Active IQ Unified Manager 구성

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/active-iq-unified-manager-918/config/concept_configure_unified_manager.html on November 13, 2026. Always check docs.netapp.com for the latest.

목차

Active IQ Unified Manager 구성 . . . 1
- Active IQ Unified Manager 구성에 대해 알아보기 . . . 1
- Active IQ Unified Manager의 구성 순서에 대해 알아보기 . . . 1
- Active IQ Unified Manager에서 웹 UI에 액세스합니다 . . . 1
- Active IQ Unified Manager 웹 UI의 초기 설정을 수행하십시오. . . . 2
- Active IQ Unified Manager에 클러스터 추가 . . . 4
- 알림 설정 . . . 6
  - Active IQ Unified Manager에서 알림 알림을 보내도록 구성합니다. . . . 6
  - Active IQ Unified Manager에서 이벤트 알림 설정 구성 . . . 7
  - Active IQ Unified Manager에서 원격 인증 활성화 . . . 8
  - Active IQ Unified Manager의 원격 인증에서 중첩 그룹 비활성화 . . . 9
  - Active IQ Unified Manager에서 인증 서비스 설정 . . . 9
  - Active IQ Unified Manager에 인증 서버 추가 . . . 10
  - Active IQ Unified Manager에서 인증 서버 구성 테스트 . . . 11
  - Active IQ Unified Manager에서 알림 추가 . . . 12
- Active IQ Unified Manager에서 로컬 사용자 암호 변경 . . . 14
- Active IQ Unified Manager에서 세션 비활성 시간 초과 설정 . . . 14
- Active IQ Unified Manager에서 CLI를 사용하여 세션 시간 초과 설정 . . . 15
- Unified Manager 호스트 이름 변경 . . . 15
  - Active IQ Unified Manager 가상 어플라이언스 호스트 이름 변경 . . . 15
  - Active IQ Unified Manager에서 HTTPS 보안 인증서 생성 . . . 16
  - Active IQ Unified Manager 가상 머신을 다시 시작합니다 . . . 17
  - Linux 시스템에서 Active IQ Unified Manager 호스트 이름 변경 . . . 18
- Active IQ Unified Manager에서 정책 기반 스토리지 관리 활성화 및 비활성화 . . . 19

Active IQ Unified Manager 구성

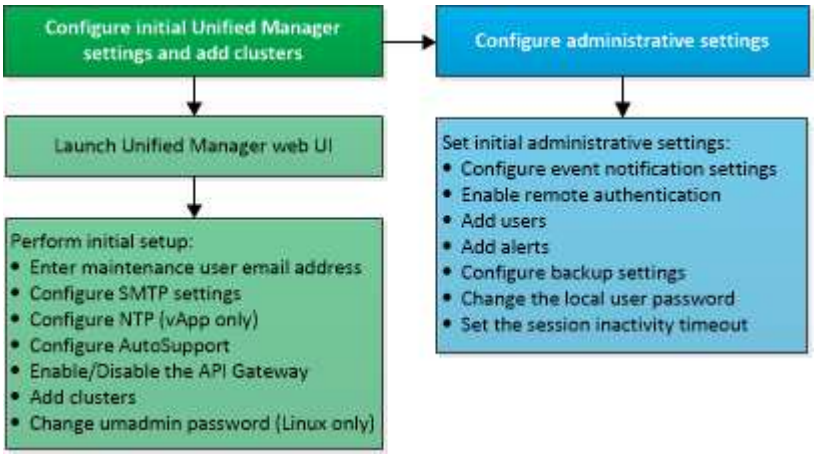
Active IQ Unified Manager 구성에 대해 알아보기

Active IQ Unified Manager(이전 명칭: OnCommand Unified Manager)를 설치한 후에는 웹 UI에 액세스하기 위해 초기 설정(첫 사용 마법사라고도 함)을 완료해야 합니다. 그런 다음 클러스터 추가, 원격 인증 구성, 사용자 추가, 경고 추가 등 추가 구성 작업을 수행할 수 있습니다.

이 설명서에 설명된 절차 중 일부는 Unified Manager 인스턴스의 초기 설정을 완료하는 데 필수적입니다. 다른 절차는 새 인스턴스에 설정해 두면 유용한 권장 구성 설정이거나 ONTAP 시스템의 정기적인 모니터링을 시작하기 전에 알아두면 좋은 설정입니다.

Active IQ Unified Manager의 구성 순서에 대해 알아보기

구성 워크플로는 Unified Manager를 사용하기 전에 수행해야 하는 작업을 설명합니다.



Active IQ Unified Manager에서 웹 UI에 액세스합니다

Unified Manager를 설치한 후에는 웹 UI에 접속하여 Unified Manager를 설정하고 ONTAP 시스템 모니터링을 시작할 수 있습니다.

시작하기 전에

- 웹 UI에 처음 접속하는 경우 유지 관리 사용자(또는 Linux 설치의 경우 umadmin 사용자)로 로그인해야 합니다.
- 사용자가 정규화된 도메인 이름(FQDN)이나 IP 주소 대신 짧은 이름을 사용하여 Unified Manager에 액세스하도록 허용하려는 경우, 네트워크 구성에서 이 짧은 이름을 유효한 FQDN으로 확인해야 합니다.
- 서버가 자체 서명된 디지털 인증서를 사용하는 경우 브라우저에 해당 인증서가 신뢰할 수 없다는 경고가 표시될 수 있습니다. 위험을 인지하고 액세스를 계속하거나 서버 인증을 위해 인증 기관(CA)에서 서명한 디지털 인증서를 설치할 수 있습니다.

단계

1. 설치가 완료될 때 표시되는 URL을 사용하여 브라우저에서 Unified Manager 웹 UI를 시작하십시오. 해당 URL은 Unified Manager 서버의 IP 주소 또는 정규화된 도메인 이름(FQDN)입니다.

링크는 다음과 같은 형식입니다: `https://URL`.

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

> 한 시간 내에 웹 UI 로그인 시도가 세 번 연속 실패할 경우 시스템 접속이 차단되며, 시스템 관리자에게 문의해야 합니다. 이는 로컬 사용자에게만 적용됩니다.

Active IQ Unified Manager 웹 UI의 초기 설정을 수행하십시오.

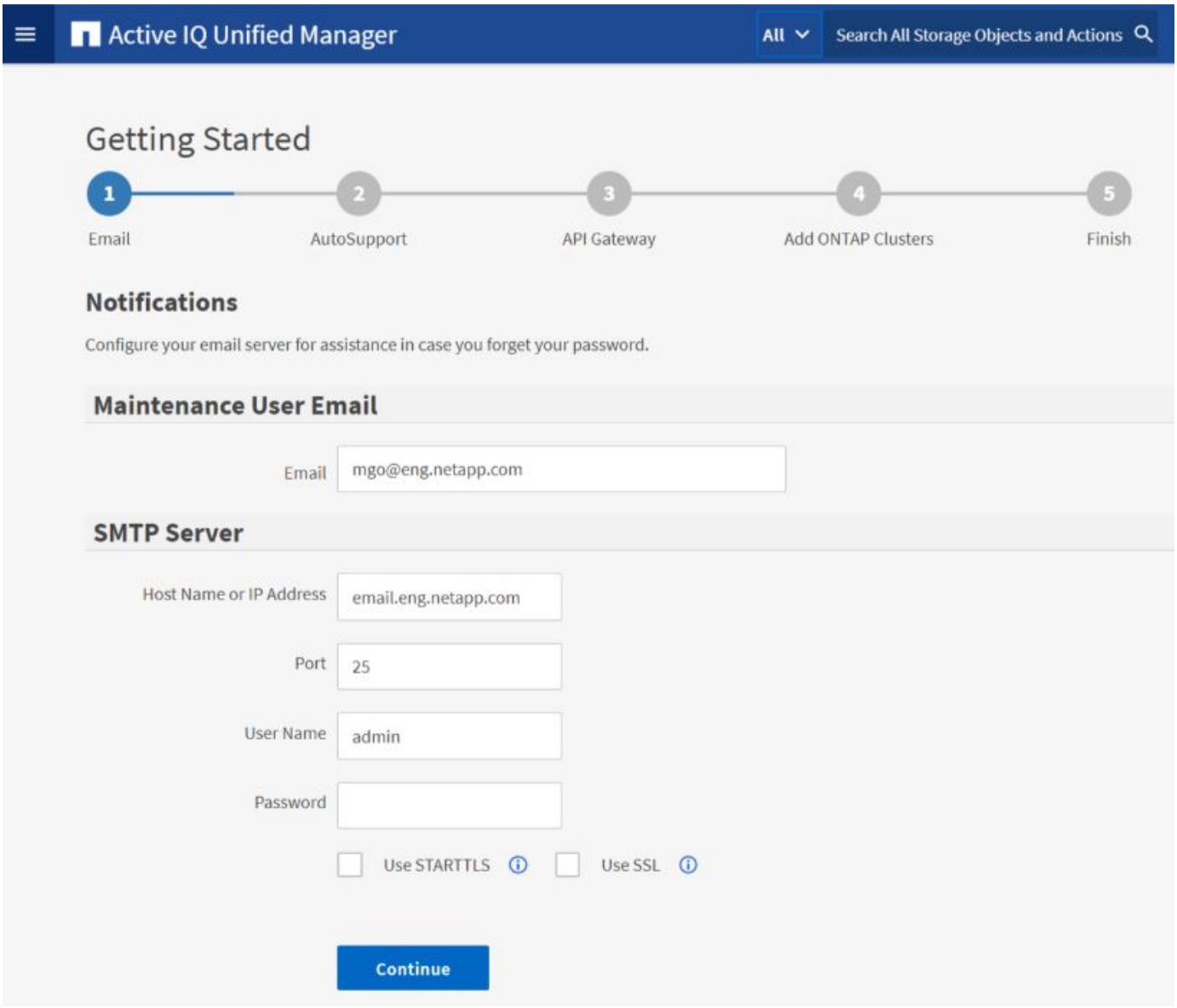
Unified Manager를 사용하려면 먼저 NTP 서버, 유지 관리 사용자 이메일 주소, SMTP 서버 호스트, ONTAP 클러스터 추가 등 초기 설정 옵션을 구성해야 합니다.

시작하기 전에

다음 작업을 수행해야 합니다:

- 설치 후 제공된 URL을 사용하여 Unified Manager 웹 UI를 실행했습니다
- 설치 중에 생성된 유지 관리 사용자 이름과 암호(Linux 설치의 경우 umadmin 사용자)를 사용하여 로그인했습니다.

Active IQ Unified ManagerGetting 시작하기 페이지는 웹 UI에 처음 접속할 때만 나타납니다. 아래 페이지는 VMware에 설치된 경우의 화면입니다.



나중에 이러한 옵션을 변경하려면 Unified Manager 왼쪽 탐색 창의 일반 옵션에서 원하는 옵션을 선택할 수 있습니다. 참고로 NTP 설정은 VMware 설치에만 해당하며, 나중에 Unified Manager 유지보수 콘솔을 사용하여 변경할 수 있습니다.

단계

1. Active IQ Unified Manager 초기 설정 페이지에서 유지 관리 사용자 이메일 주소, SMTP 서버 호스트 이름 및 추가 SMTP 옵션, 그리고 NTP 서버(VMware 설치에만 해당)를 입력합니다. 그런 다음 *계속*을 클릭합니다.

   STARTTLS 사용 또는 **SSL** 사용 옵션을 선택한 경우, 계속 버튼을 클릭하면 인증서 페이지가 표시됩니다. 인증서 세부 정보를 확인하고 인증서를 수락하여 웹 UI의 초기 설정을 계속 진행하십시오.

2. AutoSupport 페이지에서 *동의하고 계속*을 클릭하여 AutoSupport 메시지를 Unified Manager에서 NetAppActive IQ로 보낼 수 있도록 설정하십시오.

   웹 UI에서 일반 > **AutoSupport** 옵션을 사용하여 AutoSupport 콘텐츠를 전송하기 위한 인터넷 액세스를 제공하는 프록시를 지정하거나 AutoSupport를 비활성화할 수 있습니다.

3. Red Hat 시스템에서 umadmin 사용자 암호를 기본값인 “admin” 문자열에서 사용자 지정 문자열로 변경하십시오.
4. API 게이트웨이 설정 페이지에서 Unified Manager가 ONTAP REST API를 사용하여 모니터링할 ONTAP 클러스터를 관리할 수 있도록 하는 API 게이트웨이 기능을 사용할지 여부를 선택합니다. 그런 다음 *계속*을 클릭합니다.

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

5. Unified Manager에서 관리할 클러스터를 추가한 다음 *다음*을 클릭하십시오. 관리할 각 클러스터에 대해 호스트 이름 또는 클러스터 관리 IP 주소(IPv4 또는 IPv6)와 사용자 이름 및 암호 자격 증명이 있어야 합니다. 사용자는 “admin” 역할을 보유해야 합니다.

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

6. 요약 페이지에서 모든 설정이 올바른지 확인하고 *완료*를 클릭하십시오.

시작하기 페이지가 닫히고 Unified Manager 대시보드 페이지가 표시됩니다.

Active IQ Unified Manager에 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 등 클러스터 정보를 얻을 수 있는 기능이 포함됩니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 다음 정보를 준비해 두셔야 합니다:
  - Unified Manager는 온프레미스 ONTAP 클러스터, ONTAP Select, Cloud Volumes ONTAP를 지원합니다.
  - 호스트 이름 또는 클러스터 관리 IP 주소

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

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

  - 클러스터는 ONTAP 버전 9.1 이상의 소프트웨어를 실행해야 합니다.
  - ONTAP 관리자 사용자 이름 및 비밀번호

    이 계정에는 *admin* 역할이 있어야 하며 애플리케이션 액세스가 *ontapi*, *amqp*, *console* 및 _http_로 설정되어 있어야 합니다.

  - HTTPS 프로토콜을 사용하여 클러스터에 연결할 포트 번호(일반적으로 443번 포트)
  - 필요한 인증서를 보유하고 있습니다:

    SSL (HTTPS) 인증서: 이 인증서는 Unified Manager에서 소유합니다. Unified Manager를 새로 설치하면 기본적으로 자체 서명된 SSL (HTTPS) 인증서가 생성됩니다. NetApp은 보안 강화를 위해 CA에서 서명한 인증서로 업그레이드할 것을 권장합니다. 서버 인증서가 만료되면 인증서를 다시 생성하고 Unified Manager를

다시 시작하여 서비스에 새 인증서가 적용되도록 해야 합니다. SSL 인증서 다시 생성에 대한 자세한 내용은 "HTTPS 보안 인증서 생성"를 참조하십시오.

EMS 인증서: 이 인증서는 Unified Manager가 소유합니다. ONTAP에서 수신한 EMS 알림에 대한 인증 중에 사용됩니다.

상호 **TLS** 통신용 인증서: Unified Manager와 ONTAP 간의 상호 TLS 통신 중에 사용됩니다. 인증서 기반 인증은 ONTAP 버전에 따라 클러스터에 대해 활성화됩니다. 실행 중인 ONTAP 버전이 9.5 미만인 클러스터의 경우 인증서 기반 인증이 활성화되지 않습니다.

Unified Manager의 이전 버전을 업데이트하는 경우 클러스터에 대해 인증서 기반 인증이 자동으로 활성화되지 않습니다. 하지만 클러스터 세부 정보를 수정하고 저장하여 활성화할 수 있습니다. 인증서가 만료되면 새 인증서를 적용하기 위해 인증서를 다시 생성해야 합니다. 인증서 보기 및 다시 생성에 대한 자세한 내용은 "클러스터 편집"을(를) 참조하십시오.

- 웹 UI에서 클러스터를 추가할 수 있으며, 인증서 기반 인증이 자동으로 활성화됩니다.
- Unified Manager CLI를 통해 클러스터를 추가할 수 있지만, 기본적으로 인증서 기반 인증은 활성화되어 있지 않습니다. Unified Manager CLI를 사용하여 클러스터를 추가한 경우 Unified Manager UI를 사용하여 클러스터를 편집해야 합니다. Unified Manager CLI를 사용하여 클러스터를 추가하려면 "지원되는 Unified Manager CLI 명령"을(를) 참조하십시오.
- 클러스터에 인증서 기반 인증이 활성화된 경우, 서버에서 Unified Manager 백업을 수행하고 호스트 이름이나 IP 주소가 변경된 다른 Unified Manager 서버로 복원하면 클러스터 모니터링이 실패할 수 있습니다. 이러한 오류를 방지하려면 클러스터 세부 정보를 편집하고 저장하십시오. 클러스터 세부 정보 편집에 대한 자세한 내용은 "클러스터 편집"을(를) 참조하십시오.

+ 클러스터 인증서: 이 인증서는 ONTAP이 소유합니다. 만료된 인증서로는 Unified Manager에 클러스터를 추가할 수 없으며, 인증서가 이미 만료된 경우 클러스터를 추가하기 전에 인증서를 다시 생성해야 합니다. 인증서 생성에 대한 자세한 내용은 기술 자료(KB) 문서를 참조하십시오 "System Manager 사용자 인터페이스에서 ONTAP 자체 서명 인증서를 갱신하는 방법".

- Unified Manager 서버에 충분한 공간이 있어야 합니다. 데이터베이스 디렉터리의 공간이 90% 이상 사용된 경우 서버에 클러스터를 추가할 수 없습니다.

MetroCluster 구성의 경우, 로컬 클러스터와 원격 클러스터를 모두 추가해야 하며, 클러스터가 올바르게 구성되어 있어야 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, 포트 번호 등 필수 값을 지정합니다.

   클러스터 관리 IP 주소를 IPv6에서 IPv4로 또는 IPv4에서 IPv6로 변경할 수 있습니다. 새 IP 주소는 다음 모니터링 주기가 완료된 후 클러스터 그리드와 클러스터 구성 페이지에 반영됩니다.
4. *제출*을 클릭하십시오.
5. 호스트 인증 대화 상자에서 *인증서 보기*를 클릭하여 클러스터에 대한 인증서 정보를 확인합니다.
6. *예*를 클릭합니다.

클러스터 세부 정보를 저장하면 클러스터의 상호 TLS 통신에 사용되는 인증서를 확인할 수 있습니다.

인증서 기반 인증이 활성화되지 않은 경우 Unified Manager는 클러스터를 처음 추가할 때만 인증서를 확인합니다. Unified Manager는 ONTAP에 대한 각 API 호출에 대해 인증서를 확인하지 않습니다.

새 클러스터에 필요한 모든 객체가 검색되면 Unified Manager는 지난 15일간의 성능 기록 데이터를 수집하기 시작합니다. 이러한 통계는 데이터 연속성 수집 기능을 사용하여 수집됩니다. 이 기능을 통해 클러스터가 추가된 직후 2주 이상의 성능 정보를 확인할 수 있습니다. 데이터 연속성 수집 주기가 완료되면 기본적으로 5분마다 실시간 클러스터 성능 데이터가 수집됩니다.

15일간의 성능 데이터 수집은 CPU 사용량이 많으므로, 데이터 연속성 수집 폴링이 동시에 너무 많은 클러스터에서 실행되지 않도록 새 클러스터 추가를 단계적으로 진행하는 것이 좋습니다. 또한, 데이터 연속성 수집 기간 중에 Unified Manager를 재시작하면 수집이 중단되고 누락된 기간에 대한 성능 차트에 공백이 표시됩니다.

클러스터를 추가할 수 없다는 오류 메시지가 표시되면 두 시스템의 시계가 동기화되지 않았는지, Unified Manager HTTPS 인증서 시작 날짜가 클러스터의 날짜보다 늦은지 확인하십시오. NTP 또는 유사한 서비스를 사용하여 시계를 동기화해야 합니다.

관련 정보

"CA에서 서명하고 발급한 HTTPS 인증서 설치"

알림 설정

Active IQ Unified Manager에서 알림 알림을 보내도록 구성합니다**.**

환경에서 발생하는 이벤트에 대해 알려주는 알림을 보내도록 Unified Manager를 구성할 수 있습니다. 알림을 보내기 전에 몇 가지 다른 Unified Manager 옵션을 구성해야 합니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

Unified Manager를 배포하고 초기 구성을 완료한 후, 이벤트 수신을 기반으로 경고를 트리거하고 알림 이메일 또는 SNMP 트랩을 생성하도록 환경을 구성하는 것을 고려해야 합니다.

단계

1. "이벤트 알림 설정 구성".

   환경에서 특정 이벤트가 발생했을 때 경고 알림이 전송되도록 하려면 SMTP 서버를 구성하고 경고 알림을 발송할 이메일 주소를 제공해야 합니다. SNMP 트랩을 사용하려면 해당 옵션을 선택하고 필요한 정보를 제공할 수 있습니다.

2. "원격 인증 활성화".

   원격 LDAP 또는 Active Directory 사용자가 Unified Manager 인스턴스에 액세스하고 경고 알림을 수신할 수 있도록 하려면 원격 인증을 활성화해야 합니다.

3. "인증 서버 추가".

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

4. "사용자 추가".

   로컬 또는 원격 사용자를 여러 유형으로 추가하고 특정 역할을 할당할 수 있습니다. 알림을 생성할 때 알림을 받을 사용자를 지정합니다.

5. "알림 추가".

   알림 전송용 이메일 주소를 추가하고, 알림을 받을 사용자를 추가하고, 네트워크 설정을 구성하고, 환경에 필요한 SMTP 및 SNMP 옵션을 구성한 후에는 알림을 할당할 수 있습니다.

Active IQ Unified Manager에서 이벤트 알림 설정 구성

Unified Manager를 구성하여 이벤트가 발생하거나 사용자에게 이벤트가 할당될 때 경고 알림을 보낼 수 있습니다. 경고를 보내는 데 사용할 SMTP 서버를 구성할 수 있으며, 이메일이나 SNMP 트랩 등 다양한 알림 메커니즘을 설정할 수 있습니다.

시작하기 전에

다음 정보를 준비해 두셔야 합니다:

- 경고 알림이 전송되는 이메일 주소

  이메일 주소는 전송된 알림의 “From” 필드에 표시됩니다. 어떤 이유로든 이메일이 전달되지 않으면 이 이메일 주소가 배달 실패 메일의 수신자로도 사용됩니다.

- SMTP 서버 호스트 이름과 서버에 접속하기 위한 사용자 이름 및 비밀번호
- SNMP 트랩을 수신할 트랩 대상 호스트의 호스트 이름 또는 IP 주소와 함께 SNMP 버전, 아웃바운드 트랩 포트, 커뮤니티 및 기타 필요한 SNMP 구성 값

  여러 개의 트랩 대상을 지정하려면 각 호스트를 쉼표로 구분하십시오. 이 경우 버전 및 아웃바운드 트랩 포트 등 다른 모든 SNMP 설정은 목록에 있는 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 구성하십시오.

   참고:

   - 보내는 사람 주소가 "ActiveIQUnifiedManager@localhost.com"으로 미리 채워져 있는 경우, 모든 이메일 알림이 성공적으로 전달되도록 실제 사용 가능한 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** 사용 또는 **SSL** 사용 옵션을 선택한 경우, 저장 버튼을 클릭하면 인증서 페이지가 표시됩니다. 인증서 세부 정보를 확인하고 인증서를 승인하여 알림 설정을 저장하십시오.

인증서 세부 정보 보기 버튼을 클릭하여 인증서 세부 정보를 볼 수 있습니다. 기존 인증서가 만료된 경우 **STARTTLS** 사용 또는 **SSL** 사용 확인란의 선택을 해제하고 알림 설정을 저장한 다음, **STARTTLS** 사용 또는 **SSL** 사용 확인란을 다시 선택하여 새 인증서를 확인하십시오.

Active IQ Unified Manager에서 원격 인증 활성화

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

시작하기 전에

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) 등 로컬 LDAP 클라이언트를 비활성화해야 합니다.

Open LDAP 또는 Active Directory를 사용하여 원격 인증을 활성화할 수 있습니다. 원격 인증이 비활성화된 경우 원격 사용자는 Unified Manager에 액세스할 수 없습니다.

원격 인증은 LDAP 및 LDAPS(보안 LDAP)를 통해 지원됩니다. Unified Manager는 보안되지 않은 통신에는 기본 포트로 389를, 보안 통신에는 기본 포트로 636을 사용합니다.

사용자 인증에 사용되는 인증서는 X.509 형식을 준수해야 합니다.

단계

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

인증 유형의 경우...	다음 정보를 입력하세요...
Active Directory	• 다음 형식 중 하나로 된 인증 서버 관리자 이름: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (적절한 LDAP 표기법을 사용하여) • 관리자 암호 • 기본 고유 이름(적절한 LDAP 표기법 사용)
Open LDAP	• 바인드 고유 이름(적절한 LDAP 표기법 사용) • 바인드 비밀번호 • 기본 고유 이름

Active Directory 사용자 인증에 시간이 오래 걸리거나 시간 초과가 발생하는 경우, 인증 서버의 응답 속도가 느린 것이 원인일 수 있습니다. Unified Manager에서 중첩 그룹 지원을 비활성화하면 인증 시간을 단축할 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 테스트하십시오.
5. *저장*을 클릭합니다.

Active IQ Unified Manager의 원격 인증에서 중첩 그룹 비활성화

원격 인증이 활성화된 경우, 중첩 그룹 인증을 비활성화하여 그룹 구성원이 아닌 개별 사용자만 Unified Manager에 원격으로 인증할 수 있도록 할 수 있습니다. Active Directory 인증 응답 시간을 개선하려는 경우 중첩 그룹을 비활성화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 역할이 있어야 합니다.
- 중첩 그룹 비활성화는 Active Directory를 사용하는 경우에만 적용됩니다.

Unified Manager에서 중첩 그룹 지원을 비활성화하면 인증 시간이 단축될 수 있습니다. 중첩 그룹 지원이 비활성화된 상태에서 원격 그룹을 Unified Manager에 추가하면 개별 사용자는 Unified Manager에 인증하기 위해 해당 원격 그룹의 구성원이어야 합니다.

단계

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

Active IQ Unified Manager에서 인증 서비스 설정

인증 서비스를 사용하면 원격 사용자 또는 원격 그룹이 Unified Manager에 액세스하기 전에 인증 서버에서 인증을 받을 수 있습니다. Active Directory 또는 OpenLDAP 등 사전 정의된 인증 서비스를 사용하거나 자체 인증 메커니즘을 구성하여 사용자를 인증할 수 있습니다.

시작하기 전에

- 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 선택하십시오:

선택하시면...	그런 다음 이렇게 하십시오...
Active Directory	a. 관리자 이름과 비밀번호를 입력하세요. b. 인증 서버의 기본 고유 이름을 지정하십시오. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com+인 경우 기본 고유 이름은 *cn=ou,dc=domain,dc=com*입니다.
OpenLDAP	a. 바인딩 고유 이름과 바인딩 암호를 입력하십시오. b. 인증 서버의 기본 고유 이름을 지정하십시오. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com+인 경우 기본 고유 이름은 *cn=ou,dc=domain,dc=com*입니다.
기타	a. 바인딩 고유 이름과 바인딩 암호를 입력하십시오. b. 인증 서버의 기본 고유 이름을 지정하십시오. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com+인 경우 기본 고유 이름은 *cn=ou,dc=domain,dc=com*입니다. c. 인증 서버에서 지원하는 LDAP 프로토콜 버전을 지정하십시오. d. 사용자 이름, 그룹 멤버십, 사용자 그룹 및 멤버 속성을 입력하십시오.

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

3. *저장*을 클릭합니다.

Active IQ Unified Manager에 인증 서버 추가

관리 서버에 인증 서버를 추가하고 원격 인증을 활성화하면 인증 서버 내의 원격 사용자가 Unified Manager에 액세스할 수 있습니다.

시작하기 전에

- 다음 정보가 준비되어 있어야 합니다:
  - 인증 서버의 호스트 이름 또는 IP 주소
  - 인증 서버의 포트 번호
- 관리 서버가 인증 서버에서 원격 사용자 또는 그룹을 인증할 수 있도록 원격 인증을 활성화하고 인증 서비스를 구성해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

추가하려는 인증 서버가 고가용성(HA) 쌍(동일한 데이터베이스 사용)의 일부인 경우 파트너 인증 서버도 추가할 수 있습니다. 이렇게 하면 인증 서버 중 하나에 연결할 수 없는 경우에도 관리 서버가 파트너와 통신할 수 있습니다.

단계

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

원하신다면...	그런 다음 이렇게 하십시오...
활성화하십시오	a. 보안 연결 사용 옵션을 선택합니다. b. 인증 서버 영역에서 *추가*를 클릭합니다. c. 인증 서버 추가 대화 상자에서 서버의 인증 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다. d. 호스트 인증 대화 상자에서 인증서 보기를 클릭합니다. e. 인증서 보기 대화 상자에서 인증서 정보를 확인한 다음 *닫기*를 클릭합니다. f. 호스트 권한 부여 대화 상자에서 *예*를 클릭합니다. 보안 연결 인증 사용 옵션을 활성화하면 Unified Manager가 인증 서버와 통신하고 인증서를 표시합니다. Unified Manager는 보안 통신에 기본 포트 636을 사용하고, 일반 통신에는 포트 번호 389를 사용합니다.
비활성화하세요	a. 보안 연결 사용 옵션을 해제하십시오. b. 인증 서버 영역에서 *추가*를 클릭합니다. c. 인증 서버 추가 대화 상자에서 서버의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)와 포트 세부 정보를 지정합니다. d. *추가*를 클릭합니다.

추가하신 인증 서버가 서버 영역에 표시됩니다.

3. 추가한 인증 서버에서 사용자를 인증할 수 있는지 확인하기 위해 테스트 인증을 수행하십시오.

Active IQ Unified Manager에서 인증 서버 구성 테스트

관리 서버가 인증 서버와 통신할 수 있는지 확인하기 위해 인증 서버의 구성을 검증할 수 있습니다. 인증 서버에서 원격 사용자 또는 원격 그룹을 검색하고 구성된 설정을 사용하여 인증함으로써 구성을 검증할 수 있습니다.

시작하기 전에

- Unified Manager 서버가 원격 사용자 또는 원격 그룹을 인증할 수 있도록 원격 인증을 활성화하고 인증 서비스를 구성해야 합니다.
- 관리 서버가 원격 사용자 또는 원격 그룹을 이러한 서버에서 검색하고 인증할 수 있도록 인증 서버를 추가해야 합니다.

- 애플리케이션 관리자 역할이 있어야 합니다.

인증 서비스가 Active Directory로 설정되어 있고, 인증 서버의 기본 그룹에 속한 원격 사용자의 인증을 검증하는 경우, 인증 결과에 기본 그룹에 대한 정보가 표시되지 않습니다.

단계

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

   원격 그룹을 인증하는 경우 암호를 입력해서는 안 됩니다.

Active IQ Unified Manager에서 알림 추가

특정 이벤트가 생성될 때 알림을 받도록 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.

시작하기 전에

- Active IQ Unified Manager 서버가 이벤트 발생 시 이 설정을 사용하여 사용자에게 알림을 보낼 수 있도록 하려면 사용자 이메일 주소, SMTP 서버, SNMP 트랩 호스트 등 알림 설정을 구성해야 합니다.
- 알림을 발생시키려는 리소스와 이벤트, 그리고 알림을 받을 사용자의 사용자 이름 또는 이메일 주소를 알고 있어야 합니다.
- 이벤트에 따라 스크립트를 실행하려면 스크립트 페이지를 사용하여 Unified Manager에 스크립트를 추가해야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

여기 설명된 대로 알림 설정 페이지에서 알림을 생성하는 것 외에도 이벤트를 수신한 후 이벤트 세부 정보 페이지에서 직접 알림을 생성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 스토리지 관리 > *알림 설정*을 클릭합니다.
2. 알림 설정 페이지에서 *추가*를 클릭합니다.
3. 경고 추가 대화 상자에서 *이름*을 클릭하고 경고의 이름과 설명을 입력합니다.
4. *리소스*를 클릭하고 알림에 포함하거나 제외할 리소스를 선택하십시오.

   Name contains 필드에 텍스트 문자열을 지정하여 리소스 그룹을 선택하는 필터를 설정할 수 있습니다. 지정한 텍스트 문자열을 기준으로 사용 가능한 리소스 목록에는 필터 규칙과 일치하는 리소스만 표시됩니다. 지정하는 텍스트 문자열은 대소문자를 구분합니다.

   리소스가 지정한 포함 규칙과 제외 규칙을 모두 충족하는 경우 제외 규칙이 포함 규칙보다 우선 적용되며, 제외된 리소스와 관련된 이벤트에 대해서는 알림이 생성되지 않습니다.

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

두 개 이상의 이벤트를 선택하려면 선택하는 동안 Ctrl 키를 누르십시오.

6. *작업*을 클릭하고 알림을 받을 사용자를 선택하고, 알림 빈도를 선택하고, SNMP 트랩을 트랩 수신자에게 보낼지 여부를 선택하고, 경고가 생성될 때 실행할 스크립트를 할당합니다.

   사용자에게 지정된 이메일 주소를 수정하고 알림을 다시 열어 편집하면, 수정된 이메일 주소가 이전에 선택된 사용자에게 더 이상 매핑되지 않기 때문에 이름 필드가 비어 있게 표시됩니다. 또한, 사용자 페이지에서 선택한 사용자의 이메일 주소를 수정하더라도, 수정된 이메일 주소가 선택된 사용자에게는 업데이트되지 않습니다.

   SNMP 트랩을 통해 사용자에게 알림을 보내도록 선택할 수도 있습니다.

7. *저장*을 클릭합니다.

알림 추가 예시

이 예시는 다음 요구 사항을 충족하는 알림을 생성하는 방법을 보여줍니다:

- 알림 이름: HealthTest
- 리소스: 이름에 "`abc`"가 포함된 모든 볼륨을 포함하고, 이름에 "`xyz`"가 포함된 모든 볼륨을 제외합니다.
- 이벤트: 모든 중요 상태 이벤트를 포함합니다
- 작업: "sample@domain.com", “Test” 스크립트가 포함되며, 사용자는 15분마다 알림을 받아야 합니다

경고 추가 대화 상자에서 다음 단계를 수행하십시오:

단계

1. 이름*을 클릭하고 *알림 이름 필드에 *HealthTest*를 입력합니다.
2. *리소스*를 클릭하고 포함 탭의 드롭다운 목록에서 *볼륨*을 선택합니다.
   a. 이름에 포함된 항목 필드에 *abc*를 입력하면 이름에 "`abc`"가 포함된 볼륨이 표시됩니다.
   b. Available Resources 영역에서 **<<All Volumes whose name contains 'abc'>>** 를 선택하고 Selected Resources 영역으로 이동합니다.
   c. 제외*를 클릭하고 *이름에 포함된 내용 필드에 *xyz*를 입력한 다음 *추가*를 클릭합니다.
3. *이벤트*를 클릭하고 이벤트 심각도 필드에서 *심각*을 선택합니다.
4. 일치하는 이벤트 영역에서 *모든 중요 이벤트*를 선택하고 선택된 이벤트 영역으로 이동합니다.
5. *작업*을 클릭하고 이 사용자에게 알림 필드에 *sample@domain.com*을 입력합니다.
6. 15분마다 사용자에게 알림을 보내려면 *15분마다 알림*을 선택하세요.

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

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

Active IQ Unified Manager에서 로컬 사용자 암호 변경

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

시작하기 전에

로컬 사용자로 로그인해야 합니다.

이 단계에서는 유지 관리 사용자 및 원격 사용자의 암호를 변경할 수 없습니다. 원격 사용자 암호를 변경하려면 암호 관리자에게 문의하십시오. 유지 관리 사용자 암호를 변경하려면 "유지보수 콘솔 사용"을(를) 참조하십시오.

단계

1. Unified Manager에 로그인하십시오.
2. 상단 메뉴 모음에서 사용자 아이콘을 클릭한 다음 *비밀번호 변경*을 클릭하세요.

   원격 사용자의 경우 비밀번호 변경 옵션이 표시되지 않습니다.

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

Unified Manager가 고가용성 구성으로 구성된 경우, 설정의 두 번째 노드에서 암호를 변경해야 합니다. 두 인스턴스는 동일한 암호를 사용해야 합니다.

Active IQ Unified Manager에서 세션 비활성 시간 초과 설정

Unified Manager의 비활성 시간 제한 값을 지정하여 일정 시간 동안 활동이 없으면 세션이 자동으로 종료되도록 할 수 있습니다. 기본적으로 시간 제한은 4,320분(72시간)으로 설정되어 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이 설정은 로그인한 모든 사용자 세션에 적용됩니다.

Security Assertion Markup Language (SAML) 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 제한을 지정하십시오:

원하신다면...	그런 다음 이렇게 하십시오...
세션이 자동으로 종료되지 않도록 타임아웃을 설정하지 마십시오.	• Inactivity Timeout * 패널에서 슬라이더 버튼을 왼쪽으로 이동(끄기)하고 * Apply * 를 클릭합니다.
시간 초과 값을 특정 분 수로 설정하십시오.	비활성 시간 제한 패널에서 슬라이더 버튼을 오른쪽(켜짐)으로 이동하고 비활성 시간 제한 값을 분 단위로 지정한 다음 *적용*을 클릭합니다.

Active IQ Unified Manager에서 CLI를 사용하여 세션 시간 초과 설정

CLI를 사용하여 Unified Manager의 최대 세션 시간 초과 값을 설정하여 일정 시간이 지나면 세션이 자동으로 종료되도록 할 수 있습니다. 기본적으로 세션 시간 초과는 최대값인 4,320분(72시간)으로 설정되어 있습니다. 즉, Unified Manager에 로그인하여 활발하게 사용 중이더라도 72시간 후에는 세션이 자동으로 종료됩니다.

이 작업 정보

애플리케이션 관리자 역할이 있어야 합니다.

세션 시간 초과 설정은 로그인한 모든 사용자 세션에 적용됩니다.

단계

1. `um cli login` 명령을 입력하여 Unified Manager CLI에 로그인하십시오. 인증을 위해 유효한 사용자 이름과 암호를 사용하십시오.
2. 세션 시간 초과 값을 수정하려면 `um option set max.session.timeout.value=<in mins>` 명령을 입력하십시오.

Unified Manager 호스트 이름 변경

Active IQ Unified Manager 가상 어플라이언스 호스트 이름 변경

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

시작하기 전에

이러한 작업을 수행하려면 Unified Manager에 유지 관리 사용자 계정으로 로그인했거나 애플리케이션 관리자 역할이 할당되어 있어야 합니다.

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

호스트 이름이 어떻게 할당되었는지와 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 변경하더라도 새 인증서를 생성할 필요가 없습니다. 그러나 인증서의 호스트 이름이 실제 호스트 이름과 일치하도록 인증서를 업데이트하는 것이 모범 사례입니다.

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

새 인증서는 Unified Manager 가상 머신을 다시 시작해야 적용됩니다.

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 시작하십시오

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

Active IQ Unified Manager에서 HTTPS 보안 인증서 생성

Active IQ Unified Manager를 처음 설치할 때 기본 HTTPS 인증서가 설치됩니다. 기존 인증서를 대체할 새 HTTPS 보안 인증서를 생성할 수도 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

고유 이름(DN) 값을 더 좋게 설정하거나, 키 크기를 늘리거나, 만료 기간을 더 길게 설정하거나, 현재 인증서가 만료된 경우 등 인증서를 다시 생성해야 하는 이유는 여러 가지가 있을 수 있습니다.

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

단계

1. 왼쪽 탐색 창에서 일반 > *HTTPS 인증서*를 클릭합니다.
2. *HTTPS 인증서 재생성*을 클릭합니다.

   HTTPS 인증서 재생성 대화 상자가 표시됩니다.

3. 인증서를 생성하는 방법에 따라 다음 옵션 중 하나를 선택하십시오:

원하신다면...	이렇게 하세요...
현재 값으로 인증서를 다시 생성하십시오	현재 인증서 속성을 사용하여 재생성 옵션을 클릭하십시오.

원하신다면...	이렇게 하세요...
다른 값을 사용하여 인증서를 생성합니다	현재 인증서 속성 업데이트 옵션을 클릭하십시오. 새 값을 입력하지 않으면 Common Name 및 Alternative Names 필드는 기존 인증서의 값을 사용합니다. "`Common Name`"은 호스트의 FQDN으로 설정해야 합니다. 다른 필드는 값이 필요하지 않지만, 해당 값이 인증서에 채워지기를 원하는 경우 EMAIL, COMPANY, DEPARTMENT, City, State, Country 등에 값을 입력할 수 있습니다. 또한 사용 가능한 KEY SIZE(키 알고리즘은 "`RSA`"입니다.) 및 VALIDITY PERIOD를 선택할 수 있습니다. • 키 크기에 허용되는 값은 2048, 3072 및 `4096`입니다. • 유효 기간은 최소 1일부터 최대 36500일까지입니다. 36500일의 유효기간이 허용되더라도 397일 또는 13개월 이하의 유효기간을 사용하는 것이 좋습니다. 유효기간을 397일 이상으로 선택하고 이 인증서에 대한 CSR을 내보내어 잘 알려진 CA에서 서명을 받으려는 경우, CA에서 반환하는 서명된 인증서의 유효기간이 397일로 단축되기 때문입니다. • 인증서의 대체 이름 필드에서 로컬 식별 정보를 제거하려면 “로컬 식별 정보 제외(예: localhost)” 확인란을 선택할 수 있습니다. 이 확인란을 선택하면 필드에 입력한 내용만 대체 이름 필드에 사용됩니다. 비워 두면 생성되는 인증서에는 대체 이름 필드가 전혀 없습니다.

4. 인증서를 다시 생성하려면 *예*를 클릭하십시오.
5. 새 인증서가 적용되도록 Unified Manager 서버를 다시 시작하십시오.
6. HTTPS 인증서를 확인하여 새 인증서 정보를 검증하십시오.

Active IQ Unified Manager 가상 머신을 다시 시작합니다

Unified Manager의 유지 관리 콘솔에서 가상 머신을 다시 시작할 수 있습니다. 새 보안 인증서를 생성한 후 또는 가상 머신에 문제가 발생한 경우 다시 시작해야 합니다.

시작하기 전에

가상 어플라이언스가 켜져 있습니다.

유지보수 사용자로 유지보수 콘솔에 로그인되어 있습니다.

vSphere에서 게스트 재시작 옵션을 사용하여 가상 머신을 다시 시작할 수도 있습니다. 자세한 내용은 VMware 설명서를 참조하십시오.

단계

1. 유지보수 콘솔에 액세스합니다.
2. 시스템 구성 > *가상 머신 재부팅*을 선택하십시오.

Linux 시스템에서 Active IQ Unified Manager 호스트 이름 변경

특정 시점에 Unified Manager가 설치된 Red Hat Enterprise Linux 시스템의 호스트 이름을 변경해야 할 수도 있습니다. 예를 들어, Linux 시스템 목록을 표시할 때 Unified Manager 서버를 유형, 작업 그룹 또는 모니터링되는 클러스터 그룹별로 더 쉽게 식별하기 위해 호스트 이름을 변경할 수 있습니다.

시작하기 전에

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

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

호스트 이름이 어떻게 할당되었는지와 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 변경하더라도 새 인증서를 생성할 필요가 없습니다. 하지만 인증서의 호스트 이름이 실제 호스트 이름과 일치하도록 인증서를 업데이트하는 것이 모범 사례입니다. 새 인증서는 Linux 시스템을 재시작해야 적용됩니다.

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

단계

1. 수정하려는 Unified Manager 시스템에 루트 사용자로 로그인하십시오.
2. 다음 명령어를 입력하여 Unified Manager 소프트웨어와 연결된 MySQL 소프트웨어를 중지하십시오:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Linux `hostnamectl` 명령을 사용하여 호스트 이름을 변경하십시오:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. 서버의 HTTPS 인증서를 다시 생성하십시오:

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

5. 네트워크 서비스를 다시 시작합니다:

   ```
   systemctl restart NetworkManager.service
   ```

6. 서비스를 재시작한 후 새 호스트 이름이 자체적으로 ping할 수 있는지 확인하십시오:

   ```
   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 명령어를 입력하여 Unified Manager를 다시 시작하십시오.

   ```
   systemctl start mysqld ocie ocieau
   ```

Active IQ Unified Manager에서 정책 기반 스토리지 관리 활성화 및 비활성화

Unified Manager 9.7부터는 ONTAP 클러스터에 스토리지 워크로드(볼륨 및 LUN)를 프로비저닝하고 할당된 성능 서비스 수준에 따라 해당 워크로드를 관리할 수 있습니다. 이 기능은 ONTAP System Manager에서 워크로드를 생성하고 QoS 정책을 연결하는 것과 유사하지만, Unified Manager를 사용하면 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 않으려면 비활성화할 수 있습니다.

이 옵션을 활성화하면 사용자 인터페이스에 많은 새로운 항목이 제공됩니다:

새로운 콘텐츠	위치
새로운 워크로드를 프로비저닝하는 페이지	일반 작업 > *프로비저닝*에서 이용 가능합니다.
성능 서비스 수준 정책을 생성하는 페이지	설정 > 정책 > *성능 서비스 수준*에서 이용 가능합니다.
성능 스토리지 효율성 정책을 생성하는 페이지	설정 > 정책 > *스토리지 효율성*에서 이용 가능합니다.
현재 워크로드 성능 및 워크로드 IOPS를 설명하는 패널	대시보드에서 이용 가능합니다

이 페이지 및 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 비활성화 또는 활성화하십시오:

원하신다면...	그런 다음 이렇게 하십시오...
정책 기반 스토리지 관리 비활성화	정책 기반 스토리지 관리 패널에서 슬라이더 버튼을 왼쪽으로 이동합니다.
정책 기반 스토리지 관리 활성화	정책 기반 스토리지 관리 패널에서 슬라이더 버튼을 오른쪽으로 이동합니다.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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