



Habilite la autenticación multifactor

Element Software

NetApp
January 15, 2024

Tabla de contenidos

- Habilite la autenticación multifactor 1
- Configure la autenticación de múltiples factores 1
- Información adicional para la autenticación multifactor 2

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"](#)

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.