Unified Manager 호스트 이름 변경

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/task_change_unified_manager_host_name_on_vmware.html on November 13, 2026. Always check docs.netapp.com for the latest.

목차

Unified Manager 호스트 이름 변경 1
- Active IQ Unified Manager 가상 어플라이언스 호스트 이름 변경 1
- Active IQ Unified Manager에서 HTTPS 보안 인증서 생성 1
- Active IQ Unified Manager 가상 머신을 다시 시작합니다 3
- Linux 시스템에서 Active IQ Unified Manager 호스트 이름 변경 4

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
   ```

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.