Administra tu sistema

Element Software

NetApp
November 12, 2025

This PDF was generated from https://docs.netapp.com/es-es/element-software-128/storage/concept_system_manage_system_management.html on November 12, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Administra tu sistema

Administra tu sistema

Puedes gestionar tu sistema en la interfaz de usuario de Element. Esto incluye habilitar la autenticación multifactor, administrar la configuración del clúster, admitir los estándares federales de procesamiento de información (FIPS) y utilizar la administración de claves externas.

- "Habilitar la autenticación multifactor"
- "Configurar los ajustes del clúster"
- "Cree un clúster que admita unidades FIPS."
- "Comience con la administración de claves externas"

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Habilitar la autenticación multifactor

Configurar la autenticación multifactor

La autenticación multifactor (MFA) utiliza un proveedor de identidad (IdP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML) para gestionar las sesiones de usuario. La autenticación multifactor (MFA) permite a los administradores configurar factores de autenticación adicionales según sea necesario, como contraseña y mensaje de texto, y contraseña y mensaje de correo electrónico.

Puedes utilizar estos pasos básicos a través de la API de Element para configurar tu clúster para que utilice la autenticación multifactor.

Los detalles de cada método de la API se pueden encontrar en el "Referencia de la API de elementos".

1. Cree una nueva configuración de proveedor de identidad (IdP) de terceros para el clúster llamando al siguiente método de la API y pasando los metadatos del IdP en formato JSON: `CreateIdpConfiguration`

   Los metadatos del IdP, en formato de texto plano, se recuperan del IdP de terceros. Es necesario validar estos metadatos para asegurar que estén formateados correctamente en JSON. Existen numerosas aplicaciones de formato JSON disponibles que puedes utilizar, por ejemplo: https://freeformatter.com/json-escape.html.

2. Recupere los metadatos del clúster, a través de spMetadataUrl, para copiarlos al IdP de terceros llamando al siguiente método de API: `ListIdpConfigurations`

   spMetadataUrl es una URL utilizada para recuperar metadatos del proveedor de servicios del clúster para el IdP con el fin de establecer una relación de confianza.

3. Configure las aserciones SAML en el IdP de terceros para incluir el atributo “NameID” para identificar de forma única a un usuario para el registro de auditoría y para que el cierre de sesión único funcione correctamente.
4. Cree una o más cuentas de usuario de administrador de clúster autenticadas por un IdP de terceros para la autorización llamando al siguiente método de API:`AddIdpClusterAdmin`

> El nombre de usuario del administrador del clúster IdP debe coincidir con la asignación de nombre/valor del atributo SAML para lograr el efecto deseado, como se muestra en los siguientes ejemplos:

   - email=bob@company.com — donde el IdP está configurado para liberar una dirección de correo electrónico en los atributos SAML.
   - grupo=administrador-de-clúster - donde el IdP está configurado para liberar una propiedad de grupo a la que todos los usuarios deberían tener acceso. Tenga en cuenta que, por motivos de seguridad, el emparejamiento de nombre/valor del atributo SAML distingue entre mayúsculas y minúsculas.
5. Habilite la autenticación multifactor (MFA) para el clúster llamando al siguiente método de la API: `EnableIdpAuthentication`

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Información adicional sobre la autenticación multifactor

Debes tener en cuenta las siguientes advertencias en relación con la autenticación multifactor.

- Para actualizar los certificados IdP que ya no son válidos, deberá utilizar un usuario administrador que no sea IdP para llamar al siguiente método de la API: `UpdateIdpConfiguration`
- La autenticación multifactor (MFA) es incompatible con certificados de menos de 2048 bits de longitud. Por defecto, se crea un certificado SSL de 2048 bits en el clúster. Debe evitar establecer un certificado de tamaño reducido al llamar al método de la API: `SetSSLCertificate`

> Si el clúster utiliza un certificado de menos de 2048 bits antes de la actualización, el certificado del clúster debe actualizarse con un certificado de 2048 bits o superior después de la actualización a Element 12.0 o posterior.

- Los usuarios administradores de IdP no pueden utilizarse para realizar llamadas a la API directamente (por ejemplo, a través de SDK o Postman) ni para otras integraciones (por ejemplo, OpenStack Cinder o el complemento de vCenter). Si necesita crear usuarios con estas capacidades, agregue usuarios administradores de clúster LDAP o usuarios administradores de clúster locales.

Encuentra más información

- "Gestionar el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Configurar los ajustes del clúster

Habilitar y deshabilitar el cifrado en reposo para un clúster

Con los clústeres SolidFire , puede cifrar todos los datos en reposo almacenados en las unidades del clúster. Puede habilitar la protección de unidades de autocifrado (SED) en todo el clúster mediante cualquiera de los siguientes métodos:"Cifrado en reposo basado en hardware o software" .

Puede habilitar el cifrado de hardware en reposo mediante la interfaz de usuario o la API de Element. Habilitar la función de cifrado de hardware en reposo no afecta al rendimiento ni a la eficiencia del clúster. Solo puede habilitar el cifrado de software en reposo utilizando la API de Element.

El cifrado de datos en reposo basado en hardware no está habilitado de forma predeterminada durante la creación del clúster y se puede habilitar y deshabilitar desde la interfaz de usuario de Element.

> Para los clústeres de almacenamiento all-flash SolidFire , el cifrado de software en reposo debe habilitarse durante la creación del clúster y no puede deshabilitarse después de que se haya creado el clúster.

Lo que necesitarás

- Usted tiene privilegios de administrador de clúster para habilitar o cambiar la configuración de cifrado.
- Para el cifrado en reposo basado en hardware, debe asegurarse de que el clúster se encuentre en buen estado antes de cambiar la configuración de cifrado.
- Si va a deshabilitar el cifrado, dos nodos deben participar en un clúster para acceder a la clave para deshabilitar el cifrado en una unidad.

Comprobar el estado del cifrado en reposo

Para ver el estado actual del cifrado en reposo y/o del cifrado de software en reposo en el clúster, utilice la siguiente información:"Obtener información del clúster" método. Puedes usar el"Obtener información de cifrado de software en reposo" Método para obtener información sobre el clúster que utiliza para cifrar los datos en reposo.

> El panel de control de la interfaz de usuario del software Element en `https://<MVIP>/` Actualmente solo se muestra el estado de cifrado en reposo para el cifrado basado en hardware.

Opciones

- Habilitar el cifrado basado en hardware en reposo
- Habilitar el cifrado basado en software en reposo
- Deshabilitar el cifrado basado en hardware en reposo

Habilitar el cifrado basado en hardware en reposo

> Para habilitar el cifrado en reposo mediante una configuración de administración de claves externa, debe habilitar el cifrado en reposo a través de"API" . Habilitar esta función mediante el botón de la interfaz de usuario de Element existente hará que se vuelva a utilizar la generación interna de claves.

1. Desde la interfaz de usuario de Element, seleccione **Cluster** > **Settings**.
2. Seleccione **Habilitar cifrado en reposo**.

Habilitar el cifrado basado en software en reposo

> El cifrado de software en reposo no se puede deshabilitar después de que se haya habilitado en el clúster.

1. Durante la creación del clúster, ejecute el"método de creación de clúster" con `enableSoftwareEncryptionAtRest` empezar a `true` .

Deshabilitar el cifrado basado en hardware en reposo

1. Desde la interfaz de usuario de Element, seleccione **Cluster** > **Settings**.
2. Seleccione **Deshabilitar el cifrado en reposo**.

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Establezca el umbral completo del clúster

Puedes cambiar el nivel en el que el sistema genera una advertencia de llenado del clúster de bloques siguiendo los pasos que se indican a continuación. Además, puede utilizar el método de la API ModifyClusterFullThreshold para cambiar el nivel en el que el sistema genera una advertencia de bloqueo o de metadatos.

Lo que necesitarás

Debe tener privilegios de administrador de clúster.

Pasos

1. Haz clic en **Clúster** > **Configuración**.
2. En la sección Configuración completa del clúster, ingrese un porcentaje en **Generar una alerta de advertencia cuando quede un _% de capacidad antes de que Helix no pueda recuperarse de una falla de nodo**.
3. Haz clic en **Guardar cambios**.

Encuentra más información

"¿Cómo se calculan los umbrales de blockSpace para Element?"

Habilitar y deshabilitar el balanceo de carga de volumen

A partir de Element 12.8, puede usar el balanceo de carga de volumen para equilibrar los volúmenes entre nodos según las IOPS reales de cada volumen en lugar de las IOPS mínimas configuradas en la política de QoS. Puede activar y desactivar el balanceo de carga de volumen, que está desactivado de forma predeterminada, mediante la interfaz

de usuario o la API de Element.

Pasos

1. Seleccione **Clúster** > **Configuración**.
2. En la sección Específica del clúster, cambie el estado de Balanceo de carga de volumen:

   Habilitar el equilibrio de carga de volumen

   Seleccione **Habilitar balanceo de carga en IOPS reales** y confirme su selección.

   Deshabilitar el equilibrio de carga de volumen:

   Seleccione **Deshabilitar el balanceo de carga en IOPS reales** y confirme su selección.

3. Opcionalmente, seleccione **Informes** > **Resumen** para confirmar el cambio de estado de Balance en IOPS reales. Es posible que tengas que desplazarte hacia abajo en la información de estado del clúster para ver el estado.

Encuentra más información

- "Habilite el balanceo de carga de volumen mediante la API"
- "Deshabilitar el balanceo de carga de volumen mediante la API"
- "Crear y gestionar políticas de QoS de volumen"

Habilitar y deshabilitar el acceso de soporte

Puede habilitar el acceso de soporte para permitir temporalmente que el personal de soporte de NetApp acceda a los nodos de almacenamiento a través de SSH para la resolución de problemas.

Debe tener privilegios de administrador de clúster para cambiar el acceso de soporte.

1. Haz clic en **Clúster** > **Configuración**.
2. En la sección Habilitar/Deshabilitar acceso de soporte, ingrese la duración (en horas) durante la cual desea permitir que el soporte tenga acceso.
3. Haga clic en **Habilitar acceso de soporte**.
4. **Opcional:** Para deshabilitar el acceso al soporte, haga clic en **Deshabilitar acceso al soporte**.

Gestionar el banner de Condiciones de uso

Puedes habilitar, editar o configurar un banner que contenga un mensaje para el usuario.

Opciones

Habilita el banner de Condiciones de uso Edita el banner de Condiciones de uso Desactivar el banner de Condiciones de uso

Habilita el banner de Condiciones de uso

Puedes habilitar un banner de Condiciones de uso que aparezca cuando un usuario inicie sesión en la interfaz de usuario de Element. Cuando el usuario haga clic en el banner, aparecerá un cuadro de diálogo de texto con

el mensaje que ha configurado para el clúster. El banner puede eliminarse en cualquier momento.

Debe tener privilegios de administrador de clúster para habilitar la funcionalidad de Términos de uso.

1. Haz clic en **Usuarios** > **Condiciones de uso**.
2. En el formulario **Condiciones de uso**, introduzca el texto que se mostrará en el cuadro de diálogo de Condiciones de uso.

   No exceda los 4096 caracteres.

3. Haga clic en **Habilitar**.

Edita el banner de Condiciones de uso

Puedes editar el texto que ve un usuario cuando selecciona el banner de inicio de sesión de los Términos de uso.

Lo que necesitarás

- Para configurar las Condiciones de uso, debe tener privilegios de administrador de clúster.
- Asegúrese de que la función de Condiciones de uso esté habilitada.

Pasos

1. Haz clic en **Usuarios** > **Condiciones de uso**.
2. En el cuadro de diálogo **Condiciones de uso**, edite el texto que desea que aparezca.

   No exceda los 4096 caracteres.

3. Haz clic en **Guardar cambios**.

Desactivar el banner de Condiciones de uso

Puedes desactivar el banner de Condiciones de uso. Con el banner desactivado, ya no se le solicita al usuario que acepte los términos de uso al utilizar la interfaz de usuario de Element.

Lo que necesitarás

- Para configurar las Condiciones de uso, debe tener privilegios de administrador de clúster.
- Asegúrese de que las Condiciones de uso estén habilitadas.

Pasos

1. Haz clic en **Usuarios** > **Condiciones de uso**.
2. Haga clic en **Desactivar**.

Configurar el protocolo de tiempo de red

Configure los servidores del Protocolo de Tiempo de Red (NTP) para que el clúster los consulte.

Puede instruir a cada nodo de un clúster para que consulte a un servidor de Protocolo de Tiempo de Red (NTP) para obtener actualizaciones. El clúster solo contacta con los servidores configurados y les solicita información NTP.

El protocolo NTP se utiliza para sincronizar los relojes a través de una red. La conexión a un servidor NTP interno o externo debe formar parte de la configuración inicial del clúster.

Configure NTP en el clúster para que apunte a un servidor NTP local. Puede utilizar la dirección IP o el nombre de host FQDN. El servidor NTP predeterminado al momento de la creación del clúster se establece en us.pool.ntp.org; sin embargo, no siempre se puede establecer una conexión con este sitio dependiendo de la ubicación física del clúster SolidFire .

El uso del FQDN depende de si la configuración DNS del nodo de almacenamiento individual está implementada y operativa. Para ello, configure los servidores DNS en cada nodo de almacenamiento y asegúrese de que los puertos estén abiertos consultando la página de Requisitos de puertos de red.

Puedes introducir hasta cinco servidores NTP diferentes.

Puedes utilizar direcciones IPv4 e IPv6.

Lo que necesitarás

Para configurar este ajuste, debe tener privilegios de administrador de clúster.

Pasos

1. Configure una lista de direcciones IP y/o nombres de dominio completos (FQDN) en la configuración del servidor.
2. Asegúrese de que el DNS esté configurado correctamente en los nodos.
3. Haz clic en **Clúster** > **Configuración**.
4. En Configuración del protocolo de tiempo de red, seleccione **No**, que utiliza la configuración NTP estándar.
5. Haz clic en **Guardar cambios**.

Encuentra más información

- "Configure el clúster para que escuche las transmisiones NTP."
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Configure el clúster para que escuche las transmisiones NTP.

Al utilizar el modo de difusión, puede indicar a cada nodo de un clúster que escuche en la red los mensajes de difusión del Protocolo de tiempo de red (NTP) procedentes de un servidor determinado.

El protocolo NTP se utiliza para sincronizar los relojes a través de una red. La conexión a un servidor NTP interno o externo debe formar parte de la configuración inicial del clúster.

Lo que necesitarás

- Para configurar este ajuste, debe tener privilegios de administrador de clúster.
- Debe configurar un servidor NTP en su red como servidor de difusión.

Pasos

1. Haz clic en **Clúster** > **Configuración**.
2. Introduzca en la lista de servidores el servidor o servidores NTP que utilizan el modo de difusión.

3. En Configuración del protocolo de tiempo de red, seleccione **Sí** para usar un cliente de difusión.
4. Para configurar el cliente de difusión, en el campo **Servidor**, introduzca el servidor NTP que configuró en modo de difusión.
5. Haz clic en **Guardar cambios**.

Encuentra más información

- "Configure los servidores del Protocolo de Tiempo de Red (NTP) para que el clúster los consulte."
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Administrar SNMP

Obtenga más información sobre SNMP

Puede configurar el Protocolo Simple de Administración de Red (SNMP) en su clúster.

Puede seleccionar un solicitante SNMP, seleccionar qué versión de SNMP utilizar, identificar el usuario del modelo de seguridad basado en usuario (USM) de SNMP y configurar traps para monitorear el clúster SolidFire . También puede ver y acceder a los archivos de la base de datos de información de gestión.

Puedes utilizar direcciones IPv4 e IPv6.

Detalles SNMP

En la página SNMP de la pestaña Clúster, puede ver la siguiente información.

- **MIB SNMP**

  Los archivos MIB que puede ver o descargar.

- **Configuración general de SNMP**

  Puede habilitar o deshabilitar SNMP. Una vez habilitado SNMP, puede elegir qué versión utilizar. Si utiliza la versión 2, puede agregar solicitantes, y si utiliza la versión 3, puede configurar usuarios USM.

- **Configuración de trampas SNMP**

  Puedes identificar qué trampas quieres capturar. Puede configurar el host, el puerto y la cadena de comunidad para cada destinatario de la trampa.

Configurar un solicitante SNMP

Cuando SNMP versión 2 está habilitada, puede habilitar o deshabilitar un solicitante y configurar los solicitantes para que reciban solicitudes SNMP autorizadas.

1. Menú de clic: Clúster[SNMP].
2. En **Configuración general de SNMP**, haga clic en **Sí** para habilitar SNMP.
3. De la lista **Versión**, seleccione **Versión 2**.
4. En la sección **Solicitantes**, ingrese la **Cadena de comunidad** y la información de **Red**.

Por defecto, la cadena de comunidad es pública y la red es localhost. Puedes cambiar esta configuración predeterminada.

5. **Opcional:** Para agregar otro solicitante, haga clic en **Agregar un solicitante** e ingrese la **Cadena de comunidad** y la información de **Red**.
6. Haz clic en **Guardar cambios**.

Encuentra más información

- Configurar traps SNMP
- Visualización de datos de objetos gestionados mediante archivos de la base de información de gestión.

Configurar un usuario SNMP USM

Cuando habilite SNMP versión 3, deberá configurar un usuario USM para que reciba las solicitudes SNMP autorizadas.

1. Haga clic en **Clúster** > **SNMP**.
2. En **Configuración general de SNMP**, haga clic en **Sí** para habilitar SNMP.
3. De la lista **Versión**, seleccione **Versión 3**.
4. En la sección **Usuarios de USM**, ingrese el nombre, la contraseña y la frase de contraseña.
5. **Opcional:** Para agregar otro usuario de USM, haga clic en **Agregar un usuario de USM** e ingrese el nombre, la contraseña y la frase de contraseña.
6. Haz clic en **Guardar cambios**.

Configurar traps SNMP

Los administradores de sistemas pueden usar traps SNMP, también conocidas como notificaciones, para monitorear el estado del clúster SolidFire .

Cuando las alertas SNMP están habilitadas, el clúster SolidFire genera alertas asociadas con entradas del registro de eventos y alertas del sistema. Para recibir notificaciones SNMP, debe elegir las trampas que se deben generar e identificar los destinatarios de la información de la trampa. Por defecto, no se generan trampas.

1. Haga clic en **Clúster** > **SNMP**.
2. Seleccione uno o más tipos de traps en la sección **Configuración de traps SNMP** que el sistema debería generar:
   - Trampas de fallos de clúster
   - Trampas de fallos resueltas en clúster
   - Trampas de eventos de clúster
3. En la sección **Destinatarios de la trampa**, ingrese la información del host, el puerto y la cadena de comunidad para un destinatario.
4. **Opcional**: Para agregar otro destinatario de trampa, haga clic en **Agregar un destinatario de trampa** e ingrese la información de host, puerto y cadena de comunidad.
5. Haz clic en **Guardar cambios**.

Visualización de datos de objetos gestionados mediante archivos de la base de información de gestión.

Puede ver y descargar los archivos de la base de información de gestión (MIB) utilizados para definir cada uno de los objetos gestionados. La función SNMP admite el acceso de solo lectura a los objetos definidos en SolidFire-StorageCluster-MIB.

Los datos estadísticos proporcionados en la MIB muestran la actividad del sistema para lo siguiente:

- Estadísticas de clúster
- Estadísticas de volumen
- Estadísticas de volúmenes por cuenta
- Estadísticas de nodos
- Otros datos como informes, errores y eventos del sistema

El sistema también admite el acceso al archivo MIB que contiene los puntos de acceso de nivel superior (OIDS) a los productos de la serie SF.

Pasos

1. Haga clic en **Clúster** > **SNMP**.
2. En **SNMP MIBs**, haga clic en el archivo MIB que desea descargar.
3. En la ventana de descarga resultante, abra o guarde el archivo MIB.

Administrar unidades

Cada nodo contiene una o más unidades físicas que se utilizan para almacenar una parte de los datos del clúster. El clúster utiliza la capacidad y el rendimiento de la unidad después de que esta se haya agregado correctamente al clúster. Puedes utilizar la interfaz de usuario de Element para administrar las unidades.

Detalles de las unidades

La página Unidades en la pestaña Clúster proporciona una lista de las unidades activas en el clúster. Puede filtrar la página seleccionando entre las pestañas Activos, Disponibles, Eliminando, Borrando y Fallidos.

Cuando se inicializa un clúster por primera vez, la lista de unidades activas está vacía. Puede agregar unidades que no estén asignadas a un clúster y que aparezcan en la pestaña Disponible después de crear un nuevo clúster SolidFire .

Los siguientes elementos aparecen en la lista de unidades activas.

- **Identificador de unidad**

  El número secuencial asignado a la unidad.

- **ID del nodo**

  El número de nodo asignado cuando el nodo se agrega al clúster.

- **Nombre del nodo**

El nombre del nodo que aloja la unidad.

- **Ranura**

  El número de ranura donde se encuentra físicamente la unidad.

- **Capacidad**

  Tamaño de la unidad, en GB.

- **De serie**

  El número de serie de la unidad.

- **Desgaste restante**

  El indicador del nivel de desgaste.

  El sistema de almacenamiento informa la cantidad aproximada de desgaste disponible en cada unidad de estado sólido (SSD) para la escritura y el borrado de datos. Una unidad que ha consumido el 5 por ciento de sus ciclos de escritura y borrado diseñados reporta un desgaste restante del 95 por ciento. El sistema no actualiza automáticamente la información sobre el desgaste de la unidad; puede actualizar la página o cerrarla y volver a cargarla para actualizar la información.

- **Tipo**

  El tipo de transmisión. El tipo puede ser bloque o metadatos.

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Gestionar nodos

Gestionar nodos

Puede administrar el almacenamiento SolidFire y los nodos Fibre Channel desde la página Nodos de la pestaña Clúster.

Si un nodo recién agregado representa más del 50 por ciento de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("varada"), de modo que cumpla con la regla de capacidad. Esto seguirá siendo así hasta que se añada más capacidad de almacenamiento. Si se añade un nodo muy grande que también incumple la regla de capacidad, el nodo que antes estaba aislado dejará de estarlo, mientras que el nodo recién añadido quedará aislado. La capacidad siempre debe añadirse por pares para evitar que esto ocurra. Cuando un nodo queda aislado, se genera un fallo de clúster apropiado.

Encuentra más información

Agregar un nodo a un clúster

Agregar un nodo a un clúster

Puedes agregar nodos a un clúster cuando se necesite más almacenamiento o después de la creación del clúster. Los nodos requieren una configuración inicial cuando se encienden por primera vez. Una vez configurado el nodo, aparece en la lista de nodos pendientes y se puede agregar a un clúster.

La versión del software en cada nodo de un clúster debe ser compatible. Cuando se agrega un nodo a un clúster, este instala la versión del software NetApp Element correspondiente en el nuevo nodo, según sea necesario.

Puedes agregar nodos de menor o mayor capacidad a un clúster existente. Puede agregar capacidades de nodo mayores a un clúster para permitir el crecimiento de la capacidad. Los nodos más grandes que se agreguen a un clúster con nodos más pequeños deben agregarse por pares. Esto proporciona espacio suficiente para que Double Helix pueda mover los datos en caso de que falle uno de los nodos más grandes. Puedes agregar nodos de menor capacidad a un clúster de nodos más grande para mejorar el rendimiento.

> Si un nodo recién agregado representa más del 50 por ciento de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("varada"), de modo que cumpla con la regla de capacidad. Esto seguirá siendo así hasta que se añada más capacidad de almacenamiento. Si se añade un nodo muy grande que también incumple la regla de capacidad, el nodo que antes estaba aislado dejará de estarlo, mientras que el nodo recién añadido quedará aislado. La capacidad siempre debe añadirse por pares para evitar que esto ocurra. Cuando un nodo queda aislado, se produce un fallo de clúster strandedCapacity.

"Vídeo de NetApp : Escala a tu manera: Ampliación de un clúster SolidFire"

Puedes agregar nodos a los dispositivos NetApp HCI .

Pasos

1. Seleccione **Clúster** > **Nodos**.
2. Haz clic en **Pendientes** para ver la lista de nodos pendientes.

   Cuando finaliza el proceso de adición de nodos, estos aparecen en la lista de nodos activos. Hasta entonces, los nodos pendientes aparecerán en la lista de Nodos Activos Pendientes.

   SolidFire instala la versión del software Element del clúster en los nodos pendientes cuando los agrega a un clúster. Esto podría tardar unos minutos.

3. Debe realizar una de las siguientes acciones:
   - Para agregar nodos individuales, haga clic en el icono **Acciones** del nodo que desea agregar.
   - Para agregar varios nodos, seleccione la casilla de verificación de los nodos que desea agregar y luego **Acciones en lote**. **Nota:** Si el nodo que está agregando tiene una versión del software Element diferente a la versión que se ejecuta en el clúster, el clúster actualiza de forma asíncrona el nodo a la versión del software Element que se ejecuta en el maestro del clúster. Después de que se actualiza el nodo, se agrega automáticamente al clúster. Durante este proceso asíncrono, el nodo estará en estado pendingActive.
4. Haga clic en **Agregar**.

   El nodo aparece en la lista de nodos activos.

Encuentra más información

Control de versiones y compatibilidad de nodos

Control de versiones y compatibilidad de nodos

La compatibilidad de los nodos se basa en la versión del software Element instalada en un nodo. Los clústeres de almacenamiento basados en software de Element crean automáticamente una imagen de un nodo a la versión del software de Element en el clúster si el nodo y el clúster no tienen versiones compatibles.

La siguiente lista describe los niveles de importancia de las versiones de software que componen el número de versión del software Element:

- **Importante**

  El primer número designa una versión del software. No se puede agregar un nodo con un número de componente principal a un clúster que contenga nodos con un número de parche principal diferente, ni se puede crear un clúster con nodos de versiones principales mixtas.

- **Menor**

  El segundo número designa características de software menores o mejoras a características de software existentes que se han añadido a una versión principal. Este componente se incrementa dentro de un componente de versión principal para indicar que esta versión incremental no es compatible con ninguna otra versión incremental del software Element que tenga un componente secundario diferente. Por ejemplo, la versión 11.0 no es compatible con la 11.1, y la versión 11.1 no es compatible con la 11.2.

- **Micro**

  El tercer número designa un parche compatible (versión incremental) para la versión del software Element representada por los componentes mayor.menor. Por ejemplo, la versión 11.0.1 es compatible con la versión 11.0.2, y la versión 11.0.2 es compatible con la versión 11.0.3.

Para garantizar la compatibilidad, los números de versión principal y secundaria deben coincidir. Los números micro no tienen que coincidir para ser compatibles.

Capacidad del clúster en un entorno de nodos mixtos

Puedes mezclar diferentes tipos de nodos en un clúster. Las series SF 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 y la serie H pueden coexistir en un clúster.

La serie H consta de los nodos H610S-1, H610S-2, H610S-4 y H410S. Estos nodos son compatibles tanto con 10GbE como con 25GbE.

Lo mejor es no mezclar nodos no cifrados con nodos cifrados. En un clúster de nodos mixtos, ningún nodo puede ser mayor que el 33 por ciento de la capacidad total del clúster. Por ejemplo, en un clúster con cuatro nodos SF-Series 4805, el nodo más grande que se puede agregar individualmente es un SF-Series 9605. El umbral de capacidad del clúster se calcula en función de la pérdida potencial del nodo más grande en esta situación.

Dependiendo de la versión del software Element, los siguientes nodos de almacenamiento de la serie SF no son compatibles:

A partir de…	Nodo de almacenamiento no compatible…
Elemento 12.8	• SF4805 • SF9605 • SF19210 • SF38410
Elemento 12.7	• SF2405 • SF9608
Elemento 12.0	• SF3010 • SF6010 • SF9010

Si intenta actualizar uno de estos nodos a una versión de Element no compatible, verá un error que indica que el nodo no es compatible con Element 12.x.

Ver detalles del nodo

Puede ver detalles de nodos individuales, como etiquetas de servicio, detalles de la unidad y gráficos de utilización y estadísticas de la unidad. La página Nodos de la pestaña Clúster proporciona la columna Versión, donde puede ver la versión de software de cada nodo.

Pasos

1. Haz clic en **Clúster** > **Nodos**.
2. Para ver los detalles de un nodo específico, haga clic en el icono **Acciones** del nodo.
3. Haga clic en **Ver detalles**.
4. Revisa los detalles del nodo:
   - **ID de nodo**: El ID generado por el sistema para el nodo.
   - **Nombre del nodo**: El nombre de host del nodo.
   - **Rol del nodo**: El rol que el nodo tiene en el clúster. Valores posibles:
     - Maestro del clúster: El nodo que realiza tareas administrativas en todo el clúster y contiene el MVIP y el SVIP.
     - Nodo de conjunto: Un nodo que participa en el clúster. Hay 3 o 5 nodos de conjunto dependiendo del tamaño del clúster.
     - Canal de fibra: Un nodo en el clúster.
   - **Tipo de nodo**: El tipo de modelo del nodo.
   - **Unidades activas**: El número de unidades activas en el nodo.
   - **Utilización del nodo**: Porcentaje de utilización del nodo basado en nodeHeat. El valor mostrado es recentPrimaryTotalHeat como porcentaje. Disponible a partir del Elemento 12.8.
   - **IP de gestión**: La dirección IP de gestión (MIP) asignada al nodo para tareas de administración de red de 1GbE o 10GbE.

- **IP del clúster**: La dirección IP del clúster (CIP) asignada al nodo y utilizada para la comunicación entre nodos del mismo clúster.
- **IP de almacenamiento**: La dirección IP de almacenamiento (SIP) asignada al nodo utilizada para el descubrimiento de la red iSCSI y todo el tráfico de datos de la red.
- **ID de VLAN de administración**: El ID virtual para la red de área local de administración.
- **ID de VLAN de almacenamiento**: El ID virtual para la red de área local de almacenamiento.
- **Versión**: La versión del software que se ejecuta en cada nodo.
- **Puerto de replicación**: El puerto utilizado en los nodos para la replicación remota.
- **Etiqueta de servicio**: El número de etiqueta de servicio único asignado al nodo.
- **Dominio de protección personalizado**: El dominio de protección personalizado asignado al nodo.

Ver detalles de los puertos Fibre Channel

En la página de puertos FC puede consultar los detalles de los puertos Fibre Channel, como su estado, nombre y dirección.

Consulte la información sobre los puertos Fibre Channel conectados al clúster.

Pasos

1. Haga clic en **Clúster** > **Puertos FC**.
2. Para filtrar la información de esta página, haga clic en **Filtrar**.
3. Revisa los detalles:
   - **ID de nodo**: El nodo que aloja la sesión para la conexión.
   - **Nombre del nodo**: Nombre del nodo generado por el sistema.
   - **Ranura**: Número de ranura donde se encuentra el puerto Fibre Channel.
   - **Puerto HBA**: Puerto físico en el adaptador de bus de host de Fibre Channel (HBA).
   - **WWNN**: Nombre del nodo mundial.
   - **WWPN**: Nombre del puerto mundial de destino.
   - **WWN del switch**: Nombre mundial del switch Fibre Channel.
   - **Estado del puerto**: Estado actual del puerto.
   - **nPort ID**: El ID del puerto del nodo en la estructura Fibre Channel.
   - **Velocidad**: La velocidad negociada del canal de fibra. Los valores posibles son los siguientes:
     - 4Gbps
     - 8Gbps
     - 16Gbps

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Gestionar redes virtuales

Gestionar redes virtuales

La virtualización de redes en el almacenamiento SolidFire permite que el tráfico entre múltiples clientes que se encuentran en redes lógicas separadas se conecte a un solo clúster. Las conexiones al clúster se segregan en la pila de red mediante el uso de etiquetado VLAN.

Encuentra más información

- Agregar una red virtual
- Habilitar el enrutamiento y reenvío virtual
- Editar una red virtual
- Editar VLAN VRF
- Eliminar una red virtual

Agregar una red virtual

Puede agregar una nueva red virtual a una configuración de clúster para habilitar una conexión de entorno multiinquilino a un clúster que ejecuta el software Element.

Lo que necesitarás

- Identifique el bloque de direcciones IP que se asignarán a las redes virtuales en los nodos del clúster.
- Identifique una dirección IP de red de almacenamiento (SVIP) que se utilizará como punto final para todo el tráfico de almacenamiento de NetApp Element .

Para esta configuración, debe tener en cuenta los siguientes criterios:

- Las VLAN que no tienen habilitado VRF requieren que los iniciadores estén en la misma subred que la SVIP.
- Las VLAN que tienen habilitado VRF no requieren que los iniciadores estén en la misma subred que la SVIP, y se admite el enrutamiento.
- La SVIP predeterminada no requiere que los iniciadores estén en la misma subred que la SVIP, y admite el enrutamiento.

Cuando se agrega una red virtual, se crea una interfaz para cada nodo y cada una requiere una dirección IP de red virtual. El número de direcciones IP que especifique al crear una nueva red virtual debe ser igual o mayor que el número de nodos del clúster. Las direcciones de red virtuales se aprovisionan de forma masiva y se asignan a nodos individuales automáticamente. No es necesario asignar manualmente direcciones de red virtuales a los nodos del clúster.

Pasos

1. Haga clic en **Clúster** > **Red**.
2. Haga clic en **Crear VLAN**.
3. En el cuadro de diálogo **Crear una nueva VLAN**, introduzca los valores en los siguientes campos:
    - **Nombre de VLAN**

- **Etiqueta VLAN**
- **SVIP**
- **Máscara de red**
- (Opcional) **Descripción**

4. Ingrese la dirección **IP inicial** para el rango de direcciones IP en **Bloques de direcciones IP**.
5. Ingrese el **Tamaño** del rango de IP como el número de direcciones IP que se incluirán en el bloque.
6. Haz clic en **Agregar un bloque** para añadir un bloque no contiguo de direcciones IP para esta VLAN.
7. Haga clic en **Crear VLAN**.

Ver detalles de la red virtual

Pasos

1. Haga clic en **Clúster** > **Red**.
2. Revise los detalles.
   - **ID**: Identificador único de la red VLAN, asignado por el sistema.
   - **Nombre**: Nombre único asignado por el usuario para la red VLAN.
   - **Etiqueta VLAN**: Etiqueta VLAN asignada cuando se creó la red virtual.
   - **SVIP**: Dirección IP virtual de almacenamiento asignada a la red virtual.
   - **Máscara de red**: Máscara de red para esta red virtual.
   - **Puerta de enlace**: Dirección IP única de una puerta de enlace de red virtual. VRF debe estar habilitado.
   - **VRF habilitado**: Indicación de si el enrutamiento y reenvío virtual está habilitado o no.
   - **Direcciones IP utilizadas**: El rango de direcciones IP de red virtual utilizadas para la red virtual.

Habilitar el enrutamiento y reenvío virtual

Puede habilitar el enrutamiento y reenvío virtual (VRF), lo que permite que existan varias instancias de una tabla de enrutamiento en un enrutador y funcionen simultáneamente. Esta funcionalidad solo está disponible para redes de almacenamiento.

Solo puedes habilitar VRF al momento de crear una VLAN. Si desea volver a un modo no VRF, deberá eliminar y volver a crear la VLAN.

1. Haga clic en **Clúster** > **Red**.
2. Para habilitar VRF en una nueva VLAN, seleccione **Crear VLAN**.
   a. Introduzca la información pertinente para la nueva VRF/VLAN. Consulte la sección "Agregar una red virtual".
   b. Seleccione la casilla de verificación **Habilitar VRF**.
   c. **Opcional**: Introduzca una puerta de enlace.
3. Haga clic en **Crear VLAN**.

Encuentra más información

Agregar una red virtual

Editar una red virtual

Puedes cambiar los atributos de la VLAN, como el nombre de la VLAN, la máscara de red y el tamaño de los bloques de direcciones IP. La etiqueta VLAN y la SVIP no se pueden modificar para una VLAN. El atributo de puerta de enlace no es un parámetro válido para VLAN que no sean VRF.

Si existen sesiones iSCSI, de replicación remota u otras sesiones de red, la modificación podría fallar.

Al administrar el tamaño de los rangos de direcciones IP de VLAN, debe tener en cuenta las siguientes limitaciones:

- Solo puedes eliminar direcciones IP del rango de direcciones IP inicial asignado en el momento de la creación de la VLAN.
- Puedes eliminar un bloque de direcciones IP que se agregó después del rango de direcciones IP inicial, pero no puedes cambiar el tamaño de un bloque de IP eliminando direcciones IP.
- Cuando intentas eliminar direcciones IP, ya sea del rango de direcciones IP inicial o de un bloque IP, que están en uso por nodos del clúster, la operación podría fallar.
- No se pueden reasignar direcciones IP específicas en uso a otros nodos del clúster.

Puede agregar un bloque de direcciones IP siguiendo el siguiente procedimiento:

1. Seleccione **Clúster** > **Red**.
2. Seleccione el icono Acciones para la VLAN que desea editar.
3. Seleccione **Editar**.
4. En el cuadro de diálogo **Editar VLAN**, introduzca los nuevos atributos para la VLAN.
5. Seleccione **Agregar un bloque** para agregar un bloque no contiguo de direcciones IP para la red virtual.
6. Seleccione **Guardar cambios**.

Enlace a artículos de la base de conocimientos para la resolución de problemas

Enlace a los artículos de la Base de conocimientos para obtener ayuda con la resolución de problemas relacionados con la administración de sus rangos de direcciones IP de VLAN.

- "Advertencia de IP duplicada tras agregar un nodo de almacenamiento en la VLAN del clúster Element"
- "Cómo determinar qué direcciones IP de VLAN están en uso y a qué nodos están asignadas esas direcciones IP en Element"

Editar VLAN VRF

Puede cambiar los atributos de VLAN de VRF, como el nombre de VLAN, la máscara de red, la puerta de enlace y los bloques de direcciones IP.

1. Haga clic en **Clúster** > **Red**.
2. Haz clic en el icono Acciones de la VLAN que deseas editar.
3. Haga clic en **Editar**.
4. Introduzca los nuevos atributos para la VLAN VRF en el cuadro de diálogo **Editar VLAN**.
5. Haz clic en **Guardar cambios**.

Eliminar una red virtual

Puedes eliminar un objeto de red virtual. Debes agregar los bloques de direcciones a otra red virtual antes de eliminar una red virtual.

1. Haga clic en **Clúster** > **Red**.
2. Haz clic en el icono de Acciones de la VLAN que deseas eliminar.
3. Haga clic en **Eliminar**.
4. Confirma el mensaje.

Encuentra más información

Editar una red virtual

Cree un clúster que admita unidades FIPS.

Preparar el clúster Element para la función de unidades FIPS

La seguridad se está convirtiendo en un aspecto cada vez más crítico para el despliegue de soluciones en muchos entornos de clientes. Las Normas Federales de Procesamiento de Información (FIPS) son normas para la seguridad informática y la interoperabilidad. El cifrado certificado FIPS 140-2 para datos en reposo es un componente de la solución de seguridad general.

Para preparar la activación de la función de unidades FIPS, debe evitar mezclar nodos en los que algunos sean compatibles con unidades FIPS y otros no.

Un clúster se considera compatible con las unidades FIPS según las siguientes condiciones:

- Todas las unidades están certificadas como unidades FIPS.
- Todos los nodos son nodos de unidades FIPS.
- El cifrado en reposo (EAR) está habilitado.
- La función de controladores FIPS está habilitada. Todas las unidades y nodos deben ser compatibles con FIPS y el cifrado en reposo debe estar habilitado para poder habilitar la función de unidad FIPS.

Habilitar el cifrado en reposo

Puede habilitar y deshabilitar el cifrado en reposo para todo el clúster. Esta función no está habilitada de forma predeterminada. Para admitir unidades FIPS, debe habilitar el cifrado en reposo.

1. En la interfaz de usuario del software NetApp Element , haga clic en **Clúster** > **Configuración**.
2. Haga clic en **Habilitar cifrado en reposo**.

Encuentra más información

- Habilitar y deshabilitar el cifrado para un clúster
- "Documentación del software SolidFire y Element"

- "Plugin de NetApp Element para vCenter Server"

Identificar si los nodos están listos para la función de controladores FIPS

Debe comprobar si todos los nodos del clúster de almacenamiento están preparados para admitir unidades FIPS utilizando el método de la API GetFipsReport del software NetApp Element .

El informe resultante muestra uno de los siguientes estados:

- Ninguno: El nodo no es compatible con la función de unidades FIPS.
- Parcial: El nodo es compatible con FIPS, pero no todas las unidades son compatibles con FIPS.
- Listo: El nodo es compatible con FIPS y todas las unidades son unidades FIPS o no hay unidades presentes.

Pasos

1. Utilizando la API de Element, compruebe si los nodos y las unidades del clúster de almacenamiento son compatibles con unidades FIPS introduciendo el siguiente comando:

   ```
   GetFipsReport
   ```

2. Revise los resultados y observe si algún nodo no mostró el estado "Listo".
3. Para cualquier nodo que no muestre el estado Listo, compruebe si la unidad es compatible con la función de unidades FIPS:
   - Utilizando la API de Element, ingrese: `GetHardwareList`
   - Tenga en cuenta el valor de **DriveEncryptionCapabilityType**. Si es "fips", el hardware puede admitir la función de controladores FIPS.

     Ver detalles sobre `GetFipsReport` o `ListDriveHardware` en el "Referencia de la API de elementos".
4. Si la unidad no admite la función de unidades FIPS, reemplace el hardware con hardware FIPS (ya sea el nodo o las unidades).

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Habilitar la función de controladores FIPS

Puede habilitar la función de unidades FIPS mediante el software NetApp Element . `EnableFeature` Método API.

El cifrado en reposo debe estar habilitado en el clúster y todos los nodos y unidades deben ser compatibles con FIPS, como se indica cuando GetFipsReport muestra un estado Listo para todos los nodos.

Paso

1. Utilizando la API de Element, habilite FIPS en todas las unidades introduciendo:

```
EnableFeature params: FipsDrives
```

Encuentra más información

- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Compruebe el estado de la unidad FIPS

Puede comprobar si la función de unidades FIPS está habilitada en el clúster mediante el software NetApp Element . `GetFeatureStatus` Método API que muestra si el estado de activación de las unidades FIPS es verdadero o falso.

1. Utilizando la API de Element, compruebe la función de unidades FIPS en el clúster introduciendo:

   `GetFeatureStatus`

2. Revisar los resultados de `GetFeatureStatus` Llamada a la API. Si el valor de FIPS Drives enabled es True, la función FIPS drives está habilitada.

   ```
   {"enabled": true,
   "feature": "FipsDrives"
   }
   ```

Encuentra más información

- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Solucionar problemas de la función de la unidad FIPS

Mediante la interfaz de usuario del software NetApp Element , puede ver alertas con información sobre fallos del clúster o errores del sistema relacionados con la función de unidades FIPS.

1. Utilizando la interfaz de usuario de Element, seleccione **Informes** > **Alertas**.
2. Busque fallos en el clúster, incluidos los siguientes:
   - Las unidades FIPS no coinciden
   - FIPS genera incumplimiento
3. Para obtener sugerencias de resolución, consulte la información sobre el código de error del clúster.

Encuentra más información

- Códigos de falla del clúster
- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Establecer una comunicación segura

Habilite FIPS 140-2 para HTTPS en su clúster.

Puede utilizar el método API EnableFeature para habilitar el modo de funcionamiento FIPS 140-2 para comunicaciones HTTPS.

Con el software NetApp Element , puede optar por habilitar el modo de funcionamiento de los Estándares Federales de Procesamiento de Información (FIPS) 140-2 en su clúster. Habilitar este modo activa el Módulo de Seguridad Criptográfica de NetApp (NCSM) y aprovecha el cifrado certificado FIPS 140-2 Nivel 1 para todas las comunicaciones a través de HTTPS con la interfaz de usuario y la API de NetApp Element .

> Una vez habilitado el modo FIPS 140-2, no se puede deshabilitar. Cuando se habilita el modo FIPS 140-2, cada nodo del clúster se reinicia y ejecuta una autocomprobación para garantizar que el NCSM esté correctamente habilitado y funcionando en el modo certificado FIPS 140-2. Esto provoca una interrupción tanto en las conexiones de gestión como en las de almacenamiento del clúster. Debe planificar cuidadosamente y habilitar este modo solo si su entorno necesita el mecanismo de cifrado que ofrece.

Para obtener más información, consulte la información de la API de Element.

El siguiente es un ejemplo de la solicitud a la API para habilitar FIPS:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

Una vez habilitado este modo de funcionamiento, todas las comunicaciones HTTPS utilizan los cifrados aprobados por FIPS 140-2.

Encuentra más información

- cifrados SSL
- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

cifrados SSL

Los cifrados SSL son algoritmos de cifrado utilizados por los hosts para establecer una comunicación segura. Existen cifrados estándar que admite el software Element y cifrados no estándar cuando está habilitado el modo FIPS 140-2.

Las siguientes listas proporcionan los cifrados SSL (Secure Socket Layer) estándar compatibles con el software Element y los cifrados SSL compatibles cuando el modo FIPS 140-2 está habilitado:

- **FIPS 140-2 desactivado**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

  TLS_ECDHE_RSA_CON_AES_128_CBC_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_CON_AES_256_CBC_SHA384 (secp256r1) - A

  TLS_ECDHE_RSA_CON_AES_256_GCM_SHA384 (secp256r1) - A

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

  TLS_RSA_CON_AES_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_CON_AES_128_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_CON_AES_128_GCM_SHA256 (rsa 2048) - A

  TLS_RSA_CON_AES_256_CBC_SHA (rsa 2048) - A

  TLS_RSA_CON_AES_256_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_CON_AES_256_GCM_SHA384 (rsa 2048) - A

  TLS_RSA_CON_CAMELLIA_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_CON_CAMELLIA_256_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C

  TLS_RSA_CON_RC4_128_SHA (rsa 2048) - C

  TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A

- **FIPS 140-2 habilitado**

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

TLS_ECDHE_RSA_CON_AES_128_CBC_SHA256 (sección 571r1) - A

TLS_ECDHE_RSA_CON_AES_128_CBC_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256 (sect571r1) - A

TLS_ECDHE_RSA_CON_AES_256_CBC_SHA384 (sección 571r1) - A

TLS_ECDHE_RSA_CON_AES_256_CBC_SHA384 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_256_GCM_SHA384 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_256_GCM_SHA384 (sección 571r1) - A

TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

TLS_RSA_CON_AES_128_CBC_SHA (rsa 2048) - A

TLS_RSA_CON_AES_128_CBC_SHA256 (rsa 2048) - A

TLS_RSA_CON_AES_128_GCM_SHA256 (rsa 2048) - A

TLS_RSA_CON_AES_256_CBC_SHA (rsa 2048) - A

TLS_RSA_CON_AES_256_CBC_SHA256 (rsa 2048) - A

TLS_RSA_CON_AES_256_GCM_SHA384 (rsa 2048) - A

Encuentra más información

Habilite FIPS 140-2 para HTTPS en su clúster.

Comience con la administración de claves externas

Comience con la administración de claves externas

La gestión de claves externas (EKM) proporciona una gestión segura de claves de autenticación (AK) junto con un servidor de claves externas fuera del clúster (EKS). Las AK se utilizan para bloquear y desbloquear unidades de autocifrado (SED) cuando"cifrado en reposo" está habilitado en el clúster. El EKS proporciona generación y almacenamiento seguros de los AK. El clúster utiliza el protocolo de interoperabilidad de gestión de claves (KMIP), un protocolo estándar definido por OASIS, para comunicarse con el EKS.

- "Establecer la gestión externa"
- "Rekey cifrado de software en reposo clave maestra"
- "Recuperar claves de autenticación inaccesibles o no válidas"
- "Comandos de la API de administración de claves externas"

Encuentra más información

- "API CreateCluster que se puede usar para habilitar el cifrado de software en reposo"
- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Configurar la gestión de claves externas

Puedes seguir estos pasos y usar los métodos de la API de Element que se enumeran para configurar tu función de administración de claves externas.

Lo que necesitarás

- Si está configurando la administración de claves externas en combinación con el cifrado de software en reposo, habrá habilitado el cifrado de software en reposo mediante el uso de"CrearClúster" método en un nuevo clúster que no contiene volúmenes.

Pasos

1. Establecer una relación de confianza con el servidor de claves externo (EKS).
   a. Cree un par de claves pública/privada para el clúster de Element que se utiliza para establecer una relación de confianza con el servidor de claves llamando al siguiente método de la API:"Crear par de claves públicas y privadas"
   b. Obtenga la solicitud de firma de certificado (CSR) que la Autoridad de Certificación necesita firmar. La CSR permite al servidor de claves verificar que el clúster de Element que accederá a las claves esté autenticado como tal. Llama al siguiente método de la API:"Solicitud de firma de certificado de cliente"
   c. Utilice la EKS/Autoridad de Certificación para firmar la CSR recuperada. Consulte la documentación de terceros para obtener más información.
2. Cree un servidor y un proveedor en el clúster para comunicarse con EKS. Un proveedor de claves define dónde se debe obtener una clave, y un servidor define los atributos específicos del EKS con el que se comunicará.
   a. Cree un proveedor de claves donde residirán los detalles del servidor de claves llamando al siguiente método de la API:"CrearKeyProviderKmip"
   b. Cree un servidor de claves que proporcione el certificado firmado y el certificado de clave pública de la Autoridad de Certificación llamando a los siguientes métodos de la API:"CrearKeyServerKmip" "Servidor de claves de prueba Kmip"

      Si la prueba falla, verifique la conectividad y la configuración de su servidor. Luego, repita la prueba.

   c. Agregue el servidor de claves al contenedor del proveedor de claves llamando a los siguientes métodos de la API:"Agregar servidor de claves al proveedor Kmip" "TestKeyProviderKmip"

      Si la prueba falla, verifique la conectividad y la configuración de su servidor. Luego, repita la prueba.
3. Como siguiente paso para el cifrado en reposo, realice una de las siguientes acciones:

a. (Para cifrado de hardware en reposo) Habilitar"Cifrado de hardware en reposo" proporcionando el ID del proveedor de claves que contiene el servidor de claves utilizado para almacenar las claves mediante una llamada a"Habilitar cifrado en reposo" Método API.

> Debe habilitar el cifrado en reposo a través de"API" . Habilitar el cifrado en reposo mediante el botón existente de la interfaz de usuario de Element hará que la función vuelva a utilizar claves generadas internamente.

b. (Para el cifrado de software en reposo) Para"Cifrado de software en reposo" Para utilizar el proveedor de claves recién creado, pase el ID del proveedor de claves al"Clave maestra de cifrado de software en reposo" Método API.

Encuentra más información

- "Habilitar y deshabilitar el cifrado para un clúster"
- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Rekey cifrado de software en reposo clave maestra

Puedes usar la API de Element para volver a generar una clave existente. Este proceso crea una nueva clave maestra de reemplazo para su servidor de administración de claves externo. Las claves maestras siempre se reemplazan por nuevas claves maestras y nunca se duplican ni se sobrescriben.

Es posible que necesite volver a introducir las teclas como parte de uno de los siguientes procedimientos:

- Cree una nueva clave como parte de un cambio de gestión de claves interna a gestión de claves externa.
- Cree una nueva clave como reacción a un evento relacionado con la seguridad o como protección contra el mismo.

> Este proceso es asíncrono y devuelve una respuesta antes de que se complete la operación de reenvío de claves. Puedes usar el"ObtenerResultadoAsíncrono" Método para consultar al sistema y comprobar cuándo ha finalizado el proceso.

Lo que necesitarás

- Has habilitado el cifrado de software en reposo mediante"CrearClúster" método en un nuevo clúster que no contiene volúmenes y no tiene E/S. Utilice el siguiente enlace: ../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] para confirmar que el estado es `enabled` antes de continuar.
- Tienes"Se estableció una relación de confianza" entre el clúster SolidFire y un servidor de claves externo (EKS). Ejecutar el"TestKeyProviderKmip" Método para verificar que se ha establecido una conexión con el proveedor de claves.

Pasos

1. Ejecutar el"Proveedores de claves de lista Kmip" comando y copia del ID del proveedor de claves(`keyProviderID`).
2. Ejecutar el"Clave maestra de cifrado de software en reposo" con el `keyManagementType` parámetro como `external` y `keyProviderID` como el número de identificación del proveedor de claves del paso

anterior:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. Copia el `asyncHandle` valor de la `RekeySoftwareEncryptionAtRestMasterKey` Respuesta al comando.
4. Ejecutar el"ObtenerResultadoAsíncrono" comando con el `asyncHandle` Valor del paso anterior para confirmar el cambio de configuración. En la respuesta del comando, debería ver que la configuración de la clave maestra anterior se ha actualizado con la nueva información de la clave. Copie el nuevo ID del proveedor de claves para usarlo en un paso posterior.

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. Ejecutar el `GetSoftwareEncryptionatRestInfo` orden para confirmar que los nuevos detalles clave, incluyendo el `keyProviderID` , han sido actualizados.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Encuentra más información

- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Recuperar claves de autenticación inaccesibles o no válidas

Ocasionalmente, puede producirse un error que requiere la intervención del usuario. En caso de error, se generará un fallo de clúster (denominado código de fallo de clúster). Aquí se describen los dos casos más probables.

El clúster no puede desbloquear las unidades debido a un fallo de clúster KmipServerFault.

Esto puede ocurrir cuando el clúster se inicia por primera vez y el servidor de claves es inaccesible o la clave requerida no está disponible.

1. Siga los pasos de recuperación indicados en los códigos de error del clúster (si los hay).

Es posible que se establezca un fallo sliceServiceUnhealthy porque las unidades de metadatos se han marcado como fallidas y se han colocado en el estado "Disponible".

Pasos para despejar:

1. Vuelva a agregar las unidades.
2. Después de 3 a 4 minutos, compruebe que el `sliceServiceUnhealthy` La avería se ha solucionado.

Ver"códigos de falla del clúster" Para más información.

Comandos de la API de administración de claves externas

Lista de todas las API disponibles para gestionar y configurar EKM.

Se utiliza para establecer una relación de confianza entre el clúster y los servidores externos propiedad del cliente:

- Crear par de claves públicas y privadas
- Solicitud de firma de certificado de cliente

Se utiliza para definir los detalles específicos de los servidores externos propiedad del cliente:

- CrearKeyServerKmip
- ModificarKeyServerKmip
- EliminarKeyServerKmip
- ObtenerKeyServerKmip
- Lista de servidores clave Kmip
- Servidor de claves de prueba Kmip

Se utiliza para crear y mantener proveedores de claves que gestionan servidores de claves externos:

- CrearKeyProviderKmip
- EliminarKeyProviderKmip
- Agregar servidor de claves al proveedor Kmip
- Eliminar servidor de claves del proveedor Kmip
- ObtenerProveedorDeClavesKmip
- Proveedores de claves de lista Kmip
- Clave maestra de cifrado de software en reposo
- TestKeyProviderKmip

Para obtener información sobre los métodos de la API, consulte "Información de referencia de la API".

Información de copyright

Copyright © 2025 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 INTERRUPCIÓN 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.