계정 관리

Element Software

NetApp
November 12, 2025

목차

계정 관리

계정 관리

SolidFire 스토리지 시스템에서 테넌트는 계정을 사용하여 클라이언트가 클러스터의 볼륨에 연결하도록 할 수 있습니다. 볼륨을 생성하면 특정 계정에 할당됩니다. SolidFire 스토리지 시스템의 클러스터 관리자 계정도 관리할 수 있습니다.

- "CHAP를 사용하여 계정 작업"
- "클러스터 관리자 사용자 계정 관리"

더 많은 정보를 원하시면

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

CHAP를 사용하여 계정 작업

SolidFire 스토리지 시스템에서 테넌트는 계정을 사용하여 클라이언트가 클러스터의 볼륨에 연결하도록 할 수 있습니다. 계정에는 할당된 볼륨에 액세스하는 데 필요한 CHAP(Challenge-Handshake 인증 프로토콜) 인증이 포함되어 있습니다. 볼륨을 생성하면 특정 계정에 할당됩니다.

한 계정에는 최대 2,000개의 볼륨이 할당될 수 있지만, 볼륨은 한 계정에만 속할 수 있습니다.

CHAP 알고리즘

Element 12.7부터 보안 FIPS 호환 CHAP 알고리즘 SHA1, SHA-256, SHA3-256이 지원됩니다. 호스트 iSCSI 이니시에이터가 Element iSCSI 대상과 iSCSI 세션을 생성할 때 사용할 CHAP 알고리즘 목록을 요청합니다. Element iSCSI 대상은 호스트 iSCSI 초기자가 요청한 목록에서 지원하는 첫 번째 알고리즘을 선택합니다. Element iSCSI 대상이 가장 안전한 알고리즘을 선택하는지 확인하려면 호스트 iSCSI 초기자가 가장 안전한 알고리즘(예: SHA3-256)부터 가장 안전하지 않은 알고리즘(예: SHA1 또는 MD5) 순으로 정렬된 알고리즘 목록을 보내도록 구성해야 합니다. 호스트 iSCSI 초기자가 SHA 알고리즘을 요청하지 않으면 Element iSCSI 대상은 호스트의 제안된 알고리즘 목록에 MD5가 포함되어 있다고 가정하고 MD5를 선택합니다. 보안 알고리즘에 대한 지원을 활성화하려면 호스트 iSCSI 초기자 구성을 업데이트해야 할 수도 있습니다.

Element 12.7 이상 업그레이드 중에 SHA 알고리즘을 포함하는 목록으로 세션 요청을 보내도록 호스트 iSCSI 초기자 구성을 이미 업데이트한 경우, 스토리지 노드가 재부팅되면 새로운 보안 알고리즘이 활성화되고 가장 안전한 프로토콜을 사용하여 새 iSCSI 세션이나 다시 연결된 iSCSI 세션이 설정됩니다. 업그레이드하는 동안 모든 기존 iSCSI 세션은 MD5에서 SHA로 전환됩니다. 호스트 iSCSI 이니시에이터 구성을 SHA 요청으로 업데이트하지 않으면 기존 iSCSI 세션은 계속해서 MD5를 사용합니다. 나중에 호스트 iSCSI 이니시에이터 CHAP 알고리즘을 업데이트한 후에는 iSCSI 세션이 iSCSI 세션 재연결을 초래하는 유지 관리 활동을 기반으로 시간이 지남에 따라 MD5에서 SHA로 점진적으로 전환되어야 합니다.

예를 들어, Red Hat Enterprise Linux(RHEL) 8.3의 기본 호스트 iSCSI 초기자에는 다음이 있습니다. `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` 설정이 주석 처리되어 iSCSI 초기자가 MD5만 사용하게 됩니다. 호스트에서 이 설정의 주석 처리를 해제하고 iSCSI 초기자를 다시 시작하면 해당 호스트의

iSCSI 세션이 SHA3-256을 사용하기 시작합니다.

필요한 경우 다음을 사용할 수 있습니다. "ListISCSISessions" 각 세션에 사용되는 CHAP 알고리즘을 확인하는 API 방법입니다.

계정을 생성하세요

볼륨에 대한 액세스를 허용하려면 계정을 만들 수 있습니다.

시스템의 각 계정 이름은 고유해야 합니다.

1. 관리 > *계정*을 선택하세요.
2. *계정 만들기*를 클릭하세요.
3. *사용자 이름*을 입력하세요.
4. **CHAP** 설정 섹션에 다음 정보를 입력하세요.

   비밀번호가 자동으로 생성되도록 하려면 자격 증명 필드를 비워 두세요.

   - CHAP 노드 세션 인증을 위한 개시자 비밀
   - CHAP 노드 세션 인증을 위한 *대상 비밀*입니다.
5. *계정 만들기*를 클릭하세요.

계정 세부 정보 보기

개별 계정의 성과 활동을 그래픽 형식으로 볼 수 있습니다.

그래프 정보는 해당 계정의 I/O 및 처리량 정보를 제공합니다. 평균 및 최대 활동 수준은 10초 보고 기간 단위로 표시됩니다. 이러한 통계에는 계정에 할당된 모든 볼륨에 대한 활동이 포함됩니다.

1. 관리 > *계정*을 선택하세요.
2. 계정의 작업 아이콘을 클릭합니다.
3. *자세히 보기*를 클릭하세요.

자세한 내용은 다음과 같습니다.

- 상태: 계정의 상태입니다. 가능한 값:
  - 활성: 활성 계정.
  - 잠김: 잠긴 계정.
  - 제거됨: 삭제 및 정리된 계정입니다.
- 활성 볼륨: 계정에 할당된 활성 볼륨의 수입니다.
- 압축: 계정에 할당된 볼륨에 대한 압축 효율성 점수입니다.
- 중복 제거: 계정에 할당된 볼륨에 대한 중복 제거 효율성 점수입니다.
- 씬 프로비저닝: 계정에 할당된 볼륨에 대한 씬 프로비저닝 효율성 점수입니다.

- 전반적인 효율성: 계정에 할당된 볼륨에 대한 전반적인 효율성 점수입니다.

계정 편집

계정을 편집하여 상태를 변경하고, CHAP 비밀번호를 변경하거나, 계정 이름을 수정할 수 있습니다.

계정에서 CHAP 설정을 수정하거나 액세스 그룹에서 이니시에이터 또는 볼륨을 제거하면 이니시에이터가 예기치 않게 볼륨에 액세스할 수 없게 될 수 있습니다. 볼륨 액세스가 예기치 않게 손실되지 않도록 하려면 계정이나 액세스 그룹 변경의 영향을 받는 iSCSI 세션에서 항상 로그아웃하고, 이니시에이터 설정과 클러스터 설정에 대한 변경이 완료된 후 이니시에이터가 볼륨에 다시 연결할 수 있는지 확인하세요.

관리 서비스와 연관된 영구 볼륨은 설치 또는 업그레이드 중에 생성된 새 계정에 할당됩니다. 영구 볼륨을 사용하는 경우 연결된 계정을 수정하거나 삭제하지 마세요.

1. 관리 > *계정*을 선택하세요.
2. 계정의 작업 아이콘을 클릭합니다.
3. 나타나는 메뉴에서 *편집*을 선택합니다.
4. 선택 사항**:** *사용자 이름*을 편집하세요.
5. 선택 사항**:** 상태 드롭다운 목록을 클릭하고 다른 상태를 선택합니다.

   상태를 *잠김*으로 변경하면 해당 계정에 대한 모든 iSCSI 연결이 종료되고, 더 이상 계정에 액세스할 수 없습니다. 계정과 연결된 볼륨은 유지되지만 볼륨은 iSCSI에서 검색할 수 없습니다.

6. 선택 사항**: CHAP** 설정*에서 노드 세션 인증에 사용되는 *개시자 비밀 및 대상 비밀 자격 증명을 편집합니다.

   CHAP 설정 자격 증명을 변경하지 않으면 동일하게 유지됩니다. 자격 증명 필드를 비워 두면 시스템이 새로운 비밀번호를 생성합니다.

7. *변경 사항 저장*을 클릭하세요.

계정 삭제

더 이상 필요하지 않은 계정은 삭제할 수 있습니다.

계정을 삭제하기 전에 해당 계정과 연관된 모든 볼륨을 삭제하고 정리하세요.

관리 서비스와 연관된 영구 볼륨은 설치 또는 업그레이드 중에 생성된 새 계정에 할당됩니다. 영구 볼륨을 사용하는 경우 연결된 계정을 수정하거나 삭제하지 마세요.

1. 관리 > *계정*을 선택하세요.
2. 삭제하려는 계정의 작업 아이콘을 클릭합니다.
3. 나타나는 메뉴에서 *삭제*를 선택합니다.
4. 작업을 확인합니다.

더 많은 정보를 찾아보세요

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

클러스터 관리자 사용자 계정 관리

클러스터 관리자 계정을 생성, 삭제, 편집하고, 클러스터 관리자 비밀번호를 변경하고, 사용자의 시스템 액세스를 관리하기 위한 LDAP 설정을 구성하여 SolidFire 스토리지 시스템의 클러스터 관리자 계정을 관리할 수 있습니다.

스토리지 클러스터 관리자 계정 유형

NetApp Element 소프트웨어를 실행하는 스토리지 클러스터에는 두 가지 유형의 관리자 계정이 있습니다. 기본 클러스터 관리자 계정과 클러스터 관리자 계정입니다.

- 기본 클러스터 관리자 계정

  이 관리자 계정은 클러스터가 생성될 때 생성됩니다. 이 계정은 클러스터에 대한 가장 높은 수준의 액세스 권한을 가진 기본 관리 계정입니다. 이 계정은 Linux 시스템의 루트 사용자와 유사합니다. 이 관리자 계정의 비밀번호를 변경할 수 있습니다.

- 클러스터 관리자 계정

  클러스터 관리자 계정에 클러스터 내에서 특정 작업을 수행하기 위한 제한된 범위의 관리 액세스 권한을 부여할 수 있습니다. 각 클러스터 관리자 계정에 할당된 자격 증명은 스토리지 시스템 내에서 API 및 Element UI 요청을 인증하는 데 사용됩니다.

노드별 UI를 통해 클러스터의 활성 노드에 액세스하려면 로컬(비 LDAP) 클러스터 관리자 계정이 필요합니다. 아직 클러스터에 속하지 않은 노드에 액세스하는 데는 계정 자격 증명이 필요하지 않습니다.

클러스터 관리자 세부 정보 보기

1. 클러스터 전체(비 LDAP) 클러스터 관리자 계정을 만들려면 다음 작업을 수행하세요.
   a. 사용자 > *클러스터 관리자*를 클릭합니다.
2. 사용자 탭의 클러스터 관리자 페이지에서 다음 정보를 볼 수 있습니다.
   - **ID**: 클러스터 관리자 계정에 할당된 순차 번호입니다.
   - 사용자 이름: 클러스터 관리자 계정이 생성될 때 지정된 이름입니다.
   - 액세스: 사용자 계정에 할당된 사용자 권한입니다. 가능한 값:
     - 읽다
     - 보고
     - 노드
     - 드라이브

- 볼륨
- 계정
- 클러스터 관리자
- 관리자
- 지원 관리자

> 모든 권한은 관리자 액세스 유형에만 제공됩니다.
>
> Element UI에서는 사용할 수 없는 API를 통해 사용 가능한 액세스 유형이 있습니다.

+

- 유형: 클러스터 관리자의 유형입니다. 가능한 값:
  - 무리
  - LDAP
- 속성: 클러스터 관리자 계정이 Element API를 사용하여 생성된 경우 이 열에는 해당 방법을 사용하여 설정된 모든 이름-값 쌍이 표시됩니다.

  보다"NetApp Element 소프트웨어 API 참조" .

클러스터 관리자 계정 만들기

스토리지 시스템의 특정 영역에 대한 액세스를 허용하거나 제한하는 권한이 있는 새로운 클러스터 관리자 계정을 만들 수 있습니다. 클러스터 관리자 계정 권한을 설정하면 시스템은 클러스터 관리자에게 할당하지 않은 모든 권한에 대해 읽기 전용 권한을 부여합니다.

LDAP 클러스터 관리자 계정을 만들려면 시작하기 전에 클러스터에 LDAP가 구성되어 있는지 확인하세요.

"Element 사용자 인터페이스를 사용하여 LDAP 인증 활성화"

나중에 보고, 노드, 드라이브, 볼륨, 계정 및 클러스터 수준 액세스에 대한 클러스터 관리자 계정 권한을 변경할 수 있습니다. 권한을 활성화하면 시스템은 해당 수준에 대한 쓰기 액세스 권한을 할당합니다. 시스템은 선택하지 않은 수준에 대해서는 관리자 사용자에게 읽기 전용 액세스 권한을 부여합니다.

나중에 시스템 관리자가 만든 클러스터 관리자 사용자 계정을 제거할 수도 있습니다. 클러스터가 생성될 때 생성된 기본 클러스터 관리자 계정은 제거할 수 없습니다.

1. 클러스터 전체(비 LDAP) 클러스터 관리자 계정을 만들려면 다음 작업을 수행하세요.
   a. 사용자 > *클러스터 관리자*를 클릭합니다.
   b. *클러스터 관리자 만들기*를 클릭합니다.
   c. 클러스터 사용자 유형을 선택하세요.
   d. 계정의 사용자 이름과 비밀번호를 입력하고 비밀번호를 확인하세요.
   e. 계정에 적용할 사용자 권한을 선택합니다.
   f. 최종 사용자 라이선스 계약에 동의하려면 확인란을 선택하세요.

g. *클러스터 관리자 만들기*를 클릭합니다.

2. LDAP 디렉토리에 클러스터 관리자 계정을 만들려면 다음 작업을 수행하세요.

   a. 클러스터 > *LDAP*를 클릭합니다.

   b. LDAP 인증이 활성화되어 있는지 확인하세요.

   c. *사용자 인증 테스트*를 클릭하고 사용자 또는 사용자가 구성원인 그룹 중 하나에 표시되는 고유 이름을 복사하여 나중에 붙여넣을 수 있습니다.

   d. 사용자 > *클러스터 관리자*를 클릭합니다.

   e. *클러스터 관리자 만들기*를 클릭합니다.

   f. LDAP 사용자 유형을 선택하세요.

   g. 고유 이름 필드에서 텍스트 상자의 예를 따라 사용자 또는 그룹의 전체 고유 이름을 입력합니다. 또는, 앞서 복사한 고유 이름을 붙여넣으세요.

      고유 이름이 그룹의 일부인 경우 LDAP 서버에서 해당 그룹의 멤버인 모든 사용자는 이 관리자 계정의 권한을 갖습니다.

   LDAP 클러스터 관리자 사용자 또는 그룹을 추가하려면 사용자 이름의 일반적인 형식은 "`LDAP:<전체 고유 이름>`"입니다.

   a. 계정에 적용할 사용자 권한을 선택합니다.

   b. 최종 사용자 라이선스 계약에 동의하려면 확인란을 선택하세요.

   c. *클러스터 관리자 만들기*를 클릭합니다.

클러스터 관리자 권한 편집

보고, 노드, 드라이브, 볼륨, 계정 및 클러스터 수준 액세스에 대한 클러스터 관리자 계정 권한을 변경할 수 있습니다. 권한을 활성화하면 시스템은 해당 수준에 대한 쓰기 액세스 권한을 할당합니다. 시스템은 선택하지 않은 수준에 대해서는 관리자 사용자에게 읽기 전용 액세스 권한을 부여합니다.

1. 사용자 > *클러스터 관리자*를 클릭합니다.
2. 편집하려는 클러스터 관리자에 대한 작업 아이콘을 클릭합니다.
3. *편집*을 클릭하세요.
4. 계정에 적용할 사용자 권한을 선택합니다.
5. *변경 사항 저장*을 클릭하세요.

클러스터 관리자 계정의 비밀번호 변경

Element UI를 사용하여 클러스터 관리자 비밀번호를 변경할 수 있습니다.

1. 사용자 > *클러스터 관리자*를 클릭합니다.
2. 편집하려는 클러스터 관리자에 대한 작업 아이콘을 클릭합니다.
3. *편집*을 클릭하세요.
4. 비밀번호 변경 필드에 새 비밀번호를 입력하고 확인하세요.

5. *변경 사항 저장*을 클릭하세요.

관련 정보

- "Element API에 사용 가능한 액세스 유형에 대해 알아보세요."
- "Element 사용자 인터페이스를 사용하여 LDAP 인증 활성화"
- "LDAP 비활성화"
- "vCenter Server용 NetApp Element 플러그인"

LDAP 관리

SolidFire 저장소에 대한 안전한 디렉토리 기반 로그인 기능을 활성화하기 위해 LDAP(Lightweight Directory Access Protocol)를 설정할 수 있습니다. 클러스터 수준에서 LDAP를 구성하고 LDAP 사용자와 그룹에 권한을 부여할 수 있습니다.

LDAP 관리에는 기존 Microsoft Active Directory 환경을 사용하여 SolidFire 클러스터에 대한 LDAP 인증을 설정하고 구성을 테스트하는 작업이 포함됩니다.

IPv4와 IPv6 주소를 모두 사용할 수 있습니다.

LDAP를 활성화하려면 다음과 같은 상위 단계가 필요하며, 각 단계에 대해 자세히 설명합니다.

1. **LDAP** 지원을 위한 사전 구성 단계를 완료합니다. LDAP 인증을 구성하는 데 필요한 모든 세부 정보가 있는지 확인하세요.
2. **LDAP** 인증을 활성화합니다. Element UI나 Element API를 사용하세요.
3. **LDAP** 구성을 검증합니다. 선택적으로 GetLdapConfiguration API 메서드를 실행하거나 Element UI를 사용하여 LCAP 구성을 확인하여 클러스터가 올바른 값으로 구성되었는지 확인합니다.
4. **LDAP** 인증 테스트 (`readonly` 사용자). TestLdapAuthentication API 메서드를 실행하거나 Element UI를 사용하여 LDAP 구성이 올바른지 테스트합니다. 이 초기 테스트에서는 사용자 이름 "`sAMAccountName`"을 사용합니다. `readonly` 사용자. 이렇게 하면 클러스터가 LDAP 인증을 위해 올바르게 구성되었는지 확인하고 다음 사항도 확인합니다. `readonly` 자격 증명과 액세스 권한이 정확합니다. 이 단계가 실패하면 1~3단계를 반복합니다.
5. **LDAP** 인증을 테스트합니다 (추가하려는 사용자 계정으로). Element 클러스터 관리자로 추가하려는 사용자 계정으로 4단계를 반복합니다. 복사하다 `distinguished` 이름(DN) 또는 사용자(또는 그룹). 이 DN은 6단계에서 사용됩니다.
6. **LDAP** 클러스터 관리자 추가 (LDAP 인증 테스트 단계에서 DN을 복사하여 붙여넣습니다). Element UI 또는 AddLdapClusterAdmin API 메서드를 사용하여 적절한 액세스 수준을 가진 새로운 클러스터 관리자 사용자를 만듭니다. 사용자 이름에는 5단계에서 복사한 전체 DN을 붙여넣습니다. 이렇게 하면 DN이 올바르게 형식화됩니다.
7. 클러스터 관리자 액세스를 테스트합니다. 새로 생성된 LDAP 클러스터 관리자 사용자를 사용하여 클러스터에 로그인합니다. LDAP 그룹을 추가한 경우 해당 그룹의 모든 사용자로 로그인할 수 있습니다.

LDAP 지원을 위한 사전 구성 단계 완료

Element에서 LDAP 지원을 활성화하기 전에 Windows Active Directory 서버를 설정하고 다른 사전 구성 작업을 수행해야 합니다.

단계

1. Windows Active Directory 서버를 설정합니다.
2. 선택 사항**:** LDAPS 지원을 활성화합니다.
3. 사용자와 그룹을 생성합니다.
4. LDAP 디렉토리를 검색하는 데 사용할 읽기 전용 서비스 계정(예: “sfreadonly”)을 만듭니다.

Element 사용자 인터페이스를 사용하여 LDAP 인증 활성화

기존 LDAP 서버와 스토리지 시스템 통합을 구성할 수 있습니다. 이를 통해 LDAP 관리자는 사용자의 스토리지 시스템 액세스를 중앙에서 관리할 수 있습니다.

Element 사용자 인터페이스나 Element API를 사용하여 LDAP를 구성할 수 있습니다. 이 절차에서는 Element UI를 사용하여 LDAP를 구성하는 방법을 설명합니다.

이 예제에서는 SolidFire 에서 LDAP 인증을 구성하는 방법을 보여줍니다. `SearchAndBind` 인증 유형으로. 이 예제에서는 단일 Windows Server 2012 R2 Active Directory 서버를 사용합니다.

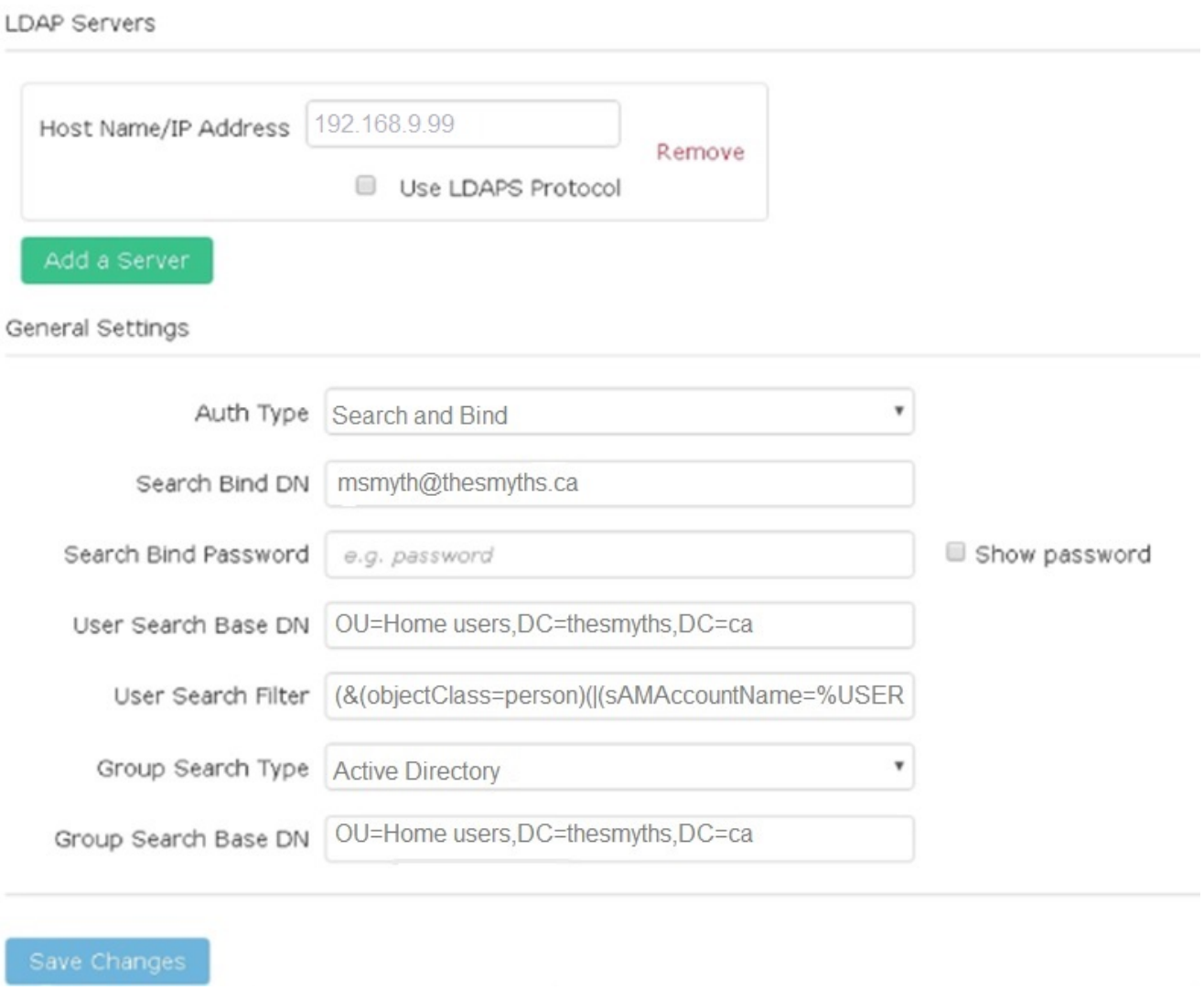
단계

1. 클러스터 > *LDAP*를 클릭합니다.
2. LDAP 인증을 활성화하려면 *예*를 클릭하세요.
3. *서버 추가*를 클릭합니다.
4. *호스트 이름/IP 주소*를 입력하세요.

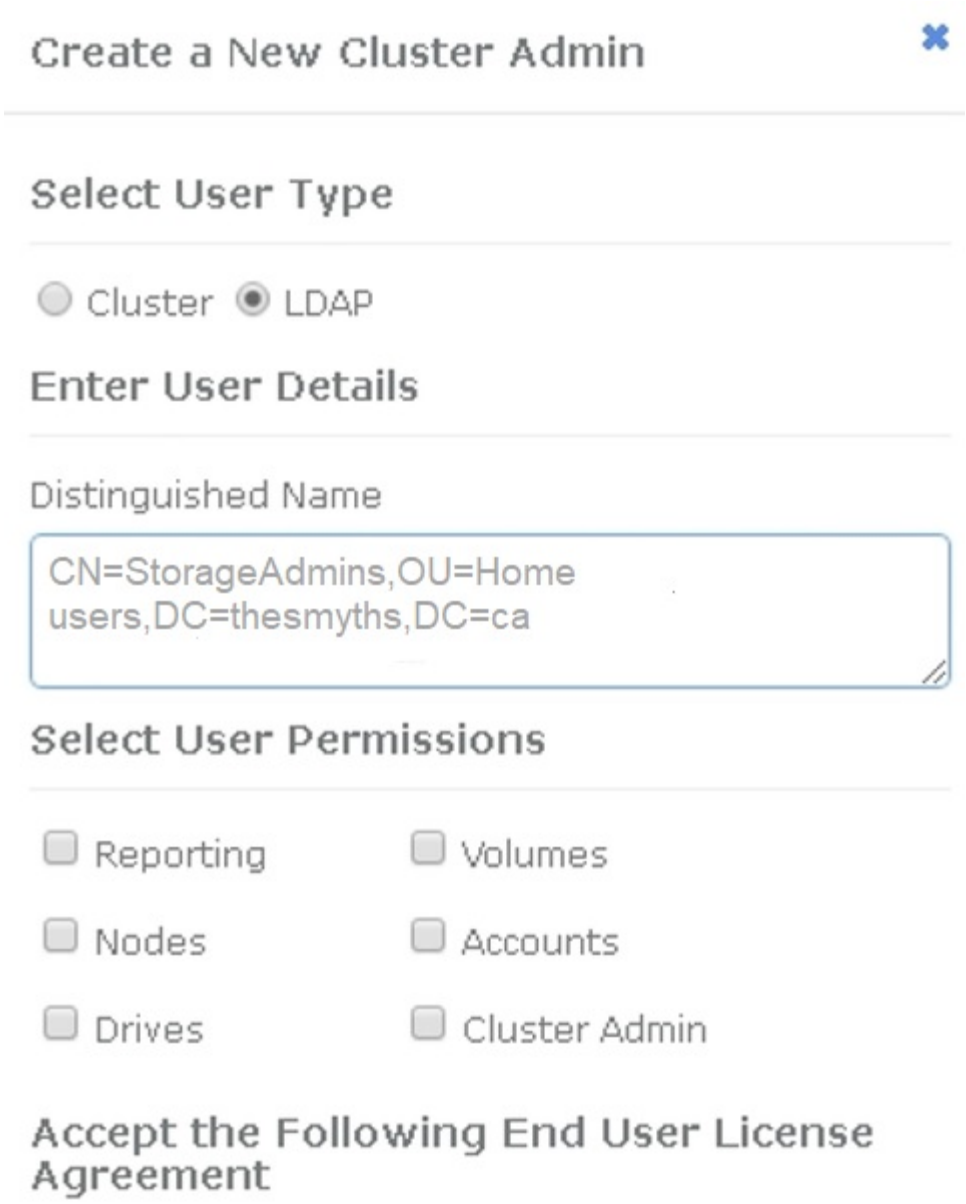
   선택적으로 사용자 정의 포트 번호를 입력할 수도 있습니다.

   예를 들어, 사용자 정의 포트 번호를 추가하려면 <호스트 이름 또는 IP 주소>:<포트 번호>를 입력합니다.

5. 선택 사항**:** *LDAPS 프로토콜 사용*을 선택합니다.
6. *일반 설정*에 필요한 정보를 입력하세요.



7. *LDAP 사용*을 클릭합니다.
8. 사용자의 서버 액세스를 테스트하려면 *사용자 인증 테스트*를 클릭하세요.
9. 나중에 클러스터 관리자를 생성할 때 사용할 고유 이름과 사용자 그룹 정보를 복사합니다.
10. 새로운 설정을 저장하려면 *변경 사항 저장*을 클릭하세요.
11. 누구나 로그인할 수 있도록 이 그룹에 사용자를 만들려면 다음을 완료하세요.
    a. 사용자 > *보기*를 클릭합니다.



b. 새 사용자의 경우 사용자 유형에서 *LDAP*를 클릭하고 복사한 그룹을 고유 이름 필드에 붙여넣습니다.
c. 일반적으로 모든 권한을 선택합니다.
d. 최종 사용자 라이선스 계약으로 스크롤하여 *동의합니다*를 클릭하세요.
e. *클러스터 관리자 만들기*를 클릭합니다.

   이제 Active Directory 그룹 값을 가진 사용자가 생겼습니다.

이를 테스트하려면 Element UI에서 로그아웃한 다음 해당 그룹의 사용자로 다시 로그인하세요.

Element API를 사용하여 LDAP 인증 활성화

기존 LDAP 서버와 스토리지 시스템 통합을 구성할 수 있습니다. 이를 통해 LDAP 관리자는 사용자의 스토리지 시스템 액세스를 중앙에서 관리할 수 있습니다.

Element 사용자 인터페이스나 Element API를 사용하여 LDAP를 구성할 수 있습니다. 이 절차에서는 Element API를

사용하여 LDAP를 구성하는 방법을 설명합니다.

SolidFire 클러스터에서 LDAP 인증을 활용하려면 먼저 클러스터에서 LDAP 인증을 활성화해야 합니다. `EnableLdapAuthentication` API 방식.

단계

1. 클러스터에서 LDAP 인증을 먼저 활성화합니다. `EnableLdapAuthentication` API 방식.
2. 필요한 정보를 입력하세요.

```
{
      "method":"EnableLdapAuthentication",
      "params":{
           "authType": "SearchAndBind",
           "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
           "groupSearchType": "ActiveDirectory",
           "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
           "searchBindPassword": "ReadOnlyPW",
           "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
           "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
           "serverURIs": [
                "ldap://172.27.1.189",
           [
      },
  "id":"1"
}
```

3. 다음 매개변수의 값을 변경합니다.

사용된 매개변수	설명
인증 유형: 검색 및 바인딩	클러스터가 읽기 전용 서비스 계정을 사용하여 먼저 인증되는 사용자를 검색한 다음, 해당 사용자를 찾아 인증하면 해당 사용자를 바인딩하도록 지정합니다.
groupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	LDAP 트리에서 그룹 검색을 시작할 위치를 지정합니다. 이 예에서는 트리의 루트를 사용했습니다. LDAP 트리가 매우 큰 경우 검색 시간을 줄이기 위해 이를 더 세부적인 하위 트리로 설정할 수 있습니다.
userSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	LDAP 트리에서 사용자 검색을 시작할 위치를 지정합니다. 이 예에서는 트리의 루트를 사용했습니다. LDAP 트리가 매우 큰 경우 검색 시간을 줄이기 위해 이를 더 세부적인 하위 트리로 설정할 수 있습니다.

사용된 매개변수	설명
groupSearchType: ActiveDirectory	Windows Active Directory 서버를 LDAP 서버로 사용합니다.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
userPrincipalName(로그인용 이메일 주소)을 사용하려면 userSearchFilter를 다음과 같이 변경할 수 있습니다.
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
또는 userPrincipalName과 sAMAccountName을 모두 검색하려면 다음 userSearchFilter를 사용할 수 있습니다.
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))" ----

SolidFire 클러스터에 로그인하기 위해 sAMAccountName을 사용자 이름으로 활용합니다. 이러한 설정은 LDAP가 sAMAccountName 속성에서 로그인 시 지정된 사용자 이름을 검색하도록 지시하고 objectClass 속성에 "person" 값이 있는 항목으로 검색을 제한합니다.	검색BindDN
이는 LDAP 디렉토리를 검색하는 데 사용되는 읽기 전용 사용자의 고유 이름입니다. Active Directory의 경우 일반적으로 사용자의 userPrincipalName(이메일 주소 형식)을 사용하는 것이 가장 쉽습니다.	검색바인드패스워드

이를 테스트하려면 Element UI에서 로그아웃한 다음 해당 그룹의 사용자로 다시 로그인하세요.

LDAP 세부 정보 보기

클러스터 탭의 LDAP 페이지에서 LDAP 정보를 확인하세요.

이러한 LDAP 구성 설정을 보려면 LDAP를 활성화해야 합니다.

1. Element UI로 LDAP 세부 정보를 보려면 클러스터 > *LDAP*를 클릭하세요.

- 호스트 이름/**IP** 주소: LDAP 또는 LDAPS 디렉토리 서버의 주소입니다.
- 인증 유형: 사용자 인증 방법입니다. 가능한 값:
  - 직접 바인딩
  - 검색 및 바인딩
- 검색 바인드 **DN**: 사용자에 대한 LDAP 검색을 수행하기 위해 로그인하는 데 사용되는 완전히 적격한 DN(LDAP 디렉토리에 대한 바인드 수준 액세스 필요).
- 검색 바인드 비밀번호: LDAP 서버에 대한 액세스를 인증하는 데 사용되는 비밀번호입니다.
- 사용자 검색 기본 **DN**: 사용자 검색을 시작하는 데 사용되는 트리의 기본 DN입니다. 시스템은 지정된 위치의 서브트리를 검색합니다.
- 사용자 검색 필터: 도메인 이름을 사용하여 다음을 입력하세요.

  ```
  (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
  ```

- 그룹 검색 유형: 기본적으로 사용되는 그룹 검색 필터를 제어하는 검색 유형입니다. 가능한 값:
  - Active Directory: 사용자의 모든 LDAP 그룹에 대한 중첩된 멤버십.
  - 그룹 없음: 그룹 지원이 없습니다.
  - 멤버 DN: 멤버 DN 스타일 그룹(단일 레벨).
- 그룹 검색 기본 **DN**: 그룹 검색을 시작하는 데 사용되는 트리의 기본 DN입니다. 시스템은 지정된 위치의 서브트리를 검색합니다.
- 사용자 인증 테스트: LDAP가 구성된 후 이를 사용하여 LDAP 서버의 사용자 이름과 비밀번호 인증을 테스트합니다. 테스트하려면 이미 존재하는 계정을 입력하세요. 고유 이름과 사용자 그룹 정보가 표시되며, 나중에 클러스터 관리자를 만들 때 복사하여 사용할 수 있습니다.

LDAP 구성 테스트

LDAP를 구성한 후 Element UI 또는 Element API를 사용하여 테스트해야 합니다. `TestLdapAuthentication` 방법.

단계

1. Element UI로 LDAP 구성을 테스트하려면 다음을 수행하세요.
   a. 클러스터 > *LDAP*를 클릭합니다.
   b. *LDAP 인증 테스트*를 클릭합니다.
   c. 아래 표의 정보를 사용하여 문제를 해결하세요.

오류 메시지	설명
`xLDAPUserNotFound`	• 테스트 중인 사용자는 구성된 곳에서 찾을 수 없습니다. `userSearchBaseDN` 서브트리. • 그만큼 `userSearchFilter` 잘못 구성되었습니다.

오류 메시지	설명
`xLDAPBindFailed (Error: Invalid credentials)`	• 테스트 중인 사용자 이름은 유효한 LDAP 사용자이지만 제공된 비밀번호가 올바르지 않습니다. • 테스트 중인 사용자 이름은 유효한 LDAP 사용자이지만, 해당 계정은 현재 비활성화되어 있습니다.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	LDAP 서버 URI가 올바르지 않습니다.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	읽기 전용 사용자 이름 또는 비밀번호가 잘못 구성되었습니다.
`xLDAPSearchFailed (Error: No such object)`	그만큼 `userSearchBaseDN` LDAP 트리 내의 유효한 위치가 아닙니다.
`xLDAPSearchFailed (Error: Referral)`	• 그만큼 `userSearchBaseDN` LDAP 트리 내의 유효한 위치가 아닙니다. • 그만큼 `userSearchBaseDN` 그리고 `groupSearchBaseDN` 중첩된 OU에 있습니다. 이로 인해 권한 문제가 발생할 수 있습니다. 해결 방법은 사용자 및 그룹 기반 DN 항목에 OU를 포함하는 것입니다(예: `ou=storage, cn=company, cn=com`)

2. Element API로 LDAP 구성을 테스트하려면 다음을 수행하세요.
   a. TestLdapAuthentication 메서드를 호출합니다.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

   b. 결과를 검토하세요. API 호출이 성공하면 결과에는 지정된 사용자의 고유 이름과 사용자가 구성원인 그룹

목록이 포함됩니다.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

LDAP 비활성화

Element UI를 사용하여 LDAP 통합을 비활성화할 수 있습니다.

시작하기 전에 모든 구성 설정을 기록해 두어야 합니다. LDAP를 비활성화하면 모든 설정이 지워지기 때문입니다.

단계

1. 클러스터 > *LDAP*를 클릭합니다.
2. *아니요*를 클릭하세요.
3. *LDAP 비활성화*를 클릭합니다.

더 많은 정보를 찾아보세요

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