



# 구성 및 관리 작업을 수행합니다

## Active IQ Unified Manager 9.13

NetApp  
December 18, 2023

# 목차

구성 및 관리 작업을 수행합니다 .....	1
Active IQ Unified Manager 구성 .....	1
Unified Manager 백업 구성 .....	20
기능 설정 관리 .....	20
유지보수 콘솔 사용 .....	23
사용자 액세스 관리 .....	36
SAML 인증 설정 관리 .....	43
인증 관리 .....	49
보안 인증서 관리 .....	56

# 구성 및 관리 작업을 수행합니다

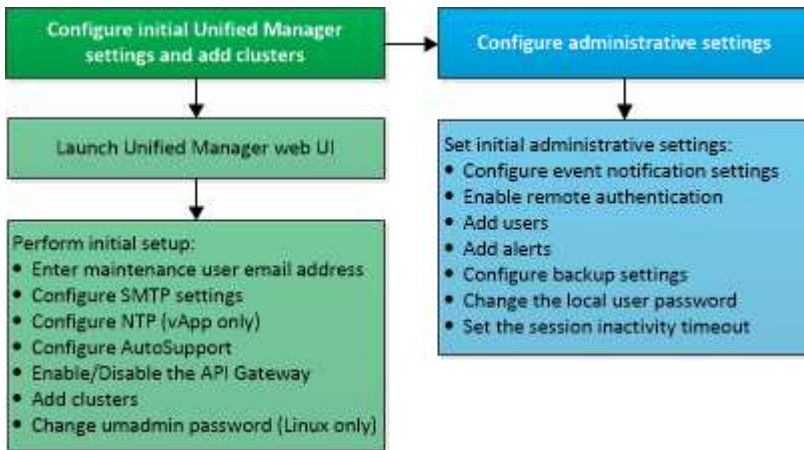
## Active IQ Unified Manager 구성

Active IQ Unified Manager(이전의 OnCommand Unified Manager)을 설치한 후 웹 UI에 액세스하려면 초기 설정(첫 번째 환경 마법사라고도 함)을 완료해야 합니다. 그런 다음 클러스터 추가, 원격 인증 구성, 사용자 추가 및 알림 추가와 같은 추가 구성 작업을 수행할 수 있습니다.

이 설명서에 설명된 일부 절차는 Unified Manager 인스턴스의 초기 설정을 완료하는 데 필요합니다. 다른 절차는 새 인스턴스에 설정하는 데 유용하거나 ONTAP 시스템의 정기적인 모니터링을 시작하기 전에 알아야 할 구성 설정을 권장합니다.

### 구성 시퀀스의 개요

구성 워크플로우에서 Unified Manager를 사용하기 전에 수행해야 하는 작업에 대해 설명합니다.



### Unified Manager 웹 UI에 액세스

Unified Manager를 설치한 후에는 웹 UI에 액세스하여 Unified Manager를 설정하여 ONTAP 시스템 모니터링을 시작할 수 있습니다.

- 필요한 것 \*
- 웹 UI에 처음 액세스하는 경우 유지 관리 사용자(또는 Linux 설치의 경우 umadmin 사용자)로 로그인해야 합니다.
- 사용자가 FQDN(정규화된 도메인 이름) 또는 IP 주소를 사용하는 대신 짧은 이름을 사용하여 Unified Manager에 액세스하도록 허용하려면 네트워크 구성에서 이 짧은 이름을 유효한 FQDN으로 해석해야 합니다.
- 서버에서 자체 서명된 디지털 인증서를 사용하는 경우 브라우저에서 인증서를 신뢰할 수 없다는 경고를 표시할 수 있습니다. 액세스를 계속할 위험을 확인하거나 서버 인증을 위해 CA(인증 기관) 서명 디지털 인증서를 설치할 수 있습니다.

### 단계

1. 설치 마지막에 표시되는 URL을 사용하여 브라우저에서 Unified Manager 웹 UI를 시작합니다. URL은 Unified Manager 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다.

링크는 다음과 같은 형식으로 되어 있습니다. <https://URL>.

2. 유지보수 사용자 자격 증명을 사용하여 Unified Manager 웹 UI에 로그인합니다.



한 시간 내에 웹 UI에 세 번 연속해서 로그인을 실패하면 시스템이 잠기므로 시스템 관리자에게 문의해야 합니다. 이 옵션은 로컬 사용자에게만 적용됩니다.

## Unified Manager 웹 UI의 초기 설정 수행

Unified Manager를 사용하려면 먼저 NTP 서버, 유지보수 사용자 이메일 주소, SMTP 서버 호스트 및 ONTAP 클러스터 추가를 포함한 초기 설정 옵션을 구성해야 합니다.

- 필요한 것 \*

다음 작업을 수행해야 합니다.

- 설치 후 제공된 URL을 사용하여 Unified Manager 웹 UI를 실행했습니다
- 설치 중에 생성된 유지보수 사용자 이름 및 암호(Linux 설치의 경우 umadmin 사용자)를 사용하여 로그인했습니다

Active IQ Unified Manager 시작 페이지는 웹 UI에 처음 액세스할 때만 나타납니다. 아래 페이지는 VMware 설치 페이지입니다.

## Getting Started



## Notifications

Configure your email server for assistance in case you forget your password.

## Maintenance User Email

Email

## SMTP Server

Host Name or IP Address

Port

User Name

Password

Use STARTTLS ⓘ     Use SSL ⓘ

**Continue**

나중에 이 옵션 중 하나를 변경하려면 Unified Manager의 왼쪽 탐색 창에서 일반 옵션에서 원하는 옵션을 선택합니다. NTP 설정은 VMware 설치에만 해당되며 나중에 Unified Manager 유지보수 콘솔을 사용하여 변경할 수 있습니다.

단계

1. Active IQ Unified Manager 초기 설정 페이지에서 유지보수 사용자 e-메일 주소, SMTP 서버 호스트 이름 및 추가 SMTP 옵션, NTP 서버(VMware 설치만 해당)를 입력합니다. 그런 다음 \* 계속 \* 을 클릭합니다.



STARTTLS\* 또는 \* SSL \* 사용 옵션을 선택한 경우 \* 계속 \* 단추를 클릭하면 인증서 페이지가 표시됩니다. 인증서 세부 정보를 확인하고 인증서를 수락하여 웹 UI의 초기 설정 설정을 계속합니다.

2. AutoSupport 페이지에서 \* 동의 및 계속 \* 을 클릭하여 AutoSupport 메시지를 Unified Manager에서 NetAppActive IQ로 보낼 수 있습니다.

AutoSupport 콘텐츠를 전송하기 위해 인터넷 액세스를 제공할 프록시를 지정해야 하거나 AutoSupport를 비활성화하려면 웹 UI에서 \* 일반 \* > \* AutoSupport \* 옵션을 사용하십시오.

3. Red Hat 및 CentOS 시스템에서 umadmin 사용자 암호를 기본 ""admin" 문자열에서 개인 문자열로 변경합니다.

4. API 게이트웨이 설정 페이지에서 ONTAP REST API를 사용하여 모니터링하려는 ONTAP 클러스터를 Unified Manager에서 관리할 수 있도록 하는 API 게이트웨이 기능을 사용할지 여부를 선택합니다. 그런 다음 \* 계속 \* 을 클릭합니다.

웹 UI의 나중에 \* 일반 \* > \* 기능 설정 \* > \* API 게이트웨이 \* 에서 이 설정을 활성화하거나 비활성화할 수 있습니다. API에 대한 자세한 내용은 를 참조하십시오 "[Active IQ Unified Manager REST API 시작하기](#)".

5. Unified Manager에서 관리할 클러스터를 추가하고 \* 다음 \* 을 클릭합니다. 관리하려는 각 클러스터마다 사용자 이름 및 암호 자격 증명과 함께 호스트 이름 또는 클러스터 관리 IP 주소(IPv4 또는 IPv6)가 있어야 합니다. 사용자는 ""admin" 역할을 가지고 있어야 합니다.

이 단계는 선택 사항입니다. 웹 UI의 나중에 \* 스토리지 관리 \* > \* 클러스터 설정 \* 에서 클러스터를 추가할 수 있습니다.

6. 요약 페이지에서 모든 설정이 올바른지 확인하고 \* 마침 \* 을 클릭합니다.

시작하기 페이지가 닫히고 Unified Manager 대시보드 페이지가 표시됩니다.

## 클러스터 추가

클러스터를 모니터링할 수 있도록 Active IQ Unified Manager에 클러스터를 추가할 수 있습니다. 여기에는 발생할 수 있는 문제를 찾아 해결할 수 있도록 클러스터의 상태, 용량, 성능, 구성 등과 같은 클러스터 정보를 가져오는 기능도 포함됩니다.

- 필요한 것 \*
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 다음 정보가 있어야 합니다.
  - Unified Manager는 사내 ONTAP 클러스터, ONTAP Select, Cloud Volumes ONTAP를 지원합니다.
  - 호스트 이름 또는 클러스터 관리 IP 주소입니다

호스트 이름은 Unified Manager가 클러스터에 연결하는 데 사용하는 FQDN 또는 짧은 이름입니다. 호스트 이름이 클러스터 관리 IP 주소로 확인되어야 합니다.

클러스터 관리 IP 주소는 관리 스토리지 가상 시스템(SVM)의 클러스터 관리 LIF여야 합니다. 노드 관리 LIF를 사용하면 작업이 실패합니다.

- 클러스터에서 ONTAP 버전 9.1 소프트웨어 이상을 실행해야 합니다.
- ONTAP 관리자 사용자 이름 및 암호
  - 이 계정에는 응용 프로그램 액세스 권한이 *ontapi*, *console* 및 *\_http\_*로 설정된 *\_admin\_* 역할이 있어야 합니다.
- HTTPS 프로토콜을 사용하여 클러스터에 연결할 포트 번호(일반적으로 포트 443)
- 필요한 인증서가 있습니다.
- SSL(HTTPS) 인증서 \*: 이 인증서는 Unified Manager에서 소유합니다. Unified Manager를 새로 설치하면 자체 서명된 기본 SSL(HTTPS) 인증서가 생성됩니다. 보안을 강화하기 위해 CA 서명 인증서로 업그레이드하는 것이 좋습니다. 서버 인증서가 만료되면 해당 인증서를 다시 생성하고 Unified Manager를 다시 시작하여 새 인증서를 통합하는 서비스를 수행해야 합니다. SSL 인증서 재생성에 대한 자세한 내용은 을 참조하십시오 "[HTTPS 보안 인증서를 생성하는 중입니다](#)".

- EMS 인증서 \*: 이 인증서는 Unified Manager에서 소유합니다. ONTAP로부터 수신한 EMS 알림에 대한 인증 중에 사용됩니다.
- 상호 TLS 통신을 위한 인증서 \*: Unified Manager와 ONTAP 간의 상호 TLS 통신 중에 사용됩니다. 인증서 기반 인증은 ONTAP 버전에 따라 클러스터에 대해 설정됩니다. ONTAP 버전을 실행하는 클러스터가 9.5보다 낮은 경우 인증서 기반 인증이 활성화되지 않습니다.

이전 버전의 Unified Manager를 업데이트하는 경우 클러스터에 대해 인증서 기반 인증이 자동으로 활성화되지 않습니다. 그러나 클러스터 세부 정보를 수정 및 저장하여 이 기능을 사용하도록 설정할 수 있습니다. 인증서가 만료되면 인증서를 다시 생성하여 새 인증서를 통합해야 합니다. 인증서 보기 및 재생에 대한 자세한 내용은 을 참조하십시오 ["클러스터 편집"](#).



- 웹 UI에서 클러스터를 추가할 수 있으며 인증서 기반 인증이 자동으로 활성화됩니다.
- Unified Manager CLI를 통해 클러스터를 추가할 수 있으며, 인증서 기반 인증은 기본적으로 사용되지 않습니다. Unified Manager CLI를 사용하여 클러스터를 추가하는 경우 Unified Manager UI를 사용하여 클러스터를 편집해야 합니다. 확인할 수 있습니다 ["지원되는 Unified Manager CLI 명령"](#) 을 사용하여 Unified Manager CLI를 사용하여 클러스터를 추가합니다.
- 클러스터에 대해 인증서 기반 인증을 사용하고 서버에서 Unified Manager 백업을 수행한 후 호스트 이름 또는 IP 주소가 변경된 다른 Unified Manager 서버로 복원하면 클러스터 모니터링이 실패할 수 있습니다. 이 문제를 방지하려면 클러스터 세부 정보를 편집하고 저장합니다. 클러스터 세부 정보 편집에 대한 자세한 내용은 을 참조하십시오 ["클러스터 편집"](#).

- 클러스터 인증서 \*: 이 인증서는 ONTAP에서 소유합니다. 만료된 인증서가 있는 클러스터는 Unified Manager에 추가할 수 없으며, 인증서가 이미 만료된 경우 클러스터를 추가하기 전에 다시 생성해야 합니다. 인증서 생성에 대한 자세한 내용은 기술 자료(KB) 문서를 참조하십시오 ["System Manager 사용자 인터페이스에서 ONTAP 자체 서명된 인증서를 갱신하는 방법"](#).
- Unified Manager 서버에 적절한 공간이 있어야 합니다. 데이터베이스 디렉토리의 공간이 이미 90% 이상 사용된 경우 서버에 클러스터를 추가할 수 없습니다.

MetroCluster 구성의 경우 로컬 클러스터와 원격 클러스터를 모두 추가해야 하며 클러스터가 올바르게 구성되어야 합니다.

#### 단계

1. 왼쪽 탐색 창에서 \* 스토리지 관리 \* > \* 클러스터 설정 \* 을 클릭합니다.
2. 클러스터 설정 페이지에서 \* 추가 \* 를 클릭합니다.
3. 클러스터 추가 대화 상자에서 클러스터의 호스트 이름 또는 IP 주소, 사용자 이름, 암호 및 포트 번호와 같은 필수 값을 지정합니다.

클러스터 관리 IP 주소를 IPv6에서 IPv4로, 또는 IPv4에서 IPv6로 변경할 수 있습니다. 새 IP 주소는 다음 모니터링 주기가 완료된 후 클러스터 그리드 및 클러스터 구성 페이지에 반영됩니다.

4. 제출 \* 을 클릭합니다.
5. 호스트 인증 대화 상자에서 \* 인증서 보기 \* 를 클릭하여 클러스터에 대한 인증서 정보를 확인합니다.
6. 예 \* 를 클릭합니다.

클러스터 세부 정보를 저장한 후에는 클러스터의 상호 TLS 통신에 대한 인증서를 볼 수 있습니다.

인증서 기반 인증이 활성화되지 않은 경우 Unified Manager는 클러스터가 처음에 추가될 때만 인증서를 확인합니다. Unified Manager에서는 ONTAP에 대한 각 API 호출의 인증서를 확인하지 않습니다.

새 클러스터의 모든 객체가 검색된 후 Unified Manager가 이전 15일 동안 기간별 성능 데이터를 수집하기 시작합니다. 이러한 통계는 데이터 연속성 수집 기능을 사용하여 수집됩니다. 이 기능은 클러스터를 추가한 직후 2주 이상의 클러스터 성능 정보를 제공합니다. 데이터 연속성 수집 주기가 완료되면 기본적으로 5분마다 실시간 클러스터 성능 데이터가 수집됩니다.



15일간의 성능 데이터 수집은 CPU를 많이 사용하므로 데이터 연속성 수집 풀이 너무 많은 클러스터에서 동시에 실행되지 않도록 새 클러스터를 추가하는 시차를 두는 것이 좋습니다. 또한, 데이터 연속성 수집 기간 동안 Unified Manager를 다시 시작하면 수집이 중단되고 성능 차트의 누락된 시간 간격이 표시됩니다.



클러스터를 추가할 수 없다는 오류 메시지가 표시되면 두 시스템의 시계가 동기화되지 않았는지, Unified Manager HTTPS 인증서 시작 날짜가 클러스터의 날짜 이후인지 확인합니다. NTP 또는 이와 유사한 서비스를 사용하여 시계가 동기화되었는지 확인해야 합니다.

• 관련 정보 \*

["서명되고 반환된 HTTPS 인증서를 설치하는 중입니다"](#)

## 경고 알림을 보내도록 Unified Manager 구성

Unified Manager에서 사용자 환경의 이벤트에 대한 알림을 보내도록 구성할 수 있습니다. 알림을 보내려면 먼저 몇 가지 다른 Unified Manager 옵션을 구성해야 합니다.

• 필요한 것 \*

애플리케이션 관리자 역할이 있어야 합니다.

Unified Manager를 구축하고 초기 구성을 완료한 후에는 이벤트 수신 시 알림을 트리거하고 알림 e-메일 또는 SNMP 트랩을 생성하도록 환경을 구성하는 것이 좋습니다.

단계

1. ["이벤트 알림 설정을 구성합니다"](#).

사용자 환경에서 특정 이벤트가 발생할 때 알림 알림을 보내려면 SMTP 서버를 구성하고 알림 알림을 보낼 이메일 주소를 제공해야 합니다. SNMP 트랩을 사용하려면 해당 옵션을 선택하고 필요한 정보를 제공할 수 있습니다.

2. ["원격 인증을 사용합니다"](#).

원격 LDAP 또는 Active Directory 사용자가 Unified Manager 인스턴스에 액세스하여 경고 알림을 받으려면 원격 인증을 설정해야 합니다.

3. ["인증 서버를 추가합니다"](#).

인증 서버 내의 원격 사용자가 Unified Manager에 액세스할 수 있도록 인증 서버를 추가할 수 있습니다.

4. ["사용자 추가"](#).

여러 가지 유형의 로컬 또는 원격 사용자를 추가하고 특정 역할을 할당할 수 있습니다. 알림을 생성할 때 사용자에게 경고 알림을 보내도록 할당합니다.

5. ["알림을 추가합니다"](#).



알림을 보낼 e-메일 주소를 추가하고 알림을 받을 사용자를 추가했으며 네트워크 설정을 구성했으며 사용자 환경에 필요한 SMTP 및 SNMP 옵션을 구성한 후 알림을 할당할 수 있습니다.

이벤트 알림 설정을 구성하는 중입니다

이벤트가 생성되거나 이벤트가 사용자에게 할당될 때 알림을 보내도록 Unified Manager를 구성할 수 있습니다. 알림을 보내는 데 사용되는 SMTP 서버를 구성할 수 있으며, 다양한 알림 메커니즘을 설정할 수 있습니다. 예를 들어, 알림 알림을 e-메일 또는 SNMP 트랩으로 보낼 수 있습니다.

- 필요한 것 \*

다음 정보가 있어야 합니다.

- 알림 메시지가 전송되는 이메일 주소입니다

보낸 알림 알림의 ""보낸 사람" 필드에 이메일 주소가 나타납니다. 어떤 이유로든 이메일을 전달할 수 없는 경우 이 이메일 주소는 배달 불가능한 메일의 받는 사람으로도 사용됩니다.

- SMTP 서버 호스트 이름 및 서버에 액세스하기 위한 사용자 이름 및 암호
- SNMP 버전, 아웃바운드 트랩 포트, 커뮤니티 및 기타 필수 SNMP 구성 값과 함께 SNMP 트랩을 수신할 트랩 대상 호스트의 호스트 이름 또는 IP 주소입니다

여러 트랩 대상을 지정하려면 각 호스트를 심표로 구분합니다. 이 경우 버전 및 아웃바운드 트랩 포트와 같은 다른 모든 SNMP 설정은 목록의 모든 호스트에 대해 동일해야 합니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 알림 \* 을 클릭합니다.

2. 알림 페이지에서 적절한 설정을 구성합니다.

◦ 참고: \*

- 보낸 사람 주소에 "ActiveIQUnifiedManager@localhost.com" 주소가 미리 입력된 경우, 모든 이메일 알림이 성공적으로 전송되도록 실제 작업 이메일 주소로 변경해야 합니다.
- SMTP 서버의 호스트 이름을 확인할 수 없는 경우 호스트 이름 대신 SMTP 서버의 IP 주소(IPv4 또는 IPv6)를 지정할 수 있습니다.

3. 저장 \* 을 클릭합니다.

4. STARTTLS\* 또는 \* SSL\* 사용 옵션을 선택한 경우 \* 저장 \* 단추를 클릭하면 인증서 페이지가 표시됩니다. 인증서 세부 정보를 확인하고 인증서를 수락하여 알림 설정을 저장합니다.

인증서 세부 정보 보기 \* 단추를 클릭하여 인증서 세부 정보를 볼 수 있습니다. 기존 인증서가 만료된 경우 \* STARTTLS \* 또는 \* SSL \* 사용 상자의 선택을 취소하고 알림 설정을 저장한 다음 \* STARTTLS \* 또는 \* SSL \* 사용 상자를 다시 선택하여 새 인증서를 봅니다.

## 원격 인증 활성화 중

Unified Manager 서버가 인증 서버와 통신할 수 있도록 원격 인증을 설정할 수 있습니다. 인증 서버 사용자는 Unified Manager 그래픽 인터페이스에 액세스하여 스토리지 객체와 데이터를 관리할 수 있습니다.

- 필요한 것 \*

애플리케이션 관리자 역할이 있어야 합니다.



Unified Manager 서버는 인증 서버에 직접 연결되어 있어야 합니다. SSSD(System Security Services Daemon) 또는 NSLCD(Name Service LDAP Caching Daemon)와 같은 로컬 LDAP 클라이언트를 비활성화해야 합니다.

Open LDAP 또는 Active Directory를 사용하여 원격 인증을 설정할 수 있습니다. 원격 인증이 비활성화되어 있으면 원격 사용자가 Unified Manager에 액세스할 수 없습니다.

원격 인증은 LDAP 및 LDAPS(Secure LDAP)를 통해 지원됩니다. Unified Manager에서는 비보안 통신의 기본 포트로 389를 사용하고 보안 통신의 기본 포트는 636를 사용합니다.



사용자를 인증하는 데 사용되는 인증서는 X.509 형식을 따라야 합니다.

### 단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 원격 인증 \* 을 클릭합니다.
2. 원격 인증 활성화... \* 확인란을 선택합니다.
3. 인증 서비스 필드에서 서비스 유형을 선택하고 인증 서비스를 구성합니다.

인증 유형...	다음 정보를 입력합니다...
Active Directory를 클릭합니다	<ul style="list-style-type: none"><li>• 인증 서버 관리자 이름은 다음 형식 중 하나입니다.<ul style="list-style-type: none"><li>◦ domainname\username</li><li>◦ username@domainname</li><li>◦ Bind Distinguished Name (적절한 LDAP 표기법 사용)</li></ul></li><li>• 관리자 암호입니다</li><li>• 기본 고유 이름(적절한 LDAP 표기법 사용)</li></ul>
LDAP를 엽니다	<ul style="list-style-type: none"><li>• 적절한 LDAP 표시법으로 고유 이름 바인딩</li><li>• 암호를 바인딩합니다</li><li>• 기본 고유 이름입니다</li></ul>

Active Directory 사용자의 인증에 오랜 시간이 걸리거나 시간이 걸리는 경우 인증 서버가 응답하는 데 시간이 오래 걸릴 수 있습니다. Unified Manager에서 중첩된 그룹에 대한 지원을 사용하지 않도록 설정하면 인증 시간이 줄어들 수 있습니다.

인증 서버에 대해 보안 연결 사용 옵션을 선택하면 Unified Manager는 SSL(Secure Sockets Layer) 프로토콜을 사용하여 인증 서버와 통신합니다.

4. \* 선택 사항: \* 인증 서버를 추가하고 인증을 테스트합니다.
5. 저장 \* 을 클릭합니다.

원격 인증에서 중첩 그룹을 해제합니다

원격 인증이 활성화된 경우 그룹 구성원이 아닌 개별 사용자만 Unified Manager에 원격으로 인증할 수 있도록 중첩된 그룹 인증을 비활성화할 수 있습니다. Active Directory 인증 응답 시간을 향상시키려면 중첩된 그룹을 사용하지 않도록 설정할 수 있습니다.

- 필요한 것 \*
- 애플리케이션 관리자 역할이 있어야 합니다.
- 중첩된 그룹을 사용하지 않도록 설정하는 것은 Active Directory를 사용하는 경우에만 적용됩니다.

Unified Manager에서 중첩된 그룹에 대한 지원을 사용하지 않도록 설정하면 인증 시간이 줄어들 수 있습니다. 중첩된 그룹 지원이 비활성화되어 있고 원격 그룹이 Unified Manager에 추가된 경우, 개별 사용자는 Unified Manager에 인증할 원격 그룹의 구성원이어야 합니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 원격 인증 \* 을 클릭합니다.
2. 중첩 그룹 조회 사용 안 함 \* 에 대한 확인란을 선택합니다.
3. 저장 \* 을 클릭합니다.

인증 서비스 설정 중

인증 서비스를 사용하면 Unified Manager에 대한 액세스를 제공하기 전에 인증 서버에서 원격 사용자 또는 원격 그룹을 인증할 수 있습니다. 사전 정의된 인증 서비스(예: Active Directory 또는 OpenLDAP)를 사용하거나 고유한 인증 메커니즘을 구성하여 사용자를 인증할 수 있습니다.

- 필요한 것 \*
- 원격 인증을 활성화해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 원격 인증 \* 을 클릭합니다.
2. 다음 인증 서비스 중 하나를 선택합니다.

다음을 선택한 경우...	다음을 수행하십시오.
Active Directory를 클릭합니다	<p>a. 관리자 이름과 암호를 입력합니다.</p> <p>b. 인증 서버의 기본 고유 이름을 지정합니다.</p> <p>예를 들어 인증 서버의 도메인 이름이 <code>+ou@domain.com</code> +인 경우 기본 고유 이름은 * <code>cn=ou, dc=domain, dc=com</code> * 입니다.</p>
OpenLDAP를 클릭합니다	<p>a. 바인딩 고유 이름 및 바인딩 암호를 입력합니다.</p> <p>b. 인증 서버의 기본 고유 이름을 지정합니다.</p> <p>예를 들어 인증 서버의 도메인 이름이 <code>+ou@domain.com</code> +인 경우 기본 고유 이름은 * <code>cn=ou, dc=domain, dc=com</code> * 입니다.</p>
기타	<p>a. 바인딩 고유 이름 및 바인딩 암호를 입력합니다.</p> <p>b. 인증 서버의 기본 고유 이름을 지정합니다.</p> <p>예를 들어 인증 서버의 도메인 이름이 <code>+ou@domain.com</code> +인 경우 기본 고유 이름은 * <code>cn=ou, dc=domain, dc=com</code> * 입니다.</p> <p>c. 인증 서버에서 지원하는 LDAP 프로토콜 버전을 지정합니다.</p> <p>d. 사용자 이름, 그룹 구성원 자격, 사용자 그룹 및 구성원 특성을 입력합니다.</p>



인증 서비스를 수정하려면 기존 인증 서버를 삭제한 다음 새 인증 서버를 추가해야 합니다.

3. 저장 \* 을 클릭합니다.

### 인증 서버 추가


인증 서버를 추가하고 관리 서버에서 원격 인증을 설정하여 인증 서버 내의 원격 사용자가 Unified Manager에 액세스할 수 있도록 할 수 있습니다.

- 필요한 것 \*
- 다음 정보를 사용할 수 있어야 합니다.
  - 인증 서버의 호스트 이름 또는 IP 주소입니다
  - 인증 서버의 포트 번호입니다
- 관리 서버가 인증 서버의 원격 사용자 또는 그룹을 인증할 수 있도록 원격 인증을 활성화하고 인증 서비스를 구성해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

추가하려는 인증 서버가 동일한 데이터베이스를 사용하는 고가용성(HA) 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.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 원격 인증 \* 을 클릭합니다.
2. 보안 연결 사용 \* 옵션을 활성화 또는 비활성화합니다.

원하는 작업	다음을 수행하십시오.
활성화	<p>a. 보안 연결 사용 * 옵션을 선택합니다.</p> <p>b. Authentication Servers 영역에서 * Add * 를 클릭합니다.</p> <p>c. Add Authentication Server 대화 상자에서 서버의 인증 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.</p> <p>d. 호스트 권한 부여 대화 상자에서 인증서 보기를 클릭합니다.</p> <p>e. 인증서 보기 대화 상자에서 인증서 정보를 확인한 다음 * 닫기 * 를 클릭합니다.</p> <p>f. 호스트 권한 부여 대화 상자에서 * 예 * 를 클릭합니다.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 20px;"> <p> 보안 연결 인증 사용 * 옵션을 활성화하면 Unified Manager가 인증 서버와 통신하고 인증서를 표시합니다. Unified Manager는 보안 통신을 위한 기본 포트로 636을 사용하고 비보안 통신을 위한 포트 번호 389를 사용합니다.</p> </div>
비활성화합니다	<p>a. 보안 연결 사용 * 옵션의 선택을 취소합니다.</p> <p>b. Authentication Servers 영역에서 * Add * 를 클릭합니다.</p> <p>c. Add Authentication Server 대화 상자에서 서버의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)와 포트 세부 정보를 지정합니다.</p> <p>d. 추가 * 를 클릭합니다.</p>

추가한 인증 서버가 Servers 영역에 표시됩니다.

3. 테스트 인증을 수행하여 추가한 인증 서버에서 사용자를 인증할 수 있는지 확인합니다.

인증 서버의 구성을 테스트하는 중입니다

관리 서버가 인증 서버와 통신할 수 있는지 확인하기 위해 인증 서버 구성을 검증할 수 있습니다.

인증 서버에서 원격 사용자 또는 원격 그룹을 검색하고 구성된 설정을 사용하여 인증하여 구성을 확인할 수 있습니다.

- 필요한 것 \*
- Unified Manager 서버가 원격 사용자 또는 원격 그룹을 인증할 수 있도록 원격 인증을 설정하고 인증 서비스를 구성해야 합니다.
- 관리 서버가 이러한 서버에서 원격 사용자 또는 원격 그룹을 검색하고 인증할 수 있도록 인증 서버를 추가해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

인증 서비스가 Active Directory로 설정되어 있고 인증 서버의 기본 그룹에 속하는 원격 사용자의 인증을 확인하는 경우 기본 그룹에 대한 정보가 인증 결과에 표시되지 않습니다.

#### 단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 원격 인증 \* 을 클릭합니다.
2. 인증 테스트 \* 를 클릭합니다.
3. 사용자 테스트 대화 상자에서 원격 사용자의 사용자 이름 및 암호 또는 원격 그룹의 사용자 이름을 지정한 다음 \* 테스트 \* 를 클릭합니다.

원격 그룹을 인증하는 경우 암호를 입력하지 않아야 합니다.

#### 알림 추가

특정 이벤트가 생성될 때 알림을 표시하도록 알림을 구성할 수 있습니다. 단일 리소스, 리소스 그룹 또는 특정 심각도 유형의 이벤트에 대한 알림을 구성할 수 있습니다. 알림을 받을 빈도를 지정하고 스크립트를 알림에 연결할 수 있습니다.

- 필요한 것 \*
- Active IQ Unified Manager 서버가 이러한 설정을 사용하여 이벤트가 생성될 때 사용자에게 알림을 보낼 수 있도록 하려면 사용자 e-메일 주소, SMTP 서버 및 SNMP 트랩 호스트와 같은 알림 설정을 구성해야 합니다.
- 알림을 트리거할 리소스 및 이벤트와 알림을 보낼 사용자의 사용자 이름 또는 이메일 주소를 알고 있어야 합니다.
- 이벤트를 기반으로 스크립트를 실행하려면 스크립트 페이지를 사용하여 Unified Manager에 스크립트를 추가해야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

여기서 설명하는 대로 알림 설정 페이지에서 알림을 생성할 뿐만 아니라 이벤트를 수신한 후 이벤트 세부 정보 페이지에서 직접 알림을 생성할 수 있습니다.

#### 단계

1. 왼쪽 탐색 창에서 \* 스토리지 관리 \* > \* 경고 설정 \* 을 클릭합니다.
2. 경고 설정 페이지에서 \* 추가 \* 를 클릭합니다.
3. 경고 추가 대화 상자에서 \* 이름 \* 을 클릭하고 경고의 이름과 설명을 입력합니다.
4. 리소스 \* 를 클릭하고 경고에 포함되거나 제외될 리소스를 선택합니다.

이름 포함 \* 필드에서 텍스트 문자열을 지정하여 리소스 그룹을 선택하여 필터를 설정할 수 있습니다. 지정한 텍스트 문자열을 기준으로 사용 가능한 자원 목록에는 필터 규칙과 일치하는 자원만 표시됩니다. 지정하는 텍스트 문자열은 대/소문자를 구분합니다.

자원이 지정한 포함 및 제외 규칙을 모두 준수하는 경우 제외 규칙이 포함 규칙보다 우선하며 제외된 리소스와 관련된 이벤트에 대해서는 알림이 생성되지 않습니다.

5. 이벤트 \* 를 클릭하고 알림을 트리거할 이벤트 이름 또는 이벤트 심각도 유형을 기반으로 이벤트를 선택합니다.



둘 이상의 이벤트를 선택하려면 Ctrl 키를 누른 상태에서 원하는 항목을 선택합니다.

6. Actions \* 를 클릭하고 알릴 사용자를 선택하고, 알림 빈도를 선택하고, SNMP 트랩을 트랩 수신기로 전송할지 여부를 선택한 다음, 경고가 생성될 때 실행할 스크립트를 할당합니다.



사용자에 대해 지정된 전자 메일 주소를 수정하고 편집을 위해 알림을 다시 열면 수정된 전자 메일 주소가 이전에 선택한 사용자에게 더 이상 매핑되지 않으므로 이름 필드가 비어 있습니다. 또한 사용자 페이지에서 선택한 사용자의 전자 메일 주소를 수정한 경우 선택한 사용자에게 대해 수정된 전자 메일 주소가 업데이트되지 않습니다.

SNMP 트랩을 통해 사용자에게 알리도록 선택할 수도 있습니다.

7. 저장 \* 을 클릭합니다.

알림 추가 예

이 예제에서는 다음 요구 사항을 충족하는 알림을 생성하는 방법을 보여 줍니다.

- 알림 이름: 상태 테스트
- 리소스: 이름에 ""abc""가 포함된 모든 볼륨을 포함하며 이름에 ""xyz""가 포함된 모든 볼륨을 제외합니다.
- 이벤트: 모든 중요한 상태 이벤트를 포함합니다
- 작업: "sample@domain.com", ""테스트"" 스크립트를 포함하며, 사용자는 15분마다 통지를 받아야 합니다

경고 추가 대화 상자에서 다음 단계를 수행합니다.

단계

1. 이름 \* 을 클릭하고 \* 알림 이름 \* 필드에 \* 상태 테스트 \* 를 입력합니다.
2. 리소스 \* 를 클릭하고 포함 탭의 드롭다운 목록에서 \* 볼륨 \* 을 선택합니다.
  - a. 이름이 ""abc""인 볼륨을 표시하려면 \* Name Contains \* 필드에 \* abc \* 를 입력합니다.
  - b. 를 선택합니다[All Volumes whose name contains 'abc']Available Resources 영역에서 + \* 를 선택한 다음 Selected Resources 영역으로 이동합니다.
  - c. 제외 \* 를 클릭하고 \* 이름 포함 \* 필드에 \* xyz \* 를 입력한 다음 \* 추가 \* 를 클릭합니다.
3. 이벤트 \* 를 클릭하고 이벤트 심각도 필드에서 \* 긴급 \* 을 선택합니다.
4. Matching Events 영역에서 \* All Critical Events \* 를 선택하고 Selected Events 영역으로 이동합니다.
5. Actions \* 를 클릭하고 Alert these users 필드에 \* sample@domain.com \* 를 입력합니다.
6. 15분마다 사용자에게 알리려면 \* 15분마다 알림 \* 을 선택합니다.

지정된 시간 동안 수신자에게 반복적으로 알림을 보내도록 알림을 구성할 수 있습니다. 알림에 대해 이벤트 알림이 활성화되는 시간을 결정해야 합니다.

7. 실행할 스크립트 선택 메뉴에서 \* 테스트 \* 스크립트를 선택합니다.
8. 저장 \* 을 클릭합니다.

## 로컬 사용자 암호 변경

잠재적인 보안 위험을 방지하기 위해 로컬 사용자 로그인 암호를 변경할 수 있습니다.

- 필요한 것 \*

로컬 사용자로 로그인해야 합니다.

유지보수 사용자 및 원격 사용자의 암호는 다음 단계를 사용하여 변경할 수 없습니다. 원격 사용자 암호를 변경하려면 암호 관리자에게 문의하십시오. 유지보수 사용자 암호를 변경하려면 를 참조하십시오 "[유지보수 콘솔 사용](#)".

단계

1. Unified Manager에 로그인합니다.
2. 상단 메뉴 모음에서 사용자 아이콘을 클릭한 다음 \* 암호 변경 \* 을 클릭합니다.

원격 사용자인 경우 \* 암호 변경 \* 옵션이 표시되지 않습니다.

3. 암호 변경 대화 상자에서 현재 암호와 새 암호를 입력합니다.
4. 저장 \* 을 클릭합니다.

Unified Manager가고가용성 구성으로 구성된 경우 설정의 두 번째 노트에서 암호를 변경해야 합니다. 두 인스턴스 모두 동일한 암호를 사용해야 합니다.

## 세션 비활성 시간 초과 설정

Unified Manager의 비활성 시간 초과 값을 지정하여 특정 시간 이후에 세션이 자동으로 종료되도록 할 수 있습니다. 기본적으로 시간 초과는 4,320분(72시간)으로 설정됩니다.

- 필요한 것 \*

애플리케이션 관리자 역할이 있어야 합니다.

이 설정은 로그인한 모든 사용자 세션에 영향을 줍니다.



SAML(Security Assertion Markup Language) 인증을 활성화한 경우에는 이 옵션을 사용할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 기능 설정 \* 을 클릭합니다.
2. 기능 설정 \* 페이지에서 다음 옵션 중 하나를 선택하여 비활성 시간 초과를 지정합니다.



원하는 작업	다음을 수행하십시오.
세션이 자동으로 닫히지 않도록 설정된 시간 제한이 없습니다	Inactivity Timeout * (비활성 시간 초과 *) 패널에서 슬라이더 버튼을 왼쪽(꺼짐)으로 이동하고 * Apply * (적용 *)를 클릭합니다.
시간 초과 값으로 특정 시간(분)을 설정합니다	Inactivity Timeout * (비활성 시간 초과 *) 패널에서 슬라이더 버튼을 오른쪽(켜짐)으로 이동하고 비활성 시간 초과 값을 분 단위로 지정한 다음 * Apply * (적용 *)를 클릭합니다.

## Unified Manager 호스트 이름을 변경하는 중입니다

경우에 따라 Unified Manager를 설치한 시스템의 호스트 이름을 변경할 수도 있습니다. 예를 들어, 호스트 이름을 유형, 작업 그룹 또는 모니터링되는 클러스터 그룹별로 Unified Manager 서버를 더 쉽게 식별하도록 변경할 수 있습니다.

호스트 이름을 변경하는 데 필요한 단계는 Unified Manager가 VMware ESXi 서버, Red Hat 또는 CentOS Linux 서버 또는 Microsoft Windows 서버에서 실행 중인지 여부에 따라 다릅니다.

### Unified Manager 가상 어플라이언스 호스트 이름을 변경하는 중입니다

Unified Manager 가상 어플라이언스를 처음 구축할 때 네트워크 호스트에 이름이 할당됩니다. 배포 후 호스트 이름을 변경할 수 있습니다. 호스트 이름을 변경하는 경우 HTTPS 인증서도 다시 생성해야 합니다.

- 필요한 것 \*

이러한 작업을 수행하려면 Unified Manager에 유지보수 사용자로 로그인하거나 애플리케이션 관리자 역할이 할당되어 있어야 합니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 Unified Manager 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP 주소를 구성한 경우 네트워크 호스트의 이름을 지정했을 것입니다. DHCP를 사용하여 네트워크를 구성한 경우 DNS에서 호스트 이름을 가져와야 합니다. DHCP 또는 DNS가 제대로 구성되지 않은 경우 호스트 이름 ""Unified Manager""가 자동으로 할당되어 보안 인증서와 연결됩니다.

호스트 이름이 할당된 방식에 관계없이 호스트 이름을 변경하고 새 호스트 이름을 사용하여 Unified Manager 웹 UI에 액세스하려는 경우 새 보안 인증서를 생성해야 합니다.

호스트 이름 대신 서버의 IP 주소를 사용하여 웹 UI에 액세스하는 경우 호스트 이름을 변경할 경우 새 인증서를 생성할 필요가 없습니다. 그러나 인증서의 호스트 이름이 실제 호스트 이름과 일치하도록 인증서를 업데이트하는 것이 가장 좋습니다.

Unified Manager에서 호스트 이름을 변경하는 경우 WFA(OnCommand Workflow Automation)에서 호스트 이름을 수동으로 업데이트해야 합니다. 호스트 이름은 WFA에서 자동으로 업데이트되지 않습니다.

새 인증서는 Unified Manager 가상 머신을 다시 시작할 때까지 적용되지 않습니다.

단계

## 1. HTTPS 보안 인증서를 생성합니다

새 호스트 이름을 사용하여 Unified Manager 웹 UI에 액세스하려면 HTTPS 인증서를 다시 생성하여 새 호스트 이름과 연결해야 합니다.

## 2. Unified Manager 가상 머신을 다시 시작합니다

HTTPS 인증서를 다시 생성한 후 Unified Manager 가상 머신을 다시 시작해야 합니다.

**HTTPS** 보안 인증서를 생성하는 중입니다

Active IQ Unified Manager를 처음 설치하면 기본 HTTPS 인증서가 설치됩니다. 기존 인증서를 대체하는 새 HTTPS 보안 인증서를 생성할 수 있습니다.

- 필요한 것 \*

애플리케이션 관리자 역할이 있어야 합니다.

고유 이름(DN)에 더 나은 값을 사용하거나 키 크기를 더 늘리거나 만료 기간을 연장하거나 현재 인증서가 만료된 경우와 같이 인증서를 다시 생성해야 하는 이유는 여러 가지가 있습니다.

Unified Manager 웹 UI에 액세스할 수 없는 경우 유지보수 콘솔을 사용하여 동일한 값으로 HTTPS 인증서를 다시 생성할 수 있습니다. 인증서를 재생성하는 동안 키 크기와 키의 유효 기간을 정의할 수 있습니다. 를 사용하는 경우 Reset Server Certificate 유지 관리 콘솔에서 옵션을 선택하면 397일 동안 유효한 새 HTTPS 인증서가 생성됩니다. 이 인증서에는 2048비트 크기의 RSA 키가 있습니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* HTTPS 인증서 \* 를 클릭합니다.
2. HTTPS 인증서 다시 생성 \* 을 클릭합니다.

HTTPS 인증서 재생성 대화 상자가 표시됩니다.

3. 인증서를 생성하는 방법에 따라 다음 옵션 중 하나를 선택합니다.

원하는 작업	수행할 작업...
현재 값을 사용하여 인증서를 다시 생성합니다	현재 인증서 특성을 사용하여 다시 생성 * 옵션을 클릭합니다.

원하는 작업	수행할 작업...
다른 값을 사용하여 인증서를 생성합니다	<p>현재 인증서 특성 업데이트 * 옵션을 클릭합니다.</p> <p>새 값을 입력하지 않으면 일반 이름 및 대체 이름 필드에 기존 인증서의 값이 사용됩니다. "공통 이름"은 호스트의 FQDN으로 설정되어야 합니다. 다른 필드에는 값이 필요하지 않지만 전자 메일, 회사, 부서 등의 값을 입력할 수 있습니다. 인증서에 해당 값을 채우려는 경우 시/도/Country를 선택합니다. 사용 가능한 키 크기(키 알고리즘은 ""RSA"")와 유효 기간 중에서 선택할 수도 있습니다.</p> <ul style="list-style-type: none"> <li>• 키 크기에 허용되는 값은 입니다 2048, 3072 및 4096.</li> <li>• 유효 기간은 최소 1일에서 최대 36500일입니다.</li> </ul> <p>유효 기간 36500일이 허용되지만 유효 기간은 397일 또는 13개월을 넘지 않는 것이 좋습니다. 397일 이상의 유효 기간을 선택하고 이 인증서에 대해 CSR을 내보내고 잘 알려진 CA가 서명한 경우 CA에서 반환한 서명된 인증서의 유효 기간이 397일로 줄어듭니다.</p> <ul style="list-style-type: none"> <li>• 인증서의 대체 이름 필드에서 로컬 식별 정보를 제거하려면 "로컬 식별 정보 제외(예: localhost)" 확인란을 선택할 수 있습니다. 이 확인란을 선택하면 필드에 입력한 항목만 대체 이름 필드에 사용됩니다. 공백으로 두면 결과 인증서에 대체 이름 필드가 전혀 없습니다.</li> </ul>

4. 예 \* 를 클릭하여 인증서를 다시 생성합니다.
5. 새 인증서가 적용되도록 Unified Manager 서버를 다시 시작합니다.
6. HTTPS 인증서를 확인하여 새 인증서 정보를 확인합니다.

**Unified Manager** 가상 머신을 재시작합니다

Unified Manager의 유지보수 콘솔에서 가상 머신을 재시작할 수 있습니다. 새 보안 인증서를 생성한 후 또는 가상 시스템에 문제가 있는 경우 를 다시 시작해야 합니다.

- 필요한 것 \*

가상 어플라이언스의 전원이 켜져 있습니다.

유지보수 사용자로 유지보수 콘솔에 로그인한 경우

또한 \* Restart Guest \* 옵션을 사용하여 vSphere에서 가상 머신을 재시작할 수 있습니다. 자세한 내용은 VMware 설명서를 참조하십시오.

단계

1. 유지보수 콘솔에 액세스합니다.
2. 시스템 구성 \* > \* 가상 시스템 재부팅 \* 을 선택합니다.

### Linux 시스템에서 Unified Manager 호스트 이름 변경

경우에 따라 Unified Manager를 설치한 Red Hat Enterprise Linux 또는 CentOS 시스템의 호스트 이름을 변경할 수 있습니다. 예를 들어 Linux 시스템을 나열할 때 호스트 이름을 Unified Manager 서버를 유형, 작업 그룹 또는 모니터링되는 클러스터 그룹별로 더 쉽게 식별하도록 변경할 수 있습니다.

- 필요한 것 \*

Unified Manager가 설치된 Linux 시스템에 대한 루트 사용자 액세스 권한이 있어야 합니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 Unified Manager 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP 주소를 구성한 경우 네트워크 호스트의 이름을 지정했을 것입니다. DHCP를 사용하여 네트워크를 구성한 경우 DNS 서버에서 호스트 이름을 가져와야 합니다.

호스트 이름이 할당된 방식에 관계없이 호스트 이름을 변경하고 새 호스트 이름을 사용하여 Unified Manager 웹 UI에 액세스하려는 경우 새 보안 인증서를 생성해야 합니다.

호스트 이름 대신 서버의 IP 주소를 사용하여 웹 UI에 액세스하는 경우 호스트 이름을 변경할 경우 새 인증서를 생성할 필요가 없습니다. 그러나 인증서의 호스트 이름이 실제 호스트 이름과 일치하도록 인증서를 업데이트하는 것이 가장 좋습니다. 새 인증서는 Linux 시스템을 다시 시작할 때까지 적용되지 않습니다.

Unified Manager에서 호스트 이름을 변경하는 경우 WFA(OnCommand Workflow Automation)에서 호스트 이름을 수동으로 업데이트해야 합니다. 호스트 이름은 WFA에서 자동으로 업데이트되지 않습니다.

단계

1. 수정할 Unified Manager 시스템의 루트 사용자로 로그인합니다.
2. 다음 명령을 입력하여 Unified Manager 소프트웨어 및 관련 MySQL 소프트웨어를 중지합니다.

```
systemctl stop ocieau ocie mysqld
```

3. Linux를 사용하여 호스트 이름을 변경합니다 hostnamectl 명령:

```
hostnamectl set-hostname new_FQDN
```

```
hostnamectl set-hostname nuhost.corp.widget.com
```

4. 서버에 대한 HTTPS 인증서를 다시 생성합니다.

```
/opt/netapp/essentials/bin/cert.sh create
```

5. 네트워크 서비스를 다시 시작합니다.

```
service network restart
```

6. 서비스가 다시 시작된 후 새 호스트 이름이 스스로 ping을 수행할 수 있는지 확인합니다.

```
ping new_hostname
```

```
ping nuhost
```

이 명령은 원래 호스트 이름에 대해 이전에 설정된 것과 동일한 IP 주소를 반환해야 합니다.

7. 호스트 이름 변경을 완료하고 확인한 후 다음 명령을 입력하여 Unified Manager를 다시 시작합니다.

```
systemctl start mysqld ocie ocieau
```

## 정책 기반 스토리지 관리 설정 및 해제

Unified Manager 9.7부터 ONTAP 클러스터에 스토리지 워크로드(볼륨 및 LUN)를 프로비저닝하고 지정된 성능 서비스 수준에 따라 해당 워크로드를 관리할 수 있습니다. 이 기능은 ONTAP System Manager에서 워크로드를 생성하고 QoS 정책을 연결하는 것과 비슷하지만, Unified Manager를 사용하여 적용할 경우 Unified Manager 인스턴스가 모니터링하는 모든 클러스터에서 워크로드를 프로비저닝하고 관리할 수 있습니다.

애플리케이션 관리자 역할이 있어야 합니다.

이 옵션은 기본적으로 활성화되어 있지만 Unified Manager를 사용하여 워크로드를 프로비저닝하고 관리하지 않으려는 경우 비활성화할 수 있습니다.

이 옵션을 활성화하면 사용자 인터페이스에 많은 새 항목이 제공됩니다.

새 콘텐츠	위치
새로운 워크로드를 프로비저닝하는 데 필요한 페이지입니다	일반 작업 * > * 프로비저닝 * 에서 사용할 수 있습니다
성능 서비스 수준 정책을 생성하는 페이지입니다	설정 * > * 정책 * > * 성능 서비스 수준 * 에서 사용할 수 있습니다
성능 스토리지 효율성 정책을 생성하는 페이지입니다	설정 * > * 정책 * > * 스토리지 효율성 * 에서 사용할 수 있습니다
현재 워크로드 성능 및 워크로드 IOPS를 설명하는 패널	대시보드에서 사용할 수 있습니다

이러한 페이지 및 이 기능에 대한 자세한 내용은 제품의 온라인 도움말을 참조하십시오.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 기능 설정 \* 을 클릭합니다.
2. 기능 설정 \* 페이지에서 다음 옵션 중 하나를 선택하여 정책 기반 스토리지 관리를 비활성화하거나 활성화합니다.

원하는 작업	다음을 수행하십시오.
정책 기반 스토리지 관리를 해제합니다	Policy-based storage management * (정책 기반 저장소 관리 *) 패널에서 슬라이더 버튼을 왼쪽으로 이동합니다.
정책 기반 스토리지 관리 설정	Policy-based storage management * (정책 기반 저장소 관리 *) 패널에서 슬라이더 버튼을 오른쪽으로 이동합니다.

## Unified Manager 백업 구성

호스트 시스템과 를 통해 유지보수 콘솔에서 수행할 구성 단계 세트를 통해 Unified Manager의 백업 기능을 구성할 수 있습니다.

구성 단계에 대한 자세한 내용은 를 참조하십시오 ["백업 및 복원 작업 관리"](#).

## 기능 설정 관리

기능 설정 페이지에서 Active IQ Unified Manager의 특정 기능을 활성화 및 비활성화할 수 있습니다. 여기에는 정책에 따라 스토리지 객체 생성 및 관리, API 게이트웨이 및 로그인 배너 활성화, 알림 관리를 위한 스크립트 업로드, 비활성 시간에 따른 웹 UI 세션 시간 초과, Active IQ 플랫폼 이벤트 수신 비활성화 등이 포함됩니다.



기능 설정 페이지는 응용 프로그램 관리자 역할을 가진 사용자만 사용할 수 있습니다.

스크립트 업로드에 대한 자세한 내용은 을 참조하십시오 ["스크립트 업로드 활성화 및 비활성화"](#).

### 정책 기반 스토리지 관리 설정

정책 기반 스토리지 관리 \* 옵션을 사용하면 서비스 수준 목표(SLO)를 기준으로 스토리지를 관리할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

이 기능을 활성화하면 Active IQ Unified Manager 인스턴스에 추가된 ONTAP 클러스터에서 스토리지 워크로드를 프로비저닝하고 할당된 성능 서비스 수준 및 스토리지 효율성 정책을 기반으로 이러한 워크로드를 관리할 수 있습니다.

이 기능은 \* 일반 \* > \* 기능 설정 \* > \* 정책 기반 스토리지 관리 \* 에서 활성화 또는 비활성화할 수 있습니다. 이 기능을 활성화하면 다음 페이지를 작동 및 모니터링할 수 있습니다.

- 프로비저닝(스토리지 워크로드 프로비저닝)
- \* 정책 \* > \* 성능 서비스 수준 \*
- \* 정책 \* > \* 스토리지 효율성 \*
- 클러스터 설정 페이지의 성능 서비스 수준별로 관리되는 작업 부하 열
- Dashboard \* 의 워크로드 성능 패널입니다

화면에서 성능 서비스 수준 및 스토리지 효율성 정책을 생성하고 스토리지 워크로드를 프로비저닝할 수 있습니다. 또한, 할당된 성능 서비스 수준과 부적합 사항을 준수하는 스토리지 워크로드를 모니터링할 수 있습니다. 또한 워크로드 성능 및 워크로드 IOPS 패널을 사용하면 프로비저닝된 스토리지 워크로드를 기준으로 데이터 센터 전체의 클러스터에서 사용 가능한 총 용량 및 성능(IOPS)을 평가할 수 있습니다.

이 기능을 활성화한 후 Unified Manager REST API를 실행하여 이러한 기능 중 일부를 \* Menu Bar \* > \* Help 버튼 \* > \* API Documentation \* > \* storage-provider \* 범주에서 수행할 수 있습니다. 또는 호스트 이름 또는 IP 주소와 URL을 입력하여 REST API 페이지에 <https://<hostname>/docs/api/> 형식으로 액세스할 수 있습니다

API에 대한 자세한 내용은 를 참조하십시오 "[Active IQ Unified Manager REST API 시작하기](#)".

## API 게이트웨이 활성화 중

API 게이트웨이 기능을 통해 Active IQ Unified Manager는 개별적으로 로그인하지 않고도 여러 ONTAP 클러스터를 관리할 수 있는 단일 제어 플레인이 될 수 있습니다.

Unified Manager에 처음 로그인할 때 나타나는 구성 페이지에서 이 기능을 사용하도록 설정할 수 있습니다. 또는 \* 일반 \* > \* 기능 설정 \* > \* API 게이트웨이 \* 에서 이 기능을 활성화 또는 비활성화할 수 있습니다.

Unified Manager REST API는 ONTAP REST API와 다르며, ONTAP REST API를 사용하여 모든 기능을 사용할 수 있는 것은 아닙니다. 그러나 Unified Manager에 노출되지 않은 특정 기능을 관리하기 위해 ONTAP API에 액세스해야 하는 특정 비즈니스 요구 사항이 있는 경우 API 게이트웨이 기능을 설정하고 ONTAP API를 실행할 수 있습니다. 게이트웨이는 ONTAP API와 동일한 형식으로 헤더와 본문 요청을 유지함으로써 API 요청을 터널링하기 위한 프록시 역할을 합니다. Unified Manager 자격 증명을 사용하고 특정 API를 실행하여 개별 클러스터 자격 증명을 전달하지 않고 ONTAP 클러스터에 액세스하고 관리할 수 있습니다. Unified Manager는 Unified Manager 인스턴스에서 관리되는 ONTAP 클러스터에서 API를 실행하기 위한 단일 관리 지점 역할을 수행합니다. API가 반환하는 응답은 ONTAP에서 직접 실행되는 각 ONTAP REST API가 반환하는 응답과 동일합니다.

이 기능을 활성화한 후 \* 메뉴 모음 \* > \* 도움말 버튼 \* > \* API 문서 \* > \* 게이트웨이 \* 범주에서 Unified Manager REST API를 실행할 수 있습니다. 또는 호스트 이름 또는 IP 주소와 URL을 입력하여 REST API 페이지에 액세스할 수 있습니다 <https://<hostname>/docs/api/>

API에 대한 자세한 내용은 를 참조하십시오 "[Active IQ Unified Manager REST API 시작하기](#)".

## 비활성 시간 초과 지정

Active IQ Unified Manager에 대한 비활성 시간 초과 값을 지정할 수 있습니다. 지정된 시간 동안 사용하지 않으면 응용 프로그램이 자동으로 로그아웃됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

이 기능을 비활성화하거나 \* 일반 \* > \* 기능 설정 \* > \* 비활성 시간 제한 \* 에서 시간을 수정할 수 있습니다. 이 기능을 활성화하면 \* 로그아웃 후 \* 필드에 비활성 시간 제한(분 단위)을 지정해야 합니다. 이 시간 이후에는 시스템이 자동으로 로그아웃됩니다. 기본값은 4320분(72시간)입니다.



SAML(Security Assertion Markup Language) 인증을 활성화한 경우에는 이 옵션을 사용할 수 없습니다.

## Active IQ 포털 이벤트 활성화

Active IQ 포털 이벤트 활성화 또는 비활성화 여부를 지정할 수 있습니다. 이 설정을 사용하면

Active IQ 포털에서 시스템 구성, 케이블 연결 등에 대한 추가 이벤트를 검색하고 표시할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

이 기능을 활성화하면 Active IQ Unified Manager는 Active IQ 포털에서 검색된 이벤트를 표시합니다. 이러한 이벤트는 모니터링되는 모든 스토리지 시스템에서 생성되는 AutoSupport 메시지에 대해 일련의 규칙을 실행하여 생성됩니다. 이러한 이벤트는 다른 Unified Manager 이벤트와 다르며, 시스템 구성, 케이블 연결, 모범 사례 및 가용성 문제와 관련된 사고 또는 위험을 식별합니다.

이 기능은 \* 일반 \* > \* 기능 설정 \* > \* Active IQ 포털 이벤트 \* 에서 활성화 또는 비활성화할 수 있습니다. 외부 네트워크에 액세스할 수 없는 사이트에서는 \* 스토리지 관리 \* > \* 이벤트 설정 \* > \* 업로드 규칙 \* 에서 수동으로 규칙을 업로드해야 합니다.

이 기능은 기본적으로 활성화되어 있습니다. 이 기능을 사용하지 않도록 설정하면 Active IQ 이벤트가 검색되지 않고 Unified Manager에 표시되지 않습니다. 이 기능을 비활성화하면 Unified Manager가 해당 클러스터 시간대의 사전 정의된 시간 00:15에서 클러스터에서 Active IQ 이벤트를 수신할 수 있습니다.

## 규정 준수를 위한 보안 설정 활성화 및 비활성화

기능 설정 페이지의 \* 보안 대시보드 \* 패널에 있는 \* 사용자 정의 \* 버튼을 사용하여 Unified Manager에서 규정 준수 모니터링을 위한 보안 매개 변수를 활성화 또는 비활성화할 수 있습니다.

이 페이지에서 설정 또는 사용하지 않도록 설정하면 Unified Manager에서 클러스터 및 스토리지 VM의 전반적인 규정 준수 상태가 적용됩니다. 선택한 항목에 따라 클러스터 인벤토리 페이지의 \* 보안: 모든 클러스터 \* 보기와 스토리지 VM 인벤토리 페이지의 \* 보안: 모든 스토리지 VM \* 보기에 해당 열이 표시됩니다.



관리자 역할을 가진 사용자만 이러한 설정을 편집할 수 있습니다.

ONTAP 클러스터, 스토리지 VM 및 볼륨의 보안 기준은 에 정의된 권장 사항을 기준으로 평가됩니다. "[Security Hardening Guide for NetApp ONTAP 9](#) 을 참조하십시오". 대시보드와 보안 페이지의 보안 패널에는 클러스터, 스토리지 VM 및 볼륨의 기본 보안 준수 상태가 표시됩니다. 보안 이벤트도 생성되고 보안 위반이 있는 클러스터 및 스토리지 VM에 대해 관리 작업이 활성화됩니다.

### 보안 설정 사용자 지정

ONTAP 환경에 적용할 수 있는 규정 준수 모니터링 설정을 사용자 지정하려면 다음 단계를 수행하십시오.

#### 단계

1. 일반 > 기능 설정 > 보안 대시보드 > 사용자 지정 \* 을 클릭합니다. 보안 대시보드 설정 사용자 지정 \* 팝업이 나타납니다.



설정 또는 해제하는 보안 규정 준수 매개 변수는 클러스터 및 스토리지 VM 화면의 기본 보안 보기, 보고서 및 예약된 보고서에 직접 영향을 줄 수 있습니다. 보안 매개 변수를 수정하기 전에 이러한 화면에서 Excel 보고서를 업로드한 경우 다운로드한 Excel 보고서에 오류가 있을 수 있습니다.

2. ONTAP 클러스터에 대한 사용자 정의 설정을 활성화 또는 비활성화하려면 \* 클러스터 \* 에서 필요한 일반 설정을 선택합니다. 클러스터 규정 준수를 사용자 지정하는 옵션에 대한 자세한 내용은 을 참조하십시오 "[클러스터 규정 준수 범주](#)".
3. 스토리지 VM에 대한 사용자 지정 설정을 활성화 또는 비활성화하려면 \* 스토리지 VM \* 에서 필요한 일반 설정을 선택합니다. 스토리지 VM 규정 준수를 사용자 지정하는 옵션에 대한 자세한 내용은 를 참조하십시오 "[스토리지 VM](#)".



규정 준수 범주".

## AutoSupport 및 인증 설정 사용자 지정

AutoSupport 설정 \* 섹션에서 AutoSupport에서 ONTAP 메시지를 보내는 데 HTTPS 전송을 사용할지 여부를 지정할 수 있습니다.

인증 설정 \* 섹션에서 기본 ONTAP 관리자 사용자에게 대해 Unified Manager 알림을 발생하도록 설정할 수 있습니다.

## 스크립트 업로드 활성화 및 비활성화

스크립트를 Unified Manager에 업로드하여 실행할 수 있는 기능은 기본적으로 활성화되어 있습니다. 보안상의 이유로 조직에서 이 작업을 허용하지 않으려는 경우 이 기능을 사용하지 않도록 설정할 수 있습니다.

- 필요한 것 \*

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 기능 설정 \* 을 클릭합니다.
2. 기능 설정 \* 페이지에서 다음 옵션 중 하나를 선택하여 스크립팅을 비활성화하거나 활성화합니다.

원하는 작업	다음을 수행하십시오.
스크립트를 사용하지 않도록 설정합니다	Script Upload* 패널에서 슬라이더 단추를 왼쪽으로 이동합니다.
스크립트를 사용하도록 설정합니다	Script Upload* 패널에서 슬라이더 단추를 오른쪽으로 이동합니다.

## 로그인 배너 추가 중

로그인 배너를 추가하면 조직에서 시스템에 액세스할 수 있는 사용자, 로그인 및 로그아웃 시 사용 약관 등의 정보를 표시할 수 있습니다.

스토리지 운영자 또는 관리자와 같은 모든 사용자는 로그인, 로그아웃 및 세션 시간 초과 중에 이 로그인 배너 팝업을 볼 수 있습니다.

## 유지보수 콘솔 사용

유지보수 콘솔을 사용하여 네트워크 설정을 구성하고, Unified Manager가 설치된 시스템을 구성 및 관리하고, 기타 유지보수 작업을 수행하여 발생할 수 있는 문제를 예방하고 해결할 수 있습니다.

유지보수 콘솔에서 제공하는 기능은 무엇입니까

Unified Manager 유지보수 콘솔을 사용하면 Unified Manager 시스템의 설정을 유지하고 문제 발생을 방지하기 위해 필요한 모든 변경을 수행할 수 있습니다.

Unified Manager를 설치한 운영 체제에 따라 유지보수 콘솔에서 다음 기능을 제공합니다.

- 특히 Unified Manager 웹 인터페이스를 사용할 수 없는 경우, 가상 어플라이언스 관련 문제를 해결합니다
- 최신 버전의 Unified Manager로 업그레이드하십시오
- 기술 지원 팀에 보낼 지원 번들을 생성합니다
- 네트워크 설정을 구성합니다
- 유지보수 사용자 암호를 변경합니다
- 외부 데이터 공급자에 연결하여 성능 통계를 보냅니다
- 성능 데이터 수집 내부 변경
- 이전에 백업한 버전에서 Unified Manager 데이터베이스 및 구성 설정을 복원합니다.

유지 관리 사용자가 수행하는 작업

유지 관리 사용자는 Red Hat Enterprise Linux 또는 CentOS 시스템에 Unified Manager를 설치하는 동안 생성됩니다. 유지보수 사용자 이름은 "umadmin" 사용자입니다. 유지 관리 사용자는 웹 UI에서 응용 프로그램 관리자 역할을 가지고 있으며, 사용자는 후속 사용자를 만들고 해당 역할을 할당할 수 있습니다.

유지보수 사용자 또는 umadmin 사용자도 Unified Manager 유지보수 콘솔에 액세스할 수 있습니다.

진단 사용자 기능

진단 액세스의 목적은 기술 지원 부서에서 문제 해결을 지원하도록 하는 것입니다. 기술 지원 부서의 지시가 있을 때만 사용해야 합니다.

진단 사용자는 문제 해결을 위해 기술 지원 부서의 지시가 있을 때 OS 레벨 명령을 실행할 수 있습니다.

유지보수 콘솔 액세스

Unified Manager 사용자 인터페이스가 작동 중이 아니거나 사용자 인터페이스에서 사용할 수 없는 기능을 수행해야 하는 경우, 유지보수 콘솔에 액세스하여 Unified Manager 시스템을 관리할 수 있습니다.

- 필요한 것 \*

Unified Manager를 설치하고 구성해야 합니다.

15분 동안 비활성 상태가 지속되면 유지보수 콘솔에서 로그아웃합니다.



VMware에 설치된 경우 VMware 콘솔을 통해 유지 관리 사용자로 이미 로그인한 경우에는 Secure Shell을 사용하여 동시에 로그인할 수 없습니다.

#### 단계

1. 다음 단계에 따라 유지보수 콘솔에 액세스합니다.

이 운영 체제에서...	다음 단계를 따르십시오...
VMware	<ol style="list-style-type: none"> <li>a. Secure Shell을 사용하여 Unified Manager 가상 어플라이언스의 IP 주소 또는 정규화된 도메인 이름에 연결합니다.</li> <li>b. 유지보수 사용자 이름과 암호를 사용하여 유지보수 콘솔에 로그인합니다.</li> </ol>
리눅스	<ol style="list-style-type: none"> <li>a. Secure Shell을 사용하여 Unified Manager 시스템의 IP 주소 또는 정규화된 도메인 이름에 연결합니다.</li> <li>b. 유지보수 사용자(umadmin) 이름 및 암호를 사용하여 시스템에 로그인합니다.</li> <li>c. 명령을 입력합니다 maintenance_console Enter 키를 누릅니다.</li> </ol>
Windows	<ol style="list-style-type: none"> <li>a. 관리자 자격 증명을 사용하여 Unified Manager 시스템에 로그인합니다.</li> <li>b. Windows 관리자로 PowerShell을 실행합니다.</li> <li>c. 명령을 입력합니다 maintenance_console Enter 키를 누릅니다.</li> </ol>

Unified Manager 유지보수 콘솔 메뉴가 표시됩니다.

### vSphere VM 콘솔을 사용하여 유지 관리 콘솔 액세스

Unified Manager 사용자 인터페이스가 작동 중이 아니거나 사용자 인터페이스에서 사용할 수 없는 기능을 수행해야 하는 경우 유지보수 콘솔에 액세스하여 가상 어플라이언스를 재구성할 수 있습니다.

- 필요한 것 \*
- 유지 보수 사용자여야 합니다.
- 유지보수 콘솔에 액세스하려면 가상 어플라이언스의 전원을 켜야 합니다.

#### 단계

1. vSphere Client에서 Unified Manager 가상 어플라이언스를 찾습니다.
2. Console \* 탭을 클릭합니다.

3. 콘솔 창 내부를 클릭하여 로그인합니다.
4. 사용자 이름 및 암호를 사용하여 유지보수 콘솔에 로그인합니다.

15분 동안 비활성 상태가 지속되면 유지보수 콘솔에서 로그아웃합니다.

## 유지보수 콘솔 메뉴

유지보수 콘솔은 Unified Manager 서버의 특수 기능 및 구성 설정을 유지 관리 및 관리할 수 있는 다양한 메뉴로 구성되어 있습니다.

Unified Manager를 설치한 운영 체제에 따라 유지보수 콘솔은 다음 메뉴로 구성됩니다.

- Unified Manager 업그레이드(VMware만 해당)
- 네트워크 구성(VMware만 해당)
- 시스템 구성(VMware만 해당)
  - a. 지원/진단
  - b. 서버 인증서를 재설정합니다
  - c. 외부 데이터 공급자
  - d. 백업 복원
  - e. 성능 폴링 간격 구성
  - f. SAML 인증을 비활성화합니다
  - g. 애플리케이션 포트 보기/변경
  - h. 디버그 로그 구성
    - i. MySQL 포트 3306에 대한 액세스를 제어합니다
    - j. Exit(종료)

특정 메뉴 옵션에 액세스하기 위해 목록에서 번호를 선택합니다. 예를 들어 백업 및 복원의 경우 \_4\_를 선택합니다.

## 네트워크 구성 메뉴

네트워크 구성 메뉴를 사용하여 네트워크 설정을 관리할 수 있습니다. Unified Manager 사용자 인터페이스를 사용할 수 없는 경우 이 메뉴를 사용해야 합니다.



Unified Manager가 Red Hat Enterprise Linux, CentOS 또는 Microsoft Windows에 설치된 경우에는 이 메뉴를 사용할 수 없습니다.

다음 메뉴를 선택할 수 있습니다.

- \* IP 주소 설정 표시 \*

IP 주소, 네트워크, 브로드캐스트 주소, 넷마스크, 게이트웨이를 포함하여 가상 어플라이언스에 대한 현재 네트워크 설정을 표시합니다. DNS 서버가 있습니다.

- \* IP 주소 설정 변경 \*

IP 주소, 넷마스크, 게이트웨이 또는 DNS 서버를 포함하여 가상 어플라이언스에 대한 네트워크 설정을 변경할 수 있습니다. 유지보수 콘솔을 사용하여 네트워크 설정을 DHCP에서 정적 네트워킹으로 전환하는 경우 호스트 이름을 편집할 수 없습니다. 변경 사항을 적용하려면 \* 변경 사항 커밋 \* 을 선택해야 합니다.

- \* 도메인 이름 검색 설정 표시 \*

호스트 이름을 확인하는 데 사용되는 도메인 이름 검색 목록을 표시합니다.

- \* 도메인 이름 검색 설정 변경 \*

호스트 이름을 확인할 때 검색할 도메인 이름을 변경할 수 있습니다. 변경 사항을 적용하려면 \* 변경 사항 커밋 \* 을 선택해야 합니다.

- \* 정적 라우트 표시 \*

현재 정적 네트워크 경로를 표시합니다.

- \* 정적 라우트 변경 \*

정적 네트워크 경로를 추가하거나 삭제할 수 있습니다. 변경 사항을 적용하려면 \* 변경 사항 커밋 \* 을 선택해야 합니다.

- \* 루트 추가 \*

정적 경로를 추가할 수 있습니다.

- \* 루트 삭제 \*

정적 라우트를 삭제할 수 있습니다.

- \* 뒤로 \*

기본 메뉴 \* 로 돌아갑니다.

- \* 종료 \*

유지보수 콘솔을 종료합니다.

- \* 네트워크 인터페이스 비활성화 \*

사용 가능한 네트워크 인터페이스를 비활성화합니다. 하나의 네트워크 인터페이스만 사용할 수 있는 경우에는 비활성화할 수 없습니다. 변경 사항을 적용하려면 \* 변경 사항 커밋 \* 을 선택해야 합니다.

- \* 네트워크 인터페이스 사용 \*

사용 가능한 네트워크 인터페이스를 활성화합니다. 변경 사항을 적용하려면 \* 변경 사항 커밋 \* 을 선택해야 합니다.

- \* 변경 사항을 커밋합니다 \*

가상 어플라이언스의 네트워크 설정에 대한 변경 사항을 적용합니다. 변경 사항을 적용하려면 이 옵션을 선택해야 합니다. 그렇지 않으면 변경 내용이 적용되지 않습니다.

- \* 호스트에 Ping \*

IP 주소 변경 또는 DNS 구성을 확인하기 위해 타겟 호스트에 ping을 보냅니다.

- \* 기본 설정으로 복원 \*

모든 설정을 출하 시 기본값으로 재설정합니다. 변경 사항을 적용하려면 \* 변경 사항 커밋 \* 을 선택해야 합니다.

- \* 뒤로 \*

기본 메뉴 \* 로 돌아갑니다.

- \* 종료 \*

유지보수 콘솔을 종료합니다.

### System Configuration(시스템 구성) 메뉴

시스템 구성 메뉴를 사용하면 서버 상태 보기, 가상 시스템 재부팅 및 종료 등의 다양한 옵션을 제공하여 가상 어플라이언스를 관리할 수 있습니다.



Unified Manager가 Linux 또는 Microsoft Windows 시스템에 설치된 경우 이 메뉴에서 ""Unified Manager 백업에서 복원" 옵션만 사용할 수 있습니다.

다음 메뉴를 선택할 수 있습니다.

- \* 서버 상태 표시 \*

현재 서버 상태를 표시합니다. 상태 옵션에는 실행 중 및 실행 중이 아닙니다.

서버가 실행되고 있지 않으면 기술 지원 부서에 문의해야 할 수 있습니다.

- \* 가상 머신을 재부팅합니다 \*

가상 시스템을 재부팅하여 모든 서비스를 중지합니다. 재부팅 후 가상 머신과 서비스가 다시 시작됩니다.

- \* 가상 머신 종료 \*

가상 머신을 종료하고 모든 서비스를 중지합니다.

이 옵션은 가상 시스템 콘솔에서만 선택할 수 있습니다.

- \* <로그인한 사용자> 사용자 암호 변경 \*

현재 로그인한 사용자의 암호를 변경합니다. 이 암호는 유지 관리 사용자만 될 수 있습니다.

- \* 데이터 디스크 크기 증가 \*

가상 시스템에서 데이터 디스크(디스크 3)의 크기를 늘립니다.

- \* 스왑 디스크 크기 증가 \*

가상 시스템에서 스왑 디스크(디스크 2)의 크기를 늘립니다.

- \* 시간대 변경 \*

시간대를 사용자의 위치로 변경합니다.

- \* NTP 서버 변경 \*

IP 주소 또는 FQDN(정규화된 도메인 이름)과 같은 NTP 서버 설정을 변경합니다.

- \* NTP 서비스 변경 \*

를 전환합니다 ntp 및 systemd-timesyncd 서비스.

- \* Unified Manager Backup에서 복원 \*

Unified Manager 데이터베이스와 구성 설정을 이전에 백업된 버전에서 복원합니다.

- \* 서버 인증서 재설정 \* 을 선택합니다

서버 보안 인증서를 재설정합니다.

- \* 호스트 이름 변경 \*

가상 어플라이언스가 설치된 호스트의 이름을 변경합니다.

- \* 뒤로 \*

시스템 구성 메뉴를 종료하고 주 메뉴로 돌아갑니다.

- \* 종료 \*

유지보수 콘솔 메뉴를 종료합니다.

## 지원 및 진단 메뉴

지원 및 진단 메뉴를 사용하면 문제 해결 지원을 위해 기술 지원 부서에 보낼 수 있는 지원 번들을 생성할 수 있습니다.

다음 메뉴 옵션을 사용할 수 있습니다.

- \* Light Support Bundle \* 생성

에서는 30일 동안의 로그 및 구성 데이터베이스 레코드를 포함하는 경량 지원 번들을 생성할 수 있습니다. 성능 데이터, 획득 기록 파일 및 서버 힙 덤프는 제외됩니다.

- \* 지원 번들 생성 \*

진단 사용자의 홈 디렉토리에 진단 정보가 포함된 전체 지원 번들(7-Zip 파일)을 생성할 수 있습니다. 시스템이 인터넷에 연결되어 있는 경우 지원 번들을 NetApp에 업로드할 수도 있습니다.

이 파일에는 AutoSupport 메시지에서 생성된 정보, Unified Manager 데이터베이스의 콘텐츠, Unified Manager

서버 내부 구성 요소에 대한 자세한 데이터, 일반적으로 AutoSupport 메시지 또는 경량 지원 번들에 포함되지 않은 자세한 레벨의 로그가 포함됩니다.

## 추가 메뉴 옵션

다음 메뉴 옵션을 사용하여 Unified Manager 서버에서 다양한 관리 작업을 수행할 수 있습니다.

다음 메뉴를 선택할 수 있습니다.

- \* 서버 인증서 재설정 \* 을 선택합니다

HTTPS 서버 인증서를 재생성합니다.

Unified Manager GUI에서 \* 일반 \* > \* HTTPS 인증서 \* > \* HTTPS 인증서 다시 생성 \* 을 클릭하여 서버 인증서를 다시 생성할 수 있습니다.

- \* SAML 인증 비활성화 \*

ID 공급자(IDP)가 Unified Manager GUI에 액세스하는 사용자에게 대해 로그인 인증을 더 이상 제공하지 않도록 SAML 인증을 비활성화합니다. 이 콘솔 옵션은 일반적으로 IDP 서버 또는 SAML 구성 문제로 인해 사용자가 Unified Manager GUI에 액세스하지 못하게 되는 경우에 사용됩니다.

- \* 외부 데이터 공급자 \*

Unified Manager를 외부 데이터 공급자에 연결하는 옵션을 제공합니다. 연결을 설정하면 성능 데이터가 외부 서버로 전송되므로 스토리지 성능 전문가가 타사 소프트웨어를 사용하여 성능 메트릭을 차트로 작성할 수 있습니다. 다음 옵션이 표시됩니다.

- \* Display Server Configuration \* — 외부 데이터 공급자에 대한 현재 연결 및 구성 설정을 표시합니다.
- \* 서버 연결 추가/수정 \* — 외부 데이터 공급자에 대한 새 연결 설정을 입력하거나 기존 설정을 변경할 수 있습니다.
- \* 서버 구성 수정 \* — 외부 데이터 공급자에 대한 새 구성 설정을 입력하거나 기존 설정을 변경할 수 있습니다.
- \* 서버 연결 삭제 \* — 외부 데이터 공급자에 대한 연결을 삭제합니다.

연결이 삭제된 후 Unified Manager는 외부 서버와의 연결이 끊어집니다.

- \* 백업 복원 \*

자세한 내용은 의 항목을 참조하십시오 ["백업 및 복원 작업 관리"](#).

- \* 성능 폴링 간격 구성 \*

Unified Manager가 클러스터에서 성능 통계 데이터를 수집하는 빈도를 구성할 수 있는 옵션을 제공합니다. 기본 수집 간격은 5분입니다.

대규모 클러스터의 컬렉션이 적시에 완료되지 않는 경우 이 간격을 10분 또는 15분으로 변경할 수 있습니다.

- \* 응용 프로그램 포트 보기/변경 \*

Unified Manager에서 보안에 필요한 경우 HTTP 및 HTTPS 프로토콜에 사용하는 기본 포트를 변경하는 옵션을 제공합니다. 기본 포트는 HTTP의 경우 80이고 HTTPS의 경우 443입니다.



- \* MySQL 포트 3306 \* 에 대한 액세스를 제어합니다

기본 MySQL 포트 3306에 대한 호스트 액세스를 제어합니다. 보안상의 이유로 Linux, Windows 및 VMware vSphere 시스템에 Unified Manager를 새로 설치하는 동안에만 이 포트를 통한 액세스가 localhost로 제한됩니다. 이 옵션을 사용하면 로컬 호스트 및 원격 호스트 간에 이 포트의 표시 여부를 전환할 수 있습니다. 즉, 사용자 환경에서 localhost만 사용하도록 설정된 경우 이 포트를 원격 호스트에서도 사용할 수 있도록 설정할 수 있습니다. 또는 모든 호스트에 대해 활성화된 경우 이 포트의 액세스를 localhost 전용으로 제한할 수 있습니다. 이전에 원격 호스트에서 액세스가 설정된 경우 구성은 업그레이드 시나리오에서 유지됩니다. 포트 표시 여부를 토글한 후 Windows 시스템의 방화벽 설정을 확인하고 MySQL 포트 3306에 대한 액세스를 제한하도록 설정이 구성된 경우 방화벽 설정을 비활성화해야 합니다.

- \* 종료 \*

유지보수 콘솔 메뉴를 종료합니다.

## Windows에서 유지 관리 사용자 암호 변경

필요한 경우 Unified Manager 유지보수 사용자 암호를 변경할 수 있습니다.

단계

1. Unified Manager 웹 UI 로그인 페이지에서 \* 암호를 잊으셨습니까 \* 를 클릭합니다.

암호를 재설정할 사용자의 이름을 묻는 페이지가 표시됩니다.

2. 사용자 이름을 입력하고 \* 제출 \* 을 클릭합니다.

암호를 재설정할 수 있는 링크가 포함된 이메일이 해당 사용자 이름에 대해 정의된 이메일 주소로 전송됩니다.

3. 이메일에서 \* 비밀번호 재설정 링크 \* 를 클릭하고 새 비밀번호를 정의합니다.

4. 웹 UI로 돌아가 새 암호를 사용하여 Unified Manager에 로그인합니다.

## Linux 시스템에서 umadmin 암호 변경

보안상의 이유로 설치 프로세스를 완료한 후 즉시 Unified Manager umadmin 사용자의 기본 암호를 변경해야 합니다. 필요한 경우 나중에 언제든지 암호를 다시 변경할 수 있습니다.

- 필요한 것 \*
- Unified Manager는 Red Hat Enterprise Linux 또는 CentOS Linux 시스템에 설치해야 합니다.
- Unified Manager가 설치된 Linux 시스템에 대한 루트 사용자 자격 증명이 있어야 합니다.

단계

1. Unified Manager가 실행 중인 Linux 시스템의 루트 사용자로 로그인합니다.

2. umadmin 암호 변경:

```
passwd umadmin
```

umadmin 사용자의 새 암호를 입력하라는 메시지가 표시됩니다.

## Unified Manager가 HTTP 및 HTTPS 프로토콜에 사용하는 포트를 변경합니다

Unified Manager가 HTTP 및 HTTPS 프로토콜에 사용하는 기본 포트는 보안에 필요한 경우 설치 후 변경할 수 있습니다. 기본 포트는 HTTP의 경우 80이고 HTTPS의 경우 443입니다.

- 필요한 것 \*

Unified Manager 서버의 유지보수 콘솔에 로그인하려면 사용자 ID와 암호가 필요합니다.



Mozilla Firefox 또는 Google Chrome 브라우저를 사용할 때 안전하지 않은 것으로 간주되는 포트가 있습니다. HTTP 및 HTTPS 트래픽에 새 포트 번호를 할당하기 전에 브라우저를 통해 확인하십시오. 안전하지 않은 포트를 선택하면 시스템에 액세스할 수 없게 될 수 있으므로 고객 지원 센터에 문의하여 문제를 해결해야 합니다.

포트를 변경한 후에는 Unified Manager 인스턴스가 자동으로 다시 시작되므로 시스템을 잠시 중단해 보십시오.

1. SSH를 사용하여 Unified Manager 호스트에 대한 유지보수 사용자로 로그인합니다.

Unified Managermaintenance 콘솔 프롬프트가 표시됩니다.

2. 응용 프로그램 포트 보기/변경 \* 이라고 표시된 메뉴 옵션의 번호를 입력한 다음 Enter 키를 누릅니다.
3. 메시지가 표시되면 유지보수 사용자 암호를 다시 입력합니다.
4. HTTP 및 HTTPS 포트의 새 포트 번호를 입력한 다음 Enter 키를 누릅니다.

포트 번호를 비워 두면 프로토콜의 기본 포트가 할당됩니다.

지금 포트를 변경하고 Unified Manager를 다시 시작할지 묻는 메시지가 표시됩니다.

5. 포트를 변경하고 Unified Manager를 다시 시작하려면 \* y \* 를 입력합니다.
6. 유지보수 콘솔을 종료합니다.

변경한 후에는 URL에 새 포트 번호를 포함하여 Unified Manager 웹 UI에 액세스해야 합니다(예: + <https://host.company.com:1234+>, + <https://12.13.14.15:1122+>, 또는 + [https://\[2001:db8:0:1\]:2123+](https://[2001:db8:0:1]:2123+).)

## 네트워크 인터페이스를 추가하는 중입니다

네트워크 트래픽을 분리해야 하는 경우 새 네트워크 인터페이스를 추가할 수 있습니다.

- 필요한 것 \*

vSphere를 사용하여 가상 어플라이언스에 네트워크 인터페이스를 추가해야 합니다.

가상 어플라이언스의 전원을 켜야 합니다.



Unified Manager가 Red Hat Enterprise Linux 또는 Microsoft Windows에 설치된 경우에는 이 작업을 수행할 수 없습니다.

단계

1. vSphere 콘솔 주 메뉴에서 \* 시스템 구성 \* > \* 운영 체제 재부팅 \* 을 선택합니다.

재부팅 후 유지보수 콘솔은 새로 추가된 네트워크 인터페이스를 감지할 수 있습니다.

2. 유지보수 콘솔에 액세스합니다.

3. Network Configuration \* > \* Enable Network Interface \* 를 선택합니다.

4. 새 네트워크 인터페이스를 선택하고 \* Enter \* 를 누릅니다.

eth1 \* 을 선택하고 \* Enter \* 를 누릅니다.

5. y \* 를 입력하여 네트워크 인터페이스를 활성화합니다.

6. 네트워크 설정을 입력합니다.

정적 인터페이스를 사용하는 경우 또는 DHCP가 감지되지 않는 경우 네트워크 설정을 입력하라는 메시지가 표시됩니다.

네트워크 설정을 입력하면 자동으로 \* 네트워크 구성 \* 메뉴로 돌아갑니다.

7. 변경 사항 커밋 \* 을 선택합니다.

네트워크 인터페이스를 추가하려면 변경 사항을 커밋해야 합니다.

## Unified Manager 데이터베이스 디렉토리에 디스크 공간 추가

Unified Manager 데이터베이스 디렉토리는 ONTAP 시스템에서 수집된 모든 상태 및 성능 데이터가 포함되어 있습니다. 경우에 따라 데이터베이스 디렉토리의 크기를 늘려야 할 수 있습니다.

예를 들어, Unified Manager가 각 클러스터에 노드가 많은 수의 클러스터에서 데이터를 수집하는 경우 데이터베이스 디렉토리가 가득 찰 수 있습니다. 데이터베이스 디렉토리가 90% 찼을 때 경고 이벤트가 수신되고 디렉토리가 95% 찼을 때 중요한 이벤트가 발생합니다.



디렉토리가 95% 꽉 찬 후 클러스터에서 추가 데이터가 수집되지 않습니다.

데이터 디렉토리에 용량을 추가하는 데 필요한 단계는 Unified Manager가 VMware ESXi 서버, Red Hat 또는 CentOS Linux 서버 또는 Microsoft Windows 서버에서 실행 중인지 여부에 따라 다릅니다.

**Linux** 호스트의 데이터 디렉토리에 공간을 추가합니다

에 디스크 공간을 충분히 할당했다면 /opt/netapp/data Unified Manager를 지원하는 디렉토리 처음에 Linux 호스트를 설정한 다음 Unified Manager를 설치하면 에서 디스크 공간을 늘려서 설치 후 디스크 공간을 추가할 수 있습니다 /opt/netapp/data 디렉토리.

• 필요한 것 \*

Unified Manager가 설치된 Red Hat Enterprise Linux 또는 CentOS Linux 시스템에 대한 루트 사용자 액세스 권한이 있어야 합니다.

데이터 디렉토리 크기를 늘리기 전에 Unified Manager 데이터베이스를 백업하는 것이 좋습니다.

단계

1. 디스크 공간을 추가할 Linux 시스템에 루트 사용자로 로그인합니다.
2. Unified Manager 서비스 및 관련 MySQL 소프트웨어를 표시된 순서대로 중지합니다.

```
systemctl stop ocieau ocie mysqld
```

3. 임시 백업 폴더 생성(예: /backup-data)에 현재 데이터를 포함할 충분한 디스크 공간이 있어야 합니다 /opt/netapp/data 디렉토리.
4. 기존 의 콘텐츠 및 권한 구성을 복사합니다 /opt/netapp/data 백업 데이터 디렉토리에 대한 디렉토리:

```
cp -arp /opt/netapp/data/* /backup-data
```

5. SE Linux가 활성화된 경우:

- a. 기존 폴더의 SE Linux 유형을 가져옵니다 /opt/netapp/data 폴더:

```
se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1
```

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
echo $se_type  
mysqld_db_t
```

- a. chcon 명령을 실행하여 백업 디렉토리에 대한 SE Linux 유형을 설정합니다.

```
chcon -R --type=mysqld_db_t /backup-data
```

6. 의 내용을 제거합니다 /opt/netapp/data 디렉터리:

- a. cd /opt/netapp/data
- b. rm -rf \*

7. 의 크기를 확장합니다 /opt/netapp/data LVM 명령을 사용하거나 추가 디스크를 추가하여 최소 150GB의 디렉토리에 디렉토리를 추가합니다.



을(를) 만든 경우 /opt/netapp/data 디스크에서 마운트를 시도하지 마십시오 /opt/netapp/data NFS 또는 CIFS 공유입니다. 이 경우 디스크 공간을 확장하려고 하면 와 같은 일부 LVM 명령이 사용됩니다 resize 및 extend 예상대로 작동하지 않을 수 있습니다.

8. 를 확인합니다 /opt/netapp/data 디렉터리 소유자(MySQL) 및 그룹(루트)은 변경되지 않습니다.

```
ls -ltr /opt/netapp/ | grep data
```

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. SE Linux가 활성화된 경우의 컨텍스트가 맞는지 확인합니다 /opt/netapp/data 디렉토리가 여전히 mysqld\_db\_t로 설정되어 있습니다.

a. touch /opt/netapp/data/abc

b. ls -Z /opt/netapp/data/abc

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0  
/opt/netapp/data/abc
```

10. 이 추가 파일이 나중에 데이터베이스 오류를 발생시키지 않도록 abc 파일을 삭제합니다.

11. 백업 데이터의 내용을 다시 확장된 로 복사합니다 /opt/netapp/data 디렉터리:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. SE Linux가 활성화된 경우 다음 명령을 실행합니다.

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. MySQL 서비스를 시작합니다.

```
systemctl start mysqld
```

14. MySQL 서비스가 시작된 후 다음 순서대로 socie 및 socieau 서비스를 시작합니다.

```
systemctl start ocie ocieau
```

15. 모든 서비스가 시작된 후 백업 폴더를 삭제합니다 /backup-data:

```
rm -rf /backup-data
```

## VMware 가상 머신의 데이터 디스크에 공간 추가

Unified Manager 데이터베이스의 데이터 디스크 공간을 늘려야 하는 경우, Unified Manager 유지보수 콘솔을 사용하여 디스크 공간을 늘려서 설치 후 용량을 추가할 수 있습니다.

- 필요한 것 \*
- vSphere Client에 대한 액세스 권한이 있어야 합니다.
- 가상 머신에 로컬에 저장된 스냅샷이 없어야 합니다.
- 유지보수 사용자 자격 증명이 있어야 합니다.

가상 디스크의 크기를 늘리기 전에 가상 시스템을 백업하는 것이 좋습니다.

## 단계

1. vSphere Client에서 Unified Manager 가상 머신을 선택한 다음 데이터에 디스크 용량을 더 추가합니다 disk 3. 자세한 내용은 VMware 설명서를 참조하십시오.

드문 경우지만 Unified Manager 배포에서는 ""하드 디스크 3"" 대신 ""하드 디스크 2""를 데이터 디스크에 사용합니다. 구축 과정에서 이 문제가 발생한 경우 더 큰 디스크의 공간을 늘리십시오. 데이터 디스크는 항상 다른 디스크보다 더 많은 공간을 갖게 됩니다.

2. vSphere 클라이언트에서 Unified Manager 가상 머신을 선택한 다음 \* Console \* 탭을 선택합니다.
3. 콘솔 창을 클릭한 다음 사용자 이름과 암호를 사용하여 유지보수 콘솔에 로그인합니다.
4. 주 메뉴에서 \* 시스템 구성 \* 옵션의 번호를 입력합니다.
5. 시스템 구성 메뉴에서 \* 데이터 디스크 크기 증가 \* 옵션에 대한 번호를 입력합니다.

## Microsoft Windows 서버의 논리 드라이브에 공간 추가

Unified Manager 데이터베이스의 디스크 공간을 늘려야 하는 경우 Unified Manager가 설치된 논리 드라이브에 용량을 추가할 수 있습니다.

- 필요한 것 \*

Windows 관리자 권한이 있어야 합니다.

디스크 공간을 추가하기 전에 Unified Manager 데이터베이스를 백업하는 것이 좋습니다.

## 단계

1. 디스크 공간을 추가할 Windows 서버에 관리자로 로그인합니다.
2. 공간을 더 추가하는 데 사용할 방법에 해당하는 단계를 따릅니다.

옵션을 선택합니다	설명
물리적 서버에서 Unified Manager 서버가 설치된 논리 드라이브에 용량을 추가합니다.	Microsoft 항목의 단계를 따릅니다. "기본 볼륨을 확장합니다"
물리적 서버에서 하드 디스크 드라이브를 추가합니다.	Microsoft 항목의 단계를 따릅니다. "하드 디스크 드라이브 추가"
가상 머신에서 디스크 파티션의 크기를 늘립니다.	VMware 항목의 단계를 따릅니다. "디스크 파티션 크기 늘리기"

## 사용자 액세스 관리

역할을 생성하고 Active IQ Unified Manager에 대한 사용자 액세스를 제어하는 기능을 할당할 수 있습니다. Unified Manager 내에서 선택한 개체에 액세스하는 데 필요한 기능이 있는

사용자를 식별할 수 있습니다. 이러한 역할 및 기능을 가진 사용자만 Unified Manager의 개체를 관리할 수 있습니다.

## 사용자 추가

사용자 페이지를 사용하여 로컬 사용자 또는 데이터베이스 사용자를 추가할 수 있습니다. 인증 서버에 속하는 원격 사용자 또는 그룹을 추가할 수도 있습니다. 이러한 사용자에게 역할을 할당할 수 있으며 역할의 권한에 따라 사용자는 Unified Manager를 사용하여 스토리지 객체 및 데이터를 관리하거나 데이터베이스의 데이터를 볼 수 있습니다.

- 필요한 것 \*
- 애플리케이션 관리자 역할이 있어야 합니다.
- 원격 사용자 또는 그룹을 추가하려면 원격 인증을 사용하고 인증 서버를 구성해야 합니다.
- IdP(Identity Provider)가 그래픽 인터페이스에 액세스하는 사용자를 인증하도록 SAML 인증을 구성하려면 이러한 사용자가 "최종" 사용자로 정의되어 있는지 확인하십시오.

SAML 인증이 활성화된 경우 ""local"" 또는 "main유지보수" 유형의 사용자는 UI에 액세스할 수 없습니다.

Windows Active Directory에서 그룹을 추가하면 중첩된 하위 그룹이 비활성화되지 않는 한 모든 직접 구성원과 중첩된 하위 그룹이 Unified Manager에 인증할 수 있습니다. OpenLDAP 또는 기타 인증 서비스에서 그룹을 추가하는 경우 해당 그룹의 직접 구성원만 Unified Manager에 인증할 수 있습니다.

### 단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 사용자 \* 를 클릭합니다.
2. 사용자 페이지에서 \* 추가 \* 를 클릭합니다.
3. 사용자 추가 대화 상자에서 추가할 사용자 유형을 선택하고 필요한 정보를 입력합니다.

필수 사용자 정보를 입력할 때는 해당 사용자에게 고유한 이메일 주소를 지정해야 합니다. 여러 사용자가 공유하는 전자 메일 주소는 지정하지 않아야 합니다.

4. 추가 \* 를 클릭합니다.

## 데이터베이스 사용자 생성

Workflow Automation과 Unified Manager 간의 연결을 지원하거나 데이터베이스 보기에 액세스하려면 먼저 Unified Manager 웹 UI에서 통합 스키마 또는 보고서 스키마 역할을 사용하여 데이터베이스 사용자를 만들어야 합니다.

- 필요한 것 \*

애플리케이션 관리자 역할이 있어야 합니다.

데이터베이스 사용자는 Workflow Automation과 통합되어 보고서 관련 데이터베이스 뷰에 액세스할 수 있습니다. 데이터베이스 사용자는 Unified Manager 웹 UI 또는 유지보수 콘솔에 액세스할 수 없으며 API 호출을 실행할 수 없습니다.

### 단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 사용자 \* 를 클릭합니다.
2. 사용자 페이지에서 \* 추가 \* 를 클릭합니다.
3. 사용자 추가 대화 상자의 \* 유형 \* 드롭다운 목록에서 \* 데이터베이스 사용자 \* 를 선택합니다.
4. 데이터베이스 사용자의 이름과 암호를 입력합니다.
5. 역할 \* 드롭다운 목록에서 적절한 역할을 선택합니다.

만약...	이 역할을 선택하십시오
Unified Manager와 워크플로우 자동화 연결	통합 스키마
보고 및 기타 데이터베이스 보기에 액세스	보고서 스키마

6. 추가 \* 를 클릭합니다.

## 사용자 설정 편집

각 사용자에게 지정된 전자 메일 주소 및 역할과 같은 사용자 설정을 편집할 수 있습니다. 예를 들어 스토리지 운영자 사용자의 역할을 변경하고 스토리지 관리자 권한을 사용자에게 할당할 수 있습니다.

- 필요한 것 \*

애플리케이션 관리자 역할이 있어야 합니다.

사용자에게 할당된 역할을 수정하면 다음 작업 중 하나가 발생할 때 변경 사항이 적용됩니다.

- 사용자가 로그아웃한 후 Unified Manager에 다시 로그인합니다.
- 24시간의 세션 시간 제한에 도달했습니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 사용자 \* 를 클릭합니다.
2. 사용자 페이지에서 설정을 편집할 사용자를 선택하고 \* 편집 \* 을 클릭합니다.
3. 사용자 편집 대화 상자에서 사용자에게 대해 지정된 적절한 설정을 편집합니다.
4. 저장 \* 을 클릭합니다.

## 사용자 보기

사용자 페이지에서 Unified Manager를 사용하여 스토리지 오브젝트 및 데이터를 관리하는 사용자 목록을 볼 수 있습니다. 사용자 이름, 사용자 유형, 전자 메일 주소, 사용자에게 할당된 역할 등 사용자에게 대한 세부 정보를 볼 수 있습니다.

- 필요한 것 \*

애플리케이션 관리자 역할이 있어야 합니다.



단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 사용자 \* 를 클릭합니다.

## 사용자 또는 그룹을 삭제하는 중입니다

특정 사용자가 Unified Manager에 액세스하지 못하도록 관리 서버 데이터베이스에서 사용자를 한 명 이상 삭제할 수 있습니다. 그룹의 모든 사용자가 더 이상 관리 서버에 액세스할 수 없도록 그룹을 삭제할 수도 있습니다.

- 필요한 것 \*
- 원격 그룹을 삭제하는 경우 원격 그룹의 사용자에게 할당된 이벤트를 다시 할당해야 합니다.

로컬 사용자 또는 원격 사용자를 삭제하는 경우 이러한 사용자에게 할당된 이벤트는 자동으로 할당되지 않습니다.

- 애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* 사용자 \* 를 클릭합니다.
2. 사용자 페이지에서 삭제할 사용자 또는 그룹을 선택한 다음 \* 삭제 \* 를 클릭합니다.
3. 예 \* 를 클릭하여 삭제를 확인합니다.

## RBAC란 무엇입니까

RBAC(역할 기반 액세스 제어)에서는 Active IQ Unified Manager 서버의 다양한 기능과 리소스에 액세스할 수 있는 사용자를 제어하는 기능을 제공합니다.

### 역할 기반 액세스 제어의 역할

역할 기반 액세스 제어(RBAC)를 통해 관리자는 역할을 정의하여 사용자 그룹을 관리할 수 있습니다. 선택한 관리자에게 특정 기능에 대한 액세스를 제한해야 하는 경우 해당 관리자에 대한 관리자 계정을 설정해야 합니다. 관리자가 볼 수 있는 정보와 관리자가 수행할 수 있는 작업을 제한하려면 사용자가 만든 관리자 계정에 역할을 적용해야 합니다.

관리 서버는 사용자 로그인 및 역할 권한에 RBAC를 사용합니다. 관리 사용자 액세스에 대한 관리 서버의 기본 설정을 변경하지 않은 경우 로그인할 필요가 없습니다.

특정 권한이 필요한 작업을 시작하면 관리 서버에 로그인하라는 메시지가 표시됩니다. 예를 들어 관리자 계정을 만들려면 응용 프로그램 관리자 계정 액세스 권한으로 로그인해야 합니다.

### 사용자 유형 정의

사용자 유형은 사용자가 보유하는 계정의 종류를 지정하며 원격 사용자, 원격 그룹, 로컬 사용자, 데이터베이스 사용자 및 유지 보수 사용자를 포함합니다. 이러한 각 유형에는 관리자 역할을 가진 사용자가 할당하는 고유한 역할이 있습니다.

Unified Manager 사용자 유형은 다음과 같습니다.

- \* 유지보수 사용자 \*

Unified Manager의 초기 구성 중에 생성됩니다. 그러면 유지 보수 사용자가 추가 사용자를 생성하고 역할을 할당합니다. 유지보수 사용자는 유지보수 콘솔에 액세스할 수 있는 유일한 사용자입니다. Unified Manager를 Red Hat Enterprise Linux 또는 CentOS 시스템에 설치하면 유지 관리 사용자에게 사용자 이름 "umadmin"이 지정됩니다.

- \* 로컬 사용자 \*

Unified Manager UI에 액세스하고 유지보수 사용자 또는 애플리케이션 관리자 역할을 가진 사용자가 제공하는 역할에 따라 기능을 수행합니다.

- \* 원격 그룹 \*

인증 서버에 저장된 자격 증명을 사용하여 Unified Manager UI에 액세스하는 사용자 그룹입니다. 이 계정의 이름은 인증 서버에 저장된 그룹의 이름과 일치해야 합니다. 원격 그룹 내의 모든 사용자는 개별 사용자 자격 증명을 사용하여 Unified Manager UI에 액세스할 수 있습니다. 원격 그룹은 할당된 역할에 따라 기능을 수행할 수 있습니다.

- \* 원격 사용자 \*

인증 서버에 저장된 자격 증명을 사용하여 Unified Manager UI에 액세스합니다. 원격 사용자는 유지보수 사용자 또는 애플리케이션 관리자 역할을 가진 사용자가 제공한 역할에 따라 기능을 수행합니다.

- \* 데이터베이스 사용자 \*

Unified Manager 데이터베이스의 데이터에 읽기 전용으로 액세스하고 Unified Manager 웹 인터페이스 또는 유지보수 콘솔에 액세스할 수 없으며 API 호출을 실행할 수 없습니다.

## 사용자 역할의 정의

유지보수 사용자 또는 애플리케이션 관리자는 모든 사용자에게 역할을 할당합니다. 각 역할에는 특정 권한이 포함됩니다. Unified Manager에서 수행할 수 있는 작업의 범위는 할당된 역할 및 역할에 포함된 권한에 따라 다릅니다.

Unified Manager에는 다음과 같은 사전 정의된 사용자 역할이 포함되어 있습니다.

- \* 연산자 \*

기록 및 용량 추세를 비롯하여 Unified Manager에서 수집한 스토리지 시스템 정보 및 기타 데이터를 확인합니다. 스토리지 운영자는 이 역할을 사용하여 이벤트에 대한 메모를 확인, 할당, 확인, 해결 및 추가할 수 있습니다.

- \* 스토리지 관리자 \*

Unified Manager 내에서 스토리지 관리 작업을 구성합니다. 스토리지 관리자는 이 역할을 통해 임계값을 구성하고 알림 및 기타 스토리지 관리 관련 옵션 및 정책을 생성할 수 있습니다.

- \* 응용 프로그램 관리자 \*

스토리지 관리와 관련 없는 설정을 구성합니다. 이 역할을 통해 사용자, 보안 인증서, 데이터베이스 액세스 및 인증을 포함한 관리 옵션을 관리할 수 있습니다. SMTP, 네트워킹 및 AutoSupport.



Linux 시스템에 Unified Manager를 설치하면 애플리케이션 관리자 역할을 가진 초기 사용자 이름이 자동으로 "umadmin"으로 지정됩니다.

• \* 통합 스키마 \*

WFA(Unified Manager)와 OnCommand Workflow Automation(Unified Manager)를 통합할 수 있도록 Unified Manager 데이터베이스 보기에 대한 읽기 전용 액세스를 지원합니다.

• \* 보고서 스키마 \*

이 역할은 Unified Manager 데이터베이스에서 직접 보고 및 기타 데이터베이스 뷰에 대한 읽기 전용 액세스를 지원합니다. 볼 수 있는 데이터베이스는 다음과 같습니다.

- NetApp\_모델\_뷰
- netapp\_performance
- ocum
- ocum\_report 를 참조하십시오
- ocum\_report\_bRT
- OPM
- 스케일로토르

## Unified Manager 사용자 역할 및 기능

할당된 사용자 역할에 따라 Unified Manager에서 수행할 수 있는 작업을 결정할 수 있습니다.

다음 표에는 각 사용자 역할이 수행할 수 있는 기능이 나와 있습니다.

기능	운영자	스토리지 관리자	응용 프로그램 관리자	통합 스키마	보고서 스키마
스토리지 시스템 정보를 봅니다	•	•	•	•	•
기록 및 용량 추세와 같은 다른 데이터를 봅니다	•	•	•	•	•
이벤트 보기, 할당 및 해결	•	•	•		
SVM 협회 및 리소스 풀과 같은 스토리지 서비스 객체를 확인합니다	•	•	•		

기능	운영자	스토리지 관리자	응용 프로그램 관리자	통합 스키마	보고서 스키마
임계값 정책을 봅니다	•	•	•		
SVM 협회 및 리소스 풀과 같은 스토리지 서비스 객체를 관리합니다		•	•		
알림을 정의합니다		•	•		
스토리지 관리 옵션을 관리합니다		•	•		
스토리지 관리 정책을 관리		•	•		
사용자 관리			•		
관리 옵션을 관리합니다			•		
임계값 정책을 정의합니다			•		
데이터베이스 액세스를 관리합니다			•		
WFA와의 통합을 관리하고 데이터베이스 뷰에 대한 액세스를 제공합니다				•	
보고서 예약 및 저장		•	•		
관리 조치로부터 "Fix it" 작업을 실행합니다		•	•		

기능	운영자	스토리지 관리자	응용 프로그램 관리자	통합 스키마	보고서 스키마
데이터베이스 보기에 대한 읽기 전용 액세스를 제공합니다					•

## SAML 인증 설정 관리

원격 인증 설정을 구성한 후에는 SAML(Security Assertion Markup Language) 인증을 설정하여 원격 사용자가 Unified Manager 웹 UI에 액세스하기 전에 IDP(Secure Identity Provider)에 의해 인증되도록 할 수 있습니다.

SAML 인증이 활성화된 후에는 원격 사용자만 Unified Manager 그래픽 사용자 인터페이스에 액세스할 수 있습니다. 로컬 사용자 및 유지 관리 사용자는 UI에 액세스할 수 없습니다. 이 구성은 유지보수 콘솔에 액세스하는 사용자에게 영향을 주지 않습니다.

### ID 공급자 요구 사항

ID 공급자(IDP)를 사용하여 모든 원격 사용자에게 대해 SAML 인증을 수행하도록 Unified Manager를 구성하는 경우 Unified Manager에 성공적으로 연결되도록 몇 가지 필수 구성 설정을 알고 있어야 합니다.

IDP 서버에 Unified Manager URI 및 메타데이터를 입력해야 합니다. 이 정보는 Unified Manager SAML 인증 페이지에서 복사할 수 있습니다. Unified Manager는 SAML(Security Assertion Markup Language) 표준의 서비스 공급자(SP)로 간주됩니다.

지원되는 암호화 표준

- AES(고급 암호화 표준): AES-128 및 AES-256
- 보안 해시 알고리즘(SHA): SHA-1 및 SHA-256

검증된 ID 공급자

- 시바볼레스
- ADFS(Active Directory Federation Services)

### ADFS 구성 요구 사항

- Unified Manager가 이 기반 당사자 신뢰 항목에 대한 ADFS SAML 응답을 구문 분석하는 데 필요한 세 가지 청구 규칙을 다음 순서로 정의해야 합니다.

청구 규칙	값
SAM-계정-이름	이름 ID입니다

청구 규칙	값
SAM-계정-이름	urn:OID: 0.9.2342.19200300.100.1.1
토큰 그룹 — 비정규화된 이름	urn:OID: 1.3.6.1.4.1.5923.1.5.1.1

- 인증 방법을 ""양식 인증""으로 설정해야 합니다. 그렇지 않을 경우 Unified Manager에서 로그아웃할 때 사용자에게 오류가 발생할 수 있습니다. 다음 단계를 수행하십시오.
  - a. ADFS 관리 콘솔을 엽니다.
  - b. 왼쪽 트리 뷰에서 Authentication Policies 폴더를 클릭합니다.
  - c. 오른쪽의 작업 에서 글로벌 기본 인증 정책 편집 을 클릭합니다.
  - d. 인트라넷 인증 방법을 기본값인 "Windows 인증" 대신 " 양식 인증"으로 설정합니다.
- 경우에 따라 Unified Manager 보안 인증서가 CA 서명되면 IDP를 통한 로그인이 거부됩니다. 이 문제를 해결하기 위한 두 가지 해결 방법이 있습니다.
  - 링크에 나와 있는 지침에 따라 연결된 CA 인증자에 대한 ADFS 서버의 해지 확인을 비활성화합니다.

"신뢰할 수 있는 당사자 신뢰에 따라 해지 확인을 비활성화합니다"

- CA 서버가 ADFS 서버 내에 상주하여 Unified Manager 서버 인증서 요청에 서명하도록 합니다.

#### 기타 구성 요구 사항

- Unified Manager 시간 차이는 5분으로 설정되어 있으므로 IDP 서버와 Unified Manager 서버 간의 시간 차이는 5분 이내이거나 인증이 실패합니다.

### SAML 인증을 사용하도록 설정합니다

SAML(Security Assertion Markup Language) 인증을 사용하면 원격 사용자가 Unified Manager 웹 UI에 액세스하기 전에 IDP(Secure Identity Provider)에서 인증을 받을 수 있습니다.

- 필요한 것 \*
- 원격 인증을 구성하고 성공적으로 수행되었는지 확인해야 합니다.
- 애플리케이션 관리자 역할을 사용하여 하나 이상의 원격 사용자 또는 원격 그룹을 만들어야 합니다.
- IDP(Identity Provider)는 Unified Manager에서 지원해야 하며 구성해야 합니다.
- IDP URL 및 메타데이터가 있어야 합니다.
- IDP 서버에 대한 액세스 권한이 있어야 합니다.

Unified Manager에서 SAML 인증을 설정한 후에는 IDP가 Unified Manager 서버 호스트 정보로 구성될 때까지 사용자가 그래픽 사용자 인터페이스에 액세스할 수 없습니다. 따라서 구성 프로세스를 시작하기 전에 연결의 두 부분을 모두 완료할 수 있도록 준비해야 합니다. IDP는 Unified Manager를 구성하기 전이나 후에 구성할 수 있습니다.

SAML 인증이 활성화된 후에는 원격 사용자만 Unified Manager 그래픽 사용자 인터페이스에 액세스할 수 있습니다. 로컬 사용자 및 유지 관리 사용자는 UI에 액세스할 수 없습니다. 이 구성은 유지보수 콘솔, Unified Manager 명령 또는

ZAPI에 액세스하는 사용자에게는 영향을 주지 않습니다.



이 페이지에서 SAML 구성을 완료하면 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* SAML 인증 \* 을 클릭합니다.
2. SAML 인증 활성화 \* 확인란을 선택합니다.

IDP 연결을 구성하는 데 필요한 필드가 표시됩니다.

3. Unified Manager 서버를 IDP 서버에 연결하는 데 필요한 IDP URI 및 IDP 메타데이터를 입력합니다.

IDP 서버에 Unified Manager 서버에서 직접 액세스할 수 있는 경우 IDP URI를 입력한 후 \* Fetch IDP Metadata \* 버튼을 클릭하여 IDP 메타데이터 필드를 자동으로 채울 수 있습니다.

4. Unified Manager 호스트 메타데이터 URI를 복사하거나 호스트 메타데이터를 XML 텍스트 파일에 저장합니다.

이 정보를 사용하여 IDP 서버를 구성할 수 있습니다.

5. 저장 \* 을 클릭합니다.

구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

6. 확인 및 로그아웃 \* 을 클릭하면 Unified Manager가 다시 시작됩니다.

다음에 권한이 있는 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 Unified Manager 로그인 페이지 대신 IDP 로그인 페이지에 자격 증명을 입력합니다.

아직 완료되지 않은 경우 IDP에 액세스하고 Unified Manager 서버 URI 및 메타데이터를 입력하여 구성을 완료합니다.



ID 공급자로 ADFS를 사용하는 경우 Unified Manager GUI는 ADFS 시간 제한을 적용하지 않으며 Unified Manager 세션 시간 제한에 도달할 때까지 계속 작동합니다. GUI 세션 시간 초과는 \* 일반 \* > \* 기능 설정 \* > \* 비활성 시간 초과 \* 를 클릭하여 변경할 수 있습니다.

## SAML 인증에 사용되는 ID 공급자를 변경합니다

Unified Manager에서 원격 사용자를 인증하는 데 사용하는 IDP(ID 공급자)를 변경할 수 있습니다.

- 필요한 것 \*
- IDP URL 및 메타데이터가 있어야 합니다.
- IDP에 대한 액세스 권한이 있어야 합니다.

Unified Manager를 구성하기 전이나 후에 새 IDP를 구성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* SAML 인증 \* 을 클릭합니다.
2. Unified Manager 서버를 IDP에 연결하는 데 필요한 새 IDP URI 및 IDP 메타데이터를 입력합니다.

IDP가 Unified Manager 서버에서 직접 액세스할 수 있는 경우 IDP URL을 입력한 후 \* Fetch IDP Metadata \* 버튼을 클릭하여 IDP 메타데이터 필드를 자동으로 채울 수 있습니다.

3. Unified Manager 메타데이터 URI를 복사하거나 메타데이터를 XML 텍스트 파일에 저장합니다.
4. 구성 저장 \* 을 클릭합니다.

구성을 변경할 것인지 확인하는 메시지 상자가 표시됩니다.

5. 확인 \* 을 클릭합니다.

새 IDP에 액세스하고 Unified Manager 서버 URI 및 메타데이터를 입력하여 구성을 완료합니다.

다음에 권한이 있는 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 이전 IDP 로그인 페이지 대신 새 IDP 로그인 페이지에 자격 증명을 입력합니다.

## Unified Manager 보안 인증서 변경 후 SAML 인증 설정을 업데이트하는 중입니다

Unified Manager 서버에 설치된 HTTPS 보안 인증서를 변경하려면 SAML 인증 구성 설정을 업데이트해야 합니다. 호스트 시스템의 이름을 바꾸거나 호스트 시스템에 새 IP 주소를 할당하거나 시스템에 대한 보안 인증서를 수동으로 변경하면 인증서가 업데이트됩니다.

보안 인증서가 변경되고 Unified Manager 서버가 다시 시작되면 SAML 인증이 작동하지 않고 사용자가 Unified Manager 그래픽 인터페이스에 액세스할 수 없습니다. 사용자 인터페이스에 대한 액세스를 다시 활성화하려면 IDP 서버 및 Unified Manager 서버 모두에서 SAML 인증 설정을 업데이트해야 합니다.

단계

1. 유지보수 콘솔에 로그인합니다.
2. 주 메뉴 \* 에서 \* SAML 인증 비활성화 \* 옵션에 대한 번호를 입력합니다.

SAML 인증을 비활성화하고 Unified Manager를 다시 시작할지 확인하는 메시지가 표시됩니다.

3. 업데이트된 FQDN 또는 IP 주소를 사용하여 Unified Manager 사용자 인터페이스를 시작하고, 업데이트된 서버 인증서를 브라우저에 적용하고, 유지 관리 사용자 자격 증명을 사용하여 로그인합니다.
4. 설정/인증 \* 페이지에서 \* SAML 인증 \* 탭을 선택하고 IDP 연결을 구성합니다.
5. Unified Manager 호스트 메타데이터 URI를 복사하거나 호스트 메타데이터를 XML 텍스트 파일에 저장합니다.
6. 저장 \* 을 클릭합니다.

구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

7. 확인 및 로그아웃 \* 을 클릭하면 Unified Manager가 다시 시작됩니다.
8. IDP 서버에 액세스한 다음 Unified Manager 서버 URI 및 메타데이터를 입력하여 구성을 완료합니다.



ID 공급자	구성 단계
고급	<ul style="list-style-type: none"> <li>a. ADFS 관리 GUI에서 기존 기반 당사자 신뢰 항목을 삭제합니다.</li> <li>b. 를 사용하여 새 신뢰할 수 있는 상대 트러스트 항목을 추가합니다 <code>saml_sp_metadata.xml</code> 업데이트된 Unified Manager 서버에서</li> <li>c. Unified Manager가 이 기반 당사자 신뢰 항목에 대한 ADFS SAML 응답을 구문 분석하는 데 필요한 세 가지 클레임 규칙을 정의합니다.</li> <li>d. ADFS Windows 서비스를 다시 시작합니다.</li> </ul>
시바볼레스	<ul style="list-style-type: none"> <li>a. Unified Manager 서버의 새 FQDN을 으로 업데이트합니다 <code>attribute-filter.xml</code> 및 <code>relying-party.xml</code> 파일.</li> <li>b. Apache Tomcat 웹 서버를 다시 시작하고 포트 8005가 온라인 상태가 될 때까지 기다립니다.</li> </ul>

9. Unified Manager에 로그인하고 IdP를 통해 SAML 인증이 예상대로 작동하는지 확인합니다.

## SAML 인증을 사용하지 않도록 설정합니다

Unified Manager 웹 UI에 로그인하기 전에 IDP(Secure Identity Provider)를 통해 원격 사용자 인증을 중지하려면 SAML 인증을 사용하지 않도록 설정할 수 있습니다. SAML 인증이 비활성화된 경우 Active Directory 또는 LDAP와 같이 구성된 디렉토리 서비스 공급자가 로그인 인증을 수행합니다.

SAML 인증을 비활성화하면 로컬 사용자 및 유지 관리 사용자가 구성된 원격 사용자 외에 그래픽 사용자 인터페이스에 액세스할 수 있습니다.

그래픽 사용자 인터페이스에 액세스할 수 없는 경우 Unified Manager 유지보수 콘솔을 사용하여 SAML 인증을 비활성화할 수도 있습니다.



SAML 인증이 비활성화된 후 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* SAML 인증 \* 을 클릭합니다.
2. SAML 인증 활성화 \* 확인란의 선택을 취소합니다.
3. 저장 \* 을 클릭합니다.

구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

4. 확인 및 로그아웃 \* 을 클릭하면 Unified Manager가 다시 시작됩니다.

다음 번에 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 IDP 로그인 페이지 대신 Unified Manager 로그인 페이지에 자격 증명을 입력합니다.

IDP에 액세스하고 Unified Manager 서버 URI 및 메타데이터를 삭제합니다.

유지 관리 콘솔에서 **SAML** 인증을 사용하지 않도록 설정합니다

Unified Manager GUI에 액세스할 수 없는 경우 유지보수 콘솔에서 SAML 인증을 비활성화해야 할 수 있습니다. 이는 구성이 잘못되거나 IDP에 액세스할 수 없는 경우에 발생할 수 있습니다.

- 필요한 것 \*

유지보수 사용자로서 유지보수 콘솔에 액세스할 수 있어야 합니다.

SAML 인증이 비활성화된 경우 Active Directory 또는 LDAP와 같이 구성된 디렉토리 서비스 공급자가 로그인 인증을 수행합니다. 로컬 사용자 및 유지 관리 사용자는 구성된 원격 사용자 외에도 그래픽 사용자 인터페이스에 액세스할 수 있습니다.

UI의 설정/인증 페이지에서 SAML 인증을 비활성화할 수도 있습니다.



SAML 인증이 비활성화된 후 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 유지보수 콘솔에 로그인합니다.
2. 주 메뉴 \* 에서 \* SAML 인증 비활성화 \* 옵션에 대한 번호를 입력합니다.

SAML 인증을 비활성화하고 Unified Manager를 다시 시작할지 확인하는 메시지가 표시됩니다.

3. y \* 를 입력한 다음 Enter 키를 누르면 Unified Manager가 다시 시작됩니다.

다음 번에 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 IDP 로그인 페이지 대신 Unified Manager 로그인 페이지에 자격 증명을 입력합니다.

필요한 경우 IDP에 액세스하고 Unified Manager 서버 URL 및 메타데이터를 삭제합니다.

## SAML 인증 페이지

SAML 인증 페이지를 사용하면 Unified Manager 웹 UI에 로그인하기 전에 IdP(Secure Identity Provider)를 통해 SAML을 사용하여 원격 사용자를 인증하도록 Unified Manager를 구성할 수 있습니다.

- SAML 구성을 생성하거나 수정하려면 애플리케이션 관리자 역할이 있어야 합니다.
- 원격 인증을 구성해야 합니다.
- 하나 이상의 원격 사용자 또는 원격 그룹을 구성해야 합니다.

원격 인증 및 원격 사용자를 구성한 후 SAML 인증 활성화 확인란을 선택하여 보안 ID 공급자를 사용하여 인증을 활성화할 수 있습니다.

- \* IDP URI \*

Unified Manager 서버에서 IDP에 액세스하기 위한 URI입니다. URI의 예는 다음과 같습니다.

ADFS 예제 URI:

`https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml`

Shibboleth 예제 URI:

`https://centos7.ntap2016.local/idp/shibboleth`

- \* IDP 메타데이터 \*

XML 형식의 IDP 메타데이터

Unified Manager 서버에서 IDP URL에 액세스할 수 있는 경우 \* Fetch IDP Metadata \* 버튼을 클릭하여 이 필드를 채울 수 있습니다.

- \* 호스트 시스템(FQDN) \*

설치 중에 정의된 Unified Manager 호스트 시스템의 FQDN입니다. 필요한 경우 이 값을 변경할 수 있습니다.

- \* 호스트 URI \*

IDP에서 Unified Manager 호스트 시스템에 액세스하기 위한 URI입니다.

- \* 호스트 메타데이터 \*

XML 형식의 호스트 시스템 메타데이터

## 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 옆에는 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 에 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.



연결 시간 초과 \* 값은 구성에 영향을 줄 수 있습니다. 설정에 정의된 값보다 응답하는 데 시간이 오래 걸리는 경우 연결 오류로 인해 구성 오류가 발생할 수 있습니다. 성공적으로 연결하려면 \* 연결 시간 초과 \* 값을 늘리고 구성을 다시 시도하십시오.

## 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 개체 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.

## 보안 인증서 관리

Unified Manager 서버에서 HTTPS를 구성하여 보안 연결을 통해 클러스터를 모니터링하고 관리할 수 있습니다.

### HTTPS 보안 인증서 보기

HTTPS 인증서 세부 정보를 브라우저에서 검색된 인증서와 비교하여 브라우저가 Unified Manager에 암호화된 연결을 가로채 가로채지 않도록 할 수 있습니다.

- 필요한 것 \*

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

인증서를 보면 다시 생성된 인증서의 내용을 확인하거나 Unified Manager에 액세스할 수 있는 주체 대체 이름(SAN)을 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* HTTPS 인증서 \* 를 클릭합니다.

HTTPS 인증서는 페이지 맨 위에 표시됩니다

HTTPS 인증서 페이지에 표시된 것보다 보안 인증서에 대한 자세한 정보를 보려면 브라우저에서 연결 인증서를 볼 수 있습니다.

### HTTPS 인증서 서명 요청을 다운로드하는 중입니다

서명할 인증 기관에 파일을 제공할 수 있도록 현재 HTTPS 보안 인증서에 대한 인증 서명 요청을 다운로드할 수 있습니다. CA 서명 인증서는 끼어들기 공격을 방지하고 자체 서명된 인증서보다 향상된 보안 보호를 제공합니다.

- 필요한 것 \*

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* HTTPS 인증서 \* 를 클릭합니다.
2. HTTPS 인증서 서명 요청 다운로드 \* 를 클릭합니다.
3. 를 저장합니다 <hostname>.csr 파일.

서명하도록 인증 기관에 파일을 제공한 다음 서명된 인증서를 설치할 수 있습니다.

## 서명되고 반환된 **HTTPS** 인증서를 설치하는 중입니다

인증 기관이 서명하여 반환한 후에 보안 인증서를 업로드 및 설치할 수 있습니다. 업로드 및 설치하는 파일은 자체 서명된 기존 인증서의 서명된 버전이어야 합니다. CA 서명 인증서는 끼어들기 공격을 방지하고 자체 서명된 인증서보다 더 나은 보안 보호를 제공합니다.

- 필요한 것 \*

다음 작업을 완료해야 합니다.

- 인증서 서명 요청 파일을 다운로드하고 인증 기관에서 서명했습니다
- 인증서 체인을 PEM 형식으로 저장했습니다
- 중간 인증서를 비롯하여 Unified Manager 서버 인증서에서 루트 서명 인증서까지 체인에 있는 모든 인증서가 포함됩니다

애플리케이션 관리자 역할이 있어야 합니다.



CSR이 생성된 인증서의 유효 기간이 397일 이상인 경우 CA가 인증서를 서명 및 반환하기 전에 유효 기간을 397일로 줄입니다

단계

1. 왼쪽 탐색 창에서 \* 일반 \* > \* HTTPS 인증서 \* 를 클릭합니다.
2. HTTPS 인증서 설치 \* 를 클릭합니다.
3. 표시되는 대화 상자에서 \* 파일 선택... \* 을 클릭하여 업로드할 파일을 찾습니다.
4. 파일을 선택한 다음 \* 설치 \* 를 클릭하여 파일을 설치합니다.

자세한 내용은 을 참조하십시오 "[외부 도구를 사용하여 생성된 HTTPS 인증서 설치](#)".

인증서 체인의 예

다음 예제에서는 인증서 체인 파일이 표시되는 방법을 보여 줍니다.

```

-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----

```

## 외부 도구를 사용하여 생성된 **HTTPS** 인증서 설치

자체 서명 또는 CA 서명된 인증서를 설치할 수 있으며 OpenSSL, BoringSSL, LetsEncrypt와 같은 외부 도구를 사용하여 생성할 수 있습니다.

이러한 인증서는 외부에서 생성된 공개-개인 키 쌍이므로 인증서 체인과 함께 개인 키를 로드해야 합니다. 허용된 키 쌍 알고리즘은 "RSA"와 "EC"입니다. HTTPS 인증서 설치 \* 옵션은 일반 섹션의 HTTPS 인증서 페이지에서 사용할 수 있습니다. 업로드하는 파일은 다음과 같은 입력 형식이어야 합니다.

1. Active IQ Unified Manager 호스트에 속한 서버의 개인 키입니다
2. 개인 키와 일치하는 서버의 인증서입니다
3. 위의 인증서에 서명하는 데 사용되는 루트까지 CA의 인증서가 반대입니다

**EC** 키 쌍을 사용하여 인증서를 로드하는 형식입니다

허용되는 곡선은 프리메256v1, 에코384r1입니다. 외부에서 생성된 EC 쌍이 있는 인증서 샘플:

```

-----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----

```

```

-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----

```

**RSA** 키 쌍을 사용하여 인증서를 로드하는 형식입니다

호스트 인증서에 속하는 RSA 키 쌍에 허용되는 키 크기는 2048, 3072 및 4096입니다. 외부에서 생성된 \* RSA 키 쌍이 포함된 인증서 \*:

```

-----BEGIN RSA PRIVATE KEY-----
<RSA private key of Server>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----

```

인증서가 업로드되면 Active IQ Unified Manager 인스턴스를 다시 시작하여 변경 내용을 적용해야 합니다.

외부에서 생성된 인증서를 업로드하는 동안 확인합니다

시스템은 외부 툴을 사용하여 생성된 인증서를 업로드하는 동안 검사를 수행합니다. 확인 중 하나라도 실패하면 인증서가 거부됩니다. 또한 제품 내에서 CSR에서 생성된 인증서 및 외부 도구를 사용하여 생성된 인증서에 대한 유효성 검사가 포함되어 있습니다.

- 입력의 개인 키는 입력의 호스트 인증서에 대해 유효성이 검사됩니다.
- 호스트 인증서의 CN(일반 이름)이 호스트의 FQDN에 대해 확인됩니다.

- 호스트 인증서의 CN(일반 이름)은 비어 있거나 비어 있어서는 안 되며 localhost로 설정해서는 안 됩니다.
- 유효 시작 날짜는 미래일 수 없으며 인증서의 유효 기간이 과거일 수 없습니다.
- 중간 CA 또는 CA가 있는 경우 인증서의 유효 시작 날짜는 미래일 수 없으며 유효 기간 만료 날짜는 과거일 수 없습니다.



입력의 개인 키는 암호화해서는 안 됩니다. 암호화된 개인 키가 있으면 시스템에서 거부됩니다.

#### 예 1

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

#### 예 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

#### 예 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

### 인증서 관리에 대한 페이지 설명입니다

HTTPS 인증서 페이지를 사용하여 현재 보안 인증서를 보고 새 HTTPS 인증서를 생성할 수 있습니다.

#### HTTPS 인증서 페이지

HTTPS 인증서 페이지에서는 현재 보안 인증서를 보거나, 인증서 서명 요청을 다운로드하거나, 자체 서명된 새 HTTPS 인증서를 생성하거나, 새 HTTPS 인증서를 설치할 수 있습니다.

자체 서명된 새 HTTPS 인증서를 생성하지 않은 경우 이 페이지에 나타나는 인증서는 설치 중에 생성된 인증서입니다.

#### 명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- \* HTTPS 인증서 서명 요청 다운로드 \*

현재 설치된 HTTPS 인증서에 대한 인증 요청을 다운로드합니다. 브라우저에서 <hostname>.csr 파일을 저장하라는 메시지를 표시하면 서명할 인증 기관에 파일을 제공할 수 있습니다.

- \* HTTPS 인증서 설치 \*

인증 기관이 서명하여 반환한 후에 보안 인증서를 업로드 및 설치할 수 있습니다. 관리 서버를 다시 시작한 후 새 인증서가 적용됩니다.

- \* HTTPS 인증서 재생성 \*

현재 보안 인증서를 대체하는 자체 서명된 새 HTTPS 인증서를 생성할 수 있습니다. 새 인증서는 Unified Manager를 다시 시작한 후에 적용됩니다.

### HTTPS 인증서 재생성 대화 상자

HTTPS 인증서 다시 생성 대화 상자에서는 보안 정보를 사용자 지정한 다음 해당 정보로 새 HTTPS 인증서를 생성할 수 있습니다.

현재 인증서 정보가 이 페이지에 나타납니다.

""현재 인증서 특성을 사용하여 재생성" 및 ""현재 인증서 특성 업데이트" 선택 항목을 사용하면 현재 정보로 인증서를 다시 생성하거나 새 정보로 인증서를 생성할 수 있습니다.

- \* 일반 이름 \*

필수 요소입니다. 보안하려는 FQDN(정규화된 도메인 이름)입니다.

Unified Manager 고가용성 구성에서 가상 IP 주소를 사용합니다.

- \* 이메일 \*

선택 사항. 조직에 연락할 이메일 주소. 일반적으로 인증서 관리자 또는 IT 부서의 이메일 주소입니다.

- \* 회사 \*

선택 사항. 일반적으로 회사의 통합 이름입니다.

- \* 부서 \*

선택 사항. 회사의 부서 이름입니다.

- \* 시 \*

선택 사항. 회사의 도시 위치입니다.

- \* 시/도 \*

선택 사항. 회사의 시/도 위치(약어로 표시되지 않음)입니다.

- \* 국가 \*

선택 사항. 회사의 국가 위치입니다. 이 코드는 일반적으로 해당 국가의 2자리 ISO 코드입니다.

- \* 대체 이름 \*

필수 요소입니다. 기존 localhost 또는 기타 네트워크 주소 외에 이 서버에 액세스하는 데 사용할 수 있는 추가, 비 기본 도메인 이름입니다. 각 대체 이름을 심표로 구분합니다.

인증서의 대체 이름 필드에서 로컬 식별 정보를 제거하려면 "로컬 식별 정보 제외(예: localhost)" 확인란을 선택합니다. 이 확인란을 선택하면 필드에 입력한 항목만 대체 이름 필드에 사용됩니다. 공백으로 두면 결과 인증서에 대체 이름 필드가 전혀 없습니다.

- \* 키 크기(키 알고리즘: RSA) \*

키 알고리즘은 RSA로 설정됩니다. 2048, 3072 또는 4096비트의 키 크기 중 하나를 선택할 수 있습니다. 기본 키 크기는 2048비트로 설정됩니다.

- \* 유효 기간 \*

기본 유효 기간은 397일입니다. 이전 버전에서 업그레이드한 경우 이전 인증서 유효성이 변경되지 않은 상태로 표시될 수 있습니다.

자세한 내용은 [을 참조하십시오 "HTTPS 인증서를 생성하는 중입니다"](#).



## 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.