Gestione su sistema

Element Software

NetApp
April 17, 2024

Tabla de contenidos

Gestione su sistema

Puede gestionar el sistema en la interfaz de usuario de Element. Esto incluye habilitar la autenticación multifactor, gestionar la configuración de clústeres, admitir estándares de procesamiento de información federal (FIPS) y el uso de gestión de claves externa.

- "Habilite la autenticación multifactor"
- "Configure las opciones del clúster"
- "Cree un clúster que admita unidades FIPS"
- "Comience con la gestión de claves externas"

Si quiere más información

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

Habilite la autenticación multifactor

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

Configure la autenticación de múltiples factores

Es posible usar estos pasos básicos a través de la API de Element para configurar el clúster con el fin de utilizar la autenticación multifactor.

Puede encontrar más detalles de cada método de API en la "Referencia de la API de Element".

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

   Los metadatos de IDP, en formato de texto sin formato, se recuperan del IDP de terceros. Estos metadatos se deben validar para asegurarse de que están formateados correctamente en JSON. Hay numerosas aplicaciones de formateador JSON disponibles que puede utilizar, por ejemplo:https://freeformatter.com/json-escape.html.

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

   SpMetadataUrl es una URL que se utiliza para recuperar metadatos del proveedor de servicios del clúster para el IDP con el fin de establecer una relación de confianza.

3. Configure las afirmaciones SAML en el IDP de terceros para incluir el atributo "'NameID'" para identificar de forma exclusiva a un usuario para el registro de auditorías y para que Single Logout funcione

correctamente.

4. Cree una o varias cuentas de usuario administrador del clúster autenticadas por un IDP de terceros para su autorización, llamando al siguiente método API:`AddIdpClusterAdmin`

> El nombre de usuario del administrador del clúster IDP debe coincidir con el mapa de nombre/valor del atributo SAML del 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.
   - Group=cluster-Administrator: Donde el IDP está configurado para liberar una propiedad de grupo en la que todos los usuarios deberían tener acceso. Tenga en cuenta que el emparejamiento nombre/valor del atributo SAML distingue mayúsculas y minúsculas por motivos de seguridad.

5. Habilite la MFA para el clúster llamando al siguiente método API: `EnableIdpAuthentication`

Obtenga más información

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

Información adicional para la autenticación multifactor

Debe conocer las siguientes advertencias en relación con la autenticación de múltiples factores.

- Para actualizar los certificados de IDP que ya no son válidos, deberá usar un usuario administrador no IDP para llamar al siguiente método API: `UpdateIdpConfiguration`
- La MFA es incompatible con certificados con una longitud inferior a 2048 bits. De manera predeterminada, se crea un certificado SSL de 2048 bits en el clúster. Debe evitar establecer un certificado de menor tamaño cuando llame al método de API: `SetSSLCertificate`

> Si el clúster utiliza un certificado que sea inferior a 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 una versión posterior.

- Los usuarios del administrador de IDP no pueden utilizarse para realizar llamadas de API directamente (por ejemplo, mediante SDK o Postman) o para otras integraciones (por ejemplo, OpenStack Cinder o el complemento vCenter). Si necesita crear usuarios que tengan estas capacidades, añada usuarios bien al administrador del clúster LDAP o usuarios de administrador del clúster local.

Obtenga más información

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

Configure las opciones del clúster

Es posible ver y modificar la configuración de todo el clúster y realizar tareas específicas del clúster en la pestaña Cluster de la interfaz de usuario de Element.

Puede configurar ajustes como el umbral de ocupación del clúster, el acceso de soporte, el cifrado en reposo, los volúmenes virtuales, SnapMirror, Y el cliente de retransmisión NTP.

Opciones

- Trabaje con volúmenes virtuales
- Use la replicación de SnapMirror entre clústeres de Element y ONTAP
- Establezca el umbral de ocupación del clúster
- Habilite y deshabilite el acceso al soporte
- "Cómo se calculan los umbrales de blockSpace para el elemento"
- Habilite y deshabilite el cifrado de un clúster
- Gestione el banner de las condiciones de uso
- Configure los servidores de protocolo de tiempo de red para que el clúster consulte
- Gestionar SNMP
- Gestionar unidades
- Gestione los nodos
- Gestionar redes virtuales
- Ver detalles de los puertos Fibre Channel

Obtenga más información

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

Habilite y deshabilite el cifrado en reposo para un clúster

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

Puede habilitar el cifrado de hardware en reposo mediante la interfaz de usuario o la API de Element. La habilitación de la función de cifrado de hardware en reposo no afecta al rendimiento o la eficiencia del clúster. Puede habilitar el cifrado de software en reposo únicamente mediante la API de Element.

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

> En los clústeres de almacenamiento all-flash de SolidFire, el cifrado del software en reposo debe habilitarse durante la creación del clúster y no se puede deshabilitar una vez que se ha creado el clúster.

Lo que necesitará

- Tiene privilegios de administrador de clúster para habilitar o modificar la configuración de cifrado.
- Para el cifrado basado en hardware en reposo, se ha asegurado de que el clúster está en estado correcto antes de cambiar la configuración de cifrado.
- Si va a deshabilitar el cifrado, debe haber dos nodos participando en un clúster para acceder a la clave para deshabilitar el cifrado en una unidad.

Comprobar el cifrado en estado de reposo

Para ver el estado actual del cifrado en reposo y/o el cifrado de software en reposo en el clúster, use el "GetClusterInfo" método. Puede utilizar el "GetSoftwareEncryptionAtRestInfo" método para obtener información que utiliza el clúster para cifrar datos en reposo.

> La consola de interfaz de usuario del software Element en `https://<MVIP>/` actualmente, solo muestra el cifrado en estado de reposo para el cifrado basado en hardware.

Opciones

- Habilite el cifrado basado en hardware en reposo
- Habilite el cifrado basado en software en reposo
- Deshabilite el cifrado basado en hardware en reposo

Habilite el cifrado basado en hardware en reposo

> Para habilitar el cifrado en reposo mediante una configuración de gestión de claves externa, debe habilitar el cifrado en reposo a través de la "API". Al habilitar el uso del botón existente de la interfaz de usuario de Element, se revierten al uso de claves generadas internamente.

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

Habilite el cifrado basado en software en reposo

> El cifrado de software en reposo no se puede deshabilitar una vez que se habilita en el clúster.

1. Durante la creación del clúster, ejecute el "cree el método de clúster" con `enableSoftwareEncryptionAtRest` establezca en `true`.

Deshabilite el cifrado basado en hardware en reposo

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

Obtenga más información

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

Establezca el umbral de ocupación del clúster

Puede cambiar el nivel en el que el sistema genera una advertencia de ocupación de la capacidad del clúster de bloques mediante los pasos siguientes. Además, puede utilizar el método API ModifyClusterFullThreshold para cambiar el nivel en el que el sistema genera una advertencia de bloque o metadatos.

Lo que necesitará

Debe tener privilegios de administrador del clúster.

Pasos

1. Haga clic en **Cluster** > **Settings**.
2. En la sección Cluster Full Settings, introduzca un porcentaje en **Raise a warning alert when _% capacity remains before Helix could not recover from a node failure**.
3. Haga clic en **Guardar cambios**.

Obtenga más información

"Cómo se calculan los umbrales de blockSpace para el elemento"

Habilite y deshabilite el acceso al soporte

Es posible habilitar el acceso de soporte para permitir temporalmente el acceso del personal de soporte de NetApp a los nodos de almacenamiento a través de SSH para solucionar problemas.

Para modificar el acceso al soporte, debe tener privilegios de administrador de clúster.

1. Haga clic en **Cluster** > **Settings**.
2. En la sección Habilitar/deshabilitar acceso de soporte, introduzca la duración (en horas) que desea permitir que el soporte tenga acceso.
3. Haga clic en **Activar acceso de soporte**.
4. **Opcional:** para desactivar el acceso al soporte técnico, haga clic en **Desactivar acceso al soporte técnico**.

Gestione el banner de las condiciones de uso

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

Opciones

Habilite el banner de las condiciones de uso Edite el banner con las condiciones de uso Deshabilite el banner con las condiciones de uso

Habilite el banner de las condiciones de uso

Si lo desea, se puede habilitar un banner con las condiciones de uso que aparece cuando un usuario inicia 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 haya configurado para el clúster. El banner se puede descartar cuando desee.

Para poder habilitar la funcionalidad de las condiciones de uso, debe tener privilegios de administrador del clúster.

1. Haga clic en **usuarios** > **Términos de uso**.
2. En el formulario **Términos de uso**, introduzca el texto que desea que aparezca en el cuadro de diálogo Términos de uso.

   No supere los 4096 caracteres.

3. Haga clic en **Activar**.

Edite el banner con las condiciones de uso

Se puede editar el texto que ven los usuarios cuando seleccionan el banner de inicio de sesión de las condiciones de uso.

Lo que necesitará

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

Pasos

1. Haga clic en **usuarios** > **Términos de uso**.
2. En el cuadro de diálogo **Términos de uso**, edite el texto que desea que aparezca.

   No supere los 4096 caracteres.

3. Haga clic en **Guardar cambios**.

Deshabilite el banner con las condiciones de uso

El banner con las condiciones de uso se puede deshabilitar. Cuando se deshabilita el banner, se deja de solicitar al usuario que acepte las condiciones de uso cuando se usa la interfaz de usuario de Element.

Lo que necesitará

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

Pasos

1. Haga clic en **usuarios** > **Términos de uso**.
2. Haga clic en **Desactivar**.

Establezca el protocolo de hora de red

La configuración del protocolo de tiempo de redes (NTP) se puede lograr de dos maneras: Indique a cada nodo de un clúster que escuche las difusiones o indique a cada nodo que consulte un servidor NTP para obtener actualizaciones.

El NTP se utiliza para sincronizar los relojes que hay en toda una red. La conexión con un servidor NTP interno o externo debe formar parte de la configuración inicial del clúster.

Configure los servidores de protocolo de tiempo de red para que el clúster consulte

Puede indicar a cada nodo de un clúster que consulte un servidor de protocolo de tiempo de redes (NTP) en busca de actualizaciones. El clúster solo contacta con los servidores configurados y solicita información NTP de ellos.

Configure el NTP en el clúster para que apunte a un servidor NTP local. Es posible usar la dirección IP o el nombre de host FQDN. El servidor NTP predeterminado en el momento de crear el clúster se establece en us.pool.ntp.org; sin embargo, no siempre es posible establecer una conexión con este sitio en función de la ubicación física del clúster de SolidFire.

El uso del FQDN depende de si la configuración de DNS del nodo de almacenamiento individual está en su lugar y operativa. Para ello, revise la página requisitos de puerto de red para configurar los servidores DNS en cada nodo de almacenamiento y asegúrese de que los puertos estén abiertos.

Es posible introducir hasta cinco servidores NTP distintos.

> Es posible usar tanto direcciones IPv4 como IPv6.

Lo que necesitará

Para poder configurar esta opción, debe tener privilegios de administrador del clúster.

Pasos

1. Configure una lista de IP y/o FQDN en la configuración del servidor.
2. Compruebe que DNS se haya configurado correctamente en los nodos.
3. Haga clic en **Cluster** > **Settings**.
4. En Configuración del protocolo de tiempo de redes, seleccione **no**, que utiliza la configuración NTP estándar.
5. Haga clic en **Guardar cambios**.

Obtenga más información

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

Configure el clúster para que escuche las transmisiones NTP

Con el modo de retransmisión, puede ordenar a cada nodo de un clúster que escuche en la red de mensajes de retransmisión de protocolo de tiempo de redes (NTP) de un servidor determinado.

Lo que necesitará

- Para poder configurar esta opción, debe tener privilegios de administrador del clúster.
- Debe configurar un servidor NTP en la red como servidor de retransmisión.

Pasos

1. Haga clic en **Cluster** > **Settings**.
2. Introduzca en la lista de servidores el servidor NTP o los servidores que utilizan el modo de retransmisión.

3. En Configuración del protocolo de tiempo de redes, seleccione **Sí** para utilizar un cliente de difusión.
4. Para establecer el cliente de difusión, en el campo **servidor**, introduzca el servidor NTP configurado en modo de difusión.
5. Haga clic en **Guardar cambios**.

Obtenga más información

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

Gestionar SNMP

Puede configurar el protocolo simple de gestión de redes (SNMP) en el clúster.

Puede seleccionar un solicitante SNMP, seleccionar la versión de SNMP que desea usar, identificar el usuario de modelo de seguridad basado en usuario de SNMP (USM) y configurar las capturas para supervisar el clúster de SolidFire. También permite ver y acceder a los archivos de base de información de gestión.

> Es posible usar tanto direcciones IPv4 como IPv6.

Detalles de SNMP

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

- **MIB SNMP**

  Los archivos MIB que hay disponibles para que pueda verlos o descargarlos.

- **Configuración general de SNMP**

  Es posible habilitar o deshabilitar SNMP. Después de habilitar SNMP, puede elegir qué versión quiere usar. Si utiliza la versión 2, puede añadir solicitantes y, si usa la versión 3, puede configurar usuarios USM.

- **Configuración de la captura SNMP**

  Puede identificar los retos que quiere recibir. Puede establecer el host, el puerto y la cadena de comunidad para cada destinatario de reto.

Configure un solicitante SNMP

Cuando se habilita la versión 2 de SNMP, puede habilitar o deshabilitar un solicitante, así como configurar solicitantes para que reciban solicitudes SNMP autorizadas.

1. Haga clic en MENU:Cluster[SNMP].
2. En **Configuración general de SNMP**, haga clic en **Sí** para activar SNMP.
3. En la lista **Versión**, seleccione **Versión 2**.
4. En la sección **Requestors**, introduzca la información **Community String** y **Network**.

De forma predeterminada, la cadena de comunidad es public y la red es localhost. No obstante, puede cambiar estas opciones predeterminadas si lo necesita.

5. **Opcional:** para añadir otro solicitante, haga clic en **Añadir un solicitante** e introduzca la información **cadena de comunidad** y **Red**.
6. Haga clic en **Guardar cambios**.

Obtenga más información

- Configurar las capturas SNMP
- Se pueden ver los datos de objetos gestionados mediante los archivos de base de información de gestión

Configure un usuario USM en SNMP

Al habilitar la versión 3 de SNMP, tendrá que configurar un usuario USM para que reciba las solicitudes de SNMP autorizadas.

1. Haga clic en **Cluster** > **SNMP**.
2. En **Configuración general de SNMP**, haga clic en **Sí** para activar SNMP.
3. En la lista **Versión**, seleccione **Versión 3**.
4. En la sección **usuarios USM**, introduzca el nombre, la contraseña y la contraseña.
5. **Opcional:** para añadir otro usuario USM, haga clic en **Añadir usuario USM** e introduzca el nombre, la contraseña y la frase de paso.
6. Haga clic en **Guardar cambios**.

Configurar las capturas SNMP

Los administradores del sistema pueden utilizar capturas SNMP, también denominadas notificaciones, para supervisar el estado del clúster de SolidFire.

Cuando se habilitan los retos SNMP, el clúster de SolidFire genera retos asociados con las entradas del registro de eventos y las alertas del sistema. Para recibir notificaciones SNMP, tiene que elegir los retos que se tendrían que generar e identificar los destinatarios de la información del reto. De forma predeterminada, no se genera ningún reto.

1. Haga clic en **Cluster** > **SNMP**.
2. Seleccione uno o varios tipos de solapamientos en la sección **Configuración de solapamientos SNMP** que el sistema debe generar:
   - Retos de fallo de clúster
   - Retos de fallo resueltos del clúster
   - Retos de evento de clúster
3. En la sección **destinatarios de la captura**, introduzca la información de host, puerto y cadena de comunidad para un destinatario.
4. **Opcional**: Para agregar otro destinatario de captura, haga clic en **Agregar un destinatario de captura** e introduzca la información de host, puerto y cadena de comunidad.
5. Haga clic en **Guardar cambios**.

Se pueden ver los datos de objetos gestionados mediante los archivos de base de información de gestión

Es posible ver y descargar los archivos de la base de datos de información de administración (MIB) que se usan para definir cada uno de los objetos gestionados. La función SNMP admite el acceso de solo lectura a los objetos que se definen en SolidFire-StorageCluster-MIB.

Los datos estadísticos que se proporcionan en el archivo MIB muestran la actividad del sistema en relación a lo siguiente:

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

El sistema también permite acceder al archivo MIB que contenga los puntos de acceso del nivel superior (OIDS) a los productos SF-Series.

Pasos

1. Haga clic en **Cluster** > **SNMP**.
2. En **MIB de SNMP**, haga clic en el archivo MIB que desee descargar.
3. En la ventana de descarga que aparece, abra o guarde el archivo MIB.

Gestionar unidades

Cada nodo contiene una o varias 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 una vez que esta se ha añadido correctamente a un clúster. Es posible usar la interfaz de usuario de Element para gestionar las unidades.

Si quiere más información

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

Detalles de unidades

En la página Drives de la pestaña Cluster, se proporciona una lista de las unidades activas del clúster. La página se puede filtrar si selecciona de las pestañas Active, Available, Removing, Erasing y Failed.

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

Los siguientes elementos se muestran en la lista de unidades activas.

- **ID de unidad**

  El número secuencial asignado a la unidad.

- **ID de nodo**

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

- **Nombre de nodo**

  El nombre del nodo que aloja la unidad.

- **Ranura**

  El número de ranura en la que la unidad se encuentra físicamente.

- **Capacidad**

  El tamaño de la unidad, en GB.

- **Serie**

  El número de serie de la unidad.

- **Desgaste restante**

  El indicador del nivel de desgaste.

  El sistema de almacenamiento informa de la cantidad aproximada de desgaste disponible en cada unidad de estado sólido (SSD) para escribir y borrar datos. Una unidad que ha consumido el 5% de los ciclos de escritura y borrado diseñados informa del 95% de desgaste restante. El sistema no actualiza automáticamente la información de desgaste de la unidad; se puede actualizar o cerrar y volver a cargar la página para actualizar la información.

- **Tipo**

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

Gestione los nodos

Desde la página Nodes de la pestaña Cluster, se pueden gestionar los nodos de almacenamiento SolidFire y Fibre Channel.

Si un nodo que se acaba de añadir supone más del 50 % de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("trenzado"), de modo que cumpla con la regla de capacidad. Este sigue siendo el caso hasta que se añada más almacenamiento. Si se añade un nodo muy grande que también desobedece la regla de capacidad, el nodo que antes se había abandonado ya no se quedará abandonado, mientras el nodo recién añadido se vuelve abandonado. La capacidad debe añadirse siempre por parejas para evitar que esto suceda. Cuando un nodo se queda sin poner en cadena, se produce un error del clúster adecuado.

Obtenga más información

Añada un nodo a un clúster

Añada un nodo a un clúster

Es posible añadir nodos a un clúster cuando se necesita más almacenamiento o después de crear el clúster. Los nodos requieren una configuración inicial cuando se conectan por primera vez. Una vez que se configura, aparece en la lista de nodos pendientes y puede añadirlos a un clúster.

La versión de software de cada nodo en un clúster tiene que ser compatible. Cuando añade un nodo a un clúster, el clúster instala la versión del clúster del software NetApp Element en el nuevo nodo según sea necesario.

Es posible añadir nodos de capacidad inferior o superior a un clúster existente. Es posible añadir capacidades de nodos superiores a un clúster para aumentar su capacidad. Cuando se añaden nodos más grandes a un clúster con nodos más pequeños, debe hacerse en parejas. De este modo se le otorga suficiente espacio para que Double Helix pueda mover los datos en caso de que uno de los nodos superiores presente errores. Es posible añadir capacidades de nodos más pequeños a un clúster de nodos más grandes para mejorar el rendimiento.

> Si un nodo que se acaba de añadir supone más del 50 % de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("trenzado"), de modo que cumpla con la regla de capacidad. Este sigue siendo el caso hasta que se añada más almacenamiento. Si se añade un nodo muy grande que también desobedece la regla de capacidad, el nodo que antes se había abandonado ya no se quedará abandonado, mientras el nodo recién añadido se vuelve abandonado. La capacidad debe añadirse siempre por parejas para evitar que esto suceda. Cuando un nodo se convierte en abandonado, se produce el error del clúster strandedCapacity.

"Vídeo de NetApp: Escale según sus necesidades: Ampliar un clúster de SolidFire"

Puede añadir nodos a dispositivos NetApp HCI.

Pasos

1. Seleccione **Cluster** > **Nodes**.
2. Haga clic en **pendiente** para ver la lista de nodos pendientes.

   Una vez completado el proceso de adición de nodos, aparecen en la lista Active Nodes. Hasta entonces, los nodos pendientes aparecen en la lista Pending Active.

   SolidFire instala la versión del software Element del clúster en los nodos pendientes cuando se añaden a un clúster. Esto puede tardar varios 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 añadir varios nodos, active la casilla de los nodos que desee agregar y, a continuación, **acciones masivas**. **Nota:** Si el nodo que está agregando tiene una versión diferente del software Element que 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 de clústeres. Después de que se actualiza el nodo, se añade automáticamente al clúster. Durante este proceso asíncrono, el nodo tendrá el estado pendingActive.
4. Haga clic en **Agregar**.

   El nodo aparece en la lista de nodos activos.

Obtenga más información

Versiones y compatibilidad de nodos

Versiones y compatibilidad de nodos

La compatibilidad del nodo se basa en la versión del software Element instalada en un nodo. Los clústeres de almacenamiento basados en software Element crean automáticamente la imagen de un nodo en la versión de software Element en el clúster cuando las versiones del nodo y el clúster no son compatibles.

En la siguiente lista, se describen los niveles de importancia de las versiones del software Element que conforman el número de versión del software Element:

- **Mayor**

  El primer número designa una versión de software. No es posible añadir un nodo con un número de componente principal a un clúster que contenga nodos de otro número de revisión principal ni se puede crear un clúster con nodos de versiones principales mixtas.

- **Menor**

  El segundo número designa mejoras o funciones de software más pequeñas que se aplican en funciones de software existentes que se han incorporado a una versión principal. Este componente aumenta dentro de un componente de versión principal para indicar que esta versión incremental no es compatible con otras versiones incrementales del software Element con un componente secundario distinto. Por ejemplo, 11.0 no es compatible con 11.1 y 11.1 no es compatible con 11.2.

- **Micro**

  El tercer número designa una revisión compatible (versión incremental) con la versión de software Element que representan los componentes principal.secundario. Por ejemplo, 11.0.1 es compatible con 11.0.2 y 11.0 es compatible con 11.0.3.

Los números de versión principal y secundario deben coincidir para ser compatibles. Los números micro no tienen que coincidir para ser compatibles.

Capacidad de clúster en un entorno de nodos mixtos

En un clúster se pueden combinar distintos tipos de nodos. SF-Series 2405, 3010, 4805, 6010, 9605 9010, 19210, 38410 y H-Series pueden coexistir en un clúster.

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

Es mejor no mezclar nodos no cifrados y no cifrados. En un clúster de nodos mixtos, ningún nodo puede superar el 33 % de la capacidad total del clúster. Por ejemplo, en un clúster con cuatro nodos SF-Series 4805, el nodo más grande que se puede añadir solo es un nodo SF-Series 9605. El umbral de capacidad del clúster se calcula en función de la pérdida potencial del nodo más grande en esta situación.

Según la versión del software Element, los siguientes nodos de almacenamiento SF-Series no son compatibles:

Empezando por…	Nodo de almacenamiento no compatible…
Elemento 12.7	• SF2405 • SF9608
Elemento 12.0	• SF3010 • SF6010 • SF9010

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

Ver los detalles del nodo

Puede ver detalles de nodos individuales, como etiquetas de servicio, detalles de unidades y gráficos para la utilización y estadísticas de unidades. La página Nodes de la pestaña Cluster proporciona la columna Version donde puede ver la versión de software de cada nodo.

Pasos

1. Haga clic en **Cluster** > **Nodes**.
2. Para ver los detalles de un nodo específico, haga clic en el icono **acciones** de un nodo.
3. Haga clic en **Ver detalles**.
4. Revise los detalles del nodo:
    - **ID de nodo**: El ID generado por el sistema para el nodo.
    - **Nombre de nodo**: El nombre de host del nodo.
    - **iops 4k** disponible: IOPS configuradas para el nodo.
    - **Función de nodo**: La función que tiene el nodo en el clúster. Los posibles valores son los siguientes:
        - Cluster Master: El nodo que realiza tareas administrativas para todo el clúster y contiene la MVIP y la SVIP.
        - Ensemble Node: Un nodo que participa en el clúster. Hay nodos de 3 o 5 conjuntos, según el tamaño del clúster.
        - Fibre Channel: Un nodo del clúster.
    - **Tipo de nodo**: Tipo de modelo del nodo.
    - **Active Drives**: Número de unidades activas en el nodo.
    - **IP de administración**: La dirección IP de administración (MIP) asignada al nodo para las tareas de administración de red de 1 GbE o 10 GbE.
    - **IP de clúster**: La dirección IP de clúster (CIP) asignada al nodo utilizado para la comunicación entre nodos del mismo clúster.
    - **IP de almacenamiento**: La dirección IP de almacenamiento (SIP) asignada al nodo utilizado para la detección de redes iSCSI y todo el tráfico de red de datos.
    - **ID de VLAN de administración**: ID virtual para la red de área local de administración.

- **Storage VLAN ID**: El ID virtual de 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 exclusivo asignado al nodo.

Ver detalles de los puertos Fibre Channel

Es posible ver detalles de los puertos Fibre Channel, como el estado, el nombre y la dirección de puerto, desde la página puertos FC.

Permite ver información sobre los puertos Fibre Channel que están conectados al clúster.

Pasos

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

Obtenga más información

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

Gestionar redes virtuales

Las redes virtuales del almacenamiento de SolidFire permiten que el tráfico entre varios clientes en redes lógicas independientes se conecten a un clúster. Las conexiones al clúster se separan en la pila de redes mediante el etiquetado de VLAN.

Obtenga más información

- Añadir una red virtual
- Habilite el enrutamiento y el reenvío virtuales
- Editar una red virtual
- Edite las VLAN de VRF
- Eliminar una red virtual

Añadir una red virtual

Es posible añadir una red virtual nueva a la configuración de un clúster para habilitar una conexión de entorno multi-tenant con un clúster donde se ejecuta el software Element.

Lo que necesitará

- 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 usará como extremo para todo el tráfico de almacenamiento de NetApp Element.

Debe tener en cuenta los siguientes criterios para esta configuración:

- Las VLAN que no están habilitadas para VRF requieren que haya iniciadores en la misma subred que la SVIP.
- Las VLAN que están habilitadas para VRF no requieren que haya iniciadores en la misma subred que la SVIP y el que enrutamiento esté admitido.
- La SVIP predeterminada no requiere que haya iniciadores en la misma subred que la SVIP y el que enrutamiento esté admitido.

Cuando se añade una red virtual, se crea una interfaz para cada nodo y cada una requiere una dirección IP de red virtual. La cantidad de direcciones IP especificada cuando se crea una red virtual nueva debe ser igual o mayor que la cantidad de nodos del clúster. Las direcciones de red virtuales se aprovisionan de forma masiva y se asignan automáticamente a los nodos individuales. No es necesario asignar manualmente direcciones de red virtual 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 valores en los siguientes campos:
    - **Nombre de VLAN**
    - **Etiqueta VLAN**
    - **SVIP**
    - **Netmask**
    - (Opcional) **Descripción**
4. Introduzca la dirección **IP inicial** para el rango de direcciones IP en **IP Address Blocks**.
5. Introduzca el **Tamaño** del intervalo IP como el número de direcciones IP que se incluirán en el bloque.
6. Haga clic en **Agregar un bloque** para agregar un bloque no continuo de direcciones IP para esta VLAN.

7. Haga clic en **Crear VLAN**.

Ver detalles de redes virtuales

Pasos

1. Haga clic en **clúster** > **Red**.
2. Revise los detalles.
   - **ID**: ID exclusivo de la red VLAN, asignada por el sistema.
   - **Nombre**: Nombre exclusivo 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.
   - **Netmask**: Máscara de red para esta red virtual.
   - **Gateway**: Dirección IP única de una puerta de enlace de red virtual. VRF debe estar habilitado.
   - **VRF Enabled**: Indica si el enrutamiento y reenvío virtuales está activado o no.
   - **IP utilizadas**: El rango de direcciones IP de red virtual que se utiliza para la red virtual.

Habilite el enrutamiento y el reenvío virtuales

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

Solo puede habilitar VRF en el momento de crear una VLAN. Si desea volver a un estado sin VRF, debe eliminar y volver a crear la VLAN.

1. Haga clic en **clúster** > **Red**.
2. Para habilitar VRF en una VLAN nueva, seleccione **Crear VLAN**.
   a. Introduzca la información relevante para la nueva VRF/VLAN. Consulte Añadir una red virtual.
   b. Active la casilla de verificación **Activar VRF**.
   c. **Opcional**: Introduzca una puerta de enlace.
3. Haga clic en **Crear VLAN**.

Obtenga más información

Añadir una red virtual

Editar una red virtual

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

Si existe alguna sesión de iSCSI, replicación remota u otras sesiones de red, se podría producir un error en la modificación.

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

- Solo es posible eliminar direcciones IP del rango de direcciones IP iniciales asignado en el momento en que se creó la VLAN.
- Puede eliminar un bloque de direcciones IP que se agregó después del rango de direcciones IP inicial, pero no puede cambiar el tamaño de un bloque IP eliminando las direcciones IP.
- Cuando intenta quitar direcciones IP, ya sea del rango de direcciones IP inicial o de un bloque IP, que están utilizando los nodos en el clúster, la operación puede generar un error.
- No se pueden reasignar direcciones IP específicas en uso a otros nodos del clúster.

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

1. Seleccione **Cluster** > **Red**.
2. Seleccione el icono Actions de la VLAN que quiera 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 continuo de direcciones IP para la red virtual.
6. Seleccione **Guardar cambios**.

Enlace a artículos de la base de conocimientos de solución de problemas

Enlace a los artículos de la base de conocimientos para obtener ayuda sobre la solución de problemas relacionados con la gestión de los intervalos de direcciones IP de VLAN.

- "Duplique la advertencia de IP después de añadir un nodo de almacenamiento en VLAN en el clúster de Element"
- "Cómo determinar a qué IP de VLAN están en uso y a qué nodos están asignados esas IP en Element"

Edite las VLAN de VRF

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

1. Haga clic en **clúster** > **Red**.
2. Haga clic en el icono Actions de la VLAN que quiera editar.
3. Haga clic en **Editar**.
4. Introduzca los nuevos atributos para la VLAN del VRF en el cuadro de diálogo **Editar VLAN**.
5. Haga clic en **Guardar cambios**.

Eliminar una red virtual

Puede eliminar un objeto de red virtual. Debe añadir los bloques de dirección a otra red virtual antes de eliminar una red virtual.

1. Haga clic en **clúster** > **Red**.
2. Haga clic en el icono Actions de la VLAN que desea eliminar.

3. Haga clic en **Eliminar**.
4. Confirme el mensaje.

Obtenga más información

Editar una red virtual

Cree un clúster que admita unidades FIPS

La seguridad cada vez resulta más importante para la puesta en marcha de soluciones en muchos entornos de cliente. Los estándares de procesamiento de información federal (FIPS) son estándares de interoperabilidad y seguridad informática. El cifrado certificado FIPS 140-2 para datos en reposo es un componente de la solución de seguridad general.

- "Evite combinar nodos para unidades FIPS"
- "Habilite el cifrado en reposo"
- "Identifique si los nodos están listos para la función de unidades FIPS"
- "Habilite la función de unidades FIPS"
- "Compruebe el estado de la unidad FIPS"
- "Solucione problemas de la función de unidad FIPS"

Evite combinar nodos para unidades FIPS

Para prepararse para habilitar la función de unidades FIPS, debe evitar combinar nodos donde algunos sean compatibles con unidades FIPS y otros no lo sean.

Un clúster se considera compatible con 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.
- Se habilitó la función de unidades FIPS. Todas las unidades y los nodos deben ser compatibles con FIPS, y el cifrado en reposo debe habilitarse para habilitar la función de unidad FIPS.

Habilite el cifrado en reposo

Puede habilitar y deshabilitar el cifrado en todo el clúster en reposo. Esta función no está habilitada de forma predeterminada. Para admitir las 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 **Activar cifrado en reposo**.

Obtenga más información

- Habilite y deshabilite el cifrado de un clúster

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

Identifique si los nodos están listos para la función de unidades FIPS

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

El informe resultante muestra uno de los siguientes Estados:

- None: El nodo no es compatible con la función de unidades FIPS.
- Parcial: El nodo es compatible con FIPS, pero no todas las unidades son unidades FIPS.
- Ready: El nodo es compatible con FIPS y todas las unidades son unidades FIPS o no existen unidades.

Pasos

1. Con la API de Element, compruebe si los nodos y las unidades del clúster de almacenamiento pueden ver las unidades FIPS introduciendo:

   ```
   GetFipsReport
   ```

2. Revise los resultados y consulte los nodos que no muestran el estado de Ready.
3. En el caso de los nodos que no muestren el estado Listo, compruebe si la unidad es compatible con la función de las unidades FIPS:
   - Utilice la API de Element, introduzca: `GetHardwareList`
   - Observe el valor de **DriveEncryptionCapabilityType**. Si es "fips", el hardware puede admitir la función de unidades FIPS.

     Consulte los detalles acerca de `GetFipsReport` o. `ListDriveHardware` en la "Referencia de la API de Element".
4. Si la unidad no puede admitir la función unidades FIPS, reemplace el hardware con hardware FIPS (nodo o unidades).

Obtenga más información

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

Habilite la función de unidades FIPS

Es posible habilitar la función 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, tal y como se indica cuando GetFipsReport muestra el estado Ready para todos los nodos.

Paso

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

```
EnableFeature params: FipsDrives
```

Obtenga más información

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

Compruebe el estado de la unidad FIPS

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

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

   ```
   GetFeatureStatus
   ```

2. Revise los resultados del `GetFeatureStatus` Llamada a API. Si el valor de unidades FIPS habilitadas es True, se habilita la función de unidades FIPS.

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

Obtenga más información

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

Solucione problemas de la función de unidad FIPS

Con la interfaz de usuario del software NetApp Element, es posible ver alertas sobre errores o errores del clúster en el sistema relacionados con la función de unidades FIPS.

1. Con la interfaz de usuario de Element, seleccione **Informes** > **Alertas**.
2. Busque fallos del clúster, entre los que se incluyen:
   - Las unidades FIPS no coinciden
   - FIPS no cumple las normativas
3. Para obtener sugerencias de resolución, consulte la información sobre el código de avería del clúster.

Obtenga más información

- códigos de error de clúster

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

Habilite FIPS 140-2 para HTTPS en el clúster

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

Con el software NetApp Element, puede optar por habilitar el modo operativo estándar de procesamiento de información federal (FIPS) 140-2 en el clúster. Al habilitar este modo, se activa el módulo de seguridad criptográfica de NetApp (NCSM) y se utiliza el cifrado certificado FIPS 140-2 de nivel 1 para toda la comunicación mediante HTTPS a la interfaz de usuario y la API de NetApp Element.

> Después de habilitar el modo FIPS 140-2-2, no puede deshabilitarse. Cuando se habilita FIPS 140-2-Mode, cada nodo del clúster se reinicia y ejecuta una prueba automática, lo que garantiza que NCSM se habilite correctamente y funcione en el modo certificado FIPS 140-2-2. Esto provoca una interrupción de las conexiones de gestión y almacenamiento en el clúster. Debe planificar con cuidado y activar este modo únicamente si su entorno necesita el mecanismo de cifrado que ofrece.

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

A continuación se muestra un ejemplo de la solicitud de API para habilitar FIPS:

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

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

Obtenga más información

- Cifrados SSL
- "Gestione el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Cifrados SSL

Los cifrados SSL son algoritmos de cifrado que utilizan los hosts para establecer una comunicación segura. Hay cifrados estándar que el software Element admite y no

estándar cuando esté habilitado el modo FIPS 140-2-2.

Las siguientes listas proporcionan los cifrados estándar de capa de socket seguro (SSL) que admite el software Element y los cifrados SSL que se admiten 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_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C

  TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A

  TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A

  TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

  TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_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_WITH_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_WITH_AES_128_CBC_SHA256 (SECT571R1) - A.

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECT571R1) - A.

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECT571R1) - A.

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECT571R1) - A.

TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C

TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

Obtenga más información

Habilite FIPS 140-2 para HTTPS en el clúster

Comience con la gestión de claves externas

La gestión de claves externas (EKM) ofrece gestión de claves de autenticación seguras (AK) en combinación con un servidor de claves externo (EKS) fuera de clúster. El AKS se utiliza para bloquear y desbloquear unidades de cifrado automático (SED) cuando "cifrado en reposo" está habilitado en el clúster. El EKS proporciona una generación y almacenamiento seguros del AKS. El clúster utiliza el protocolo de interoperabilidad de gestión de claves (KMIP, en inglés "Key Management Interoperability Protocol"), un protocolo estándar definido de OASIS para comunicarse con el EKS.

- "Configurar la administración externa"
- "Vuelva a obtener el cifrado de software en la clave maestra de REST"
- "Recuperación de claves de autenticación no válidas o inaccesibles"
- "Comandos de API de gestión de claves externas"

Obtenga más información

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

Configure la gestión de claves externas

Puede seguir estos pasos y usar los métodos API de Element que aparecen para configurar la función de gestión de claves externa.

Lo que necesitará

- Si va a configurar la gestión de claves externas en combinación con el cifrado de software en reposo, debe habilitar el cifrado de software en reposo con el "CreateCluster" 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 público/privado para el clúster de Element que se utilice para establecer una relación de confianza con el servidor de claves llamando al siguiente método de API: "CreatePublicPrivateKeyPair"
   b. Obtenga la solicitud de firma de certificado (CSR) que la entidad de certificación debe firmar. La CSR permite que el servidor de claves verifique que el clúster de Element que tendrá acceso a las claves se autentique como clúster de Element. Llame al siguiente método API: "GetClientCertificateSignRequest"
   c. Utilice la autoridad EKS/Certificate 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 el EKS. Un proveedor de claves define dónde se debe obtener una clave y un servidor define los atributos específicos del EKS con los que se comunicará.
   a. Cree un proveedor de claves en el que residirán los detalles del servidor de claves llamando al siguiente método de API: "CreateKeyProviderKmip"
   b. Cree un servidor de claves que proporcione el certificado firmado y el certificado de clave pública de la entidad emisora de certificados llamando a los siguientes métodos API: "CreateKeyServerKmip" "TestKeyServerKmip"

      Si la prueba falla, verifique la configuración y la conectividad del servidor. A continuación, repita la prueba.

   c. Para agregar el servidor de claves al contenedor de proveedor de claves, llame a los siguientes métodos API:"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

      Si la prueba falla, verifique la configuración y la conectividad del servidor. A continuación, repita la prueba.
3. Realice una de las siguientes acciones como siguiente paso para el cifrado en reposo:
   a. (Para el cifrado de hardware en reposo) Habilitar "cifrado de hardware en reposo" Mediante la identificación del proveedor de claves que contiene el servidor de claves utilizado para almacenar las claves, llame al "EnableEncryptionAtest" Método API.

> Debe habilitar el cifrado en reposo a través del "API". Si se habilita el cifrado en reposo con el botón existente de interfaz de usuario de Element, la función volverá al uso de claves generadas internamente.

b. (Para el cifrado de software en reposo) en orden de "cifrado de software en reposo" Para utilizar el proveedor de claves recién creado, pase el ID de proveedor de claves al "RekeySoftwareEncryptionAtRestMasterKey" Método API.

Obtenga más información

- "Habilite y deshabilite el cifrado de un clúster"
- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Vuelva a obtener el cifrado de software en la clave maestra de REST

Es posible usar la API de Element para volver a introducir una clave existente. Este proceso crea una nueva clave maestra de reemplazo para el servidor de gestión de claves externo. Las claves maestras siempre se sustituyen por claves maestras nuevas y nunca se duplican ni se sobrescriben.

Es posible que deba volver a introducir la clave como parte de uno de los siguientes procedimientos:

- Cree una nueva clave como parte de un cambio de la gestión de claves interna a la gestión de claves externas.
- Cree una nueva clave como reacción o como protección ante un evento relacionado con la seguridad.

> Este proceso es asíncrono y devuelve una respuesta antes de que se complete la operación de reclave. Puede utilizar el "GetAsyncResult" método para sondear el sistema para ver cuándo se ha completado el proceso.

Lo que necesitará

- Habilitó el cifrado de software en reposo mediante el "CreateCluster" Método en un nuevo clúster que no contiene volúmenes y no tiene I/O. Utilice el enlace:../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] para confirmar que el estado es `enabled` antes de continuar.
- Ya tienes "estableció una relación de confianza" Entre el clúster de SolidFire y un servidor de claves externo (EKS). Ejecute el "TestKeyProviderKmip" método para verificar que se ha establecido una conexión con el proveedor de claves.

Pasos

1. Ejecute el "ListKeyProvidersKmip" Y copie el ID del proveedor de claves (`keyProviderID`).
2. Ejecute el "RekeySoftwareEncryptionAtRestMasterKey" con la `keyManagementType` parámetro como `external` y.. `keyProviderID` Como el número de ID del proveedor de claves del paso anterior:

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

3. Copie el `asyncHandle` valor de `RekeySoftwareEncryptionAtRestMasterKey` respuesta del comando.
4. Ejecute el "GetAsyncResult" con el `asyncHandle` valor del paso anterior para confirmar el cambio en la configuración. Desde la respuesta del comando, debe ver que la configuración de la clave maestra anterior se ha actualizado con información de clave nueva. 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. Ejecute el `GetSoftwareEncryptionatRestInfo` comando para confirmar la información de la nueva clave, incluida la `keyProviderID`, se han actualizado.

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

Obtenga más información

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

Recuperación de claves de autenticación no válidas o inaccesibles

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

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

Esto puede suceder cuando el clúster se inicia por primera vez y no se puede acceder al servidor de claves o la clave requerida no está disponible.

1. Siga los pasos de recuperación indicados en los códigos de fallo del clúster (si los hubiera).

Se puede configurar un error slicServiceUnhealthy porque las unidades de metadatos se han marcado como un error y se han colocado en el estado "Available".

Pasos para borrar:

1. Vuelva a añadir las unidades.
2. Después de 3 a 4 minutos, verificar que el `sliceServiceUnhealthy` se borró el error.

Consulte "códigos de error de clúster" si quiere más información.

Comandos de API de gestión de claves externas

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

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

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

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

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

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

- CreateKeyProviderKmip
- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

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