Administración de un sistema StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

Administración de un sistema StorageGRID

Siga estas instrucciones para configurar y administrar un sistema StorageGRID.

Estas instrucciones describen cómo usar Grid Manager para configurar grupos y usuarios, crear cuentas de inquilino para permitir que las aplicaciones de cliente S3 y Swift almacenen y recuperen objetos, configurar y gestionar redes StorageGRID, configurar AutoSupport, gestionar los ajustes de nodo, etc.

Se han movido las instrucciones de gestión de objetos con reglas y políticas de gestión de ciclo de vida de la información (ILM) a."Gestión de objetos con ILM".

Estas instrucciones están dirigidas al personal técnico que configurará, administre y prestará soporte técnico para un sistema StorageGRID después de que se haya instalado.

Lo que necesitará

- Tiene una visión general del sistema StorageGRID.
- Tiene un conocimiento muy detallado de los shell de comandos de Linux, las conexiones de red y la instalación y configuración del hardware de servidor.

Requisitos del navegador web

Debe utilizar un navegador web compatible.

Navegador Web	Versión mínima admitida
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Debe establecer la ventana del navegador en un ancho recomendado.

Ancho del navegador	Píxeles
Mínimo	1024
Óptimo	1280

Iniciando sesión en Grid Manager

Para acceder a la página de inicio de sesión de Grid Manager, introduzca el nombre de dominio completo (FQDN) o la dirección IP de un nodo de administración en la barra de direcciones de un explorador web compatible.

Lo que necesitará

- Debe tener sus credenciales de inicio de sesión.

- Debe tener la dirección URL de Grid Manager.
- Debe utilizar un navegador web compatible.
- Las cookies deben estar habilitadas en su navegador web.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

Cada sistema StorageGRID incluye un nodo de administrador primario y cualquier número de nodos de administrador que no son primarios. Puede iniciar sesión en Grid Manager en cualquier nodo de administrador para gestionar el sistema StorageGRID. Sin embargo, los nodos del administrador no son exactamente los mismos:

- Las confirmaciones de alarma (sistema heredado) realizadas en un nodo de administración no se copian en otros nodos de administración. Por este motivo, es posible que la información mostrada para las alarmas no tenga el mismo aspecto en cada nodo de administración.
- Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

Si se incluyen nodos de administración en un grupo de alta disponibilidad (ha), puede conectarse mediante la dirección IP virtual del grupo de alta disponibilidad o un nombre de dominio completo que asigne la dirección IP virtual. El nodo de administración principal se debe seleccionar como principal preferido del grupo, de manera que al acceder al Administrador de grid, tenga acceso al nodo de administración principal a menos que el nodo de administración principal no esté disponible.

Pasos

1. Inicie un explorador web compatible.
2. En la barra de direcciones del navegador, introduzca la dirección URL de Grid Manager:

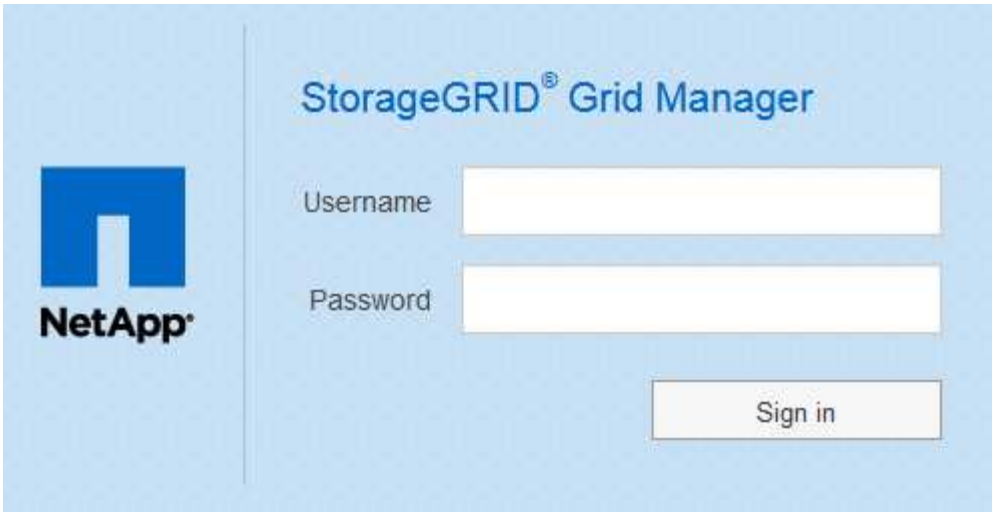
   `https://FQDN_or_Admin_Node_IP/`

   donde *`FQDN_or_Admin_Node_IP`* Es un nombre de dominio completo o la dirección IP de un nodo de administrador o la dirección IP virtual de un grupo ha de nodos de administrador.

   Si debe acceder a Grid Manager en un puerto distinto del puerto estándar para HTTPS (443), introduzca lo siguiente, donde *`FQDN_or_Admin_Node_IP`* Es un nombre de dominio completo o una dirección IP y el puerto es el número de puerto:

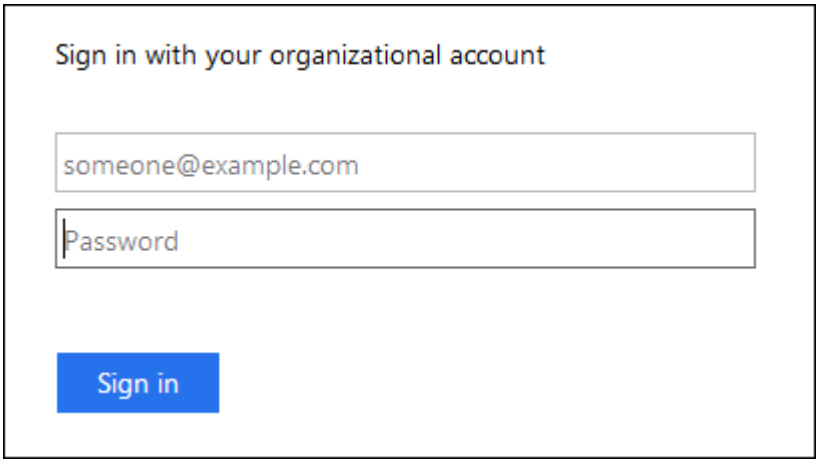
   `https://FQDN_or_Admin_Node_IP:port/`

3. Si se le solicita una alerta de seguridad, instale el certificado con el asistente de instalación del explorador.
4. Inicie sesión en Grid Manager:
   - Si su sistema StorageGRID no utiliza el inicio de sesión único (SSO):
     i. Introduzca su nombre de usuario y contraseña para el administrador de grid.
     ii. Haga clic en **Iniciar sesión**.



- Si SSO está habilitado para el sistema StorageGRID y esta es la primera vez que accede a la URL en este navegador:
  i. Haga clic en **Iniciar sesión**. Puede dejar el campo ID de cuenta en blanco.

  ii. Introduzca sus credenciales de SSO estándar en la página de inicio de sesión con SSO de su organización. Por ejemplo:

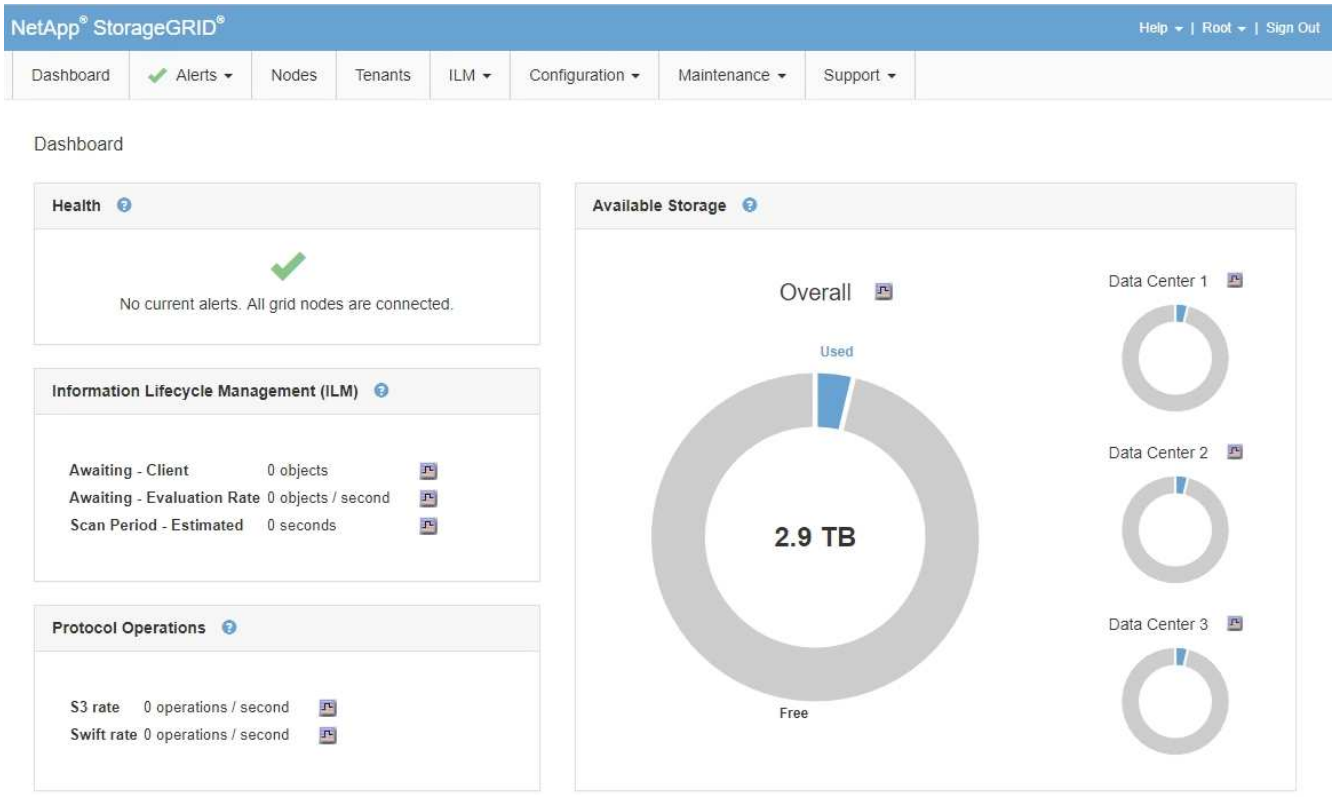


- Si SSO está habilitado para el sistema StorageGRID y ya ha accedido previamente a Grid Manager o a una cuenta de inquilino:

i. Realice una de las siguientes acciones:

- Introduzca **0** (el ID de cuenta de Grid Manager) y haga clic en **Iniciar sesión**.
- Seleccione **Grid Manager** si aparece en la lista de cuentas recientes y haga clic en **Iniciar sesión**.

ii. Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización. Cuando haya iniciado sesión, aparecerá la página de inicio de Grid Manager, que incluye el Panel. Para saber qué información se proporciona, consulte «'visualización del panel» en las instrucciones de supervisión y solución de problemas de StorageGRID.



5. Si desea iniciar sesión en otro nodo de administración:

Opción	Pasos
SSO no está habilitado	a. En la barra de direcciones del navegador, introduzca el nombre de dominio completo o la dirección IP del otro nodo de administración. Incluya el número de puerto según sea necesario. b. Introduzca su nombre de usuario y contraseña para el administrador de grid. c. Haga clic en **Iniciar sesión**.
SSO habilitado	En la barra de direcciones del navegador, introduzca el nombre de dominio completo o la dirección IP del otro nodo de administración. Si inició sesión en un nodo de administrador, puede acceder a otros nodos de administrador sin tener que volver a iniciar sesión. Sin embargo, si su sesión SSO caduca, se le solicitará de nuevo sus credenciales. **Nota:** SSO no está disponible en el puerto restringido de Grid Manager. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único.

Información relacionada

"Requisitos del navegador web"

"Controlar el acceso mediante firewalls"

"Configuración de certificados de servidor"

"Configuración del inicio de sesión único"

"Gestión de los grupos de administración"

"Gestionar grupos de alta disponibilidad"

"Usar una cuenta de inquilino"

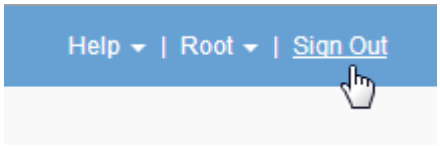
"Solución de problemas de monitor"

Cierre la sesión en Grid Manager

Cuando haya terminado de trabajar con Grid Manager, deberá cerrar sesión para asegurarse de que los usuarios no autorizados no puedan acceder al sistema StorageGRID. Es posible que cerrar el navegador no le cierre la sesión del sistema según la configuración de cookies del navegador.

Pasos

1. Busque el enlace **Cerrar sesión** en la esquina superior derecha de la interfaz de usuario.



2. Haga clic en **Cerrar sesión**.

Opción	Descripción
SSO no en uso	Ha cerrado sesión en el nodo de administrador. Se muestra la página de inicio de sesión de Grid Manager. **Nota:** Si ha iniciado sesión en más de un nodo de administración, debe cerrar sesión en cada nodo.
SSO habilitado	Inició sesión en todos los nodos de administrador a los que accedían. Aparece la página de inicio de sesión de StorageGRID. **Grid Manager** aparece como el valor predeterminado en la lista desplegable **Cuentas recientes**, y el campo **ID de cuenta** muestra 0. **Nota:** Si SSO está activado y también ha iniciado sesión en el Administrador de arrendatarios, también debe cerrar sesión en la cuenta de arrendatario para cerrar sesión en SSO.

Información relacionada

"Configuración del inicio de sesión único"

"Usar una cuenta de inquilino"

Cambiando la contraseña

Si es un usuario local de Grid Manager, puede cambiar su propia contraseña.

Lo que necesitará

Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Acerca de esta tarea

Si inicia sesión en StorageGRID como usuario federado o si está activado el inicio de sesión único (SSO), no podrá cambiar la contraseña en Grid Manager. En su lugar, debe cambiar la contraseña en el origen de identidad externo, por ejemplo, Active Directory u OpenLDAP.

Pasos

1. En el encabezado de Grid Manager, seleccione ***su nombre*** **> Cambiar contraseña**.
2. Introduzca su contraseña actual.

3. Escriba una nueva contraseña.

   La contraseña debe contener al menos 8 caracteres y no más de 32. Las contraseñas distinguen mayúsculas de minúsculas.

4. Vuelva a introducir la nueva contraseña.
5. Haga clic en **Guardar**.

Cambiar la clave de acceso de aprovisionamiento

Use este procedimiento para cambiar la clave de acceso de aprovisionamiento de StorageGRID. La frase de acceso es necesaria para los procedimientos de recuperación, expansión y mantenimiento. También se requiere la contraseña para descargar las copias de seguridad del paquete de recuperación que incluyen la información de topología de la cuadrícula y las claves de cifrado del sistema StorageGRID.

Lo que necesitará

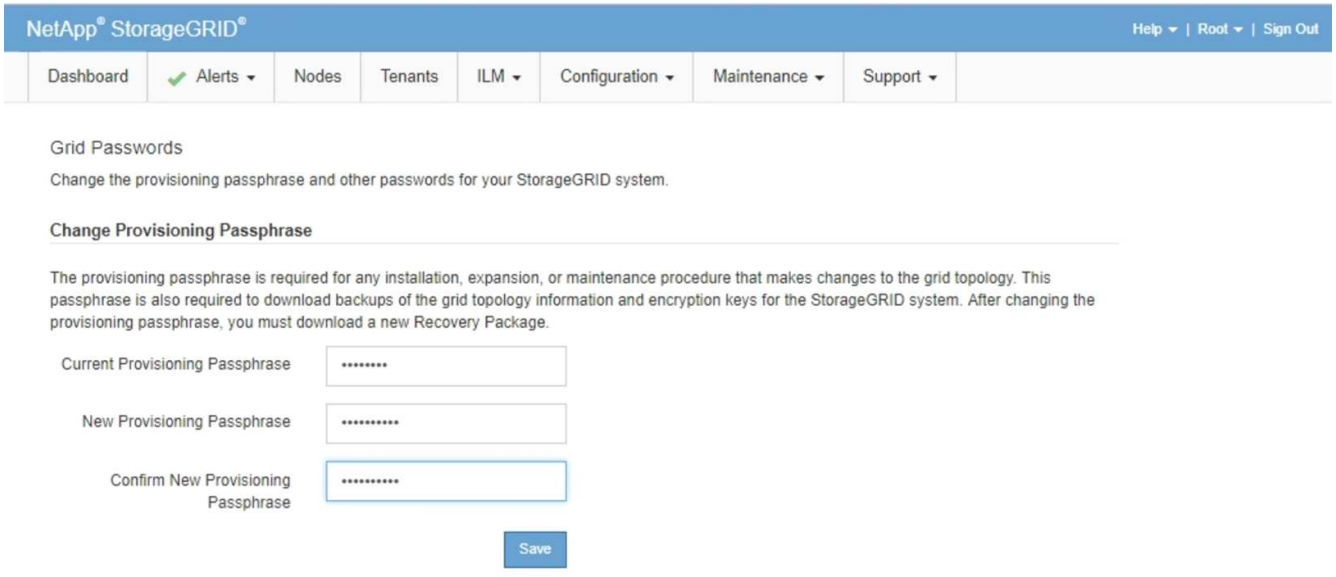
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de mantenimiento o acceso raíz.
- Debe tener la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

La clave de acceso de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento y para descargar el paquete de recuperación. La clave de acceso de aprovisionamiento no aparece en la `Passwords.txt` archivo. Asegúrese de documentar la frase de acceso de aprovisionamiento y mantenerla en una ubicación segura.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **contraseñas de cuadrícula**.



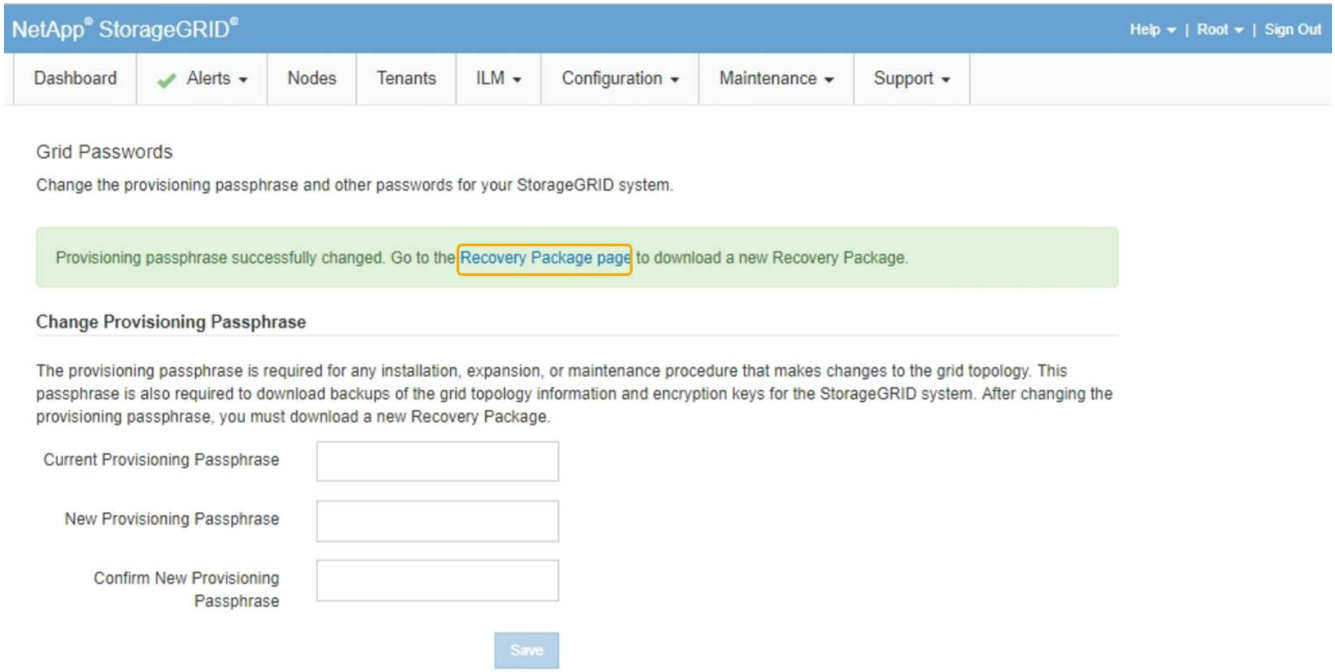
2. Introduzca la clave de acceso de aprovisionamiento actual.

3. Introduzca el nuevo pasepartido.la frase de contraseña debe contener al menos 8 caracteres y no más de 32. Las passphrasas distinguen entre mayúsculas y minúsculas.

> Almacene la nueva clave de acceso de aprovisionamiento en una ubicación segura. Es necesario para los procedimientos de instalación, expansión y mantenimiento.

4. Vuelva a introducir la nueva contraseña y haga clic en **Guardar**.

   El sistema muestra un banner verde de éxito cuando se completa el cambio de la clave de acceso de aprovisionamiento. El cambio debe tardar menos de un minuto.



5. Seleccione el enlace **página del paquete de recuperación** que se encuentra dentro del banner de éxito.
6. Descargue el nuevo paquete de recuperación desde Grid Manager. Seleccione **Mantenimiento** > **paquete de recuperación** e introduzca la nueva contraseña de aprovisionamiento.

> Después de cambiar la contraseña de aprovisionamiento, debe descargar inmediatamente un nuevo paquete de recuperación. El archivo de paquete de recuperación permite restaurar el sistema si se produce un fallo.

Cambiar el tiempo de espera de la sesión del explorador

Puede controlar si los usuarios de Grid Manager y de arrendatario Manager han cerrado la sesión si están inactivos durante más de un cierto período de tiempo.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

El valor predeterminado de tiempo de espera de inactividad de la interfaz gráfica de usuario es 900 segundos

(15 minutos). Si la sesión del explorador de un usuario no está activa durante este período de tiempo, se agota el tiempo de espera de la sesión.

Según sea necesario, puede aumentar o reducir el tiempo de espera mediante la configuración de la opción de visualización tiempo de espera de inactividad de la interfaz gráfica de usuario.

Si se activa el inicio de sesión único (SSO) y se agota el tiempo de espera de la sesión del explorador de un usuario, el sistema se comporta como si el usuario hiciera clic en **Cerrar sesión** manualmente. El usuario debe volver a introducir sus credenciales de SSO para volver a acceder a StorageGRID.

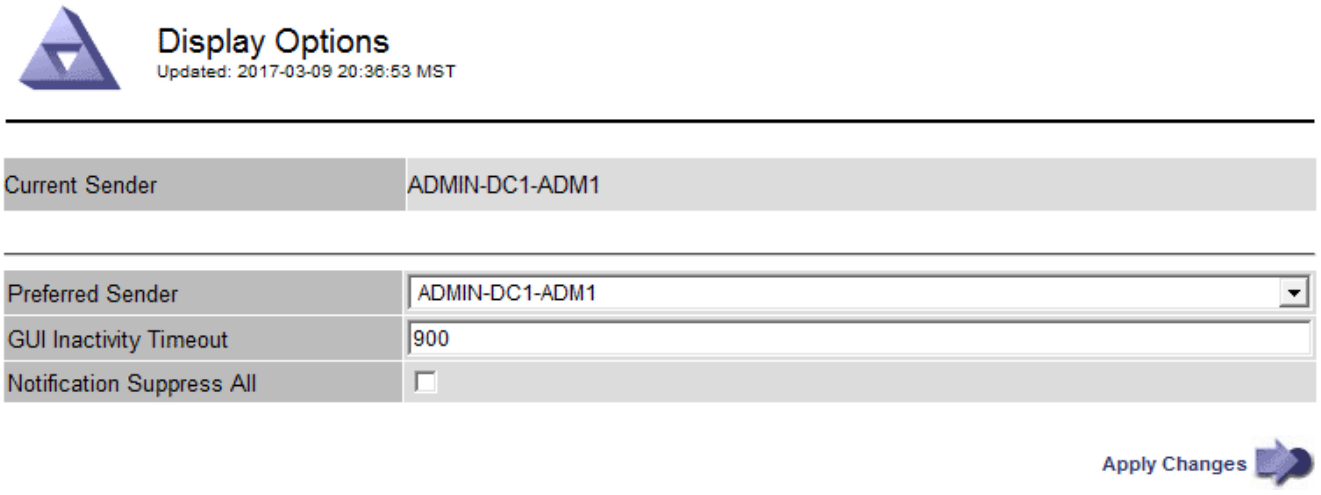
El tiempo de espera de la sesión de usuario también puede controlarse por lo siguiente:

- Temporizador StorageGRID independiente no configurable, que se incluye para la seguridad del sistema. De forma predeterminada, el token de autenticación de cada usuario caduca 16 horas después de que el usuario inicia sesión. Cuando caduca la autenticación de un usuario, ese usuario se cierra automáticamente, incluso si no se ha alcanzado el valor de tiempo de espera de inactividad de la interfaz gráfica de usuario. Para renovar el token, el usuario debe volver a iniciar sesión.
- Se ha agotado el tiempo de espera de la configuración del proveedor de identidades, suponiendo que SSO esté habilitado para StorageGRID.

Pasos

1. Seleccione **Configuración** > **Configuración del sistema** > **Opciones de pantalla**.
2. Para **tiempo de espera de inactividad de la GUI**, introduzca un período de tiempo de espera de 60 segundos o más.

   Configure este campo en 0 si no desea utilizar esta funcionalidad. Los usuarios se firman 16 horas después de iniciar sesión, cuando caducan sus tokens de autenticación.



3. Haga clic en **aplicar cambios**.

   La nueva configuración no afecta a los usuarios que han iniciado sesión actualmente. Los usuarios deben iniciar sesión de nuevo o actualizar sus exploradores para que la nueva configuración de tiempo de espera tenga efecto.

Información relacionada

"Cómo funciona el inicio de sesión único"

"Usar una cuenta de inquilino"

Ver información de licencias de StorageGRID

Puede ver la información de licencia del sistema StorageGRID, como la capacidad de almacenamiento máxima de su grid, cuando sea necesario.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Acerca de esta tarea

Si se produce un problema con la licencia de software para este sistema StorageGRID, el panel Estado del Panel incluye un icono de estado de licencia y un enlace **Licencia**. El número indica cuántos problemas relacionados con la licencia existen.

Paso

Para ver la licencia, realice una de las siguientes acciones:

- En el panel Estado del Panel, haga clic en el icono Estado de la licencia o en el enlace **Licencia**. Este vínculo sólo aparece si hay un problema con la licencia.
- Seleccione **Mantenimiento** > **sistema** > **Licencia**.

Aparece la página Licencia y proporciona la siguiente información de sólo lectura acerca de la licencia actual:

- ID del sistema de StorageGRID, que es el número de identificación exclusivo para esta instalación de StorageGRID
- Número de serie de la licencia
- Capacidad de almacenamiento bajo licencia del grid
- Fecha de finalización de la licencia del software
- Fecha de finalización del contrato de servicio de soporte
- Contenido del archivo de texto de licencia

Para las licencias emitidas antes de StorageGRID 10.3, la capacidad de almacenamiento con licencia no está incluida en el archivo de licencia y se muestra un mensaje "Ver acuerdo de licencia" en lugar de un valor.

Actualizar la información de licencia de StorageGRID

Debe actualizar la información de licencia del sistema de StorageGRID en cualquier momento que cambien las condiciones de su licencia. Por ejemplo, debe actualizar la información de la licencia si adquiere capacidad de almacenamiento adicional para su grid.

Lo que necesitará

- Debe tener un nuevo archivo de licencia para aplicar al sistema StorageGRID.
- Debe tener permisos de acceso específicos.
- Debe tener la clave de acceso de aprovisionamiento.

Pasos

1. Seleccione **Mantenimiento** > **sistema** > **Licencia**.
2. Introduzca la frase de acceso de aprovisionamiento del sistema StorageGRID en el cuadro de texto **frase de paso** de aprovisionamiento.
3. Haga clic en **examinar**.
4. En el cuadro de diálogo Abrir, busque y seleccione el nuevo archivo de licencia (`.txt`) Y haga clic en **Abrir**.

   El nuevo archivo de licencia se valida y muestra.

5. Haga clic en **Guardar**.

Uso de la API de gestión de grid

Puede realizar tareas de administración del sistema mediante la API REST de Grid Management en lugar de la interfaz de usuario de Grid Manager. Por ejemplo, se recomienda utilizar la API para automatizar operaciones o crear varias entidades, como los usuarios, más rápidamente.

La API de gestión de grid utiliza la plataforma API de código abierto de Swagger. Swagger proporciona una interfaz de usuario intuitiva que permite a los desarrolladores y no desarrolladores realizar operaciones en tiempo real en StorageGRID con la API.

Recursos de alto nivel

La API de gestión de grid proporciona los siguientes recursos de nivel superior:

- `/grid`: Access está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados.
- `/org`: Access está restringido a los usuarios que pertenecen a un grupo LDAP local o federado para una cuenta de inquilino. Para obtener detalles, consulte la información acerca del uso de cuentas de inquilino.

- `/private`: Access está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados. Estas API están pensadas para el uso interno únicamente y no se documentan públicamente. Estas API también están sujetas a cambios sin previo aviso.

Información relacionada

"Usar una cuenta de inquilino"

"Prometheus: Aspectos básicos de las consultas"

Operaciones de API de gestión de grid

La API de gestión de grid organiza las operaciones de API disponibles en las siguientes secciones.

- **Cuentas** — Operaciones para administrar cuentas de arrendatarios de almacenamiento, incluyendo la creación de cuentas nuevas y la recuperación del uso del almacenamiento para una cuenta determinada.
- **Alarms** — Operaciones para enumerar las alarmas actuales (sistema heredado), y devolver información sobre el estado de la cuadrícula, incluyendo las alertas actuales y un resumen de los estados de conexión de los nodos.
- **Historial de alertas** — Operaciones en alertas resueltas.
- **ALERT-receptores** — Operaciones en receptores de notificación de alertas (correo electrónico).
- **Reglas de alerta** — Operaciones en reglas de alerta.
- **Silencios de alerta** — Operaciones en silencios de alerta.
- **Alertas** — Operaciones en alertas.
- **Audit** — Operaciones para enumerar y actualizar la configuración de auditoría.
- **Auth** — Operaciones para realizar la autenticación de sesión de usuario.

  La API de administración de grid admite el esquema de autenticación de token de Bearer. Para iniciar sesión, debe proporcionar un nombre de usuario y una contraseña en el cuerpo JSON de la solicitud de autenticación (es decir, `POST /api/v3/authorize`). Si el usuario se autentica correctamente, se devuelve un token de seguridad. Este token se debe proporcionar en el encabezado de las siguientes solicitudes de API ("autorización: Portador *token*").

  > Si el inicio de sesión único está habilitado para el sistema StorageGRID, debe realizar pasos diferentes para la autenticación. Consulte «"autenticación en la API si está activado el inicio de sesión único"."

  Consulte «"Protección contra la falsificación de solicitudes entre sitios"» para obtener información sobre la mejora de la seguridad de la autenticación.

- **Certificados cliente** — Operaciones para configurar certificados de cliente de modo que se pueda acceder a StorageGRID de forma segura utilizando herramientas de supervisión externas.
- **Config** — Operaciones relacionadas con la versión del producto y las versiones de la API de gestión de grid. Es posible mostrar la versión del producto y las versiones principales de la API de Grid Management compatibles con esta versión, así como deshabilitar las versiones obsoletas de la API.
- **Características desactivadas** — Operaciones para ver las funciones que podrían haberse desactivado.
- **servidores dns** — Operaciones para enumerar y cambiar los servidores DNS externos configurados.

- **Nombres-dominio-terminal** — Operaciones para enumerar y cambiar los nombres de dominio de punto final.
- **Codificación de borrado** — Operaciones en perfiles de codificación de borrado.
- **Expansión** — Operaciones de expansión (nivel de procedimiento).
- **Nodos de expansión** — Operaciones en expansión (a nivel de nodo).
- **Expansion-sites** — Operaciones en expansión (a nivel de sitio).
- **Grid-Networks** — Operaciones para enumerar y cambiar la Lista de redes Grid.
- **Grid-password** — Operaciones para la gestión de contraseñas de grid.
- **Grupos** — Operaciones para administrar grupos de administradores de grid locales y recuperar grupos de administradores de grid federados desde un servidor LDAP externo.
- **Identity-source** — Operaciones para configurar un origen de identidad externo y sincronizar manualmente la información del grupo federado y del usuario.
- **ilm** — Operaciones en la gestión del ciclo de vida de la información (ILM).
- **Licencia** — Operaciones para recuperar y actualizar la licencia de StorageGRID.
- **Logs** — Operaciones para recopilar y descargar archivos de registro.
- **Métricas** — Operaciones en métricas StorageGRID incluyendo consultas métricas instantáneas en un único punto en el tiempo y consultas métricas de rango en un intervalo de tiempo. La API de gestión de grid utiliza la herramienta de supervisión de sistemas Prometheus como origen de datos de back-end. Para obtener información sobre la construcción de consultas Prometheus, consulte el sitio web Prometheus.

> Métricas que incluyen`private` en sus nombres sólo se utilizan de forma interna. Estas métricas están sujetas a cambios entre las versiones de StorageGRID sin previo aviso.

- **Estado del nodo** — Operaciones en el estado del nodo.
- **ntp-Server** — Operaciones para enumerar o actualizar servidores de Protocolo de tiempo de redes (NTP) externos.
- **Objetos** — Operaciones en objetos y metadatos de objetos.
- **Recuperación** — Operaciones para el procedimiento de recuperación.
- **Paquete de recuperación** — Operaciones para descargar el paquete de recuperación.
- **Regiones** — Operaciones para ver y crear regiones.
- **s3-object-lock** — Operaciones en la configuración global de S3 Object Lock.
- **Server-certificate** — Operaciones para ver y actualizar certificados de servidor de Grid Manager.
- **snmp** — Operaciones en la configuración actual de SNMP.
- **Traffic-claes** — Operaciones para directivas de clasificación de tráfico.
- **Red-cliente-no confiable** — Operaciones en la configuración de Red cliente no confiable.
- **Usuarios** — Operaciones para ver y administrar usuarios de Grid Manager.

Emitir solicitudes API

La interfaz de usuario de Swagger proporciona detalles y documentación completos para cada operación de API.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

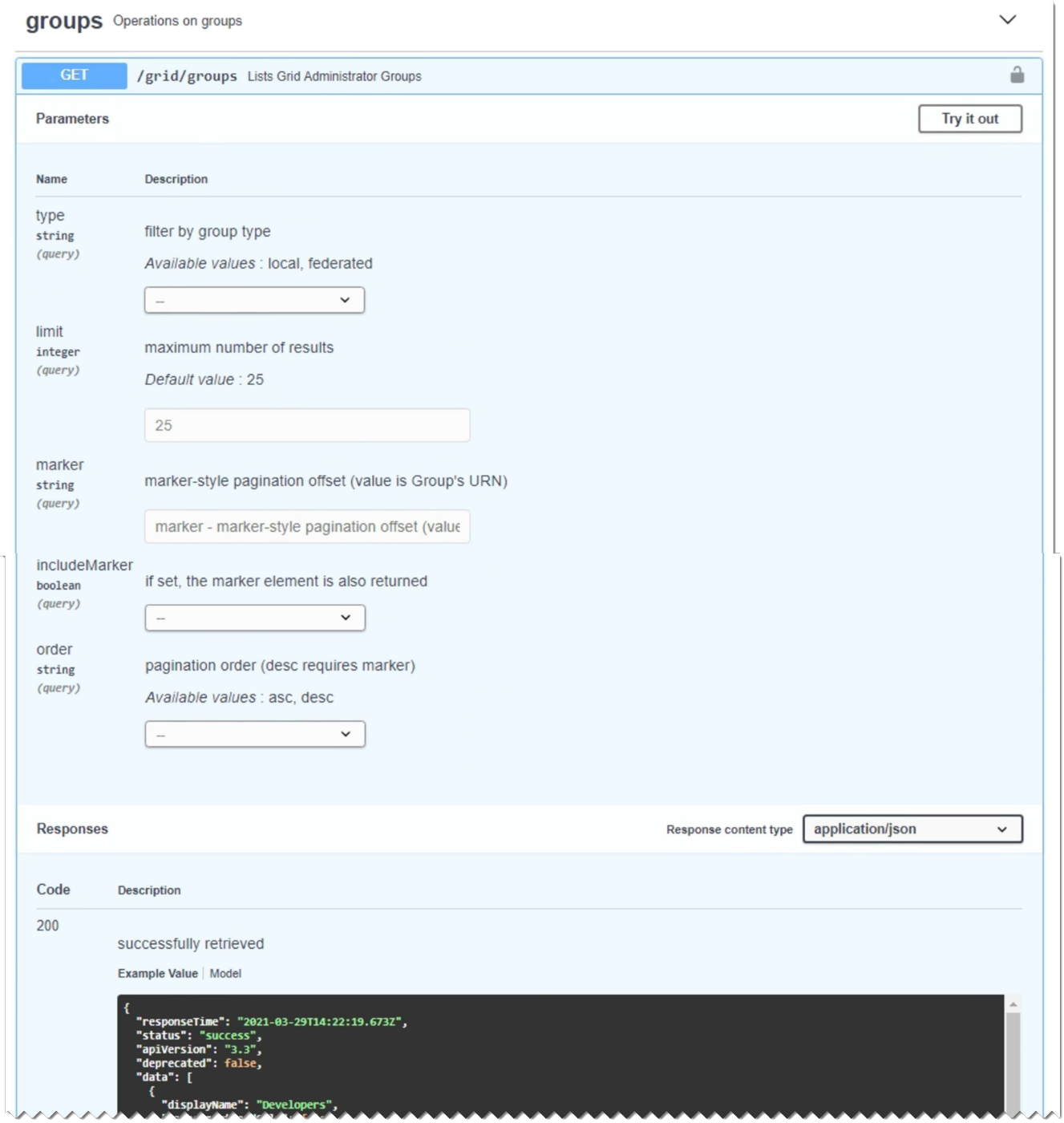
> Cualquier operación de API que realice mediante la página web de documentos de API es una operación en directo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

Pasos

1. Seleccione **Ayuda** > **Documentación de API** en el encabezado de Grid Manager.
2. Seleccione la operación deseada.

   Al expandir una operación de API, puede ver las acciones HTTP disponibles, como GET, PUT, UPDATE y DELETE.

3. Seleccione una acción HTTP para ver los detalles de la solicitud, incluida la dirección URL del extremo, una lista de los parámetros necesarios o opcionales, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.



4. Determine si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. A continuación, obtenga estos valores. Es posible que primero deba emitir una solicitud de API diferente para obtener la información que necesita.
5. Determine si necesita modificar el cuerpo de solicitud de ejemplo. Si es así, puede hacer clic en **Modelo** para conocer los requisitos de cada campo.
6. Haga clic en **probar**.
7. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.
8. Haga clic en **Ejecutar**.
9. Revise el código de respuesta para determinar si la solicitud se ha realizado correctamente.

Creación de versiones de la API de gestión de grid

La API de gestión de grid utiliza versiones para permitir actualizaciones sin interrupciones.

Por ejemplo, esta URL de solicitud especifica la versión 3 de la API.

`https://hostname_or_ip_address/api/v3/authorize`

La versión principal de la API de administración de arrendatarios se bONTAP cuando se realizan cambios que son ***no compatibles*** con versiones anteriores. La versión menor de la API de administración de arrendatarios se bONTAP cuando se hacen cambios que ***are sea compatible*** con versiones anteriores. Los cambios compatibles incluyen la adición de nuevos extremos o nuevas propiedades. En el ejemplo siguiente se muestra cómo la versión de API se bONTAP en función del tipo de cambios realizados.

Tipo de cambio en la API	Versión anterior	Nueva versión
Compatible con versiones anteriores	2.1	2.2
No es compatible con versiones anteriores	2.1	3.0

Al instalar el software StorageGRID por primera vez, sólo se activa la versión más reciente de la API de gestión de grid. Sin embargo, cuando actualice a una versión de función nueva de StorageGRID, seguirá teniendo acceso a la versión de API anterior para al menos una versión de función de StorageGRID.

> Puede utilizar la API de gestión de grid para configurar las versiones compatibles. Consulte la sección «'config'» de la documentación de API de Swagger para obtener más información. Debe desactivar la compatibilidad con la versión anterior después de actualizar todos los clientes de la API de Grid Management para que utilicen la versión más reciente.

Las solicitudes obsoletas se marcan como obsoletas de las siguientes formas:

- El encabezado de la respuesta es "Dedeprecated: True"
- El cuerpo de respuesta JSON incluye "obsoleto": TRUE
- Se agrega una advertencia obsoleta a nms.log. Por ejemplo:

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

Determinar qué versiones de API son compatibles con la versión actual

Utilice la siguiente solicitud de API para devolver una lista de las versiones principales de API admitidas:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Especificar una versión de API para una solicitud

Puede especificar la versión de API mediante un parámetro path (`/api/v3`) o un encabezado (`Api-Version: 3`). Si proporciona ambos valores, el valor de encabezado anula el valor de ruta de acceso.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Protección contra falsificación de solicitudes entre sitios (CSRF)

Puede ayudar a protegerse contra ataques de falsificación de solicitudes entre sitios (CSRF) contra StorageGRID mediante tokens CSRF para mejorar la autenticación que usa cookies. El administrador de grid y el administrador de inquilinos habilitan automáticamente esta característica de seguridad; otros clientes de API pueden elegir si habilitar la función cuando se conectan.

Un atacante que pueda activar una solicitud a un sitio diferente (por ejemplo, con UNA POST de formulario HTTP) puede provocar ciertas solicitudes mediante las cookies del usuario que ha iniciado sesión.

StorageGRID ayuda a proteger contra ataques de CSRF mediante tokens CSRF. Cuando se activa, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro DE cuerpo DE POST específico.

Para habilitar la función, configure la `csrfToken` parámetro a. `true` durante la autenticación. El valor predeterminado es `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Cuando es verdadero, un `GridCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en Grid Manager y en `AccountCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en el Administrador de inquilinos.

Si la cookie está presente, todas las solicitudes que puedan modificar el estado del sistema (POST, PUT, PATCH, DELETE) deben incluir una de las siguientes:

- La `X-Csrf-Token` Encabezado, con el valor del encabezado establecido en el valor de la cookie de token de CSRF.
- Para los extremos que aceptan un cuerpo codificado mediante formulario: A. `csrfToken` parámetro de cuerpo de solicitud codificado mediante formulario.

Consulte la documentación de API en línea para obtener detalles y ejemplos adicionales.

> Las solicitudes que tienen un conjunto de cookies de token CSRF también harán cumplir el `"Content-Type: application/json"` Encabezado para cualquier solicitud que espera un cuerpo de solicitud JSON como protección adicional contra ataques CSRF.

Usar la API si está activado el inicio de sesión único

Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, no puede utilizar las solicitudes estándar de la API de autenticación para iniciar sesión y cerrar sesión en la API de administración de grid o en la API de gestión de inquilinos.

Iniciar sesión en la API si el inicio de sesión único está habilitado

Si se ha activado el inicio de sesión único (SSO), debe emitir una serie de solicitudes API para obtener un token de autenticación de AD FS que sea válido para la API de gestión de grid o la API de gestión de inquilinos.

Lo que necesitará

- Conoce el nombre de usuario y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- La `storagegrid-ssoauth.py` Script Python, que se encuentra en el directorio de archivos de instalación de StorageGRID (`./rpms` Para Red Hat Enterprise Linux o CentOS, `./debs` Para Ubuntu o

Debian, y. `./vsphere` Para VMware).

- Ejemplo de flujo de trabajo de solicitudes curl.

  El flujo de trabajo curl podría llegar a ocurrir si lo hace demasiado lentamente. Es posible que aparezca el error: No se ha encontrado una confirmación de suscripción válida en esta respuesta.

  > El flujo de trabajo curl de ejemplo no protege la contraseña de ser vista por otros usuarios.

Si tiene un problema de codificación URL, es posible que aparezca el error: Versión de SAML no compatible.

Pasos

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
   - Utilice la `storagegrid-ssoauth.py` Guión Python. Vaya al paso 2.
   - Usar solicitudes curl. Vaya al paso 3.
2. Si desea utilizar el `storagegrid-ssoauth.py` Guión, pase el script al intérprete Python y ejecute el script.

   Cuando se le solicite, escriba valores para los siguientes argumentos:

   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID
   - La dirección de StorageGRID
   - Si desea acceder a la API de gestión de inquilinos, introduzca el ID de cuenta de inquilino.

   +

   ```
   python3 /tmp/storagegrid-ssoauth.py
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

3. Si desea usar solicitudes curl, use el siguiente procedimiento.

   a. Declare las variables necesarias para iniciar sesión.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID=’12345’
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

Para acceder a la API de gestión de grid, utilice 0 AS `TENANTACCOUNTID`.

b. Para recibir una URL de autenticación firmada, emita una solicitud DE ENVÍO `/api/v3/authorize-saml`, Y quite la codificación JSON adicional de la respuesta.

En este ejemplo se muestra una solicitud POST para una dirección URL de autenticación firmada `TENANTACCOUNTID`. Los resultados se pasan a python -m json.tool para quitar la codificación JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La respuesta de este ejemplo incluye una dirección URL firmada codificada por URL, pero no incluye la capa de codificación JSON adicional.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Guarde la `SAMLRequest` de la respuesta para su uso en comandos posteriores.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Obtenga una URL completa que incluya el ID de solicitud de cliente de AD FS.

Una opción es solicitar el formulario de inicio de sesión mediante la URL de la respuesta anterior.

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

La respuesta incluye el ID de solicitud del cliente:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Guarde el ID de solicitud de cliente de la respuesta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envíe sus credenciales a la acción de formulario de la respuesta anterior.

```
curl -X POST
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --data
"UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMLPASSWORD&AuthMethod=For
msAuthentication" --include
```

AD FS devuelve un redireccionamiento 302, con información adicional en los encabezados.

> Si la autenticación multifactor (MFA) está habilitada para el sistema SSO, la entrada del formulario también contendrá la segunda contraseña u otras credenciales.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Guarde la `MSISAuth` cookie de la respuesta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envíe una solicitud GET a la ubicación especificada con las cookies de LA PUBLICACIÓN de autenticación.

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --cookie "MSISAuth=$MSISAuth" --include
```

Los encabezados de respuesta contendrán información de sesión de AD FS para el uso posterior del cierre de sesión y el cuerpo de respuesta contiene el SAMLResponse en un campo de formulario oculto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Guarde la `SAMLResponse` en el campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizando el guardado `SAMLResponse`, Haga un StorageGRID`/api/saml-response` Solicitud para generar un token de autenticación de StorageGRID.

Para `RelayState`, Utilice el ID de cuenta de arrendatario o utilice 0 si desea iniciar sesión en la API de administración de grid.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La respuesta incluye el token de autenticación.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Guarde el token de autenticación en la respuesta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ahora puede utilizar `MYTOKEN` Para otras solicitudes, del mismo modo que utilizaría la API si no se utiliza SSO.

Cerrar sesión en la API si se habilita el inicio de sesión único

Si se ha activado el inicio de sesión único (SSO), debe emitir una serie de solicitudes API para cerrar sesión en la API de gestión de grid o en la API de gestión de inquilinos.

Acerca de esta tarea

Si es necesario, puede cerrar la sesión de la API de StorageGRID simplemente cerrando la sesión en la página única de cierre de sesión de su empresa. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, que requiere un token de portador de StorageGRID válido.

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `cookie "sso=true"` En la API de SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Se devuelve una URL de cierre de sesión:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Guarde la URL de cierre de sesión.

```
export
LOGOUT_REQUEST='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEI
RfhZ...HcQ%3D%3D'
```

3. Envíe una solicitud a la URL de cierre de sesión para activar SLO y redirigir de nuevo a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta de 302. La ubicación de redirección no se aplica a la salida de sólo API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Elimine el token del portador de StorageGRID.

La eliminación del token del portador de StorageGRID funciona de la misma forma que sin SSO. Si `cookie "sso=true"` No proporciona, el usuario cierra la sesión de StorageGRID sin afectar al estado de SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

1. `204 No Content` la respuesta indica que el usuario ha cerrado la sesión.

```
HTTP/1.1 204 No Content
```

Usar certificados de seguridad StorageGRID

Los certificados de seguridad son archivos de datos pequeños que se utilizan para crear conexiones seguras y de confianza entre componentes de StorageGRID y entre componentes de StorageGRID y sistemas externos.

StorageGRID utiliza dos tipos de certificados de seguridad:

- **Se requieren certificados de servidor** cuando se utilizan conexiones HTTPS. Los certificados de servidor se utilizan para establecer conexiones seguras entre clientes y servidores, autenticar la identidad de un servidor a sus clientes y proporcionar una ruta de comunicación segura para los datos. Cada servidor y el cliente tienen una copia del certificado.
- **Los certificados de cliente** autentican una identidad de cliente o usuario al servidor, proporcionando una autenticación más segura que las contraseñas solamente. Los certificados de cliente no cifran datos.

Cuando un cliente se conecta al servidor mediante HTTPS, el servidor responde con el certificado de servidor, que contiene una clave pública. El cliente verifica este certificado comparando la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión con el servidor utilizando la misma clave pública.

StorageGRID funciona como servidor para algunas conexiones (como el extremo de equilibrio de carga) o como cliente para otras conexiones (como el servicio de replicación de CloudMirror).

Una entidad de certificación externa (CA) puede emitir certificados personalizados que cumplan plenamente con las políticas de seguridad de la información de su empresa. StorageGRID también incluye una entidad de certificación (CA) integrada que genera certificados de CA internos durante la instalación del sistema. Estos certificados de CA internos se utilizan, de forma predeterminada, para proteger el tráfico StorageGRID interno. Si bien se pueden utilizar los certificados de CA internos para un entorno que no sea de producción, la práctica recomendada para un entorno de producción es usar certificados personalizados firmados por una entidad de certificación externa. Las conexiones no seguras que no tienen ningún certificado también se admiten, pero no se recomienda.

- Los certificados de CA personalizados no quitan los certificados internos; sin embargo, los certificados personalizados deben ser los especificados para verificar las conexiones del servidor.
- Todos los certificados personalizados deben cumplir las directrices de endurecimiento del sistema para los certificados de servidor.

  "Endurecimiento del sistema"

- StorageGRID admite la agrupación de certificados de una CA en un único archivo (conocido como paquete de certificados de CA).

> StorageGRID también incluye certificados de CA del sistema operativo que son los mismos en todos los entornos Grid. En los entornos de producción, asegúrese de especificar un certificado personalizado firmado por una entidad de certificación externa en lugar del certificado de CA del sistema operativo.

Las variantes de los tipos de certificado de servidor y cliente se implementan de varias maneras. Es necesario tener preparados todos los certificados necesarios para la configuración específica de StorageGRID antes de configurar el sistema.

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de cliente de administrador	Cliente	Instalado en cada cliente, lo que permite que StorageGRID autentique el acceso de los clientes externos. • Permite a los clientes externos autorizados acceder a la base de datos Prometheus de StorageGRID. • Permite una supervisión segura de StorageGRID mediante herramientas externas.	**Configuración** > **Control de acceso** > **certificados de cliente**	"Configurar certificados de cliente de administrador"
Certificado de federación de identidades	Servidor	Autentica la conexión entre StorageGRID y un Active Directory, OpenLDAP o Oracle Directory Server externo.used for Identity federation, que permite que los grupos y usuarios de administración sean administrados por un sistema externo.	**Configuración** > **Control de acceso** > **Federación de identidades**	"Mediante la federación de identidades"

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de inicio de sesión único (SSO)	Servidor	Autentica la conexión entre Active Directory Federation Services (AD FS) y StorageGRID que se utiliza para solicitudes de inicio de sesión único (SSO).	**Configuración** > **Control de acceso** > **Inicio de sesión único**	"Configuración del inicio de sesión único"
Certificado de servidor de gestión de claves (KMS)	Servidor y cliente	Autentica la conexión entre StorageGRID y un servidor de gestión de claves (KMS) externo, que proporciona claves de cifrado a los nodos de los dispositivos StorageGRID.	**Configuración** > **Configuración del sistema** > **servidor de administración de claves**	"Adición de un servidor de gestión de claves (KMS)"

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de notificación de alertas por correo electrónico	Servidor y cliente	Autentica la conexión entre un servidor de correo electrónico SMTP y una StorageGRID que se usa para notificaciones de alerta. • Si las comunicaciones con el servidor SMTP requieren Transport Layer Security (TLS), debe especificar el certificado de CA del servidor de correo electrónico. • Especifique un certificado de cliente solo si el servidor de correo SMTP requiere certificados de cliente para la autenticación.	**Alertas** > **Configuración de correo electrónico**	"Solución de problemas de monitor"

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de punto final de equilibrador de carga	Servidor	Autentica la conexión entre clientes S3 o Swift y el servicio StorageGRID Load Balancer en nodos de puerta de enlace o nodos de administrador. Se carga o se genera un certificado de equilibrador de carga cuando se configura un extremo de equilibrador de carga.las aplicaciones cliente utilizan el certificado de equilibrador de carga al conectarse a StorageGRID para guardar y recuperar datos de objeto. **Nota:** el certificado de equilibrador de carga es el certificado más utilizado durante el funcionamiento normal de StorageGRID.	**Configuración** > **Configuración de red** > **parámetros de equilibrio de carga**	• "Configuración de los extremos del equilibrador de carga" • Creación de un extremo de equilibrador de carga para FabricPool "Configure StorageGRID para FabricPool"

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de servidor de interfaz de gestión	Servidor	Autentica la conexión entre los exploradores web del cliente y la interfaz de gestión de StorageGRID, lo que permite a los usuarios acceder a Grid Manager y al Gestor de inquilinos sin advertencias de seguridad. Este certificado también autentica las conexiones API de gestión de grid y API de gestión de inquilinos. Puede usar el certificado de CA interno o cargar un certificado personalizado.	**Configuración** > **Configuración de red** > **certificados de servidor**	• "Configuración de certificados de servidor" • "Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos"
Certificado de extremo de Cloud Storage Pool	Servidor	Autentica la conexión de Cloud Storage Pool de StorageGRID a una ubicación de almacenamiento externa (como S3 Glacier o almacenamiento blob de Microsoft Azure). Se necesita un certificado diferente para cada tipo de proveedor de cloud.	**ILM** > **agrupaciones de almacenamiento**	"Gestión de objetos con ILM"
Certificado de extremo de servicios de plataforma	Servidor	Autentica la conexión desde el servicio de plataforma StorageGRID a un recurso de almacenamiento S3.	**Administrador de inquilinos** > **ALMACENAMIENTO (S3)** > **terminales de servicios de plataforma**	"Usar una cuenta de inquilino"

Certificado	Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Certificado de servidor de extremo de servicio de Object Storage API	Servidor	Autentica conexiones de cliente Swift o S3 seguras con el servicio LDR (Local Distribution Router, LDR) en un nodo de almacenamiento o con el servicio Connection Load Balancer (CLB) obsoleto en un nodo de puerta de enlace.	**Configuración** > **Configuración de red** > **parámetros de equilibrio de carga**	"Configuración de un certificado de servidor personalizado para las conexiones al nodo de almacenamiento o al servicio CLB"

Ejemplo 1: Servicio de equilibrador de carga

En este ejemplo, StorageGRID actúa como servidor.

1. Se configura un extremo de equilibrador de carga y se carga o genera un certificado de servidor en StorageGRID.
2. Debe configurar una conexión de cliente S3 o Swift al extremo de equilibrio de carga y cargar el mismo certificado en el cliente.
3. Cuando el cliente desea guardar o recuperar datos, se conecta al extremo de equilibrio de carga mediante HTTPS.
4. StorageGRID responde con el certificado de servidor, que contiene una clave pública y una firma basada en la clave privada.
5. El cliente verifica este certificado comparando la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión utilizando la misma clave pública.
6. El cliente envía datos de objeto a StorageGRID.

Ejemplo 2: Servidor de gestión de claves externo (KMS)

En este ejemplo, StorageGRID actúa como cliente.

1. Con el software de servidor de gestión de claves externo, configura StorageGRID como un cliente KMS y obtiene un certificado de servidor firmado por CA, un certificado de cliente público y la clave privada del certificado de cliente.
2. Con el Administrador de grid, configura un servidor KMS y carga los certificados de servidor y cliente y la clave privada de cliente.
3. Cuando un nodo StorageGRID necesita una clave de cifrado, realiza una solicitud al servidor KMS que incluye datos del certificado y una firma basada en la clave privada.
4. El servidor KMS valida la firma del certificado y decide que puede confiar en StorageGRID.
5. El servidor KMS responde mediante la conexión validada.