Active IQ Unified Manager 구성

Active IQ Unified Manager

NetApp
March 26, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/active-iq-unified-manager-97/config/concept-overview-of-the-configuration-sequence.html on March 26, 2025. Always check docs.netapp.com for the latest.

목차

Active IQ Unified Manager 구성 . . . 1
구성 시퀀스의 개요 . . . 1
Unified Manager 웹 UI에 액세스 . . . 1
시작하기 전에 . . . 1
단계 . . . 1
Unified Manager 웹 UI의 초기 설정 수행 . . . 2
시작하기 전에 . . . 2
이 작업에 대해 . . . 2
단계 . . . 3
결과 . . . 3
클러스터 추가 . . . 3
시작하기 전에 . . . 3
이 작업에 대해 . . . 4
단계 . . . 4
결과 . . . 4
경고 알림을 보내도록 Unified Manager 구성 . . . 5
시작하기 전에 . . . 5
이 작업에 대해 . . . 5
단계 . . . 5
이벤트 알림 설정을 구성하는 중입니다 . . . 6
원격 인증 활성화 중 . . . 6
원격 인증에서 중첩 그룹을 해제합니다 . . . 8
인증 서버 추가 . . . 8
인증 서버의 구성을 테스트하는 중입니다 . . . 9
사용자 추가 . . . 10
알림 추가 . . . 11
Unified Manager에 자동으로 추가되는 EMS 이벤트입니다 . . . 12
ONTAP EMS 이벤트 가입 . . . 16
시작하기 전에 . . . 16
이 작업에 대해 . . . 16
단계 . . . 17
작업을 마친 후 . . . 17
SAML 인증 설정 관리 . . . 17
ID 공급자 요구 사항 . . . 17
SAML 인증을 사용하도록 설정합니다 . . . 18
데이터베이스 백업 설정을 구성하는 중입니다 . . . 20
시작하기 전에 . . . 20
이 작업에 대해 . . . 20
단계 . . . 20

로컬 사용자 암호 변경 . . . 21
시작하기 전에 . . . 21
이 작업에 대해 . . . 21
단계 . . . 21
작업을 마친 후 . . . 21
세션 비활성 시간 초과 설정 . . . 21
시작하기 전에 . . . 21
이 작업에 대해 . . . 21
단계 . . . 22
Unified Manager 호스트 이름을 변경하는 중입니다 . . . 22
Unified Manager 가상 어플라이언스 호스트 이름을 변경하는 중입니다 . . . 22
Linux 시스템에서 Unified Manager 호스트 이름 변경 . . . 25
정책 기반 스토리지 관리 설정 및 해제 . . . 26
시작하기 전에 . . . 26
이 작업에 대해 . . . 26
단계 . . . 26

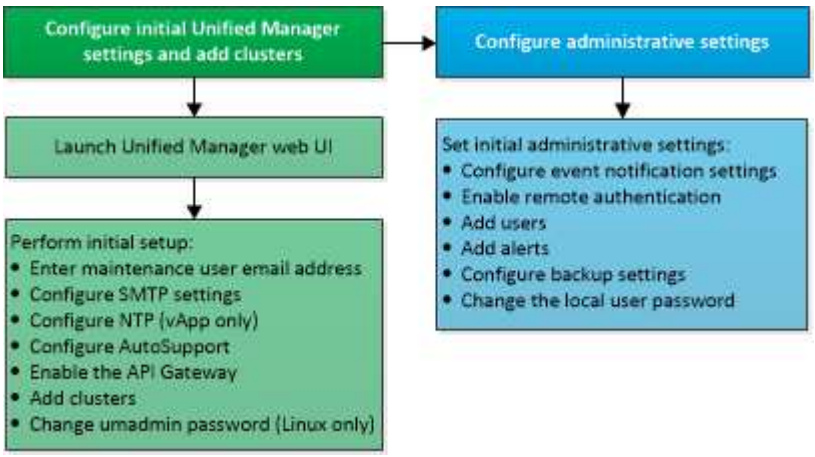
Active IQ Unified Manager 구성

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.

시작하기 전에

- 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 https:/ 형식으로 표시됩니다/`URL`.

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

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.

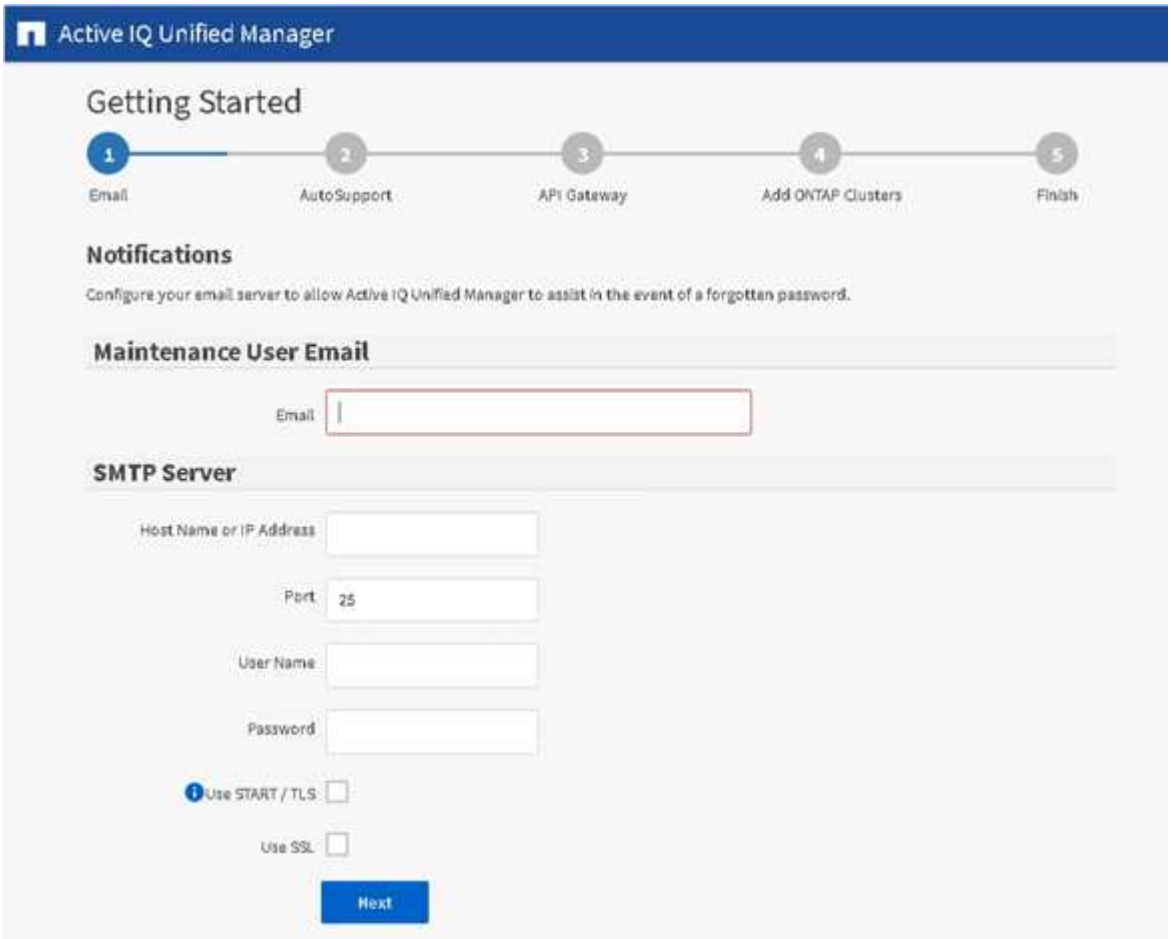
시작하기 전에

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

이 작업에 대해

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.
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 사용자 정의 문자열로 변경할 수 있습니다.
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.

결과

시작하기 페이지가 닫히고 Unified ManagerDashboard 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.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 다음 정보가 있어야 합니다.
  - 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*, *ssh* 및 _http_로 설정된 _admin_역할이 있어야 합니다.

- HTTPS 프로토콜을 사용하여 클러스터에 연결할 포트 번호(일반적으로 포트 443)

Unified Manager NAT IP 주소를 사용하여 NAT/방화벽 뒤에 있는 클러스터를 추가할 수 있습니다. 연결된 모든 Workflow Automation 또는 SnapProtect 시스템은 NAT/방화벽 뒤에 있어야 하며 SnapProtect API 호출은 NAT IP 주소를 사용하여 클러스터를 식별해야 합니다.

- Unified Manager 서버에 적절한 공간이 있어야 합니다. 데이터베이스 디렉토리의 공간이 이미 90% 이상 사용된 경우 서버에 클러스터를 추가할 수 없습니다.

이 작업에 대해

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

Unified Manager의 각 인스턴스가 다른 LIF를 통해 연결되도록 클러스터에 두 번째 클러스터 관리 LIF를 구성한 경우, Unified Manager의 두 인스턴스를 통해 단일 클러스터를 모니터링할 수 있습니다.

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 봅니다.
6. 예 * 를 클릭합니다.

   Unified Manager는 처음에 클러스터를 추가할 때만 인증서를 확인합니다. Unified Manager에서는 ONTAP에 대한 각 API 호출의 인증서를 확인하지 않습니다.

   인증서가 만료된 경우 새 클러스터를 추가할 수 없습니다. 먼저 SSL 인증서를 갱신한 다음 클러스터를 추가해야 합니다.

결과

새 클러스터의 모든 객체가 검색되고(약 15분), 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.

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.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이 작업에 대해

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.

시작하기 전에

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 구성하고 * 저장 * 을 클릭합니다.

```
**If the From Address is pre-filled with the address
"ActiveIQUnifiedManager@localhost.com", you should change it
to a real, working email address to make sure that all email
notifications are delivered successfully.
** If the host name of the SMTP server cannot be resolved,
you can specify the IP address (IPv4 or IPv6) of the SMTP
server instead of the host name.
```

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.

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)와 같은 로컬 LDAP 클라이언트를 비활성화해야 합니다.

이 작업에 대해

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. Authentication Service* 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. 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.

시작하기 전에

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

이 작업에 대해

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 서버 추가

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

시작하기 전에

- 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.

이 작업에 대해

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.

시작하기 전에

- 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.

이 작업에 대해

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. Test User * (사용자 테스트 *) 대화 상자에서 원격 사용자의 사용자 이름 및 암호 또는 원격 그룹의 사용자 이름을 지정한 다음 * Test * (테스트 *)를 클릭합니다.

   원격 그룹을 인증하는 경우 암호를 입력하지 않아야 합니다.

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.

시작하기 전에

- 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.

이 작업에 대해

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.

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.

시작하기 전에

- 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.

이 작업에 대해

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. Alert Setup * 페이지에서 * Add * 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: "ample@domain.com", "테스트" 스크립트를 포함하며, 사용자는 15분마다 통지를 받아야 합니다

경고 추가 대화 상자에서 다음 단계를 수행합니다.

1. 이름 * 을 클릭하고 을 입력합니다 `HealthTest` 경고 이름 * 필드에 입력합니다.
2. 리소스 * 를 클릭하고 포함 탭의 드롭다운 목록에서 * 볼륨 * 을 선택합니다.
   a. 를 입력합니다 `abc` 이름에 ""abc""가 포함된 볼륨을 표시하기 위한 * 포함 * 필드.
   b. Available Resources 영역에서 이름이 'abc' * 인 모든 볼륨을 선택하고 Selected Resources 영역으로 이동합니다.
   c. 제외 * 를 클릭하고 를 입력합니다 `xyz` 이름 포함 * 필드에서 * 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 를 입력합니다 `sample@domain.com` 경고 사용자 필드에서
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.

Unified Manager에 자동으로 추가되는 EMS 이벤트입니다

다음 ONTAP EMS 이벤트가 Unified Manager에 자동으로 추가됩니다. 이러한 이벤트는 Unified Manager가 모니터링하는 모든 클러스터에서 트리거될 때 생성됩니다.

ONTAP 9.5 이상의 소프트웨어를 실행 중인 클러스터를 모니터링할 때 다음과 같은 EMS 이벤트를 사용할 수 있습니다.

Unified Manager 이벤트 이름입니다	**EMS** 이벤트 이름입니다	영향을 받는 리소스입니다	**Unified Manager**의 심각도
애그리게이트 재배치에 대한 클라우드 계층 액세스가 거부되었습니다	arl.netra.ca.check.failed	집계	오류
스토리지 페일오버 중 애그리게이트 재배치에 대한 클라우드 계층 액세스가 거부되었습니다	gb.netra.ca.check.failed	집계	오류
FabricPool 미러 복제 재동기화가 완료되었습니다	wafl.ca.resync.complete	클러스터	오류
FabricPool 공간이 거의 찼습니다	거의 다 찼습니다	클러스터	오류
NVMe - 유예 기간 시작됨	nvmf.graceperiod.start	클러스터	경고
NVMe - 유예 기간 활성	nvmf.graceperiod.active	클러스터	경고
NVMe - 유예 기간이 만료되었습니다	nvmf.graceperiod.expired	클러스터	경고
LUN이 제거되었습니다	lun.destroy	LUN을 클릭합니다	정보
Cloud AWS MetaDataConnFail	Cloud.AWS.metadataConnFail입니다	노드	오류
클라우드 AWS IAMCredsExpired	Cloud.AWS.iamCredsExpired를 참조하십시오	노드	오류
클라우드 AWS IAMCredsInvalid	Cloud.AWS.iamCredsInvalid	노드	오류
Cloud AWS IAMCredsNotFound 를 참조하십시오	Cloud.AWS.iamCredsNotFound 를 참조하십시오	노드	오류
Cloud AWS IAMCredsNotInitialized를 참조하십시오	Cloud.AWS.iamNotInitialized를 초기화합니다	노드	정보
Cloud AWS IAMRoleInvalid	Cloud.AWS.iamRoleInvalid	노드	오류

Unified Manager 이벤트 이름입니다	**EMS** 이벤트 이름입니다	영향을 받는 리소스입니다	**Unified Manager**의 심각도
Cloud AWS IAMRoleNotFound를 참조하십시오	Cloud.AWS.iamRoleNotFound 를 참조하십시오	노드	오류
클라우드 계층 호스트를 확인할 수 없습니다	objstore.host.unresolable을 선택합니다	노드	오류
클라우드 계층 간 클러스터 LIF가 다운되었습니다	objstore.interclusterlifDown	노드	오류
요청 불일치 클라우드 계층 서명	OSC.signaturemismatch.(OSCC.sign	노드	오류
NFSv4 풀 중 하나가 소진되었습니다	Nblade.nfsV4PoolExhaust	노드	심각
QoS 모니터 메모리 최대 용량	QoS.MONITOR.MEMORY.MEMORY	노드	오류
QoS Monitor 메모리가 잠졌습니다	QoS.MONITOR.MEMORY.abated를 참조하십시오	노드	정보
NVMeNS 제거	NVMeNS.destroy	네임스페이스	정보
NVMeNS 온라인	오프라인, NVMeNS	네임스페이스	정보
NVMeNS 오프라인	온라인, NVMeNS	네임스페이스	정보
데이터 보호 공간 부족	데이터 보호. 공간 부족	네임스페이스	경고
동기식 복제가 동기화되지 않았습니다	sms.status.out.of.sync	SnapMirror 관계	경고
동기식 복제가 복구되었습니다	sms.status.in.sync	SnapMirror 관계	정보
동기 복제 자동 재동기화에 실패했습니다	SMS.resync.attempt.failed를 참조하십시오	SnapMirror 관계	오류
많은 CIFS 접속	Nblade.cifsManyAuhs를 참조하십시오	SVM	오류
최대 CIFS 접속이 초과되었습니다	nblade.cifsMaxOpenSameFile을 참조하십시오	SVM	오류

Unified Manager 이벤트 이름입니다	**EMS** 이벤트 이름입니다	영향을 받는 리소스입니다	**Unified Manager**의 심각도
사용자당 최대 CIFS 연결 수를 초과했습니다	Nblade.cifsMaxSessPerUsrConn	SVM	오류
CIFS NetBIOS 이름이 충돌합니다	nblade.cifsNbNameConflictt	SVM	오류
존재하지 않는 CIFS 공유를 연결하려고 시도합니다	Nblade.cifsNoPrivShare	SVM	심각
CIFS 섀도우 복제본 작업이 실패했습니다	cifs.shadowcopy.실패	SVM	오류
AV 서버에서 바이러스가 발견되었습니다	Nblade.vscanVirusDetected 를 참조하십시오	SVM	오류
바이러스 검사를 위한 AV 서버 연결이 없습니다	Nblade.vscanNoScannerConn을 참조하십시오	SVM	심각
등록된 AV 서버가 없습니다	NBlade.vscanNoRegdScanner	SVM	오류
응답이 없는 AV 서버 연결	NBlade.vscanConnInactive	SVM	정보
AV 서버가 새 스캔 요청을 수락하기에 너무 사용 중입니다	NBlade.vscanConnBackPressure	SVM	오류
권한이 없는 사용자가 AV 서버를 시도합니다	Nblade.vscanBadUserPrivaccess를 참조하십시오	SVM	오류
FlexGroup 구성요소에 공간 문제가 있습니다	flexgroup.flexpodues.space.문제로 이동합니다	볼륨	오류
FlexGroup 구성 요소인 공간 상태가 모두 정상입니다	flexgroup.성분.space.status.all.ok	볼륨	정보
FlexGroup 구성 요소에는 inode 문제가 있습니다	flexgroup.constituents.have.inodes.issues	볼륨	오류
FlexGroup 구성 요소에서는 inode 상태가 모두 정상입니다	flexgroup.constituents.inodes.status.all.ok	볼륨	정보

Unified Manager 이벤트 이름입니다	**EMS** 이벤트 이름입니다	영향을 받는 리소스입니다	**Unified Manager**의 심각도
볼륨 논리 공간이 거의 찼습니다	monitor.vol.nearFull.inc.sav	볼륨	경고
볼륨 논리적 공간이 가득 찼습니다	monitor.vol.full.inc.sav	볼륨	오류
볼륨 논리적 공간이 정상입니다	monitor.vol.one.ok.inc.sav	볼륨	정보
WAFL 볼륨 자동 크기 조정 실패	wafl.vol.autoSize.fail	볼륨	오류
WAFL 볼륨 자동 크기 조정이 완료되었습니다	wafl.vol.autoSize.done	볼륨	정보
WAFL readdir 파일 작업 시간 초과	WAFL.readdir.expired를 참조하십시오	볼륨	오류

ONTAP EMS 이벤트 가입

ONTAP 소프트웨어가 설치된 시스템에서 생성되는 EMS(이벤트 관리 시스템) 이벤트를 구독하여 받을 수 있습니다. EMS 이벤트의 하위 집합이 Unified Manager에 자동으로 보고되지만 이러한 이벤트에 가입한 경우에만 추가 EMS 이벤트가 보고됩니다.

시작하기 전에

Unified Manager에 이미 추가된 EMS 이벤트를 자동으로 구독하지 마십시오. 동일한 문제에 대해 두 개의 이벤트를 수신할 때 혼란이 발생할 수 있습니다.

이 작업에 대해

EMS 이벤트 수에 관계없이 구독할 수 있습니다. 구독하는 모든 이벤트의 유효성을 검증하며, 검증된 이벤트만 Unified Manager에서 모니터링하는 클러스터에 적용됩니다. _ONTAP 9 EMS 이벤트 카탈로그_는 지정된 버전의 ONTAP 9 소프트웨어에 대한 모든 EMS 메시지에 대한 자세한 정보를 제공합니다. 해당 이벤트 목록을 보려면 ONTAP 9 제품 설명서 페이지에서 해당 버전의 _EMS 이벤트 카탈로그_를 찾으십시오.

"ONTAP 9 제품 라이브러리"

구독하는 ONTAP EMS 이벤트에 대한 알림을 구성할 수 있으며 이러한 이벤트에 대해 실행할 사용자 지정 스크립트를 만들 수 있습니다.

구독한 ONTAP EMS 이벤트를 수신하지 않으면 클러스터의 DNS 구성에 문제가 발생하여 클러스터가 Unified Manager 서버에 도달하지 못할 수 있습니다. 이 문제를 해결하려면 클러스터 관리자가 클러스터의 DNS 구성을 수정한 다음 Unified Manager를 다시 시작해야 합니다. 이렇게 하면 보류 중인 EMS 이벤트가 Unified Manager 서버로 플러시됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 이벤트 설정 * 을 클릭합니다.
2. 이벤트 설정 * 페이지에서 * EMS 이벤트 가입 * 버튼을 클릭합니다.
3. EMS 이벤트 가입 * 대화 상자에서 가입하려는 ONTAP EMS 이벤트의 이름을 입력합니다.

   가입할 수 있는 EMS 이벤트의 이름을 보려면 ONTAP 클러스터 쉘에서 을 사용할 수 있습니다 `event route show` 명령(ONTAP 9 이전) 또는 `event catalog show` 명령(ONTAP 9 이상)

   "OnCommand Unified Manager/Active IQ Unified Manager에서 ONTAP EMS 이벤트 구독을 구성하는 방법"

4. 추가 * 를 클릭합니다.

   EMS 이벤트는 가입된 EMS 이벤트 목록에 추가되지만, 해당 to Cluster 열에 추가한 EMS 이벤트에 대한 상태가 ""Unknown""으로 표시됩니다.

5. Save and Close * 를 클릭하여 EMS 이벤트 구독을 클러스터에 등록합니다.
6. EMS 이벤트 가입 * 을 다시 클릭합니다.

   추가한 EMS 이벤트에 대해 클러스터에 적용 가능한 열에 ""예"" 상태가 표시됩니다.

   상태가 "예"가 아닌 경우 ONTAP EMS 이벤트 이름의 철자를 확인합니다. 이름을 잘못 입력한 경우 잘못된 이벤트를 제거한 다음 이벤트를 다시 추가해야 합니다.

작업을 마친 후

ONTAP EMS 이벤트가 발생하면 이벤트 페이지에 이벤트가 표시됩니다. Event details 페이지에서 EMS 이벤트에 대한 세부 정보를 볼 이벤트를 선택할 수 있다. 이벤트 처리를 관리하거나 이벤트에 대한 알림을 생성할 수도 있습니다.

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 사용자에 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 ManagerSAML 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
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.

    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

  - 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.

시작하기 전에

- 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.

이 작업에 대해

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.

결과

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

작업을 마친 후

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. Unified Manager가 Windows, Red Hat 또는 CentOS에 배포되면 다음 Unified Manager CLI 명령을 사용하여 GUI 세션 시간 초과를 변경할 수 있습니다. `um option set absolute.session.timeout=00:15:00`이 명령은 Unified Manager GUI 세션 시간 초과를 15분으로 설정합니다.

데이터베이스 백업 설정을 구성하는 중입니다

Unified Manager 데이터베이스 백업 설정을 구성하여 데이터베이스 백업 경로, 보존 수 및 백업 일정을 설정할 수 있습니다. 매일 또는 매주 예약된 백업을 설정할 수 있습니다. 기본적으로 예약된 백업은 사용되지 않습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 백업 경로로 정의한 위치에서 최소 150GB의 공간을 사용할 수 있어야 합니다.

  Unified Manager 호스트 시스템 외부에 있는 원격 위치를 사용하는 것이 좋습니다.

- Linux 시스템에 Unified Manager를 설치할 때 ""jboss"" 사용자가 백업 디렉토리에 대한 쓰기 권한을 가지고 있는지 확인합니다.
- Unified Manager에서 15일의 기간별 성능 데이터를 수집하는 동안 새 클러스터를 추가한 직후에 백업 작업이 발생하도록 예약해서는 안 됩니다.

이 작업에 대해

첫 번째 백업은 전체 백업이므로 백업을 처음 수행할 때보다 더 많은 시간이 필요합니다. 전체 백업은 1GB가 넘고 3~4시간이 소요될 수 있습니다. 후속 백업은 증분 백업이므로 더 적은 시간이 필요합니다.

증분 백업 파일 수가 백업에 할당된 공간에 비해 너무 많은 경우 새 전체 백업을 정기적으로 생성하여 이전의 전체 백업과 모든 하위 증분 파일을 대체할 수 있습니다.

"Active IQ Unified Manager 내에서 새 증분 백업 체인을 시작하는 방법"

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 데이터베이스 백업 * 을 클릭합니다.
2. 데이터베이스 백업 * 페이지에서 * 백업 설정 * 을 클릭합니다.
3. 백업 경로, 보존 수 및 스케줄에 대한 적절한 값을 구성합니다.

   보존 수의 기본값은 10이며 무제한 백업을 생성하는 데 0을 사용할 수 있습니다.

4. Scheduled Daily * 또는 * Scheduled Weekly * 버튼을 선택한 후 일정 세부 정보를 지정합니다.

5. 적용 * 을 클릭합니다.

로컬 사용자 암호 변경

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

시작하기 전에

로컬 사용자로 로그인해야 합니다.

이 작업에 대해

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.

작업을 마친 후

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.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이 작업에 대해

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.

시작하기 전에

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

이 작업에 대해

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

다른 인증 기관에 서명하거나 현재 보안 인증서가 만료된 경우 등 여러 가지 이유로 새 HTTPS 보안 인증서를 생성할 수 있습니다. 새 인증서가 기존 인증서를 대체합니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이 작업에 대해

Unified Manager 웹 UI에 액세스할 수 없는 경우 유지보수 콘솔을 사용하여 동일한 값으로 HTTPS 인증서를 다시 생성할 수 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	Click the *Update the Current Certificate Attributes* option. 새 값을 입력하지 않으면 일반 이름 및 대체 이름 필드에 기존 인증서의 값이 사용됩니다. 다른 필드에는 값이 필요하지 않지만, 인증서에 해당 값을 채우려면 시/도, 국가 등의 값을 입력할 수 있습니다. 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.

작업을 마친 후

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.

시작하기 전에

가상 어플라이언스의 전원이 켜져 있습니다.

유지보수 사용자로 유지보수 콘솔에 로그인한 경우

이 작업에 대해

또한 **Restart Guest** 옵션을 사용하여 vSphere에서 가상 머신을 재시작할 수도 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.

시작하기 전에

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

이 작업에 대해

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.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이 작업에 대해

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.

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

저작권 정보

Copyright © 2025 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.