



디렉토리 서비스를 사용합니다

SANtricity 11.7

NetApp
February 12, 2024

목차

디렉토리 서비스를 사용합니다	1
디렉토리 서버를 추가합니다	1
디렉토리 서버 설정 및 역할 매핑을 편집합니다	5
디렉토리 서버를 제거합니다	8

디렉토리 서비스를 사용합니다

디렉토리 서버를 추가합니다

액세스 관리에 대한 인증을 구성하려면 Unified Manager용 웹 서비스 프록시를 실행하는 호스트와 LDAP 서버 간의 통신을 설정해야 합니다. 그런 다음 LDAP 사용자 그룹을 로컬 사용자 역할에 매핑합니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- 사용자 그룹은 디렉토리 서비스에 정의되어 있어야 합니다.
- 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
- 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.

이 작업에 대해

디렉토리 서버를 추가하는 과정은 2단계로 이루어집니다. 먼저 도메인 이름과 URL을 입력합니다. 서버에서 보안 프로토콜을 사용하는 경우 비표준 서명 기관이 서명한 경우 인증을 위해 CA 인증서도 업로드해야 합니다. 바인딩 계정에 대한 자격 증명에 있는 경우 사용자 계정 이름 및 암호를 입력할 수도 있습니다. 다음으로 LDAP 서버의 사용자 그룹을 로컬 사용자 역할에 매핑합니다.

단계

1. 액세스 관리 * 를 선택합니다.
2. 디렉토리 서비스 * 탭에서 * 디렉토리 서버 추가 * 를 선택합니다.

디렉토리 서버 추가 대화 상자가 열립니다.

3. 서버 설정 * 탭에서 LDAP 서버의 자격 증명을 입력합니다.

필드 상세정보

설정	설명
<ul style="list-style-type: none"> • 구성 설정 * 	도메인
LDAP 서버의 도메인 이름을 입력합니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인(<i>username@domain</i>)에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.	서버 URL
LDAP 서버에 액세스하기 위한 URL을 형식으로 입력합니다 ldap[s]:// host :*port*	인증서 업로드(선택 사항)
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">  </div> <div> <p>이 필드는 LDAPS 프로토콜이 위의 서버 URL 필드에 지정된 경우에만 나타납니다.</p> </div> </div> <p>찾아보기 * 를 클릭하고 업로드할 CA 인증서를 선택합니다. LDAP 서버를 인증하는 데 사용되는 신뢰할 수 있는 인증서 또는 인증서 체인입니다.</p>	BIND ACCOUNT(선택 사항)

설정	설명
<p>LDAP 서버에 대한 검색 쿼리 및 그룹 내에서 검색할 읽기 전용 사용자 계정을 입력합니다. LDAP 유형 형식으로 계정 이름을 입력합니다. 예를 들어, 바인딩 사용자가 "bindacct"라고 하는 경우 등의 값을 입력할 수 있습니다 CN=bindacct,CN=Users,DC=cpoc,DC=local.</p>	<p>바인딩 암호(선택 사항)</p>
<div style="display: flex; align-items: center;">  <div style="border-left: 1px solid #ccc; padding-left: 10px;"> <p>이 필드는 바인딩 계정을 입력할 때 나타납니다.</p> </div> </div> <p>바인딩 계정의 암호를 입력합니다.</p>	<p>추가하기 전에 서버 연결을 테스트합니다</p>
<p>시스템이 입력한 LDAP 서버 구성과 통신할 수 있는지 확인하려면 이 확인란을 선택합니다. 이 테스트는 대화 상자 하단의 * 추가 * 를 클릭하면 발생합니다.</p> <p>이 확인란을 선택하고 테스트에 실패하면 구성이 추가되지 않습니다. 오류를 해결하거나 확인란을 선택 취소해야 테스트를 건너뛰고 구성을 추가할 수 있습니다.</p>	<p>• 권한 설정 *</p>
<p>검색 기준 DN</p>	<p>LDAP 컨텍스트를 입력하여 사용자를 검색합니다(일반적으로 의 형식) CN=Users, DC=cpoc, DC=local.</p>
<p>사용자 이름 특성입니다</p>	<p>인증을 위해 사용자 ID에 바인딩된 특성을 입력합니다. 예를 들면 다음과 같습니다. sAMAccountName.</p>

설정	설명
그룹 속성	그룹 대 역할 매핑에 사용되는 사용자의 그룹 속성 목록을 입력합니다. 예를 들면 다음과 같습니다. <code>memberOf, managedObjects</code> .

- 역할 매핑 * 탭을 클릭합니다.
- 미리 정의된 역할에 LDAP 그룹을 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.

필드 상세정보

설정	설명
• 매핑 *	그룹 DN
매핑할 LDAP 사용자 그룹의 그룹 DN(고유 이름)을 지정합니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 정규식 패턴의 일부가 아닌 경우 백슬래시(\)로 이스케이프되어야 합니다. <code>\.[]{}() <> * +-=!/?^\$</code>	
역할	<p>필드를 클릭하고 그룹 DN에 매핑할 로컬 사용자 역할 중 하나를 선택합니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. SANtricity Unified Manager에 로그인하려면 Monitor 역할이 다른 역할과 함께 필요합니다. 매핑된 역할에는 다음 권한이 포함됩니다.</p> <ul style="list-style-type: none"> • * 스토리지 관리자 * — 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다. • * 보안 관리자 * — 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다. • * 지원 관리자 * — 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다. • * Monitor * — 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.



Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다.

- 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
- 매핑을 마쳤으면 * 추가 * 를 클릭합니다.

시스템은 스토리지 시스템 및 LDAP 서버가 통신할 수 있도록 검증을 수행합니다. 오류 메시지가 나타나면 대화 상자에 입력한 자격 증명을 확인하고 필요한 경우 정보를 다시 입력합니다.

디렉토리 서버 설정 및 역할 매핑을 편집합니다

이전에 Access Management에서 디렉토리 서버를 구성한 경우 언제든지 해당 설정을 변경할 수 있습니다. 설정에는 서버 연결 정보와 그룹 대 역할 매핑이 포함됩니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- 디렉토리 서버를 정의해야 합니다.

단계

1. 액세스 관리 * 를 선택합니다.
2. 디렉토리 서비스 * 탭을 선택합니다.
3. 둘 이상의 서버가 정의된 경우 테이블에서 편집할 서버를 선택합니다.
4. 설정 보기/편집 * 을 선택합니다.

Directory Server Settings(디렉토리 서버 설정) 대화 상자가 열립니다.

5. 서버 설정 * 탭에서 원하는 설정을 변경합니다.

필드 상세정보

설정	설명
• 구성 설정 *	도메인
LDAP 서버의 도메인 이름입니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인(<i>username@domain</i>)에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.	서버 URL
의 형식으로 LDAP 서버에 액세스하기 위한 URL입니다 <code>ldap[s]://host:port.</code>	BIND ACCOUNT(선택 사항)
LDAP 서버에 대한 검색 쿼리 및 그룹 내 검색을 위한 읽기 전용 사용자 계정입니다.	바인딩 암호(선택 사항)
바인딩 계정의 암호입니다. (이 필드는 바인딩 계정을 입력할 때 나타납니다.)	저장하기 전에 서버 연결을 테스트합니다
시스템이 LDAP 서버 구성과 통신할 수 있는지 확인합니다. 테스트는 * 저장 * 을 클릭한 후에 수행됩니다. 이 확인란을 선택하고 검사에 실패하면 구성이 변경되지 않습니다. 테스트를 건너뛰고 구성을 다시 편집하려면 오류를 해결하거나 확인란을 선택 해제해야 합니다.	• 권한 설정 *
검색 기준 DN	사용자를 검색하는 LDAP 컨텍스트로, 일반적으로 의 형식입니다 <code>CN=Users, DC=cpoc, DC=local.</code>

설정	설명
사용자 이름 특성입니다	인증을 위해 사용자 ID에 바인딩된 속성입니다. 예를 들면 다음과 같습니다. sAMAccountName.
그룹 속성	그룹-역할 매핑에 사용되는 사용자의 그룹 속성 목록입니다. 예를 들면 다음과 같습니다. memberOf, managedObjects.

6. 역할 매핑 * 탭에서 원하는 매핑을 변경합니다.

필드 상세정보

설정	설명
• 매핑 *	그룹 DN
매핑할 LDAP 사용자 그룹의 도메인 이름입니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 정규식 패턴의 일부가 아닌 경우 백슬래시(\)로 이스케이프되어야 합니다. \ <> * +-=!/?^\$	
역할	<p>그룹 DN에 매핑할 역할입니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. SANtricity Unified Manager에 로그인하려면 Monitor 역할이 다른 역할과 함께 필요합니다. 역할은 다음과 같습니다.</p> <ul style="list-style-type: none"> • * 스토리지 관리자 * — 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다. • * 보안 관리자 * — 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다. • * 지원 관리자 * — 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다. • * Monitor * — 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.



Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다.

7. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.

8. 저장 * 을 클릭합니다.

결과

이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

디렉토리 서버를 제거합니다

디렉토리 서버와 웹 서비스 프록시 간의 연결을 끊는 경우 Access Management 페이지에서 서버 정보를 제거할 수 있습니다. 새 서버를 구성한 다음 이전 서버를 제거하려는 경우 이 작업을 수행할 수 있습니다.

시작하기 전에

보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

이 작업에 대해

이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

단계

1. 액세스 관리 * 를 선택합니다.
2. 디렉토리 서비스 * 탭을 선택합니다.
3. 목록에서 삭제할 디렉토리 서버를 선택합니다.
4. 제거 * 를 클릭합니다.

디렉토리 서버 제거 대화 상자가 열립니다.

5. 유형 remove 필드에서 * 제거 * 를 클릭합니다.

디렉토리 서버 구성 설정, 권한 설정 및 역할 매핑이 제거됩니다. 사용자는 더 이상 이 서버의 자격 증명으로 로그인할 수 없습니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.