계정 관리

Element Software

NetApp
October 01, 2024

목차

계정 관리

SolidFire 스토리지 시스템에서 테넌트는 계정을 사용하여 클라이언트가 클러스터의 볼륨에 연결할 수 있도록 설정할 수 있습니다. 볼륨을 생성하면 특정 계정에 할당됩니다. SolidFire 스토리지 시스템의 클러스터 관리자 계정을 관리할 수도 있습니다.

- "CHAP를 사용하여 계정 작업"
- "클러스터 관리자 사용자 계정을 관리합니다"

를 참조하십시오

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

CHAP를 사용하여 계정 작업

SolidFire 스토리지 시스템에서 테넌트는 계정을 사용하여 클라이언트가 클러스터의 볼륨에 연결할 수 있도록 설정할 수 있습니다. 계정에는 할당된 볼륨에 액세스하는 데 필요한 CHAP(Challenge-Handshake Authentication Protocol) 인증이 포함되어 있습니다. 볼륨을 생성하면 특정 계정에 할당됩니다.

계정에는 최대 2천 개의 볼륨이 할당될 수 있지만 볼륨은 하나의 계정에만 속할 수 있습니다.

CHAP 알고리즘입니다

Element 12.7부터 보안 FIPS 호환 CHAP 알고리즘 SHA1, SHA-256 및 SHA3-256이 지원됩니다. Element 12.7을 사용하는 경우 호스트 iSCSI 이니시에이터가 Element iSCSI 타겟과 함께 iSCSI 세션을 생성하는 경우 사용할 CHAP 알고리즘 목록을 요청합니다. Element iSCSI 대상은 호스트 iSCSI 초기자가 요청한 목록에서 지원하는 첫 번째 알고리즘을 선택합니다. Element iSCSI 타겟이 가장 안전한 알고리즘을 선택하는지 확인하려면 호스트 iSCSI 초기자가 가장 안전한(예: SHA3-256)에서 주문한 알고리즘 목록을 가장 안전한 것으로 보내도록 구성해야 합니다. SHA1 또는 MD5. 호스트 iSCSI 초기자가 SHA 알고리즘을 요청하지 않으면 Element iSCSI 대상이 MD5를 선택하며, 호스트의 제안된 알고리즘 목록에 MD5가 포함되어 있다고 가정합니다. 보안 알고리즘을 지원하려면 호스트 iSCSI 이니시에이터 구성을 업데이트해야 할 수 있습니다.

Element 12.7 업그레이드 중에 스토리지 노드가 재부팅될 때 SHA 알고리즘을 포함하는 목록이 포함된 세션 요청을 보내도록 호스트 iSCSI 이니시에이터 구성을 이미 업데이트한 경우 새로운 보안 알고리즘이 활성화되고 가장 안전한 프로토콜을 사용하여 새 iSCSI 세션 또는 다시 연결된 iSCSI 세션이 설정됩니다. 업그레이드 중에 기존의 모든 iSCSI 세션이 MD5에서 SHA로 전환됩니다. 호스트 iSCSI 이니시에이터 구성을 SHA를 요청하기 위해 업데이트하지 않으면 기존 iSCSI 세션에서 계속 MD5를 사용합니다. 나중에 호스트 iSCSI 이니시에이터 CHAP 알고리즘을 업데이트한 후 iSCSI 세션이 다시 연결되는 유지 보수 작업에 따라 iSCSI 세션이 점차 MD5에서 SHA로 전환되어야 합니다.

예를 들어, Red Hat Enterprise Linux(RHEL) 8.3의 기본 호스트 iSCSI 초기자는 `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` 주석 처리를 통해 iSCSI 초기자가 MD5만 사용하게 됩니다. 호스트에서 이 설정의 주석 처리를 해제하고 iSCSI 이니시에이터를 다시 시작하면 해당 호스트에서 iSCSI 세션이 트리거되어 SHA3-256을 사용합니다.

필요한 경우 API 메소드를 사용하여 각 세션에 사용되는 CHAP 알고리즘을 확인할 수 "목록 세션" 있습니다.

계정을 만듭니다

볼륨에 대한 액세스를 허용하는 계정을 생성할 수 있습니다.

시스템의 각 계정 이름은 고유해야 합니다.

1. Management * > * Accounts * 를 선택합니다.
2. 계정 만들기 * 를 클릭합니다.
3. 사용자 이름 * 을 입력합니다.
4. CHAP 설정 * 섹션에서 다음 정보를 입력합니다.

   자격 증명 필드를 비워 두면 두 암호를 자동으로 생성할 수 있습니다.

   - CHAP 노드 세션 인증을 위한 * 초기자 암호 *.
   - CHAP 노드 세션 인증을 위한 * Target Secret * 입니다.
5. 계정 만들기 * 를 클릭합니다.

계정 세부 정보를 봅니다

개별 계정의 성능 활동을 그래픽 형식으로 볼 수 있습니다.

그래프 정보는 계정에 대한 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. Management * > * Accounts * 를 선택합니다.
2. 계정의 작업 아이콘을 클릭합니다.
3. 세부 정보 보기 * 를 클릭합니다.

다음은 몇 가지 세부 사항입니다.

- * 상태 *: 계정 상태입니다. 가능한 값:
  - 활성: 활성 계정.
  - 잠김: 잠긴 계정입니다.
  - 제거됨: 삭제 및 삭제된 계정입니다.
- * 활성 볼륨 *: 계정에 할당된 활성 볼륨의 수입니다.
- * 압축 *: 계정에 할당된 볼륨의 압축 효율성 점수입니다.
- * 중복 제거 *: 계정에 할당된 볼륨의 중복 제거 효율성 점수입니다.
- * 씬 프로비저닝 *: 계정에 할당된 볼륨의 씬 프로비저닝 효율성 점수입니다.
- * Overall Efficiency *: 계정에 할당된 볼륨의 전체 효율성 점수입니다.

계정을 편집합니다

계정을 편집하여 상태를 변경하거나 CHAP 암호를 변경하거나 계정 이름을 수정할 수 있습니다.

계정의 CHAP 설정을 수정하거나 액세스 그룹에서 이니시에이터 또는 볼륨을 제거하면 초기자가 예기치 않게 볼륨에 액세스할 수 없게 될 수 있습니다. 볼륨 액세스가 예기치 않게 손실되지 않는지 확인하려면 계정 또는 액세스 그룹 변경의 영향을 받는 iSCSI 세션을 항상 로그아웃하고 이니시에이터 설정 및 클러스터 설정을 변경한 후 초기자가 볼륨에 다시 연결할 수 있는지 확인합니다.

관리 서비스와 연결된 영구 볼륨은 설치 또는 업그레이드 중에 생성되는 새 계정에 할당됩니다. 영구 볼륨을 사용하는 경우 연결된 계정을 수정하거나 삭제하지 마십시오.

1. Management * > * Accounts * 를 선택합니다.
2. 계정의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Edit * 를 선택합니다.
4. * 선택 사항: * 사용자 이름 * 을 편집합니다.
5. * 선택 사항: * 상태 * 드롭다운 목록을 클릭하고 다른 상태를 선택합니다.

   상태를 * locked * 로 변경하면 계정에 대한 모든 iSCSI 연결이 종료되고 계정에 더 이상 액세스할 수 없습니다. 계정과 연결된 볼륨은 유지되지만 볼륨은 iSCSI를 검색할 수 없습니다.

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

   CHAP 설정 * 자격 증명을 변경하지 않으면 자격 증명은 그대로 유지됩니다. 자격 증명 필드를 비워 두면 새 암호가 생성됩니다.

7. 변경 내용 저장 * 을 클릭합니다.

계정을 삭제합니다

더 이상 필요하지 않은 계정은 삭제할 수 있습니다.

계정을 삭제하기 전에 계정과 연결된 모든 볼륨을 삭제하고 삭제하십시오.

관리 서비스와 연결된 영구 볼륨은 설치 또는 업그레이드 중에 생성되는 새 계정에 할당됩니다. 영구 볼륨을 사용하는 경우 연결된 계정을 수정하거나 삭제하지 마십시오.

1. Management * > * Accounts * 를 선택합니다.
2. 삭제할 계정의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 삭제 * 를 선택합니다.
4. 작업을 확인합니다.

자세한 내용을 확인하십시오

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

클러스터 관리자 사용자 계정을 관리합니다

SolidFire 스토리지 시스템의 클러스터 관리자 계정은 클러스터 관리자 계정을 생성, 삭제 및 편집하고, 클러스터 관리자 암호를 변경하고, 사용자에 대한 시스템 액세스를 관리하도록 LDAP 설정을 구성하여 관리할 수 있습니다.

스토리지 클러스터 관리자 계정 유형입니다

NetApp Element 소프트웨어를 실행하는 스토리지 클러스터에 존재할 수 있는 관리자 계정은 운영 클러스터 관리자 계정과 클러스터 관리자 계정 두 가지입니다.

- * 기본 클러스터 관리자 계정 *

  이 관리자 계정은 클러스터를 생성할 때 생성됩니다. 이 계정은 클러스터에 대한 최고 수준의 액세스 권한을 가진 기본 관리 계정입니다. 이 계정은 Linux 시스템의 루트 사용자와 유사합니다. 이 관리자 계정의 암호를 변경할 수 있습니다.

- * 클러스터 관리자 계정 *

  클러스터 관리자 계정에 제한된 범위의 관리 액세스 권한을 부여하여 클러스터 내에서 특정 작업을 수행할 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(LDAP가 아닌) 클러스터 관리자 계정이 필요합니다. 아직 클러스터에 속하지 않은 노드에 액세스하려면 계정 자격 증명이 필요하지 않습니다.

클러스터 관리자의 세부 정보를 봅니다

1. 클러스터 전체(LDAP가 아닌) 클러스터 관리자 계정을 생성하려면 다음 작업을 수행합니다.
   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 계정을 만들 때 지정한 이름입니다.
   - * 액세스 *: 사용자 계정에 할당된 사용자 권한. 가능한 값:
     - 읽기
     - 보고
     - 노드
     - 드라이브
     - 볼륨
     - 계정
     - 클러스터 관리자
     - 관리자

- 지원관리자

  모든 권한은 관리자 액세스 유형에 사용할 수 있습니다.

- * 유형 *: 클러스터 관리자의 유형입니다. 가능한 값:
  - 클러스터
  - LDAP를 지원합니다
- * 특성 *: 클러스터 관리자 계정이 Element API를 사용하여 생성된 경우 이 열에는 해당 방법을 사용하여 설정된 모든 이름 값 쌍이 표시됩니다.

  을 "NetApp Element 소프트웨어 API 참조서"참조하십시오.

클러스터 관리자 계정을 생성합니다

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

LDAP 클러스터 관리자 계정을 생성하려면 시작하기 전에 클러스터에 LDAP가 구성되어 있는지 확인하십시오.

"Element 사용자 인터페이스를 사용하여 LDAP 인증을 설정합니다"

나중에 보고, 노드, 드라이브, 볼륨, 계정 및 클러스터 레벨 액세스를 지원합니다. 사용 권한을 설정하면 시스템에서 해당 수준에 대한 쓰기 권한을 할당합니다. 시스템은 사용자가 선택하지 않은 수준에 대해 관리자 사용자에게 읽기 전용 액세스 권한을 부여합니다.

나중에 시스템 관리자가 생성한 모든 클러스터 관리자 사용자 계정을 제거할 수도 있습니다. 클러스터를 생성할 때 생성한 운영 클러스터 관리자 계정은 제거할 수 없습니다.

1. 클러스터 전체(LDAP가 아닌) 클러스터 관리자 계정을 생성하려면 다음 작업을 수행합니다.
   a. 사용자 * > * 클러스터 관리자 * 를 클릭합니다.
   b. Create Cluster Admin * 을 클릭합니다.
   c. Cluster * 사용자 유형을 선택합니다.
   d. 계정의 사용자 이름과 암호를 입력하고 암호를 확인합니다.
   e. 계정에 적용할 사용자 권한을 선택합니다.
   f. 최종 사용자 사용권 계약에 동의하려면 확인란을 선택합니다.
   g. Create Cluster Admin * 을 클릭합니다.
2. LDAP 디렉토리에 클러스터 관리자 계정을 생성하려면 다음 작업을 수행하십시오.
   a. Cluster * > * LDAP * 를 클릭합니다.
   b. LDAP 인증이 활성화되어 있는지 확인합니다.
   c. 사용자 인증 테스트 * 를 클릭하고 사용자에게 표시되는 고유 이름 또는 사용자가 구성원인 그룹 중 하나를 복사하여 나중에 붙여 넣을 수 있습니다.
   d. 사용자 * > * 클러스터 관리자 * 를 클릭합니다.

e. Create Cluster Admin * 을 클릭합니다.

f. LDAP 사용자 유형을 선택합니다.

g. 고유 이름 필드에서 텍스트 상자의 예제를 따라 사용자 또는 그룹의 전체 고유 이름을 입력합니다. 또는 이전에 복사한 고유 이름에서 붙여 넣습니다.

   고유 이름이 그룹의 일부인 경우 LDAP 서버에서 해당 그룹의 구성원인 사용자는 이 admin 계정의 권한을 갖게 됩니다.

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

a. 계정에 적용할 사용자 권한을 선택합니다.

b. 최종 사용자 사용권 계약에 동의하려면 확인란을 선택합니다.

c. Create Cluster Admin * 을 클릭합니다.

클러스터 관리자 권한을 편집합니다

보고, 노드, 드라이브, 볼륨, 계정 및 클러스터 레벨 액세스를 지원합니다. 사용 권한을 설정하면 시스템에서 해당 수준에 대한 쓰기 권한을 할당합니다. 시스템은 사용자가 선택하지 않은 수준에 대해 관리자 사용자에게 읽기 전용 액세스 권한을 부여합니다.

1. 사용자 * > * 클러스터 관리자 * 를 클릭합니다.
2. 편집할 클러스터 관리자의 작업 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. 계정에 적용할 사용자 권한을 선택합니다.
5. 변경 내용 저장 * 을 클릭합니다.

클러스터 관리자 계정의 암호를 변경합니다

Element UI를 사용하여 클러스터 관리자 암호를 변경할 수 있습니다.

1. 사용자 * > * 클러스터 관리자 * 를 클릭합니다.
2. 편집할 클러스터 관리자의 작업 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. 암호 변경 필드에 새 암호를 입력하고 확인합니다.
5. 변경 내용 저장 * 을 클릭합니다.

자세한 내용을 확인하십시오

- "Element 사용자 인터페이스를 사용하여 LDAP 인증을 설정합니다"
- "LDAP를 비활성화합니다"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

LDAP 관리

LDAP(Lightweight Directory Access Protocol)를 설정하여 SolidFire 스토리지에 대한 안전한 디렉터리 기반 로그인 기능을 사용할 수 있습니다. 클러스터 레벨에서 LDAP를 구성하고 LDAP 사용자 및 그룹에 권한을 부여할 수 있습니다.

LDAP를 관리하려면 기존 Microsoft Active Directory 환경을 사용하여 SolidFire 클러스터에 LDAP 인증을 설정하고 구성을 테스트해야 합니다.

IPv4와 IPv6 주소를 모두 사용할 수 있습니다.

LDAP 활성화에는 다음과 같은 고급 단계가 포함됩니다(자세한 설명 참조).

1. * LDAP 지원을 위한 완전한 사전 구성 단계 *. LDAP 인증을 구성하는 데 필요한 모든 세부 정보가 있는지 확인합니다.
2. * LDAP 인증 활성화 *. Element UI 또는 Element API를 사용합니다.
3. * LDAP 구성 검증 *. 필요에 따라 GetLdapConfiguration API 메서드를 실행하거나 Element UI를 사용하여 LCAP 구성을 확인하여 클러스터가 올바른 값으로 구성되었는지 확인합니다.
4. * LDAP 인증 테스트 * (사용자와 함께 `readonly`). TestLdapAuthentication API 메서드를 실행하거나 Element UI를 사용하여 LDAP 구성이 올바른지 테스트합니다. 이 초기 테스트에는 사용자의 사용자 이름 ""samAccountName""을 `readonly` 사용합니다. 이렇게 하면 클러스터가 LDAP 인증을 위해 올바르게 구성되어 있는지 확인하고 자격 증명과 액세스가 올바른지 `readonly` 확인합니다. 이 단계가 실패하면 1단계부터 3단계까지 반복합니다.
5. * LDAP 인증 * 을 테스트합니다(추가할 사용자 계정으로). Element 클러스터 관리자로 추가할 사용자 계정으로 setp 4를 반복합니다. `distinguished`이름(DN) 또는 사용자(또는 그룹)를 복사합니다. 이 DN은 6단계에서 사용됩니다.
6. * LDAP 클러스터 관리자 추가 * (LDAP 인증 테스트 단계에서 DN 복사 및 붙여넣기) Element UI 또는 AddLdapClusterAdmin API 메서드를 사용하여 적절한 액세스 수준으로 새 클러스터 관리자 사용자를 생성합니다. 사용자 이름의 경우 5단계에서 복사한 전체 DN을 붙여 넣습니다. 이렇게 하면 DN 형식이 올바르게 지정됩니다.
7. * 클러스터 관리자 액세스 테스트 *. 새로 생성한 LDAP 클러스터 admin 사용자를 사용하여 클러스터에 로그인합니다. LDAP 그룹을 추가한 경우 해당 그룹의 모든 사용자로 로그인할 수 있습니다.

LDAP 지원을 위한 사전 구성 단계를 완료합니다

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

단계

1. Windows Active Directory Server를 설정합니다.
2. * 선택 사항: * LDAPS 지원 활성화.
3. 사용자 및 그룹을 생성합니다.
4. LDAP 디렉토리 검색에 사용할 읽기 전용 서비스 계정("sfreadonly" 등)을 생성합니다.

Element 사용자 인터페이스를 사용하여 LDAP 인증을 설정합니다

기존 LDAP 서버와의 스토리지 시스템 통합을 구성할 수 있습니다. 이를 통해 LDAP 관리자는 사용자에 대한 스토리지

시스템 액세스를 중앙에서 관리할 수 있습니다.

Element 사용자 인터페이스 또는 Element API를 사용하여 LDAP를 구성할 수 있습니다. 이 절차에서는 Element UI를 사용하여 LDAP를 구성하는 방법에 대해 설명합니다.

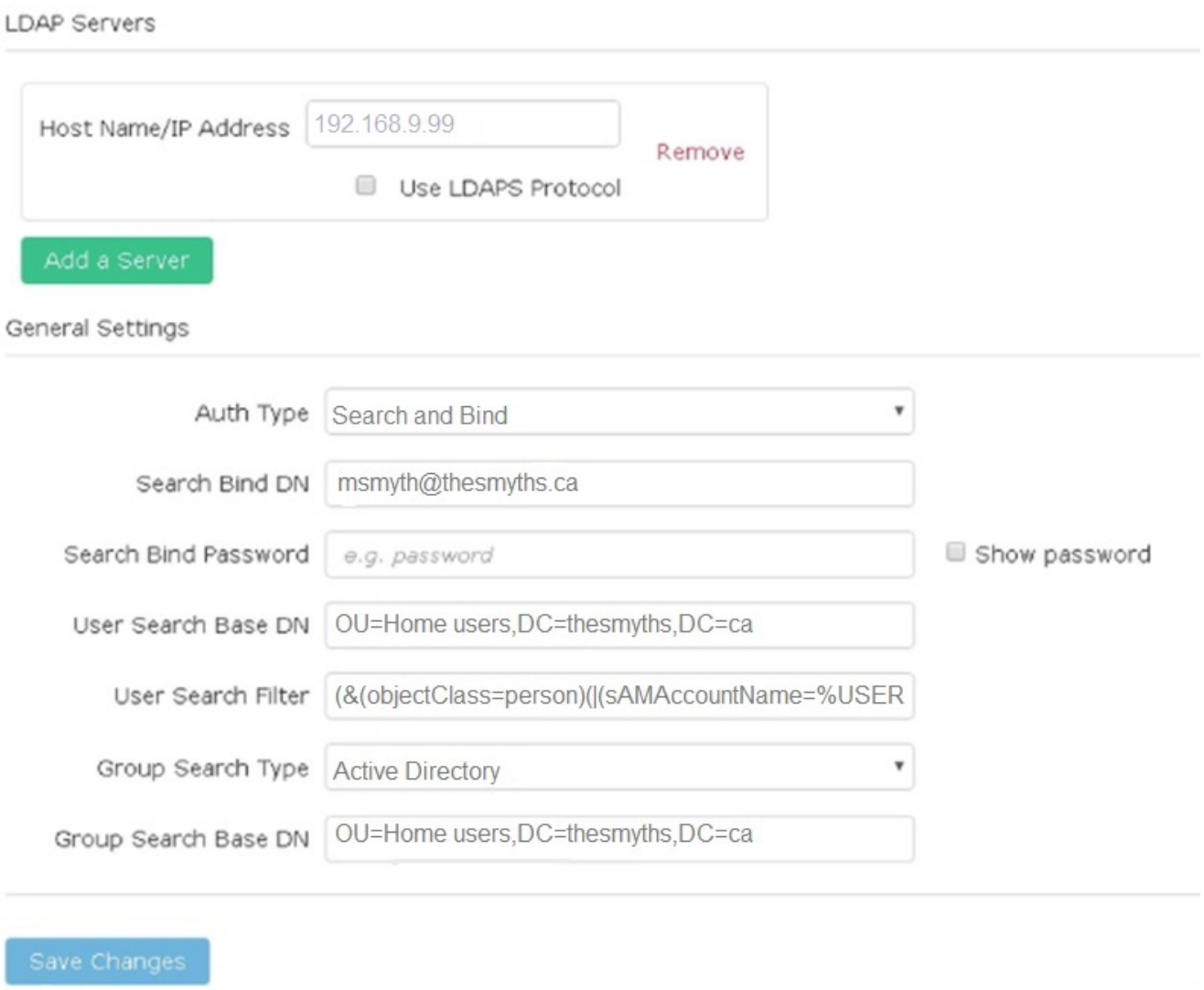
이 예에서는 SolidFire에서 LDAP 인증을 구성하는 방법과 인증 유형으로 를 사용하는 방법을 보여 `SearchAndBind` 줍니다. 이 예에서는 단일 Windows Server 2012 R2 Active Directory Server를 사용합니다.

단계

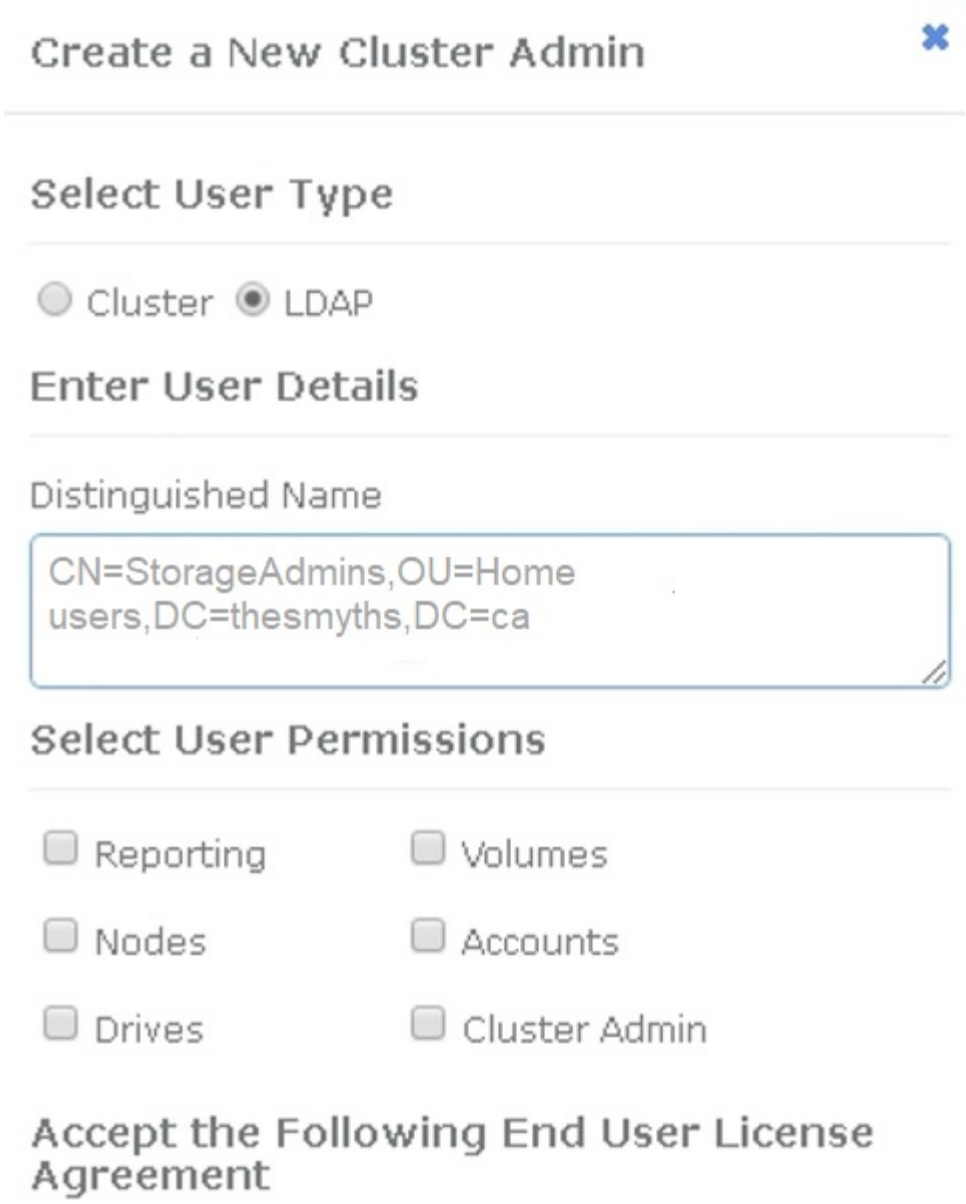
1. Cluster * > * LDAP * 를 클릭합니다.
2. 예 * 를 클릭하여 LDAP 인증을 활성화합니다.
3. 서버 추가 * 를 클릭합니다.
4. 호스트 이름/IP 주소 * 를 입력합니다.

   옵션 사용자 지정 포트 번호를 입력할 수도 있습니다.

   예를 들어, 사용자 지정 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 입력합니다.



7. LDAP * 활성화 를 클릭합니다.
8. 사용자에 대한 서버 액세스를 테스트하려면 * 사용자 인증 테스트 * 를 클릭합니다.
9. 클러스터 관리자를 생성할 때 나중에 사용할 수 있도록 표시되는 고유 이름 및 사용자 그룹 정보를 복사합니다.
10. 새 설정을 저장하려면 * 변경 사항 저장 * 을 클릭합니다.
11. 이 그룹에 사용자를 만들어 누구나 로그인할 수 있도록 하려면 다음을 완료합니다.
    a. 사용자 * > * 보기 * 를 클릭합니다.



b. 새 사용자의 경우 사용자 유형으로 * LDAP * 를 클릭하고 복사한 그룹을 고유 이름 필드에 붙여 넣습니다.
c. 사용 권한(일반적으로 모든 사용 권한)을 선택합니다.
d. 최종 사용자 사용권 계약까지 아래로 스크롤하여 * I accept * 를 클릭합니다.
e. Create Cluster Admin * 을 클릭합니다.

   이제 Active Directory 그룹 값을 가진 사용자가 있습니다.

이를 테스트하려면 Element UI에서 로그아웃한 후 해당 그룹의 사용자로 다시 로그인합니다.

Element API를 사용하여 **LDAP** 인증을 설정합니다

기존 LDAP 서버와의 스토리지 시스템 통합을 구성할 수 있습니다. 이를 통해 LDAP 관리자는 사용자에 대한 스토리지 시스템 액세스를 중앙에서 관리할 수 있습니다.

Element 사용자 인터페이스 또는 Element API를 사용하여 LDAP를 구성할 수 있습니다. 이 절차에서는 Element API를 사용하여 LDAP를 구성하는 방법에 대해 설명합니다.

SolidFire 클러스터에서 LDAP 인증을 활용하려면 먼저 API 방법을 사용하여 클러스터에서 LDAP 인증을 설정해야 합니다. `EnableLdapAuthentication`

단계

1. API 방법을 사용하여 클러스터에서 먼저 LDAP 인증을 활성화합니다 `EnableLdapAuthentication`.
2. 필요한 정보를 입력합니다.

```
{
      "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 매개 변수의 값을 변경합니다.

사용된 매개 변수	설명
AuthType: SearchAndBind	클러스터에서 인증된 사용자를 먼저 검색하고 찾은 경우 해당 사용자를 바인딩하기 위해 읽기 전용 서비스 계정을 사용하도록 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 보다 세분화된 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 보다 세분화된 하위 트리로 설정할 수 있습니다.
groupSearchType:ActiveDirectory입니다	Windows Active Directory 서버를 LDAP 서버로 사용합니다.

사용된 매개 변수	설명

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
userPrincipalName(로그인에 대한 이메일 주소)을 사용하려면 userSearchFilter를 다음과 같이 변경합니다.
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
또는 userPrincipalName 과 sAMAccountName 을 모두 검색하려면 다음 userSearchFilter 를 사용합니다.
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%username%)(userPrincipalName=%username%))"-----
	
	searchBindDN

sAMAccountName을 SolidFire 클러스터에 로그인하기 위한 사용자 이름으로 활용합니다. 이 설정은 LDAP에 sAMAccountName 속성에 로그인할 때 지정된 사용자 이름을 검색하도록 하고 objectClass 속성의 값으로 ""person""이 있는 항목으로 검색을 제한합니다.	
LDAP 디렉토리를 검색하는 데 사용되는 읽기 전용 사용자의 고유 이름입니다. Active Directory의 경우 일반적으로 사용자에게 userPrincipalName(전자 메일 주소 형식)을 사용하는 것이 가장 쉽습니다.	searchBindPassword를 입력합니다

이를 테스트하려면 Element UI에서 로그아웃한 후 해당 그룹의 사용자로 다시 로그인합니다.

LDAP 세부 정보 보기

클러스터 탭의 LDAP 페이지에서 LDAP 정보를 봅니다.

이러한 LDAP 구성 설정을 보려면 LDAP를 활성화해야 합니다.

1. Element UI로 LDAP 세부 정보를 보려면 * Cluster * > * LDAP * 를 클릭합니다.
   - * 호스트 이름/IP 주소 *: LDAP 또는 LDAPS 디렉토리 서버의 주소입니다.
   - * 인증 유형 *: 사용자 인증 방법. 가능한 값:
     - 직접 바인딩

- 검색 및 바인딩

- * Search Bind DN *: 사용자에 대한 LDAP 검색을 수행하기 위해 로그인할 수 있는 정규화된 DN(LDAP 디렉토리에 대한 바인딩 레벨 액세스 필요).
- * 검색 바인딩 암호 *: LDAP 서버에 대한 액세스를 인증하는 데 사용되는 암호입니다.
- * 사용자 검색 기준 DN *: 사용자 검색을 시작하는 데 사용되는 트리의 기본 DN. 시스템은 지정된 위치에서 하위 트리를 검색합니다.
- * 사용자 검색 필터 *: 도메인 이름을 사용하여 다음을 입력합니다.

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

- * 그룹 검색 유형 *: 사용되는 기본 그룹 검색 필터를 제어하는 검색 유형입니다. 가능한 값:
  - Active Directory: 사용자의 모든 LDAP 그룹의 중첩된 구성원
  - 그룹 없음: 그룹이 지원되지 않습니다.
  - 구성원 DN: 구성원 DN 스타일 그룹(단일 수준).
- * 그룹 검색 기준 DN *: 그룹 검색을 시작하는 데 사용되는 트리의 기본 DN. 시스템은 지정된 위치에서 하위 트리를 검색합니다.
- * 사용자 인증 테스트 *: LDAP가 구성된 후 이를 사용하여 LDAP 서버에 대한 사용자 이름 및 암호 인증을 테스트합니다. 이미 존재하는 계정을 입력하여 테스트합니다. 고유 이름 및 사용자 그룹 정보가 표시되며, 이 정보는 나중에 클러스터 관리자를 생성할 때 사용할 수 있도록 복사할 수 있습니다.

LDAP 구성을 테스트합니다

LDAP를 구성한 후에는 Element UI 또는 Element API 방법을 사용하여 테스트해야 `TestLdapAuthentication` 합니다.

단계

1. Element UI를 사용하여 LDAP 구성을 테스트하려면 다음을 수행합니다.
   a. Cluster * > * LDAP * 를 클릭합니다.
   b. LDAP 인증 테스트 * 를 클릭합니다.
   c. 아래 표의 정보를 사용하여 문제를 해결하십시오.

오류 메시지	설명
`xLDAPUserNotFound`	• 구성된 하위 트리에서 테스트 중인 사용자를 찾을 `userSearchBaseDN` 수 없습니다. • 가 `userSearchFilter` 잘못 구성되었습니다.
`xLDAPBindFailed (Error: Invalid credentials)`	• 테스트 중인 사용자 이름은 유효한 LDAP 사용자이지만 입력한 암호가 올바르지 않습니다. • 테스트 중인 사용자 이름은 유효한 LDAP 사용자이지만 계정은 현재 비활성화되어 있습니다.

오류 메시지	설명
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	LDAP 서버 URI가 잘못되었습니다.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	읽기 전용 사용자 이름 또는 암호가 잘못 구성되었습니다.
`xLDAPSearchFailed (Error: No such object)`	가 `userSearchBaseDN` LDAP 트리 내의 올바른 위치가 아닙니다.
`xLDAPSearchFailed (Error: Referral)`	• 가 `userSearchBaseDN` LDAP 트리 내의 올바른 위치가 아닙니다. • 및 `groupSearchBaseDN` 는 `userSearchBaseDN` 중첩된 OU에 있습니다. 이로 인해 권한 문제가 발생할 수 있습니다. 해결 방법은 사용자 및 그룹 기본 DN 항목에 OU를 포함하는 것입니다(예 `ou=storage, cn=company, cn=com`:).

2. Element API를 사용하여 LDAP 구성을 테스트하려면 다음을 수행합니다.
   a. TestLdapAuthentication 메서드를 호출합니다.

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

   b. 결과를 검토합니다. API 호출이 성공한 경우 지정된 사용자의 고유 이름과 사용자가 구성원인 그룹 목록이 결과에 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"
     }
}
```

LDAP를 비활성화합니다

Element UI를 사용하여 LDAP 통합을 비활성화할 수 있습니다.

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

단계

1. Cluster * > * LDAP * 를 클릭합니다.
2. 아니요 * 를 클릭합니다.
3. LDAP 비활성화 * 를 클릭합니다.

자세한 내용을 확인하십시오

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

저작권 정보

상표 정보