



인증 관리

Active IQ Unified Manager 9.12

NetApp

December 18, 2023

목차

인증 관리	1
인증 서버 편집	1
인증 서버를 삭제하는 중입니다	1
Active Directory 또는 OpenLDAP를 사용한 인증	2
로깅 감사	2
원격 인증 페이지	4

인증 관리

Unified Manager 서버에서 LDAP 또는 Active Directory를 사용하여 인증을 설정하고 서버와 함께 작동하도록 구성하여 원격 사용자를 인증할 수 있습니다.

원격 인증 활성화, 인증 서비스 설정 및 인증 서버 추가에 대한 자세한 내용은 * Unified Manager에서 경고 알림을 보내도록 구성 * 의 이전 섹션을 참조하십시오.

인증 서버 편집

Unified Manager 서버가 인증 서버와 통신하는 데 사용하는 포트를 변경할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
2. 중첩된 그룹 조회 사용 안 함 * 상자를 선택합니다.
3. Authentication Servers * 영역에서 편집할 인증 서버를 선택한 다음 * Edit * 를 클릭합니다.
4. 인증 서버 편집 * 대화 상자에서 포트 세부 정보를 편집합니다.
5. 저장 * 을 클릭합니다.

인증 서버를 삭제하는 중입니다

Unified Manager 서버가 인증 서버와 통신하지 못하도록 하려면 인증 서버를 삭제할 수 있습니다. 예를 들어 관리 서버가 통신하는 인증 서버를 변경하려는 경우 인증 서버를 삭제하고 새 인증 서버를 추가할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

인증 서버를 삭제하면 인증 서버의 원격 사용자 또는 그룹이 Unified Manager에 더 이상 액세스할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
2. 삭제할 인증 서버를 하나 이상 선택한 다음 * 삭제 * 를 클릭합니다.
3. 예 * 를 클릭하여 삭제 요청을 확인합니다.

보안 연결 사용 * 옵션을 활성화하면 인증 서버와 연관된 인증서가 인증 서버와 함께 삭제됩니다.

Active Directory 또는 OpenLDAP를 사용한 인증

관리 서버에서 원격 인증을 사용하도록 설정하고 인증 서버 내의 사용자가 Unified Manager에 액세스할 수 있도록 인증 서버와 통신하도록 관리 서버를 구성할 수 있습니다.

다음 미리 정의된 인증 서비스 중 하나를 사용하거나 고유한 인증 서비스를 지정할 수 있습니다.

- Microsoft Active Directory를 클릭합니다



Microsoft Lightweight Directory Services는 사용할 수 없습니다.

- OpenLDAP를 클릭합니다

필요한 인증 서비스를 선택하고 적절한 인증 서버를 추가하여 인증 서버의 원격 사용자가 Unified Manager에 액세스할 수 있도록 할 수 있습니다. 원격 사용자 또는 그룹에 대한 자격 증명은 인증 서버에서 관리합니다. 관리 서버는 LDAP(Lightweight Directory Access Protocol)를 사용하여 구성된 인증 서버 내에서 원격 사용자를 인증합니다.

Unified Manager에서 만든 로컬 사용자의 경우 관리 서버에서 사용자 이름과 암호 데이터베이스를 자체적으로 유지 관리합니다. 관리 서버는 인증을 수행하고 Active Directory 또는 OpenLDAP를 인증에 사용하지 않습니다.

로깅 감사

감사 로그를 사용하여 감사 로그가 손상되었는지 여부를 감지할 수 있습니다. 사용자가 수행하는 모든 작업은 감사 로그에 모니터링 및 기록됩니다. 감사는 Active IQ Unified Manager의 모든 사용자 인터페이스 및 공개적으로 노출된 API 기능에 대해 수행됩니다.

감사 로그: 파일 보기 * 를 사용하여 Active IQ Unified Manager에서 사용 가능한 모든 감사 로그 파일을 보고 액세스할 수 있습니다. Audit Log: File View(감사 로그: 파일 보기)의 파일은 생성 날짜를 기준으로 나열됩니다. 이 보기에는 설치 또는 업그레이드 시 캡처된 모든 감사 로그의 정보가 시스템에 있는 것으로 표시됩니다. Unified Manager에서 작업을 수행할 때마다 정보가 업데이트되고 로그에서 사용할 수 있습니다. 각 로그 파일의 상태는 로그 파일의 변조 또는 삭제를 감지하기 위해 능동적으로 모니터링되는 ""파일 무결성 상태"" 속성을 사용하여 캡처됩니다. 시스템에서 감사 로그를 사용할 수 있는 경우 감사 로그에 다음 상태 중 하나가 포함될 수 있습니다.

상태	설명
활성	로그가 현재 로그되고 있는 파일입니다.
정상	비활성, 압축 및 시스템에 저장된 파일입니다.
변조되었습니다	파일을 수동으로 편집한 사용자에게 의해 손상된 파일입니다.
manual_delete(수동 삭제)	권한이 있는 사용자가 삭제한 파일입니다.
롤오버_삭제	롤링 구성 정책에 따라 롤오프로 인해 삭제된 파일입니다.
Unexpected_delete를 선택합니다	알 수 없는 이유로 삭제된 파일입니다.

감사 로그 페이지에는 다음과 같은 명령 단추가 있습니다.

- 구성
- 삭제
- 다운로드

delete * 버튼을 사용하면 Audit Logs 보기에 나열된 감사 로그를 삭제할 수 있습니다. 감사 로그를 삭제하고 나중에 유효한 삭제를 확인하는 데 도움이 되는 파일을 삭제할 이유를 선택적으로 제공할 수 있습니다. Reason 열에는 삭제 작업을 수행한 사용자의 이름과 함께 이유가 나열됩니다.



로그 파일을 삭제하면 시스템에서 파일이 삭제되지만 DB 테이블의 항목은 삭제되지 않습니다.

감사 로그 섹션의 * 다운로드 * 버튼을 사용하여 Active IQ Unified Manager에서 감사 로그를 다운로드하고 감사 로그 파일을 내보낼 수 있습니다. "정상" 또는 "무단 변경"으로 표시된 파일은 압축된 상태로 다운로드됩니다. .gzip 형식.

감사 로그 파일은 주기적으로 보관되며 참조를 위해 데이터베이스에 저장됩니다. 보관 전에 보안 및 무결성을 유지하기 위해 감사 로그에 디지털 서명됩니다.

전체 AutoSupport 번들이 생성되면 지원 번들에는 아카이빙 및 액티브 감사 로그 파일이 모두 포함됩니다. 하지만 간단한 지원 번들이 생성되면 활성 감사 로그만 포함됩니다. 보관된 감사 로그는 포함되지 않습니다.

감사 로그 구성

감사 로그 섹션의 * 구성 * 버튼을 사용하여 감사 로그 파일에 대한 롤링 정책을 구성하고 감사 로그에 대한 원격 로깅을 활성화할 수 있습니다.

시스템에 저장할 데이터의 양과 빈도에 따라 * MAX 파일 크기 * 및 * 감사 로그 보존 일 * 의 값을 설정할 수 있습니다. 필드 * 총 감사 로그 크기 * 의 값은 시스템에 있는 총 감사 로그 데이터의 크기입니다. 롤오버 정책은 * 감사 로그 보존 기간 *, * 최대 파일 크기 * 및 * 총 감사 로그 크기 * 필드의 값에 따라 결정됩니다. 감사 로그 백업의 크기가 * TOTAL AUDIT LOG SIZE * 에 구성된 값에 도달하면 먼저 아카이빙된 파일이 삭제됩니다. 즉, 가장 오래된 파일이 삭제됩니다. 그러나 파일 항목은 데이터베이스에서 계속 사용할 수 있으며 ""롤오버 삭제""로 표시됩니다. 감사 로그 보존 기간 * 값은 감사 로그 파일이 보존되는 일수입니다. 이 필드에 설정된 값보다 오래된 파일은 롤오버됩니다.

단계

1. 감사 로그 * >> * 구성 * 을 클릭합니다.
2. 최대 파일 크기 *, * 총 감사 로그 크기 * 및 * 감사 로그 보존 기간 * 에 값을 입력합니다.

원격 로깅을 활성화하려면 * 원격 로깅 사용 * 을 선택해야 합니다.

감사 로그의 원격 로깅을 사용하도록 설정합니다

감사 로그 구성 대화 상자에서 * 원격 로깅 사용 * 확인란을 선택하여 원격 감사 로깅을 활성화할 수 있습니다. 이 기능을 사용하여 감사 로그를 원격 Syslog 서버로 전송할 수 있습니다. 이렇게 하면 공간 제약 조건이 있을 때 감사 로그를 관리할 수 있습니다.

감사 로그의 원격 로깅은 Active IQ Unified Manager 서버의 감사 로그 파일이 변조될 경우에 대비하여 변조 불가능한 백업을 제공합니다.

단계

1. 감사 로그 구성 * 대화 상자에서 * 원격 로깅 사용 * 확인란을 선택합니다.

원격 로깅을 구성하는 추가 필드가 표시됩니다.

2. 연결할 원격 서버의 * HOSTNAME * 및 * 포트 * 를 입력합니다.
3. server CA certificate * 필드에서 * browse * 를 클릭하여 대상 서버의 공용 인증서를 선택합니다.

인증서를 업로드해야 합니다 .pem 형식. 이 인증서는 대상 Syslog 서버에서 받아야 하며 만료되지 않아야 합니다. 인증서는 의 일부로 선택한 "호스트 이름"을 포함해야 합니다 SubjectAltName (SAN) 속성.

4. * CHARSET *, * CONNECTION TIMEOUT *, * 재연결 지연 * 필드에 값을 입력합니다.

이러한 필드의 값은 밀리초 단위입니다.

5. 필요한 Syslog 형식과 TLS 프로토콜 버전을 * format * 및 * protocol * 필드에서 선택합니다.
6. 대상 Syslog 서버에 인증서 기반 인증이 필요한 경우 * 클라이언트 인증 활성화 * 확인란을 선택합니다.

감사 로그 구성을 저장하기 전에 클라이언트 인증 인증서를 다운로드하여 Syslog 서버에 업로드해야 합니다. 그렇지 않으면 연결이 실패합니다. Syslog 서버의 유형에 따라 클라이언트 인증 인증서의 해시를 만들어야 할 수도 있습니다.

예: syslog-ng 명령을 사용하여 인증서의 <hash>를 만들어야 합니다 `openssl x509 -noout -hash -in cert.pem` 그런 다음 클라이언트 인증 인증서를 <hash>.0 뒤에 명명된 파일에 연결해야 합니다.

7. 저장 * 을 클릭하여 서버와의 연결을 구성하고 원격 로깅을 활성화합니다.

감사 로그 페이지로 리디렉션됩니다.

원격 인증 페이지

원격 인증 페이지를 사용하여 Unified Manager 웹 UI에 로그인하려는 원격 사용자를 인증하도록 Unified Manager를 인증 서버와 통신하도록 구성할 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

원격 인증 활성화 확인란을 선택한 후 인증 서버를 사용하여 원격 인증을 활성화할 수 있습니다.

• * 인증 서비스 *

Active Directory, OpenLDAP 등의 디렉터리 서비스 공급자에서 사용자를 인증하도록 관리 서버를 구성하거나 고유한 인증 메커니즘을 지정할 수 있습니다. 원격 인증을 설정한 경우에만 인증 서비스를 지정할 수 있습니다.

◦ * Active Directory *

▪ 관리자 이름

인증 서버의 관리자 이름을 지정합니다.

▪ 암호

인증 서버에 액세스할 암호를 지정합니다.

- 기본 고유 이름

인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 `+ou@domain.com` +인 경우 기본 고유 이름은 `* cn=ou, dc=domain, dc=com *` 입니다.

- 중첩된 그룹 조회를 비활성화합니다

중첩 그룹 조회 옵션을 사용할지 여부를 지정합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. Active Directory를 사용하는 경우 중첩된 그룹에 대한 지원을 비활성화하여 인증 속도를 높일 수 있습니다.

- 보안 연결을 사용합니다

인증 서버와 통신하는 데 사용되는 인증 서비스를 지정합니다.

- * OpenLDAP *

- 고유 이름 바인딩

인증 서버에서 원격 사용자를 찾기 위해 기본 고유 이름과 함께 사용되는 바인딩 고유 이름을 지정합니다.

- 바인딩 암호

인증 서버에 액세스할 암호를 지정합니다.

- 기본 고유 이름

인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 `+ou@domain.com` +인 경우 기본 고유 이름은 `* cn=ou, dc=domain, dc=com *` 입니다.

- 보안 연결을 사용합니다

LDAP 인증 서버와 통신하는 데 Secure LDAP를 사용하도록 지정합니다.

- 기타 *

- 고유 이름 바인딩

구성한 인증 서버에서 원격 사용자를 찾기 위해 기본 고유 이름과 함께 사용되는 바인딩 고유 이름을 지정합니다.

- 바인딩 암호

인증 서버에 액세스할 암호를 지정합니다.

- 기본 고유 이름

인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 `+ou@domain.com` +인 경우 기본 고유 이름은 `* cn=ou, dc=domain, dc=com *` 입니다.

- 프로토콜 버전

인증 서버에서 지원하는 LDAP(Lightweight Directory Access Protocol) 버전을 지정합니다. 프로토콜

버전을 자동으로 감지할지 또는 버전을 2나 3으로 설정할지 지정할 수 있습니다.

- 사용자 이름 특성

관리 서버에서 인증할 사용자 로그인 이름이 포함된 인증 서버의 속성 이름을 지정합니다.

- 그룹 구성원 자격 특성

사용자의 인증 서버에 지정된 속성 및 값을 기반으로 관리 서버 그룹 구성원 자격을 원격 사용자에게 할당하는 값을 지정합니다.

- UGID

원격 사용자가 인증 서버에 `groupOfUniqueNames` 개체의 구성원으로 포함된 경우 이 옵션을 사용하면 해당 `groupOfUniqueNames` 개체의 지정된 속성에 따라 관리 서버 그룹 구성원을 원격 사용자에게 할당할 수 있습니다.

- 중첩된 그룹 조회를 비활성화합니다

중첩 그룹 조회 옵션을 사용할지 여부를 지정합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. Active Directory를 사용하는 경우 중첩된 그룹에 대한 지원을 비활성화하여 인증 속도를 높일 수 있습니다.

- 회원

인증 서버가 그룹의 개별 구성원에 대한 정보를 저장하는 데 사용하는 속성 이름을 지정합니다.

- 사용자 객체 클래스

원격 인증 서버에 있는 사용자의 객체 클래스를 지정합니다.

- 그룹 객체 클래스

원격 인증 서버에 있는 모든 그룹의 객체 클래스를 지정합니다.



Member, User 개체 클래스 및 *Group* 개체 클래스 속성에 입력하는 값은 Active Directory, OpenLDAP 및 LDAP 구성에 추가된 값과 같아야 합니다. 그렇지 않으면 인증에 실패할 수 있습니다.

- 보안 연결을 사용합니다

인증 서버와 통신하는 데 사용되는 인증 서비스를 지정합니다.



인증 서비스를 수정하려면 기존 인증 서버를 삭제하고 새 인증 서버를 추가해야 합니다.

Authentication Servers 영역

인증 서버 영역에는 관리 서버가 원격 사용자를 찾고 인증하기 위해 통신하는 인증 서버가 표시됩니다. 원격 사용자 또는 그룹에 대한 자격 증명은 인증 서버에서 관리합니다.

• * 명령 버튼 *

인증 서버를 추가, 편집 또는 삭제할 수 있습니다.

- 추가

인증 서버를 추가할 수 있습니다.

추가하려는 인증 서버가 같은 데이터베이스를 사용하는 고가용성 쌍의 일부인 경우 파트너 인증 서버를 추가할 수도 있습니다. 이렇게 하면 인증 서버 중 하나에 연결할 수 없을 때 관리 서버가 파트너와 통신할 수 있습니다.

- 편집

선택한 인증 서버에 대한 설정을 편집할 수 있습니다.

- 삭제

선택한 인증 서버를 삭제합니다.

- * 이름 또는 IP 주소 *

관리 서버에서 사용자를 인증하는 데 사용되는 인증 서버의 호스트 이름 또는 IP 주소를 표시합니다.

- * 포트 *

인증 서버의 포트 번호를 표시합니다.

- * 인증 테스트 *

이 단추는 원격 사용자 또는 그룹을 인증하여 인증 서버 구성을 확인합니다.

테스트하는 동안 사용자 이름만 지정하면 관리 서버가 인증 서버에서 원격 사용자를 검색하지만 사용자를 인증하지는 않습니다. 사용자 이름과 암호를 모두 지정하면 관리 서버가 원격 사용자를 검색하고 인증합니다.

원격 인증이 비활성화되어 있으면 인증을 테스트할 수 없습니다.

저작권 정보

Copyright © 2023 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.