Active IQ Unified Manager 구성

Active IQ Unified Manager 9.14

NetApp
March 13, 2025

목차

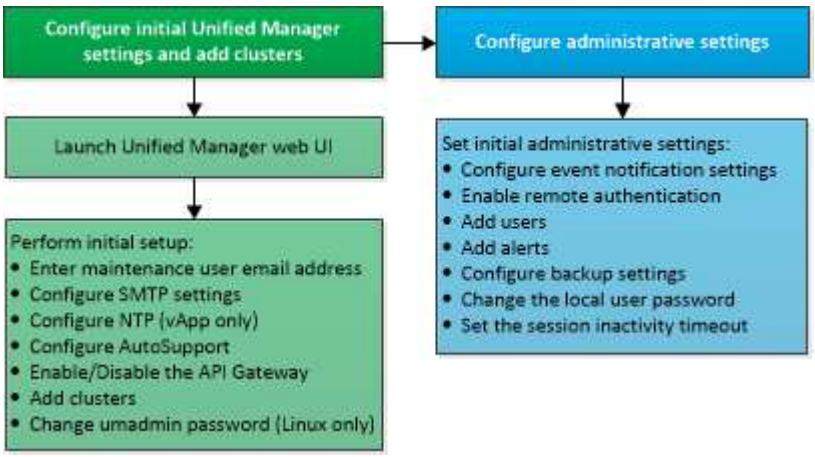
Active IQ Unified Manager 구성

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

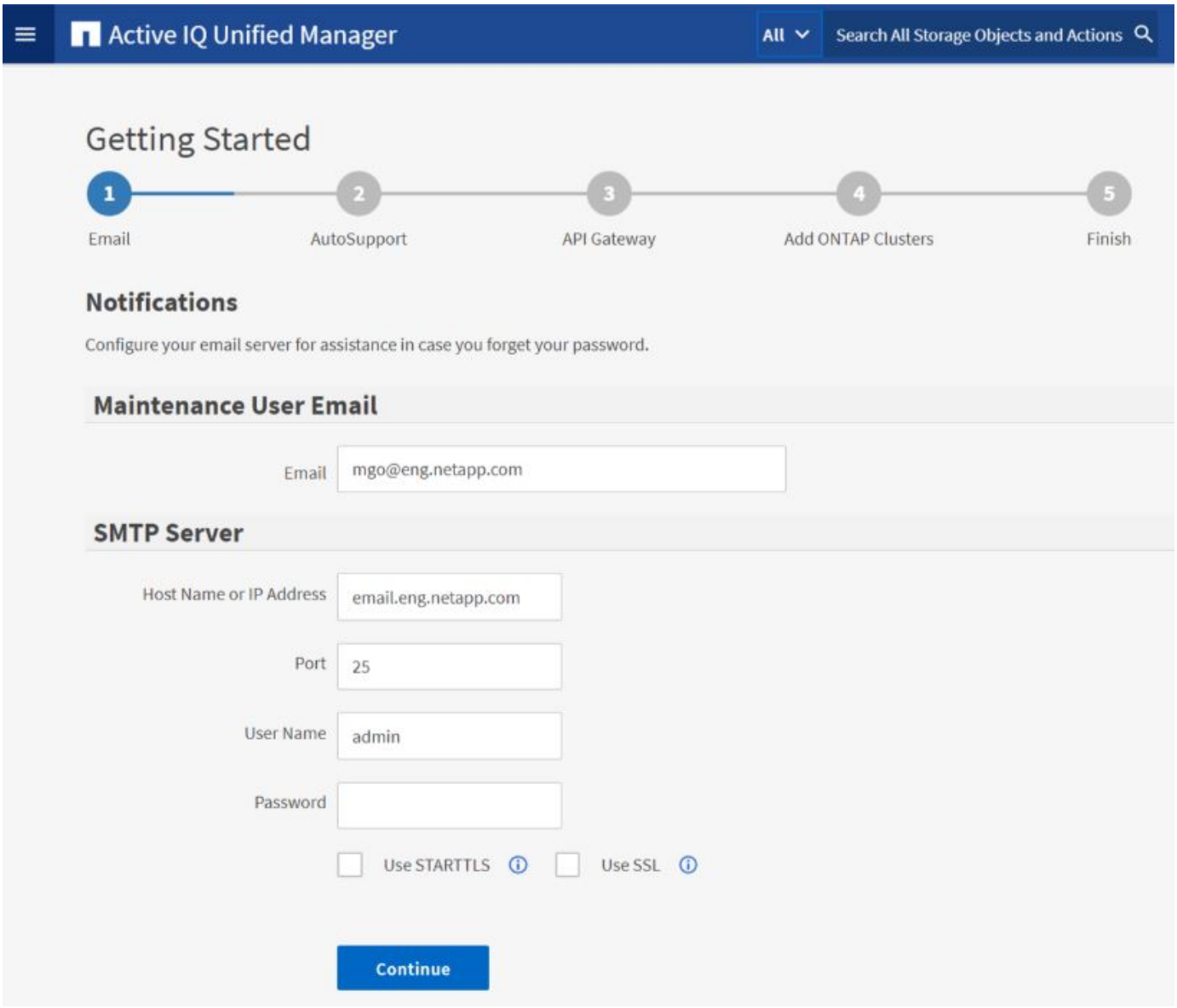
Unified Manager를 사용하려면 먼저 NTP 서버, 유지보수 사용자 이메일 주소, SMTP 서버 호스트 및 ONTAP 클러스터 추가를 포함한 초기 설정 옵션을 구성해야 합니다.

- 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.



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 "HTTPS 보안 인증서를

생성하는 중입니다"참조하십시오.

- EMS 인증서 *: 이 인증서는 Unified Manager에서 소유합니다. ONTAP로부터 수신한 EMS 알림에 대한 인증 중에 사용된다.
- 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 재생성에 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. 에서 Unified Manager CLI를 사용하여 클러스터를 추가할 수 "지원되는 Unified Manager CLI 명령"있습니다.

  ◦ 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 "System Manager 사용자 인터페이스에서 ONTAP 자체 서명된 인증서를 갱신하는 방법"참조하십시오.
- 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 폴이 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 쉼표로 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 채워져 있는 경우 모든 전자 메일 알림이 제대로 전달되도록 실제 작동 중인 전자 메일 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 636을 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	• 인증 서버 관리자 이름은 다음 형식 중 하나입니다. ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (적절한 LDAP 표기법 사용) • 관리자 암호입니다 • 기본 고유 이름(적절한 LDAP 표기법 사용)
LDAP를 엽니다	• 적절한 LDAP 표시법으로 고유 이름 바인딩 • 암호를 바인딩합니다 • 기본 고유 이름입니다

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	a. 관리자 이름과 암호를 입력합니다. b. 인증 서버의 기본 고유 이름을 지정합니다. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com +인 경우 기본 고유 이름은 * cn=ou, dc=domain, dc=com * 입니다.
OpenLDAP를 클릭합니다	a. 바인딩 고유 이름 및 바인딩 암호를 입력합니다. b. 인증 서버의 기본 고유 이름을 지정합니다. 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 이름 및 바인딩 암호를 입력합니다. b. 인증 서버의 기본 고유 이름을 지정합니다. 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 지정합니다. d. 사용자 이름, 그룹 구성원 자격, 사용자 그룹 및 구성원 특성을 입력합니다.

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	a. 보안 연결 사용 * 옵션을 선택합니다. b. Authentication Servers 영역에서 * Add * 를 클릭합니다. c. Add Authentication Server 대화 상자에서 서버의 인증 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다. d. 호스트 권한 부여 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 통신을 위한 기본 포트로 636을 사용하고 비보안 통신을 위한 포트 번호 389를 사용합니다.
비활성화합니다	a. 보안 연결 사용 * 옵션의 선택을 취소합니다. b. Authentication Servers 영역에서 * Add * 를 클릭합니다. c. Add Authentication Server 대화 상자에서 서버의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)와 포트 세부 정보를 지정합니다. d. 추가 * 를 클릭합니다.

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 사용자에 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
- 조치: "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. Available Resources(사용 가능한 자원) 영역에서 * + + * 를 선택하고[All Volumes whose name contains 'abc'] Selected Resources(선택한 자원) 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 Manager가 고가용성 구성으로 구성된 경우 설정의 두 번째 노드에서 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. 유지 관리 콘솔에서 옵션을 사용하는 경우 `Reset Server Certificate` 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	현재 인증서 특성 업데이트 * 옵션을 클릭합니다. 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. • 키 크기에 허용되는 값은 2048, 3072 및 `4096`입니다. • 유효 기간은 최소 1일에서 최대 36500일입니다. 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. • 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.

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. Linux 명령을 사용하여 호스트 이름을 `hostnamectl` 변경합니다.

   ```
   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.

```
systemctl restart NetworkManager.service
```

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.