다중 요소 인증을 사용합니다

Element Software

NetApp
October 01, 2024

목차

다중 요소 인증을 사용합니다 1
다중 요소 인증을 설정합니다 1
다중 요소 인증에 대한 추가 정보 2

다중 요소 인증을 사용합니다

MFA(Multi-factor Authentication)는 SAML(Security Assertion Markup Language)을 통해 타사 ID 공급자(IdP)를 사용하여 사용자 세션을 관리합니다. 관리자는 MFA를 사용하여 암호 및 텍스트 메시지, 암호 및 전자 메일 메시지 등 필요에 따라 추가 인증 요소를 구성할 수 있습니다.

다중 요소 인증을 설정합니다

Element API를 통해 이러한 기본 단계를 사용하여 다중 요소 인증을 사용하도록 클러스터를 설정할 수 있습니다.

각 API 방법에 대한 자세한 내용은 에서 "요소 API 참조입니다"확인할 수 있습니다.

1. 다음 API 메서드를 호출하고 IDP 메타데이터를 JSON 형식으로 전달하여 클러스터에 대한 새로운 타사 IDP(Identity Provider) 구성을 생성합니다. `CreateIdpConfiguration`

   IDP 메타데이터는 일반 텍스트 형식으로 타사 IDP에서 검색됩니다. 이 메타데이터는 JSON으로 올바르게 포맷되었는지 확인하기 위해 유효성을 검증해야 합니다. https://freeformatter.com/json-escape.html.와 같이 사용할 수 있는 JSON 포맷터 응용 프로그램은 매우 다양합니다

2. 다음 API 메서드를 호출하여 spMetadataUrl 을 통해 클러스터 메타데이터를 검색하여 타사 IDP에 복사합니다. `ListIdpConfigurations`

   SpMetadataUrl 은 신뢰 관계를 설정하기 위해 IDP의 클러스터에서 서비스 공급자 메타데이터를 검색하는 데 사용되는 URL입니다.

3. 타사 IDP의 SAML 어설션을 구성하여 감사 로깅을 위한 사용자를 고유하게 식별하고 단일 로그아웃이 제대로 작동하는지 ""NameID"" 속성을 포함시킵니다.
4. 다음 API 메서드를 호출하여 타사 IDP에서 인증을 받은 하나 이상의 클러스터 관리자 사용자 계정을 생성합니다 `.AddIdpClusterAdmin`

   > IDP 클러스터 관리자의 사용자 이름은 다음 예와 같이 원하는 효과에 대한 SAML 속성 이름/값 매핑과 일치해야 합니다.

   - email=bob@company.com — SAML 속성에서 이메일 주소를 해제하도록 IDP가 구성된 경우.
   - group=cluster-administrator - IDP가 모든 사용자가 액세스해야 하는 그룹 속성을 해제하도록 구성되어 있습니다. SAML 속성 이름/값 페어링은 보안을 위해 대/소문자를 구분합니다.
5. 다음 API 메서드를 호출하여 클러스터에 MFA를 사용하도록 설정합니다. `EnableIdpAuthentication`

자세한 내용을 확인하십시오

- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

다중 요소 인증에 대한 추가 정보

다중 요소 인증과 관련하여 다음과 같은 주의사항을 염두에 두어야 합니다.

- 더 이상 유효하지 않은 IDP 인증서를 새로 고치려면 비 IDP 관리자를 사용하여 다음 API 메서드를 호출해야 합니다. `UpdateIdpConfiguration`
- MFA는 길이가 2048비트 미만인 인증서와 호환되지 않습니다. 기본적으로 2048비트 SSL 인증서가 클러스터에 생성됩니다. API 메서드를 호출할 때 더 작은 크기의 인증서를 설정하지 않아야 합니다. `SetSSLCertificate`

> 클러스터가 2048비트 사전 업그레이드 미만의 인증서를 사용하는 경우 Element 12.0 이상으로 업그레이드한 후 2048비트 이상의 인증서로 클러스터 인증서를 업데이트해야 합니다.

- IDP 관리 사용자는 SDK 또는 Postman을 통해 API 호출을 직접 수행하거나 다른 통합(예: OpenStack Cinder 또는 vCenter 플러그인)에 사용할 수 없습니다. 이러한 기능을 가진 사용자를 생성해야 하는 경우 LDAP 클러스터 관리자 사용자 또는 로컬 클러스터 관리자 사용자를 추가합니다.

자세한 내용을 확인하십시오

- "Element API를 사용하여 스토리지 관리"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

저작권 정보

상표 정보