a corto plazo para acceder a AWS. Esto se ajusta a las prácticas recomendadas de seguridad. Para obtener información sobre las prácticas recomendadas, consulta Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.	Siga las instrucciones en Introducción en la Guía del usuario de AWS IAM Identity Center .	Configure el acceso programático configurando el AWS CLI que se utilizará AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario.
En IAM (no recomendado)	Usar credenciales a largo plazo para acceder a AWS.	Siga las instrucci ones en Creación del primer grupo de usuarios y usuario de administrador de IAM en la Guía del usuario de IAM.	Configure el acceso programático mediante Administr ación de las claves de acceso de los usuarios de IAM en la Guía del usuario de IAM.

> **Note**
>
> También puede asignar la política administrada de `AWSWickrFullAccess` para conceder todos los permisos administrativos al servicio Wickr. Para obtener más información, consulte AWS política gestionada: AWSWickr FullAccess.

Siguientes pasos

Ha completado los pasos de configuración de requisito previo. Para empezar a configurar Wickr, consulte Introducción.

Introducción a AWS Wickr

En esta guía le mostramos cómo comenzar a utilizar Wickr, crear una red, configurarla y crear usuarios.

Temas

- Requisitos previos
- Paso 1: crear una red
- Paso 2: configurar su red
- Paso 3: crear e invitar a usuarios

Requisitos previos

Antes de empezar, asegúrese de que cumple los requisitos siguientes si no lo ha hecho todavía:

- Registro en Amazon Web Services (AWS) Para obtener más información, consulte Configuración de AWS Wickr.
- Compruebe que tiene los permisos necesarios para administrar Wickr. Para obtener más información, consulte AWS política gestionada: AWSWickr FullAccess.
- No se olvide de incluir en la lista de puertos y dominios permitidos los apropiados para Wickr. Para obtener más información, consulte Lista de puertos y dominios a permitir para tu red Wickr.

Paso 1: crear una red

Puedes crear una red Wickr.

Siga el procedimiento que se indica a continuación para crear una red de Wickr para la cuenta.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/

> **Note**
>
> Si no ha creado una red de Wickr anteriormente, verá la página informativa del servicio de Wickr. Después de crear una o más redes de Wickr, verá la página Redes, con una lista de todas las redes de Wickr que ha creado.

2. Elija Crear una red.
3. Introduzca un nombre para la red en el cuadro de texto Nombre de la red. Seleccione un nombre significativo para los miembros de su organización, como el de su empresa o equipo.
4. Elija un plan. Puede elegir uno de los siguientes planes de red de Wickr:

   - Estándar: para equipos de pequeñas y grandes empresas que necesitan flexibilidad y controles administrativos.
   - Prueba gratuita Premium o Premium: para empresas que requieren los límites de funciones más altos, controles administrativos detallados y retención de datos.

   Los administradores tienen la opción de seleccionar una versión de prueba gratuita premium, que está disponible para un máximo de 30 usuarios y dura tres meses. Para AWS WickrGov ello, la opción de prueba gratuita premium permite hasta 50 usuarios y también dura tres meses. Durante el período de prueba premium gratuito, los administradores pueden actualizar o bajar de categoría a los planes Premium o Estándar.

   Para obtener más información sobre los planes y precios de Wickr disponibles, visite la página de precios de Wickr.
5. (Opcional) Seleccione Agregar nueva etiqueta si desea agregar una etiqueta a su red. Las etiquetas constan de un par clave-valor. Las etiquetas se pueden usar para buscar y filtrar los recursos o para un seguimiento de los costos de AWS . Para obtener más información, consulte Etiquetas de red.
6. Seleccione Crear red.

   Se te redirigirá a la página de redes AWS Management Console de Wickr y la nueva red aparecerá en la página.

Paso 2: configurar su red

Complete el siguiente procedimiento AWS Management Console para acceder a Wickr, donde podrá agregar usuarios, agregar grupos de seguridad, configurar el SSO, configurar la retención de datos y otros ajustes de red.

1. En la página Redes, selecciona el nombre de la red para ir a esa red.

   Se le redirigirá a la consola de administración de Wickr de la red seleccionada.

2. Están disponibles las siguientes opciones de administración de usuarios. Para obtener más información sobre la configuración de estos ajustes, consulte Cómo administrar su red de AWS Wickr.

   - Grupo de seguridad: administre los grupos de seguridad y su configuración, como las políticas de complejidad de contraseñas, las preferencias de mensajería, las características de llamada, las características de seguridad y la federación externa. Para obtener más información, consulte Grupos de seguridad para AWS Wickr .
   - Configuración de inicio de sesión único (SSO): configure el SSO y vea la dirección del punto final de su red Wickr. Wickr solo es compatible con los proveedores de SSO que utilizan OpenID Connect (OIDC). No se admiten los proveedores que utilizan lenguaje de marcado para configuraciones de seguridad (SAML). Para obtener más información, consulte Configuración de inicio de sesión único para AWS Wickr.

Paso 3: crear e invitar a usuarios

Para crear usuarios en la red de Wickr puede utilizar los métodos siguientes:

- Inicio de sesión único (SSO): si configura el SSO, puede invitar a usuarios compartiendo su ID de empresa de Wickr. Los usuarios finales se registran en Wickr con el ID de empresa proporcionado y su dirección de correo electrónico de empresa. Para obtener más información, consulte Configuración de inicio de sesión único para AWS Wickr.
- Invitación: puede crear usuarios manualmente en la AWS Management Console de Wickr y enviarles una invitación por correo electrónico. Los usuarios finales pueden registrarse en Wickr con el enlace del correo electrónico.

> **Note**
>
> También puede habilitar a usuarios invitados para su red de Wickr. Para obtener más información, consulte Usuarios invitados en la red AWS Wickr

Siga los procedimientos que se indican a continuación para crear usuarios o invitarlos.

> **Note**
>
> Se considera que los administradores también son usuarios y, por lo tanto, se les debe invitar a las redes de Wickr con SSO o sin SSO.

Para crear usuarios de Wickr y enviar invitaciones con el inicio de sesión único:

Escriba un correo electrónico y envíelo a los usuarios de SSO para que se registren en Wickr. En el mensaje, incluya la información siguiente:

- Su ID de empresa de Wickr. Al configurar el SSO, se especifica un ID de empresa de la red de Wickr. Para obtener más información, consulte Configurar el inicio de sesión único en AWS Wickr.
- La dirección de correo electrónico que deben usar para registrarse.
- La URL para descargar el cliente de Wickr. Los usuarios pueden descargar los clientes de Wickr desde la página de descargas de AWS Wickr en https://aws.amazon.com/wickr/ download/.

> **Note**
>
> Si creó su red Wickr en AWS GovCloud (EE. UU. al oeste), pida a sus usuarios que descarguen e instalen el cliente. WickrGov Para el resto de AWS regiones, pide a tus usuarios que descarguen e instalen el cliente Wickr estándar. Para obtener más información al respecto AWS WickrGov, consulte AWS WickrGovla Guía del AWS GovCloud (US) usuario.

Los usuarios que se van registrando en su red de Wickr se agregan al directorio del equipo de Wickr con el estado activo.

Para crear usuarios de Wickr manualmente y enviar invitaciones, siga estos pasos:

1. Abre el formulario AWS Management Console Wickr Cat https://console.aws.amazon.com/wickr/.
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.

   Se te redirigirá a la red Wickr. En la red Wickr, puedes agregar usuarios, agregar grupos de seguridad, configurar el SSO, configurar la retención de datos y ajustar ajustes adicionales.
3. En el panel de navegación, selecciona Administración de usuarios.

4. En la página de administración de usuarios, en la pestaña del directorio del equipo, selecciona Invitar usuario.

   También puedes invitar a usuarios de forma masiva seleccionando la flecha desplegable situada junto a Invitar a un usuario. En la página Invitar usuarios de forma masiva, selecciona Descargar plantilla para descargar una plantilla CSV que podrás editar y cargar con tu lista de usuarios.
5. Especifique el nombre y apellidos, el código de país, el número de teléfono y la dirección de correo electrónico del usuario. El único campo obligatorio es la dirección de correo electrónico. Asegúrese de elegir el grupo de seguridad adecuado para los usuarios.
6. Elija Invitar.

   Wickr envía al usuario un correo electrónico de invitación a la dirección que se especifique. El correo electrónico incluye enlaces para descargar las aplicaciones de cliente Wickr y un enlace para registrarse en Wickr. Para obtener más información sobre la experiencia del usuario final, consulte (Descargar la aplicación Wickr y aceptar la invitación en la Guía del usuario de AWS Wickr.

   A medida que los usuarios se registren en Wickr utilizando su enlace del correo electrónico, su estado en el directorio del equipo de Wickr cambiará de Pendiente a Activo.

Pasos a seguir a continuación

Ya ha completado los primeros pasos. Para administrar Wickr, consulta lo siguiente:

- Cómo administrar su red de AWS Wickr
- Cómo gestionar usuarios en AWS Wickr

Cómo administrar su red de AWS Wickr

En el caso AWS Management Console de Wickr, puede administrar el nombre de su red de Wickr, los grupos de seguridad, la configuración de SSO y la configuración de retención de datos.

Temas

- Detalles de la red de AWS Wickr
- Grupos de seguridad para AWS Wickr
- Configuración de inicio de sesión único para AWS Wickr
- Etiquetas de red para AWS Wickr
- Lea los recibos de AWS Wickr
- Gestione el plan de red para AWS Wickr
- Retención de datos para AWS Wickr
- ¿Qué es ATAK?
- Lista de puertos y dominios a permitir para tu red Wickr
- GovCloud clasificación y federación transfronterizas
- Vista previa del archivo AWS Wickr

Detalles de la red de AWS Wickr

Puedes editar el nombre de tu red de Wickr y ver tu ID de red en la sección de detalles de la red de Wickr. AWS Management Console

Temas

- Vea los detalles de la red en AWS Wickr
- Editar el nombre de la red en AWS Wickr
- Eliminar la red en AWS Wickr

Vea los detalles de la red en AWS Wickr

Puedes ver los detalles de tu red de Wickr, incluidos el nombre y el ID de la red.

Siga el procedimiento indicado a continuación para ver el perfil de su red de Wickr y el ID de la red.

1. Abre el formulario AWS Management Console Wickr en. https://console.aws.amazon.com/wickr/
2. En la página Redes, busca la red que deseas ver.
3. En la parte derecha de la red que quieres ver, selecciona el icono de puntos suspensivos verticales (tres puntos) y, a continuación, selecciona Ver detalles.

   La página de inicio de la red muestra el nombre y el ID de la red de Wickr en la sección de detalles de la red. Use el ID de red para configurar la federación.

Editar el nombre de la red en AWS Wickr

Puede editar el nombre de su red de Wickr.

Siga el procedimiento que se indica a continuación para editar el nombre de la red de Wickr.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página de redes, selecciona el nombre de la red para ir a la consola de administración de Wickr correspondiente a esa red.
3. En la página de inicio de la red, en la sección de detalles de la red, selecciona Editar.
4. Ingrese un nuevo nombre para la red en el cuadro de texto Nombre de la red.
5. Selecciona Guardar para guardar el nuevo nombre de la red.

Eliminar la red en AWS Wickr

Puede eliminar su red de AWS Wickr.

> **Note**
>
> Si elimina una red premium de prueba gratuita, no podrá crear otra.

Para eliminar tu red Wickr en la página de inicio de Redes, completa el siguiente procedimiento.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, busca la red que deseas eliminar.
3. En la parte derecha de la red que deseas eliminar, selecciona el icono de puntos suspensivos verticales (tres puntos) y, a continuación, selecciona Eliminar red.

4. Escribe confirmar en la ventana emergente y, a continuación, selecciona Eliminar.

   La red puede tardar unos minutos en eliminarse.

Para eliminar su red Wickr mientras está en la red, complete el siguiente procedimiento.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona la red que deseas eliminar.
3. Cerca de la esquina superior derecha de la página de inicio de la red, selecciona Eliminar red.
4. Escribe confirmar en la ventana emergente y, a continuación, selecciona Eliminar.

   La red puede tardar unos minutos en eliminarse.

> **Note**
>
> Los datos retenidos por su configuración de retención de datos (si está habilitada) no se eliminarán cuando elimine la red. Para obtener más información, consulte Retención de datos para AWS Wickr.

Grupos de seguridad para AWS Wickr

En la sección Grupos de seguridad de Wickr, puede administrar los AWS Management Console grupos de seguridad y su configuración, como las políticas de complejidad de las contraseñas, las preferencias de mensajería, las funciones de llamadas, las funciones de seguridad y la federación de redes.

Temas

- Ver los grupos de seguridad en AWS Wickr
- Crear un grupo de seguridad en AWS Wickr
- Edición de un grupo de seguridad en AWS Wickr
- Eliminar un grupo de seguridad en AWS Wickr

Ver los grupos de seguridad en AWS Wickr

Puede ver los detalles de sus grupos de seguridad de Wickr.

Siga el procedimiento indicado a continuación para ver los grupos de seguridad.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Grupos de seguridad.

   La página Grupos de seguridad muestra tus grupos de seguridad actuales de Wickr y te da la opción de crear uno nuevo.

   En la página Grupos de seguridad, selecciona el grupo de seguridad que deseas ver. La página mostrará los detalles actuales de ese grupo de seguridad.

Crear un grupo de seguridad en AWS Wickr

Puedes crear un nuevo grupo de seguridad de Wickr.

Siga el procedimiento indicado a continuación para crear un grupo de seguridad.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Grupos de seguridad.
4. En la página Grupos de seguridad, elija Crear grupo de seguridad para crear un grupo de seguridad nuevo.

   > **Note**
   >
   > Se agrega automáticamente un nuevo grupo de seguridad con un nombre predeterminado a la lista de grupos de seguridad.

5. En la página Crear grupo de seguridad, introduzca el nombre del grupo de seguridad.
6. Elija Creación de grupo de seguridad.

   Para más información sobre cómo editar el nuevo grupo de seguridad, consulte Edición de un grupo de seguridad en AWS Wickr.

Edición de un grupo de seguridad en AWS Wickr

Puede editar los detalles de su grupo de seguridad de Wickr.

Siga el procedimiento indicado a continuación para editar grupos de seguridad.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Grupos de seguridad.
4. Seleccione el nombre del grupo de seguridad que desee editar.

   La página de detalles del grupo de seguridad muestra la configuración del grupo de seguridad en diferentes pestañas.
5. Están disponibles las pestañas y la configuración correspondiente siguientes:

   - Detalles del grupo de seguridad: elija Editar en la sección de detalles del grupo de seguridad para editar el nombre.
   - Mensajería: sirve para gestionar las características de mensajería para los miembros del grupo.
     - B urn-on-read — Controla el valor máximo que los usuarios pueden establecer para sus burn-on-read temporizadores en sus clientes de Wickr. Para obtener más información, consulta Cómo configurar los temporizadores de caducidad y grabación de los mensajes en el cliente Wickr.
     - Temporizador de caducidad: controla el valor máximo que los usuarios pueden establecer para el temporizador de caducidad de los mensajes en sus clientes de Wickr. Para obtener más información, consulta Cómo configurar los temporizadores de caducidad y grabación de los mensajes en el cliente de Wickr.
     - Respuestas rápidas: establece una lista de respuestas rápidas para que los usuarios respondan a los mensajes.
     - Proteja la intensidad de la trituradora: configure la frecuencia con la que se ejecuta el control de la trituradora segura para los usuarios. Para obtener más información, consulte Mensajería.
   - Llamar: permite gestionar las características de llamada para los miembros del grupo.
     - Habilitar las llamadas de audio: los usuarios pueden iniciar llamadas de audio.
     - Habilita las videollamadas y el uso compartido de pantalla: los usuarios pueden iniciar videollamadas o compartir la pantalla durante una llamada.

  - Llamadas TCP: la activación (o la fuerza) de las llamadas TCP se suele utilizar cuando el departamento de TI o seguridad de una organización no permite los puertos UDP VoIP estándar. Si las llamadas TCP están deshabilitadas y los puertos UDP no están disponibles para su uso, los clientes de Wickr probarán primero con UDP y recurrirán a TCP.
- Medios y enlaces: administre la configuración relacionada con los medios y los enlaces para los miembros del grupo.

  Tamaño de descarga del archivo: seleccione Transferencia de mejor calidad para que los usuarios puedan transferir los archivos y adjuntos en su forma cifrada original. Si seleccionas Transferencia con poco ancho de banda, el servicio de transferencia de archivos de Wickr comprimirá los archivos adjuntos que envíen los usuarios de Wickr.
- Ubicación: administre la configuración de uso compartido de la ubicación para los miembros del grupo.

  Compartir la ubicación: los usuarios pueden compartir sus ubicaciones mediante dispositivos con GPS. Esta función muestra un mapa visual basado en los valores predeterminados del sistema operativo del dispositivo. Los usuarios tienen la opción de deshabilitar la visualización del mapa y, en su lugar, compartir un enlace que contenga sus coordenadas GPS.
- Seguridad: sirve para configurar las características de seguridad adicionales del grupo.
  - Habilite la protección contra el robo de cuentas: aplique una autenticación de dos factores cuando un usuario añada un nuevo dispositivo a su cuenta. Para verificar un dispositivo nuevo, el usuario puede generar un código Wickr desde su dispositivo anterior o realizar una verificación por correo electrónico. Se trata de una capa de seguridad adicional para evitar el acceso no autorizado a las cuentas de AWS Wickr.
  - Habilite siempre la reautenticación: obligue a los usuarios a volver a autenticarse siempre cuando vuelvan a ingresar a la aplicación.
  - Clave maestra de recuperación: crea una clave maestra de recuperación cuando se crea una cuenta. Los usuarios pueden aprobar la adición de un nuevo dispositivo a su cuenta si no hay otros dispositivos disponibles.
- Notificación y visibilidad: configure los ajustes de notificación y visibilidad, como las vistas previas de los mensajes en las notificaciones de los miembros del grupo.
- Acceso abierto de Wickr: configura los ajustes de acceso abierto de Wickr para los miembros del grupo.
  - Habilitar el acceso abierto de Wickr: habilitar el acceso abierto de Wickr ocultará el tráfico para proteger los datos en redes restringidas y monitoreadas. Según la ubicación

geográfica, el acceso abierto de Wickr se conectará a varios servidores proxy globales que ofrecen la mejor ruta y protocolos para ocultar el tráfico.

- Forzar el acceso abierto de Wickr: habilita y aplica automáticamente el acceso abierto de Wickr en todos los dispositivos.

- Federación: controle la capacidad de sus usuarios para comunicarse con otras redes de Wickr.
  - Federación local: la capacidad de federarse con AWS usuarios de otras redes de la misma región. Por ejemplo, si hay dos redes en la región de AWS Canadá (Central) con la federación local habilitada, podrán comunicarse entre sí.
  - Federación global: la posibilidad de federarse con usuarios de Wickr Enterprise o AWS con usuarios de una red diferente que pertenezcan a otras regiones. Por ejemplo, un usuario de una red de Wickr en la región de AWS Canadá (Central) y un usuario de una red de la región de AWS Europa (Londres) podrán comunicarse entre sí cuando la federación global esté activada para ambas redes.
  - Federación restringida: permite enumerar redes específicas de AWS Wickr o Wickr Enterprise con las que los usuarios pueden federarse. Cuando se configura, los usuarios solo pueden comunicarse con usuarios externos en las redes permitidas de la lista. Ambas redes deben permitir que se enumeren entre sí para utilizar la federación restringida.

    Para obtener información sobre la federación de invitados, consulte Habilitar o deshabilitar usuarios invitados en la red de AWS Wickr.
- Configuración del complemento ATAK: para obtener más información sobre cómo habilitar ATAK, consulte ¿Qué es ATAK? .

6. Seleccione Guardar para guardar las modificaciones que realice en los detalles del grupo de seguridad.

Eliminar un grupo de seguridad en AWS Wickr

Puedes eliminar tu grupo de seguridad de Wickr.

Siga el procedimiento indicado a continuación para eliminar un grupo de seguridad.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Grupos de seguridad.

4. En la página Grupos de seguridad, busque el grupo de seguridad que desee eliminar.
5. En la parte derecha del grupo de seguridad que desee eliminar, seleccione el icono de puntos suspensivos verticales (tres puntos) y, a continuación, elija Eliminar.
6. Escriba confirmar en la ventana emergente y, a continuación, seleccione Eliminar.

   Si se elimina un grupo de seguridad que tiene usuarios asignados, dichos usuarios se agregarán automáticamente al grupo de seguridad predeterminado. Para modificar el grupo de seguridad asignado a los usuarios, consulte Edición de usuarios en la red AWS Wickr.

Configuración de inicio de sesión único para AWS Wickr

En el caso de Wickr, puede configurar Wickr AWS Management Console para que utilice un sistema de inicio de sesión único para autenticarse. El SSO proporciona una capa de seguridad adicional cuando se combina con un sistema de autenticación multifactor (MFA) adecuado. Wickr solo es compatible con los proveedores de SSO que utilizan OpenID Connect (OIDC). No se admiten los proveedores que utilizan lenguaje de marcado para configuraciones de seguridad (SAML).

Temas

- Vea los detalles del SSO en AWS Wickr
- Configurar el inicio de sesión único en AWS Wickr
- Periodo de gracia para la actualización del token

Vea los detalles del SSO en AWS Wickr

Puede ver los detalles de la configuración de inicio de sesión único para su red de Wickr y el punto final de la red.

Siga el procedimiento indicado a continuación para ver la configuración de inicio de sesión único actual de la red Wickr, si la hay.

1. Abre el formulario Wickr en AWS Management Console . https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.

   En la página de administración de usuarios, la sección de inicio de sesión único muestra tu terminal de red Wickr y la configuración de SSO actual.

Configurar el inicio de sesión único en AWS Wickr

Para garantizar un acceso seguro a su red de Wickr, puede configurar su configuración de inicio de sesión único actual. Hay guías detalladas disponibles para ayudarte en este proceso.

Para obtener más información sobre la configuración del SSO, consulta las siguientes guías:

> **Important**
>
> Al configurar el SSO, se especifica un ID de empresa para la red de Wickr. Asegúrese de escribir el ID de su empresa de su red de Wickr. Debe proporcionárselo a sus usuarios finales cuando envíe los correos electrónicos de invitación. Los usuarios finales deben especificar el ID de su empresa cuando se registren en su red de Wickr.

- Configuración del inicio de sesión único (SSO) de AWS Wickr con Microsoft Entra (Azure AD)
- Configuración del inicio de sesión único (SSO) de AWS Wickr con Okta
- Configuración del inicio de sesión único (SSO) de AWS Wickr con Amazon Cognito

Configuración de AWS Wickr con el inicio de sesión único de Microsoft Entra (Azure AD)

AWS Wickr se puede configurar para usar Microsoft Entra (Azure AD) como proveedor de identidades. Para ello, complete los siguientes procedimientos tanto en Microsoft Entra como en la consola de administración de AWS Wickr.

> **Warning**
>
> Cuando se habilita el SSO en una red, se cierra la sesión de los usuarios activos en Wickr y se les obliga a volver a autenticarse con el proveedor de SSO.

Paso 1: Registrar AWS Wickr como aplicación en Microsoft Entra

Complete el siguiente procedimiento para registrar AWS Wickr como aplicación en Microsoft Entra.

> **Note**
>
> Consulte la documentación de Microsoft Entra para obtener capturas de pantalla detalladas y solucionar problemas. Para obtener más información, consulte Registrar una aplicación en la plataforma de identidad de Microsoft

1. En el panel de navegación, elija Aplicaciones y, a continuación, Registros de aplicaciones.
2. En la página de registros de aplicaciones, elija Registrar una aplicación y, a continuación, introduzca el nombre de la aplicación.
3. Seleccione solo las cuentas de este directorio organizativo (solo en el directorio predeterminado: arrendatario único).
4. En URI de redireccionamiento, selecciona Web y, a continuación, introduce la siguiente dirección web:`https://messaging-pro-prod.wickr.com/deeplink/oidc.php`.

   > **Note**
   >
   > El URI de redireccionamiento también se puede copiar de los ajustes de configuración del SSO en la consola de administración de AWS Wickr.

5. Elija Registro.
6. Tras el registro, copie o guarde el ID de aplicación (cliente) generado.

7. Seleccione la pestaña Endpoints para tomar nota de lo siguiente:

   1. Punto final de autorización de Oauth 2.0 (v2): Por ejemplo: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
   2. Edita este valor para eliminar los caracteres «oauth2/» y «autorizar». Por ejemplo, la URL fija tendrá este aspecto: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
   3. Se hará referencia a esto como el emisor del SSO.

Paso 2: Configurar la autenticación

Complete el siguiente procedimiento para configurar la autenticación en Microsoft Entra.

1. En el panel de navegación, elija Autenticación.
2. En la página de autenticación, asegúrese de que el URI de redireccionamiento web sea el mismo que el introducido anteriormente (en Registrar AWS Wickr como aplicación).
3. Seleccione los identificadores de acceso que se utilizan para los flujos implícitos y los identificadores de identificación que se utilizan para los flujos implícitos e híbridos.
4. Seleccione Save.

Paso 3: Configurar certificados y secretos

Complete el siguiente procedimiento para configurar los certificados y secretos en Microsoft Entra.

1. En el panel de navegación, elija Certificados y secretos.
2. En la página Certificados y secretos, seleccione la pestaña Secretos del cliente.
3. En la pestaña Secretos del cliente, selecciona Nuevo secreto de cliente.
4. Introduce una descripción y selecciona un período de caducidad para el secreto.
5. Elija Agregar.
6. Una vez creado el certificado, copie el valor secreto del cliente.

> **Note**
>
> Se necesitará el valor secreto del cliente (no el identificador secreto) para el código de la aplicación cliente. Es posible que no pueda ver ni copiar el valor secreto después de salir de esta página. Si no lo copias ahora, tendrás que volver a crear un nuevo secreto de cliente.

Paso 4: Configurar la configuración del token

Complete el siguiente procedimiento para configurar el token en Microsoft Entra.

1. En el panel de navegación, elija la configuración del token.
2. En la página de configuración del token, selecciona Añadir reclamación opcional.

3. En Reclamaciones opcionales, selecciona el tipo de token como ID.
4. Después de seleccionar el ID, en Reclamar, selecciona correo electrónico y nombre de usuario.
5. Elija Agregar.

Paso 5: Configurar los permisos de la API

Complete el siguiente procedimiento para configurar los permisos de la API en Microsoft Entra.

1. En el panel de navegación, elija Permisos de API.
2. En la página de permisos de la API, selecciona Añadir un permiso.

3. Seleccione Microsoft Graph y, a continuación, seleccione Permisos delegados.
4. Selecciona la casilla de verificación de email, offline_access, openid o profile.
5. Elija Añadir permisos.

Paso 6: Exponer una API

Complete el siguiente procedimiento para mostrar una API para cada uno de los 4 ámbitos de Microsoft Entra.

1. En el panel de navegación, selecciona Exponer una API.
2. En la página Exponer una API, selecciona Añadir un ámbito.

   El URI del ID de la aplicación debe rellenarse automáticamente y el ID que sigue al URI debe coincidir con el ID de la aplicación (creado en Register AWS Wickr como aplicación).

3. Elija Guardar y continuar.
4. Seleccione la etiqueta Administradores y usuarios y, a continuación, introduzca el nombre del ámbito como offline_access.
5. Selecciona Estado y, a continuación, selecciona Activar.
6. Selecciona Añadir ámbito.
7. Repita los pasos 1 a 6 de esta sección para añadir los siguientes ámbitos: correo electrónico, openid y perfil.

8. En Aplicaciones cliente autorizadas, elija Agregar una aplicación cliente.
9. Seleccione los cuatro ámbitos creados en el paso anterior.
10. Introduzca o verifique el ID de la aplicación (cliente).
11. Elija Agregar aplicación.

Paso 7: Configuración de AWS Wickr SSO

Complete el siguiente procedimiento de configuración en la consola de AWS Wickr.

1. Abra el formulario AWS Management Console Wickr en. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, selecciona Administración de usuarios y, a continuación, selecciona Configurar el SSO.
4. En Punto final de red, asegúrese de que el URI de redireccionamiento coincida con la siguiente dirección web (que se agregó en el paso 4 en Registrar AWS Wickr como aplicación).

   `https://messaging-pro-prod.wickr.com/deeplink/oidc.php`.
5. Escriba la información siguiente:

   - Emisor: es el punto final que se modificó anteriormente (p. ej.). `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
   - ID de cliente: es el ID de la aplicación (cliente) del panel de información general.
   - Secreto de cliente (opcional): es el secreto de cliente del panel Certificados y secretos.
   - Ámbitos: son los nombres de los ámbitos que aparecen en el panel Exponer una API. Introduzca el correo electrónico, el perfil, offline_access y openid.
   - Ámbito de nombre de usuario personalizado (opcional): introduce upn.
   - ID de la empresa: puede ser un valor de texto único que incluya caracteres alfanuméricos y de subrayado. Esta frase es la que introducirán los usuarios cuando se registren en dispositivos nuevos.

   Los demás campos son opcionales.
6. Elija Siguiente.

7. Compruebe los detalles en la página Revisar y guardar y, a continuación, seleccione Guardar cambios.

La configuración del SSO está completa. Para comprobarlo, ahora puede añadir un usuario a la aplicación en Microsoft Entra e iniciar sesión con el usuario mediante el inicio de sesión único y el identificador de empresa.

Para obtener más información sobre cómo invitar e incorporar usuarios, consulte Crear e invitar usuarios.

Solución de problemas

A continuación, se muestran los problemas más comunes que pueden surgir y sugerencias para resolverlos.

- La prueba de conexión SSO falla o no responde:
  - Asegúrese de que el emisor del SSO esté configurado según lo esperado.
  - Asegúrese de que los campos obligatorios del SSO configurado estén configurados según lo esperado.
- La prueba de conexión se ha realizado correctamente, pero el usuario no puede iniciar sesión:
  - Asegúrese de que el usuario esté agregado a la aplicación Wickr que registró en Microsoft Entra.
  - Asegúrese de que el usuario utiliza el identificador de empresa correcto, incluido el prefijo. Por ejemplo, UE1 DemoNetwork w_DRQTVA.
  - Es posible que el secreto de cliente no esté configurado correctamente en la configuración de AWS Wickr SSO. Vuelva a configurarlo creando otro secreto de cliente en Microsoft Entra y establezca el nuevo secreto de cliente en la configuración de SSO de Wickr.

Periodo de gracia para la actualización del token

Los proveedores de identidad pueden sufrir interrupciones temporales o prolongadas. Como consecuencia de ello, la sesión de los usuarios se puede cerrar de forma inesperada debido a un error en el token de actualización de la sesión de cliente. Para evitar este problema, puede establecer un período de gracia que permita a sus usuarios mantener la sesión iniciada incluso en caso de error del token de actualización del cliente durante dichas interrupciones.

Las opciones disponibles para el período de gracia son las siguientes:

- Sin período de gracia (opción predeterminada): la sesión de los usuarios se cerrará inmediatamente después del error de token de actualización.
- Período de gracia de 30 minutos: los usuarios pueden permanecer conectados hasta 30 minutos después del error de token de actualización.
- Período de gracia de 60 minutos: los usuarios pueden permanecer conectados hasta 60 minutos después del error de token de actualización.

Etiquetas de red para AWS Wickr

Es posible aplicar etiquetas a las redes de Wickr, Luego puedes usar esas etiquetas para buscar y filtrar tus redes de Wickr o hacer un seguimiento de tus AWS costos. Puedes configurar las etiquetas de red en la página de inicio de la red de AWS Management Console Wickr.

Una etiqueta es un par clave-valor que se aplica a un recurso para almacenar metadatos sobre ese recurso. Cada etiqueta consta de una clave y un valor. Para más información sobre las etiquetas, consulte también ¿Qué son las etiquetas? y Casos de uso de etiquetado.

Temas

- Administrar etiquetas de red en AWS Wickr
- Añadir una etiqueta de red en AWS Wickr
- Edición de una etiqueta de red en AWS Wickr
- Eliminar una etiqueta de red en AWS Wickr

Administrar etiquetas de red en AWS Wickr

Puede administrar las etiquetas de red de su red de Wickr.

Siga el procedimiento indicado a continuación para administrar las etiquetas de red en su red Wickr.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En la página de inicio de la red, en la sección Etiquetas, selecciona Administrar etiquetas.
4. En la página Administrar etiquetas, puede completar una de las siguientes opciones:
    - Agregar etiquetas nuevas: escriba nuevas etiquetas en forma de pares clave-valor. Seleccione Agregar nueva etiqueta para añadir varios pares clave-valor. Las etiquetas distinguen entre

mayúsculas y minúsculas. Para obtener más información, consulte Añadir una etiqueta de red en AWS Wickr.

- Editar las etiquetas existentes: seleccione el texto de la clave o el valor de una etiqueta existente y, a continuación, modifique la información necesaria en el cuadro de texto. Para obtener más información, consulte Edición de una etiqueta de red en AWS Wickr.
- Eliminar etiquetas existentes: haga clic en el botón Eliminar junto a la etiqueta que desee eliminar. Para obtener más información, consulte Eliminar una etiqueta de red en AWS Wickr.

Añadir una etiqueta de red en AWS Wickr

Puedes añadir una etiqueta de red a tu red de Wickr.

Siga el procedimiento que se indica a continuación para agregar etiquetas a la red de Wickr. Para más información sobre la administración de etiquetas, consulte Administrar etiquetas de red en AWS Wickr.

1. En la página de inicio de la red, en la sección Etiquetas, selecciona Añadir nueva etiqueta.
2. En la página Administración de etiquetas, seleccione Agregar nueva etiqueta.
3. En los campos Clave y Valor que estén vacíos, indique el nuevo par de clave-valor de la etiqueta.
4. Seleccione Guardar cambios para guardar las nuevas etiquetas.

Edición de una etiqueta de red en AWS Wickr

Puedes editar una etiqueta de red en tu red de Wickr.

Siga el procedimiento indicado a continuación para editar etiquetas asociadas a la red de Wickr. Para más información sobre la administración de etiquetas, consulte Administrar etiquetas de red en AWS Wickr.

1. En la página Administrar etiquetas, edite el valor de la etiqueta.

> **Note**
>
> No es posible editar las claves de las etiquetas. En su lugar, elimine el par de clave-valor y agregue una nueva etiqueta con la nueva clave.

2. Elija Guardar cambios para guardar las modificaciones.

Eliminar una etiqueta de red en AWS Wickr

Puedes eliminar una etiqueta de red de tu red de Wickr.

Siga el procedimiento indicado a continuación para eliminar etiquetas de red de Wickr. Para más información sobre la administración de etiquetas, consulte Administrar etiquetas de red en AWS Wickr.

1. En la página Administrar etiquetas, elija Eliminar junto a las etiquetas que desee suprimir.
2. Elija Guardar cambios para guardar las modificaciones.

Lea los recibos de AWS Wickr

Las confirmaciones de lectura de AWS Wickr son notificaciones que se envían al remitente para mostrar cuándo se ha leído su mensaje. Estos recibos están disponibles en one-on-one las conversaciones. Aparecerá una sola marca de verificación para los mensajes enviados y un círculo continuo con una marca de verificación para los mensajes leídos. Para ver las confirmaciones de lectura de los mensajes durante las conversaciones externas, ambas redes deben tener habilitadas las confirmaciones de lectura.

Los administradores pueden activar o desactivar las confirmaciones de lectura en el panel de administración. Esta configuración se aplicará a toda la red.

Complete el siguiente procedimiento para activar o desactivar las confirmaciones de lectura.

1. Abre el formulario AWS Management Console Wickr Cat https://console.aws.amazon.com/wickr/.
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Políticas de red.
4. En la página Políticas de red, en la sección Mensajería, elija Editar.
5. Selecciona la casilla de verificación para activar o desactivar las confirmaciones de lectura.
6. Seleccione Save changes (Guardar cambios).

Gestione el plan de red para AWS Wickr

En el caso AWS Management Console de Wickr, puede administrar su plan de red en función de las necesidades de su empresa.

Para administrar su plan de red, complete el siguiente procedimiento.

1. Abra el formulario AWS Management Console Wickr Cat https://console.aws.amazon.com/wickr/.
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En la página de inicio de la red, en la sección Detalles de la red, selecciona Editar.
4. En la página Editar detalles de la red, selecciona el plan de red que desees. Puede modificar su plan de red actual seleccionando una de las siguientes opciones:

   - Estándar: para equipos de pequeñas y grandes empresas que necesitan flexibilidad y controles administrativos.
   - Prueba gratuita Premium o Premium: para empresas que requieren los límites de funciones más altos, controles administrativos detallados y retención de datos.

     Los administradores tienen la opción de seleccionar una versión de prueba gratuita premium, que está disponible para un máximo de 30 usuarios y dura tres meses. Para AWS WickrGov ello, la opción de prueba gratuita premium permite hasta 50 usuarios y también dura tres meses. Esta oferta está abierta a planes nuevos y estándar. Durante el período de prueba premium gratuito, los administradores pueden actualizar o bajar de categoría a los planes Premium o Estándar

     > **Note**
     >
     > Para detener el uso y la facturación en su red, elimine todos los usuarios de la red, incluidos los usuarios suspendidos.

Limitaciones de la prueba gratuita de Premium

La prueba gratuita premium tiene las siguientes limitaciones:

- Si un plan ha estado inscrito anteriormente en una prueba gratuita premium, no será elegible para otra prueba.
- Solo se puede inscribir una red para cada AWS cuenta en una prueba gratuita premium.

- La función de usuario invitado no está disponible durante la prueba gratuita premium.
- Si una red estándar tiene más de 30 usuarios (más de 50 usuarios AWS WickrGov), no será posible pasarse a una versión de prueba gratuita premium.

Retención de datos para AWS Wickr

Según la retención de datos de AWS Wickr, se pueden conservar todas las conversaciones en la red. Esto incluye las conversaciones a través de mensajería directa y las de grupos o salas entre miembros de la red (internos) y miembros de otros equipos (externos) con los que la red comparta una federación. La retención de datos solo está disponible para los usuarios del plan Premium de AWS Wickr y los clientes empresariales que elijan la retención de datos. Para más información sobre el plan Premium, consulte Tarifas de Wickr.

Cuando un administrador de red configure y active la retención de datos para su red, todos los mensajes y archivos compartidos en su red se conservarán de acuerdo con las políticas de cumplimiento de la organización. El administrador de la red puede acceder a los archivos .txt generados en una ubicación externa (por ejemplo, en almacenamiento local, bucket de Amazon S3 o cualquier otro almacenamiento que elija el usuario); desde allí, se pueden analizar, borrar o transferir.

> **Note**
>
> Wickr no accede nunca a sus mensajes y archivos. Por lo tanto, es su responsabilidad configurar un sistema de retención de datos.

Temas

- Vea los detalles de retención de datos en AWS Wickr
- Configurar la retención de datos para AWS Wickr
- Obtenga los registros de retención de datos para su red Wickr
- Métricas y eventos de retención de datos para su red de Wickr

Vea los detalles de retención de datos en AWS Wickr

Siga el procedimiento indicado a continuación para consultar la información relativa a la retención de datos de su red de Wickr. También puede habilitar o deshabilitar la retención de datos para su red de Wickr.

1. Abre el formulario AWS Management Console Wickr Cat https://console.aws.amazon.com/wickr/.
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Políticas de red.
4. La página de políticas de red muestra los pasos para configurar la retención de datos y la opción de activar o desactivar la función de retención de datos. Para más información sobre cómo configurar la retención de datos, consulte Configurar la retención de datos para AWS Wickr.

> **Note**
>
> Cuando la retención de datos esté activada, se mostrará el mensaje Retención de datos activada a todos los usuarios de la red, notificándoles que la red se ha habilitado para la retención de datos.

Configurar la retención de datos para AWS Wickr

Para configurar la retención de datos para su red de AWS Wickr, debe implementar la imagen de Docker del bot de retención de datos en un contenedor de un host, como un ordenador local o una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Una vez que se ha implementado el bot, puede configurarlo para que almacene datos de forma local o en un bucket de Amazon Simple Storage Service (Amazon S3). También puedes configurar el bot de retención de datos para que utilice otros AWS servicios como AWS Secrets Manager (Secrets Manager), Amazon CloudWatch (CloudWatch), Amazon Simple Notification Service (Amazon SNS) y (). AWS Key Management Service AWS KMS Los siguientes temas describen cómo configurar y ejecutar el bot de retención de datos para su red Wickr.

Temas

- Requisitos previos para configurar la retención de datos para AWS Wickr
- Contraseña para el bot de retención de datos en AWS Wickr
- Opciones de almacenamiento para la red AWS Wickr
- Variables de entorno para configurar el bot de retención de datos en AWS Wickr
- Valores de Secrets Manager para AWS Wickr
- Política de IAM para utilizar la retención de datos con los servicios de AWS
- Inicie el bot de retención de datos para su red Wickr
- Detenga el bot de retención de datos de su red Wickr

Requisitos previos para configurar la retención de datos para AWS Wickr

Antes de empezar, debe obtener el nombre del bot de retención de datos (denominado Nombre de usuario) y la contraseña inicial de Wickr AWS Management Console . Debe especificar estos dos valores la primera vez que inicie el bot de retención de datos. También debe habilitar la retención de datos en la consola. Para obtener más información, consulte Vea los detalles de retención de datos en AWS Wickr.

Contraseña para el bot de retención de datos en AWS Wickr

La primera vez que inicie el bot de retención de datos, especifique la contraseña inicial mediante una de las siguientes opciones:

- La variable de entorno `WICKRIO_BOT_PASSWORD`. Las variables de entorno del bot de retención de datos se describen en la sección Variables de entorno para configurar el bot de retención de datos en AWS Wickr que aparece más adelante en esta guía.
- El valor de la contraseña de Secrets Manager identificada por la variable de entorno `AWS_SECRET_NAME`. Los valores de Secrets Manager para el bot de retención de datos se describen en la sección Valores de Secrets Manager para AWS Wickr que aparece más adelante en esta guía.
- Introduzca la contraseña cuando el bot de retención de datos se lo pida. Deberá ejecutar el bot de retención de datos con acceso TTY interactivo mediante la opción `-ti`.

Cuando configure el bot de retención de datos por primera vez, se generará una nueva contraseña. Si necesita volver a instalar el bot de retención de datos, use la contraseña generada. La contraseña inicial no es válida después de la instalación inicial del bot de retención de datos.

La nueva contraseña generada se mostrará como se indica en el siguiente ejemplo.

> **Important**
>
> Guarde la contraseña en un lugar seguro. Si pierde la contraseña, no podrá volver a instalar el bot de retención de datos. No comparta esta contraseña. Ofrece la posibilidad de iniciar la retención de datos para su red Wickr.

```
*****************************************************************
**** GENERATED PASSWORD
```

```
**** DO NOT LOSE THIS PASSWORD, YOU WILL NEED TO ENTER IT EVERY TIME
**** TO START THE BOT
 "HuEXAMPLERAW4lGgEXAMPLEn"
 ******************************************************************
```

Opciones de almacenamiento para la red AWS Wickr

Una vez que la retención de datos esté habilitada y el bot de retención de datos esté configurado para su red Wickr, capturará todos los mensajes y archivos enviados dentro de su red. Los mensajes se guardan en archivos que están limitados a un tamaño o límite de tiempo específicos que se pueden configurar mediante una variable de entorno. Para obtener más información, consulte Variables de entorno para configurar el bot de retención de datos en AWS Wickr.

Puede configurar una de las opciones siguientes para almacenar estos datos:

- Almacene todos los mensajes y archivos capturados de forma local. Esta es la opción predeterminada. Es responsabilidad suya desplazar los archivos locales a otro sistema para almacenarlos a largo plazo y asegurarse de que el disco host no se quede sin memoria ni espacio.
- Almacene todos los mensajes y archivos capturados en un bucket de Amazon S3. El bot de retención de datos guardará todos los mensajes y archivos descifrados en el bucket de Amazon S3 que especifique. Los mensajes y archivos capturados se eliminan de la máquina host una vez guardados correctamente en el bucket.
- Almacene todos los mensajes capturados y archivos cifrados en un bucket de Amazon S3. El bot de retención de datos volverá a cifrar todos los mensajes y archivos capturados con una clave que usted proporcione, y los guardará en el bucket de Amazon S3 que especifique. Los mensajes y archivos capturados se eliminan de la máquina host una vez cifrados de nuevo y guardados correctamente en el bucket. Necesitará un software para descifrar los mensajes y archivos.

  Para obtener más información acerca de la creación de un bucket para usar su bot de retención de datos de Amazon S3, consulte la sección Creación de un bucket en la Guía del usuario de Amazon S3

Variables de entorno para configurar el bot de retención de datos en AWS Wickr

Puede usar las siguientes variables de entorno para configurar el bot de retención de datos. Estas variables de entorno se configuran mediante la opción `-e` cuando se ejecuta la imagen de Docker del bot de retención de datos. Para obtener más información, consulte Inicie el bot de retención de datos para su red Wickr.

> **Note**
>
> Estas variables de entorno son opcionales a menos que se especifique lo contrario.

Use las siguientes variables de entorno para especificar las credenciales del bot de retención de datos:

- `WICKRIO_BOT_NAME`: el nombre del bot de retención de datos. Esta variable es obligatoria cuando se ejecuta la imagen de Docker del bot de retención de datos.
- `WICKRIO_BOT_PASSWORD`: la contraseña inicial del bot de retención de datos. Para obtener más información, consulte Requisitos previos para configurar la retención de datos para AWS Wickr. Esta variable es obligatoria si no planea iniciar el bot de retención de datos con una solicitud de contraseña o si no planea usar Secrets Manager para almacenar las credenciales del bot de retención de datos.

Use las siguientes variables de entorno para configurar las capacidades de transmisión de retención de datos predeterminadas:

- `WICKRIO_COMP_MESGDEST`: el nombre de la ruta al directorio donde se transmitirán los mensajes. El valor predeterminado es `/tmp/<botname>/compliance/messages`.
- `WICKRIO_COMP_FILEDEST`: el nombre de la ruta al directorio donde se transmitirán los archivos. El valor predeterminado es `/tmp/<botname>/compliance/attachments`.
- `WICKRIO_COMP_BASENAME`: el nombre base de los archivos de mensajes recibidos. El valor predeterminado es `receivedMessages`.
- `WICKRIO_COMP_FILESIZE`: el tamaño de archivo máximo de un archivo de mensajes recibidos en kibibyte (KiB). Se inicia un nuevo archivo cuando se alcanza el tamaño máximo. El valor predeterminado es `1000000000`, como en 1024 GiB.
- `WICKRIO_COMP_TIMEROTATE`: el tiempo, en minutos, durante el que el bot de retención de datos colocará los mensajes recibidos en un archivo de mensajes recibidos. Se inicia un nuevo archivo cuando se alcanza el tiempo límite. Solo puede usar el tamaño o el tiempo del archivo para limitar el tamaño del archivo de mensajes recibidos. El valor predeterminado es `0`, como sin límite.

Utilice la siguiente variable de entorno para definir la variable de entorno predeterminada Región de AWS que se utilizará.

- `AWS_DEFAULT_REGION`— Es la opción predeterminada Región de AWS para AWS servicios como Secrets Manager (no se usa para Amazon S3 o AWS KMS). Se usa de forma predeterminada la región `us-east-1` si esta variable de entorno no está definida.

Utilice las siguientes variables de entorno para especificar el secreto de Secrets Manager que se utilizará cuando opte por utilizar Secrets Manager para almacenar las credenciales del bot de retención de datos y la información de AWS servicio. Para obtener más información sobre los valores que puede almacenar en Secrets Manager, consulte Valores de Secrets Manager para AWS Wickr.

- `AWS_SECRET_NAME`— El nombre del secreto de Secrets Manager que contiene las credenciales y la información de AWS servicio que necesita el bot de retención de datos.
- `AWS_SECRET_REGION`— En el Región de AWS que se encuentra el AWS secreto. Si está utilizando AWS secretos y este valor no está definido, se utilizará el `AWS_DEFAULT_REGION` valor.

> **Note**
>
> Puede almacenar todas las siguientes variables de entorno como valores en Secrets Manager. Si opta por usar Secrets Manager y almacena estos valores allí, no necesitará especificarlos como variables de entorno cuando ejecute la imagen de Docker del bot de retención de datos. Solo tiene que especificar la variable de entorno de `AWS_SECRET_NAME` descrita anteriormente en esta guía. Para obtener más información, consulte Valores de Secrets Manager para AWS Wickr.

Use las siguientes variables de entorno para especificar el bucket de Amazon S3 cuando opte por almacenar mensajes y archivos en un bucket.

- `WICKRIO_S3_BUCKET_NAME`: el nombre del bucket de Amazon S3 donde se almacenarán los mensajes y archivos.
- `WICKRIO_S3_REGION`— La AWS región del bucket de Amazon S3 en la que se almacenarán los mensajes y los archivos.
- `WICKRIO_S3_FOLDER_NAME`: el nombre de carpeta opcional en el bucket de Amazon S3 donde se almacenarán los mensajes y archivos. El nombre de esta carpeta irá precedido de la clave de los mensajes y archivos guardados en el bucket de Amazon S3.

Utilice las siguientes variables de entorno para especificar los AWS KMS detalles cuando opte por utilizar el cifrado del lado del cliente para volver a cifrar los archivos al guardarlos en un bucket de Amazon S3.

- `WICKRIO_KMS_MSTRKEY_ARN`— El nombre del recurso de Amazon (ARN) de la clave AWS KMS maestra utilizada para volver a cifrar los archivos de mensajes y los archivos del bot de retención de datos antes de guardarlos en el bucket de Amazon S3.
- `WICKRIO_KMS_REGION`— La AWS región en la que se encuentra la clave AWS KMS maestra.

Utilice la siguiente variable de entorno para especificar los detalles de Amazon SNS cuando opte por enviar eventos de retención de datos a un tema de Amazon SNS. Los eventos enviados incluyen el inicio, el cierre y las condiciones de error.

- `WICKRIO_SNS_TOPIC_ARN`: el ARN del tema de Amazon SNS al que desea que se envíen los eventos de retención de datos.

Utilice la siguiente variable de entorno para enviar las métricas de retención de datos a CloudWatch. Si se especifica, las métricas se generarán cada 60 segundos.

- `WICKRIO_METRICS_TYPE`— Defina el valor de esta variable de entorno en `cloudwatch` el que enviar las métricas CloudWatch.

Valores de Secrets Manager para AWS Wickr

Puede usar Secrets Manager para almacenar las credenciales del bot de retención de datos y la información AWS del servicio. Para obtener más información sobre cómo crear un secreto de Secrets Manager, consulte Crear un AWS Secrets Manager secreto en la Guía del usuario de Secrets Manager.

El secreto de Secrets Manager puede tener los siguientes valores:

- `password`: la contraseña del bot de retención de datos.
- `s3_bucket_name`: el nombre del bucket de Amazon S3 donde se almacenarán los mensajes y archivos. Si no se establece, se utilizará la transmisión de archivos predeterminada.
- `s3_region`— La AWS región del bucket de Amazon S3 en la que se almacenarán los mensajes y los archivos.

- `s3_folder_name`: el nombre de carpeta opcional en el bucket de Amazon S3 donde se almacenarán los mensajes y archivos. El nombre de esta carpeta irá precedido de la clave de los mensajes y archivos guardados en el bucket de Amazon S3.
- `kms_master_key_arn`— El ARN de la clave AWS KMS maestra utilizada para volver a cifrar los archivos de mensajes y los archivos del bot de retención de datos antes de guardarlos en el bucket de Amazon S3.
- `kms_region`— La AWS región en la que se encuentra la clave AWS KMS maestra.
- `sns_topic_arn`: el ARN del tema de Amazon SNS al que desea que se envíen los eventos de retención de datos.

Política de IAM para utilizar la retención de datos con los servicios de AWS

Si planeas utilizar otros AWS servicios con el bot de retención de datos de Wickr, debes asegurarte de que el anfitrión tenga la función y la política AWS Identity and Access Management (IAM) adecuadas para acceder a ellos. Puede configurar el bot de retención de datos para que utilice Secrets Manager, Amazon S3 CloudWatch, Amazon SNS y. AWS KMS La siguiente política de IAM permite el acceso a acciones específicas para estos servicios.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "secretsmanager:GetSecretValue",
                "sns:Publish",
                "cloudwatch:PutMetricData",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Puede crear una política de IAM más estricta identificando los objetos específicos de cada servicio a los que quiere permitir el acceso de los contenedores de su host. Elimine las acciones de los AWS servicios que no vaya a utilizar. Por ejemplo, si piensa utilizar solo un bucket de Amazon S3, utilice la siguiente política, que elimina las acciones `secretsmanager:GetSecretValue`, `sns:Publish`, `kms:GenerateDataKey` y `cloudwatch:PutMetricData`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "*"
        }
    ]
}
```

Si utilizas una instancia de Amazon Elastic Compute Cloud (Amazon EC2) para alojar tu bot de retención de datos, crea un rol de IAM utilizando el caso EC2 común de Amazon y asigna una política según la definición de política anterior.

Inicie el bot de retención de datos para su red Wickr

Antes de ejecutar el bot de retención de datos, debe determinar cómo quiere configurarlo. Si planea ejecutar el bot en un host que:

- No tendrá acceso a AWS los servicios, por lo que sus opciones son limitadas. En ese caso, utilizará las opciones de transmisión de mensajes predeterminadas. Debe decidir si desea limitar el tamaño de los archivos de mensajes capturados a un tamaño o intervalo de tiempo específicos. Para obtener más información, consulte Variables de entorno para configurar el bot de retención de datos en AWS Wickr.
- Si tiene acceso a AWS los servicios, debe crear un secreto de Secrets Manager para almacenar las credenciales del bot y los detalles de configuración del AWS servicio. Una vez configurados los servicios de AWS , puede iniciar la imagen de Docker del bot de retención de datos. Para obtener

más información sobre los detalles que puede almacenar en un secreto de Secrets Manager, consulte Valores de Secrets Manager para AWS Wickr

En las siguientes secciones se muestran ejemplos de comandos para ejecutar la imagen de Docker del bot de retención de datos. En cada uno de los comandos de ejemplo, sustituya los siguientes valores de ejemplo por los suyos:

- *compliance_1234567890_bot* con el nombre de su bot de retención de datos.
- *password* con la contraseña de su bot de retención de datos.
- *wickr/data/retention/bot* con el nombre de su secreto de Secrets Manager para usarlo con su bot de retención de datos.
- *bucket-name* con el nombre del bucket de Amazon S3 donde se almacenarán los mensajes y archivos.
- *folder-name* con el nombre de carpeta en el bucket de Amazon S3 donde se almacenarán los mensajes y archivos.
- *us-east-1*con la AWS región del recurso que estás especificando. Por ejemplo, la región de la clave AWS KMS maestra o la región del bucket de Amazon S3.
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-ababababababab*con el nombre de recurso de Amazon (ARN) de la clave AWS KMS maestra para volver a cifrar los archivos y archivos de mensajes.

Inicie el bot con la variable de entorno de contraseña (sin servicio) AWS

El siguiente comando de Docker inicia el bot de retención de datos. La contraseña se especifica mediante la variable de entorno de `WICKRIO_BOT_PASSWORD`. El bot comienza a usar la transmisión de archivos predeterminada y a usar los valores predeterminados definidos en la sección Variables de entorno para configurar el bot de retención de datos en AWS Wickr de esta guía.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
wickr/bot-compliance-cloud:latest
```

Inicie el bot con una solicitud de contraseña (sin AWS servicio)

El siguiente comando de Docker inicia el bot de retención de datos. La contraseña se introduce cuando el bot de retención de datos se lo pida. Comenzará a usar la transmisión de archivos predeterminada mediante los valores predeterminados definidos en la sección Variables de entorno para configurar el bot de retención de datos en AWS Wickr de esta guía.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest

docker attach compliance_1234567890_bot
.
.
.
Enter the password:************
Re-enter the password:************
```

Ejecute el bot utilizando la opción `-ti` para recibir la solicitud de contraseña. También debe ejecutar el comando `docker attach <container ID or container name>` inmediatamente después de iniciar la imagen de docker para que aparezca la solicitud de contraseña. Debe ejecutar ambos comandos en un script. Si lo adjunta a la imagen de docker y no ve el mensaje, presione Intro y verá el mensaje.

Inicie el bot con una rotación del archivo de mensajes de 15 minutos (sin AWS servicio)

El siguiente comando de Docker inicia el bot de retención de datos mediante variables de entorno. También lo configura para rotar los archivos de mensajes recibidos a 15 minutos.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=15 \
wickr/bot-compliance-cloud:latest
```

Cómo iniciar el bot y especificar la contraseña inicial con Secrets Manager

Puede utilizar Secrets Manager para identificar la contraseña del bot de retención de datos. Cuando inicie el bot de retención de datos, necesitará configurar una variable de entorno que especifique al Secrets Manager donde se almacena esta información.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickrpro/alpha/new-3-bot' \
wickr/bot-compliance-cloud:latest
```

El secreto de `wickrpro/compliance/compliance_1234567890_bot` tiene el siguiente valor secreto, que se muestra como texto sin formato.

```
{
    "password":"password"
}
```

Cómo iniciar el bot y configurar Amazon S3 con Secrets Manager

Puede usar Secrets Manager para alojar las credenciales y la información del bucket de Amazon S3. Cuando inicie el bot de retención de datos, necesitará configurar una variable de entorno que especifique al Secrets Manager donde se almacena esta información.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest
```

El secreto de `wickrpro/compliance/compliance_1234567890_bot` tiene el siguiente valor secreto, que se muestra como texto sin formato.

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
```

```
    "s3_folder_name":"folder-name"
}
```

Los mensajes y archivos que reciba el bot se colocarán en el bucket de `bot-compliance` de la carpeta denominada `network1234567890`.

Inicie el bot y configure Amazon S3 y AWS KMS Secrets Manager

Puede usar Secrets Manager para alojar las credenciales, el bucket de Amazon S3 y la información de la clave AWS KMS maestra. Cuando inicie el bot de retención de datos, necesitará configurar una variable de entorno que especifique al Secrets Manager donde se almacena esta información.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest
```

El secreto de `wickrpro/compliance/compliance_1234567890_bot` tiene el siguiente valor secreto, que se muestra como texto sin formato.

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name",
    "kms_master_key_arn":"arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-
a617-abababababab",
    "kms_region":"us-east-1"
}
```

Los mensajes y archivos recibidos por el bot se cifrarán con la clave KMS identificada por el valor del ARN y, a continuación, se colocarán en el bucket de “conformidad del bot” de la carpeta denominada “network1234567890”. Asegúrese de que tiene la configuración de la política de IAM adecuada.

Cómo iniciar el bot y configurar Amazon S3 mediante variables de entorno

Si no quiere usar Secrets Manager para alojar las credenciales del bot de retención de datos, puede iniciar la imagen de Docker del bot de retención de datos con las siguientes variables de

entorno. Debe identificar el nombre del bot de retención de datos mediante la variable de entorno de `WICKRIO_BOT_NAME`.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_S3_BUCKET_NAME='bot-compliance' \
-e WICKRIO_S3_FOLDER_NAME='network1234567890' \
-e WICKRIO_S3_REGION='us-east-1' \
wickr/bot-compliance-cloud:latest
```

Puede usar los valores del entorno para identificar las credenciales del bot de retención de datos, la información sobre los buckets de Amazon S3 y la información de configuración para la transmisión de archivos predeterminada.

Detenga el bot de retención de datos de su red Wickr

El software que se ejecuta en el robot de retención de datos capturará las señales de `SIGTERM` y se apagará sin problemas. Utilice el comando `docker stop <container ID or container name>`, como se muestra en el siguiente ejemplo, para enviar el comando `SIGTERM` a la imagen de Docker del bot de retención de datos.

```
docker stop compliance_1234567890_bot
```

Obtenga los registros de retención de datos para su red Wickr

El software que se ejecuta en la imagen de Docker del bot de retención de datos enviará sus resultados a los archivos de registro del directorio `/tmp/<botname>/logs` Se rotará hasta 5 archivos como máximo. Ejecute el comando siguiente para obtener los registros.

```
docker logs <botname>
```

Ejemplo:

```
docker logs compliance_1234567890_bot
```

Métricas y eventos de retención de datos para su red de Wickr

A continuación se muestran las métricas de Amazon CloudWatch (CloudWatch) y los eventos del Amazon Simple Notification Service (Amazon SNS) que actualmente admite la versión 5.116 del bot de retención de datos Wickr de AWS.

Temas

- CloudWatch métricas para su red de Wickr
- Eventos de Amazon SNS para tu red de Wickr

CloudWatch métricas para su red de Wickr

El bot genera las métricas en intervalos de 1 minuto y las transmite al CloudWatch servicio asociado a la cuenta en la que se ejecuta la imagen de Docker del bot de retención de datos.

A continuación se muestran las métricas existentes que son compatibles con el bot de retención de datos.

Métrica	Descripción
Messages_Rx	Mensajes recibidos
Messages_Rx_Failed	Errores al procesar los mensajes recibidos.
Messages_Saved	Mensajes guardados en el archivo de mensajes recibidos.
Messages_Saved_Failed	Errores al guardar los mensajes en el archivo de mensajes recibidos.
Files_Saved	Archivos recibidos.
Files_Saved_Bytes	Número de bytes de los archivos recibidos.
Files_Saved_Failed	Errores al guardar los archivos.
Inicios de sesión	Inicios de sesión (normalmente 1 por intervalo).

Métrica	Descripción
Login_Failures	Errores al iniciar sesión (normalmente 1 por intervalo).
S3_Post_Errors	Errores al publicar archivos de mensajes y archivos del bucket de Amazon S3.
Watchdog_Failures	Errores de watchdog.
Watchdog_Warnings	Advertencias de watchdog

Las métricas se generan para que las consuma. CloudWatch El espacio de nombre utilizado para los bots es `WickrIO`. Cada métrica tiene una matriz de dimensiones. La lista siguiente recoge las dimensiones que se publican con las métricas anteriores.

Dimensión	Valor
Id	El nombre de usuario del bot.
Dispositivo	Descripción de una instancia o un dispositivo específico del bot. Es útil si se ejecutan varios dispositivos o instancias de bots.
Producto	El producto para el bot. Puede ser `WickrPro_` o `WickrEnterprise_` con `Alpha`, `Beta` o `Production` anexado.
BotType	El tipo de bot. Etiquetado como Conformidad para los bots de conformidad.
Network	El ID de la red asociada.

Eventos de Amazon SNS para tu red de Wickr

Los eventos siguientes se publican en el tema de Amazon SNS definido por el valor del nombre de recurso de Amazon (ARN) identificado mediante la variable de entorno `WICKRIO_SNS_TOPIC_ARN` o el valor secreto de Secrets Manager `sns_topic_arn`. Para obtener más información, consulte

Variables de entorno para configurar el bot de retención de datos en AWS Wickr y Valores de Secrets Manager para AWS Wickr.

Los eventos generados por el bot de retención de datos se envían como cadenas JSON. En los eventos se incluyen los valores siguientes a partir de la versión 5.116 del bot de retención de datos.

Nombre	Valor
complianceBot	El nombre de usuario del bot de retención de datos.
dataTime	La fecha y hora en que se produjo el evento.
device	La descripción del dispositivo o instancia del bot específico. Es útil si se ejecutan varias instancias de bot.
dockerImage	La imagen de Docker asociada al bot.
dockerTag	La etiqueta o versión de la imagen de Docker.
message	El mensaje del evento. Para obtener más información, consulte Eventos críticos y Eventos normales.
notificationType	Este valor será `Bot Event`.
severity	La gravedad del evento. Puede ser `normal` o `critical`.

Debe suscribirse al tema de Amazon SNS para poder recibir los eventos. Si se suscribe con una dirección de correo electrónico, se le enviará un correo electrónico con información similar a la del siguiente ejemplo.

```
{
"complianceBot": "compliance_1234567890_bot",
 "dateTime": "2022-10-12T13:05:39",
 "device": "Desktop 1234567890ab",
 "dockerImage": "wickr/bot-compliance-cloud",
 "dockerTag": "5.116.13.01",
```

```
 "message": "Logged in",
 "notificationType": "Bot Event",
 "severity": "normal"
}
```

Eventos críticos

Estos eventos hacen que el bot se detenga o se reinicie. Para evitar otros problemas, el número de reinicios es limitado.

Errores de inicio de sesión

Los eventos siguientes se pueden generar cuando el bot no consigue iniciar sesión. En cada mensaje se indica el motivo del error de inicio de sesión.

Tipo de evento	Mensaje de evento
failedlogin	Credenciales incorrectas. Compruebe la contraseña.
failedlogin	Usuario no encontrado
failedlogin	La cuenta o el dispositivo están suspendidos.
provisioning	El usuario abandonó el comando.
provisioning	La contraseña del archivo `config.wickr` es incorrecta.
provisioning	No se puede leer el archivo `config.wickr` .
failedlogin	Error en todos los inicios de sesión.
failedlogin	Nuevo usuario en una base de datos que ya existe.

Más eventos críticos

Tipo de evento	Mensajes de los eventos
Cuenta suspendida	Wickr IOClient Main: slotAdminUser Suspender : código (%1): motivo: %2»
BotDevice Suspendido	El dispositivo está suspendido.
WatchDog	El SwitchBoard sistema ha estado inactivo durante más de < *N* > minutos
Errores de S3	No se pudo colocar el archivo < *file-name* ≫ en el bucket S3. Error: < *AWS-error* >
Clave Fallback (alternativa)	EL SERVIDOR ENVIÓ UNA CLAVE FALLBACK (ALTERNATIVA): no es una clave alternativa activa reconocida por el cliente. Envíe los registros al equipo de ingeniería del escritorio.

Eventos normales

Los eventos siguientes advierten sobre un funcionamiento normal No obstante, puede ser motivo de preocupación si se producen demasiados eventos de este tipo en un período de tiempo determinado.

Dispositivo agregado a la cuenta

Este evento se genera cuando se agrega un nuevo dispositivo a la cuenta del bot de retención de datos. En determinadas circunstancias, esto puede ser un indicio importante de se ha creado una instancia del bot de retención de datos. El mensaje siguiente corresponde a este evento:

```
A device has been added to this account!
```

El bot ha iniciado sesión

Este evento se genera cuando el bot ha iniciado sesión correctamente. El mensaje siguiente corresponde a este evento:

```
Logged in
```

Cerrando

Este evento se genera cuando el bot se cierra. Si el usuario no lo inició de forma explícita, puede indicar que ha habido un problema. El mensaje siguiente corresponde a este evento:

```
Shutting down
```

Actualizaciones disponibles

Este evento se genera cuando se inicia el bot de retención de datos e identifica que hay disponible una versión más reciente de la imagen de Docker asociada. Este evento se genera cuando se inicia el bot y diariamente. Este evento incluye el campo de la matriz `versions` que identifica las nuevas versiones disponibles. Consulte el ejemplo de este evento a continuación.

```
{
  "complianceBot": "compliance_1234567890_bot",
  "dateTime": "2022-10-12T13:05:55",
  "device": "Desktop 1234567890ab",
  "dockerImage": "wickr/bot-compliance-cloud",
  "dockerTag": "5.116.13.01",
  "message": "There are updates available",
  "notificationType": "Bot Event",
  "severity": "normal",
  "versions": [
    "5.116.10.01"
  ]
}
```

¿Qué es ATAK?

El kit Android Team Awareness Kit (ATAK), o Android Tactical Assault Kit (también conocido como ATAK) para uso militar, es una aplicación de infraestructura geoespacial y conciencia situacional para teléfonos inteligentes que permite una colaboración segura a nivel geográfico. Aunque inicialmente se diseñó para su uso en zonas de combate, ATAK se ha adaptado para adaptarse a los objetivos de agencias locales, estatales y federales.

Temas

- Cómo habilitar ATAK en el panel de la red de Wickr
- Información adicional sobre ATAK

- Cómo instalar y vincular el complemento de Wickr para ATAK
- Desvincula el plugin Wickr para ATAK
- Marca y recibe una llamada en ATAK
- Envía un archivo en ATAK
- Envía un mensaje de voz seguro (Push-to-talk) en ATAK
- Molinete (acceso rápido) para ATAK
- Navegación para ATAK

Cómo habilitar ATAK en el panel de la red de Wickr

AWS Wickr es compatible con muchas agencias que utilizan Android Tactical Assault Kit (ATAK). Sin embargo, hasta ahora, los operadores de ATAK que utilizan Wickr han tenido que salir de la aplicación para poder hacerlo. Para ayudar a reducir las interrupciones y el riesgo operativo, Wickr ha desarrollado un complemento que mejora ATAK con características de comunicación seguras. Con el complemento Wickr para ATAK, los usuarios pueden enviar mensajes, colaborar y transferir archivos en Wickr dentro de la aplicación ATAK. Esto elimina las interrupciones y la complejidad de la configuración con las características de chat de ATAK.

Cómo habilitar ATAK en el panel de la red de Wickr

Complete el siguiente procedimiento para habilitar ATAK en el panel de la red de Wickr.

1. Abre el formulario AWS Management Console Wickr Cat https://console.aws.amazon.com/wickr/.
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Grupos de seguridad.
4. En la página Grupos de seguridad, seleccione el grupo de seguridad deseado para el que desee habilitar ATAK.
5. En la pestaña Integración, en la sección del complemento ATAK, elija Editar.
6. En la página Editar el complemento ATAK, selecciona la casilla Habilitar el complemento ATAK.
7. Selecciona Añadir nuevo paquete
8. Introduzca el nombre del paquete en el cuadro de texto Paquetes. Puede introducir uno de los siguientes valores en función de la versión de ATAK que vayan a instalar y utilizar los usuarios:

- `com.atakmap.app.civ`: introduzca este valor en el cuadro de texto Paquetes si los usuarios finales de Wickr van a instalar y utilizar la versión civil de la aplicación ATAK en sus dispositivos Android.
- `com.atakmap.app.mil`: introduzca este valor en el cuadro de texto Paquetes si los usuarios finales de Wickr van a instalar y utilizar la versión militar de la aplicación ATAK en sus dispositivos Android.

9. Seleccione Save.

   Ahora, ATAK está habilitado para la red de Wickr y el grupo de seguridad seleccionados. Debe pedir a los usuarios de Android del grupo de seguridad para el que ha habilitado la funcionalidad de ATAK que instalen el complemento Wickr para ATAK. Para obtener más información, consulte Instalar y vincular el complemento Wickr para ATAK.

Información adicional sobre ATAK

Para obtener más información sobre el plugin de Wickr para ATA, consulte lo siguiente:

- Descripción general del complemento Wickr para ATAK
- Información adicional sobre el complemento Wickr para ATAK

Cómo instalar y vincular el complemento de Wickr para ATAK

El kit de Android Team Awareness Kit (ATAK) es una solución para Android que utilizan las agencias militares, estatales y gubernamentales de los EE. UU. que requieren capacidades de información situacional para planificar las misiones, ejecutarlas y responder a incidentes. La arquitectura de complementos de ATAK permite a los desarrolladores agregar funcionalidades. Además, los usuarios pueden navegar utilizando datos de mapas geoespaciales y GPS superpuestos con información situacional en tiempo real sobre los eventos en curso. En este documento le mostramos cómo instalar el complemento de Wickr para ATAK en un dispositivo Android y vincularlo con el cliente Wickr. De este modo podrá enviar mensajes y colaborar en Wickr sin salir de la aplicación ATAK.

Cómo instalar el complemento de Wickr para ATAK

Siga los pasos que se indican a continuación para instalar el complemento de Wickr para ATAK en un dispositivo Android.

1. Visite la tienda Google Play e instale el complemento de Wickr para ATAK.
2. Abra la aplicación ATAK en su dispositivo Android.
3. En la aplicación ATAK, seleccione el icono de menú ( ) en la parte superior derecha de la pantalla y, a continuación, seleccione Complementos.
4. Seleccione Importar.
5. En la ventana Selección del tipo de importación emergente, elija SD Local y vaya al lugar donde guardó el archivo .apk del complemento Wickr para ATAK.
6. Seleccione el archivo del complemento y siga las instrucciones para instalarlo.

> **Note**
>
> Si se le pide que envíe el archivo del complemento para escanearlo, seleccione No.

7. La aplicación ATAK le preguntará si desea cargar el complemento. Seleccione OK (Aceptar).

El complemento de Wickr para ATAK ya está instalado. Siga a la sección Emparejar ATAK con Wickr para completar el proceso.

Cómo vincular ATAK con Wickr

Siga el procedimiento que se indica a continuación para vincular la aplicación ATAK con Wickr una vez instalado correctamente el complemento de Wickr para ATAK.

1. En la aplicación ATAK, seleccione el icono de menú ( ) en la parte superior derecha de la pantalla y, a continuación, Complemento de Wickr.
2. Elija Vincular Wickr.

   Aparecerá un mensaje de notificación pidiéndole que revise los permisos del complemento de Wickr para ATAK. En caso contrario, abra el cliente Wickr y vaya a Ajustes y, a continuación, a Aplicaciones conectadas. Debería ver el complemento en la sección Pendiente de la pantalla.
3. Seleccione Aprobar para vincularlo.
4. Selecciona el botón Abrir complemento de Wickr ATAK para volver a la aplicación ATAK.

   Se ha vinculado correctamente el complemento ATAK y Wickr; ya puede usarlo para enviar mensajes y colaborar con Wickr sin salir de la aplicación ATAK.

Desvincula el plugin Wickr para ATAK

Puedes desvincular el plugin Wickr para ATAK.

Complete el siguiente procedimiento para desvincular el complemento ATAK de Wickr.

1. En la consola, elija Configuración y, a continuación, elija Aplicaciones conectadas.
2. En la pantalla Aplicaciones conectadas, seleccione Complemento Wickr para ATAK.
3. En la pantalla Complemento Wickr para ATAK, seleccione Eliminar en la parte inferior de la pantalla.

   Ahora has desemparejado correctamente el plugin Wickr para ATAK.

Marca y recibe una llamada en ATAK

Puede marcar y recibir una llamada en el complemento Wickr para ATAK.

Complete el siguiente procedimiento para marcar y recibir una llamada.

1. Abra una ventana de chat.
2. En la vista Mapa, seleccione el icono del usuario al que quiere llamar.
3. Elija el icono de teléfono de la parte superior derecha de la pantalla.
4. Una vez conectado, puede volver a la vista del complemento ATAK y recibir una llamada.

Envía un archivo en ATAK

Descubra cómo enviar un archivo en el complemento Wickr para ATAK.

Siga el procedimiento que se indica a continuación para enviar un archivo.

1. Abra una ventana de chat.
2. En la vista Mapa, busque al usuario al que quiere enviar un archivo.
3. Cuando encuentre al usuario al que quiere enviar un archivo, seleccione su nombre.
4. En la pantalla Enviar archivo, seleccione Elegir archivo y, a continuación, navegue hasta el archivo que desea enviar.

5. En la ventana del navegador, seleccione el archivo deseado.
6. En la pantalla Enviar archivo, seleccione Enviar archivo.

   Aparecerá el icono de descarga, que indica que se está descargando el archivo que ha seleccionado.

Envía un mensaje de voz seguro (Push-to-talk) en ATAK

Puedes enviar un mensaje de voz seguro (Push-to-talk) en el complemento Wickr para ATAK.

Complete el siguiente procedimiento para enviar un mensaje de voz de seguro.

1. Abra una ventana de chat.
2. Selecciona el Push-to-Talk icono de la parte superior de la pantalla, indicado por el icono de una persona hablando.
3. Seleccione y mantenga presionado el botón Presione el botón para grabar.
4. Grabe su mensaje.
5. Después de grabar el mensaje, suelte el botón para enviarlo.

Molinete (acceso rápido) para ATAK

La función de molinete o acceso rápido se utiliza para one-one-one conversaciones o mensajes directos.

Complete el siguiente procedimiento para usar la rueda de opciones.

1. Abra la vista en pantalla dividida del mapa de ATAK y del complemento Wickr para ATAK de forma simultánea. El mapa muestra a sus compañeros de equipo o los activos en la vista de mapa.
2. Seleccione el icono de usuario para abrir la rueda de opciones.
3. Seleccione el icono de Wickr para ver las opciones disponibles para el usuario seleccionado.
4. En la rueda de opciones, elija uno de los siguientes iconos:

- Teléfono: elija llamar.
- Mensaje: elija participar en un chat.
- Envío de archivos: elija enviar un archivo.

Navegación para ATAK

La interfaz de usuario del complemento contiene tres vistas del complemento que se indican mediante las figuras azules y blancas situadas en la parte inferior derecha de la pantalla. Deslice el dedo hacia la izquierda y hacia la derecha para navegar entre las vistas.

- Vista de contactos: cree un grupo de mensajes directos o una conversación de sala.
- DMs ver: Crear una one-to-one conversación. La funcionalidad de chat funciona igual que en la aplicación nativa de Wickr. Esta funcionalidad le permite permanecer en la vista de mapa y comunicarse con otras personas a través del complemento.
- Vista de salas: las salas existentes en la aplicación nativa se transfieren. Todo lo que se haga en el complemento se reflejará en la aplicación nativa de Wickr.

> **Note**
>
> Algunas funciones, como la eliminación de una sala, solo se pueden realizar en la aplicación nativa y de forma presencial para evitar modificaciones no deseadas por parte de los usuarios y las interferencias causadas por el equipo de campo.

Lista de puertos y dominios a permitir para tu red Wickr

Permite enumerar los siguientes puertos para garantizar que Wickr funcione correctamente:

Puertos

- Puerto TCP 443 (para mensajes y archivos adjuntos)
- Puertos UDP 16384-16584 (para llamadas)

Lista de dominios y direcciones a permitir por región

Si necesitas incluir en una lista todos los dominios de llamadas y direcciones IP de servidores posibles, consulta la siguiente lista de posibles dominios CIDRs por región. Consulte esta lista periódicamente, ya que está sujeta a cambios.

> **Note**
>
> Los correos electrónicos de registro y verificación se envían desde `no-reply@amazonaws.com` y `donotreply@wickr.email`.

Este de EE. UU. (Norte de Virginia)

Dominios:	• gw-pro-prod.wickr.com • api.messaging. wickr.us-east-1.amazonaws.com
Llamando a direcciones CIDR:	• 44.211.195.0/27 • 4421383,32/28
Direcciones IP de llamadas:	• 44.211.195.0 • 44,211,195,1 • 44,211,195,2 • 44,211,195.3 • 44,211,195,4 • 44,211,195,5 • 44,211,195,6 • 44,211,195,7 • 44,211.195,8 • 44,211.195,9 • 44211195,10 • 44,211.195,11 • 44,211.195,12 • 44,211.195,13

	• 44,211.195,14 • 44,211.195,15 • 44,211.195,16 • 44,211.195,17 • 44,211.195,18 • 44,211.195,19 • 44211195,20 • 44,211.195,21 • 44,211.195,22 • 44,211.195,23 • 44,211.195,24 • 44211195,25 • 44,211.195,26 • 44,211.195,27 • 44,211.195,28 • 44211195,29 • 44,211.195,30 • 44,211.195,31 • 4421383,32 • 4421383,33 • 4421383,34 • 4421383,35 • 4421383,36 • 4421383,37 • 4421383,38 • 4421383,39 • 4421383,40 • 4421383,41 • 4421383,42 • 4421383,43

	• 4421383,44 • 4421383,45 • 4421383,46 • 4421383,47

Asia-Pacífico (Malasia)

Dominios:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-5.amazon aws.com
Llamando a direcciones CIDR:	• 43.216.226.160/28
Direcciones IP de llamadas:	• 43.216.226.160 • 43216226,161 • 43216226,162 • 43216,226,163 • 43216,226,164 • 43216,226,165 • 43216,226,166 • 43216,226,167 • 43216,226,168 • 43216,226,169 • 43216,226,170 • 43216,226,171 • 43216,226,172 • 43216,226,173 • 43216,226,174 • 43216,226,175

Asia-Pacífico (Singapur)

Dominio:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-1.amazon aws.com
Llamando a direcciones CIDR:	• 47.129.23.144/28
Direcciones IP de llamadas:	• 47.129.23.144 • 4712923,145 • 4712923,146 • 4712923,147 • 4712923,148 • 4712923,149 • 4712923,150 • 4712923,151 • 4712923,152 • 4712923,153 • 4712923,154 • 4712923,155 • 4712923,156 • 4712923,157 • 4712923,158 • 4712923,159

Asia-Pacífico (Sídney)

Dominio:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-2.amazon aws.com
Llamando a direcciones CIDR:	• 3.27.180.208/28

Direcciones IP de llamadas:	• 3.27.180.208 • 3,27180,209 • 3,27,180,210 • 3.27,180,211 • 3.27,180,212 • 3,27,180,213 • 3,27,180,214 • 3.27,180,215 • 3,27,180,216 • 3.27,180,217 • 3.27,180,218 • 3.27,180,219 • 3,27180,220 • 3.27180,221 • 3.27180,222 • 3.27180,223

Asia-Pacífico (Tokio)

Dominio:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-northeast-1.amazon aws.com
Llamando a direcciones CIDR:	• 57.181.142.240/28
Direcciones IP de llamadas:	• 57.181.142.240 • 57,181,142,241 • 57,181,142,242 • 57,181,142,243 • 57,181,142,244 • 57,181,142,245 • 57,181,142,246

	• 57,181,142,247 • 57,181,142,248 • 57,181,142,249 • 57,181,142,250 • 57,181,142251 • 57,181,142,252 • 57,181,142,253 • 57,181,142,254 • 57,181,142,25

Canadá (centro)

Dominio:	• gw-pro-prod.wickr.com • api.messaging. wickr.ca-central-1.amazonaws.com
Llamando a direcciones CIDR:	• 15.156.152.96/28
Direcciones IP de llamadas:	• 15.156.152.96 • 15,156152,97 • 15,156152,98 • 15,156,15,99 • 15,156,152,100 • 15,156,152,101 • 15,156,152,102 • 15,156,152,103 • 15,156,152,104 • 15,156,152,105 • 15,156,152,106 • 15,156,152,107 • 15,156,152,108 • 15,156,152,109

	• 15,156,152,110 • 15,156,152,111

Europa (Fráncfort)

Dominio:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-central-1.amazonaws.com
Llamando a direcciones CIDR:	• 3.78.252.32/28
Direcciones IP de llamadas:	• 3.78.252.32 • 3,78,252,33 • 3,78,252,34 • 3,78,252,35 • 3,78,252,36 • 3,78,252,37 • 3,78,252,38 • 3,78,252,39 • 3,78,252,40 • 3,78,252,41 • 3,78,252,42 • 3,78,252,43 • 3,78,252,44 • 3,78,252,45 • 3,78,252,46 • 3,78,252,47
Direcciones IP de mensajería:	• 3.163.236.183 • 3,163,238,183 • 3,163,251,183 • 3,163,232,183

	• 3,163,241,183 • 3,163,245,183 • 3,163,248,183 • 3,163,234,183 • 3,163,237,183 • 3,163,243,183 • 3,163,247,183 • 3,163,240,183 • 3,163,242,183 • 3,163,244,183 • 3,163,246,183 • 3,163,249,183 • 3,163,252,183 • 3,163,235,183 • 3,163,250,183 • 3,163,239,183 • 3,163,233183

Europa (Londres)

Dominio:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-west-2.am azonaws.com
Llamando a direcciones CIDR:	• 13.43.91.48/28
Direcciones IP de llamadas:	• 13.43.91.48 • 13,4391,49 • 13,4391,50 • 13,4391,51 • 13,4391,52 • 13,4391,53

	• 13,4391,54 • 13,4391,55 • 13,4391,56 • 13,4391,57 • 13,4391,58 • 13,4391,59 • 13,4391,60 • 13,4391,61 • 13,4391,62 • 13,4391,63

Europa (Estocolmo)

Dominio:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-north-1.amazonaws.com
Llamando a direcciones CIDR:	• 13.60.1.64/28
Direcciones IP de llamadas:	• 13.60.1.64 • 13,601,65 • 13,601,66 • 13,601,67 • 13,601,68 • 13,601,69 • 13,601,70 • 13,601,71 • 13,601,72 • 13,601,73 • 13,601,74 • 13,601,75 • 13,601,76

	• 13,601,77 • 13,601,78 • 13,601,79

Europa (Zúrich)

Dominio:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-central-2.amazonaws.com
Llamando a direcciones CIDR:	• 16.63.106.224/28
Direcciones IP de llamadas:	• 16.63.106.224 • 16,63106,225 • 16,63106,226 • 16,63106,227 • 16,63106,228 • 16,63106,229 • 16,63106,230 • 16,63106,231 • 16,63106,232 • 16,63106,233 • 16,63106,234 • 16,63106,235 • 16,63106,236 • 16,63106,237 • 16,63106,238 • 16,63106,239

AWS GovCloud (Estados Unidos-Oeste)

Dominio:	• gw-pro-prod.wickr.com

	• api.messaging.wickr. us-gov-west-1.amazonaws.com
Llamar a direcciones CIDR:	• 3.30.186.208/28
Direcciones IP de llamadas:	• 3.30.186.208 • 3,30186,209 • 3,30186,210 • 3,30186,211 • 3,30186,212 • 3,30186,213 • 3,30186,214 • 3,30186,215 • 3,30186,216 • 3,30186,217 • 3,30186,218 • 3,30186,219 • 3,30186,220 • 3,30186,221 • 3,30186222 • 3,30186,223

GovCloud clasificación y federación transfronterizas

AWS Wickr ofrece un WickrGov cliente personalizado para GovCloud los usuarios. La GovCloud Federación permite la comunicación entre GovCloud usuarios y usuarios comerciales. La función de clasificación transfronteriza permite a los usuarios modificar la interfaz de usuario en las GovCloud conversaciones. Como GovCloud usuario, debe cumplir con las directrices estrictas relativas a la clasificación definida por el gobierno. Cuando GovCloud los usuarios entablen conversaciones con usuarios comerciales (Enterprise, AWS Wickr, usuarios invitados), verán las siguientes advertencias no clasificadas:

- Una etiqueta U en la lista de habitaciones

- Un reconocimiento no clasificado en la pantalla de mensajes
- Un banner no clasificado en la parte superior de la conversación

> **Note**
>
> Estas advertencias solo se mostrarán cuando un GovCloud usuario esté conversando o formando parte de una sala con usuarios externos. Desaparecerán si los usuarios externos abandonan la conversación. No se mostrará ninguna advertencia en las conversaciones entre GovCloud usuarios.

Vista previa del archivo AWS Wickr

Las organizaciones que utilizan el nivel Premium de Wickr (incluida la prueba gratuita de Premium) ahora pueden gestionar los permisos de descarga de archivos a nivel de grupo de seguridad.

Las descargas de archivos están habilitadas de forma predeterminada en los grupos de seguridad. Los administradores pueden activar o desactivar las descargas de archivos a través del panel de administración. Esta configuración se aplica a toda la red de Wickr.

Para activar o desactivar la descarga de archivos, complete el siguiente procedimiento.

1. Abre el formulario AWS Management Console Wickr Cat https://console.aws.amazon.com/wickr/.
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Grupos de seguridad.
4. Seleccione el nombre del grupo de seguridad que desee editar.

   La página de detalles del grupo de seguridad muestra la configuración del grupo de seguridad en diferentes pestañas.
5. En la pestaña Mensajería, en la sección Contenido multimedia y enlaces, seleccione Editar.
6. En la página Editar contenido multimedia y enlaces, marca o desmarca la opción Descargas de archivos.
7. Seleccione Save changes (Guardar cambios).

Cuando las descargas de archivos están habilitadas para un grupo de seguridad, los usuarios pueden descargar los archivos compartidos en salas y mensajes directos. Si las descargas están deshabilitadas, solo pueden previsualizar estos archivos y subirlos a la pestaña Archivos, pero no podrán descargarlos. Los usuarios tampoco pueden hacer capturas de pantalla; si lo intentan, la pantalla aparecerá en negro.

> **Note**
>
> Cuando las descargas de archivos estén deshabilitadas, todos los usuarios de ese grupo de seguridad deberán utilizar la versión 6.54 o superior de Wickr para que se aplique esta configuración de archivos.

> **Note**
>
> En las salas en las que hay usuarios de diferentes redes (debido a la federación) y grupos de seguridad, la capacidad de cada usuario para previsualizar o descargar archivos depende de la configuración específica de su grupo de seguridad. Como resultado, algunos usuarios pueden descargar archivos en una sala, mientras que otros solo pueden previsualizarlos.

Cómo gestionar usuarios en AWS Wickr

En la sección de administración de usuarios de AWS Management Console Wickr, puedes ver los usuarios y bots actuales de Wickr y modificar sus detalles.

Temas

- Directorio de equipos en la red AWS Wickr
- Usuarios invitados en la red AWS Wickr

Directorio de equipos en la red AWS Wickr

Puede ver los usuarios actuales de Wickr y modificar sus detalles en la sección de administración de usuarios de Wickr. AWS Management Console

Temas

- Ver los usuarios de la red AWS Wickr
- Invitar a un usuario en la red AWS Wickr
- Edición de usuarios en la red AWS Wickr
- Eliminar un usuario de la red AWS Wickr
- Eliminación masiva de usuarios en la red AWS Wickr
- Suspender masivamente a los usuarios de la red AWS Wickr

Ver los usuarios de la red AWS Wickr

Puede ver los detalles de los usuarios registrados en su red de Wickr.

Siga el procedimiento que se indica a continuación para ver los usuarios registrados en su red de Wickr.

1. Abre el formulario AWS Management Console Wickr en. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.

   La pestaña del directorio del equipo muestra los usuarios registrados en tu red Wickr, incluidos su nombre, dirección de correo electrónico, grupo de seguridad asignado y estado actual. En el

caso de los usuarios actuales, puede ver sus dispositivos, editar su información, suspenderlos, eliminarlos y cambiarlos a otra red de Wickr.

Invitar a un usuario en la red AWS Wickr

Puedes invitar a un usuario de tu red de Wickr.

Complete el siguiente procedimiento para invitar a un usuario a su red Wickr.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.
4. En la pestaña del directorio del equipo, selecciona Invitar a un usuario.
5. En la página Invitar a un usuario, introduce la dirección de correo electrónico y el grupo de seguridad del usuario. La dirección de correo electrónico y el grupo de seguridad son los únicos campos obligatorios. Asegúrese de elegir el grupo de seguridad adecuado para los usuarios. Wickr les enviará un correo electrónico de invitación a la dirección que se indique.
6. Elija Invite user.

   Se enviará un correo electrónico al usuario. El correo electrónico incluye enlaces para descargar las aplicaciones de cliente Wickr y un enlace para registrarse en Wickr. A medida que los usuarios se registren en Wickr utilizando su enlace del correo electrónico, su estado en el directorio del equipo de Wickr cambiará de Pendiente a Activo.

Edición de usuarios en la red AWS Wickr

Puede editar los usuarios de su red de Wickr.

Siga el procedimiento que se indica a continuación para editar usuarios.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.
4. En la pestaña del directorio del equipo, selecciona el icono de puntos suspensivos verticales (tres puntos) del usuario que quieres editar.
5. Elija Edit (Edición de).

6. Edita la información del usuario y, a continuación, selecciona Guardar cambios.

Eliminar un usuario de la red AWS Wickr

Puede eliminar un usuario de su red de Wickr.

Siga el procedimiento que se indica a continuación para eliminar un usuario.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.
4. En la pestaña del directorio del equipo, selecciona el icono de puntos suspensivos verticales (tres puntos) del usuario que quieres eliminar.
5. Seleccione Eliminar para eliminarlo.

   Cuando se elimina a un usuario, dicho usuario ya no puede iniciar sesión en su red de Wickr del cliente Wickr.
6. En la ventana emergente, elija Eliminar.

Eliminación masiva de usuarios en la red AWS Wickr

Puede eliminar de forma masiva los usuarios de la red de Wickr en la sección de administración de usuarios de Wickr. AWS Management Console

> **Note**
>
> La opción de eliminar usuarios de forma masiva solo se aplica cuando el SSO no está activado.

Para eliminar en bloque los usuarios de su red de Wickr mediante una plantilla CSV, siga el procedimiento indicado a continuación.

1. Abre el formulario AWS Management Console Wickr at. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.

4. La pestaña del directorio del equipo muestra los usuarios registrados en tu red Wickr.
5. En la pestaña del directorio del equipo, selecciona Administrar usuarios y, a continuación, selecciona Eliminar de forma masiva.
6. En la página Eliminar usuarios de forma masiva, descarga la plantilla CSV de ejemplo. Para descargar la plantilla de ejemplo, selecciona Descargar plantilla.
7. Complete la plantilla añadiendo el correo electrónico de los usuarios que desee eliminar de forma masiva de la red.
8. Cargue la plantilla CSV una vez completada. Puede arrastrar y soltar el archivo en el cuadro de carga o seleccionar un archivo.
9. Seleccione la casilla de verificación, entiendo que la eliminación del usuario no es reversible.
10. Selecciona Eliminar usuarios.

> **Note**
>
> Esta acción empezará a eliminar a usuarios inmediatamente y puede tardar varios minutos. Los usuarios eliminados ya no podrán iniciar sesión en su red de Wickr del cliente Wickr.

Para eliminar en bloque a usuarios de su red de Wickr descargando un CSV del directorio de su equipo, siga el procedimiento indicado a continuación.

1. Abre el formulario AWS Management Console Wickr en https://console.aws.amazon.com/wickr/.
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.
4. La pestaña del directorio del equipo muestra los usuarios registrados en tu red Wickr.
5. En la pestaña del directorio del equipo, selecciona Administrar usuarios y, a continuación, selecciona Descargar como CSV.
6. Tras descargar la plantilla CSV del directorio del equipo, elimine las filas de usuarios que desee conservar.
7. En la pestaña del directorio del equipo, selecciona Administrar usuarios y, a continuación, selecciona Eliminar de forma masiva.
8. En la página Eliminar usuarios de forma masiva, sube la plantilla CSV del directorio del equipo. Puedes arrastrar y soltar el archivo en el cuadro de carga o seleccionar Elegir un archivo.

9. Selecciona la casilla de verificación, entiendo que eliminar un usuario no es reversible.
10. Selecciona Eliminar usuarios.

> **Note**
>
> Esta acción empezará a eliminar a usuarios inmediatamente y puede tardar varios minutos. Los usuarios eliminados ya no podrán iniciar sesión en su red de Wickr del cliente Wickr.

Suspender masivamente a los usuarios de la red AWS Wickr

Puedes suspender de forma masiva a los usuarios de la red Wickr en la sección de administración de usuarios de Wickr. AWS Management Console

> **Note**
>
> La opción de suspender usuarios de forma masiva solo se aplica cuando el SSO no está activado.

Para suspender en bloque a los usuarios de la red de Wickr, siga el procedimiento que se detalla a continuación.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.
4. La pestaña del directorio del equipo muestra los usuarios registrados en tu red Wickr.
5. En la pestaña del directorio del equipo, selecciona Administrar usuarios y, a continuación, selecciona Suspender de forma masiva.
6. En la página de suspensión masiva de usuarios, descarga la plantilla CSV de ejemplo. Para descargar la plantilla de ejemplo, selecciona Descargar plantilla.
7. Rellene la plantilla con el correo electrónico de los usuarios que desee suspender en bloque de la red.
8. Cargue la plantilla CSV una vez completada. Puede arrastrar y soltar el archivo en el cuadro de carga o seleccionar un archivo.

9. Selecciona Suspender usuarios.

> **Note**
>
> Esta acción empezará a suspender a los usuarios de forma inmediata y puede tardar varios minutos. Los usuarios suspendidos no podrán iniciar sesión en su red de Wickr del cliente Wickr. Cuando se suspende a un usuario que está conectado a la red de Wickr del cliente, la sesión de dicho usuario se cierra automáticamente.

Usuarios invitados en la red AWS Wickr

La característica de usuario invitado de Wickr permite que usuarios invitados individuales inicien sesión en el cliente Wickr y colaboren con los usuarios de la red de Wickr. Los administradores de Wickr pueden habilitar o deshabilitar los usuarios invitados en sus redes de Wickr.

Una vez habilitada la característica, los usuarios invitados a su red de Wickr pueden interactuar con los usuarios de su red de Wickr. Se le aplicará una tarifa Cuenta de AWS por la función de usuario invitado. Para obtener más información sobre los precios de la característica de usuario invitado, consulta la página de Precios de Wickr en los complementos Precios.

Temas

- Habilitar o deshabilitar los usuarios invitados en la red AWS Wickr
- Ver el recuento de usuarios invitados en la red AWS Wickr
- Ver el uso mensual en la red AWS Wickr
- Ver los usuarios invitados en la red AWS Wickr
- Bloquear a un usuario invitado en la red AWS Wickr

Habilitar o deshabilitar los usuarios invitados en la red AWS Wickr

Puede activar o desactivar los usuarios invitados en su red de Wickr.

Complete el procedimiento siguiente para habilitar o deshabilitar usuarios invitados para su red de Wickr.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/

2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Grupos de seguridad.
4. Seleccione el nombre de un grupo de seguridad específico.

> **Note**
>
> Puede habilitar usuarios invitados únicamente para grupos de seguridad individuales. Para habilitar usuarios invitados en todos los grupos de seguridad de su red de Wickr, debe habilitar la característica para cada grupo de seguridad de su red.

5. Elija la pestaña Federación en el grupo de seguridad.
6. Hay dos ubicaciones en las que está disponible la opción de habilitar a los usuarios invitados:
   - Federación local: para las redes del este de EE. UU. (Virginia del Norte), selecciona Editar en la sección de federaciones locales de la página.
   - Federación global: para el resto de redes de otras regiones, selecciona Editar en la sección Federación global de la página.
7. En la página Editar federación, selecciona Habilitar la federación.
8. Elija Guardar cambios para guardar el cambio y hacerlo efectivo para el grupo de seguridad.

   Los usuarios registrados en el grupo de seguridad específico de su red de Wickr ahora pueden interactuar con usuarios invitados. Para obtener más información, consulte Usuarios invitados en la Guía del usuario de Wickr.

Ver el recuento de usuarios invitados en la red AWS Wickr

Puede ver el recuento de usuarios invitados en su red de Wickr.

Siga el procedimiento indicado a continuación para ver la cuenta de usuario invitado de su red de Wickr.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.

   La página de administración de usuarios muestra un recuento de usuarios invitados en tu red Wickr.

Ver el uso mensual en la red AWS Wickr

Puede ver el número de usuarios invitados con los que se ha comunicado su red durante un período de facturación.

Complete el siguiente procedimiento para ver el uso mensual de su red Wickr.

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.
4. Seleccione la pestaña Usuarios invitados.

   La pestaña Usuarios invitados muestra el uso mensual de los usuarios invitados.

   > **Note**
   >
   > Los datos de facturación de invitados se actualizan cada 24 horas.

Ver los usuarios invitados en la red AWS Wickr

Puede ver los usuarios invitados con los que se ha comunicado un usuario de la red durante un período de facturación específico.

Complete el siguiente procedimiento para ver los usuarios invitados con los que se comunicó un usuario de la red durante un período de facturación específico.

1. Abre el formulario AWS Management Console Wickr Cat https://console.aws.amazon.com/wickr/.
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.
4. Seleccione la pestaña Usuarios invitados.

   La pestaña Usuarios invitados muestra los usuarios invitados de la red.

Bloquear a un usuario invitado en la red AWS Wickr

Puedes bloquear y desbloquear a un usuario invitado en tu red de Wickr. Los usuarios bloqueados no pueden comunicarse con nadie de su red.

Cómo bloquear a un usuario invitado

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.
4. Seleccione la pestaña Usuarios invitados.

   La pestaña Usuarios invitados muestra los usuarios invitados de la red.
5. En la sección Usuarios invitados, busque el correo electrónico del usuario invitado que desea bloquear.
6. En la parte derecha del nombre del usuario invitado, seleccione los tres puntos y elija Bloquear usuario invitado.
7. Seleccione Bloquear en la ventana emergente.
8. Para ver la lista de usuarios bloqueados en tu red de Wickr, selecciona el menú desplegable Estado y, a continuación, selecciona Bloqueado.

Cómo bloquear a un usuario invitado

1. Abre el formulario AWS Management Console Wickr Cat. https://console.aws.amazon.com/wickr/
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Administración de usuarios.
4. Seleccione la pestaña Usuarios invitados.

   La pestaña Usuarios invitados muestra los usuarios invitados de la red.
5. Selecciona el menú desplegable Estado y, a continuación, selecciona Bloqueado.
6. En la sección Bloqueado, busca el correo electrónico del usuario invitado que quieres desbloquear.
7. En la parte derecha del nombre del usuario invitado, selecciona los tres puntos y elige Desbloquear usuario.
8. Selecciona Desbloquear en la ventana emergente.

Seguridad en AWS Wickr

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 más información sobre los programas de conformidad que se aplican a AWS Wickr, consulte AWS Servicios dentro del alcance por programa de conformidad AWS Servicios incluidos .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Wickr. En los siguientes temas, se le mostrará cómo configurar Wickr para satisfacer sus objetivos de seguridad y conformidad. También aprenderás a usar otros AWS servicios que te ayudan a monitorear y proteger tus recursos de Wickr.

Temas

- Protección de datos en AWS Wickr
- Administración de identidades y accesos en alta AWS Wickr
- Validación de conformidad
- Resiliencia en AWS Wickr
- Seguridad de la infraestructura en AWS Wickr
- Configuración y análisis de vulnerabilidades en AWS Wickr
- Prácticas recomendadas de seguridad para AWS Wickr

Protección de datos en AWS Wickr

El modelo de se aplica a protección de datos en AWS Wickr. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres 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, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta 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:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. 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. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza 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 140-3 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, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

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 trabajas con Wickr u otro dispositivo Servicios de AWS mediante la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese

en etiquetas o campos de texto 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.

Administración de identidades y accesos en alta AWS Wickr

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Wickr. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Audiencia de AWS Wickr
- Autenticación con identidades para AWS Wickr
- Administración del acceso mediante políticas de AWS Wickr
- AWS políticas administradas para AWS Wickr
- Cómo funciona AWS Wickr con IAM
- Ejemplos de políticas basadas en identidades de AWS Wickr
- Solución de problemas de identidades y accesos en AWS Wickr

Audiencia de AWS Wickr

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en Wickr.

Usuario de servicio: si utiliza el servicio de Wickr para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Wickr para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Wickr, consulte Solución de problemas de identidades y accesos en AWS Wickr.

Administrador de servicio: si está a cargo de los recursos de Wickr en su empresa, probablemente tenga acceso completo a Wickr. Su trabajo consiste en determinar a qué características y recursos

de Wickr deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM 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 su empresa puede utilizar IAM con Wickr, consulte Cómo funciona AWS Wickr con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Wickr. Para consultar ejemplos de políticas basadas en la identidad de Wickr que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidades de AWS Wickr.

Autenticación con identidades para AWS Wickr

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que 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 Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión 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. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios empresarial, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos 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 Casos de uso para usuarios de IAM 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 de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

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

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener

información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM 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 al 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. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo 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 que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración del acceso mediante políticas de AWS Wickr

Puede controlar el acceso AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. 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 en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza 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 de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en 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 sobre 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. Los 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 asocia 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 en función de 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 () ACLs

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

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la 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.

- Límites 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 identidad. 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 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 de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para 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.

AWS políticas administradas para AWS Wickr

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.

Servicios de AWS mantener y actualizar las políticas AWS 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 gestionada por 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.

AWS política gestionada: AWSWickr FullAccess

Puede adjuntar la política `AWSWickrFullAccess` a las identidades de IAM. Esta política concede todos los permisos administrativos al servicio Wickr, incluida la AWS Management Console para Wickr en AWS Management Console. Para más información sobre cómo adjuntar políticas a una

identidad, consulte Adición y eliminación de permisos de identidad de IAM en la Guía del usuario de AWS Identity and Access Management .

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `wickr`: concede todos los permisos administrativos al servicio Wickr.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "wickr:*",
            "Resource": "*"
        }
    ]
}
```

Wickr actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Wickr desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Wickr.

Cambio	Descripción	Fecha
AWSWickrFullAccess: política nueva	Wickr agregó una nueva política que otorga todos los permisos administrativos al servicio Wickr, incluida la consola de administrador de Wickr en AWS Management Console.	28 de noviembre de 2022

Cambio	Descripción	Fecha
Wickr comenzó el seguimiento de los cambios	Wickr comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	28 de noviembre de 2022

Cómo funciona AWS Wickr con IAM

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

Características de IAM que puede utilizar con AWS Wickr

Característica de IAM	Compatibilidad de Wickr
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	No
Claves de condición de política	No
ACLs	No
ABAC (etiquetas en políticas)	No
Credenciales temporales	No
Permisos de entidades principales	No
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una visión general de cómo funcionan Wickr y otros AWS servicios con la mayoría de las funciones de IAM, consulta los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades de Wickr

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en 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 identidades de IAM, puede especificar las acciones y los 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 asociada. Para obtener más información sobre 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 Wickr

Para ver ejemplos de políticas basadas en identidad de Wickr, consulte Ejemplos de políticas basadas en identidades de AWS Wickr.

Políticas basadas en recursos de Wickr

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los 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 asocia 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 en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones de política para Wickr

Compatibilidad con las acciones 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 en 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 Wickr, consulte Acciones definidas por AWS Wickr en la Referencia de autorizaciones de servicio.

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

```
wickr
```

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

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

Para ver ejemplos de políticas basadas en identidad de Wickr, consulte Ejemplos de políticas basadas en identidades de AWS Wickr.

Recursos de políticas de Wickr

Compatibilidad con recursos de políticas: no

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 en 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). Puedes 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, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de Wickr y sus correspondientes ARNs, consulte Recursos definidos por AWS Wickr en la Referencia de autorización de servicios. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recursos, consulte Acciones definidas por AWS Wickr.

Para ver ejemplos de políticas basadas en identidad de Wickr, consulte Ejemplos de políticas basadas en identidades de AWS Wickr.

Claves de condición de política para Wickr

Compatibilidad con claves de condición de políticas específicas del servicio: no

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 en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones

condicionales que utilizan 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 `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta 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 AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Wickr, consulte Claves de condición para AWS Wickr en la Referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por AWS Wickr.

Para ver ejemplos de políticas basadas en identidad de Wickr, consulte Ejemplos de políticas basadas en identidades de AWS Wickr.

ACLs en Wickr

Soportes ACLs: No

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

ABAC con Wickr

Compatibilidad con ABAC (etiquetas en las políticas): no

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.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

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`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de 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 Wickr

Compatible con el uso de credenciales temporales: no

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles 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 mediante 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 sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (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 obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios de Wickr

Compatibilidad con sesiones de acceso directo (FAS): no

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio de Wickr

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM 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 Wickr. Edite los roles de servicio solo cuando Wickr proporcione orientación para hacerlo.

Roles vinculados a servicios de Wickr

Compatibilidad con roles vinculados al servicio: no

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 al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta 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 AWS Wickr

De forma predeterminada, un nuevo usuario de IAM no tiene permisos para realizar ninguna actividad. Un administrador de IAM debe crear y asignar políticas de IAM que concedan permisos a los usuarios para administrar el servicio AWS Wickr. A continuación se muestra un ejemplo de una política de permisos.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wickr:CreateAdminSession",
                "wickr:ListNetworks"
            ],
            "Resource": "*"
        }
    ]
}
```

Este ejemplo de política otorga a los usuarios permisos para crear, ver y administrar redes de Wickr mediante Wickr. AWS Management Console Para obtener más información sobre los elementos de una instrucción de política de IAM, consulte Políticas basadas en identidades de Wickr. Para obtener más información acerca de cómo crear una política 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 sobre las políticas
- Uso de la AWS Management Console para Wickr
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Wickr de la 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 con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la AWS Management Console para Wickr

Adjunta la política `AWSWickrFullAccess` AWS gestionada a tus identidades de IAM para concederles todos los permisos administrativos necesarios para acceder al servicio de Wickr, incluida la consola de administrador de Wickr. AWS Management Console Para obtener más información, consulte AWS política gestionada: AWSWickr FullAccess.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
```

```
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solución de problemas de identidades y accesos en AWS Wickr

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

Temas

- No estoy autorizado a realizar ninguna acción administrativa en nombre de Wickr AWS Management Console

No estoy autorizado a realizar ninguna acción administrativa en nombre de Wickr AWS Management Console

Si el formulario AWS Management Console de Wickr te indica que no estás autorizado a realizar una acción, debes ponerte en contacto con tu administrador para obtener ayuda. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente ejemplo de error se produce cuando el usuario de `mateojackson` IAM intenta usar AWS Management Console for Wickr para crear, administrar o ver las redes de Wickr en AWS Management Console for Wickr, pero no tiene los permisos y. `wickr:CreateAdminSession` `wickr:ListNetworks`

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wickr:ListNetworks
```

En este caso, Mateo pide a su administrador que actualice sus políticas para poder acceder a las de Wickr mediante AWS Management Console las acciones y. `wickr:CreateAdminSession` `wickr:ListNetworks` Para obtener más información, consulte Ejemplos de políticas basadas en identidades de AWS Wickr y AWS política gestionada: AWSWickr FullAccess.

Validación de conformidad

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de cumplimiento específicos, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de cumplimiento y . 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 conformidad al utilizar Wickr se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido sobre : estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- Evaluación de los recursos con las reglas de la guía para AWS Config desarrolladores: AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS Wickr

La infraestructura AWS global se basa Regiones de AWS en zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, Wickr ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos. Para obtener más información, consulte Retención de datos para AWS Wickr.

Seguridad de la infraestructura en AWS Wickr

Como servicio gestionado, AWS Wickr está protegido por los procedimientos de seguridad de red AWS global que se describen en el documento técnico Amazon Web Services: Overview of Security Processes.

Configuración y análisis de vulnerabilidades en AWS Wickr

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted, nuestro cliente. Para obtener más información, consulte el modelo de responsabilidad AWS compartida.

Es su responsabilidad configurar Wickr de acuerdo con las especificaciones y las directrices, indicar periódicamente a sus usuarios que descarguen la última versión del cliente Wickr, asegurarse de que está ejecutando la última versión del bot de retención de datos de Wickr y supervisar el uso de Wickr por parte de sus usuarios.

Prácticas recomendadas de seguridad para AWS Wickr

Wickr proporciona un número 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 constituyen 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.

Para evitar posibles eventos de seguridad asociados con el uso de Wickr, siga estas prácticas recomendadas:

- Implemente un acceso de privilegio mínimo y cree roles específicos para usarlos en las acciones de Wickr. Use plantillas de IAM para crear un rol. Para obtener más información, consulte AWS políticas administradas para AWS Wickr.

- Acceda al AWS Management Console de Wickr autenticándose con el AWS Management Console primero. No comparta las credenciales de su consola personal. Cualquier usuario de Internet puede navegar hasta la consola, pero no puede iniciar sesión a menos que tenga credenciales válidas para acceder a la consola.

Supervisión de AWS Wickr

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Wickr y el resto de sus AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para vigilar Wickr, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas. Para obtener más información, consulte la AWS CloudTrail Guía del usuario de . Para obtener más información sobre cómo registrar las llamadas a la API de Wickr mediante CloudTrail, consulteRegistro de llamadas a la API Wickr de AWS mediante AWS CloudTrail.

Registro de llamadas a la API Wickr de AWS mediante AWS CloudTrail

AWS Wickr está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Wickr. CloudTrail captura todas las llamadas a la API de Wickr como eventos. Las llamadas capturadas incluyen llamadas de Wickr y llamadas en código a las operaciones de la API de Wickr. AWS Management Console Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Wickr. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a Wickr, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales. Para obtener más información CloudTrail, consulta la Guía del AWS CloudTrail usuario.

Información sobre Wickr en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Wickr, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulta Cómo ver eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los de Wickr, 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 AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar 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 y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de Wickr las registra. CloudTrail Por ejemplo, las llamadas a y `ListNetworks` las acciones generan entradas en los archivos de CloudTrail registro. `CreateAdminSession`

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 AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas de los archivos de registro de Wickr

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 única de cualquier fuente e incluye 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 registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateAdminSession` acción.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T08:19:24Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateAdminSession",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkId": 56019692
    },
    "responseElements": {
        "sessionCookie": "***",
        "sessionNonce": "***"
    },
    "requestID": "39ed0e6f-36e9-460d-8a6e-f24be0ec11c5",
    "eventID": "98ccb633-0e6c-4325-8996-35c3043022ac",
    "readOnly": false,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `CreateNetwork` acción.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T07:54:09Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateNetwork",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "BOT_Network",
        "accessLevel": "3000"
    },
```

```
    "responseElements": null,
    "requestID": "b83c0b6e-73ae-45b6-8c85-9910f64d33a1",
    "eventID": "551277bb-87e0-4e66-b2a0-3cc1eff303f3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `ListNetworks` acción.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T12:19:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T12:29:32Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListNetworks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
```

```
    "requestParameters": null,
    "responseElements": null,
    "requestID": "b9800ba8-541a-43d1-9c8e-efd94d5f2115",
    "eventID": "5fbc83d7-771b-457d-9329-f85163a6a428",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `UpdateNetworkdetails` acción.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T22:42:58Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "UpdateNetworkDetails",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
```

```
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "CloudTrailTest1",
        "networkId": <network-id>
    },
    "responseElements": null,
    "requestID": "abced980-23c7-4de1-b3e3-56aaf0e1fdbb",
    "eventID": "a4dc3391-bdce-487d-b9b0-6f76cedbb198",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `TagResource` acción.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T23:06:04Z",
```

```
    "eventSource": "wickr.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "resource-arn": "<arn>",
        "tags": {
            "some-existing-key-3": "value 1"
        }
    },
    "responseElements": null,
    "requestID": "4ff210e1-f69c-4058-8ac3-633fed546983",
    "eventID": "26147035-8130-4841-b908-4537845fac6a",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `ListTagsForResource` acción.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<access-key-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2023-03-08T18:50:37Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T18:50:37Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListTagsForResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "axios/0.27.2",
    "errorCode": "AccessDenied",
    "requestParameters": {
        "resource-arn": "<arn>"
    },
    "responseElements": {
        "message": "User: <arn> is not authorized to perform: wickr:ListTagsForResource
 on resource: <arn> with an explicit deny"
    },
    "requestID": "c7488490-a987-4ca2-a686-b29d06db89ed",
    "eventID": "5699d5de-3c69-4fe8-b353-8ae62f249187",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Panel de análisis en AWS Wickr

Puede usar el panel de análisis para ver cómo su organización utiliza AWS Wickr. El siguiente procedimiento explica cómo acceder al panel de análisis mediante la consola de AWS Wickr.

Para acceder al panel de análisis

1. Abre el formulario AWS Management Console Wickr en https://console.aws.amazon.com/wickr/.
2. En la página Redes, selecciona el nombre de la red para navegar hasta esa red.
3. En el panel de navegación, elija Analytics (Análisis).

   La página de análisis muestra las métricas de su red en diferentes pestañas.

En la página de análisis, encontrarás un filtro de plazos en la esquina superior derecha de cada pestaña. Este filtro se aplica a toda la página. Además, en la esquina superior derecha de cada pestaña, puede exportar los puntos de datos del intervalo de tiempo seleccionado seleccionando la opción de exportación disponible.

> **Note**
>
> La hora seleccionada está en UTC (hora universal coordinada).

Están disponibles las siguientes pestañas:

- Muestra la descripción general:
  - Registrados: el número total de usuarios registrados, incluidos los usuarios activos y suspendidos en la red durante el tiempo seleccionado. No incluye los usuarios pendientes ni los invitados.
  - Pendiente: el número total de usuarios pendientes en la red durante el tiempo seleccionado.
  - Registro de usuarios: el gráfico muestra el número total de usuarios registrados en el intervalo de tiempo seleccionado.
  - Dispositivos: el número de dispositivos en los que la aplicación ha estado activa.
  - Versiones de cliente: la cantidad de dispositivos activos clasificados según sus versiones de cliente.

- Los miembros muestran:
  - Estado: usuarios activos en la red durante el período de tiempo seleccionado.
  - Usuarios activos:
    - El gráfico muestra el recuento de usuarios activos a lo largo del tiempo y se puede agregar por día, semana o mes (dentro del intervalo de tiempo seleccionado anteriormente).
    - El recuento de usuarios activos se puede desglosar por plataforma, versión de cliente o grupo de seguridad. Si se eliminó un grupo de seguridad, el recuento total se mostrará como Eliminado#.

- Aparecen los mensajes:
  - Mensajes enviados: el recuento de mensajes únicos enviados por todos los usuarios y bots de la red en el período de tiempo seleccionado.

- Llamadas: número de llamadas únicas realizadas por todos los usuarios de la red.
- Archivos: número de archivos enviados por los usuarios de la red (incluye notas de voz).
- Dispositivos: el gráfico circular muestra la cantidad de dispositivos activos clasificados por su sistema operativo.
- Versiones de cliente: la cantidad de dispositivos activos clasificados según sus versiones de cliente.

Historial del documento

En la tabla siguiente se detallan las versiones de la documentación de Wickr.

Cambio	Descripción	Fecha
La vista previa del archivo ya está disponible	Las redes de Wickr tienen ahora la capacidad de federarse en todas Para obtener más información, consulte Vista previa del archivo de AWS Wickr.	29 de 2025
Ya está disponible la consola de administración Wickr, recientemente rediseñada	Wickr ha mejorado la consola de administración de Wickr para mejorar la navegació n y la accesibilidad para los administradores.	13 de marzo de 2025
Ahora Wickr está disponible en la de Europa (Londres). Región de AWS	Ahora Wickr está disponible en la de Europa (Londres). Región de AWS Para obtener más información, consulta Disponibilidad regional.	20 de noviembre de 2024
La opción Eliminar red ya está disponible	Las redes de Wickr tienen ahora la capacidad de federarse en todas Para obtener más información, consulte Eliminar la red en AWS Wickr.	4 de octubre de 2024
Ya está disponible la configura ción de AWS Wickr con el inicio de sesión único de Microsoft Entra (Azure AD)	AWS Wickr se puede configurar para usar Microsoft Entra (Azure AD) como proveedor de identidades. Para obtener más informaci	18 de septiembre de 2024

	ón, consulte Configurar AWS Wickr con el inicio de sesión único de Microsoft Entra (Azure AD).	
Ahora Wickr está disponible en la de Europa (Londres). Región de AWS	Ahora Wickr está disponible en la de Europa (Londres). Región de AWS Para obtener más información, consulta Disponibilidad regional.	12 de agosto de 2024
La clasificación y federación transfronterizas ya están disponibles	La función de clasificación transfronteriza permite a los usuarios cambiar las conversaciones de la interfaz de GovCloud usuario. Para obtener más información, consulte Clasificación y federación GovCloud transfronterizas.	25 de junio de 2024
La función de lectura de recibos ya está disponible	Los administradores de Wickr ahora pueden activar o desactivar la función de confirmación de lectura en la Consola de administración. Para obtener más información, consulte Leer recibos.	23 de abril de 2024

Global Federation ahora admite la federación restringida y los administradores pueden ver los análisis de uso en la Consola de administración	Global Federation ahora admite la federación restringida. Esto funciona para las redes de Wickr en otras Regiones de AWS. Para obtener más información, consulte Grupos de seguridad. Además, los administradores ahora pueden ver sus análisis de uso en el panel de análisis de la consola de administración. Para obtener más información, consulte el panel de análisis.	28 de marzo de 2024
Ya está disponible una prueba gratuita de tres meses del plan Premium de AWS Wickr	Los administradores de Wickr ahora pueden elegir un plan Premium de prueba gratuito de tres meses para un máximo de 30 usuarios. Durante la prueba gratuita, están disponibles todas las funciones de los planes Estándar y Premium, incluidos los controles de administración ilimitados y la retención de datos. La característica de usuario invitado está disponible de forma general y se han agregado más controles de administración. Para obtener más información, consulta Administrar el plan.	9 de febrero de 2024

La característica de usuario invitado está disponible de forma general y se han agregado más controles de administración.	Los administradores de Wickr pueden ahora acceder a una serie de nuevas caracterí sticas, como la lista de usuarios invitados, la posibilid ad de eliminar o suspender usuarios de forma masiva y la opción de impedir que los usuarios invitados se comuniquen en su red de Wickr. Si desea obtener más información, consulte Usuarios invitados.	8 de noviembre de 2023
Ahora Wickr está disponible en la de Europa (Fráncfort). Región de AWS	Ahora Wickr está disponible en la de Europa (Fráncfort). Región de AWS Para obtener más información, consulta Disponibilidad regional.	26 de octubre de 2023
Las redes de Wickr tienen ahora la capacidad de federarse en todas Regiones de AWS	Las redes de Wickr tienen ahora la capacidad de federarse en todas Regiones de AWS. Para obtener más información, consulte Grupos de seguridad.	29 de septiembre de 2023
Ahora Wickr está disponible en la de Europa (Londres). Región de AWS	Ahora Wickr está disponible en la de Europa (Londres). Región de AWS Para obtener más información, consulta Disponibilidad regional.	23 de agosto de 2023

Ahora Wickr está disponible en la de Canadá (Centro). Región de AWS	Ahora Wickr está disponible en la de Canadá (Centro). Región de AWS Para obtener más información, consulta Disponibilidad regional.	3 de julio de 2023
La característica de usuario invitado está ahora disponible para su vista previa	Los usuarios invitados pueden iniciar sesión en el cliente Wickr y colaborar con usuarios de la red de Wickr. Para más información, consulte Usuarios invitados (vista previa).	31 de mayo de 2023
AWS Wickr está ahora integrado con AWS CloudTrail, y está disponible en GovCloud AWS GovCloud (Oeste de EE. UU.) como WickrGov. WickrGov	AWS Wickr está ya integrado con AWS CloudTrail. Para obtener más información, consulte Registro de llamadas a la API de AWS Wickr mediante AWS CloudTrail. Ahora Wickr está disponible en la de Canadá AWS GovCloud (Oeste de EE. UU.). WickrGov Para obtener más información, consulte AWS WickrGov en la Guía del usuario de AWS GovCloud (US) .	30 de marzo de 2023
Etiquetado y creación de redes múltiples	AWS Wickr admite ahora el etiquetado. Para obtener más información, consulta Etiquetas de red. Ahora se pueden crear varias redes en Wickr. Para obtener más información, consulte Creación de una red.	7 de marzo de 2023

Versión inicial	Versión inicial de la Guía de administración de Wickr	28 de noviembre de 2022

Notas de la versión

Para ayudarle a realizar un seguimiento de las mejoras y de las actualizaciones continuas en Wickr, estamos publicando notificaciones de la versión que describen los cambios recientes.

Mayo de 2025

- La vista previa del archivo ya está disponible. Si el administrador deshabilita las descargas de archivos en la consola de administración de un grupo de seguridad, los usuarios solo podrán ver una lista de los archivos compatibles en las pestañas Mensajes y Archivos.

Marzo de 2025

- La consola de administración de Wickr rediseñada ya está disponible.

Octubre de 2024

- Wickr ahora admite la eliminación de redes. Para obtener más información, consulte Eliminar la red en AWS Wickr.

Septiembre de 2024

- Los administradores ahora pueden configurar AWS Wickr con el inicio de sesión único de Microsoft Entra (Azure AD). Para obtener más información, consulte Configurar AWS Wickr con el inicio de sesión único de Microsoft Entra (Azure AD).

Agosto de 2024

- Mejoras
  - Wickr ya está disponible en Europa (Zúrich). Región de AWS

Junio de 2024

- La clasificación y federación transfronterizas ya están disponibles para GovCloud los usuarios. Para obtener más información, consulte Clasificación y federación GovCloud transfronterizas.

Abril de 2024

- Wickr ahora admite confirmaciones de lectura. Para obtener más información, consulta Leer recibos.

Marzo de 2024

- La federación global ahora admite la federación restringida, donde la federación global solo se puede habilitar para redes seleccionadas que se agreguen bajo la federación restringida. Esto funciona para las redes de Wickr en otras Regiones de AWS. Para obtener más información, consulte Grupos de seguridad.
- Los administradores ahora pueden ver sus análisis de uso en el panel de análisis de la Consola de administración. Para obtener más información, consulte el panel de análisis.

Febrero de 2024

- AWS Wickr ofrece ahora una prueba gratuita de tres meses de su plan Premium para un máximo de 30 usuarios. Los cambios y las limitaciones incluyen:
  - Todas las funciones de los planes Estándar y Premium, como los controles administrativos ilimitados y la retención de datos, ahora están disponibles en la versión de prueba gratuita del plan Premium. La función de usuario invitado no está disponible durante la prueba gratuita de Premium.
  - La versión de prueba gratuita anterior ya no está disponible. Puedes actualizar tu versión de prueba gratuita o tu plan Estándar a una versión de prueba gratuita Premium si aún no la has utilizado. Para obtener más información, consulta Administrar el plan.

Noviembre de 2023

- La característica de usuarios invitados está ahora disponible de forma general. Los cambios y las adiciones incluyen:
  - Posibilidad de denunciar el abuso por parte de otros usuarios de Wickr.
  - Los administradores pueden ver una lista de los usuarios invitados con los que ha interactuado una red y los recuentos de uso mensual.
  - Los administradores pueden impedir que los usuarios invitados se comuniquen con su red.
  - Precios de complementos para usuarios invitados.

- Mejoras en el control del administrador
  - Posibilidad de agrupar delete/suspend usuarios.
  - Configuración de SSO adicional para configurar un periodo de gracia para la actualización de tokens.

Octubre de 2023

- Mejoras
  - Ahora Wickr está disponible en la Región de AWS de Europa (Fráncfort).

Septiembre de 2023

- Mejoras
  - Las redes de Wickr tienen ahora la capacidad de federarse en todas Regiones de AWS. Para obtener más información, consulte Grupos de seguridad.

Agosto de 2023

- Mejoras
  - Ahora Wickr está disponible en la Región de AWS de Europa (Londres).

Julio de 2023

- Mejoras
  - Ahora Wickr está disponible en la Región de AWS de Canadá (Centro).

Mayo de 2023

- Mejoras
  - Se ha añadido compatibilidad para usuarios invitados. Para obtener más información, consulte Usuarios invitados en la red AWS Wickr.

Marzo de 2023

- Wickr ahora está integrado con AWS CloudTrail. Para obtener más información, consulte Registro de llamadas a la API Wickr de AWS mediante AWS CloudTrail.
- Wickr ahora está disponible en AWS GovCloud (EE. UU.-West) As. WickrGov Para obtener más información, consulte AWS WickrGov en la Guía del usuario de AWS GovCloud (US) .
- Wickr ahora admite el etiquetado. Para obtener más información, consulte Etiquetas de red para AWS Wickr. Ahora se pueden crear varias redes en Wickr. Para obtener más información, consulte Paso 1: crear una red.

Febrero de 2023

- Wickr es ahora compatible con el Kit de Asalto Táctico Android (ATAK). Para obtener más información, consulte Cómo habilitar ATAK en el panel de la red de Wickr.

Enero de 2023

- El inicio de sesión único (SSO) ahora se puede configurar en todos los planes, incluidos los de prueba gratuita y estándar.

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.