Habilitar la autenticación multifactor

Element Software

NetApp
November 12, 2025

Tabla de contenidos

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"

Información de copyright

Información de la marca comercial