



Ativar a autenticação multifator

Element Software

NetApp
November 21, 2024

Índice

- Ativar a autenticação multifator 1
- Configurar a autenticação multifator 1
- Informações adicionais para autenticação multifator 2

Ativar a autenticação multifator

A autenticação multifator (MFA) usa um provedor de identidade (IDP) de terceiros por meio da Security Assertion Markup Language (SAML) para gerenciar sessões de usuários. O MFA permite que os administradores configurem fatores adicionais de autenticação conforme necessário, como senha e mensagem de texto, senha e mensagem de e-mail.

Configurar a autenticação multifator

Você pode usar essas etapas básicas por meio da API Element para configurar seu cluster para usar a autenticação multifator.

Os detalhes de cada método de API podem ser encontrados no ["Referência da API do Element"](#).

1. Crie uma nova configuração de provedor de identidade (IDP) de terceiros para o cluster chamando o seguinte método de API e passando os metadados IDP no formato JSON: `CreateIdpConfiguration`

Os metadados IDP, em formato de texto simples, são recuperados do IDP de terceiros. Esses metadados precisam ser validados para garantir que estejam formatados corretamente em JSON. Existem vários aplicativos de formatador JSON disponíveis que você pode usar, por exemplo: <https://freeformatter.com/json-escape.html>.

2. Recupere metadados de cluster, via `spMetadataUrl`, para copiar para o IDP de terceiros chamando o seguinte método API: `ListIdpConfigurations`

`SpMetadataUrl` é um URL usado para recuperar metadados do provedor de serviços do cluster para o IDP, a fim de estabelecer um relacionamento de confiança.

3. Configure asserções SAML no IDP de terceiros para incluir o atributo `"NameID"` para identificar exclusivamente um usuário para o Registro de auditoria e para que o Logout único funcione corretamente.
4. Crie uma ou mais contas de usuário de administrador de cluster autenticadas por um IDP de terceiros para autorização chamando o seguinte método de API: `AddIdpClusterAdmin`



O nome de usuário do administrador do cluster IDP deve corresponder ao mapeamento de nome/valor do atributo SAML para o efeito desejado, como mostrado nos exemplos a seguir:

- `bob@company.com` — onde o IDP está configurado para liberar um endereço de e-mail nos atributos SAML.
- Administrador de cluster - onde o IDP está configurado para liberar uma propriedade de grupo na qual todos os usuários devem ter acesso. Observe que o pareamento Nome/valor do atributo SAML diferencia maiúsculas de minúsculas para fins de segurança.

5. Ative o MFA para o cluster chamando o seguinte método de API: `EnableIdpAuthentication`

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)

- ["Plug-in do NetApp Element para vCenter Server"](#)

Informações adicionais para autenticação multifator

Você deve estar ciente das seguintes advertências em relação à autenticação multifator.

- Para atualizar os certificados IDP que não são mais válidos, você precisará usar um usuário admin que não seja IDP para chamar o seguinte método de API: `UpdateIdpConfiguration`
- MFA é incompatível com certificados com menos de 2048 bits de comprimento. Por padrão, um certificado SSL de 2048 bits é criado no cluster. Você deve evitar definir um certificado de tamanho menor ao chamar o método API: `SetSSLCertificate`



Se o cluster estiver usando um certificado com menos de 2048 bits de pré-atualização, o certificado do cluster deve ser atualizado com um certificado de 2048 bits ou superior após a atualização para o elemento 12,0 ou posterior.

- Os usuários de administração de IDP não podem ser usados para fazer chamadas de API diretamente (por exemplo, via SDKs ou Postman) ou para outras integrações (por exemplo, OpenStack Cinder ou vCenter Plug-in). Adicione usuários de administrador de cluster LDAP ou usuários de administrador de cluster local se você precisar criar usuários com essas habilidades.

Encontre mais informações

- ["Gerenciamento de storage com a API Element"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.