인증 관리

Active IQ Unified Manager

NetApp
May 15, 2026

목차

인증 관리

Unified Manager 서버에서 LDAP 또는 Active Directory를 사용하여 인증을 활성화하고 원격 사용자를 인증하기 위해 서버와 함께 작동하도록 구성할 수 있습니다.

원격 인증 활성화, 인증 서비스 설정 및 인증 서버 추가에 대한 자세한 내용은 이전 섹션인 *Unified Manager를 구성하여 알림 보내기*를 참조하세요.

인증 서버 편집

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

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 중첩 그룹 조회 비활성화 상자를 선택하세요.
3. 인증 서버 영역에서 편집하려는 인증 서버를 선택한 다음 *편집*을 클릭합니다.
4. 인증 서버 편집 대화 상자에서 포트 세부 정보를 편집합니다.
5. *저장*을 클릭하세요.

인증 서버 삭제

Unified Manager 서버가 인증 서버와 통신하는 것을 방지하려면 인증 서버를 삭제할 수 있습니다. 예를 들어, 관리 서버가 통신하는 인증 서버를 변경하려는 경우 인증 서버를 삭제하고 새 인증 서버를 추가할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

인증 서버를 삭제하면 인증 서버의 원격 사용자나 그룹은 더 이상 Unified Manager에 액세스할 수 없습니다.

단계

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

   보안 연결 사용 옵션이 활성화된 경우 인증 서버와 연결된 인증서가 인증 서버와 함께 삭제됩니다.

Active Directory 또는 OpenLDAP를 통한 인증

관리 서버에서 원격 인증을 활성화하고 관리 서버가 인증 서버와 통신하도록 구성하여 인증 서버

내의 사용자가 Unified Manager에 액세스할 수 있도록 할 수 있습니다.

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

- 마이크로소프트 액티브 디렉토리

  Microsoft Lightweight Directory Services를 사용할 수 없습니다.

- 오픈LDAP

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

Unified Manager에서 생성된 로컬 사용자의 경우, 관리 서버는 사용자 이름과 비밀번호의 자체 데이터베이스를 유지 관리합니다. 관리 서버는 인증을 수행하며 인증을 위해 Active Directory나 OpenLDAP를 사용하지 않습니다.

감사 로깅

감사 로그를 사용하면 감사 로그가 손상되었는지 감지할 수 있습니다. 사용자가 수행하는 모든 활동은 모니터링되어 감사 로그에 기록됩니다. 감사는 Active IQ Unified Manager 의 모든 사용자 인터페이스와 공개적으로 노출된 API 기능에 대해 수행됩니다.

*감사 로그: 파일 보기*를 사용하면 Active IQ Unified Manager 에서 사용 가능한 모든 감사 로그 파일을 보고 액세스할 수 있습니다. 감사 로그: 파일 보기의 파일은 생성 날짜를 기준으로 나열됩니다. 이 보기에서는 시스템에 설치 또는 업그레이드한 이후 현재까지 캡처된 모든 감사 로그에 대한 정보가 표시됩니다. Unified Manager에서 작업을 수행할 때마다 정보가 업데이트되어 로그에서 사용할 수 있습니다. 각 로그 파일의 상태는 "파일 무결성 상태" 속성을 사용하여 캡처되며, 이 속성은 로그 파일의 변조 또는 삭제를 감지하기 위해 적극적으로 모니터링됩니다. 감사 로그가 시스템에서 사용 가능한 경우 감사 로그는 다음 상태 중 하나를 가질 수 있습니다.

상태	설명
활동적인	현재 로그가 기록되고 있는 파일입니다.
정상	비활성화되어 압축되어 시스템에 저장된 파일입니다.
변조됨	사용자가 수동으로 파일을 편집하여 손상된 파일입니다.
수동 삭제	권한이 있는 사용자에 의해 삭제된 파일입니다.
롤오버 삭제	롤링 구성 정책에 따라 롤링 오프로 인해 삭제된 파일입니다.
예상치 못한 삭제	알 수 없는 이유로 삭제된 파일입니다.

감사 로그 페이지에는 다음과 같은 명령 단추가 포함되어 있습니다.

- 구성

- 삭제
- 다운로드

삭제 버튼을 사용하면 감사 로그 보기에 나열된 감사 로그를 삭제할 수 있습니다. 감사 로그를 삭제할 수 있으며, 선택적으로 파일을 삭제하는 이유를 제공할 수 있습니다. 이는 나중에 유효한 삭제를 판별하는 데 도움이 됩니다. REASON 열에는 삭제 작업을 수행한 사용자의 이름과 이유가 나열됩니다.

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

감사 로그 섹션의 다운로드 버튼을 사용하여 Active IQ Unified Manager 에서 감사 로그를 다운로드하고 감사 로그 파일을 내보낼 수 있습니다. “NORMAL” 또는 "`TAMPERED`"로 표시된 파일은 압축 파일로 다운로드됩니다. `.gzip` 체재.

감사 로그 파일은 주기적으로 보관되며 참조를 위해 데이터베이스에 저장됩니다. 보관하기 전에 감사 로그는 보안과 무결성을 유지하기 위해 디지털 서명됩니다.

전체 AutoSupport 번들이 생성되면 지원 번들에는 보관된 감사 로그 파일과 활성 감사 로그 파일이 모두 포함됩니다. 하지만 가벼운 지원 번들이 생성되면 활성 감사 로그만 포함됩니다. 보관된 감사 로그는 포함되지 않습니다.

감사 로그 구성

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

시스템에 저장하려는 데이터의 양과 빈도에 따라 최대 파일 크기 및 감사 로그 보존 일수 값을 설정할 수 있습니다. 총 감사 로그 크기 필드의 값은 시스템에 있는 총 감사 로그 데이터의 크기입니다. 롤오버 정책은 감사 로그 보존 일수, 최대 파일 크기, 총 감사 로그 크기 필드의 값에 따라 결정됩니다. 감사 로그 백업의 크기가 총 감사 로그 크기*에 구성된 값에 도달하면 먼저 보관된 파일이 삭제됩니다**.** 즉**,** 가장 오래된 파일이 삭제됩니다**.** 하지만 파일 항목은 데이터베이스에 계속 남아 있으며 **"**롤오버 삭제**"**로 표시됩니다**.** *감사 로그 보존 일수 값은 감사 로그 파일이 보존되는 일 수입니다. 이 필드에 설정된 값보다 오래된 파일은 롤오버됩니다.

단계

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

   원격 로깅을 활성화하려면 *원격 로깅 활성화*를 선택해야 합니다. /// 2025-6-11, OTHERDOC-133

감사 로그의 원격 로깅 활성화

원격 감사 로깅을 활성화하려면 감사 로그 구성 대화 상자에서 원격 로깅 활성화 확인란을 선택하세요. 이 기능을 사용하면 감사 로그를 원격 Syslog 서버로 전송할 수 있습니다. 이를 통해 공간 제약이 있을 때에도 감사 로그를 관리할 수 있습니다.

감사 로그의 원격 로깅은 Active IQ Unified Manager 서버의 감사 로그 파일이 변조된 경우 변조 방지 백업을 제공합니다.

단계

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

원격 로깅을 구성하기 위한 추가 필드가 표시됩니다.

2. 연결하려는 원격 서버의 *호스트 이름*과 *포트*를 입력하세요.
3. 서버 **CA** 인증서 필드에서 *찾아보기*를 클릭하여 대상 서버의 공개 인증서를 선택합니다.

   인증서는 다음에 업로드되어야 합니다. `.pem` 체재. 이 인증서는 대상 Syslog 서버에서 얻어야 하며 만료되어서는 안 됩니다. 인증서에는 선택된 "`호스트 이름`"이 포함되어야 합니다. `SubjectAltName` (SAN) 속성.

4. 다음 필드에 값을 입력하세요: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   이러한 필드의 값은 밀리초 단위여야 합니다.

5. **FORMAT** 및 **PROTOCOL** 필드에서 필요한 Syslog 형식과 TLS 프로토콜 버전을 선택합니다.
6. 대상 Syslog 서버에 인증서 기반 인증이 필요한 경우 클라이언트 인증 사용 확인란을 선택합니다.

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

   예: syslog-ng는 다음 명령을 사용하여 인증서의 <해시>를 생성해야 합니다. `openssl x509 -noout -hash -in cert.pem` 그런 다음 클라이언트 인증 인증서를 <hash> .0 …

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

   감사 로그 페이지로 리디렉션됩니다.

> ⓘ 연결 시간 초과 값은 구성에 영향을 줄 수 있습니다. 정의된 값보다 구성에 응답하는 데 시간이 오래 걸리는 경우 연결 오류로 인해 구성이 실패할 수 있습니다. 연결을 성공적으로 설정하려면 연결 시간 초과 값을 늘리고 구성을 다시 시도하세요.

원격 인증 페이지

원격 인증 페이지를 사용하여 Unified Manager가 인증 서버와 통신하여 Unified Manager 웹 UI에 로그인을 시도하는 원격 사용자를 인증하도록 구성할 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

원격 인증 사용 확인란을 선택하면 인증 서버를 사용하여 원격 인증을 사용할 수 있습니다.

- 인증 서비스

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

  - 액티브 디렉토리
    - 관리자 이름

      인증 서버의 관리자 이름을 지정합니다.

    - 비밀번호

인증 서버에 접근하기 위한 비밀번호를 지정합니다.

- 기본 고유 이름

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

- 중첩된 그룹 조회 비활성화

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

- 보안 연결 사용

  인증 서버와 통신하는 데 사용되는 인증 서비스를 지정합니다.

◦ 오픈**LDAP**

- 고유 이름 바인딩

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

- 바인드 비밀번호

  인증 서버에 접근하기 위한 비밀번호를 지정합니다.

- 기본 고유 이름

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

- 보안 연결 사용

  LDAP 인증 서버와 통신하는 데 보안 LDAP가 사용됨을 지정합니다.

◦ 기타

- 고유 이름 바인딩

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

- 바인드 비밀번호

  인증 서버에 접근하기 위한 비밀번호를 지정합니다.

- 기본 고유 이름

  인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어, 인증 서버의 도메인 이름이 +ou@domain.com+이면 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 아니면 버전을 2 또는 3으로 설정할지 지정할 수 있습니다.

- 사용자 이름 속성

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

- 그룹 멤버십 속성

  사용자 인증 서버에 지정된 속성과 값을 기반으로 원격 사용자에게 관리 서버 그룹 멤버십을 할당하는 값을 지정합니다.

- 우지드

  원격 사용자가 인증 서버의 GroupOfUniqueNames 개체의 멤버로 포함된 경우, 이 옵션을 사용하면 해당 GroupOfUniqueNames 개체의 지정된 속성을 기반으로 원격 사용자에게 관리 서버 그룹 멤버십을 할당할 수 있습니다.

- 중첩된 그룹 조회 비활성화

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

- 회원

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

- 사용자 객체 클래스

  원격 인증 서버에서 사용자의 개체 클래스를 지정합니다.

- 그룹 객체 클래스

  원격 인증 서버의 모든 그룹의 개체 클래스를 지정합니다.

> *Member*, *User Object Class*, *Group Object Class* 특성에 입력한 값은 Active Directory, OpenLDAP, LDAP 구성에 추가된 값과 동일해야 합니다. 그렇지 않으면 인증이 실패할 수 있습니다.

- 보안 연결 사용

  인증 서버와 통신하는 데 사용되는 인증 서비스를 지정합니다.

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

인증 서버 영역

인증 서버 영역에는 관리 서버가 원격 사용자를 찾아 인증하기 위해 통신하는 인증 서버가 표시됩니다. 원격 사용자 또는 그룹의 자격 증명은 인증 서버에서 유지 관리됩니다.

- 명령 버튼

  인증 서버를 추가, 편집 또는 삭제할 수 있습니다.

  - 추가하다

    인증 서버를 추가할 수 있습니다.

  추가하려는 인증 서버가 고가용성 쌍(동일한 데이터베이스 사용)의 일부인 경우 파트너 인증 서버도 추가할 수 있습니다. 이를 통해 인증 서버 중 하나에 연결할 수 없을 때 관리 서버가 파트너와 통신할 수 있습니다.

  - 편집하다

    선택한 인증 서버의 설정을 편집할 수 있습니다.

  - 삭제

    선택한 인증 서버를 삭제합니다.

- 이름 또는 **IP** 주소

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

- 포트

  인증 서버의 포트 번호를 표시합니다.

- 테스트 인증

  이 버튼은 원격 사용자나 그룹을 인증하여 인증 서버 구성을 검증합니다.

  테스트 시 사용자 이름만 지정하면 관리 서버는 인증 서버에서 원격 사용자를 검색하지만 사용자를 인증하지는 않습니다. 사용자 이름과 비밀번호를 모두 지정하면 관리 서버는 원격 사용자를 검색하고 인증합니다.

  원격 인증이 비활성화된 경우 인증을 테스트할 수 없습니다.