



AWS

Cloud Manager 3.8

NetApp
March 25, 2024

Tabla de contenidos

- AWS 1
 - Credenciales y permisos de AWS 1
 - Gestión de las credenciales y suscripciones de AWS para Cloud Manager 3

AWS

Credenciales y permisos de AWS

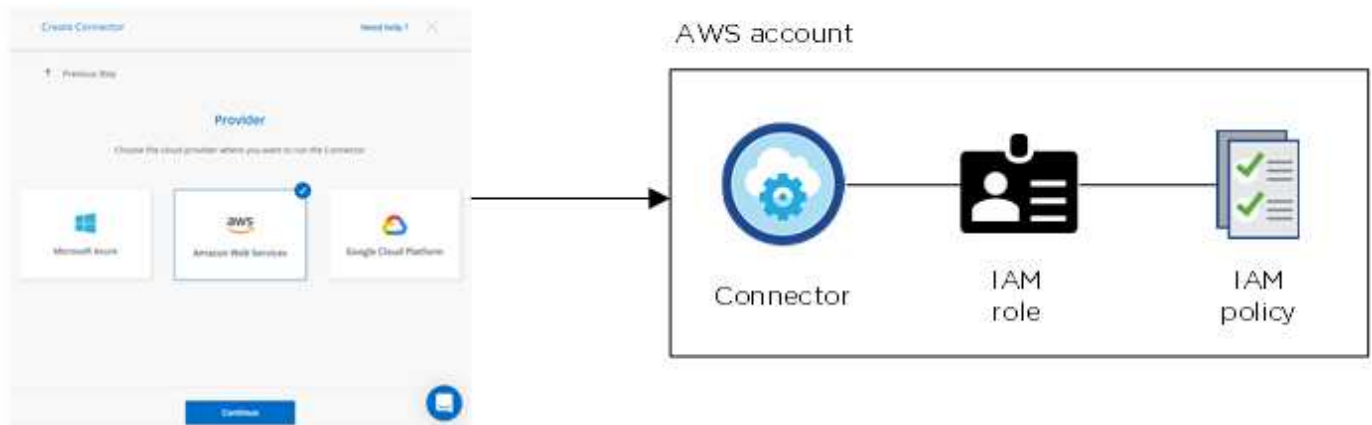
Cloud Manager le permite elegir las credenciales de AWS que desea utilizar al implementar Cloud Volumes ONTAP. Puede implementar todos sus sistemas Cloud Volumes ONTAP con las credenciales iniciales de AWS o bien añadir credenciales adicionales.

Credenciales iniciales de AWS

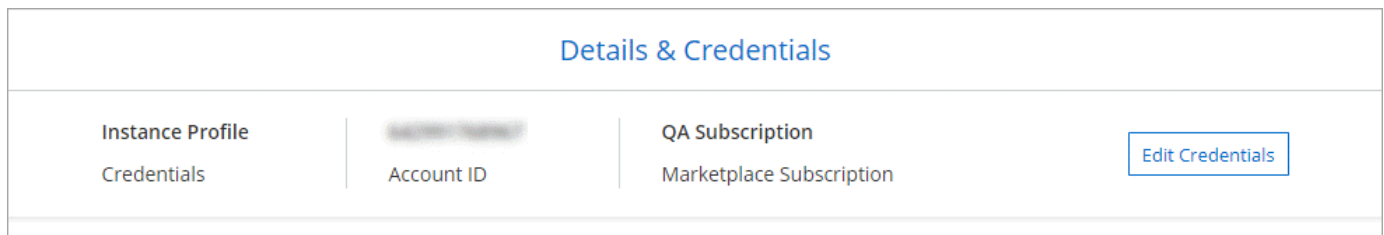
Al implementar un conector desde Cloud Manager, necesita utilizar una cuenta de AWS que tenga permisos para ejecutar la instancia de Connector. Los permisos necesarios se enumeran en la ["La política de implementación de conectores para AWS"](#).

Cuando Cloud Manager inicia la instancia de Connector en AWS, crea un rol IAM y un perfil de instancia para la instancia. También une una política que ofrece permisos para gestionar recursos y procesos dentro de esa cuenta de AWS. ["Revise cómo Cloud Manager utiliza los permisos"](#).

Cloud Manager

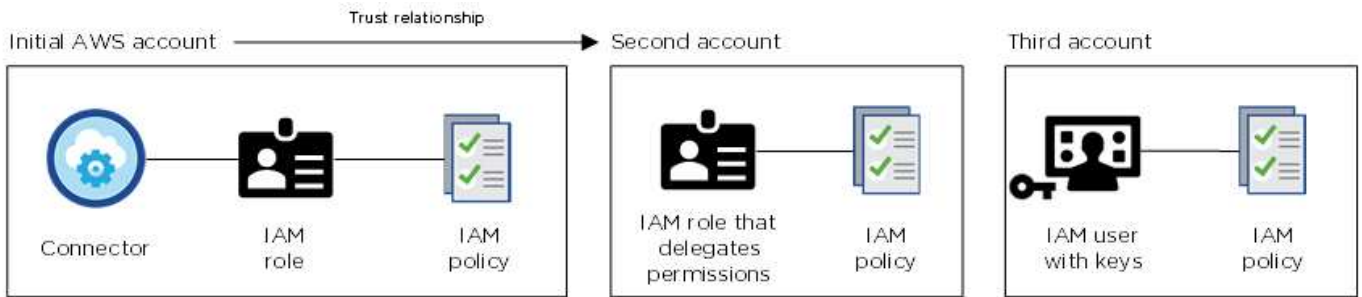


Cloud Manager selecciona estas credenciales de AWS de forma predeterminada al crear un entorno de trabajo nuevo para Cloud Volumes ONTAP:



Credenciales adicionales de AWS

Si desea ejecutar Cloud Volumes ONTAP en diferentes cuentas de AWS, puede hacerlo también ["Proporcione las claves AWS para un usuario de IAM o el ARN de un rol en una cuenta de confianza"](#). En la siguiente imagen se muestran dos cuentas adicionales, una que proporciona permisos a través de una función IAM en una cuenta de confianza y otra a través de las claves AWS de un usuario de IAM:



Entonces lo haría "Añada las credenciales de la cuenta a Cloud Manager" Especificando el nombre de recurso de Amazon (ARN) del rol de IAM o las claves de AWS del usuario de IAM.

Después de añadir otro conjunto de credenciales, puede cambiar a ellas al crear un nuevo entorno de trabajo:

Edit Account & Add Subscription

Credentials

- Keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]**
- QA Subscription

Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

+ Add Subscription

Apply **Cancel**

¿Qué pasa con las puestas en marcha de Marketplace y las puestas en marcha en las instalaciones?

En las secciones anteriores se describe el método de implementación recomendado para el conector, que es de Cloud Manager. También puede implementar un conector en AWS desde el ["Mercado AWS"](#) y usted puede ["Instale el conector en las instalaciones"](#).

Si utiliza el Marketplace, los permisos se proporcionan de la misma manera. Solo tiene que crear y configurar manualmente el rol IAM y, a continuación, proporcionar permisos para cualquier cuenta adicional.

En el caso de las implementaciones locales, no se puede configurar la función de IAM para el sistema Cloud Manager, pero se pueden proporcionar permisos del mismo modo que se busca para cuentas de AWS adicionales.

¿Cómo puedo rotar mis credenciales de AWS de forma segura?

Como se ha descrito anteriormente, Cloud Manager permite proporcionar credenciales de AWS de varias maneras: Una función IAM asociada con la instancia de Connector, asumiendo un rol IAM en una cuenta de confianza o proporcionando claves de acceso de AWS.

Con las dos primeras opciones, Cloud Manager utiliza AWS Security Token Service para obtener credenciales temporales que giran constantemente. Este proceso es la mejor práctica, es automático y seguro.

Si proporciona claves de acceso a Cloud Manager para AWS, debe rotar las claves se actualizan en Cloud Manager a un intervalo regular. Este es un proceso completamente manual.

Gestión de las credenciales y suscripciones de AWS para Cloud Manager

Al crear un sistema de Cloud Volumes ONTAP, debe seleccionar las credenciales y la suscripción de AWS para utilizarlas con ese sistema. Si administra varias suscripciones de AWS, puede asignar cada una de ellas a diferentes credenciales de AWS desde la página Credentials.

Antes de añadir las credenciales de AWS a Cloud Manager, tiene que proporcionar los permisos necesarios para esa cuenta. Los permisos permiten que Cloud Manager gestione recursos y procesos dentro de esa cuenta de AWS. La forma en la que proporcione los permisos depende de si desea proporcionar a Cloud Manager claves de AWS o el ARN del rol en una cuenta de confianza.



Cuando implementó un conector desde Cloud Manager, Cloud Manager agregó automáticamente credenciales de AWS para la cuenta en la que implementó el conector. Esta cuenta inicial no se agrega si instaló manualmente el software Connector en un sistema existente. ["Obtenga más información acerca de los permisos y credenciales de AWS"](#).

opciones

- [Concesión de permisos proporcionando claves AWS](#)
- [Otorgar permisos asumiendo roles de IAM en otras cuentas](#)

¿Cómo puedo rotar mis credenciales de AWS de forma segura?

Cloud Manager le permite proporcionar credenciales de AWS de varias maneras: Una función IAM asociada con la instancia de Connector, asumiendo un rol IAM en una cuenta de confianza o proporcionando claves de acceso de AWS. ["Obtenga más información acerca de las credenciales y permisos de AWS"](#).

Con las dos primeras opciones, Cloud Manager utiliza AWS Security Token Service para obtener credenciales temporales que giran constantemente. Este proceso es la mejor práctica, es automático y seguro.

Si proporciona claves de acceso a Cloud Manager para AWS, debe rotar las claves se actualizan en Cloud Manager a un intervalo regular. Este es un proceso completamente manual.

Concesión de permisos proporcionando claves AWS

Si desea proporcionar a Cloud Manager claves AWS para un usuario IAM, debe conceder los permisos necesarios a ese usuario. La política de IAM de Cloud Manager define las acciones y los recursos de AWS que se permite el uso de Cloud Manager.

Pasos

1. Descargue la política de IAM de Cloud Manager desde el ["Directivas de Cloud Manager"](#).
2. Desde la consola de IAM, cree su propia política copiando y pegando el texto de la política IAM de Cloud Manager.

["Documentación de AWS: Crear políticas de IAM"](#)

3. Asocie la política a un rol de IAM o a un usuario de IAM.
 - ["Documentación de AWS: Crear roles de IAM"](#)
 - ["Documentación de AWS: Adición y eliminación de políticas de IAM"](#)

Resultado

La cuenta ahora tiene los permisos necesarios. [Ahora puede añadirlo a Cloud Manager.](#)

Otorgar permisos asumiendo roles de IAM en otras cuentas

Puede configurar una relación de confianza entre la cuenta AWS de origen en la que ha implementado la instancia de Connector y otras cuentas de AWS mediante los roles IAM. A continuación, debe proporcionar a Cloud Manager el ARN de las funciones de IAM de las cuentas de confianza.

Pasos

1. Vaya a la cuenta de destino donde desea implementar Cloud Volumes ONTAP y cree una función IAM seleccionando **otra cuenta de AWS**.

No olvide hacer lo siguiente:

- Introduzca el código de la cuenta en la que reside la instancia de Connector.
- Adjunte la política IAM de Cloud Manager, que está disponible en la ["Directivas de Cloud Manager"](#).

Create role



Select type of trusted entity

Four options for trusted entity type are shown in a row:

- AWS service**: EC2, Lambda and others.
- Another AWS account**: Belonging to you or 3rd party. This option is selected and highlighted with a blue border.
- Web identity**: Cognito or any OpenID provider.
- SAML 2.0 federation**: Your corporate directory.

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* ⓘ

- Options**
- Require external ID (Best practice when a third party will assume this role)
 - Require MFA ⓘ

2. Vaya a la cuenta de origen en la que se encuentra la instancia de Connector y seleccione la función IAM asociada a la instancia.
 - a. Haga clic en **Adjuntar directivas** y, a continuación, en **Crear directiva**.
 - b. Cree una directiva que incluya la acción "sts:AssumeRole" y el ARN del rol que creó en la cuenta de destino.

ejemplo

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
  }
}
```

Resultado

La cuenta ahora tiene los permisos necesarios. [Ahora puede añadirlo a Cloud Manager](#).

Adición de credenciales de AWS a Cloud Manager

Después de proporcionar una cuenta de AWS con los permisos requeridos, puede añadir las credenciales para dicha cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.



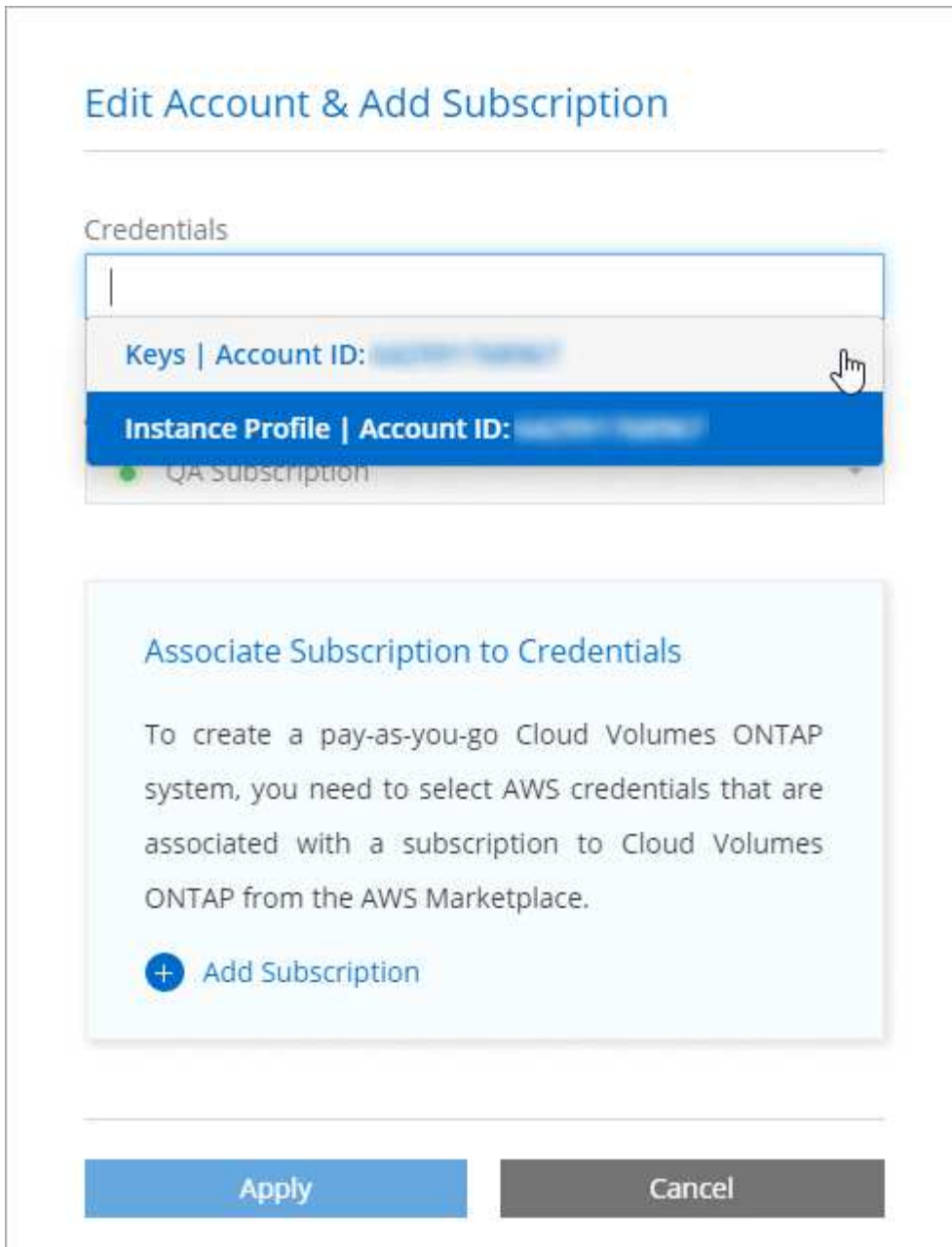
2. Haga clic en **Agregar credenciales** y seleccione **AWS**.
3. Proporcione las claves AWS o el ARN del rol de IAM de confianza.
4. Confirme que se han cumplido los requisitos de la directiva y haga clic en **continuar**.
5. Elija la suscripción de pago por uso que desee asociar con las credenciales o haga clic en **Agregar suscripción** si aún no tiene una.

Para crear un sistema Cloud Volumes ONTAP de pago por uso, las credenciales de AWS deben estar asociadas con una suscripción a Cloud Volumes ONTAP desde AWS Marketplace.

6. Haga clic en **Agregar**.

Resultado

Ahora puede cambiar a un conjunto de credenciales diferente de la página Details y Credentials al crear un nuevo entorno de trabajo:



Asociación de una suscripción de AWS a credenciales

Después de añadir sus credenciales de AWS a Cloud Manager, puede asociar una suscripción a AWS Marketplace con estas credenciales. La suscripción le permite crear un sistema de pago por uso Cloud Volumes ONTAP y usar otros servicios cloud de NetApp.

Hay dos escenarios en los que puede asociar una suscripción a AWS Marketplace después de haber añadido las credenciales a Cloud Manager:

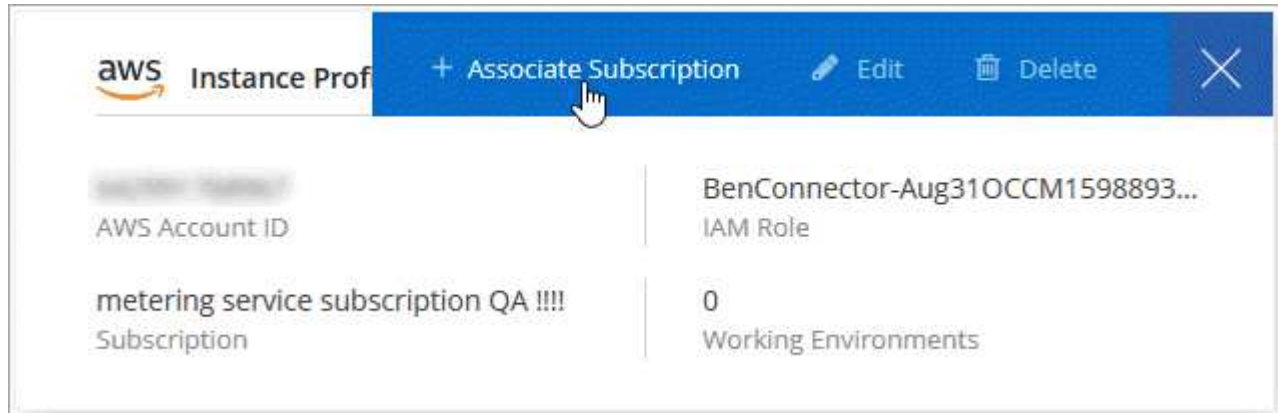
- No asoció una suscripción al agregar inicialmente las credenciales a Cloud Manager.
- Desea sustituir una suscripción existente de AWS Marketplace por una nueva suscripción.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "[Vea cómo](#)".

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.
2. Pase el ratón sobre un conjunto de credenciales y haga clic en el menú de acciones.
3. En el menú, haga clic en **Suscripción asociada**.



4. Seleccione una suscripción de la lista desplegable o haga clic en **Agregar suscripción** y siga los pasos para crear una nueva suscripción.

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_aws.mp4 (video)

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.