Gestione su cuenta

Astra Control Center

NetApp
November 21, 2023

Tabla de contenidos

Gestione su cuenta

Gestione usuarios locales y roles

Puede añadir, eliminar y editar usuarios de la instalación de Astra Control Center mediante la interfaz de usuario de Astra Control. Puede utilizar la interfaz de usuario de Astra Control o. "La API de control Astra" para gestionar usuarios.

También se puede utilizar LDAP para realizar autenticación para los usuarios seleccionados.

Utilice LDAP

LDAP es un protocolo estándar del sector para acceder a información de directorio distribuida y una opción muy popular para la autenticación empresarial. Puede conectar Astra Control Center a un servidor LDAP para realizar la autenticación de los usuarios seleccionados de Astra Control. En un nivel elevado, la configuración implica integrar Astra con LDAP y definir los usuarios y grupos de Astra Control correspondientes a las definiciones LDAP. Puede utilizar la API Astra Control o la interfaz de usuario web para configurar la autenticación LDAP y los usuarios y grupos LDAP. En la siguiente documentación, se ofrece más información:

- "Utilice la API Astra Control para gestionar la autenticación y los usuarios remotos"
- "Utilice la interfaz de usuario de Astra Control para gestionar grupos y usuarios remotos"
- "Utilice la interfaz de usuario de Astra Control para gestionar la autenticación remota"

Añadir usuarios

Los propietarios y administradores de cuentas pueden agregar más usuarios a la instalación de Astra Control Center.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. Seleccione **Agregar usuario**.
4. Introduzca el nombre del usuario, la dirección de correo electrónico y una contraseña temporal.

   El usuario deberá cambiar la contraseña en el primer inicio de sesión.

5. Seleccione una función de usuario con los permisos de sistema adecuados.

   Cada rol proporciona los siguientes permisos:

   - Un **Visor** puede ver los recursos.
   - Un **Miembro** tiene permisos de función de Viewer y puede administrar aplicaciones y clústeres, anular la administración de aplicaciones y eliminar instantáneas y copias de seguridad.
   - Un **Admin** tiene permisos de rol de miembro y puede agregar y quitar cualquier otro usuario excepto el propietario.
   - **Owner** tiene permisos de función de administrador y puede agregar y eliminar cualquier cuenta de usuario.
6. Para agregar restricciones a un usuario con un rol de miembro o de visor, active la casilla de verificación

restringir la función a restricciones .

Para obtener más información sobre cómo agregar restricciones, consulte "Gestione usuarios locales y roles".

7. Seleccione **Agregar**.

Gestionar contraseñas

Puede gestionar las contraseñas de las cuentas de usuario en Astra Control Center.

Cambie la contraseña

Puede cambiar la contraseña de su cuenta de usuario en cualquier momento.

Pasos

1. Seleccione el icono Usuario situado en la parte superior derecha de la pantalla.
2. Seleccione **Perfil**.
3. En el menú Opciones de la columna **acciones** y seleccione **Cambiar contraseña**.
4. Introduzca una contraseña que se ajuste a los requisitos de contraseña.
5. Introduzca una vez más la contraseña para confirmarla.
6. Seleccione **Cambiar contraseña**.

Restablecer la contraseña de otro usuario

Si su cuenta tiene permisos de rol de administrador o propietario, puede restablecer las contraseñas de otras cuentas de usuario así como las suyas propias. Al restablecer una contraseña, asigna una contraseña temporal que el usuario tendrá que cambiar al iniciar sesión.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la lista desplegable **acciones**.
3. Seleccione **Restablecer contraseña**.
4. Introduzca una contraseña temporal que cumpla los requisitos de contraseña.
5. Introduzca una vez más la contraseña para confirmarla.

   La próxima vez que el usuario inicie sesión, se le pedirá que cambie la contraseña.

6. Seleccione **Restablecer contraseña**.

Quitar usuarios

Los usuarios con el rol propietario o administrador pueden eliminar otros usuarios de la cuenta en cualquier momento.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. En la ficha **usuarios** , active la casilla de verificación en la fila de cada usuario que desee quitar.

3. En el menú Opciones de la columna **acciones**, seleccione **Eliminar usuario/s**.
4. Cuando se le solicite, confirme la eliminación escribiendo la palabra "eliminar" y, a continuación, seleccione **Sí, Eliminar usuario**.

Resultado

Astra Control Center elimina al usuario de la cuenta.

Gestionar roles

Es posible gestionar roles si se añaden restricciones de espacio de nombres y se restringen los roles del usuario a dichas restricciones. Esto le permite controlar el acceso a los recursos de su organización. Puede utilizar la interfaz de usuario de Astra Control o. "La API de control Astra" para administrar roles.

Agregar una restricción de espacio de nombres a una función

Un usuario Administrador o propietario puede agregar restricciones de espacio de nombres a las funciones de miembro o de visor.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. En la columna **acciones**, seleccione el botón de menú para un usuario con la función Miembro o Visor.
4. Seleccione **Editar rol**.
5. Active la casilla de verificación **restringir rol a restricciones**.

   La casilla de verificación sólo está disponible para funciones de miembro o de visor. Puede seleccionar un rol diferente de la lista desplegable **rol**.

6. Seleccione **Agregar restricción**.

   Se puede ver la lista de restricciones disponibles por espacio de nombres o por etiqueta de espacio de nombres.

7. En la lista desplegable **Tipo de restricción**, seleccione **espacio de nombres Kubernetes** o **etiqueta de espacio de nombres Kubernetes** dependiendo de cómo estén configurados los espacios de nombres.
8. Seleccione uno o más espacios de nombres o etiquetas de la lista para redactar una restricción que restrinja las funciones a esos espacios de nombres.
9. Seleccione **Confirmar**.

   La página **Editar función** muestra la lista de restricciones que ha elegido para esta función.

10. Seleccione **Confirmar**.

    En la página **cuenta**, puede ver las restricciones de cualquier rol de miembro o de visor en la columna **rol**.

> Si habilita restricciones para una función y selecciona **Confirmar** sin agregar restricciones, se considera que la función tiene restricciones completas (se deniega el acceso a cualquier recurso asignado a espacios de nombres).

Quitar una restricción de espacio de nombres de una función

Un usuario Admin o Owner puede eliminar una restricción de espacio de nombres de una función.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. En la columna **acciones**, seleccione el botón de menú para un usuario con la función Miembro o Visor que tiene restricciones activas.
4. Seleccione **Editar rol**.

   El cuadro de diálogo **Editar función** muestra las restricciones activas para la función.

5. Seleccione **X** a la derecha de la restricción que debe eliminar.
6. Seleccione **Confirmar**.

Si quiere más información

- "Roles de usuario y espacios de nombres"

Administrar la autenticación remota

LDAP es un protocolo estándar del sector para acceder a información de directorio distribuida y una opción muy popular para la autenticación empresarial. Puede conectar Astra Control Center a un servidor LDAP para realizar la autenticación de los usuarios seleccionados de Astra Control.

En un nivel elevado, la configuración implica integrar Astra con LDAP y definir los usuarios y grupos de Astra Control correspondientes a las definiciones LDAP. Puede utilizar la API Astra Control o la interfaz de usuario web para configurar la autenticación LDAP y los usuarios y grupos LDAP.

> Astra Control Center utiliza la dirección de correo electrónico en el atributo "mail" LDAP para buscar y realizar un seguimiento de los usuarios remotos. Este atributo puede ser un campo opcional o vacío en su directorio. Debe existir una dirección de correo electrónico en este campo para los usuarios remotos que desee que aparezcan en Astra Control Center. Esta dirección de correo electrónico se utiliza como nombre de usuario en Astra Control Center para la autenticación.

Añada un certificado para la autenticación LDAPS

Agregue el certificado TLS privado del servidor LDAP para que Astra Control Center pueda autenticarse con el servidor LDAP cuando utilice una conexión LDAPS. Sólo tiene que hacerlo una vez o cuando caduque el certificado que ha instalado.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **certificados**.
3. Seleccione **Agregar**.

4. Cargue el `.pem` archiva o pega el contenido del archivo desde el portapapeles.
5. Seleccione la casilla de verificación **Trusted**.
6. Seleccione **Agregar certificado**.

Habilite la autenticación remota

Puede habilitar la autenticación LDAP y configurar la conexión entre Astra Control y el servidor LDAP remoto.

Antes de empezar

Si planea utilizar LDAPS, asegúrese de que el certificado TLS privado del servidor LDAP está instalado en Astra Control Center para que Astra Control Center pueda autenticarse con el servidor LDAP. Consulte Añada un certificado para la autenticación LDAPS si desea obtener instrucciones.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **conectar**.
4. Introduzca la dirección IP del servidor, el puerto y el protocolo de conexión preferido (LDAP o LDAPS).

> Como práctica recomendada, use LDAPS al conectarse con el servidor LDAP. Debe instalar el certificado TLS privado del servidor LDAP en Astra Control Center antes de conectarse con LDAPS.

5. Introduzca las credenciales de la cuenta de servicio en formato de correo electrónico (administrator@example.com). Astra Control utilizará estas credenciales al conectar con el servidor LDAP.
6. En la sección **coincidencia de usuario**, introduzca el DN base y un filtro de búsqueda de usuario apropiado que se utilizará al recuperar información de usuario del servidor LDAP.
7. En la sección **coincidencia de grupo**, introduzca el DN base de búsqueda de grupo y un filtro de búsqueda de grupo personalizado adecuado.

> Asegúrese de utilizar el nombre completo (DN) de base correcto y un filtro de búsqueda apropiado para **coincidencia de usuario** y **coincidencia de grupo**. El DN base indica a Astra Control en qué nivel del árbol de directorios iniciar la búsqueda, y el filtro de búsqueda limita las partes del árbol de directorios de las búsquedas de Astra Control.

8. Seleccione **Enviar**.

Resultado

El estado del panel **autenticación remota** pasa a **pendiente** y a **conectado** cuando se establece la conexión con el servidor LDAP.

Desactivar la autenticación remota

Puede deshabilitar temporalmente una conexión activa con el servidor LDAP.

> Cuando se deshabilita una conexión a un servidor LDAP, se guardan todas las opciones y se conservan todos los usuarios y grupos remotos que se agregaron a Astra Control desde ese servidor LDAP. Puede volver a conectarse a este servidor LDAP en cualquier momento.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **Desactivar**.

Resultado

El estado del panel **autenticación remota** pasa a **Desactivada**. Se conservan todos los ajustes de autenticación remota, usuarios remotos y grupos remotos, y se puede volver a habilitar la conexión en cualquier momento.

Edite la configuración de autenticación remota

Si ha desactivado la conexión al servidor LDAP o el panel **autenticación remota** se encuentra en el estado "error de conexión", puede editar los valores de configuración.

> No puede editar la dirección IP o la dirección URL del servidor LDAP cuando el panel **autenticación remota** está en estado "Desactivada". Necesita hacerlo Desconecte la autenticación remota primero.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **Editar**.
4. Realice los cambios necesarios y seleccione **Editar**.

Desconecte la autenticación remota

Puede desconectarse de un servidor LDAP y eliminar los ajustes de configuración de Astra Control.

> Cuando se desconecta del servidor LDAP, todas las opciones de configuración de ese servidor LDAP se eliminan de Astra Control, así como todos los usuarios y grupos remotos que se hayan agregado de ese servidor LDAP.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **desconectar**.

Resultado

El estado del panel **autenticación remota** pasa a **desconectado**. La configuración de autenticación remota, los usuarios remotos y los grupos remotos se eliminan de Astra Control.

Administrar grupos y usuarios remotos

Si ha activado la autenticación LDAP en el sistema Astra Control, puede buscar usuarios y grupos LDAP e incluirlos en los usuarios aprobados del sistema.

Agregar un usuario remoto

Los propietarios y administradores de cuentas pueden agregar usuarios remotos a Astra Control.

> No puede agregar un usuario remoto si ya existe en el sistema un usuario local con la misma dirección de correo electrónico. Para agregar el usuario como usuario remoto, elimine primero el usuario local del sistema.

> Astra Control Center utiliza la dirección de correo electrónico en el atributo "mail" LDAP para buscar y realizar un seguimiento de los usuarios remotos. Este atributo puede ser un campo opcional o vacío en su directorio. Debe existir una dirección de correo electrónico en este campo para los usuarios remotos que desee que aparezcan en Astra Control Center. Esta dirección de correo electrónico se utiliza como nombre de usuario en Astra Control Center para la autenticación.

Pasos

1. Vaya al área **cuenta**.
2. Seleccione la ficha **usuarios y grupos**.
3. En el extremo derecho de la página, seleccione **usuarios remotos**.
4. Seleccione **Agregar**.
5. Opcionalmente, busque un usuario LDAP introduciendo la dirección de correo electrónico del usuario en el campo **Filtrar por correo electrónico**.
6. Seleccione uno o varios usuarios de la lista.
7. Asigne un rol al usuario.

   > Si asigna roles diferentes a un usuario y al grupo del usuario, tiene prioridad el rol más permisivo.

8. Opcionalmente, asigne una o más restricciones de espacio de nombres a este usuario y seleccione **restringir rol a restricciones** para aplicarlas. Puede agregar una nueva restricción de espacio de nombres seleccionando **Agregar restricción**.

   > Cuando a un usuario se le asignan varias funciones a través de la pertenencia a grupos LDAP, las restricciones de la función más permisiva son las únicas que surtan efecto. Por ejemplo, si un usuario con una función de visor local se une a tres grupos que están enlazados a la función Member, la suma de las restricciones de las funciones Member se aplicará y se ignoran todas las restricciones de la función Viewer.

9. Seleccione **Agregar**.

Resultado

El nuevo usuario aparece en la lista de usuarios remotos. En esta lista, puede ver restricciones activas en el usuario, así como administrar el usuario desde el menú **acciones**.

Agregar un grupo remoto

Para agregar muchos usuarios remotos a la vez, los propietarios de cuentas y los administradores pueden agregar grupos remotos a Astra Control. Cuando agrega un grupo remoto, todos los usuarios remotos de ese grupo se agregan a Astra Control y heredan la misma función.

Pasos

1. Vaya al área **cuenta**.
2. Seleccione la ficha **usuarios y grupos**.
3. En el extremo derecho de la página, seleccione **grupos remotos**.
4. Seleccione **Agregar**.

   En esta ventana, puede ver una lista de los nombres comunes y nombres distintivos de los grupos LDAP que Astra Control ha recuperado del directorio.

5. Opcionalmente, busque un grupo LDAP introduciendo el nombre común del grupo en el campo **filtro por nombre común**.
6. Seleccione uno o varios grupos de la lista.
7. Asigne un rol a los grupos.

   El rol que seleccione se asigna a todos los usuarios de este grupo. Si asigna roles diferentes a un usuario y al grupo del usuario, tiene prioridad el rol más permisivo.

8. Opcionalmente, asigne una o más restricciones de espacio de nombres a este grupo y seleccione **restringir rol a restricciones** para aplicarlas. Puede agregar una nueva restricción de espacio de nombres seleccionando **Agregar restricción**.

   Cuando a un usuario se le asignan varias funciones a través de la pertenencia a grupos LDAP, las restricciones de la función más permisiva son las únicas que surtan efecto. Por ejemplo, si un usuario con una función de visor local se une a tres grupos que están enlazados a la función Member, la suma de las restricciones de las funciones Member se aplicará y se ignoran todas las restricciones de la función Viewer.

9. Seleccione **Agregar**.

Resultado

El nuevo grupo aparece en la lista de grupos remotos y todos los usuarios remotos de este grupo aparecen en la lista de usuarios remotos. En esta lista, puede ver detalles sobre el grupo, así como administrar el grupo desde el menú **acciones**.

Ver y gestionar notificaciones

Astra le notifica cuando las acciones se han completado o han fallado. Por ejemplo, verá una notificación si una copia de seguridad de una aplicación se ha completado correctamente.

Puede gestionar estas notificaciones desde la parte superior derecha de la interfaz:

Pasos

1. Seleccione el número de notificaciones sin leer en la parte superior derecha.

2. Revise las notificaciones y seleccione **Marcar como leído** o **Mostrar todas las notificaciones**.

   Si ha seleccionado **Mostrar todas las notificaciones**, se cargará la página Notificaciones.

3. En la página **Notificaciones**, vea las notificaciones, seleccione las que desea marcar como leídas, seleccione **Acción** y seleccione **Marcar como leído**.

Añada y elimine credenciales

Añada y elimine credenciales de proveedores de cloud privado local como ONTAP S3, clústeres de Kubernetes gestionados con OpenShift o clústeres de Kubernetes no gestionados de su cuenta en cualquier momento. Astra Control Center utiliza estas credenciales para descubrir los clústeres y las aplicaciones de Kubernetes en los clústeres, y para aprovisionar recursos en su nombre.

Tenga en cuenta que todos los usuarios de Astra Control Center comparten los mismos conjuntos de credenciales.

Añada credenciales

Puede agregar credenciales a Astra Control Center cuando gestiona los clústeres. Para añadir credenciales al añadir un clúster nuevo, consulte "Añada un clúster de Kubernetes".

> Si crea el suyo propio `kubeconfig` file, debe definir sólo un elemento de contexto **uno** en él. Consulte "Documentación de Kubernetes" para obtener información acerca de cómo crear `kubeconfig` archivos.

Quite las credenciales

Eliminar credenciales de una cuenta en cualquier momento. Solo debe quitar credenciales después de "desgestione todos los clústeres asociados".

> El primer conjunto de credenciales que agregue a Astra Control Center está siempre en uso porque Astra Control Center utiliza las credenciales para autenticarse en el bloque de copia de seguridad. Lo mejor es no eliminar estas credenciales.

Pasos

1. Seleccione **cuenta**.
2. Seleccione la ficha **credenciales**.
3. Seleccione el menú Opciones de la columna **Estado** para obtener las credenciales que desea quitar.
4. Seleccione **Quitar**.
5. Escriba la palabra "quitar" para confirmar la eliminación y, a continuación, seleccione **Sí, Eliminar credenciales**.

Resultado

Astra Control Center elimina las credenciales de la cuenta.

Controlar la actividad de la cuenta

Puede ver los detalles de las actividades en su cuenta de Astra Control. Por ejemplo, cuando se invitó a nuevos usuarios, cuando se agregaba un clúster o cuando se tomaba una snapshot. También puede exportar la actividad de su cuenta a un archivo CSV.

Si gestiona los clústeres de Kubernetes desde Astra Control y Astra Control se conecta a Cloud Insights, Astra Control envía registros de eventos a Cloud Insights. La información de registro, incluida la información sobre la implementación de POD y los archivos adjuntos de PVC, aparece en el registro de actividad de control de Astra. Utilice esta información para identificar cualquier problema en los clústeres de Kubernetes que está gestionando.

Ver toda la actividad de la cuenta en Astra Control

1. Seleccione **actividad**.
2. Utilice los filtros para restringir la lista de actividades o utilice el cuadro de búsqueda para encontrar exactamente lo que busca.
3. Seleccione **Exportar a CSV** para descargar la actividad de su cuenta en un archivo CSV.

Ver la actividad de la cuenta de una aplicación específica

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **actividad**.

Ver la actividad de la cuenta de los clústeres

1. Seleccione **Clusters** y, a continuación, seleccione el nombre del clúster.
2. Seleccione **actividad**.

Tome la acción para resolver eventos que requieren atención

1. Seleccione **actividad**.
2. Seleccione un evento que requiera atención.
3. Seleccione la opción desplegable **tomar acción**.

   En esta lista, puede ver las posibles acciones correctivas que puede adoptar, ver la documentación relacionada con el problema y obtener soporte para ayudar a resolver el problema.

Actualizar una licencia existente

Puede convertir una licencia de evaluación a una licencia completa, o puede actualizar una evaluación existente o una licencia completa con una nueva licencia. Si no tiene una licencia completa, trabaje con su contacto de ventas de NetApp para obtener un número de serie y una licencia completa. Puede utilizar la interfaz de usuario de Astra Control Center o "La API de control Astra" para actualizar una licencia existente.

Pasos

1. Inicie sesión en la "Sitio de soporte de NetApp".
2. Acceda a la página de descarga de Astra Control Center, introduzca el número de serie y descargue el archivo de licencia completo de NetApp (NLF).

3. Inicie sesión en la interfaz de usuario de Astra Control Center.
4. En la navegación de la izquierda, seleccione **cuenta** > **Licencia**.
5. En la página **cuenta** > **Licencia**, seleccione el menú desplegable de estado de la licencia existente y seleccione **Reemplazar**.
6. Busque el archivo de licencia que descargó.
7. Seleccione **Agregar**.

La página **cuenta** > **licencias** muestra la información de la licencia, la fecha de caducidad, el número de serie de la licencia, el ID de cuenta y las unidades de CPU utilizadas.

Si quiere más información

- "Licencias de Astra Control Center"

Información de copyright

Información de la marca comercial