

vRealize Automation 설치 및 업그레이드

2021년 7월 21일

vRealize Automation 7.5

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

<https://docs.vmware.com/kr/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

목차

1 vRealize Automation 설치 또는 업그레이드	4
vRealize Automation 보안 구성	4
vRealize Automation 보안 기준선 개요	4
설치 미디어의 무결성 확인	5
VMware 시스템 소프트웨어 인프라 강화	5
설치된 소프트웨어 검토	7
VMware 보안 권고 사항 및 패치	7
보안 구성	8
호스트 네트워크 보안 구성	41
감사 및 로깅	56
vRealize Automation 참조 아키텍처	57
초기 배포 및 구성 권장 사항	57
vRealize Automation 배포	58
vRealize Business for Cloud 배포 고려 사항	60
vRealize Automation 확장성	60
vRealize Business for Cloud 확장성	63
vRealize Automation 고가용성 구성 고려 사항	63
vRealize Business for Cloud 고가용성 고려 사항	65
vRealize Automation 하드웨어 규격 및 최대 용량	65
vRealize Automation 소규모 배포 요구 사항	68
vRealize Automation 중간 규모 배포 요구 사항	73
vRealize Automation 대규모 배포 요구 사항	78
vRealize Automation 다중 데이터 센터 배포	84
vRealize Automation 설치	85
설치 개요	85
설치 준비	93
vRealize Automation 장치 배포	110
설치 마법사를 사용하여 설치	115
표준 설치 인터페이스	140
자동 설치	216
사후 설치 작업	222
설치 문제 해결	238
vRealize Automation 업그레이드 및 마이그레이션	266
vRealize Automation 7.1 이상에서 7.5로 업그레이드	269
vRealize Automation 6.2.5를 7.5로 업그레이드	326
vRealize Automation 마이그레이션	393

vRealize Automation 설치 또는 업그레이드

1

vRealize Automation을 처음 설치하거나, 현재 환경을 최신 버전으로 업그레이드할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- vRealize Automation 보안 구성
- vRealize Automation 참조 아키텍처
- vRealize Automation 설치
- vRealize Automation 업그레이드 및 마이그레이션

vRealize Automation 보안 구성

보안 구성은 VMware 지침에 따라 vRealize Automation 배포의 보안 프로파일을 확인, 구성 및 업데이트하는 방식에 대해 설명합니다.

보안 구성은 다음과 같은 항목을 다룹니다.

- 소프트웨어 인프라 보안
- 배포된 구성 보안
- 호스트 네트워크 보안

vRealize Automation 보안 기준선 개요

VMware는 vRealize Automation 시스템을 위한 보안 기준선을 확인 및 구성하는 데 도움이 되는 포괄적인 권장 사항을 제공합니다.

VMware에서 지정한 대로 적절한 도구 및 절차를 사용하여 vRealize Automation 시스템을 위한 강화된 보안 기준선 구성을 확인 및 유지 보수합니다. 일부 vRealize Automation 구성 요소는 강화된 상태 또는 부분적으로 강화된 상태로 설치되지만 VMware 보안 권장 사항, 회사 보안 정책 및 알려진 위협 요소 측면에서 각 구성 요소의 구성을 검토 및 확인해야 합니다.

vRealize Automation 보안 태세

vRealize Automation의 보안 태세는 시스템 및 네트워크 구성, 조직 보안 정책 및 보안 모범 사례를 기반으로 전체적 보안 환경을 가정합니다.

vRealize Automation 시스템의 강화를 확인 및 구성하는 경우 VMware 강화 권장 사항에서 제시한 대로 다음 각 영역을 고려합니다.

- 보안 배포
- 보안 구성
- 네트워크 보안

시스템의 보안 강화를 확인하려면 이러한 각 개념 영역과 관련된 VMware 권장 사항 및 로컬 보안 정책을 고려합니다.

시스템 구성 요소

vRealize Automation 시스템의 강화 및 보안 구성을 고려하는 경우 모든 구성 요소를 비롯해 시스템 기능을 지원하기 위한 해당 구성 요소의 상호 작동 방식을 이해해야 합니다.

보안 시스템을 계획 및 구현할 때 다음 구성 요소를 고려합니다.

- vRealize Automation 장치
- IaaS 구성 요소

vRealize Automation 및 구성 요소의 상호 작동 방식을 숙지하려면 VMware vRealize Automation 설명서 센터에서 [기초 및 개념](#)을 참조하십시오. 일반 vRealize Automation 배포 및 아키텍처에 대한 자세한 내용은 [vRealize Automation 참조 아키텍처](#) 항목을 참조하십시오.

설치 미디어의 무결성 확인

항상 사용자는 VMware 제품을 설치하기 전에 설치 미디어의 무결성을 확인해야 합니다.

ISO, 오프라인 번들 또는 패치를 다운로드한 후에는 항상 SHA1 해시를 확인하여 다운로드한 파일의 무결성과 신뢰성을 확인합니다. VMware에서 받은 물리적 미디어의 보안 봉인이 파손된 경우 소프트웨어를 VMware에 반환하여 교체 받으십시오.

미디어를 다운로드한 후에는 MD5/SHA1 합계 값을 사용하여 다운로드의 무결성을 확인합니다. MD5/SHA1 해시 출력을 VMware 웹 사이트에 게시된 값과 비교합니다. SHA1 또는 MD5 해시가 일치해야 합니다.

설치 미디어의 무결성 확인에 대한 자세한 내용은 <http://kb.vmware.com/kb/1537>을 참조하십시오.

VMware 시스템 소프트웨어 인프라 강화

강화 프로세스의 일부로 VMware 시스템을 지원하는 배포된 소프트웨어 인프라를 평가하고 VMware 강화 지침을 준수하는지 확인합니다.

완벽하게 강화된 보안 환경을 만들 수 있도록 VMware 시스템을 강화하기 전에 지원 소프트웨어 인프라의 보안 결함을 검토하고 해결합니다. 고려해야 하는 소프트웨어 인프라 요소에는 운영 체제 구성 요소, 지원 소프트웨어 및 데이터베이스 소프트웨어가 포함됩니다. 제조업체의 권장 사항 및 기타 관련된 보안 프로토콜에 따라 이러한 구성 요소와 기타 구성 요소의 보안 문제를 해결합니다.

VMware vSphere ® 환경 강화

VMware vSphere ® 환경을 평가하여 적절한 수준의 vSphere 강화 지침이 적용 및 유지되고 있는지 확인합니다.

강화에 대한 자세한 지침은 <http://www.vmware.com/security/hardening-guides.html> 페이지를 참조하십시오.

VMware vSphere ® 인프라는 전체적으로 강화된 환경의 일부로 VMware에서 정의한 보안 지침을 준수해야 합니다.

Infrastructure as a Service 호스트 강화

Infrastructure as a Service Microsoft Windows 호스트 시스템이 VMware 지침에 따라 강화되었는지 확인합니다.

해당 Microsoft Windows 강화 및 보안 모범 사례 지침에 나와 있는 권장 사항을 검토하고, 사용 중인 Windows Server 호스트가 적절하게 강화되었는지 확인합니다. 강화 권장 사항을 따르지 않으면 Windows 릴리스에 포함된 안전하지 않은 구성 요소의 알려진 보안 취약성에 노출될 수 있습니다.

사용 중인 버전이 지원되는지 확인하려면 [vRealize Automation 지원 매트릭스](#)를 참조하십시오.

Microsoft 제품 강화 사례의 올바른 지침에 대해서는 Microsoft 벤더에게 문의하십시오.

Microsoft SQL Server 강화

Microsoft SQL Server 데이터베이스가 Microsoft 및 VMware의 보안 지침을 준수하는지 확인합니다.

해당하는 Microsoft SQL Server 강화 및 보안 모범 사례 지침에 제시된 권장 사항을 검토합니다. 설치되어 있는 Microsoft SQL Server 버전과 관련된 모든 Microsoft 보안 공지를 검토합니다. 강화 권장 사항을 따르지 않으면 Microsoft SQL Server 버전에 포함된 안전하지 않은 구성 요소의 알려진 보안 취약성에 노출될 수 있습니다.

사용 중인 Microsoft SQL Server 버전이 지원되는지 확인하려면 [vRealize Automation 지원 매트릭스](#)를 참조하십시오.

Microsoft 제품 강화 사례의 지침에 대해서는 Microsoft 벤더에게 문의하십시오.

Microsoft .NET 강화

Microsoft .NET은 전체적으로 강화된 환경의 일부로 Microsoft 및 VMware에서 제시하는 보안 지침을 준수해야 합니다.

해당하는 .NET 강화 및 보안 모범 사례 지침에 제시된 권장 사항을 검토합니다. 또한 현재 사용 중인 Microsoft SQL Server 버전과 관련된 모든 Microsoft 보안 공지를 검토합니다. 강화 권장 사항을 따르지 않으면 안전하지 않은 Microsoft.NET 구성 요소의 알려진 보안 취약성에 노출될 수 있습니다.

사용 중인 Microsoft .NET 버전이 지원되는지 확인하려면 [vRealize Automation 지원 매트릭스](#)를 참조하십시오.

Microsoft 제품 강화 사례의 지침에 대해서는 Microsoft 벤더에게 문의하십시오.

Microsoft IIS(인터넷 정보 서비스) 강화

Microsoft IIS(인터넷 정보 서비스)가 Microsoft 및 VMware 보안 지침을 모두 준수하는지 확인합니다.

해당하는 Microsoft IIS 강화 및 보안 모범 사례 지침에 제시된 권장 사항을 검토합니다. 또한 현재 사용 중인 IIS 버전과 관련된 모든 Microsoft 보안 공지를 검토합니다. 강화 권장 사항을 따르지 않으면 알려진 보안 취약성에 노출될 수 있습니다.

사용 중인 버전이 지원되는지 확인하려면 [vRealize Automation 지원 매트릭스](#)를 참조하십시오.

Microsoft 제품 강화 사례의 지침에 대해서는 Microsoft 벤더에게 문의하십시오.

설치된 소프트웨어 검토

타사 및 미사용 소프트웨어의 취약성이 인증되지 않은 시스템 액세스 및 가용성 중단 위험을 높이기 때문에 VMware 호스트 시스템에 설치된 모든 소프트웨어를 검토하고 해당 용도를 평가하는 것이 중요합니다.

VMware 호스트 시스템에 시스템의 보안 작업에 필요하지 않은 소프트웨어를 설치하지 마십시오. 미사용 또는 관련 없는 소프트웨어를 제거합니다.

인벤토리 설치 지원되지 않는 소프트웨어

설치된 제품의 VMware 배포 및 인벤토리에 액세스하여 지원되지 않는 관련 없는 소프트웨어가 설치되지 않았는지 확인합니다.

타사 제품을 위한 지원 정책에 대한 자세한 내용은 VMware 지원 문서(<https://www.vmware.com/support/policies/thirdparty.html>)를 참조하십시오.

타사 소프트웨어 확인

VMware는 테스트 및 확인되지 않은 타사 소프트웨어의 설치를 지원하지 않거나 권장하지 않습니다. VMware 호스트 시스템에 설치된 보안되지 않거나 패치되지 않거나 인증되지 않은 타사 소프트웨어는 시스템을 인증되지 않은 액세스 및 가용성 중단 위험에 처하게 할 수 있습니다. 지원되지 않는 타사 소프트웨어를 사용해야 하는 경우 타사 벤더에 보안 구성 및 패치 요구 사항을 문의하십시오.

VMware 보안 권고 사항 및 패치

시스템에 대한 최대 보안을 유지 보수하려면 VMware 보안 권고 사항을 따르고 모든 관련 패치를 적용합니다.

VMware는 제품에 대한 보안 권고 사항을 릴리스합니다. 이러한 권고 사항을 모니터링하여 제품이 알려진 위협 요소로부터 보호되고 있는지 확인합니다.

vRealize Automation 설치, 패치 및 업그레이드 기록을 평가하고 릴리스된 VMware 보안 권고 사항을 따르고 적용하는지 확인합니다.

현재 VMware 보안 권고 사항에 대한 자세한 내용은 <http://www.vmware.com/security/advisories/>를 참조하십시오.

보안 구성

시스템 구성에 맞게 vRealize Automation 가상 장치에 대한 보안 설정 및 IaaS(Infrastructure as a Service) 구성 요소를 확인 및 업데이트합니다. 또한 기타 구성 요소 및 애플리케이션의 구성을 확인 및 업데이트합니다.

vRealize Automation 설치 보안 구성에는 각 구성 요소의 개별 구성 및 상호 작동 시 구성이 포함됩니다. 알맞은 보안 기준선을 달성하려면 모든 시스템 구성 요소의 상호 협동 구성을 고려합니다.

vRealize Automation 장치 보호

시스템 구성의 필요에 따라 vRealize Automation 장치에 대한 보안 설정을 확인 및 업데이트합니다.

가상 장치 및 해당 호스트 운영 체제에 대한 보안 설정을 구성하십시오. 또한 다른 관련 구성 요소 및 애플리케이션에 대한 구성을 설정하거나 확인하십시오. 경우에 따라 기존 설정을 확인해야 하고 다른 경우에는 적절한 구성을 사용하기 위해 설정을 변경하거나 추가해야 합니다.

루트 암호 변경

vRealize Automation 장치의 루트 암호를 변경할 수 있습니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 **관리** 탭을 클릭합니다.
- 3 **관리** 하위 메뉴를 클릭합니다.
- 4 **현재 관리자 암호** 텍스트 상자에 기존 암호를 입력합니다.
- 5 **새 관리자 암호** 텍스트 상자에 새 암호를 입력합니다.
- 6 **새 관리자 암호 다시 입력** 텍스트 상자에 새 암호를 입력합니다.
- 7 **설정 저장**을 클릭합니다.

루트 암호 해시 및 복잡성 확인

루트 암호가 조직의 회사 암호 복잡성 요구 사항을 충족하는지 확인하십시오.

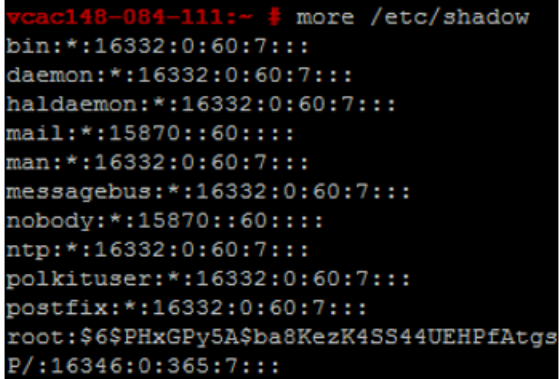
루트 암호 복잡성 검증은 루트 사용자가 사용자 계정에 적용되는 pam_cracklib 모듈 암호 복잡성 검사를 우회할 때 필요합니다.

계정 암호는 sha512 해시를 나타내는 \$6\$로 시작해야 합니다. 이는 모든 강화된 장치에 대한 표준 해시입니다.

절차

- 1 루트 암호의 해시를 확인하려면 루트로 로그인하고 `# more /etc/shadow` 명령을 실행합니다.
해시 정보가 표시됩니다.

그림 1-1. 암호 해시 결과



```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgsP/:16346:0:365:7:::
```

- 2 루트 암호에 sha512 해시가 포함되지 않은 경우 `passwd` 명령을 실행하여 변경합니다.

결과

모든 강화된 장치는 `/etc/pam.d/common-password` 파일에서 `pw_history` 모듈에 대해 `enforce_for_root`를 사용하도록 설정합니다. 시스템은 기본적으로 마지막 5개 암호를 기억합니다. 각 사용자의 이전 암호는 `/etc/securetty/passwd` 파일에 저장됩니다.

루트 암호 기록 확인

암호 기록이 루트 계정에 대해 적용되는지 확인합니다.

모든 강화된 장치는 `/etc/pam.d/common-password` 파일에서 `pw_history` 모듈에 대해 `enforce_for_root`를 사용하도록 설정합니다. 시스템은 기본적으로 마지막 5개 암호를 기억합니다. 각 사용자의 이전 암호는 `/etc/securetty/passwd` 파일에 저장됩니다.

절차

- 1 다음 명령을 실행합니다.
`cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so`
- 2 `enforce_for_root`가 반환된 결과에 표시되는지 확인합니다.
`password required pam_pwhistory.so enforce_for_root remember=5 retry=3`

암호 만료 기한 관리

조직의 보안 정책에 따라 모든 계정 암호 만료 기한을 구성합니다.

기본적으로 모든 강화된 VMware 가상 장치 계정의 암호 만료 기한은 60일입니다. 대부분의 강화된 장치에서 루트 계정의 암호 만료 기한은 365일로 설정됩니다. 모범 사례로 모든 계정의 만료 기한이 보안 및 운영 요구 사항 표준 둘 모두를 준수하는지 확인하는 것이 좋습니다.

루트 암호는 만료되면 복구할 수 없습니다. 관리 및 루트 암호가 만료되지 않도록 사이트별 정책을 구현해야 합니다.

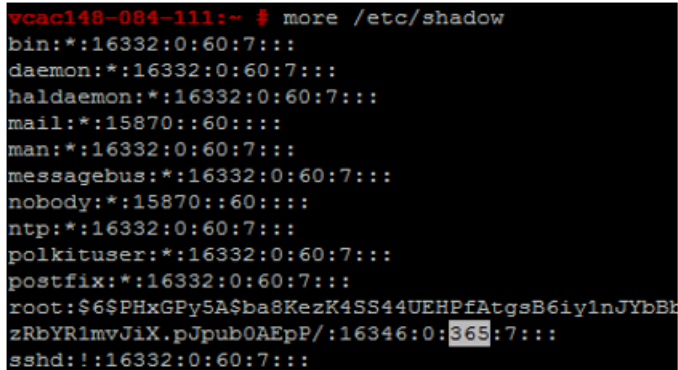
절차

- 1 가상 장치 시스템에 루트로 로그인한 후 다음 명령을 실행하여 모든 계정의 암호 만료 기한을 확인합니다.

```
# cat /etc/shadow
```

암호 만료 기한은 새도 파일의 다섯 번째 필드입니다(필드는 콜론으로 구분됨). 루트 만료 기한은 일 단위로 설정됩니다.

그림 1-2. 암호 만료 기한 필드



```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgsB6iy1nJYbBkzRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

- 2 루트 계정의 만료 기한을 수정하려면 다음 형식으로 명령을 실행합니다.

```
# passwd -x 365 root
```

이 명령에서 365는 암호 만료까지의 일 수를 지정합니다. 같은 명령을 사용하여 원하는 사용자를 수정할 수 있으며, 이 경우 'root'를 특정 계정으로 대체하고 조직의 만료 기한 표준에 맞게 일 수를 바꾸면 됩니다.

보안 셸 및 관리 계정 관리

원격 연결의 경우 강화된 모든 장치에는 SSH(보안 셸) 프로토콜이 포함됩니다. 시스템 보안을 유지하려면 SSH를 필요한 경우에만 사용하고 적절하게 관리해야 합니다.

SSH는 VMware 가상 장치에 대한 원격 연결을 지원하는 대화형 명령줄 환경입니다. 기본적으로 SSH 액세스를 위해서는 높은 권한을 가진 사용자 계정 자격 증명이 필요합니다. 루트 사용자 SSH 작업은 일반적으로 RBAC(역할 기반 액세스 제어) 및 가상 장치의 감사 제어를 생략합니다.

모범 사례로 운영 환경에서는 SSH를 사용 안 함으로 설정하고, 다른 방법으로는 해결할 수 없는 문제를 해결할 때만 활성화합니다. 특정 용도로 필요한 경우에만 조직의 보안 정책에 따라 SSH를 사용 가능한 상태로 둡니다. vRealize Automation 장치에서 SSH는 기본적으로 사용하지 않도록 설정됩니다. vSphere 구성에 따라 OVF(Open Virtualization Format) 템플릿 배포 시 SSH를 사용 또는 사용 안 함으로 설정할 수 있습니다.

시스템에서 SSH가 사용하도록 설정되었는지를 테스트하는 가장 간단한 방법은 SSH를 사용하여 연결을 열어보는 것입니다. 연결이 열리고 자격 증명 요청 메시지가 표시되면 SSH가 사용하도록 설정되고 연결에 사용 가능한 상태입니다.

보안 셸 루트 사용자 계정

VMware 장치에는 미리 구성된 사용자 계정이 포함되어 있지 않기 때문에 기본적으로 루트 계정이 SSH를 사용하여 직접 로그인할 수 있습니다. SSH는 루트 권한으로 가능한 빨리 사용 안 함으로 설정해야 합니다.

거부 없음에 대한 규정 표준을 준수하기 위해 모든 강화된 장치에서 SSH 서버에는 AllowGroups 쉘 항목이 미리 구성되어 SSH 액세스가 보조 그룹 쉘로 제한됩니다. 책임 분담을 위해 /etc/ssh/sshd_config 파일에서 sshd 같이 다른 그룹을 사용하도록 AllowGroups 쉘 항목을 수정할 수 있습니다.

쉘 그룹은 슈퍼유저 액세스를 위해 pam_wheel 모듈을 사용하도록 설정되므로 쉘 그룹의 구성원은 루트로 su할 수 있으며, 이때 루트 암호가 필요합니다. 그룹을 분리하면 사용자가 SSH를 통해 장치에 연결할 수 있지만 루트로 su할 수 없습니다. 장치 기능이 올바르게 작동하도록 AllowGroups 필드의 다른 항목은 제거하거나 수정하지 마십시오. 값을 변경한 후에는 # service sshd restart 명령을 실행하여 SSH 대몬을 다시 시작해야 합니다.

vRealize Automation 장치에서 보안 셸 사용 또는 사용 안 함

문제 해결을 위해서만 vRealize Automation 장치에 SSH(보안 셸)를 사용하도록 설정합니다. 일반적인 운영 작업 중에는 이러한 구성 요소에서 SSH를 사용 안 함으로 설정합니다.

vRealize Automation 장치 관리 인터페이스를 사용하여 vRealize Automation 장치에서 SSH를 사용 또는 사용하지 않도록 설정할 수 있습니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 2 관리 탭을 클릭합니다.

- 3 관리 하위 메뉴를 클릭합니다.

- 4 SSH 서비스 사용 확인란을 선택하여 SSH를 사용하도록 설정하거나 확인란을 선택 취소하여 SSH를 사용하지 않도록 설정합니다.

- 5 설정 저장을 클릭하여 변경 내용을 저장합니다.

보안 셸용 로컬 관리자 계정 생성

보안 모범 사례로 가상 장치 호스트 시스템에서 보안 셸(SSH)용 로컬 관리자 계정을 생성하고 구성합니다. 또한 적절한 계정을 생성한 후 루트 SSH 액세스를 제거하십시오.

SSH용 로컬 관리자 계정 또는 보조 wheel 그룹의 구성원을 생성하거나 두 가지 모두를 생성합니다. 직접적인 루트 액세스를 사용하지 않도록 설정하기 전에 인증된 관리자가 AllowGroups를 사용하여 SSH에 액세스할 수 있는지, wheel 그룹을 사용하여 루트로 su할 수 있는지 테스트합니다.

절차

- 1 가상 장치에 루트로 로그인하고 적절한 사용자 이름을 사용하여 다음 명령을 실행합니다.

```
# useradd -g users <username> -G wheel -m -d /home/<username>
# passwd <username>
```

Wheel은 ssh 액세스를 위해 AllowGroups에 지정된 그룹입니다. 여러 개의 보조 그룹을 추가하려면 `-G wheel,sshd`를 사용합니다.

- 2 해당 사용자로 전환하고 새 암호를 제공하여 암호 복잡성 확인을 적용합니다.

```
# su -<username>
# <username>@hostname:~>passwd
```

암호 복잡성이 충족되면 암호가 업데이트됩니다. 암호 복잡성이 충족되지 않으면 암호가 원래 암호로 되돌아가고 암호 명령을 다시 실행해야 합니다.

- 3 SSH에 직접 로그인을 제거하려면 `/etc/ssh/sshd_config` 파일을 수정하여 `(#)PermitRootLogin yes`를 `PermitRootLogin no`로 교체하십시오.

또는 **관리** 탭의 **관리자 SSH 로그인 사용** 확인란을 선택하거나 선택 취소하여 가상 장치 관리 인터페이스(VAMI)에서 SSH를 사용하거나 사용하지 않도록 설정할 수 있습니다.

다음에 수행할 작업

루트로 직접 로그인을 사용하지 않도록 설정합니다. 기본적으로 강화된 장치는 콘솔을 통해 루트로 직접 로그인을 허용합니다. 부인 방지에 대한 관리 계정을 생성하고 `su-root wheel` 액세스에 대해 해당 계정을 테스트한 후 `/etc/security` 파일을 루트로 편집하고 `tty1` 항목을 `console`로 교체하여 직접 루트 로그인을 사용하지 않도록 설정합니다.

- 1 텍스트 편집기에서 `/etc/securetty` 파일을 엽니다.
- 2 `tty1`을 찾아서 `console`로 교체합니다.
- 3 파일을 저장하고 닫습니다.

보안 셸 서버 구성 강화

가능한 경우 모든 VMware 장치에는 기본 강화된 구성이 있습니다. 구성 파일에서 글로벌 옵션 섹션의 서버 및 클라이언트 서비스 설정을 검토하여 현재 구성이 적절하게 강화되었는지 확인할 수 있습니다.

절차

- 1 VMware 장치에서 `/etc/ssh/sshd_config` 서버 구성 파일을 열고 설정이 올바른지 확인합니다.

설정	상태
서버 대문 프로토콜	Protocol 2
CBC 암호	aes256-ctr 및 aes128-ctr

설정	상태
TCP 포워딩	AllowTCPForwarding no
서버 게이트웨이 포트	Gateway Ports no
X11 포워딩	X11Forwarding no
SSH 서비스	AllowGroups 필드를 사용하여 액세스가 허용된 그룹을 지정합니다. 이 그룹에 적절한 구성원을 추가합니다.
GSSAPI 인증	GSSAPIAuthentication no(사용하지 않는 경우)
Keberos 인증	KeberosAuthentication no(사용하지 않는 경우)
로컬 변수(AcceptEnv 글로벌 옵션)	disabled by commenting out 또는 enabled for LC_* or LANG variables로 설정
터널 구성	PermitTunnel no
네트워크 세션	MaxSessions 1
사용자 동시 연결	루트 및 기타 모든 사용자에게 대해 1로 설정. /etc/security/limits.conf 파일에도 동일한 설정이 구성되어 있어야 합니다.
엄격한 모드 확인	Strict Modes yes
권한 구분	UsePrivilegeSeparation yes
rhosts RSA 인증	RhostsESAAuthentication no
압축	Compression delayed 또는 Compression no
메시지 인증 코드	MACs hmac-sha1
사용자 액세스 제한	PermitUserEnvironment no

2 변경 사항을 저장하고 파일을 닫습니다.

보안 셸 클라이언트 구성 강화

시스템 강화 프로세스의 일부로 SSH 클라이언트의 강화를 확인합니다. 이를 위해 가상 장치 호스트 시스템에서 SSH 클라이언트 구성 파일이 VMware 지침에 따라 구성되었는지 검토합니다.

절차

- 1 SSH 클라이언트 구성 파일 /etc/ssh/ssh_config를 열고 글로벌 옵션 섹션의 설정이 올바른지 확인합니다.

설정	상태
클라이언트 프로토콜	Protocol 2
클라이언트 게이트웨이 포트	Gateway Ports no
GSSAPI 인증	GSSAPIAuthentication no
로컬 변수(SendEnv 글로벌 옵션)	LC_* 또는 LANG 변수만 제공

설정	상태
CBC 암호	aes256-ctr 및 aes128-ctr만
메시지 인증 코드	MACs hmac-sha1 항목에만 사용됨

2 변경 사항을 저장하고 파일을 닫습니다.

보안 셸 키 파일 사용 권한 확인

악의적 공격의 가능성을 최소화하려면 가상 장치 호스트 시스템에 대한 중요 SSH 키 파일 사용 권한을 유지 보수합니다.

SSH 구성을 지정하거나 업데이트한 후 항상 다음 SSH 키 파일 사용 권한이 변경되지 않도록 확인합니다.

- `/etc/ssh/*key.pub`에 있는 공용 호스트 키 파일은 루트 사용자가 소유하며 `0644(-rw-r--r--)`로 설정된 사용 권한이 있습니다.
- `/etc/ssh/*key`에 있는 개인 호스트 키 파일은 루트 사용자가 소유하며 `0600(-rw-----)`으로 설정된 사용 권한이 있습니다.

SSH 키 파일 사용 권한 확인

SSH 사용 권한이 공용 키 파일과 개인 키 파일 둘 모두에 적용되는지 확인합니다.

절차

- 1 다음 명령을 실행하여 SSH 공용 키 파일을 확인합니다. `ls -l /etc/ssh/*key.pub`
- 2 소유자가 루트이고, 그룹 소유자가 루트이며 파일의 사용 권한이 `0644(-rw-r--r--)`로 설정되었는지 확인합니다.
- 3 다음 명령을 실행하여 모든 문제를 해결합니다.

```
chown root /etc/ssh/*key.pub
```

```
chgrp root /etc/ssh/*key.pub
```

```
chmod 644 /etc/ssh/*key.pub
```

- 4 다음 명령을 실행하여 SSH 개인 키 파일을 확인합니다. `ls -l /etc/ssh/*key`

- 5 소유자가 루트이고, 그룹 소유자가 루트이며, 파일의 사용 권한이 `0600(-rw-----)`으로 설정되었는지 확인합니다. 다음 명령을 실행하여 모든 문제를 해결합니다.

```
chown root /etc/ssh/*key
```

```
chgrp root /etc/ssh/*key
```

```
chmod 600 /etc/ssh/*key
```

가상 장치 관리 인터페이스 사용자 변경

가상 장치 관리 인터페이스에서 사용자를 추가하고 삭제하여 적절한 보안 수준을 생성할 수 있습니다.

가상 장치 관리 인터페이스의 루트 사용자 계정은 인증을 위해 PAM을 사용하기 때문에 PAM에 의해 설정된 클리핑 수준도 적용됩니다. 가상 장치 관리 인터페이스를 적절하게 분리하지 않은 경우에는 공격자가 무차별 암호 대입 공격으로 로그인을 시도할 경우 시스템 루트 계정에 잠금이 설정될 수 있습니다. 또한 루트 계정이 조직에 속한 사용자 두 명 이상의 부인 방지를 제공하는 데 부족하다고 판단될 경우에는 관리 인터페이스의 관리자를 변경하도록 선택할 수 있습니다.

사전 요구 사항

절차

- 1 다음 명령을 실행하여 새 사용자를 생성한 후 가상 장치 관리 인터페이스 그룹에 추가합니다.

```
useradd -G vami,root user
```

- 2 사용자의 암호를 생성합니다.

```
passwd user
```

- 3 (선택 사항) 다음 명령을 실행하여 가상 장치 관리 인터페이스에서 루트 액세스를 사용하지 않도록 설정합니다.

```
usermod -R vami root
```

참고 가상 장치 관리 인터페이스에 대한 루트 액세스를 사용하지 않도록 설정하면 [관리] 탭에서 관리자(또는 루트) 암호를 업데이트할 수 있는 기능도 사용할 수 없습니다.

부팅 로더 인증 설정

적절한 보안 수준을 제공하려면 VMware 가상 장치에서 부팅 로더 인증을 구성합니다.

시스템의 부팅 로더에 인증이 필요하지 않은 경우 시스템 콘솔 액세스 권한이 있는 사용자는 시스템 부팅 구성을 변경하거나 시스템을 단일 사용자 또는 유지 보수 모드로 부팅할 수 있으며 이로 인해 서비스 거부 또는 인증되지 않은 시스템 액세스가 발생할 수 있습니다. 부팅 로더 인증은 VMware 가상 장치에서 기본적으로 설정되지 않기 때문에 GRUB 암호를 생성하여 이를 구성해야 합니다.

절차

- 1 가상 장치의 `/boot/grub/menu.lst` 파일에서 `password --md5 <password-hash>` 줄을 찾아 부팅 암호가 있는지 확인합니다.

- 2 암호가 없는 경우 가상 장치에서 `# /usr/sbin/grub-md5-crypt` 명령을 실행합니다.

MD5 암호가 생성되고 명령이 md5 해시 출력을 제공합니다.

- 3 `# password --md5 <hash from grub-md5-crypt>` 명령을 실행하여 암호를 `menu.lst` 파일에 추가합니다.

NTP 구성

중요한 시간 소싱의 경우 vRealize Automation 장치에서 호스트 시간 동기화를 사용하지 않도록 설정하고 NTP(네트워크 시간 프로토콜)를 사용합니다.

vRealize Automation 장치의 NTP 데몬은 동기화된 시간 서비스를 제공합니다. NTP는 기본적으로 사용하지 않도록 설정되기 때문에 수동으로 구성해야 합니다. 가능한 경우 정확한 감사 및 로그 유지를 통해 사용자 작업을 추적하고 잠재적인 악성 공격 및 침입을 감지하기 위해 운영 환경에서 NTP를 사용합니다. NTP 보안 알림에 대한 자세한 내용은 NTP 웹 사이트를 참조하십시오.

NTP 구성 파일은 각 장치의 `/etc/` 폴더에 있습니다. vRealize Automation 장치에 대해 NTP 서비스를 사용하도록 설정하고 가상 장치 관리 인터페이스의 **관리** 탭에서 시간 서버를 추가할 수 있습니다.

절차

- 1 텍스트 편집기를 사용하여 가상 장치 호스트 시스템에서 `/etc/ntp.conf` 구성 파일을 엽니다.
- 2 파일 소유권을 **root:root**로 설정합니다.
- 3 사용 권한을 **0640**으로 설정합니다.
- 4 NTP 서비스에 대한 서비스 거부 증폭 공격의 위험을 완화하려면 `/etc/ntp.conf` 파일을 열고 `restrict` 줄이 파일에 있는지 확인합니다.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- 5 변경 사항이 있으면 저장하고 파일을 닫습니다.

전송 중인 vRealize Automation 장치 데이터에 대한 TLS 구성

vRealize Automation 배포에서 강력한 TLS 프로토콜을 사용하여 vRealize Automation 장치 구성 요소에 대한 전송 채널을 보호하는지 확인합니다.

성능 고려 사항을 위해 TLS는 일부 애플리케이션 서비스 간의 `localhost` 연결에 사용되지 않도록 설정되어 있습니다. 심층 방어가 중요한 경우 모든 `localhost` 통신에 TLS를 사용하도록 설정하십시오.

중요 로드 밸런서에서 TLS를 종료하는 경우 모든 로드 밸런서에서 SSLv2, SSLv3 및 TLS 1.0과 같이 안전하지 않은 프로토콜을 사용하지 않도록 설정하십시오.

Localhost 구성에 TLS 사용

기본적으로 일부 `localhost` 통신에는 TLS가 사용되지 않습니다. 모든 `localhost` 연결에 TLS를 사용하도록 설정하여 보안을 강화할 수 있습니다.

절차

- 1 SSH를 사용하여 vRealize Automation 장치에 연결합니다.
- 2 다음 명령을 실행하여 `vcac` 키 저장소에 대한 사용 권한을 설정합니다.

```
usermod -A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```


3 HAProxy 구성을 업데이트합니다.

- a `/etc/haproxy/conf.d`에 있는 HAProxy 구성 파일을 열고 `20-vcac.cfg` 서비스를 선택합니다.
- b 다음 문자열이 포함된 줄을 찾습니다.

`server local 127.0.0.1...` 그런 후 이러한 줄의 끝에 `ssl verify none`을 추가합니다.

이 섹션에는 다음과 같은 줄도 포함됩니다.

<code>backend-horizon</code>	<code>backend-vro</code>
<code>backend-vra</code>	<code>backend-artifactory</code>
<code>backend-vra-health</code>	

- c `backend-horizon`의 포트를 `8080`에서 `8443`으로 변경합니다.

4 keystorePass의 암호를 가져옵니다.

- a `/etc/vcac/security.properties` 파일에서 `certificate.store.password` 속성을 찾습니다.

예: `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

- b 다음 명령을 사용하여 값을 해독합니다.

`vcac-config prop-util -d --p VALUE`

예: `vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

5 vRealize Automation 서비스를 구성합니다.

- a `/etc/vcac/server.xml` 파일을 엽니다.
- b Connector 태그에 다음 특성을 추가합니다. 이때 `certificate.store.password`를 `etc/vcac/security.properties`에 있는 인증서 저장소 암호 값으로 바꿉니다.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

6 vRealize Orchestrator 서비스를 구성합니다.

- a `/etc/vco/app-server.xml` 파일을 엽니다.
- b Connector 태그에 다음 특성을 추가합니다. 이때 `certificate.store.password`를 `etc/vcac/security.properties`에 있는 인증서 저장소 암호 값으로 바꿉니다.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

7 vRealize Orchestrator, vRealize Automation 및 haproxy 서비스를 다시 시작합니다.

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

참고 vco-server가 다시 시작되지 않으면 호스트 컴퓨터를 재부팅하십시오.

8 가상 장치 관리 인터페이스를 구성합니다.

vRealize Automation 가상 장치에서 다음 명령을 실행하여 서비스 상태를 나열할 수 있습니다.

```
curl -ks -H "Content-Type: application/json" https://localhost/component-registry/services/status/
current?limit=200 | jq -re '.content[]|"\(.serviceStatus.serviceName) \
(.serviceStatus.serviceInitializationStatus)"'
```

참고 가상 장치 관리 인터페이스에서 SSL을 사용하도록 설정하면 서비스 탭에 vRealize Automation 서비스의 상태가 나열되지 않습니다.

a /opt/vmware/share/htdocs/service/café-services/services.py 파일을 엽니다.

b conn = httplib.HTTP() 줄을 conn = httplib.HTTPS()로 변경하여 보안 기능을 향상시킵니다.

FIPS(Federal Information Processing Standard) 140-2 규격 사용

vRealize Automation 장치는 이제 모든 인바운드 및 아웃바운드 네트워크 트래픽에 대해 TLS를 통한 전송 중 데이터에 OpenSSL의 FIPS(Federal Information Processing Standard) 140-2 인증 버전을 사용합니다.

FIPS 모드는 vRealize Automation 장치 관리 인터페이스에서 사용 또는 사용하지 않도록 설정할 수 있습니다. 루트로 로그인한 상태에서 다음 명령을 사용하여 명령줄에서 FIPS를 구성할 수도 있습니다.

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

FIPS를 사용하면 포트 443의 인바운드 및 아웃바운드 vRealize Automation 장치 네트워크 트래픽에 FIPS 140-2 규격 암호화가 사용됩니다. FIPS 설정에 관계없이 vRealize Automation은 AES-256을 사용하여 vRealize Automation 장치에 저장된 보안 데이터를 보호합니다.

참고 현재 vRealize Automation은 일부 내부 구성 요소가 인증된 암호화 모듈을 사용하지 않기 때문에 FIPS 규격을 부분적으로만 사용합니다. 인증된 모듈이 아직 구현되지 않은 경우에는 모든 암호화 알고리즘에 AES-256 기반 암호화가 사용됩니다.

참고 다음 절차에서 구성을 변경하면 물리적 시스템이 재부팅됩니다.

절차

1 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

2 **vRA > 호스트 설정**을 선택합니다.

3 오른쪽 위에서 [작업] 제목 아래의 버튼을 클릭하여 **FIPS**를 사용 또는 사용 안 함으로 설정합니다.

4 **예**를 클릭하여 vRealize Automation 장치를 다시 시작합니다.

SSLv3, TLS 1.0 및 TLS 1.1이 사용되지 않도록 설정되었는지 확인

강화 프로세스의 일부로 배포된 vRealize Automation 장치가 보안 전송 채널을 사용하는지 확인합니다.

참고 TLS 1.0/1.1을 사용하지 않도록 설정하고 TLS 1.2를 사용하도록 설정한 경우 클러스터에 가입 작업을 실행할 수 없습니다.

사전 요구 사항

[Localhost 구성에 TLS 사용](#)을 완료합니다.

절차

1 SSLv3, TLS 1.0 및 TLS 1.1이 vRealize Automation 장치의 HAProxy https 핸들러에서 사용되지 않도록 설정되었는지 확인합니다.

이 파일 검토	다음 항목이 있는지 확인	표시된 대로 적절한 줄에 있음
/etc/haproxy/conf.d/20-vcac.cfg	no-ssl3 no-tls10 no-tls11 force-tls12	bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH +AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA +AES:@STRENGTH no-ssl3 no-tls10 no-tls11
/etc/haproxy/conf.d/30-vro-config.cfg	no-ssl3 no-tls10 no-tls11 force-tls12	bind :::8283 v4v6 ssl crt /opt/vmware/etc/ lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH +AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH +AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no- tls11

2 서비스를 다시 시작합니다.

```
service haproxy restart
```

3 /opt/vmware/etc/lighttpd/lighttpd.conf 파일을 열고 올바른 사용 안 함 항목이 표시되는지 확인합니다.

참고 Lighttpd에서 TLS 1.0 또는 TLS 1.1을 사용 안 함으로 설정하는 지시문은 없습니다. TLS 1.0 및 TLS 1.1 사용에 대한 제한은 OpenSSL에서 TLS 1.0 및 TLS 1.1의 암호 그룹을 사용하지 않도록 강제 적용하여 부분적으로 완화할 수 있습니다.

```
ssl.use-ssl2 = "disable"
ssl.use-ssl3 = "disable"
```

- 4 SSLv3, TLS 1.0 및 TLS 1.1이 vRealize Automation 장치의 콘솔 프록시에 대해 사용되지 않도록 설정되었는지 확인합니다.

- a 다음 줄을 추가하거나 수정하여 `/etc/vcac/security.properties` 파일을 편집합니다.

```
consoleproxy.ssl.server.protocols = TLSv1.2
```

- b 다음 명령을 실행하여 서버를 다시 시작합니다.

```
service vcac-server restart
```

- 5 SSLv3, TLS 1.0 및 TLS 1.1이 vCO 서비스에 대해 사용되지 않도록 설정되었는지 확인합니다.

- a `/etc/vco/app-server/server.xml` 파일에서 `<Connector>` 태그를 찾고 다음 특성을 추가합니다.

```
sslEnabledProtocols = "TLSv1.2"
```

- b 다음 명령을 실행하여 vCO 서비스를 다시 시작합니다.

```
service vco-server restart
```

- 6 SSLv3, TLS 1.0 및 TLS 1.1이 vRealize Automation 서비스에 대해 사용되지 않도록 설정되었는지 확인합니다.

- a `/etc/vcac/server.xml` 파일의 `<Connector>` 태그에 다음 특성을 추가합니다.

```
sslEnabledProtocols = "TLSv1.2"
```

- b 다음 명령을 실행하여 vRealize Automation 서비스를 다시 시작합니다.

```
service vcac-server restart
```

- 7 SSLv3, TLS 1.0 및 TLS 1.1이 RabbitMQ에 대해 사용되지 않도록 설정되었는지 확인합니다.

`/etc/rabbitmq/rabbitmq.config` 파일을 열고 `ssl` 및 `ssl_options` 섹션에 `{versions, ['tlsv1.2']}`만 있는지 확인합니다.

```
[
  {ssl, [
    {versions, ['tlsv1.2']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]},
  ]},
```

```
{mnesia_table_loading_timeout,600000},
{cluster_partition_handling, autoheal},
{heartbeat, 600}
}],
{kernel, [{net_ticktime, 120}]}
].
```

8 RabbitMQ 서버를 다시 시작합니다.

```
# service rabbitmq-server restart
```

9 SSLv3, TLS 1.0 및 TLS 1.1이 vIDM 서비스에 대해 사용되지 않도록 설정되었는지 확인합니다.

SSLEnabled="true"가 포함된 커넥터의 각 인스턴스에 대한 `opt/vmware/horizon/workspace/conf/server.xml` 파일을 열어서 다음 줄이 있는지 확인합니다.

```
sslEnabledProtocols="TLSv1.2"
```

vRealize Automation 구성 요소에 대한 TLS 암호 그룹 구성

최상의 보안을 위해 강력한 암호를 사용하도록 vRealize Automation 구성 요소를 구성해야 합니다.

서버와 브라우저 사이에 협상되는 암호화 암호는 TLS 세션에 사용되는 암호화 강도를 결정합니다.

강력한 암호만 선택되도록 하려면 vRealize Automation 구성 요소에서 약한 암호를 사용하지 않도록 설정합니다. 강력한 암호만 지원하고 충분한 키 크기를 사용하도록 서버를 구성합니다. 또한 모든 암호를 적합한 순서로 구성합니다.

NULL 암호 그룹, aNULL 또는 eNULL과 같이 인증을 제공하지 않는 암호 그룹은 사용하지 않도록 설정합니다. 또한 익명 Diffie-Hellman 키 교환(ADH), 내보내기 수준 암호(EXP, DES를 포함하는 암호), 페이로드 트래픽 암호화에 대한 128비트 미만의 키 크기, 페이로드 트래픽에 대한 해시 메커니즘으로 MD5 사용, IDEA 암호화 그룹 및 RC4 암호화 그룹을 사용하지 않도록 설정합니다. 또한 Diffie-Hellman(DHE) 키 교환을 사용하는 암호 그룹을 사용하지 않도록 설정되었는지 확인합니다.

TLS를 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 [기술 자료 문서 2146570](#)을 참조하십시오.

HA 프록시에 약한 암호 사용 안 함

허용되는 암호 목록을 기준으로 vRealize Automation 장치 HA 프록시 서비스 암호를 검토하고 약한 것으로 생각되는 모든 암호를 사용 안 함으로 설정합니다.

NULL 암호 그룹, aNULL 또는 eNULL과 같이 인증을 제공하지 않는 암호 그룹은 사용하지 않도록 설정합니다. 또한 익명 Diffie-Hellman 키 교환(ADH), 내보내기 수준 암호(EXP, DES를 포함하는 암호), 페이로드 트래픽 암호화에 대한 128비트 미만의 키 크기, 페이로드 트래픽에 대한 해시 메커니즘으로 MD5 사용, IDEA 암호화 그룹 및 RC4 암호화 그룹을 사용하지 않도록 설정합니다.

절차

1 /etc/haproxy/conf.d/20-vcac.cfg 파일에서 bind 지시문의 암호 항목을 검토하고, 약한 것으로 생각되는 모든 암호를 사용 안 함으로 설정합니다.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11
```

- 2 /etc/haproxy/conf.d/30-vro-config.cfg 파일에서 bind 지시문의 암호 항목을 검토하고, 약한 것으로 생각되는 모든 암호를 사용 안 함으로 설정합니다.

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11
```

vRealize Automation 장치 vRealize Automation 장치 콘솔 프록시 서비스에서 약한 암호 사용 안 함 허용되는 암호 목록을 기준으로 vRealize Automation 장치 콘솔 프록시 서비스 암호를 검토하고 약한 것으로 생각되는 모든 암호를 사용 안 함으로 설정합니다.

NULL 암호 그룹, aNULL 또는 eNULL과 같이 인증을 제공하지 않는 암호 그룹은 사용하지 않도록 설정합니다. 또한 익명 Diffie-Hellman 키 교환(ADH), 내보내기 수준 암호(EXP, DES를 포함하는 암호), 페이로드 트래픽 암호화에 대한 128비트 미만의 키 크기, 페이로드 트래픽에 대한 해시 메커니즘으로 MD5 사용, IDEA 암호화 그룹 및 RC4 암호화 그룹을 사용하지 않도록 설정합니다.

절차

- 1 /etc/vcac/security.properties 파일을 텍스트 편집기에서 엽니다.
- 2 원하지 않는 암호 그룹을 사용 안 함으로 설정하는 줄을 파일에 추가합니다.

다음 줄을 변형하여 사용하십시오.

```
consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2,etc
```

예를 들어 AES 128 및 AES 256 암호 그룹을 사용하지 않도록 설정하려면 다음 줄을 추가합니다.

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- 3 다음 명령을 사용하여 서버를 다시 시작합니다.

```
service vcac-server restart
```

vRealize Automation 장치 vCO 서비스에서 약한 암호 사용 안 함 허용되는 암호 목록을 기준으로 vRealize Automation 장치 vCO 서비스 암호를 검토하고 약한 것으로 생각되는 모든 암호를 사용 안 함으로 설정합니다.

NULL 암호 그룹, aNULL 또는 eNULL과 같이 인증을 제공하지 않는 암호 그룹은 사용하지 않도록 설정합니다. 또한 익명 Diffie-Hellman 키 교환(ADH), 내보내기 수준 암호(EXP, DES를 포함하는 암호), 페이로드 트래픽 암호화에 대한 128비트 미만의 키 크기, 페이로드 트래픽에 대한 해시 메커니즘으로 MD5 사용, IDEA 암호화 그룹 및 RC4 암호화 그룹을 사용하지 않도록 설정합니다.

절차

- 1 /etc/vco/app-server/server.xml 파일에서 <Connector> 태그를 찾습니다.

2 원하는 암호 그룹을 사용하도록 암호 특성을 편집하거나 추가합니다.

다음 예를 참조하십시오.

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

vRealize Automation 장치 RabbitMQ 서비스에서 약한 암호 사용 안 함

허용되는 암호 목록을 기준으로 vRealize Automation 장치 RabbitMQ 서비스 암호를 검토하고 약한 것으로 생각되는 모든 암호를 사용 안 함으로 설정합니다.

NULL 암호 그룹, aNULL 또는 eNULL과 같이 인증을 제공하지 않는 암호 그룹은 사용하지 않도록 설정합니다. 또한 익명 Diffie-Hellman 키 교환(ADH), 내보내기 수준 암호(EXP, DES를 포함하는 암호), 페이로드 트래픽 암호화에 대한 128비트 미만의 키 크기, 페이로드 트래픽에 대한 해시 메커니즘으로 MD5 사용, IDEA 암호화 그룹 및 RC4 암호화 그룹을 사용하지 않도록 설정합니다.

절차

- 1 지원되는 암호 그룹을 평가하기 위해 `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'` 명령을 실행합니다.

다음 예에서 반환되는 암호는 지원되는 암호만 나타냅니다. RabbitMQ 서버는 `rabbitmq.config` 파일에 구성된 경우가 아니면 이러한 암호를 사용하거나 알리지 않습니다.

```
["ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384",
 "ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA384",
 "ECDH-ECDSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-GCM-SHA384",
 "ECDH-ECDSA-AES256-SHA384", "ECDH-RSA-AES256-SHA384",
 "DHE-RSA-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384",
 "DHE-RSA-AES256-SHA256", "DHE-DSS-AES256-SHA256", "AES256-GCM-SHA384",
 "AES256-SHA256", "ECDHE-ECDSA-AES128-GCM-SHA256",
 "ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES128-SHA256",
 "ECDHE-RSA-AES128-SHA256", "ECDH-ECDSA-AES128-GCM-SHA256",
 "ECDH-RSA-AES128-GCM-SHA256", "ECDH-ECDSA-AES128-SHA256",
 "ECDH-RSA-AES128-SHA256", "DHE-RSA-AES128-GCM-SHA256",
 "DHE-DSS-AES128-GCM-SHA256", "DHE-RSA-AES128-SHA256", "DHE-DSS-AES128-SHA256",
 "AES128-GCM-SHA256", "AES128-SHA256", "ECDHE-ECDSA-AES256-SHA",
 "ECDHE-RSA-AES256-SHA", "DHE-RSA-AES256-SHA", "DHE-DSS-AES256-SHA",
 "ECDH-ECDSA-AES256-SHA", "ECDH-RSA-AES256-SHA", "AES256-SHA",
 "ECDHE-ECDSA-DES-CBC3-SHA", "ECDHE-RSA-DES-CBC3-SHA", "EDH-RSA-DES-CBC3-SHA",
 "EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
 "DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
 "DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
 "ECDH-RSA-AES128-SHA", "AES128-SHA"]
```

- 2 조직의 보안 요구 사항을 충족하는 지원 암호를 선택합니다.

예를 들어 ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384만 허용하려면 `/etc/rabbitmq/rabbitmq.config` 파일을 검토하고 `ssl` 및 `ssl_options`에 다음 줄을 추가합니다.

```
{ciphers, [ "ECDHE-ECDSA-AES128-GCM-SHA256" , "ECDHE-ECDSA-AES256-GCM-SHA384" ] }
```

3 다음 명령을 사용하여 RabbitMQ 서버를 다시 시작합니다.

```
service rabbitmq-server restart
```

미사용 데이터의 보안 확인

vRealize Automation에 사용되는 데이터베이스 사용자 및 계정의 보안을 확인합니다.

Postgres 사용자

Postgres Linux 사용자 계정은 Postgres 데이터베이스 슈퍼 사용자 계정 역할에 연결되어 있으며 기본적으로 잠긴 계정입니다. 이는 루트 사용자 계정에서만 액세스할 수 있기 때문에 이 사용자에게 가장 안전한 구성입니다. 이 사용자 계정을 잠금 해제하지 마십시오.

데이터베이스 사용자 계정 역할

기본 Postgres 사용자 계정 역할은 애플리케이션 기능 이외의 용도로 사용되어서는 안 됩니다. 기본이 아닌 데이터베이스 검토 또는 보고 작업을 지원하려면 추가 계정이 생성되어야 하며 암호가 적절히 보호되어야 합니다.

명령줄에서 다음 스크립트를 실행합니다.

```
vcac-vami add-db-user newUsername newPassword
```

그러면 새 사용자가 추가되고 암호가 해당 사용자를 통해 제공됩니다.

참고 이 스크립트는 기본-보조 HA Postgres 설정이 구성된 기본 Postgres 데이터베이스에 대해 실행되어야 합니다.

PostgreSQL 클라이언트 인증 구성

vRealize Automation 장치 PostgreSQL 데이터베이스에 대해 로컬 신뢰 인증이 구성되어 있지 않은지 확인합니다. 이 구성은 데이터베이스 슈퍼유저를 포함한 모든 로컬 사용자가 암호 없이 모든 PostgreSQL 사용자로 로그인할 수 있도록 허용합니다.

참고 Postgres 슈퍼유저 계정은 로컬 신뢰로 두어야 합니다.

암호화된 암호를 보내는 md5 인증 방법을 사용하는 것이 좋습니다.

클라이언트 인증 구성 설정은 `/storage/db/pgdata/pg_hba.conf` 파일에 있습니다.

```
# TYPE DATABASE USER ADDRESS METHOD

# "local" is for Unix domain socket connections only
local all postgres trust

# IPv4 local connections:
#host all all 127.0.0.1/32 md5
hostssl all all 127.0.0.1/32 md5

# IPv6 local connections:
#host all all ::1/128 md5
hostssl all all ::1/128 md5

# Allow remote connections for VCAC user.
```



```
#host    vcac          vcac          0.0.0.0/0      md5
hostssl  vcac          vcac          0.0.0.0/0      md5
hostssl  vcac          vcac          ::0/0          md5
# Allow remote connections for VCAC replication user.
#host    vcac          vcac_replication 0.0.0.0/0      md5
hostssl  vcac          vcac_replication 0.0.0.0/0      md5
hostssl  vcac          vcac_replication ::0/0          md5
# Allow replication connections by a user with the replication privilege.
#host    replication  vcac_replication 0.0.0.0/0      md5
hostssl  replication  vcac_replication 0.0.0.0/0      md5
hostssl  replication  vcac_replication ::0/0          md5
```

pg_hba.conf 파일을 편집할 경우, 다음 명령을 실행하여 Postgres 서버를 다시 시작해야만 변경 내용이 적용됩니다.

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

vRealize Automation 애플리케이션 리소스 구성

vRealize Automation 애플리케이션 리소스를 검토하고 파일 사용 권한을 제한합니다.

절차

- 1 다음 명령을 실행하여 SUID 및 GUID 비트가 설정된 파일이 올바르게 정의되었는지 확인합니다.

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

다음 목록이 표시되어야 합니다.

```
2197357  24 -rwsr-xr-x  1 polkituser root      23176 Mar 31  2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354  16 -rwxr-sr-x  1 root    polkituser 14856 Mar 31  2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353  12 -rwsr-x---  1 root    polkituser 10744 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352  20 -rwxr-sr-x  1 root    polkituser 19208 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper
2197351  20 -rwxr-sr-x  1 root    polkituser 19008 Mar 31  2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356  24 -rwxr-sr-x  1 root    polkituser 23160 Mar 31  2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203 460 -rws---x--x  1 root    root      465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858  12 -rwxr-sr-x  1 root    tty       10680 May 10  2010 /usr/sbin/utempter
2142482 144 -rwsr-xr-x  1 root    root      142890 Sep 15  2015 /usr/bin/passwd
2142477 164 -rwsr-xr-x  1 root    shadow    161782 Sep 15  2015 /usr/bin/chage
2142467 156 -rwsr-xr-x  1 root    shadow    152850 Sep 15  2015 /usr/bin/chfn
1458298 364 -rwsr-xr-x  1 root    root      365787 Jul 22  2015 /usr/bin/sudo
2142481  64 -rwsr-xr-x  1 root    root      57776 Sep 15  2015 /usr/bin/newgrp
1458249  40 -rwsr-x---  1 root    trusted   40432 Mar 18  2015 /usr/bin/crontab
2142478 148 -rwsr-xr-x  1 root    shadow    146459 Sep 15  2015 /usr/bin/chsh
2142480 156 -rwsr-xr-x  1 root    shadow    152387 Sep 15  2015 /usr/bin/gpasswd
2142479  48 -rwsr-xr-x  1 root    shadow    46967 Sep 15  2015 /usr/bin/expiry
```

```

311484 48 -rwsr-x--- 1 root messagebus 47912 Sep 16 2014 /lib64/dbus-1/dbus-daemon-launch-helper
876574 36 -rwsr-xr-x 1 root shadow 35688 Apr 10 2014 /sbin/unix_chkpwd
876648 12 -rwsr-xr-x 1 root shadow 10736 Dec 16 2011 /sbin/unix2_chkpwd
49308 68 -rwsr-xr-x 1 root root 63376 May 27 2015 /opt/likewise/bin/ksu
1130552 40 -rwsr-xr-x 1 root root 40016 Apr 16 2015 /bin/su
1130511 40 -rwsr-xr-x 1 root root 40048 Apr 15 2011 /bin/ping
1130600 100 -rwsr-xr-x 1 root root 94808 Mar 11 2015 /bin/mount
1130601 72 -rwsr-xr-x 1 root root 69240 Mar 11 2015 /bin/umount
1130512 36 -rwsr-xr-x 1 root root 35792 Apr 15 2011 /bin/ping6 2012 /lib64/dbus-1/dbus-daemon-launch-helper

```

- 2 다음 명령을 실행하여 가상 장치에 있는 모든 파일에 대해 소유자가 있는지 확인합니다.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

- 3 다음 명령을 실행하여 가상 장치에 대한 모든 파일의 사용 권한을 검토하고 world writable 사용 권한이 없는지 확인합니다.

```
find / -name ".*" -type f -perm -a+w | xargs ls -ldb
```

- 4 다음 명령을 실행하여 vcac 사용자만 올바른 파일을 소유하는지 확인합니다.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/vmware-vcac/*"
```

결과가 표시되지 않으면 모든 올바른 파일을 vcac 사용자만 소유하고 있는 것입니다.

- 5 다음 파일에 대해 vcac 사용자만 쓰기 가능한지 확인합니다.

```

/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore
/etc/vcac/vcac/vcac.properties

```

다음 파일과 해당 하위 디렉토리도 확인합니다.

```

/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*

```

- 6 vcac 또는 루트 사용자만 다음 디렉토리와 해당 하위 디렉토리의 올바른 파일을 읽을 수 있는지 확인합니다.

```

/etc/vcac/*
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*

```

- 7 다음 디렉토리와 해당 하위 디렉토리에 나와 있는 올바른 파일을 vco 또는 루트 사용자만 소유하고 있는지 확인합니다.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

- 8 다음 디렉토리와 해당 하위 디렉토리에 나와 있는 올바른 파일에 대해 vco 또는 루트 사용자만 쓰기 가능한지 확인합니다.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

- 9 다음 디렉토리와 해당 하위 디렉토리에 나와 있는 올바른 파일에 대해 vco 또는 루트 사용자만 읽기 가능한지 확인합니다.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

콘솔 프록시 구성 사용자 지정

문제 해결 및 조직 업무를 용이하게 하기 위해 vRealize Automation에 대한 원격 콘솔 구성을 사용자 지정할 수 있습니다.

vRealize Automation을 설치, 구성 또는 유지 보수하는 경우 설치에 대한 디버깅 및 문제 해결이 가능하도록 일부 설정을 변경할 수 있습니다. 필요한 용도에 따라 적용 가능한 구성 요소의 보안을 제대로 유지할 수 있도록 변경하는 모든 내용을 목록으로 작성하고 감사를 수행하십시오. 구성 변경에 대한 보안이 올바른지가 확실하지 않으면 운영 환경으로 전환하지 마십시오.

VMware Remote Console 티켓 만료 기한 사용자 지정

VMware Remote Console 연결 설정에 사용되는 원격 콘솔 티켓에 대한 유효 기간을 사용자 지정할 수 있습니다.

사용자가 VMware Remote Console 연결을 생성하는 경우 시스템은 가상 시스템에 특정 연결을 설정하는 일회성 자격 증명을 생성하고 반환합니다. 지정된 기간에 대해 티켓 만료 기한을 분 단위로 설정할 수 있습니다.

절차

- 1 `/etc/vcac/security.properties` 파일을 텍스트 편집기에서 엽니다.

- 2 `consoleproxy.ticket.validitySec=30` 형식의 줄을 파일에 추가합니다.

이 줄에서 숫자 값은 티켓이 만료되기까지의 시간(분)을 지정합니다.

- 3 파일을 저장하고 닫습니다.

- 4 `/etc/init.d/vcac-server restart` 명령을 사용하여 `vcac-server`를 다시 시작합니다.

결과

티켓 만료 기한 값이 분 단위의 지정된 시간으로 재설정됩니다.

콘솔 프록시 서버 포트 사용자 지정

VMware Remote Console 콘솔 프록시가 메시지를 수신하는 포트를 사용자 지정할 수 있습니다.

절차

- 1 `/etc/vcac/security.properties` 파일을 텍스트 편집기에서 엽니다.

- 2 `consoleproxy.service.port=8445` 형식의 줄을 파일에 추가합니다.

숫자 값은 콘솔 프록시 서비스 포트 번호를 지정하며, 이 경우 **8445**입니다.

- 3 파일을 저장하고 닫습니다.

- 4 `/etc/init.d/vcac-server restart` 명령을 사용하여 `vcac-server`를 다시 시작합니다.

결과

프록시 서비스 포트가 지정된 포트 번호로 변경됩니다.

X-XSS-Protection 응답 헤더 구성

X-XSS-Protection 응답 헤더를 `haproxy` 구성 파일에 추가합니다.

절차

- 1 편집을 위해 `/etc/haproxy/conf.d/20-vcac.cfg`를 엽니다.

- 2 프론트 엔드 섹션에 다음 줄을 추가합니다.

```
rspdel X-XSS-Protection:\ 1;\ mode=block
rspadd X-XSS-Protection:\ 1;\ mode=block
```

- 3 다음 명령을 사용하여 `HAProxy` 구성을 다시 로드합니다.

```
/etc/init.d/haproxy reload
```

X-Content-Type-Options 응답 헤더 구성

X-Content-Type-Options 응답 헤더를 `HAProxy` 구성에 추가합니다.

절차

- 1 편집을 위해 `/etc/haproxy/conf.d/20-vcac.cfg`를 엽니다.

- 2 프론트 엔드 섹션에 다음 줄을 추가합니다.

```
http-response set-header X-Content-Type-Options nosniff
```

- 3 다음 명령을 사용하여 HAProxy 구성을 다시 로드합니다.

```
/etc/init.d/haproxy reload
```

HTTP Strict Transport Security 응답 헤더 구성

HTTP Strict Transport Security(HSTS) 응답 헤더를 HAProxy 구성에 추가합니다.

절차

- 1 편집을 위해 `/etc/haproxy/conf.d/20-vcac.cfg`를 엽니다.
- 2 프론트 엔드 섹션에 다음 줄을 추가합니다.

```
rspdel Strict-Transport-Security:\ max-age=31536000
rspadd Strict-Transport-Security:\ max-age=31536000
```

- 3 다음 명령을 사용하여 HAProxy 구성을 다시 로드합니다.

```
/etc/init.d/haproxy reload
```

X-Frame-Options 응답 헤더 구성

X-Frame-Options 응답 헤더는 경우에 따라 두 번 표시될 수 있습니다.

X-Frame-Options 응답 헤더는 vIDM 서비스가 이 헤더를 백엔드는 물론 HAProxy에 추가하기 때문에 두 번 표시될 수 있습니다. 적절한 구성을 통해 두 번 표시되는 것을 막을 수 있습니다.

절차

- 1 편집을 위해 `/etc/haproxy/conf.d/20-vcac.cfg`를 엽니다.
- 2 프론트 엔드 섹션에서 다음 줄을 찾습니다.

```
rspadd X-Frame-Options:\ SAMEORIGIN
```

- 3 위 단계에서 찾은 줄 앞에 다음 줄을 추가합니다.

```
rspdel X-Frame-Options:\ SAMEORIGIN
```

- 4 다음 명령을 사용하여 HAProxy 구성을 다시 로드합니다.

```
/etc/init.d/haproxy reload
```

서버 응답 머리글 구성

보안 모범 사례로 잠재적 공격자가 사용할 수 있는 정보를 제한하도록 vRealize Automation 시스템을 구성합니다.

최대한 시스템이 해당 ID 및 버전에 대해 공유하는 정보 양을 최소화합니다. 해커 및 악의적 작업자는 이 정보를 사용하여 웹 서버 또는 버전에 대한 지정된 공격을 만들 수 있습니다.

Lighttpd 서버 응답 헤더 구성

vRealize Automation 장치 lighttpd 서버에 대한 빈 서버 헤더를 생성하는 것이 가장 좋습니다.

절차

- 1 `/opt/vmware/etc/lighttpd/lighttpd.conf` 파일을 텍스트 편집기에서 엽니다.

- 2 `server.tag = " "`를 파일에 추가합니다.
- 3 변경 사항을 저장하고 파일을 닫습니다.
- 4 `# /opt/vmware/etc/init.d/vami-lighttpd restart` 명령을 실행하여 `lighttpd` 서버를 다시 시작합니다.

vRealize Automation 장치에 대한 TCServer 응답 헤더 구성

악성 공격자가 소중한 정보를 입수할 가능성을 제한하기 위해 vRealize Automation 장치와 함께 사용되는 TCServer 응답 헤더에 대한 사용자 지정 빈 서버 헤더를 생성하는 것이 가장 좋습니다.

절차

- 1 `/etc/vco/app-server/server.xml` 파일을 텍스트 편집기에서 엽니다.
- 2 각 `<Connector>` 요소에 `server=" "`를 추가합니다.
예: `<Connector protocol="HTTP/1.1" server="" />`
- 3 변경 사항을 저장하고 파일을 닫습니다.
- 4 다음 명령을 사용하여 서버를 다시 시작합니다.

```
service vco-server restart
```

인터넷 정보 서비스 서버 응답 헤더 구성

악성 공격자가 소중한 정보를 입수할 가능성을 제한하기 위해 Identity Appliance와 함께 사용되는 IIS(인터넷 정보 서비스) 서버에 대한 사용자 지정 빈 서버 헤더를 생성하는 것이 가장 좋습니다.

절차

- 1 `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` 파일을 텍스트 편집기에서 엽니다.
- 2 `RemoveServerHeader=0`을 검색하여 `RemoveServerHeader=1`로 변경합니다.
- 3 변경 사항을 저장하고 파일을 닫습니다.
- 4 `iisreset` 명령을 실행하여 서버를 다시 시작합니다.

다음에 수행할 작업

IIS 관리자 콘솔의 목록에서 HTTP 응답 헤더를 제거하여 IIS X-Powered By 헤더를 사용하지 않도록 설정합니다.

- 1 IIS 관리자 콘솔을 엽니다.
- 2 HTTP 응답 헤더를 열고 목록에서 제거합니다.
- 3 `iisreset` 명령을 실행하여 서버를 다시 시작합니다.

vRealize Automation 장치 세션 시간 초과 설정

회사 보안 정책에 따라 vRealize Automation 장치에서 세션 시간 초과 설정을 구성합니다.

사용자 비활성에 대한 vRealize Automation 장치 기본 세션 시간 초과는 30분입니다. 조직의 보안 정책을 준수하도록 이 시간 초과 값을 조정하려면 vRealize Automation 장치 호스트 시스템에서 **web.xml** 파일을 편집합니다.

절차

- 1 텍스트 편집기에서 **/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml** 파일을 엽니다.
- 2 **session-config**를 찾고 세션 시간 초과 값을 설정합니다. 다음 코드 샘플을 확인합니다.

```
<!-- 30 minutes session expiration time -->
<session-config>
  <session-timeout>30</session-timeout>
  <tracking-mode>COOKIE</tracking-mode>
  <cookie-config>
    <path>/</path>
  </cookie-config>
</session-config>
```

- 3 다음 명령을 실행하여 서버를 다시 시작합니다.

```
service vcac-server restart
```

불필요한 소프트웨어 관리

보안 위험을 최소화하려면 vRealize Automation 호스트 시스템에서 불필요한 소프트웨어를 제거하거나 구성합니다.

제조업체 권장 사항 및 보안 모범 사례에 따라 제거하지 않는 모든 소프트웨어를 구성하여 보안 위반 가능성을 최소화합니다.

USB 대용량 스토리지 처리기 보안

VMware 가상 장치 호스트 시스템에서 USB 디바이스 처리기로 사용되지 않도록 하려면 USB 대용량 스토리지 처리기를 보안합니다. 잠재적 공격자는 이 처리기를 이용하여 시스템을 손상시킬 수 있습니다.

절차

- 1 텍스트 편집기에서 **/etc/modprobe.conf.local** 파일을 엽니다.
- 2 이 파일에 **install usb-storage /bin/true** 줄이 표시되는지 확인합니다.
- 3 파일을 저장하고 닫습니다.

Bluetooth 프로토콜 처리기 보안

가상 장치 호스트 시스템에서 Bluetooth 프로토콜 처리기를 보안하여 잠재적 공격자가 이를 이용하지 못하도록 합니다.

Bluetooth 프로토콜을 네트워크 스택에 바인딩하는 것은 불필요하며 이렇게 할 경우 호스트의 공격 표면이 증가할 수 있습니다.

절차

- 1 텍스트 편집기에서 **/etc/modprobe.conf.local** 파일을 엽니다.

- 이 파일에 다음 줄이 표시되는지 확인합니다.

```
install bluetooth /bin/true
```

- 파일을 저장하고 닫습니다.

SCTP(Stream Control Transmission Protocol) 보안

기본적으로 시스템에서 SCTP(Stream Control Transmission Protocol)가 로드되지 못하도록 합니다. 잠재적 공격자는 이 프로토콜을 이용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요한 경우가 아니면 SCTP(Stream Control Transmission Protocol) 모듈이 로드되지 못하도록 시스템을 구성합니다. SCTP는 미사용 IETF 표준화 전송 계층 프로토콜입니다. 이 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 표면이 증가합니다. 권한 없는 로컬 프로세스는 프로토콜로 소켓을 열어 커널이 동적으로 프로토콜 처리기를 로드하게 할 수 있습니다.

절차

- 텍스트 편집기에서 `/etc/modprobe.conf.local` 파일을 엽니다.
- 이 파일에 다음 줄이 표시되는지 확인합니다.

```
install sctp /bin/true
```

- 파일을 저장하고 닫습니다.

DCCP(Datagram Congestion Protocol) 보안

시스템 강화 작업의 일부로 기본적으로 DCCP(Datagram Congestion Protocol)가 가상 장치 호스트 시스템에서 로드되지 못하도록 합니다. 잠재적 공격자는 이 프로토콜을 이용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요한 경우가 아니면 DCCP(Datagram Congestion Protocol) 모듈을 로드하지 않습니다. DCCP는 사용되지 않는 제안된 전송 계층 프로토콜입니다. 이 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 표면이 증가합니다. 권한 없는 로컬 프로세스는 프로토콜로 소켓을 열어 커널이 동적으로 프로토콜 처리기를 로드하게 할 수 있습니다.

절차

- 텍스트 편집기에서 `/etc/modprobe.conf.local` 파일을 엽니다.
- 이 파일에 DCCP 줄이 표시되는지 확인합니다.

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

- 파일을 저장하고 닫습니다.

네트워크 브리징 보안

기본적으로 시스템에서 네트워크 브리징 모듈이 로드되지 못하도록 합니다. 잠재적 공격자는 이 모듈을 이용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요한 경우가 아니면 네트워크가 로드하지 못하도록 시스템을 구성합니다. 잠재적 공격자는 이 모듈을 사용하여 네트워크 파티셔닝 및 보안을 우회할 수 있습니다.

절차

- 1 모든 VMware 가상 장치 호스트 시스템에서 다음 명령을 실행합니다.

```
# rmmod bridge
```

- 2 텍스트 편집기에서 `/etc/modprobe.conf.local` 파일을 엽니다.

- 3 이 파일에 다음 줄이 표시되는지 확인합니다.

```
install bridge /bin/false
```

- 4 파일을 저장하고 닫습니다.

보안 RDS(Reliable Datagram Sockets) 프로토콜

시스템 강화 작업의 일부로 기본적으로 RDS(Reliable Datagram Sockets) 프로토콜이 가상 장치 호스트 시스템에서 로드되지 못하도록 합니다. 잠재적 공격자는 이 프로토콜을 이용하여 시스템을 손상시킬 수 있습니다.

RDS(Reliable Datagram Sockets) 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 표면이 증가합니다. 권한 없는 로컬 프로세스는 프로토콜로 소켓을 열어 시스템이 동적으로 프로토콜 처리기를 로드하게 할 수 있습니다.

절차

- 1 텍스트 편집기에서 `/etc/modprobe.conf.local` 파일을 엽니다.

- 2 이 파일에 `install rds /bin/true` 줄이 표시되는지 확인합니다.

- 3 파일을 저장하고 닫습니다.

TIPC(Transparent Inter-Process Communication) 프로토콜 보안

시스템 강화 작업의 일부로 기본적으로 TIPC(Transparent Inter-Process Communication) 프로토콜이 가상 장치 호스트 시스템에서 로드되지 못하도록 합니다. 잠재적 공격자는 이 프로토콜을 이용하여 시스템을 손상시킬 수 있습니다.

TIPC(Transparent Inter-Process Communication) 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 표면이 증가합니다. 권한 없는 로컬 프로세스는 프로토콜로 소켓을 열어 커널이 동적으로 프로토콜 처리기를 로드하게 할 수 있습니다.

절차

- 1 텍스트 편집기에서 `/etc/modprobe.conf.local` 파일을 엽니다.

- 2 이 파일에 `install tipc /bin/true` 줄이 표시되는지 확인합니다.

- 3 파일을 저장하고 닫습니다.

IPX(Internetwork Packet Exchange) 프로토콜 보안

기본적으로 시스템에서 IPX(Internetwork Packet Exchange) 프로토콜이 로드되지 못하도록 합니다. 잠재적 공격자는 이 프로토콜을 이용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요한 경우가 아니면 **IPX(Internetnetwork Packet Exchange)** 프로토콜 모듈을 로드하지 않습니다. **IPX** 프로토콜은 사용되지 않는 네트워크 계층 프로토콜입니다. 이 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 표면이 증가합니다. 권한 없는 로컬 프로세스는 프로토콜로 소켓을 열어 시스템이 동적으로 프로토콜 처리기를 로드하게 할 수 있습니다.

절차

- 1 텍스트 편집기에서 **/etc/modprobe.conf.local** 파일을 엽니다.
- 2 이 파일에 다음 줄이 표시되는지 확인합니다.

```
install ipx /bin/true
```

- 3 파일을 저장하고 닫습니다.

Appletalk 프로토콜 보안

기본적으로 시스템에서 **Appletalk** 프로토콜이 로드되지 못하도록 합니다. 잠재적 공격자는 이 프로토콜을 이용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요한 경우가 아니면 **Appletalk** 프로토콜 모듈을 로드하지 않습니다. 이 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 표면이 증가합니다. 권한 없는 로컬 프로세스는 프로토콜로 소켓을 열어 시스템이 동적으로 프로토콜 처리기를 로드하게 할 수 있습니다.

절차

- 1 텍스트 편집기에서 **/etc/modprobe.conf.local** 파일을 엽니다.
- 2 이 파일에 다음 줄이 표시되는지 확인합니다.

```
install appletalk /bin/true
```

- 3 파일을 저장하고 닫습니다.

DECnet 프로토콜 보안

기본적으로 시스템에서 **DECnet** 프로토콜이 로드되지 못하도록 합니다. 잠재적 공격자는 이 프로토콜을 이용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요한 경우가 아니면 **DECnet** 프로토콜 모듈을 로드하지 않습니다. 이 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 표면이 증가합니다. 권한 없는 로컬 프로세스는 프로토콜로 소켓을 열어 시스템이 동적으로 프로토콜 처리기를 로드하게 할 수 있습니다.

절차

- 1 텍스트 편집기에서 **DECnet** 프로토콜 **/etc/modprobe.conf.local** 파일을 엽니다.
- 2 이 파일에 다음 줄이 표시되는지 확인합니다.

```
install decnet /bin/true
```

- 3 파일을 저장하고 닫습니다.

Firewire 모듈 보안

기본적으로 시스템에서 **Firewire** 모듈이 로드되지 못하도록 합니다. 잠재적 공격자는 이 프로토콜을 이용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요한 경우가 아니면 **Firewire** 모듈을 로드하지 않습니다.

절차

1 텍스트 편집기에서 `/etc/modprobe.conf.local` 파일을 엽니다.

2 이 파일에 다음 줄이 표시되는지 확인합니다.

```
install ieee1394 /bin/true
```

3 파일을 저장하고 닫습니다.

laaS(Infrastructure as a Service) 구성 요소 보안

시스템을 강화하는 경우 vRealize Automation laaS(Infrastructure as a Service) 구성 요소 및 해당 호스트 시스템을 보안하여 잠재적 공격자가 이를 이용하지 못하도록 합니다.

vRealize Automation laaS(Infrastructure as a Service) 구성 요소 및 해당 구성 요소가 상주하는 호스트에 대한 보안 설정을 구성해야 합니다. 기타 관련 구성 요소 및 애플리케이션의 구성을 설정하거나 확인해야 합니다. 경우에 따라 기존 설정을 확인할 수 있으며 그렇지 않으면 적절한 구성을 위한 설정을 변경하거나 추가해야 합니다.

NTP 구성

보안 모범 사례로 vRealize Automation 운영 환경에서는 호스트 시간 동기화보다는 인증된 시간 서버를 사용합니다.

운영 환경에서 사용자 작업을 정확하게 추적하고 발생 가능한 악의적인 공격 및 침입을 감사 및 로깅을 통해 식별하려면 호스트 시간 동기화를 사용 안 함으로 설정하고 인증된 시간 서버를 사용하는 것이 좋습니다.

전송 중인 Infrastructure as a Service 데이터에 대한 TLS 구성

vRealize Automation 배포에서 강력한 TLS 프로토콜을 사용하여 Infrastructure as a Service 구성 요소에 대한 전송 채널을 보호하는지 확인하십시오.

SSL(Secure Sockets Layer) 및 보다 최근에 개발된 TLS(전송 계층 보안)는 서로 다른 시스템 구성 요소 간의 네트워크 통신 중에 시스템 보안을 보장하도록 도와주는 암호화 프로토콜입니다. SSL은 오래된 표준이기 때문에 다수의 SSL 구현 사항이 더 이상 잠재적인 공격에 대해 충분한 보안을 제공하지 못합니다. SSLv2 및 SSLv3을 비롯한 이전 SSL 프로토콜에서 심각한 약점이 확인되었습니다. 이러한 프로토콜은 더 이상 안전한 것으로 간주되지 않습니다.

조직의 보안 정책에 따라서 TLS 1.0도 사용하지 않도록 설정하는 것이 좋습니다.

참고 로드 밸런서에서 TLS를 종료하는 경우, SSLv2, SSLv3은 물론 필요한 경우 TLS 1.0 및 1.1과 같은 약한 프로토콜도 사용하지 않도록 설정하십시오.

laaS에 대해 TLS 1.1 및 1.2 프로토콜 사용

laaS 구성 요소를 호스팅하는 모든 가상 시스템에서 TLS 1.1 및 1.2 프로토콜을 사용하도록 설정하고 강제 적용합니다.

절차

1 시작을 클릭한 다음 실행을 클릭합니다.

2 Regedit를 입력하고 확인을 클릭합니다.

3 다음 레지스트리 하위 키를 찾아서 엽니다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols

4 다음을 확인하고 필요에 따라 새 항목을 생성합니다.

- Protocols 아래에 이름이 TLS 1.1인 하위 키가 없으면 하나 생성합니다.
- TLS 1.1 아래에 이름이 Client인 하위 키가 없으면 하나 생성합니다.
- Client 하위 키에 이름이 DisabledByDefault인 키가 없으면 DWORD 유형으로 하나를 생성합니다.
- DisabledByDefault를 마우스 오른쪽 버튼으로 클릭하고 [수정]을 선택한 후 값을 0으로 설정합니다.
- Client 하위 키에 Enabled라는 키가 없으면 DWORD 유형으로 하나를 생성합니다.
- Enabled를 마우스 오른쪽 버튼으로 클릭하고 [수정]을 선택한 다음 값을 1로 설정합니다.
- TLS 1.1 아래에 이름이 Server인 하위 키가 없으면 하나 생성합니다.
- Server 하위 키에 이름이 DisabledByDefault인 키가 없으면 DWORD 유형으로 하나를 생성합니다.
- DisabledByDefault를 마우스 오른쪽 버튼으로 클릭하고 [수정]을 선택한 후 값을 0으로 설정합니다.
- Server 하위 키에 Enabled라는 키가 없으면 DWORD 유형으로 하나를 생성합니다.
- Enabled를 마우스 오른쪽 버튼으로 클릭하고 [수정]을 선택한 다음 값을 1로 설정합니다.

5 TLS 1.2 프로토콜에 대해 위 단계를 반복합니다.

참고 TLS 1.1 및 1.2 사용을 강제 적용하려면 이후 단계에 설명되어 있는 추가 설정이 필요합니다.

6 다음 레지스트리 하위 키를 찾아서 엽니다.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319

7 다음을 확인하고 필요에 따라 새 항목을 생성합니다.

- SchUseStrongCrypto라는 DWORD 항목이 없으면 생성하고 값을 1로 설정합니다.
- SystemDefaultTlsVersions라는 DWORD 항목이 없으면 생성하고 값을 1로 설정합니다.

8 다음 레지스트리 하위 키를 찾아서 엽니다.

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319

9 다음을 확인하고 필요에 따라 새 항목을 생성합니다.

- SchUseStrongCrypto라는 DWORD 항목이 없으면 생성하고 값을 1로 설정합니다.
- SystemDefaultTlsVersions라는 DWORD 항목이 없으면 생성하고 값을 1로 설정합니다.

IaaS에 대해 SSL 3.0 및 TLS 1.0을 사용하지 않도록 설정

IaaS 구성 요소에 대해 SSL 3.0 및 더 이상 사용되지 않는 TLS 1.0 프로토콜을 사용하지 않도록 설정합니다.

절차

1 시작을 클릭한 다음 실행을 클릭합니다.

2 Regedit를 입력한 다음 확인을 클릭합니다.

3 다음 레지스트리 하위 키를 찾아서 엽니다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols

4 다음을 확인하고 필요에 따라 새 항목을 생성합니다.

- Protocols 아래에 이름이 SSL 3.0인 하위 키가 없으면 하나 생성합니다.
- SSL 3.0 아래에 이름이 Client인 하위 키가 없으면 하나 생성합니다.
- Client 하위 키에 이름이 DisabledByDefault인 키가 없으면 DWORD 유형으로 하나를 생성합니다.
- DisabledByDefault를 마우스 오른쪽 버튼으로 클릭하고 [수정]을 선택한 후 값을 1로 설정합니다.
- Enabled를 마우스 오른쪽 버튼으로 클릭하고 [수정]을 선택한 후 값을 0으로 설정합니다.
- SSL 3.0 아래에 이름이 Server인 하위 키가 없으면 하나 생성합니다.
- Server 하위 키에 이름이 DisabledByDefault인 키가 없으면 DWORD 유형으로 하나를 생성합니다.
- DisabledByDefault를 마우스 오른쪽 버튼으로 클릭하고 [수정]을 선택한 후 값을 1로 설정합니다.
- Server에 Enabled라는 키가 없으면 DWORD 유형으로 하나를 생성합니다.
- Enabled를 마우스 오른쪽 버튼으로 클릭하고 [수정]을 선택한 다음 값을 0으로 설정합니다.

5 TLS 1.0 프로토콜에 대해 위 단계를 반복합니다.

IaaS에 대해 TLS 1.0 사용 안 함

보안을 극대화하려면 풀링을 사용하고 TLS 1.0을 사용하지 않도록 IaaS를 구성합니다.

자세한 내용은 Microsoft 기술 자료 문서(<https://support.microsoft.com/en-us/kb/245030>)를 참조하십시오.

절차

1 웹 소켓 대신 폴링을 사용하도록 IaaS를 구성합니다.

- a <appSettings> 섹션에 다음 값을 추가하여 Manager Service 구성 파일인 C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config를 업데이트합니다.

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

- b Manager Service(VMware vCloud Automation Center 서비스)를 다시 시작합니다.

2 IaaS 서버에 대해 TLS 1.0이 사용 안 함으로 설정되었는지 확인합니다.

- a 관리자 권한으로 레지스트리 편집기를 실행합니다.
- b 레지스트리 창에서 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\로 이동합니다.
- c Protocols를 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > 키**를 선택한 후 **TLS 1.0**을 입력합니다.
- d 탐색 트리에서 방금 만든 TLS 1.0 키를 마우스 오른쪽 버튼으로 클릭하고, 팝업 메뉴에서 **새로 만들기 > 키**를 선택한 후 **Client**를 입력합니다.
- e 탐색 트리에서 방금 만든 TLS 1.0 키를 마우스 오른쪽 버튼으로 클릭하고, 팝업 메뉴에서 **새로 만들기 > 키**를 선택한 후 **Server**를 입력합니다.
- f 탐색 트리에서 TLS 1.0 아래에 있는 **Client**를 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > DWORD(32비트) 값**을 클릭한 후 **DisabledByDefault**를 입력합니다.
- g 탐색 트리에서 TLS 1.0 아래에 있는 **Client**를 선택하고, 오른쪽 창의 **DisabledByDefault** DWORD를 두 번 클릭한 후 **1**을 입력합니다.
- h 탐색 트리에서 TLS 1.0 아래에 있는 **Server**를 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > DWORD(32비트) 값**을 선택한 후 **Enabled**를 입력합니다.
- i 탐색 트리에서 TLS 1.0 아래에 있는 **Server**를 선택하고, 오른쪽 창의 **Enabled** DWORD를 두 번 클릭한 후 **0**을 입력합니다.
- j Windows Server를 다시 시작합니다.

TLS 암호 그룹 구성

최상의 보안을 위해 강력한 암호를 사용하도록 vRealize Automation 구성 요소를 구성해야 합니다. 서버와 브라우저 사이에 협상되는 암호화 암호는 TLS 세션에 사용되는 암호화 강도를 결정합니다. 강력한 암호만 선택되도록 하려면 vRealize Automation 구성 요소에서 약한 암호를 사용하지 않도록 설정합니다. 강력한 암호만 지원하고 충분한 키 크기를 사용하도록 서버를 구성합니다. 또한 모든 암호를 적합한 순서로 구성합니다.

허용되지 않는 암호 그룹

NULL 암호 그룹, aNULL 또는 eNULL과 같이 인증을 제공하지 않는 암호 그룹은 사용하지 않도록 설정합니다. 또한 익명 Diffie-Hellman 키 교환(ADH), 내보내기 수준 암호(EXP, DES를 포함하는 암호), 페이로드 트래픽 암호화에 대한 128비트 미만의 키 크기, 페이로드 트래픽에 대한 해시 메커니즘으로 MD5 사용, IDEA 암호화 그룹 및 RC4 암호화 그룹을 사용하지 않도록 설정합니다. 또한 Diffie-Hellman(DHE) 키 교환을 사용하는 암호 그룹을 사용하지 않도록 설정되었는지 확인합니다.

vRealize Automation에서 정적 키 암호를 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 [기술 자료 문서 71094](#)를 참조하십시오.

호스트 서버 보안 확인

보안 모범 사례로 IaaS(Infrastructure as a Service) 호스트 서버 시스템의 보안 구성을 확인합니다.

Microsoft는 호스트 서버 시스템에서 보안을 확인하는 데 도움이 되는 여러 도구를 제공합니다. 이러한 도구의 가장 적절한 사용에 대한 지침은 Microsoft 벤더에 문의하십시오.

호스트 서버 보안 기준선 확인

MBSA(Microsoft Baseline Security Analyzer)를 실행하여 서버에 최신 업데이트 또는 핫 픽스가 있는지 신속하게 확인합니다. MBSA를 사용하여 Microsoft로부터 누락된 보안 패치를 설치함으로써 Microsoft 보안 권장 사항으로 서버를 최신 상태로 유지할 수 있습니다.

Microsoft 웹 사이트에서 최신 버전의 MBSA 도구를 다운로드합니다.

호스트 서버 보안 구성 확인

Windows SCW(보안 구성 마법사) 및 Microsoft SCM(보안 규정 준수 관리자) 툴킷을 사용하여 호스트 서버가 보안 구성되었는지 확인합니다.

Windows Server의 관리 도구에서 SCW를 실행합니다. 이 도구는 서버의 역할과 설치된 기능(네트워킹, Windows 방화벽 및 레지스트리 설정 등)을 식별할 수 있습니다. 보고서를 Windows Server에 대한 관련 SCM의 최신 강화 지침과 비교합니다. 결과를 기반으로 네트워크 서비스, 계정 설정 및 Windows 방화벽과 같은 각 기능에 대한 보안 설정을 미세 조정하고 설정을 서버에 적용할 수 있습니다.

Microsoft Technet 웹 사이트에서 SCW 도구에 대한 자세한 정보를 찾을 수 있습니다.

애플리케이션 리소스 보호

보안 모범 사례로 모든 관련 Infrastructure as a Service 파일의 사용 권한이 적절한지 확인합니다.

Infrastructure as a Service 설치를 기준으로 Infrastructure as a Service 파일을 검토합니다. 대부분의 경우 모든 폴더의 하위 폴더 및 파일의 설정은 해당 상위 폴더의 설정과 동일해야 합니다.

디렉토리 또는 파일	그룹 또는 사용자	모든 권한	수정	읽기 및 실행		
				읽기	쓰기	
VMware\VCAC\Agents \<agent_name>\logs	시스템	X	X	X	X	X
	관리자	X	X	X	X	X
	관리자	X	X	X	X	X

디렉토리 또는 파일	그룹 또는 사용자	모든 권한	수정	읽기 및 실행	읽기	쓰기
VMware\VCAC\Agents\ <agent_name> \temp	시스템	X	X	X	X	X
	관리자	X	X	X	X	X
	관리자	X	X	X	X	X
VMware\VCAC\Agents\	시스템	X	X	X	X	X
	관리자	X	X	X	X	X
	사용자			X	X	
VMware\VCAC\Distributed Execution Manager\	시스템	X	X	X	X	X
	관리자	X	X	X	X	X
	사용자			X	X	
VMware\VCAC\Distributed Execution Manager\DEM\Logs	시스템	X	X	X	X	X
	관리자	X	X	X	X	X
	관리자	X	X	X	X	X
VMware\VCAC\Distributed Execution Manager\DEO\Logs	시스템	X	X	X	X	X
	관리자	X	X	X	X	X
	관리자	X	X	X	X	X
VMware\VCAC\Management Agent\	시스템	X	X	X	X	X
	관리자	X	X	X	X	X
	사용자			X	X	
VMware\VCAC\Server\	시스템	X	X	X	X	X
	관리자	X	X	X	X	X
	사용자			X	X	
VMware\VCAC\Web API	시스템	X	X	X	X	X
	관리자	X	X	X	X	X
	사용자			X	X	

Infrastructure as a Service 호스트 시스템 보안

보안 모범 사례로 IaaS(Infrastructure as a Service) 호스트 시스템의 기본 설정을 검토하여 보안 지침을 따르는지 확인합니다.

IaaS(Infrastructure as a Service) 호스트 시스템의 기타 계정, 애플리케이션, 포트 및 서비스를 보호하십시오.

서버 사용자 계정 설정 확인

불필요한 로컬 및 도메인 사용자 계정 및 설정이 존재하지 않는지 확인합니다. 애플리케이션 기능과 관련이 없는 사용자 계정은 관리, 유지 보수 및 문제 해결에 필요한 최소 한도로 제한합니다. 도메인 사용자 계정의 원격 액세스 권한은 서버를 유지 보수하는 데 필요한 최소한의 권한으로 제한합니다. 이러한 계정을 엄격하게 제어하고 감사를 수행합니다.

불필요한 애플리케이션 삭제

호스트 서버에서 불필요한 애플리케이션을 모두 삭제합니다. 불필요한 애플리케이션은 알 수 없거나 패치가 적용되지 않은 취약성으로 인해 노출 위험을 높입니다.

불필요한 포트 및 서비스 사용 안 함

호스트 서버의 방화벽에서 열린 포트 목록을 검토합니다. IaaS 구성 요소 또는 중요한 시스템 작업에 필요하지 않은 포트를 모두 차단합니다. [포트 및 프로토콜 구성](#) 항목을 참조하십시오. 호스트 서버에서 실행 중인 서비스에 대해 감사를 수행하고 필요하지 않은 서비스는 사용하지 않도록 설정합니다.

호스트 네트워크 보안 구성

알려진 보안 위협에 대해 최상의 보호를 제공하려면 모든 VMware 호스트 시스템에 네트워크 인터페이스 및 통신 설정을 구성하십시오.

포괄적인 보안 계획의 일환으로 설정된 보안 지침에 따라 VMware 가상 장치 및 Infrastructure as a Service 구성 요소에 대한 네트워크 인터페이스 보안 설정을 구성하십시오.

VMware 장치에 대한 네트워크 설정 구성

VMware 가상 장치 호스트 시스템이 안전하고 필요한 통신만 지원하도록 하려면 해당 네트워크 통신 설정을 검토하고 편집합니다.

VMware 호스트 시스템의 네트워크 IP 프로토콜 구성을 검사하고 보안 지침에 따라 네트워크 설정을 구성합니다. 필요하지 않은 모든 통신 프로토콜을 사용하지 않도록 설정합니다.

사용자의 네트워크 인터페이스 제어 방지

보안 모범 사례로 VMware 장치 호스트 시스템에서 자신의 작업을 수행하는 데 필요한 시스템 권한만 사용자에게 허용해야 합니다.

네트워크 인터페이스를 조작할 수 있는 권한을 사용자 계정에 허용하면 네트워크 보안 메커니즘 생략 또는 서비스 거부 문제가 발생할 수 있습니다. 네트워크 인터페이스 설정을 변경할 수 있는 기능은 권한 있는 사용자만 사용할 수 있도록 제한해야 합니다.

절차

1 각 VMware 장치 호스트 시스템에서 다음 명령을 실행합니다.

```
# grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

2 각 인터페이스가 NO로 설정되었는지 확인합니다.

TCP 백로그 대기열 크기 설정

악의적 공격에 대한 일정 수준의 방어를 제공하려면 VMware 장치 호스트 시스템에서 기본 TCP 백로그 대기열 크기를 구성합니다.

TCP 백로그 대기열 크기를 적절한 기본 크기로 설정하여 TCP 서비스 거부 공격에 대한 완화를 제공합니다. 권장되는 기본 설정은 1280입니다.

절차

- 1 각 VMware 장치 호스트 시스템에서 다음 명령을 실행합니다.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```
- 2 텍스트 편집기에서 `/etc/sysctl.conf` 파일을 엽니다.
- 3 다음 항목을 파일에 추가하여 기본 TCP 백로그 대기열 크기를 설정합니다.

```
net.ipv4.tcp_max_syn_backlog=1280
```

- 4 변경 사항을 저장하고 파일을 닫습니다.

브로드캐스트 주소에 대한 ICMPv4 에코 거부

보안 모범 사례로 VMware 장치 호스트 시스템이 ICMP 브로드캐스트 주소 에코 요청을 무시하는지 확인합니다.

브로드캐스트 ICMP(Internet Control Message Protocol) 에코에 대한 응답은 증폭 공격에 대한 공격 벡터를 제공하고 악성 에이전트의 네트워크 매핑을 용이하게 할 수 있습니다. 장치 호스트 시스템이 ICMPv4 에코를 무시하도록 구성되면 해당 공격으로부터 시스템을 보호할 수 있습니다.

절차

- 1 VMware 가상 장치 호스트 시스템에서 `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` 명령을 실행하여 시스템이 IPv4 브로드캐스트 주소 에코 요청을 거부하는지 확인합니다.
 호스트 시스템이 IPv4 리디렉션을 거부하도록 구성되어 있는 경우, 이 명령은 `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`에 대해 0 값을 반환합니다.
- 2 가상 장치 호스트 시스템이 ICMPv4 브로드캐스트 주소 에코 요청을 거부하도록 구성하려면, Windows 호스트 시스템의 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.
- 3 `net.ipv4.icmp_echo_ignore_broadcasts=0` 이라고 쓰여 있는 항목을 찾습니다. 이 항목의 값이 0으로 설정되어 있지 않거나 해당 항목이 없는 경우 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.
- 4 변경 사항을 저장하고 파일을 닫습니다.

IPv4 프록시 ARP 사용 안 함

VMware 장치 호스트 시스템에서 필요한 경우가 아니면 무단 정보 공유를 방지하기 위해 IPv4 프록시 ARP를 사용 안 함으로 설정했는지 확인합니다.

IPv4 프록시 ARP를 통해 시스템은 특정 인터페이스에서 다른 인터페이스에 연결된 호스트를 대신하여 ARP 요청에 대해 응답을 보낼 수 있습니다. 필요하지 않은 경우에는 연결된 네트워크 세그먼트 사이의 주소 정보 유출을 방지하기 위해 이 기능을 사용 안 함으로 설정하십시오.

절차

- 1 VMware 가상 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"` 명령을 실행하여 IPv4 프록시 ARP가 사용되지 않도록 설정되었는지 확인합니다.

호스트 시스템에서 IPv6 프록시 ARP가 사용 안 함으로 설정되어 있으면 이 명령이 0을 값으로 반환합니다.

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 호스트 시스템에 IPv6 프록시 ARP를 구성해야 하면 텍스트 편집기에서 `/etc/sysctl.conf` 파일을 엽니다.
- 3 다음 항목을 확인합니다.

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

해당 항목이 없거나 해당 값이 0으로 설정되어 있지 않으면 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

- 4 변경한 사항이 있으면 저장하고 파일을 닫습니다.

IPv4 ICMP Redirect 메시지 거부

보안 모범 사례로 VMware 가상 장치 호스트 시스템에서 IPv4 ICMP Redirect 메시지를 거부하는지 확인합니다.

라우터는 ICMP Redirect 메시지를 사용하여 대상에 보다 직접적인 경로가 있다는 사실을 호스트에 알려 줍니다. 악성 ICMP Redirect 메시지는 메시지 가로채기 공격을 용이하게 만들 수 있습니다. 이러한 메시지는 호스트의 경로 테이블을 수정하며 인증되지 않습니다. 달리 필요한 경우가 아니라면 시스템에서 이러한 메시지를 무시하도록 구성해야 합니다.

절차

- 1 VMware 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` 명령을 실행하여 시스템이 IPv4 리디렉션 메시지를 거부하는지 확인합니다.

호스트 시스템이 IPv4 리디렉션을 거부하도록 구성되어 있는 경우, 이 명령은 다음을 반환합니다.

```
/proc/sys/net/ipv4/conf/all/accept_reidrects:0
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

- 가상 장치 호스트 시스템이 IPv4 리디렉션 메시지를 거부하도록 구성하려면 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.

- `net.ipv4.conf`로 시작하는 줄의 값을 확인합니다.

다음 항목의 값이 0으로 설정되어 있지 않거나 해당 항목이 없는 경우 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

- 변경한 사항을 저장하고 파일을 닫습니다.

IPv6 ICMP redirect 메시지 거부

보안 모범 사례로 VMware 가상 장치 호스트 시스템이 IPv6 ICMP redirect 메시지를 거부하는지 확인합니다.

라우터는 ICMP Redirect 메시지를 사용하여 대상에 보다 직접적인 경로가 있다는 사실을 호스트에 알려 줍니다. 악성 ICMP Redirect 메시지는 메시지 가로채기 공격을 용이하게 만들 수 있습니다. 이러한 메시지는 호스트의 경로 테이블을 수정하며 인증되지 않습니다. 필요한 경우가 아니면 이러한 메시지를 무시하도록 시스템이 구성되었는지 확인합니다.

절차

- VMware 가상 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` 명령을 실행하여 시스템에서 IPv6 리디렉션 메시지를 거부하는지 확인합니다.

IPv6 리디렉션을 거부하도록 호스트 시스템이 구성되어 있으면 이 명령이 다음을 반환합니다.

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

- IPv4 리디렉션 메시지를 거부하도록 가상 장치 호스트 시스템을 구성하려면 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.

- `net.ipv6.conf`로 시작하는 줄의 값을 확인합니다.

파일에서 다음 항목의 값이 0으로 설정되지 않았거나 항목 자체가 없으면 파일에 해당 항목을 추가하거나, 기존 항목을 적절하게 업데이트합니다.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 변경 사항을 저장하고 파일을 닫습니다.

IPv4 Martian 패킷 기록

보안 모범 사례로 VMware 가상 장치 호스트 시스템이 IPv4 Martian 패킷을 기록하는지 확인합니다.

Martian 패킷에는 시스템에서 잘못된 것으로 알고 있는 주소가 포함됩니다. 잘못된 구성 또는 진행 중인 공격을 식별할 수 있게 이러한 메시지를 기록하도록 호스트 시스템을 구성하십시오.

절차

- 1 VMware 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default|all"` 명령을 실행하여 시스템이 IPv4 Martian 패킷을 기록하는지 확인합니다.

Martian 패킷을 기록하도록 구성된 가상 시스템에서는 다음을 반환합니다.

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/conf/default/log_martians:1
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 IPv4 martian 패킷을 기록하도록 가상 시스템을 구성해야 할 경우에는 텍스트 편집기에서 `/etc/sysctl.conf` 파일을 엽니다.
- 3 `net.ipv4.conf`로 시작하는 줄의 값을 확인합니다.

다음 항목의 값이 1로 설정되지 않았거나 항목 자체가 없으면 파일에 해당 항목을 추가하거나, 기존 항목을 적절하게 업데이트합니다.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

- 4 변경 사항을 저장하고 파일을 닫습니다.

IPv4 역방향 경로 필터링 사용

보안 모범 사례로 VMware 가상 장치 호스트 시스템에서 IPv4 역방향 경로 필터링을 사용하는지 확인합니다.

역방향 경로 필터링은 시스템에서 경로가 없는 소스 주소 또는 원본 인터페이스를 가리키지 않는 경로가 있는 소스 주소가 포함된 패킷을 삭제하도록 하여 스푸핑된 소스 주소로부터 시스템을 보호합니다. 가능할 때마다 역방향 경로 필터링을 사용하도록 호스트 시스템을 구성하십시오. 시스템 역할에 따라서 역방향 경로 필터링으로 인해 시스템이 정당한 트래픽을 삭제하는 경우가 있습니다. 이러한 문제가 발생하는 경우에는 더 허용되는 모드를 사용하거나 역방향 경로 필터링을 사용하지 않도록 함께 설정해야 할 수 있습니다.

절차

- 1 VMware 가상 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` 명령을 실행하여 IPv4 역방향 경로 필터링을 사용하는지 확인합니다.

가상 시스템에서 IPv4 역방향 경로 필터링을 사용하는 경우 이 명령은 다음을 반환합니다.

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/re_filter:1
```

가상 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 호스트 시스템에 IPv4 역방향 경로 필터링을 구성해야 하는 경우 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.

3 net.ipv4.conf로 시작하는 줄의 값을 확인합니다.

다음 항목의 값이 1로 설정되어 있지 않거나 해당 항목이 없는 경우 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

4 변경 사항을 저장하고 파일을 닫습니다.

IPv4 전달 거부

VMware 장치 호스트 시스템이 IPv4 전달을 거부하는지 확인합니다.

시스템이 IP 전달을 위해 구성되어 있지만 지정된 라우터가 아닌 경우, 공격자는 이 시스템을 사용하여 네트워크 디바이스에서 필터링되지 않은 통신 경로를 제공하여 네트워크 보안을 무시할 수 있습니다. 이러한 위험을 방지하기 위해 가상 장치 호스트 시스템이 IPv4 전달을 거부하도록 구성하십시오.

절차

1 VMware 장치 호스트 시스템에서 # cat /proc/sys/net/ipv4/ip_forward 명령을 실행하여 시스템이 IPv4 전달을 거부하는지 확인합니다.

호스트 시스템이 IPv4 전달을 거부하도록 구성되어 있는 경우, 이 명령은 /proc/sys/net/ipv4/ip_forward에 대해 0 값을 반환합니다. 가상 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

2 가상 장치 호스트 시스템이 IPv4 전달을 거부하도록 구성하려면 /etc/sysctl.conf 파일을 텍스트 편집기에서 엽니다.

3 net.ipv4.ip_forward=0이라고 쓰여 있는 항목을 찾습니다. 이 항목의 값이 현재 0으로 설정되어 있지 않거나 해당 항목이 없는 경우 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

4 변경 사항이 있으면 저장하고 파일을 닫습니다.

IPv6 전달 거부

보안 모범 사례로 VMware 장치 호스트 시스템이 IPv6 전달을 거부하는지 확인합니다.

시스템이 IP 전달을 위해 구성되어 있지만 지정된 라우터가 아닌 경우, 공격자는 이 시스템을 사용하여 네트워크 디바이스에서 필터링되지 않은 통신 경로를 제공하여 네트워크 보안을 무시할 수 있습니다. 이러한 위험을 방지하기 위해 가상 장치 호스트 시스템이 IPv6 전달을 거부하도록 구성하십시오.

절차

1 VMware 장치 호스트 시스템에서 # grep [01] /proc/sys/net/ipv6/conf/*/forwarding | egrep "default|all" 명령을 실행하여 시스템이 IPv6 전달을 거부하는지 확인합니다.

호스트 시스템이 IPv6 전달을 거부하도록 구성되어 있는 경우, 이 명령은 다음을 반환합니다.

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 호스트 시스템이 IPv6 전달을 거부하도록 구성하려면 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.

- 3 `net.ipv6.conf`로 시작하는 줄의 값을 확인합니다.

다음 항목의 값이 0으로 설정되어 있지 않거나 해당 항목이 없는 경우 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 변경한 사항이 있으면 저장하고 파일을 닫습니다.

IPv4 TCP Syncookie 사용

VMware 장치 호스트 시스템이 IPv4 TCP Syncookie를 사용하는지 확인합니다.

TCP SYN 플러드 공격은 시스템의 TCP 연결 테이블을 SYN_RCVD 상태의 연결로 채워 서비스 거부를 초래할 수 있습니다. Syncookie는 후속 ACK를 수신할 때까지 연결 추적을 방지하여 이니시에이터가 유효한 연결을 시도하고 있으며 플러드 소스가 아님을 확인합니다. 이 기술은 완전한 표준 준수 방식으로 작동하지 않지만 플러드 조건 동안에만 활성화되며 계속해서 유효한 요청을 서비스하는 동안 시스템 방어를 허용합니다.

절차

- 1 VMware 장치 호스트 시스템에서 `# cat /proc/sys/net/ipv4/tcp_syncookies` 명령을 실행하여 해당 시스템이 IPv4 TCP Syncookie를 사용하는지 확인합니다.

호스트 시스템이 IPv4 포워딩을 거부하도록 구성된 경우 이 명령은 `/proc/sys/net/ipv4/tcp_syncookies`에 대해 값 1을 반환합니다. 가상 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 IPv4 TCP Syncookie를 사용하도록 가상 장치를 구성해야 하는 경우 텍스트 편집기에서 `/etc/sysctl.conf`를 엽니다.

- 3 `net.ipv4.tcp_syncookies=1`이라고 쓰여 있는 항목을 찾습니다.

이 항목의 값이 현재 1로 설정되어 있지 않거나 해당 항목이 없는 경우 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

- 4 변경한 사항이 있으면 저장하고 파일을 닫습니다.

IPv6 라우터 알림 거부

VMware 호스트 시스템이 시스템 운영에 달리 필요하지 않는 한 라우터 알림 및 ICMP Redirect 수락을 거부하는지 확인하십시오.

IPv6를 사용하면 시스템이 네트워크의 정보를 자동으로 사용하여 네트워크 디바이스를 구성하는 것이 가능합니다. 보안의 관점에서 중요한 구성 정보를 인증되지 않는 방식으로 네트워크에서 수락하기보다는 수동으로 구성하는 것이 더 좋습니다.

절차

- 1 VMware 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` 명령을 실행하여 시스템이 라우터 알림을 거부하는지 확인합니다.

호스트 시스템이 IPv6 라우터 알림을 거부하도록 구성되어 있는 경우, 이 명령은 0 값을 반환합니다.

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 호스트 시스템이 IPv6 라우터 알림을 거부하도록 구성하려면 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.
- 3 다음 항목을 확인합니다.

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

이러한 항목이 없거나 해당 값이 0으로 설정되어 있지 않으면 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

- 4 변경한 사항이 있으면 저장하고 파일을 닫습니다.

IPv6 라우터 요청 거부

보안 모범 사례로 VMware 장치 호스트 시스템이 시스템 운영에 달리 필요하지 않는 한 IPv6 라우터 요청을 거부하는지 확인합니다.

라우터 요청 설정은 인터페이스를 활성화할 때 보낼 라우터 요청의 수를 결정합니다. 주소가 정적으로 할당되면 요청을 보낼 필요가 없습니다.

절차

- 1 VMware 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations | egrep "default|all"` 명령을 실행하여 시스템이 IPv6 라우터 요청을 거부하는지 확인합니다.

호스트 시스템이 IPv6 라우터 알림을 거부하도록 구성되어 있는 경우, 이 명령은 다음을 반환합니다.

```
/proc/sys/net/ipv6/conf/all/router_solicitations:0
/proc/sys/net/ipv6/conf/default/router_solicitations:0
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 호스트 시스템이 IPv6 라우터 요청을 거부하도록 구성하려면 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.

3 다음 항목을 확인합니다.

```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

해당 항목이 없거나 해당 값이 0으로 설정되어 있지 않으면 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

4 변경 사항이 있으면 저장하고 파일을 닫습니다.

라우터 요청의 IPv6 라우터 기본 설정 거부

VMware 장치 호스트 시스템이 시스템 운영에 달리 필요하지 않는 한 IPv6 라우터 요청을 거부하는지 확인하십시오.

요청 설정의 라우터 기본 설정은 라우터 기본 설정을 결정합니다. 주소가 정적으로 할당되면 요청에 대한 라우터 기본 설정을 수신할 필요가 없습니다.

절차

- 1 VMware 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref|egrep "default|all"` 명령을 실행하여 시스템이 IPv6 라우터 요청을 거부하는지 확인합니다.

호스트 시스템이 IPv6 라우터 알림을 거부하도록 구성되어 있는 경우, 이 명령은 다음을 반환합니다.

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 호스트 시스템이 IPv6 라우터 요청을 거부하도록 구성하려면 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.
- 3 다음 항목을 확인합니다.

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

해당 항목이 없거나 해당 값이 0으로 설정되어 있지 않으면 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

4 변경한 사항이 있으면 저장하고 파일을 닫습니다.

IPv6 라우터 접두사 거부

VMware 장치 호스트 시스템이 시스템 운영에 달리 필요하지 않는 한 IPv6 라우터 접두사 정보를 거부하는지 확인하십시오.

`accept_ra_pinfo` 설정은 시스템이 라우터의 접두사 정보를 수락할지 여부를 제어합니다. 주소가 정적으로 할당되면 라우터 접두사 정보를 수신할 필요가 없습니다.

절차

- 1 VMware 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo|egrep "default|all"` 명령을 실행하여 시스템이 IPv6 라우터 접두사 정보를 거부하는지 확인합니다.

호스트 시스템이 IPv6 라우터 알림을 거부하도록 구성되어 있는 경우, 이 명령은 다음을 반환합니다.

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 호스트 시스템이 IPv6 라우터 접두사 정보를 거부하도록 구성하려면 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.
- 3 다음 항목을 확인합니다.

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

해당 항목이 없거나 해당 값이 0으로 설정되어 있지 않으면 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

- 4 변경 사항이 있으면 저장하고 파일을 닫습니다.

IPv6 라우터 알림 홉 제한 설정 거부

VMware 장치 호스트 시스템이 필요한 경우가 아니면 IPv6 라우터 홉 제한 설정을 거부하는지 확인하십시오.

`accept_ra_defrtr` 설정은 시스템이 라우터 알림의 홉 제한 설정을 수락할지 여부를 제어합니다. 이 값을 0으로 설정하면 라우터가 송신 패킷에 대한 기본 IPv6 홉 제한을 변경할 수 없습니다.

절차

- 1 VMware 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr|egrep "default|all"` 명령을 실행하여 시스템이 IPv6 라우터 홉 제한 설정을 거부하는지 확인합니다.

호스트 시스템이 IPv6 라우터 홉 제한 설정을 거부하도록 구성되어 있는 경우, 이 명령은 0 값을 반환합니다.

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 호스트 시스템이 IPv6 라우터 홉 제한 설정을 거부하도록 구성하려면 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.

3 다음 항목을 확인합니다.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

해당 항목이 없거나 해당 값이 0으로 설정되어 있지 않으면 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

4 변경한 사항이 있으면 저장하고 파일을 닫습니다.

IPv6 라우터 알림 Autoconf 설정 거부

VMware 장치 호스트 시스템이 필요한 경우를 제외하고 IPv6 라우터 autoconf 설정을 거부하는지 확인하십시오.

autoconf 설정은 라우터 알림으로 인해 시스템이 글로벌 유니캐스트 주소를 인터페이스에 할당할지 여부를 제어합니다.

절차

1 VMware 장치 호스트 시스템에서 # grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all" 명령을 실행하여 시스템이 IPv6 라우터 autoconf 설정을 거부하는지 확인합니다.

호스트 시스템이 IPv6 라우터 autoconf 설정을 거부하도록 구성되어 있는 경우, 이 명령은 0 값을 반환합니다.

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

2 호스트 시스템이 IPv6 라우터 autoconf 설정을 거부하도록 구성하려면 /etc/sysctl.conf 파일을 텍스트 편집기에서 엽니다.

3 다음 항목을 확인합니다.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

해당 항목이 없거나 해당 값이 0으로 설정되어 있지 않으면 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

4 변경한 사항이 있으면 저장하고 파일을 닫습니다.

IPv6 인접 라우터 요청 거부

VMware 장치 호스트 시스템이 필요한 경우를 제외하고 IPv6 인접 라우터 요청을 거부하는지 확인하십시오.

dad_transmits 설정은 인터페이스를 활성화할 때 원하는 주소가 네트워크에서 고유한지 확인하기 위해 주소(글로벌 또는 링크 로컬)당 보낼 인접 라우터 요청의 수를 결정합니다.

절차

- 1 VMware 장치 호스트 시스템에서 `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` 명령을 실행하여 시스템이 IPv6 인접 라우터 요청을 거부하는지 확인합니다.

호스트 시스템이 IPv6 인접 라우터 요청을 거부하도록 구성되어 있는 경우, 이 명령은 0 값을 반환합니다.

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 호스트 시스템이 IPv6 인접 라우터 요청을 거부하도록 구성하려면 `/etc/sysctl.conf` 파일을 텍스트 편집기에서 엽니다.
- 3 다음 항목을 확인합니다.

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

해당 항목이 없거나 해당 값이 0으로 설정되어 있지 않으면 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다.

- 4 변경한 사항이 있으면 저장하고 파일을 닫습니다.

IPv6 최대 주소 제한

VMware 장치 호스트 시스템이 IPv6 최대 주소 설정을 시스템 작업에 필요한 최소값으로 제한하는지 확인합니다.

최대 주소 설정은 각 인터페이스에 사용할 수 있는 글로벌 유니캐스트 IPv6 주소 수를 결정합니다. 기본값은 16이지만 시스템에 필요한 정적으로 구성된 글로벌 주소 수로 정확히 설정해야 합니다.

절차

- 1 VMware 장치 호스트 시스템에서 `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"` 명령을 실행하여 해당 시스템이 IPv6 최대 주소를 적절히 제한하는지 확인합니다.

호스트 시스템이 IPv6 최대 주소를 제한하도록 구성된 경우 이 명령은 값 1을 반환합니다.

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

호스트 시스템이 제대로 구성된 경우에는 추가 작업이 필요하지 않습니다.

- 2 호스트 시스템에서 IPv6 최대 주소를 구성해야 하는 경우 텍스트 편집기에서 `/etc/sysctl.conf` 파일을 엽니다.

3 다음 항목을 확인합니다.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

항목이 없거나 해당 값이 1로 설정되지 않은 경우 항목을 추가하거나 기존 항목을 적절히 업데이트합니다.

4 변경한 사항이 있으면 저장하고 파일을 닫습니다.

Infrastructure as a Service 호스트에 대한 네트워크 설정 구성

보안 모범 사례로 VMware 요구 사항 및 지침에 따라 VMware IaaS(Infrastructure as a Service) 구성 요소 호스트 시스템에서 네트워크 통신 설정을 구성합니다.

적절한 보안과 함께 전체 vRealize Automation 기능을 지원하도록 IaaS(Infrastructure as a Service) 호스트 시스템의 네트워크 구성을 구성하십시오.

IaaS(Infrastructure as a Service) 구성 요소 보안 항목을 참조하십시오.

포트 및 프로토콜 구성

보안 모범 사례로 VMware 지침에 따라 모든 vRealize Automation 장치와 구성 요소의 포트 및 프로토콜을 구성합니다.

중요한 시스템 구성 요소가 운영 환경에서 작동하도록 vRealize Automation 구성 요소의 수신 및 송신 포트를 필요에 맞게 구성합니다. 불필요한 모든 포트와 프로토콜을 사용하지 않도록 설정합니다. VMware vRealize Automation 설명서에서 "vRealize Automation 참조 아키텍처"를 참조하십시오.

포트 및 프로토콜 도구

포트 및 프로토콜 도구를 사용하면 단일 대시보드에서 다양한 VMware 제품 및 조합에 대한 포트 정보를 볼 수 있습니다. 오프라인 액세스를 위해 도구에서 선택한 데이터를 내보낼 수도 있습니다. 현재 지원되는 포트 및 프로토콜 도구는 다음과 같습니다.

- vSphere
- vSAN
- NSX for vSphere
- vRealize Network Insight
- vRealize Operations Manager
- vRealize Automation

이 도구는 <https://ports.vmware.com/>에서 사용할 수 있습니다.

사용자 필수 포트

보안 모범 사례로 VMware 지침에 따라 vRealize Automation 사용자 포트를 구성합니다.

필수 포트는 보안 네트워크를 통해서만 노출하십시오.

서버	포트
vRealize Automation 장치	443, 8443

관리자 필수 포트

보안 모범 사례로 VMware 지침에 따라 vRealize Automation 관리자 포트를 구성합니다.

필수 포트는 보안 네트워크를 통해서만 노출하십시오.

서버	포트
vRealize Application Services 서버	5480

vRealize Automation 장치 포트

보안 모범 사례로 VMware 권장 사항에 따라 vRealize Automation 장치에 대한 수신 및 송신 포트를 구성합니다.

수신 포트

vRealize Automation 장치에 대한 최소 필수 수신 포트를 구성합니다. 시스템 구성에 필요한 경우 선택적 포트를 구성합니다.

표 1-1. 필요한 최소 수신 포트

포트	프로토콜	설명
443	TCP	vRealize Automation 콘솔 및 API 호출에 액세스
8443	TCP	VMware Remote Console 프록시.
5480	TCP	vRealize Automation 장치 관리 인터페이스에 액세스.
5488, 5489	TCP	내부용. 업데이트를 위해 vRealize Automation 장치에서 사용됩니다.
5672	TCP	RabbitMQ 메시징.
		참고 vRealize Automation 장치 인스턴스를 클러스터하는 경우 오픈 포트 4369 및 25672를 구성해야 할 수 있습니다.
40002	TCP	vIDM 서비스에 필요합니다. 이는 HA 구성에서 추가하는 경우 기타 vRealize Automation 장치 노드에서의 트래픽을 제외하고 모든 외부 트래픽에 방화벽을 사용합니다.

필요한 경우 선택적 수신 포트를 구성합니다.

표 1-2. 선택적 수신 포트

포트	프로토콜	설명
22	TCP	(선택 사항) SSH입니다. 운영 환경에서 포트 22에서 수신하는 SSH 서비스를 사용하지 않도록 설정하고 포트 22를 닫습니다.
80	TCP	(선택 사항) 443으로 리디렉션됩니다.

송신 포트

필수 송신 포트를 구성합니다.

표 1-3. 필요한 최소 송신 포트

포트	프로토콜	설명
25,587	TCP, UDP	아웃바운드 알림 이메일 전송용 SMTP.
53	TCP, UDP	DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
110, 995	TCP, UDP	인바운드 알림 이메일 수신용 POP.
143, 993	TCP, UDP	인바운드 알림 이메일 수신용 IMAP.
443	TCP	HTTPS를 통한 Infrastructure as a Service Manager Service.

필요한 경우 선택적 송신 포트를 구성합니다.

표 1-4. 선택적 송신 포트

포트	프로토콜	설명
80	TCP	(선택 사항) 소프트웨어 업데이트를 가져오는 데 사용. 업데이트를 별도로 다운로드하고 적용할 수 있습니다.
123	TCP, UDP	(선택 사항) 호스트 시간을 사용하는 대신 NTP에 직접 연결하는 데 사용.

포트 및 프로토콜 도구

포트 및 프로토콜 도구를 사용하면 단일 대시보드에서 다양한 VMware 제품 및 조합에 대한 포트 정보를 볼 수 있습니다. 오프라인 액세스를 위해 도구에서 선택한 데이터를 내보낼 수도 있습니다. 현재 지원되는 포트 및 프로토콜 도구는 다음과 같습니다.

- vSphere
- vSAN
- NSX for vSphere
- vRealize Network Insight
- vRealize Operations Manager
- vRealize Automation

이 도구는 <https://ports.vmware.com/>에서 사용할 수 있습니다.

Infrastructure as a Service 포트

보안 모범 사례로, VMware 지침에 따라 IaaS(Infrastructure as a Service) 구성 요소의 수신 및 송신 포트를 구성합니다.

수신 포트

IaaS 구성 요소에 대해 필요한 최소 수신 포트를 구성합니다.

표 1-5. 필요한 최소 수신 포트

구성 요소	포트	프로토콜	설명
Manager Service	443	TCP	HTTPS를 통한 IaaS 구성 요소 및 vRealize Automation 장치와의 통신. 프록시 에이전트가 관리하는 모든 가상화 호스트에도 수신 트래픽을 위한 TCP 포트 443이 열려 있어야 합니다.

송신 포트

IaaS 구성 요소에 대해 필요한 최소 송신 포트를 구성합니다.

표 1-6. 필요한 최소 송신 포트

구성 요소	포트	프로토콜	설명
모두	53	TCP, UDP	DNS.
모두		TCP, UDP	DHCP.
Manager Service	443	TCP	HTTPS를 통한 vRealize Automation 장치와의 통신.
웹 사이트	443	TCP	HTTPS를 통한 Manager Service와의 통신.
Distributed Execution Manager	443	TCP	HTTPS를 통한 Manager Service와의 통신.
프록시 에이전트	443	TCP	HTTPS를 통한 Manager Service 및 가상화 호스트와의 통신
게스트 에이전트	443	TCP	HTTPS를 통한 Manager Service와의 통신.
Manager Service, 웹 사이트	1433	TCP	MSSQL.

필요한 경우 선택적 송신 포트를 구성합니다.

표 1-7. 선택적 송신 포트

구성 요소	포트	프로토콜	설명
모두	123	TCP, UDP	NTP는 선택 사항입니다.

감사 및 로깅

보안 모범 사례로 VMware 권장 사항에 따라 vRealize Automation 시스템에 감사 및 로깅을 설정합니다.

중앙 로그 호스트에 원격 로깅을 사용하면 로그 파일을 위한 안전한 저장소가 제공됩니다. 로그 파일을 중앙 호스트에 모으면 단일 도구를 사용하여 환경을 모니터링할 수 있습니다. 또한 인프라 내 여러 엔티티에 대한 전략적인 공격과 같은 위협 증거에 대해 종합적인 분석 및 검색을 수행할 수 있습니다. 안전한 중앙 집중식 로그 서버에 로깅하면 로그 번조를 방지하는 데 도움이 되고 장기적인 감사 기록도 제공됩니다.

원격 로깅 서버의 보안 확인

공격자가 호스트 시스템의 보안을 침해한 후 로그 파일을 검색하고 변조하여 자신의 흔적을 감추고 몰래 시스템에 대한 제어를 유지하려고 시도하는 경우가 종종 있습니다. 원격 로깅 서버를 적절하게 보호하면 로그 변조를 방지하는 데 도움이 됩니다.

인증된 NTP 서버 사용

모든 호스트 시스템이 적절한 지역화 오프셋을 포함한 동일한 상대 시간 소스를 사용하며, 상대 시간 소스를 협정 세계시(UTC)와 같이 합의된 시간 표준과 연관시킬 수 있는지 확인합니다. 시간 소스에 대한 올바른 접근 방식을 사용하면 적절한 로그 파일을 검토하여 침입자의 활동을 신속하게 추적하고 상관관계를 파악할 수 있습니다. 시간 설정이 정확하지 않으면 로그 파일을 검사하고 연관시켜서 공격을 감지하기 어려워지고 감사가 부정확해질 수 있습니다.

외부 시간 소스의 NTP 서버를 3개 이상 사용하거나 신뢰할 수 있는 네트워크에 3개 이상의 외부 시간 소스로부터 차례로 시간을 가져오는 로컬 NTP 서버를 여러 개 구성합니다.

vRealize Automation 참조 아키텍처

참조 아키텍처는 일반적인 vRealize Automation 배포의 구조와 구성을 설명합니다. 또한 고가용성, 확장성 및 배포 프로파일에 대한 정보를 제공합니다.

참조 아키텍처에는 다음 구성 요소에 대한 정보가 포함됩니다.

- VMware vRealize Automation
- VMware vRealize Business for Cloud

소프트웨어 요구 사항, 설치 및 지원되는 플랫폼에 대해서는 각 제품의 설명서를 참조하십시오.

초기 배포 및 구성 권장 사항

VMware 권장 사항에 따라 모든 VMware vRealize Automation 구성 요소를 배포하고 구성합니다.

vRealize Automation, vRealize Business for Cloud 및 vRealize Orchestrator를 동일한 표준 시간대로 유지하고 클럭을 동기화해야 합니다.

vRealize Automation, vRealize Business for Cloud 및 vRealize Orchestrator를 같은 관리 클러스터에 설치합니다. 사용자 워크로드 및 서버 워크로드를 분리할 수 있도록 관리 클러스터와 별개인 클러스터에 시스템을 프로비저닝합니다.

프록시 에이전트가 통신하는 끝점과 동일한 데이터 센터에 프록시 에이전트를 배포합니다. VMware에서는 원격 데이터 센터에 DEM 작업자를 배치하는 것을 권장하지 않습니다. 단, 그러한 배치를 필요로 하는 명확한 워크플로 기술 기반 사용 사례가 있는 경우는 예외로 합니다. 프록시 에이전트와 DEM 작업자를 제외한 모든 구성 요소는 동일한 데이터 센터 또는 MAN(Metro Area Network) 내의 데이터 센터에 배포해야 합니다. MAN(Metro Area Network)의 데이터 센터 간 대역폭이 1GB/s 미만이어서는 안 되며 지연 시간은 5밀리초 미만이어야 합니다.

지원 설명을 비롯한 자세한 내용은 VMware 기술 자료 문서 "분산된 다중 사이트 인스턴스에 VMware vRealize Automation 설치" ([VMware 기술 자료 문서 2134842](#))를 참조하십시오.

vRealize Automation 배포

VMware 리소스 권장 사항을 vRealize Automation 배포 계획을 위한 시작 기준으로 사용합니다.

초기 테스트 및 운영 환경으로의 배포 후에는 필요한 경우 [vRealize Automation 확장성](#)에 설명된 대로 성능 모니터링과 추가 리소스 할당을 계속합니다.

인증

vRealize Automation을 구성할 때, 사용자 인증을 위해 기본 디렉토리 관리 커넥터를 사용하거나 기존의 SAML 기반 ID 제공자를 지정하여 Single Sign-On 환경을 지원할 수 있습니다.

이중 인증이 필요한 경우 vRealize Automation은 RSA SecurID와의 통합을 지원합니다. 이 통합점이 구성될 때 사용자에게 사용자 ID와 암호를 입력하라는 메시지가 표시됩니다.

로드 밸런서 고려 사항

최소 응답 시간 또는 라운드 로빈 방식을 사용하여 vRealize Automation 장치 및 인프라 웹 서버에 대한 트래픽을 밸런싱합니다. 각 고유 세션의 이후 요청을 로드 밸런서 풀에 있는 동일한 웹 서버로 보내려면 세션 신호도 또는 고정 세션 기능을 사용합니다.

Manager Service에 대한 페일오버 관리를 위해 로드 밸런서를 사용할 수 있지만 Manager Service는 한 번에 하나만 활성화되므로 로드 밸런싱 알고리즘은 사용하지 마십시오. 또한 로드 밸런서로 페일오버를 관리할 때에는 세션 신호도를 사용하지 마십시오.

vRealize Automation 장치를 로드 밸런싱할 때에는 포트 443과 8444를 사용합니다. Infrastructure Website 및 Infrastructure Manager Service의 경우 포트 443만 로드 밸런싱해야 합니다.

다른 로드 밸런서를 사용할 수 있지만 테스트가 완료된 NSX, F5 BIG-IP 하드웨어 및 F5 BIG-IP Virtual Edition을 사용하는 것이 좋습니다.

로드 밸런서 구성에 대한 자세한 내용은 vRealize Automation 설명서를 참조하십시오.

데이터베이스 배포

vRealize Automation은 7.0 이상 릴리스에서 장치 데이터베이스를 자동으로 클러스터합니다. 모든 새로운 7.0 이상 배포에서는 내장된 장치 데이터베이스를 사용해야 합니다. 7.1 이상으로 업그레이드되는 vRealize Automation 인스턴스는 해당 외부 데이터베이스를 장치 데이터베이스로 병합해야 합니다. 업그레이드 프로세스에 대한 자세한 내용은 vRealize Automation 제품 설명서를 참조하십시오.

인프라 구성 요소의 운영 배포인 경우 전용 데이터베이스 서버를 사용하여 MSSQL(Microsoft SQL) Server 데이터베이스를 호스팅합니다. vRealize Automation에서 MSDTC(Microsoft Distributed Transaction Coordinator)를 사용하려면 데이터베이스 서버와 통신하는 시스템을 구성해야 합니다. 기본적으로 MSDTC에는 포트 135와 포트 1024 ~ 65535가 필요합니다.

기본 MSDTC 포트 변경에 대한 자세한 내용은 Microsoft 기술 자료 문서 “Microsoft DTC(Distributed Transaction Coordinator)가 방화벽을 통해 작동하도록 구성” ([Microsoft 기술 자료 문서 250367](#))을 참조하십시오.

IaaS Manager Service 호스트는 IaaS SQL Server 데이터베이스 호스트의 NETBIOS 이름을 확인할 수 있어야 합니다. NETBIOS 이름을 확인할 수 없는 경우 SQL Server NETBIOS 이름을 Manager Service 시스템 /etc/hosts 파일에 추가하고 Manager Service를 다시 시작합니다.

vRealize Automation은 Microsoft SQL Server 2016에서만 SQL AlwaysON 그룹을 지원합니다. SQL Server 2016을 설치할 때 데이터베이스를 100 모드에서 생성해야 합니다. 이전 버전의 Microsoft SQL Server를 사용하는 경우 공유 디스크가 포함된 페일오버 클러스터 인스턴스를 사용합니다. MSDTC를 사용한 SQL AlwaysOn 그룹 구성에 대한 자세한 내용은 <https://msdn.microsoft.com/ko-kr/library/ms366279.aspx> 항목을 참조하십시오.

데이터 수집 구성

기본 데이터 수집 설정은 대부분의 구현에 적절한 시작 기준을 제공합니다. 운영 환경에 배포한 후에는 데이터 수집의 성능을 지속적으로 모니터링하여 설정 조정이 필요한지 여부를 확인합니다.

프록시 에이전트

성능을 극대화하려면 에이전트가 연결되어 있는 끝점과 동일한 데이터 센터에 에이전트를 배포합니다. 에이전트를 추가로 설치하여 시스템 처리량과 동시성을 높일 수 있습니다. 분산 배포는 세계 전역에 분산되어 있는 여러 에이전트 서버를 가질 수 있습니다.

에이전트를 에이전트에 연결된 끝점과 동일한 데이터 센터에 설치하는 경우 평균적으로 데이터 수집 성능이 200% 증가하는 것을 확인할 수 있습니다. 측정된 수집 시간에는 프록시 에이전트와 Manager Service 간 데이터를 전송하는 데 걸린 시간만 포함됩니다. Manager Service가 데이터를 처리하는 데 걸리는 시간은 포함되지 않습니다.

예를 들어 현재 팰로앨토에 있는 데이터 센터에 제품을 배포하고 있고 vSphere 끝점이 팰로앨토, 보스턴 및 런던에 있다고 가정합니다. 이 구성에서, vSphere 프록시 에이전트를 각각의 끝점에 대해 팰로앨토, 보스턴 및 런던에 배포합니다. 대신 에이전트가 팰로앨토에만 배포될 경우 보스턴 및 런던의 데이터 수집 시간이 200% 증가하는 것을 볼 수 있습니다.

Distributed Execution Manager 구성

일반적으로 DEM(Distributed Execution Manager)은 Model Manager 호스트와 최대한 가깝게 배치합니다. DEM 조정자에는 항상 Model Manager에 대한 강력한 네트워크 연결이 있어야 합니다. 기본적으로 설치 관리자는 DEM 조정자를 Manager Service와 함께 배치합니다. 두 개의 DEM 조정자 인스턴스(하나 는 페일오버용)를 생성하고 기본 데이터 센터에 두 개의 DEM 작업자 인스턴스를 생성합니다.

DEM 작업자 인스턴스에서 위치별 워크플로를 실행해야 하는 경우 해당 위치에 인스턴스를 설치합니다.

관련 워크플로와 DEM에 기술을 할당하여 해당 워크플로가 항상 올바른 위치의 DEM에 의해 실행되도록 합니다. vRealize Automation 디자이너 콘솔을 사용하여 워크플로 및 DEM에 기술을 할당하는 방법에 대한 자세한 내용은 vRealize Automation 확장성 설명서를 참조하십시오.

최상의 성능을 위해서는 DEM과 에이전트를 별도의 시스템에 설치합니다. vRealize Automation 에이전트 설치에 대한 추가 정보는 [에이전트 설치](#)를 참조하십시오.

vRealize Orchestrator

모든 새 배포에 대해 내장된 vRealize Orchestrator 인스턴스를 사용합니다. 필요한 경우 기존 배포는 계속해서 외부 vRealize Orchestrator를 사용할 수 있습니다. 내장된 vRealize Orchestrator 인스턴스에 할당된 메모리를 늘리는 절차는 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2147109를 참조하십시오.

최상의 제품 성능을 위해 vRealize Orchestrator 콘텐츠를 운영 배포로 가져오기 전에 "vRealize Orchestrator 코딩 설계 가이드"에 설명된 구성 지침을 검토 및 구현합니다.

vRealize Business for Cloud 배포 고려 사항

VMware 지침에 따라 이전에 vRealize Business Standard Edition이라고 알려진 vRealize Business for Cloud을 배포합니다.

로드 밸런서 고려 사항

데이터 수집 연결에는 로드 밸런싱이 지원되지 않습니다. 자세한 내용은 [vRealize Automation 확장성](#)을 참조하십시오. vRealize Business for Cloud 장치의 사용자 인터페이스 및 API 클라이언트 연결에는 vRealize Automation 로드 밸런서를 사용할 수 있습니다.

vRealize Automation 확장성

vRealize Automation 시스템을 구성할 때에는 적용 가능한 모든 확장성 요소를 고려하십시오.

사용자

vRealize Automation 장치는 100,000명 미만의 사용자를 동기화하도록 구성됩니다. 시스템에 더 많은 사용자가 포함되어 있는 경우 vRealize Automation 디렉토리 관리에 메모리를 추가해야 할 수 있습니다. 디렉토리 관리에 메모리 추가에 대한 자세한 내용은 [디렉토리 관리에 메모리 추가](#)를 참조하십시오.

동시 프로비저닝 설정

VMware에서 vRealize Automation 7.5의 기본 설정을 평가하고 조정했습니다. 다음 기본값은 새로 설치 및 vRealize Automation 7.5로 업그레이드 모두에 적용됩니다.

기본 설정	세부 정보
ManagerService.exe.config에서 Manager Service 폴링 빈도를 10초에서 2초로 단축했습니다.	<ul style="list-style-type: none"> RepositoryWorkflowTimerCallbackMilliseconds = 2000 MachineRequestTimerCallbackMilliseconds = 2000 MachineWorkflowCreationTimerCallbackMilliseconds = 2000
폴링 간격 당 가져온 개체 수가 구성 설정으로 노출되며 10에서 100으로 증가했습니다.	<ul style="list-style-type: none"> VirtualMachineObserverQueryCount = 100
vSphere 프록시 에이전트 폴링 간격 및 작업 항목의 최대 수가 증가되었습니다.	<ul style="list-style-type: none"> workitemTimeInterval = 00:00:05 workitemRetrievalCount = 100 activeQueueSize = 100

기본적으로 vRealize Automation은 끝점당 8개의 동시 프로비저닝만 처리합니다. 이 제한을 늘리는 방법에 대한 자세한 내용은 [동시 시스템 프로비저닝 구성](#)을 참조하십시오.

Distributed Execution Manager - 작업자

모든 배포를 최소 두 개의 DEM 작업자와 함께 시작하는 것이 좋습니다. 6.x에서, 각 DEM 작업자는 동시에 15개의 워크플로를 처리할 수 있습니다. vRealize Automation 7.0 이상에서는 이 개수가 30개로 증가했습니다.

워크플로 스텝을 통해 시스템을 사용자 지정하는 경우 동시 프로비저닝할 20개의 시스템당 하나의 DEM 작업자가 있어야 합니다. 예를 들어, 100개의 동시 프로비저닝을 지원하는 시스템에는 최소한 5개의 DEM 작업자가 필요합니다.

DEM 작업자 및 확장성에 대한 자세한 내용은 [Distributed Execution Manager 성능 분석 및 조정](#) 항목을 참조하십시오.

데이터 수집 확장성

데이터 수집 완료 시간은 여러 변수 중에서도 계산 리소스 용량, 계산 리소스 또는 끝점의 시스템 수 및 네트워크 로드와 좌우됩니다. 성능은 데이터 수집 유형에 따라 서로 다른 속도로 변화합니다.

각 데이터 수집 유형에는 재정의하거나 수정할 수 있는 기본 간격이 있습니다. 인프라 관리자는 인프라 소스 끝점에 대해 수동으로 데이터 수집을 시작할 수 있습니다. 패브릭 관리자는 계산 리소스에 대해 수동으로 데이터 수집을 시작할 수 있습니다. 다음 값은 데이터 수집에 대한 기본 간격입니다.

표 1-8. 데이터 수집 기본 간격

데이터 수집 유형	기본 간격
인벤토리	24시간마다(매일)
상태	15분마다
성능	24시간마다(매일)

성능 분석 및 조정

데이터를 수집하는 리소스의 수가 증가하면 데이터 수집 완료 시간이 데이터 수집 사이의 간격보다 길어질 수 있습니다(특히 상태 데이터 수집의 경우). 계산 리소스 또는 끝점에 대한 데이터 수집을 제 시간에 완료할지 아니면 대기열에 넣을지 결정하려면 [데이터 수집] 페이지를 참조하십시오. [마지막으로 완료됨] 필드 값이 데이터 수집이 마지막으로 완료된 타임 스탬프 대신 대기열에 있음 또는 진행 중을 표시할 수 있습니다. 이 문제가 발생하는 경우 데이터 수집 사이의 간격을 늘려 데이터 수집 빈도를 줄일 수 있습니다.

또는, 에이전트당 동시 데이터 수집 제한을 늘릴 수도 있습니다. 기본적으로 vRealize Automation은 동시 데이터 수집 작업을 에이전트당 두 개로 제한하고 이 제한을 초과하는 요청을 대기열에 넣습니다. 이와 같은 제한을 통해 전반적인 성능에 영향을 미치지 않고 데이터 수집 작업을 빨리 완료할 수 있습니다. 동시 데이터 수집을 사용할 수 있는 제한을 올릴 수 있지만 그럴 경우에는 이 옵션 사용에 따른 전반적인 성능 저하 문제도 함께 고려해야 합니다.

구성된 vRealize Automation 에이전트당 제한을 늘리는 경우 이러한 실행 시간 초과 간격 중 하나 이상을 늘려야 할 수 있습니다. 데이터 수집 동시성 및 시간 초과 간격을 구성하는 방법에 대한 자세한 내용은 vRealize Automation 시스템 관리 설명서를 참조하십시오. Manager Service 데이터 수집은 CPU를 많이 사용합니다. Manager Service 호스트의 처리 능력을 높이면 전체 데이터 수집에 필요한 시간을 줄일 수 있습니다.

Amazon Elastic Compute Cloud(Amazon AWS)에 대한 데이터 수집, 특히 시스템이 여러 지역에서 동시에 데이터를 수집하고 해당 지역에서 이전에 데이터가 수집되지 않은 경우 CPU 소모가 클 수 있습니다. 이러한 데이터 수집 유형은 웹 사이트의 전반적인 성능 저하를 유발할 수 있습니다. 현저한 성능 영향이 있는 경우 Amazon AWS 인벤토리 데이터 수집의 빈도를 줄입니다.

워크플로 처리 확장성

DEM 조정자가 워크플로에 대한 전처리를 시작하는 시점부터 워크플로가 실행을 완료하는 시점까지의 평균 워크플로 처리 시간은 동시 워크플로의 수와 함께 증가합니다. 워크플로 볼륨은 시스템 요청, 일부 데이터 수집 작업을 포함한 vRealize Automation 작업량의 함수입니다.

대량의 데이터를 위한 Manager Service 구성

많은 수의 개체가 포함된 VMware vSphere 클러스터(예: 3000개 이상의 가상 시스템)를 사용해야 하는 경우 더 큰 값으로 Manager Service 구성 파일을 수정합니다. 이 설정을 수정하지 않으면 대규모 인벤토리 데이터 수집이 실패할 수 있습니다.

ManagerService.exe.config 파일에서 ProxyAgentServiceBinding 및 maxStringContentLength 설정의 기본값을 수정합니다.

절차

- 1 텍스트 편집기에서 ManagerService.exe.config 파일을 엽니다.

일반적으로 이 파일은 C:\Program Files (x86)\VMware\VCAC\Server에 상주합니다.

- 2 파일에서 binding name 및 readerQuotas 줄을 찾습니다.

```
<binding name=" ProxyAgentServiceBinding" maxReceivedMessageSize=" 13107200" >
  <readerQuotas maxStringContentLength=" 13107200" />
```

참고 이 두 줄과 문자열 binding name = "ProvisionServiceBinding"이 들어 있는 유사한 줄을 혼동하지 마십시오.

- 3 maxReceivedMessageSize 및 maxStringContentLength 특성에 할당된 숫자 값을 더 큰 값으로 바꿉니다.

최적의 크기는 나중에 VMware vSphere 클러스터에 얼마나 많은 개체를 포함할지에 따라 달라집니다. 예를 들어 테스트를 위해 이러한 숫자를 10배 늘릴 수 있습니다.

- 4 변경 사항을 저장하고 파일을 닫습니다.
- 5 vRealize Automation Manager Service를 다시 시작합니다.

Distributed Execution Manager 성능 분석 및 조정

언제라도 [Distributed Execution 상태] 페이지에서 진행 중이거나 보류 중인 워크플로의 총 수를 볼 수 있으며 [워크플로 기록] 페이지를 사용하여 지정된 워크플로를 실행하는 데 걸리는 시간을 결정할 수 있습니다.

보류 중인 워크플로의 수가 많은 경우 또는 워크플로를 완료하는 데 예상보다 시간이 더 걸리는 경우 워크플로 처리를 위해 더 많은 DEM(Distributed Execution Manager) 작업자 인스턴스를 추가합니다. 각 DEM 작업자 인스턴스는 30개의 동시 워크플로를 처리할 수 있습니다. 초과분의 워크플로는 실행을 위해 대기열에 추가됩니다.

동시에 시작하는 워크플로의 수를 최소화하기 위해 워크플로 스케줄을 조정할 수 있습니다. 예를 들어 모든 시간 기반 워크플로를 매시간의 시작 시점에 실행하는 대신 워크플로 실행 시간에 시차를 두어 워크플로가 DEM 리소스를 얻기 위해 경쟁하지 않도록 할 수 있습니다. 워크플로에 대한 자세한 내용은 vRealize Automation 확장성 설명서를 참조하십시오.

일부 워크플로, 특히 특정 사용자 지정 워크플로는 CPU를 많이 사용할 수 있습니다. DEM 작업자 시스템의 CPU 로드가 크면 DEM 시스템의 처리 능력을 높이거나 환경에 DEM 시스템을 추가하는 것을 고려하십시오.

vRealize Business for Cloud 확장성

VMware 지침에 따라 확장성을 위해 vRealize Business for Cloud 설치를 구성합니다.

vRealize Business for Cloud은 10개의 VMware vCenter Server 인스턴스에 걸쳐 있는 최대 20,000개의 가상 시스템으로 확장할 수 있습니다. 첫 번째 인벤토리 데이터 수집 동기화 시 세 개의 VMware vCenter Server 인스턴스에 걸쳐 있는 20,000개의 가상 시스템을 동기화하는 데 약 3시간이 걸립니다. VMware vCenter Server의 통계 동기화에는 20,000개의 가상 시스템에 대해 약 1시간이 걸립니다. 기본적으로, 비용 계산 작업은 매일 실행되고 20,000개의 가상 시스템에 대해 실행당 약 2시간이 걸립니다.

참고 vRealize Business for Cloud 1.0에서, 기본 가상 장치 구성은 최대 20,000개의 가상 시스템을 지원할 수 있습니다. 가상 장치의 제한을 기본 구성 이상으로 늘려도 지원 가능한 가상 시스템의 수는 증가하지 않습니다.

vRealize Automation 고가용성 구성 고려 사항

최대의 시스템 견고성이 필요한 경우 VMware 지침에 따라 고가용성을 위해 vRealize Automation 시스템을 구성합니다.

vRealize Automation 장치

vRealize Automation 장치는 장치 데이터베이스를 제외한 모든 구성 요소에 대해 액티브-액티브 고가용성을 지원합니다. 7.3 릴리스부터는 배포된 노드가 세 개이고 노드 두 개 사이에 동기식 복제가 구성되어 있으면 데이터베이스 페일오버가 자동으로 사용됩니다. vRealize Automation 장치에서는 데이터베이스 장애가 감지되면 적합한 데이터베이스 서버를 컨트롤러로 승격시킵니다. vRealize Automation 장치 관리 인터페이스 클러스터 탭에서 장치 데이터베이스를 모니터링하고 관리할 수 있습니다.

이러한 장치에 대해 고가용성을 사용하려면 장치를 로드 밸런서 아래에 배치합니다. 자세한 내용은 [로드 밸런서 구성](#) 항목을 참조하십시오. 7.0 릴리스부터 장치 데이터베이스 및 vRealize Orchestrator는 자동으로 클러스터되고 사용할 수 있습니다.

vRealize Automation 디렉토리 관리

각 vRealize Automation 장치에는 사용자 인증을 지원하는 커넥터가 포함되어 있지만 일반적으로 디렉토리 동기화를 수행하기 위한 단 하나의 커넥터만 구성되어 있습니다. 어떤 커넥터를 선택하여 동기화 커넥터로 사용하든 상관 없습니다. 디렉토리 관리 고가용성을 지원하려면 두 번째 vRealize Automation 장치에 해당하는 두 번째 커넥터를 구성해야 합니다. 이것은 ID 제공자에 연결하고 동일한 Active Directory를 가리킵니다. 이 구성을 사용하면 하나의 장치가 실패하는 경우 다른 장치가 사용자 인증 관리를 담당합니다.

고가용성 환경에서 모든 노드는 동일한 Active Directory 집합, 사용자, 인증 방법 등을 제공해야 합니다. 이러한 작업을 성공적으로 수행할 수 있는 가장 직접적인 방법은 로드 밸런서 호스트를 ID 제공자 호스트로 설정하여 ID 제공자를 클러스터로 승격시키는 것입니다. 이 구성을 사용하면 모든 인증 요청이 로드 밸런서로 전송되고 로드 밸런서는 요청을 두 커넥터 중 하나로 적절하게 전달합니다.

고가용성을 위한 디렉토리 관리 구성에 대한 자세한 내용은 [Configure Directories Management for High Availability](#)를 참조하십시오.

Infrastructure Web Server

Infrastructure Web Server 구성 요소는 액티브-액티브 고가용성을 모두 지원합니다. 이러한 구성 요소에 대해 고가용성을 사용하려면 장치를 로드 밸런서 아래에 배치합니다.

Infrastructure Manager Service

Manager Service 구성 요소는 액티브-패시브 고가용성을 지원합니다. 이 구성 요소에 대해 고가용성을 사용하려면 두 개의 Manager Service를 하나의 로드 밸런서 아래에 배치합니다. vRealize Automation 7.3 이상에서는 페일오버가 자동으로 사용됩니다.

액티브 Manager Service가 실패하면 Windows 서비스를 중지합니다(로드 밸런서 아래에서 아직 중지되지 않은 경우). 패시브 Manager Service를 사용하도록 설정하고 로드 밸런서 아래에서 Windows 서비스를 다시 시작합니다. [활성 Manager Service 설치](#) 항목을 참조하십시오.

에이전트

에이전트는 액티브-액티브 고가용성을 지원합니다. 고가용성을 위한 에이전트 구성에 대한 자세한 내용은 vRealize Automation 구성 설명서를 참조하십시오. 고가용성을 위해 대상 서비스를 확인합니다.

Distributed Execution Manager 작업자

작업자 역할로 실행 중인 DEM(Distributed Execution Manager)은 액티브-액티브 고가용성을 지원합니다. DEM 작업자 인스턴스가 실패하면 DEM 조정자가 실패를 감지하고 DEM 작업자 인스턴스가 실행 중인 워크플로를 취소합니다. DEM 작업자 인스턴스가 다시 온라인 상태가 되면 DEM 조정자가 인스턴스의 워크플로를 취소했음을 감지하고 이에 대한 실행을 중지합니다. 워크플로가 중간에 취소되는 것을 방지하려면 해당 워크플로를 취소하기 전에 DEM 작업자 인스턴스를 몇 분 동안 오프라인 상태로 둡니다.

Distributed Execution Manager Orchestrator

Orchestrator 역할로 실행 중인 DEM은 액티브-액티브 고가용성을 지원합니다. DEM 조정자가 시작되면 실행 중인 다른 DEM 조정자를 검색합니다.

- 실행 중인 DEM 조정자 인스턴스를 찾지 못한 경우 이 DEM 조정자는 기본 DEM 조정자로 실행을 시작합니다.
- 실행 중인 다른 DEM 조정자를 찾은 경우에는 운영 중단 감지를 위해 다른 기본 DEM 조정자를 모니터링합니다.
- 운영 중단이 감지되면 기본 인스턴스를 대체합니다.

이전의 기본 인스턴스가 다시 온라인 상태가 되면 다른 DEM 조정자가 기본 인스턴스로서의 자신의 역할을 대신했음을 감지하고 기본 Orchestrator 인스턴스의 실패를 모니터링합니다.

인프라 구성 요소를 위한 MSSQL Database Server

vRealize Automation은 Microsoft SQL Server 2016에서만 SQL AlwaysON 그룹을 지원합니다. SQL Server 2016을 설치할 때 데이터베이스를 100 모드에서 생성해야 합니다. 이전 버전의 Microsoft SQL Server를 사용하는 경우 공유 디스크가 포함된 파일오버 클러스터 인스턴스를 사용합니다. MSDTC를 사용한 SQL AlwaysOn 그룹 구성에 대한 자세한 내용은 Microsoft 문서 <https://msdn.microsoft.com/ko-kr/library/ms366279.aspx>를 참조하십시오.

vRealize Orchestrator

vRealize Orchestrator의 내장된 고가용성 인스턴스가 vRealize Automation 장치의 일부로 제공됩니다.

vRealize Business for Cloud 고가용성 고려 사항

vRealize Business for Cloud 장치의 VMware vSphere HA 기능을 사용합니다.

VMware ESXi 호스트에서 VMware vSphere HA 기능을 구성하려면 vCenter Server 및 호스트 관리 설명서를 참조하십시오.

vRealize Automation 하드웨어 규격 및 최대 용량

사용자 환경의 각 vRealize Automation 서버 프로파일에 필요한 구성 및 용량에 따라 적합한 구성 요소를 설치합니다.

서버 역할	구성 요소	필수 하드웨어 규격	권장 하드웨어 규격
vRealize Automation 장치	vRealize Automation 서비스, vRealize Orchestrator, vRealize Automation 장치 데이터베이스	CPU: 4 vCPU RAM: 18GB(자세한 내용은 vRealize Automation 확장성 참조) 디스크: 140GB 네트워크: 1GB/s	필수 하드웨어 규격과 동일합니다.
Infrastructure Core Server	웹 사이트, Manager Service, DEM 조정자, DEM 작업자, 프록시 에이전트	CPU: 4 vCPU RAM: 8GB 디스크: 40GB 네트워크: 1GB/s	필수 하드웨어 규격과 동일합니다.
Infrastructure Web Server	웹 사이트	CPU: 2 vCPU RAM: 8GB 디스크: 40GB 네트워크: 1GB/s	CPU: 2 vCPU RAM: 8GB 디스크: 40GB 네트워크: 1GB/s
Infrastructure Manager Server	Manager Service, DEM 조정자	CPU: 2 vCPU RAM: 8GB 디스크: 40GB 네트워크: 1GB/s	CPU: 2 vCPU* RAM: 8GB 디스크: 40GB 네트워크: 1GB/s * 100개가 넘는 동시 프로비저닝을 수행하는 경우 4 vCPU.
Infrastructure Web/Manager Server	Infrastructure Web/Manager Server	CPU: 2 vCPU RAM: 8GB 디스크: 40GB 네트워크: 1GB/s	CPU: 2 vCPU RAM: 8GB 디스크: 40GB 네트워크: 1GB/s
Infrastructure DEM Server	(하나 이상) DEM 작업자	CPU: 2 vCPU RAM: 8GB 디스크: 40GB 네트워크: DEM 작업자당 1GB/s	CPU: 2 vCPU* RAM: 8GB 디스크: 40GB 네트워크: DEM 작업자당 1GB/s * 100개가 넘는 동시 프로비저닝을 수행하는 경우 4vCPU.
Infrastructure Agent Server	(하나 이상) 프록시 에이전트	CPU: 2 vCPU RAM: 8GB 디스크: 40GB 네트워크: 1GB/s	CPU: 2 vCPU RAM: 8GB 디스크: 40GB 네트워크: 1GB/s

서버 역할	구성 요소	필수 하드웨어 규격	권장 하드웨어 규격
MSSQL 데이터베이스 서버	Infrastructure 데이터베이스	CPU: 2 vCPU RAM: 8GB 디스크: 40GB 네트워크: 1GB/s	CPU: 8 vCPU RAM: 16GB 디스크: 80GB 네트워크: 1GB/s
vRealize Business for Cloud 장치	vRealize Business for Cloud 장치 서비스 vRealize Business for Cloud 데이터베이스 서버	CPU: 2 vCPU RAM: 4GB 디스크: 50GB 네트워크: 1GB/s	필수 하드웨어 규격과 동일합니다.

vRealize Automation 권장 최대 용량

다음 리소스 용량 최대값은 vRealize Automation 대규모 배포 프로파일에 적용됩니다.

표 1-9. vRealize Automation 리소스 최대 용량

매개 변수	최대값
테넌트	100
vSphere 끝점	45* * 서버당 vCenter 에이전트 최대 25개.
계산 리소스	200
관리되는 시스템	75,000
피크 동시 요청	
상수	100
버스트	250
비즈니스 그룹	5,000(비즈니스 그룹별로 고유 사용자가 10명이고 50개가 넘는 비즈니스 그룹의 멤버인 사용자가 없음)
예약	14,000(비즈니스 그룹당 예약 3개 포함)
Blueprint	
CBP만	6,000
CBP + XaaS	8,000
카탈로그 항목	
테넌트 전체	4,000
단일 테넌트	6,000
사용자/그룹 동기화(기본 18GB 메모리 포함)	
사용자 수	95,000

표 1-9. vRealize Automation 리소스 최대 용량 (계속)

매개 변수	최대값
그룹 수	20,000(각 그룹에 사용자 4명과 중첩 수준 1개 포함)
사용자/그룹(30GB로 메모리 증가)	
사용자 수	100,000
그룹 수	750(각 그룹에 사용자 4,000명이 포함되고 각 사용자가 30개 그룹에 속함)

vRealize Automation 소규모 배포 요구 사항

vRealize Automation 소규모 배포는 10,000개 이하의 관리되는 시스템으로 구성되며 적절한 가상 시스템, 로드 밸런서 및 포트 구성이 포함됩니다. 소규모 배포는 지원되는 방식을 사용하여 중간 규모 또는 대규모 배포로 확장할 수 있는 vRealize Automation 배포의 시작 기준 역할을 합니다.

vRealize Automation을 배포할 때, 엔터프라이즈 배포 프로세스를 사용하여 별도의 Infrastructure Web 사이트 및 Manager Service 주소를 제공합니다.

지원

소규모 배포는 다음 항목을 지원할 수 있습니다.

- 10,000개의 관리되는 시스템
- 500개의 카탈로그 항목
- 10개의 동시 시스템 프로비저닝

요구 사항

소규모 배포는 적절한 구성 요소를 사용하여 구성해야 합니다.

- vRealize Automation 장치: vrava-1.ra.local
- Infrastructure Core Server: inf-1.ra.local.
- MSSQL 데이터베이스 서버: mssql.ra.local
- vRealize Business for Cloud 장치: vrb.ra.local

DNS 항목

DNS 항목	가리키는 대상
vrava.ra.local	vrava-1.ra.local
web.ra.local	inf.ra.local
manager.ra.local	inf.ra.local

인증서

이 테이블에서 사용되는 호스트 이름은 단지 예로 제시된 것입니다.

서버 역할	CN 또는 SAN
vRealize Automation 장치	SAN에 vra.va.sqa.local 및 vra.va-1.sqa.local이 포함됨
Infrastructure Core Server	SAN에 web.ra.local, managers.ra.local 및 inf-1.ra.local이 포함됨
vRealize Business for Cloud Server	CN = vrb.ra.local

포트

사용자가 특정 포트에 액세스해야 합니다. 나열된 모든 포트는 기본 포트입니다.

서버 역할	포트
vRealize Automation 장치	443, 8444. 가상 시스템 원격 콘솔에는 포트 8444가 필요합니다. vRealize Orchestrator 제어 센터에 액세스하기 위해 포트 8283이 필요합니다.

사용자에게 필요한 포트 외에 관리자가 특정 포트에 액세스해야 합니다.

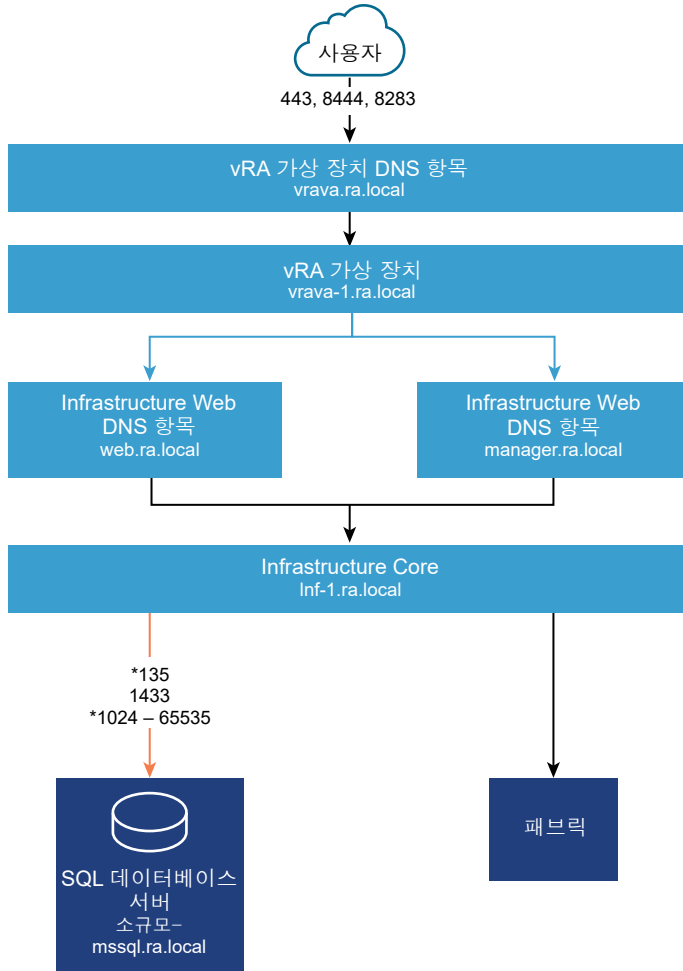
서버 역할	포트
vRealize Automation 장치	5480, 8443. 포트 8443은 고급 ID 관리 구성에 사용됩니다. VMware Identity Manager와 Active Directory 사이: 389, 636, 3268, 3269 VMware Identity Manager와 도메인 컨트롤러 사이: 88, 464, 135
vRealize Business for Cloud	5480

서버 역할	인바운드 포트	서비스/시스템 아웃바운드 포트
vRealize Automation 장치	HTTPS: 443 어댑터 구성: 8443 원격 콘솔 프록시: 8444 SSH: 22 vRealize Automation 장치 관리 인터페이스: 5480	LDAP: 389 LDAPS: 636 VMware ESXi: 902 VMware Remote Console에 대한 티켓을 가져오려면 Infrastructure Core가 vSphere 끝점 포트 443에 액세스해야 합니다. 소비자에 대한 트래픽을 프록시 처리하려면 vRealize Automation 장치가 ESXi 호스트 포트 902에 액세스해야 합니다. Infrastructure Core Server: 443 Kerberos 인증: 88 컴퓨터 개체 암호 갱신: 464
Infrastructure Core Server	HTTPS: 443 MSDTC: 135, 1024 - 65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오.	vRealize Automation 가상 장치: 443, 5480 vSphere 끝점: 443 VMware Remote Console에 대한 티켓을 가져오려면 Infrastructure Core가 vSphere 끝점 포트 443에 액세스해야 합니다. 소비자에 대한 트래픽을 프록시 처리하려면 vRealize Automation 장치가 ESXi 호스트 포트 902에 액세스해야 합니다. MSSQL: 135, 1433, 1024 - 65535 MSDTC: 135, 1024 - 65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오.

서버 역할	인바운드 포트	서비스/시스템 아웃바운드 포트
MSSQL 데이터베이스 서버	MSSQL: 1433 MSDTC: 135, 1024 - 65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오.	Infrastructure Core Server: 135, 1024 - 65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오. MSDTC: 135, 1024 - 65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오.
vRealize Business for Cloud 장치	HTTPS: 443 SSH: 22 vRealize Automation 장치 관리 인터페이스: 5480	vRealize Automation 가상 장치: 443 Infrastructure Core: 443
글로벌 카탈로그		글로벌 카탈로그: 3268, 3269

최소 설치 공간

그림 1-3. vRealize Automation 소규모 구성을 위한 최소 설치 공간

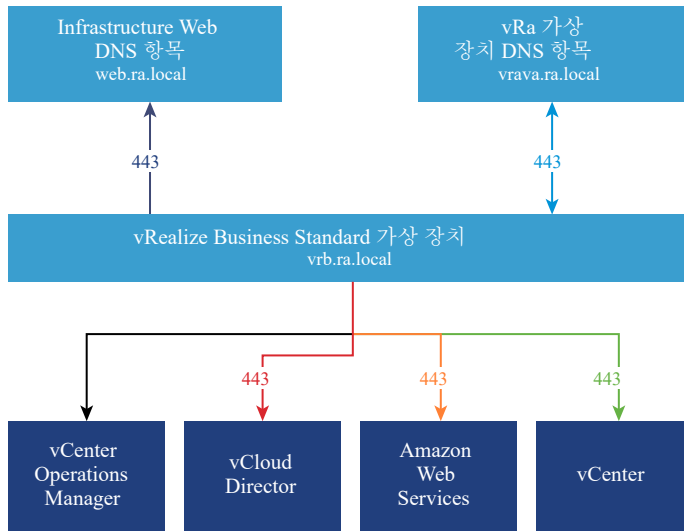


표시되지 않은 내용:
로그 수집(vRA > 클러스터 >
가상 장치:5480에서
로그 수집)이 작동하려면
모든 인프라 시스템이
모든 vRealize Appliance의
포트 5480에 액세스해야 합니다.

가상 시스템 원격 콘솔의 경우
vRealize Appliance가 VMware ESXi
포트 902에 액세스해야 하고
Infrastructure Core Server가
vSphere 끝점 포트 443에
액세스해야 합니다.

*이 범위를 줄일 수 있는 방법에 대한 정보는 데이터베이스 배포 섹션을 참조하십시오.
또한 양방향 통신이 필요합니다.

그림 1-4. vRealize Business for Cloud 소규모 구성을 위한 최소 설치 공간



vRealize Automation 중간 규모 배포 요구 사항

vRealize Automation 중간 규모 배포는 30,000개 이하의 관리되는 시스템으로 구성되며 적절한 가상 시스템, 로드 밸런서 및 포트 구성이 포함됩니다.

지원

중간 규모 배포는 다음 항목을 지원할 수 있습니다.

- 30,000개의 관리되는 시스템
- 1000개의 카탈로그 항목
- 50개의 시스템 프로비저닝

요구 사항

중간 규모 배포는 적절한 시스템 구성 요구 사항을 충족해야 합니다.

가상 장치

- vRealize Automation 장치 1: vrava-1.ra.local
- vRealize Automation 장치 2: vrava-2.ra.local
- vRealize Automation 장치 3: vrava-3.ra.local
- vRealize Business for Cloud 장치: vrb.ra.local

Windows Server 가상 시스템

- Infrastructure Web/Manager Server 1(활성 Web 또는 DEM-O, 활성 Manager): inf-1.ra.local
- Infrastructure Web/Manager Server 2(활성 Web 또는 DEM-O, 수동 Manager): inf-2.ra.local
- Infrastructure DEM Server 1: dem-1.ra.local

- Infrastructure DEM Server 2: dem-2.ra.local
- Infrastructure Agent Server 1: agent-1.ra.local
- Infrastructure Agent Server 2: agent-2.ra.local

데이터베이스 서버

- MSSQL 페일오버 클러스터 인스턴스: mssql.ra.local

로드 밸런서

- vRealize Automation 장치 로드 밸런서: med-vrava.ra.local
- Infrastructure Web 로드 밸런서: med-web.ra.local
- Infrastructure Manager Service 로드 밸런서: med-manager.ra.local

인증서

이 테이블에서 표시되는 호스트 이름은 단지 예로 제시된 것입니다.

서버 역할	CN 또는 SAN
vRealize Automation 장치	<p>SAN에는 다음 호스트 이름이 포함되어 있습니다.</p> <ul style="list-style-type: none"> ■ vrava.ra.local ■ vrava-1.ra.local ■ vrava-2.ra.local
Infrastructure Web 또는 Manager Server	<p>SAN에는 다음 호스트 이름이 포함되어 있습니다.</p> <ul style="list-style-type: none"> ■ web.ra.local ■ manager.ra.local ■ inf-1.ra.local ■ inf-2.ra.local
vRealize Business for Cloud 장치	CN = vrb.ra.local

포트

사용자가 특정 포트에 액세스해야 합니다. 나열된 모든 포트는 기본 포트입니다.

서버 역할	포트
vRealize Automation 장치 로드 밸런서	443, 8444. 가상 시스템 원격 콘솔에는 포트 8444가 필요합니다.

사용자에게 필요한 포트 외에 관리자가 특정 포트에 액세스해야 합니다.

서버 역할	포트
vRealize Automation 장치 관리 인터페이스	5480, 8443. 포트 8443은 고급 ID 관리 구성을 위한 것입니다. VMware Identity Manager와 Active Directory 사이: 389, 636, 3268, 3269 VMware Identity Manager와 도메인 컨트롤러 사이: 88, 464, 135
vRealize Appliance Orchestrator 제어 센터	8283
vRealize Business for Cloud Server	5480

다음 테이블은 애플리케이션 간 통신을 보여 줍니다.

서버 역할	인바운드 포트	서비스 또는 시스템용 아웃바운드 포트
vRealize Automation 장치	HTTPS: 어댑터 구성: 8443 원격 콘솔 프록시: 8444 Postgres: 5432 RabbitMQ: 4369, 25672, 5671, 5672 ElasticSearch: 9300, 40002, 40003 Stomp: 61613 SSH: 22	LDAP:389 LDAPS: 636 vRealize Automation 장치(기타 전체): 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003 vRealize Automation Infrastructure Web 로드 밸런서: 443 VMware ESXi: 902. 가상 시스템 원격 콘솔에 대한 티켓을 얻으려면 Infrastructure Web 또는 Manager에서 vSphere 끝점 포트 443에 액세스해야 합니다. 사용자에게 대한 콘솔 데이터를 프록시 처리하려면 vRealize Automation 장치가 ESXi 호스트 포트 902에 액세스해야 합니다. Kerberos 인증: 88 컴퓨터 개체 암호 갱신: 464
Infrastructure Web/Manager Server	HTTPS: 443 MSDTC: 135, 1024-65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오.	vRealize Automation 장치 로드 밸런서: 443 vRealize Automation Infrastructure Web 로드 밸런서: 443 vRealize Automation 장치: 5480. vSphere 끝점: 443. 가상 시스템 원격 콘솔에 대한 티켓을 얻으려면 Infrastructure Web 또는 Manager에서 vSphere 끝점 포트 443에 액세스해야 합니다. 사용자에게 대한 콘솔 데이터를 프록시 처리하려면 vRealize Automation 장치가 ESXi 호스트 포트 902에 액세스해야 합니다. MSSQL: 135, 1433, 1024-65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오.

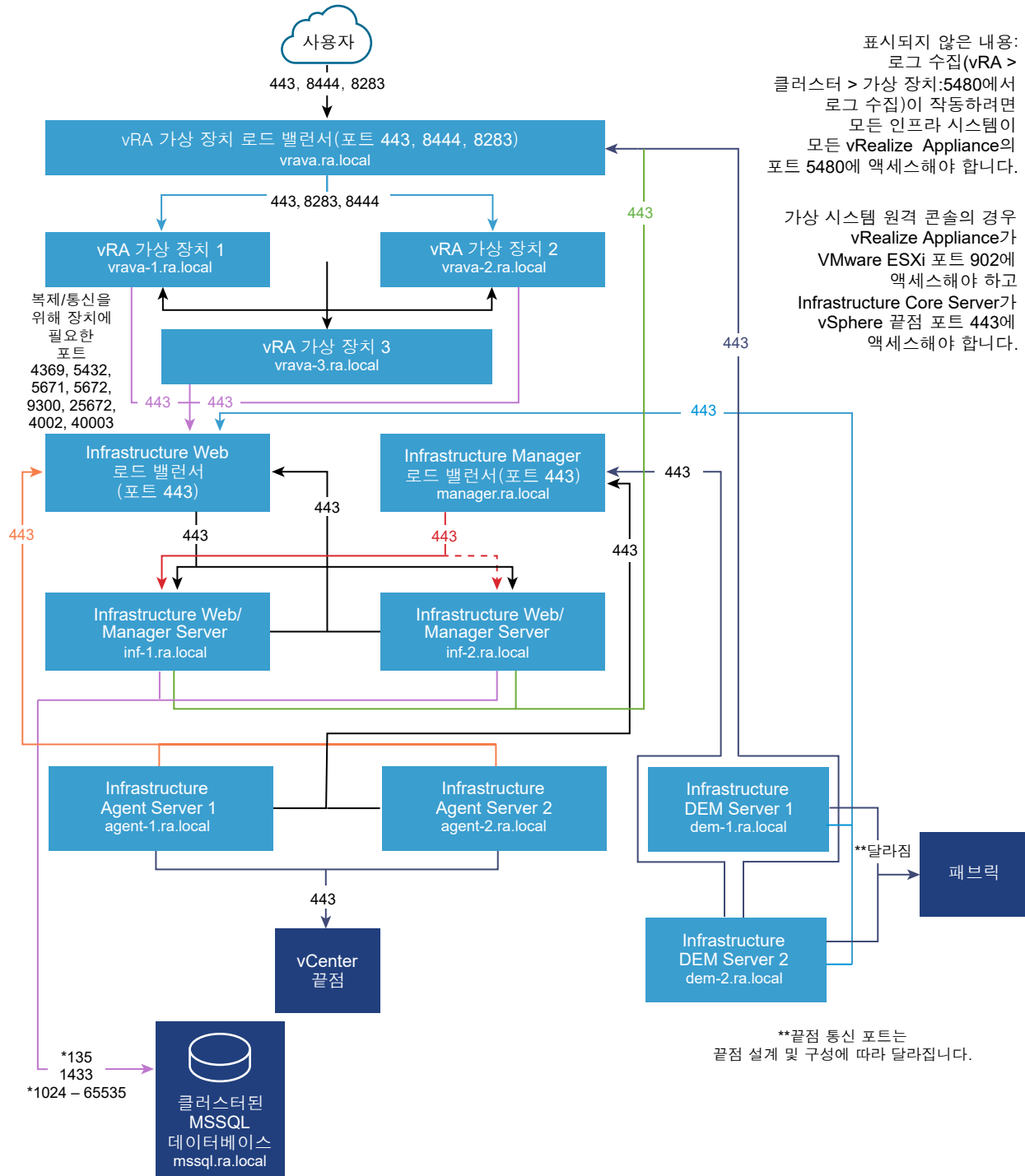
서버 역할	인바운드 포트	서비스 또는 시스템용 아웃바운드 포트
Infrastructure DEM Server	해당 없음	vRealize Automation 장치 로드 밸런서: 443 vRealize Automation Infrastructure Web 로드 밸런서: 443 vRealize Automation infrastructure Manager 로드 밸런서: 443 vRealize Automation 장치: 5480.
Infrastructure Agent Server	해당 없음	vRealize Automation Infrastructure Web 로드 밸런서: 443 vRealize Automation infrastructure Manager 로드 밸런서: 443 vRealize Automation 장치: 5480.
MSSQL 데이터베이스 서버	MSSQL: 1433 MSDTC: 135, 1024 - 65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오.	Infrastructure Web/Manager Server: 135, 1024 - 65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오.
vRealize Business for Cloud Server	HTTPS: 443 SSH: 22 vRealize Automation 장치 관리 인터페이스: 5480	vRealize Automation 장치 로드 밸런서: 443 vRealize Automation Infrastructure Web 로드 밸런서: 443
글로벌 카탈로그		글로벌 카탈로그: 3268, 3269

로드 밸런서는 다음 포트를 통해 액세스해야 합니다.

로드 밸런서	밸런싱되는 포트
vRealize Automation 장치 로드 밸런서	443, 8444
vRealize Automation Infrastructure Web 로드 밸런서	443
vRealize Automation Infrastructure Manager Service 로드 밸런서	443

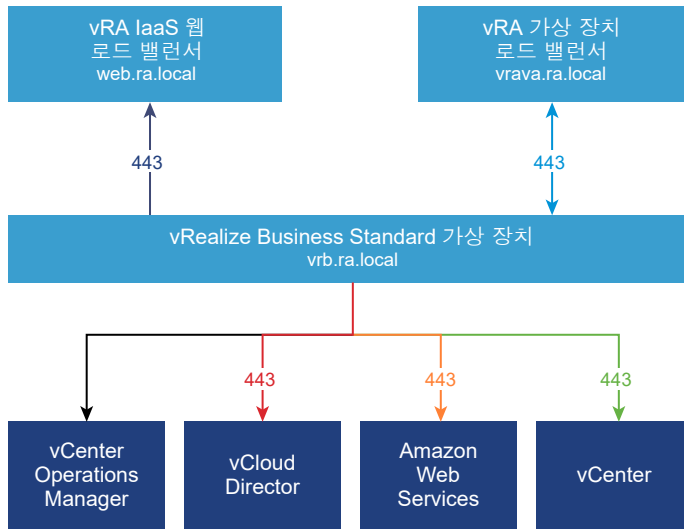
그래픽

그림 1-5. vRealize Automation 중간 규모 구성을 위한 최소 설치 공간



*이 범위를 줄일 수 있는 방법에 대한 정보는 데이터베이스 배포 섹션을 참조하십시오.
또한 양방향 통신이 필요합니다.

그림 1-6. vRealize Business for Cloud 중간 규모 배포를 위한 최소 설치 공간



vRealize Automation 대규모 배포 요구 사항

vRealize Automation 대규모 배포는 75,000개 이하의 관리되는 시스템으로 구성되며 적절한 가상 시스템, 로드 밸런서 및 포트 구성이 포함됩니다.

지원

대규모 배포는 다음 항목을 지원할 수 있습니다.

- 75,000개의 관리되는 시스템
- 2500개의 카탈로그 항목
- 100개의 동시 시스템 프로비저닝

요구 사항

대규모 배포는 적절한 시스템 구성 요구 사항을 충족해야 합니다.

가상 장치

- vRealize Automation 장치 1: vrava-1.ra.local
- vRealize Automation 장치 2: vrava-2.ra.local
- vRealize Automation 장치 2: vrava-3.ra.local
- vRealize Business for Cloud 장치: vrb.ra.local

Windows Server 가상 시스템

- Infrastructure Web Server 1: web-1.ra.local
- Infrastructure Web Server 2: web-2.ra.local
- Infrastructure Manager Server 1: manager-1.ra.local

- Infrastructure Manager Server 2: manager-2.ra.local
- Infrastructure DEM Server 1: dem-1.ra.local
- Infrastructure DEM Server 2: dem-2.ra.local
- Infrastructure Agent Server 1: agent-1.ra.local
- Infrastructure Agent Server 2: agent-2.ra.local
- 클러스터된 MSSQL 데이터베이스: mssql.ra.local

로드 밸런서

- vRealize Automation 장치 로드 밸런서: vrava.ra.local
- Infrastructure Web 로드 밸런서: web.ra.local
- Infrastructure Manager Service 로드 밸런서: manager.ra.local

인증서

이 테이블에서 사용되는 호스트 이름은 단지 예로 제시된 것입니다.

서버 역할	CN 또는 SAN
vRealize Automation 장치	<p>SAN에는 다음 호스트 이름이 포함되어 있습니다.</p> <ul style="list-style-type: none"> ■ vrava.ra.local ■ vrava-1.ra.local ■ vrava-2.ra.local
Infrastructure Web Server	<p>SAN에는 다음 호스트 이름이 포함되어 있습니다.</p> <ul style="list-style-type: none"> ■ web.ra.local ■ web-1.ra.local ■ web-2.ra.local
Infrastructure Manager Server	<p>SAN에는 다음 호스트 이름이 포함되어 있습니다.</p> <ul style="list-style-type: none"> ■ manager.ra.local ■ manager-1.ra.local ■ manager-2.ra.local
vRealize Business for Cloud 장치	CN = vrb.ra.local

포트

사용자가 특정 포트에 액세스해야 합니다. 나열된 모든 포트는 기본 포트입니다.

서버 역할	포트
vRealize Automation 장치 로드 밸런서	<p>VMware Remote Console의 경우 443, 8444, 8283 포트 8444가 필요하고, vRealize Orchestrator 제어 센터의 경우 포트 8382가 필요합니다.</p>

사용자에게 필요한 포트 외에 관리자가 특정 포트에 액세스해야 합니다.

서버 역할	포트
vRealize Automation 장치	5480, 8283, 8443. 포트 8443은 고급 ID 관리 구성에 사용됩니다. VMware Identity Manager와 Active Directory 사이: 389, 636, 3268, 3269 VMware Identity Manager와 도메인 컨트롤러 사이: 88, 464, 135
vRealize Business for Cloud 서버	5480

시스템에서 적절한 애플리케이션 간 통신을 지원해야 합니다.

서버 역할	인바운드 포트	서비스 또는 시스템용 아웃바운드 포트
vRealize Automation		
vRealize Automation 장치	HTTPS: 443 어댑터 구성: 8443 원격 콘솔 프록시: 8444 Postgres: 5432 Rabbit MQ: 4369, 25672, 5671, 5672 ElasticSearch: 9300, 40002, 40003 Stomp: 61613 SSH: 22 제어 센터: 8283	LDAP: 389 LDAPS: 636 vRealize Automation 장치: 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003. vRealize Automation Infrastructure Web 로드 밸런서: 443 VMware ESXi: 902. VMware Remote Console에 대한 티켓을 가져오려면 Infrastructure Web이 vSphere 끝점 포트 443에 액세스해야 합니다. 사용자에게 대한 콘솔 데이터를 프록시 처리하려면 vRealize Automation 장치에서 ESXi 호스트 포트 902에 액세스해야 합니다. Kerberos 인증: 88 컴퓨터 개체 암호 갱신: 464

서버 역할	인바운드 포트	서비스 또는 시스템용 아웃바운드 포트
Infrastructure Web Server	<p>HTTPS: 443</p> <p>MSDTC: 443, 1024-65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포의 "데이터베이스 배포" 섹션을 참조하십시오.</p>	<p>vRealize Automation 장치 로드 밸런서: 443</p> <p>vRealize Automation 장치 가상 장치: 5480</p> <p>vSphere 끝점: 443 VMware Remote Console에 대한 티켓을 가져오려면 Infrastructure Web이 vSphere 끝점 포트 443에 액세스해야 합니다. 사용자에게 대한 콘솔 데이터를 프록시 처리하려면 vRealize Automation 장치가 ESXi 호스트 포트 902에 액세스해야 합니다.</p> <p>MSSQL: 135, 1433, 1024-65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포의 "데이터베이스 배포" 섹션을 참조하십시오.</p>
Infrastructure Manager Server	<p>HTTPS: 443</p> <p>MSDTC: 135, 1024-65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포의 "데이터베이스 배포" 섹션을 참조하십시오.</p>	<p>vRealize Automation 장치 로드 밸런서: 443</p> <p>vRealize Automation Infrastructure Web 로드 밸런서: 443</p> <p>vRealize Automation 장치: 443, 5480</p> <p>MSSQL: 135, 1433, 1024-65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포의 "데이터베이스 배포" 섹션을 참조하십시오.</p>
Infrastructure DEM Server	해당 없음	<p>vRealize Automation 장치 로드 밸런서: 443</p> <p>vRealize Automation Infrastructure Web 로드 밸런서: 443</p> <p>vRealize Automation infrastructure Manager 로드 밸런서: 443</p> <p>vRealize Orchestrator 로드 밸런서: 8281</p> <p>vRealize Automation 장치: 5480.</p>
Infrastructure Agent Server	해당 없음	<p>vRealize Automation Infrastructure Web 로드 밸런서: 443</p> <p>vRealize Automation infrastructure Manager 로드 밸런서: 443</p> <p>vRealize Automation 장치: 5480.</p>

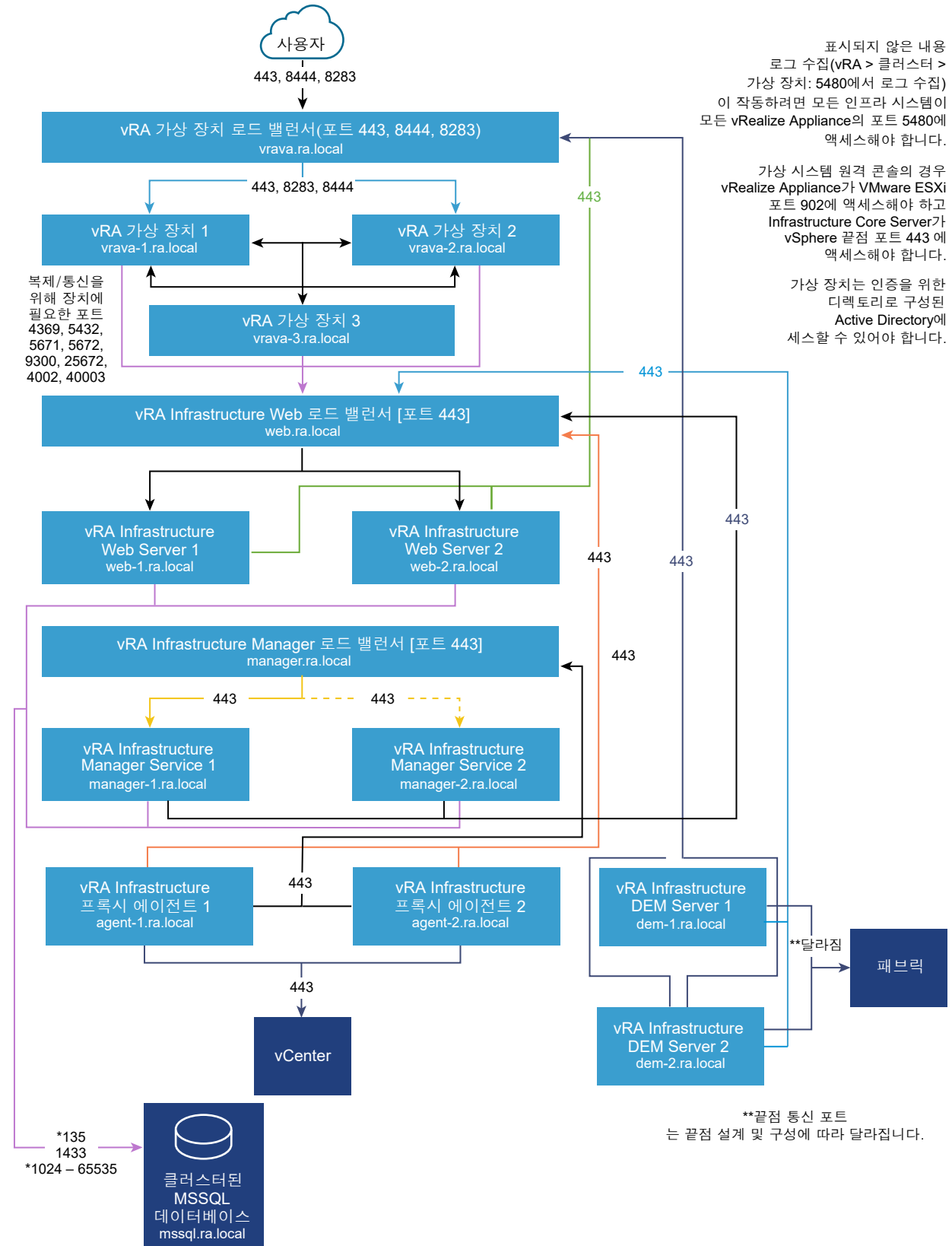
서버 역할	인바운드 포트	서비스 또는 시스템용 아웃바운드 포트
MSSQL 데이터베이스 서버	MSSQL: 1433 MSDTC: 135, 1024-65535. 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오.	Infrastructure Web Server: 135, 1024-65535 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오. Infrastructure Manager Server: 135, 1024-65535 이 범위를 좁히는 방법에 대한 자세한 내용은 vRealize Automation 배포 의 "데이터베이스 배포" 섹션을 참조하십시오.
vRealize Business for Cloud 서버	HTTPS: 443 SSH: 22 vRealize Automation 장치 관리 인터페이스: 5480	vRealize Automation 장치 로드 밸런서: 443 vRealize Automation Infrastructure Web 로드 밸런서: 443
글로벌 카탈로그		글로벌 카탈로그: 3268, 3269

로드 밸런서는 다음 포트를 통해 액세스해야 합니다.

로드 밸런서	백런싱되는 포트
vRealize Automation 장치 로드 밸런서	443, 8444
vRealize Automation Infrastructure Web 로드 밸런서	443
vRealize Automation Manager Server 로드 밸런서	443

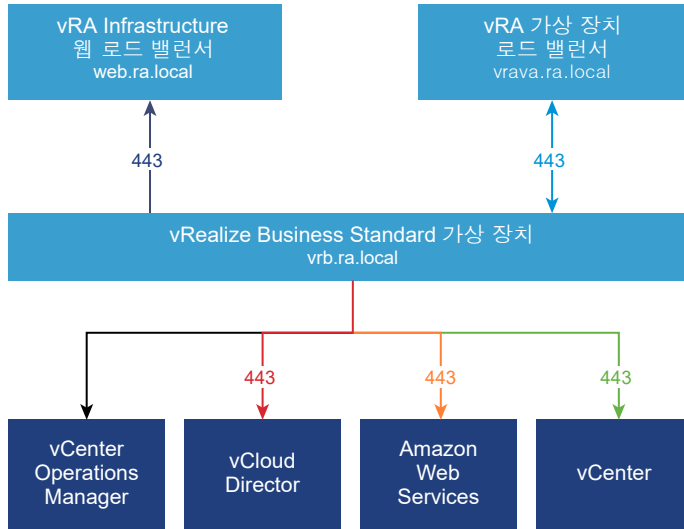
그래픽

그림 1-7. vRealize Automation 대규모 구성을 위한 최소 설치 공간



*이 범위를 줄일 수 있는 방법에 대한 정보는 데이터베이스 배포 섹션을 참조하십시오.
또한 양방향 통신이 필요합니다.

그림 1-8. vRealize Business for Cloud 대규모 구성을 위한 최소 설치 공간



vRealize Automation 다중 데이터 센터 배포

vRealize Automation은 원격 데이터 센터에서의 리소스 관리를 지원합니다.

원격 데이터 센터에서 vSphere, HyperV 또는 Xen 리소스를 관리하려면 원격 데이터 센터의 가상 시스템에 프록시 에이전트를 배포하십시오.

참고 아래의 다이어그램은 vSphere 배포를 보여 줍니다. 다른 끝점에는 추가 구성이 필요하지 않습니다.

vRealize Orchestrator 워크플로는 잠재적으로 WAN을 통해 통신하므로 "vRealize Orchestrator 코딩 설계 가이드"에 설명된 모범 사례를 확인하십시오.

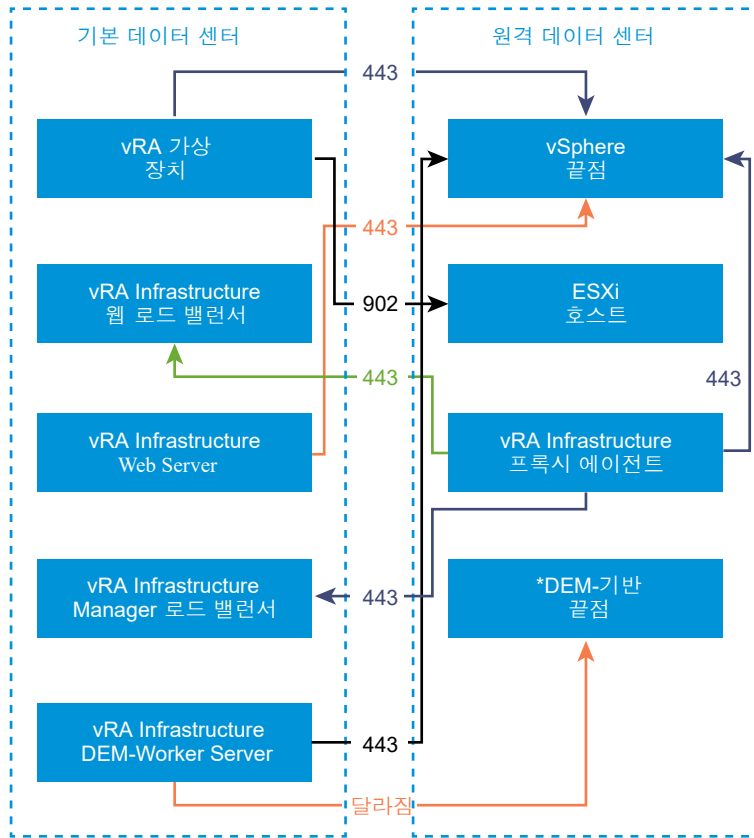
표 1-10. WAN 통신에 필요한 포트

역할	인바운드 포트	서비스/시스템 아웃바운드 포트
vRealize Automation 장치 - 포함된 vRealize Orchestrator 포함	해당 없음	vSphere 끝점: 443 ESXi 호스트: 902
vRealize Automation Infrastructure 로드 밸런서	vRealize Automation Infrastructure 프록시 에이전트: 443	해당 없음
vRealize Automation Infrastructure Web Server	해당 없음	vSphere 끝점: 443
vRealize Automation Infrastructure Manager 로드 밸런서	vRealize Automation Infrastructure 프록시 에이전트: 443	해당 없음
vRealize Automation Infrastructure DEM-Worker Server	해당 없음	끝점: **달라짐

* Manager Service 시스템 또는 다른 서버에 DEM-Worker가 설치된 경우 이러한 포트는 해당 시스템과 대상 끝점 간에 열려 있어야 합니다.

** 외부 끝점과 통신하는 데 필요한 포트는 끝점에 따라 달라집니다. 기본적으로 vSphere에 대해서는 포트 443이 사용됩니다.

그림 1-9. vRealize Automation 다중 사이트 구성



vRealize Automation 설치

제공된 지침에 따라 vRealize Automation의 새 인스턴스를 설치합니다.

vRealize Automation 설치 개요

최소한의 개념 증명 환경을 지원하거나 프로덕션 워크로드를 처리할 수 있는 다양한 크기의 분산 엔터프라이즈 구성을 지원하도록 vRealize Automation을 설치할 수 있습니다. 설치하는 대화형 또는 자동 설치일 수 있습니다.

설치한 후 설정을 사용자 지정하고 사용자에게 클라우드 서비스의 셀프 서비스 프로비저닝 및 수명 주기 관리에 대한 액세스 권한을 제공하는 테넌트를 구성하여 vRealize Automation 사용을 시작합니다.

vRealize Automation 설치 정보

각각 대화형 수준이 다른 여러 방법을 통해 vRealize Automation을 설치할 수 있습니다.

설치하려면 vRealize Automation 장치를 배포한 후 다음 옵션 중 하나를 사용하여 실제 설치를 완료합니다.

- 통합된 브라우저 기반 설치 마법사
- 별도의 브라우저 기반 장치 구성 및 IaaS 서버 구성 요소에 대한 별도의 Windows 설치
- 응답 속성 파일의 입력을 수락하는 명령줄 기반 자동 설치 관리자
- JSON 형식의 입력을 수락하는 설치 REST API

Lifecycle Manager를 사용하여 vRealize Automation을 설치할 수도 있습니다. 자세한 내용은 [vRealize Suite Lifecycle Manager 설치, 업그레이드 및 관리 가이드](#)를 참조하십시오.

vRealize Suite Lifecycle Manager는 단일 창 방식으로 설치, 구성, 업그레이드, 패치, 구성 관리, 편차 업데이트 적용 및 상태를 자동화합니다. [vRealize Suite Lifecycle Manager](#)를 설치하려면 여기를 클릭하십시오. Lifecycle Manager는 클라우드 관리 리소스의 IT 관리자에게 가치 실현 시간, 안정성 및 일관성을 향상시키면서 비즈니스 크리티컬 이니셔티브에 집중할 수 있는 기능을 제공합니다.

이 vRealize Automation 설치의 새로운 기능

vRealize Automation의 이전 버전을 설치한 경우 이 릴리스의 설치 변경 사항을 확인하십시오.

vRealize Automation 장치 관리 인터페이스가 변경되었습니다.

- [데이터베이스] 탭 기능이 [클러스터] 탭으로 이동했습니다. [데이터베이스] 탭이 제거되었으며 [클러스터] 탭이 기본 탭이 되었습니다.
- [마이그레이션] 탭이 기본 탭이 되었고 이제 vRealize Automation 및 vRealize Orchestrator 마이그레이션이 포함됩니다.
- 지원 번들 옵션이 [로그] 탭으로 이동했습니다.
- [라이센싱] 탭에서 vRealize Code Stream가 제거되었습니다.

vRealize Automation 설치 구성 요소

일반 vRealize Automation 설치에는 vRealize Automation 장치와 하나 이상의 Windows Server로 이루어진 조합으로, vRealize AutomationIaaS(Infrastructure as a Service)를 제공합니다.

vRealize Automation 장치

vRealize Automation 장치는 미리 구성된 Linux 가상 장치입니다. vRealize Automation 장치는 vSphere와 같은 기존의 가상화된 인프라에 배포하는 Open Virtualization 파일로 제공됩니다.

vRealize Automation 장치는 vRealize Automation에 중요한 여러 기능을 수행합니다.

- 장치에는 vRealize Automation 제품 포털을 호스팅하는 서버가 포함되어 있습니다. 이 포털에서는 사용자가 로그인하여 클라우드 서비스의 셀프 서비스 프로비저닝 및 관리에 액세스합니다.
- 장치는 사용자 권한 부여 및 인증을 위한 SSO(Single Sign-On)를 관리합니다.
- 장치 서버는 vRealize Automation 장치 설정을 위한 관리 인터페이스를 호스팅합니다.

- 장치에는 내부 vRealize Automation 장치 작업에 사용되는 미리 구성된 PostgreSQL 데이터베이스가 포함됩니다.

중복 장치가 포함된 대규모 배포에서는 보조 장치 데이터베이스가 고가용성을 제공하기 위한 복제본 역할을 합니다.

- 장치에는 vRealize Orchestrator의 미리 구성된 인스턴스가 포함되어 있습니다. vRealize Automation은 vRealize Orchestrator 워크플로 및 작업을 사용하여 해당 기능을 확장합니다.

vRealize Orchestrator의 포함된 인스턴스는 이제 권장됩니다. 하지만 이전 배포나 특수한 경우에는 사용자가 vRealize Automation을 대신 외부 vRealize Orchestrator에 연결할 수 있습니다.

- 장치에는 다운로드 가능한 관리 에이전트 설치 관리자가 포함되어 있습니다. vRealize Automation IaaS를 구성하는 모든 Windows Server는 관리 에이전트를 설치해야 합니다.

관리 에이전트는 IaaS Windows Server를 vRealize Automation 장치에 등록하고, IaaS 구성 요소의 설치 및 관리를 자동화하고, 지원 및 원격 분석 정보를 수집합니다.

Infrastructure as a Service

vRealize Automation IaaS는 함께 작동하여 개인, 공용 또는 하이브리드 클라우드 인프라에서 시스템을 모델링하고 프로비저닝하는 하나 이상의 Windows Server로 구성되어 있습니다.

하나 이상의 가상 또는 물리적 Windows Server에 vRealize Automation IaaS 구성 요소를 설치합니다. 설치가 완료되면 IaaS 작업이 제품 인터페이스의 [인프라] 탭 아래에 나타납니다.

IaaS는 배포 크기에 따라 함께 설치하거나 별도로 설치할 수 있는 다음과 같은 구성 요소로 이루어져 있습니다.

웹 서버

IaaS 웹 서버는 인프라 관리 및 서비스 작성을 vRealize Automation 제품 인터페이스에 제공합니다. 웹 서버 구성 요소는 Manager Service와의 통신을 통해 DEM(Distributed Execution Manager), SQL Server 데이터베이스 및 에이전트의 업데이트를 제공합니다.

Model Manager

vRealize Automation은 모델을 사용하여 외부 시스템 및 데이터베이스와의 통합을 용이하게 합니다. 모델은 DEM에서 사용하는 비즈니스 논리를 구현합니다.

Model Manager는 모델 요소의 유지, 버전 관리, 보안 및 배포를 위한 서비스와 유틸리티를 제공합니다. Model Manager는 IaaS 웹 서버 중 하나에서 호스팅되며 DEM, SQL Server 데이터베이스 및 제품 인터페이스 웹 사이트와 통신합니다.

Manager Service

Manager Service는 IaaS DEM, SQL Server 데이터베이스, 에이전트 및 SMTP 간 통신을 조정하는 Windows 서비스입니다. 또한 Manager Service는 Model Manager를 통해 웹 서버와 통신하며 모든 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정으로 실행되어야 합니다.

자동 Manager Service 페일오버를 사용하도록 설정한 경우가 아니라면 IaaS에서는 한 번에 하나의 Windows 시스템만 Manager Service를 현재 실행해야 합니다. 백업 또는 고가용성을 위해 추가적인 Manager Service 시스템을 배포할 수 있지만 수동 페일오버 방식을 사용하려면 백업 시스템이 서비스를 중지하고 수동으로 시작하도록 구성되어야 합니다.

자세한 내용은 [자동 Manager Service 페일오버 정보](#) 항목을 참조하십시오.

SQL Server 데이터베이스

IaaS는 Microsoft SQL Server 데이터베이스를 사용하여 관리하는 시스템에 대한 정보, 자체 요소 및 정책을 유지합니다. 대부분의 사용자는 설치 중에 vRealize Automation에서 데이터베이스를 생성하도록 허용합니다. 또는 사이트 정책에 따라 데이터베이스를 별도로 생성할 수 있습니다.

Distributed Execution Manager

IaaS DEM 구성 요소는 사용자 지정 모델의 비즈니스 논리를 실행하여 IaaS SQL Server 데이터베이스, 외부 데이터베이스 및 시스템과 상호 작용합니다. 일반적인 접근 방법은 액티브 Manager Service를 호스팅하는 IaaS Windows Server에 DEM을 설치하는 것이지만 필수는 아닙니다.

각 DEM 인스턴스는 작업자 또는 Orchestrator 역할을 합니다. 역할은 동일한 서버에 또는 별도의 서버에 설치할 수 있습니다.

DEM 작업자 - DEM 작업자에는 워크플로를 실행하는 하나의 기능이 있습니다. DEM 작업자가 여러 개인 경우 용량이 증가하며 여러 DEM 작업자를 동일한 서버에 설치하거나 별도의 서버에 설치할 수 있습니다.

DEM 조정자 - DEM 조정자는 다음과 같은 감독 기능을 수행합니다.

- DEM 작업자를 모니터링합니다. 작업자가 Model Manager에 대한 연결을 중지하거나 연결이 끊기면 DEM 조정자가 워크플로를 다른 DEM 작업자로 이동합니다.
- 예약된 시간에 워크플로 인스턴스를 생성하여 워크플로를 예약합니다.
- 지정된 시간에 예약된 워크플로의 인스턴스 하나만 실행되게 합니다.
- 실행에 앞서 워크플로를 사전 처리합니다. 사전 처리에는 워크플로에 대한 전제 조건 확인, 워크플로 실행 기록 생성이 포함됩니다.

액티브 DEM 조정자에는 Model Manager 호스트에 대한 강력한 네트워크 연결이 필요합니다. 별도의 서버에 여러 DEM Orchestrator가 있는 대규모 배포에서는 보조 Orchestrator가 백업 역할을 합니다. 보조 DEM Orchestrator는 활성 DEM Orchestrator를 모니터링하고 활성 DEM Orchestrator에 문제가 발생하면 이중화 및 페일오버를 제공합니다. 이러한 페일오버 구성의 경우, 액티브 DEM 조정자를 액티브 Manager Service 호스트와 함께 설치하고 보조 DEM 조정자를 대기 Manager Service 호스트와 함께 설치하는 것을 고려해 볼 수 있습니다.

에이전트

vRealize Automation IaaS는 에이전트를 사용하여 외부 시스템과 통합하고 vRealize Automation 구성 요소 간에 정보를 관리합니다.

일반적인 접근 방법은 액티브 Manager Service를 호스팅하는 IaaS Windows Server에 vRealize Automation 에이전트를 설치하는 것이지만 필수는 아닙니다. 에이전트가 여러 개인 경우 용량이 증가하며 여러 에이전트를 동일한 서버에 설치하거나 별도의 서버에 설치할 수 있습니다.

가상화 프록시 에이전트

vRealize Automation은 가상화 호스트에서 가상 시스템을 생성하고 관리합니다. 가상화 프록시 에이전트는 vSphere ESX Server, XenServer 및 Hyper-V 호스트와 여기에서 프로비저닝되는 가상 시스템 간에 명령을 보내고 데이터를 수집합니다.

가상화 프록시 에이전트에는 다음과 같은 특성이 있습니다.

- 일반적으로 자신이 관리하는 가상화 플랫폼에 대해 관리자 권한이 필요합니다.
- IaaS Manager Service와 통신합니다.
- 별도로 설치되고 고유한 구성 파일이 있습니다.

대부분의 vRealize Automation 배포에서는 vSphere 프록시 에이전트를 설치합니다. 사이트에서 사용 중인 가상화 리소스에 따라 다른 프록시 에이전트를 설치할 수도 있습니다.

가상 데스크톱 통합 에이전트

VDI(가상 데스크톱 통합) PowerShell 에이전트를 통해 vRealize Automation은 외부 가상 데스크톱 시스템과 통합할 수 있습니다. VDI 에이전트에는 외부 시스템에 대한 관리자 권한이 필요합니다.

vRealize Automation에서 프로비저닝하는 가상 시스템을 사용자가 vRealize Automation에서 XenDesktop 웹 인터페이스에 액세스하도록 허용하는 Citrix DDC(Desktop Delivery Controller)의 XenDesktop에 등록할 수 있습니다.

외부 프로비저닝 통합 에이전트

EPI(외부 프로비저닝 통합) PowerShell 에이전트를 통해 vRealize Automation은 외부 시스템을 시스템 프로비저닝 프로세스에 통합할 수 있습니다.

예를 들어 Citrix Provisioning Server와의 통합은 요청 시 디스크 스트리밍으로 시스템 프로비저닝을 지원하며, EPI 에이전트를 통해 프로비저닝 프로세스 중에 추가 단계로 Visual Basic 스크립트를 실행할 수 있습니다.

EPI 에이전트에는 자신이 상호 작용하는 외부 시스템에 대한 관리자 권한이 필요합니다.

Windows Management Instrumentation 에이전트

vRealize Automation WMI(Windows Management Instrumentation) 에이전트는 Windows 시스템 정보를 모니터링 및 제어하는 기능을 개선하고 중앙 위치에서 원격 Windows Server를 관리할 수 있게 합니다. 또한 WMI 에이전트를 통해 vRealize Automation에서 관리하는 Windows Server의 데이터를 수집할 수도 있습니다.

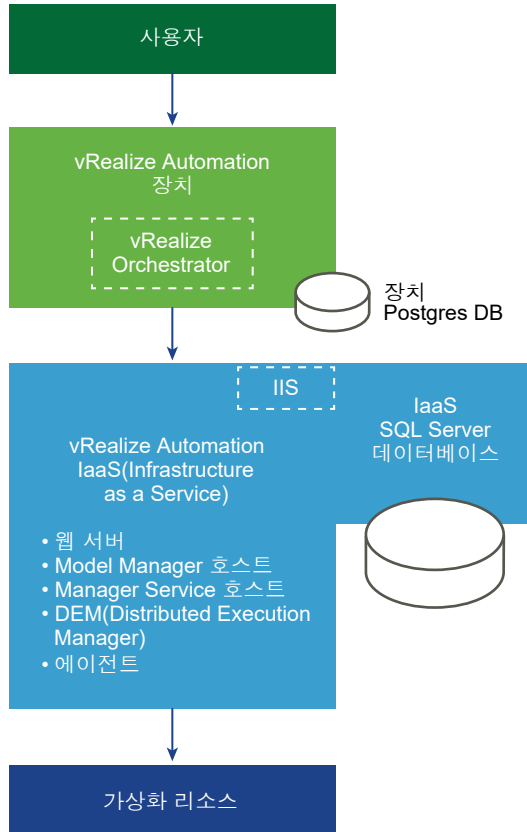
배포 유형

vRealize Automation을 개념 설명 또는 개발 작업을 위해 최소 배포로 설치하거나 중간 또는 대규모 프로덕션 작업에 적합한 분산 구성에 설치할 수 있습니다.

최소 vRealize Automation 배포

최소 배포에는 IaaS 구성 요소를 호스팅하는 하나의 Windows Server와 하나의 vRealize Automation 장치가 포함됩니다. 최소 배포에서 vRealize Automation SQL Server 데이터베이스는 IaaS 구성 요소와 동일한 IaaS Windows Server 또는 별도의 Windows Server에 있을 수 있습니다.

그림 1-10. 최소 vRealize Automation 배포

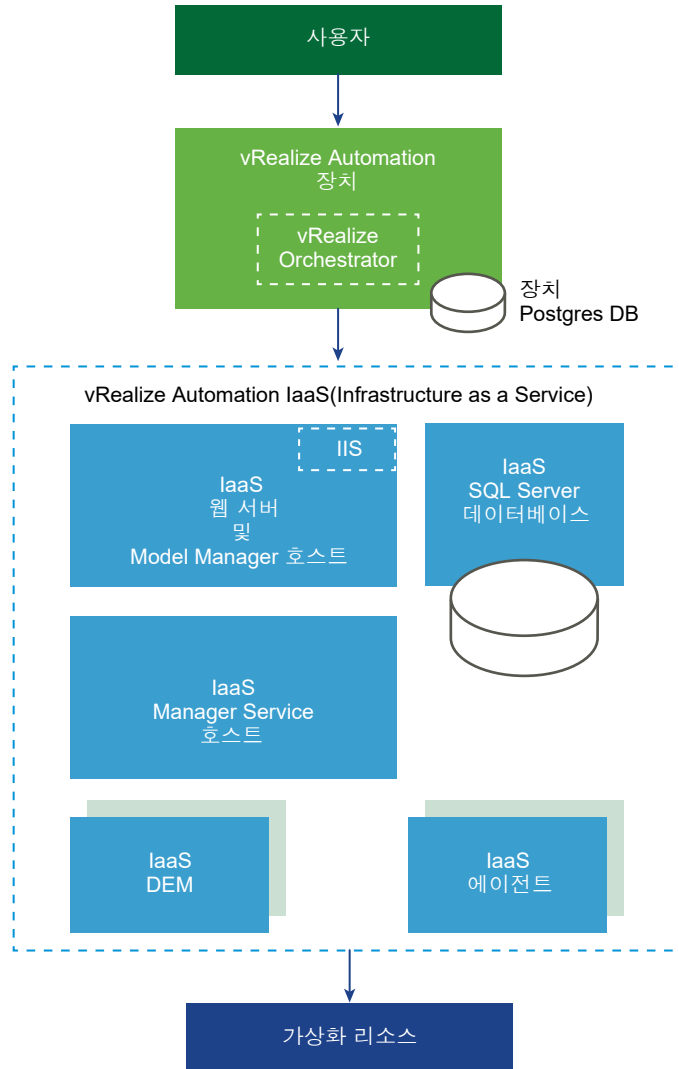


최소 배포를 엔터프라이즈 배포로 변환할 수 없습니다. 배포를 스케일 업하려면 소규모 엔터프라이즈 배포로 시작하고 여기에 구성 요소를 추가하십시오. 최소 배포로 시작하는 것은 지원되지 않습니다.

vRealize Automation 분산 배포

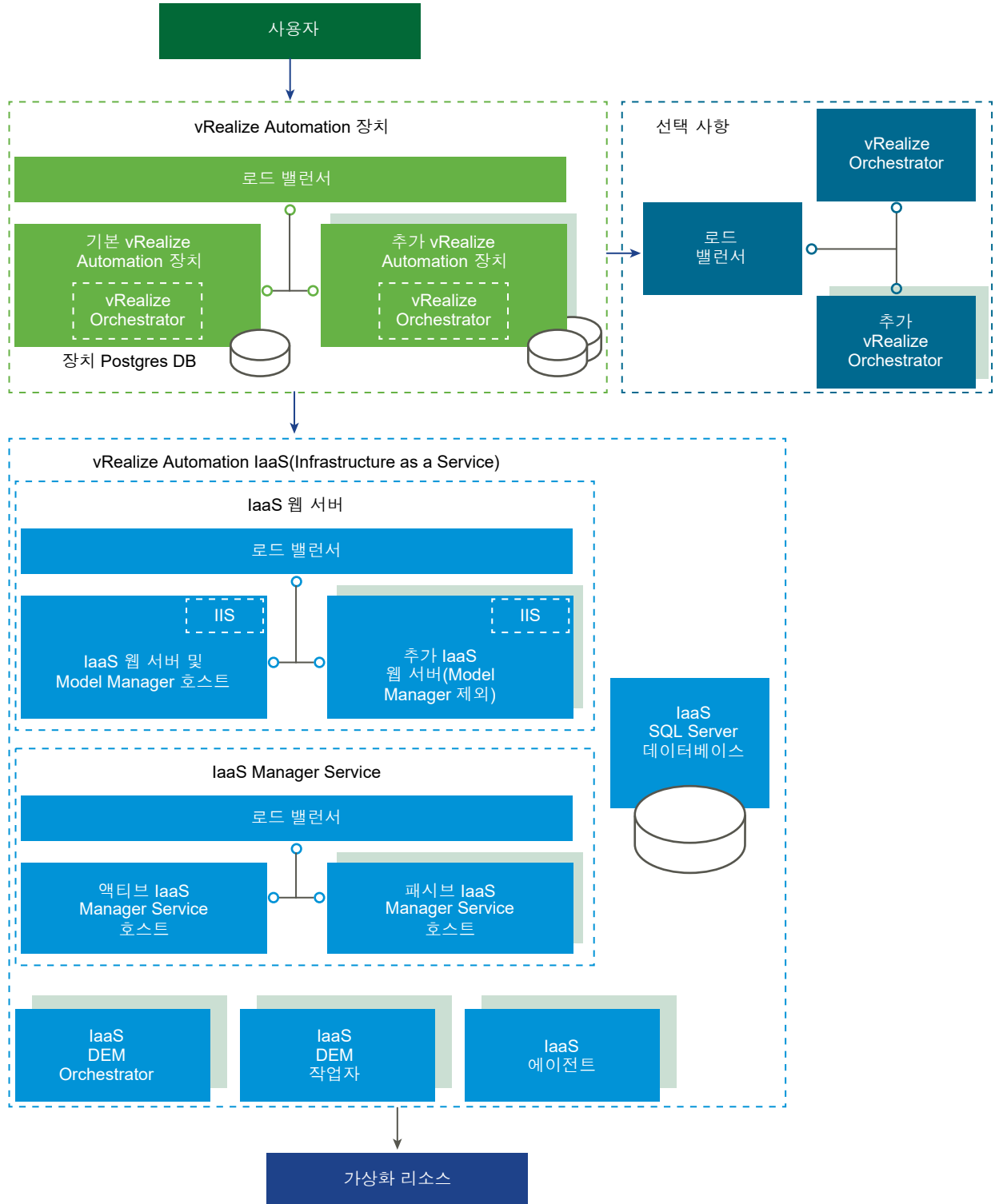
분산 엔터프라이즈 배포는 다양한 크기로 구성할 수 있습니다. 기본 분산 배포의 경우 다음 그림과 같이 별도의 Windows 서버에서 IaaS 구성 요소를 호스팅하여 vRealize Automation을 개선할 수 있습니다.

그림 1-11. vRealize Automation 분산 배포



많은 프로덕션 배포는 더 나아가 중복 장치, 중복 서버 및 더 많은 용량을 위한 로드 밸런싱을 구현합니다. 대규모 분산 배포는 확장성, 고가용성 및 재해 복구 기능을 향상시킵니다. 이제는 vRealize Orchestrator의 포함된 인스턴스가 권장되지만 이전 배포에서 vRealize Automation이 외부 vRealize Orchestrator에 연결되었을 수 있습니다.

그림 1-12. 분산 및 로드 밸런싱된 대규모 vRealize Automation 배포



확장성 및 고가용성에 대한 자세한 내용은 "vRealize Automation 참조 아키텍처" 가이드를 참조하십시오.

설치 방법 선택

통합된 vRealize Automation 설치 마법사는 vRealize Automation의 새 설치를 위한 기본 도구입니다. 또는 수동의 개별 설치 프로세스를 수행하거나 자동 설치를 수행할 수도 있습니다.

- 설치 마법사를 사용하면 최소 배포부터 로드 밸런서를 포함하거나 포함하지 않는 분산 엔터프라이즈 배포까지 빠르고 간단한 방법으로 설치할 수 있습니다. 대부분의 사용자는 설치 마법사를 실행합니다.
- vRealize Automation 배포를 확장하려는 경우 또는 설치 마법사가 어떤 이유로 중지된 경우 수동 설치 단계가 필요합니다. 수동 설치를 시작한 후에는 다시 돌아가 설치 마법사를 실행할 수 없습니다.
- 사이트 요구에 따라 자동, 명령줄 또는 API 기반 설치를 활용할 수도 있습니다.

vRealize Automation 설치 준비

기존 가상화 인프라에 vRealize Automation을 설치합니다. 설치를 시작하기 전에 특정 환경 및 시스템 요구 사항을 해결해야 합니다.

일반적 준비

vRealize Automation을 설치하기 전에 유의해야 할 몇 가지 배포 고려 사항이 있습니다.

지원되는 운영 체제 및 브라우저 버전을 비롯한 개괄적인 환경 요구 사항에 대한 자세한 내용은 [vRealize Automation 지원 매트릭스](#)를 참조하십시오.

사용자 웹 브라우저

다중 브라우저 창 및 탭은 지원되지 않습니다. vRealize Automation는 사용자별로 하나의 세션을 지원합니다.

vSphere에서 프로비저닝된 VMware Remote Console은 vRealize Automation 지원 브라우저 중 일부만 지원합니다.

타사 소프트웨어

모든 타사 소프트웨어에는 최신 벤더 패치가 적용되어 있어야 합니다. 타사 소프트웨어에는 Microsoft Windows 및 SQL Server가 포함됩니다.

시간 동기화

모든 vRealize Automation 장치 및 IaaS Windows Server는 동일한 시간 소스와 동기화되어야 합니다. 다음 원본 중 하나만 사용할 수 있습니다. 시간 소스를 혼용하지 마십시오.

- vRealize Automation 장치 호스트
- 외부 NTP(네트워크 시간 프로토콜) 서버 1개

vRealize Automation 장치 호스트를 사용하려면 ESXi 호스트에서 NTP를 실행해야 합니다. 시간 계측에 대한 자세한 내용은 [VMware 기술 자료 문서 1318](#) 항목을 참조하십시오.

설치 마법사의 [설치 사전 요구 사항] 페이지에서 시간 소스를 선택합니다.

계정 및 암호

vRealize Automation을 설치하기 전에 생성하거나 해당 설정을 계획해야 하는 몇 가지 사용자 계정과 암호가 있습니다.

IaaS 서비스 계정

IaaS는 단일 사용자 계정으로 실행해야 하는 여러 Windows 서비스를 설치합니다.

- 계정은 도메인 사용자여야 합니다.
- 계정이 도메인 관리자일 필요는 없지만 모든 IaaS Windows Server에 설치를 수행하려면 계정에 로컬 관리자 사용 권한이 있어야 합니다.
- 계정 암호에 큰따옴표(") 문자를 사용할 수 없습니다.
- IaaS Windows Server용 관리 에이전트 설치 관리자는 계정 자격 증명을 요구합니다.
- 계정에 **서비스로 로그인** 사용 권한이 있어야 Manager Service가 시작되고 로그 파일을 생성할 수 있습니다.
- 계정에 IaaS 데이터베이스에 대한 **dbo** 사용 권한이 있어야 합니다.

설치 관리자를 사용하여 데이터베이스를 생성하는 경우 설치 전에 SQL Server에 계정 로그인을 추가합니다. 설치 관리자는 데이터베이스를 만든 후 **dbo** 사용 권한을 부여합니다.

- 설치 관리자를 사용하여 데이터베이스를 생성하는 경우 설치 전에 SQL에서 계정에 **sysadmin** 역할을 추가합니다.

이미 존재하는 빈 데이터베이스를 사용하도록 선택한 경우 **sysadmin** 역할이 필요하지 않습니다.

- 사이트에서 그룹 정책 보안 설정을 사용하는 경우 계정에 대해 다음 설정을 확인합니다. **gpedit.msc** 그룹 정책 편집기를 실행하고 **컴퓨터 구성 > Windows 설정 > 보안 설정 > 로컬 정책 > 사용자 권한 할당**을 확인합니다.
 - 로컬 로그인 거부—계정을 추가하지 마십시오.
 - 로컬 로그인 허용—계정을 추가합니다.
 - 네트워크에서 이 컴퓨터 액세스 거부—계정을 추가하지 마십시오.
 - 네트워크에서 이 컴퓨터 액세스—계정을 추가합니다.

IIS 애플리케이션 풀 ID

Model Manager 웹 서비스에 대한 IIS 애플리케이션 풀 ID로 사용하는 계정에는 **일괄 작업으로 로그인** 사용 권한이 있어야 합니다.

IaaS 데이터베이스 자격 증명

vRealize Automation 설치 관리자가 데이터베이스를 생성하게 하거나 SQL Server를 사용하여 개별적으로 데이터베이스를 생성할 수 있습니다. vRealize Automation 설치 관리자가 데이터베이스를 생성하는 경우 다음과 같은 요구 사항이 적용됩니다.

- vRealize Automation 설치 관리자에서 Windows 인증을 선택한 경우 기본 IaaS 웹 서버에서 관리 에이전트를 실행하는 계정에는 데이터베이스를 생성하고 크기를 변경할 수 있도록 SQL에 sysadmin 역할이 있어야 합니다.
- vRealize Automation 설치 관리자에서 Windows 인증을 선택하지 않은 경우에도 런타임에 자격 증명이 사용되므로 기본 IaaS 웹 서버에서 관리 에이전트를 실행하는 계정에는 SQL에 sysadmin 역할이 있어야 합니다.
- 데이터베이스를 개별적으로 생성하는 경우 사용자가 제공하는 Windows 사용자 또는 SQL 사용자 자격 증명에는 해당 데이터베이스에 대한 dbo 사용 권한만 있으면 됩니다.

IaaS 데이터베이스 보안 암호

데이터베이스 보안 암호는 IaaS SQL 데이터베이스의 데이터를 보호하는 암호화 키를 생성합니다. 설치 마법사의 [IaaS 호스트] 페이지에서 보안 암호를 지정합니다.

- 각 구성 요소가 동일한 암호화 키를 갖도록 전체 설치에서 동일한 데이터베이스 보안 암호를 사용해야 합니다.
- 장애가 발생한 경우 데이터베이스를 복원하거나 초기 설치 후에 구성 요소를 추가하려면 암호가 필요하므로 암호를 기록합니다.
- 데이터베이스 보안 암호에는 큰따옴표(") 문자를 사용할 수 없습니다. 이러한 암호는 생성할 수는 있지만 설치 실패의 원인이 됩니다.

vSphere 끝점

vSphere 끝점에 프로비저닝하려는 경우 대상에서 작업을 수행할 수 있는 충분한 사용 권한이 있는 도메인 또는 로컬 계정이 필요합니다. 또한 계정에 vRealize Orchestrator에 구성된 적절한 수준의 사용 권한이 필요합니다.

vRealize Automation 관리자 암호

설치 후 vRealize Automation 관리자 암호를 사용하여 기본 테넌트에 로그인합니다. 설치 마법사의 [Single Sign-On] 페이지에서 관리자 암호를 지정합니다.

vRealize Automation 관리자 암호에는 후행 등호(=) 문자를 사용할 수 없습니다. 이러한 암호는 생성은 가능하지만 나중에 끝점을 저장하는 등의 작업을 수행할 때 오류의 원인이 됩니다.

호스트 이름 및 IP 주소

vRealize Automation을 사용하려면 특정 요구 사항에 따라 설치 환경에서 호스트의 이름을 지정해야 합니다.

- 설치 환경의 모든 vRealize Automation 시스템이 FQDN(정규화된 도메인 이름)으로 서로를 확인할 수 있어야 합니다.

설치를 수행하는 동안 vRealize Automation 시스템을 식별 또는 선택할 때 항상 완전한 FQDN을 입력합니다. IP 주소 또는 짧은 시스템 이름을 입력하지 마십시오.

- FQDN 요구 사항 외에 Model Manager Web Service, Manager Service 및 Microsoft SQL Server 데이터베이스를 호스팅하는 Windows 시스템은 WINS(Windows 인터넷 이름 서비스) 이름으로 서버를 확인할 수 있어야 합니다.

이러한 짧은 WINS 호스트 이름을 확인하려면 DNS(도메인 이름 시스템)를 구성합니다.

- vRealize Automation 시스템 이름이 문자(a-z, A-Z)로 시작하고, 문자 또는 숫자(0-9)로 끝나며, 중간에는 문자, 숫자 또는 하이픈(-)만 사용되도록 도메인 및 시스템 이름 지정에 대한 계획을 미리 세웁니다. 밑줄 문자(_)는 호스트 이름 또는 FQDN에 포함되어서는 안 됩니다.

허용 가능한 이름에 대한 자세한 내용은 Internet Engineering Task Force에서 호스트 이름 규격을 검토하십시오. www.ietf.org를 참조하십시오.

- 일반적으로 vRealize Automation 시스템에 대해 계획한 호스트 이름 및 FQDN을 유지해야 합니다. 호스트 이름을 변경하는 것이 항상 가능한 것은 아닙니다. 변경이 가능해도 절차가 복잡할 수 있습니다.
- 모든 vRealize Automation 장치 및 IaaS Windows Server에 대해 정적 IP 주소를 예약하고 사용하는 것이 좋습니다. vRealize Automation은 DHCP를 지원하지만 운영 환경과 같은 장기 배포에서는 정적 IP 주소를 사용하는 것이 좋습니다.
 - OVF 또는 OVA 배포 중 vRealize Automation 장치에 IP 주소를 적용합니다.
 - IaaS Windows Server의 경우 일반적인 운영 체제 프로세스를 따릅니다. vRealize Automation IaaS를 설치하기 전에 IP 주소를 설정합니다.

지연 시간 및 대역폭

vRealize Automation은 다중 사이트 분산 설치를 지원하지만 이 기능을 사용하려면 최소한의 데이터 전송 속도 및 볼륨 사전 요구 사항을 충족해야 합니다.

vRealize Automation은 네트워크 지연 시간이 5밀리초 이하이고 대역폭이 1GB 이상인 환경에 다음 구성 요소가 필요합니다.

- vRealize Automation 장치
- IaaS 웹 서버
- IaaS Model Manager 호스트
- IaaS Manager Service 호스트
- IaaS SQL Server 데이터베이스
- IaaS DEM Orchestrator

다음 구성 요소는 지연 시간이 더 긴 사이트에서도 작동할 수 있지만 이는 권장되지 않습니다.

- IaaS DEM 작업자

통신 대상 끝점이 있는 사이트에 다음 구성 요소를 설치할 수 있습니다.

■ IaaS 프록시 에이전트

vRealize Automation 장치

대부분의 vRealize Automation 장치 요구 사항은 배포하는 OVF 또는 OVA에 미리 구성되어 있습니다. 독립형, 마스터 또는 복제 vRealize Automation 장치에 동일한 요구 사항이 적용됩니다.

배포가 가능한 최소 가상 시스템 하드웨어는 버전 7 또는 ESX/ESXi 4.x 이상입니다. [VMware 기술 자료 문서 2007240](#)의 내용을 참조하십시오. 하드웨어 리소스 요구 때문에 VMware Workstation에 배포하지 마십시오.

VMware는 장치 수정 또는 사용자 지정을 지원하지 않습니다. 바이러스 백신 소프트웨어를 포함하여 패키지나 사용자 지정 스크립트를 추가, 제거 또는 업데이트하지 마십시오.

배포 후 Active Directory 요구 사항을 충족하기 위해 vSphere를 사용하여 vRealize Automation 장치 하드웨어 설정을 조정할 수 있습니다. 다음 테이블을 참조하십시오.

표 1-11. Active Directory에 대한 vRealize Automation 장치 하드웨어 요구 사항

소형 Active Directory용 vRealize Automation 장치	대형 Active Directory용 vRealize Automation 장치
<ul style="list-style-type: none"> ■ CPU 4개 ■ 18GB 메모리 ■ 60GB 디스크 스토리지 	<ul style="list-style-type: none"> ■ CPU 4개 ■ 22GB 메모리 ■ 60GB 디스크 스토리지

소형 Active Directory에는 OU(조직 구성 단위)에 ID 저장소 구성에서 동기화될 최대 25,000명의 사용자가 있습니다. 대형 Active Directory에는 OU에 25,000명 이상의 사용자가 있습니다.

vRealize Automation 장치 포트

vRealize Automation 장치의 포트는 일반적으로 배포하는 OVF 또는 OVA에 미리 구성되어 있습니다.

다음은 vRealize Automation 장치가 사용하는 포트입니다.

표 1-12. 수신 포트

포트	프로토콜	설명
22	TCP	선택 사항. SSH 세션에 대한 액세스.
80	TCP	선택 사항. 443으로 리디렉션됨
88	TCP(UDP 선택 사항)	외부 모바일 디바이스에서의 클라우드 KDC Kerberos 인증.
443	TCP	vRealize Automation 콘솔 및 API 호출에 액세스 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 다운로드하는 시스템에 대한 액세스. 로드 밸런서, 브라우저에 대한 액세스.
4369, 5671, 5672, 25672	TCP	RabbitMQ 메시징.

표 1-12. 수신 포트 (계속)

포트	프로토콜	설명
5480	TCP	가상 장치 관리 인터페이스에 액세스. 관리 에이전트가 사용.
5488, 5489	TCP	업데이트를 위해 vRealize Automation 장치가 내부적으로 사용.
8230, 8280, 8281, 8283	TCP	내부 vRealize Orchestrator 인스턴스.
8443	TCP	브라우저에 대한 액세스. HTTPS를 통한 Identity Manager 관리자 포트.
8444	TCP	vSphere VMware Remote Console 연결을 위한 콘솔 프록시 통신.
8494	TCP	컨테이너 서비스 클러스터 동기화
9300 – 9400	TCP	Identity Manager 감사에 대한 액세스.
54328	UDP	
40002, 40003	TCP	vIDM 클러스터 동기화
8090, 8092	TCP	상태 서비스가 vRA 노드 간에 연결하는 데 사용됨

표 1-13. 송신 포트

포트	프로토콜	설명
25, 587	TCP, UDP	아웃바운드 알림 이메일 전송용 SMTP.
53	TCP, UDP	DNS 서버.
67, 68, 546, 547	TCP, UDP	DHCP.
80	TCP	선택 사항. 소프트웨어 업데이트 가져오기용. 업데이트를 개별적으로 다운로드하여 적용할 수 있음
88, 464, 135	TCP, UDP	도메인 컨트롤러.
110, 995	TCP, UDP	인바운드 알림 이메일 수신용 POP.
143, 993	TCP, UDP	인바운드 알림 이메일 수신용 IMAP.
123	TCP, UDP	선택 사항. 호스트 시간을 사용하는 대신 NTP에 직접 연결하는 데 사용
389	TCP	View 연결 서버에 대한 액세스.
389, 636, 3268, 3269	TCP	Active Directory. 기본 포트가 표시되지만 구성 가능.
443	TCP	HTTPS를 통한 IaaS Manager Service 및 인프라 끝점 호스트와의 통신. HTTPS를 통한 vRealize Automation 소프트웨어 서비스와의 통신. Identity Manager 업그레이드 서버에 대한 액세스.

표 1-13. 송신 포트 (계속)

포트	프로토콜	설명
		View 연결 서버에 대한 액세스.
445	TCP	Identity Manager의 ThinApp 저장소에 대한 액세스.
902	TCP	ESXi 네트워크 파일 복사 작업 및 VMware Remote Console 연결.
5050	TCP	선택 사항. vRealize Business for Cloud와의 통신용.
5432	TCP, UDP	선택 사항. 다른 장치 PostgreSQL 데이터베이스와의 통신에 필요.
5500	TCP	RSA SecurID 시스템. 기본 포트가 표시되지만 구성 가능.
8281	TCP	선택 사항. 외부 vRealize Orchestrator 인스턴스와의 통신용.
8494	TCP	컨테이너 서비스 클러스터 동기화
9300 – 9400	TCP	Identity Manager 감사에 대한 액세스.
54328	UDP	
40002, 40003	TCP	vIDM 클러스터 동기화

기타 포트는 외부 시스템과 통신하는 특정 vRealize Orchestrator 플러그인에서 필요로 할 수 있습니다. 자세한 내용은 vRealize Orchestrator 플러그인에 대한 설명서를 참조하십시오.

IaaS Windows Server

IaaS 구성 요소를 호스팅하는 모든 Windows Server는 특정 요구 사항을 충족해야 합니다. vRealize Automation 설치 마법사 또는 표준 Windows 기반 설치 관리자를 실행하기 전에 요구 사항을 해결합니다.

중요 설치하면 Windows 방화벽이 사용되지 않도록 설정됩니다. 사이트 정책에 Windows 방화벽이 필요한 경우 설치 후 다시 사용하도록 설정하고 IaaS Windows Server 포트를 개별적으로 엽니다. [IaaS Windows Server 포트](#)의 내용을 참조하십시오.

- 모든 IaaS Windows Server를 동일한 도메인에 배치합니다. 작업 그룹을 사용하지 마십시오.
- 각 서버에는 최소한 다음과 같은 하드웨어가 필요합니다.
 - CPU 2개
 - 8GB 메모리
 - 40 GB 디스크 스토리지

IaaS 구성 요소와 함께 SQL 데이터베이스를 호스팅하는 서버에는 추가 하드웨어가 필요할 수 있습니다.

- IaaS Windows Server와 SQL Server 데이터베이스 호스트는 NETBIOS 이름으로 서로를 확인할 수 있어야 합니다. 필요한 경우 각 IaaS Windows Server 및 SQL Server 데이터베이스 호스트의 `/etc/hosts` 파일에 NETBIOS 이름을 추가하고 시스템을 다시 시작합니다.
- 하드웨어 리소스 요구 때문에 VMware Workstation에 배포하지 마십시오.
- Microsoft .NET Framework 3.5를 설치합니다.
- Microsoft .NET Framework 4.5.2 이상을 설치합니다.

모든 vRealize Automation 장치에서 .NET의 복사본을 사용할 수 있습니다.

<https://vrealize-automation-appliance-FQDN:5480/installer>

Internet Explorer를 사용하여 다운로드하는 경우 보안 강화 구성이 사용되지 않도록 설정되었는지 확인합니다. Windows Server에서 `res://iesetup.dll/SoftAdmin.htm`으로 이동합니다.

- 사용 중인 Windows 버전에 따라 Microsoft PowerShell 3.0 또는 4.0을 설치합니다.
일부 vRealize Automation 업그레이드 또는 마이그레이션의 경우 현재 실행 중인 PowerShell 버전 외에 이전 버전 또는 새로운 버전의 PowerShell이 필요할 수 있습니다.
- 최소 배포보다 큰 배포의 경우 IaaS Windows 서버를 영어 로케일로 설정합니다.
- 동일한 Windows Server에 둘 이상의 IaaS 구성 요소를 설치하는 경우 동일한 설치 폴더에 설치하는 것을 계획하십시오. 다른 경로를 사용하지 마십시오.
- IaaS 서버는 일부 Windows 서버에서 기본적으로 사용하도록 설정되는 TLS를 인증에 사용합니다.
일부 사이트에서는 보안상의 이유로 TLS를 사용하지 않도록 설정하지만 하나 이상의 TLS 프로토콜은 사용하도록 설정해야 합니다. 이 vRealize Automation 버전은 TLS 1.2를 지원합니다.
- DTC(Distributed Transaction Coordinator) 서비스를 사용하도록 설정합니다. IaaS는 데이터베이스 트랜잭션 및 워크플로 생성과 같은 작업에 DTC를 사용합니다.

참고 IaaS Windows Server를 만들기 위해 시스템을 복제하는 경우 복제 후 복제본에 DTC를 설치합니다. DTC가 이미 있는 시스템을 복제하는 경우에는 고유한 식별자가 복제본에 복사되므로 통신에 실패하게 됩니다. [Manager Service 통신의 오류](#) 항목을 참조하십시오.

IaaS와 분리되어 있는 경우 SQL 데이터베이스를 호스팅하는 서버에도 DTC를 사용하도록 설정합니다. DTC 지원에 대한 자세한 내용은 [VMware 기술 자료 문서 2038943](#) 항목을 참조하십시오.

- 보조 로그인 서비스가 실행 중인지 확인합니다. 원하는 경우 설치가 완료된 이후 서비스를 중지할 수 있습니다.

IaaS Windows Server 포트

vRealize Automation 설치 전에 IaaS Windows Server에서 포트를 구성해야 합니다.

다음 테이블에 따라 모든 IaaS Windows Server 간에서 포트를 엽니다. IaaS와 별도로 SQL 데이터베이스를 호스팅하는 경우 해당 서버를 포함합니다. 또는, 사이트 정책에서 허용하는 경우 IaaS Windows Server 및 SQL Server 간에 방화벽이 사용되지 않도록 설정할 수 있습니다.

표 1-14. 수신 포트

포트	프로토콜	구성 요소	설명
443	TCP	Manager Service	HTTPS를 통한 IaaS 구성 요소 및 vRealize Automation 장치와의 통신
443	TCP	vRealize Automation 장치	HTTPS를 통한 IaaS 구성 요소 및 vRealize Automation 장치와의 통신
443	TCP	인프라 끝점 호스트	HTTPS를 통한 IaaS 구성 요소 및 vRealize Automation 장치와의 통신. 일반적으로, 443이 가상 및 클라우드 인프라 끝점 호스트의 기본 통신 포트이지만 인프라 호스트가 제공하는 설명서를 참조하여 기본 포트 및 필수 포트의 전체 목록을 확인하십시오.
443	TCP	게스트 에이전트 소프트웨어 부트스트랩 에이전트	HTTPS를 통한 Manager Service와의 통신
443	TCP	DEM 작업자	NSX Manager와의 통신
1433	TCP	SQL Server 인스턴스	MSSQL

표 1-15. 송신 포트

포트	프로토콜	구성 요소	설명
53	TCP, UDP	모두	DNS
67, 68, 546, 547	TCP, UDP	모두	DHCP
123	TCP, UDP	모두	선택 사항. NTP
443	TCP	Manager Service	HTTPS를 통한 vRealize Automation 장치와의 통신
443	TCP	Distributed Execution Manager	HTTPS를 통한 Manager Service와의 통신
443	TCP	프록시 에이전트	HTTPS를 통한 Manager Service 및 인프라 끝점 호스트와의 통신
443	TCP	관리 에이전트	vRealize Automation 장치와의 통신
443	TCP	게스트 에이전트 소프트웨어 부트스트랩 에이전트	HTTPS를 통한 Manager Service와의 통신
1433	TCP	Manager Service 웹 사이트	MSSQL
5480	TCP	모두	vRealize Automation 장치와의 통신.

또한 모든 서버 간에서 DTC를 사용하도록 설정하기 때문에 DTC에는 TCP를 통한 포트 135와 1024~65535 사이의 무작위 포트가 필요합니다. 필수 구성 요소 검사기는 DTC가 실행 중이고 필요한 포트가 열려 있는지 검증합니다.

IaaS 웹 서버

웹 구성 요소를 호스팅하는 Windows Server는 모든 IaaS Windows Server의 요구 사항과 더불어 다음과 같은 추가 요구 사항을 충족해야 합니다.

웹 구성 요소가 Model Manager를 호스팅하는지 여부에 관계없이 요구 사항은 동일합니다.

- Java를 구성합니다.

- 64비트 Java 1.8 업데이트 191을 설치합니다. 32비트를 사용하지 마십시오.

JRE면 충분합니다. 전체 JDK는 필요하지 않습니다.

- JAVA_HOME 환경 변수를 Java 설치 폴더로 설정합니다.

- %JAVA_HOME%\bin\java.exe를 사용할 수 있는지 확인합니다.

- 다음 테이블에 따라 IIS(인터넷 정보 서비스)를 구성합니다.

Windows 2008 변형용 IIS 7.5, Windows 2012용 IIS 8, Windows 2012 R2용 IIS 8.5 및 Windows 2016용 IIS 10이 필요합니다.

구성 설정 외에 IIS에서 추가 웹 사이트를 호스팅하지 마십시오. vRealize Automation은 할당되지 않은 모든 IP 주소에 통신 포트에 대한 바인딩을 설정하기 때문에 추가 바인딩이 불가능합니다. 기본 vRealize Automation 통신 포트는 443입니다.

표 1-16. IaaS 인터넷 정보 서비스

IIS 구성 요소	설정
IIS(인터넷 정보 서비스) 역할	<ul style="list-style-type: none"> ■ Windows 인증 ■ 정적 콘텐츠 ■ 기본 문서 ■ ASP.NET 3.5 및 ASP.NET 4.5 ■ ISAPI 확장 ■ ISAPI 필터
IIS Windows 프로세스 활성화 서비스 역할	<ul style="list-style-type: none"> ■ 구성 API ■ 네트워크 환경 ■ 프로세스 모델 ■ WCF 활성화(Windows 2008 변형만 해당) ■ HTTP 활성화 ■ 비HTTP 활성화(Windows 2008 변형만 해당) <p>(Windows 2012 변형: 기능 > .Net Framework 3.5 기능 > 비HTTP 활성화로 이동)</p>
IIS 인증 설정	<p>다음 비기본 항목을 설정합니다.</p> <ul style="list-style-type: none"> ■ Windows 인증 사용 ■ 익명 인증 사용 안 함 <p>다음 기본값을 변경하지 마십시오.</p> <ul style="list-style-type: none"> ■ 제공자 협상 사용 ■ NTLM 제공자 사용 ■ Windows 인증 커널 모드 사용 ■ Windows 인증 확장된 보호 사용 안 함 ■ SHA512를 사용하는 인증서의 경우, Windows 2012 변형에서 TLS1.2를 사용하지 않도록 설정해야 함

IaaS Manager Service 호스트

Manager Service 구성 요소를 호스팅하는 Windows Server는 모든 IaaS Windows Server에 대한 요구 사항 외에 추가적인 요구 사항을 충족해야 합니다.

Manager Service 호스트와 DEM 호스트 간에는 방화벽이 존재할 수 없습니다. 포트 정보는 [IaaS Windows Server 포트](#) 항목을 참조하십시오.

Manager Service 호스트가 기본이든 백업이든 요구 사항은 동일합니다.

IaaS SQL Server 호스트

IaaS SQL 데이터베이스를 호스팅하는 Windows Server는 특정 요구 사항을 충족해야 합니다.

SQL Server는 IaaS Windows Server 중 하나 또는 별도의 호스트에 상주할 수 있습니다. IaaS 구성 요소와 함께 호스팅되는 경우 이러한 요구 사항이 모든 IaaS Windows 서버에 대한 요구 사항에 추가됩니다.

- 이 vRealize Automation 릴리스에서는 기본 SQL Server 2016 130 호환성 모드를 지원하지 않습니다. IaaS에서 사용할 비어 있는 SQL Server 2016 데이터베이스를 별도로 생성하는 경우 100 또는 120 호환성 모드를 사용하십시오.

vRealize Automation 설치 관리자를 통해 데이터베이스를 생성하는 경우 호환성이 이미 구성되어 있습니다.

동일한 동작이 SQL Server 2017에도 적용됩니다.

- AAG(AlwaysOn 가용성 그룹)는 SQL Server 2016 Enterprise 또는 SQL Server 2017 Enterprise에서만 지원됩니다. AAG를 사용할 경우 AAG 수신기 FQDN을 SQL Server 호스트로 지정합니다. AAG를 생성할 때 DTC_Support = Per_DB를 설정합니다. AAG가 생성된 후에는 설정할 수 없습니다.
- IaaS 구성 요소와 함께 호스팅되는 경우 Java를 구성합니다.
 - 64비트 Java 1.8 업데이트 181 이상을 설치합니다. 32비트를 사용하지 마십시오. JRE면 충분합니다. 전체 JDK는 필요하지 않습니다.
 - JAVA_HOME 환경 변수를 Java 설치 폴더로 설정합니다.
 - %JAVA_HOME%\bin\java.exe를 사용할 수 있는지 확인합니다.
- [vRealize Automation 지원 매트릭스](#)에서 지원되는 SQL Server 버전을 사용합니다.
- SQL Server에 대해 TCP/IP 프로토콜을 사용하도록 설정합니다.
- SQL Server에는 SQL 인스턴스에서 생성된 모든 데이터베이스의 템플릿으로 사용되는 모델 데이터베이스가 포함되어 있습니다. IaaS가 올바르게 설치되도록 모델 데이터베이스 크기를 변경하지 마십시오.
- 일반적으로 이 서버에는 [IaaS Windows Server](#)에 설명된 최소 사양보다 고성능의 하드웨어가 필요합니다.

자세한 내용은 [vRealize Automation 하드웨어 규격 및 최대 용량](#) 항목을 참조하십시오.

- vRealize Automation 설치 관리자를 실행하기 전에 계정을 식별하고 SQL에서 사용 권한을 추가해야 합니다. [계정 및 암호](#) 항목을 참조하십시오.

IaaS Distributed Execution Manager 호스트

DEM(Distributed Execution Manager) Orchestrator 또는 작업자 구성 요소를 호스팅하는 Windows Server는 모든 IaaS Windows Server에 대한 요구 사항 외에 추가적인 요구 사항을 충족해야 합니다.

DEM 호스트와 Manager Service 호스트 간에는 방화벽이 존재할 수 없습니다. 포트 정보는 [IaaS Windows Server 포트](#) 항목을 참조하십시오.

DEM 작업자는 자신이 상호 작용하는 프로비저닝 리소스에 따라 추가 요구 사항이 있을 수 있습니다.

Amazon Web Services를 사용하는 DEM 작업자

AWS(Amazon Web Services)와 통신하는 vRealize AutomationIaaS DEM 작업자는 일반적으로 모든 IaaS Windows Server 및 DEM에 대한 요구 사항 외에 추가적인 요구 사항을 충족해야 합니다.

DEM 작업자는 프로비저닝을 위해 AWS와 통신할 수 있습니다. DEM 작업자는 Amazon EC2 계정과 통신하고 이 계정에서 데이터를 수집합니다.

- DEM 작업자는 인터넷에 액세스할 수 있어야 합니다.
- DEM 작업자에 방화벽이 설정되어 있는 경우 `aws.amazon.com`과 더불어 AWS 계정에서 액세스할 수 있는 EC2 영역에 대한 URL(예: 미국 동부 영역의 `ec2.us-east-1.amazonaws.com`)을 대상으로 HTTPS 트래픽이 허용되어야 합니다.

각 URL은 IP 주소 범위로 확인되므로 Network Solutions Web 사이트에서 사용 가능한 도구 등의 도구를 사용하여 해당 IP 주소를 나열하고 구성해야 할 수 있습니다.

- DEM 작업자가 프록시 서버를 통해 인터넷에 연결하는 경우 DEM 서비스는 프록시 서버에 인증할 수 있는 자격 증명에서 실행 중이어야 합니다.

DEM 작업자와 Openstack 또는 PowerVC

Openstack 또는 PowerVC에서 통신을 수행하고 데이터를 수집하는 vRealize AutomationIaaS DEM 작업자는 일반적으로 모든 IaaS Windows Server 및 DEM에 대한 요구 사항 외에 추가적인 요구 사항을 충족해야 합니다.

표 1-17. DEM 작업자 Openstack 및 PowerVC 요구 사항

설치	요구 사항
모두	<p>Windows 레지스트리에서 .NET 프레임워크에 대해 TLS v1.2 지원을 사용하도록 설정합니다. 예:</p> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre>
Windows 2008 DEM 호스트	<p>Windows 레지스트리에서 TLS v1.2 프로토콜을 사용하도록 설정합니다. 예:</p> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre>
인프라 끝점 호스트의 자체 서명된 인증서	<p>PowerVC 또는 Openstack 인스턴스가 신뢰할 수 있는 인증서를 사용하지 않는 경우, PowerVC 또는 Openstack 인스턴스에서 vRealize Automation DEM을 설치할 각 IaaS Windows 서버의 신뢰할 수 있는 루트 CA(인증 기관) 저장소로 SSL 인증서를 가져옵니다.</p>

DEM 작업자와 Red Hat Enterprise 가상화

RHEV(Red Hat Enterprise Virtualization)에서 통신을 수행하고 데이터를 수집하는 vRealize AutomationIaaS DEM 작업자는 일반적으로 모든 IaaS Windows Server 및 DEM에 대한 요구 사항 외에 추가적인 요구 사항을 충족해야 합니다.

- 각 RHEV 환경을 DEM 작업자 서버가 포함된 도메인에 가입시켜야 합니다.
- RHEV 환경을 나타내는 끝점을 관리하는 데 사용되는 자격 증명은 RHEV 환경에서 관리자 권한을 가지고 있어야 합니다. RHEV를 프로비저닝에 사용하는 경우 DEM 작업자가 해당 계정에서 통신을 수행하고 데이터를 수집합니다.
- 이러한 자격 증명은 환경 내의 호스트에 개체를 생성할 수 있는 권한도 가지고 있어야 합니다.

DEM 작업자와 SCVMM

SCVMM(System Center Virtual Machine Manager)을 통해 가상 시스템을 관리하는 vRealize AutomationIaaS DEM 작업자는 일반적으로 모든 IaaS Windows Server 및 DEM에 대한 요구 사항 외에 추가적인 요구 사항을 충족해야 합니다.

- SCVMM 콘솔을 사용하여 동일한 시스템에 DEM 작업자를 설치합니다.
별도의 DEM 작업자에 SCVMM 콘솔을 설치하는 것이 좋습니다.
- DEM 작업자는 콘솔과 함께 설치된 SCVMM PowerShell 모듈에 액세스할 수 있어야 합니다.
- PowerShell 실행 정책은 RemoteSigned 또는 Unrestricted로 설정되어 있어야 합니다.
PowerShell 실행 정책을 확인하려면 PowerShell 명령 프롬프트에서 다음 명령 중 하나를 입력합니다.

```
help about_signing
help Set-ExecutionPolicy
```

- 인스턴스 내의 모든 DEM 작업자가 이러한 요구 사항을 충족하는 시스템에 없는 경우 기술 명령을 사용하여 SCVMM 관련 워크플로를 DEM 작업자로 전달합니다.

vRealize Automation은 SCVMM 사설 클라우드 구성을 사용하는 배포 환경을 지원하지 않습니다.

vRealize Automation은 현재 SCVMM 사설 클라우드를 기반으로 수집, 할당 또는 프로비저닝할 수 없습니다.

SCVMM에는 다음과 같은 추가적인 요구 사항이 적용됩니다.

- vRealize Automation은 PowerShell 3 이상이 필요한 SCVMM 2012 R2를 지원합니다.
- SCVMM 작업 항목을 사용하는 vRealize Automation DEM 작업자를 설치하기 전에 SCVMM 콘솔을 설치합니다.

DEM 작업자를 SCVMM 콘솔보다 먼저 설치하면 다음 예와 유사한 로그 오류가 표시됩니다.

다음과 같은 예외가 발생하여 'ScvmmEndpointDataCollection' 워크플로가 실패했습니다.

'Get-VMMServer' 용어를 cmdlet, 함수, 스크립트 파일 또는 작동 가능한 프로그램의 이름으로 확인할 수 없습니다. 이 이름의 철자를 확인하고, 경로가 포함된 경우에는 해당 경로가 올바른지 확인한 후 다시 시도해 보십시오.

이 문제를 해결하려면 SCVMM 콘솔이 설치되어 있는지 확인하고 DEM 작업자 서비스를 다시 시작합니다.

- SCVMM 인스턴스 각각을 서버가 포함된 도메인에 가입시켜야 합니다.
- SCVMM 인스턴스를 나타내는 끝점을 관리하는 데 사용되는 자격 증명은 SCVMM 서버에 대한 관리자 권한을 가지고 있어야 합니다.

이 자격 증명은 인스턴스 내의 Hyper-V 서버에 대한 관리자 권한도 가지고 있어야 합니다.

- SCVMM 리소스에서 시스템을 프로비저닝하려면 카탈로그 항목을 요청하는 vRealize Automation 사용자가 SCVMM 인스턴스 내에서 관리자 역할이 있어야 합니다.
- 관리해야 하는 SCVMM 인스턴스 내의 Hyper-V 서버는 Hyper-V가 설치된 Windows 2008 R2 SP1 Server여야 합니다. 프로세서에는 필요한 가상화 확장이 준비되어 있어야 합니다. 즉 .NET Framework 4.5.2 이상이 설치되어 있어야 하고 WMI(Windows Management Instrumentation)가 사용하도록 설정되어 있어야 합니다.
- SCVMM 2012 R2 리소스에서 2세대 시스템을 프로비저닝하려면 Blueprint에서 다음과 같은 속성을 추가해야 합니다.

```
Scvmm.Generation2 = true
Hyperv.Network.Type = synthetic
```

2세대 Blueprint에는 [Blueprint 빌드 정보] 페이지의 기존 데이터 수집된 vHDX(virtualHardDisk)가 있어야 합니다. 이 항목을 비워 두면 2세대 프로비저닝이 실패합니다.

시스템 프로비저닝 준비에 대한 자세한 내용은 [SCVMM 환경 준비](#)를 참조하십시오.

인증서

vRealize Automation은 vRealize Automation 장치의 인스턴스 및 IaaS 구성 요소 간의 보안 통신을 위해 SSL 인증서를 사용합니다. 장치 및 Windows 설치 시스템은 해당 인증서를 교환하여 신뢰할 수 있는 연결을 설정합니다. 내부 또는 외부 인증 기간에서 인증서를 얻거나, 각 구성 요소에 대한 배포 프로세스 중에 자체 서명된 인증서를 생성할 수 있습니다.

인증서에 대한 문제 해결, 지원 및 신뢰 요구 사항에 대한 중요 정보는 [VMware 기술 자료 문서 2106583](#) 항목을 참조하십시오.

참고 vRealize Automation은 SHA2 인증서를 지원합니다. 시스템에 의해 생성되는 자체 서명된 인증서는 RSA 암호화가 적용된 SHA-256을 사용합니다. 운영 체제 또는 브라우저 요구 사항 때문에 SHA2 인증서로 업데이트해야 할 수 있습니다.

배포 후 인증서를 업데이트하거나 교체할 수 있습니다. 예를 들어 인증서가 만료될 수 있거나, 초기 배포 중에 자체 서명된 인증서를 사용하지만, 그런 다음 vRealize Automation 구현으로 라이브로 전환되기 전에 신뢰할 수 있는 기관에서 인증서를 얻도록 선택할 수 있습니다.

표 1-18. 인증서 구현

구성 요소	최소 배포(비프로덕션)	분산 배포(프로덕션 준비됨)
vRealize Automation 장치	장치 구성 중에 자체 서명된 인증서를 생성합니다.	각 장치 클러스터의 경우 내부 또는 외부 CA(인증 기관)의 인증서를 사용할 수 있습니다. 다용도 및 와일드카드 인증서가 지원됩니다.
IaaS 구성 요소	설치 시, 생성된 자체 서명된 인증서를 수락하거나 인증서 억제를 선택합니다.	Web Client가 신뢰하는 내부 또는 외부 인증 기관에서 SAN(주체 대체 이름) 인증서와 같은 다중 사용 인증서를 얻습니다.

인증서 체인

인증서 체인을 사용하는 경우 다음 순서로 인증서를 지정합니다.

- 중간 CA 인증서에 의해 서명된 클라이언트/서버 인증서
- 하나 이상의 중간 인증서
- 루트 CA 인증서

인증서를 가져올 때 각 인증서에 대한 BEGIN CERTIFICATE 머리글 및 END 바닥글을 포함시킵니다.

vRealize Automation 로그인 URL을 사용자 지정할 경우 인증서 변경

사용자가 vRealize Automation 장치 또는 로드 밸런서 이름이 아닌 URL 이름으로 로그인하도록 하려면 [vRealize Automation 로그인 URL을 사용자 지정 이름으로 설정](#)에서 설치 이전 및 설치 이후 CNAME 단계를 참조하십시오.

vRealize Automation 인증서 요구 사항

vRealize Automation과 함께 자체 인증서를 사용할 때 인증서는 특정 요구 사항을 충족해야 합니다.

지원되는 인증서 유형

많은 조직에서 인증서는 회사 요구 사항에 따라 외부 기관에서 발급하거나 요청합니다.

다음 요구 사항은 일반적인 vRealize Automation 배포에 사용되는 일반 ID 형식 및 인증서 유형을 다룹니다.

인증서 속성	요구 사항
해시 알고리즘	SHA1, SHA2,(256, 584, 512)
서명 알고리즘	RSASSA-PKCS1_V1_5
키 길이	2084, 4096

참고 RSASSA-PSS 서명은 vRealize Automation 배포에는 지원되지 않습니다. 이 서명은 Windows 2012 R2의 Microsoft CA에 대한 기본값입니다. 서명은 구성 가능한 매개 변수이므로 Microsoft CA를 사용할 때 서명이 적절하게 설정되어 있는지 확인해야 합니다.

vRealize Automation 인증서 지원 매트릭스

해시 알고리즘	SHA1		SHA2-256					
서명 알고리즘	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS	
키 크기	2048	4096	2048	4096	2048	4096	2048	4096
vRealize Automation 지원됨	지원됨 확인됨	지원됨 확인됨	지원되지 않음	지원되지 않음	지원됨 확인됨	지원됨 확인됨	지원되지 않음	지원되지 않음

해시 알고리즘	SHA2-384				SHA2-512			
서명 알고리즘	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS	
키 크기	2048	4096	2048	4096	2048	4096	2048	4096
vRealize Automation 지원됨	지원됨 확인됨	지원됨 확인됨	지원되지 않음	지원되지 않음	지원됨 확인됨	지원됨 확인됨	지원되지 않음	지원되지 않음

인증서 및 개인 키 추출

가상 장치의 인증서는 PEM 형식이어야 합니다.

인증 기관에서 PFX 형식의 인증서를 제공한 경우 OpenSSL을 사용하여 PFX를 PEM으로 변환합니다.

```
openssl pkcs12 -in path-to-pfx -out desired-path-to-pem -nodes
```

예:

```
openssl pkcs12 -in C:\vra-cert.pfx -out C:\vra-cert.pem -nodes
```

PFX 인증서에 암호가 포함되어 있으면 암호를 입력하라는 메시지가 표시될 수 있습니다.

vRealize Automation 장치 배포

vRealize Automation 장치는 기존의 가상화된 인프라에 배포하는 Open Virtualization 파일로 제공됩니다.

vRealize Automation 장치 배포 정보

모든 설치에는 실제 vRealize Automation 설치 옵션 중 하나를 계속하기 전에 먼저 배포되었지만 구성되지 않은 vRealize Automation 장치가 필요합니다.

- 통합된 브라우저 기반 설치 마법사
- 별도의 브라우저 기반 장치 구성으로 그 뒤에 IaaS 서버에 대한 별도의 Windows 설치가 옴
- 응답 속성 파일의 입력을 수락하는 명령줄 기반 자동 설치 관리자
- JSON 형식의 입력을 수락하는 설치 REST API

vRealize Automation 장치 배포

설치 경로 중 하나를 가져오려면 vRealize Automation에서 하나 이상의 vRealize Automation 장치를 배포해야 합니다.

장치를 생성하려면 vSphere Client를 사용하여 템플릿에서 부분적으로 구성된 가상 시스템을 다운로드 및 배포합니다. 고가용성 및 페일오버 기능을 갖춘 엔터프라이즈 배포를 생성하려는 경우 절차를 두 번 이상 수행해야 할 수 있습니다. 이러한 배포에는 대개 로드 밸런서 뒤에 여러 vRealize Automation 장치가 있습니다.

사전 요구 사항

- 인벤토리에 OVF 템플릿을 배포할 수 있는 사용 권한이 있는 계정으로 vSphere Client에 로그인합니다.
- vRealize Automation 장치 .ovf 또는 .ova 파일을 vSphere Client에서 액세스 가능한 위치에 다운로드합니다.

절차

- 1 vSphere **OVF 템플릿 배포** 옵션을 선택합니다.
- 2 vRealize Automation 장치 .ovf 또는 .ova 파일에 대한 경로를 입력합니다.
- 3 템플릿 세부 정보를 검토합니다.
- 4 최종 사용자 라이선스 계약을 읽고 동의해야 합니다.
- 5 장치 이름 및 인벤토리 위치를 입력합니다.

장치를 배포할 때 장치별로 다른 이름을 사용하고 이름에 밑줄(_)과 같은 영숫자가 아닌 문자를 포함하지 마십시오.

- 6 장치가 상주할 호스트 및 클러스터를 선택합니다.
- 7 장치가 상주할 리소스 풀을 선택합니다.

8 장치를 호스팅할 스토리지를 선택합니다.

9 디스크 형식을 선택합니다.

썸 형식은 성능을 향상하고 썸 형식은 스토리지 공간을 절약합니다.

형식은 장치 디스크 크기에 영향을 미치지 않습니다. 장치에 데이터를 위한 더 많은 공간이 필요한 경우 배포 후 vSphere를 사용하여 디스크를 추가합니다.

10 드롭다운 메뉴에서 대상 네트워크를 선택합니다.

11 장치 속성을 완료합니다.

a 루트 암호를 입력하고 확인합니다.

루트 계정 자격 증명을 사용하면 장치에서 호스팅하는 브라우저 기반 관리 인터페이스 또는 장치 운영 체제 명령줄 콘솔에 로그인할 수 있습니다.

b 명령줄 콘솔에 대한 원격 SSH 연결을 허용할지 여부를 선택합니다.

SSH를 사용하지 않도록 설정하는 것이 더욱 안전하지만 별도의 터미널 클라이언트를 통해 액세스하는 대신 vSphere에서 직접 콘솔에 액세스해야 합니다.

- c **호스트 이름**의 경우 장치 FQDN을 입력합니다.

최상의 결과를 얻으려면 DHCP를 사용하는 경우에도 FQDN을 입력합니다.

참고 vRealize Automation은 DHCP를 지원하지만 운영 배포에서는 정적 IP 주소가 권장됩니다.

- d 정적 IP 주소를 사용 중인 경우 [네트워크 속성]에 게이트웨이, 넷마스크 및 DNS 서버의 값을 입력합니다. 다음 예에 나와 있는 것처럼 장치 자체에 대한 IP 주소, FQDN 및 도메인도 입력해야 합니다.

그림 1-13. 가상 장치 속성 예제

▼ Application	3 settings
Enable SSH service in the appliance	This will be used as an initial status of the SSH service in the appliance. You can change it later from the appliance Web console. <input checked="" type="checkbox"/>
Hostname	The host name for this virtual machine. Provide the fully qualified domain name if you use a static IP. Leave blank to try to reverse look up the IP address if you use DHCP. va1.mycompany.com
Initial root password	This will be used as an initial password for the root user account. You can change the password later (by using the passwd command or from the appliance Web console). Enter password: <input type="password"/> Confirm password: <input type="password"/>
▼ Networking Properties	6 settings
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. 12.34.56.79
Domain Name	The domain name of this VM. Leave blank if DHCP is desired. mycompany.com
Domain Name Servers	The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired. 12.34.56.80, 12.34.56.81
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired. mycompany.com
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. 12.34.56.78
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. 255.255.254.0

- 12 배포, vCenter Server 및 DNS 구성에 따라 배포를 완료하고 장치의 전원을 켜는 다음 방법 중 하나를 선택합니다.

- vSphere에 배포했고 [완료 준비] 페이지에서 **배포 후 전원 켜기**를 사용할 수 있는 경우 다음 단계를 수행합니다.
 - a **배포 후 전원 켜기**를 선택하고 **완료**를 클릭합니다.
 - b vCenter Server에 파일 배포가 완료되었으면 **닫기**를 클릭합니다.
 - c 가상 시스템이 시작할 때까지 기다립니다. 최대 5분이 걸릴 수 있습니다.

- vSphere에 배포했고 [완료 준비] 페이지에서 **배포 후 전원 켜기**를 사용할 수 없는 경우 다음 단계를 수행합니다.
 - a vCenter Server에 파일 배포가 완료되었으면 **닫기**를 클릭합니다.
 - b vRealize Automation 장치의 전원을 끕니다.
 - c 가상 시스템이 시작할 때까지 기다립니다. 최대 5분이 걸릴 수 있습니다.
 - d 해당 FQDN을 ping하여 vRealize Automation 장치가 배포되었는지 확인합니다. 장치를 ping할 수 없는 경우 가상 시스템을 다시 시작합니다.
 - e 가상 시스템이 시작할 때까지 기다립니다. 최대 5분이 걸릴 수 있습니다.
- vCloud Director를 사용하여 vRealize Automation 장치를 vCloud에 배포한 경우 OVA 배포 중 입력한 암호를 vCloud가 재정의할 수 있습니다. 재정의 방지하려면 다음 단계를 수행합니다.
 - a vCloud Director에 배포한 후 vApp을 클릭하여 vRealize Automation 장치를 봅니다.
 - b vRealize Automation 장치를 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.
 - c **게스트 운영 체제 사용자 지정** 탭을 클릭합니다.
 - d **암호 재설정** 아래에서 **로컬 관리자 암호 허용** 옵션을 지우고 **확인**을 클릭합니다.
 - e vRealize Automation 장치의 전원을 끕니다.
 - f 가상 시스템이 시작할 때까지 기다립니다. 최대 5분이 걸릴 수 있습니다.

13 해당 FQDN을 ping하여 vRealize Automation 장치가 배포되었는지 확인합니다.

다음에 수행할 작업

- (선택 사항) NIC를 추가합니다. **설치 관리자 실행 전 네트워크 인터페이스 컨트롤러 추가** 항목을 참조하십시오.
- 브라우저 기반 관리 인터페이스에 로그인하여 통합된 설치 마법사를 실행하거나 수동으로 장치를 구성합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 또는 vRealize Automation 자동 또는 API 기반 설치를 활용할 수 있도록 로그인을 건너뛸 수도 있습니다.

설치 관리자 실행 전 네트워크 인터페이스 컨트롤러 추가

vRealize Automation은 여러 NIC(네트워크 인터페이스 컨트롤러)를 지원합니다. 설치 관리자를 실행하기 전에 NIC를 vRealize Automation 장치나 IaaS Windows Server에 추가할 수 있습니다.

vRealize Automation 설치 마법사를 실행하기 전에 여러 NIC가 필요하면 vCenter에 배포한 후 마법사를 시작하기 전에 NIC를 추가합니다. 추가 NIC가 초기에 필요할 수 있는 이유는 다음 예와 같습니다.

- 사용자와 인프라 네트워크를 구분하고자 합니다.
- IaaS 서버가 Active Directory 도메인에 가입할 수 있도록 추가 NIC가 필요합니다.

여러 NIC 시나리오에 대한 자세한 내용은 이 [VMware 클라우드 관리 블로그 게시물](#)을 참조하십시오.

NIC가 3개 이상인 경우 다음 제한 사항을 알아 두어야 합니다.

- VIDM이 Postgres 데이터베이스 및 Active Directory에 액세스할 수 있어야 합니다.
- HA 클러스터에서는 VIDM이 로드 밸런서 URL에 액세스할 수 있어야 합니다.
- 앞의 VIDM 연결은 처음 두 개의 NIC를 통해 이루어져야 합니다.
- 두 번째 NIC 이후의 NIC는 VIDM에서 사용되거나 인식되지 않아야 합니다.
- 두 번째 NIC 이후의 NIC는 Active Directory에 연결하는 데 사용되지 않아야 합니다.

vRealize Automation에서 디렉토리를 구성할 때는 첫 번째 또는 두 번째 NIC를 사용합니다.

사전 요구 사항

vRealize Automation 장치 OVF 및 Windows 가상 시스템을 배포하지만 로그인하거나 설치 마법사를 시작하지는 않습니다.

절차

- 1 vCenter에서 각 vRealize Automation 장치에 NIC를 추가합니다.
 - a 새로 배포된 장치를 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
 - b VMXNETn NIC를 추가합니다.
 - c 전원이 켜져 있으면 장치를 다시 시작합니다.

- 2 vRealize Automation 장치 명령줄에 root로 로그인합니다.

- 3 각 NIC에 대해 다음 명령을 실행하여 NIC를 구성합니다.

기본 게이트웨이 주소를 포함해야 합니다. 이 절차를 마친 후 정적 경로를 구성할 수 있습니다.

```
/opt/vmware/share/vami/vami_set_network network-interface (STATICV4|STATICV4+DHCPV6|
STATICV4+AUTOV6) IPv4-addressnetmaskgateway-v4-address
```

예:

```
/opt/vmware/share/vami/vami_set_network eth1 STATICV4 192.168.100.20 255.255.255.0
192.168.100.1
```

- 4 모든 vRealize Automation 노드가 DNS 이름으로 서로를 확인할 수 있는지 확인합니다.
- 5 모든 vRealize Automation 노드가 vRealize Automation 구성 요소에 대해 로드 밸런싱된 FQDN에 액세스할 수 있는지 확인합니다.
- 6 분할 브레인 DNS를 사용하는 경우 모든 vRealize Automation 노드 및 VIP가 각 노드 IP 및 VIP에 대해 DNS에서 동일한 FQDN을 갖는지 확인합니다.

- 7 vCenter에서 IaaS Windows Server에 NIC를 추가합니다.
 - a IaaS 서버를 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
 - b NIC를 IaaS 서버 가상 시스템에 추가합니다.
- 8 Windows에서 추가된 IaaS 서버 NIC와 해당 IP 주소를 구성합니다. 필요하면 Microsoft 설명서를 참조하십시오.

다음에 수행할 작업

- (선택 사항) 정적 경로가 필요한 경우 설치를 계속하기 전에 **정적 경로 구성**의 지침을 따릅니다.
- 브라우저 기반 관리 인터페이스에 로그인하여 통합된 설치 마법사를 실행하거나 수동으로 장치를 구성합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 또는 vRealize Automation 자동 또는 API 기반 설치를 활용할 수 있도록 로그인을 건너뛸 수도 있습니다.

설치 마법사를 사용하여 vRealize Automation 설치

vRealize Automation 설치 마법사를 사용하면 최소 배포 또는 엔터프라이즈 배포를 쉽고 빠르게 설치할 수 있습니다.

마법사를 시작하기 전에 사전 요구 사항을 충족할 수 있도록 vRealize Automation 장치를 배포하고 IaaS Windows Server를 구성합니다. 설치 마법사는 새로 배포된 vRealize Automation 장치에 처음 로그인할 때 나타납니다.

- 마법사를 중지하고 나중에 다시 돌아오려면 **로그아웃**을 클릭합니다.
- 마법사를 사용하지 않으려면 **취소**를 클릭하거나 로그아웃한 다음 표준 인터페이스를 통해 수동 설치를 시작합니다.

마법사는 새 vRealize Automation 설치를 위한 기본 도구입니다. 마법사를 실행한 후에 기존 vRealize Automation 배포를 확장하고 싶다면 **표준 vRealize Automation 설치 인터페이스**의 절차를 참조하십시오.

최소 배포를 위한 설치 마법사 사용

최소 배포는 vRealize Automation의 작동 방식을 보여 주지만 일반적으로 엔터프라이즈 운영 환경을 지원하기에 충분한 용량을 가지고 있지 않습니다.

POC(Proof of Concept) 작업을 수행하거나 vRealize Automation을 숙지하기 위한 최소 배포를 설치합니다.

최소 배포를 위해 설치 마법사 시작

최소 배포는 일반적으로 하나의 vRealize Automation 장치, 하나의 IaaS Windows Server 및 끝점용 vSphere 에이전트로 구성됩니다. 최소 설치에는 단일 Windows Server에 모든 IaaS 구성 요소를 배치합니다.

사전 요구 사항

- **vRealize Automation 설치 준비**의 사전 요구 사항을 해결합니다.
- 구성되지 않은 장치를 생성합니다. **vRealize Automation 장치 배포** 항목을 참조하십시오.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 설치 마법사가 나타나면 **다음**을 클릭합니다.
- 3 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 4 [배포 유형] 페이지에서 **최소 배포** 및 **Infrastructure as a Service 설치**를 선택하고 **다음**을 클릭합니다.
- 5 [설치 사전 요구 사항] 페이지에서 IaaS Windows Server에 로그인하고 관리 에이전트를 설치합니다.
관리 에이전트를 사용하면 vRealize Automation 장치에서 해당 IaaS 서버를 검색하고 연결할 수 있습니다.

다음에 수행할 작업

IaaS Windows Server에서 관리 에이전트를 설치합니다. **vRealize Automation 관리 에이전트 설치** 항목을 참조하십시오.

vRealize Automation 관리 에이전트 설치

모든 IaaS Windows Server에는 Windows Server를 해당하는 vRealize Automation 장치에 연결하는 관리 에이전트가 필요합니다.

IaaS 구성 요소를 호스팅하지 않는 별도의 Windows 시스템에서 vRealize Automation SQL Server 데이터베이스를 호스팅하는 경우에는 SQL Server 시스템에 관리 에이전트가 필요하지 않습니다.

관리 에이전트는 IaaS Windows Server를 특정 vRealize Automation 장치에 등록하고, IaaS 구성 요소의 설치와 관리를 자동화하고, 지원 및 원격 분석 정보를 수집합니다. 관리 에이전트는 IaaS Windows Server에서 관리자 권한을 가진 도메인 계정을 사용하여 Windows 서비스로 실행됩니다.

사전 요구 사항

vRealize Automation 장치를 생성하고 [설치 마법사]를 시작합니다.

vRealize Automation 장치 배포 및 **최소 배포**를 위해 **설치 마법사 시작** 항목을 참조하십시오.

절차

- 1 루트로 vRealize Automation 장치 콘솔에 로그인합니다.
- 2 다음 명령을 입력합니다.

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```

- 3 나중에 확인할 수 있도록 지문을 복사합니다. 예:

71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89

- 4 관리자 권한을 가진 계정을 사용하여 IaaS Windows Server에 로그인합니다.
5 웹 브라우저를 열고 vRealize Automation 장치 설치 관리자 URL에 연결합니다.

<https://vrealize-automation-appliance-FQDN:5480/installer>

- 6 **관리 에이전트 설치 관리자**를 클릭하고 .msi 파일을 저장 및 실행합니다.

- 7 시작 페이지를 읽습니다.

- 8 최종 사용자 라이선스 계약에 동의합니다.

- 9 설치 폴더를 그대로 사용하거나 변경합니다.

Program Files (x86)\VMware\VCAC\Management Agent

- 10 vRealize Automation 장치 세부 정보를 입력합니다.

- a FQDN 및 :5480 포트 번호를 포함하여 장치 HTTPS 주소를 입력합니다.
b 장치 루트 계정 자격 증명을 입력합니다.
c **로드**를 클릭하고, 지문이 앞에서 복사한 지문과 일치하는지 확인합니다. 콜론은 무시합니다.

지문이 일치하지 않는 경우, 장치 주소가 올바른지 확인합니다.

그림 1-14. 관리 에이전트 - vRealize Automation 장치 세부 정보

- 11 서비스 계정의 도메인\사용자 이름 및 암호를 입력합니다.

서비스 계정은 IaaS Windows Server에서 관리자 권한을 가진 도메인 계정이어야 합니다. 동일한 서비스 계정을 계속 사용합니다.

- 12 프롬프트에 따라 관리 에이전트 설치를 마칩니다.

결과

참고 관리 에이전트와 vRealize Automation 장치는 연결되어 있으므로 장치를 바꿀 경우 관리 에이전트를 다시 설치해야 합니다.

Windows Server에서 IaaS를 제거해도 관리 에이전트는 제거되지 않습니다. 관리 에이전트를 제거하려면 Windows의 [프로그램 추가/제거] 옵션을 따로 사용해야 합니다.

다음에 수행할 작업

브라우저 기반의 [설치 마법사]로 돌아갑니다. 관리 에이전트가 설치되어 있는 IaaS Windows Server가 [검색된 호스트]에 표시됩니다.

설치 마법사 완료

관리 에이전트 설치 후 마법사로 돌아가서 프롬프트를 따릅니다. 설정에 대한 추가적인 지침이 필요한 경우 마법사의 오른쪽 상단에 있는 [도움말] 링크를 클릭하십시오.

- 마법사를 마치면 마지막 페이지에 속성 파일의 경로와 이름이 표시됩니다. 파일을 편집하고 이 파일을 사용하여 마법사 세션과 동일한 또는 유사한 설정으로 vRealize Automation 자동 설치를 수행할 수 있습니다. [자동 vRealize Automation 설치](#) 항목을 참조하십시오.
- 초기 콘텐츠를 생성한 경우 configurationadmin 사용자로 기본 테넌트에 로그인하여 카탈로그 항목을 요청할 수 있습니다.
- 다른 사용자에게 기본 테넌트에 대한 액세스를 구성하려면 [기본 테넌트에 대한 액세스 구성](#)을 참조하십시오.

엔터프라이즈 배포를 위한 설치 마법사 사용

조직의 요구에 따라 엔터프라이즈 배포를 조정할 수 있습니다. 엔터프라이즈 배포는 분산된 구성 요소 또는 로드 밸런서와 함께 구성된 고가용성 배포를 포함할 수 있습니다.

엔터프라이즈 배포는 분산되고 중복된 구성 요소를 포함하는 보다 복잡한 설치 구조를 위해 설계된 것으로 보통 로드 밸런서가 포함됩니다. IaaS 구성 요소의 설치에는 이 두 가지 배포 유형에서 선택 사항입니다.

로드 밸런싱된 배포의 경우, 여러 개의 활성 웹 서버 인스턴스와 여러 vRealize Automation 장치는 설치 실패를 유발합니다. 설치 중에는 단일 웹 서버 인스턴스와 단일 vRealize Automation 장치만 활성화되어야 합니다.

엔터프라이즈 배포를 위해 설치 마법사 시작

엔터프라이즈 배포는 운영 환경에 대해 충분히 큰 규모입니다. 설치 마법사를 사용하여 분산 설치를 배포하거나 고가용성과 페일오버를 위해 로드 밸런서와 함께 분산 설치를 배포할 수 있습니다.

로드 밸런서와 함께 분산 설치를 배포하는 경우 vRealize Automation 환경 구성을 담당하는 팀에게 알려십시오. 테넌트 관리자는 Active Directory에 대한 링크를 구성할 때 고가용성을 위한 디렉토리 관리를 구성해야 합니다.

사전 요구 사항

- **vRealize Automation 설치 준비**의 사전 요구 사항을 해결합니다.
- 구성되지 않은 장치를 생성합니다. **vRealize Automation 장치 배포** 항목을 참조하십시오.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 설치 마법사가 나타나면 **다음**을 클릭합니다.
- 3 최종 사용자 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 4 [배포 유형] 페이지에서 **엔터프라이즈 배포** 및 **Infrastructure as a Service 설치**를 선택합니다.
- 5 [설치 사전 요구 사항] 페이지에서 IaaS Windows Server에 로그인하고 관리 에이전트를 설치합니다.
관리 에이전트를 사용하면 vRealize Automation 장치에서 해당 IaaS 서버를 검색하고 연결할 수 있습니다.

다음에 수행할 작업

IaaS Windows Server에서 관리 에이전트를 설치합니다. **vRealize Automation 관리 에이전트 설치** 항목을 참조하십시오.

vRealize Automation 관리 에이전트 설치

모든 IaaS Windows Server에는 Windows Server를 해당하는 기본 vRealize Automation 장치에 연결하는 관리 에이전트가 필요합니다.

IaaS 구성 요소를 호스팅하지 않는 별도의 Windows 시스템에서 vRealize Automation SQL Server 데이터베이스를 호스팅하는 경우에는 SQL Server 시스템에 관리 에이전트가 필요하지 않습니다.

관리 에이전트는 IaaS Windows Server를 기본 vRealize Automation 장치에 등록하고, IaaS 구성 요소의 설치와 관리를 자동화하고, 지원 및 원격 분석 정보를 수집합니다. 관리 에이전트는 IaaS Windows Server에서 관리자 권한을 가진 도메인 계정을 사용하여 Windows 서비스로 실행됩니다.

사전 요구 사항

vRealize Automation 장치를 생성하고 설치 마법사를 시작합니다.

vRealize Automation 장치 배포 및 **엔터프라이즈 배포**를 위해 **설치 마법사 시작** 항목을 참조하십시오.

절차

- 1 루트로 기본 vRealize Automation 장치 콘솔에 로그인합니다.
- 2 다음 명령을 입력합니다.
`openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1`
- 3 나중에 확인할 수 있도록 지문을 복사합니다. 예:
`71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89`

- 4 관리자 권한을 가진 계정을 사용하여 IaaS Windows Server에 로그인합니다.
- 5 웹 브라우저를 열고 기본 vRealize Automation 장치 설치 관리자 URL에 연결합니다.

<https://vrealize-automation-appliance-FQDN:5480/installer>

- 6 **관리 에이전트 설치 관리자**를 클릭하고 .msi 파일을 저장 및 실행합니다.
- 7 시작 페이지를 읽습니다.
- 8 최종 사용자 라이선스 계약에 동의합니다.
- 9 설치 폴더를 그대로 사용하거나 변경합니다.

Program Files (x86)\VMware\VCAC\Management Agent

- 10 기본 vRealize Automation 장치 세부 정보를 입력합니다.
 - a FQDN 및 :5480 포트 번호를 포함하여 기본 장치 HTTPS 주소를 입력합니다.
 - b 기본 장치 루트 계정 자격 증명을 입력합니다.
 - c **로드**를 클릭하고, 지문이 앞에서 복사한 지문과 일치하는지 확인합니다. 콜론은 무시합니다.
지문이 일치하지 않는 경우, 장치 주소가 올바른지 확인합니다.

그림 1-15. 관리 에이전트 - vRealize Automation 장치 세부 정보

- 11 서비스 계정의 도메인\사용자 이름 및 암호를 입력합니다.

서비스 계정은 IaaS Windows Server에서 관리자 권한을 가진 도메인 계정이어야 합니다. 동일한 서비스 계정을 계속 사용합니다.

- 12 프롬프트에 따라 관리 에이전트 설치를 마칩니다.

결과

IaaS 구성 요소를 호스팅할 모든 Windows Server에서 절차를 반복합니다.

참고 관리 에이전트와 vRealize Automation 장치는 연결되어 있으므로 장치를 바꿀 경우 관리 에이전트를 다시 설치해야 합니다.

Windows Server에서 IaaS를 제거해도 관리 에이전트는 제거되지 않습니다. 관리 에이전트를 제거하려면 Windows의 [프로그램 추가/제거] 옵션을 따로 사용해야 합니다.

다음에 수행할 작업

브라우저 기반의 [설치 마법사]로 돌아갑니다. 관리 에이전트가 설치되어 있는 IaaS Windows Server가 [검색된 호스트]에 표시됩니다.

설치 마법사 완료

관리 에이전트 설치 후 마법사로 돌아가서 프롬프트를 따릅니다. 설정에 대한 추가적인 지침이 필요한 경우 마법사의 오른쪽 상단에 있는 [도움말] 링크를 클릭하십시오.

- 마법사를 마치면 마지막 페이지에 속성 파일의 경로와 이름이 표시됩니다. 파일을 편집하고 이 파일을 사용하여 마법사 세션과 동일한 또는 유사한 설정으로 vRealize Automation 자동 설치를 수행할 수 있습니다. [자동 vRealize Automation 설치](#) 항목을 참조하십시오.
- 초기 콘텐츠를 생성한 경우 configurationadmin 사용자로 기본 테넌트에 로그인하여 카탈로그 항목을 요청할 수 있습니다.
- 다른 사용자에게 기본 테넌트에 대한 액세스를 구성하려면 [기본 테넌트에 대한 액세스 구성](#)을 참조하십시오.

vRealize Automation 설치 마법사 단계별 실행

vRealize Automation 설치 마법사는 사전 요구 사항을 검사하고, 설정을 입력하고, 설정을 검증하고, vRealize Automation 구성 요소를 설치할 수 있는 사용이 간편한 페이지를 제공합니다.

참고 마법사에는 로드 밸런서나 IaaS Windows Server와 같은 다른 시스템에 로그인하기 위해 일시 중지하는 단계가 포함되어 있습니다.

사전 요구 사항

- 하나 이상의 구성되지 않은 장치를 생성합니다. [vRealize Automation 장치 배포](#) 항목을 참조하십시오.
최소 배포에서는 하나의 vRealize Automation 장치를 사용합니다. 엔터프라이즈 배포는 로드 밸런싱 뒤에 여러 장치가 있을 수 있습니다.
- IaaS 구성 요소를 호스팅할 하나 이상의 Windows 시스템을 준비합니다.
- vRealize Automation 장치 관리 인터페이스에 루트로 로그인하여 마법사를 시작합니다.

<https://vrealize-automation-appliance-FQDN:5480>

절차

1 배포 유형

[배포 유형] 페이지에서 설치할 vRealize Automation 구성 요소와 각 구성 요소의 수를 결정합니다.

2 설치 사전 요구 사항

[설치 사전 요구 사항] 페이지에서 일시 중지하고 vRealize Automation IaaS를 호스팅할 Windows 시스템에 대한 연결을 설정합니다. 또한 시간 동기화 원본을 선택합니다.

3 vRealize Appliance

(엔터프라이즈 배포만 해당) [vRealize Appliance] 페이지에는 여러 vRealize Automation 장치를 사용하는 고가용성 배포를 생성하는 옵션이 있습니다.

4 서버 역할

(엔터프라이즈 배포만 해당) [서버 역할] 페이지에서 vRealize AutomationIaaS 구성 요소 역할을 이전에 관리 에이전트를 설치한 Windows 시스템에 할당합니다.

5 사전 요구 사항 검사기

[사전 요구 사항 검사기] 페이지에서 IaaS 설치를 지원하도록 vRealize Automation Windows Server를 확인 및 수정합니다.

6 vRealize Automation 호스트

[vRealize Automation 호스트] 페이지에서 vRealize Automation의 기본 URL 주소를 설정합니다. 이 주소는 일반적으로 vRealize Automation 장치이지만 고가용성 배포에서는 로드 밸런서입니다.

7 Single Sign On

[Single Sign-On] 페이지에서 vRealize Automation 기본 테넌트 시스템 관리자 로그인 자격 증명을 설정합니다.

8 IaaS 호스트

[IaaS 호스트] 페이지에서 특정 IaaS 구성 요소에 대한 기본 URL 주소를 설정합니다. 또한 vRealize AutomationIaaS SQL 데이터베이스에 대한 보안 암호를 생성합니다.

9 Microsoft SQL Server

[Microsoft SQL Server] 페이지에서 vRealize AutomationIaaS SQL 데이터베이스를 구성합니다. IaaS 데이터베이스는 프로비저닝된 시스템, 관련 요소 및 정책을 기록합니다.

10 웹 역할

(엔터프라이즈 배포만 해당) [웹 역할] 페이지에서 IIS의 vRealize AutomationIaaS 웹 사이트를 별도로 구성합니다.

11 Manager Service 역할

(엔터프라이즈 배포만 해당) [Manager Service 역할] 페이지에서 IaaS Manager Service를 호스팅하는 별도의 vRealize Automation Windows 시스템을 구성합니다.

12 Distributed Execution Manager

[Distributed Execution Manager] 페이지에서 IaaS DEM을 호스팅하는 vRealize Automation Windows 시스템을 구성합니다. 다중 DEM 호스트가 지원됩니다.

13 에이전트

[에이전트] 페이지에서 인프라가 배포되는 가상화 리소스와 vRealize AutomationIaaS 간의 연결을 생성합니다. 에이전트 유형을 선택하고 해당 끝점에 대한 세부 정보를 완성합니다.

14 vRealize Appliance 인증서

[vRealize Appliance 인증서] 페이지에서 vRealize Automation 장치가 사용하는 인증 인증서를 생성하거나 선택합니다. 인증서가 자체 서명된 경우 최종 사용자가 브라우저에서 vRealize Automation에 로그인할 때 확인하는 메시지가 표시됩니다.

15 웹 인증서

[웹 인증서] 페이지에서 IaaS 웹 서버가 사용하는 인증 인증서를 생성하거나 선택합니다. vRealize Automation 장치는 웹 서버에 연결하여 이를 인증하고 신뢰해야 합니다.

16 Manager Service 인증서

(엔터프라이즈 배포만 해당) [Manager Service 인증서] 페이지에서 vRealize Automation IaaS Manager Service 호스트가 사용하는 인증 인증서를 생성하거나 선택합니다. 다른 IaaS Windows Server는 Manager Service 호스트에 연결하여 이를 인증하고 신뢰해야 합니다.

17 로드 밸런서

(엔터프라이즈 배포만 해당) [로드 밸런서] 페이지에서 vRealize Automation 구성원 시스템의 올바른 풀에 대해 로드 밸런서를 구성합니다.

18 검증

[검증] 페이지에서 vRealize Automation 설치를 진행할 수 있는지 확인합니다.

19 스냅샷 생성

[스냅샷 생성] 페이지에서는 일시 중지하고 설치를 계속하기 전에 모든 vRealize Automation 구성 요소에 대한 가상 시스템 스냅샷을 생성합니다.

20 설치 세부 정보

[설치 세부 정보] 페이지에서 vRealize Automation 설치를 시작하거나 문제가 발생한 경우 재시도합니다.

21 라이선싱

[라이선싱] 페이지에서 설치된 vRealize Automation 제품을 활성화하는 키를 입력합니다.

22 원격 분석

[원격 분석] 페이지에서 고객 환경 향상 프로그램의 일환으로 vRealize Automation이 VMware에 사용 통계를 보내도록 허용할지 여부를 결정합니다.

23 설치 후 옵션

[설치 후 옵션] 페이지에는 새 vRealize Automation 데이터를 생성하거나 기존 배포 데이터를 새 설치로 마이그레이션하는 옵션이 있습니다.

24 초기 콘텐츠 구성

[초기 콘텐츠 구성] 페이지에서 vSphere 끝점에 대한 콘텐츠 워크플로를 시작할 수 있는 새로운 로컬 vRealize Automation 기본 테넌트 사용자를 생성합니다.

25 마이그레이션 구성

[마이그레이션 구성] 페이지에서 또 다른 이전 vRealize Automation 배포를 새로 설치한 배포로 전송할 수 있습니다.

배포 유형

[배포 유형] 페이지에서 설치할 vRealize Automation 구성 요소와 각 구성 요소의 수를 결정합니다.

최소

최소 배포에서는 IaaS 구성 요소를 호스팅하는 Windows Server 하나와 vRealize Automation 장치 하나만 사용합니다. 최소 배포에서 별도의 SQL Server 시스템에서 IaaS 데이터베이스를 호스팅하거나 IaaS Windows Server에 SQL을 설치할 수 있습니다.

최소 배포를 엔터프라이즈 배포로 변환할 수 없습니다. 배포를 스케일 업하려면 소규모 엔터프라이즈 배포로 시작하고 여기에 구성 요소를 추가하십시오. 최소 배포로 시작하는 것은 지원되지 않습니다.

엔터프라이즈

엔터프라이즈 배포에는 여러 개의 개별 장치와 Windows 호스트가 포함되며, 일반적으로 로드 밸런싱이 사용됩니다. 또한 엔터프라이즈 배포에서는 별도의 SQL Server 시스템이나 IaaS Windows Server 중 하나에서 IaaS 데이터베이스를 호스팅할 수 있습니다.

엔터프라이즈 배포를 선택하는 경우 마법사 왼쪽의 요약 목록에 추가적인 설치 마법사 페이지가 나타납니다.

Infrastructure as a Service

IaaS(Infrastructure as a Service) 옵션은 기존 Windows 시스템에서 vRealize Automation 모델링 및 프로비저닝 기능을 구성할지 여부를 선택합니다.

대부분의 사용자가 설치하지만 vRealize Automation에 IaaS가 반드시 필요하지는 않습니다. XaaS 프로비저닝 지원만 필요한 경우 vRealize Automation 장치만 설치할 수 있습니다. 이 구성에서는 vRealize Automation 장치 관리 인터페이스에 주의 메시지가 표시됩니다. `/etc/vcac/validation.properties`를 편집하여 메시지를 사용하지 않도록 설정할 수 있습니다. `iaas.primary.web.validation.enabled`를 `false`로 변경하십시오.

IaaS를 선택하는 경우 마법사 왼쪽의 요약 목록에 추가적인 설치 마법사 페이지가 나타납니다.

설치 사전 요구 사항

[설치 사전 요구 사항] 페이지에서 일시 중지하고 vRealize Automation IaaS를 호스팅할 Windows 시스템에 대한 연결을 설정합니다. 또한 시간 동기화 원본을 선택합니다.

IaaS Windows Server

Windows 시스템을 IaaS 구성 요소 호스트로 사용하려면 Windows 시스템에서 `VCAC-IaaSManagementAgent-Setup.msi`를 다운로드하여 설치해야 합니다.

관리 에이전트를 설치하려면 실행 중인 vRealize Automation 장치와 통신해야 합니다. Windows에 관리 에이전트를 설치할 때마다 해당 시스템은 특정 장치 및 배포와 고유하게 연결됩니다.

올바른 관리 에이전트가 설치된 잠재적인 IaaS Windows Server가 **검색된 호스트** 아래에 나타납니다.

설치 마법사가 검색된 호스트를 무시하게 하려면 **삭제**를 클릭합니다. Windows 호스트를 삭제해도 해당 관리 에이전트는 제거되지 않습니다. 에이전트를 제거하려면 Windows에서 직접 프로그램 추가/제거 기능을 사용합니다.

시간 소스

모든 vRealize Automation 장치 및 IaaS Windows Server를 동일한 시간 소스와 동기화해야 합니다. 다음과 같은 원본을 사용할 수 있습니다.

- 호스트 시간 사용 — vRealize Automation 장치 ESXi 호스트와 동기화합니다.
- 시간 서버 사용 — 외부 NTP(네트워크 시간 프로토콜) 서버와 동기화합니다. NTP 서버의 FQDN 또는 IP 주소를 입력합니다.

한 vRealize Automation 배포 내에서 시간 소스를 혼용하지 마십시오.

vRealize Appliance

(엔터프라이즈 배포만 해당) [vRealize Appliance] 페이지에는 여러 vRealize Automation 장치를 사용하는 고가용성 배포를 생성하는 옵션이 있습니다.

여러 장치가 별도로 설치한 로드 밸런서 뒤에서 호스팅되고 있어야 합니다. 이후 마법사 페이지에서 장치 및 로드 밸런서의 구성을 확인하고 완료합니다. 추가하는 각 vRealize Automation 장치에 대해 FQDN 및 루트 자격 증명을 입력합니다.

서버 역할

(엔터프라이즈 배포만 해당) [서버 역할] 페이지에서 vRealize Automation IaaS 구성 요소 역할을 이전에 관리 에이전트를 설치한 Windows 시스템에 할당합니다.

IaaS Windows 시스템은 기본 및 추가 웹 서버, Manager Service 호스트, DEM 호스트 및 에이전트 호스트 역할을 할 수 있습니다. IaaS 구성 요소 역할에 대한 자세한 내용은 [Infrastructure as a Service](#)를 참조하십시오.

IaaS 서버 역할의 분리는 엔터프라이즈 배포에서만 가능합니다. 최소 배포에서는 하나의 Windows 시스템이 모든 역할을 수행합니다.

사전 요구 사항 검사기

[사전 요구 사항 검사기] 페이지에서 IaaS 설치를 지원하도록 vRealize Automation Windows Server를 확인 및 수정합니다.

사전 요구 사항 검사기는 관리 에이전트를 설치한 Windows 시스템을 검사하고 IaaS 구성 요소를 호스팅합니다. 사전 요구 사항에는 Java, IIS(인터넷 정보 서비스) 설정, Microsoft DTC(Distributed Transaction Coordinator) 서비스 등이 포함됩니다. 사전 요구 사항의 세부 목록을 보려면 **세부 정보 표시**를 클릭합니다.

설치 마법사를 사용하면 사전 요구 사항에 대한 확인 없이 설치를 진행할 수 있지만 설치가 실패할 수 있습니다.

- 사전 요구 사항을 확인하려면 **실행**을 클릭합니다.

- 사전 요구 사항이 누락된 경우 **세부 정보 표시**를 클릭하여 자세한 내용을 확인하고 **수정**을 클릭합니다.

설치 마법사는 대부분의 소프트웨어 또는 설정 기반 사전 요구 사항을 수정할 수 있습니다. 변경을 수행한 후 설치 마법사가 IaaS 호스트를 다시 시작합니다.

마법사는 메모리 또는 CPU 부족을 해결할 수 없습니다. 그러한 문제가 발생하면 vSphere 또는 하드웨어에서 문제를 해결해야 합니다.

vRealize Automation 호스트

[vRealize Automation 호스트] 페이지에서 vRealize Automation의 기본 URL 주소를 설정합니다. 이 주소는 일반적으로 vRealize Automation 장치이지만 고가용성 배포에서는 로드 밸런서입니다.

- 로드 밸런서 없이 vRealize Automation 장치 하나만 배포하는 경우 vRealize Automation 장치 FQDN을 입력합니다. 클릭하면 설치 마법사가 FQDN을 채웁니다.
- 로드 밸런싱 뒤에 하나 이상의 vRealize Automation 장치가 포함된 엔터프라이즈 구성을 배포하는 경우에는 대신 로드 밸런서 FQDN을 입력합니다.

단일 vRealize Automation 장치도 로드 밸런서 뒤에 배포할 수 있습니다. 이 접근 방식을 사용하면 나중에 장치를 추가하여 배포를 쉽게 확장할 수 있습니다.

Single Sign On

[Single Sign-On] 페이지에서 vRealize Automation 기본 테넌트 시스템 관리자 로그인 자격 증명을 설정합니다.

기본 테넌트 시스템 관리자는 추가 테넌트 생성을 포함한, 모든 사용자의 권한을 대부분 가지고 있습니다. 기본 테넌트 시스템 관리자 자격 증명은 vRealize Automation 장치 루트 자격 증명과 별개입니다.

IaaS 호스트

[IaaS 호스트] 페이지에서 특정 IaaS 구성 요소에 대한 기본 URL 주소를 설정합니다. 또한 vRealize Automation IaaS SQL 데이터베이스에 대한 보안 암호를 생성합니다.

최소 배포

설정	설명
IaaS 웹 주소	IaaS Windows Server FQDN을 입력합니다.
IaaS 구성 요소 설치	IaaS Windows Server FQDN을 선택 또는 입력합니다.
Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
암호	계정 암호를 입력합니다.

설정	설명
보안 암호	<p>laaS SQL 데이터베이스에 데이터를 암호화할 암호를 생성합니다.</p> <ul style="list-style-type: none"> ■ 장애가 발생하는 경우 데이터베이스를 복원하거나 초기 설치 후 구성 요소를 추가할 때 암호가 필요하므로 암호를 기록합니다. ■ 암호에는 큰따옴표(") 문자를 사용할 수 없습니다.
암호 확인	암호를 다시 입력합니다.

엔터프라이즈 배포

설정	설명
laaS 웹 주소	기본 laaS 웹 서버 FQDN을 입력합니다. 로드 밸런싱된 여러 개의 laaS 웹 서버가 포함된 엔터프라이즈 구성을 배포하는 경우 로드 밸런서 FQDN을 대신 입력합니다.
Manager Service 주소	기본 Manager Service 호스트 FQDN을 입력합니다. 로드 밸런싱된 여러 개의 Manager Service 호스트가 포함된 엔터프라이즈 구성을 배포하는 경우 로드 밸런서 FQDN을 대신 입력합니다.
보안 암호	<p>laaS SQL 데이터베이스에 데이터를 암호화할 암호를 생성합니다.</p> <ul style="list-style-type: none"> ■ 장애가 발생하는 경우 데이터베이스를 복원하거나 초기 설치 후 구성 요소를 추가할 때 암호가 필요하므로 암호를 기록합니다. ■ 암호에는 큰따옴표(") 문자를 사용할 수 없습니다.
암호 확인	암호를 다시 입력합니다.

Microsoft SQL Server

[Microsoft SQL Server] 페이지에서 vRealize Automation laaS SQL 데이터베이스를 구성합니다. laaS 데이터베이스는 프로비저닝된 시스템, 관련 요소 및 정책을 기록합니다.

설정	설명
서버 이름	<p>SQL Server 호스트의 FQDN을 입력합니다. 이러한 호스트는 laaS Windows Server 이거나 개별 서버일 수 있습니다.</p> <p>포트 번호 또는 명명된 인스턴스를 지정해야 한다면 FQDN,Port\Instance 형식을 사용합니다.</p> <p>SQL AAG(AlwaysOn 가용성 그룹)를 사용하는 경우, AAG 수신기 FQDN을 지정합니다.</p>
데이터베이스 이름	기본값인 vra 를 적용하거나 laaS 데이터베이스에 대해 다른 이름을 입력합니다.
새 데이터베이스 생성	<p>설치 마법사가 데이터베이스를 생성할 수 있게 합니다.</p> <p>이 옵션이 작동하려면 기본 laaS 웹 서버에서 관리 에이전트를 실행하는 계정에 SQL의 sysadmin 역할이 있어야 합니다.</p>
기존의 빈 데이터베이스 사용	<p>설치 마법사가 데이터베이스를 생성하도록 허용하지 않습니다.</p> <p>데이터베이스를 개별적으로 생성하는 경우 사용자가 제공하는 Windows 사용자 또는 SQL 사용자 자격 증명에 데이터베이스에 대한 dbo 사용 권한이 필요합니다.</p>

설정	설명
기본 설정	(새 데이터베이스만 해당) IaaS 데이터 및 로그 파일에 대해 대체 스토리지 위치를 사용하려는 경우에만 이 옵션을 선택 취소합니다. 해제한 경우 데이터(MDF) 및 로그에 대한 디렉토리를 입력합니다. SQL Server 서비스 계정에 해당 디렉토리에 대한 쓰기 권한이 있어야 합니다.
데이터베이스 연결에 SSL 사용	데이터베이스에 대한 연결을 암호화합니다. 이 옵션을 사용하려면 SSL 용 SQL Server 호스트를 별도로 구성해야 합니다. 또한 IaaS 웹 서버 및 Manager Service 호스트는 SQL Server 호스트의 SSL 인증서를 신뢰해야 합니다.
Windows 인증	Windows 대신 SQL 인증을 사용하려는 경우에만 이 옵션을 해제합니다. 해제한 경우 SQL 인증 자격 증명을 입력합니다.
설치 경로	해제된 상태로 두어 기본값인 %ProgramFiles(x86)%\VMware 를 사용하거나, 대체 위치를 입력합니다. <ul style="list-style-type: none"> ■ vRealize Automation 파일은 SQL Server 호스트에 설치되지 않습니다. 이러한 파일은 기본 IaaS 웹 서버에 저장됩니다. ■ 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.

웹 역할

(엔터프라이즈 배포만 해당) [웹 역할] 페이지에서 **IIS**의 **vRealize AutomationIaaS** 웹 사이트를 별도로 구성합니다.

엔터프라이즈 배포에서는 웹 구성 요소를 호스팅하는 **IaaS Windows** 시스템을 별도로 지정합니다. 고가용성을 위해 다중 호스트가 지원됩니다.

설정		설명
웹 사이트 이름		이름을 사용자 지정하거나 [IIS 기본 웹 사이트]로 남겨 둡니다. IIS에서 추가 웹 사이트를 호스팅하지 마십시오. vRealize Automation은 할당되지 않은 모든 IP 주소에 통신 포트에 대한 바인딩을 설정하기 때문에 추가 바인딩이 불가능합니다.
포트		포트를 사용자 지정하거나 기본값인 443을 그대로 사용합니다.
IaaS 웹 서버	IaaS 호스트 이름	IaaS 웹 구성 요소를 호스팅하는 각 IaaS Windows 시스템의 FQDN을 입력합니다.
	Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
	암호	계정 암호를 입력합니다.
	설치 경로	해제된 상태로 두어 기본값인 %ProgramFiles(x86)%\VMware를 사용하거나, 대체 위치를 입력합니다. 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.

Manager Service 역할

(엔터프라이즈 배포만 해당) [Manager Service 역할] 페이지에서 IaaS Manager Service를 호스팅하는 별도의 vRealize Automation Windows 시스템을 구성합니다.

엔터프라이즈 배포에서는 Windows 서비스인 Manager Service의 호스트를 별도로 지정합니다. 고가용성을 위해 다중 호스트가 지원됩니다.

설정	설명
Active	기본 Manager Service 호스트를 선택합니다. 모든 추가 호스트는 기본 호스트의 백업으로 사용됩니다. 설치 마법사를 사용하여 설치하는 경우 문제가 발생하면 서비스가 원활하게 백업으로 페일오버됩니다. 자동 Manager Service 페일오버 정보 항목을 참조하십시오.
IaaS 호스트 이름	Manager Service를 호스팅하는 각 IaaS Windows 시스템의 FQDN을 입력합니다.
Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
암호	계정 암호를 입력합니다.
설치 경로	해제된 상태로 두어 기본값인 %ProgramFiles(x86)%\VMware를 사용하거나, 대체 위치를 입력합니다. 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.

Distributed Execution Manager

[Distributed Execution Manager] 페이지에서 IaaS DEM을 호스팅하는 vRealize Automation Windows 시스템을 구성합니다. 다중 DEM 호스트가 지원됩니다.

설정	설명
IaaS 호스트 이름	DEM을 호스팅하는 각 IaaS Windows 시스템의 FQDN을 입력합니다.
인스턴스 이름	각 DEM의 고유 식별자를 입력합니다. 모든 DEM 이름은 동일한 호스트에 있는지, 아니면 서로 다른 호스트에 있는지 여부와 관계없이 고유해야 합니다.
Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
암호	계정 암호를 입력합니다.
인스턴스 설명	필요한 경우 각 DEM과 연결된 워크플로에 대한 설명을 입력합니다.
설치 경로	해제된 상태로 두어 기본값인 %ProgramFiles(x86)%\VMware를 사용하거나, 대체 위치를 입력합니다. 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.

에이전트

[에이전트] 페이지에서 인프라가 배포되는 가상화 리소스와 vRealize AutomationIaaS 간의 연결을 생성합니다. 에이전트 유형을 선택하고 해당 끝점에 대한 세부 정보를 완성합니다.

- 동일한 또는 서로 다른 유형의 여러 에이전트가 지원됩니다.
- 동일한 또는 별도의 서버에 에이전트를 설치할 수 있습니다.
- 동일한 서버에 있는 경우 유형에 관계없이 최대 25개의 에이전트가 지원됩니다.
- 동일한 유형의 여러 에이전트가 동일한 서버에 있는 경우 각각 고유한 이름과 서로 다른 끝점을 가져야 합니다.
- 고가용성을 위해 별도의 서버에 동일한 유형, 이름 및 끝점의 에이전트를 설치할 수 있습니다.
- 보통 vSphere는 에이전트 유형 중 하나입니다.
- 설치 후에 에이전트를 추가할 수 있습니다.

에이전트 유형

표 1-19. vSphere

설정	설명
에이전트 유형	드롭다운에서 vSphere를 선택합니다.
IaaS 호스트 이름	드롭다운에서 에이전트를 호스팅하는 IaaS Windows 시스템의 FQDN을 선택합니다.
에이전트 이름	고가용성을 위해 별도의 서버에 동일한 에이전트 이름 및 끝점을 추가하는 경우가 아니라면 고유한 식별자를 입력합니다.
끝점	vSphere 끝점의 이름을 입력합니다.
설치 경로	해제된 상태로 두어 기본값인 %ProgramFiles(x86)%\VMware를 사용하거나, 대체 위치를 입력합니다. 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.
Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
암호	계정 암호를 입력합니다.

표 1-20. EPI PowerShell

설정	설명
에이전트 유형	드롭다운에서 EpiPowerShell을 선택합니다.
IaaS 호스트 이름	드롭다운에서 에이전트를 호스팅하는 IaaS Windows 시스템의 FQDN을 선택합니다.
에이전트 이름	고가용성을 위해 별도의 서버에 동일한 에이전트 이름 및 끝점을 추가하는 경우가 아니라면 고유한 식별자를 입력합니다.
Type	드롭다운에서 EPIServer 끝점이 호스팅하는 프로비저닝의 브랜드를 선택합니다.

표 1-20. EPI PowerShell (계속)

설정	설명
서버	EPIServer의 FQDN을 입력합니다.
설치 경로	해제된 상태로 두어 기본값인 %ProgramFiles(x86)%\VMware를 사용하거나, 대체 위치를 입력합니다. 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.
Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
암호	계정 암호를 입력합니다.

표 1-21. HyperV

설정	설명
에이전트 유형	드롭다운에서 HyperV를 선택합니다.
IaaS 호스트 이름	드롭다운에서 에이전트를 호스팅하는 IaaS Windows 시스템의 FQDN을 선택합니다.
에이전트 이름	고가용성을 위해 별도의 서버에 동일한 에이전트 이름 및 끝점을 추가하는 경우가 아니라면 고유한 식별자를 입력합니다.
Username	HyperV 끝점 인스턴스에 대한 로그인 계정을 입력합니다.
암호	계정 암호를 입력합니다.
설치 경로	해제된 상태로 두어 기본값인 %ProgramFiles(x86)%\VMware를 사용하거나, 대체 위치를 입력합니다. 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.
Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
암호	계정 암호를 입력합니다.

표 1-22. VDI PowerShell

설정	설명
에이전트 유형	드롭다운에서 VdiPowerShell을 선택합니다.
IaaS 호스트 이름	드롭다운에서 에이전트를 호스팅하는 IaaS Windows 시스템의 FQDN을 선택합니다.
에이전트 이름	고가용성을 위해 별도의 서버에 동일한 에이전트 이름 및 끝점을 추가하는 경우가 아니라면 고유한 식별자를 입력합니다.
Type	끝점 유형은 기본적으로 XenDesktop이며 변경할 수 없습니다.
서버	XenDesktop 끝점의 FQDN을 입력합니다.
XenDesktop 버전	드롭다운에서 버전을 선택합니다.

표 1-22. VDI PowerShell (계속)

설정	설명
설치 경로	해제된 상태로 두어 기본값인 <code>%ProgramFiles(x86)%\VMware</code> 를 사용하거나, 대체 위치를 입력합니다. 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.
Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
암호	계정 암호를 입력합니다.

표 1-23. Xen

설정	설명
에이전트 유형	드롭다운에서 Xen을 선택합니다.
IaaS 호스트 이름	드롭다운에서 에이전트를 호스팅하는 IaaS Windows 시스템의 FQDN을 선택합니다.
에이전트 이름	고가용성을 위해 별도의 서버에 동일한 에이전트 이름 및 끝점을 추가하는 경우가 아니라면 고유한 식별자를 입력합니다.
Username	Xen 끝점 인스턴스에 대한 로그인 계정을 입력합니다.
암호	계정 암호를 입력합니다.
설치 경로	해제된 상태로 두어 기본값인 <code>%ProgramFiles(x86)%\VMware</code> 를 사용하거나, 대체 위치를 입력합니다. 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.
Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
암호	계정 암호를 입력합니다.

표 1-24. WMI

설정	설명
에이전트 유형	드롭다운에서 WMI를 선택합니다.
IaaS 호스트 이름	드롭다운에서 에이전트를 호스팅하는 IaaS Windows 시스템의 FQDN을 선택합니다.
에이전트 이름	고가용성을 위해 별도의 서버에 동일한 에이전트 이름 및 끝점을 추가하는 경우가 아니라면 고유한 식별자를 입력합니다.
설치 경로	해제된 상태로 두어 기본값인 <code>%ProgramFiles(x86)%\VMware</code> 를 사용하거나, 대체 위치를 입력합니다. 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.

표 1-24. WMI (계속)

설정	설명
Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
암호	계정 암호를 입력합니다.

표 1-25. 테스트

설정	설명
에이전트 유형	드롭다운에서 Test 를 선택합니다.
IaaS 호스트 이름	드롭다운에서 에이전트를 호스팅하는 IaaS Windows 시스템의 FQDN을 선택합니다.
에이전트 이름	고가용성을 위해 별도의 서버에 동일한 에이전트 이름 및 끝점을 추가하는 경우가 아니라면 고유한 식별자를 입력합니다.
설치 경로	해제된 상태로 두어 기본값인 %ProgramFiles(x86)%\VMware를 사용하거나, 대체 위치를 입력합니다. 동일한 Windows 시스템에 여러 IaaS 구성 요소를 설치하는 경우 모든 구성 요소를 동일한 설치 경로에 설치합니다.
Username	DOMAIN\username 형식으로 서비스 계정을 입력합니다. 이 계정은 IaaS Windows Server에 대한 로컬 관리자 권한이 있는 도메인 계정이어야 합니다.
암호	계정 암호를 입력합니다.

vRealize Appliance 인증서

[vRealize Appliance 인증서] 페이지에서 vRealize Automation 장치가 사용하는 인증 인증서를 생성하거나 선택합니다. 인증서가 자체 서명된 경우 최종 사용자가 브라우저에서 vRealize Automation에 로그인할 때 확인하는 메시지가 표시됩니다.

설정	설명	
인증서 작업	기존 유지	이 vRealize Automation 장치의 기존 인증서를 사용합니다. 아래 항목에서 일련 번호 및 지문과 같은 세부 정보를 확인합니다.
	인증서 생성	마법사를 사용하여 vRealize Automation 장치의 자체 서명된 인증서를 생성합니다.
	서명 요청 생성	<p>CA(인증 기관)에 제공할 CSR(인증서 서명 요청) 파일을 생성합니다. CA는 CSR을 통해 올바른 값을 사용하여 사용자가 가져올 수 있는 인증서를 생성할 수 있습니다.</p> <ol style="list-style-type: none">1 조직, 조직 구성 단위 및 국가 코드를 입력합니다(아래 참조).2 서명 요청 생성을 클릭합니다.3 CA에 대한 CSR 파일을 다운로드하려면 나타나는 링크를 클릭합니다.

설정	설명
가져오기	<p>PEM 형식의 인증서 파일을 식별하고, 마법사가 올바른 저장소에 파일을 추가하게 하고, vRealize Automation에서 사용하도록 로드합니다.</p> <p>CSR에서 생성된 인증서를 가져오는 경우가 아닌 한, 이 옵션을 사용하려면 인증서 개인 키, 개인 키 암호(있는 경우) 및 인증서 체인을 입력해야 합니다.</p> <p>CSR에서 생성된 CA 제공 PEM을 가져올 때에는 개인 키 및 암호를 비워 둡니다.</p>
일반 이름	<p>vRealize Automation 장치의 FQDN입니다.</p> <p>다중 장치 앞에 로드 밸런서가 있는 고가용성 엔터프라이즈 배포에서는 이 항목이 로드 밸런서 FQDN입니다.</p>
조직	대규모 부서 또는 사업부를 나타내는 텍스트를 입력합니다.
조직 구성 단위	소규모 부서 또는 작업 그룹을 나타내는 텍스트를 입력합니다.
국가 코드	운영 국가의 약어를 입력합니다.
일련 번호	고유한 영숫자 식별자
지문	인증서를 식별하거나 다른 인증서를 비교하는 데 사용되는 고유한 영숫자 문자열
유효 기간 시작	인증서를 사용할 수 있게 되는 시작 시간을 알려주는 타임 스탬프
유효 기간 종료	인증서를 더 이상 사용할 수 없게 되는 시간을 알려주는 타임 스탬프

웹 인증서

[웹 인증서] 페이지에서 IaaS 웹 서버가 사용하는 인증 인증서를 생성하거나 선택합니다. vRealize Automation 장치는 웹 서버에 연결하여 이를 인증하고 신뢰해야 합니다.

설정	설명
인증서 작업	<p>기존 유지</p> <p>이 IaaS 웹 서버의 기존 인증서를 사용합니다. 아래 항목에서 일련 번호 및 지문과 같은 세부 정보를 확인합니다.</p>
	<p>인증서 생성</p> <p>마법사를 사용하여 IaaS 웹 서버의 자체 서명된 인증서를 생성합니다.</p>
	<p>서명 요청 생성</p> <p>CA(인증 기관)에 제공할 CSR(인증서 서명 요청) 파일을 생성합니다. CA는 CSR을 통해 올바른 값을 사용하여 사용자가 가져올 수 있는 인증서를 생성할 수 있습니다.</p> <ol style="list-style-type: none"> 1 조직, 조직 구성 단위 및 국가 코드를 입력합니다(아래 참조). 2 서명 요청 생성을 클릭합니다. 3 CA에 대한 CSR 파일을 다운로드하려면 나타나는 링크를 클릭합니다.

설정	설명
가져오기	<p>PEM 형식의 인증서 파일을 식별하고, 마법사가 올바른 저장소에 파일을 추가하게 하고, vRealize Automation에서 사용하도록 로드합니다.</p> <p>CSR에서 생성된 인증서를 가져오는 경우가 아닌 한, 이 옵션을 사용하려면 인증서 개인 키, 개인 키 암호(있는 경우) 및 인증서 체인을 입력해야 합니다.</p> <p>CSR에서 생성된 CA 제공 PEM을 가져올 때에는 개인 키 및 암호를 비워 둡니다.</p>
인증서 지문 제공	이전에 올바른 저장소에 추가한 인증서를 로드합니다.
일반 이름	<p>IaaS 웹 서버의 FQDN.</p> <p>다중 웹 서버 앞에 로드 밸런서가 있는 고가용성 엔터프라이즈 배포에서는 이 항목이 로드 밸런서 FQDN입니다.</p>
조직	대규모 부서 또는 사업부를 나타내는 텍스트를 입력합니다.
조직 구성 단위	소규모 부서 또는 작업 그룹을 나타내는 텍스트를 입력합니다.
국가 코드	운영 국가의 약어를 입력합니다.
일련 번호	고유한 영숫자 식별자
지문	인증서를 식별하거나 다른 인증서를 비교하는 데 사용되는 고유한 영숫자 문자열
유효 기간 시작	인증서를 사용할 수 있게 되는 시작 시간을 알려주는 타임 스탬프
유효 기간 종료	인증서를 더 이상 사용할 수 없게 되는 시간을 알려주는 타임 스탬프

Manager Service 인증서

(엔터프라이즈 배포만 해당) [Manager Service 인증서] 페이지에서 vRealize Automation IaaS Manager Service 호스트가 사용하는 인증 인증서를 생성하거나 선택합니다. 다른 IaaS Windows Server는 Manager Service 호스트에 연결하여 이를 인증하고 신뢰해야 합니다.

이 페이지는 IaaS 웹 서버와 별도의 시스템에 Manager Service를 호스팅하는 경우에만 나타납니다. 동일한 시스템에서 호스팅되는 경우에는 웹 인증서가 두 역할 모두에 대한 인증을 제공합니다.

설정	설명
인증서 작업	<p>기존 유지</p> <p>이 IaaS Manager Service 호스트의 기존 인증서를 사용합니다. 아래 항목에서 일련 번호 및 지문과 같은 세부 정보를 확인합니다.</p>
	<p>인증서 생성</p> <p>마법사를 사용하여 IaaS Manager Service 호스트의 자체 서명된 인증서를 생성합니다.</p>

설정	설명
서명 요청 생성	CA(인증 기관)에 제공할 CSR(인증서 서명 요청) 파일을 생성합니다. CA는 CSR을 통해 올바른 값을 사용하여 사용자가 가져올 수 있는 인증서를 생성할 수 있습니다. 1 조직, 조직 구성 단위 및 국가 코드를 입력합니다(아래 참조). 2 서명 요청 생성 을 클릭합니다. 3 CA에 대한 CSR 파일을 다운로드하려면 나타나는 링크를 클릭합니다.
가져오기	PEM 형식의 인증서 파일을 식별하고, 마법사가 올바른 저장소에 파일을 추가하게 하고, vRealize Automation에서 사용하도록 로드합니다. CSR에서 생성된 인증서를 가져오는 경우가 아닌 한, 이 옵션을 사용하려면 인증서 개인 키, 개인 키 암호(있는 경우) 및 인증서 체인을 입력해야 합니다. CSR에서 생성된 CA 제공 PEM을 가져올 때에는 개인 키 및 암호를 비워 둡니다.
인증서 지문 제공	이전에 올바른 저장소에 추가한 인증서를 로드합니다.
일반 이름	IaaS Manager Service 호스트의 FQDN입니다. 다중 Manager Service 호스트 앞에 로드 밸런서가 있는 고가용성 엔터프라이즈 배포에서는 이 항목이 로드 밸런서 FQDN입니다.
조직	대규모 부서 또는 사업부를 나타내는 텍스트를 입력합니다.
조직 구성 단위	소규모 부서 또는 작업 그룹을 나타내는 텍스트를 입력합니다.
국가 코드	운영 국가의 약어를 입력합니다.
일련 번호	고유한 영숫자 식별자
지문	인증서를 식별하거나 다른 인증서를 비교하는 데 사용되는 고유한 영숫자 문자열
유효 기간 시작	인증서를 사용할 수 있게 되는 시작 시간을 알려주는 타임 스탬프
유효 기간 종료	인증서를 더 이상 사용할 수 없게 되는 시간을 알려주는 타임 스탬프

로드 밸런서

(엔터프라이즈 배포만 해당) [로드 밸런서] 페이지에서 vRealize Automation 구성원 시스템의 올바른 풀에 대해 로드 밸런서를 구성합니다.

로드 밸런서 목록은 정보 제공용으로만 사용됩니다. 이 목록은 이전의 마법사 항목을 기반으로 구성원, 해당 구성 요소 역할, FQDN, 포트 번호와 함께 배포의 각 로드 밸런서를 제공합니다.

여기에서 로드 밸런서에 로그인하는 동안 목록을 사용하여 vRealize Automation 구성원을 추가하고 포트를 엽니다.

호스트에서 로드 밸런싱하는 방법에 대한 자세한 내용은 [vRealize Automation 로드 밸런싱](#)을 참조하십시오.

검증

[검증] 페이지에서 vRealize Automation 설치를 진행할 수 있는지 확인합니다.

모든 vRealize Automation 구성 요소, 역할 및 계정이 올바른지 그리고 시스템에서 서로를 인증할 수 있는지 확인하려면 **검증**을 클릭합니다. 프로세스는 환경에 따라 30분 이상 걸릴 수 있습니다.

오류가 발생하면 실패한 라인 항목을 확장하고 제공된 상태 및 메시지를 기반으로 내용을 수정합니다. 검증을 통과할 때까지 vRealize Automation 설치를 진행할 수 없습니다.

스냅샷 생성

[스냅샷 생성] 페이지에서는 일시 중지하고 설치를 계속하기 전에 모든 vRealize Automation 구성 요소에 대한 가상 시스템 스냅샷을 생성합니다.

검증이 통과된 경우에도 설치와 관련하여 예기치 않은 문제가 발생할 경우를 대비하는 것이 좋습니다. 설치를 시작하기 전에 vSphere 클라이언트를 사용하여 모든 vRealize Automation 장치 및 IaaS Windows Server의 스냅샷을 작성합니다. 그렇지 않으면 이 시점으로 돌아가기 위해 모든 마법사 설정을 다시 입력해야 합니다.

충분한 리소스가 있는 경우 실행 중인 가상 시스템의 스냅샷을 생성할 수 있습니다. 더 나은 방법은 시스템을 먼저 중지하는 것입니다.

- 1 설치 마법사의 오른쪽 상단에서 **로그아웃**을 클릭합니다.

중요 **로그아웃** 이외의 방법으로 마법사를 닫은 경우 마법사를 다시 열 수 없습니다.

- 2 vSphere에서 모든 vRealize Automation 장치 및 IaaS Windows Server의 게스트 운영 체제를 종료합니다.
- 3 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **스냅샷 생성**을 선택합니다.
- 4 스냅샷에 이름을 지정합니다.
- 5 스냅샷에 시스템 메모리를 포함하려면 **가상 시스템 메모리 스냅샷**을 선택합니다.
- 6 **확인**을 클릭합니다.

스냅샷이 생성될 때까지 기다립니다.

- 7 모든 vRealize Automation 장치 및 IaaS Windows Server의 게스트 운영 체제 전원을 켭니다.
- 8 루트로 다시 로그인하여 설치 마법사 스냅샷 페이지로 돌아갑니다.

<https://vrealize-automation-appliance-FQDN:5480>

설치 세부 정보

[설치 세부 정보] 페이지에서 vRealize Automation 설치를 시작하거나 문제가 발생한 경우 재시도합니다.

팁 중복된 데이터베이스 키에 대한 우발적인 설치 오류가 보고되었습니다. 가능한 오류를 사전에 방지하려면 **설치**를 클릭하기 전에 내장된 vPostgres 데이터베이스에서 다음 SQL update 문을 실행합니다.

```
update cluster_commands set output='' where type like '%install%';
```

설치를 시작하려면 **설치**를 클릭합니다. 환경에 따라 설치에 최대 1시간 이상이 걸릴 수 있습니다.

설치 중 또는 설치 후에 **로그 수집** 버튼을 클릭할 수 있습니다.

- 로그를 수집할 때 ZIP 파일 다운로드 링크가 상태 테이블 위에 나타납니다.
- 로그를 두 번 이상 수집하는 경우 각 수집이 이전 수집을 덮어씁니다.

현재의 로그를 원하는 경우 **로그 수집**을 다시 클릭하기 전에 로그를 다운로드하십시오.

문제가 발생한 경우 마법사가 설치를 중지하고 문제 해결에 도움이 되는 메시지를 표시합니다. 메시지를 확인하고 필요한 교정 조치를 기록한 후에는 생성한 스냅샷이 필요할 수도 있고 필요하지 않을 수도 있습니다.

스냅샷으로 되돌리지 **않음**

마법사가 **실패 재시도**를 사용하도록 설정된 경우 시스템을 스냅샷으로 되돌리지 않고 교정 조치를 취한 후 설치를 다시 시도할 수 있습니다.

교정 조치를 취한 후 **실패 재시도**를 클릭합니다.

IaaS Windows Server를 스냅샷으로 되돌리기

마법사에서 **모든 IaaS 항목 재시도**를 사용할 수 있는 경우 다음 단계를 수행합니다.

- 1 vSphere에서 모든 IaaS Windows 시스템을 이전 마법사 페이지에서 생성한 스냅샷으로 되돌립니다.
- 2 종료된 후에 스냅샷을 생성한 경우 게스트 운영 체제의 전원을 켭니다.
- 3 외부 SQL Server를 사용한 경우 vRealize Automation SQL 데이터베이스를 삭제합니다.
- 4 교정 조치를 취합니다.
- 5 **모든 IaaS 항목 재시도**를 클릭합니다.

모든 IaaS 항목 재시도가 동일한 키가 있는 항목이 이미 추가되었다는 오류가 표시되면서 실패하면 내장된 vPostgres 데이터베이스에 다음 SQL update 문을 실행합니다. 그런 다음, **모든 IaaS 항목 재시도**를 다시 시도합니다.

```
update cluster_commands set output='' where type like '%install%';
```

장치 및 IaaS Windows Server를 스냅샷으로 되돌리기

마법사에 vRealize Automation 장치에 대한 메시지가 표시되면 다음 단계를 수행합니다.

- 1 vSphere에서 모든 vRealize Automation 장치 및 IaaS Windows 시스템을 이전 마법사 페이지에서 생성한 스냅샷으로 되돌립니다.

- 2 종료된 후에 스냅샷을 생성한 경우 게스트 운영 체제의 전원을 켭니다.
- 3 외부 SQL Server를 사용한 경우 vRealize Automation SQL 데이터베이스를 삭제합니다.
- 4 교정 조치를 취합니다.
- 5 루트로 다시 로그인하여 설치 마법사로 돌아옵니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 6 [설치 세부 정보] 페이지로 돌아가 **설치**를 클릭합니다.

라이센싱

[라이센싱] 페이지에서 설치된 vRealize Automation 제품을 활성화하는 키를 입력합니다.

새 라이선스 키에 키를 입력하고 **키 제출**을 클릭합니다. 독립형 vRealize Automation, vRealize Suite, vRealize Business for Cloud 및 vRealize Code Stream에 대한 키를 포함하여 둘 이상의 키를 별도로 제출할 수 있습니다.

원격 분석

[원격 분석] 페이지에서 고객 환경 향상 프로그램의 일환으로 vRealize Automation이 VMware에 사용 통계를 보내도록 허용할지 여부를 결정합니다.

CEIP(고객 환경 향상 프로그램)에 참여하는 옵션을 선택하거나 선택 취소합니다.

자세한 내용은 [고객 환경 향상 프로그램](#)을 참조하십시오.

설치 후 옵션

[설치 후 옵션] 페이지에는 새 vRealize Automation 데이터를 생성하거나 기존 배포 데이터를 새 설치로 마이그레이션하는 옵션이 있습니다.

- **초기 콘텐츠 구성**은 기본 테넌트의 새로운 로컬 사용자를 생성합니다. 이 로컬 사용자는 기본 테넌트에서 구성 프로세스를 시작할 수 있습니다.

이 옵션을 사용하려면 이전에 설치 마법사의 [에이전트] 페이지에서 적어도 vSphere 끝점 하나를 추가해야 합니다.
- **배포 마이그레이션**은 기존 vRealize Automation 데이터를 이 새로 설치된 배포로 전송합니다. 마이그레이션은 그룹, Blueprint 및 끝점과 같은 필수 요소를 보존합니다.
- **계속**을 선택하면 설치 마법사의 끝으로 이동합니다.

초기 콘텐츠 구성

[초기 콘텐츠 구성] 페이지에서 vSphere 끝점에 대한 콘텐츠 워크플로를 시작할 수 있는 새로운 로컬 vRealize Automation 기본 테넌트 사용자를 생성합니다.

참고 이 옵션은 앞서 [에이전트] 페이지에서 vSphere 끝점을 하나 이상 추가한 경우에만 사용할 수 있습니다.

새로운 로컬 사용자 이름은 **configurationadmin**입니다. vRealize Automation은 **configurationadmin**에게 다음과 같은 권한을 부여합니다.

- 테넌트 관리자
- IaaS 관리자
- 승인 관리자
- 카탈로그 관리자
- 인프라 설계자
- XaaS 설계자
- vRealize Orchestrator 관리자

configurationadmin의 로그인 암호를 입력하고 확인합니다. **configurationadmin**이 기본 테넌트에 로그인한 후 구성 프로세스를 시작할 수 있도록 카탈로그 항목을 생성하려면 **초기 콘텐츠 생성**을 클릭합니다.

마이그레이션 구성

[마이그레이션 구성] 페이지에서 또 다른 이전 vRealize Automation 배포를 새로 설치한 배포로 전송할 수 있습니다.

이전 배포를 마이그레이션하기 전에 다음 지침을 따르십시오.

- 이전 배포 버전에 해당하는 vRealize Automation 마이그레이션 가이드를 철저히 검토합니다. 사전 요구 사항 및 기타 세부 정보가 다를 수 있습니다.
- 이전 테넌트 및 ID 저장소를 새로운 배포의 VMware Identity Manager로 마이그레이션합니다.
- 이전 IaaS SQL Server 데이터베이스를 복제한 후 새 배포 IaaS 데이터베이스로 복원합니다. 복제된 데이터베이스의 이름을 기록합니다.
- 이전 IaaS SQL Server 데이터베이스의 암호화 키를 가져오고 기록합니다.
- 마이그레이션된 데이터를 다시 암호화할 수 있는 새로운 암호를 생성하고 기록합니다.
- 이전 vRealize Automation 장치 또는 로드 밸런서 FQDN과 루트 로그인 자격 증명을 기록합니다.
- 새 배포의 루트 로그인 자격 증명을 기록합니다.

표준 vRealize Automation 설치 인터페이스

설치 마법사를 실행한 후 표준 인터페이스를 통해 특정 설치 작업을 수동으로 수행할 필요가 있습니다.

설치 마법사를 사용하여 vRealize Automation 설치에서 설명하는 설치 마법사는 새 vRealize Automation 설치를 위한 기본 도구입니다. 하지만 마법사를 실행한 후 일부 작업에는 여전히 이전의 수동 설치 프로세스가 필요합니다.

vRealize Automation 배포를 확장하려는 경우 또는 마법사가 어떤 이유로 중지된 경우 수동 단계가 필요합니다. 예를 들어 다음과 같은 상황에서 이 섹션의 절차를 참조해야 할 수 있습니다.

- 설치를 완료하기 전에 마법사를 취소했습니다.

- 마법사를 사용하여 설치하지 못했습니다.
- 고가용성을 위해 다른 vRealize Automation 장치를 추가하려고 합니다.
- 고가용성을 위해 다른 IaaS 웹 서버를 추가하려 합니다.
- 다른 프록시 에이전트가 필요합니다.
- 다른 DEM 작업자 또는 Orchestrator가 필요합니다.

모든 수동 프로세스 또는 일부 수동 프로세스만 사용할 수 있습니다. 이 섹션 전반의 자료를 검토하고 상황에 맞는 절차를 따르십시오.

최소 배포를 위한 표준 인터페이스 사용

개발 환경에서 사용하거나 개념 증명으로 사용할 독립형 최소 배포를 설치할 수 있습니다. 최소 배포는 운영 환경에는 적합하지 않습니다.

최소 배포 검사 목록

개념 증명 또는 개발 작업을 위해 최소 구성으로 vRealize Automation을 설치합니다. 최소 배포는 더 적은 단계로 설치할 수 있지만 엔터프라이즈 배포의 운영 용량이 부족합니다.

다음 순서로 개괄 작업을 완료합니다.

표 1-26. 최소 배포 검사 목록

작업	세부 정보
<input type="checkbox"/> 환경 및 주소 설치 사전 요구 사항을 계획합니다.	vRealize Automation 설치 준비
<input type="checkbox"/> 구성되지 않은 vRealize Automation 장치를 생성합니다.	vRealize Automation 장치 배포
<input type="checkbox"/> vRealize Automation 장치를 수동으로 구성합니다.	vRealize Automation 장치 구성
<input type="checkbox"/> 단일 Windows Server에 IaaS 구성 요소를 설치합니다.	IaaS 구성 요소 설치
<input type="checkbox"/> 필요한 경우 추가적인 에이전트를 설치합니다.	vRealize Automation 에이전트 설치
<input type="checkbox"/> 기본 테넌트를 구성하는 것과 같은 사후 설치 작업을 수행합니다.	기본 테넌트에 대한 액세스 구성

vRealize Automation 장치 구성

vRealize Automation 장치는 vRealize Automation 서버 및 사용자 웹 포털을 호스팅하는 부분적으로 구성된 가상 시스템입니다. 장치 OVF(Open Virtualization Format) 템플릿을 다운로드하고 vCenter Server 또는 ESX/ESXi 인벤토리에 배포합니다.

사전 요구 사항

- 구성되지 않은 장치를 생성합니다. [vRealize Automation 장치 배포](#) 항목을 참조하십시오.
- vRealize Automation 장치에 대한 인증서를 가져옵니다.

절차

- 1 구성되지 않은 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

모든 인증서 경고를 무시하고 계속합니다.

- 2 설치 마법사가 나타나면 마법사 대신 관리 인터페이스로 이동할 수 있도록 취소합니다.
- 3 **관리 > 시간 설정**을 선택하고 시간 동기화 소스를 설정합니다.

옵션	설명
호스트 시간	vRealize Automation 장치 ESXi 호스트에 동기화합니다.
시간 서버	외부 NTP(네트워크 시간 프로토콜) 서버 하나에 동기화합니다. NTP 서버의 FQDN 또는 IP 주소를 입력합니다.

vRealize Automation 장치와 IaaS Windows Server를 동일한 시간 소스에 동기화해야 합니다. 한 vRealize Automation 배포 내에서 시간 소스를 혼용하지 마십시오.

- 4 **vRA > 호스트 설정**을 선택합니다.

옵션	작업
자동으로 해결	vRealize Automation 장치에 대한 현재 호스트의 사용자 이름을 지정하려면 자동으로 해결 을 선택합니다.
호스트 업데이트	새 호스트인 경우 호스트 업데이트 를 선택합니다. 호스트 이름 텍스트 상자에 vRealize Automation 장치의 정규화된 도메인 이름(<i>vra-hostname.domain.name</i>)을 입력합니다. 로드 밸런서를 사용하는 분산 배포의 경우 호스트 업데이트 를 선택합니다. 호스트 이름 텍스트 상자에 로드 밸런서 서버의 정규화된 도메인 이름(<i>vra-loadbalancename.domain.name</i>)을 입력합니다.

참고 **호스트 업데이트**를 사용하여 호스트 이름을 설정할 때마다 이 절차의 뒷부분에서 설명하는 대로 SSO 설정을 구성하십시오.

- 5 **인증서 작업** 메뉴에서 적절한 작업을 선택합니다.

PEM 형식의 인코딩된 인증서를 사용하는 경우(예: 분산된 환경)에는 **가져오기**를 선택합니다.

가져오는 인증서는 신뢰할 수 있어야 할 뿐 아니라 SAN(주체 대체 이름) 인증서를 통해 vRealize Automation 장치의 모든 인스턴스와 모든 로드 밸런서에 적용 가능해야 합니다.

인증 기관에 제출할 수 있는 새 인증서 CSR 요청을 생성하려면 **서명 요청 생성**을 선택합니다. CA는 CSR을 통해 올바른 값을 사용하여 사용자가 가져올 수 있는 인증서를 생성할 수 있습니다.

참고 인증서 체인을 사용하는 경우 다음 순서로 인증서를 지정합니다.

- a 중간 CA 인증서에 의해 서명된 클라이언트/서버 인증서
- b 하나 이상의 중간 인증서
- c 루트 CA 인증서

옵션	작업
기존 유지	현재 SSL 구성을 그대로 둡니다. 이 옵션은 변경 사항을 취소할 때 선택합니다.
인증서 생성	<ul style="list-style-type: none"> a 일반 이름 텍스트 상자에 표시되는 값은 페이지 위쪽 부분에 나타나는 호스트 이름입니다. vRealize Automation 장치의 추가 인스턴스를 사용할 수 있는 경우 FQDN이 인증서의 SAN 특성에 포함됩니다. b 조직 이름(예: 회사 이름)을 조직 텍스트 상자에 입력합니다. c 조직 구성 단위(예: 부서 이름 또는 위치)를 조직 구성 단위 텍스트 상자에 입력합니다. d 두 글자의 ISO 3166 국가 코드(예: KO)를 국가 텍스트 상자에 입력합니다.
서명 요청 생성	<ul style="list-style-type: none"> a 서명 요청 생성을 선택합니다. b 조직, 조직 구성 단위, 국가 코드 및 일반 이름 텍스트 상자의 내용을 검토합니다. 이러한 항목은 기존 인증서로부터 채워집니다. 필요한 경우 이러한 항목을 편집할 수 있습니다. c CSR 생성을 클릭하여 인증서 서명 요청을 생성한 후 생성된 CSR을 여기에 다운로드 링크를 클릭하여, 인증 기관에 보낼 수 있는 위치에 CSR을 저장하기 위한 대화상자를 엽니다. d 준비된 인증서를 받으면 가져오기를 클릭한 후 지침을 따라 인증서를 vRealize Automation에 가져옵니다.
가져오기	<ul style="list-style-type: none"> a 머리글 및 바닥글을 포함하여 BEGIN PRIVATE KEY에서 END PRIVATE KEY까지 인증서 값을 복사한 후 RSA 개인 키 텍스트 상자에 붙여 넣습니다. b 머리글 및 바닥글을 포함하여 BEGIN CERTIFICATE에서 END CERTIFICATE까지 인증서 값을 복사한 후 인증서 체인 텍스트 상자에 붙여 넣습니다. 인증서 값이 여러 개인 경우, 각 인증서에 대해 BEGIN CERTIFICATE 머리글과 END CERTIFICATE 바닥글을 포함합니다. <p>참고 체인 인증서의 경우 추가 특성이 사용 가능할 수 있습니다.</p> <ul style="list-style-type: none"> c (선택 사항) 인증서의 인증서 키가 암호를 사용하여 암호화된 경우에는 해당 암호를 복사하여 암호 텍스트 상자에 붙여 넣습니다.

6 설정 저장을 클릭하여 호스트 정보와 SSL 구성을 저장합니다.

7 SSO 설정을 구성합니다.

8 메시징을 클릭합니다. 장치에 대한 구성 설정과 메시징 상태가 표시됩니다. 이러한 설정은 변경하지 마십시오.

9 원격 분석 탭을 클릭하여 VMware CEIP(고객 환경 향상 프로그램)에 참여할지 여부를 선택합니다.

CEIP를 통해 수집된 데이터에 대한 세부 정보 및 VMware에서 CEIP를 사용하는 목적이 Trust & Assurance Center의 <http://www.vmware.com/trustvmware/ceip.html>에 기술되어 있습니다.

- 프로그램에 참여하려면 **VMware 고객 환경 향상 프로그램에 참여**를 선택합니다.
- 프로그램에 참여하지 않으려면 **VMware 고객 환경 향상 프로그램에 참여**를 선택 취소합니다.

10 서비스를 클릭하고 서비스가 등록되었는지 확인합니다.

이 작업은 사이트 구성에 따라 10분 정도 소요될 수 있습니다.

참고 장치에 로그인하고 `tail -f /var/log/vcac/catalina.out` 명령을 실행하여 서비스 시작을 모니터링할 수 있습니다.

11 라이선스 정보를 입력합니다.

- a **vRA > 라이선싱**을 클릭합니다.
- b **라이선싱**을 클릭합니다.
- c 설치 파일을 다운로드할 때 함께 다운로드한 유효한 vRealize Automation 라이선스 키를 입력하고 **키 제출**을 클릭합니다.

참고 연결 오류가 발생하면 로드 밸런서에서 문제가 발생한 것일 수 있습니다. 로드 밸런서에 대한 네트워크 연결을 확인합니다.

12 vRealize Automation에 로그인할 수 있는지 확인합니다.

- a 브라우저를 열고 vRealize Automation 제품 인터페이스 URL로 이동합니다.
`https://vrealize-automation-appliance-FQDN/vcac`
- b vRealize Automation 인증서를 수락합니다.
- c SSO 인증서를 수락합니다.
- d administrator@vsphere.local 및 SSO를 구성할 때 지정한 암호를 사용하여 로그인합니다.
인터페이스의 [테넌트] 페이지에서 **관리** 탭이 열립니다. 이름이 vsphere.local인 테넌트 하나가 목록에 표시됩니다.

결과

vRealize Automation 장치의 배포와 구성을 마쳤습니다. 구성 이후에 장치가 제대로 동작하지 않으면 장치를 다시 배포하고 재구성하십시오. 기존 장치는 변경하지 마십시오.

다음에 수행할 작업

인프라 구성 요소 설치 항목을 참조하십시오.

IaaS 구성 요소 설치

관리자가 Windows 시스템(물리적 또는 가상)에 인프라(IaaS) 구성 요소의 전체 집합을 설치합니다. 이러한 작업을 수행하는 데 관리자 권한이 필요합니다.

최소 설치에는 별도의 서버에 설치할 수 있는 SQL 데이터베이스를 제외하고 동일한 Windows 서버에 모든 구성 요소를 설치합니다.

Windows Server에서 시간 동기화 사용

성공적인 설치를 보장하기 위해 vRealize Automation 서버 및 Windows 서버의 클럭이 동기화되어야 합니다.

다음 단계는 VMware Tools를 사용하여 ESX/ESXi 호스트와 함께 시간 동기화를 사용하는 방법에 대해 설명합니다. 물리적 호스트에 IaaS 구성 요소를 설치하거나 시간 동기화에 VMware Tools를 사용하지 않으려는 경우 기본 설정 방법을 사용하여 서버 시간이 정확한지 확인합니다.

절차

- 1 Windows 설치 시스템에서 명령 프롬프트를 엽니다.
- 2 다음 명령을 입력하여 VMware Tools 디렉토리로 이동합니다.

```
cd C:\Program Files\VMware\VMware Tools
```

- 3 timesync 상태를 표시하기 위한 명령을 입력합니다.

```
VMwareToolboxCmd.exe timesync status
```

- 4 timesync가 사용하지 않도록 설정된 경우 다음 명령을 입력하여 사용하도록 설정합니다.

```
VMwareToolboxCmd.exe timesync enable
```

IaaS 인증서

vRealize Automation IaaS 구성 요소는 인증서 및 SSL을 사용하여 구성 요소 간의 통신을 보호합니다. 개념 증명 목적의 최소 설치에서 자체 서명된 인증서를 사용할 수 있습니다.

분산 환경에서 신뢰할 수 있는 인증 기관의 도메인 인증서를 가져옵니다. IaaS 구성 요소에 대한 도메인 인증서 설치에 대한 자세한 내용은 분산 배포 장의 [IaaS 인증서 설치](#)를 참조하십시오.

인프라 구성 요소 설치

시스템 관리자는 Windows 시스템에 로그인한 후 설치 마법사를 사용하여 IaaS 서비스를 Windows 가상 시스템 또는 물리적 시스템에 설치합니다.

사전 요구 사항

- 서버가 [IaaS Windows Server](#)의 요구 사항을 충족하는지 확인합니다.
- [Windows Server에서 시간 동기화 사용](#).

- vRealize Automation 장치를 배포하고 완전하게 구성했으며 필요한 서비스(plugin-service, catalog-service, iaas-proxy-provider)가 실행 중인지 확인합니다.

절차

1 vRealize Automation IaaS 설치 관리자 다운로드

최소 가상 또는 물리적 Windows Server에 IaaS를 설치하려면 vRealize Automation 장치에서 IaaS 설치 관리자의 사본을 다운로드합니다.

2 설치 유형 선택

시스템 관리자는 Windows 2008 또는 2012 설치 시스템에서 설치 관리자 마법사를 실행합니다.

3 사전 요구 사항 확인

사전 요구 사항 검사기는 시스템이 IaaS 설치 요구 사항을 충족하는지 확인합니다.

4 서버 및 계정 설정 지정

vRealize Automation 시스템 관리자는 Windows 설치 서버에 대한 서버 및 계정 설정을 지정하며 SQL 데이터베이스 서버 인스턴스와 인증 방법을 선택합니다.

5 관리자 및 에이전트 지정

최소 설치에는 필수 Distributed Execution Manager와 기본 vSphere 프록시 에이전트를 설치합니다. 시스템 관리자는 설치를 마친 후 사용자 지정 설치 관리자를 사용하여 추가적인 프록시 에이전트(예: XenServer 또는 Hyper-V)를 설치할 수 있습니다.

6 IaaS 구성 요소 등록

시스템 관리자가 IaaS 인증서를 설치하고 IaaS 구성 요소를 SSO에 등록합니다.

7 설치 완료

시스템 관리자가 IaaS 설치를 완료합니다.

vRealize Automation IaaS 설치 관리자 다운로드

최소 가상 또는 물리적 Windows Server에 IaaS를 설치하려면 vRealize Automation 장치에서 IaaS 설치 관리자의 사본을 다운로드합니다.

이 프로세스 중에 인증서 경고가 표시되면 경고를 무시하고 계속하여 설치를 마칩니다.

사전 요구 사항

- IaaS Windows Server 요구 사항을 검토합니다. [IaaS Windows Server](#) 항목을 참조하십시오.
- Internet Explorer를 사용하여 다운로드하는 경우 보안 강화 구성 설정을 사용하지 말아야 합니다. Windows Server에서 `res://iesetup.dll/SoftAdmin.htm`으로 이동합니다.

절차

- 1 관리자 권한이 있는 계정을 사용하여 IaaS Windows Server에 로그인합니다.

- 2 웹 브라우저에서 바로 vRealize Automation 장치 설치 관리자 URL을 엽니다.

`https://vrealize-automation-appliance-FQDN:5480/installer`

3 IaaS 설치 관리자를 클릭합니다.

4 setup__vrealize-automation-appliance-FQDN@5480을 Windows Server에 저장합니다.

설치 관리자 파일 이름을 변경하지 마십시오. 이는 설치를 vRealize Automation 장치에 연결하는 데 사용됩니다.

설치 유형 선택

시스템 관리자는 Windows 2008 또는 2012 설치 시스템에서 설치 관리자 마법사를 실행합니다.

사전 요구 사항

[vRealize Automation IaaS 설치 관리자 다운로드](#).

절차

1 setup__vrealize-automation-appliance-FQDN@5480.exe 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

2 다음을 클릭합니다.

3 라이선스 계약에 동의하고 **다음**을 클릭합니다.

4 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.

a 사용자 이름(**root**)과 암호를 입력합니다.

암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.

b **인증서 수락**을 선택합니다.

c **인증서 보기**를 클릭합니다.

인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.

5 인증서 수락을 선택합니다.

6 다음을 클릭합니다.

7 최소 배포를 생성하는 경우, **전체 설치**를 **설치 유형** 페이지에서 선택하고 **다음**을 클릭합니다.

사전 요구 사항 확인

사전 요구 사항 검사기는 시스템이 IaaS 설치 요구 사항을 충족하는지 확인합니다.

사전 요구 사항

[설치 유형 선택](#).

절차

- 1 사전 요구 사항 확인을 완료합니다.

옵션	설명
오류 없음	다음을 클릭합니다.
심각하지 않은 오류	무시를 클릭합니다.
심각한 오류	심각한 오류를 무시하면 설치가 실패합니다. 경고가 표시되면 왼쪽 창에서 경고를 선택한 다음 오른쪽에 있는 지침을 따릅니다. 심각한 오류를 모두 해결하고 다시 확인 을 클릭하여 확인합니다.

- 2 다음을 클릭합니다.

결과

시스템이 설치 요구 사항을 충족합니다.

서버 및 계정 설정 지정

vRealize Automation 시스템 관리자는 Windows 설치 서버에 대한 서버 및 계정 설정을 지정하며 SQL 데이터베이스 서버 인스턴스와 인증 방법을 선택합니다.

사전 요구 사항

[사전 요구 사항 확인.](#)

절차

- 1 **서버 및 계정 설정** 페이지 또는 **감지된 설정** 페이지에서 Windows 서비스 계정의 사용자 이름과 암호를 입력합니다. 이 서비스 계정은 SQL 관리자 권한도 가진 로컬 관리자 계정이어야 합니다.

- 2 **암호** 텍스트 상자에 암호를 입력합니다.

암호는 데이터베이스 데이터를 보호하기 위한 암호화 키를 생성하는 일련의 단어입니다.

참고 향후 설치 또는 시스템 복구 시 사용할 수 있도록 암호를 저장하십시오.

- 3 IaaS 구성 요소가 있는 동일한 서버에 데이터베이스 인스턴스를 설치하려면 [SQL Server 데이터베이스 설치 정보] 섹션에 있는 **서버** 텍스트 상자의 기본 서버를 그대로 사용합니다.

데이터베이스가 다른 시스템에 있는 경우 서버를 다음 형식으로 입력합니다.

machine-FQDN,port-number\named-database-instance

- 4 **데이터베이스 이름** 텍스트 상자의 기본값을 그대로 사용하거나, 필요한 경우 적절한 이름을 입력합니다.

5 인증 방법을 선택합니다.

- ◆ 현재 사용자의 Windows 자격 증명을 사용하여 데이터베이스를 생성하려면 **Windows 인증 사용**을 선택합니다. 사용자는 SQL sys_admin 권한을 가지고 있어야 합니다.
- ◆ SQL 인증을 사용하여 데이터베이스를 생성하려면 **Windows 인증 사용**의 선택을 취소합니다. SQL Server 인스턴스에 대해 SQL sys_admin 권한을 가진 SQL Server 사용자의 **사용자 이름** 및 **암호**를 입력합니다.

Windows 인증을 사용하는 것이 좋습니다. SQL 인증을 선택하면 암호화되지 않은 데이터베이스 암호가 특정 구성 파일에 나타납니다.

6 (선택 사항) 데이터베이스 연결에 SSL 사용 확인란을 선택합니다.

기본적으로 이 확인란은 사용하도록 설정되어 있습니다. SSL은 IaaS 서버와 SQL 데이터베이스 간에 보다 안전한 연결을 제공합니다. 그러나 이 옵션을 지원하려면 먼저 SQL Server에서 SSL을 구성해야 합니다. SQL Server에서 SSL 구성에 대한 자세한 내용은 [Microsoft Technet 문서 189067](#) 항목을 참조하십시오.

7 다음을 클릭합니다.

관리자 및 에이전트 지정

최소 설치에 필수 Distributed Execution Manager와 기본 vSphere 프록시 에이전트를 설치합니다. 시스템 관리자는 설치를 마친 후 사용자 지정 설치 관리자를 사용하여 추가적인 프록시 에이전트(예: XenServer 또는 Hyper-V)를 설치할 수 있습니다.

사전 요구 사항

[서버 및 계정 설정 지정.](#)

절차

- 1 **Distributed Execution Manager 및 프록시 vSphere 에이전트** 페이지에서 기본값을 그대로 사용하거나, 필요한 경우 이름을 변경합니다.
- 2 기본값 그대로 vSphere 에이전트를 설치하여 vSphere를 이용한 프로비저닝을 사용하도록 설정하거나, 필요한 경우 기본값의 선택을 해제합니다.
 - a **vSphere 에이전트 설치 및 구성**을 선택합니다.
 - b 기본 에이전트와 끝점을 그대로 사용하거나, 이름을 입력합니다.

끝점 이름 값을 기록해 둡니다. vRealize Automation 콘솔에서 vSphere 끝점을 구성할 때 이 정보를 올바르게 입력하지 않으면 구성이 실패할 수 있습니다.

3 다음을 클릭합니다.

IaaS 구성 요소 등록

시스템 관리자가 IaaS 인증서를 설치하고 IaaS 구성 요소를 SSO에 등록합니다.

사전 요구 사항

[vRealize Automation IaaS 설치 관리자 다운로드.](#)

절차

- 1 설치 관리자를 다운로드한 vRealize Automation 장치 서버의 정규화된 도메인 이름이 채워지는 기본 **서버** 값을 그대로 사용합니다. 정규화된 도메인 이름이 서버를 식별하는 데 사용되고, IP 주소가 아닌지 확인합니다.

가상 장치가 여러 개 있고 로드 밸런서를 사용하는 경우에는 로드 밸런서 가상 장치 경로를 입력하십시오.

- 2 **로드**를 클릭하여 **SSO 기본 테넌트**의 값(vsphere.local)을 채웁니다.
- 3 **다운로드**를 클릭하여 vRealize Automation 장치에서 인증서를 검색합니다.
인증서 보기를 클릭하면 인증서 세부 정보를 볼 수 있습니다.
- 4 **인증서 수락**을 선택하여 SSO 인증서를 설치합니다.
- 5 [SSO 관리자] 패널에서 **사용자 이름** 텍스트 상자에 **administrator**를 입력하고, SSO를 구성할 때 이 사용자에게 대해 정의한 암호를 **암호** 및 **암호 확인**에 입력합니다.
- 6 **사용자 이름** 필드 오른쪽에 있는 텍스트 링크를 클릭하여, 입력한 암호가 올바른지 확인합니다.
- 7 **laaS 서버**의 기본값을 그대로 사용합니다. 여기에는 현재 설치를 수행 중인 Windows 시스템의 호스트 이름이 표시됩니다.
- 8 **laaS 서버** 필드 오른쪽에 있는 텍스트 링크를 클릭하여, 연결이 유효한지 확인합니다.
- 9 **다음**을 클릭합니다.
다음을 클릭한 이후에 오류가 표시되면 계속하기 전에 오류를 해결해야 합니다.

설치 완료

시스템 관리자가 laaS 설치를 완료합니다.

사전 요구 사항

- **laaS 구성 요소 등록.**
- 설치하고 있는 시스템이 네트워크에 연결되어 있고 laaS 설치 관리자를 다운로드하는 vRealize Automation 장치에 연결할 수 있는지 확인합니다.

절차

- 1 **설치 준비** 페이지에서 정보를 검토하고 **설치**를 클릭합니다.
설치가 시작됩니다. 설치는 네트워크 구성에 따라 5분에서 1시간까지 걸릴 수 있습니다.
- 2 성공 메시지가 나타나면 **초기 구성 과정 안내** 확인란이 선택된 상태에서 **다음** 및 **완료**를 클릭합니다.
- 3 **시스템 구성** 메시지 상자를 닫습니다.

결과

이제 설치가 완료되었습니다.

다음에 수행할 작업

IaaS 서비스 확인.

분산 배포를 위한 표준 인터페이스 사용

엔터프라이즈 배포는 운영 환경의 보다 큰 vRealize Automation 용량을 위해 설계되었으며 여러 개의 시스템에 구성 요소를 배포해야 합니다. 엔터프라이즈 배포는 로드 밸런서 뒤에 중복 시스템이 포함될 수도 있습니다.

분산 배포 검사 목록

시스템 관리자는 분산 구성에 vRealize Automation을 배포할 수 있으며 이는 이중화를 통한 페일오버 보호 및 고가용성을 제공합니다.

분산 배포 검사 목록은 분산 설치를 수행하는 데 필요한 단계의 간략한 개요를 제공합니다.

표 1-27. 분산 배포 검사 목록

작업	세부 정보
<input type="checkbox"/> 설치 환경을 계획 및 준비하고 모든 설치 사전 요구 사항이 충족되었는지 확인합니다.	vRealize Automation 설치 준비
<input type="checkbox"/> SSL 인증서를 계획하고 가져옵니다.	분산 배포의 인증서 신뢰 요구 사항
<input type="checkbox"/> 리드 vRealize Automation 장치 서버와 이중화 및 고가용성에 필요한 추가 장치를 배포합니다.	vRealize Automation 장치 배포
<input type="checkbox"/> vRealize Automation 장치 트래픽을 처리하기 위한 로드 밸런서를 구성합니다.	로드 밸런서 구성
<input type="checkbox"/> 리드 vRealize Automation 장치 서버와 이중화 및 고가용성을 위해 배포한 추가 장치를 구성합니다.	vRealize Automation 장치 구성
<input type="checkbox"/> vRealize Automation IaaS 구성 요소 트래픽을 처리하기 위한 로드 밸런서를 구성하고 vRealize Automation IaaS 구성 요소를 설치합니다.	분산 구성에서 IaaS 구성 요소 설치
<input type="checkbox"/> 필요한 경우 외부 시스템과 통합하기 위한 에이전트를 설치합니다.	vRealize Automation 에이전트 설치
<input type="checkbox"/> 기본 테넌트를 구성하고 IaaS 라이선스를 제공합니다.	기본 테넌트에 대한 액세스 구성

vRealize Orchestrator

vRealize Automation 장치에는 새 설치와 함께 사용하도록 권장되는 vRealize Orchestrator의 포함된 버전이 있습니다. 하지만, 이전 배포나 특수한 경우에는 분리된 외부 vRealize Orchestrator에 vRealize Automation을 연결할 수 있습니다. <https://www.vmware.com/products/vrealize-orchestrator.html>을 참조하십시오.

vRealize Automation 및 vRealize Orchestrator 연결에 대한 자세한 내용은 [vRealize Automation용 VMware vRealize Orchestrator 플러그인](#)을 참조하십시오.

디렉토리 관리

고가용성과 페일오버를 위해 로드 밸런서와 함께 분산 설치를 설치하는 경우 vRealize Automation 환경 구성을 담당하는 팀에게 알려십시오. 테넌트 관리자는 Active Directory에 대한 링크를 구성할 때 고가용성을 위한 디렉토리 관리를 구성해야 합니다.

로드 밸런서 상태 점검을 사용하지 않도록 설정

상태 점검은 로드 밸런서가 작동 중인 노드에만 트래픽을 전송하는지 확인합니다. 로드 밸런서는 지정된 빈도로 모든 노드에 상태 점검을 전송합니다. 실패 임계값을 초과하는 노드는 새 트래픽에 대해 부적격한 상태가 됩니다.

워크로드 배포 및 페일오버를 위해 여러 vRealize Automation 장치를 로드 밸런서 뒤에 배치할 수 있습니다. 또한 여러 IaaS 웹 서버와 여러 IaaS Manager Service 서버를 각각의 로드 밸런서 뒤에 배치할 수 있습니다.

로드 밸런서를 사용할 때 로드 밸런서가 설치 중 아무 때나 상태 점검을 전송하도록 허용하지 마십시오. 상태 점검으로 인해 설치가 방해받거나 설치 중 예기치 않은 동작이 발생할 수 있습니다.

- vRealize Automation 장치 또는 IaaS 구성 요소를 기존 로드 밸런서 뒤에 배포하는 경우, 구성 요소를 설치하기 전에 제안된 구성의 모든 로드 밸런서에 대해 상태 점검을 사용하지 않도록 설정합니다.
- 모든 vRealize Automation 장치 및 IaaS 구성 요소를 포함하여 vRealize Automation 전체를 설치 및 구성한 후 상태 점검을 다시 사용하도록 설정할 수 있습니다.

분산 배포의 인증서 신뢰 요구 사항

vRealize Automation은 인증서를 사용하여 신뢰 관계를 유지하고 분산 배포의 구성 요소 간에 보안 통신을 제공합니다.

분산 배포 또는 클러스터링된 배포에서 인증서 조직은 주로 3계층 vRealize Automation 아키텍처를 따릅니다.

- vRealize Automation 장치
- IaaS Web 구성 요소
- IaaS Manager Service 구성 요소

분산 배포에서는 특정 계층의 각 시스템이 인증서를 공유합니다. 예를 들어 각 vRealize Automation 장치가 공통 인증서를 공유하고 각 Manager Service 호스트가 공통 인증서를 공유합니다.

Web 및 Manager Service 구성 요소가 동일한 시스템에서 호스팅되는 경우 두 계층 모두에 대해 하나의 인증서면 충분합니다.

시스템 생성 인증서

버전 7.0부터는 사용자가 인증서를 제공하지 않으면 vRealize Automation 설치 마법사가 자체 서명된 인증서를 자동으로 생성하여 이것이 필요한 분산 구성 요소의 적절한 신뢰 저장소에 배치합니다.

시스템에서 생성한 자체 서명된 인증서를 사용자 또는 CA 제공 인증서로 업데이트해야 하는 경우 [vRealize Automation 인증서 업데이트](#)를 참조하십시오.

자체 인증서 제공

표준 수동 설치 관리자를 실행하는 경우에는 직접 생성한 자체 서명 인증서 또는 CA(인증 기관) 인증서를 제공합니다.

OpenSSL 또는 다른 방법을 사용하여 자체적인 인증서를 제공하거나 생성하는 경우에는 와일드카드 또는 SAN(주체 대체 이름) 인증서를 사용할 수 있습니다.

IaaS 인증서는 다중 사용 인증서여야 합니다. 인증서를 제공하는 경우에는 클러스터의 IaaS 구성 요소를 포함하는 다중 사용 인증서를 확보하여, 이 인증서를 각 구성 요소의 신뢰 저장소에 복사해야 합니다.

로드 밸런서

고가용성 및 페일오버를 위해, 분산 vRealize Automation 구성 요소 앞에 로드 밸런서를 추가할 수 있습니다. vRealize Automation 로드 밸런서에 대해서는 패스스루 구성을 사용하는 것이 좋습니다. 패스스루 구성에서는 로드 밸런서가 암호 해독 없이 구성 요소에 요청을 전달합니다. 그런 다음 vRealize Automation 장치 및 IaaS 호스트가 필요한 암호 해독을 수행합니다.

로드 밸런서를 사용하는 경우 클러스터 다중 사용 인증서의 신뢰할 수 있는 주소에 로드 밸런서 FQDN을 포함해야 합니다.

로드 밸런서 사용 및 구성에 대한 자세한 내용은 "vRealize Automation 로드 밸런싱"을 참조하십시오.

인증서 신뢰 요구 사항

다음 테이블에는 가져온 다양한 인증서에 대한 신뢰 등록 요구 사항이 요약되어 있습니다.

가져오기	등록
vRealize Automation 장치 클러스터	IaaS 웹 구성 요소 클러스터
IaaS Web 구성 요소 클러스터	<ul style="list-style-type: none"> ■ vRealize Automation 장치 클러스터 ■ Manager Service 구성 요소 클러스터 ■ DEM Orchestrator 및 DEM 작업자 구성 요소
IaaS Manager Service 구성 요소 클러스터	<ul style="list-style-type: none"> ■ DEM Orchestrator 및 DEM 작업자 구성 요소 ■ 에이전트 및 프록시 에이전트

인증서 신뢰 및 표준 설치 관리자

표준 수동 설치 관리자를 실행하거나 다시 실행하여 IaaS 구성 요소를 생성할 때마다 해당 IaaS 구성 요소에 대해 인증서 신뢰를 구성해야 합니다. 예를 들어 표준 설치 관리자를 사용하여 기존 배포를 확장할 수 있습니다.

■ IaaS Web 및 Manager Service 호스트

web.pfx 및 ms.pfx 파일을 다음 위치로 가져옵니다.

```
Host Computer/Certificates/Personal certificate store
Host Computer/Certificates/Trusted People certificate store
```

■ IaaS DEM Orchestrator, DEM 작업자 및 프록시 에이전트 호스트

web.pfx 및 ms.pfx 파일을 다음 위치로 가져옵니다.

Host Computer/Certificates/Trusted People certificate store

신뢰된 사용자 인증서 저장소에서는 인증서와 함께 개인 키를 가져올 필요가 없습니다. 자동 설치 프로세스는 신뢰된 사용자 인증서 저장소에 인증서만 설치합니다.

Web 구성 요소, Manager Service 및 DEM 호스트 인증서 신뢰 구성

사용자 인증 지원을 위해 미리 설치된 PFX 파일과 함께 지문을 사용하는 고객은 웹 호스트, Manager Service, DEM Orchestrator 및 작업자 호스트 시스템에서 엄지손가락 지문 신뢰를 구성해야 합니다.

PEM 파일을 가져오거나 자체 서명된 인증서를 사용하는 고객은 이 절차를 무시할 수 있습니다.

사전 요구 사항

엄지손가락 지문 인증에 사용할 수 있는 올바른 web.pfx 및 ms.pfx.

절차

- 1 web.pfx 파일과 ms.pfx 파일을 Web 구성 요소 및 Manager Service 호스트 시스템의 다음 위치로 가져옵니다.

- Host Computer/Certificates/Personal certificate store
- Host Computer/Certificates/Trusted People certificate store

- 2 web.pfx 파일과 ms.pfx 파일을 DEM Orchestrator 및 작업자 호스트 시스템의 다음 위치로 가져옵니다.

Host Computer/Certificates/Trusted People certificate store

- 3 해당하는 각 호스트 시스템에서 Microsoft 관리 콘솔 창을 엽니다.

참고 관리 콘솔의 실제 경로와 옵션은 Windows 버전과 시스템 구성에 따라 다소 다를 수 있습니다.

- a 스냅인 추가/제거를 선택합니다.
- b 인증서를 선택합니다.
- c 로컬 컴퓨터를 선택합니다.
- d 이전에 가져온 인증서 파일을 열고 엄지손가락 지문을 복사합니다.

다음에 수행할 작업

Manager Service, Web 구성 요소 및 DEM 구성 요소의 vRealize Automation 마법사 인증서 페이지에 엄지손가락 지문을 삽입합니다.

설치 워크시트

워크시트는 설치 중 참조해야 하는 중요한 정보를 기록합니다.

설정은 대/소문자를 구분합니다. 분산 배포를 설치하는 경우 더 많은 구성 요소를 위한 추가 공간이 있음에 유의해야 합니다. 워크시트의 모든 공간이 필요하지 않을 수 있습니다. 또한 시스템은 2개 이상의 IaaS 구성 요소를 호스팅할 수 있습니다. 예를 들어 기본 웹 서버 및 DEM Orchestrator는 동일한 FQDN에 있을 수 있습니다.

표 1-28. vRealize Automation 장치

변수	내 값	예
기본 vRealize Automation 장치 FQDN		automation.mycompany.com
기본 vRealize Automation 장치 IP 주소 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.1.105
추가 vRealize Automation 장치 FQDN		automation2.mycompany.com
추가 vRealize Automation 장치 IP 주소 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.1.106
vRealize Automation 장치 로드 밸런서 FQDN		automation-balance.mycompany.com
vRealize Automation 장치 로드 밸런서 IP 주소 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.1.201
관리 인터페이스(https://appliance-FQDN:5480) 사용자 이름	루트(기본값)	root
관리 인터페이스 암호		admin123
기본 테넌트	vsphere.local(기본값)	vsphere.local
기본 테넌트 사용자 이름	administrator@vsphere.local(기본값)	administrator@vsphere.local
기본 테넌트 암호		login123

표 1-29. IaaS Windows Server

변수	내 값	예
Model Manager Data FQDN이 포함된 기본 IaaS Web Server		web.mycompany.com
Model Manager Data IP 주소가 포함된 기본 IaaS Web Server 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.1.107
추가 IaaS Web Server FQDN		web2.mycompany.com
추가 IaaS Web Server IP 주소 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.1.108

표 1-29. IaaS Windows Server (계속)

변수	내 값	예
IaaS Web Server 로드 밸런서 FQDN		web-balance.mycompany.com
IaaS Web Server 로드 밸런서 IP 주소 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.1.202
액티브 IaaS Manager Service 호스트 FQDN		mgr-svc.mycompany.com
액티브 IaaS Manager Service 호스트 IP 주소 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.1.109
패시브 IaaS Manager Service 호스트 FQDN		mgr-svc2.mycompany.com
패시브 IaaS Manager Service 호스트 IP 주소 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.1.110
IaaS Manager Service 호스트 로드 밸런서 FQDN		mgr-svc-balance.mycompany.com
IaaS Manager Service 호스트 로드 밸런서 IP 주소 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.203
IaaS 서비스의 경우 호스트에 대한 관리자 권한을 가진 도메인 계정		SUPPORT\provisioner
계정 암호		login123

표 1-30. IaaS SQL Server 데이터베이스

변수	내 값	예
데이터베이스 인스턴스		IAASSQL
데이터베이스 이름	vcac(기본값)	vcac
암호(설치, 업그레이드 및 마이그레이션 시 사용됨)		login123

표 1-31. IaaS Distributed Execution Manager

변수	내 값	예
DEM 호스트 FQDN		dem.mycompany.com
DEM 호스트 IP 주소 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.1.111
DEM 호스트 FQDN		dem2.mycompany.com
DEM 호스트 IP 주소 오직 참조용, IP 주소를 입력하지 마십시오.		123.234.1.112
고유한 DEM Orchestrator 이름		Orchestrator-1
고유한 DEM Orchestrator 이름		Orchestrator-2
고유한 DEM 작업자 이름		Worker-1
고유한 DEM 작업자 이름		Worker-2
고유한 DEM 작업자 이름		Worker-3
고유한 DEM 작업자 이름		Worker-4

로드 밸런서 구성

vRealize Automation에 대해 장치를 배포한 후 로드 밸런서를 설정하여 vRealize Automation 장치의 여러 인스턴스 간에 트래픽을 분산할 수 있습니다.

다음 목록은 vRealize Automation 트래픽에 대한 로드 밸런서를 구성하는 데 필요한 일반적인 단계의 개요를 설명합니다.

- 1 로드 밸런서를 설치합니다.
- 2 고정 세션이라고도 하는 세션 신호도를 사용하도록 설정합니다.
- 3 로드 밸런서의 시간 제한이 100초 이상인지 확인합니다.
- 4 네트워크 또는 로드 밸런서에 필요한 경우 인증서를 로드 밸런서로 가져옵니다. 신뢰 관계 및 인증서에 대한 자세한 내용은 [분산 배포의 인증서 신뢰 요구 사항](#)을 참조하십시오. 인증서 추출에 대한 자세한 내용은 [인증서 및 개인 키 추출](#)을 참조하십시오.
- 5 vRealize Automation 장치 트래픽에 대해 로드 밸런서를 구성합니다.
- 6 vRealize Automation의 장치를 구성합니다. [vRealize Automation 장치 구성](#) 항목을 참조하십시오.

참고 vRealize Automation에서 사용하도록 구성된 가상 장치에 대해서만 로드 밸런서 아래에 가상 장치를 설정하십시오. 구성되지 않은 장치가 설정되면 오류 응답이 표시됩니다.

로드 밸런서에 대한 자세한 내용은 [vRealize Automation 로드 밸런싱](#)을 참조하십시오.

확장성과 고가용성에 대한 자세한 내용은 "vRealize Automation 참조 아키텍처" 가이드를 참조하십시오.

vRealize Automation 장치 구성

장치를 배포하고 로드 밸런싱을 구성한 후 vRealize Automation의 장치를 구성합니다.

클러스터의 첫 번째 vRealize Automation 장치 구성

vRealize Automation 장치는 vRealize Automation 서버 및 사용자 웹 포털을 호스팅하는 부분적으로 구성된 가상 시스템입니다. 장치 OVF(Open Virtualization Format) 템플릿을 다운로드하고 vCenter Server 또는 ESX/ESXi 인벤토리에 배포합니다.

사전 요구 사항

- 구성되지 않은 장치를 생성합니다. [vRealize Automation 장치 배포](#) 항목을 참조하십시오.
- vRealize Automation 장치에 대한 인증서를 가져옵니다.
네트워크나 로드 밸런서에 필요한 경우 이후 절차에서 인증서를 로드 밸런서 및 추가 장치에 복사합니다.

절차

- 1 구성되지 않은 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
모든 인증서 경고를 무시하고 계속합니다.
- 2 설치 마법사가 나타나면 마법사 대신 관리 인터페이스로 이동할 수 있도록 취소합니다.
- 3 **관리 > 시간 설정**을 선택하고 시간 동기화 소스를 설정합니다.

옵션	설명
호스트 시간	vRealize Automation 장치 ESXi 호스트에 동기화합니다.
시간 서버	외부 NTP(네트워크 시간 프로토콜) 서버 하나에 동기화합니다. NTP 서버의 FQDN 또는 IP 주소를 입력합니다.

모든 vRealize Automation 장치와 IaaS Windows Server를 동일한 시간 소스에 동기화해야 합니다. 한 vRealize Automation 배포 내에서 시간 소스를 혼용하지 마십시오.

4 vRA > 호스트 설정을 선택합니다.

옵션	작업
자동으로 해결	vRealize Automation 장치에 대한 현재 호스트의 이름을 지정하려면 자동으로 해결 을 선택합니다.
호스트 업데이트	새 호스트인 경우 호스트 업데이트 를 선택합니다. 호스트 이름 텍스트 상자에 vRealize Automation 장치의 FQDN(정규화된 도메인 이름)(<i>vra-hostname.domain.name</i>)을 입력합니다. 로드 밸런서를 사용하는 분산 배포의 경우 호스트 업데이트 를 선택합니다. 호스트 이름 텍스트 상자에 로드 밸런서 서버의 정규화된 도메인 이름(<i>vra-loadbalancername.domain.name</i>)을 입력합니다.

참고 호스트 업데이트를 사용하여 호스트 이름을 설정할 때마다 이 절차의 뒷부분에서 설명하는 대로 SSO 설정을 구성하십시오.

5 인증서 작업 메뉴에서 적절한 작업을 선택합니다.

PEM 형식의 인코딩된 인증서를 사용하는 경우(예: 분산된 환경)에는 **가져오기**를 선택합니다.

가져오는 인증서는 신뢰할 수 있어야 할 뿐 아니라 SAN(주체 대체 이름) 인증서를 통해 vRealize Automation 장치의 모든 인스턴스와 모든 로드 밸런서에 적용 가능해야 합니다.

인증 기관에 제출할 수 있는 새 인증서 CSR 요청을 생성하려면 **서명 요청 생성**을 선택합니다. CA는 CSR을 통해 올바른 값을 사용하여 사용자가 가져올 수 있는 인증서를 생성할 수 있습니다.

참고 인증서 체인을 사용하는 경우 다음 순서로 인증서를 지정합니다.

- 중간 CA 인증서에 의해 서명된 클라이언트/서버 인증서
- 하나 이상의 중간 인증서
- 루트 CA 인증서

옵션	작업
기존 유지	현재 SSL 구성을 그대로 둡니다. 이 옵션은 변경 사항을 취소할 때 선택합니다.
인증서 생성	<ol style="list-style-type: none"> 일반 이름 텍스트 상자에 표시되는 값은 페이지 위쪽 부분에 나타나는 호스트 이름입니다. vRealize Automation 장치의 추가 인스턴스를 사용할 수 있는 경우 FQDN이 인증서의 SAN 특성에 포함됩니다. 조직 이름(예: 회사 이름)을 조직 텍스트 상자에 입력합니다. 조직 구성 단위(예: 부서 이름 또는 위치)를 조직 구성 단위 텍스트 상자에 입력합니다. 두 글자의 ISO 3166 국가 코드(예: KO)를 국가 텍스트 상자에 입력합니다.

옵션	작업
서명 요청 생성	<ul style="list-style-type: none"> a 서명 요청 생성을 선택합니다. b 조직, 조직 구성 단위, 국가 코드 및 일반 이름 텍스트 상자의 내용을 검토합니다. 이러한 항목은 기존 인증서로부터 채워집니다. 필요한 경우 이러한 항목을 편집할 수 있습니다. c CSR 생성을 클릭하여 인증서 서명 요청을 생성한 후 생성된 CSR을 여기에 다운로드 링크를 클릭하여, 인증 기관에 보낼 수 있는 위치에 CSR을 저장하기 위한 대화상자를 엽니다. d 준비된 인증서를 받으면 가져오기를 클릭한 후 지침을 따라 인증서를 vRealize Automation에 가져옵니다.
가져오기	<ul style="list-style-type: none"> a 머리글 및 바닥글을 포함하여 BEGIN PRIVATE KEY에서 END PRIVATE KEY까지 인증서 값을 복사한 후 RSA 개인 키 텍스트 상자에 붙여 넣습니다. b 머리글 및 바닥글을 포함하여 BEGIN CERTIFICATE에서 END CERTIFICATE까지 인증서 값을 복사한 후 인증서 체인 텍스트 상자에 붙여 넣습니다. 인증서 값이 여러 개인 경우, 각 인증서에 대해 BEGIN CERTIFICATE 머리글과 END CERTIFICATE 바닥글을 포함합니다. <p>참고 체인 인증서의 경우 추가 특성이 사용 가능할 수 있습니다.</p> <ul style="list-style-type: none"> c (선택 사항) 인증서의 인증서 키가 암호를 사용하여 암호화된 경우에는 해당 암호를 복사하여 암호 텍스트 상자에 붙여 넣습니다.

6 설정 저장을 클릭하여 호스트 정보와 SSL 구성을 저장합니다.

7 네트워크 또는 로드 밸런서에 필요한 경우, 가져온 또는 새로 생성된 인증서를 가상 장치 로드 밸런서에 복사합니다.

인증서를 내보내려면 루트 SSH 액세스를 사용하도록 설정해야 합니다.

- a 이미 로그인되어 있지 않은 경우 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- b **관리** 탭을 클릭합니다.

- c **관리** 하위 메뉴를 클릭합니다.

- d **SSH 서비스 사용** 확인란을 선택합니다.

완료되었을 때 SSH를 사용하지 않으려면 확인란을 선택 해제합니다.

- e **관리자 SSH 로그인 사용** 확인란을 선택합니다.

완료되었을 때 SSH를 사용하지 않으려면 확인란을 선택 해제합니다.

- f **설정 저장**을 클릭합니다.

8 SSO 설정을 구성합니다.

9 서비스를 클릭합니다.

라이센스를 설치하거나 콘솔에 로그인하려면 먼저 모든 서비스가 실행되고 있어야 합니다. 일반적으로 약 10분 후에 시작됩니다.

참고 서비스를 시작을 모니터링하기 위해 장치에 로그인하고 `tail -f /var/log/vcac/catalina.out`을 실행할 수도 있습니다.

10 라이선스 정보를 입력합니다.

- a **vRA > 라이선싱**을 클릭합니다.
- b **라이선싱**을 클릭합니다.
- c 설치 파일을 다운로드할 때 함께 다운로드한 유효한 vRealize Automation 라이선스 키를 입력하고 **키 제출**을 클릭합니다.

참고 연결 오류가 발생하면 로드 밸런서에서 문제가 발생한 것일 수 있습니다. 로드 밸런서에 대한 네트워크 연결을 확인합니다.

11 메시징을 클릭합니다. 장치에 대한 구성 설정과 메시징 상태가 표시됩니다. 이러한 설정은 변경하지 마십시오.

12 원격 분석 탭을 클릭하여 VMware CEIP(고객 환경 향상 프로그램)에 참여할지 여부를 선택합니다.

CEIP를 통해 수집된 데이터에 대한 세부 정보 및 VMware에서 CEIP를 사용하는 목적이 Trust & Assurance Center의 <http://www.vmware.com/trustvmware/ceip.html>에 기술되어 있습니다.

- 프로그램에 참여하려면 **VMware 고객 환경 향상 프로그램에 참여**를 선택합니다.
- 프로그램에 참여하지 않으려면 **VMware 고객 환경 향상 프로그램에 참여**를 선택 취소합니다.

13 설정 저장을 클릭합니다.

14 vRealize Automation에 로그인할 수 있는지 확인합니다.

- a 브라우저를 열고 vRealize Automation 제품 인터페이스 URL로 이동합니다.
`https://vrealize-automation-appliance-FQDN/vcac`
- b 인증서 경고가 나타나는 경우 무시하고 계속합니다.
- c `administrator@vsphere.local` 및 SSO를 구성할 때 지정한 암호를 사용하여 로그인합니다.

인터페이스의 [테넌트] 페이지에서 **관리** 탭이 열립니다. 이름이 `vsphere.local`인 테넌트 하나가 목록에 표시됩니다.

vRealize Automation 장치의 추가 인스턴스 구성

시스템 관리자는 고가용성 환경에서 이중화를 보장하기 위해 vRealize Automation 장치의 여러 인스턴스를 배포할 수 있습니다.

각 vRealize Automation 장치에 대해 시간 동기화를 사용하도록 설정하고 장치를 클러스터에 추가해야 합니다. 장치를 클러스터에 추가할 때 초기(기본) vRealize Automation 장치의 설정에 기반한 구성 정보가 자동으로 추가됩니다.

고가용성과 페일오버를 위해 로드 밸런서와 함께 분산 설치를 설치하는 경우 vRealize Automation 환경 구성을 담당하는 팀에게 알려십시오. 테넌트 관리자는 Active Directory에 대한 링크를 구성할 때 고가용성을 위한 디렉토리 관리를 구성해야 합니다.

클러스터에 다른 vRealize Automation 장치 추가

고가용성을 위해 분산 설치에서는 vRealize Automation 장치 노드의 클러스터 앞에 로드 밸런서를 사용할 수 있습니다.

새 vRealize Automation 장치에서 관리 인터페이스를 사용하여 하나 이상의 장치의 기존 클러스터에 가입시킵니다. 가입 작업은 인증서, SSO, 라이선싱, 데이터베이스, 메시징 정보를 포함한 구성 정보를 추가하려는 새 장치에 복사합니다.

Active Directory—각 vRealize Automation 장치에는 사용자 인증을 지원하는 커넥터가 포함되어 있지만 일반적으로 하나의 커넥터만 디렉토리 동기화를 수행하도록 구성됩니다. 다른 장치를 추가한 후에는 추가된 장치에 해당하는 두 번째 커넥터를 구성해야 합니다. 두 번째 커넥터는 ID 제공자에 연결되고 동일한 Active Directory를 가리킵니다. 이렇게 하면 첫 번째 장치가 실패하는 경우 두 번째 장치가 사용자 인증 관리를 대신 수행합니다.

장치를 클러스터에 추가할 때에는 병렬 방식이 아니라 한 번에 하나씩 추가해야 합니다.

사전 요구 사항

- 클러스터에 하나 이상의 vRealize Automation 장치가 이미 있습니다. 이 중에서 하나는 기본 노드가 됩니다. [클러스터의 첫 번째 vRealize Automation 장치 구성](#) 항목을 참조하십시오.
- 새 장치를 클러스터에 가입시킨 후에만 새 장치를 기본 노드로 설정할 수 있습니다.
- 새 장치 노드를 생성합니다. [vRealize Automation 장치 배포](#) 항목을 참조하십시오.
- 로드 밸런서가 새 장치와 함께 사용하도록 구성되었는지 확인합니다.
- 트래픽이 로드 밸런서를 통과하여 모든 현재 노드 및 추가하려는 새 노드에 연결할 수 있는지 확인합니다.
- 모든 vRealize Automation 서비스가 현재 노드에서 시작되었는지 확인합니다.

절차

- 1 새 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

모든 인증서 경고를 무시하고 계속합니다.

- 2 설치 마법사가 나타나면 마법사 대신 관리 인터페이스로 이동할 수 있도록 취소합니다.
- 3 **관리 > 시간 설정**을 선택하고 시간 소스를 나머지 클러스터 장치가 사용하는 것과 같은 시간 소스로 설정합니다.
- 4 **vRA > 클러스터**를 선택합니다.

- 5 이전에 구성된 vRealize Automation 장치의 FQDN을 **선행 클러스터 노드** 텍스트 상자에 입력합니다.
기본 vRealize Automation 장치의 FQDN이나 클러스터에 이미 가입한 vRealize Automation 장치 중 하나의 FQDN을 사용할 수 있습니다.
- 6 **암호** 텍스트 상자에 루트 암호를 입력합니다.
- 7 **클러스터에 가입**을 클릭합니다.
- 8 모든 인증서 경고를 무시하고 계속합니다.
클러스터의 서비스가 다시 시작됩니다.
- 9 서비스가 실행 중인지 확인합니다.
 - a **서비스** 탭을 클릭합니다.
 - b **새로 고침** 탭을 클릭하여 서비스 시작 진행률을 모니터링합니다.

결과

[클러스터에 가입] 작업에 시간이 오래 걸려서 결국 시간이 초과되면 [VMware 기술 자료 문서 58708](#)을 참조하십시오.

사용되지 않는 서비스 사용 안 함

vRealize Orchestrator의 외부 인스턴스가 사용되는 경우 내부 리소스를 절약하기 위해 포함된 vRealize Orchestrator 서비스를 사용하지 않도록 설정할 수 있습니다.

사전 요구 사항

[클러스터에 다른 vRealize Automation 장치 추가](#)

절차

- 1 vRealize Automation 장치 콘솔에 로그인합니다.
- 2 vRealize Orchestrator 서비스를 중지합니다.

```
service vco-server stop
chkconfig vco-server off
```

분산 배포 검증

vRealize Automation 장치의 추가 인스턴스를 배포한 후에는 클러스터된 장치에 액세스할 수 있는지 검증합니다.

절차

- 1 로드 밸런서 관리 인터페이스 또는 구성 파일에서 현재 테스트 중인 노드를 제외한 모든 노드를 임시로 사용하지 않도록 설정합니다.
- 2 로드 밸런서 주소를 통해 vRealize Automation에 로그인할 수 있는지 확인합니다.

<https://vrealize-automation-appliance-load-balancer-FQDN/vcac>

- 3 로드 밸런서를 통해 새 vRealize Automation 장치에 액세스할 수 있는지 확인한 후 다른 노드를 다시 사용하도록 설정합니다.

분산 구성에서 IaaS 구성 요소 설치

장치가 배포되고 완전하게 구성된 이후에 시스템 관리자가 IaaS 구성 요소를 설치합니다. IaaS 구성 요소는 vRealize Automation 인프라 기능에 대한 액세스를 제공합니다.

모든 구성 요소가 동일한 서비스 계정 사용자로 실행되어야 하며, 이 계정은 각 분산 IaaS 서버에 대한 권한이 있는 도메인 계정이어야 합니다. 로컬 시스템 계정을 사용하지 마십시오.

사전 요구 사항

- 클러스터의 첫 번째 vRealize Automation 장치 구성.
- 사이트에 여러 vRealize Automation 장치가 포함되어 있으면 클러스터에 다른 vRealize Automation 장치 추가.
- 서버가 IaaS Windows Server의 요구 사항을 충족하는지 확인합니다.
- 구성 요소 웹 사이트 및 Model Manager 데이터를 설치하고자 하는 시스템의 신뢰할 수 있는 루트 인증서 저장소로 가져올 인증서를 신뢰할 수 있는 인증 기관에서 가져옵니다.
- 환경에서 로드 밸런서를 사용하는 경우, 해당 로드 밸런서가 구성 요구 사항을 충족하는지 확인합니다.

절차

1 IaaS 인증서 설치

운영 환경인 경우 신뢰할 수 있는 인증 기관에서 도메인 인증서를 가져옵니다. IaaS를 설치하는 동안 Website 구성 요소와 Manager Service(IIS 시스템)를 설치하려는 모든 시스템의 신뢰할 수 있는 루트 인증서 저장소에 이 인증서를 가져옵니다.

2 vRealize Automation IaaS 설치 관리자 다운로드

분산 가상 또는 물리적 Windows Server에 IaaS를 설치하려면 vRealize Automation 장치에서 IaaS 설치 관리자의 사본을 다운로드합니다.

3 IaaS 데이터베이스 선택 시나리오

vRealize Automation IaaS는 관리하는 시스템에 대한 정보 및 고유한 해당 요소와 정책을 유지하기 위해 Microsoft SQL Server 데이터베이스를 사용합니다.

4 IaaS 웹 사이트 구성 요소 및 Model Manager Data 설치

시스템 관리자는 vRealize Automation 웹 콘솔의 인프라 기능에 대한 액세스를 제공하기 위해 웹 사이트 구성 요소를 설치합니다. 웹 사이트 구성 요소의 인스턴스는 하나만 설치하거나 여러 개 설치할 수 있지만 그러기 위해서는 첫 번째 웹 사이트 구성 요소를 호스팅하는 시스템에 Model Manager Data를 반드시 구성해야 합니다. Model Manager Data는 한 번만 설치합니다.

5 추가 IaaS 웹 서버 구성 요소 설치

웹 서버는 vRealize Automation의 인프라 기능에 대한 액세스를 제공합니다. 첫 번째 웹 서버를 설치한 후 IaaS 웹 서버를 추가로 설치하여 성능을 늘릴 수 있습니다.

6 활성화 Manager Service 설치

활성 Manager Service는 IaaS Distributed Execution Manager, 데이터베이스, 에이전트, 프록시 에이전트와 SMTP 간 통신을 조정하는 Windows 서비스입니다.

7 백업 Manager Service 구성 요소 설치

백업 Manager Service는 이중화 및 고가용성을 제공하며 활성 서비스가 중지되는 경우 수동으로 시작할 수 있습니다.

8 Distributed Execution Manager 설치

Distributed Execution Manager는 두 가지 역할인 DEM 조정자 또는 DEM 작업자 중 하나로 설치합니다. 각 역할에는 DEM 인스턴스를 하나 이상 설치해야 하며, 페일오버 및 고가용성을 지원하기 위해 DEM 인스턴스를 추가적으로 설치할 수 있습니다.

9 IaaS 데이터베이스 액세스를 위한 Windows 서비스 구성

시스템 관리자는 실행 시간 동안 SQL 데이터베이스에 액세스하는 데 사용되는 인증 방법을 변경할 수 있습니다(설치 완료 후). 기본적으로, 현재 로그인한 계정의 Windows ID가 설치 후 데이터베이스 연결에 사용됩니다.

10 IaaS 서비스 확인

설치 후 시스템 관리자는 IaaS 서비스가 실행 중인지 확인합니다. 서비스가 실행 중이면 설치가 성공한 것입니다.

다음에 수행할 작업

DEM 조정자 및 하나 이상의 DEM 작업자 인스턴스를 설치합니다. [Distributed Execution Manager 설치](#) 항목을 참조하십시오.

IaaS 인증서 설치

운영 환경인 경우 신뢰할 수 있는 인증 기관에서 도메인 인증서를 가져옵니다. IaaS를 설치하는 동안 Website 구성 요소와 Manager Service(IIS 시스템)를 설치하려는 모든 시스템의 신뢰할 수 있는 루트 인증서 저장소에 이 인증서를 가져옵니다.

사전 요구 사항

Windows 2012 시스템에서, SHA512를 사용하는 인증서에 대해 TLS1.2를 사용하지 않도록 설정해야 합니다. TLS1.2를 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 [Microsoft 기술 자료 문서 245030](#) 항목을 참조하십시오.

절차

- 1 신뢰할 수 있는 인증 기관의 인증서를 가져옵니다.
- 2 IIS(인터넷 정보 서비스) 관리자를 엽니다.
- 3 기능 보기에서 **서버 인증서**를 두 번 클릭합니다.

4 작업 창에서 **가져오기**를 클릭합니다.

- a **인증서 파일** 텍스트 상자에 파일 이름을 입력하거나 찾아보기 버튼 (...)을 클릭하여 내보낸 인증서가 저장된 파일의 이름으로 이동합니다.
- b 인증서를 암호와 함께 내보낸 경우 **암호** 텍스트 상자에 암호를 입력합니다.
- c **이 키를 내보내기 가능으로 표시**를 선택합니다.

5 **확인**을 클릭합니다.**6** 가져온 인증서를 클릭하고 **보기**를 선택합니다.**7** 인증서와 체인을 신뢰할 수 있는지 확인합니다.

인증서를 신뢰할 수 없는 경우 이 **CA** 루트 인증서를 신뢰할 수 없습니다. 메시지가 표시됩니다.

참고 설치를 계속하기 전에 신뢰 문제를 해결해야 합니다. 계속하면 배포가 실패합니다.

8 IIS를 다시 시작하거나 상승된 명령 프롬프트 창을 열고 **iisreset**를 입력합니다.

다음에 수행할 작업

[vRealize Automation IaaS 설치 관리자 다운로드.](#)

vRealize Automation IaaS 설치 관리자 다운로드

분산 가상 또는 물리적 Windows Server에 IaaS를 설치하려면 vRealize Automation 장치에서 IaaS 설치 관리자의 사본을 다운로드합니다.

이 프로세스 중에 인증서 경고가 표시되면 경고를 무시하고 계속하여 설치를 마칩니다.

사전 요구 사항

- 클러스터의 첫 번째 vRealize Automation 장치 구성 및 클러스터에 다른 vRealize Automation 장치 추가(선택 사항)을 수행합니다.
- 서버가 **IaaS Windows Server**의 요구 사항을 충족하는지 확인합니다.
- IIS로 인증서를 가져오고, 인증서 루트 또는 인증 기관이 설치 시스템의 신뢰할 수 있는 루트에 있는지 확인합니다.
- 환경에서 로드 밸런서를 사용하는 경우, 해당 로드 밸런서가 구성 요구 사항을 충족하는지 확인합니다.

절차

1 (선택 사항) Windows 2012 시스템에 설치하는 경우, HTTP를 활성화합니다.

- a [서버 관리자]에서 **기능 > 기능 추가**를 선택합니다.
- b .NET Framework 기능 아래에서 **WCF 서비스**를 확장합니다.
- c **HTTP 활성화**를 선택합니다.

2 관리자 권한이 있는 계정을 사용하여 IaaS Windows Server에 로그인합니다.

- 3 웹 브라우저에서 바로 vRealize Automation 장치 설치 관리자 URL을 엽니다. 로드 밸런서 주소를 사용하지 마십시오.

`https://vrealize-automation-appliance-FQDN:5480/installer`

- 4 **IaaS 설치 관리자**를 클릭합니다.

- 5 `setup__vrealize-automation-appliance-FQDN@5480`을 Windows Server에 저장합니다.

설치 관리자 파일 이름을 변경하지 마십시오. 이는 설치를 vRealize Automation 장치에 연결하는 데 사용됩니다.

- 6 구성 요소를 설치하는 각 IaaS Windows Server로 설치 관리자 파일을 다운로드합니다.

다음에 수행할 작업

IaaS 데이터베이스를 설치합니다(IaaS 데이터베이스 선택 시나리오 참조).

IaaS 데이터베이스 선택 시나리오

vRealize Automation IaaS는 관리하는 시스템에 대한 정보 및 고유한 해당 요소와 정책을 유지하기 위해 Microsoft SQL Server 데이터베이스를 사용합니다.

기본 설정 및 권한에 따라 IaaS 데이터베이스 선택에서 생성까지 여러 절차가 있습니다.

참고 SQL 데이터베이스를 생성하거나 업그레이드할 때 보안 SSL을 사용하도록 설정할 수 있습니다. 예를 들어 SQL 데이터베이스를 생성하거나 업그레이드하는 경우, SQL 데이터베이스에 연결할 때 SQL Server에 이미 지정된 SSL 구성이 적용되도록 지정하는 데 보안 SSL 옵션을 사용할 수 있습니다. SSL은 IaaS 서버와 SQL 데이터베이스 간에 보다 안전한 연결을 제공합니다. 사용자 지정 설치 마법사에서 제공되는 이 옵션을 사용하려면 이미 SQL Server에 SSL이 구성되어 있어야 합니다. SQL Server에서 SSL 구성과 관련된 정보는 [Microsoft Technet 문서 189067](#) 항목을 참조하십시오.

표 1-32. IaaS 데이터베이스 선택 시나리오

시나리오	절차
제공된 데이터베이스 스크립트를 사용하여 수동으로 IaaS 데이터베이스를 생성합니다. 이 옵션을 사용하면 데이터베이스 관리자가 데이터베이스를 생성하기 전에 변경 내용을 자세히 검토할 수 있습니다.	수동으로 IaaS 데이터베이스 생성.
빈 데이터베이스를 준비하고 설치 관리자를 사용하여 데이터베이스 스키마를 채웁니다. 이 옵션을 사용하면 설치 관리자가 dbo 권한을 가진 데이터베이스 사용자를 사용하여 데이터베이스를 채울 수 있습니다.	빈 데이터베이스 준비.
설치 관리자를 사용하여 데이터베이스를 생성합니다. 이는 가장 간단한 옵션이지만 설치 관리자에서 sysadmin 권한을 사용해야 합니다.	설치 마법사를 사용하여 IaaS 데이터베이스 생성.

수동으로 IaaS 데이터베이스 생성

vRealize Automation 시스템 관리자는 VMware 제공 스크립트를 사용하여 수동으로 데이터베이스를 생성할 수 있습니다.

사전 요구 사항

- SQL Server 호스트에 Microsoft .NET Framework 4.5.2 이상을 설치합니다.
- SQL 인증이 아닌 Windows 인증을 사용하여 데이터베이스에 연결합니다.
- 데이터베이스 설치 사전 요구 사항을 확인합니다. [IaaS SQL Server 호스트](#) 항목을 참조하십시오.
- 웹 브라우저를 열고 vRealize Automation 장치 설치 관리자 URL로 이동한 후 IaaS 데이터베이스 설치 스크립트를 다운로드합니다.

<https://vrealize-automation-appliance-FQDN:5480/installer>

절차

- 1 설치 Zip 아카이브를 추출한 Database 하위 디렉토리로 이동합니다.
- 2 DBInstall.zip 아카이브를 로컬 디렉토리에 추출합니다.
- 3 충분한 권한으로 Windows 데이터베이스 호스트에 로그인하여 SQL Server 인스턴스에서 데이터베이스 **sysadmin** 권한을 생성 및 삭제합니다.
- 4 필요에 따라 데이터베이스 배포 스크립트를 검토합니다. 특히 CreateDatabase.sql의 DBSettings 섹션 설정을 검토하고 필요한 경우 설정을 편집합니다.

스크립트의 설정이 권장 설정입니다. ALLOW_SNAPSHOT_ISOLATION ON 및 READ_COMMITTED_SNAPSHOT ON만 필수 항목입니다.

- 5 테이블에 설명된 인수를 사용하여 다음 명령을 실행합니다.

```
BuildDB.bat /p:DBServer=db_server;
DBName=db_name;DBDir=db_dir;
LogDir=[ log_dir];ServiceUser=service_user;
ReportLogin=web_user;
VersionString=version_string
```

표 1-33. 데이터베이스 값

변수	값
<i>db_server</i>	dbhostname[,port number]\SQL instance 형식으로 SQL Server 인스턴스를 지정합니다. 기본이 아닌 포트를 사용 중인 경우에만 포트 번호를 지정합니다. Microsoft SQL 기본 포트 번호는 1433입니다. <i>db_server</i> 의 기본값은 localhost입니다.
<i>db_name</i>	데이터베이스의 이름. 기본값은 vra 입니다. 데이터베이스 이름은 128자(ASCII 문자)를 넘지 않아야 합니다.
<i>db_dir</i>	마지막 슬래시를 제외한 데이터베이스의 데이터 디렉토리 경로.
<i>log_dir</i>	마지막 슬래시를 제외한 데이터베이스의 로그 디렉토리 경로.
<i>service_user</i>	Manager Service를 실행하는 사용자 이름.

표 1-33. 데이터베이스 값 (계속)

변수	값
<code>Web_user</code>	Web Services를 실행하는 사용자 이름.
<code>version_string</code>	vRealize Automation 버전. vRealize Automation 장치에 로그인하고 [업데이트] 탭을 클릭하면 확인할 수 있습니다. 예를 들어 vRealize Automation 6.1 버전 문자열은 6.1.0.1200입니다.

결과

데이터베이스가 생성되었습니다.

다음에 수행할 작업

분산 구성에서 **laaS 구성 요소 설치**.

빈 데이터베이스 준비

vRealize Automation 시스템 관리자는 **laaS** 스키마를 임의의 빈 데이터베이스에 설치할 수 있습니다. 이 설치 방법을 사용하면 데이터베이스 보안에 대한 제어 기능을 극대화할 수 있습니다.

사전 요구 사항

- 데이터베이스 설치 사전 요구 사항을 확인합니다. **laaS SQL Server 호스트** 항목을 참조하십시오.
- 웹 브라우저를 열고 vRealize Automation 장치 설치 관리자 URL로 이동한 후 **laaS** 데이터베이스 설치 스크립트를 다운로드합니다.

<https://vrealize-automation-appliance-FQDN:5480/installer>

절차

- 1 설치 zip 아카이브를 추출한 디렉토리 내의 **Database** 디렉토리로 이동합니다.
- 2 **DBInstall.zip** 아카이브를 로컬 디렉토리에 추출합니다.
- 3 SQL Server 인스턴스 내에서 **sysadmin** 권한을 사용하여 Windows 데이터베이스 호스트에 로그인합니다.
- 4 다음 파일을 편집하고 테이블에 있는 변수의 모든 인스턴스를 환경에 맞는 올바른 값으로 바꿉니다.

```
CreateDatabase.sql
SetDatabaseSettings.sql
```

표 1-34. 데이터베이스 값

변수	값
<code>\$(DBName)</code>	데이터베이스의 이름(예: <code>vra</code>). 데이터베이스 이름은 128자(ASCII 문자)를 넘지 않아야 합니다.
<code>\$(DBDir)</code>	마지막 슬래시를 제외한 데이터베이스의 데이터 디렉토리 경로.
<code>\$(LogDir)</code>	마지막 슬래시를 제외한 데이터베이스의 로그 디렉토리 경로.

- 5 `SetDatabaseSettings.sql`의 DB 설정 섹션에서 설정을 검토하고 필요한 경우 편집합니다.

스크립트의 설정은 IaaS 데이터베이스에 대해 권장되는 설정입니다. `ALLOW_SNAPSHOT_ISOLATION` 및 `READ_COMMITTED_SNAPSHOT ON`된 필요합니다.

- 6 SQL Server Management Studio를 엽니다.

- 7 새 쿼리를 클릭합니다.

SQL 쿼리 창이 열립니다.

- 8 쿼리 메뉴에서 **SQLCMD 모드**가 선택되었는지 확인합니다.

- 9 `CreateDatabase.sql`의 수정된 모든 콘텐츠를 쿼리 창에 붙여 넣습니다.

- 10 `CreateDatabase.sql` 콘텐츠 아래에 수정된 `SetDatabaseSettings.sql`의 전체 콘텐츠를 붙여 넣습니다.

- 11 실행을 클릭합니다.

스크립트가 실행되어 데이터베이스를 생성합니다.

다음에 수행할 작업

분산 구성에서 IaaS 구성 요소 설치.

설치 마법사를 사용하여 IaaS 데이터베이스 생성

vRealize Automation은 Microsoft SQL Server 데이터베이스를 사용하여 관리하는 시스템에 대한 정보, 자체 요소 및 정책을 유지합니다.

다음 단계는 설치 관리자를 사용하여 IaaS 데이터베이스를 생성하거나 기존의 빈 데이터베이스를 채우는 방법에 대해 설명합니다. 데이터베이스를 수동으로 생성할 수도 있습니다. 수동으로 IaaS 데이터베이스 생성 항목을 참조하십시오.

사전 요구 사항

- SQL 인증이 아닌 Windows 인증을 사용하여 데이터베이스를 생성 중인 경우 설치 관리자를 실행하는 사용자에게 SQL Server에 대한 **sysadmin** 권한이 있는지 확인합니다.
- [vRealize Automation IaaS 설치 관리자 다운로드](#).

절차

- 1 `setup__vrealize-automation-appliance-FQDN@5480.exe` 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 2 **다음**을 클릭합니다.
- 3 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 4 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.
 - a 사용자 이름(**root**)과 암호를 입력합니다.
암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.
 - b **인증서 수락**을 선택합니다.
 - c **인증서 보기**를 클릭합니다.
인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.
- 5 **다음**을 클릭합니다.
- 6 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.
- 7 [설치 유형] 페이지의 [구성 요소 선택] 아래에서 **IaaS 서버**를 선택합니다.
- 8 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.
분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다.
IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.
- 9 **다음**을 클릭합니다.
- 10 IaaS 서버 사용자 지정 설치 페이지에서 **데이터베이스**를 선택합니다.
- 11 **데이터베이스 인스턴스** 텍스트 상자에서 데이터베이스 인스턴스를 지정하거나 **검색**을 클릭하고 인스턴스 목록에서 선택합니다. 데이터베이스 인스턴스가 기본이 아닌 포트에 있는 경우 `dbhost,SQL_port_number\SQLinstance` 형식을 사용하여 인스턴스 규격에 포트 번호를 포함시킵니다. Microsoft SQL 기본 포트 번호는 1443입니다.
- 12 (선택 사항) **데이터베이스 연결에 SSL 사용** 확인란을 선택합니다.
기본적으로 이 확인란은 사용하도록 설정되어 있습니다. SSL은 IaaS 서버와 SQL 데이터베이스 간에 보다 안전한 연결을 제공합니다. 그러나 이 옵션을 지원하려면 먼저 SQL Server에서 SSL을 구성해야 합니다. SQL Server에서 SSL 구성에 대한 자세한 내용은 [Microsoft Technet 문서 189067](#) 항목을 참조하십시오.
- 13 **데이터베이스 이름** 패널에서 데이터베이스 설치 유형을 선택합니다.
 - 기존 데이터베이스에서 스키마를 생성하려면 **기존의 빈 데이터베이스 사용**을 선택합니다.

- 새 데이터베이스 이름을 입력하거나 기본 이름 **vra**를 사용하여 새 데이터베이스를 생성합니다. 데이터베이스 이름은 128자(ASCII 문자)를 넘지 않아야 합니다.

14 기본 데이터 및 로그 디렉토리 사용을 선택 해제하고 대체 위치를 지정하거나 선택된 상태로 두고 기본 디렉토리를 사용합니다(권장).

15 인증 목록에서 데이터베이스 설치를 위한 인증 방법을 선택합니다.

- 설치 관리자를 실행 중인 자격 증명을 사용하여 데이터베이스를 생성하려면 **Windows ID 사용...**을 선택합니다.
- SQL 인증을 사용하려면 **Windows ID 사용...**을 선택 해제합니다. 사용자 및 암호 텍스트 상자에 SQL 자격 증명을 입력합니다.

기본적으로, 데이터베이스에 대한 런타임 액세스 동안에는 Windows 서비스 사용자 계정이 사용됩니다. 이 계정에는 SQL Server 인스턴스에 대한 sysadmin 권한이 있어야 합니다. 런타임 시 데이터베이스 액세스에 사용되는 자격 증명에서 SQL 자격 증명을 사용하도록 구성할 수 있습니다.

Windows 인증을 사용하는 것이 좋습니다. SQL 인증을 선택하면 암호화되지 않은 데이터베이스 암호가 특정 구성 파일에 나타납니다.

16 다음을 클릭합니다.

17 사전 요구 사항 확인을 완료합니다.

옵션	설명
오류 없음	다음을 클릭합니다.
심각하지 않은 오류	무시를 클릭합니다.
심각한 오류	심각한 오류를 무시하면 설치가 실패합니다. 경고가 표시되면 왼쪽 창에서 경고를 선택한 다음 오른쪽에 있는 지침을 따릅니다. 심각한 오류를 모두 해결하고 다시 확인 을 클릭하여 확인합니다.

18 설치를 클릭합니다.

19 성공 메시지가 나타나면 **초기 구성 과정 안내**를 선택 해제하고 **다음**을 클릭합니다.

20 완료를 클릭합니다.

결과

데이터베이스를 사용할 준비가 되었습니다.

IaaS 웹 사이트 구성 요소 및 Model Manager Data 설치

시스템 관리자는 vRealize Automation 웹 콘솔의 인프라 기능에 대한 액세스를 제공하기 위해 웹 사이트 구성 요소를 설치합니다. 웹 사이트 구성 요소의 인스턴스는 하나만 설치하거나 여러 개 설치할 수 있지만 그러기 위해서는 첫 번째 웹 사이트 구성 요소를 호스팅하는 시스템에 Model Manager Data를 반드시 구성해야 합니다. Model Manager Data는 한 번만 설치합니다.

사전 요구 사항

- IaaS 데이터베이스를 설치합니다(IaaS 데이터베이스 선택 시나리오 참조).

- 다른 IaaS 구성 요소를 이미 설치했다면 생성한 데이터베이스 암호를 알고 있는지 확인합니다.
- 환경에서 로드 밸런서를 사용하는 경우, 해당 로드 밸런서가 구성 요구 사항을 충족하는지 확인합니다.

절차

1 첫 번째 IaaS 웹 서버 구성 요소 설치

IaaS 웹 서버 구성 요소를 설치하여 vRealize Automation의 인프라 기능에 대한 액세스를 제공합니다.

2 Model Manager Data 구성

첫 번째 웹 서버 구성 요소를 호스팅하는 동일한 시스템에서 Model Manager 구성 요소를 설치합니다. Model Manager Data를 한 번만 설치합니다.

결과

추가 웹 사이트 구성 요소를 설치하거나 Manager Service를 설치할 수 있습니다. [추가 IaaS 웹 서버 구성 요소 설치](#) 또는 [활성 Manager Service 설치](#) 항목을 참조하십시오.

첫 번째 IaaS 웹 서버 구성 요소 설치

IaaS 웹 서버 구성 요소를 설치하여 vRealize Automation의 인프라 기능에 대한 액세스를 제공합니다.

여러 IaaS 웹 서버를 설치할 수 있지만 첫 번째 웹 서버에만 Model Manager Data가 포함됩니다.

사전 요구 사항

- [설치 마법사를 사용하여 IaaS 데이터베이스 생성](#).
- 서버가 [IaaS Windows Server](#)의 요구 사항을 충족하는지 확인합니다.
- 다른 IaaS 구성 요소를 이미 설치했다면 생성한 데이터베이스 암호를 알고 있는지 확인합니다.
- 환경에서 로드 밸런서를 사용하는 경우, 해당 로드 밸런서가 구성 요구 사항을 충족하는지 확인합니다.

절차

- 1 로드 밸런서를 사용하는 경우, 로드 밸런서 아래의 다른 노드를 사용하지 않도록 설정하고 트래픽이 원하는 노드로 전달되는지 확인합니다.

또한, 모든 vRealize Automation 구성 요소가 설치되고 구성될 때까지 로드 밸런서 상태 점검을 사용하지 않도록 설정합니다.

- 2 `setup__vrealize-automation-appliance-FQDN@5480.exe` 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

- 3 **다음**을 클릭합니다.

- 4 라이선스 계약에 동의하고 **다음**을 클릭합니다.

- 5 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.

a 사용자 이름(**root**)과 암호를 입력합니다.

암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.

b **인증서 수락**을 선택합니다.

c **인증서 보기**를 클릭합니다.

인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.

- 6 다음을 클릭합니다.

- 7 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.

- 8 [설치 유형] 페이지의 [구성 요소 선택] 아래에서 **IaaS 서버**를 선택합니다.

- 9 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.

분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다.

IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.

- 10 다음을 클릭합니다.

- 11 **IaaS 서버 사용자 지정 설치** 페이지에서 **웹 사이트** 및 **ModelManagerData**를 선택합니다.

- 12 **관리 및 Model Manager 웹 사이트** 탭에서 기본 웹 사이트를 수락하거나, 사용 가능한 웹 사이트 중에서 웹 사이트를 선택합니다.

- 13 사용 가능한 포트 번호를 **포트 번호** 텍스트 상자에 입력하거나, 기본 포트 443을 수락합니다.

- 14 **바인딩 테스트**를 클릭하여 해당 포트 번호가 사용 가능한지 확인합니다.

- 15 이 구성 요소의 인증서를 선택합니다.

a 설치를 시작한 이후에 인증서를 가져온 경우에는 **새로 고침**을 클릭하여 목록을 업데이트합니다.

b **사용 가능한 인증서**에서 사용할 인증서를 선택합니다.

c 알기 쉬운 인증서 이름이 아니거나 인증서가 목록에 표시되지 않는 경우, **알기 쉬운 이름을 사용하는 인증서 표시**의 선택을 취소하고 **새로 고침**을 클릭합니다.

로드 밸런서를 사용하지 않는 환경에 설치하는 경우에는 인증서를 선택하는 대신 **자체 서명된 인증서 생성**을 선택할 수 있습니다. 로드 밸런서 뒤에 추가적인 웹 사이트 구성 요소를 설치하는 경우에는 자체 서명된 인증서를 생성하지 마십시오. 이 경우에는 로드 밸런서 뒤에 있는 모든 서버에 동일한 인증서를 사용하도록 기본 IaaS 웹 서버에서 인증서를 가져와야 합니다.

- 16 (선택 사항) **인증서 보기**를 클릭하여 인증서를 본 후 **확인**을 클릭하여 정보 창을 닫습니다.

- 17 (선택 사항)** 인증서 오류를 표시하지 않으려면 **인증서 불일치 표시 안 함**을 선택합니다. 이렇게 하면 인증서 이름 불일치 오류뿐 아니라 모든 원격 인증서 해지 목록 일치 오류가 설치 과정 중에 무시됩니다.
- 이 옵션은 보안 수준이 낮습니다.

Model Manager Data 구성

첫 번째 웹 서버 구성 요소를 호스팅하는 동일한 시스템에서 Model Manager 구성 요소를 설치합니다. Model Manager Data를 한 번만 설치합니다.

사전 요구 사항

첫 번째 **IaaS 웹 서버 구성 요소 설치**.

절차

- Model Manager Data** 탭을 클릭합니다.
- 서버** 텍스트 상자에 vRealize Automation 장치 FQDN(정규화된 도메인 이름)을 입력합니다.
vrealize-automation-appliance.mycompany.com
IP 주소를 입력하지 마십시오.
- 로드**를 클릭하여 **SSO 기본 테넌트**를 표시합니다.
Single Sign-On을 구성할 때 **vsphere.local** 기본 테넌트가 자동으로 생성됩니다. 이를 수정하지 마십시오.
- 다운로드**를 클릭하여 가상 장치에서 인증서를 가져옵니다.
인증서를 다운로드하려면 몇 분 정도 소요될 수 있습니다.
- (선택 사항) **인증서 보기**를 클릭하여 인증서를 본 후 **확인**을 클릭하여 정보 창을 닫습니다.
- 인증서 수락**을 클릭합니다.
- 사용자 이름** 텍스트 상자에 **administrator@vsphere.local**을 입력하고 **암호** 및 **확인** 텍스트 상자에 SSO를 구성했을 때 생성한 암호를 입력합니다.
- (선택 사항) **테스트**를 클릭하여 자격 증명을 확인합니다.
- IaaS 서버** 텍스트 상자에서 IaaS 웹 서버 구성 요소를 식별합니다.

옵션	설명
로드 밸런서를 사용하는 경우	IaaS 웹 서버 구성 요소에 대한 로드 밸런서의 정규화된 도메인 이름 및 포트 번호를 입력합니다(<i>web-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	IaaS 웹 서버 구성 요소를 설치한 시스템의 정규화된 도메인 이름 및 포트 번호를 입력합니다(<i>web.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

- 10 테스트**를 클릭하여 서버 연결을 확인합니다.

11 다음을 클릭합니다.

12 사전 요구 사항 확인을 완료합니다.

옵션	설명
오류 없음	다음을 클릭합니다.
심각하지 않은 오류	무시를 클릭합니다.
심각한 오류	심각한 오류를 무시하면 설치가 실패합니다. 경고가 표시되면 왼쪽 창에서 경고를 선택한 다음 오른쪽에 있는 지점을 따릅니다. 심각한 오류를 모두 해결하고 다시 확인 을 클릭하여 확인합니다.

13 [서버 및 계정 설정] 페이지의 **서버 설치 정보** 텍스트 상자에 현재 설치 서버에 대한 관리 권한이 있는 서비스 계정 사용자의 사용자 이름과 암호를 입력합니다.

서비스 계정 사용자는 각 분산 IaaS 서버에 대한 권한이 있는 하나의 도메인 계정이어야 합니다. 로컬 시스템 계정을 사용하지 마십시오.

14 데이터베이스를 보호하는 암호화 키 생성에 사용되는 암호를 제공합니다.

옵션	설명
이 환경에 구성 요소를 이미 설치한 경우	이전에 암호 및 확인 텍스트 상자에서 생성한 암호를 입력합니다.
첫 번째 설치인 경우	암호 및 확인 텍스트 상자에 암호를 입력합니다. 이 암호는 새 구성 요소를 설치할 때마다 사용해야 합니다.

나중에 사용할 수 있도록 이 암호를 안전한 위치에 두어야 합니다.

15 IaaS 데이터베이스 서버, 데이터베이스 이름 및 데이터베이스 서버의 인증 방법을 **Microsoft SQL 데이터베이스 설치 정보** 텍스트 상자에 지정합니다.

이는 앞서 생성한 IaaS 데이터베이스 서버, 이름 및 인증 정보입니다.

16 다음을 클릭합니다.

17 설치를 클릭합니다.

18 설치가 완료되면 **초기 구성 과정 안내**의 선택을 취소하고 **다음**을 클릭합니다.

다음에 수행할 작업

추가 웹 서버 구성 요소를 설치하거나 Manager Service를 설치할 수 있습니다. [추가 IaaS 웹 서버 구성 요소 설치](#) 또는 [활성 Manager Service 설치](#) 항목을 참조하십시오.

추가 IaaS 웹 서버 구성 요소 설치

웹 서버는 vRealize Automation의 인프라 기능에 대한 액세스를 제공합니다. 첫 번째 웹 서버를 설치한 후 IaaS 웹 서버를 추가로 설치하여 성능을 늘릴 수 있습니다.

Model Manager Data를 추가 웹 서버 구성 요소와 함께 설치하지 마십시오. 첫 번째 웹 서버 구성 요소만 Model Manager Data를 호스팅합니다.

사전 요구 사항

- **laaS 웹 사이트 구성 요소 및 Model Manager Data 설치.**
- 새 서버가 **laaS Windows Server**의 요구 사항을 충족하는지 확인합니다.
- vRealize Automation 장치 관리 인터페이스를 사용하여 새 노드의 FQDN을 포함하도록 인증서를 대체합니다. **vRealize Automation 장치의 인증서 교체**를 참조하십시오.
- 다른 laaS 구성 요소를 이미 설치했다면 생성한 데이터베이스 암호를 알고 있는지 확인합니다.
- 환경에서 로드 밸런서를 사용하는 경우, 해당 로드 밸런서가 구성 요구 사항을 충족하는지 확인합니다.

절차

- 1 로드 밸런서를 사용하는 경우, 로드 밸런서 아래의 다른 노드를 사용하지 않도록 설정하고 트래픽이 원하는 노드로 전달되는지 확인합니다.

또한, 모든 vRealize Automation 구성 요소가 설치되고 구성될 때까지 로드 밸런서 상태 점검을 사용하지 않도록 설정합니다.

- 2 **setup__vrealize-automation-appliance-FQDN@5480.exe** 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

- 3 **다음**을 클릭합니다.

- 4 라이선스 계약에 동의하고 **다음**을 클릭합니다.

- 5 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.

- a 사용자 이름(**root**)과 암호를 입력합니다.

암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.

- b **인증서 수락**을 선택합니다.

- c **인증서 보기**를 클릭합니다.

인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.

- 6 **다음**을 클릭합니다.

- 7 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.

- 8 [설치 유형] 페이지의 [구성 요소 선택] 아래에서 **laaS 서버**를 선택합니다.

- 9 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.

분산 배포인 경우에도 동일한 Windows 서버에 laaS 구성 요소를 둘 이상 설치하는 경우가 있습니다.

laaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.

- 10 **다음**을 클릭합니다.

- 11 **IaaS 서버 사용자 지정 설치** 페이지에서 **웹 사이트**를 선택합니다.
- 12 **관리 및 Model Manager 웹 사이트** 탭에서 기본 웹 사이트를 수락하거나, 사용 가능한 웹 사이트 중에서 웹 사이트를 선택합니다.
- 13 사용 가능한 포트 번호를 **포트 번호** 텍스트 상자에 입력하거나, 기본 포트 **443**을 수락합니다.
- 14 **바인딩 테스트**를 클릭하여 해당 포트 번호가 사용 가능한지 확인합니다.
- 15 이 구성 요소의 인증서를 선택합니다.
 - a 설치를 시작한 이후에 인증서를 가져온 경우에는 **새로 고침**을 클릭하여 목록을 업데이트합니다.
 - b **사용 가능한 인증서**에서 사용할 인증서를 선택합니다.
 - c 알기 쉬운 인증서 이름이 아니거나 인증서가 목록에 표시되지 않는 경우, **알기 쉬운 이름을 사용하여 인증서 표시**의 선택을 취소하고 **새로 고침**을 클릭합니다.

로드 밸런서를 사용하지 않는 환경에 설치하는 경우에는 인증서를 선택하는 대신 **자체 서명된 인증서 생성**을 선택할 수 있습니다. 로드 밸런서 뒤에 추가적인 웹 사이트 구성 요소를 설치하는 경우에는 자체 서명된 인증서를 생성하지 마십시오. 이 경우에는 로드 밸런서 뒤에 있는 모든 서버에 동일한 인증서를 사용하도록 기본 IaaS 웹 서버에서 인증서를 가져와야 합니다.
- 16 (선택 사항) **인증서 보기**를 클릭하여 인증서를 본 후 **확인**을 클릭하여 정보 창을 닫습니다.
- 17 (선택 사항) 인증서 오류를 표시하지 않으려면 **인증서 불일치 표시 안 함**을 선택합니다. 이렇게 하면 인증서 이름 불일치 오류뿐 아니라 모든 원격 인증서 해지 목록 일치 오류가 설치 과정 중에 무시됩니다. 이 옵션은 보안 수준이 낮습니다.
- 18 **IaaS 서버** 텍스트 상자에서 첫 번째 IaaS 웹 서버 구성 요소를 식별합니다.

옵션	설명
로드 밸런서를 사용하는 경우	IaaS 웹 서버 구성 요소에 대한 로드 밸런서의 정규화된 도메인 이름 및 포트 번호를 입력합니다(<i>web-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	첫 번째 IaaS 웹 서버 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

- 19 **테스트**를 클릭하여 서버 연결을 확인합니다.
- 20 **다음**을 클릭합니다.

21 사전 요구 사항 확인을 완료합니다.

옵션	설명
오류 없음	다음을 클릭합니다.
심각하지 않은 오류	무시를 클릭합니다.
심각한 오류	심각한 오류를 무시하면 설치가 실패합니다. 경고가 표시되면 왼쪽 창에서 경고를 선택한 다음 오른쪽에 있는 지침을 따릅니다. 심각한 오류를 모두 해결하고 다시 확인 을 클릭하여 확인합니다.

22 [서버 및 계정 설정] 페이지의 **서버 설치 정보** 텍스트 상자에 현재 설치 서버에 대한 관리 권한이 있는 서비스 계정 사용자의 사용자 이름과 암호를 입력합니다.

서비스 계정 사용자는 각 분산 IaaS 서버에 대한 권한이 있는 하나의 도메인 계정이어야 합니다. 로컬 시스템 계정을 사용하지 마십시오.

23 데이터베이스를 보호하는 암호화 키 생성에 사용되는 암호를 제공합니다.

옵션	설명
이 환경에 구성 요소를 이미 설치한 경우	이전에 암호 및 확인 텍스트 상자에서 생성한 암호를 입력합니다.
첫 번째 설치인 경우	암호 및 확인 텍스트 상자에 암호를 입력합니다. 이 암호는 새 구성 요소를 설치할 때마다 사용해야 합니다.

나중에 사용할 수 있도록 이 암호를 안전한 위치에 두어야 합니다.

24 IaaS 데이터베이스 서버, 데이터베이스 이름 및 데이터베이스 서버의 인증 방법을 **Microsoft SQL 데이터베이스 설치 정보** 텍스트 상자에 지정합니다.

이는 앞서 생성한 IaaS 데이터베이스 서버, 이름 및 인증 정보입니다.

25 다음을 클릭합니다.**26** 설치를 클릭합니다.**27** 설치가 완료되면 **초기 구성 과정 안내**의 선택을 취소하고 다음을 클릭합니다.

다음에 수행할 작업

[활성 Manager Service 설치](#) .

활성 Manager Service 설치

활성 Manager Service는 IaaS Distributed Execution Manager, 데이터베이스, 에이전트, 프록시 에이전트와 SMTP 간 통신을 조정하는 Windows 서비스입니다.

자동 Manager Service 페일오버를 사용하도록 설정하지 않는 한 IaaS 배포에서는 한 번에 하나의 Windows 시스템에서만 Manager Service를 실행하고 있어야 합니다. 백업 시스템에서는 서비스가 중지되고 수동으로 시작하도록 구성되어 있어야 합니다.

[자동 Manager Service 페일오버 정보](#) 항목을 참조하십시오.

사전 요구 사항

- 다른 IaaS 구성 요소를 이미 설치했다면 생성한 데이터베이스 암호를 알고 있는지 확인합니다.
- (선택 사항) 기본 웹 사이트 이외의 웹 사이트에 **Manager Service**를 설치하려면 먼저 인터넷 정보 서비스에 웹 사이트를 생성해야 합니다.
- IIS로 가져온 인증 기관의 인증서가 있고, 루트 인증서 또는 인증 기관을 신뢰할 수 있는지 확인합니다. 로드 밸런서 아래에 있는 모든 구성 요소는 동일한 인증서를 사용해야 합니다.
- 웹 사이트 로드 밸런서가 구성되어 있고 로드 밸런서의 시간 초과 값이 180초 이상으로 설정되었는지 확인합니다.
- **IaaS 웹 사이트 구성 요소 및 Model Manager Data 설치.**

절차

- 1 로드 밸런서를 사용하는 경우, 로드 밸런서 아래의 다른 노드를 사용하지 않도록 설정하고 트래픽이 원하는 노드로 전달되는지 확인합니다.

또한, 모든 vRealize Automation 구성 요소가 설치되고 구성될 때까지 로드 밸런서 상태 점검을 사용하지 않도록 설정합니다.
- 2 **setup__vrealize-automation-appliance-FQDN@5480.exe** 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 3 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 4 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.
 - a 사용자 이름(**root**)과 암호를 입력합니다.

암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.
 - b **인증서 수락**을 선택합니다.
 - c **인증서 보기**를 클릭합니다.

인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.
- 5 **다음**을 클릭합니다.
- 6 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.
- 7 [설치 유형] 페이지의 [구성 요소 선택] 아래에서 **IaaS 서버**를 선택합니다.
- 8 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.

분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다. IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.
- 9 **다음**을 클릭합니다.

10 IaaS 서버 사용자 지정 설치 페이지에서 **Manager Service**를 선택합니다.

11 IaaS 서버 텍스트 상자에서 IaaS 웹 서버 구성 요소를 식별합니다.

옵션	설명
로드 밸런서를 사용하는 경우	IaaS 웹 서버 구성 요소에 대한 로드 밸런서의 정규화된 도메인 이름 및 포트 번호를 입력합니다(<code>web-load-balancer.mycompany.com:443</code>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	IaaS 웹 서버 구성 요소를 설치한 시스템의 정규화된 도메인 이름 및 포트 번호를 입력합니다(<code>web.mycompany.com:443</code>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

12 시작 유형이 자동으로 설정된 활성 노드를 선택합니다.

13 관리 및 Model Manager 웹 사이트 탭에서 기본 웹 사이트를 수락하거나, 사용 가능한 웹 사이트 중에서 웹 사이트를 선택합니다.

14 사용 가능한 포트 번호를 **포트 번호** 텍스트 상자에 입력하거나, 기본 포트 **443**을 수락합니다.

15 바인딩 테스트를 클릭하여 해당 포트 번호가 사용 가능한지 확인합니다.

16 이 구성 요소의 인증서를 선택합니다.

- a 설치를 시작한 이후에 인증서를 가져온 경우에는 **새로 고침**을 클릭하여 목록을 업데이트합니다.
- b **사용 가능한 인증서**에서 사용할 인증서를 선택합니다.
- c 알기 쉬운 인증서 이름이 아니거나 인증서가 목록에 표시되지 않는 경우, **알기 쉬운 이름을 사용하는 인증서 표시**의 선택을 취소하고 **새로 고침**을 클릭합니다.

로드 밸런서를 사용하지 않는 환경에 설치하는 경우에는 인증서를 선택하는 대신 **자체 서명된 인증서 생성**을 선택할 수 있습니다. 로드 밸런서 뒤에 추가적인 웹 사이트 구성 요소를 설치하는 경우에는 자체 서명된 인증서를 생성하지 마십시오. 이 경우에는 로드 밸런서 뒤에 있는 모든 서버에 동일한 인증서를 사용하도록 기본 IaaS 웹 서버에서 인증서를 가져와야 합니다.

17 (선택 사항) 인증서 보기를 클릭하여 인증서를 본 후 **확인**을 클릭하여 정보 창을 닫습니다.

18 다음을 클릭합니다.

19 사전 요구 사항을 확인하고 **다음**을 클릭합니다.

20 [서버 및 계정 설정] 페이지의 **서버 설치 정보** 텍스트 상자에 현재 설치 서버에 대한 관리 권한이 있는 서비스 계정 사용자의 사용자 이름과 암호를 입력합니다.

서비스 계정 사용자는 각 분산 IaaS 서버에 대한 권한이 있는 하나의 도메인 계정이어야 합니다. 로컬 시스템 계정을 사용하지 마십시오.

21 데이터베이스를 보호하는 암호화 키 생성에 사용되는 암호를 제공합니다.

옵션	설명
이 환경에 구성 요소를 이미 설치한 경우	이전에 암호 및 확인 텍스트 상자에서 생성한 암호를 입력합니다.
첫 번째 설치인 경우	암호 및 확인 텍스트 상자에 암호를 입력합니다. 이 암호는 새 구성 요소를 설치할 때마다 사용해야 합니다.

나중에 사용할 수 있도록 이 암호를 안전한 위치에 두어야 합니다.

22 IaaS 데이터베이스 서버, 데이터베이스 이름 및 데이터베이스 서버의 인증 방법을 **Microsoft SQL 데이터베이스 설치 정보** 텍스트 상자에 지정합니다.

이는 앞서 생성한 IaaS 데이터베이스 서버, 이름 및 인증 정보입니다.

23 다음을 클릭합니다.**24** 설치를 클릭합니다.**25** 설치가 완료되면 **초기 구성 과정 안내**의 선택을 취소하고 **다음**을 클릭합니다.**26** 완료를 클릭합니다.

다음에 수행할 작업

- 설치한 **Manager Service**가 활성 인스턴스인지 확인하려면 vCloud Automation Center 서비스가 실행 중이고 시작 유형이 "자동"으로 설정되었는지 확인합니다.
- **Manager Service** 구성 요소의 다른 인스턴스를 설치할 수 있습니다. 이 인스턴스는 활성 인스턴스가 실패했을 때 수동으로 시작할 수 있습니다. **백업 Manager Service 구성 요소 설치** 항목을 참조하십시오.
- 시스템 관리자는 실행 시간 동안 **SQL** 데이터베이스에 액세스하는 데 사용되는 인증 방법을 변경할 수 있습니다(설치 완료 후). **IaaS 데이터베이스 액세스를 위한 Windows 서비스 구성** 항목을 참조하십시오.

백업 Manager Service 구성 요소 설치

백업 **Manager Service**는 이중화 및 고가용성을 제공하며 활성 서비스가 중지되는 경우 수동으로 시작할 수 있습니다.

자동 **Manager Service** 페일오버를 사용하도록 설정하지 않는 한 IaaS 배포에서는 한 번에 하나의 **Windows** 시스템에서만 **Manager Service**를 실행하고 있어야 합니다. 백업 시스템에서는 서비스가 중지되고 수동으로 시작하도록 구성되어 있어야 합니다.

자동 **Manager Service 페일오버 정보** 항목을 참조하십시오.

사전 요구 사항

- 다른 IaaS 구성 요소를 이미 설치했다면 생성한 데이터베이스 암호를 알고 있는지 확인합니다.
- (선택 사항) 기본 웹 사이트 이외의 웹 사이트에 **Manager Service**를 설치하려면 먼저 인터넷 정보 서비스에 웹 사이트를 생성해야 합니다.

- vRealize Automation 장치 관리 인터페이스를 사용하여 새 노드의 FQDN을 포함하도록 인증서를 대체합니다. [vRealize Automation 장치의 인증서 교체](#)를 참조하십시오.
- IIS로 가져온 인증 기관의 인증서가 있고, 루트 인증서 또는 인증 기관을 신뢰할 수 있는지 확인합니다. 로드 밸런서 아래에 있는 모든 구성 요소는 동일한 인증서를 사용해야 합니다.
- 웹 사이트 로드 밸런서가 구성되어 있는지 확인합니다.
- [IaaS 웹 사이트 구성 요소 및 Model Manager Data 설치](#).

절차

- 1 로드 밸런서를 사용하는 경우, 로드 밸런서 아래의 다른 노드를 사용하지 않도록 설정하고 트래픽이 원하는 노드로 전달되는지 확인합니다.

또한, 모든 vRealize Automation 구성 요소가 설치되고 구성될 때까지 로드 밸런서 상태 점검을 사용하지 않도록 설정합니다.
- 2 `setup__vrealize-automation-appliance-FQDN@5480.exe` 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 3 **다음**을 클릭합니다.
- 4 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 5 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.
 - a 사용자 이름(**root**)과 암호를 입력합니다.

암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.
 - b **인증서 수락**을 선택합니다.
 - c **인증서 보기**를 클릭합니다.

인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.
- 6 **다음**을 클릭합니다.
- 7 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.
- 8 [설치 유형] 페이지의 [구성 요소 선택] 아래에서 **IaaS 서버**를 선택합니다.
- 9 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.

분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다. IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.
- 10 **다음**을 클릭합니다.
- 11 **IaaS 서버 사용자 지정 설치** 페이지에서 **Manager Service**를 선택합니다.

12 IaaS 서버 텍스트 상자에서 IaaS 웹 서버 구성 요소를 식별합니다.

옵션	설명
로드 밸런서를 사용하는 경우	IaaS 웹 서버 구성 요소에 대한 로드 밸런서의 정규화된 도메인 이름 및 포트 번호를 입력합니다(<i>web-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	IaaS 웹 서버 구성 요소를 설치한 시스템의 정규화된 도메인 이름 및 포트 번호를 입력합니다(<i>web.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

13 재해 복구 콜드 대기 노드를 선택합니다.

14 관리 및 Model Manager 웹 사이트 탭에서 기본 웹 사이트를 수락하거나, 사용 가능한 웹 사이트 중에서 웹 사이트를 선택합니다.

15 사용 가능한 포트 번호를 **포트 번호** 텍스트 상자에 입력하거나, 기본 포트 443을 수락합니다.

16 바인딩 테스트를 클릭하여 해당 포트 번호가 사용 가능한지 확인합니다.

17 이 구성 요소의 인증서를 선택합니다.

- a 설치를 시작한 이후에 인증서를 가져온 경우에는 **새로 고침**을 클릭하여 목록을 업데이트합니다.
- b **사용 가능한 인증서**에서 사용할 인증서를 선택합니다.
- c 알기 쉬운 인증서 이름이 아니거나 인증서가 목록에 표시되지 않는 경우, **알기 쉬운 이름을 사용하는 인증서 표시**의 선택을 취소하고 **새로 고침**을 클릭합니다.

로드 밸런서를 사용하지 않는 환경에 설치하는 경우에는 인증서를 선택하는 대신 **자체 서명된 인증서 생성**을 선택할 수 있습니다. 로드 밸런서 뒤에 추가적인 웹 사이트 구성 요소를 설치하는 경우에는 자체 서명된 인증서를 생성하지 마십시오. 이 경우에는 로드 밸런서 뒤에 있는 모든 서버에 동일한 인증서를 사용하도록 기본 IaaS 웹 서버에서 인증서를 가져와야 합니다.

18 (선택 사항) **인증서 보기**를 클릭하여 인증서를 본 후 **확인**을 클릭하여 정보 창을 닫습니다.

19 **다음**을 클릭합니다.

20 사전 요구 사항을 확인하고 **다음**을 클릭합니다.

21 [서버 및 계정 설정] 페이지의 **서버 설치 정보** 텍스트 상자에 현재 설치 서버에 대한 관리 권한이 있는 서비스 계정 사용자의 사용자 이름과 암호를 입력합니다.

서비스 계정 사용자는 각 분산 IaaS 서버에 대한 권한이 있는 하나의 도메인 계정이어야 합니다. 로컬 시스템 계정을 사용하지 마십시오.

22 데이터베이스를 보호하는 암호화 키 생성에 사용되는 암호를 제공합니다.

옵션	설명
이 환경에 구성 요소를 이미 설치한 경우	이전에 암호 및 확인 텍스트 상자에서 생성한 암호를 입력합니다.
첫 번째 설치인 경우	암호 및 확인 텍스트 상자에 암호를 입력합니다. 이 암호는 새 구성 요소를 설치할 때마다 사용해야 합니다.

나중에 사용할 수 있도록 이 암호를 안전한 위치에 두어야 합니다.

23 IaaS 데이터베이스 서버, 데이터베이스 이름 및 데이터베이스 서버의 인증 방법을 **Microsoft SQL 데이터베이스 설치 정보** 텍스트 상자에 지정합니다.

이는 앞서 생성한 IaaS 데이터베이스 서버, 이름 및 인증 정보입니다.

24 다음을 클릭합니다.**25** 설치를 클릭합니다.**26** 설치가 완료되면 **초기 구성 과정 안내**의 선택을 취소하고 다음을 클릭합니다.**27** 완료를 클릭합니다.

다음에 수행할 작업

- 설치한 **Manager Service**가 수동 백업 인스턴스인지 확인하려면 vRealize Automation 서비스가 실행 중이 아니고 시작 유형이 "수동"으로 설정되었는지 확인합니다.
- 시스템 관리자는 실행 시간 동안 **SQL 데이터베이스**에 액세스하는 데 사용되는 인증 방법을 변경할 수 있습니다(설치 완료 후). **IaaS 데이터베이스 액세스를 위한 Windows 서비스 구성** 항목을 참조하십시오.

Distributed Execution Manager 설치

Distributed Execution Manager는 두 가지 역할인 **DEM 조정자** 또는 **DEM 작업자** 중 하나로 설치합니다. 각 역할에는 **DEM 인스턴스**를 하나 이상 설치해야 하며, 페일오버 및 고가용성을 지원하기 위해 **DEM 인스턴스**를 추가적으로 설치할 수 있습니다.

시스템 관리자는 미리 정의된 시스템 요구 사항을 충족하는 설치 시스템을 선택해야 합니다. **DEM 조정자**와 **작업자**는 같은 시스템에 상주할 수 있습니다.

Distributed Execution Manager의 설치를 계획할 때는 다음과 같은 사항을 염두에 두는 것이 좋습니다.

- **DEM 조정자**는 활성-활성 고가용성을 지원합니다. 일반적으로 **DEM 조정자**는 각 **Manager Service** 시스템에 하나씩 설치합니다.
- 조정자는 **Model Manager** 호스트와의 네트워크 연결이 강력한 시스템에 설치합니다.
- 페일오버를 구현하려면 다른 시스템에 보조 **DEM 조정자**를 설치합니다.
- 일반적으로 **DEM 작업자**는 **IaaS Manager Service** 서버 또는 별도의 서버에 설치합니다. 서버는 **Model Manager** 호스트에 네트워크로 연결되어 있어야 합니다.
- 이중화 및 확장성을 위해 추가적인 **DEM 인스턴스**를 설치할 수 있으며, 같은 시스템에 인스턴스를 여러 개 포함할 수 있습니다.

사용하는 끝점에 따라 DEM 설치에 특정 요구 사항이 적용됩니다. [IaaS Distributed Execution Manager 호스트](#) 항목을 참조하십시오.

Distributed Execution Manager 설치

DEM 작업자와 DEM 조정자를 각각 하나 이상 설치해야 합니다. 설치 절차는 두 역할 모두에 대해 동일합니다.

DEM 조정자는 활성-활성 고가용성을 지원합니다. 일반적으로 DEM 조정자는 각 Manager Service 시스템에 하나씩 설치합니다. DEM 조정자와 DEM 작업자를 같은 시스템에 설치할 수 있습니다.

사전 요구 사항

[vRealize Automation IaaS 설치 관리자 다운로드](#).

절차

- 1 `setup__vrealize-automation-appliance-FQDN@5480.exe` 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 2 **다음**을 클릭합니다.
- 3 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 4 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.
 - a 사용자 이름(**root**)과 암호를 입력합니다.
암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.
 - b **인증서 수락**을 선택합니다.
 - c **인증서 보기**를 클릭합니다.
인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.
- 5 **다음**을 클릭합니다.
- 6 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.
- 7 [설치 유형] 페이지의 [구성 요소 선택] 아래에서 **Distributed Execution Manager**를 선택합니다.
- 8 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.
분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다.
IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.
- 9 **다음**을 클릭합니다.
- 10 사전 요구 사항을 확인하고 **다음**을 클릭합니다.

- 11 서비스를 실행하는 데 사용할 로그인 자격 증명을 입력합니다.

서비스 계정이 로컬 관리자 권한을 갖고 있어야 하며 IaaS 설치 전체에서 사용자가 사용해 온 도메인 계정이어야 합니다. 서비스 계정은 각 분산 IaaS 서버에 대한 권한을 가지며 로컬 시스템 계정이 아니어야 합니다.

- 12 다음을 클릭합니다.

- 13 **DEM 역할** 드롭다운 메뉴에서 설치 유형을 선택합니다.

옵션	설명
작업자	작업자는 워크플로를 실행합니다.
Orchestrator	Orchestrator는 워크플로 스케줄링 및 사전 처리를 포함한 DEM 작업자의 작업을 감독하고 DEM 작업자의 온라인 상태를 모니터링합니다.

- 14 DEM을 식별하는 고유한 이름을 **DEM 이름** 텍스트 상자에 입력합니다.

이름은 공백을 포함할 수 없으며 128자보다 길 수 없습니다. 이전에 사용된 이름을 입력하면 "DEM 이름이 이미 있습니다. 이 DEM에 대해 다른 이름을 입력하려면 [예]를 클릭하십시오. 같은 이름으로 DEM을 복원하거나 DEM을 다시 설치하는 경우에는 [아니요]를 클릭하십시오."

- 15 (선택 사항) 이 인스턴스에 대한 설명을 **DEM 설명**에 입력합니다.

- 16 **Manager Service 호스트 이름** 및 **Model Manager Web Service 호스트 이름** 텍스트 상자에 호스트 이름과 포트를 입력합니다.

옵션	설명
로드 밸런서를 사용하는 경우	Manager Service 구성 요소 및 Model Manager를 호스팅하는 웹 서버에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc-load-balancer.mycompany.com:443</i> 및 <i>web-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	Manager Service 구성 요소 및 Model Manager를 호스팅하는 웹 서버가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc.mycompany.com:443</i> 및 <i>web.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

- 17 (선택 사항) **테스트**를 클릭하여 Manager Service 및 Model Manager Web Service에 대한 연결을 테스트합니다.

- 18 **추가**를 클릭합니다.

- 19 **다음**을 클릭합니다.

- 20 **설치**를 클릭합니다.

- 21 설치가 완료되면 **초기 구성 과정 안내**의 선택을 취소하고 **다음**을 클릭합니다.

- 22 **완료**를 클릭합니다.

다음에 수행할 작업

- 서비스가 실행 중이고 로그에 오류가 표시되지 않는지 확인합니다. 서비스 이름은 VMware DEM Role - Name이며, 여기서 role은 Orchestrator 또는 작업자입니다. 로그 위치는 *Install Location* \Distributed Execution Manager\Name\Logs입니다.
- 이 절차를 반복하여 추가적인 DEM 인스턴스를 설치합니다.

다른 설치 경로에서 SCVMM에 연결하도록 DEM 구성

기본적으로 DEM 작업자 구성 파일은 Microsoft SCVMM(System Center Virtual Machine Manager) 콘솔의 기본 설치 경로를 사용합니다. SCVMM 콘솔을 기본값이 아닌 위치에 설치할 경우 파일을 업데이트해야 합니다.

SCVMM 끝점 및 에이전트가 있는 경우에만 이 절차가 필요합니다.

사전 요구 사항

- SCVMM 콘솔을 설치한 기본값이 아닌 경로를 알고 있어야 합니다.

다음은 구성 파일에서 바뀌어야 하는 기본 경로입니다.

```
path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"
```

절차

- 1 DEM 작업자 서비스를 중지합니다.
- 2 텍스트 편집기에서 다음 파일을 엽니다.

```
Program Files (x86)\VMware\VCAC\Distributed Execution Manager\instance-name
\DynamicOps.DEM.exe.config
```

- 3 <assemblyLoadConfiguration> 섹션을 찾습니다.
- 4 다음 예를 지침으로 사용하여 각 path를 업데이트합니다.

```
<assemblyLoadConfiguration>
  <assemblies>
    <!-- List of required assemblies for Scvmm -->
    <add name="Errors" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Microsoft.SystemCenter.VirtualMachineManager" path="D:\Microsoft System Center 2012
R2\Virtual Machine Manager\bin"/>
    <add name="Remoting" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="TraceWrapper" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager
\bin"/>
    <add name="Utils" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
  </assemblies>
</assemblyLoadConfiguration>
```

- 5 DynamicOps.DEM.exe.config를 저장한 후 닫습니다.
- 6 DEM 작업자 서비스를 다시 시작합니다.

결과

자세한 내용은 [DEM 작업자와 SCVMM](#) 항목을 참조하십시오.

SCVMM 환경 준비 및 SCVMM 끝점 생성에 대한 추가 정보는 [SCVMM 환경 준비](#) 및 [Hyper-V\(SCVMM\) 끝점 생성](#)에서 볼 수 있습니다.

IaaS 데이터베이스 액세스를 위한 Windows 서비스 구성

시스템 관리자는 실행 시간 동안 SQL 데이터베이스에 액세스하는 데 사용되는 인증 방법을 변경할 수 있습니다(설치 완료 후). 기본적으로, 현재 로그인한 계정의 Windows ID가 설치 후 데이터베이스 연결에 사용됩니다.

서비스 사용자의 IaaS 데이터베이스에 액세스 설정

SQL 데이터베이스가 Manager Service와는 다른 호스트에 설치되어 있는 경우에는 Manager Service에서 데이터베이스에 액세스할 수 있도록 설정해야 합니다. Manager Service를 실행할 사용자 이름이 데이터베이스의 소유자인 경우에는 별도의 작업이 필요하지 않습니다. 사용자가 데이터베이스 소유자가 아닌 경우에는 시스템 관리자가 액세스 권한을 부여해야 합니다.

사전 요구 사항

- [IaaS 데이터베이스 선택 시나리오](#).
- Manager Service를 실행할 사용자 이름이 데이터베이스의 소유자가 아닌지 확인합니다.

절차

- 1 설치 zip 아카이브를 추출한 디렉토리 내의 **Database** 하위 디렉토리로 이동합니다.
- 2 DBInstall.zip 아카이브를 로컬 디렉토리에 추출합니다.
- 3 SQL Server 인스턴스에서 **sysadmin** 역할을 가진 사용자로 데이터베이스 호스트에 로그인합니다.
- 4 VMPS0psUser.sql을 편집하여 \$(Service User)의 모든 인스턴스를 Manager Service를 실행할 사용자(3단계)로 바꿉니다.

WHERE name = N'ServiceUser')로 끝나는 줄에서는 ServiceUser를 바꾸지 마십시오.

- 5 SQL Server Management Studio를 엽니다.
- 6 왼쪽 창의 **데이터베이스**에서 데이터베이스(기본값: vCAC)를 선택합니다.
- 7 **새 쿼리**를 클릭합니다.

오른쪽 창에 [SQL 쿼리] 창이 열립니다.

- 8 VMPS0psUser.sql의 수정된 콘텐츠를 쿼리 창에 붙여 넣습니다.
- 9 **실행**을 클릭합니다.

결과

Manager Service에서 데이터베이스에 액세스할 수 있도록 설정되었습니다.

SQL 인증을 사용하도록 Windows 서비스 계정 구성

데이터베이스에 SQL 인증을 구성한 경우에도 기본적으로 Windows 서비스 계정은 런타임 동안 해당 데이터베이스에 액세스합니다. 런타임 인증을 Windows에서 SQL로 변경할 수 있습니다.

예를 들어 데이터베이스가 신뢰할 수 없는 도메인에 있는 경우 런타임 인증을 변경할 수 있습니다.

사전 요구 사항

vRealize Automation SQL Server 데이터베이스가 있는지 확인합니다. [IaaS 데이터베이스 선택 시나리오](#)로 시작하십시오.

절차

- 1 관리자 권한이 있는 계정을 사용하여 Manager Service를 호스팅하는 IaaS Windows Server에 로그인합니다.
- 2 **관리 도구 > 서비스**에서 **VMware vCloud Automation Center** 서비스를 중지합니다.
- 3 텍스트 편집기에서 다음 파일을 엽니다.

```
C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
```

- 4 각 파일에서 <connectionStrings> 섹션을 찾습니다.

- 5 다음 항목을

```
Integrated Security=True;
```

다음과 같이 바꿉니다.

```
User Id=database-username;Password=database-password;
```

- 6 파일을 저장한 후 닫습니다.

```
ManagerService.exe.config
Web.config
```

- 7 **VMware vCloud Automation Center** 서비스를 시작합니다.

- 8 `iisreset` 명령을 사용하여 IIS를 다시 시작합니다.

IaaS 서비스 확인

설치 후 시스템 관리자는 IaaS 서비스가 실행 중인지 확인합니다. 서비스가 실행 중이면 설치가 성공한 것입니다.

절차

- 1 IaaS 시스템의 Windows 데스크톱에서 **관리 도구 > 서비스**를 선택합니다.
- 2 다음 서비스를 찾아서 상태가 '시작됨'이고 시작 유형이 '자동'으로 설정되어 있는지 확인합니다.
 - VMware DEM - Orchestrator - 이름(여기서 이름은 설치 도중 **DEM 이름** 상자에 제공한 문자열입니다.
 - VMware DEM - 작업자 - 이름(여기서 이름은 설치 도중 **DEM 이름** 상자에 제공한 문자열입니다.
 - VMware vCloud Automation Center Agent 에이전트 이름

■ VMware vCloud Automation Center Service

3 서비스 창을 닫습니다.

vRealize Automation 에이전트 설치

vRealize Automation는 에이전트를 사용하여 외부 시스템과 통합합니다. 시스템 관리자는 다른 가상화 플랫폼과의 통신을 위해 설치할 에이전트를 선택할 수 있습니다.

vRealize Automation은 다음과 같은 유형의 에이전트를 사용하여 외부 시스템을 관리합니다.

- 하이퍼바이저 프록시 에이전트(vSphere, Citrix Xen Server 및 Microsoft Hyper-V Server)
- EPI(외부 프로비저닝 인프라) 통합 에이전트
- VDI(Virtual Desktop Infrastructure) 에이전트
- WMI(Windows Management Instrumentation) 에이전트

고가용성을 구현하려면 단일 끝점에 대해 여러 개의 에이전트를 설치할 수 있습니다. 중복 에이전트 각각을 별도의 서버에 설치하되 에이전트를 동일한 이름으로 지정하고 구성합니다. 중복 에이전트는 어느 정도의 Fault Tolerance를 제공하지만 페일오버는 제공하지 않습니다. 예를 들어 vSphere 에이전트 두 개를 서버 A와 서버 B에 하나씩 설치한 경우, 서버 A를 사용할 수 없게 되면 서버 B에 설치된 에이전트가 작업 항목을 계속해서 처리합니다. 그러나 서버 A 에이전트가 이미 시작한 작업 항목에 대한 처리는 서버 B 에이전트가 완료할 수 없습니다.

vSphere 에이전트를 최소 설치의 일부로 설치하도록 선택할 수도 있지만, 설치를 완료한 이후에도 추가적인 vSphere 에이전트를 비롯하여 다른 에이전트를 추가할 수도 있습니다. 분산 배포의 경우에는 기본 분산 설치를 완료한 이후에 에이전트를 설치합니다. 설치하는 에이전트는 인프라의 리소스에 따라 달라집니다.

vSphere 에이전트 사용에 대한 자세한 내용은 [vSphere 에이전트 요구 사항](#)을 참조하십시오.

PowerShell 실행 정책을 RemoteSigned로 설정

로컬 PowerShell 스크립트를 실행할 수 있게 허용하려면 PowerShell 실행 정책을 Restricted에서 RemoteSigned 또는 Unrestricted로 설정해야 합니다.

PowerShell 실행 정책에 대한 자세한 내용은 [실행 정책에 대한 Microsoft PowerShell 문서](#) 항목을 참조하십시오. PowerShell 실행 정책이 그룹 정책 수준에서 관리되는 경우 정책 변경 제한 사항에 대해서는 해당 IT 지원에 문의하고 [그룹 정책 설정에 대한 Microsoft PowerShell 문서](#) 항목을 참조하십시오.

사전 요구 사항

- 에이전트 설치를 수행하기 이전에 Microsoft PowerShell이 설치 호스트에 설치되어 있는지 확인합니다. 필요한 버전은 설치 호스트의 운영 체제에 따라 다릅니다. Microsoft 도움말 및 지원 센터를 참조하십시오.
- PowerShell 실행 정책에 대한 자세한 내용을 보려면 PowerShell 명령 프롬프트에서 `help about_signing` 또는 `help Set-ExecutionPolicy`를 실행하십시오.

절차

- 1 관리자 계정을 사용하여 에이전트가 설치되어 있는 IaaS 호스트 시스템에 로그인합니다.
- 2 **시작 > 모든 프로그램 > Windows PowerShell 버전 > Windows PowerShell**을 선택합니다.
- 3 RemoteSigned로 설정하려면 **Set-ExecutionPolicy RemoteSigned**를 실행합니다.
- 4 Unrestricted로 설정하려면 **Set-ExecutionPolicy Unrestricted**를 실행합니다.
- 5 명령으로 인해 오류가 생성되지 않았는지 확인합니다.
- 6 PowerShell 명령 프롬프트에서 **Exit**를 입력합니다.

에이전트 설치 선택 시나리오

설치해야 하는 에이전트는 통합하려는 외부 시스템에 따라 다릅니다.

표 1-35. 에이전트 선택 시나리오

통합 시나리오	에이전트 요구 사항 및 절차
Amazon Web Services 또는 Red Hat Enterprise Linux OpenStack Platform 등 클라우드 환경과 통합하여 클라우드 시스템을 프로비저닝합니다.	에이전트를 설치할 필요가 없습니다.
vSphere 환경과 통합하여 가상 시스템을 프로비저닝합니다.	vSphere용 프록시 에이전트 설치 및 구성
Microsoft Hyper-V Server 환경과 통합하여 가상 시스템을 프로비저닝합니다.	Hyper-V 또는 XenServer용 프록시 에이전트 설치
XenServer 환경과 통합하여 가상 시스템을 프로비저닝합니다.	<ul style="list-style-type: none"> ■ Hyper-V 또는 XenServer용 프록시 에이전트 설치 ■ Citrix용 EPI 에이전트 설치
XenDesktop 환경과 통합하여 가상 시스템을 프로비저닝합니다.	<ul style="list-style-type: none"> ■ XenDesktop의 VDI 에이전트 설치 ■ Citrix용 EPI 에이전트 설치
시스템을 프로비저닝하기 전이나 후에 또는 프로비저닝 해제할 때 프로비저닝 프로세스의 추가 단계로 Visual Basic 스크립트를 실행합니다.	Visual Basic 스크립팅용 EPI 에이전트 설치
프로비저닝된 Windows 시스템에서 데이터를 수집합니다(예: 시스템 소유자의 Active Directory 상태).	원격 WMI 요청용 WMI 에이전트 설치
지원되는 다른 가상 플랫폼과 통합하여 가상 시스템을 프로비저닝합니다.	에이전트를 설치할 필요가 없습니다.

에이전트 설치 위치 및 요구 사항

일반적으로 시스템 관리자는 활성 Manager Service 구성 요소를 호스팅하는 vRealize Automation 서버에 에이전트를 설치합니다.

에이전트가 다른 호스트에 설치된 경우 네트워크 구성에서 에이전트와 Manager Service 설치 시스템 간 통신을 허용해야 합니다.

각 에이전트는 vRealize Automation 설치 디렉토리(일반적으로 Program Files(x86)\VMware\VCAC) 아래의 고유한 디렉토리 Agents\agentname에서 고유한 이름 아래에 설치됩니다. 해당 구성은 이 디렉토리에서 VRMAgent.exe.config 파일에 저장됩니다.

vSphere용 프록시 에이전트 설치 및 구성

시스템 관리자는 vSphere 서버 인스턴스와 통신하기 위해 프록시 에이전트를 설치합니다. 에이전트는 사용 가능한 작업을 검색하고 호스트 정보를 검색하며, 완료된 작업 항목과 기타 호스트 상태 변경 내용을 보고합니다.

vSphere 에이전트 요구 사항

vSphere 끝점 자격 증명 또는 에이전트 서비스 실행에 사용되는 자격 증명에는 설치 호스트에 액세스할 수 있는 관리 액세스 권한이 있어야 합니다. 여러 vSphere 에이전트가 vRealize Automation 구성 요구 사항을 충족해야 합니다.

자격 증명

vSphere 에이전트로 관리될 vCenter Server 인스턴스를 나타내는 끝점을 생성할 때 에이전트는 서비스 실행에 사용되는 자격 증명을 사용하여 vCenter Server와 상호 작용하거나 별도의 끝점 자격 증명을 지정해야 합니다.

VApp.Import 권한은 OVF에서 가져온 설정을 사용하여 vSphere 시스템을 배포할 수 있도록 합니다. 이 vSphere 권한에 대한 자세한 내용은 [vSphere SDK 설명서](#)에서 확인할 수 있습니다. vSphere 끝점을 사용하여 OVF 템플릿에서 VM을 배포하려는 경우 자격 증명에 해당 끝점과 연결된 vCenter Server의 vSphere 권한 VApp.Import가 포함되어 있는지 확인합니다.

다음 표에는 vCenter Server 인스턴스를 관리하기 위해 vSphere 끝점 자격 증명에서 갖추어야 하는 사용 권한이 나와 있습니다. 끝점을 호스팅하는 클러스터만이 아닌 vCenter Server의 모든 클러스터에 해당 사용 권한이 설정되어야 합니다.

표 1-36. vSphere 에이전트가 vCenter Server 인스턴스를 관리하기 위해 필요한 사용 권한

특성 값	사용 권한
데이터스토어	공간 할당
	데이터스토어 찾아보기
데이터스토어 클러스터	데이터스토어 클러스터 구성
폴더	폴더 생성
	폴더 삭제
글로벌	사용자 지정 특성 관리
	사용자 지정 특성 설정
네트워크	네트워크 할당
사용 권한	수정 권한
vApp	가져오기
	vApp 애플리케이션 구성

표 1-36. vSphere 에이전트가 vCenter Server 인스턴스를 관리하기 위해 필요한 사용 권한 (계속)

특성 값		사용 권한
리소스		VM을 리소스 풀에 할당
		전원이 꺼진 가상 시스템 마이그레이션
		전원이 켜진 가상 시스템 마이그레이션
가상 시스템	인벤토리	기존 항목에서 생성
		새로 생성
		이동
		제거
	상호 작용	CD 미디어 구성
		콘솔 상호 작용
		디바이스 연결
		전원 끄기
		전원 켜기
		재설정
		일시 중단
		도구 설치
	구성	기존 디스크 추가
		새 디스크 추가
		디바이스 추가 또는 제거
		디스크 제거
		고급
		CPU 수 변경
		리소스 변경
		가상 디스크 확장
		디스크 변경 내용 추적
		메모리
		디바이스 설정 수정
		이름 변경
		주석 설정(버전 5.0 이상)

표 1-36. vSphere 에이전트가 vCenter Server 인스턴스를 관리하기 위해 필요한 사용 권한 (계속)

특성 값	사용 권한
프로비저닝	설정
	스왑 파일 배치
	사용자 지정
	템플릿 복제
	가상 시스템 복제
	템플릿 배포
	사용자 지정 사양 읽기
상태	스냅샷 생성
	스냅샷 제거
	스냅샷으로 되돌리기

vRealize Automation 외부에서 가상 시스템의 전원 상태를 변경할 수 있는 모든 타사 소프트웨어를 사용하지 않도록 설정하거나 재구성합니다. 이러한 변경은 vRealize Automation의 시스템 수명 주기 관리에 방해될 수 있습니다.

vSphere 에이전트 설치

vSphere 에이전트는 vCenter Server 인스턴스를 관리하기 위해 설치합니다. 고가용성을 구현하려면 동일한 vCenter Server 인스턴스에 대해 두 번째의 중복 vSphere 에이전트를 설치할 수 있습니다. 이 경우 두 vSphere 에이전트를 동일한 이름으로 지정하고 구성해야 하며 서로 다른 시스템에 설치해야 합니다.

사전 요구 사항

- 웹 서버 및 Manager Service 호스트를 포함하여 IaaS를 설치합니다.
- 에이전트를 설치한 시스템이 IaaS 구성 요소가 설치된 도메인에서 신뢰하는 도메인에 있는지 확인합니다.
- [vSphere 에이전트 요구 사항](#)의 요구 사항이 충족되었는지 확인합니다.
- 이 에이전트에서 사용할 vSphere 끝점을 이미 생성한 경우에는 해당 끝점 이름을 기록해 둡니다.
- [vRealize Automation IaaS 설치 관리자 다운로드](#).

절차

- 1 `setup__vrealize-automation-appliance-FQDN@5480.exe` 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 2 **다음**을 클릭합니다.
- 3 라이선스 계약에 동의하고 **다음**을 클릭합니다.

- 4 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.

a 사용자 이름(**root**)과 암호를 입력합니다.

암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.

b **인증서 수락**을 선택합니다.

c **인증서 보기**를 클릭합니다.

인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.

- 5 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.

- 6 [구성 요소 선택] 영역에서 **프록시 에이전트**를 선택합니다.

- 7 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.

분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다.

IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.

- 8 **다음**을 클릭합니다.

- 9 설치 시스템의 Windows 서비스에 대한 관리자 권한을 사용하여 로그인합니다.

서비스는 동일한 설치 시스템에서 실행되어야 합니다.

- 10 **다음**을 클릭합니다.

- 11 **에이전트 유형** 목록에서 vSphere를 선택합니다.

- 12 이 에이전트의 ID를 **에이전트 이름** 텍스트 상자에 입력합니다.

각 에이전트에 대해 에이전트 이름, 자격 증명, 끝점 이름 및 플랫폼 인스턴스의 기록을 유지해야 합니다. 이 정보는 나중에 끝점을 구성하고 호스트를 추가하는 데 필요합니다.

중요 고가용성을 위해 중복 에이전트를 추가하고 이를 동일하게 구성할 수 있습니다. 그렇지 않은 경우 에이전트를 고유하게 유지하십시오.

옵션	설명
중복 에이전트	서로 다른 서버에 중복 에이전트를 설치합니다. 중복 에이전트를 동일하게 이름 지정하고 구성합니다.
독립형 에이전트	에이전트에 고유한 이름을 할당합니다.

13 IaaS Manager Service 호스트에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	Manager Service 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	Manager Service 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

14 IaaS 웹 서버에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	웹 서버 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	웹 서버 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

15 테스트를 클릭하여 각 호스트에 대한 연결을 확인합니다.**16** 끝점 이름을 입력합니다.

vRealize Automation에서 구성하는 끝점 이름은 설치 중 vSphere 프록시 에이전트에 제공된 끝점 이름과 반드시 일치해야 하며 그렇지 않으면 끝점이 작동할 수 없습니다.

17 추가를 클릭합니다.**18** 다음을 클릭합니다.**19** 설치를 클릭하여 설치를 시작합니다.

몇 분 정도 후에 성공 메시지가 표시됩니다.

20 다음을 클릭합니다.**21** 완료를 클릭합니다.**22** 설치가 완료되었는지 확인합니다.**23** (선택 사항) 서로 다른 구성 및 동일한 끝점을 가진 여러 에이전트를 같은 시스템에 추가합니다.

다음에 수행할 작업

[vSphere 에이전트 구성](#).

vSphere 에이전트 구성

vRealize Automation Blueprint에서 vSphere 끝점을 생성 및 사용할 수 있도록 vSphere 에이전트를 구성합니다.

에이전트 구성 파일의 암호화된 부분을 수정하거나 가상화 플랫폼에 대한 시스템 삭제 정책을 변경하려는 경우 프록시 에이전트 유틸리티를 사용합니다. **VRMAgent.exe.config** 에이전트 구성 파일의 일부만 암호화됩니다. 예를 들어 **serviceConfiguration** 섹션은 암호화되지 않습니다.

사전 요구 사항

관리자 권한이 있는 계정을 사용하여 vSphere 에이전트를 설치한 IaaS Windows Server에 로그인합니다.

절차

- 1 관리자 권한으로 Windows 명령 프롬프트를 엽니다.
- 2 에이전트 설치 폴더로 변경합니다. 여기서 *agent-name*은 vSphere 에이전트를 포함하는 폴더입니다.

```
cd %SystemDrive%\Program Files (x86)\VMware\VCAC\Agents\agent-name
```

- 3 (선택 사항) 현재 구성 설정을 보려면 다음 명령을 입력합니다.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

다음은 명령 출력 예제입니다.

```
managementEndpointName: VCendpoint
doDeletes: True
```

- 4 (선택 사항) 설치 시 구성한 끝점의 이름을 변경하려면 다음 명령을 사용합니다.

```
set managementEndpointName
```

예: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName my-endpoint`

이 방법을 사용하면 끝점을 변경하는 대신 vRealize Automation 내에서 끝점 이름을 바꿀 수 있습니다.

- 5 (선택 사항) 가상 시스템 삭제 정책을 구성하려면 다음 명령을 사용합니다.

```
set doDeletes
```

예: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes false`

옵션	설명
true	(기본값) vRealize Automation에서 제거된 가상 시스템을 vCenter Server에서 삭제합니다.
false	vRealize Automation에서 제거된 가상 시스템을 vCenter Server의 VRMDeleted 디렉토리로 이동합니다.

- 6 **관리 도구 > 서비스**를 열고 vRealize Automation Agent - *agent-name* 서비스를 다시 시작합니다.

다음에 수행할 작업

고가용성을 위해 끝점에 대해 중복 에이전트를 설치하고 구성할 수 있습니다. 중복 에이전트 각각을 별도의 서버에 설치하지만 에이전트를 동일한 이름으로 지정하고 구성합니다.

Hyper-V 또는 XenServer용 프록시 에이전트 설치

시스템 관리자는 Hyper-V 및 XenServer 서버 인스턴스와 통신하기 위해 프록시 에이전트를 설치합니다. 에이전트는 사용 가능한 작업을 검색하고 호스트 정보를 검색하며, 완료된 작업 항목과 기타 호스트 상태 변경 내용을 보고합니다.

Hyper-V 및 XenServer 요구 사항

Hyper-V Hypervisor 프록시 에이전트는 설치를 위한 시스템 관리자 자격 증명을 필요로 합니다.

에이전트 서비스를 실행하는 자격 증명에는 설치 호스트에 대한 관리자 액세스 권한이 있어야 합니다.

관리자 수준 자격 증명이 에이전트에서 관리될 호스트의 모든 XenServer 또는 Hyper-V 인스턴스에 필요 합니다.

Xen 풀을 사용하는 경우 Xen 풀 내의 모든 노드가 정규화된 도메인 이름에 의해 식별되어야 합니다.

참고 기본적으로 Hyper-V는 원격 관리를 위해 구성되지 않습니다. vRealize Automation Hyper-V 프록시 에이전트는 원격 관리가 사용되지 않으면 Hyper-V 서버와 통신할 수 없습니다.

원격 관리를 위한 Hyper-V를 구성하는 방법에 대한 자세한 내용은 **Microsoft Windows Server** 설명서를 참조하십시오.

Hyper-V 또는 XenServer 에이전트 설치

Hyper-V 에이전트는 Hyper-V 서버 인스턴스를 관리합니다. XenServer 에이전트는 XenServer 서버 인스턴스를 관리합니다.

사전 요구 사항

- 웹 서버 및 Manager Service 호스트를 포함하여 IaaS를 설치합니다.
- [vRealize Automation IaaS 설치 관리자 다운로드](#).
- Hyper-V 하이퍼바이저 프록시 에이전트가 시스템 관리자 자격 증명을 가지고 있는지 확인합니다.
- 에이전트 서비스를 실행할 자격 증명을 사용하여 설치 호스트에 관리자 권한으로 액세스할 수 있는지 확인합니다.
- 에이전트가 관리하는 호스트의 모든 XenServer 또는 Hyper-V 인스턴스에 관리자 수준 자격 증명이 있는지 확인합니다.
- Xen 풀을 사용하는 경우에는 Xen 풀 내의 모든 노드를 해당하는 정규화된 도메인 이름으로 식별해야 합니다.

Xen 풀 내에서 정규화된 도메인 이름으로 식별되지 않는 모든 노드는 vRealize Automation이 통신하거나 관리할 수 없습니다.

- Hyper-V 서버가 vRealize Automation Hyper-V 프록시 에이전트와 통신할 수 있도록 Hyper-V에 대해 원격 관리 기능을 구성합니다.

원격 관리를 위한 Hyper-V를 구성하는 방법에 대한 자세한 내용은 Microsoft Windows Server 설명서를 참조하십시오.

절차

- 1 `setup__vrealize-automation-appliance-FQDN@5480.exe` 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 2 **다음**을 클릭합니다.
- 3 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 4 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.
 - a 사용자 이름(**root**)과 암호를 입력합니다.
 암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.
 - b **인증서 수락**을 선택합니다.
 - c **인증서 보기**를 클릭합니다.
 인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.
- 5 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.
- 6 [설치 유형] 페이지에서 **구성 요소 선택**을 선택합니다.
- 7 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.
 분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다.
 IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.
- 8 **다음**을 클릭합니다.
- 9 설치 시스템의 Windows 서비스에 대한 관리자 권한을 사용하여 로그인합니다.
 서비스는 동일한 설치 시스템에서 실행되어야 합니다.
- 10 **다음**을 클릭합니다.
- 11 **에이전트 유형** 목록에서 에이전트를 선택합니다.
 - Xen
 - Hyper-V

12 이 에이전트의 ID를 **에이전트 이름** 텍스트 상자에 입력합니다.

각 에이전트에 대해 에이전트 이름, 자격 증명, 끝점 이름 및 플랫폼 인스턴스의 기록을 유지해야 합니다. 이 정보는 나중에 끝점을 구성하고 호스트를 추가하는 데 필요합니다.

중요 고가용성을 위해 중복 에이전트를 추가하고 이를 동일하게 구성할 수 있습니다. 그렇지 않은 경우 에이전트를 고유하게 유지하십시오.

옵션	설명
중복 에이전트	서로 다른 서버에 중복 에이전트를 설치합니다. 중복 에이전트를 동일하게 이름 지정하고 구성합니다.
독립형 에이전트	에이전트에 고유한 이름을 할당합니다.

13 끝점을 구성하는 IaaS 관리자에게 **에이전트 이름**을 알려줍니다.

액세스 및 데이터 수집이 가능하도록 설정하려면 해당 기능이 구성된 에이전트에 끝점이 연결되어 있어야 합니다.

14 IaaS Manager Service 호스트에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	Manager Service 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	Manager Service 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

15 IaaS 웹 서버에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	웹 서버 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	웹 서버 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

16 **테스트**를 클릭하여 각 호스트에 대한 연결을 확인합니다.**17** 관리되는 서버 인스턴스에 대해 관리 수준의 사용 권한을 가진 사용자의 자격 증명을 입력합니다.**18** **추가**를 클릭합니다.

19 다음을 클릭합니다.

20 (선택 사항) 다른 에이전트를 추가합니다.

예를 들어, 이전에 Hyper-V 에이전트를 추가했다면 Xen 에이전트를 추가할 수 있습니다.

21 설치를 클릭하여 설치를 시작합니다.

몇 분 정도 후에 성공 메시지가 표시됩니다.

22 다음을 클릭합니다.

23 완료를 클릭합니다.

24 설치가 완료되었는지 확인합니다.

다음에 수행할 작업

고가용성을 위해 끝점에 대해 중복 에이전트를 설치하고 구성할 수 있습니다. 중복 에이전트 각각을 별도의 서버에 설치하지만 에이전트를 동일한 이름으로 지정하고 구성합니다.

[Hyper-V 또는 XenServer 에이전트 구성](#).

Hyper-V 또는 XenServer 에이전트 구성

시스템 관리자는 가상화 플랫폼에 대한 삭제 정책과 같은 프록시 에이전트 구성 설정을 수정할 수 있습니다. 프록시 에이전트 유틸리티를 사용하여 에이전트 구성 파일에서 암호화된 초기 구성을 수정할 수 있습니다.

사전 요구 사항

에이전트를 설치한 시스템에 **시스템 관리자**로 로그인합니다.

절차

- 1** `agent_name`이 프록시 에이전트를 포함한 디렉토리이며 에이전트가 설치된 이름이기도 한 에이전트 설치 디렉토리로 변경합니다.

```
cd Program Files (x86)\VMware\VCAC Agents\agent_name
```

- 2** 현재 구성 설정을 봅니다.

`DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get`을 입력합니다.

다음은 명령 출력의 예입니다.

```
Username: XSadmin
```

- 3** `set` 명령을 입력하여 속성을 변경합니다. 여기서 속성은 테이블에 표시된 옵션 중 하나입니다.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set 속성 값
```

값을 생략하는 경우 유틸리티는 새 값을 입력하라는 메시지를 표시합니다.

속성	설명
username	에이전트가 통신하는 XenServer 또는 Hyper-V Server에 대한 관리자 수준 자격 증명을 나타내는 사용자 이름입니다.
password	관리자 수준의 사용자 이름에 대한 암호입니다.

4 시작 > 관리 도구 > 서비스를 클릭하고 vRealize Automation 에이전트 - 에이전트 이름 서비스를 다시 시작합니다.

예제: 관리자 수준 자격 증명 변경

다음 명령을 입력하여 에이전트 설치 중 지정된 가상화 플랫폼에 대한 관리자 수준 자격 증명을 변경합니다.

```
Dynamic0ps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
```

```
Dynamic0ps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

다음에 수행할 작업

고가용성을 위해 끝점에 대해 중복 에이전트를 설치하고 구성할 수 있습니다. 중복 에이전트 각각을 별도의 서버에 설치하지만 에이전트를 동일한 이름으로 지정하고 구성합니다.

XenDesktop의 VDI 에이전트 설치

vRealize Automation은 프로비저닝하는 XenDesktop 시스템을 외부 데스크톱 관리 시스템에 등록하는데 VDI(가상 데스크톱 통합) PowerShell 에이전트를 사용합니다.

VDI 통합 에이전트는 등록된 시스템 소유자가 XenDesktop 웹 인터페이스에 직접 연결할 수 있도록 해줍니다. VDI 에이전트를 단일 DDC(Desktop Delivery Controller)와 상호 작용하는 전용 에이전트로 설치하거나, 여러 DDC와 상호 작용할 수 있는 일반 에이전트로 설치할 수 있습니다.

XenDesktop 요구 사항

시스템 관리자는 VDI(Virtual Desktop Infrastructure) 에이전트를 설치하여 XenDesktop 서버를 vRealize Automation에 통합합니다.

여러 서버와 상호 작용하기 위한 일반 VDI 에이전트를 설치할 수 있습니다. 로드 밸런싱 또는 인증 때문에 서버당 하나의 전용 에이전트를 설치하는 경우, 에이전트를 설치할 때 XenDesktop DDC 서버의 이름을 제공해야 합니다. 전용 에이전트는 해당 구성에 지정된 서버로 방향 지정되는 등록 요청만 처리할 수 있습니다.

XenDesktop DDC 서버에 대해 지원되는 XenDesktop 버전에 대한 자세한 내용은 VMware 웹 사이트에서 "vRealize Automation 지원 매트릭스"를 참조하십시오.

설치 호스트 및 자격 증명

에이전트 실행에 사용되는 자격 증명에는 상호 작용하는 모든 XenDesktop DDC 서버에 대한 관리 액세스 권한이 있어야 합니다.

XenDesktop 요구 사항

XenDesktop 서버에서 XenServer 호스트에 지정된 이름은 XenCenter에서 Xen 풀의 UUID에 일치해야 합니다. 자세한 내용은 [XenServer 호스트 이름 설정](#)를 참조하십시오.

시스템을 등록하려는 각 XenDesktop DDC 서버는 다음 방법으로 구성되어야 합니다.

- vRealize Automation과 함께 사용하려면 그룹/카탈로그 유형을 **기존**으로 설정해야 합니다.
- DDC 서버의 vCenter Server 호스트 이름은 vRealize Automation vSphere 끝점에 입력된 vCenter Server 인스턴스의 이름에 일치해야 합니다(도메인 제외). 끝점은 IP 주소가 아니라 FQDN(정규화된 도메인 이름)으로 구성되어야 합니다. 예를 들어 끝점의 주소가 <https://virtual-center27.domain/sdk>인 경우 DDC 서버의 호스트 이름은 virtual-center27로 설정되어야 합니다.

vRealize Automation vSphere 끝점이 IP 주소로 구성된 경우 FQDN을 사용하도록 변경해야 합니다. 끝점 설정에 대한 자세한 내용은 "IaaS 구성"을 참조하십시오.

XenDesktop 에이전트 호스트 요구 사항

XenDesktop SDK가 설치되어 있어야 합니다. XenDesktop용 SDK는 XenDesktop 설치 디스크에 포함되어 있습니다.

에이전트 설치를 수행하기 이전에 Microsoft PowerShell이 설치 호스트에 설치되어 있는지 확인합니다. 필요한 버전은 설치 호스트의 운영 체제에 따라 다릅니다. Microsoft 도움말 및 지원 센터를 참조하십시오.

MS PowerShell 실행 정책이 RemoteSigned 또는 Unrestricted로 설정되었는지 확인합니다.

[PowerShell 실행 정책을 RemoteSigned로 설정](#) 항목을 참조하십시오.

PowerShell 실행 정책에 대한 자세한 내용을 보려면 PowerShell 명령 프롬프트에서 `help about_signing` 또는 `help Set-ExecutionPolicy`를 실행하십시오.

XenServer 호스트 이름 설정

XenDesktop에서 XenDesktop 서버의 XenServer 호스트에 지정된 이름은 XenCenter에서 XenPool의 UUID와 일치해야 합니다. XenPool이 구성되어 있지 않으면 해당 이름은 XenServer 자체의 UUID와 일치해야 합니다.

절차

- 1 Citrix XenCenter에서 XenPool 또는 독립형 XenServer를 선택하고 **일반** 탭을 클릭합니다. UUID를 기록해 둡니다.
- 2 XenServer 풀 또는 독립형 호스트를 XenDesktop에 추가할 때 이전 단계에서 기록해 둔 UUID를 **연결** 이름으로 입력합니다.

XenDesktop 에이전트 설치

VDI(가상 데스크톱 통합) PowerShell 에이전트는 XenDesktop 및 Citrix 같은 외부 가상 데스크톱 시스템과 통합됩니다. VDI PowerShell 에이전트는 XenDesktop 시스템을 관리하는 데 사용할 수 있습니다.

사전 요구 사항

- 웹 서버 및 Manager Service 호스트를 포함하여 IaaS를 설치합니다.
- [XenDesktop 요구 사항](#)의 요구 사항이 충족되었는지 확인합니다.
- [vRealize Automation IaaS 설치 관리자 다운로드](#).

절차

- 1 `setup__vrealize-automation-appliance-FQDN@5480.exe` 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 2 **다음**을 클릭합니다.
- 3 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 4 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.
 - a 사용자 이름(**root**)과 암호를 입력합니다.
 암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.
 - b **인증서 수락**을 선택합니다.
 - c **인증서 보기**를 클릭합니다.
 인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.
- 5 **다음**을 클릭합니다.
- 6 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.
- 7 [구성 요소 선택] 창에서 **프록시 에이전트**를 선택합니다.
- 8 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.
 분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다.
 IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.
- 9 **다음**을 클릭합니다.
- 10 설치 시스템의 Windows 서비스에 대한 관리자 권한을 사용하여 로그인합니다.
 서비스는 동일한 설치 시스템에서 실행되어야 합니다.
- 11 **다음**을 클릭합니다.
- 12 **에이전트 유형** 목록에서 **VdiPowerShell**을 선택합니다.

13 이 에이전트의 ID를 **에이전트 이름** 텍스트 상자에 입력합니다.

각 에이전트에 대해 에이전트 이름, 자격 증명, 끝점 이름 및 플랫폼 인스턴스의 기록을 유지해야 합니다. 이 정보는 나중에 끝점을 구성하고 호스트를 추가하는 데 필요합니다.

중요 고가용성을 위해 중복 에이전트를 추가하고 이를 동일하게 구성할 수 있습니다. 그렇지 않은 경우 에이전트를 고유하게 유지하십시오.

옵션	설명
중복 에이전트	서로 다른 서버에 중복 에이전트를 설치합니다. 중복 에이전트를 동일하게 이름 지정하고 구성합니다.
독립형 에이전트	에이전트에 고유한 이름을 할당합니다.

14 IaaS Manager Service 호스트에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	Manager Service 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	Manager Service 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

15 IaaS 웹 서버에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	웹 서버 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	웹 서버 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

16 테스트를 클릭하여 각 호스트에 대한 연결을 확인합니다.**17** VDI 버전을 선택합니다.**18** 관리되는 서버의 정규화된 도메인 이름을 **VDI 서버** 텍스트 상자에 입력합니다.**19** 추가를 클릭합니다.**20** 다음을 클릭합니다.

21 설치를 클릭하여 설치를 시작합니다.

몇 분 정도 후에 성공 메시지가 표시됩니다.

22 다음을 클릭합니다.

23 완료를 클릭합니다.

24 설치가 완료되었는지 확인합니다.

25 (선택 사항) 서로 다른 구성 및 동일한 끝점을 가진 여러 에이전트를 같은 시스템에 추가합니다.

다음에 수행할 작업

고가용성을 위해 끝점에 대해 중복 에이전트를 설치하고 구성할 수 있습니다. 중복 에이전트 각각을 별도의 서버에 설치하지만 에이전트를 동일한 이름으로 지정하고 구성합니다.

Citrix용 EPI 에이전트 설치

EPI(External Provisioning Integration) PowerShell 에이전트는 Citrix 외부 시스템을 프로비저닝 프로세스에 통합합니다. EPI 에이전트는 시스템이 부팅되고 실행되는 Citrix 디스크 이미지에 대해 요청 시 스트리밍 기능을 제공합니다.

전용 EPI 에이전트는 단일 외부 프로비저닝 서버와 상호 작용합니다. EPI 에이전트는 Citrix 프로비저닝 서버 인스턴스마다 하나씩 설치해야 합니다.

Citrix Provisioning Server 요구 사항

시스템 관리자는 EPI(External Provisioning Infrastructure) 에이전트를 사용하여 Citrix Provisioning Server를 통합하고 프로비저닝 프로세스에서 Visual Basic 스크립트를 사용하도록 설정합니다.

설치 위치 및 자격 증명

Citrix Provisioning Services 인스턴스에 대해 PVS 호스트에 에이전트를 설치합니다. 에이전트를 설치하기 전에 설치 호스트가 **Citrix 에이전트 호스트 요구 사항**을 충족하는지 확인하십시오.

일반적으로 EPI 에이전트는 여러 서버와 상호 작용할 수 있지만 Citrix Provisioning Server에는 전용 EPI 에이전트가 필요합니다. 각 Citrix Provisioning Server 인스턴스에 대해 하나의 EPI 에이전트를 설치하고 이를 호스팅하는 서버의 이름을 제공해야 합니다. 에이전트가 실행되는 자격 증명에는 Citrix Provisioning Server 인스턴스에 대한 관리자 액세스 권한이 있어야 합니다.

지원되는 Citrix PVS 버전에 대한 자세한 내용은 "vRealize Automation 지원 매트릭스"를 참조하십시오.

Citrix 에이전트 호스트 요구 사항

에이전트를 설치하기 전에 설치 호스트에 PowerShell 및 Citrix Provisioning Services SDK를 설치해야 합니다. 자세한 내용은 VMware 웹 사이트에서 "vRealize Automation 지원 매트릭스"를 참조하십시오.

에이전트 설치를 수행하기 이전에 Microsoft PowerShell이 설치 호스트에 설치되어 있는지 확인합니다. 필요한 버전은 설치 호스트의 운영 체제에 따라 다릅니다. Microsoft 도움말 및 지원 센터를 참조하십시오.

PowerShell 스냅인이 설치되어 있는지도 확인해야 합니다. 자세한 내용은 Citrix 웹 사이트에서 "Citrix Provisioning Services PowerShell 프로그래머 가이드"를 참조하십시오.

MS PowerShell 실행 정책이 RemoteSigned 또는 Unrestricted로 설정되었는지 확인합니다.

PowerShell 실행 정책을 RemoteSigned로 설정 항목을 참조하십시오.

PowerShell 실행 정책에 대한 자세한 내용을 보려면 PowerShell 명령 프롬프트에서 `help about_signing` 또는 `help Set-ExecutionPolicy`를 실행하십시오.

Citrix 에이전트 설치

EPI(External Provisioning Integration) PowerShell 에이전트는 외부 시스템을 시스템 프로비저닝 프로세스에 통합합니다. EPI PowerShell 에이전트를 사용하여 Citrix 프로비저닝 서버와 통합하면 요청 시 디스크 스트리밍을 통해 시스템을 프로비저닝할 수 있습니다.

사전 요구 사항

- 웹 서버 및 Manager Service 호스트를 포함하여 IaaS를 설치합니다.
- Citrix Provisioning Server 요구 사항의 요구 사항이 충족되었는지 확인합니다.
- vRealize Automation IaaS 설치 관리자 다운로드.

절차

- 1 `setup__vrealize-automation-appliance-FQDN@5480.exe` 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 2 **다음**을 클릭합니다.
- 3 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 4 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.
 - a 사용자 이름(**root**)과 암호를 입력합니다.
암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.
 - b **인증서 수락**을 선택합니다.
 - c **인증서 보기**를 클릭합니다.
인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.
- 5 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.
- 6 [설치 유형] 페이지에서 **구성 요소 선택**을 선택합니다.
- 7 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.
분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다.
IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.
- 8 **다음**을 클릭합니다.

- 9 설치 시스템의 Windows 서비스에 대한 관리자 권한을 사용하여 로그인합니다.

서비스는 동일한 설치 시스템에서 실행되어야 합니다.

- 10 다음을 클릭합니다.

- 11 [에이전트 유형] 목록에서 **EPIPowerShell**을 선택합니다.

- 12 이 에이전트의 ID를 **에이전트 이름** 텍스트 상자에 입력합니다.

각 에이전트에 대해 에이전트 이름, 자격 증명, 끝점 이름 및 플랫폼 인스턴스의 기록을 유지해야 합니다. 이 정보는 나중에 끝점을 구성하고 호스트를 추가하는 데 필요합니다.

중요 고가용성을 위해 중복 에이전트를 추가하고 이를 동일하게 구성할 수 있습니다. 그렇지 않은 경우 에이전트를 고유하게 유지하십시오.

옵션	설명
중복 에이전트	서로 다른 서버에 중복 에이전트를 설치합니다. 중복 에이전트를 동일하게 이름 지정하고 구성합니다.
독립형 에이전트	에이전트에 고유한 이름을 할당합니다.

- 13 IaaS Manager Service 호스트에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	Manager Service 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	Manager Service 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

- 14 IaaS 웹 서버에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	웹 서버 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	웹 서버 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

- 15 **테스트**를 클릭하여 각 호스트에 대한 연결을 확인합니다.

- 16 EPI 유형을 선택합니다.

17 관리되는 서버의 정규화된 도메인 이름을 **EPI 서버** 텍스트 상자에 입력합니다.

18 **추가**를 클릭합니다.

19 **다음**을 클릭합니다.

20 **설치**를 클릭하여 설치를 시작합니다.

몇 분 정도 후에 성공 메시지가 표시됩니다.

21 **다음**을 클릭합니다.

22 **완료**를 클릭합니다.

23 설치가 완료되었는지 확인합니다.

24 (선택 사항) 서로 다른 구성 및 동일한 끝점을 가진 여러 에이전트를 같은 시스템에 추가합니다.

다음에 수행할 작업

고가용성을 위해 끝점에 대해 중복 에이전트를 설치하고 구성할 수 있습니다. 중복 에이전트 각각을 별도의 서버에 설치하지만 에이전트를 동일한 이름으로 지정하고 구성합니다.

Visual Basic 스크립팅용 EPI 에이전트 설치

시스템 관리자는 시스템을 프로비저닝하기 전이나 후의 프로비저닝 프로세스 또는 시스템 프로비저닝을 해제할 때 Visual Basic 스크립트를 추가적인 단계로 지정할 수 있습니다. Visual Basic 스크립트를 실행할 수 있으려면 먼저 EPI(External Provisioning Integration) PowerShell을 설치해야 합니다.

Visual Basic 스크립트는 시스템이 프로비저닝되는 Blueprint에 지정됩니다. 이러한 스크립트는 시스템과 관련된 모든 사용자 지정 속성에 액세스하고 해당 속성 값을 업데이트할 수 있습니다. 워크플로의 다음 단계는 이러한 새 값에 액세스하는 것입니다.

예를 들어 스크립트를 사용하면 프로비저닝 이전에 인증서나 보안 토큰을 생성하여 시스템 프로비저닝 과정에서 사용할 수 있습니다.

프로비저닝 중에 스크립트를 사용하도록 설정하려면 특정 유형의 EPI 에이전트를 설치하고, 사용하려는 스크립트를 에이전트가 설치되어 있는 시스템에 배치해야 합니다.

스크립트를 실행할 때 EPI 에이전트는 시스템의 모든 사용자 지정 속성을 스크립트에 인수로 전달합니다. 업데이트된 속성 값을 반환하려면 이러한 속성을 사전에 배치하고 vRealize Automation 함수를 호출해야 합니다. EPI 에이전트 설치 디렉토리의 **scripts** 하위 디렉토리에 샘플 스크립트가 포함되어 있습니다. 이 스크립트에는 모든 인수를 사전에 로드하는 머리글, 함수를 포함할 수 있는 본문 및 업데이트된 사용자 지정 속성 값을 반환하는 바닥글이 포함되어 있습니다.

참고 여러 서버에 EPI/VBScripts 에이전트를 여러 개 설치하고, 특정 에이전트와 해당 에이전트의 호스트에 있는 Visual Basic 스크립트를 사용하여 프로비저닝을 수행할 수 있습니다. 이렇게 하려면 VMware 고객 지원팀에 문의하십시오.

Visual Basic 스크립팅 요구 사항

시스템 관리자는 프로비저닝 프로세스에서 Visual Basic 스크립트를 사용할 수 있도록 EPI(External Provisioning Infrastructure) 에이전트를 설치합니다.

다음 표에서는 프로비저닝 프로세스에서 Visual Basic 스크립트를 사용할 수 있도록 EPI 에이전트를 설치할 때 적용되는 요구 사항을 설명합니다.

표 1-37. 가상 스크립팅용 EPI 에이전트

요구 사항	설명
자격 증명	에이전트 실행에 사용될 자격 증명에는 설치 호스트에 대한 관리 액세스 권한이 있어야 합니다.
Microsoft PowerShell	에이전트 설치 전에 Microsoft PowerShell을 설치 호스트에 설치해야 합니다. 필요한 버전은 설치 호스트의 운영 체제에 따라 다르며 해당 운영 체제와 함께 설치되어 있을 수 있습니다. 자세한 내용은 http://support.microsoft.com 을 참조하십시오.
MS PowerShell 실행 정책	MS PowerShell 실행 정책을 RemoteSigned 또는 Unrestricted 로 설정해야 합니다. PowerShell 실행 정책에 대한 정보를 보려면 Power-Shell 명령 프롬프트에서 다음 명령 중 하나를 실행하십시오.
	<pre>help about_signing help Set-ExecutionPolicy</pre>

Visual Basic 스크립팅용 에이전트 설치

EPI(External Provisioning Integration) PowerShell 에이전트를 사용하면 외부 시스템을 시스템 프로비저닝 프로세스에 통합할 수 있습니다. EPI 에이전트는 프로비저닝 프로세스 중의 추가적인 단계로 Visual Basic 스크립트를 실행하는 데 사용할 수 있습니다.

사전 요구 사항

- 웹 서버 및 Manager Service 호스트를 포함하여 IaaS를 설치합니다.
- [Visual Basic 스크립팅 요구 사항](#)의 요구 사항이 충족되었는지 확인합니다.
- [vRealize Automation IaaS 설치 관리자 다운로드](#).

절차

- 1 `setup__vrealize-automation-appliance-FQDN@5480.exe` 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 2 **다음**을 클릭합니다.
- 3 라이선스 계약에 동의하고 **다음**을 클릭합니다.

- 4 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.

a 사용자 이름(**root**)과 암호를 입력합니다.

암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.

b **인증서 수락**을 선택합니다.

c **인증서 보기**를 클릭합니다.

인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.

- 5 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.

- 6 [설치 유형] 페이지에서 **구성 요소 선택**을 선택합니다.

- 7 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.

분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다.

IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.

- 8 **다음**을 클릭합니다.

- 9 설치 시스템의 Windows 서비스에 대한 관리자 권한을 사용하여 로그인합니다.

서비스는 동일한 설치 시스템에서 실행되어야 합니다.

- 10 **다음**을 클릭합니다.

- 11 [에이전트 유형] 목록에서 **EPIPowerShell**을 선택합니다.

- 12 이 에이전트의 ID를 **에이전트 이름** 텍스트 상자에 입력합니다.

각 에이전트에 대해 에이전트 이름, 자격 증명, 끝점 이름 및 플랫폼 인스턴스의 기록을 유지해야 합니다. 이 정보는 나중에 끝점을 구성하고 호스트를 추가하는 데 필요합니다.

중요 고가용성을 위해 중복 에이전트를 추가하고 이를 동일하게 구성할 수 있습니다. 그렇지 않은 경우 에이전트를 고유하게 유지하십시오.

옵션	설명
중복 에이전트	서로 다른 서버에 중복 에이전트를 설치합니다. 중복 에이전트를 동일하게 이름 지정하고 구성합니다.
독립형 에이전트	에이전트에 고유한 이름을 할당합니다.

13 IaaS Manager Service 호스트에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	Manager Service 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	Manager Service 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

14 IaaS 웹 서버에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	웹 서버 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	웹 서버 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

15 테스트를 클릭하여 각 호스트에 대한 연결을 확인합니다.**16** EPI 유형을 선택합니다.**17** 관리되는 서버의 정규화된 도메인 이름을 **EPI 서버** 텍스트 상자에 입력합니다.**18** 추가를 클릭합니다.**19** 다음을 클릭합니다.**20** 설치를 클릭하여 설치를 시작합니다.

몇 분 정도 후에 성공 메시지가 표시됩니다.

21 다음을 클릭합니다.**22** 완료를 클릭합니다.**23** 설치가 완료되었는지 확인합니다.**24** (선택 사항) 서로 다른 구성 및 동일한 끝점을 가진 여러 에이전트를 같은 시스템에 추가합니다.

원격 WMI 요청용 WMI 에이전트 설치

시스템 관리자는 데이터 및 작업을 관리하기 위해 WMI(Windows Management Instrumentation) 프로토콜을 사용 가능하도록 설정하고, 관리되는 모든 Windows 시스템에 WMI 에이전트를 설치합니다. 이 에이전트는 시스템 소유자의 Active Directory 상태 등과 같은 데이터를 Windows 시스템에서 수집하는 데 필요합니다.

Windows 시스템에서 원격 WMI 요청 사용

WMI 에이전트를 사용하려면 관리되는 Windows 서버에서 원격 WMI 요청을 사용하도록 설정해야 합니다.

절차

- 1 프로비저닝되고 관리되는 Windows 가상 시스템이 포함된 각 도메인에서 Active Directory 그룹을 생성하고 프로비저닝된 시스템에서 원격 WMI 요청을 실행하는 WMI 에이전트의 서비스 자격 증명에 추가합니다.
- 2 프로비저닝된 각 Windows 시스템에서 에이전트 자격 증명을 포함하는 Active Directory 그룹에 대해 원격 WMI 요청을 사용하도록 설정합니다.

WMI 에이전트 설치

WMI(Windows Management Instrumentation) 에이전트는 Windows 관리 시스템에서 데이터를 수집할 수 있게 해줍니다.

사전 요구 사항

- 웹 서버 및 Manager Service 호스트를 포함하여 IaaS를 설치합니다.
- [Windows 시스템에서 원격 WMI 요청 사용](#)의 요구 사항이 충족되었는지 확인합니다.
- [vRealize Automation IaaS 설치 관리자 다운로드](#).

절차

- 1 `setup__vrealize-automation-appliance-FQDN@5480.exe` 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 2 **다음**을 클릭합니다.
- 3 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 4 [로그인] 페이지에서 vRealize Automation 장치에 대한 관리자 자격 증명을 입력하고 SSL 인증서를 확인합니다.
 - a 사용자 이름(**root**)과 암호를 입력합니다.
암호는 vRealize Automation 장치를 배포할 때 지정한 암호입니다.
 - b **인증서 수락**을 선택합니다.
 - c **인증서 보기**를 클릭합니다.
인증서 지문과 vRealize Automation 장치의 지문 집합을 비교합니다. vRealize Automation 장치 인증서는 vRealize Automation 장치 관리 인터페이스를 포트 5480에서 액세스한 경우에 클라이언트 브라우저에서 볼 수 있습니다.
- 5 [설치 유형] 페이지에서 **사용자 지정 설치**를 선택합니다.
- 6 [설치 유형] 페이지에서 **구성 요소 선택**을 선택합니다.

- 7 루트 설치 위치를 수락하거나, **변경**을 클릭하고 설치 경로를 선택합니다.

분산 배포인 경우에도 동일한 Windows 서버에 IaaS 구성 요소를 둘 이상 설치하는 경우가 있습니다.

IaaS 구성 요소를 둘 이상 설치하는 경우 항상 동일한 경로에 설치합니다.

- 8 다음을 클릭합니다.

- 9 설치 시스템의 Windows 서비스에 대한 관리자 권한을 사용하여 로그인합니다.

서비스는 동일한 설치 시스템에서 실행되어야 합니다.

- 10 다음을 클릭합니다.

- 11 에이전트 유형 목록에서 **WMI**를 선택합니다.

- 12 이 에이전트의 ID를 **에이전트 이름** 텍스트 상자에 입력합니다.

각 에이전트에 대해 에이전트 이름, 자격 증명, 끝점 이름 및 플랫폼 인스턴스의 기록을 유지해야 합니다. 이 정보는 나중에 끝점을 구성하고 호스트를 추가하는 데 필요합니다.

중요 고가용성을 위해 중복 에이전트를 추가하고 이를 동일하게 구성할 수 있습니다. 그렇지 않은 경우 에이전트를 고유하게 유지하십시오.

옵션	설명
중복 에이전트	서로 다른 서버에 중복 에이전트를 설치합니다. 중복 에이전트를 동일하게 이름 지정하고 구성합니다.
독립형 에이전트	에이전트에 고유한 이름을 할당합니다.

- 13 IaaS Manager Service 호스트에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	Manager Service 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	Manager Service 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>mgr-svc.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

14 IaaS 웹 서버에 대한 연결을 구성합니다.

옵션	설명
로드 밸런서를 사용하는 경우	웹 서버 구성 요소에 대한 로드 밸런서의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web-load-balancer.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.
로드 밸런서를 사용하지 않는 경우	웹 서버 구성 요소가 설치된 시스템의 FQDN(정규화된 도메인 이름)과 포트 번호를 입력합니다(<i>web.mycompany.com:443</i>). IP 주소를 입력하지 마십시오.

기본 포트는 443입니다.

15 테스트를 클릭하여 각 호스트에 대한 연결을 확인합니다.**16** 추가를 클릭합니다.**17** 다음을 클릭합니다.**18** 설치를 클릭하여 설치를 시작합니다.

몇 분 정도 후에 성공 메시지가 표시됩니다.

19 다음을 클릭합니다.**20** 완료를 클릭합니다.**21** 설치가 완료되었는지 확인합니다.**22** (선택 사항) 서로 다른 구성 및 동일한 끝점을 가진 여러 에이전트를 같은 시스템에 추가합니다.

자동 vRealize Automation 설치

vRealize Automation에는 명령줄에서 스크립트 기반의 자동 설치를 수행하는 옵션과 API 기반 자동 설치를 수행하는 옵션이 포함되어 있습니다. 이 두 접근 방식을 사용하려면 일반적인 설치 중에 직접 입력해야 하는 값을 미리 준비해야 합니다.

자동 vRealize Automation 설치 정보

vRealize Automation 자동 설치에는 텍스트 기반 응답 파일을 참조하는 실행 파일이 사용됩니다.

응답 파일에는 대개 일반적인 마법사 기반 설치 또는 수동 설치 과정 중에 추가하는 시스템 FQDN, 계정 자격 증명 및 기타 설정을 미리 구성합니다. 자동 설치는 다음과 같은 종류의 배포에 유용합니다.

- 거의 동일한 여러 개의 환경 배포
- 동일한 환경을 반복적으로 다시 배포
- 무인 설치 수행
- 스크립트를 사용하여 설치 수행

vRealize Automation 자동 설치 수행

새로 배포된 vRealize Automation 장치의 콘솔에서 vRealize Automation 자동 설치를 수행할 수 있습니다.

사전 요구 사항

- 구성되지 않은 장치를 생성합니다. [vRealize Automation 장치 배포](#) 항목을 참조하십시오.
- IaaS Windows Server를 생성 또는 식별하고 해당 사전 요구 사항을 구성합니다.
- IaaS Windows Server에서 관리 에이전트를 설치합니다.

기존의 .msi 파일 다운로드 또는 [vRealize Automation 관리 에이전트 자동 설치 수행](#)에 설명된 자동 프로세스를 사용하여 관리 에이전트를 설치할 수 있습니다.

절차

- 1 루트로 vRealize Automation 장치 콘솔에 로그인합니다.

- 2 다음 디렉토리로 이동합니다.

```
/usr/lib/vcac/tools/install
```

- 3 텍스트 편집기에서 **ha.properties** 응답 파일을 엽니다.

- 4 배포 관련 항목을 **ha.properties**에 추가한 후 파일을 저장하고 닫습니다.

또는, 전체 기본 파일을 편집하는 대신 다른 배포에서 **ha.properties** 파일을 복사 및 수정하여 시간을 절약할 수 있습니다.

- 5 동일한 디렉토리에서 다음 명령을 실행하여 설치를 시작합니다.

```
vra-ha-config.sh
```

환경 및 배포 크기에 따라 설치에 최대 한 시간 이상 걸릴 수 있습니다.

- 6 (선택 사항) 설치가 완료되면 로그 파일을 검토합니다.

```
/var/log/vcac/vra-ha-config.log
```

자동 설치 관리자는 암호, 라이선스 또는 인증서와 같은 독점 데이터를 로그에 저장하지 않습니다.

vRealize Automation 관리 에이전트 자동 설치 수행

모든 IaaS Windows Server에서 명령줄 기반 vRealize Automation 관리 에이전트 설치를 수행할 수 있습니다.

관리 에이전트 자동 설치에는 몇 가지 설정을 사용자 지정하는 Windows PowerShell 스크립트로 구성됩니다. 배포 관련 설정을 추가한 후 각각 동일한 스크립트 사본을 실행하여 모든 IaaS Windows Server에 관리 에이전트를 자동으로 설치할 수 있습니다.

사전 요구 사항

- 구성되지 않은 장치를 생성합니다. [vRealize Automation 장치 배포](#) 항목을 참조하십시오.

- IaaS Windows Server를 생성 또는 식별하고 해당 사전 요구 사항을 구성합니다.

절차

- 1 관리자 권한이 있는 계정을 사용하여 IaaS Windows Server에 로그인합니다.
- 2 웹 브라우저를 열고 vRealize Automation 장치 설치 관리자 URL에 연결합니다.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 `InstallManagementAgent.ps1` PowerShell 스크립트 파일에 대한 링크를 마우스 오른쪽 버튼으로 클릭하고 IaaS Windows Server의 바탕 화면 또는 폴더에 파일을 저장합니다.
- 4 텍스트 편집기에서 `InstallManagementAgent.ps1`을 엽니다.
- 5 스크립트 파일의 상단에 배포 관련 설정을 추가합니다.
 - vRealize Automation 장치 URL
`https://vrealize-automation-appliance-FQDN:5480`
 - vRealize Automation 장치 루트 사용자 계정 자격 증명
 - vRealize Automation 서비스 사용자 자격 증명, IaaS Windows Server에 대해 관리자 권한을 가진 도메인 계정
 - 관리 에이전트를 설치하려는 폴더(기본적으로 `Program Files (x86)`)
 - (선택 사항) 인증에 사용 중인 PEM 형식 인증서의 지문
- 6 `InstallManagementAgent.ps1`을 저장한 후 닫습니다.
- 7 관리 에이전트를 자동으로 설치하려면 `InstallManagementAgent.ps1`을 두 번 클릭합니다.
- 8 (선택 사항) 프로그램 및 기능의 Windows 제어판 목록 그리고 실행 중인 Windows 서비스 목록에서 **VMware vCloud Automation Center 관리 에이전트**를 찾아 설치가 완료되었는지 확인합니다.

vRealize Automation 자동 설치 응답 파일

vRealize Automation 자동 설치를 위해서는 텍스트 기반 응답 파일을 미리 준비해야 합니다.

새로 배포된 모든 vRealize Automation 장치에는 기본 응답 파일이 포함되어 있습니다.

`/usr/lib/vcac/tools/install/ha.properties`

자동 설치를 수행하려면 텍스트 편집기를 사용하여 설치하려는 배포에 맞게 `ha.properties`의 설정을 사용자 지정해야 합니다. 다음은 반드시 추가해야 하는 몇 가지 설정 및 정보에 대한 예입니다.

- vRealize Automation 또는 제품군 라이선스 키
- vRealize Automation 장치 노드 FQDN
- vRealize Automation 장치 루트 사용자 계정 자격 증명
- 웹 노드, Manager Service 노드 등의 역할을 할 IaaS Windows Server FQDN

- vRealize Automation 서비스 사용자 자격 증명, IaaS Windows Server에 대해 관리자 권한을 가진 도메인 계정
- 로드 밸런서 FQDN
- SQL Server 데이터베이스 매개 변수
- 가상화 리소스에 연결하기 위한 프록시 에이전트 매개 변수
- 자동 설치 관리자가 누락된 IaaS Windows Server 사전 요구 사항에 대한 수정을 시도해야 하는지 여부

자동 설치 관리자는 누락된 여러 Windows 사전 요구 사항을 수정할 수 있습니다. 하지만 CPU 부족과 같은 일부 구성 문제점은 자동 설치 관리자가 변경할 수 없습니다.

시간 절약을 위해, 설정이 유사한 다른 배포를 위해 구성했던 **ha.properties** 파일을 수정하여 재사용할 수 있습니다. 또한 설치 마법사를 통해 수동으로 vRealize Automation을 설치할 때 마법사는 설정을 생성한 후 **ha.properties** 파일에 저장합니다. 유사한 배포를 자동으로 설치할 때 이 파일을 수정하여 재사용하면 유용할 수 있습니다.

마법사는 암호, 라이선스 또는 인증서와 같은 독점 설정을 **ha.properties** 파일에 저장하지 않습니다.

vRealize Automation 설치 명령줄

vRealize Automation에는 초기 설치 후 필요할 수 있는 설치 조정을 수행하기 위한 콘솔 기반의 명령줄 인터페이스가 포함되어 있습니다.

CLI(명령줄 인터페이스)는 초기 설치 후 브라우저 기반 인터페이스를 통해서는 더 이상 사용할 수 없는 설치 및 구성 작업을 실행할 수 있습니다. CLI 기능에는 사전 요구 사항 재검사, IaaS 구성 요소 설치, 인증서 설치 또는 사용자가 웹 브라우저에서 지정하는 vRealize Automation 호스트 이름 설정이 포함됩니다.

또한 CLI는 특정 작업을 스크립트로 작성하려는 고급 사용자에게도 유용합니다. 일부 CLI 기능은 자동 설치에 사용되므로 두 가지 기능에 모두 익숙해지면 vRealize Automation 설치 스크립팅에 대한 지식을 더욱 효과적으로 활용할 수 있습니다.

vRealize Automation 설치 명령줄 기본 사항

vRealize Automation 설치 명령줄 인터페이스는 최상위 기본 작업을 포함합니다.

기본 작업은 vRealize Automation 노드 ID 표시, 명령 실행, 명령 상태 보고 또는 도움말 정보 표시입니다. 콘솔 디스플레이에 이러한 작업 및 해당 옵션을 표시하려면 옵션 또는 한정자 없이 다음 명령을 입력합니다.

vra-command

노드 ID 표시

올바른 대상 시스템에 대해 명령을 실행할 수 있도록 vRealize Automation 노드 ID가 필요합니다. 노드 ID를 표시하려면 다음 명령을 입력합니다.

vra-command list-nodes

특정 시스템에 대해 명령을 실행하기 전에 노드 ID를 기록해 둡니다.

명령 실행

대부분의 명령줄 기능은 vRealize Automation 클러스터의 노드에 대해 명령을 실행하는 것과 관련됩니다. 명령을 실행하려면 다음 구문을 사용합니다.

```
vra-command execute --node node-IDcommand-name --parameter-nameparameter-value
```

앞의 구문에 표시된 대로 대부분의 명령에 매개 변수와 사용자가 선택한 매개 변수 값이 필요합니다.

명령 상태 표시

일부 명령은 완료하는 데 몇 분 또는 그 이상이 걸립니다. 입력된 명령의 진행률을 모니터링하려면 다음 명령을 입력합니다.

```
vra-command status
```

상태 명령은 대규모 배포의 경우 시간이 오래 걸릴 수 있는 자동 설치를 모니터링하는 데 특히 유용합니다.

도움말 표시

사용 가능한 모든 명령에 대해 도움말을 표시하려면 다음 명령을 입력합니다.

```
vra-command help
```

단일 명령에 대해 도움말을 표시하려면 다음 명령을 입력합니다.

```
vra-command help command-name
```

vRealize Automation 설치 명령 이름

명령은 초기 설치 후에 수행하려는 여러 vRealize Automation 설치 및 구성 작업에 대한 콘솔 액세스를 제공합니다.

사용 가능한 명령의 예에는 다음 기능이 포함됩니다.

- 다른 vRealize Automation 장치를 기존 설치에 추가
- 사용자가 vRealize Automation에 액세스할 때 사용자가 웹 브라우저에서 지정하는 호스트 이름 설정
- IaaS SQL Server 데이터베이스 생성
- IaaS Windows Server에 대해 사전 요구 사항 검사기 실행
- 인증서 가져오기

사용 가능한 vRealize Automation 명령의 전체 목록을 보려면 vRealize Automation 장치 콘솔에 로그인하고 다음 명령을 입력합니다.

```
vra-command help
```

명령 이름 및 매개 변수의 긴 목록은 별도의 문서에 복제되지 않습니다. 목록을 효과적으로 사용하려면 원하는 명령을 식별하고 다음 명령을 입력하여 범위를 좁힙니다.

```
vra-command help command-name
```

vRealize Automation 설치 API

설치용 vRealize Automation REST API는 vRealize Automation에 대해 순수하게 소프트웨어에서 제어되는 설치를 생성하는 기능을 제공합니다.

설치 API에는 CLI 기반 설치가 **ha.properties** 응답 파일에서 가져오는 동일한 항목의 JSON 형식의 버전이 필요합니다. 다음 지점은 API의 작동 방식을 안내합니다. 여기에서 vRealize Automation을 설치하기 위한 API에 대한 프로그래밍 방식 호출을 설계할 수 있어야 합니다.

- API 설명서에 액세스하려면 웹 브라우저를 다음 vRealize Automation 장치 페이지로 가리킵니다.

`https://vrealize-automation-appliance-FQDN:5480/config`

구성되지 않은 vRealize Automation 장치가 필요합니다. **vRealize Automation 장치 배포** 항목을 참조하십시오.

- API 기반 설치로 실험하려면 다음 PUT 명령을 찾아 확장합니다.

`PUT /vra-install`

- **install_json** 상자에서 텍스트 편집기로 채워지지 않은 JSON을 복사합니다. **ha.properties**에 대해 수행하는 것과 동일한 방식으로 응답 값을 입력합니다. JSON 형식의 응답이 준비되면 코드를 다시 **install_json**으로 복사하고 채워지지 않은 JSON을 덮어씁니다.

또는 다음 템플릿 JSON을 편집하고 결과를 **install_json**으로 복사할 수 있습니다.

`/usr/lib/vcac/tools/install/installationProperties.json`

완료된 **ha.properties**를 JSON으로 변환하거나 그 반대로 수행할 수도 있습니다.

- 작업 상자에서 **검증**을 선택하고 **시도**를 클릭합니다.

검증 작업은 vRealize Automation 사전 요구 사항 검사기 및 수정기를 실행합니다.

- 검증 응답에는 다음 GET 명령에 삽입할 수 있는 영숫자 명령 ID가 포함됩니다.

`GET /commands/command-id/aggregated-status`

GET에 대한 응답에는 검증 작업의 진행률이 포함됩니다.

- 검증이 성공하면 프로세스를 반복하여 실제 설치를 실행할 수 있습니다. 작업 상자에서 **검증** 대신 **설치**를 선택하기만 하면 됩니다.

배포 크기에 따라 설치에 오랜 시간이 걸릴 수 있습니다. 다시 명령 ID를 찾고 집계된 상태 GET 명령을 사용하여 설치 진행률을 가져옵니다. GET 응답은 다음 예와 유사할 수 있습니다.

```
"progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18,
"queued": 3, "processing": 1}, "failed-commands": 0
```

- 설치에 문제가 발생하는 경우 다음 명령을 사용하여 모든 노드에 대해 로그 수집을 트리거할 수 있습니다.

`PUT /commands/log-bundle`

설치와 마찬가지로 반환된 영숫자 명령 ID를 사용하여 로그 수집 상태를 모니터링할 수 있습니다.

vRealize Automation 자동 속성 및 JSON 간 변환

자동 vRealize Automation CLI 또는 API 기반 설치의 경우 완전한 속성 응답 파일을 JSON으로 변환하거나 그 반대로 수행할 수 있습니다. 자동 CLI 설치에는 속성 파일이 필요하지만 API에는 JSON 형식이 필요합니다.

사전 요구 사항

완전한 속성 응답 파일 또는 완전한 JSON 파일

```
/usr/lib/vcac/tools/install/ha.properties
```

또는

```
/usr/lib/vcac/tools/install/installationProperties.json
```

절차

1 vRealize Automation 장치 콘솔 세션에 루트로 로그인합니다.

2 적절한 변환기 스크립트를 실행합니다.

- JSON을 속성으로 변환

```
/usr/lib/vcac/tools/install/convert-properties --from-json  
installationProperties.json
```

스크립트는 다음 예와 같은 이름으로 타임 스탬프가 포함된 새 속성 파일을 생성합니다.

```
ha.2016-10-17_13.02.15.properties
```

- 속성을 JSON으로 변환

```
/usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
```

스크립트는 다음 예와 같은 이름으로 타임 스탬프가 포함된 새 installationProperties.json 파일을 생성합니다.

```
installationProperties.2016-10-17_13.36.13.json
```

결과

스크립트에 대한 도움말을 표시할 수도 있습니다.

```
/usr/lib/vcac/tools/install/convert-properties --help
```

vRealize Automation 사후 설치 작업

vRealize Automation을 설치한 후 주의를 요하는 사후 설치 작업을 수행해야 합니다.

vRealize Automation 표준 시간대 변경 안 함

vRealize Automation 장치 관리 인터페이스에 표준 시간대를 변경할 수 있는 옵션이 제공되지만, vRealize Automation 표준 시간대는 항상 Etc/UTC로 설정해 두어야 합니다.

Etc/UTC 이외의 표준 시간대를 사용하면 실패한 마이그레이션 및 모든 vRealize Automation 노드의 항목이 포함되지 않은 로그 번들 등과 같은 비정상적인 오류가 발생하는 것으로 알려져 있습니다.

피해야 하는 vRealize Automation 장치 관리 인터페이스 옵션은 **시스템 > 표준 시간대** 아래에 있습니다.

Federal Information Processing Standard 규격 암호화 구성

인바운드 및 아웃바운드 vRealize Automation 장치 네트워크 트래픽에 대해 FIPS(Federal Information Processing Standard) 140-2 규격 암호화를 사용하거나 사용하지 않도록 설정할 수 있습니다.

FIPS 설정을 변경하려면 vRealize Automation을 다시 시작해야 합니다. FIPS는 기본적으로 사용하지 않도록 설정되어 있습니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 2 **vRA > 호스트 설정**을 클릭합니다.

- 3 오른쪽 위에 있는 버튼을 클릭하여 FIPS를 사용하거나 사용하지 않도록 설정합니다.

사용하도록 설정되면 포트 443의 인바운드 및 아웃바운드 vRealize Automation 장치 네트워크 트래픽에서 FIPS 140-2 규격 암호화를 사용합니다. FIPS 설정에 관계없이 vRealize Automation은 AES-256 규격 알고리즘을 사용하여 vRealize Automation 장치에 저장된 보안 데이터를 보호합니다.

참고 이 vRealize Automation 릴리스에서는 일부 내부 구성 요소가 인증된 암호화 모듈을 사용하지 않기 때문에 FIPS 규격을 부분적으로만 사용합니다. 인증된 모듈이 아직 구현되지 않은 경우에는 AES-256 규격 알고리즘이 사용됩니다.

- 4 **예**를 클릭하여 vRealize Automation을 다시 시작합니다.

결과

다음 명령을 사용하여 vRealize Automation 장치 콘솔 세션에서 루트로 FIPS를 구성할 수도 있습니다.

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

자동 Manager Service 페일오버 사용

표준 vRealize Automation Windows Installer를 사용하여 Manager Service를 설치 또는 업그레이드하는 경우 자동 Manager Service 페일오버는 기본적으로 사용되지 않도록 설정됩니다.

표준 Windows Installer를 실행 한 후 자동 Manager Service 페일오버를 사용하도록 설정하려면 다음 단계를 수행합니다.

다중 노드 구성에서는 vRealize Automation 장치 노드에서 단계를 한 번만 수행해야 합니다.

절차

1 vRealize Automation 장치의 콘솔 세션에 루트로 로그인합니다.

2 다음 디렉토리로 이동합니다.

```
/usr/lib/vcac/tools/vami/commands
```

3 다음 명령을 입력합니다.

```
python ./manager-service-automatic-failover ENABLE
```

결과

laaS 배포 전체에서 자동 페일오버를 사용하지 않도록 설정하려면 다음 명령을 대신 입력합니다.

```
python ./manager-service-automatic-failover DISABLE
```

자동 Manager Service 페일오버 정보

기본 Manager Service가 중지되면 백업으로 페일오버되도록 vRealize AutomationlaaS Manager Service를 구성할 수 있습니다.

vRealize Automation 7.3부터 기본 또는 백업 역할을 할 호스트를 제어하기 위해 이제 더 이상 각 Windows Server에서 Manager Service를 수동으로 시작 또는 중지할 필요가 없습니다. 다음과 같은 경우 기본적으로 자동 Manager Service 페일오버가 사용되도록 설정됩니다.

- 자동으로 또는 설치 마법사를 사용하여 vRealize Automation을 설치하는 경우.
- 관리 인터페이스를 통해 또는 자동 업그레이드 스크립트를 사용하여 laaS를 업그레이드하는 경우.

표준 Windows 기반 설치 관리자를 사용하여 Manager Service 호스트를 추가하거나 laaS를 업그레이드하는 경우 페일오버가 사용되도록 설정되지 않습니다. 사용하도록 설정하려면 [자동 Manager Service 페일오버 사용](#) 항목을 참조하십시오.

자동 페일오버를 사용하도록 설정하면 백업을 포함한 모든 Manager Service 호스트에서 Manager Service가 자동으로 시작됩니다. 자동 페일오버 기능을 사용하면 호스트가 서로를 투명하게 모니터링하고 필요할 때 페일오버를 수행할 수 있습니다. 이 기능을 사용하려면 모든 호스트에서 Windows 서비스를 실행해야 합니다.

참고 자동 페일오버를 사용하지 않아도 됩니다. 자동 페일오버를 사용하지 않도록 설정하고 Windows 서비스를 계속 수동으로 시작하고 중지하여 기본 또는 백업 역할을 할 호스트를 제어할 수 있습니다. 수동 페일오버 방식을 사용하는 경우 한 번에 하나의 호스트에서만 서비스를 시작해야 합니다. 자동 페일오버가 사용되지 않도록 설정된 상태로 여러 laaS 서버에서 동시에 서비스를 실행하면 vRealize Automation을 사용할 수 없게 됩니다.

자동 페일오버를 선택적으로 사용 또는 사용하지 않도록 설정하지 마십시오. 자동 페일오버는 laaS 배포의 모든 Manager Service 호스트에서 설정되거나 해제된 상태로 항상 동기화되어야 합니다.

자동 페일오버가 작동하지 않는 경우에는 [자동 Manager Service 페일오버가 활성화되지 않음](#)에서 문제 해결 팁을 참조하십시오.

Manager Service 호스트에서 로드 밸런싱하는 방법에 대한 자세한 내용은 [vRealize Automation 로드 밸런싱](#)을 참조하십시오.

자동 vRealize Automation PostgreSQL 데이터베이스 페일오버

고가용성 vRealize Automation 배포에서, 일부 구성은 포함된 vRealize Automation PostgreSQL 데이터베이스의 자동 페일오버를 허용합니다.

자동 페일오버는 다음과 같은 조건에서 자동으로 설정됩니다.

- 고가용성 배포에는 3개의 vRealize Automation 장치가 포함되어 있습니다.
2개의 장치만 있는 경우 자동 페일오버가 지원되지 않습니다.
- vRealize Automation 관리 인터페이스 [클러스터] 탭에서 데이터베이스 복제가 [동기 모드]로 설정되어 있습니다.

보통 자동 페일오버가 사용되도록 설정된 경우에는 수동 페일오버를 수행하지 말아야 합니다. 하지만 일부 노드 문제의 경우 자동 페일오버를 사용하도록 설정한 경우에도 자동 페일오버가 발생하지 않을 수 있습니다. 이러한 경우에는 수동 페일오버 수행이 필요한지 여부를 확인하십시오.

- 1 기본 PostgreSQL 데이터베이스 노드에 장애가 발생한 후 나머지 클러스터가 안정화될 때까지 최대 5분간 기다립니다.
- 2 아직 사용 가능한 vRealize Automation 장치 노드에서, 브라우저를 열고 다음 URL로 이동합니다.
`https://vrealize-automation-appliance-FQDN:5434/api/status`
- 3 `manualFailoverNeeded`를 검색합니다.
- 4 `manualFailoverNeeded`가 True이면 수동 페일오버를 수행합니다.

자세한 내용은 [수동 vRealize Automation 장치 데이터베이스 페일오버 수행](#)을 참조하십시오.

자체 서명된 인증서를 기관에서 제공하는 인증서로 바꾸기

자체 서명된 인증서를 사용하여 vRealize Automation을 설치한 경우, 운영 환경에 배포하기 전에 해당 인증서를 인증 기관이 제공하는 인증서로 바꾸는 것이 좋습니다.

인증서 업데이트에 대한 자세한 내용은 [vRealize Automation 인증서 업데이트](#)를 참조하십시오.

호스트 이름 및 IP 주소 변경

일반적으로 vRealize Automation 시스템에 대해 계획한 호스트 이름, FQDN 및 IP 주소를 유지해야 합니다. 일부 사후 설치 변경이 가능하지만 복잡할 수 있습니다.

- IaaS SQL Server 데이터베이스를 호스팅하는 Windows 시스템의 호스트 이름을 변경하는 경우 [새 호스트 이름에 대한 SQL 데이터베이스 구성](#)을 참조하십시오.
- IaaS 구성 요소를 복원하는 경우 호스트의 이름을 변경하면 IaaS 웹 호스트, Manager Service 호스트 또는 해당하는 각 로드 밸런서에 영향을 미칠 수 있습니다. "vRealize Suite" 백업 및 복원 지침에 따라 이러한 호스트 또는 로드 밸런서를 복원합니다.

vRealize Automation 장치 호스트 이름 또는 IP 주소를 변경하려면 다음 섹션을 참조하십시오.

vRealize Automation 장치 호스트 이름 변경

환경 또는 네트워크를 유지 관리하는 경우 vRealize Automation 장치에 다른 호스트 이름을 할당해야 할 수도 있습니다.

중요 이름을 변경하면 vRealize Automation이 몇 분 동안 오프라인으로 전환됩니다.

독립형, 마스터 및 복제 vRealize Automation 장치에 동일한 단계가 적용됩니다.

절차

- 1 DNS에서 새로운 노드 호스트 이름을 사용하여 추가 레코드를 생성합니다.

이전 호스트 이름을 사용하는 기존 DNS 레코드를 아직 제거하지 마십시오.

- 2 DNS 복제 및 영역 배포가 수행될 때까지 기다립니다.

- 3 vRealize Automation 장치 명령줄에 루트로 로그인합니다.

- 4 다음 명령을 실행합니다.

```
vcac-config hostname-change --host new-hostname --certificate certificate-file-name
```

이전 장치 호스트 이름이 인증서에 사용되었던 경우가 아니면 인증서 파일은 선택 사항입니다. 이전 장치 호스트 이름이 사용된 경우 새로운 호스트 이름이 있는 업데이트된 인증서를 제공합니다.

인증서 파일을 지정하면 이름 변경 명령이 인증서를 가져오고 인증서 ID도 반환합니다.

인증서 파일은 `/config/ssl/generate-certificate` API 명령의 텍스트 출력과 동일한 형식이어야 하며 SAN 필드에 새로운 DNS 이름을 포함해야 합니다.

- 5 이름 변경 프로세스가 완료될 때까지 최대 15분 이상 기다립니다. 명령 작업에 몇 분이 소요되며 이후 서비스 재등록에 추가로 몇 분이 소요됩니다.
- 6 이전 장치 호스트 이름이 HA 환경의 로드 밸런서에 사용된 경우 해당 로드 밸런서를 선택하고 새 이름으로 재구성합니다.
- 7 DNS에서 이전 호스트 이름을 사용하는 기존 DNS 레코드를 제거합니다.

결과

호스트 이름을 변경하는 데 문제가 있는 경우 대신 vRealize Automation 7.3 설명서의 개별 절차를 시도합니다.

vRealize Automation 장치 IP 주소 변경

환경 또는 네트워크를 유지 관리하는 경우 기존 vRealize Automation 장치에 다른 IP 주소를 할당해야 할 수도 있습니다.

사전 요구 사항

- 하나의 예방 조치로 vRealize Automation 장치 및 IaaS 서버의 스냅샷을 생성합니다.
- vRealize Automation 장치에 대한 루트로 콘솔 세션에서 `/etc/hosts` 파일의 항목을 검사합니다.

새 IP 주소 계획과 충돌할 수 있는 주소 할당을 찾고 필요에 따라 변경합니다.

모든 IaaS 서버에서 Windows\system32\drivers\etc\hosts 파일에 대한 프로세스를 반복합니다.

- 모든 vRealize Automation 장치를 종료합니다.
- IaaS 서버에서 모든 vRealize Automation 서비스를 중지합니다.

절차

- 1 변경할 vRealize Automation 장치를 vSphere에서 찾은 후 **작업 > 설정 편집**을 선택합니다.
- 2 **vApp 옵션**을 클릭합니다.
- 3 **IP 할당**을 확장하고 **OVF 환경** 옵션을 사용하도록 설정합니다.
- 4 **OVF 설정**을 확장하고 **ISO 이미지** 옵션을 사용하도록 설정합니다.

Virtual Hardware	VM Options	SDRS Rules	vApp Options
<div> <div>IP allocation</div> <div> <div>IP allocation scheme</div> <div> A vApp can obtain its network configuration through the OVF environment or a DHCP server. Specify the network configuration schemes supported by this vApp: <div> <input type="checkbox"/> DHCP <input checked="" type="checkbox"/> OVF environment </div> <div> The IP allocation schemes determine what IP allocation policy options are enabled. </div> </div> </div> </div>			
<div> <div>IP protocol</div> <div> Specify the IP protocols supported by this vApp: <div>Both</div> </div> </div>			
<div> <div>OVF settings</div> <div> <div>OVF environment</div> <div>View...</div> <div> The OVF environment is only available when the VM is powered on. </div> </div> </div>			
<div> <div>OVF environment transport</div> <div> <input checked="" type="checkbox"/> ISO image <div> An ISO image, containing the OVF environment document, is mounted on the first available CD-ROM drive. </div> </div> </div>			
<div> <div>VMware Tools</div> <div> <input checked="" type="checkbox"/> VMware Tools <div> The VMware tools guestInfo.ovfEnv variable is initialized with the OVF environment document. </div> </div> </div>			
<div> <div>Installation boot</div> <div> <input type="checkbox"/> Enable <div> The installation boot automatically gets reset upon first power-on of the virtual machine. </div> </div> </div>			
<div> <div>0</div> <div> Specify the delay in seconds to wait for the VM to power off. A value of zero means wait until the VM is powered off </div> </div>			

- 5 **확인**을 클릭합니다.
- 6 변경하려는 vRealize Automation 장치를 시작합니다.
- 7 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.
<https://vrealize-automation-appliance-FQDN:5480>
- 8 **네트워크** 탭을 클릭합니다.
- 9 탭 아래에서 **주소**를 클릭합니다.
- 10 IP 주소를 업데이트합니다.

- 11 오른쪽 위에서 **설정 저장**을 클릭합니다.
- 12 변경하려는 vRealize Automation 장치를 종료합니다.
- 13 DNS에서 새 IP 주소에 대한 항목을 업데이트합니다.

기존 A 유형 레코드만 업데이트합니다. FQDN을 변경하지 마십시오.

로드 밸런서를 사용하는 경우 필요에 따라 백엔드 노드, 서비스 풀 및 가상 서버에 대한 로드 밸런서 IP 설정도 업데이트합니다.

- 14 DNS 복제 및 영역 배포가 수행될 때까지 기다립니다.
- 15 모든 vRealize Automation 장치를 시작합니다.
- 16 IaaS 서버에서 vRealize Automation 서비스를 시작합니다.
- 17 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 18 다음 영역에서 vRealize Automation 장치의 상태를 확인합니다.

- **클러스터** 아래의 데이터베이스 연결 상태
- **vRA > 메시징** 아래의 RabbitMQ 상태
- **vRA > Xenon** 아래의 Xenon 상태
- **서비스**에 모든 서비스가 [등록됨] 상태로 표시됨

변경된 호스트 이름에 맞게 SQL 데이터베이스 조정

vRealize Automation IaaS SQL 데이터베이스를 다른 호스트 이름으로 이동하면 구성 설정을 수정해야 합니다.

호스트 이름이 동일한 경우에는 추가적인 단계 없이 백업에서 SQL 데이터베이스를 복원할 수 있습니다. 다른 호스트 이름에 복원하는 경우에는 구성 파일을 편집하여 추가적인 변경 사항을 적용해야 합니다.

SQL 데이터베이스를 다른 호스트 이름으로 이동할 때 필요한 변경 사항에 대해서는 [VMware 기술 자료 문서 2074607](#) 항목을 참조하십시오.

IaaS 서버 IP 주소 변경

환경 또는 네트워크를 유지 관리하는 경우 기존 vRealize Automation IaaS Windows Server에 다른 IP 주소를 할당해야 할 수도 있습니다.

사전 요구 사항

- vRealize Automation 장치 IP 주소를 변경해야 하는 경우 이 작업을 먼저 수행합니다. [vRealize Automation 장치 IP 주소 변경](#) 항목을 참조하십시오.
- 하나의 예방 조치로 vRealize Automation 장치 및 IaaS 서버의 스냅샷을 생성합니다.
- vRealize Automation 장치에 대한 루트로 콘솔 세션에서 `/etc/hosts` 파일의 항목을 검사합니다.
새 IP 주소 계획과 충돌할 수 있는 주소 할당을 찾고 필요에 따라 변경합니다.

모든 IaaS 서버에서 `Windows\system32\drivers\etc\hosts` 파일에 대한 프로세스를 반복합니다.

- vRealize Automation 장치를 종료합니다.
- IaaS 서버에서 모든 vRealize Automation 서비스를 중지합니다.

절차

- 1 관리자 권한이 있는 계정을 사용하여 IaaS 서버에 로그인합니다.

- 2 Windows에서 IP 주소를 변경합니다.

인터넷 프로토콜 속성 아래에서 Windows 네트워크 어댑터 설정의 IP 주소를 찾습니다.

- 3 변경 내용으로 로컬 DNS를 새로 고칩니다.

DNS를 새로 고치면 IaaS Windows Server가 서로를 찾을 수 있고 연결이 끊긴 경우 Windows Server에 다시 연결할 수 있습니다.

- 4 Manager Service 호스트에서 텍스트 편집기의 다음 파일을 검사합니다.

`install-folder\VCAC\Server\ManagerService.exe.config`

기본 설치 폴더는 `C:\Program Files (x86)\VMware`입니다.

vRealize Automation 장치 및 IaaS Windows Server의 IP 주소 또는 FQDN을 확인합니다.

- 5 모든 IaaS Windows Server에서 텍스트 편집기의 다음 파일을 검사합니다.

`install-folder\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`

vRealize Automation 장치의 IP 주소 또는 FQDN을 확인합니다.

- 6 SQL Server 호스트에 로그인합니다.

- 7 저장소 주소가 `ConnectionString` 열의 FQDN을 사용하도록 올바르게 구성되어 있는지 확인합니다.

예를 들어 SQL Management Studio를 열고 다음 쿼리를 실행합니다.

```
"SELECT Name, ConnectionString FROM [database-name].[DynamicOps.RepositoryModel].[Models]"
```

- 8 vRealize Automation 장치를 시작합니다.

- 9 IaaS 서버에서 vRealize Automation 서비스를 시작합니다.

- 10 로그 파일을 검사하여 에이전트, DEM 작업자, Manager Service 및 웹 호스트 서비스가 성공적으로 시작되었는지 확인합니다.

- 11 인프라 관리자 역할이 있는 사용자로 vRealize Automation에 로그인합니다.

- 12 **인프라 > 모니터링 > Distributed Execution** 상태로 이동하고 모든 서비스가 실행 중인지 확인합니다.

- 13 장치 서비스를 점검하고, 프로비저닝을 테스트하거나, vRealize 운영 테스트 도구를 사용하여 작업이 올바른지 테스트합니다.

IaaS 서버 호스트 이름 변경

환경 또는 네트워크를 유지 관리하는 경우 기존 vRealize Automation IaaS Windows 서버에 다른 호스트 이름을 할당해야 할 수 있습니다.

절차

- 1 IaaS 서버의 스냅샷을 생성합니다.
- 2 IaaS 서버에서 IIS 관리자를 사용하여 vRealize Automation 애플리케이션 폴인 저장소, VMware vRealize Automation 및 Wapi를 중지합니다.
- 3 IaaS 서버에서 [관리 도구] > [서비스]를 사용하여 모든 vRealize Automation 서비스, 에이전트 및 DEM을 중지합니다.
- 4 DNS에서 새 호스트 이름을 사용하여 추가 레코드를 생성합니다.
이전 호스트 이름을 사용하는 기존 DNS 레코드를 아직 제거하지 마십시오.
- 5 DNS 복제 및 영역 배포가 수행될 때까지 기다립니다.
- 6 IaaS 서버에서 호스트 이름을 변경하되, 메시지가 표시되어도 다시 시작하지 않습니다.
Windows 시스템 속성의 컴퓨터 이름, 도메인 및 작업 그룹 설정 아래에서 호스트 이름을 찾습니다.
다시 시작하라는 메시지가 표시되면 나중에 다시 시작하는 옵션을 클릭합니다.
- 7 이전 호스트 이름을 사용하여 인증서를 생성한 경우, 인증서를 업데이트합니다.
자세한 내용은 [vRealize Automation 인증서 업데이트](#)를 참조하십시오.
- 8 텍스트 편집기를 사용하여 구성 파일 내에서 호스트 이름을 찾아 업데이트합니다.
변경한 IaaS 서버 호스트 이름에 따라 업데이트를 적용합니다. 분산 HA 배포의 경우 두 개 이상의 서버에 액세스해야 할 수 있습니다. DEM Orchestrator 또는 DEM 작업자의 호스트 이름을 변경한 경우에는 업데이트가 필요하지 않습니다.

참고 이전 Windows 서버 버호스트 이름만 업데이트합니다. 로드 밸런서 이름을 대신 찾을 경우에는 로드 밸런서 이름을 그대로 둡니다.

표 1-38. 웹 노드 호스트 이름을 변경할 때 업데이트할 파일

IaaS 서버	경로	파일
웹 노드	install-folder\Server\Website	Web.config
	install-folder\Server\Website\Cafe	Vcac-Config.exe.config
	install-folder\Web API	Web.config
	install-folder\Web API\ConfigTool	Vcac-Config.exe.config
Model Manager 구성 요소가 설치되어 있는 노드	install-folder\Server\Model Manager Data	Repoutil.exe.config

표 1-38. 웹 노드 호스트 이름을 변경할 때 업데이트할 파일 (계속)

laaS 서버	경로	파일
	<i>install-folder\Server\Model Manager Data\Cafe</i>	Vcac-Config.exe.config
Manager Service 노드	<i>install-folder\Server</i>	ManagerService.exe.config
DEM Orchestrator 노드	<i>install-folder\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
DEM 작업자 노드	<i>install-folder\Distributed Execution Manager\DEM-name</i>	DynamicOps.DEM.exe.config
에이전트 노드	<i>install-folder\Agents\agent-name</i>	RepoUtil.exe.config
	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

표 1-39. Manager Service 노드 호스트 이름을 변경할 때 업데이트할 파일

laaS 서버	경로	파일
DEM Orchestrator 노드	<i>install-folder\Distributed Execution Manager\DEM-name</i>	DynamicOps.DEM.exe.config
DEM 작업자 노드	<i>install-folder\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
에이전트 노드	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

표 1-40. 에이전트 노드 호스트 이름을 변경할 때 업데이트할 파일

laaS 서버	경로	파일
에이전트 노드	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

- 9 호스트 이름을 변경한 laaS 서버를 다시 시작합니다.
- 10 앞 단계에서 중지한 vRealize Automation 애플리케이션 풀을 시작합니다.
- 11 앞 단계에서 중지한 vRealize Automation 서비스, 에이전트 및 DEM을 시작합니다.
- 12 이전 laaS 서버 호스트 이름이 HA 환경의 로드 밸런서에 사용된 경우 해당 로드 밸런서를 선택하고 새 이름으로 재구성합니다.
- 13 DNS에서 이전 호스트 이름을 사용하는 기존 DNS 레코드를 제거합니다.
- 14 DNS 복제 및 영역 배포가 수행될 때까지 기다립니다.
- 15 Manager Service 호스트의 호스트 이름을 변경한 경우 다음과 같은 추가 단계를 수행합니다.
 - a 기존 가상 시스템의 소프트웨어 에이전트를 업데이트합니다.
 - b 게스트 에이전트가 포함된 ISO 또는 템플릿을 재생성합니다.

다음에 수행할 작업

vRealize Automation이 사용할 준비가 되었는지 확인합니다. [vRealize Suite 백업 및 복원](#) 설명서를 참조하십시오.

vRealize Automation 로그인 URL을 사용자 지정 이름으로 설정

vRealize Automation 사용자가 vRealize Automation 장치 또는 로드 밸런서 이름이 아닌 URL 이름에 로그인하도록 하려면 설치 전후에 사용자 지정 조치를 취합니다.

절차

- 1 설치하기 전에 원하는 CNAME과 vRealize Automation 장치 및 로드 밸런서 이름이 포함된 인증서를 준비합니다.
- 2 vRealize Automation을 설치하고 평소대로 장치 또는 로드 밸런서 이름을 입력합니다. 설치하는 동안 사용자 지정 인증서를 가져옵니다.
- 3 설치 후 DNS에서 일반 이름의 CNAME 별칭을 생성하고 장치 또는 로드 밸런서 VIP 주소를 가리키도록 구성합니다.
- 4 vRealize Automation 장치 관리자 인터페이스에 root로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 5 **vRA > 호스트 설정** 아래에서, **호스트 이름**을 선택한 CNAME으로 변경합니다.

vRealize Automation 장치 노드 제거

HA 환경을 유지 보수하는 경우, 실패한 vRealize Automation 장치 노드를 클러스터에서 제거해야 할 수도 있습니다.

노드를 제거하려면 [VMware 기술 자료 문서 2149866](#)의 지침을 따르십시오.

IaaS 서버에 vRealize Log Insight Agent 설치

vRealize Automation IaaS 구성의 Windows 서버에는 기본적으로 vRealize Log Insight Agent가 포함되어 있지 않습니다.

vRealize Log Insight는 로그 집계 및 인덱싱을 제공하며 로그를 수집하고, 가져오고, 분석하여 시스템 문제를 드러낼 수 있습니다. vRealize Log Insight를 사용하여 IaaS 서버의 로그를 캡처 및 분석하려는 경우 Windows용 vRealize Log Insight Agent를 별도로 설치해야 합니다.

자세한 내용은 [VMware vRealize Log Insight 설명서](#)를 참조하십시오.

vRealize Automation 장치에는 기본적으로 vRealize Log Insight Agent가 포함되어 있습니다.

VMware Remote Console 프록시 포트 변경

사이트가 포트 8444를 차단하거나 예약한 경우 VMware Remote Console에서 사용하는 기본 프록시 포트를 변경할 수 있습니다.

절차

- 1 루트로 vRealize Automation 장치 명령 프롬프트에 액세스합니다.
- 2 텍스트 편집기에서 다음 파일을 엽니다.
`/etc/vcac/security.properties`
- 3 `consoleproxy.service.port`를 기본값인 **8444**에서 사용하지 않는 포트로 변경합니다.
- 4 `security.properties`를 저장하고 닫습니다.
- 5 vRealize Automation 장치를 다시 시작합니다.

결과

HA 환경에서 모든 vRealize Automation 장치를 동일하게 변경합니다.

vRealize Automation 장치 FQDN을 원래 FQDN으로 변경

경우에 따라서는 vRealize Automation 장치 FQDN이 원하지 않는데도 변경될 수 있습니다. 예를 들어 장치가 있는 도메인이 아닌 다른 도메인에 대해 IWA(통합 Windows 인증) 디렉토리를 생성하면 FQDN이 변경됩니다.

다른 도메인에 대해 IWA 디렉토리를 생성한 경우에는 다음 단계에 따라 장치 FQDN을 원래 FQDN으로 다시 변경해야 합니다.

절차

- 1 vRealize Automation에 로그인하여 일반적인 방법으로 IWA 디렉토리를 생성합니다.
[LDAP/IWA를 통한 Active Directory 링크 구성](#)을 참조하십시오.
- 2 HA 환경인 경우에는 [고가용성을 위한 디렉토리 관리 구성](#)에 나와 있는 단계도 따라야 합니다.
- 3 장치가 있는 도메인이 아닌 다른 도메인에 대해 IWA 디렉토리를 생성하면 장치 FQDN이 자동으로 변경됩니다.

예를 들어 `domain2.local`의 IWA 디렉토리를 생성하면 `va1.domain1.local`이 `va1.domain2.local`로 변경됩니다.

각 장치의 이름을 원래 FQDN으로 바꿔서 이 변경을 실행 취소합니다. [호스트 이름 및 IP 주소 변경](#)에 나와 있는 관련 절차를 참조하십시오.

- 4 원래 FQDN을 사용하여 장치가 다시 온라인 상태가 되면 각 IaaS 노드에 로그인한 후 다음 단계를 수행합니다.
 - a 텍스트 편집기에서 다음 파일을 엽니다.
`C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`
 - b 각 장치 `endpoint address`=FQDN을 원래 FQDN으로 변경합니다.

예:

```
<endpoint address="https://va1.domain2.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain2.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

위의 FQDN을 다음과 같이 변경합니다.

```
<endpoint address="https://va1.domain1.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain1.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

C VMware.IaaS.Management.Agent.exe.Config를 저장하고 닫습니다.

5 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

6 **vRA > 메시징**으로 이동하여 **RabbitMQ 클러스터 재설정**을 클릭합니다.

7 재설정이 완료되면 각 장치 관리 인터페이스에 로그인합니다.

8 **클러스터**로 이동하여 모든 노드가 클러스터에 연결되었는지 확인합니다.

SQL AlwaysOn 가용성 그룹 구성

vRealize Automation 설치 후 SQL AAG(AlwaysOn 가용성 그룹)를 설정할 경우에는 구성을 변경해야 합니다.

설치 후 SQL AAG를 설정하는 경우에는 [VMware 기술 자료 문서 2074607](#)에 나와 있는 단계에 따라 AAG 수신기 FQDN을 SQL Server 호스트로 사용하여 vRealize Automation을 구성합니다.

vRealize Automation 설치 후 네트워크 인터페이스 컨트롤러 추가

vRealize Automation은 여러 NIC(네트워크 인터페이스 컨트롤러)를 지원합니다. 설치 후 vRealize Automation 장치나 IaaS Windows Server에 NIC를 추가할 수 있습니다.

예를 들어 다음과 같은 경우 일부 vRealize Automation 배포에는 여러 NIC가 필요할 수 있습니다.

- 사용자와 인프라 네트워크를 구분하고자 합니다.
- IaaS 서버가 Active Directory 도메인에 가입할 수 있도록 추가 NIC가 필요합니다.

여러 NIC 시나리오에 대한 자세한 내용은 이 [VMware 클라우드 관리 블로그 게시물](#)을 참조하십시오.

NIC가 3개 이상인 경우 다음 제한 사항을 알아 두어야 합니다.

- VIDM이 Postgres 데이터베이스 및 Active Directory에 액세스할 수 있어야 합니다.
- HA 클러스터에서는 VIDM이 로드 밸런서 URL에 액세스할 수 있어야 합니다.
- 앞의 VIDM 연결은 처음 두 개의 NIC를 통해 이루어져야 합니다.
- 두 번째 NIC 이후의 NIC는 VIDM에서 사용되거나 인식되지 않아야 합니다.

- 두 번째 NIC 이후의 NIC는 Active Directory에 연결하는 데 사용되지 않아야 합니다.

vRealize Automation에서 디렉토리를 구성할 때는 첫 번째 또는 두 번째 NIC를 사용합니다.

사전 요구 사항

vRealize Automation을 vCenter 환경에 완전히 설치합니다.

절차

- 1 vCenter에서 각 vRealize Automation 장치에 NIC를 추가합니다.
 - a 장치를 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
 - b VMXNETn NIC를 추가합니다.
 - c 전원이 켜져 있으면 장치를 다시 시작합니다.
- 2 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
<https://vrealize-automation-appliance-FQDN:5480>
- 3 **네트워크**를 선택하고 여러 NIC를 사용할 수 있는지 확인합니다.
- 4 **주소**를 선택하고 NIC의 IP 주소를 구성합니다.

표 1-41. NIC 구성의 예

설정	값
IPv4 주소 유형	정적
IPv4 주소	172.22.0.2
넷마스크	255.255.255.0

- 5 모든 vRealize Automation 노드가 DNS 이름으로 서로를 확인할 수 있는지 확인합니다.
- 6 모든 vRealize Automation 노드가 vRealize Automation 구성 요소에 대해 로드 밸런싱된 FQDN에 액세스할 수 있는지 확인합니다.
- 7 분할 브레인 DNS를 사용하는 경우 모든 vRealize Automation 노드 및 VIP가 각 노드 IP 및 VIP에 대해 DNS에서 동일한 FQDN을 갖는지 확인합니다.
- 8 vCenter에서 IaaS Windows Server에 NIC를 추가합니다.
 - a IaaS 서버를 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
 - b NIC를 IaaS 서버 가상 시스템에 추가합니다.
- 9 Windows에서 추가된 IaaS 서버 NIC와 해당 IP 주소를 구성합니다. 필요하다면 Microsoft 설명서를 참조하십시오.

다음에 수행할 작업

(선택 사항) 정적 경로가 필요한 경우 [정적 경로 구성](#) 항목을 참조합니다.

정적 경로 구성

vRealize Automation 설치에 NIC를 추가할 때 정적 경로가 필요하면 명령 프롬프트 세션을 열어서 구성합니다.

사전 요구 사항

vRealize Automation 장치나 IaaS Windows Server에 여러 NIC를 추가합니다.

절차

- 1 vRealize Automation 장치 명령줄에 root로 로그인합니다.
- 2 텍스트 편집기에서 경로 파일을 엽니다.
`/etc/sysconfig/network/routes`
- 3 기본 게이트웨이에 대한 `default` 줄을 찾고 수정하지는 않습니다.

참고 기본 게이트웨이를 변경해야 하는 경우에는 vRealize Automation 관리 인터페이스를 대신 사용합니다.

- 4 `default` 줄 아래에 정적 경로에 대한 새 줄을 추가합니다. 예:

```
default 10.10.10.1 - -
172.30.30.0 192.168.100.1 255.255.255.0 eth0
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 경로 파일을 저장하고 닫습니다.
- 6 장치를 다시 시작합니다.
- 7 HA 클러스터에서 각 장치에 대해 이 과정을 반복합니다.
- 8 관리자로 IaaS Windows Server에 로그인합니다.
- 9 관리자 권한으로 명령 프롬프트를 엽니다.
- 10 정적 경로를 구성하려면 `route -p add` 명령을 입력합니다. 여기서 `-p`는 다시 시작한 후에도 정적 경로를 유지합니다. 예:

```
C:\Windows\system32> route -p add 172.30.30.0 mask 255.255.255.0 192.168.100.1 metric 1
OK!
```

Windows에서 정적 경로 구성에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

패치 관리 액세스

vRealize Automation 설치에 대한 기술 지원에는 vRealize Automation 장치 관리 인터페이스를 사용해 설치하거나 제거하는 소프트웨어 패치가 포함될 수 있습니다.

문제는 거의 실시간으로 발생할 수 있기 때문에 패치, 사전 요구 사항 및 설치 지침은 [VMware 기술 자료](#)에 릴리스됩니다. 예를 들어 [VMware 기술 자료 문서 60310](#)은 최신 vRealize Automation 7.5 패치 정보로 모니터링되고 업데이트됩니다.

다음 vRealize Automation 구성 요소는 패치 인터페이스가 패치할 수 없습니다.

- 관리 에이전트
- vSphere 에이전트 이외의 에이전트(예: XenServer, VDI 또는 Hyper-V)

절차

- 1 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 **vRA > 패치**를 클릭합니다.
- 3 [패치 관리] 아래에서 필요한 옵션을 클릭하고 표시되는 메시지를 따릅니다.

옵션	설명
새 패치	다운로드한 새 패치를 설치합니다.
설치된 패치	가장 최근에 설치된 패치를 새로 추가된 클러스터 노드에 추가합니다.
롤백	가장 최근에 설치된 패치를 제거하고 vRealize Automation을 이전 패치 수준으로 롤백합니다.
기록	설치 및 제거된 패치의 목록을 검사합니다.

패치 관리를 사용하거나 사용하지 않도록 설정하려면 vRealize Automation 장치 명령 프롬프트에 root로 로그인하고 다음 명령 중 하나를 입력합니다.

```
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh enable
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh disable
```

기본 테넌트에 대한 액세스 구성

팀에서 vRealize Automation 구성 작업을 시작할 수 있으려면 먼저 기본 테넌트에 대한 액세스 권한을 팀에게 부여해야 합니다.

설치 마법사에서 Single Sign-On을 구성할 때 기본 테넌트가 자동으로 생성됩니다. 이름 또는 URL 토큰 같은 테넌트 세부 정보를 편집할 수 없지만 언제든지 로컬 사용자를 새로 생성하고 추가적인 테넌트 관리자 또는 IaaS 관리자를 지정할 수 있습니다.

절차

- 1 기본 테넌트의 관리자로 vRealize Automation에 로그인합니다.
 - a vRealize Automation 제품 인터페이스로 이동합니다.
`https://vrealize-automation-FQDN/vcac`
 - b 사용자 이름 **administrator** 및 SSO를 구성할 때 이 사용자에게 대해 정의한 암호로 로그인합니다.
- 2 **관리 > 테넌트**를 선택합니다.
- 3 기본 테넌트의 이름인 **vsphere.local**을 클릭합니다.

4 로컬 사용자 탭을 클릭합니다.**5 vRealize Automation 기본 테넌트의 로컬 사용자 계정을 생성합니다.**

로컬 사용자는 테넌트에서만 사용되며, 자신이 소속된 테넌트에만 액세스할 수 있습니다.

- a 추가(+) 아이콘을 클릭합니다.
- b 인프라 관리를 담당하는 사용자에 대한 세부 정보를 입력합니다.
- c **추가**를 클릭합니다.
- d 이 단계를 반복하여 기본 테넌트의 구성을 담당하는 사용자를 한 명 이상 더 추가합니다.

6 관리자 탭을 클릭합니다.**7** 로컬 사용자를 테넌트 관리자 및 IaaS 관리자 역할에 할당합니다.

- a **테넌트 관리자** 검색 상자에 사용자 이름을 입력하고 Enter 키를 누릅니다.
- b **IaaS 관리자** 검색 상자에 사용자 이름을 입력하고 Enter 키를 누릅니다.

IaaS 관리자는 vRealize Automation에서 인프라 끝점을 생성하고 관리하는 일을 담당합니다. 이 역할은 시스템 관리자만 부여할 수 있습니다.

8 업데이트를 클릭합니다.

다음에 수행할 작업

팀이 vRealize Automation 구성을 시작할 수 있도록 이렇게 생성한 사용자 계정에 대한 액세스 URL 및 로그인 정보를 제공합니다.

- 테넌트 관리자는 고가용성을 위한 디렉토리 관리 구성을 포함하여 사용자 인증과 같은 설정을 구성합니다. [테넌트 설정 구성](#)을 참조하십시오.
- IaaS 관리자는 프로비저닝을 위한 외부 리소스를 준비합니다. [프로비저닝을 위한 외부적 준비](#)를 참조하십시오.
- 설치하는 동안 초기 콘텐츠 생성을 구성한 경우 구성 관리자가 개념 증명을 빠르게 채우기 위해 초기 콘텐츠 카탈로그 항목을 요청할 수 있습니다.

vRealize Automation 설치 문제 해결

vRealize Automation 문제 해결은 vRealize Automation을 설치 또는 구성할 때 발생할 수 있는 문제를 해결하는 절차를 제공합니다.

기본 로그 위치

설치 실패에 대한 자세한 정보는 시스템 및 제품 로그 파일을 참조하십시오.

참고 로그 수집을 위해 vRealize Log Insight용 vRealize Automation 및 vRealize Orchestrator 콘텐츠 팩의 장점을 활용하는 것이 좋습니다. 콘텐츠 팩 및 Log Insight는 vRealize Suite의 구성 요소에 대한 통합된 로그 이벤트 요약を提供합니다. 자세한 내용은 [VMware Solution Exchange](#)에서 확인하십시오.

최신 로그 위치 목록은 [VMware 기술 자료 문서 2141175](#) 항목을 참조하십시오.

Windows 로그

Windows 이벤트에 대한 로그 파일은 다음에서 찾을 수 있습니다.

로그	위치
Windows 이벤트 뷰어 로그	시작 > 제어판 > 관리 도구 > 이벤트 뷰어

설치 로그

설치 로그는 다음 위치에 있습니다.

로그	기본 위치
설치 로그	C:\Program Files (x86)\vCAC\InstallLogs C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\Log
WAPI 설치 로그	C:\Program Files (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX>

IaaS 로그

IaaS 로그는 다음 위치에 있습니다.

로그	기본 위치
웹 사이트 로그	C:\Program Files (x86)\VMware\vCAC\Server\Website\Logs
저장소 로그	C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Logs
Manager 서비스 로그	C:\Program Files (x86)\VMware\vCAC\Server\Logs
DEM 조정자 로그	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager \<system-name> DEO \Logs
에이전트 로그	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Agents\<agent-name>\logs

vRealize Automation 프레임워크 로그

vRealize Automation 프레임워크의 로그 항목은 다음 위치에 있습니다.

로그	기본 위치
프레임워크 로그	/var/log/vmware

소프트웨어 구성 요소 프로비저닝 로그

소프트웨어 구성 요소 프로비저닝 로그는 다음 위치에 있습니다.

로그	기본 위치
소프트웨어 에이전트 부트스트랩 로그	/opt/vmware-appdirector(Linux의 경우) 또는 \opt\vmware-appdirector(Windows의 경우)
소프트웨어 수명 주기 스크립트 로그	/tmp/taskId(Linux의 경우) \Users\darwin\AppData\Local\Temp\taskId (Windows의 경우)

분산 배포의 로그 모음

분산 배포의 구성 요소에 대한 모든 로그를 묶는 zip 파일을 생성할 수 있습니다..

실패한 설치 롤백

설치가 실패하여 롤백이 수행되면 시스템 관리자는 다른 설치를 시작하기 전에 먼저 모든 필수 파일이 제거되었는지 확인해야 합니다. 일부 파일은 수동으로 제거해야 합니다.

최소 설치 롤백

실패한 vRealize Automation IaaS 설치를 완전하게 제거하려면 시스템 관리자가 수동 방식으로 일부 파일을 제거하고 데이터베이스를 되돌려야 합니다.

절차

1 다음과 같은 구성 요소가 아직 있으면 Windows 제거 프로그램을 사용하여 제거합니다.

- vRealize Automation 에이전트
- vRealize Automation DEM-Worker
- vRealize Automation DEM-Orchestrator
- vRealize Automation Server
- vRealize Automation WAPI

참고 다음과 같은 메시지가 표시되면 시스템을 다시 시작한 다음 이 절차의 단계를 따르십시오. 설치 로그 파일을 여는 동안 오류가 발생했습니다. 지정한 로그 파일 위치가 있는지 그리고 이 로그 파일에 쓸 수 있는지 확인하십시오.

참고 Windows 시스템 파일을 되돌리거나, IaaS를 제거한 경우에는 vRealize Automation IaaS를 재설치하기 전에 **iisreset** 명령을 실행해야 합니다.

- 2** 설치를 시작하기 전의 상태로 데이터베이스를 되돌립니다. 원래 데이터베이스 설치 모드에 따라 사용하는 방법이 달라집니다.
- 3** IIS(인터넷 정보 서비스) 관리자에서 [기본 웹 사이트](또는 사용자 지정 사이트)를 선택하고 **바인딩**을 클릭합니다. **https** 바인딩(기본값: 443)을 제거합니다.
- 4** 애플리케이션 저장소, vRealize Automation 및 WAPI가 삭제되었고 애플리케이션 풀 RepositoryAppPool, vCACAppPool 및 WapiAppPool도 삭제되었는지 확인합니다.

결과

설치가 완전하게 제거되었습니다.

분산 설치 롤백

실패한 IaaS 설치를 완전하게 제거하려면 시스템 관리자가 수동 방식으로 일부 파일을 제거하고 데이터베이스를 되돌려야 합니다.

절차

1 다음과 같은 구성 요소가 아직 있으면 Windows 제거 프로그램을 사용하여 제거합니다.

- vRealize Automation Server
- vRealize Automation WAPI

참고 다음과 같은 메시지가 표시되면 시스템을 다시 시작한 다음 이 절차를 따르십시오. 설치 로그 파일을 여는 동안 오류가 발생했습니다. 지정한 로그 파일 위치가 있는지 그리고 이 로그 파일에 쓸 수 있는지 확인하십시오.

참고 Windows 시스템 파일을 되돌리거나, IaaS를 제거한 경우에는 vRealize Automation IaaS를 재설치하기 전에 `iisreset` 명령을 실행해야 합니다.

- 2 설치를 시작하기 전의 상태로 데이터베이스를 되돌립니다. 원래 데이터베이스 설치 모드에 따라 사용하는 방법이 달라집니다.
- 3 IIS(인터넷 정보 서비스) 관리자에서 [기본 웹 사이트](또는 사용자 지정 사이트)를 선택하고 **바인딩**을 클릭합니다. `https` 바인딩(기본값: 443)을 제거합니다.
- 4 애플리케이션 저장소, vCAC 및 WAPI가 삭제되었고 애플리케이션 풀 RepositoryAppPool, vCACAppPool 및 WapiAppPool도 삭제되었는지 확인합니다.

결과

표 1-42. 실패 지점 롤백

실패 지점	작업
Manager Service 설치	vCloud Automation Center 서버가 있는 경우, vCloud Automation Center 서버를 제거합니다.
DEM-Orchestrator 설치	있는 경우, DEM 조정자를 제거합니다.
DEM-Worker 설치	있는 경우, 모든 DEM 작업자를 제거합니다.
에이전트 설치	있는 경우, 모든 vRealize Automation 에이전트를 제거합니다.

vRealize Automation 지원 번들 생성

vRealize Automation 장치 관리 인터페이스를 사용하여 vRealize Automation 지원 번들을 생성할 수 있습니다. 지원 번들은 로그를 수집하고, 사용자 또는 VMware 기술 지원에서 vRealize Automation 문제를 해결하는 데 도움을 줍니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 **vRA > 로그**를 클릭합니다.
- 3 **지원 번들 생성**을 클릭합니다.
- 4 **다운로드**를 클릭하고 지원 번들 파일을 시스템에 저장합니다.

결과

지원 번들에는 vRealize Automation 장치 및 IaaS Windows Server의 정보가 포함됩니다. vRealize Automation 장치와 IaaS 구성 요소 간 연결이 끊어지면 지원 번들에 IaaS 구성 요소 로그가 누락될 수 있습니다.

어떤 로그 파일이 수집되었는지 확인하려면 지원 번들의 압축을 풀고 웹 브라우저에서 **Environment.html** 파일을 엽니다. 연결이 없는 경우 IaaS 구성 요소가 노드 테이블에서 빨간색으로 나타날 수 있습니다. 빨간색으로 나타나는 IaaS Windows Server에서 vRealize Automation 관리 에이전트 서비스가 중지된 경우에도 IaaS 로그가 누락될 수 있습니다.

명령줄 - vRealize Automation 장치 명령줄에서 루트로 지원 번들을 생성하려는 경우 `vcac-support` 또는 `vcac-config log-bundle`을 실행할 수 있습니다.

또는 다음 예에서와 같이 전체 `log-bundle` 명령을 실행할 수 있습니다. `vra-command` 실행에 대한 일반 정보는 [vRealize Automation 설치 명령줄 기본 사항](#) 항목을 참조하십시오.

```
# vra-command execute --node cafe.node.497772175.21500 log-bundle --requestor va-1.mycompany.com

Parent command with id='981e3028-c99b-5c92-1bae-7d2bf5b6aaaa' was created.
Waiting for all child commands to complete...
...
Command execution result:
Command id: 3d64d122-0af1-28dd-b5a5-d932b78b3678
  Type: log-bundle
  Node id: cafe.node.497772175.21500
  Node host: va-1.mycompany.com
  Result: The command was successfully executed.
  Result description: {"path": "/opt/vmware/var/support-bundle/log/
va-1.mycompany.com_cafe.node.497772175.21500-VA.zip"}

Status: COMPLETED
```

일반 설치 문제 해결

vRealize Automation 장치의 문제 해결 항목은 vRealize Automation을 사용할 때 발생할 수 있는 잠재적인 설치 관련 문제점에 대한 해결책을 제공합니다.

로드 밸런서 시간 초과 오류와 함께 설치 또는 업그레이드가 실패함

로드 밸런서가 있는 분산 배포의 vRealize Automation 설치 또는 업그레이드가 503 서비스 사용 불가 오류를 표시하며 실패합니다.

문제

로드 밸런서 시간 초과 설정에서 작업을 완료할 시간이 충분히 허용되지 않아서 설치 또는 업그레이드가 실패합니다.

원인

로드 밸런서 시간 초과 설정이 충분하지 않아서 실패가 발생할 수 있습니다. 로드 밸런서 시간 초과 설정을 100초 이상으로 늘리고 작업을 다시 실행하여 문제를 수정할 수 있습니다.

해결책

- 1 로드 밸런서 시간 초과 값을 100초 이상으로 늘리십시오.
- 2 설치 또는 업그레이드를 다시 실행하십시오.

서버 시간이 동기화되지 않음

IaaS 시간 서버가 vRealize Automation 장치와 동기화되어 있지 않으면 설치가 실패할 수 있습니다.

문제

설치 후 로그인할 수 없거나, 설치가 완료되는 과정에서 실패합니다.

원인

모든 서버의 시간 서버가 동기화되지 않았을 수 있습니다.

해결책

모든 vRealize Automation 장치와 IaaS Windows Server를 동일한 시간 소스에 동기화합니다. 한 vRealize Automation 배포 내에서 시간 소스를 혼용하지 마십시오.

- vRealize Automation 장치 시간 소스를 설정합니다.
 - a vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
https://vrealize-automation-appliance-FQDN:5480
 - b **관리 > 시간 설정**을 선택하고 시간 동기화 소스를 설정합니다.

옵션	설명
호스트 시간	vRealize Automation 장치 ESXi 호스트에 동기화합니다.
시간 서버	외부 NTP(네트워크 시간 프로토콜) 서버 하나에 동기화합니다. NTP 서버의 FQDN 또는 IP 주소를 입력합니다.

- IaaS Windows Server의 경우 [Windows Server에서 시간 동기화 사용](#) 항목을 참조하십시오.

Windows 7에서 Internet Explorer 9 또는 10 사용 시 빈 페이지가 나타날 수 있음

Windows 7에서 Internet Explorer 9 또는 10을 사용하고 호환성 모드가 사용되게 설정되어 있는 경우 일부 페이지에 콘텐츠가 표시되지 않습니다.

사전 요구 사항

메뉴 모음이 표시되는지 확인합니다. Internet Explorer 9 또는 10을 사용하고 있는 경우 **Alt** 키를 눌러 메뉴 모음을 표시합니다(또는 주소 표시줄을 마우스 오른쪽 버튼으로 클릭한 후 **메뉴 모음** 선택).

문제

Windows 7에서 Internet Explorer 9 또는 10 사용 시 다음 페이지에 콘텐츠가 없습니다.

- 인프라
- Orchestrator 페이지의 기본 테넌트 폴더
- Orchestrator 페이지의 서버 구성

원인

이 문제는 사용되도록 설정되어 있는 호환성 모드와 관련이 있을 수 있습니다. 다음 단계에 따라 Internet Explorer에 대한 호환성 모드를 사용하지 않게 설정할 수 있습니다.

해결책

- 1 도구 > 호환성 보기 설정을 선택합니다.
- 2 호환성 보기에서 인트라넷 사이트 표시를 선택 해제합니다.
- 3 닫기를 클릭합니다.

SSL/TLS 보안 채널에 대한 신뢰 관계를 설정할 수 없음

"vCloud Automation Center의 보안 인증서를 업그레이드할 때 SSL/TLS 보안 채널에 대한 신뢰 관계를 설정할 수 없습니다." 메시지가 표시될 수 있습니다.

문제

보안 인증서를 업그레이드할 때 vcac-config.exe에서 인증서 문제가 발생하는 경우 다음 메시지가 표시될 수 있습니다.

기본 연결이 닫혀 있습니다. SSL/TLS 보안 채널에 대해 신뢰 관계를 설정할 수 없습니다.

다음 절차를 사용하여 문제의 원인에 대한 자세한 정보를 찾을 수 있습니다.

해결책

- 1 텍스트 편집기에서 vcac-config.exe.config 파일을 열고 다음 저장소 주소를 찾습니다.
`<add key="repositoryAddress" value="https://IaaS-address:443/repository/" />`
- 2 Internet Explorer를 열고 이 주소로 이동합니다.

- 3 인증서 신뢰 문제에 대한 모든 오류 메시지로 계속 진행합니다.
- 4 Internet Explorer에서 보안 보고서를 얻고 해당 보고서를 사용하여 인증서가 신뢰되지 않는 이유에 대한 문제를 해결합니다.

해결책

문제가 계속되면 등록해야 할 주소, 즉 `vcac-config.exe`로 등록하는 데 사용한 끝점 주소로 이동하여 해당 절차를 반복합니다.

프록시 서버를 통해 네트워크에 연결

일부 사이트는 프록시 서버를 통해 인터넷에 연결할 수 있습니다.

사전 요구 사항

사이트 관리자로부터 프록시 서버 이름, 포트 번호 및 자격 증명을 확인해야 합니다.

문제

배포 환경에서 개방형 인터넷에 연결할 수 없습니다. 예를 들어 웹 사이트, 사용자가 관리하는 공용 클라우드 또는 소프트웨어나 업데이트를 다운로드하는 벤더 주소에 액세스할 수 없습니다.

원인

사용자의 사이트가 프록시 서버를 통해 인터넷에 연결합니다.

해결책

- 1 웹 브라우저를 열고 vRealize Automation 장치 관리 인터페이스 URL로 이동합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 루트로 로그인하고 **네트워크**를 클릭합니다.
- 3 사이트 프록시 서버 FQDN 또는 IP 주소 및 포트 번호를 입력합니다.
- 4 프록시 서버가 자격 증명을 요청하면 사용자 이름과 암호를 입력합니다.
- 5 **설정 저장**을 클릭합니다.

다음에 수행할 작업

프록시를 사용하도록 구성하면 VMware Identity Manager 사용자 액세스에 영향을 미칠 수 있습니다. 문제를 해결하려면 [프록시 때문에 VMware Identity Manager 사용자 로그인이 차단된 항목을 참조하십시오](#).

초기 콘텐츠 구성을 위한 콘솔 단계

vRealize Automation 설치 인터페이스를 사용하는 대신 구성 관리자 계정과 초기 콘텐츠를 생성하는 방법이 있습니다.

인터페이스를 사용하는 대신 콘솔 명령을 입력하여 구성 관리자 사용자 및 초기 콘텐츠를 생성합니다. 프로세스의 일부가 완료된 후 인터페이스가 실패할 수 있습니다. 따라서 이 경우에는 일부 명령만 필요할 수 있습니다.

예를 들어 로그 및 vRealize Orchestrator 워크플로 실행 검사를 통해 인터페이스 기반 설치에서 구성 관리자 사용자는 생성했지만 초기 콘텐츠는 생성하지 못한 경우가 확인될 수 있습니다. 이 경우에는 마지막 두 콘솔 명령만 입력하여 프로세스를 완료할 수 있습니다.

문제

vRealize Automation 설치의 마지막 단계로 프로세스에 따라 새 암호를 입력하고, 구성 관리자 로컬 사용자 계정을 생성하고, 초기 콘텐츠를 생성합니다. 오류가 발생하고 인터페이스가 복구 불능 상태가 됩니다.

해결책

- 1 루트로 vRealize Automation 장치 콘솔에 로그인합니다.

- 2 다음 명령을 입력하여 vRealize Orchestrator 워크플로를 가져옵니다.

```
/usr/sbin/vcac-config -e content-import --workflow /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-workflow.package --user $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --tenant $TENANT
```

- 3 워크플로를 실행하여 구성 관리자 사용자를 생성합니다.

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --workflowid f2b3064a-75ca-4199-a824-1958d9c1efed --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 4 다음 명령을 입력하여 ASD Blueprint를 가져옵니다.

```
/usr/sbin/vcac-config -e content-import --blueprint /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-asd.zip --user $CONFIGURATIONADMIN_USERNAME --password $CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 5 워크플로를 실행하여 초기 콘텐츠를 구성합니다.

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
```

vRealize Automation 라이선스를 다운그레이드할 수 없음

낮은 제품 버전의 라이선스 키를 제출하는 경우 오류가 발생합니다.

문제

vRealize Automation 관리 인터페이스 라이선싱 페이지를 사용하여 현재 버전보다 낮은 제품 버전의 키를 제출하는 경우 다음 메시지가 표시됩니다. 예를 들어 Enterprise 라이선스를 시작하고 Advanced 라이선스를 입력하려고 합니다.

Unable to downgrade existing license edition

원인

이 vRealize Automation 릴리스는 라이선스 다운그레이드를 지원하지 않습니다. 같거나 높은 버전의 라이선스만 추가할 수 있습니다.

해결책

낮은 버전으로 변경하려면 vRealize Automation을 다시 설치하십시오.

vRealize Automation 장치 문제 해결

vRealize Automation 장치의 문제 해결 항목은 vRealize Automation 장치를 사용할 때 발생할 수 있는 잠재적인 설치 관련 문제점에 대한 해결책을 제공합니다.

설치 관리자 다운로드가 실패함

vRealize Automation 장치에서 설치 관리자가 다운로드를 수행할 수 없습니다.

문제

설치 관리자는 `setup__vrealize-automation-appliance-FQDN@5480.exe`를 실행할 때 다운로드하지 않습니다.

원인

- vRealize Automation 장치 시스템에 연결할 때 네트워크 연결 문제가 발생했습니다.
- 시스템이 범위 내에 없거나, 연결 시간이 초과되기 전까지 시스템이 응답할 수 없어 vRealize Automation 장치 시스템에 연결할 수 없습니다.

해결책

- 1 웹 브라우저에서 다음 vRealize Automation URL에 연결할 수 있는지 확인합니다.

`https://vrealize-automation-appliance-FQDN`

- 2 다른 vRealize Automation 장치 문제 해결 항목을 확인합니다.
- 3 설정 파일을 다운로드하고 vRealize Automation 장치에 다시 연결합니다.

Encryption.key 파일에 잘못된 사용 권한이 있음

잘못된 사용 권한이 가상 장치에 대한 Encryption.key 파일에 할당된 경우 시스템 오류가 발생할 수 있습니다.

사전 요구 사항

오류를 표시하는 가상 장치에 로그인합니다.

참고 가상 장치가 로드 밸런서에서 실행되고 있는 경우 각 가상 장치를 확인해야 합니다.

문제

vRealize Automation 장치에 로그인하면 테넌트 페이지가 표시됩니다. 페이지가 로드를 시작한 후 시스템 오류 메시지가 표시됩니다.

원인

Encryption.key 파일에 잘못된 사용 권한이 있거나 그룹 또는 소유자 사용자 수준이 잘못 할당되었습니다.

해결책

- 1 로그 파일 /var/log/vcac/catalina.out을 보고 메시지 /etc/vcac/Encryption.key에 쓸 수 없습니다.를 검색합니다.
- 2 /etc/vcac/ 디렉토리로 이동하고 Encryption.key 파일에 대한 사용 권한 및 소유권을 확인합니다. 다음과 유사한 줄이 표시되어야 합니다.

```
-rw----- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

읽기 및 쓰기 권한이 필요하며 파일에 대한 소유자 및 그룹이 vcac이어야 합니다.

- 3 표시되는 출력이 다른 경우 필요에 따라 파일의 사용 권한 또는 소유권을 변경합니다.

다음에 수행할 작업

테넌트 페이지에 로그인하여 오류 없이 로그인할 수 있는지 확인합니다.

Horizon Workspace 다시 시작 후 디렉토리 관리 Identity Manager가 시작되지 않음

vRealize Automation고가용성 환경에서는 Horizon Workspace 서비스가 다시 시작된 후 디렉토리 관리 Identity Manager가 시작되지 않을 수 있습니다.

문제

다음과 유사한 오류로 인해 Horizon Workspace 서비스를 시작할 수 없습니다.

```
Error creating bean with name
'liquibase' defined in class path resource [spring/datastore-wireup.xml]:
Invocation of init method failed; nested exception is
liquibase.exception.LockException: Could not acquire change log lock. Currently
locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0
(fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15
```


원인

vRealize Automation에 사용되는 liquibase 데이터 관리 유틸리티의 문제로 인해 Identity Manager가 고가용성 환경에서 시작되지 않을 수 있습니다.

해결책

1 vRealize Automation 장치의 콘솔 세션에 루트로 로그인합니다.

2 다음 명령을 입력하여 Horizon Workspace 서비스를 중지합니다.

```
#service horizon-workspace stop
```

3 슈퍼 사용자 권한으로 Postgres 셸을 엽니다.

```
su postgres
```

4 올바른 bin 디렉토리로 이동합니다.

```
cd /opt/vmware/vpostgres/current/bin
```

5 데이터베이스에 연결합니다.

```
psql vcac
```

6 saas.databasechangelock에서 다음 SQL 쿼리를 실행합니다.

```
select * from databasechangelock;
```

출력이 "t" 값(True)을 표시하면 잠금을 수동으로 해제해야 합니다.

7 잠금을 수동으로 해제하려면 다음 SQL 쿼리를 실행합니다.

```
update saas.databasechangelock set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;
```

8 saas.databasechangelock에서 다음 SQL 쿼리를 실행합니다.

```
select * from databasechangelock;
```

출력이 "f" 값(False)을 표시해야 합니다. 이는 잠금이 해제되었음을 의미합니다.

9 Postgres vcac 데이터베이스를 종료합니다.

```
vcac=# \q
```

10 Postgres 셸을 닫습니다.

```
exit
```

11 Horizon Workspace 서비스를 시작합니다.

```
#service horizon-workspace start
```

폐일오버 후 잘못된 장치 역할 할당

폐일오버 발생 후 마스터 및 복제 vRealize Automation 장치 노드에 잘못된 역할이 할당되어 데이터베이스 쓰기 액세스 권한이 필요한 모든 서비스에 영향을 줄 수 있습니다.

문제

vRealize Automation 장치의 고가용성 클러스터에서 마스터 데이터베이스 노드를 종료하거나 액세스할 수 없는 상태로 만듭니다. 다른 노드에서 관리 인터페이스를 사용하여 해당 노드를 새 마스터로 승격하면 vRealize Automation 데이터베이스 쓰기 액세스 권한이 복원됩니다.

나중에 이전 master 노드를 다시 온라인 상태로 전환하면 해당 관리 인터페이스의 [클러스터] 탭에는 사실과 다르게 이 노드가 계속 master 노드로 표시됩니다. 임의의 노드 관리 인터페이스에서 이전 노드를 다시 마스터로 정식 승격하여 문제를 해결하려는 시도는 실패합니다.

해결책

페일오버가 발생하는 경우 이전 master 노드와 새 master 노드를 구성할 때 다음 지침을 따릅니다.

- 다른 노드를 마스터로 승격하기 전에 vRealize Automation 장치 노드의 로드 밸런서 풀에서 이전 마스터 노드를 제거합니다.
- vRealize Automation에서 이전 master 노드를 다시 클러스터로 가져오도록 이전 시스템을 온라인으로 설정합니다. 그런 다음 새 마스터 관리 인터페이스를 엽니다. [클러스터] 탭 아래에 **invalid**로 표시된 이전 노드를 찾은 다음 해당하는 **재설정** 버튼을 클릭합니다.

재설정이 완료되면 이전 노드를 vRealize Automation 장치 노드의 로드 밸런서 풀로 복원할 수 있습니다.

- 수동으로 이전 master 노드를 클러스터로 다시 가져오려면 시스템을 온라인으로 설정하고 이전 노드를 새 노드인 것처럼 클러스터에 가입시킵니다. 가입하는 동안 새로 승격된 노드를 기본 노드로 지정합니다.

가입이 완료되면 이전 노드를 로드 밸런서 풀의 vRealize Automation 장치 노드로 복원할 수 있습니다.

- 이전 master 노드가 올바르게 재설정되거나 클러스터에 다시 가입될 때까지 클러스터 관리 작업을 위해 해당 관리 인터페이스를 사용하지 마십시오. 노드가 다시 온라인으로 설정된 경우에도 마찬가지입니다.
- 이전 노드를 올바르게 재설정 또는 다시 가입했다면 이전 노드를 다시 마스터로 승격할 수 있습니다.

복제 및 마스터 노드의 승격 후 실패

복제 및 마스터 vRealize Automation 장치 데이터베이스 노드의 승격과 함께 디스크 공간 문제로 인해 프로비저닝 관련 문제가 발생할 수 있습니다.

문제

마스터 노드에 디스크 공간이 부족합니다. 해당 관리 인터페이스 데이터베이스 페이지에 로그인하고 충분한 공간을 가진 복제 노드를 새 마스터로 승격합니다. 관리 인터페이스 페이지를 새로 고치면 오류 메시지가 표시되기는 하지만 승격이 성공한 것으로 나타납니다.

그런 다음, 이전에 마스터였던 노드에서 디스크 공간을 확보합니다. 이 노드를 다시 마스터로 승격하려고 하면 **IN_PROGRESS** 상태에 멈추면서 프로비저닝 작업이 실패합니다.

원인

부족한 공간으로 인한 문제가 발생할 때 vRealize Automation은 이전 마스터 노드 구성을 제대로 업데이트할 수 없습니다.

해결책

승격 중 관리 인터페이스에서 오류를 표시하는 경우 로드 밸런서에서 해당 노드를 일시적으로 제외합니다. 로드 밸런서에 해당 노드를 다시 포함하기 전에 노드 문제점을 해결합니다(예: 디스크 추가). 그런 다음 관리 인터페이스 데이터베이스 페이지를 새로 고치고 올바른 노드가 마스터 및 복제로 지정되었는지 확인합니다.

잘못된 vRealize Automation 구성 요소 서비스 등록

vRealize Automation 장치 관리 인터페이스는 vRealize Automation 구성 요소 서비스 관련 등록 문제를 해결하는 데 도움을 줍니다.

문제

정상적인 작업 상태에서 모든 vRealize Automation 구성 요소 서비스는 고유해야 하며 [등록됨] 상태여야 합니다. 다른 조건 집합은 vRealize Automation에 예기치 않은 동작을 유발할 수 있습니다.

원인

다음은 vRealize Automation 구성 요소 서비스에서 발생할 수 있는 문제의 예입니다.

- 서비스가 비활성 상태가 되었습니다.
- 서버 설정으로 인해 서비스가 [등록됨] 이외의 상태가 되었습니다.
- 다른 서비스에 대한 종속성으로 인해 서비스가 [등록됨] 이외의 상태가 되었습니다.
- SQL 서비스가 실행되고 있지 않을 수 있습니다.

해결책

문제가 있는 것으로 보이는 구성 요소 서비스를 다시 등록합니다.

- 1 vRealize Automation 장치의 스냅샷을 생성합니다.

다른 서비스 변경을 시도하고 장치의 상태가 예상과 다른 경우 스냅샷으로 되돌려야 할 수 있습니다.

- 2 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 3 **서비스**를 클릭합니다.

- 4 서비스 목록에서 올바른 상태가 아니거나 기타 문제가 있는 서비스를 찾습니다.

- 5 문제가 있는 서비스가 **iaas-service**인 경우 다음 단계로 이동합니다.

그렇지 않은 경우 vRealize Automation이 서비스를 다시 등록하도록 하려면 vRealize Automation 장치의 콘솔 세션에 root로 로그인하고 다음 명령을 입력하여 vRealize Automation을 다시 시작합니다.

```
service vcac-server restart
```

포함된 vRealize Orchestrator 인스턴스에 연결된 서비스가 있는 경우 다음 명령을 추가로 입력합니다.

```
service vco-restart restart
```

6 문제가 있는 서비스가 `iaas-service`인 경우 다음 단계를 수행하여 다시 등록합니다.

- a 서비스를 등록 취소하지 마십시오.
- b 기본 IaaS 웹 서버에 관리자 권한을 가진 계정으로 로그인합니다.
- c 관리자 권한으로 명령 프롬프트를 엽니다.
- d 다음 명령을 실행합니다.

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterSolutionUser -url https://appliance-or-load-balancer-IP-or-FQDN/ -t
vsphere.local -cu administrator -cp password -f "C:\Program Files (x86)\VMware\VCAC
\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

암호는 administrator@vsphere.local 암호입니다.

- e 명령을 실행하여 IaaS 데이터베이스에서 등록 정보를 업데이트합니다.

Windows 인증을 사용하는 SQL Server:

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
MoveRegistrationDataToDb -s IaaS-SQL-server-IP-or-FQDN -d SQL-database-name -f
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

Native SQL 인증을 사용하는 SQL Server:

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
MoveRegistrationDataToDb -s SQL-server-IP-or-FQDN -d SQL-database-name -su SQL-user -
sp SQL-user-password -f "C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data
\Cafe\Vcac-Config.data" -v
```

서버 또는 데이터베이스 이름을 찾으려면 텍스트 편집기에서 다음 파일을 검사하고 repository를 검색합니다. 데이터 소스 및 최초 카탈로그 값이 서버 주소와 데이터베이스 이름을 각각 나타냅니다.

```
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
```

SQL 사용자는 데이터베이스에 대한 DBO 권한이 있어야 합니다.

- f 다음 명령을 실행하여 끝점을 등록합니다.

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /vcac
--Endpoint ui -v
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /WAPI
--Endpoint wapi -v
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /
repository --Endpoint repo -v
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /
WAPI/api/status --Endpoint status -v
```

- g 다음 명령을 실행하여 카탈로그 항목을 등록합니다.

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterCatalogTypesAsync -v
```

- h IIS를 다시 시작합니다.

```
iisreset
```

- i 기본 IaaS Manager Service 호스트에 로그인합니다.

- j vRealize Automation Windows 서비스를 다시 시작합니다.

```
VMware vCloud Automation Center Service
```

- 7 외부 vRealize Orchestrator 인스턴스와 같이 외부 시스템에 연결된 서비스를 다시 등록하려면 외부 시스템에 로그인하고 해당 위치에서 서비스를 다시 시작합니다.

추가 NIC로 인해 관리 인터페이스 오류가 발생함

vRealize Automation 장치에 두 번째 NIC(네트워크 인터페이스 카드)를 추가한 후에 일부 vRealize Automation 관리 인터페이스 페이지가 제대로 로드되지 않습니다.

문제

vCenter를 사용하여 두 번째 NIC를 추가하고 다음 vRealize Automation 관리 인터페이스 페이지가 로드되지 않고 오류를 표시합니다.

- **네트워크 > 상태** 페이지에서 응답하지 않는 스크립트에 관한 오류를 표시합니다.
- **네트워크 > 주소** 페이지에서 네트워크 인터페이스 정보 읽기 실패에 관한 오류를 표시합니다.

원인

버전 7.3부터 vRealize Automation 장치는 이중 NIC를 지원할 수 있습니다. 하지만 솔루션을 적용할 때까지 장치의 기반이 되는 엔지니어링 템플릿으로 인해 관리 인터페이스가 제대로 작동할 수 없습니다.

해결책

추가적인 NIC를 추가한 후에 vRealize Automation 장치를 다시 시작합니다.

보조 가상 장치를 마스터로 승격할 수 없음

vRealize Automation에서, 가상 장치 메모리 부족은 클러스터에서 가상 장치 승격을 방해할 수 있습니다.

문제

메모리가 부족한 상태에서 마스터 노드가 실행됩니다. 해당 관리 인터페이스 [데이터베이스] 페이지에 로그인하고 보조 노드를 새 마스터로 승격시키기 위해 시도합니다. 이때 다음 오류가 발생합니다.

```
Fail to execute on Node node-name, host is master-FQDN
because of: Could not read remote lock command result for node: node-name
on address: master-FQDN, reason is: 500 Internal Server Error
```

원인

승격은 모든 노드가 새로 승격된 마스터에 대한 재구성을 확인할 수 있을 때만 성공합니다. 메모리 부족은 모든 노드에 연결할 수 있는 경우라도 이전 마스터의 확인 작업을 방해할 수 있습니다.

해결책

메모리가 부족한 마스터 노드의 전원을 끕니다. 보조 노드 관리 인터페이스 [데이터베이스] 페이지에 로그인하고 보조 노드를 승격합니다.

Active Directory 동기화 로그 보존 기간이 너무 짧음

vRealize Automation에서, Active Directory 동기화 로그는 단 몇 일만 보존됩니다.

문제

이틀이 지나면 Active Directory 동기화 로그가 관리 인터페이스에서 사라집니다. 로그 폴더도 다음 vRealize Automation 장치 디렉토리에서 사라집니다.

```
/db/elasticsearch/horizon/nodes/0/indices
```

원인

공간을 절약하기 위해, vRealize Automation은 Active Directory 동기화 로그에 대한 최대 보존 기간을 3일로 설정합니다.

해결책

- 1 vRealize Automation 장치의 콘솔 세션에 루트로 로그인합니다.
- 2 텍스트 편집기에서 다음 파일을 엽니다.
`/usr/local/horizon/conf/runtime-config.properties`
- 3 `analytics.maxQueryDays` 속성의 값을 늘립니다.
- 4 `runtime-config.properties`를 저장하고 닫습니다.

5 Identity Manager와 elasticsearch 서비스를 다시 시작합니다.

```
service horizon-workspace restart
service elasticsearch restart
```

RabbitMQ가 호스트 이름을 확인할 수 없음

RabbitMQ는 기본적으로 vRealize Automation 장치에 짧은 호스트 이름을 사용하므로 노드가 서로를 확인하지 못할 수 있습니다.

문제

다른 vRealize Automation 장치를 클러스터에 연결하려고 하면 다음과 유사한 오류가 발생합니다.

```
Clustering node 'rabbit@sc2-rdops-vm01-dhcp-62-2' with rabbit@company ...
Error: unable to connect to nodes [rabbit@company]: nodedown

DIAGNOSTICS
=====

attempted to contact: [rabbit@company]

rabbit@company:
  * unable to connect to epmd (port 4369) on company: nxdomain (non-existing domain)

current node details:
- node name: 'rabbitmq-cli-11@sc2-rdops-vm01-dhcp-62-2'
- home dir: /var/lib/rabbitmq
- cookie hash: 4+kP1tKnxGYaGjrPL2C8bQ==

[2017-09-01 14:58:04] [root] [INFO] RabbitMQ join failed with exit code: 69, see RabbitMQ logs for details.
```

원인

네트워크 구성으로 인해 vRealize Automation 장치가 짧은 호스트 이름으로 서로를 확인할 수 없습니다.

해결책

1 배포의 모든 vRealize Automation 장치에 대해 콘솔 세션에 root로 로그인합니다.

2 RabbitMQ 서비스를 중지합니다.

```
service rabbitmq-server stop
```

3 텍스트 편집기에서 다음 파일을 엽니다.

```
/etc/rabbitmq/rabbitmq-env.conf
```

4 다음 속성을 true로 설정합니다.

```
USE_LONGNAME=true
```

5 rabbitmq-env.conf를 저장한 후 닫습니다.

6 RabbitMQ를 재설정합니다.

```
vcac-vami rabbitmq-cluster-config reset-rabbitmq-node
```

7 단 하나의 vRealize Automation 장치 노드에서 다음 스크립트를 실행합니다.

```
vcac-config cluster-config-ping-nodes --services rabbitmq-server
```

8 모든 노드에서 RabbitMQ 서비스가 시작되었는지 확인합니다.

```
vcac-vami rabbitmq-cluster-config get-rabbitmq-status
```

IaaS 구성 요소 문제 해결

vRealize Automation IaaS 구성 요소의 문제 해결 항목은 vRealize Automation을 사용할 때 발생할 수 있는 잠재적인 설치 관련 문제에 대한 해결책을 제공합니다.

DTC(Distributed Transaction Coordinator) 연결이 거부됨

Microsoft RPC(원격 프로시저 호출) 설정은 vRealize Automation의 DTC(Distributed Transaction Coordinator)에 영향을 줄 수 있습니다.

문제

오류가 발생하여 IaaS Windows Server 또는 vRealize Automation SQL 데이터베이스 서버 간의 DTC 연결이 거부되고 있음을 표시합니다.

원인

RPC 연결 설정은 액세스를 제한하며 사용하지 않도록 설정해야 합니다.

해결책

모든 IaaS Windows Server 및 vRealize Automation SQL 데이터베이스 서버에서 다음 레지스트리 키를 제거하거나 0으로 설정합니다.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients
```

사전 요구 사항 수정기가 .NET 기능을 설치할 수 없음

vRealize Automation 사전 요구 사항 검사기 **수정** 옵션이 실패하고 NET 3.5.1의 설치 소스를 찾을 수 없다는 메시지를 표시합니다.

문제

IIS 7.5가 있는 Windows Server 2008 R2 시스템 및 IIS 8이 있는 Windows Server 2012 R2 시스템에 대한 요구 사항 충족을 위해 사전 요구 사항 검사기를 통해 .NET 3.5.1이 설치되어 있는지 확인해야 합니다.

원인

Windows Server 2012 R2의 경우 인터넷에 연결할 수 없으면 .NET을 자동으로 설치하지 못할 수 있습니다. 특정 Windows 2012 R2 업데이트도 설치하지 못할 수 있습니다. 이 문제는 Windows 버전에 .NET Framework 3.5 설치 소스의 로컬 복사본이 없기 때문에 발생합니다.

해결책

.NET Framework 3.5 설치 소스를 수동으로 제공합니다.

- 1 Windows 호스트에서 Windows Server 2012 R2 설치 미디어의 ISO를 마운트합니다.
- 2 Server Manager에서 역할 및 기능 추가 마법사를 사용하여 .NET Framework 3.5를 사용하도록 설정합니다.
- 3 마법사를 실행하는 동안 ISO 미디어의 .NET Framework 3.5 설치 경로로 이동합니다.
- 4 .NET Framework 3.5를 추가한 후 vRealize Automation 사전 요구 사항을 검사기를 다시 실행합니다.

IaaS에 대해 서버 인증서의 유효성 검사

vcac-Config.exe 명령을 사용하여 IaaS 서버가 vRealize Automation 장치 및 SSO 장치 인증서를 수락하는지 확인할 수 있습니다.

문제

IaaS 기능을 사용할 때 인증 오류가 발생합니다.

원인

IaaS가 다른 구성 요소의 보안 인증서를 인식하지 않는 경우 인증 오류가 발생할 수 있습니다.

해결책

- 1 관리자 권한으로 명령 프롬프트를 열고 Cafe 디렉토리 `vra-installation-dir\Server\Model Manager Data\Cafe`(일반적으로 `C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe`)로 이동합니다.
- 2 **Vcac-Config.exe CheckServerCertificates -d [vra-database] -s [vRA SQL server] -v** 형식의 명령을 입력합니다. 선택적 매개 변수는 `-su [SQL 사용자 이름]` 및 `-sp [암호]`입니다.

명령이 성공하면 다음 메시지가 표시됩니다.

```
Certificates validated successfully.
Command succeeded.
```

명령이 실패하면 상세한 오류 메시지가 표시됩니다.

참고 이 명령은 Model Manager Data 구성 요소에 대한 노드에서만 사용할 수 있습니다.

IaaS 설치 관리자를 실행하는 동안 자격 증명 오류가 발생함

IaaS 구성 요소를 설치하면 가상 장치 자격 증명을 입력할 때 오류가 표시됩니다.

문제

IaaS 설치 관리자에 자격 증명을 제공하고 나면 `org.xml.sax.SAXParseException` 오류가 나타납니다.

원인

잘못된 자격 증명 또는 잘못된 자격 증명 형식을 사용했습니다.

해결책

- ◆ 올바른 테넌트 및 사용자 이름 값을 사용하는지 확인합니다.

예를 들어 SSO 기본 테넌트는 administrator@vsphere.local이 아니라 vsphere.local 같은 도메인 이름을 사용합니다.

IaaS 설치 중 설정 저장 경고가 표시됨

메시지가 IaaS 설치 중 표시됩니다. 경고: IaaS 설치 중 설정을 가상 장치에 저장할 수 없습니다.

문제

사용자 설정이 저장되지 않았음을 나타내는 부정확한 오류 메시지가 IaaS 설치 중 표시됩니다.

원인

통신 또는 네트워크 문제로 인해 이러한 메시지가 잘못 표시될 수 있습니다.

해결책

오류 메시지를 무시하고 설치를 계속합니다. 이 메시지로 인해 설치가 실패해서는 안 됩니다.

웹 사이트 서버 및 Distributed Execution Manager의 설치가 실패함

IaaS 서비스 계정의 암호에 큰따옴표가 포함되어 있으면 vRealize Automation 장치 인프라 웹 사이트 서버 및 Distributed Execution Manager의 설치를 계속할 수 없습니다.

문제

msiexec 매개 변수가 잘못되었기 때문에 vRealize Automation 장치 DEM(Distributed Execution Manager) 및 웹 사이트 서버의 설치가 실패했다는 메시지가 표시됩니다.

원인

IaaS 서비스 계정 암호는 큰따옴표 문자를 사용합니다.

해결책

- 1 IaaS 서비스 계정 암호의 일부로 큰따옴표가 포함되어 있지 않은지 확인합니다.
- 2 암호에 큰따옴표가 포함된 경우 새 암호를 생성하십시오.
- 3 설치를 다시 시작합니다.

IaaS 웹 및 모델 관리 설치 중 IaaS 인증 실패

사전 요구 사항 검사기를 실행할 때 IIS 인증 검사가 실패했다는 메시지가 표시됩니다.

문제

인증이 사용하도록 설정되지 않았다는 메시지가 표시되지만 IIS 인증 확인란이 선택되었습니다.

해결책

- 1 Windows 인증 확인란을 선택 해제합니다.
- 2 **저장**을 클릭합니다.
- 3 Windows 인증 확인란을 선택합니다.
- 4 **저장**을 클릭합니다.
- 5 사전 요구 사항 검사기를 다시 실행합니다.

Model Manager Data 및 웹 구성 요소의 설치가 실패함

IaaS 설치 관리자가 Model Manager Data 구성 요소와 웹 구성 요소를 저장하지 못하면 vRealize Automation 설치가 실패할 수 있습니다.

문제

다음 메시지와 함께 설치가 실패합니다.

IaaS 설치 관리자가 Model Manager Data 및 웹 구성 요소를 저장하지 못했습니다.

원인

이 실패의 원인으로는 몇 가지가 가능합니다.

- vRealize Automation 장치에 대한 연결 문제 또는 장치 사이에 연결 문제가 있는 경우. 응답이 없거나, 연결을 설정할 수 없어 연결 시도가 실패한 경우
- 분산 구성을 사용할 때 IaaS에 신뢰할 수 있는 인증서 문제가 있는 경우
- 분산 구성에서 인증서 이름이 일치하지 않는 경우
- 인증서가 잘못되거나 인증서 체인에 오류가 있는 경우
- 저장소 서비스를 시작할 수 없는 경우
- 분산 환경에서 로드 밸런서의 구성이 잘못된 경우

해결책

◆ 연결

웹 브라우저에서 다음 vRealize Automation URL에 연결할 수 있는지 확인합니다.

<https://vrealize-automation-appliance-FQDN>

◆ 신뢰할 수 있는 인증서 문제

- IaaS에서 `mmc.exe` 명령을 사용하여 Microsoft Management Console을 열고, 설치에 사용된 인증서가 시스템의 [신뢰할 수 있는 루트 인증서 저장소]에 추가되어 있는지 확인합니다.

- 웹 브라우저에서 MetaModel 서비스의 상태를 확인하고 인증서 오류가 나타나지 않는지 확인합니다.

`https://FQDN-or-IP/repository/data/MetaModel.svc`

◆ 인증서 이름 불일치

이 오류는 인증서에 특정 이름을 지정했지만 다른 이름이나 IP 주소를 사용한 경우에 발생할 수 있습니다. 설치 시 인증서 이름 불일치 오류를 표시하지 않으려면 **인증서 불일치 표시 안 함**을 선택합니다.

[인증서 불일치 표시 안 함] 옵션은 원격 인증서 해지 목록 불일치 오류를 무시하는 데도 사용될 수 있습니다.

◆ 인증서가 잘못됨

`mmc.exe` 명령을 사용하여 Microsoft Management Console을 엽니다. 인증서가 만료되지 않았는지 그리고 상태가 올바른지 확인합니다. 인증서 체인의 모든 인증서에 대해 이 작업을 수행합니다. 인증서 계층을 사용할 때 체인에 포함된 다른 인증서를 [신뢰할 수 있는 루트 인증서 저장소]로 가져와야 할 수도 있습니다.

◆ 저장소 서비스

다음과 같은 작업을 사용하여 저장소 서비스의 상태를 확인합니다.

- 웹 브라우저에서 MetaModel 서비스의 상태를 확인합니다.

`https://FQDN-or-IP/repository/data/MetaModel.svc`

- `Repository.log`에서 오류를 확인합니다.
- 웹 사이트에서 호스팅된 애플리케이션(저장소, vRealize Automation 또는 WAPI)에 문제가 있는 경우 IIS를 재설정(`iisreset`)합니다.
- `%SystemDrive%\inetpub\logs\LogFiles`에 있는 웹 사이트 로그에서 추가적인 로깅 정보를 확인합니다.
- 요구 사항을 확인하는 동안 [사전 요구 사항 검사기]가 통과했는지 확인합니다.
- Windows 2012에서 .NET Framework 아래의 WCF 서비스가 설치되고 HTTP 활성화가 설치되었는지 확인합니다.

IaaS Windows Server가 FIPS를 지원하지 않음

FIPS(Federal Information Processing Standard)를 사용하도록 설정한 경우 설치에 성공할 수 없습니다.

문제

IaaS 웹 구성 요소를 설치하는 중 설치가 다음 오류와 함께 실패합니다.

이 구현은 Windows Platform FIPS 검증 암호화 알고리즘의 일부가 아닙니다.

원인

vRealize Automation IaaS는 FIPS를 지원하지 않는 Microsoft WCF(Windows Communication Foundation)를 기반으로 구축되었습니다.

해결책

IaaS Windows Server에서 FIPS 정책을 사용하지 않도록 설정합니다.

- 1 시작 > 제어판 > 관리 도구 > 로컬 보안 정책으로 이동합니다.
- 2 로컬 정책 아래의 [그룹 정책] 대화상자에서 **보안 옵션**을 선택합니다.
- 3 다음 항목을 찾아 해당 항목이 사용되지 않도록 설정합니다.

시스템 암호화: 암호화, 해시, 서명에 FIPS 호환 알고리즘 사용.

XaaS 끝점을 추가하면 내부 오류 발생

XaaS 끝점을 생성하려고 하면 내부 오류 메시지가 나타납니다.

문제

끝점 생성이 실패하고 다음 내부 오류 메시지가 나타납니다. 내부 오류가 발생했습니다. 문제가 지속되면 시스템 관리자에게 문의하십시오. 시스템 관리자에게 문의할 때 **c0DD0C01**이라는 참조 코드를 사용하십시오. 참조 코드는 임의로 생성되고 특정 오류 메시지에 연결되지 않습니다.

해결책

- 1 vRealize Automation 장치 로그 파일을 엽니다.
`/var/log/vcac/catalina.out`
- 2 오류 메시지에서 참조 코드를 찾습니다.
예: **c0DD0C01**.
- 3 로그 파일에서 참조 코드를 검색하여 연결된 항목을 찾습니다.
- 4 연결된 항목 위와 아래에 나타나는 항목을 검토하여 문제를 해결합니다.
연결된 로그 항목이 문제의 소스를 구체적으로 나타내지는 않습니다.

프록시 에이전트 제거가 실패함

Windows Installer 로깅을 사용하도록 설정한 경우 프록시 에이전트 제거가 실패할 수 있습니다.

문제

Windows 제어판에서 프록시 에이전트를 제거하려고 할 때 제거가 실패하고 다음 오류가 나타납니다.

Error opening installation log file. Verify that the specified log file location exists and is writable

원인

이 문제는 Windows Installer 로깅을 사용하도록 설정했지만 Windows Installer 엔진이 제거 로그 파일을 적절하게 쓸 수 없을 때 발생할 수 있습니다. 자세한 내용은 [Microsoft 기술 자료 문서 2564571](#) 항목을 참조하십시오.

해결책

- 1 시스템을 다시 시작하거나 작업 관리자에서 `explorer.exe`를 다시 시작합니다.
- 2 에이전트를 제거합니다.

원격 트랜잭션을 사용하지 않도록 설정한 경우에 시스템 요청이 실패함

Windows Server 시스템에 Microsoft DTC(Distributed Transaction Coordinator) 원격 트랜잭션이 사용할 수 없도록 설정되어 있으면 시스템 요청이 실패합니다.

문제

Model Manager 포털 또는 SQL Server에서 원격 트랜잭션이 사용할 수 없도록 설정되어 있는 경우에 시스템을 프로비저닝하면 요청이 완료되지 않습니다. 데이터 수집이 실패하고 시스템 요청이 CloneWorkflow 상태로 남아 있습니다.

원인

vRealize Automation 시스템에서 사용하는 IaaS SQL 인스턴스에 DTC 원격 트랜잭션이 사용할 수 없도록 설정되었습니다.

해결책

- 1 Windows Server Manager를 시작하여 모든 vRealize 서버와 관련 SQL 서버에서 DTC를 사용하도록 설정합니다.

Windows 7에서 **시작 > 관리 도구 > 구성 요소 서비스**로 이동합니다.

참고 모든 Windows Server가 MSDTC 구성에 필요한 고유한 SID를 가지고 있는지 확인합니다.

- 2 모든 노드를 열고 로컬 DTC 또는 클러스터된 DTC(클러스터된 시스템을 사용하는 경우)를 찾습니다.
구성 요소 서비스 > 컴퓨터 > 내 컴퓨터 > Distributed Transaction Coordinator로 이동합니다.
- 3 로컬 또는 클러스터된 DTC를 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.
- 4 [보안] 탭을 클릭합니다.
- 5 **네트워크 DTC 액세스** 옵션을 선택합니다.
- 6 **원격 클라이언트 허용** 및 **원격 관리 허용** 옵션을 선택합니다.
- 7 **인바운드 허용** 및 **아웃바운드 허용** 옵션을 선택합니다.
- 8 DTC 로그인 계정에 대한 **계정** 필드에서 NT AUTHORITY\Network Service를 입력하거나 선택합니다.
- 9 **확인**을 클릭합니다.

10 CloneWorkflow 상태의 중단된 시스템을 제거합니다.

- a vRealize Automation 제품 인터페이스에 로그인합니다.

`https://vrealize-automation-appliance-FQDN/vcac/org/tenant-name`

- b **인프라 > 관리되는 시스템**으로 이동합니다.
- c 대상 시스템을 마우스 오른쪽 버튼으로 클릭합니다.
- d **삭제**를 선택하여 시스템을 제거합니다.

Manager Service 통신의 오류

DTC가 이미 설치된 템플릿에서 복제된 IaaS 서버에는 DTC에 대한 중복 식별자가 포함되어 있어서 노드 간의 통신을 방해합니다.

문제

IaaS Manager Service가 실패하고 Manager Service 로그에 다음과 같은 오류가 게시됩니다.

```
Communication with the underlying transaction manager has failed. --->
System.Runtime.InteropServices.COMException: The MSDTC transaction manager was unable to pull the
transaction from the source transaction manager due to communication problems. Possible causes are: a
firewall is present and it doesn't have an exception for the MSDTC process, the two machines cannot
find each other by their NetBIOS names, or the support for network transactions is not enabled for
one of the two transaction managers.
```

원인

DTC가 이미 설치된 IaaS 서버를 복제하는 경우 복제에 상위와 동일한 DTC의 고유 식별자가 포함됩니다. 두 시스템 간의 통신이 실패합니다.

해결책

- 1 복제에서 관리자 명령 프롬프트를 엽니다.
- 2 다음 명령을 실행합니다.

```
msdtc -uninstall
```

- 3 복제를 다시 시작합니다.
- 4 다른 명령 프롬프트를 열고 다음 명령을 실행합니다.

```
msdtc -install manager-service-host-FQDN
```

이메일 사용자 지정 동작이 변경됨

vRealize Automation 6.0 이상에서는 IaaS 구성 요소에서 생성된 알림만 이전 버전의 이메일 템플릿 기능을 통해 사용자 지정할 수 있습니다.

해결책

다음과 같은 XSLT 템플릿을 사용할 수 있습니다.

- ArchivePeriodExpired
- EpiRegister
- EpiUnregister
- LeaseAboutToExpire
- LeaseExpired
- LeaseExpiredPowerOff
- ManagerLeaseAboutToExpire
- ManagerLeaseExpired
- ManagerReclamationExpiredLeaseModified
- ManagerReclamationForcedLeaseModified
- ReclamationExpiredLeaseModified
- ReclamationForcedLeaseModified
- VdiRegister
- VdiUnregister

이메일 템플릿은 서버 설치 디렉토리(일반적으로 *%SystemDrive%\Program Files x86\VMware\VCAC\Server*에 위치)의 *\Templates* 디렉토리에 있습니다. *\Templates* 디렉토리에는 더 이상 지원되지 않으며 수정할 수 없는 XSLT 템플릿도 포함되어 있습니다.

로그인 오류 문제 해결

vRealize Automation의 로그인 오류에 대한 문제 해결 항목은 vRealize Automation을 사용할 때 발생할 수 있는 잠재적인 설치 관련 문제점에 대한 해결책을 제공합니다.

잘못된 UPN 형식 자격 증명을 사용하여 IaaS 관리자로 로그인하려고 하면 아무 설명 없이 실패함

IaaS 관리자로 vRealize Automation에 로그인하려고 하면 아무 설명 없이 해당 로그인 페이지로 리디렉션됩니다.

문제

사용자 이름의 *@yourdomain* 부분을 포함하지 않는 UPN 자격 증명을 사용하여 IaaS 관리자로 vRealize Automation에 로그인하려고 하면 아무 설명 없이 즉시 SSO에서 로그아웃되고 로그인 페이지로 리디렉션됩니다.

원인

`yourname.admin@yourdomain` 형식에 따라 UPN을 입력해야 합니다. 예를 들어 사용자 이름으로 `jsmith.admin@sqa.local`을 사용하여 로그인하지만 UPN이 Active Directory에 `jsmith.admin`으로만 설정되어 있으면 로그인이 실패합니다.

해결책

문제를 해결하려면 필요한 `@yourdomain` 부분을 포함하도록 `userPrincipalName` 값을 변경하고 로그인을 다시 시도합니다. 이 예에서 UPN 이름은 `jsmith.admin@sqa.local`이어야 합니다. 이 정보는 `log/vcac` 폴더 안의 로그 파일에서도 제공됩니다.

고가용성에서 로그인 실패

둘 이상의 vRealize Automation 장치가 있는 경우 장치가 짧은 호스트 이름으로 서로를 식별할 수 있어야 합니다. 그렇지 않으면 로그인할 수 없습니다.

고가용성 vRealize Automation 장치의 클러스터가 짧은 호스트 이름을 확인할 수 있도록 허용하려면 다음 접근 방법 중 하나를 사용합니다. 클러스터의 모든 장치를 수정해야 합니다.

문제

vRealize Automation 장치를 추가로 설치하여 고가용성을 위해 vRealize Automation을 구성합니다. vRealize Automation에 로그인하려고 시도할 때 잘못된 라이선스에 관한 메시지가 나타납니다. 라이선스가 올바른 것을 확인했기 때문에 이 메시지는 잘못된 것입니다.

원인

vRealize Automation 장치 노드는 클러스터 노드의 짧은 호스트 이름을 확인할 수 있을 때까지 고가용성 클러스터를 올바르게 구성하지 않습니다.

해결책

- ◆ `/etc/resolv.conf`에서 검색 줄을 편집 또는 생성합니다. 이 줄에는 vRealize Automation 장치가 있는 도메인이 포함되어야 합니다. 도메인이 여러 개인 경우 공백으로 구분합니다. 예:

```
search sales.mycompany.com support.mycompany.com
```

- ◆ `/etc/resolv.conf`에서 도메인 줄을 편집 또는 생성합니다. 각 줄에는 vRealize Automation 장치가 있는 도메인이 포함되어야 합니다. 예:

```
domain support.mycompany.com
```

- ◆ 줄을 `/etc/hosts` 파일에 추가하여 vRealize Automation 장치의 짧은 이름 각각이 해당 FQDN(정규화된 도메인 이름)에 매핑되도록 합니다. 예:

```
node1    node1.support.mycompany.com
node2    node2.support.mycompany.com
```

프록시 때문에 VMware Identity Manager 사용자 로그인이 차단됨

프록시를 사용하도록 구성하면 VMware Identity Manager 사용자가 로그인하지 못할 수 있습니다.

사전 요구 사항

프록시 서버를 통해 네트워크에 액세스하도록 vRealize Automation을 구성합니다. [프록시 서버를 통해 네트워크에 연결](#) 항목을 참조하십시오.

문제

프록시 서버를 통해 네트워크에 액세스하도록 vRealize Automation을 구성하면 VMware Identity Manager 사용자가 로그인하려고 할 때 다음 오류가 표시됩니다.

Error Unable to get metadata

해결책

- 1 vRealize Automation 장치의 콘솔에 루트로 로그인합니다.
- 2 텍스트 편집기에서 다음 파일을 엽니다.
`/etc/sysconfig/proxy`
- 3 VMware Identity Manager 로그인 시 프록시 서버를 무시하도록 NO_PROXY 줄을 업데이트합니다.
`NO_PROXY=vrealize-automation-hostname`
예: `NO_PROXY="localhost, 127.0.0.1, automation.mycompany.com"`
- 4 저장하고 프록시를 닫습니다.
- 5 다음 명령을 입력하여 Horizon 작업 공간 서비스를 다시 시작합니다.
`service horizon-workspace restart`

vRealize Automation 업그레이드 및 마이그레이션

현재 vRealize Automation 환경을 최신 버전으로 업그레이드할 수 있습니다.

인플레이스 업그레이드 및 단계별 업그레이드

현재 vRealize Automation 환경에 따라 인플레이스 업그레이드 또는 단계별 업그레이드를 수행하여 최신 버전으로 업그레이드할 수 있습니다. 사용자 환경에 가장 알맞은 업그레이드 방법을 결정하려면 이 페이지의 정보를 검토합니다.

인플레이스 업그레이드는 여러 단계의 프로세스입니다. 현재 환경에서 다양한 구성 요소를 업데이트하려면 특정 순서로 절차를 수행합니다. 모든 제품 구성 요소를 동일한 버전으로 업그레이드해야 합니다. 이러한 경로에 대해서는 인플레이스 업그레이드만 수행할 수 있습니다.

- vRealize Automation 6.2.5에서 7.5로
- vRealize Automation 7.1.x에서 7.5로
- vRealize Automation 7.2.x에서 7.5로
- vRealize Automation 7.3.x에서 7.5로
- vRealize Automation 7.4.x에서 7.5로

단계별 업그레이드는 현재 vRealize Automation 환경의 데이터를 최신 버전의 vRealize Automation으로 배포된 대상 환경으로 마이그레이션합니다. 이러한 경로에 대해 단계별 업그레이드를 수행할 수 있습니다.

- vRealize Automation 6.2.0~6.2.5에서 7.5로
- vRealize Automation 7.0 및 7.0.1에서 7.5로
- vRealize Automation 7.1.x, 7.2.x, 7.3.x, 7.4.x에서 7.5로

마이그레이션은 현재의 환경을 변경하지 않습니다. 현재 환경이 vCloud Director, vCloud Air와 통합되어 있거나 물리적 끝점이 있는 경우에는 마이그레이션을 사용하여 업그레이드해야 합니다. 마이그레이션은 대상 환경에서 지원되지 않는 모든 끝점 그리고 여기에 연결된 모든 항목을 제거합니다.

이 테이블에서 현재의 vRealize Automation 버전을 찾습니다. 오른쪽의 설명서를 사용하여 사용자의 vRealize Automation 환경을 최신 버전으로 업그레이드합니다.

표 1-43. 현재 vRealize Automation 릴리스에 지원되는 업그레이드 경로

현재 설치된 버전	증분 업그레이드에 대한 설명서
vRealize Automation 7.1.x, 7.2.x, 7.3.x 및 7.4.x	다음 항목 중 하나를 참조하십시오. <ul style="list-style-type: none"> ■ vRealize Automation 7.1 이상에서 7.5로 업그레이드 ■ vRealize Automation 마이그레이션
vRealize Automation 7.0 또는 7.0.1	vRealize Automation 마이그레이션 의 내용을 참조하십시오.
vRealize Automation 6.2.5	다음 항목 중 하나를 참조하십시오. <ul style="list-style-type: none"> ■ vRealize Automation 6.2.5를 7.5로 업그레이드 ■ vRealize Automation 마이그레이션
vRealize Automation 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.2.4	vRealize Automation 마이그레이션 의 내용을 참조하십시오.

이 테이블에는 이전 vCloud Automation Center 릴리스로부터의 업그레이드에 관한 정보가 나와 있습니다. 최신 vRealize Automation 버전으로 업그레이드하기 전에 vRealize Automation 6.2.5로 업그레이드해야 합니다. 5.x 및 6.x 버전의 vCloud Automation Center 및 vRealize Automation 설명서 링크는 <https://www.vmware.com/support/pubs/vcac-pubs.html>에서 찾을 수 있습니다.

표 1-44. vRealize Automation 6.2.5로의 지원되는 업그레이드 경로

현재 설치된 버전	증분 업그레이드에 대한 설명서
vCloud Automation Center 6.0	업그레이드 수행 순서: <ol style="list-style-type: none"> 1 "vCloud Automation Center 6.0에서 6.0.1로 업그레이드" 2 "vCloud Automation Center 6.1로 업그레이드" 3 "vRealize Automation 6.2.x로 업그레이드"
vCloud Automation Center 6.0.1	업그레이드 수행 순서: <ol style="list-style-type: none"> 1 "vCloud Automation Center 6.1로 업그레이드" 2 "vRealize Automation 6.2.x로 업그레이드"

표 1-44. vRealize Automation 6.2.5로의 지원되는 업그레이드 경로 (계속)

현재 설치된 버전	증분 업그레이드에 대한 설명서
vCloud Automation Center 6.1.x	"vRealize Automation 6.2.x로 업그레이드"
vRealize Automation 6.2.x	"vRealize Automation 6.2.x로 업그레이드"의 설명에 따라 6.2.5 릴리스로 직접 업그레이드

참고 6.2.0부터 vCloud Automation Center의 브랜드가 vRealize Automation으로 변경되었습니다. 사용자 인터페이스와 서비스 이름만 변경되었습니다. vcac가 포함된 디렉토리 이름과 프로그램 이름은 영향을 받지 않습니다.

6.2.x 환경에서 업그레이드하는 경우 이러한 항목을 검토합니다.

- VMware vRealize Production Test Upgrade Assessment Tool은 vRealize Automation 6.2.x 환경을 분석하여 업그레이드 문제를 일으킬 수 있는 기능 구성을 파악하고 환경이 업그레이드할 준비가 되었는지 확인합니다. 이 도구 및 관련 설명서를 다운로드하려면 [VMware vRealize Production Test Tool](#) 제품 다운로드 페이지로 이동하십시오.
- 6.2.x 환경에서 최신 버전의 vRealize Automation으로 업그레이드하면 여러 기능적 변경이 발생합니다. 자세한 내용은 이 [vRealize Automation 버전으로의 업그레이드에 대한 고려 사항](#) 항목을 참조하십시오.
- vRealize Automation 6.2.x 배포를 사용자 지정한 경우 업그레이드 고려 사항에 대한 추가 정보는 CCE 지원부 직원에게 문의하십시오.
- 업그레이드한 후 지원되지 않는 속성 사전 컨트롤은 vRealize Orchestrator 및 속성 사전 관계를 사용하여 복원될 수 있습니다.
- 소스 환경에 사용되지 않는 코드가 포함된 워크플로가 있는 경우 "vRealize Automation 확장성 마이그레이션 가이드"에서 이벤트 브로커 구독으로의 전환에 필요한 코드 변경 사항에 대한 자세한 내용을 참조하십시오. 이 문서는 [vRealize Automation 제품 설명서](#)의 "vRealize Automation에 대해 자세히 살펴보기" 섹션에 제공됩니다.

vRealize Automation 6.2.0에서 업그레이드할 때 알려진 문제를 방지하려면 업그레이드하기 전에 각 IaaS 웹 사이트 노드에서 다음 단계를 수행합니다. 이 문제는 6.2.0에만 영향을 미칩니다. 기타 6.2.x 버전에는 영향을 미치지 않습니다.

- 1 관리자 권한으로 메모장을 엽니다. [시작]에서 메모장 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

- 2 다음 파일을 엽니다.

C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\web.config

- 3 이 파일에서 다음 문을 찾습니다.

```
<!-- add key="DisableMessageSignatureCheck" value="false"-->
```

- 4 문에서 주석 처리를 제거하고 값을 false에서 true로 변경합니다.

```
<add key="DisableMessageSignatureCheck" value="true" />
```

5 파일을 저장합니다.

메모장에서 다른 이름으로 저장 창을 표시한다면 메모장을 관리자 권한으로 열지 않은 것이며, 이 경우 1단계로 이동해야 합니다.

6 관리자 권한으로 명령 프롬프트를 엽니다. [시작]에서 명령 프롬프트 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

7 재설정을 실행합니다.

8 모든 웹 사이트 노드에 대해 1~7단계를 반복합니다.

vRealize Automation 7.1 이상에서 7.5로 업그레이드

vRealize Automation 7.1 이상의 환경을 7.5로 업그레이드할 때 7.1 이상의 환경과 관련된 업그레이드 절차를 사용합니다.

이 정보는 vRealize Automation 7.1 이상을 7.5로 업그레이드하는 것과 관련되어 있습니다. 지원되는 다른 업그레이드 경로에 대한 자세한 내용은 [vRealize Automation 업그레이드 및 마이그레이션](#) 항목을 참조하십시오.

vRealize Automation 7.1.x에서 업그레이드

vRealize Automation 7.1.x를 이 vRealize Automation 릴리스로 업그레이드할 수 있습니다. 이 버전과 관련된 업그레이드 절차를 사용하여 환경을 업그레이드합니다.

인플레이스 업그레이드는 3단계의 프로세스입니다. 현재 환경의 구성 요소를 다음 순서로 업그레이드합니다.

1 vRealize Automation 장치

2 IaaS 웹 서버

3 vRealize Orchestrator 마이그레이션

모든 제품 구성 요소를 동일한 버전으로 업그레이드해야 합니다.

vRealize Automation 7.2부터 JFrog Artifactory Pro는 vRealize Automation 장치와 함께 제공되지 않습니다. vRealize Automation의 이전 버전에서 업그레이드하면 업그레이드 프로세스가 JFrog Artifactory Pro를 제거합니다. 자세한 내용은 [기술 자료 2147237](#)을 참조하십시오.

업그레이드하는 동안 managerservice.exe.config의 메시지 크기 및 최대 문자열에 대한 기존 수정 사항이 기본값(<binding name="ProxAgentBinding" maxReceivedMessageSize="13107200"> 및 <readerQuotas maxStringContentLength="13107200" />)으로 재설정됩니다. 업그레이드하기 전에 이러한 문자열의 값을 기록하고 그에 따라 업그레이드 후에 적절히 수정합니다.

vRealize Automation 업그레이드를 위한 사전 요구 사항

vRealize Automation 업그레이드 프로세스를 시작하기 전에 다음 사전 요구 사항을 검토합니다.

시스템 구성 요구 사항

업그레이드를 시작하기 전에 다음과 같은 사전 요구 사항을 충족하는지 확인합니다.

- 배포의 일부인 모든 장치와 서버가 최신 버전에 대한 시스템 요구 사항을 충족하는지 확인합니다. 자세한 내용은 [vRealize Automation 제품 설명서](#)에서 vRealize Automation 지원 매트릭스 링크를 참조하십시오.
- 다른 VMware 제품과의 호환성에 대한 자세한 내용은 VMware 웹 사이트에서 "VMware 제품 상호 운용성 매트릭스"를 참조하십시오. 자세한 내용은 [vRealize Automation 제품 설명서](#)에서 vRealize Automation 상호 운용성 매트릭스 링크를 참조하십시오.
- 업그레이드하려는 vRealize Automation의 작동 상태가 안정적인지 확인합니다. 업그레이드하기 전에 모든 문제를 해결합니다.
- 기본값에서 최소 10분으로 로드 밸런서 시간 초과 설정을 변경했는지 확인합니다.

하드웨어 구성 요구 사항

환경의 하드웨어가 업그레이드하는 대상 vRealize Automation 릴리스에 적합한지 확인합니다.

[vRealize Automation 하드웨어 규격 및 최대 용량](#)의 내용을 참조하십시오.

업그레이드를 시작하기 전에 다음과 같은 사전 요구 사항을 충족하는지 확인합니다.

- 업그레이드를 실행하기 전에 최소 18GB RAM, 4개의 CPU, Disk1 = 50GB, Disk3=25GB 및 Disk4=50GB가 있어야 합니다.

가상 시스템이 vCloud Networking and Security에 있는 경우 추가 RAM 공간을 할당해야 할 수 있습니다.

vCloud Networking and Security에 대한 일반 지원이 종료되었지만 VCNS 사용자 지정 속성은 NSX용으로 계속 유효합니다. [기술 자료 문서 2144733](#)을 참조하십시오.

- 다음 노드에는 최소 5GB의 여유 디스크 공간이 있어야 합니다.
 - 기본 IaaS 웹 사이트
 - Microsoft SQL 데이터베이스
 - Model Manager
- 업그레이드를 다운로드하고 실행하려면 다음과 같은 리소스가 있어야 합니다.
 - 루트 파티션에 최소 15 GB
 - 마스터 vRealize Automation 장치의 /storage/db 파티션에 5 GB
 - 각 복제 가상 장치의 루트 파티션에 15 GB
- 공간을 정리하려면 /storage/log 하위 폴더를 확인하고 오래된 ZIP 파일을 제거합니다.

일반 사전 요구 사항

업그레이드를 시작하기 전에 다음과 같은 사전 요구 사항을 충족하는지 확인합니다.

- 업그레이드 후에 이 파일에 대한 사용자 지정 업데이트가 재정의되기 때문에 업그레이드를 시작하기 전에 `setenv.sh` 파일을 백업하십시오. 이 파일은 `/usr/lib/vco/app-server/bin/setenv.sh`에 있습니다. 업그레이드 후에, 해당되는 경우 값을 업데이트하고 `vco-server`를 다시 시작하여 변경 내용을 적용합니다.
- vRealize Automation 업그레이드에 참여하거나 이 업그레이드에 의해 영향을 받는 모든 로드 밸런서 및 모든 데이터베이스에 대한 액세스 권한을 가지고 있습니다.
- 업그레이드를 수행하는 동안 사용자가 시스템을 사용할 수 없게 만듭니다.
- vRealize Automation을 쿼리하는 애플리케이션을 사용하지 않도록 설정합니다.
- Microsoft Distributed Transaction Coordinator(MSDTC)가 모든 vRealize Automation 및 연결된 SQL Server에서 사용하도록 설정되어 있는지 확인합니다. 자세한 내용은 [기술 자료 문서 2089503](#)을 참조하십시오.
- 포함된 PostgreSQL 데이터베이스가 구성되어 있는 분산 환경을 업그레이드하는 경우 다음 단계를 완료하십시오.
 - a 복제 호스트를 업그레이드하기 전에 마스터 호스트의 `pgdata` 디렉토리에 있는 파일을 검사합니다.
 - b 마스터 호스트의 PostgreSQL 데이터 폴더(`/var/vmware/vpostgres/current/pgdata/`)로 이동합니다.
 - c `pgdata` 디렉토리에서 `.swp` 파일을 모두 닫고 제거합니다. 접미사가 `.swp`인 파일은 VI 세션을 닫고 파일을 삭제해야 합니다.
 - d 이 디렉토리의 모든 파일에 올바른 소유 이름(`postgres:<owner-group>`)이 있는지 확인합니다.
- DynamicTypes 플러그인을 사용하는 경우 vRealize Orchestrator DynamicTypes 플러그인 구성을 패키지로 내보냅니다.
 - a Java Client에 관리자 사용자로 로그인합니다.
 - b 워크플로 탭을 선택합니다.
 - c 라이브러리 > 동적 유형 > 구성을 선택합니다.
 - d 패키지로 구성 내보내기 워크플로를 선택하고 실행합니다.
 - e 설정 안 함 > 값 삽입을 클릭합니다.
 - f 내보낼 네임 스페이스를 선택하고 **추가**를 클릭하여 패키지에 추가합니다.
 - g **제출**을 클릭하여 패키지를 내보냅니다.

또한 사용자 지정 속성의 이름에 공백이 없는지 확인합니다. 업그레이드된 vRealize Automation 설치에서 사용자 지정 속성을 인식할 수 있으려면 이 vRealize Automation 릴리스로 업그레이드하기 전에 공백을 밑줄 문자로 바꾸는 방법처럼 사용자 지정 속성 이름에서 모든 공백 문자를 제거해야 합니다. vRealize Automation 사용자 지정 속성 이름은 공백을 포함할 수 없습니다. 이 문제는 vRealize Automation, vRealize Orchestrator 또는 둘 모두의 이전 릴리스에서 공백이 포함된 사용자 지정 속성을 사용하던 업그레이드된 vRealize Orchestrator 설치의 사용에 영향을 줄 수 있습니다.

vRealize Automation 업그레이드 검사 목록

vRealize Automation 7.x 이상을 업그레이드할 때는 모든 vRealize Automation 구성 요소를 특정 순서로 업데이트합니다.

업그레이드 순서는 최소 환경 업그레이드인지 아니면 여러 vRealize Automation 장치를 포함하는 분산 환경 업그레이드인지에 따라 다릅니다.

업그레이드가 완료되면 검사 목록을 사용하여 관련 작업을 추적하십시오. 작업은 제시된 순서대로 완료하십시오.

표 1-45. vRealize Automation 최소 환경 업그레이드를 위한 검사 목록

작업	지침
<input type="checkbox"/> 업그레이드하기 전에 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행합니다. 이 단계는 vRealize Automation이 NSX와 통합된 경우에만 필요합니다.	vRealize Automation 업그레이드 전에 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행 항목을 참조하십시오.
<input type="checkbox"/> 현재 설치를 백업합니다. 중요한 단계입니다.	시스템을 백업하고 복원하는 방법에 대한 자세한 내용은 기존 vRealize Automation 환경 백업 항목을 참조하십시오. 일반 정보는 http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf 의 "Symantec Netbackup을 사용하여 백업 및 복원 구성"을 참조하십시오.
<input type="checkbox"/> vRealize Automation 장치에 대한 업데이트를 다운로드합니다.	vRealize Automation 장치 업데이트 다운로드 항목을 참조하십시오.
<input type="checkbox"/> vRealize Automation 장치 및 IaaS 구성 요소에 업데이트를 설치합니다.	vRealize Automation 장치 및 IaaS 구성 요소에 업데이트 설치의 내용을 참조하십시오.

표 1-46. vRealize Automation 분산 환경 업그레이드를 위한 검사 목록

작업	지침
<input type="checkbox"/> vRealize Automation 7.x를 업그레이드하기 전에 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행합니다. 이 작업은 vRealize Automation이 NSX와 통합된 경우에만 필요합니다.	vRealize Automation 업그레이드 전에 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행 항목을 참조하십시오.
<input type="checkbox"/> 현재 설치를 백업합니다. 중요한 단계입니다.	시스템을 백업하고 복원하는 방법에 대한 자세한 내용은 기존 vRealize Automation 환경 백업 항목을 참조하십시오. 자세한 내용은 http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf 의 "Symantec Netbackup을 사용하여 백업 및 복원 구성"을 참조하십시오.

표 1-46. vRealize Automation 분산 환경 업그레이드를 위한 검사 목록 (계속)

작업	지침
<input type="checkbox"/> vRealize Automation 7.3.x에서 업그레이드하는 경우 PostgreSQL 자동 페일오버를 사용하지 않도록 설정합니다.	vRealize Automation PostgreSQL 복제 모드를 비동기식으로 설정 항목을 참조하십시오.
<input type="checkbox"/> vRealize Automation 장치에 대한 업데이트를 다운로드합니다.	vRealize Automation 장치 업데이트 다운로드 항목을 참조하십시오.
<input type="checkbox"/> 로드 밸런서를 사용하지 않도록 설정합니다.	<p>각 보조 노드를 사용하지 않도록 설정하고 다음 항목에 대한 vRealize Automation 상태 모니터를 제거합니다.</p> <ul style="list-style-type: none"> ■ vRealize Automation 장치 ■ IaaS 웹 사이트 ■ IaaS Manager Service <p>업그레이드를 완료하려면 다음 항목을 확인합니다.</p> <ul style="list-style-type: none"> ■ 로드 밸런서 트래픽이 기본 노드로만 전달됩니다. ■ 장치, 웹 사이트 및 Manager Service에 대한 vRealize Automation 상태 모니터가 제거되었습니다.
<input type="checkbox"/> 마스터 vRealize Automation 장치 및 IaaS 구성 요소에 업데이트를 설치합니다.	vRealize Automation 장치 및 IaaS 구성 요소에 업데이트 설치 항목을 참조하십시오.
참고 분산 환경의 마스터 장치에 업데이트를 설치해야 합니다.	
<input type="checkbox"/> 로드 밸런서를 사용하도록 설정합니다.	로드 밸런서 사용

vRealize Automation 환경 사용자 인터페이스

몇 가지 인터페이스로 vRealize Automation 환경을 사용하고 관리합니다.

사용자 인터페이스

다음 테이블은 vRealize Automation 환경을 관리하는 데 사용하는 인터페이스를 설명합니다.

표 1-47. vRealize Automation 관리 콘솔

용도	액세스	필요한 자격 증명
vRealize Automation 콘솔을 사용하여 다음과 같은 시스템 관리자 작업을 수행합니다.	1 브라우저로 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 장치 시작 페이지를 엽니다.	시스템 관리자 역할을 가진 사용자여야 합니다.
<ul style="list-style-type: none"> ■ 테넌트를 추가합니다. ■ vRealize Automation 사용자 인터페이스 사용자 지정합니다. ■ 이메일 서버를 구성합니다. ■ 이벤트 로그를 봅니다. ■ vRealize Orchestrator를 구성합니다. 	<p>https://vrealize-automation-appliance-FQDN.</p> <p>2 vRealize Automation 콘솔을 클릭합니다.</p> <p>다음 URL을 사용하여 vRealize Automation 콘솔을 열 수도 있습니다. https://vrealize-automation-appliance-FQDN/vcac</p> <p>3 로그인합니다.</p>	

표 1-48. vRealize Automation 테넌트 콘솔. 이 인터페이스는 서비스와 리소스를 생성하고 관리하는 데 사용되는 기본 사용자 인터페이스입니다.

용도	액세스	필요한 자격 증명
<p>vRealize Automation을 사용하여 다음과 같은 작업을 수행합니다.</p> <ul style="list-style-type: none"> ■ 새 IT 서비스 Blueprint를 요청합니다. ■ 클라우드 및 IT 리소스를 생성하고 관리합니다. ■ 사용자 지정 그룹을 생성하고 관리합니다. ■ 비즈니스 그룹을 만들고 관리합니다. ■ 사용자에게 역할을 할당합니다. 	<ol style="list-style-type: none"> 1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름과 테넌트 URL 이름을 사용하여 테넌트의 URL을 입력합니다. https://vrealize-automation-appliance-FQDN/vcac/org/tenant_URL_name . 2 로그인합니다. 	<p>다음 역할 중 하나 이상을 가진 사용자여야 합니다.</p> <ul style="list-style-type: none"> ■ 애플리케이션 설계자 ■ 승인 관리자 ■ 카탈로그 관리자 ■ 컨테이너 관리자 ■ 컨테이너 설계자 ■ 상태 소비자 ■ 인프라 설계자 ■ 소비자 보안 내보내기 ■ 소프트웨어 설계자 ■ 테넌트 관리자 ■ XaaS 설계자

표 1-49. vRealize Automation 장치 관리 인터페이스.

용도	액세스	필요한 자격 증명
<p>vRealize Automation 장치 관리를 사용하여 다음과 같은 작업을 수행합니다.</p> <ul style="list-style-type: none"> ■ 등록된 서비스의 상태를 봅니다. ■ 시스템 정보를 보고 장치를 재부팅하거나 종료합니다. ■ 고객 환경 향상 프로그램에 대한 참여를 관리합니다. ■ 네트워크 상태를 봅니다. ■ 업데이트 상태를 보고 업데이트를 설치합니다. ■ 관리 설정을 관리합니다. ■ vRealize Automation 호스트 설정을 관리합니다. ■ SSO 설정을 관리합니다. ■ 제품 라이선스를 관리합니다. ■ vRealize Automation Postgres 데이터베이스를 구성합니다. ■ vRealize Automation 메시징을 구성합니다. ■ vRealize Automation 로깅을 구성합니다. ■ IaaS 구성 요소를 설치합니다. ■ 기존 vRealize Automation 설치에서 마이그레이션합니다. ■ IaaS 구성 요소 인증서를 관리합니다. ■ Xenon 서비스를 구성합니다. 	<ol style="list-style-type: none"> 1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 장치 시작 페이지를 엽니다. <code>https://vrealize-automation-appliance-FQDN</code> 2 vRealize Automation 장치 관리를 클릭합니다. 다음 URL을 사용하여 vRealize Automation 장치 관리 인터페이스를 열 수도 있습니다. <code>https://vrealize-automation-appliance-FQDN:5480</code> 3 로그인합니다. 	<ul style="list-style-type: none"> ■ 사용자 이름: root ■ 암호: vRealize Automation 장치를 배포할 때 입력한 암호.

표 1-50. vRealize Orchestrator 클라이언트

용도	액세스	필요한 자격 증명
<p>vRealize Orchestrator 클라이언트를 사용하여 다음과 같은 작업을 수행합니다.</p> <ul style="list-style-type: none"> ■ 작업을 개발합니다. ■ 워크플로를 개발합니다. ■ 정책을 관리합니다. ■ 패키지를 설치합니다. ■ 사용자 및 사용자 그룹 사용 권한을 관리합니다. ■ URI 개체에 태그를 연결합니다. ■ 인벤토리를 봅니다. 	<ol style="list-style-type: none"> 1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 시작 페이지를 엽니다. <code>https://vrealize-automation-appliance-FQDN</code> 2 로컬 컴퓨터에 client.jnlp 파일을 다운로드하려면 vRealize Orchestrator Client를 클릭합니다. 3 client.jnlp 파일을 마우스 오른쪽 버튼으로 클릭하고 시작을 선택합니다. 4 [계속하시겠습니까?] 대화 상자에서 계속을 클릭합니다. 5 로그인합니다. 	<p>vRealize Orchestrator 제어 센터 인증 제공자 설정에 구성된 vcoadmins 그룹에 속하거나 시스템 관리자 역할이 있는 사용자여야 합니다.</p>

표 1-51. vRealize Orchestrator 제어 센터

용도	액세스	필요한 자격 증명
vRealize Orchestrator 제어 센터를 사용하여 vRealize Automation에 내장된 기본 vRealize Orchestrator 인스턴스의 구성을 편집합니다.	<ol style="list-style-type: none"> 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 장치 시작 페이지를 엽니다. <code>https://vrealize-automation-appliance-FQDN</code> vRealize Automation 장치 관리를 클릭합니다. 다음 URL을 사용하여 vRealize Automation 장치 관리 인터페이스를 열 수도 있습니다. <code>https://vrealize-automation-appliance-FQDN:5480</code> 로그인합니다. vRA > Orchestrator를 클릭합니다. Orchestrator 사용자 인터페이스를 선택합니다. 시작을 클릭합니다. Orchestrator 사용자 인터페이스 URL을 클릭합니다. 로그인합니다. 	<p>사용자 이름</p> <ul style="list-style-type: none"> 역할 기반 인증이 구성되지 않은 경우 root를 입력합니다. 역할 기반 인증에 대해 구성된 경우 vRealize Automation 사용자 이름을 입력합니다. <p>암호</p> <ul style="list-style-type: none"> 역할 기반 인증이 구성되지 않은 경우 vRealize Automation 장치를 배포했을 때 입력한 암호를 입력합니다. 사용자 이름이 역할 기반 인증에 대해 구성된 경우 사용자 이름에 대한 암호를 입력합니다.

표 1-52. Linux 명령 프롬프트

용도	액세스	필요한 자격 증명
<p>호스트(예: vRealize Automation 장치 호스트)에서 Linux 명령 프롬프트를 사용하여 다음과 같은 작업을 수행합니다.</p> <ul style="list-style-type: none"> 서비스 중지 또는 시작 구성 파일 편집 명령 실행 데이터 검색 	<ol style="list-style-type: none"> vRealize Automation 장치 호스트에서 명령 프롬프트를 엽니다. 로컬 컴퓨터에서 명령 프롬프트를 여는 한 가지 방법은 PuTTY와 같은 애플리케이션을 사용하여 호스트에서 세션을 시작하는 것입니다. 로그인합니다. 	<ul style="list-style-type: none"> 사용자 이름: root 암호: vRealize Automation 장치를 배포할 때 생성한 암호.

표 1-53. Windows 명령 프롬프트

용도	액세스	필요한 자격 증명
호스트(예: IaaS 호스트)에서 Windows 명령 프롬프트를 사용하여 스크립트를 실행할 수 있습니다.	<ol style="list-style-type: none"> IaaS 호스트에서 Windows에 로그인합니다. 로컬 컴퓨터에서 로그인하는 한 가지 방법은 원격 데스크톱 세션을 시작하는 것입니다. Windows 명령 프롬프트를 엽니다. 명령 프롬프트를 여는 한 가지 방법은 호스트에서 [시작] 아이콘을 마우스 오른쪽 버튼으로 클릭하고 명령 프롬프트 또는 명령 프롬프트(관리자)를 선택하는 것입니다. 	<ul style="list-style-type: none"> 사용자 이름: 관리자 권한이 있는 사용자. 암호: 사용자의 암호.

vRealize Automation에 통합된 VMware 제품 업그레이드

vRealize Automation을 업그레이드할 때는 vRealize Automation 환경에 통합되어 있는 모든 VMware 제품을 관리해야 합니다.

vRealize Automation 환경이 하나 이상의 추가적인 제품과 통합되어 있으면 추가적인 제품을 업데이트하기 전에 vRealize Automation부터 업그레이드해야 합니다. vRealize Business for Cloud가 vRealize Automation과 통합되어 있는 경우에는 vRealize Automation을 업그레이드하기 전에 vRealize Business for Cloud를 등록 취소해야 합니다.

vRealize Automation을 업그레이드하는 경우에 통합된 제품을 관리하기 위해 제안된 워크플로를 따르십시오.

- 1 vRealize Automation을 업그레이드합니다.
- 2 VMware vRealize Operations Manager를 업그레이드합니다.
- 3 VMware vRealize Log Insight를 업그레이드합니다.
- 4 VMware vRealize Business for Cloud를 업그레이드합니다.

이 섹션에서는 vRealize Automation 환경에 통합되어 있는 vRealize Business for Cloud를 관리하기 위한 추가적인 지침을 제공합니다.

vRealize Automation에 통합된 vRealize Operations Manager 업그레이드

vRealize Automation을 업그레이드한 후에 vRealize Operations Manager를 업그레이드합니다.

절차

- 1 vRealize Automation을 업그레이드합니다.
- 2 vRealize Operations Manager를 업그레이드합니다. 자세한 내용은 [VMware vRealize Operations Manager 설명서](#)에서 "소프트웨어 업데이트" 항목을 참조하십시오.

vRealize Automation에 통합된 vRealize Log Insight 업그레이드

vRealize Automation을 업그레이드한 후에 vRealize Log Insight를 업그레이드합니다.

절차

- 1 vRealize Automation을 업그레이드합니다.
- 2 vRealize Log Insight를 업그레이드합니다. 자세한 내용은 [VMware vRealize Log Insight 설명서](#)에서 "vRealize Log Insight 업그레이드" 항목을 참조하십시오.

vRealize Automation에 통합된 vRealize Business for Cloud 업그레이드

vRealize Automation 환경을 업그레이드할 경우 vRealize Business for Cloud에 대한 연결을 등록 취소하고 등록해야 합니다.

vRealize Automation 환경을 업그레이드할 때 vRealize Business for Cloud 서비스를 지속적으로 실행하려면 이 절차를 수행하십시오.

절차

- 1 vRealize Automation에서 vRealize Business for Cloud를 등록 취소합니다. 자세한 내용은 [VMware vRealize Business for Cloud 설명서](#)에서 "vRealize Automation에서 vRealize Business for Cloud 등록 취소" 항목을 참조하십시오.
- 2 vRealize Automation을 업그레이드합니다.
- 3 필요한 경우 vRealize Business for Cloud를 업그레이드합니다. [VMware vRealize Business for Cloud 설명서](#)에서 "vRealize Business for Cloud 업그레이드" 항목을 참조하십시오.
- 4 vRealize Business for Cloud를 vRealize Automation에 등록합니다. [VMware vRealize Business for Cloud 설명서](#)에서 "vRealize Automation에 vRealize Business for Cloud 등록" 항목을 참조하십시오.

vRealize Automation 업그레이드 준비

vRealize Automation 7.x에서 업그레이드하기 전에 다음 작업을 수행합니다.

검사 목록에 나와 있는 순서대로 이러한 작업을 완료합니다. [vRealize Automation 업그레이드 검사 목록](#) 항목을 참조하십시오.

vRealize Automation 업그레이드 전에 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행

vRealize Automation 7.1 이상을 업그레이드하기 전에 업그레이드하는 소스 vRealize Automation 7.1 이상 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행해야 합니다.

이 데이터 수집은 vRealize Automation 배포에서 로드 밸런서 재구성 작업을 수행하는 데 필요합니다.

절차

- ◆ 업그레이드를 시작하기 전에 업그레이드하는 소스 vRealize Automation 7.1 이상 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행합니다. 자세한 내용은 [끝점 데이터 수집 수동 시작](#) 항목을 참조하십시오.

다음에 수행할 작업

[vRealize Automation 업그레이드를 위한 백업 사전 요구 사항](#).

vRealize Automation 업그레이드를 위한 백업 사전 요구 사항

업그레이드를 시작하기 전에 백업 사전 요구 사항을 완료합니다.

사전 요구 사항

- 소스 환경이 완전하게 설치되고 구성되었는지 확인합니다.
- vSphere Client에 로그인하고 소스 환경의 각 장치에 대해 다음 디렉토리의 모든 vRealize Automation 장치 구성 파일을 백업합니다.
 - /etc/vcac/
 - /etc/vco/

- /etc/apache2/
- /etc/rabbitmq/
- IaaS Microsoft SQL Server 데이터베이스를 백업합니다. 자세한 내용을 보려면 [Microsoft Developer Network](#)에서 전체 SQL Server 데이터베이스 백업 생성에 대한 문서를 검색하십시오.
- DataCenterLocations.xml과 같은 사용자 지정된 모든 파일을 백업합니다.
- 가상 장치 및 IaaS 서버에 대해 각각 스냅샷을 생성합니다. vRealize Automation 업그레이드가 실패할 경우에 대비하여 전체 시스템 백업을 위한 일반 지침을 따르십시오. [vRealize Automation 설치에 대한 백업 및 복구](#)를 참조하십시오.

기존 vRealize Automation 환경 백업

업데이트에 실패하면 스냅샷을 사용하여 마지막으로 확인된 정상 구성으로 되돌리고 다른 업그레이드를 시도합니다.

사전 요구 사항

vRealize Automation 7.1 이상에서 업그레이드하기 전에 시스템을 종료하고 Windows 노드의 vRealize Automation IaaS 서버와 Linux 노드의 vRealize Automation 장치에 대해 각각 스냅샷을 생성하십시오.

- [vRealize Automation 업그레이드를 위한 백업 사전 요구 사항](#).
- PostgreSQL 데이터베이스는 고가용성 모드로 구성되어 있습니다. vRealize Automation 장치 관리 인터페이스에 로그인하고 **클러스터**를 선택하여 현재 마스터 노드를 찾습니다. 데이터베이스 구성이 외부 데이터베이스로 나열되면 이 외부 데이터베이스의 수동 백업을 생성합니다.
- vRealize Automation Microsoft SQL 데이터베이스가 IaaS 서버에서 호스팅되지 않는 경우 데이터베이스 백업 파일을 생성합니다.
- 업그레이드를 위한 백업 사전 요구 사항을 충족했는지 확인합니다.
- 시스템이 종료되는 동안 시스템의 스냅샷을 생성했는지 확인합니다. 이는 기본 스냅샷 생성 방법입니다. 스냅샷 생성 및 관리에 대한 자세한 내용은 [vSphere 제품 설명서](#)를 참조하십시오.

참고 vRealize Automation 장치와 IaaS 구성 요소를 백업할 때 메모리 내 스냅샷과 중지된 스냅샷을 사용하지 않도록 설정하십시오.

- IaaS 서버에서 *.exe.config(예: managervice.exe.config) 파일을 수정한 경우 이 파일의 백업을 만듭니다. [app.config 파일에 로깅 변경 내용 복원](#) 항목을 참조하십시오.
- 외부 워크플로 구성(xmlldb) 파일의 백업을 만듭니다. [외부 워크플로 시간 초과 파일 복원](#) 항목을 참조하십시오.
- 현재 폴더 외부에 백업 파일을 저장할 수 있는 위치가 있는지 확인합니다. [.xml 파일 백업 복사본으로 인한 시스템 시간 초과](#) 항목을 참조하십시오.

절차

- 1 vSphere 클라이언트에 로그인합니다.

- 2 각 vRealize Automation IaaS Windows 시스템과 각 vRealize Automation 장치 노드를 찾습니다.
- 3 데이터 무결성을 유지하려면 특정 순서로 종료해야 합니다. 가상 시스템 관리를 위해 vCenter Server를 사용 중인 경우 vRealize Automation을 종료하려면 게스트 **shutdown** 명령을 사용합니다.
[vRealize Automation 종료](#)를 참조하여 지정된 순서를 따르십시오.
- 4 각 vRealize Automation 시스템에 대한 스냅샷을 생성합니다.
- 5 원하는 백업 방법을 사용하여 각 장치 노드의 전체 백업을 생성합니다.
- 6 정전이나 제어된 종료 이후 또는 복구를 마친 후에 처음으로 vRealize Automation을 시작하는 경우에는 구성 요소를 지정된 순서로 시작해야 합니다. 자세한 내용은 [vRealize Automation 시작](#)을 참조하십시오.
- 7 각 vRealize Automation 장치 관리 콘솔에 로그인하고 시스템이 제대로 작동하는지 확인합니다.
 - a 서비스를 클릭합니다.
 - b 각 서비스가 [등록됨] 상태인지 확인합니다.

다음에 수행할 작업

[vRealize Automation PostgreSQL 복제 모드를 비동기식으로 설정](#).

vRealize Automation PostgreSQL 복제 모드를 비동기식으로 설정

PostgreSQL 동기식 복제 모드에서 작동하는 분산 vRealize Automation 환경에서 업그레이드하는 경우 업그레이드 전에 복제 모드를 비동기식으로 변경해야 합니다.

사전 요구 사항

업그레이드하려는 분산 vRealize Automation 환경이 있습니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 **클러스터**를 클릭합니다.
- 3 **비동기식 모드**를 클릭하고 작업이 완료될 때까지 기다립니다.
- 4 [동기화 상태] 열의 모든 노드가 비동기화 상태를 표시하는지 확인합니다.

다음에 수행할 작업

[vRealize Automation 장치 업데이트 다운로드](#)

vRealize Automation 장치 업데이트 다운로드

vRealize Automation 장치 관리 인터페이스에서 업데이트를 확인하고 다음 방법 중 하나를 사용하여 업데이트를 다운로드할 수 있습니다.

업그레이드 성능을 최적화하려면 ISO 파일 방법을 사용합니다. 최적의 업그레이드 성능을 위해 또는 RPM 파일을 다운로드하는 인터넷 액세스가 제한되어있는 경우, ISO 파일 메서드를 사용하여 update_repo.iso를 로컬 데이터스토어로 가져옵니다.

장치 업그레이드 시 발생 가능한 문제를 방지하기 위해 또는 장치 업그레이드 중 문제가 발생한 경우 [VMware 기술 자료 문서 "vRealize Orchestrator 데이터베이스의 중복 항목으로 인한 vRealize Automation 업그레이드 실패\(54987\)"](#)를 참조하십시오.

CD-ROM 드라이브에서 사용할 가상 장치 업데이트 다운로드

가상 CD-ROM 드라이브에서 장치가 읽어 들이는 ISO 파일로 가상 장치를 업데이트할 수 있습니다. 이것이 기본 방법입니다.

ISO 파일을 다운로드하고, 이 파일을 사용하여 장치를 업그레이드하도록 기본 장치를 설정합니다.

사전 요구 사항

- 기존 vRealize Automation 환경을 백업합니다.
- vRealize Automation 장치를 업데이트하기 전에 업그레이드에 사용할 모든 CD-ROM 드라이브가 사용되도록 설정되었는지 확인합니다. vSphere Client의 가상 시스템에 CD-ROM 드라이브를 추가하는 데 대한 내용은 vSphere 설명서를 참조하십시오.

절차

- 1 업데이트 저장소 ISO 파일을 다운로드합니다.
 - a 브라우저를 시작하고 [vRealize Automation 제품 페이지](http://www.vmware.com)(www.vmware.com)로 이동합니다.
 - b 이 페이지에서 **vRealize Automation 다운로드**를 클릭하여 VMware 다운로드 페이지로 이동합니다.
 - c 적절한 파일을 다운로드합니다.
- 2 시스템에 다운로드된 파일을 찾아 파일 크기가 VMware 다운로드 페이지의 파일과 같은지 확인합니다. 다운로드 페이지에 제공된 체크섬을 사용하여 다운로드 파일의 무결성을 검증합니다. 자세한 내용은 VMware 다운로드 페이지 아래쪽에 있는 링크를 참조하십시오.
- 3 기본 가상 장치의 전원이 켜져 있는지 확인합니다.
- 4 기본 가상 장치의 CD-ROM 드라이브를 다운로드한 ISO 파일에 연결합니다.

참고 ISO 파일이 가상 시스템에 연결된 후 업데이트를 확인할 수 없으면, 장치에 로그인하고 `mount /dev/sr0 /media/cdrom` 파일 경로를 사용하여 Linux 내에 CD-ROM을 마운트합니다.

- 5 기본 vRealize Automation 장치에서 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **root**로 vRealize Automation 장치 관리에 로그인합니다.
- 6 **업데이트** 탭을 클릭합니다.
- 7 **설정**을 클릭합니다.
- 8 [업데이트 저장소] 아래에서 **CD-ROM 업데이트 사용**을 선택합니다.
- 9 **설정 저장**을 클릭합니다.

VMware 저장소에서 vRealize Automation 장치 업데이트 다운로드

vmware.com 웹 사이트의 공용 저장소에서 vRealize Automation 장치에 대한 업데이트를 다운로드할 수 있습니다.

사전 요구 사항

- 기존 vRealize Automation 환경을 백업합니다.
- vRealize Automation 장치의 전원이 켜져 있는지 확인합니다.

절차

- 1 기본 vRealize Automation 장치에서 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **root**로 vRealize Automation 장치 관리에 로그인합니다.
- 2 **업데이트** 탭을 클릭합니다.
- 3 **설정**을 클릭합니다.
- 4 (선택 사항) [자동 업데이트] 패널에서 업데이트 확인 주기를 설정합니다.
- 5 [업데이트 저장소] 패널에서 **기본 저장소 사용**을 선택합니다.
기본 저장소는 정확한 VMware.com URL로 설정됩니다.
- 6 **설정 저장**을 클릭합니다.

Postgres 데이터베이스 정리

업그레이드 또는 마이그레이션을 위해 Postgres 데이터베이스를 준비하려면 데이터베이스 정리를 수행하십시오.

로그 및 원격 분석 번들을 저장하는 `pg_largeobject` 테이블의 큰 개체와 애플리케이션 개체는 업그레이드 또는 마이그레이션을 느리게 하거나 중지할 수 있습니다. 업그레이드 또는 마이그레이션을 시도하기 전에 `vacuum` 데이터베이스 정리를 수행하여 Postgres 데이터베이스를 준비할 수 있습니다.

참고 서비스가 실행 중일 때는 데이터베이스 정리를 수행할 수 없습니다.

절차

- 1 VAMI의 클러스터 페이지에서 Postgres 데이터베이스 덤프를 생성하거나 마스터 가상 장치의 백업/스냅샷을 생성하여 장치 백업부터 시작합니다.
- 2 vRA VAMI에서 복제를 동기화에서 비동기로 전환합니다.
- 3 마스터 vRA의 Postgres 사용자(`su-postgres`)로, 데이터베이스에 `vacuum`을 실행하여 로그 항목을 제거합니다.

```
su - postgres -c "/opt/vmware/vpostgres/current/bin/vacuumlo -v -p 5432 vcac"
```

```
su - postgres -c "/opt/vmware/vpostgres/current/bin/vacuumdb -f -p 5432 -t pg_largeobject  
-t pg_largeobject_metadata vcac"
```

4 데이터베이스 공간을 회수하려면 `vacuum full` 명령을 사용합니다.

```
psql -d vcac
vacuum full
vacuum analyze
```

vRealize Automation 장치 및 IaaS 구성 요소 업데이트

업그레이드 사전 요구 사항을 완료하고 가상 장치 업데이트를 다운로드한 후 업데이트를 설치합니다.

최소 환경인 경우 vRealize Automation 장치에 업데이트를 설치합니다. 분산 환경인 경우 마스터 장치 노드에 업데이트를 설치합니다. 업데이트를 완료하는 데 필요한 시간은 환경 및 네트워크에 따라 다릅니다. 업데이트가 완료되면 vRealize Automation 장치 관리의 [업데이트 상태] 페이지에 변경 내용이 표시됩니다. 장치 업데이트가 완료되면 장치를 재부팅해야 합니다. 분산 환경에서 마스터 장치를 재부팅하면 각 복제 노드가 재부팅됩니다.

재부팅 후에는 [업데이트 상태] 페이지에 VA 서비스 시작을 기다리는 중이 표시됩니다. 시스템이 완전하게 초기화되고 모든 서비스가 실행 중이면 IaaS 업데이트가 시작됩니다. IaaS 업데이트 진행률은 [업데이트 상태] 페이지에서 볼 수 있습니다. 첫 번째 IaaS 서버 구성 요소를 완료하는 데 30분 정도 소요될 수 있습니다. 업그레이드 중에는 `web1-vra.mycompany.com` 노드의 서버 구성 요소 업그레이드 중과 유사한 메시지가 표시됩니다.

각 Manager Service 노드에 대한 업그레이드 프로세스 마지막에는 `mgr-vra.mycompany.com` 노드에 대해 ManagerService 자동 페일오버 모드를 사용하도록 설정하는 중과 유사한 메시지가 표시됩니다. vRealize Automation 7.3부터, 어떤 노드가 페일오버 서버로 지정되는지에 대해 액티브 Manager Service 노드의 수동 선택 방식이 시스템 자동 선택 방식으로 변경됩니다. 이 기능은 업그레이드 중에 사용하도록 설정됩니다. 이 기능과 관련해서 문제가 있는 경우에는 [업데이트를 통한 관리 에이전트 업그레이드 실패](#) 항목을 참조하십시오.

vRealize Automation 장치 및 IaaS 구성 요소에 업데이트 설치

소스 vRealize Automation 가상 장치에 업데이트를 설치하여 vRealize Automation과 IaaS 구성 요소를 대상 vRealize Automation 릴리스로 업그레이드할 수 있습니다.

업데이트를 설치하는 동안 vRealize Automation 장치 관리 인터페이스를 닫지 마십시오.

업그레이드 프로세스 중 문제가 발생하는 경우 [vRealize Automation 업그레이드 문제 해결](#) 항목을 참조하십시오.

참고 IaaS 가상 시스템에서 관리 에이전트를 업그레이드하는 동안 VMware 공용 인증서가 신뢰할 수 있는 게시자 인증서 저장소에 일시적으로 설치됩니다. 관리 에이전트 업그레이드 프로세스에는 이 인증서로 서명된 PowerShell 스크립트가 사용됩니다. 업그레이드가 완료되면 이 인증서가 인증서 저장소에서 제거됩니다.

사전 요구 사항

- 다운로드 방법을 선택했고 해당 방법의 절차를 완료했는지 확인합니다. [vRealize Automation 장치 업데이트 다운로드](#) 항목을 참조하십시오.

- 모든 고가용성 환경의 경우 **기존 vRealize Automation 환경 백업** 항목을 참조하십시오.
- 로드 밸런서가 있는 환경의 경우, 모든 중복 노드를 사용하지 않도록 설정하고 상태 모니터를 제거했는지 확인합니다. 자세한 내용은 로드 밸런서 설명서를 참조하십시오.
 - vRealize Automation 장치
 - IaaS 웹 사이트
 - IaaS Manager Service

참고 vRealize Automation 7.4 이상에서 자동 업그레이드를 수행하는 경우 보조 IaaS 웹 로드 밸런서 모니터를 사용하지 않도록 설정할 필요가 없습니다. 업그레이드하기 전에 IaaS Manager Server 로드 밸런서 모니터를 사용하지 않도록 설정하지 마십시오. 기존 IaaS 설치 관리자를 사용하여 IaaS 노드를 수동으로 업그레이드하는 경우 업그레이드하기 전에 보조 웹 노드에 대한 트래픽을 사용하지 않도록 설정해야 합니다.

- 로드 밸런서가 포함된 환경의 경우, 트래픽이 기본 노드로만 전달되는지 확인합니다.
- 다음 단계를 수행하여 Microsoft IIS(인터넷 정보 서비스)에서 호스팅된 IaaS 서비스가 실행되고 있는지 확인합니다.
 - a 브라우저를 시작하고 URL **https://webhostname/Repository/Data/MetaModel.svc**를 입력하여 웹 저장소가 실행 중인지 확인합니다. 성공한 경우 오류가 반환되지 않으며 모델 목록이 XML 형식으로 표시됩니다.
 - b IaaS 웹 사이트에 로그인하고 **Repository.log** 파일에 기록된 상태를 검사하여 정상 상태가 보고되었는지 확인합니다. 해당 파일은 **/Server/Model Manager Web/Logs/Repository.log**의 VCAC 홈 폴더에 있습니다.

참고 분산 IaaS 웹 사이트인 경우 MMD 없이 보조 웹 사이트에 로그인하고 Microsoft IIS를 일시적으로 중지합니다. 로드 밸런서 트래픽이 기본 웹 노드를 통해서만 전달되도록 하려면 **MetaModel.svc** 연결을 선택하고 Microsoft IIS를 다시 시작합니다.

- 다음 단계를 수행하여 모든 IaaS 노드가 정상 상태인지 확인합니다.
 - a vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
https://vrealize-automation-appliance-FQDN:5480
 - b **클러스터**를 선택합니다.
 - c **최근 연결**에서 다음을 확인합니다.

- 테이블의 IaaS 노드의 최근 연결 시간이 30초 미만입니다.
- 가상 장치 노드의 최근 연결 시간이 10분 미만입니다.

IaaS 노드가 vRealize Automation 장치와 통신하지 않으면 업그레이드에 실패합니다.

관리 에이전트와 가상 장치 사이의 연결 문제를 진단하려면 다음 단계를 수행합니다.

- 1 목록에 없거나 **최근 연결** 시간이 30초를 초과하는 각 IaaS 노드에 로그인합니다.

- 2 관리 에이전트 로그에 오류가 기록되었는지 검사합니다.
 - 3 관리 에이전트가 실행 중이 아니면 서비스 콘솔에서 에이전트를 다시 시작합니다.
- d 테이블에 나열된 분리된 노드를 확인합니다. 분리된 노드는 호스트에서 보고되었지만 호스트에 없는 중복된 노드입니다. 분리된 노드는 모두 삭제해야 합니다. 자세한 내용은 [vRealize Automation에서 분리된 노드 삭제](#) 항목을 참조하십시오.
- 더 이상 클러스터의 일부가 아닌 복제 가상 장치가 있는 경우 클러스터 테이블에서 해당 장치를 삭제해야 합니다. 이 장치를 삭제하지 않으면 업그레이드 프로세스에서는 복제 업데이트가 실패했다는 주의 메시지를 표시합니다.
 - 업그레이드 전에, 저장되고 진행 중인 모든 요청이 완료되었는지 확인합니다.
 - vRealize Automation 소스 장치를 업데이트한 이후에 IaaS 구성 요소를 수동으로 업그레이드하는 경우에는 [IaaS 업그레이드 제외](#) 항목을 참조하십시오. IaaS를 수동으로 업그레이드할 계획이면 각 IaaS 노드에서 관리 에이전트를 제외한 모든 IaaS 서비스도 중지해야 합니다.

절차

- 1 기본 또는 마스터 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 서비스를 클릭하고 모든 서비스가 [등록됨] 상태인지 확인합니다.
- 3 클러스터를 선택하고 이 장치가 마스터 vRealize Automation 장치인지 확인합니다.
마스터 vRealize Automation 장치에만 업데이트를 설치합니다. 각 복제 vRealize Automation 장치가 마스터 장치로 업데이트됩니다.
- 4 업데이트 > 상태를 선택합니다.
- 5 업데이트 확인을 클릭하여 업데이트가 있는지 확인합니다.
- 6 (선택 사항) vRealize Automation 장치 인스턴스의 경우 장치 버전 영역에서 세부 정보를 클릭하여 릴리스 정보의 위치에 대한 정보를 확인합니다.
- 7 업데이트 설치를 클릭합니다.
- 8 확인을 클릭합니다.
업데이트가 진행 중임을 알리는 메시지가 나타납니다. 시스템에서는 업그레이드 동안의 변경 내용을 [업데이트 요약] 페이지에 보여 줍니다. 업데이트를 완료하는 데 필요한 시간은 환경 및 네트워크에 따라 다릅니다.
- 9 (선택 사항) 업데이트를 보다 세부적으로 모니터링하려면 터미널 에뮬레이터를 사용하여 기본 장치에 로그인합니다. `/opt/vmware/var/log/vami/updatecli.log`에서 `updatecli.log` 파일을 봅니다.
다음 파일에서 추가 업그레이드 프로세스 정보를 볼 수도 있습니다.
 - `/opt/vmware/var/log/vami/vami.log`
 - `/var/log/vmware/horizon/horizon.log`

■ /var/log/bootstrap/*.log

업그레이드 프로세스 중에 로그아웃한 경우 로그 파일을 통해 업데이트 진행 상태를 계속 추적할 수 있습니다. `updatecli.log` 파일에 업그레이드 이전의 vRealize Automation 버전에 대한 정보가 표시될 수 있습니다. 표시된 이 버전이 업그레이드 프로세스의 후반부에 올바른 버전으로 변경됩니다.

- 10 vRealize Automation 장치 업데이트가 완료되면 vRealize Automation 장치 관리 인터페이스에서 **시스템 > 재부팅**을 클릭합니다.

분산 환경에서는 마스터 장치를 재부팅하면 성공적으로 업그레이드된 모든 복제 장치 노드가 재부팅됩니다.

시스템이 초기화되고 모든 서비스가 가동되어 실행 중이면 IaaS 업데이트가 시작됩니다. IaaS 업그레이드 진행률을 보려면 **업데이트 > 상태**를 클릭합니다.

- 11 IaaS 업데이트가 완료되면 vRealize Automation 장치 관리 인터페이스에서 **클러스터**를 클릭하고 모든 IaaS 노드와 구성 요소의 버전 번호가 현재 버전인지 확인합니다.

- 12 vRealize Automation 장치 관리 인터페이스에서 **원격 분석**을 클릭합니다. CEIP(고객 환경 향상 프로그램) 참여에 대한 참고 사항을 읽고 프로그램에 참여할지 여부를 선택합니다.

CEIP를 통해 수집된 데이터에 대한 세부 정보 및 VMware에서 CEIP를 사용하는 목적이 Trust & Assurance Center의 <http://www.vmware.com/trustvmware/ceip.html>에 기술되어 있습니다.

고객 환경 향상 프로그램에 대한 자세한 내용은 [vRealize Automation에 대한 고객 환경 향상 프로그램 참여 또는 탈퇴](#) 항목을 참조하십시오.

다음에 수행할 작업

배포에서 로드 밸런서를 사용하는 경우 다음 단계를 수행합니다.

- 1 로드 밸런서 vRealize Automation 상태 점검을 사용하도록 설정합니다.
- 2 모든 vRealize Automation 노드에 대해 로드 밸런서 트래픽을 다시 사용하도록 설정합니다.

IaaS 구성 요소 업그레이드가 실패한 경우, [업데이트 프로세스가 실패한 경우 IaaS 서버 구성 요소를 별도로 업그레이드](#) 항목을 참조하십시오.

업데이트 프로세스가 실패한 경우 IaaS 서버 구성 요소를 별도로 업그레이드

자동 업데이트 프로세스가 실패하는 경우 IaaS 구성 요소를 별도로 업그레이드할 수 있습니다.

vRealize Automation IaaS 웹 사이트 및 Manager Service가 성공적으로 업그레이드되면 업그레이드 전에 생성한 스냅샷으로 되돌리지 않고 IaaS 업그레이드 셀 스크립트를 다시 실행할 수 있습니다. 종종 동일한 가상 시스템에 설치된 여러 IaaS 구성 요소를 업그레이드하는 동안 생성된 오류 중인 재부팅 이벤트로 인해 업그레이드가 실패할 수 있습니다. 이러한 경우에는 IaaS 노드를 수동으로 재부팅하고 업그레이드를 다시 실행하여 문제 해결을 시도합니다. 그래도 업그레이드가 실패한다면 VMware 지원에 문의하거나 다음 단계에 따라 수동 업그레이드를 시도합니다.

- 1 vRealize Automation 장치를 업데이트 전 상태로 되돌립니다.

- 2 업데이트 프로세스에서 IaaS 구성 요소를 제외하는 명령을 실행합니다. **IaaS 업그레이드 제외** 항목을 참조하십시오.
- 3 vRealize Automation 장치에서 업데이트 프로세스를 실행합니다.
- 4 업그레이드 셸 스크립트 또는 최신 릴리스 vRealize Automation IaaS 설치 관리자 MSI 패키지를 사용하여 IaaS 구성 요소를 별도로 업데이트합니다.

vRealize Automation 장치 업그레이드 후 업그레이드 셸 스크립트를 사용하여 **IaaS** 구성 요소 업그레이드

업그레이드 셸 스크립트를 사용하여 각 vRealize Automation 7.1 이상 장치를 업그레이드하려는 vRealize Automation 릴리스로 업데이트한 후 IaaS 구성 요소를 업그레이드합니다.

업데이트된 vRealize Automation 장치에는 각 IaaS 노드 및 구성 요소를 업그레이드하는 데 사용하는 셸 스크립트가 포함됩니다.

가상 시스템의 vSphere 콘솔을 사용하거나 SSH 콘솔 세션을 사용하여 업그레이드 스크립트를 실행할 수 있습니다. vSphere 콘솔을 사용하면 스크립트 실행을 중단시킬 수 있는 간헐적인 네트워크 연결 문제를 방지할 수 있습니다.

구성 요소를 업그레이드하는 동안 스크립트를 중지할 경우, 구성 요소 업그레이드가 완료된 후에 스크립트가 중지됩니다. 업그레이드해야 할 다른 구성 요소가 노드에 남아 있는 경우에는 스크립트를 다시 실행할 수 있습니다.

업그레이드가 완료되면 업그레이드 로그 파일(/opt/vmware/var/log/vami/upgrade-iaas.log)을 열어 업그레이드 결과를 검토할 수 있습니다.

사전 요구 사항

- **vRealize Automation** 업그레이드 문제 해결 항목을 검토합니다.
- 모든 vRealize Automation 장치의 성공적인 업데이트를 확인합니다.
- 모든 vRealize Automation 장치를 업데이트한 후 IaaS 구성 요소를 업그레이드하기 전에 IaaS 서버를 재부팅하는 경우, 관리 에이전트 서비스를 제외한 모든 IaaS 서비스를 Windows에서 중지합니다.
- 마스터 vRealize Automation 장치 노드에서 업그레이드 셸 스크립트를 실행하기 전에 vRealize Automation 장치 관리 인터페이스에서 **서비스**를 클릭합니다. **iaas-service**를 제외한 각 서비스가 [등록됨]인지 확인합니다.
- 각 IaaS 노드에 IaaS 관리 에이전트를 수동으로 설치하려면 다음 단계를 완료합니다.
 - a 브라우저를 열고 장치의 [IaaS 설치] 페이지로 이동합니다.
<https://vrealize-automation-appliance-FQDN:5480/installer>
 - b 관리 에이전트 설치 관리자인 vCAC-iaasManagementAgent-Setup.msi를 다운로드합니다.
 - c 각 vRealize Automation IaaS 시스템에 로그인한 후 관리 에이전트 설치 관리자를 사용하여 관리 에이전트를 업그레이드합니다. Windows 관리 에이전트 서비스를 다시 시작합니다.

- 기본 IaaS 웹 사이트 및 Model Manager 노드에 JAVA SE Runtime Environment 8, 64비트, 업데이트 181 이상이 설치되어 있는지 확인합니다. Java를 설치한 후 각 서버 노드에서 환경 변수 JAVA_HOME을 새 버전으로 설정해야 합니다.
- 각 IaaS 웹 사이트 노드에 로그인하고 생성 날짜가 web.config 파일의 수정된 날짜 이전인지 확인합니다. web.config 파일의 생성 날짜가 수정된 날짜와 같거나 이후인 경우 [IaaS 웹 사이트 구성 요소에 대한 업그레이드 실패](#)의 절차를 수행합니다.
- 각 IaaS 노드에서 다음 단계를 수행하여 해당 IaaS 노드에 업그레이드된 IaaS 관리 에이전트가 있는지 확인합니다.
 - a vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
https://vrealize-automation-appliance-FQDN:5480
 - b 클러스터를 선택합니다.
 - c 각 IaaS 노드에서 설치된 모든 구성 요소 목록을 확장하고 IaaS 관리 에이전트를 찾습니다.
 - d 관리 에이전트 버전이 최신인지 확인합니다.
- [IaaS 업그레이드 제외](#).
- 롤백해야 하는 경우 IaaS Microsoft SQL Server 데이터베이스 백업에 액세스할 수 있는지 확인합니다.
- 해당 배포의 IaaS 서버 스냅샷이 사용 가능한지 확인합니다.
업그레이드가 실패하면 스냅샷 및 데이터베이스 백업으로 되돌리고 다른 업그레이드를 시도합니다.

절차

- 1 vRealize Automation 장치 호스트에서 새 콘솔 세션을 엽니다. 루트 계정으로 로그인합니다.
- 2 디렉토리를 /usr/lib/vcac/tools/upgrade/로 변경합니다.
./upgrade 셸 스크립트를 실행하기 전에 모든 IaaS 관리 에이전트가 업그레이드되고 정상 상태여야 합니다. 업그레이드 셸 스크립트를 실행할 때 IaaS 관리 에이전트에 문제가 있는 경우 [업데이트를 통한 관리 에이전트 업그레이드 실패](#) 항목을 참조하십시오.
- 3 업그레이드 스크립트를 실행합니다.
 - a 명령 프롬프트에서 ./upgrade를 입력합니다.
 - b Enter 키를 누릅니다.

IaaS 업그레이드 프로세스에 대한 설명은 [vRealize Automation 장치 및 IaaS 구성 요소 업데이트](#) 항목을 참조하십시오.

업그레이드 셸 스크립트가 실패한 경우 upgrade-iaas.log 파일을 검토합니다.

문제를 해결한 후 업그레이드 스크립트를 다시 실행할 수 있습니다.

다음에 수행할 작업

- 1 기본 제공 vRealize Orchestrator 제어 센터에 대한 액세스 복원.
- 2 배포에서 로드 밸런서를 사용하는 경우 vRealize Automation 상태 모니터 및 모든 노드에 대한 트래픽을 다시 사용하도록 설정합니다.

자세한 내용은 [vRealize Automation 제품 설명서](#)에서 "vRealize Automation 로드 밸런싱" 링크를 참조하십시오.

vRealize Automation 장치 업그레이드 후 IaaS 설치 관리자 실행 파일을 사용하여 IaaS 구성 요소 업그레이드

vRealize Automation 7.1 이상 장치를 업그레이드한 후 이 대체 방법을 사용하여 IaaS 구성 요소를 업그레이드할 수 있습니다.

vRealize Automation 장치를 업그레이드한 후 IaaS 구성 요소 업그레이드를 위해 IaaS 설치 관리자 다운로드

vRealize Automation 장치를 대상 릴리스로 업그레이드한 후 업그레이드할 IaaS 구성 요소가 설치되어 있는 시스템에 IaaS 설치 관리자를 다운로드합니다.

이 절차를 진행하는 중에 인증서 경고가 표시될 수 있습니다. 이 경고는 무시해도 됩니다.

참고 Manager Service의 패시브 백업 인스턴스를 제외하고, 업그레이드 프로세스 중 모든 서비스에 대한 시작 유형은 [자동]으로 설정되어야 합니다. 업그레이드 프로세스가 실패하면 서비스를 [수동]으로 설정합니다.

사전 요구 사항

- IaaS 설치 시스템에 Microsoft .NET Framework 4.5.2 이상이 설치되어 있는지 확인합니다. vRealize Automation 설치 관리자 웹 페이지에서 .NET 설치 관리자를 다운로드할 수 있습니다. 설치의 일부로 다시 시작된 서비스와 시스템을 종료한 후 .NET을 4.5.2로 업데이트하는 경우 관리 에이전트를 제외한 모든 IaaS 서비스를 수동으로 중지해야 합니다.
- .NET 3.5 Framework 비HTTP 활성화 기능이 구성되어 있는지 확인합니다. 모든 IaaS 노드(웹, Manager Service, 프록시 에이전트, DEM)에 .NET 3.5 Framework 비HTTP 활성화 기능이 설정되어 있지 않으면 vRealize Automation 업그레이드가 실패합니다. 이 오류는 사전 요구 사항 검사기가 최신 .NET 버전을 다운로드하고 설치하기 위해 인터넷에 액세스할 수 없는 경우에 발생합니다. 이 기능을 추가하려면:
 - a 역할 및 기능 추가 마법사를 엽니다.
 - b .NET Framework 3.5 기능을 선택합니다.
 - c 비HTTP 활성화 확인란을 선택합니다.
- Internet Explorer를 사용하여 다운로드하는 경우 보안 강화 구성 설정을 사용하지 말아야 합니다. 검색 창에 `res://iesetup.dll/SoftAdmin.htm`을 입력하고 Enter 키를 누릅니다.
- Windows Server에 로컬 관리자로 로그인합니다. Windows Server에는 업그레이드하려는 IaaS 구성 요소 중 하나 이상이 설치되어 있습니다.

절차

- 1 브라우저를 열고 기본 또는 마스터 vRealize Automation 장치의 [IaaS 설치] 페이지로 이동합니다.

<https://vrealize-automation-appliance-FQDN:5480/installer>

- 2 IaaS 설치 관리자를 클릭합니다.

- 3 메시지가 표시되면 `setup__vrealize-automation-appliance-FQDN@5480.exe`를 데스크톱에 저장합니다.

파일 이름은 변경하지 마십시오. 이 이름은 설치를 올바른 vRealize Automation 장치에 연결합니다.

다음에 수행할 작업

vRealize Automation을 대상 릴리스로 업그레이드한 후 IaaS 구성 요소 업그레이드.

vRealize Automation을 대상 릴리스로 업그레이드한 후 IaaS 구성 요소 업그레이드

SQL 데이터베이스를 업그레이드하고 IaaS 구성 요소가 설치되어 있는 모든 시스템을 구성해야 합니다. 최소 설치와 분산 설치를 위해 이러한 단계를 사용할 수 있습니다.

참고 IaaS 설치 관리자는 업그레이드할 IaaS 구성 요소가 있는 시스템에 있어야 합니다. 웹 노드에서 원격으로도 업그레이드할 수 있는 Microsoft SQL 데이터베이스를 제외하고 외부 위치에서는 설치 관리자를 실행할 수 없습니다.

해당 배포의 IaaS 서버 스냅샷이 사용 가능한지 확인합니다. 업그레이드가 실패하면 해당 스냅샷으로 되돌리고 다른 업그레이드를 시도할 수 있습니다.

서비스가 다음 순서로 업그레이드되도록 업그레이드를 수행합니다.

- 1 IaaS 웹 사이트

로드 밸런서를 사용 중인 경우 기본이 아닌 모든 노드에 대해 트래픽을 사용하지 않도록 설정합니다.

웹 사이트 서비스를 실행 중인 다음 서버를 업그레이드하기 전에 현재 서버에 대한 업그레이드를 완료합니다. Model Manager Data 구성 요소가 설치되어 있는 것부터 시작합니다.

외부 Microsoft SQL 데이터베이스에 대한 수동 업그레이드를 수행 중인 경우 웹 노드를 업그레이드하기 전에 외부 SQL을 업그레이드해야 합니다. 웹 노드에서 외부 SQL을 원격으로 업그레이드할 수 있습니다.

- 2 Manager Service

패시브 Manager Service를 업그레이드하기 전에 액티브 Manager Service를 업그레이드합니다.

SQL 인스턴스에서 SSL 암호화가 사용되도록 설정되지 않은 경우 SQL 정의 옆에 있는 [IaaS 업그레이드 구성] 대화 상자에서 [SSL 암호화] 확인란을 선택 취소합니다.

- 3 DEM 조정자 및 DEM 작업자

모든 DEM 조정자 및 DEM 작업자를 업그레이드합니다. 다음 서버를 업그레이드하기 전에 현재 서버에 대한 업그레이드를 완료합니다.

- 4 에이전트

에이전트를 실행 중인 다음 서버를 업그레이드하기 전에 현재 서버에 대한 업그레이드를 완료합니다.

5 관리 에이전트

업그레이드 프로세스의 일부로 자동 업데이트됩니다.

한 서버에서 서로 다른 서비스를 사용 중인 경우 업그레이드하면 적절한 순서로 서비스가 업데이트됩니다. 예를 들어 사이트의 동일한 서버에 웹 사이트와 **Manager Service**가 있는 경우 모두 업데이트하도록 선택합니다. 업그레이드 설치 관리자가 적절한 순서로 업데이트를 적용합니다. 한 서버에 대한 업그레이드를 완료한 후에 다른 서버에 대한 업그레이드를 시작해야 합니다.

참고 배포에서 로드 밸런서를 사용하는 경우 기본 장치를 로드 밸런서에 연결해야 합니다. 캐시 오류를 피하려면 업그레이드를 적용하기 전에 로드 밸런서 트래픽에 대해 vRealize Automation 장치의 다른 모든 인스턴스를 사용하지 않도록 설정해야 합니다.

사전 요구 사항

- 기존 vRealize Automation 환경을 백업합니다.
- 모든 vRealize Automation 장치를 업데이트한 후에 하지만 IaaS 구성 요소를 업그레이드하기는 전에 IaaS 서버를 재부팅하는 경우 서버에서 관리 에이전트 서비스를 제외한 모든 IaaS Windows 서비스를 중지합니다.
- vRealize Automation 장치를 업그레이드한 후 IaaS 구성 요소 업그레이드를 위해 IaaS 설치 관리자 다운로드.
- 기본 IaaS 웹 사이트, Microsoft SQL 데이터베이스 및 Model Manager 노드에 JAVA SE Runtime Environment 8, 64비트, 업데이트 181 이상이 설치되어 있는지 확인합니다. Java를 설치한 후 각 서버 노드에서 환경 변수 JAVA_HOME을 새 버전으로 설정해야 합니다.
- 생성 날짜가 web.config 파일의 수정된 날짜 이전인지 확인합니다. web.config 파일의 생성 날짜가 수정된 날짜와 같거나 이후인 경우 IaaS 웹 사이트 구성 요소에 대한 업그레이드 실패의 절차를 수행합니다.
- 다음 단계를 완료하여 Microsoft DTC(Distributed Transaction Coordinator)를 재구성합니다.

참고 Distributed Transaction Coordinator를 사용하도록 설정하더라도 방화벽이 켜져 있으면 분산 트랜잭션이 실패할 수 있습니다.

- a vRealize Automation 장치에서 **시작 > 관리 도구 > 구성 요소 서비스**를 선택합니다.
- b **구성 요소 서비스 > 컴퓨터 > 내 컴퓨터 > Distributed Transaction Coordinator**를 확장합니다.
- c 적절한 작업을 선택합니다.
 - 로컬 독립형 DTC의 경우 **로컬 DTC**를 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.
 - 클러스터된 DTC의 경우 **클러스터된 DTC**를 확장하고 명명된 클러스터된 DTC를 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.
- d **보안**을 클릭합니다.

e 다음을 모두 선택합니다.

- 네트워크 DTC 액세스
- 원격 클라이언트 허용
- 인바운드 허용
- 아웃바운드 허용
- 수동 인증 필요

f **확인**을 클릭합니다.

절차

1 로드 밸런서를 사용하고 있는 경우 환경을 준비합니다.

a Model Manager Data가 포함된 IaaS 웹 사이트 노드가 로드 밸런서 트래픽에 대해 사용되도록 설정되었는지 확인합니다.

vCAC Folder\Server\ConfigTool 폴더가 있는지 여부로 이 노드를 식별할 수 있습니다.

b 로드 밸런서 트래픽에 대해 기본이 아닌 Manager Service 및 기타 모든 IaaS 웹 사이트를 사용하지 않도록 설정합니다.

2 **setup__vrealize-automation-appliance-FQDN@5480.exe** 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

3 다음을 클릭합니다.

4 라이선스 계약에 동의하고 다음을 클릭합니다.

5 [로그인] 페이지에서 현재 배포에 대한 관리자 자격 증명을 입력합니다.

사용자 이름은 **root**이고 암호는 장치를 배포할 때 지정한 암호입니다.

6 **인증서 수락**을 선택합니다.

7 **설치 유형** 페이지에서 **업그레이드**가 선택되었는지 확인합니다.

업그레이드가 선택되지 않았다면 이 시스템의 구성 요소가 이미 이 버전으로 업그레이드된 것입니다.

8 다음을 클릭합니다.

9 업그레이드 설정을 구성합니다.

옵션	작업
Model Manager Data를 업그레이드하는 경우	[vCAC 서버] 섹션에서 Model Manager Data 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다. Model Manager Data는 한 번만 업그레이드합니다. 분산 설치를 업그레이드하기 위해 여러 시스템에서 설정 파일을 실행하고 있는 경우 웹 서버와 Model Manager Data 간 버전 불일치가 있으면 웹 서버가 작동을 중지합니다. Model Manager Data와 모든 웹 서버를 업그레이드했다면 모든 웹 서버가 작동해야 합니다.
Model Manager Data를 업그레이드하지 않는 경우	[vCAC 서버] 섹션에서 Model Manager Data 확인란을 선택 해제합니다.
사용자 지정 워크플로를 Model Manager Data에서 최신 버전으로 유지하려는 경우	Model Manager Data를 업그레이드하는 경우 [확장성 워크플로] 섹션에서 내 최신 워크플로 버전 유지 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다. 사용자 지정 워크플로는 항상 유지됩니다. 확인란은 버전 순서만 결정합니다. Model Manager에서 워크플로 사용자 지정을 위해 vRealize Automation Designer를 사용한 경우, 업그레이드하기 전 사용자 지정된 각 워크플로의 가장 최신 버전을 업그레이드 후 가장 최신 버전으로 유지하려면 이 옵션을 선택합니다. 이 옵션을 선택하지 않으면 vRealize Automation Designer와 함께 제공된 각 워크플로의 버전이 업그레이드 후 가장 최신이 되며 업그레이드 전 가장 최신이었던 버전은 두 번째로 최신인 버전이 됩니다. vRealize Automation Designer에 대한 자세한 내용은 vRealize Automation Designer를 사용하여 시스템 수명 주기 연장을 참조하십시오 .
Distributed Execution Manager 또는 프록시 에이전트를 업그레이드하는 경우	[서비스 계정] 섹션에 관리자 계정의 자격 증명을 입력합니다. 업그레이드하는 모든 서비스는 이 계정으로 실행됩니다.
Microsoft SQL Server 데이터베이스를 유지하려는 경우	Model Manager Data를 업그레이드하는 경우 데이터베이스 인스턴스 및 데이터베이스 서버의 이름을 [Microsoft SQL Server 데이터베이스 설치 정보] 섹션의 서버 텍스트 상자에 입력합니다. 데이터베이스 이름 텍스트 상자에 데이터베이스 서버 이름의 FQDN(정규화된 도메인 이름)을 입력합니다. 데이터베이스 인스턴스가 기본이 아닌 SQL 포트에 있는 경우 서버 인스턴스 규격에 포트 번호를 포함합니다. Microsoft SQL 기본 포트 번호는 1433입니다. 관리자 노드를 업그레이드하는 경우 기본적으로 MSSQL SSL 옵션이 선택되어 있습니다. 해당 데이터베이스가 SSL을 사용하지 않는 경우 데이터베이스 연결에 SSL 사용 을 선택 취소합니다.

10 다음을 클릭합니다.

11 업그레이드하려는 모든 서비스가 [업그레이드 준비 완료] 페이지에 나타나는지 확인하고 **업그레이드**를 클릭합니다.

[업그레이드] 페이지와 진행률 표시기가 나타납니다. 업그레이드 프로세스가 완료되면 **다음** 버튼이 활성화됩니다.

12 다음을 클릭합니다.

13 **완료**를 클릭합니다.

14 모든 서비스가 다시 시작되었는지 확인합니다.

- 15 권장 순서에 따라 배포의 각 IaaS 서버에 대해 이러한 단계를 반복합니다.
- 16 모든 구성 요소가 업그레이드되면 vRealize Automation 장치 관리 인터페이스에 로그인하고 이제 IaaS를 포함한 모든 서비스가 등록되어 있는지 확인합니다.
- 17 (선택 사항) 자동 Manager Service 패일오버를 사용하도록 설정합니다. [업그레이드 후 자동 Manager Service 패일오버를 사용하도록 설정](#) 항목을 참조하십시오.

결과

선택된 모든 구성 요소는 새 릴리스로 업그레이드됩니다.

다음에 수행할 작업

- 1 기본 제공 vRealize Orchestrator 제어 센터에 대한 액세스 복원.
- 2 배포에서 로드 밸런서를 사용하는 경우 각 로드 밸런서 노드를 업그레이드하여 vRealize Automation 상태 점검을 사용하고 연결되지 않은 노드에 대해 로드 밸런서 트래픽을 다시 사용하도록 설정합니다.
자세한 내용은 "vRealize Automation 로드 밸런싱" 을 참조하십시오.

기본 제공 vRealize Orchestrator 제어 센터에 대한 액세스 복원

IaaS 서버 구성 요소를 업그레이드한 후에는 vRealize Orchestrator에 대한 액세스를 복원해야 합니다.

vRealize Automation으로 업그레이드할 때 최근에 도입된 역할 기반 액세스 제어 기능을 수용하려면 이 절차를 수행해야 합니다. 이 절차는 고가용성 환경을 위해 작성된 것입니다.

사전 요구 사항

vRealize Automation 환경에 대한 스냅샷을 생성합니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 클러스터를 선택합니다.
- 3 마스터 노드와 복제 노드를 식별합니다.
- 4 각 복제 노드에서 SSH 세션을 열고 관리자로 로그인한 후 다음 명령을 실행합니다.
`service vco-server stop && service vco-configurator stop`
- 5 마스터 노드에서 SSH 세션을 열고 관리자로 로그인한 후 다음 명령을 실행합니다.
`rm /etc/vco/app-server/vco-registration-id`
- 6 마스터 노드에서 디렉토리를 `/etc/vco/app-server/`로 변경합니다.
- 7 `sso.properties` 파일을 엽니다.

- 8 속성 이름 `com.vmware.o11n.sso.admin.group.name`에 공백이 있거나 Bash 명령에서 특수 문자로 인정될 수 있는 아포스트로피(') 또는 달러 기호(\$)와 같은 기타 Bash 관련 문자가 포함되어 있는 경우 다음 단계를 완료합니다.
 - a `com.vmware.o11n.sso.admin.group.name` 속성이 포함된 줄을 복사하고 값에 대해 AdminGroup을 입력합니다.
 - b `com.vmware.o11n.sso.admin.group.name` 속성이 포함된 원래 줄의 맨 앞에 #을 추가하여 줄에 주석 처리를 합니다.
 - c `sso.properties` 파일을 저장하고 닫습니다.
- 9 다음 명령을 실행합니다.


```
vcac-vami vco-service-reconfigure
```
- 10 `sso.properties` 파일을 엽니다. 파일이 변경된 경우 다음 단계를 완료합니다.
 - a `com.vmware.o11n.sso.admin.group.name` 속성이 포함된 원래 줄의 맨 앞에서 #을 제거하여 줄에서 주석 처리를 제거합니다.
 - b `com.vmware.o11n.sso.admin.group.name` 속성이 포함된 줄의 사본을 제거합니다.
 - c `sso.properties` 파일을 저장하고 닫습니다.
- 11 다음 명령을 실행하여 vco-server 서비스를 다시 시작합니다.


```
service vco-server restart
```
- 12 다음 명령을 실행하여 vco-configurator 서비스를 다시 시작합니다.


```
service vco-configurator restart
```
- 13 vRealize Automation 장치 관리 인터페이스에서 **서비스**를 클릭하고 마스터 노드의 모든 서비스가 [등록됨] 상태가 될 때까지 기다립니다.
- 14 모든 서비스가 등록되면 vRealize Automation 복제 노드를 vRealize Automation 클러스터에 가입시켜 vRealize Orchestrator 구성을 동기화합니다.

다음에 수행할 작업

vRealize Automation을 업그레이드한 후 외부 vRealize Orchestrator 마이그레이션.

vRealize Automation을 업그레이드한 후 외부 vRealize Orchestrator 마이그레이션

vRealize Orchestrator 7.5부터는 외부 vRealize Orchestrator 환경을 더 이상 업그레이드할 수 없습니다. 외부 vRealize Orchestrator 환경을 최신 버전으로 이동하려면 마이그레이션해야 합니다.

참고 vRealize Automation에 내장된 vRealize Orchestrator 인스턴스는 vRealize Automation 업그레이드를 통해 자동으로 업그레이드됩니다. 내장된 vRealize Orchestrator만 사용하면 작업이 필요하지 않습니다.

vRealize Orchestrator 마이그레이션은 워크플로, 동작, 구성 및 리소스 요소, 패키지, 작업, 정책, 인증서, 플러그인 및 기타 기존 요소를 모두 덮어써서 외부 소스 vRealize Orchestrator 구성을 새로 구성된 vRealize Orchestrator 7.5 환경으로 전송합니다.

최신 vRealize Automation 릴리스로 업그레이드하는 경우 외부 vRealize Orchestrator 마이그레이션에는 두 가지 옵션이 있습니다.

- 외부 vRealize Orchestrator를 다른 외부 vRealize Orchestrator 인스턴스로 마이그레이션합니다. vRealize Orchestrator 설명서에서 [외부 Orchestrator 서버를 외부 vRealize Orchestrator 7.5로 마이그레이션](#)을 참조하십시오.
- 외부 vRealize Orchestrator 서버를 vRealize Automation에 내장된 vRealize Orchestrator 인스턴스로 마이그레이션합니다. vRealize Orchestrator 설명서에서 [외부 Orchestrator 서버를 vRealize Orchestrator 7.5로 마이그레이션](#)을 참조하십시오.

참고 내장된 vRealize Orchestrator 인스턴스를 외부 vRealize Orchestrator 환경으로 마이그레이션하는 기능은 지원되지 않습니다.

로드 밸런서 사용

배포가 로드 밸런서를 사용하는 경우 보조 노드 및 상태 점검을 다시 사용하도록 설정하고 로드 밸런서 시간 초과 설정을 되돌립니다.

vRealize Automation의 상태 점검은 버전에 따라 다릅니다. 자세한 내용은 [VMware vRealize Automation 설명서](#)에서 "vRealize Automation 로드 밸런싱 구성 가이드" 항목을 참조하십시오.

로드 밸런서 시간 초과 설정을 10분에서 다시 기본값으로 변경합니다.

vRealize Automation 업그레이드를 위한 사후 업그레이드 작업

vRealize Automation 7.1 이상에서 업그레이드한 후에는 필수 사후 업그레이드 작업을 수행해야 합니다.

vRealize Automation 표준 시간대 변경 안 함

vRealize Automation 장치 관리 인터페이스에 표준 시간대를 변경할 수 있는 옵션이 제공되지만, vRealize Automation 표준 시간대는 항상 Etc/UTC로 설정해 두어야 합니다.

Etc/UTC 이외의 표준 시간대를 사용하면 실패한 마이그레이션 및 모든 vRealize Automation 노드의 항목이 포함되지 않은 로그 번들 등과 같은 비정상적인 오류가 발생하는 것으로 알려져 있습니다.

피해야 하는 vRealize Automation 장치 관리 인터페이스 옵션은 **시스템 > 표준 시간대** 아래에 있습니다.

소프트웨어 에이전트를 TLS 1.2로 업그레이드

vRealize Automation를 업그레이드한 후 vRealize Automation 7.1 이상 환경에서 TLS 1.2로 소프트웨어 에이전트를 업그레이드하기 위한 여러 작업을 수행해야 합니다.

vRealize Automation 7.4부터, vRealize Automation 및 브라우저 간 데이터 통신에 지원되는 TLS(Transport Layer Security) 프로토콜은 TLS 1.2가 유일합니다.

마이그레이션한 후에는 모든 기존 가상 시스템은 물론 vRealize Automation 7.1 이상 환경의 기존 가상 시스템 템플릿을 업그레이드해야 합니다.

vRealize Automation 가상 시스템 템플릿 업데이트

대상 vRealize Automation 릴리스로의 업그레이드를 완료했으면 기존 템플릿을 업데이트하여 소프트웨어 에이전트가 TLS 1.2 프로토콜을 사용하도록 해야 합니다.

게스트 에이전트 및 에이전트 부트스트랩 코드는 소스 vRealize Automation 릴리스의 템플릿에서 업데이트되어야 합니다. 연결된 클론 옵션을 사용 중이라면 새로 생성된 가상 시스템과 해당 스냅샷에 템플릿을 다시 매핑해야 할 수 있습니다.

템플릿을 업그레이드하려면 다음 작업을 완료합니다.

- 1 vSphere에 로그인합니다.
- 2 소스 vRealize Automation 릴리스의 각 템플릿을 가상 시스템으로 변환하고 시스템의 전원을 끕니다.
- 3 적절한 소프트웨어 설치 관리자를 가져오고 각 가상 시스템에서 해당 소프트웨어 설치 관리자를 실행합니다.
- 4 각 가상 시스템을 다시 템플릿으로 변환합니다.

Linux 또는 Windows용 소프트웨어 설치 관리자를 찾으려면 이 절차를 사용합니다.

사전 요구 사항

대상 vRealize Automation 릴리스로 업그레이드를 완료합니다.

절차

- 1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름(<https://vra-vr-hostname.domain.name>)을 사용하여 대상 vRealize Automation 장치 시작 페이지를 엽니다.
- 2 **게스트 및 소프트웨어 에이전트 페이지**를 클릭합니다.
- 3 Linux 또는 Windows 소프트웨어 설치 관리자에 대한 지침을 따릅니다.

다음에 수행할 작업

[소프트웨어 에이전트 업그레이드가 필요한 가상 시스템 식별](#).

소프트웨어 에이전트 업그레이드가 필요한 가상 시스템 식별

vRealize Automation의 상태 서비스를 사용하여 TLS 1.2로의 소프트웨어 에이전트 업데이트가 필요한 가상 시스템을 식별할 수 있습니다.

상태 서비스를 사용하여 TLS 1.2로 소프트웨어 에이전트 업데이트가 필요한 가상 시스템을 식별할 수 있습니다. vRealize Automation 환경의 모든 소프트웨어 에이전트를 업데이트해야 브라우저와 vRealize Automation 간의 보안 통신이 필요한 사후 프로비저닝 절차를 수행할 수 있습니다.

사전 요구 사항

- vRealize Automation 릴리스로 업그레이드되었습니다.
- 기본 가상 장치의 대상 vRealize Automation 릴리스에 테넌트 관리자로 로그인했습니다.

절차

- 1 **관리 > 상태**를 클릭합니다.
- 2 **새 구성**을 클릭합니다.
- 3 [구성 세부 정보] 페이지에 요청된 정보를 입력합니다.

옵션	설명
이름	SW Agent verification 을 입력합니다.
설명	선택적 설명(예: Locate software agents for upgrade to TLS 1.2)을 추가합니다.
제품	업그레이드했거나 마이그레이션한 vRealize Automation 릴리스를 선택합니다.
스케줄	없음 을 선택합니다.

- 4 **다음**을 클릭합니다.
- 5 [테스트 집합 선택] 페이지에서 **vRealize Automation에 대한 시스템 테스트** 및 **vRealize Automation에 대한 테넌트 테스트**를 선택합니다.
- 6 **다음**을 클릭합니다.
- 7 [매개 변수 구성] 페이지에 요청된 정보를 입력합니다.

표 1-54. vRealize Automation 가상 장치

옵션	설명
공개 웹 서버 주소	<ul style="list-style-type: none"> ■ 최소 배포의 경우 vRealize Automation 장치 호스트에 대한 기본 URL입니다. 예: <code>https://va-host.domain/</code> ■ 고가용성 배포의 경우 vRealize Automation 로드 밸런서에 대한 기본 URL입니다. 예: <code>https://load-balancer-host.domain/</code>
SSH 콘솔 주소	vRealize Automation 장치의 정규화된 도메인 이름입니다. 예: <code>va-host.domain</code>
SSH 콘솔 사용자	root
SSH 콘솔 암호	루트의 암호입니다.
최대 서비스 응답 시간(ms)	허용 기본값: 2000

표 1-55. vRealize Automation 시스템 테넌트

옵션	설명
시스템 테넌트 관리자	관리자
시스템 테넌트 암호	관리자의 암호입니다.

표 1-56. vRealize Automation 디스크 공간 모니터링

옵션	설명
경고 임계값 백분율	허용 기본값: 75
위험 임계값 백분율	허용 기본값: 90

표 1-57. vRealize Automation 테넌트

옵션	설명
테스트 중인 테넌트	테스트를 위해 선택한 테넌트입니다.
패브릭 관리자 사용자 이름	패브릭 관리자 사용자 이름입니다. 예: admin@va-host.local 참고 모든 테스트를 실행하려면 이 패브릭 관리자에게 테넌트 관리자 및 IaaS 관리자 역할도 있어야 합니다.
패브릭 관리자 암호	패브릭 관리자의 암호입니다.

8 다음을 클릭합니다.

9 [요약] 페이지에서 정보를 검토하고 **완료**를 클릭합니다.

소프트웨어 에이전트 확인 구성이 완료되었습니다.

10 소프트웨어 에이전트 확인 카드에서 **실행**을 클릭합니다.

11 테스트가 완료되면 소프트웨어 에이전트 확인 카드의 가운데를 클릭합니다.

12 소프트웨어 에이전트 확인 결과 페이지에서 테스트 결과 페이지를 넘겨 보고 [이름] 열에서 [소프트웨어 에이전트 버전 확인] 테스트를 찾습니다. 테스트 결과가 실패이면 [원인] 열의 **원인** 링크를 클릭하여 오래된 소프트웨어 에이전트가 포함된 가상 시스템을 확인합니다.

다음에 수행할 작업

오래된 소프트웨어 에이전트가 포함된 가상 시스템이 있는 경우 **vSphere**에서 **소프트웨어 에이전트 업그레이드** 항목을 참조하십시오.

vSphere에서 소프트웨어 에이전트 업그레이드

업그레이드한 후 vRealize Automation 장치 관리를 사용하여 vSphere에서 오래된 소프트웨어 에이전트를 TLS 1.2로 업그레이드할 수 있습니다.

이 절차는 업그레이드된 환경의 가상 시스템에서 오래된 소프트웨어 에이전트를 TLS 1.2로 업데이트합니다. 대상 vRealize Automation 릴리스로 업그레이드하는 데 필요합니다.

사전 요구 사항

- 대상 vRealize Automation 릴리스로 업그레이드를 완료합니다.
- 상태 서비스를 사용하여 오래된 소프트웨어 에이전트가 포함된 가상 장치를 식별했습니다.

절차

- 1 기본 vRealize Automation 장치에서 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **root**로 vRealize Automation 장치 관리에 로그인합니다.

고가용성 환경의 경우 마스터 장치에서 장치 관리를 엽니다.

- 2 **vRA > 소프트웨어 에이전트**를 클릭합니다.

- 3 **TLS 1.0, 1.1 전환**을 클릭합니다.

TLS v1.0, v1.1 상태가 [사용]입니다.

- 4 테넌트 자격 증명의 경우 대상 vRealize Automation 장치에 대한 요청된 정보를 입력합니다.

옵션	설명
테넌트 이름	업그레이드된 vRealize Automation 장치의 테넌트 이름입니다. 참고 테넌트 사용자에게 소프트웨어 설계자 역할이 할당되어 있어야 합니다.
Username	vRealize Automation 장치의 테넌트 관리자 사용자 이름입니다.
암호	테넌트 관리자 암호입니다.

- 5 **연결 테스트**를 클릭합니다.

연결이 설정된 경우 성공 메시지가 표시됩니다.

- 6 **배치 나열**을 클릭합니다.

[배치 선택 목록] 테이블이 표시됩니다.

- 7 **표시**를 클릭합니다.

오래된 소프트웨어 에이전트가 포함된 가상 시스템 목록을 나열하는 테이블이 표시됩니다.

- 8 [업그레이드 가능] 상태에 있는 가상 시스템에 대한 소프트웨어 에이전트를 업그레이드합니다.

- 개별 가상 시스템의 소프트웨어 에이전트를 업그레이드하려면 가상 시스템 그룹에 대해 **표시**를 클릭하고, 업그레이드할 가상 시스템을 식별한 후 **실행**을 클릭하여 업그레이드 프로세스를 시작합니다.
- 가상 시스템 배치에 대해 소프트웨어 에이전트를 업그레이드하려면 업그레이드할 그룹을 식별한 후 **실행**을 클릭하여 업그레이드 프로세스를 시작합니다.

업그레이드할 가상 시스템이 200개가 넘는 경우 다음 매개 변수에 대한 값을 입력하여 배치 업그레이드 프로세스 속도를 제어할 수 있습니다.

옵션	설명
배치 크기	배치 업그레이드에 대해 선택된 가상 시스템의 수입니다. 이 숫자를 변경하여 업그레이드 속도를 조정할 수 있습니다.
대기열 크기	한 번에 수행되는 병렬 업그레이드 실행의 횟수입니다. 예: 20. 이 숫자를 변경하여 업그레이드 속도를 조정할 수 있습니다.
배치 오류	배치 업그레이드 속도 저하를 일으키는 REST 오류 수입니다. 예를 들어 업그레이드의 안정성을 향상시키기 위해 5번의 실패 후 현재 배치 업그레이드를 중지하려는 경우 텍스트 필드에 5를 입력합니다.
배치 실패	배치 처리 속도 저하를 일으키는 실패한 소프트웨어 에이전트 업그레이드 수입니다. 예를 들어 업그레이드의 안정성을 향상시키기 위해 5번의 실패 후 현재 배치 업그레이드를 중지하려는 경우 텍스트 필드에 5를 입력합니다.
배치 폴링	업그레이드 프로세스를 확인하기 위해 업그레이드 프로세스가 폴링되는 간격입니다. 이 숫자를 변경하여 업그레이드 속도를 조정할 수 있습니다.

업그레이드 프로세스가 너무 느리거나 너무 많은 업그레이드 실패를 생성하는 경우 업그레이드 성능을 향상시키기 위해 이러한 매개 변수를 조정할 수 있습니다.

참고 새로 고침을 클릭하면 배치 목록이 지워집니다. 업그레이드 프로세스에는 영향을 주지 않습니다. TLS 1.2 설정 여부에 대한 정보도 새로 고치며 또한 새로 고침을 클릭하면 vRealize Automation 서비스의 상태 점검도 수행합니다. 서비스가 실행되고 있지 않은 경우 시스템이 오류 메시지를 표시하며 다른 모든 작업 버튼을 비활성화합니다.

9 TLS 1.0, 1.1 전환을 클릭합니다.

TLS v1.0, v1.1 상태가 [사용 안 함]입니다.

Amazon Web Service 또는 Azure에서 소프트웨어 에이전트 업그레이드

AWS(Amazon Web Service) 또는 Azure에서 수동으로 가상 시스템의 모든 오래된 소프트웨어 에이전트를 업그레이드할 수 있습니다.

사전 요구 사항

- 대상 vRealize Automation 릴리스로 업그레이드를 완료합니다.
- 소프트웨어 터널이 있으며 터널 가상 시스템 IP 주소가 알려져 있습니다.

절차

- 1 업그레이드해야 하는 각 노드에 대해 노드 파일을 생성합니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

참고 인플레이스 업그레이드의 경우 \$DestinationVRAServer가 \$SourceVRAServer와 동일합니다.

2 Linux 또는 Windows 가상 시스템에서 소프트웨어 에이전트를 업그레이드하기 위한 계획 파일을 생성합니다.

- AWS 또는 Azure 끝점에 해당하는 개인 IP 주소의 값을 포함하도록 `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`에서 마이그레이션 매개 변수 파일을 수정합니다.

```
"key": "ipAddress",

    "value": {

        "type": "string",

        "value": "<$PrivateIp:$PrivatePort>"

    }
}
```

- Linux 시스템 업데이트에 다음 명령을 사용합니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL
Software.LinuxAgentUpdate "버전" --source_cloud_provider azure
```

- Windows 시스템 업데이트에 다음 명령을 사용합니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW
Software.WindowsAgentUpdate "버전" --source_cloud_provider azure
```

- 다음 명령은 계획 파일을 실행합니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/
webapps/ROOT/software/plan
```

3 1단계의 노드 파일 및 2단계의 계획 파일을 사용하여 소프트웨어 에이전트를 업데이트하려면 다음 명령을 사용합니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <
$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate "버전" --
component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/
software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --
source_cloud_provider azure --action plan_batch -S <$SourceVRAServer>
```

대안으로 노드 인덱스를 제공하여 노드 파일에서 한 번에 하나의 노드를 실행하도록 다음 명령을 사용할 수 있습니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <
$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate "버전" --
```

```
component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/
software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --
source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through
n-1>
```

이 절차를 수행하면서 vRealize Automation 가상 장치 및 호스트 시스템에서 로그를 추적하여 서버 에이전트 업그레이드 프로세스를 확인할 수 있습니다.

업그레이드한 후 업그레이드 프로세스가 Windows 또는 Linux에 대한 소프트웨어 업데이트 스크립트를 vRealize Automation 가상 장치로 가져옵니다. vRealize Automation 가상 장치 호스트로 로그인하여 소프트웨어 구성 요소를 성공적으로 가져왔는지 확인할 수 있습니다. 구성 요소를 가져온 후 소프트웨어 업데이트가 이전 EBS(Event Broker Service)로 전송되어 소프트웨어 업데이트 스크립트를 식별된 가상 시스템에 릴레이합니다. 업그레이드가 완료되고 새로운 소프트웨어 에이전트가 작동되면 ping 요청을 전송하여 새 vRealize Automation 가상 장치에 바인딩됩니다.

참고 유용한 로그 파일

- 소스 vRealize Automation에 대한 Catalina 출력: /var/log/vcac/catalina.out. 이 파일에는 에이전트 마이그레이션이 수행될 때 수행되는 업그레이드 요청이 표시됩니다. 이 작업은 소프트웨어 프로비저닝 요청을 수행하는 것과 동일합니다.
- 대상 vRealize Automation에 대한 Catalina 출력: /var/log/vcac/catalina.out. 이 파일에는 마이그레이션된 가상 시스템이 "version".O-SNAPSHOT 버전 번호를 포함하기 위해 수행한 해당 ping 요청이 보고됩니다. EBS 항목 이름(예: sw-agent-UUID)을 비교하여 이를 함께 기록할 수 있습니다.
- 대상 vRealize Automation 시스템 마스터 업그레이드 로그 파일에 대한 에이전트 업데이트 폴더: /var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log. 이 파일을 추적하여 진행 중인 업그레이드 작업을 확인할 수 있습니다.
- 개별 로그는 테넌트 폴더 /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}에서 확인할 수 있습니다. 개별 노드는 실패 및 진행 중 확장자가 포함된 많은 파일로 여기에 나열됩니다.
- 마이그레이션된 VM: /opt/vmware-appdirector/agent/logs/darwin*.log. 수신되고 있는 소프트웨어 업데이트 요청과 agent_bootstrap + 소프트웨어 에이전트의 최종적인 다시 시작을 나열하는 이 위치를 불시 점검할 수 있습니다.

vRealize Automation PostgreSQL 복제 모드를 동기식으로 설정

업그레이드 전에 PostgreSQL 복제 모드를 비동기식으로 설정했다면 분산 vRealize Automation 환경을 업그레이드한 후에 PostgreSQL 복제 모드를 동기식으로 설정할 수 있습니다.

사전 요구 사항

분산 vRealize Automation 환경을 업그레이드했습니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.
<https://vrealize-automation-appliance-FQDN:5480>
- 2 **클러스터**를 클릭합니다.
- 3 **동기식 모드**를 클릭하고 작업이 완료될 때까지 기다립니다.
- 4 [동기화 상태] 열의 모든 노드가 동기화 상태를 표시하는지 확인합니다.

다음에 수행할 작업

연결 테스트 실행 및 업그레이드된 끝점 확인.

연결 테스트 실행 및 업그레이드된 끝점 확인

이전 vRealize Automation 릴리스에서 업그레이드하면 대상 환경에서 특정 끝점이 변경됩니다.

vRealize Automation으로 업그레이드한 후에는 적용 가능한 모든 끝점에 대해 **연결 테스트** 작업을 사용해야 합니다. 업그레이드된 일부 끝점을 수정해야 할 수도 있습니다. 자세한 내용은 [업그레이드 또는 마이그레이션된 끝점 사용 시 고려 사항](#)을 참조하십시오.

업그레이드 또는 마이그레이션된 끝점의 기본 보안 설정은 신뢰할 수 없는 인증서를 허용하지 않는 것입니다.

신뢰할 수 없는 인증서를 사용하고 있는 경우에는 이전 버전의 vRealize Automation 설치에서 업그레이드 또는 마이그레이션한 후 인증서 검증을 사용하도록 모든 vSphere 및 NSX 끝점에 대해 다음 단계를 수행해야 합니다. 그렇지 않으면 인증서 오류가 발생하고 끝점 작업이 실패합니다. 자세한 내용은 <http://kb.vmware.com/kb/2150230>의 VMware 기술 자료 문서 "vRA 7.3으로 업그레이드 후 끝점 통신이 끊김 (2150230)" 및 <http://kb.vmware.com/kb/2108294>의 "웹 브라우저 인증서 주의를 방지하도록 vCenter Server 루트 인증서를 다운로드 및 설치하는 방법(2108294)"을 참조하십시오.

- 1 업그레이드 또는 마이그레이션 후에 vRealize AutomationvSphere 에이전트 시스템에 로그인하고 **서비스** 탭을 사용하여 vSphere 에이전트를 다시 시작합니다.
마이그레이션이 모든 에이전트를 다시 시작하지 못할 수 있으므로 필요한 경우 에이전트를 수동으로 다시 시작합니다.
- 2 적어도 하나 이상의 ping 보고가 완료될 때까지 기다립니다. ping 보고가 완료되려면 1~2분 정도가 소요됩니다.
- 3 vSphere 에이전트가 데이터 수집을 시작하면 vRealize Automation에 IaaS 관리자로 로그인합니다.
- 4 **인프라 > 끝점 > 끝점**을 클릭합니다.
- 5 vSphere 끝점을 편집하고 **연결 테스트**를 클릭합니다.
- 6 인증서 프롬프트가 표시되면 **확인**을 클릭하여 인증서를 수락합니다.

인증서 프롬프트가 표시되지 않으면 현재 끝점에 대한 Windows 시스템 호스팅 서비스의 신뢰할 수 있는 루트 인증 기관(예: 프록시 에이전트 시스템 또는 DEM 시스템)에 인증서가 올바르게 저장되어 있을 수 있습니다.

- 7 **확인**을 클릭하여 인증서 수락을 적용하고 끝점을 저장합니다.
- 8 각 vSphere 끝점에 대해 이 절차를 반복합니다.
- 9 각 NSX 끝점에 대해 이 절차를 반복합니다.
- 10 **인프라 > 계산 리소스**로 이동하여 **vCenter 계산** 리소스를 마우스 오른쪽 버튼으로 클릭하고 **데이터 수집**을 실행합니다.

연결 테스트 작업이 성공해도 일부 데이터 수집 또는 프로비저닝 작업이 실패하면 끝점 역할을 하는 모든 에이전트 시스템과 모든 DEM 시스템에 동일한 인증서를 설치할 수 있습니다. 또는 기존 시스템에서 인증서를 제거하고 실패한 끝점에 대해 이전 절차를 반복할 수 있습니다.

vRealize Automation에서 업그레이드한 후 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행

vRealize Automation에서 업그레이드한 후에 업그레이드된 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행해야 합니다.

이 데이터 수집 작업은 배포에서 로드 밸런서 재구성 옵션을 지원하는 데 필요합니다.

사전 요구 사항

- vRealize Automation 업그레이드 전에 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행.
- vRealize Automation을 업그레이드합니다.

절차

- ◆ 업그레이드 후 vRealize Automation에서 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행합니다. 자세한 내용은 **끝점 데이터 수집 수동 시작** 항목을 참조하십시오.

클러스터에 복제 장치 가입

마스터 vRealize Automation 장치 업데이트를 완료한 후 업데이트된 각 복제 노드가 자동으로 마스터 노드에 가입됩니다. 복제 노드를 개별적으로 업데이트해야 하는 경우 복제 노드를 클러스터에 수동으로 가입시킵니다.

절차

- 1 클러스터에 가입되지 않은 복제 노드에서, vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 2 **클러스터**를 선택합니다.
- 3 **클러스터에 가입**을 클릭합니다.

고가용성 배포를 위한 포트 구성

고가용성 배포에서 업그레이드를 완료한 후에는 포트 8444의 트래픽을 vRealize Automation 장치에 전달하도록 로드 밸런서를 구성하여 원격 콘솔 기능을 지원해야 합니다.

자세한 내용은 [vRealize Automation 설명서](#)에서 "vRealize Automation 로드 밸런싱 구성 가이드"를 참조하십시오.

외부 워크플로 시간 초과 파일 복원

업그레이드 프로세스에서 xmlldb 파일을 덮어쓰기 때문에 vRealize Automation 외부 워크플로 시간 초과 파일을 재구성해야 합니다.

절차

- 1 시스템의 다음 디렉토리에서 외부 워크플로 구성(xmlldb) 파일을 엽니다.

`\VMware\VCAC\Server\ExternalWorkflows\xmlldb\.`

- 2 xmlldb 파일을 마이그레이션 전에 백업한 파일로 바꿉니다. 백업 파일이 없는 경우 외부 워크플로 시간 초과 설정을 재구성합니다.
- 3 설정을 저장합니다.

app.config 파일에 로깅 변경 내용 복원

업그레이드 프로세스에서는 구성 파일에서 로깅과 관련하여 변경한 내용을 덮어씁니다. 업그레이드를 완료했으면 업그레이드하기 전에 변경한 내용을 `app.config` 파일에 복원해야 합니다.

사전 요구 사항 작업 중에 백업한 IaaS 서버에 대해 병합을 수행하거나 *.exe.config 파일(예: `managerservice.exe.config`)의 수정 사항을 덮어쓰지 않고 변경 내용을 복원할 수 있습니다.

Azure 끝점 업그레이드 후 재구성

업그레이드 후에는 Microsoft Azure 끝점을 재구성해야 합니다.

Microsoft Azure 끝점 각각에 대해 이 절차를 수행합니다.

사전 요구 사항

- vRealize Automation의 대상 버전으로 업그레이드를 완료합니다.
- 대상 vRealize Automation 콘솔에 로그인합니다.
 - a 대상 가상 장치의 정규화된 도메인 이름(`https://vra-vd-hostname.domain.name/vcac`)을 사용하여 vRealize Automation 콘솔을 엽니다.
고가용성 환경인 경우, 대상 가상 장치 로드 밸런서의 정규화된 도메인 이름(`https://vra-vd-lb-hostname.domain.name/vcac`)을 사용하여 콘솔을 엽니다.
 - b IaaS 관리자 사용자로 로그인합니다.

절차

- 1 **관리 > vRO 구성 > 끝점**을 선택합니다.
- 2 Microsoft Azure 끝점을 선택합니다.
- 3 **편집**을 클릭합니다.

- 4 세부 정보를 클릭합니다.
- 5 Azure 환경 드롭다운 메뉴에서 영역을 선택합니다.
- 6 클라이언트 암호 텍스트 상자에 원래 클라이언트 암호를 입력합니다.
- 7 Azure 스토리지 URI 텍스트 상자에 스토리지 URL을 입력합니다.
예: https://mystorageaccount.blob.core.windows.net
- 8 완료를 클릭합니다.
- 9 각 Azure 끝점에 대해 반복합니다.

업그레이드 후 자동 **Manager Service** 페일오버를 사용하도록 설정

vRealize Automation을 업그레이드하면 자동 Manager Service 페일오버는 기본적으로 사용하지 않도록 설정됩니다.

업그레이드 후 자동 Manager Service 페일오버를 사용하도록 설정하려면 다음 단계를 완료합니다.

절차

- 1 vRealize Automation 장치에서 루트로 명령 프롬프트를 엽니다.
- 2 디렉토리를 `/usr/lib/vcac/tools/vami/commands`로 변경합니다.
- 3 자동 Manager Service 페일오버를 사용하도록 설정하려면 다음 명령을 실행합니다.

```
python ./manager-service-automatic-failover ENABLE
```

IaaS 배포 전체에서 자동 페일오버를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

```
python ./manager-service-automatic-failover DISABLE
```

자동 **Manager Service** 페일오버 정보

기본 Manager Service가 중지되면 백업으로 자동 페일오버되도록 vRealize Automation IaaS Manager Service를 구성할 수 있습니다.

vRealize Automation 7.3부터 기본 또는 백업 역할을 할 호스트를 제어하기 위해 이제 더 이상 각 Windows Server에서 Manager Service를 수동으로 시작 또는 중지할 필요가 없습니다. 업그레이드 셸 스크립트 또는 IaaS 설치 관리자 실행 파일을 사용하여 IaaS를 업그레이드하는 경우에는 자동 Manager Service 페일오버가 기본적으로 사용하지 않도록 설정됩니다.

자동 페일오버를 사용하도록 설정하면 백업을 포함한 모든 Manager Service 호스트에서 Manager Service가 자동으로 시작됩니다. 자동 페일오버 기능을 사용하면 호스트가 서로를 투명하게 모니터링하고 필요한 경우 페일오버할 수 있지만 모든 호스트에서 Windows 서비스가 실행되고 있어야 합니다.

참고 자동 페일오버를 사용하지 않아도 됩니다. 자동 페일오버를 사용하지 않도록 설정하고 Windows 서비스를 계속 수동으로 시작하고 중지하여 기본 또는 백업 역할을 할 호스트를 제어할 수 있습니다. 수동 페일오버 방식을 사용하는 경우 한 번에 하나의 호스트에서만 서비스를 시작해야 합니다. 자동 페일오버가 사용되지 않도록 설정된 상태로 여러 IaaS 서버에서 동시에 서비스를 실행하면 vRealize Automation을 사용할 수 없게 됩니다.

자동 페일오버를 선택적으로 사용 또는 사용하지 않도록 설정하지 마십시오. 자동 페일오버는 IaaS 배포의 모든 Manager Service 호스트에서 설정되거나 해제된 상태로 항상 동기화되어야 합니다.

DynamicTypes 플러그인 가져오기

DynamicTypes 플러그인을 사용하고 업그레이드 전에 구성을 패키지로 내보낸 경우 다음 워크플로를 가져와야 합니다.

- 1 대상 환경에서 동적 유형 구성을 가져옵니다.
 - a Java Client에 관리자로 로그인합니다.
 - b **워크플로** 탭을 선택합니다.
 - c **라이브러리 > 동적 유형 > 구성**을 선택합니다.
 - d **패키지에서 구성 가져오기** 워크플로를 선택하고 실행합니다.
 - e **가져올 구성 패키지**를 클릭합니다.
 - f 내보낸 패키지 파일을 찾아 **파일 첨부**를 클릭합니다.
 - g 패키지에 연결된 네임스페이스에 대한 정보를 검토하고 **제출**을 클릭합니다.
- 2 **인벤토리 > 동적 유형**을 선택하여 동적 유형 네임스페이스를 가져왔는지 확인합니다.

VMware Identity Manager Connector 업그레이드

vRealize Automation 애플리케이션을 7.5로 업그레이드한 후, 스마트 카드 인증을 위해 외부 VMware Identity Manager Connector(vIDM)를 업그레이드해야 할 수도 있습니다.

vRealize Automation 7.5에는 vIDM 버전 3.1 이상이 필요합니다. 최신 vIDM 버전으로 업그레이드하는 방법에 대한 자세한 내용은 [VMware Identity Manager 설명서](#)를 참조하십시오.

참고 vIDM 커넥터가 2.7 이하 버전인 경우, 먼저 2.8.3으로 업그레이드한 다음 3.1 이상으로 업그레이드해야 합니다.

vRealize Automation 업그레이드 문제 해결

업그레이드 문제 해결 항목에서는 vRealize Automation 7.1 이상에서 업그레이드할 때 발생할 수 있는 문제에 대한 해결 방법을 제공합니다.

자동 Manager Service 페일오버가 활성화되지 않음

manager-service-automatic-failover 명령 문제 해결을 위한 제안 사항입니다.

해결책

- ◆ manager-service-automatic-failover 명령이 실패하거나, 2분 넘게 다음 메시지가 표시됩니다. 다음 노드에 Manager Service 자동 페일오버 모드를 사용하도록 설정하는 중:

IAAS_MANAGER_SERVICE_NODEID.

- a vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

b 클러스터를 선택합니다.

c 관리 에이전트 서비스가 모든 Manager Service 호스트에서 실행 중인지 확인합니다.

d 모든 IaaS Manager Service 노드의 마지막 연결 시간이 30초 미만인지 확인합니다.

관리 에이전트 연결 문제가 발견될 경우, 문제를 수동으로 해결하고 Manager Service 자동 페일오버를 사용하도록 설정하는 명령을 다시 시도하십시오.

- ◆ manager-service-automatic-failover 명령이 Manager Service 노드에서 페일오버를 사용하도록 설정하지 못합니다. 문제를 해결하기 위해 명령을 다시 실행할 수 있습니다.
- ◆ IaaS 배포에 있는 일부 Manager Service 호스트는 페일오버를 사용하도록 설정된 반면 다른 호스트는 페일오버를 사용하지 않도록 설정되었습니다. IaaS 배포에 있는 모든 Manager Service 호스트에 이 기능이 설정되어 있어야 하며, 그렇지 않을 경우 기능이 작동하지 않습니다. 이 문제를 해결하려면 다음 중 하나를 수행합니다.
 - 모든 Manager Service 노드에서 페일오버를 사용하지 않도록 설정하고, 수동 페일오버 방식을 대신 사용합니다. 한 번에 하나의 호스트에서만 페일오버를 실행합니다.
 - Manager Service 노드에서 이 기능을 사용하도록 설정하는 시도가 여러 번 실패할 경우, 이 노드에서 Windows VMware vCloud Automation Center 서비스를 중지하고, 문제가 해결될 때까지 노드 시작 유형을 [수동]으로 설정합니다.
- ◆ Python을 사용하여, 각 Manager Service 노드가 페일오버를 사용하도록 설정되었는지 검증합니다.
 - a SSH를 사용하여 마스터 vRealize Automation 장치에 **root**로 로그인합니다.
 - b `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover ENABLE`을 실행합니다.
 - c 다음 노드에 Manager Service 자동 페일오버 모드를 사용하도록 설정하는 중:
`IAAS_MANAGER_SERVICE_NODEID` 완료 메시지를 시스템에서 반환하는지 확인합니다.
- ◆ Manager Service 구성 파일을 검사하여 각 Manager Service 노드가 페일오버를 사용하도록 설정되었는지 검증합니다.
 - a Manager Service 노드에서 명령 프롬프트를 엽니다.
 - b vRealize Automation 설치 폴더로 이동하여 Manager Service 구성 파일(`VMware\VCAC\Server\ManagerService.exe.config`)을 엽니다.
 - c <appSettings> 섹션에 다음 요소가 있는지 확인합니다.
 - `<add key="FailoverModeEnabled" value="True" />`
 - `<add key="FailoverPingIntervalMilliseconds" value="30000" />`
 - `<add key="FailoverNodeState" value="active" />`
 - `<add key="FailoverMaxFailedDatabasePingAttempts" value="5" />`
 - `<add key="FailoverMaxFailedRepositoryPingAttempts" value="5" />`

- ◆ Windows VMware vCloud Automation Center 서비스 상태가 [시작됨]이고 시작 유형이 [자동]인지 확인합니다.
- ◆ Python을 사용하여, 각 Manager Service 노드가 페일오버를 사용하지 않도록 설정되었는지 검증합니다.
 - a SSH를 사용하여 마스터 vRealize Automation 장치에 **root**로 로그인합니다.
 - b `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover DISABLE`을 실행합니다.
 - c 노드에서 Manager Service 자동 페일오버 모드를 사용하지 않도록 설정하는 중:
`IAAS_MANAGER_SERVICE_NODEID` 완료 메시지를 시스템에서 반환하는지 확인합니다.
- ◆ Manager Service 구성 파일을 검사하여 각 Manager Service 노드가 페일오버를 사용하지 않도록 설정되었는지 검증합니다.
 - a Manager Service 노드에서 명령 프롬프트를 엽니다.
 - b vRealize Automation 설치 폴더로 이동하여 Manager Service 구성 파일(`VMware\VCAC\Server\ManagerService.exe.config`)을 엽니다.
 - c <appSettings> 섹션에 다음 요소가 있는지 확인합니다.
 - `<add key="FailoverModeEnabled" value="False" />`
- ◆ 콜드 대기 Manager Service 노드를 생성하려면 Windows VMware vCloud Automation Center 서비스 노드 상태를 [중지됨]으로 설정하고 시작 유형을 [수동]으로 설정합니다.
- ◆ 액티브 Manager Service 노드의 경우에는 Windows VMware vCloud Automation Center 서비스 노드 상태가 [시작됨]이고 시작 유형이 [자동]이어야 합니다.
- ◆ `manager-service-automatic-failover` 명령이 Manager Service 노드 내부 ID - `IAAS_MANAGER_SERVICE_NODEID`를 사용합니다 이 내부 ID에 해당하는 호스트 이름을 찾으려면 `vra-command list-nodes` 명령을 실행하고 노드 ID가 `IAAS_MANAGER_SERVICE_NODEID`인 Manager Service 호스트를 찾습니다.
- ◆ 시스템에서 현재 활성 상태로 자동 선택한 Manager Service를 찾으려면 다음 단계를 수행합니다.
 - a SSH를 사용하여 마스터 vRealize Automation 장치에 **root**로 로그인합니다.
 - b `vra-command list-nodes --components`를 실행합니다.
 - 페일오버를 사용하도록 설정된 경우, 상태가 [활성]인 Manager Service 노드를 찾습니다.
 - 페일오버를 사용하지 않도록 설정된 경우, 상태가 [시작됨]인 Manager Service 노드를 찾습니다.

로드 밸런서 시간 초과 오류와 함께 설치 또는 업그레이드가 실패함

로드 밸런서가 있는 분산 배포의 vRealize Automation 설치 또는 업그레이드가 503 서비스 사용 불가 오류를 표시하며 실패합니다.

문제

로드 밸런서 시간 초과 설정에서 작업을 완료할 시간이 충분히 허용되지 않아서 설치 또는 업그레이드가 실패합니다.

원인

로드 밸런서 시간 초과 설정이 충분하지 않아서 실패가 발생할 수 있습니다. 로드 밸런서 시간 초과 설정을 100초 이상으로 늘리고 작업을 다시 실행하여 문제를 수정할 수 있습니다.

해결책

- 1 로드 밸런서 시간 초과 값을 100초 이상으로 늘리십시오.
- 2 설치 또는 업그레이드를 다시 실행하십시오.

IaaS 웹 사이트 구성 요소에 대한 업그레이드 실패

IaaS 업그레이드가 실패하고 업그레이드를 계속할 수 없습니다.

문제

웹 사이트 구성 요소에 대해 IaaS 업그레이드가 실패합니다. 다음 오류 메시지가 설치 관리자 로그 파일에 표시됩니다.

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- Description: An application error
occurred on the server. The current custom error settings for this application
prevent the details of the application error from being viewed remotely (for
security reasons). It could, however, be viewed by browsers running on the
local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files
(x86)\VMware\VCAC\Server\Model Manager Data\DeployRepository.xml"
(InstallRepoModel target(s)) -- FAILED.

다음 오류 메시지가 저장소 로그 파일에 표시됩니다.

- [Error]: [sub-thread-Id="20"
context="" token=""] Failed to start repository service. Reason:
System.InvalidOperationException: Configuration section encryptionKey is not
protected

```

at
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration
config)
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2
decryptFunc)
at
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object
t
sender, ObjectMaterializedEventArgs e)
at
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()
at
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
at
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValu
e(CoreModelEntities
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().

```

원인

laaS 업그레이드는 **web.config** 파일의 생성 날짜가 수정된 날짜와 같거나 이후인 경우에 실패합니다.

해결책

- 1 laaS 호스트에서 Windows에 로그인합니다.
- 2 Windows 명령 프롬프트를 엽니다.
- 3 vRealize Automation 설치 폴더로 디렉토리를 변경합니다.

4 관리자 권한으로 실행 옵션으로 기본 텍스트 편집기를 시작합니다.

5 web.config 파일을 찾아 선택하고 파일을 저장하여 해당 파일 수정 날짜를 변경합니다.

6 web.config 파일 속성을 검사하여 파일 수정 날짜가 생성 날짜 이후인지 확인합니다.

7 IaaS를 업그레이드합니다.

Manager Service가 런타임 중에 SSL 검증 오류로 인해 실행되지 못함

Manager Service가 SSL 검증 오류로 인해 실행되지 못합니다.

문제

Manager Service가 로그의 다음 오류 메시지와 함께 실패합니다.

[Info]: Thread-Id="6" - context="" token="" 핵심 데이터베이스에 연결하지 못함, 00:00:05
이내에 재시도함, 오류 세부 정보: 서버에 연결했지만 로그인하는 동안 오류가 발생했습니다. (제
공사: SSL 제공자, 오류: 0 - 인증서 체인이 신뢰할 수 없는 기관으로부터 발급되었습니다.)

원인

런타임 중에 Manager Service가 SSL 검증 오류로 인해 실행되지 못합니다.

해결책

1 ManagerService.config 구성 파일을 엽니다.

2 다음 줄에서 **Encrypt=False**를 업데이트합니다.

```
<add name="vcac-repository" providerName="System.Data.SqlClient" connectionString="Data
Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated Security=True;Pooling=True;Max
Pool Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

업그레이드 후 로그인 실패

동기화되지 않은 사용자 계정을 사용하는 세션에 대한 업그레이드 후에는 브라우저를 종료하고 다시 로그인해야 합니다.

문제

vRealize Automation을 업그레이드한 후 로그인할 때 시스템에서 동기화되지 않은 사용자 계정에 대한 액세스를 거부합니다.

해결책

브라우저를 종료하고 vRealize Automation을 다시 시작합니다.

vRealize Automation에서 분리된 노드 삭제

분리된 노드는 호스트에서 보고되었지만 호스트에 없는 중복된 노드입니다.

문제

각각의 IaaS 및 가상 장치 노드가 정상 상태인지 확인할 때 호스트에 하나 이상의 분리된 노드가 있는 것을 발견할 수도 있습니다. 분리된 노드는 모두 삭제해야 합니다.

해결책

- 1 기본 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

`https://vrealize-automation-appliance-FQDN:5480`

- 2 클러스터를 선택합니다.

- 3 테이블에 표시된 각 분리된 노드에 대해 **삭제**를 클릭합니다.

고가용성 환경을 업그레이드한 후 클러스터에 가입 명령이 실패함

보조 클러스터 노드의 vRealize Automation 장치 관리 인터페이스에서 **클러스터에 가입**을 클릭했을 때 진행률 표시기가 사라집니다.

문제

업그레이드 후 vRealize Automation 장치 관리 인터페이스를 사용하여 기본 노드에 보조 클러스터 노드를 가입시키면 진행률 표시기가 사라지고 오류 또는 성공 메시지가 표시되지 않습니다. 이 동작은 간헐적으로 발생하는 문제입니다.

원인

진행률 표시기가 사라지는 이유는 일부 브라우저가 서버의 응답 대기를 중지하기 때문입니다. 이 동작으로 클러스터에 가입 프로세스가 중지되지는 않습니다. `/var/log/vmware/vcac/vcac-config.log`에서 로그 파일을 확인하여 클러스터에 가입 프로세스가 성공했는지 확인할 수 있습니다.

PostgreSQL 데이터베이스 업그레이드 병합 실패

외부 PostgreSQL 데이터베이스와 포함된 PostgreSQL 데이터베이스 병합이 실패합니다.

문제

PostgreSQL 데이터베이스 업그레이드 병합이 성공하지 못한 경우 수동 병합을 수행할 수 있습니다.

해결책

- 1 vRealize Automation 가상 장치를 업그레이드 이전에 생성한 스냅샷으로 되돌립니다.
- 2 데이터베이스 병합이 실패하는 경우 vRealize Automation 가상 장치에 로그인하고 다음 명령을 실행하여 업그레이드를 완료합니다.

```
touch /tmp/allow-external-db
```

이 명령으로 자동 병합이 사용되지 않도록 설정되지는 않습니다.

- 3 원격 PostgreSQL 데이터베이스 호스트에서 psql 도구를 사용하여 PostgreSQL 데이터베이스에 연결하고 다음 명령을 실행합니다.

```
CREATE EXTENSION IF NOT EXISTS "hstore";
```

```
CREATE EXTENSION IF NOT EXISTS "uuid-oss";
```

```
CREATE SCHEMA saas AUTHORIZATION vcac;
```

이 명령의 사용자는 vcac입니다. vRealize Automation이 다른 사용자로 외부 데이터베이스에 연결하는 경우 이 명령의 vcac를 해당 사용자의 이름으로 바꿉니다.

```
CREATE EXTENSION IF NOT EXISTS "citext" SCHEMA saas;
```

- 4 업그레이드를 실행합니다.

업그레이드가 성공하면 시스템이 외부 PostgreSQL 데이터베이스와 함께 예상대로 작동합니다. 외부 PostgreSQL 데이터베이스가 제대로 실행되고 있는지 확인합니다.

- 5 vRealize Automation 가상 장치에 로그인하고 다음 명령을 실행합니다.

```
/etc/bootstrap/postupdate.d/00-20-db-merge-external
```

```
/etc/bootstrap/postupdate.d/11-db-merge-external
```

복제 vRealize Automation 장치의 업데이트가 실패함

마스터 장치 업데이트 중 복제 vRealize Automation 장치를 업데이트하지 못합니다.

원인

연결 문제 또는 다른 오류 때문에 복제 장치를 업데이트하지 못할 수 있습니다. 이런 경우 마스터 vRealize Automation 장치 **업데이트** 탭에서 업데이트하지 못한 복제를 강조 표시하는 주의 메시지가 표시됩니다.

해결책

- 1 복제 가상 장치 스냅샷을 되돌리거나 사전 업데이트 상태로 백업하고 전원을 켭니다.
- 2 복제 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.
<https://vrealize-automation-appliance-FQDN:5480>
- 3 **업데이트 > 설정**을 클릭합니다.
- 4 [업데이트 저장소] 섹션에서 VMware 저장소 또는 CDROM에서 업데이트를 다운로드하도록 선택합니다.
- 5 **상태**를 클릭합니다.
- 6 **업데이트 확인**을 클릭하여 업데이트가 있는지 확인합니다.
- 7 **업데이트 설치**를 클릭합니다.

8 확인을 클릭합니다.

업데이트가 진행 중임을 알리는 메시지가 나타납니다.

9 로그 파일을 열어 업그레이드가 성공적으로 진행되고 있는지 확인합니다.

- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`

업그레이드 프로세스 중에 로그아웃했다가 업그레이드가 완료되기 전에 다시 로그인하는 경우 계속하여 로그 파일의 업데이트 진행률을 파악할 수 있습니다. `updatecli.log` 파일에 업그레이드 이전의 vRealize Automation 버전에 대한 정보가 표시될 수 있습니다. 표시된 이 버전이 업그레이드 프로세스의 후반부에 올바른 버전으로 변경됩니다.

업데이트를 완료하는 데 필요한 시간은 환경에 따라 다릅니다.

10 업데이트가 완료되면 가상 장치를 재부팅합니다.

- a **시스템**을 클릭합니다.
- b **재부팅**을 클릭하고 선택을 확인합니다.

11 클러스터를 선택합니다.**12** 마스터 vRealize Automation 장치 FQDN을 입력하고 **클러스터에 가입**을 클릭합니다.**.xml 파일 백업 복사본으로 인한 시스템 시간 초과**

vRealize Automation은 확장명이 .xml인 모든 파일을 \VMware\VCAC\Server\ExternalWorkflows\xml\db\ 디렉토리에 등록합니다. 이 디렉토리에 확장명이 .xml인 백업 파일이 포함되어 있으면 시스템 시간 초과를 유발하는 중복 워크플로가 실행됩니다.

해결 방법: 이 디렉토리에 파일을 백업하는 경우에는 해당 백업을 다른 디렉토리로 이동하거나 백업 파일의 확장명을 .xml이 아닌 값으로 변경하십시오.

IaaS 업그레이드 제외

IaaS 구성 요소를 업그레이드하지 않고 vRealize Automation 장치를 업데이트할 수 있습니다.

IaaS 구성 요소를 업그레이드하지 않고 vRealize Automation 장치를 업데이트하려는 경우 다음 절차를 사용합니다. 이 절차에서는

- IaaS 서비스를 중지하지 않습니다.
- 관리 에이전트 업데이트를 건너뜁니다.
- vRealize Automation 장치 업데이트 후 IaaS 구성 요소의 자동 업데이트를 차단합니다.

절차

- 1** 기본 vRealize Automation 장치 노드에 대한 보안 셸 연결을 엽니다.
- 2** 명령 프롬프트에서 다음 명령을 실행하여 전환 파일을 생성합니다.

```
touch /tmp/disable-iaas-upgrade
```

3 IaaS 서비스를 수동으로 중지합니다.

- a IaaS Windows Server에 로그인합니다.
- b 시작 > 관리 도구 > 서비스를 선택합니다.
- c 다음과 같은 순서로 이러한 서비스를 중지합니다.

참고 IaaS Windows Server를 종료하지 않습니다.

- 1 각 VMware vRealize Automation 프록시 에이전트.
 - 2 각 VMware DEM 작업자.
 - 3 VMware DEM 조정자.
 - 4 VMware vCloud Automation Center 서비스.
- 4** 기본 vRealize Automation 장치 관리 인터페이스에 액세스하고 기본 vRealize Automation 장치를 업데이트합니다.

vRealize Automation에서 새 디렉토리를 생성할 수 없음

첫 번째 동기화 커넥터가 있는 새 디렉토리를 추가하려는 시도가 실패합니다.

문제

이 문제는 `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`에 있는 잘못된 `config-state.json` 파일로 인해 발생합니다.

이 문제를 해결하는 방법에 대한 자세한 내용은 [기술 자료 문서 2145438](#)을 참조하십시오.

vRealize Automation 복제 가상 장치 업데이트가 시간 초과됨

마스터 가상 장치를 업데이트할 때 vRealize Automation 복제 가상 장치 업데이트가 시간 초과됩니다.

문제

마스터 가상 장치를 업데이트할 때 마스터 vRealize Automation 관리 인터페이스 [업데이트] 탭에 업데이트 시간 초과 제한에 도달한 복제 가상 장치가 강조 표시되어 나타납니다.

원인

성능 문제나 인프라 문제 때문에 업데이트 시간이 초과됩니다.

해결책

1 복제 가상 장치 업데이트 진행률을 확인합니다.

- a 복제 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- b **업데이트 > 상태**를 선택하고 업데이트 진행률을 확인합니다.

다음 중 하나를 수행합니다.

- 업데이트가 실패한 경우, 문제 해결 항목 **복제 vRealize Automation 장치의 업데이트가 실패함**에 나와 있는 단계를 따릅니다.
- 복제 가상 장치 업그레이드가 진행 중인 경우, 업데이트를 마칠 때까지 기다렸다가 2단계로 이동합니다.

2 가상 장치를 재부팅합니다.

- a **시스템**을 클릭합니다.
- b **재부팅**을 클릭하고 선택을 확인합니다.

3 클러스터를 선택합니다.

4 마스터 vRealize Automation 가상 장치 FQDN을 입력하고 **클러스터에 가입**을 클릭합니다.

업그레이드 시 일부 가상 시스템의 배포가 생성되지 않음

업그레이드할 때 누락된 상태의 가상 시스템에 대해서는 해당하는 배포가 대상 환경에 생성되지 않습니다.

문제

업그레이드 시 소스 환경에서 가상 시스템이 누락된 상태인 경우, 해당하는 배포가 대상 환경에 생성되지 않습니다. 업그레이드 이후에 가상 시스템이 더 이상 누락된 상태가 아니면 대량 가져오기를 사용하여 시스템을 대상 배포로 가져올 수 있습니다.

인증서를 신뢰할 수 없음 오류

vRealize Automation 장치 콘솔에서 인프라 [로그 뷰어] 페이지를 확인할 때, **Certificate is not trusted** 메시지가 포함된 끝점 연결 장애 보고서가 표시될 수 있습니다.

문제

vRealize Automation 장치 콘솔에서 **인프라 > 모니터링 > 로그**를 선택합니다. [로그 뷰어] 페이지에 다음과 유사한 보고서가 표시될 수 있습니다.

끝점에 연결하지 못했습니다. 이 끝점에 대해 보안 연결을 설정할 수 있는지 검증하려면 [끝점] 페이지에서 vSphere 끝점으로 이동한 후 [연결 테스트]를 클릭합니다.

내부 예외: 인증서를 신뢰할 수 없습니다(RemoteCertificateChainErrors). 주체: C=US, CN=vc6.mycompany.com 지문: DC5A8816231698F4C9013C42692B0AF93D7E35F1

원인

vRealize Automation의 이전 릴리스에서 업그레이드하면 원래 환경의 끝점이 변경됩니다. vRealize Automation 업그레이드 후 IaaS 관리자는 보안 **https** 연결을 사용하는 업그레이드된 각 끝점을 검토해야 합니다. 끝점에 **Certificate is not trusted** 오류가 있으면 해당 끝점이 제대로 작동하지 않습니다.

해결책

- 1 인프라 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 2 **인프라 > 끝점 > 끝점**을 선택합니다.
- 3 보안 연결을 사용하는 각 끝점에 대해 다음 단계를 완료합니다.
 - a **편집**을 클릭합니다.
 - b **연결 테스트**를 클릭합니다.
 - c 인증서 세부 정보를 검토한 후, 인증서를 신뢰할 수 있으면 **확인**을 클릭합니다.
 - d 이 끝점에 사용되는 모든 IaaS 프록시 에이전트에 대한 Windows 서비스를 다시 시작합니다.
- 4 인프라 [로그 뷰어] 페이지에 **Certificate is not trusted** 오류가 더 이상 표시되지 않는지 확인합니다.

사전 요구 사항 수정을 적용하는 동안 vRealize Automation 업그레이드 설치 실패

vRealize Automation 설치 또는 업그레이드가 실패하고 로그 파일에 오류 메시지가 나타납니다.

문제

vRealize Automation 설치 또는 업그레이드 시 해당 절차가 실패합니다. 일반적으로 이 문제는 설치 또는 업그레이드 중에 수정이 제대로 적용되지 않은 경우에 발생합니다. 로그 파일에 **Security error.**

Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped와 유사한 오류 메시지가 나타납니다.

원인

Windows 환경에 [사용]으로 설정된 PowerShell 스크립트 실행에 대한 그룹 정책이 있습니다.

해결책

- 1 Windows 호스트 시스템에서 **gpedit.msc**를 실행하여 로컬 그룹 정책 편집기를 엽니다.
- 2 왼쪽 창의 **컴퓨터 구성** 아래에서 확장 버튼을 클릭하여 **관리 템플릿 > Windows 구성 요소 > Windows PowerShell**을 엽니다.
- 3 **스크립트 실행 설정**의 경우 상태를 **Enabled**에서 **Not Configured**로 변경합니다.

DEM 및 DEO 구성 요소를 업데이트할 수 없음

vRealize Automation을 7.2에서 7.3.x로 업그레이드하는 동안 DEM 및 DEO 구성 요소를 업데이트할 수 없습니다.

문제

vRealize Automation 7.2를 7.3.x로 업그레이드한 후 사용자 지정 경로(예: D: 드라이브)에 설치된 DEM 및 DEO 구성 요소가 업데이트되지 않습니다.

기술 자료 문서 2150517을 참조하십시오.

업데이트를 통한 관리 에이전트 업그레이드 실패

vRealize Automation 장치 관리 인터페이스 [업데이트 상태] 페이지에서 **업데이트 설치**를 클릭하면 관리 에이전트에 대한 오류 메시지가 표시됩니다.

문제

업그레이드 프로세스가 실패했습니다. 다음 메시지가 나타납니다. 노드 x에서 관리 에이전트를 업그레이드할 수 없습니다. 메시지가 두 개 이상의 노드를 나열하는 경우가 종종 있습니다.

원인

이 문제는 여러 가지 상황에 의해 발생할 수 있습니다. 오류 메시지는 영향을 받은 시스템의 노드 ID만 식별합니다. 자세한 정보는 명령이 실패한 시스템의 관리 에이전트에 대한 **All.log** 파일에서 찾을 수 있습니다.

상황에 따라 영향을 받는 노드에 대해 다음 작업을 수행하십시오.

해결책

- ◆ 관리 에이전트 서비스가 실행 중이 아닌 경우 서비스를 시작하고 가상 장치에서 업그레이드를 다시 시작합니다.
- ◆ 관리 에이전트 서비스가 실행 중이고 관리 에이전트가 업그레이드된 경우 가상 장치에서 업그레이드를 다시 시작합니다.
- ◆ 관리 에이전트 서비스가 실행 중이지만 관리 에이전트가 업그레이드되지 않은 경우 수동 업그레이드를 수행합니다.
 - a 브라우저에서 [IaaS 설치] 페이지로 이동합니다.
<https://vrealize-automation-appliance-FQDN:5480/installer>
 - b 관리 에이전트 설치 관리자를 다운로드하고 실행합니다.
 - c 관리 에이전트 시스템을 재부팅합니다.
 - d 가상 장치에서 업그레이드를 다시 시작합니다.

관리 에이전트 업그레이드 실패

vRealize Automation 업그레이드 중에 관리 에이전트 업그레이드가 실패합니다.

문제

파일오버 문제로 인해 기본 및 보조 관리 에이전트 호스트가 전환된 경우 자동화된 업그레이드 프로세스가 필요한 호스트를 찾지 못해 업그레이드가 실패합니다. 관리 에이전트가 업그레이드되지 않은 각 IaaS 노드에서 이 절차를 수행합니다.

해결책

- 1 관리 에이전트 로그 폴더(C:\Program Files (x86)\VMware\vCAC\Management Agent\Logs\)\에서 All.log를 엽니다.

설치 폴더의 위치가 기본 위치와 다를 수 있습니다.

- 2 로그 파일에서 오래되거나 전원이 꺼진 가상 장치에 관한 메시지를 검색합니다.

예: INNER EXCEPTION: System.Net.WebException: 원격 서버에 연결할 수 없습니다. ---> System.Net.Sockets.SocketException: 연결된 대상이 일정 시간 이후에 제대로 응답하지 않아 연결 시도가 실패했거나 연결된 호스트가 응답하지 않아 설정된 연결이 실패했습니다.
IP_Address: 5480

- 3 C:\Program Files (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config에 있는 관리 에이전트 구성 파일을 편집하여 기존 alternativeEndpointaddress 값을 기본 가상 장치 끝점의 URL로 바꿉니다.

설치 폴더의 위치가 기본 위치와 다를 수 있습니다.

VMware.IaaS.Management.Agent.exe.config에 있는 alternativeEndpointaddress의 예.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="thumbprint number" />
```

- 4 관리 에이전트 Windows 서비스를 다시 시작하고 All.log 파일을 검토하여 작동 중인지 확인합니다.
- 5 기본 vRealize Automation 장치에서 업그레이드 절차를 실행합니다.

기본 시간 초과 설정 때문에 vRealize Automation 업데이트가 실패함

사용자 환경에서 데이터베이스 동기화를 위한 기본 설정이 너무 짧은 경우 업데이트를 위한 시간 설정을 늘릴 수 있습니다.

문제

데이터베이스 동기화가 3600초의 기본값보다 오래 걸리는 일부 환경에서는 Vcac-Config SynchronizeDatabases 명령에 대한 시간 초과 설정이 충분하지 않습니다.

Vcac-Config.exe.config 파일의 cafeTimeoutInSeconds 및 cafeRequestPageSize 속성 값은 API와 Vcac-config.exe 유틸리티 도구 간의 통신을 제어합니다. 해당 파일은 IaaS 설치 위치\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config에 있습니다.

다음 선택적 매개 변수에 대해 값을 제공하여 SynchronizeDatabases 명령에 대해서만 기본 시간 초과 값을 재정의할 수 있습니다.

매개 변수	짧은 이름	설명
--DatabaseSyncTimeout	-dstm	초 단위로 SynchronizeDatabases 전용 http 요청 시간 초과 값을 설정합니다.
--DatabaseSyncPageSize	-dsps	예약 또는 예약 정책 동기화 전용 동기화 요청 페이지 크기를 설정합니다. 기본값은 10입니다.

이러한 매개 변수가 **Vcac-Config.exe.config** 파일에 설정되지 않은 경우 시스템은 기본 시간 초과 값을 사용합니다.

고가용성 환경에서 IaaS 업그레이드 실패

로드 밸런싱을 사용하도록 설정하고 기본 웹 서버 노드에서 IaaS 업그레이드 프로세스를 실행하면 실패합니다. 다음과 같은 오류 메시지가 표시될 수 있습니다. "System.Net.WebException: 작업이 시간 초과됨" 또는 "401 - 승인되지 않음: 잘못된 자격 증명으로 인해 액세스가 거부되었습니다."

문제

로드 밸런싱을 사용하도록 설정한 상태에서 IaaS를 업그레이드하면 간헐적으로 장애가 발생할 수 있습니다. 이러한 문제가 발생하면 로드 밸런싱을 사용하지 않도록 설정하고 vRealize Automation 업그레이드를 다시 실행해야 합니다.

해결책

- 1 환경을 업데이트 전 스냅샷으로 되돌립니다.
- 2 기본 IaaS 웹 서버 노드에 대한 원격 데스크톱 연결을 엽니다.
- 3 Windows hosts 파일이 있는 위치(c:\windows\system32\drivers\etc)로 이동합니다.
- 4 hosts 파일을 열고 웹 서버 로드 밸런서를 생략하도록 이 줄을 추가합니다.
IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn
예:
10.10.10.5 vra-iaas-web-lb.domain.com
- 5 hosts 파일을 저장하고 vRealize Automation 업데이트를 다시 시도합니다.
- 6 vRealize Automation 업데이트가 완료되면 hosts 파일을 열고 4단계에서 추가한 줄을 제거합니다.

업그레이드 후 스토리지가 지연될 수 있음

예약 탭에 스토리지가 표시되지 않습니다.

업그레이드 후 [예약] 탭에 스토리지가 표시되지 않으면 모든 노드에서 **vcac-server**를 다시 시작해야 합니다. [예약] 탭의 [리소스] 섹션에 스토리지가 표시되려면 최대 1시간이 걸릴 수 있습니다.

업그레이드 문제 해결

업그레이드 문제를 해결하기 위해 업그레이드 프로세스를 수정할 수 있습니다.

vRealize Automation 환경 업그레이드에 문제가 발생하는 경우 이 절차를 사용하여 사용 가능한 플래그 중 하나를 선택하여 업그레이드 프로세스를 수정할 수 있습니다.

해결책

- 1 기본 vRealize Automation 장치 노드에 대한 보안 셸 연결을 엽니다.
- 2 명령 프롬프트에서 다음 명령을 실행하여 전환 파일을 생성합니다.

touch available_flag

예: **touch /tmp/disable-iaas-upgrade**

표 1-58. 사용 가능한 플래그

플래그	설명
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> ■ 가상 장치가 다시 시작된 후 IaaS 업그레이드 프로세스를 차단합니다. ■ 관리 에이전트 업그레이드를 차단합니다. ■ 자동 사전 요구 사항 확인 및 수정을 차단합니다. ■ IaaS 서비스 중지를 차단합니다.
/tmp/do-not-upgrade-ma	관리 에이전트 업그레이드를 차단합니다. 이 플래그는 관리 에이전트가 수동으로 업그레이드되는 경우에 적합합니다.
/tmp/skip-prereq-checks	자동 사전 요구 사항 확인 및 수정을 차단합니다. 이 플래그는 자동 사전 요구 사항 수정에 문제가 있으며 수정이 대신 수동으로 적용된 경우에 적합합니다.
/tmp/do-not-stop-services	IaaS 서비스 중지를 차단합니다. 업그레이드가 Manager Service, DEM 및 에이전트와 같은 IaaS Windows 서비스를 중지하지 않습니다.
/tmp/do-not-upgrade-servers	데이터베이스, 웹 사이트, WAPI, 리포지토리, Model Mfrontanager 데이터 및 Manager Service와 같은 모든 서버 IaaS 구성 요소의 자동 업그레이드를 차단합니다. 참고 이 플래그는 Manager Service 자동 페일오버 모드 사용도 차단합니다.
/tmp/do-not-upgrade-dems	DEM 업그레이드를 차단합니다.
/tmp/do-not-upgrade-agents	IaaS 프록시 에이전트 업그레이드를 차단합니다.

3 선택한 플래그에 대한 작업을 완료합니다.

표 1-59. 추가 작업

플래그	작업
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> ■ 수동으로 관리 에이전트를 업그레이드합니다. ■ 수동으로 필수 IaaS 사전 요구 사항을 적용합니다. ■ IaaS 서비스를 수동으로 중지합니다. <ol style="list-style-type: none"> a IaaS Windows Server에 로그인합니다. b 시작 > 관리 도구 > 서비스를 선택합니다. c 다음과 같은 순서로 이러한 서비스를 중지합니다. <div style="border: 1px solid black; padding: 2px; margin: 5px 0;">참고 IaaS Windows Server를 종료하지 않습니다.</div> <ol style="list-style-type: none"> a 각 VMwarevRealize Automation 프록시 에이전트. b 각 VMware DEM 작업자. c VMware DEM 조정자. d VMware vCloud Automation Center 서비스. ■ 가상 장치 업그레이드가 완료된 후 수동으로 IaaS 업그레이드를 시작합니다.
/tmp/do-not-upgrade-ma	수동으로 관리 에이전트를 업그레이드합니다.
/tmp/skip-prereq-checks	수동으로 필수 IaaS 사전 요구 사항을 적용합니다.
/tmp/do-not-stop-services	<p>IaaS 서비스를 수동으로 중지합니다.</p> <ol style="list-style-type: none"> 1 IaaS Windows Server에 로그인합니다. 2 시작 > 관리 도구 > 서비스를 선택합니다. 3 다음과 같은 순서로 이러한 서비스를 중지합니다. <div style="border: 1px solid black; padding: 2px; margin: 5px 0;">참고 IaaS Windows Server를 종료하지 않습니다.</div> <ol style="list-style-type: none"> a 각 VMwarevRealize Automation 프록시 에이전트. b 각 VMware DEM 작업자. c VMware DEM 조정자. d VMware vCloud Automation Center 서비스.
/tmp/do-not-upgrade-servers	
/tmp/do-not-upgrade-dems	
/tmp/do-not-upgrade-agents	

4 기본 vRealize Automation 장치 관리 콘솔에 액세스하고 기본 vRealize Automation 장치를 업데이트합니다.

참고 각 플래그는 제거될 때까지 활성 상태로 유지되기 때문에 업그레이드 후에

rm /flag_path/flag_name 명령을 실행하여 선택한 플래그를 제거합니다. 예:

rm /tmp/disable-iaas-upgrade.

laaS 사전 요구 사항 검사 중 가상 장치 업그레이드가 실패함

laaS 사전 요구 사항 검사를 통해 사용자 지정 IIS 웹 사이트 이름으로 구성된 환경의 유효성을 검사할 수 없습니다. 자동화된 laaS 업그레이드를 사용하지 않도록 설정하면 문제가 해결됩니다.

문제

설치 전 스크립트 및 설치 후 스크립트를 실행하면서 laaS 사전 요구 사항을 검사하는 동안 가상 장치 업그레이드가 실패합니다.

Error: Unrecognized configuration path MACHINE/WEBROOT/APPHOST/Default Web Site can not find path IIS:\Sites\Default Web Site because it does not exist.

오류가 발생하면 다음과 유사한 오류 메시지가 표시됩니다. Applying automatic fix for <사전 요구 사항 검사 이름> prerequisite failed.

원인

laaS 사전 요구 사항 검사기를 통해 사용자 지정 IIS 웹 사이트 이름으로 구성된 환경의 유효성을 검사할 수 없습니다. 문제를 해결하려면 자동화된 laaS 사전 요구 사항 검사기를 사용하지 않도록 설정해야 합니다.

해결책

- 1 자동화된 laaS 업그레이드 사전 요구 사항 검사 및 수정을 사용하지 않도록 설정합니다.
- 2 vRealize Automation 업그레이드를 실행합니다. [업그레이드 문제 해결](#)을 참조하십시오.
- 3 업그레이드 프롬프트를 따릅니다. vRealize Automation을 재부팅하라고 프롬프트에 표시되면 laaS 설치 관리자를 사용하여 충족되지 않은 laaS 사전 요구 사항을 검색하고 수동으로 수정할 수 있습니다.

참고 laaS 사전 요구 사항 유효성 검사를 완료할 때까지 장치를 다시 시작하지 마십시오.

- 4 모든 laaS 웹 사이트 노드에 대해 다음 단계를 사용합니다.
 - a laaS 설치 관리자를 다운로드합니다. [vRealize Automation 장치를 업그레이드한 후 laaS 구성 요소 업그레이드를 위해 laaS 설치 관리자 다운로드](#)를 참조하십시오.
 - b laaS 설치 관리자를 처음 초기화하면 확장명이 **.exe.config**인 새 구성 파일이 동일한 디렉토리에 생성됩니다.
 - c laaS 설치 관리자를 닫고 구성 파일의 <appSettings> 섹션에 다음 키를 추가합니다. 이 키는 사용자 지정 웹 사이트 이름을 laaS 사전 요구 사항 검사기로 전달합니다.


```
<add key="PreReqChecker.Default.DefaultWebSite" value="custom_web_site_name"/>
```
 - d 구성 파일을 저장하고 laaS 설치 관리자를 다시 실행합니다. 사전 요구 사항 유효성 검사가 완료될 때까지 화면에 나타나는 지침을 따릅니다. 실패한 사전 요구 사항이 있으면 수동으로 해결합니다.

- 5 IaaS 설치 관리자를 닫고 업그레이드된 vRealize Automation 장치를 재부팅하여 IaaS 자동 업그레이드를 활성화합니다.

참고 IaaS 설치 관리자를 사용하여 수동으로 IaaS 업그레이드를 계속하려면, 먼저 업그레이드된 vRealize Automation 장치를 재부팅하고 모든 서비스가 등록될 때까지 기다립니다. IaaS 구성 요소가 설치되어 있는 모든 시스템을 업그레이드하고 구성해야 합니다. 자세한 내용은 [vRealize Automation을 대상 릴리스로 업그레이드한 후 IaaS 구성 요소 업그레이드](#)를 참조하십시오.

vRealize Automation 6.2.5를 7.5로 업그레이드

vRealize Automation 6.2.5 환경을 7.5로 업그레이드할 때 6.2.5 환경과 관련된 업그레이드 절차를 사용합니다.

이 정보는 vRealize Automation 6.2.5를 7.5로 업그레이드하는 것과 관련되어 있습니다. 지원되는 다른 업그레이드 경로에 대한 자세한 내용은 [vRealize Automation 업그레이드 및 마이그레이션](#) 항목을 참조하십시오.

vRealize Automation 6.2.5에서 업그레이드

현재 vRealize Automation 6.2.5 환경을 인플레이스 업그레이드할 수 있습니다. 이 버전 관련 업그레이드 절차를 사용하여 환경을 업그레이드하십시오.

인플레이스 업그레이드는 3단계의 프로세스입니다. 현재 환경의 구성 요소를 다음 순서로 업데이트합니다.

- 1 vRealize Automation 장치
- 2 IaaS 웹 서버
- 3 vRealize Orchestrator 마이그레이션

모든 제품 구성 요소를 동일한 버전으로 업그레이드해야 합니다.

vRealize Production Test Upgrade Assist Tool은 vRealize Automation 6.2.x 환경을 분석하여 업그레이드 문제를 일으킬 수 있는 기능 구성을 파악하고 환경이 업그레이드할 준비가 되었는지 확인합니다. 이 도구 및 관련 설명서를 다운로드하려면 [VMware vRealize Production Test Tool](#) 제품 다운로드 페이지로 이동하십시오.

업그레이드한 후 지원되지 않는 속성 사전 컨트롤은 vRealize Orchestrator 및 속성 사전 관계를 사용하여 복원될 수 있습니다.

소스 환경에 사용되지 않는 코드가 포함된 워크플로가 있는 경우 [vRealize Automation 확장성 마이그레이션 가이드](#)에서 이벤트 브로커 구독으로의 전환에 필요한 코드 변경 사항에 대한 자세한 내용을 참조하십시오.

vRealize Automation 7.2부터 JFrog Artifactory Pro는 vRealize Automation 장치에 함께 제공되지 않습니다. vRealize Automation의 이전 버전에서 업그레이드하면 업그레이드 프로세스가 JFrog Artifactory Pro를 제거합니다. 자세한 내용은 [기술 자료 2147237](#)을 참조하십시오.

참고 현재 vRealize Automation 6.2.5 환경을 사용자 지정한 경우에는 지원 담당 직원에게 추가 업그레이드 정보를 문의하십시오.

vRealize Automation 업그레이드를 위한 사전 요구 사항

vRealize Automation 6.2.5에서 업그레이드하기 전에 다음 사전 요구 사항을 검토합니다.

시스템 구성 요구 사항

업그레이드를 시작하기 전에 다음과 같은 시스템 요구 사항을 충족하는지 확인합니다.

- 배포의 일부인 모든 장치와 서버가 최신 버전에 대한 시스템 요구 사항을 충족하는지 확인합니다. 자세한 내용은 [vRealize Automation 제품 설명서](#)에서 vRealize Automation 지원 매트릭스 링크를 참조하십시오.
- 다른 VMware 제품과의 호환성에 대한 자세한 내용은 VMware 웹 사이트에서 "VMware 제품 상호 운용성 매트릭스"를 참조하십시오. 자세한 내용은 [vRealize Automation 제품 설명서](#)에서 vRealize Automation 상호 운용성 매트릭스 링크를 참조하십시오.
- 업그레이드하려는 vRealize Automation의 작동 상태가 안정적인지 확인합니다. 업그레이드하기 전에 모든 문제를 해결합니다.
- vRealize Automation 6.2.5에서 업그레이드하는 경우 현재 vRealize Automation 환경에서 사용 중인 vCloud Suite 라이선스 키를 기록합니다. 업그레이드되면 기존 라이선스 키는 데이터베이스에서 제거됩니다.
- 기본값에서 최소 10분으로 로드 밸런서 시간 초과 설정을 변경했는지 확인합니다.

하드웨어 구성 요구 사항

사용 환경의 하드웨어가 대상 vRealize Automation 릴리스에 적합한지 확인합니다.

[vRealize Automation 하드웨어 규격 및 최대 용량](#)의 내용을 참조하십시오.

업그레이드를 시작하기 전에 다음과 같은 시스템 요구 사항을 충족하는지 확인합니다.

- 업그레이드를 다운로드하기 전에 현재 하드웨어를 구성해야 합니다. [vRealize Automation 6.2.5용 vCenter Server 하드웨어 리소스 늘리기](#) 항목을 참조하십시오.
- 업그레이드를 실행하기 전에 최소 18GB RAM, 4개의 CPU, Disk1 = 50GB, Disk3=25GB 및 Disk4=50GB가 있어야 합니다.

가상 시스템이 vCloud Networking and Security에 있는 경우 추가 RAM 공간을 할당해야 할 수 있습니다.

vCloud Networking and Security에 대한 일반 지원이 종료되었지만 VCNS 사용자 지정 속성은 NSX용으로 계속 유효합니다. [기술 자료 문서 2144733](#)을 참조하십시오.

- 다음 노드에는 최소 5GB의 여유 디스크 공간이 있어야 합니다.
 - 기본 IaaS 웹 사이트
 - Microsoft SQL 데이터베이스
 - Model Manager
- 업그레이드를 다운로드하고 실행하려면 다음과 같은 리소스가 있어야 합니다.
 - 루트 파티션에 최소 15 GB
 - 마스터 vRealize Automation 장치의 `/storage/db` 파티션에 5 GB
 - 각 복제 가상 장치의 루트 파티션에 15 GB
- 공간을 정리하려면 `/storage/log` 하위 폴더를 확인하고 오래된 ZIP 파일을 제거합니다.

일반 사전 요구 사항

업그레이드를 시작하기 전에 다음과 같은 시스템 요구 사항을 충족하는지 확인합니다.

- 업그레이드 후에 이 파일에 대한 사용자 지정 업데이트가 재정의되기 때문에 업그레이드를 시작하기 전에 `setenv.sh` 파일을 백업하십시오. 이 파일은 `/usr/lib/vco/app-server/bin/setenv.sh`에 있습니다. 업그레이드 후에, 해당되는 경우 값을 업데이트하고 `vco-server`를 다시 시작하여 변경 내용을 적용합니다.
- 디렉토리에 바인딩할 수 있는 사용 권한을 가진 `username@domain` 형식의 Active Directory 계정에 액세스할 수 있습니다.
- 다음 조건이 충족되어야 합니다.
 - SAMaccountName 형식의 계정에 액세스할 수 있습니다.
 - 컴퓨터 개체를 동적으로 생성하거나 사전 생성된 개체에 병합하여 시스템을 도메인에 가입시킬 수 있는 충분한 권한이 있습니다.
- vRealize Automation 업그레이드에 참여하거나 이 업그레이드에 의해 영향을 받는 모든 로드 밸런서 및 모든 데이터베이스에 대한 액세스 권한을 가지고 있습니다.
- 업그레이드를 수행하는 동안 사용자가 시스템을 사용할 수 없게 만듭니다.
- vRealize Automation을 쿼리하는 애플리케이션을 사용하지 않도록 설정합니다.
- Microsoft Distributed Transaction Coordinator(MSDTC)가 모든 vRealize Automation 및 연결된 SQL Server에서 사용하도록 설정되어 있는지 확인합니다. 자세한 내용은 [기술 자료 문서 2089503](#)을 참조하십시오.
- 환경에 외부 vRealize Orchestrator 장치 및 Identity Appliance에 연결된 외부 vRealize Orchestrator 장치가 있는 경우에는 vRealize Automation을 업그레이드하기 전에 vRealize Orchestrator를 업그레이드합니다.
- 업그레이드하기 전에 vRealize Automation 가상 시스템을 준비하기 위한 추가적인 작업을 완료해야 합니다. 업그레이드하기 전에 [기술 자료 문서 51531](#)을 검토합니다.

- 기본값에서 최소 10분으로 로드 밸런서 시간 초과 설정을 변경했는지 확인합니다.
- DynamicTypes 플러그인을 사용하는 경우 vRealize Orchestrator DynamicTypes 플러그인 구성을 패키지로 내보냅니다.
 - a Java Client에 관리자 사용자로 로그인합니다.
 - b 워크플로 탭을 선택합니다.
 - c 라이브러리 > 동적 유형 > 구성을 선택합니다.
 - d 패키지로 구성 내보내기 워크플로를 선택하고 실행합니다.
 - e 설정 안 함 > 값 삽입을 클릭합니다.
 - f 내보낼 네임스페이스를 선택하고 **추가**를 클릭하여 패키지에 추가합니다.
 - g **제출**을 클릭하여 패키지를 내보냅니다.
- 포함된 PostgreSQL 데이터베이스가 구성되어 있는 분산 환경을 업그레이드하는 경우 다음 단계를 완료하십시오.
 - a 복제 호스트를 업그레이드하기 전에 마스터 호스트의 **pgdata** 디렉토리에 있는 파일을 검사합니다.
 - b 마스터 호스트의 PostgreSQL 데이터 폴더(/var/vmware/vpostgres/current/pgdata/)로 이동합니다.
 - c **pgdata** 디렉토리에서 **.swp** 파일을 모두 닫고 제거합니다. 접미사가 **.swp**인 파일은 VI 세션을 닫고 파일을 삭제해야 합니다.
 - d 이 디렉토리의 모든 파일에 올바른 소유 이름(postgres:<owner-group>)이 있는지 확인합니다.

이 vRealize Automation 버전으로의 업그레이드에 대한 고려 사항

vRealize Automation 7 이상에서는 업그레이드 프로세스 진행 중과 완료 후에 다양한 기능이 변경됩니다. vRealize Automation 6.2.5 배포를 새 버전으로 업그레이드하기 전에 변경 내용을 검토해야 합니다.

업그레이드하기 전에 이러한 고려 사항을 검토합니다.

업그레이드 및 Identity Appliance 규격

vRealize Automation 업그레이드 프로세스 중에 Identity Appliance 업그레이드에 대해 표시되는 메시지에 응답합니다.

대상 배포에서는 VMware Identity Manager를 사용합니다.

업그레이드 및 라이선싱

업그레이드 중 기존의 vRealize Automation 6.2.5 라이선스와 보유하고 있는 모든 vCloud Suite 6.x 라이선스가 제거됩니다. 대상 vRealize Automation 릴리스 vRealize Automation 장치 관리 인터페이스에 라이선스를 다시 입력해야 합니다.

이제 vRealize Automation 장치에 라이선스 키 정보를 입력하여 가상 장치 및 IaaS에 대해 vRealize Automation 라이선싱을 사용합니다. 라이선싱 정보는 이제 더 이상 IaaS 사용자 인터페이스에서 사용할 수 없으며 IaaS는 더 이상 라이선싱 확인을 수행하지 않습니다. EULA(최종 사용자 라이선스 계약)를 통해 끝점과 할당량이 적용됩니다.

참고 vCloud Suite 6.x 라이선스 키를 vRealize Automation 6.2.5에 대해 사용한 경우 업그레이드 전에 해당 키를 기록해 두십시오. 업그레이드되면 기존 라이선스 키는 데이터베이스에서 제거됩니다.

업그레이드 중이나 업그레이드 이후에 라이선스 정보를 다시 입력하는 데 대한 자세한 내용은 [라이선스 키 업데이트](#) 항목을 참조하십시오.

역할 업그레이드 방법 이해

vRealize Automation을 업그레이드하면 조직의 기존 역할 할당 정보가 유지됩니다. 또한 업그레이드는 추가 Blueprint 설계자 역할을 지원하기 위한 일부 역할 할당을 생성합니다.

다음 설계자 역할은 설계 캔버스의 Blueprint 정의를 지원하는 데 사용됩니다.

- 애플리케이션 설계자. 기존 구성 요소 및 Blueprint를 구성하여 복합 Blueprint를 생성합니다.
- 인프라 설계자. 가상 시스템 Blueprint를 생성하고 관리합니다.
- XaaS 설계자. XaaS Blueprint를 생성 및 관리합니다.
- 소프트웨어 설계자. Software 구성 요소를 생성 및 관리합니다.

vRealize Automation 7에서는 기본적으로 테넌트 관리자와 비즈니스 그룹 관리자가 설계 Blueprint를 설계할 수 없습니다. 업그레이드된 테넌트 관리자와 비즈니스 그룹 관리자에게는 인프라 설계자 역할이 부여됩니다.

vRealize Automation 6.2.x 소스 버전에서 가상 시스템을 재구성할 수 있는 사용자는 새 버전으로 업그레이드한 이후에 가상 시스템 소유권을 변경할 수 있습니다.

업그레이드 중 다음 역할이 할당됩니다. 테이블에 나열되지 않은 역할은 대상 배포의 동일한 역할 이름으로 업그레이드됩니다.

표 1-60. 업그레이드 중 할당된 역할

소스 배포에서의 역할	대상 배포에서의 역할
테넌트 관리자	테넌트 관리자 및 인프라 설계자
비즈니스 그룹 관리자	비즈니스 그룹 관리자 및 인프라 설계자
서비스 설계자	XaaS 설계자
애플리케이션 설계자	소프트웨어 설계자

역할에 대한 자세한 내용은 [vRealize Automation의 테넌트 역할 및 책임](#)을 참조하십시오.

Blueprint 업그레이드 방법 이해

일반적으로 게시된 Blueprint는 게시된 Blueprint로 업그레이드됩니다.

하지만 이 규칙에는 예외가 있습니다. 다중 시스템 Blueprint는 Blueprint 구성 요소를 포함하는 복합 Blueprint로 업그레이드됩니다. 지원되지 않는 설정이 포함된 다중 시스템 Blueprint는 게시 취소됨으로 업그레이드됩니다.

참고 vRealize Automation 7.x는 배포 시 Blueprint 스냅샷을 생성합니다. 배포의 CPU 및 RAM 같은 시스템 속성을 업데이트할 때 재구성 문제가 발생한 경우에는 기술 자료 문서 [2150829 vRA 7.x Blueprint 스냅샷 생성](#)을 참조하십시오.

Blueprint 업그레이드에 대한 자세한 내용은 [업그레이드와 vApp Blueprint, vCloud 끝점 및 vCloud 예약](#) 및 [다중 시스템 Blueprint의 업그레이드 방법 이해](#) 항목을 참조하십시오.

업그레이드와 vApp Blueprint, vCloud 끝점 및 vCloud 예약

vApp(vCloud) 끝점을 포함하는 배포는 업그레이드할 수 없습니다. vApp(vCloud) 끝점이 있으면 이 vRealize Automation 버전으로 업그레이드할 수 없습니다.

소스 배포에 vApp(vCloud) 끝점이 있으면 마스터 가상 장치에서 업그레이드가 실패합니다. 이 경우 사용자 인터페이스와 로그에 메시지가 표시됩니다. 소스 배포에 vApp(vCloud) 끝점이 있는지 확인하려면 IaaS 관리자 사용자로 vRealize Automation 콘솔에 로그인합니다. **인프라 > 끝점**을 선택합니다. 끝점 목록에 vApp(vCloud) 끝점이 포함되어 있으면 이 vRealize Automation 버전으로 업그레이드할 수 없습니다.

관리되는 vCloud Air용 vApp 또는 vCloud Director 리소스는 대상 vRealize Automation 환경에서 지원되지 않습니다.

참고 다음과 같은 승인 정책 유형은 더 이상 사용되지 않습니다. 이러한 승인 정책 유형은 업그레이드가 완료된 후에 사용 가능한 승인 정책 유형 목록에 표시되더라도 사용할 수 없습니다.

- 서비스 카탈로그 - 카탈로그 항목 요청 - vApp
- 서비스 카탈로그 - 카탈로그 항목 요청 - vApp 구성 요소

대상 배포에서 vCloud Air 및 vCloud Director 끝점과 예약을 생성할 수 있습니다. vCloud Air 또는 vCloud Director 가상 시스템 구성 요소가 있는 Blueprint도 생성할 수 있습니다.

다중 시스템 Blueprint의 업그레이드 방법 이해

지원되는 vRealize Automation 6.2.x 버전 배포에서 관리되는 서비스, 다중 시스템 Blueprint를 업그레이드할 수 있습니다.

다중 시스템 Blueprint를 업그레이드하면 구성 요소 Blueprint가 개별 단일 시스템 Blueprint로 업그레이드됩니다. 다중 시스템 Blueprint는 이전 하위 항목 Blueprint가 개별 Blueprint 구성 요소로 중첩된 복합 Blueprint로 업그레이드됩니다.

업그레이드는 소스 다중 시스템 Blueprint에 있는 구성 요소 Blueprint 각각에 대해 가상 시스템 구성 요소 한 개가 포함된 단일 복합 Blueprint를 대상 배포에 생성합니다. 새 버전에서 지원되지 않는 설정이 Blueprint에 있는 경우, 해당 Blueprint는 업그레이드되어 초안 상태로 설정됩니다. 예를 들어 다중 시스템 Blueprint에 전용 네트워크 프로파일이 포함되어 있는 경우 업그레이드 시 프로파일 설정이 무시되고 Blueprint가 초안 상태로 업그레이드됩니다. 초안 Blueprint를 편집하여 지원되는 네트워크 프로파일 정보를 입력하고 게시할 수 있습니다.

참고 소스 배포의 게시된 Blueprint가 초안 상태 Blueprint로 업그레이드되는 경우 해당 Blueprint는 더 이상 서비스 또는 사용 권한의 일부가 아닙니다. 업그레이드된 vRealize Automation 버전에서 Blueprint를 업데이트하고 게시한 후 필요한 승인 정책과 사용 권한을 다시 생성해야 합니다.

연결된 PLR Edge 설정이 있는 전용 네트워크 프로파일 및 라우팅된 네트워크 프로파일을 포함하여 일부 다중 시스템 Blueprint 설정은 대상 vRealize Automation 배포에서 지원되지 않습니다. 사용자 지정 속성을 사용하여 PLR Edge 설정(V CNS . LoadBalancerEdgePool . Names)을 지정한 경우 해당 사용자 지정 속성이 업그레이드됩니다.

vSphere 끝점과 NSX 네트워크 및 보안 설정이 있는 다중 시스템 Blueprint를 업그레이드할 수 있습니다. 업그레이드된 Blueprint에는 NSX 네트워크 및 보안 구성 요소가 설계 캔버스에 포함됩니다.

참고 다중 시스템 Blueprint의 라우팅된 게이트웨이 규격(예약에 정의됨)은 업그레이드됩니다. 그러나 대상 vRealize Automation 배포는 연결된 PLR Edge 설정이 포함된 라우팅된 프로파일에 대해 예약을 지원하지 않습니다. 소스 예약에 PLR Edge에 대한 라우팅된 게이트웨이 값이 포함되어 있는 경우 예약이 업그레이드되지만 라우팅된 게이트웨이 설정이 무시됩니다. 따라서 업그레이드가 로그 파일에서 오류 메시지를 생성하고 예약이 사용하지 않도록 설정됩니다.

업그레이드 중, 참조된 네트워크 및 보안 구성 요소 이름에서 공백 및 특수 문자가 제거됩니다.

참고 vRealize Automation 7.x는 배포 시 Blueprint 스냅샷을 생성합니다. 배포의 CPU 및 RAM 같은 시스템 속성을 업데이트할 때 재구성 문제가 발생한 경우에는 기술 자료 문서 [2150829 vRA 7.x Blueprint 스냅샷 생성](#)을 참조하십시오.

설정 유형에 따라 네트워크 및 보안 정보가 새 Blueprint에서 여러 설정으로 캡처됩니다.

- 해당 속성 페이지의 전체 Blueprint에 대한 설정. 이 정보에는 App 분리, 전송 영역 및 라우팅된 게이트웨이 또는 NSX Edge 예약 정책 정보가 포함됩니다.
- 설계 캔버스의 NSX 네트워크 및 보안 구성 요소의 vSphere 가상 시스템 구성 요소에 대해 사용 가능한 설정.
- 설계 캔버스의 개별 vSphere 가상 시스템 구성 요소의 네트워크 및 보안 탭의 설정.

업그레이드와 물리적 끝점, 예약 및 Blueprint

물리적 끝점을 포함하는 배포는 업그레이드할 수 없습니다. 물리적 끝점이 있으면 vRealize Automation 업그레이드 프로세스가 실패합니다.

vRealize Automation 6.2.x 배포에 물리적 끝점이 있으면 마스터 가상 장치에서 업그레이드가 실패합니다. 이 경우 마이그레이션 인터페이스와 로그에 실패 메시지가 표시됩니다. vRealize Automation 6.2.x 배포에 물리적 끝점이 있는지 확인하려면 IaaS 관리자 사용자로 vRealize Automation에 로그인합니다. **인프라 > 끝점**을 선택하고 끝점 목록을 검토합니다. 목록에 **Platform Type Physical** 끝점이 있으면 vRealize Automation 7.0 이상으로 업그레이드할 수 없습니다.

Blueprint에 있는 물리적 끝점, 예약 및 가상 시스템 구성 요소는 vRealize Automation 7.0 이상에서 지원되지 않습니다.

업그레이드 및 네트워크 프로파일 설정

vRealize Automation 7 이상에서는 전용 네트워크 프로파일이 지원되지 않습니다. 이러한 프로파일은 업그레이드 중에 무시됩니다. 연결된 **PLR Edge** 설정이 있는 라우팅된 네트워크 프로파일도 vRealize Automation 7 이상에서 지원되지 않습니다. 이러한 프로파일도 업그레이드 중에 무시됩니다.

vRealize Automation 7 이상에서는 전용 네트워크 프로파일 유형이 지원되지 않습니다. vRealize Automation 업그레이드 프로세스 중에 전용 네트워크 프로파일이 소스 배포에서 발견되면 해당 네트워크 프로파일이 무시됩니다. 그러한 전용 네트워크를 참조하는 로드 밸런서도 업그레이드 중에 무시됩니다. 연결된 **PLR Edge** 설정이 있는 라우팅된 네트워크 프로파일에 대한 업그레이드 조건도 동일합니다. 어떠한 네트워크 프로파일 구성도 업그레이드되지 않습니다.

예약에 전용 네트워크 프로파일이 포함되어 있는 경우 업그레이드 중 전용 네트워크 프로파일 설정이 무시되고 예약은 대상 배포에서 사용할 수 없는 상태로 업그레이드됩니다.

예약에 연결된 **PLR Edge** 설정이 있는 라우팅된 네트워크 프로파일이 포함되어 있는 경우 업그레이드 중 라우팅된 네트워크 프로파일 규격이 무시되고 예약은 대상 배포에서 사용할 수 없는 상태로 업그레이드됩니다.

네트워크 설정이 포함된 다중 시스템 Blueprint 업그레이드에 대한 자세한 내용은 [다중 시스템 Blueprint의 업그레이드 방법 이해](#) 항목을 참조하십시오.

업그레이드 및 권한 있는 작업

가상 시스템 작업은 업그레이드할 수 없습니다.

Blueprint 규격에 따라 프로비저닝된 가상 시스템에서 수행할 수 있는 작업은 업그레이드되지 않습니다. 가상 시스템에서 수행할 수 있는 작업을 다시 생성하려면 특정 작업만 사용하도록 Blueprint에 대한 사용 권한을 사용자 지정하십시오.

관련 정보는 [사용 권한 내의 작업](#)을 참조하십시오.

업그레이드 및 사용자 지정 속성

vRealize Automation에서 제공하는 모든 사용자 지정 속성을 업그레이드된 배포에서 사용할 수 있습니다. 사용자 지정 속성 및 속성 그룹이 업그레이드됩니다.

용어 및 관련 변경 내용

소스 배포에서 생성한 모든 빌드 프로파일은 속성 그룹으로 업그레이드됩니다. 용어 "빌드 프로파일"은 더 이상 사용되지 않습니다.

용어 "속성 집합"은 더 이상 사용되지 않으며 CSV 속성 집합 파일도 더 이상 사용할 수 없습니다.

사용자 지정 속성 이름의 대/소문자 구분

vRealize Automation 7.0 이전에는 사용자 지정 속성 이름이 대/소문자를 구분하지 않았습니다. vRealize Automation 7.0 이상에서는 사용자 지정 속성 이름이 대/소문자를 구분합니다. 업그레이드 중 사용자 지정 속성 이름은 정확하게 일치해야 합니다. 이렇게 하면 속성 값이 서로를 재정의하지 않고 속성 사전 정의와 일치하도록 할 수 있습니다. 예를 들어 vRealize Automation 7.0 이상에서는 사용자 지정 속성 `hostname`과 `HOSTNAME`이 서로 다른 사용자 지정 속성으로 간주됩니다. 사용자 지정 속성 `hostname`과 `HOSTNAME`은 업그레이드 중에 서로를 재정의하지 않습니다.

사용자 지정 속성 이름의 공백

업그레이드된 vRealize Automation 설치에서 사용자 지정 속성을 인식할 수 있으려면 이 vRealize Automation 릴리스로 업그레이드하기 전에 공백을 밑줄 문자로 바꾸는 방법처럼 사용자 지정 속성 이름에서 모든 공백 문자를 제거해야 합니다. vRealize Automation 사용자 지정 속성 이름은 공백을 포함할 수 없습니다. 이 문제는 vRealize Automation, vRealize Orchestrator 또는 둘 모두의 이전 릴리스에서 공백이 포함된 사용자 지정 속성을 사용하던 업그레이드된 vRealize Orchestrator 설치의 사용에도 영향을 줄 수 있습니다.

예약된 속성 이름

몇몇 키워드가 이제 예약되므로 업그레이드된 일부 속성이 영향을 받을 수 있습니다. Blueprint 코드에 사용되는 일부 키워드는 vRealize CloudClient Blueprint 가져오기 기능을 사용하여 가져올 수 있습니다. 이러한 키워드는 예약된 것으로 간주되어 업그레이드될 속성에 대해서는 사용할 수 없습니다. 키워드에는 `cpu`, `storage`, `memory`가 포함됩니다(이에 국한되지 않음).

업그레이드 및 Application Services

대상 vRealize Automation 릴리스로 마이그레이션한 후에는 vRealize Automation Application Services 마이그레이션 도구를 사용하여 애플리케이션 서비스를 업그레이드할 수 있습니다.

다음의 단계를 완료하여 도구를 다운로드하십시오.

1 [VMware vRealize Automation 다운로드](#)를 클릭합니다.

2 **드라이버 및 도구 > VMware vRealize Application Services 마이그레이션 도구**를 선택합니다.

업그레이드 및 고급 서비스 설계

vRealize Automation 7 이상으로 업그레이드하면 고급 서비스 설계 항목이 XaaS 요소로 업그레이드됩니다.

XaaS 구성 요소를 설계 캔버스에서 사용할 수 있습니다.

업그레이드 및 Blueprint 가격 정보

7.0부터는 vRealize Automation 가격 프로파일이 더 이상 지원되지 않으며 업그레이드 중 대상 배포로 마이그레이션되지 않습니다. 그러나 vRealize Business for Cloud와의 개선된 통합을 사용하여 vRealize Automation 리소스 비용을 관리할 수 있습니다.

vRealize Business for Cloud가 이제 vRealize Automation과 긴밀하게 통합되었으며 다음과 같은 개선된 가격 책정 기능을 지원합니다.

- 다음에 대한 유연한 가격 책정 정책을 정의하기 위한 vRealize Business for Cloud의 통합 위치:
 - 인프라 리소스, 시스템 및 애플리케이션 Blueprint.

- vRealize Automation에서 vCenter Server, vCloud Director, Amazon Web Services, Azure, OpenStack 같은 지원되는 끝점에 대해 프로비저닝된 가상 시스템
- 프로비저닝된 가상 시스템의 모든 운영 가격, 1회 가격 및 사용자 지정 속성 가격.
- 배포(배포 내의 가상 시스템 가격 포함)
- vRealize Business for Cloud의 역할 기반 쇼백(Showback) 보고서.
- vRealize Business for Cloud의 새 기능을 완전하게 활용.

업그레이드하기 전에 참조를 위해 소스 vRealize Automation 인스턴스에서 기존 비용 보고서를 내보낼 수 있습니다. 업그레이드를 완료한 후 vRealize Business for Cloud를 설치 및 구성하여 가격 책정을 처리할 수 있습니다.

참고 vRealize Automation은 vRealize Business for Cloud의 동일한 릴리스와만 호환됩니다.

업그레이드 및 카탈로그 항목

vRealize Automation 6.2.x를 최신 버전으로 업그레이드한 후 일부 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없습니다.

최신 버전의 vRealize Automation으로 마이그레이션한 후 이러한 속성 정의를 사용하는 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없습니다.

- 제어 유형: 확인란 또는 링크.
- 특성: 관계, 정규식 또는 속성 레이아웃.

vRealize Automation 7.x에서, 속성 정의는 더 이상 이러한 요소를 사용하지 않습니다. 포함된 제어 유형이나 특성이 아니라 vRealize Orchestrator 스크립트 작업을 사용하도록 속성 정의를 다시 만들거나 속성 정의를 구성해야 합니다. 자세한 내용은 [업그레이드 후 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없음](#) 항목을 참조하십시오.

vRealize Automation 업그레이드 검사 목록

vRealize Automation 6.2.5를 업그레이드할 때는 모든 vRealize Automation 구성 요소를 특정 순서로 업데이트합니다.

업그레이드가 완료되면 검사 목록을 사용하여 관련 작업을 추적하십시오. 작업은 제시된 순서대로 완료하십시오.

참고 이 표에 나와 있는 순서대로 구성 요소를 업그레이드하고 모든 구성 요소를 업그레이드해야 합니다. 순서를 다르게 하면 업그레이드 이후에 예기치 않은 동작이 발생하거나, 업그레이드가 완료되지 않을 수 있습니다. 이전 릴리스 업그레이드 설명서에 대한 자세한 내용은 [vRealize Automation 제품 설명서](#)를 참조하십시오.

업그레이드 순서는 최소 환경 업그레이드인지 아니면 여러 vRealize Automation 장치를 포함하는 분산 환경 업그레이드인지에 따라 다릅니다.

표 1-61. 최소 vRealize Automation 환경 업그레이드를 위한 검사 목록

작업	지침
<input type="checkbox"/> 현재 설치를 백업합니다. 이 백업 만들기는 중요한 작업입니다.	시스템을 백업하고 복원하는 방법에 대한 자세한 내용은 기존 vRealize Automation 6.2.5 환경 백업 항목을 참조하십시오. 일반 정보는 http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf 의 "Symantec Netbackup을 사용하여 백업 및 복원 구성"을 참조하십시오.
<input type="checkbox"/> 업그레이드를 위해 vRealize Automation 6.2.x 가상 시스템을 준비합니다.	업그레이드하기 전에 기술 자료 문서 51531 을 검토하고 환경에서 모든 관련 수정을 수행해야 합니다.
<input type="checkbox"/> IaaS 서버에서 vRealize Automation Windows 서비스를 종료합니다.	IaaS Windows Server에서 vRealize Automation 서비스 중지 항목을 참조하십시오.
<input type="checkbox"/> 공통 구성 요소 카탈로그가 설치된 경우 업그레이드하기 전에 이를 제거해야 합니다.	<p>공통 구성 요소 카탈로그 구성 요소를 제거하는 방법에 대한 자세한 내용은 "공통 구성 요소 카탈로그 설치 가이드"를 참조하십시오.</p> <p>이 가이드를 사용할 수 없는 경우 각 IaaS 노드에서 다음 단계를 수행합니다.</p> <ol style="list-style-type: none"> 1 IaaS 노드에 로그인합니다. 2 시작을 클릭합니다. 3 프로그램 및 파일 검색 텍스트 상자에 services를 입력합니다. 4 서비스를 클릭합니다. 5 [서비스] 창의 오른쪽 영역에서 각 IaaS 서비스를 마우스 오른쪽 버튼으로 클릭하고 중지를 선택하여 각 서비스를 중지합니다. 6 시작 > 제어판 > 프로그램 및 기능을 클릭합니다. 7 설치된 각 공통 구성 요소 카탈로그 구성 요소를 마우스 오른쪽 버튼으로 클릭하고 제거를 선택합니다. 8 시작 > 명령 프롬프트를 클릭합니다. 9 명령 프롬프트에서 iisreset를 실행합니다.
<input type="checkbox"/> 이 vRealize Automation 버전으로 업그레이드하기 위한 고려 사항을 검토하여 업그레이드할 수 있는 항목과 업그레이드할 수 없는 항목을 식별하고 업그레이드된 항목의 동작 방식에 어떠한 변화가 있는지 파악합니다. <p>Blueprint, 예약 및 끝점을 포함한 일부 항목은 업그레이드할 수 없습니다. 지원되지 않는 일부 구성이 있는 경우 업그레이드가 차단됩니다.</p>	이 vRealize Automation 버전으로의 업그레이드에 대한 고려 사항 항목을 참조하십시오.
<input type="checkbox"/> 하드웨어 리소스를 구성합니다.	vRealize Automation 6.2.5용 vCenter Server 하드웨어 리소스 늘리기 항목을 참조하십시오.
<input type="checkbox"/> vRealize Automation 장치에 대한 업데이트를 다운로드합니다.	vRealize Automation 장치 업데이트 다운로드 항목을 참조하십시오.
<input type="checkbox"/> vRealize Automation 장치에 업데이트를 설치합니다.	vRealize Automation 장치에 업데이트 설치 항목을 참조하십시오.

표 1-61. 최소 vRealize Automation 환경 업그레이드를 위한 검사 목록 (계속)

작업	지침
<input type="checkbox"/> Single-Sign On 유틸리티를 VMware Identity Manager 유틸리티로 업데이트합니다.	VMware Identity Manager에 대한 Single Sign-On 암호 업데이트 항목을 참조하십시오.
<input type="checkbox"/> 라이선스 키를 업데이트합니다.	라이선스 키 업데이트 항목을 참조하십시오.
<input type="checkbox"/> ID 저장소를 VMware Identity Manager로 마이그레이션합니다.	ID 저장소를 VMware Identity Manager로 마이그레이션 항목을 참조하십시오.
<input type="checkbox"/> IaaS 구성 요소를 업그레이드합니다.	vRealize Automation 업그레이드 후 IaaS 서버 구성 요소 업그레이드 항목을 참조하십시오.
<input type="checkbox"/> 외부 vRealize Orchestrator를 마이그레이션합니다.	"vRealize Orchestrator 마이그레이션 가이드"의 외부 Orchestrator 서버를 외부 vRealize Orchestrator 7.5로 마이그레이션 을 참조하십시오.
<input type="checkbox"/> Active Directory 연결에 사용자 또는 그룹을 추가합니다.	Active Directory 연결에 사용자 또는 그룹 추가 항목을 참조하십시오.

표 1-62. vRealize Automation 분산 환경 업그레이드를 위한 검사 목록

작업	지침
<input type="checkbox"/> 현재 설치를 백업합니다. 이 백업 만들기는 중요한 작업입니다.	시스템을 백업하고 복원하는 방법에 대한 자세한 내용은 기존 vRealize Automation 6.2.5 환경 백업 항목을 참조하십시오. 자세한 내용은 http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf 의 "Symantec Netbackup을 사용하여 백업 및 복원 구성"을 참조하십시오.
<input type="checkbox"/> 업그레이드를 위해 vRealize Automation 6.2.x 가상 시스템을 준비합니다.	기술 자료 문서 51531 을 검토하고 업그레이드하기 전에 환경에서 모든 관련 수정을 수행해야 합니다.
<input type="checkbox"/> IaaS Windows Server에서 vRealize Automation 서비스를 종료합니다.	IaaS Windows Server에서 vRealize Automation 서비스 중지 항목을 참조하십시오.

표 1-62. vRealize Automation 분산 환경 업그레이드를 위한 검사 목록 (계속)

작업	지침
<input type="checkbox"/> 공통 구성 요소 카탈로그가 설치된 경우 업그레이드하기 전에 이를 제거해야 합니다.	<p>공통 구성 요소 카탈로그 구성 요소를 제거하는 방법에 대한 자세한 내용은 "공통 구성 요소 카탈로그 설치 가이드"를 참조하십시오.</p> <p>이 가이드를 사용할 수 없는 경우 각 IaaS 노드에서 다음 단계를 수행합니다.</p> <ol style="list-style-type: none"> 1 IaaS 노드에 로그인합니다. 2 시작을 클릭합니다. 3 프로그램 및 파일 검색 텍스트 상자에 services를 입력합니다. 4 서비스를 클릭합니다. 5 [서비스] 창의 오른쪽 영역에서 각 IaaS 서비스를 마우스 오른쪽 버튼으로 클릭하고 중지를 선택하여 각 서비스를 중지합니다. 6 시작 > 제어판 > 프로그램 및 기능을 클릭합니다. 7 설치된 각 공통 구성 요소 카탈로그 구성 요소를 마우스 오른쪽 버튼으로 클릭하고 제거를 선택합니다. 8 시작 > 명령 프롬프트를 클릭합니다. 9 명령 프롬프트에서 iisreset를 실행합니다.
<input type="checkbox"/> 업그레이드를 위한 하드웨어 리소스를 구성합니다.	vRealize Automation 6.2.5용 vCenter Server 하드웨어 리소스 늘리기 항목을 참조하십시오.
<input type="checkbox"/> 로드 밸런서를 사용하지 않도록 설정합니다.	<p>각 보조 노드를 사용하지 않도록 설정하고 다음 항목에 대한 vRealize Automation 상태 모니터를 제거합니다.</p> <ul style="list-style-type: none"> ■ vRealize Automation 장치 ■ IaaS 웹 사이트 ■ IaaS Manager Service <p>업그레이드를 완료하려면 다음을 확인합니다.</p> <ul style="list-style-type: none"> ■ 로드 밸런서 트래픽이 기본 노드로만 전달됩니다. ■ 장치, 웹 사이트 및 Manager Service에 대한 vRealize Automation 상태 모니터가 제거되었습니다.
<input type="checkbox"/> vRealize Automation 장치에 대한 업데이트를 다운로드합니다.	vRealize Automation 장치 업데이트 다운로드 항목을 참조하십시오.
<input type="checkbox"/> 설치의 첫 번째 vRealize Automation 장치에 업데이트를 설치합니다. 특정 장치를 마스터로 지정한 경우 이 장치를 먼저 업그레이드합니다.	vRealize Automation 장치에 업데이트 설치 항목을 참조하십시오.
<input type="checkbox"/> Single-Sign On 유틸리티를 VMware Identity Manager 유틸리티로 업데이트합니다.	VMware Identity Manager에 대한 Single Sign-On 암호 업데이트 항목을 참조하십시오.
<input type="checkbox"/> 라이선스 키를 업데이트합니다.	라이선스 키 업데이트 항목을 참조하십시오.
<input type="checkbox"/> ID 저장소를 VMware Identity Manager 유틸리티로 마이그레이션합니다.	ID 저장소를 VMware Identity Manager로 마이그레이션 항목을 참조하십시오.

표 1-62. vRealize Automation 분산 환경 업그레이드를 위한 검사 목록 (계속)

작업	지침
<input type="checkbox"/> 나머지 vRealize Automation 장치에 업데이트를 설치합니다.	추가 vRealize Automation 장치에 업데이트 설치 항목을 참조하십시오.
<input type="checkbox"/> IaaS 구성 요소를 업그레이드합니다.	vRealize Automation 업그레이드 후 IaaS 서버 구성 요소 업그레이드 항목을 참조하십시오.
<input type="checkbox"/> 외부 vRealize Orchestrator를 마이그레이션합니다.	"vRealize Orchestrator 마이그레이션 가이드"의 외부 Orchestrator 서버를 외부 vRealize Orchestrator 7.5로 마이그레이션 을 참조하십시오.
<input type="checkbox"/> 로드 밸런서를 사용하도록 설정합니다.	로드 밸런서 사용 항목을 참조하십시오.

vRealize Automation 환경 사용자 인터페이스

몇 가지 인터페이스로 vRealize Automation 환경을 사용하고 관리합니다.

사용자 인터페이스

다음 테이블은 vRealize Automation 환경을 관리하는 데 사용하는 인터페이스를 설명합니다.

표 1-63. vRealize Automation 관리 콘솔

용도	액세스	필요한 자격 증명
vRealize Automation 콘솔을 사용하여 다음과 같은 시스템 관리자 작업을 수행합니다.	1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 장치 시작 페이지를 엽니다.	시스템 관리자 역할을 가진 사용자여야 합니다.
<ul style="list-style-type: none"> 테넌트를 추가합니다. vRealize Automation 사용자 인터페이스 사용자 지정합니다. 이메일 서버를 구성합니다. 이벤트 로그를 봅니다. vRealize Orchestrator를 구성합니다. 	2 https://vrealize-automation-appliance-FQDN . vRealize Automation 콘솔 을 클릭합니다. 다음 URL을 사용하여 vRealize Automation 콘솔을 열 수도 있습니다. https://vrealize-automation-appliance-FQDN/vcac	
	3 로그인합니다.	

표 1-64. vRealize Automation 테넌트 콘솔. 이 인터페이스는 서비스와 리소스를 생성하고 관리하는 데 사용되는 기본 사용자 인터페이스입니다.

용도	액세스	필요한 자격 증명
<p>vRealize Automation을 사용하여 다음과 같은 작업을 수행합니다.</p> <ul style="list-style-type: none"> ■ 새 IT 서비스 Blueprint를 요청합니다. ■ 클라우드 및 IT 리소스를 생성하고 관리합니다. ■ 사용자 지정 그룹을 생성하고 관리합니다. ■ 비즈니스 그룹을 만들고 관리합니다. ■ 사용자에게 역할을 할당합니다. 	<ol style="list-style-type: none"> 1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름과 테넌트 URL 이름을 사용하여 테넌트의 URL을 입력합니다. https://vrealize-automation-appliance-FQDN/vcac/org/tenant_URL_name . 2 로그인합니다. 	<p>다음 역할 중 하나 이상을 가진 사용자여야 합니다.</p> <ul style="list-style-type: none"> ■ 애플리케이션 설계자 ■ 승인 관리자 ■ 카탈로그 관리자 ■ 컨테이너 관리자 ■ 컨테이너 설계자 ■ 상태 소비자 ■ 인프라 설계자 ■ 소비자 보안 내보내기 ■ 소프트웨어 설계자 ■ 테넌트 관리자 ■ XaaS 설계자

표 1-65. vRealize Automation 장치 관리 인터페이스.

용도	액세스	필요한 자격 증명
<p>vRealize Automation 장치 관리를 사용하여 다음과 같은 작업을 수행합니다.</p> <ul style="list-style-type: none"> ■ 등록된 서비스의 상태를 봅니다. ■ 시스템 정보를 보고 장치를 재부팅하거나 종료합니다. ■ 고객 환경 향상 프로그램에 대한 참여를 관리합니다. ■ 네트워크 상태를 봅니다. ■ 업데이트 상태를 보고 업데이트를 설치합니다. ■ 관리 설정을 관리합니다. ■ vRealize Automation 호스트 설정을 관리합니다. ■ SSO 설정을 관리합니다. ■ 제품 라이선스를 관리합니다. ■ vRealize Automation Postgres 데이터베이스를 구성합니다. ■ vRealize Automation 메시징을 구성합니다. ■ vRealize Automation 로깅을 구성합니다. ■ IaaS 구성 요소를 설치합니다. ■ 기존 vRealize Automation 설치에서 마이그레이션합니다. ■ IaaS 구성 요소 인증서를 관리합니다. ■ Xenon 서비스를 구성합니다. 	<ol style="list-style-type: none"> 1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 장치 시작 페이지를 엽니다. <code>https://vrealize-automation-appliance-FQDN</code> 2 vRealize Automation 장치 관리를 클릭합니다. 다음 URL을 사용하여 vRealize Automation 장치 관리 인터페이스를 열 수도 있습니다. <code>https://vrealize-automation-appliance-FQDN:5480</code> 3 로그인합니다. 	<ul style="list-style-type: none"> ■ 사용자 이름: root ■ 암호: vRealize Automation 장치를 배포할 때 입력한 암호.

표 1-66. vRealize Orchestrator 클라이언트

용도	액세스	필요한 자격 증명
<p>vRealize Orchestrator 클라이언트를 사용하여 다음과 같은 작업을 수행합니다.</p> <ul style="list-style-type: none"> ■ 작업을 개발합니다. ■ 워크플로를 개발합니다. ■ 정책을 관리합니다. ■ 패키지를 설치합니다. ■ 사용자 및 사용자 그룹 사용 권한을 관리합니다. ■ URI 개체에 태그를 연결합니다. ■ 인벤토리를 봅니다. 	<ol style="list-style-type: none"> 1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 시작 페이지를 엽니다. <code>https://vrealize-automation-appliance-FQDN</code> 2 로컬 컴퓨터에 client.jnlp 파일을 다운로드하려면 vRealize Orchestrator Client를 클릭합니다. 3 client.jnlp 파일을 마우스 오른쪽 버튼으로 클릭하고 시작을 선택합니다. 4 [계속하시겠습니까?] 대화 상자에서 계속을 클릭합니다. 5 로그인합니다. 	<p>vRealize Orchestrator 제어 센터 인증 제공자 설정에 구성된 vcoadmins 그룹에 속하거나 시스템 관리자 역할이 있는 사용자여야 합니다.</p>

표 1-67. vRealize Orchestrator 제어 센터

용도	액세스	필요한 자격 증명
vRealize Orchestrator 제어 센터를 사용하여 vRealize Automation에 내장된 기본 vRealize Orchestrator 인스턴스의 구성을 편집합니다.	<ol style="list-style-type: none"> 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 장치 시작 페이지를 엽니다. <code>https://vrealize-automation-appliance-FQDN</code> vRealize Automation 장치 관리를 클릭합니다. 다음 URL을 사용하여 vRealize Automation 장치 관리 인터페이스를 열 수도 있습니다. <code>https://vrealize-automation-appliance-FQDN:5480</code> 로그인합니다. vRA > Orchestrator를 클릭합니다. Orchestrator 사용자 인터페이스를 선택합니다. 시작을 클릭합니다. Orchestrator 사용자 인터페이스 URL을 클릭합니다. 로그인합니다. 	<p>사용자 이름</p> <ul style="list-style-type: none"> ■ 역할 기반 인증이 구성되지 않은 경우 root를 입력합니다. ■ 역할 기반 인증에 대해 구성된 경우 vRealize Automation 사용자 이름을 입력합니다. <p>암호</p> <ul style="list-style-type: none"> ■ 역할 기반 인증이 구성되지 않은 경우 vRealize Automation 장치를 배포했을 때 입력한 암호를 입력합니다. ■ 사용자 이름이 역할 기반 인증에 대해 구성된 경우 사용자 이름에 대한 암호를 입력합니다.

표 1-68. Linux 명령 프롬프트

용도	액세스	필요한 자격 증명
호스트(예: vRealize Automation 장치 호스트)에서 Linux 명령 프롬프트를 사용하여 다음과 같은 작업을 수행합니다. <ul style="list-style-type: none"> ■ 서비스 중지 또는 시작 ■ 구성 파일 편집 ■ 명령 실행 ■ 데이터 검색 	<ol style="list-style-type: none"> vRealize Automation 장치 호스트에서 명령 프롬프트를 엽니다. 로컬 컴퓨터에서 명령 프롬프트를 여는 한 가지 방법은 PuTTY와 같은 애플리케이션을 사용하여 호스트에서 세션을 시작하는 것입니다. 로그인합니다. 	<ul style="list-style-type: none"> ■ 사용자 이름: root ■ 암호: vRealize Automation 장치를 배포할 때 생성한 암호.

표 1-69. Windows 명령 프롬프트

용도	액세스	필요한 자격 증명
호스트(예: IaaS 호스트)에서 Windows 명령 프롬프트를 사용하여 스크립트를 실행할 수 있습니다.	<ol style="list-style-type: none"> IaaS 호스트에서 Windows에 로그인합니다. 로컬 컴퓨터에서 로그인하는 한 가지 방법은 원격 데스크톱 세션을 시작하는 것입니다. Windows 명령 프롬프트를 엽니다. 명령 프롬프트를 여는 한 가지 방법은 호스트에서 [시작] 아이콘을 마우스 오른쪽 버튼으로 클릭하고 명령 프롬프트 또는 명령 프롬프트(관리자)를 선택하는 것입니다. 	<ul style="list-style-type: none"> ■ 사용자 이름: 관리자 권한이 있는 사용자. ■ 암호: 사용자의 암호.

vRealize Automation에 통합된 VMware 제품 업그레이드

vRealize Automation을 업그레이드할 때는 vRealize Automation 환경에 통합되어 있는 모든 VMware 제품을 관리해야 합니다.

vRealize Automation 환경이 하나 이상의 추가적인 제품과 통합되어 있으면 추가적인 제품을 업데이트하기 전에 vRealize Automation부터 업그레이드해야 합니다. vRealize Business for Cloud가 vRealize Automation과 통합되어 있는 경우에는 vRealize Automation을 업그레이드하기 전에 vRealize Business for Cloud를 등록 취소해야 합니다.

vRealize Automation을 업그레이드하는 경우에 통합된 제품을 관리하기 위해 제안된 워크플로를 따르십시오.

- 1 vRealize Automation을 업그레이드합니다.
- 2 VMware vRealize Operations Manager를 업그레이드합니다.
- 3 VMware vRealize Log Insight를 업그레이드합니다.
- 4 VMware vRealize Business for Cloud를 업그레이드합니다.

이 섹션에서는 vRealize Automation 환경에 통합되어 있는 vRealize Business for Cloud를 관리하기 위한 추가적인 지침을 제공합니다.

vRealize Automation에 통합된 vRealize Operations Manager 업그레이드

vRealize Automation을 업그레이드한 후에 vRealize Operations Manager를 업그레이드합니다.

절차

- 1 vRealize Automation을 업그레이드합니다.
- 2 vRealize Operations Manager를 업그레이드합니다. 자세한 내용은 [VMware vRealize Operations Manager 설명서](#)에서 "소프트웨어 업데이트" 항목을 참조하십시오.

vRealize Automation에 통합된 vRealize Log Insight 업그레이드

vRealize Automation을 업그레이드한 후에 vRealize Log Insight를 업그레이드합니다.

절차

- 1 vRealize Automation을 업그레이드합니다.
- 2 vRealize Log Insight를 업그레이드합니다. 자세한 내용은 [VMware vRealize Log Insight 설명서](#)에서 "vRealize Log Insight 업그레이드" 항목을 참조하십시오.

vRealize Automation에 통합된 vRealize Business for Cloud 업그레이드

vRealize Automation 환경을 업그레이드할 경우 vRealize Business for Cloud에 대한 연결을 등록 취소하고 등록해야 합니다.

vRealize Automation 환경을 업그레이드할 때 vRealize Business for Cloud 서비스를 지속적으로 실행하려면 이 절차를 수행하십시오.

절차

- 1 vRealize Automation에서 vRealize Business for Cloud를 등록 취소합니다. 자세한 내용은 [VMware vRealize Business for Cloud 설명서](#)에서 "vRealize Automation에서 vRealize Business for Cloud 등록 취소" 항목을 참조하십시오.
- 2 vRealize Automation을 업그레이드합니다.
- 3 필요한 경우 vRealize Business for Cloud를 업그레이드합니다. [VMware vRealize Business for Cloud 설명서](#)에서 "vRealize Business for Cloud 업그레이드" 항목을 참조하십시오.
- 4 vRealize Business for Cloud를 vRealize Automation에 등록합니다. [VMware vRealize Business for Cloud 설명서](#)에서 "vRealize Automation에 vRealize Business for Cloud 등록" 항목을 참조하십시오.

vRealize Automation 업그레이드 준비

vRealize Automation 6.2.5에서 업그레이드하기 전에 다양한 작업과 절차를 수행해야 합니다.

업그레이드 검사 목록에 표시되는 순서대로 작업을 수행합니다. [vRealize Automation 업그레이드 검사 목록](#) 항목을 참조하십시오.

vRealize Automation 업그레이드를 위한 백업 사전 요구 사항

vRealize Automation 6.2.5에서 업그레이드하기 전에 백업 사전 요구 사항을 완료하십시오.

사전 요구 사항

- 소스 환경이 완전하게 설치되고 구성되었는지 확인합니다.
- 소스 환경의 각 장치에 대해 다음 디렉토리의 모든 vRealize Automation 장치 구성 파일을 백업합니다.
 - /etc/vcac/
 - /etc/vco/
 - /etc/apache2/
 - /etc/rabbitmq/
- 시스템에 vRealize Automation 외부 워크플로 구성(xmlldb) 파일을 백업합니다. 백업 파일을 임시 디렉토리에 저장합니다. 해당 파일은 \VMware\vCA\Server\ExternalWorkflows\xmlldb\에 있습니다. 마이그레이션 후 새 시스템에 xmlldb 파일을 복원합니다. [외부 워크플로 시간 초과 파일 복원](#) 항목을 참조하십시오.

관련 문제는 [.xml 파일 백업 복사본으로 인한 시스템 시간 초과](#) 항목을 참조하십시오.

- 외부 vRealize Automation PostgreSQL 데이터베이스를 백업합니다. PostgreSQL 데이터베이스가 외부 데이터베이스인지 확인하려면 다음 단계를 완료합니다.
 - a 기본 또는 마스터 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

b 클러스터를 선택합니다.

c vRealize Automation PostgreSQL 데이터베이스 노드 호스트가 vRealize Automation 장치 호스트와 다르면 데이터베이스를 백업합니다. 데이터베이스 노드 호스트가 장치 호스트와 동일하면 데이터베이스를 백업하지 않아도 됩니다.

PostgreSQL 데이터베이스 백업에 대한 자세한 내용은 <https://www.postgresql.org/> 사이트를 참조하십시오.

- 테넌트 구성 및 할당된 사용자의 스냅샷을 생성합니다.
- DataCenterLocations.xml과 같은 사용자 지정된 모든 파일을 백업합니다.
- 가상 장치 및 IaaS 서버에 대해 각각 스냅샷을 생성합니다. vRealize Automation 업그레이드가 실패할 경우에 대비하여 전체 시스템 백업을 위한 일반 지침을 따르십시오. [vRealize Automation 설치에 대한 백업 및 복구](#)를 참조하십시오.

기존 vRealize Automation 6.2.5 환경 백업

업그레이드하기 전에 시스템을 종료하고 vRealize Automation 6.2.5 환경 구성 요소의 스냅샷을 생성합니다.

업그레이드하기 전에 시스템이 종료된 동안 다음 구성 요소의 스냅샷을 생성합니다.

- vRealize Automation IaaS 서버(Windows 노드)
- vRealize Automation 장치(Linux 노드)
- vRealize Automation(SSO) Identity 노드

업그레이드가 실패하면 스냅샷을 사용하여 마지막으로 확인된 정상 구성으로 되돌리고 다른 업그레이드를 시도합니다.

사전 요구 사항

- 포함된 PostgreSQL 데이터베이스가 고가용성 모드에 있는지 확인합니다. 그렇다면 현재 Master 노드를 찾습니다. 기술 자료 문서 <http://kb.vmware.com/kb/2105809>를 참조하십시오.
- 환경에 외부 PostgreSQL 데이터베이스가 있는 경우 데이터베이스 백업 파일을 생성합니다.
- vRealize Automation Microsoft SQL 데이터베이스가 IaaS 서버에서 호스팅되지 않는 경우 데이터베이스 백업 파일을 생성합니다. 자세한 내용을 보려면 [Microsoft Developer Network](#)에서 전체 SQL Server 데이터베이스 백업을 생성하는 데 대한 문서를 검색하십시오.
- 업그레이드를 위한 백업 사전 요구 사항을 충족했는지 확인합니다.
- 시스템이 종료되는 동안 시스템의 스냅샷을 생성했는지 확인합니다. 이는 기본 스냅샷 생성 방법입니다. 스냅샷 생성 및 관리에 대한 자세한 내용은 [vSphere 제품 설명서](#)를 참조하십시오.

참고 vRealize Automation 장치와 IaaS 구성 요소를 백업할 때 메모리 내 스냅샷과 중지된 스냅샷을 사용하지 않도록 설정하십시오.

- app.config 파일을 수정한 경우 이 파일의 백업을 만듭니다. [app.config 파일에 로깅 변경 내용 복원](#) 항목을 참조하십시오.

- 외부 워크플로 구성(xmlldb) 파일의 백업을 만듭니다. [외부 워크플로 시간 초과 파일 복원](#) 항목을 참조하십시오.
- 현재 폴더 외부에 백업 파일을 저장할 수 있는 위치가 있는지 확인합니다. [.xml 파일 백업 복사본으로 인한 시스템 시간 초과](#) 항목을 참조하십시오.

절차

- 1 vCenter Server에 로그인합니다.
- 2 다음 vRealize Automation 6.2.5 구성 요소를 찾습니다.
 - vRealize Automation IaaS 서버(Windows 노드)
 - vRealize Automation 장치(Linux 노드)
 - vRealize Automation(SSO) Identity 노드
- 3 다음 가상 시스템 중 각각에 대해 가상 시스템을 선택하고 **게스트 종료**를 클릭한 후 가상 시스템이 중지할 때까지 기다립니다. 다음과 같은 순서로 이러한 가상 시스템을 종료합니다.
 - a IaaS 프록시 에이전트 가상 시스템
 - b DEM 작업자 가상 시스템
 - c DEM 조정자 가상 시스템
 - d Manager Service 가상 시스템
 - e Web Service 가상 시스템
 - f 보조 vRealize Automation 가상 장치
 - g 기본 vRealize Automation 가상 장치
 - h Manager 가상 시스템(있는 경우)
 - i Identity Appliance
- 4 각 vRealize Automation 6.2.5 가상 시스템의 스냅샷을 생성합니다.
- 5 각 vRealize Automation 장치 노드를 복제합니다.
업그레이드는 복제된 가상 시스템에서 수행합니다.
- 6 복제된 가상 시스템을 업그레이드하기 전에 원본 vRealize Automation 장치 가상 시스템 각각의 전원을 끕니다.
원본 가상 시스템을 전원을 끈 상태로 유지하고 시스템을 복원해야 하는 경우에만 이러한 시스템을 사용합니다.

다음에 수행할 작업

[vRealize Automation 6.2.5용 vCenter Server 하드웨어 리소스 늘리기](#).

vRealize Automation 6.2.5용 vCenter Server 하드웨어 리소스 늘리기

vRealize Automation 6.2.5에서 업그레이드하기 전에 각 vRealize Automation 장치의 하드웨어 리소스를 늘려야 합니다.

이 절차에서는 Windows vCenter Server 클라이언트를 사용한다고 가정합니다.

사전 요구 사항

- 각 vRealize Automation 장치의 복제본이 있는지 확인합니다.
- 각 장치 복제본에 대해 140GB 이상의 사용 가능한 공간이 vCenter Server에 있는지 확인합니다.
- 원본 장치의 전원을 껐는지 확인합니다.

절차

- 1 vCenter Server에 로그인합니다.
- 2 복제된 vRealize Automation 장치 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 3 **메모리**를 선택하고 값을 18GB로 설정합니다.
- 4 **CPU**를 선택하고 **가상 소켓 수** 값을 4로 설정합니다.
- 5 가상 디스크 1의 크기를 50GB로 확장합니다.
 - a 디스크 1을 선택합니다.
 - b 크기를 50GB로 변경합니다.
 - c **확인**을 클릭합니다.
- 6 디스크 3이 없으면 다음 단계를 완료하여 25GB의 디스크 크기를 가진 디스크 3을 추가합니다.
 - a 리소스 테이블 위의 **추가**를 클릭하여 가상 디스크를 추가합니다.
 - b **디바이스 유형**으로 **하드 디스크**를 선택하고 **다음**을 클릭합니다.
 - c **새 가상 디스크 생성**을 선택하고 **다음**을 클릭합니다.
 - d **디스크 크기** 값을 25GB로 설정합니다.
 - e **가상 시스템과 함께 저장**을 선택하고 **다음**을 클릭합니다.
 - f **모드**에 대해 **독립** 옵션이 선택 해제되고 **가상 디바이스 모드**에 대해 **SCSI(0:2)**가 선택되었는지 확인한 후 **다음**을 클릭합니다.

권장 설정을 수락하라는 메시지가 표시되면 권장 설정을 수락합니다.

 - g **완료**를 클릭합니다.
 - h **확인**을 클릭합니다.

- 7 이전 vRealize Automation 릴리스의 기존 가상 디스크 4가 있는 경우 다음 단계를 완료하십시오.
 - a 기본 가상 장치 복제본의 전원을 켜고 1분 동안 기다립니다.
 - b 보조 가상 장치 복제본의 전원을 켭니다.
 - c 기본 가상 장치 복제본에서 새 명령 프롬프트를 열고 `/etc/fstab`로 이동합니다.
 - d 기본 가상 장치 복제본에서 `fstab` 파일을 열고 `Wal_Archive` 미리 쓰기 로그가 포함된 `/dev/sdd`로 시작하는 줄을 제거합니다.
 - e 기본 가상 장치 복제본에서 파일을 저장합니다.
 - f 보조 가상 장치 복제본에서 새 명령 프롬프트를 열고 `/etc/fstab`로 이동합니다.
 - g 보조 가상 장치 복제본에서 `fstab` 파일을 열고 `Wal_Archive` 미리 쓰기 로그가 포함된 `/dev/sdd`로 시작하는 줄을 제거합니다.
 - h 보조 가상 장치 복제본에서 파일을 저장합니다.
 - i 보조 가상 장치 복제본의 전원을 끄고 1분 동안 기다립니다.
 - j 기본 가상 장치 복제본의 전원을 끕니다.
 - k 복제된 vRealize Automation 기본 장치 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
 - l 복제된 기본 가상 장치 시스템에서 디스크 4를 삭제합니다.
 - m 복제된 vRealize Automation 보조 장치 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
 - n 복제된 보조 가상 장치 시스템에서 디스크 4를 삭제합니다.
- 8 다음 단계를 완료하여 복제된 기본 및 보조 가상 장치 시스템에 디스크 크기가 50GB인 디스크 4를 추가합니다.
 - a 리소스 테이블 위의 **추가**를 클릭하여 가상 디스크를 추가합니다.
 - b **디바이스 유형**으로 **하드 디스크**를 선택하고 **다음**을 클릭합니다.
 - c **새 가상 디스크 생성**을 선택하고 **다음**을 클릭합니다.
 - d **디스크 크기** 값을 50GB로 설정합니다.
 - e **가상 시스템과 함께 저장**을 선택하고 **다음**을 클릭합니다.
 - f **모드**에 대해 **독립** 옵션이 선택 해제되고 **가상 디바이스 모드**에 대해 **SCSI(0:3)**가 선택되었는지 확인한 후 **다음**을 클릭합니다.

권장 설정을 수락하라는 메시지가 표시되면 권장 설정을 수락합니다.
 - g **완료**를 클릭합니다.
 - h **확인**을 클릭합니다.
- 9 복제된 기본 가상 장치 시스템 및 복제된 보조 가상 장치 시스템의 스냅샷을 생성합니다.

다음에 수행할 작업

전체 시스템의 전원 켜기.

전체 시스템의 전원 켜기

업그레이드를 위해 vCenter 하드웨어 리소스를 늘렸다면 업그레이드를 수행하기 전에 시스템의 전원을 켭니다.

사전 요구 사항

- 기존 vRealize Automation 6.2.5 환경 백업.
- vRealize Automation 6.2.5용 vCenter Server 하드웨어 리소스 늘리기.

절차

- 1 전체 시스템의 전원을 켭니다.

지침은 vRealize Automation 6.2 버전의 "vRealize Automation 시작" 항목을 참조하십시오.

참고 고가용성 환경이 있는 경우 이 절차에 따라 가상 장치의 전원을 켭니다.

- a 마지막으로 전원을 끈 가상 장치의 전원을 켭니다.
 - b 1분간 기다립니다.
 - c 나머지 가상 장치의 전원을 켭니다.
-

- 2 시스템이 완전히 작동하는지 확인합니다.

다음에 수행할 작업

IaaS Windows Server에서 vRealize Automation 서비스 중지.

IaaS Windows Server에서 vRealize Automation 서비스 중지

필요한 경우 다음 절차를 사용하여 IaaS 서비스를 실행 중인 각 서버에서 vRealize Automation 서비스를 중지할 수 있습니다.

업그레이드를 시작하기 전에 각 IaaS Windows Server에서 vRealize Automation 서비스를 중지합니다.

참고 Manager Service의 패시브 백업 인스턴스를 제외하고, 업그레이드 프로세스 중 모든 서비스에 대한 시작 유형은 [자동]으로 설정되어야 합니다. 서비스를 [수동]으로 설정하는 경우 업그레이드 프로세스가 실패합니다.

절차

- 1 IaaS Windows Server에 로그인합니다.
- 2 시작 > 관리 도구 > 서비스를 선택합니다.

- 3 다음과 같은 순서로 서비스를 중지합니다. 가상 시스템을 종료하지 않도록 주의하십시오.
각 가상 시스템에는 각 서비스 집합과 함께 중지되어야 하는 관리 에이전트가 있습니다.
 - a 각 VMware vCloud Automation Center 에이전트
 - b 각 VMware DEM 작업자
 - c VMware DEM-Orchestrator
 - d VMware vCloud Automation Center 서비스
- 4 로드 밸런서가 포함된 분산 배포의 경우, 각 보조 노드를 사용하지 않도록 설정하고 다음 항목에 대해 vRealize Automation 상태 모니터를 제거합니다.
 - a vRealize Automation 장치
 - b IaaS 웹 사이트
 - c IaaS Manager Service

로드 밸런서 트래픽이 기본 노드로만 전달되고 장치, 웹 사이트 및 Manager Service에 대해 vRealize Automation 상태 모니터가 제거되었는지 확인합니다. 그렇지 않으면 업그레이드가 실패합니다.
- 5 다음 단계를 수행하여 Microsoft IIS(인터넷 정보 서비스)에서 호스팅되는 IaaS 서비스가 실행 중인지 확인합니다.
 - a 브라우저에서 URL **https://webhostname/Repository/Data/MetaModel.svc**로 이동하여 웹 저장소가 실행되고 있는지 확인합니다. 성공한 경우 오류가 반환되지 않으며 모델 목록이 XML 형식으로 표시됩니다.
 - b IaaS 가상 시스템의 웹 노드에 있는 **Repository.log** 파일에 기록된 상태를 검사하여 정상 상태가 보고되는지 확인합니다. 해당 파일은 **/Server/Model Manager Web/Logs/Repository.log**의 VCAC 홈 폴더에 있습니다.

분산 IaaS 웹 사이트인 경우 MMD 없이 보조 웹 사이트에 로그인하고 Microsoft IIS 서버를 일시적으로 중지합니다. **MetaModel.svc** 연결을 확인합니다. 로드 밸런서 트래픽이 기본 웹 노드만 통과하는지 확인하려면 Microsoft IIS 서버를 시작합니다.

다음에 수행할 작업

[vRealize Automation 장치 업데이트 다운로드.](#)

vRealize Automation 장치 업데이트 다운로드

vRealize Automation 장치 관리 인터페이스에서 업데이트를 확인하고 다음 방법 중 하나를 사용하여 업데이트를 다운로드합니다.

업그레이드 성능을 최적화하려면 ISO 파일 방법을 사용합니다.

장치 업그레이드 시 발생 가능한 문제를 방지하기 위해 또는 장치 업그레이드 중 문제가 발생한 경우 [VMware 기술 자료 문서 "vRealize Orchestrator 데이터베이스의 중복 항목으로 인한 vRealize Automation 업그레이드 실패\(54987\)"](#) 를 참조하십시오.

■ **VMware 저장소에서 vRealize Automation 장치 업데이트 다운로드**

vmware.com 웹 사이트의 공용 저장소에서 vRealize Automation 장치에 대한 업데이트를 다운로드할 수 있습니다.

■ **CD-ROM 드라이브에서 사용할 가상 장치 업데이트 다운로드**

가상 CD-ROM 드라이브에서 장치가 읽어 들이는 ISO 파일로 가상 장치를 업데이트할 수 있습니다. 이것이 기본 방법입니다.

VMware 저장소에서 vRealize Automation 장치 업데이트 다운로드

vmware.com 웹 사이트의 공용 저장소에서 vRealize Automation 장치에 대한 업데이트를 다운로드할 수 있습니다.

사전 요구 사항

- 기존 vRealize Automation 환경을 백업합니다.
- vRealize Automation 장치의 전원이 켜져 있는지 확인합니다.

절차

- 1 기본 vRealize Automation 장치에서 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **root**로 vRealize Automation 장치 관리에 로그인합니다.
- 2 **업데이트** 탭을 클릭합니다.
- 3 **설정**을 클릭합니다.
- 4 (선택 사항) [자동 업데이트] 패널에서 업데이트 확인 주기를 설정합니다.
- 5 [업데이트 저장소] 패널에서 **기본 저장소 사용**을 선택합니다.
기본 저장소는 정확한 VMware.com URL로 설정됩니다.
- 6 **설정 저장**을 클릭합니다.

CD-ROM 드라이브에서 사용할 가상 장치 업데이트 다운로드

가상 CD-ROM 드라이브에서 장치가 읽어 들이는 ISO 파일로 가상 장치를 업데이트할 수 있습니다. 이것이 기본 방법입니다.

ISO 파일을 다운로드하고, 이 파일을 사용하여 장치를 업그레이드하도록 기본 장치를 설정합니다.

사전 요구 사항

- 기존 vRealize Automation 환경을 백업합니다.
- vRealize Automation 장치를 업데이트하기 전에 업그레이드에 사용할 모든 CD-ROM 드라이브가 사용되도록 설정되었는지 확인합니다. vSphere Client의 가상 시스템에 CD-ROM 드라이브를 추가하는 데 대한 내용은 vSphere 설명서를 참조하십시오.

절차

- 1 업데이트 저장소 ISO 파일을 다운로드합니다.
 - a 브라우저를 시작하고 **vRealize Automation 제품 페이지**(www.vmware.com)로 이동합니다.
 - b 이 페이지에서 **vRealize Automation 다운로드**를 클릭하여 VMware 다운로드 페이지로 이동합니다.
 - c 적절한 파일을 다운로드합니다.
- 2 시스템에 다운로드된 파일을 찾아 파일 크기가 VMware 다운로드 페이지의 파일과 같은지 확인합니다. 다운로드 페이지에 제공된 체크섬을 사용하여 다운로드 파일의 무결성을 검증합니다. 자세한 내용은 VMware 다운로드 페이지 아래쪽에 있는 링크를 참조하십시오.
- 3 기본 가상 장치의 전원이 켜져 있는지 확인합니다.
- 4 기본 가상 장치의 CD-ROM 드라이브를 다운로드한 ISO 파일에 연결합니다.

참고 ISO 파일이 가상 시스템에 연결된 후 업데이트를 확인할 수 없으면, 장치에 로그인하고 `mount /dev/sr0 /media/cdrom` 파일 경로를 사용하여 Linux 내에 CD-ROM을 마운트합니다.

- 5 기본 vRealize Automation 장치에서 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **root**로 vRealize Automation 장치 관리에 로그인합니다.
- 6 **업데이트** 탭을 클릭합니다.
- 7 **설정**을 클릭합니다.
- 8 [업데이트 저장소] 아래에서 **CD-ROM 업데이트 사용**을 선택합니다.
- 9 **설정 저장**을 클릭합니다.

vRealize Automation 장치 업그레이드

업그레이드 사전 요구 사항을 완료하고 가상 장치 업데이트를 다운로드한 후에 vRealize Automation 6.2.5 장치를 현재 릴리스로 업데이트합니다.

또한 기본 vRealize Automation 장치에 대한 일부 설정을 재구성할 수도 있습니다.

기본 vRealize Automation 장치를 업그레이드한 후 환경의 다른 노드를 다음 순서로 업그레이드합니다.

- 1 각 보조 vRealize Automation 장치.
- 2 IaaS 웹 사이트.
- 3 IaaS Manager Service.
- 4 IaaS DEM.
- 5 IaaS 에이전트.
- 6 각 외부 vRealize Orchestrator 인스턴스 업그레이드 또는 마이그레이션.

vRealize Automation 장치에 업데이트 설치

vRealize Automation 6.2.5 장치에 vRealize Automation 업데이트를 설치하고 장치 설정을 구성합니다.

외부 PostgreSQL 데이터베이스에 대한 지원은 vRealize Automation 7.1부터 중단됩니다. 업그레이드 프로세스에서는 기존 PostgreSQL 외부 데이터베이스의 데이터를 vRealize Automation 장치의 일부인 PostgreSQL 내부 데이터베이스와 병합합니다.

CEIP를 통해 수집된 데이터에 대한 세부 정보 및 VMware에서 CEIP를 사용하는 목적이 Trust & Assurance Center의 <http://www.vmware.com/trustvmware/ceip.html>에 기술되어 있습니다.

업데이트를 설치하는 동안 vRealize Automation 장치 관리 인터페이스를 닫지 마십시오.

업그레이드 프로세스 중 문제가 발생하는 경우 [vRealize Automation 업그레이드 문제 해결](#) 항목을 참조하십시오.

사전 요구 사항

- 다운로드 방법을 선택했고 업데이트를 다운로드했는지 확인합니다. [vRealize Automation 장치 업데이트 다운로드](#) 항목을 참조하십시오.
- 고가용성 분산 배포의 경우에는 [기존 vRealize Automation 6.2.5 환경 백업](#)의 내용을 참조하십시오.
- 로드 밸런서가 있는 배포의 경우 트래픽이 기본 노드로만 전달되고 상태 모니터가 사용되지 않도록 설정되었는지 확인합니다.
- 공통 구성 요소 카탈로그 구성 요소가 환경에 설치된 경우 업그레이드하기 전에 해당 구성 요소를 제거합니다. 자세한 내용은 "공통 구성 요소 카탈로그 설치 가이드"를 참조하십시오. 이 가이드를 사용할 수 없으면 [vRealize Automation 업그레이드 검사 목록](#)에 나와 있는 대체 절차를 사용하십시오.
- jdbc:postgresql 데이터베이스 연결이 마스터 PostgreSQL 노드의 외부 IP 주소를 가리키는지 확인합니다.
 - a 각 vRealize Automation 장치에서 새 명령 프롬프트를 엽니다.
 - b `/etc/vcac/server.xml`로 이동하고 `server.xml`을 백업합니다.
 - c `server.xml`을 엽니다.
 - d 필요한 경우 Postgres 데이터베이스를 가리키는 `server.xml` 파일 항목 `jdbc:posgresql`을 편집하고 해당 항목이 마스터 PostgreSQL 노드의 외부 IP 주소(외부 PostgreSQL의 경우) 또는 기본 가상 장치(포함된 PostgreSQL의 경우)를 가리키도록 지정합니다.

예: `jdbc:postgresql://198.15.100.60:5432/vcac`
- 업그레이드 전에, 저장되고 진행 중인 모든 요청이 완료되었는지 확인합니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스를 엽니다.
 - a 기본 vRealize Automation 장치에서 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **root**로 vRealize Automation 장치 관리에 로그인합니다.
 - b **root**라는 사용자 이름과 장치를 배포할 때 입력한 암호를 사용하여 로그인합니다.
- 2 서비스를 클릭하고 iaas-service를 제외한 각 서비스가 [등록됨]으로 나열되었는지 확인합니다.
- 3 업데이트 > 설정을 선택합니다.
- 4 다음 중 하나를 선택합니다.
 - 기본 저장소 사용.
 - CDROM 업데이트 사용
- 5 설정 저장을 클릭합니다.
- 6 상태를 선택합니다.
- 7 업데이트 확인을 클릭하여 업데이트가 있는지 확인합니다.
- 8 (선택 사항) vRealize Automation 장치 인스턴스의 경우 장치 버전 영역에서 세부 정보를 클릭하여 릴리스 정보의 위치에 대한 정보를 확인합니다.
- 9 업데이트 설치를 클릭합니다.
- 10 확인을 클릭합니다.

업데이트가 진행 중임을 알리는 메시지가 나타납니다.
- 11 (선택 사항) 디스크 1의 크기를 50GB로 수동 조정하지 않았다면 다음 단계를 수행합니다.
 - a 가상 장치를 재부팅하라는 메시지가 나타나면 시스템을 클릭하고 재부팅을 클릭합니다.

재부팅하는 동안 시스템에서 업데이트에 필요한 공간이 조정됩니다.
 - b 시스템이 재부팅된 후 vRealize Automation 장치 관리 인터페이스에 다시 로그인하여 iaas-service를 제외한 각 서비스가 [등록됨]으로 나열되었는지 확인하고 업데이트 > 상태를 선택합니다.
 - c 업데이트 확인 및 업데이트 설치를 클릭합니다.
- 12 업그레이드 진행률을 보려면 다음 로그 파일을 엽니다.
 - /opt/vmware/var/log/vami/updatecli.log
 - /opt/vmware/var/log/vami/vami.log
 - /var/log/vmware/horizon/horizon.log
 - /var/log/bootstrap/*.log

업그레이드 프로세스 중에 로그아웃했다가 업그레이드가 완료되기 전에 다시 로그인하는 경우 계속하여 로그 파일의 업데이트 진행률을 파악할 수 있습니다. `updatecli.log` 파일에 업그레이드 이전의 vRealize Automation 버전에 대한 정보가 표시될 수 있습니다. 표시된 이 버전이 업그레이드 프로세스의 후반부에 올바른 버전으로 변경됩니다.

업데이트를 완료하는 데 필요한 시간은 환경에 따라 다릅니다.

- 13 vRealize Automation 장치 관리 인터페이스에서 **원격 분석**을 클릭합니다. CEIP(고객 환경 향상 프로그램) 참여에 대한 참고 사항을 읽고 프로그램에 참여할지 여부를 선택합니다.

CEIP를 통해 수집된 데이터에 대한 세부 정보 및 VMware에서 CEIP를 사용하는 목적이 Trust & Assurance Center의 <http://www.vmware.com/trustvmware/ceip.html>에 기술되어 있습니다.

고객 환경 향상 프로그램에 대한 자세한 내용은 [vRealize Automation에 대한 고객 환경 향상 프로그램 참여 또는 탈퇴](#) 항목을 참조하십시오.

다음에 수행할 작업

[VMware Identity Manager에 대한 Single Sign-On 암호 업데이트](#).

VMware Identity Manager에 대한 Single Sign-On 암호 업데이트

업데이트를 설치한 후 VMware Identity Manager에 대한 Single Sign-On 암호를 업데이트해야 합니다.

VMware Identity Manager는 Identity Appliance 및 vSphere SSO 구성 요소를 바꿉니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스에서 로그아웃하고 브라우저를 닫은 다음 브라우저를 다시 열어 다시 로그인합니다.

- 2 **vRA > SSO**를 선택합니다.

- 3 새 VMware Identity Manager 암호를 입력하고 **설정 저장**을 클릭합니다.

단순한 암호를 사용하지 마십시오. 다음 오류 메시지가 나타나면 무시해도 됩니다. SSO 서버가 연결되지 않았습니다. 서비스를 다시 시작하려면 몇 분이 걸릴 수 있습니다.

암호가 수락되었습니다.

고가용성 배포의 경우 암호가 첫 번째 vRealize Automation 장치 노드에 적용되고 모든 보조 vRealize Automation 장치 노드에 전파됩니다.

- 4 가상 장치를 재부팅합니다.

a **시스템** 탭을 클릭합니다.

b **재부팅**을 클릭하고 선택을 확인합니다.

5 모든 서비스가 실행 중인지 확인합니다.

- a vRealize Automation 장치 관리 인터페이스에 로그인합니다.
- b 콘솔에서 **서비스** 탭을 클릭합니다.
- c **새로 고침** 탭을 클릭하여 서비스 시작 진행률을 모니터링합니다.

최소 35개의 서비스가 보여야 합니다.

6 IaaS 서비스를 제외하고 모든 서비스가 등록되었는지 확인합니다.

릴리스 관리 서비스는 vRealize Code Stream 라이선스 키 없이 시작되지 않습니다.

다음에 수행할 작업

라이선스 키 업데이트.

라이선스 키 업데이트

최신 버전의 vRealize Automation 장치를 사용하려면 라이선스 키를 업그레이드해야 합니다.

절차

1 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

2 **vRA > 라이선싱**을 클릭합니다.

라이선싱 탭을 사용할 수 없는 경우 다음 단계를 수행하고 해당 절차를 반복합니다.

- a 관리 인터페이스에서 로그아웃합니다.
- b 브라우저 캐시를 지웁니다.

3 **새 라이선스 키** 텍스트 상자에 새 라이선스 키를 입력합니다.

EULA(최종 사용자 라이선스 계약)에 따라 끝점 및 할당량이 플래그 지정됩니다.

4 **키 제출**을 클릭합니다.

다음에 수행할 작업

ID 저장소를 VMware Identity Manager로 마이그레이션.

ID 저장소를 VMware Identity Manager로 마이그레이션

vRealize Automation 6.2.5에서 최신 버전으로 업그레이드할 때 ID 저장소를 마이그레이션해야 합니다.

다음 절차에 필요한 대로 6.2.5 테넌트 구성 정보의 스냅샷을 참조하십시오.

참고 ID 저장소를 마이그레이션한 후 vRealize Code Stream의 사용자는 수동으로 vRealize Code Stream 역할을 재할당해야 합니다.

절차

1 해당 테넌트에 대한 로컬 사용자 계정 생성

로컬 사용자 계정을 사용하여 테넌트를 설정하고 해당 로컬 사용자 계정에 테넌트 관리자 권한을 할당해야 합니다.

2 Active Directory 링크에 대한 사용자 및 그룹 동기화

디렉토리 관리 기능을 사용하여 사용자 및 그룹을 vRealize Automation으로 가져오려면 Active Directory 링크에 연결해야 합니다.

3 사용자 지정 그룹을 대상 VMware Identity Manager로 마이그레이션

소스 환경의 모든 사용자 지정 그룹을 대상 배포의 vIDM(VMware Identity Manager)으로 마이그레이션해야 합니다.

4 여러 테넌트 및 IaaS 관리자 마이그레이션

테넌트 또는 IaaS 관리자가 있는 각 vRealize Automation 테넌트에 대해 각 관리자를 수동으로 삭제하고 복원해야 합니다.

해당 테넌트에 대한 로컬 사용자 계정 생성

로컬 사용자 계정을 사용하여 테넌트를 설정하고 해당 로컬 사용자 계정에 테넌트 관리자 권한을 할당해야 합니다.

테넌트 각각에 대해 이 절차를 반복합니다.

사전 요구 사항

새로운 VMware Identity Manager 암호를 설정했는지 확인합니다. [VMware Identity Manager에 대한 Single Sign-On 암호 업데이트](#) 항목을 참조하십시오.

절차

1 기본 시스템 관리자 사용자 이름 **administrator** 및 암호로 vRealize Automation 콘솔에 로그인합니다.

콘솔 위치는 <https://vra-appliance/vcac/>입니다.

2 테넌트를 클릭합니다.

예를 들어 기본 테넌트의 경우 **vsphere.local**을 클릭합니다.

3 로컬 사용자 탭을 선택합니다.

4 새로 만들기를 클릭합니다.

5 로컬 사용자 계정을 생성합니다.

이 사용자에게 테넌트 관리자 역할을 할당합니다. 로컬 사용자 이름이 `vsphere.local Active Directory`에 대해 고유한지 확인합니다.

6 **확인**을 클릭합니다.**7** **관리자**를 클릭합니다.**8** **테넌트 관리자** 검색 상자에 로컬 사용자 이름을 입력하고 **Enter** 키를 누릅니다.**9** **완료**를 클릭합니다.**10** 콘솔에서 로그아웃합니다.

다음에 수행할 작업

[Active Directory 링크에 대한 사용자 및 그룹 동기화](#).

Active Directory 링크에 대한 사용자 및 그룹 동기화

디렉토리 관리 기능을 사용하여 사용자 및 그룹을 vRealize Automation으로 가져오려면 **Active Directory 링크**에 연결해야 합니다.

테넌트 각각에 대해 이 절차를 수행합니다.

사전 요구 사항

Active Directory에 대한 액세스 권한이 있는지 확인합니다.

절차

1 `https://vra-appliance/vcac/org/tenant_name`에서 vRealize Automation 콘솔에 로그인합니다.**2** **관리 > 디렉토리 관리 > 디렉토리**를 선택합니다.**3** **디렉토리 추가**를 클릭하고 **LDAP/IWA를 통한 Active Directory 추가**를 선택합니다.**4** Active Directory 계정 설정을 입력합니다.

◆ 비네이티브 Active Directory

옵션	샘플 입력
디렉토리 이름	고유한 디렉토리 이름을 입력합니다. 비네이티브 Active Directory를 사용하는 경우 [LDAP를 통한 Active Directory]를 선택합니다.
이 디렉토리는 DNS 서비스를 지원합니 다.	이 옵션을 선택 해제합니다.
기본 DN	서버가 검색하는 디렉토리에 대한 시작점의 DN(고유 이름)을 입력합니다. 예를 들어 <code>cn=users,dc=rainpole,dc=local</code> 을 입력합니다.

옵션	샘플 입력
Bind DN	사용자를 검색할 권한이 있는 Active Directory 사용자 계정의 CN(일반 이름)을 포함하여 전체 DN(고유 이름)을 입력합니다. 예를 들어 cn=config_admin infra,cn=users,dc=rainpole,dc=local 을 입력합니다.
Bind DN 암호	사용자를 검색할 수 있는 계정에 대한 Active Directory 암호를 입력합니다.

◆ 네이티브 Active Directory

옵션	샘플 입력
디렉토리 이름	고유한 디렉토리 이름을 입력합니다. 네이티브 Active Directory를 사용하는 경우 [Active Directory(Windows 통합 인증)]를 선택합니다.
도메인 이름	가입할 도메인의 이름을 입력합니다.
도메인 관리자 사용자 이름	도메인 관리자의 사용자 이름을 입력합니다.
도메인 관리자 암호	도메인 관리자 계정의 암호를 입력합니다.
Bind 사용자 UPN	이메일 주소 형식을 사용하여 도메인을 인증할 수 있는 사용자의 이름을 입력합니다.
Bind DN 암호	사용자를 검색할 수 있는 계정에 대한 Active Directory Bind 계정 암호를 입력합니다.

5 **연결 테스트**를 클릭하여 구성된 디렉토리에 대한 연결을 테스트합니다.

6 **저장 및 다음**을 클릭합니다.

도메인 선택 페이지가 표시되고 도메인 목록이 표시됩니다.

7 기본 도메인 설정을 수락하고 **다음**을 클릭합니다.

8 특성 이름이 올바른 Active Directory 특성에 매핑되어 있는지 확인하고 **다음**을 클릭합니다.

9 동기화할 그룹과 사용자를 선택합니다.

a **새로 만들기** 아이콘을 클릭합니다.

b 사용자 도메인을 입력하고 **그룹 찾기**를 클릭합니다.

예를 들어 **dc=vcac,dc=local**을 입력합니다.

c 동기화할 그룹을 선택하려면 **선택**을 클릭하고 **다음**을 클릭합니다.

d **사용자 선택** 페이지에서 동기화할 사용자를 선택하고 **다음**을 클릭합니다.

10 사용자 및 그룹이 디렉토리에 동기화되고 있는지 검토하고 **디렉토리 동기화**를 클릭합니다.

디렉토리 동기화에 시간이 걸리며 백그라운드에서 실행됩니다.

11 **관리 > 디렉토리 관리 > ID 제공자**를 선택하고 새 ID 제공자를 클릭합니다.

예: **WorkspaceIDP__1**.

- 12 페이지 맨 아래로 스크롤하고 vRealize Automation 로드 밸런서에 대한 FQDN을 가리키도록 IdP 호스트 이름 속성의 값을 업데이트합니다.
- 13 **저장**을 클릭합니다.
- 14 각 테넌트 및 ID 제공자에 대해 11~13단계를 반복합니다.
- 15 모든 vRealize Automation 노드를 업그레이드한 후 각 테넌트에 로그인하고 **관리 > 디렉토리 관리 > ID 제공자**를 선택합니다.

각 ID 제공자에 모든 vRealize Automation 커넥터가 추가되어 있습니다.

예를 들어 배포에 두 개의 vRealize Automation 장치가 있는 경우 ID 제공자에는 두 개의 연결된 커넥터가 있습니다.

사용자 지정 그룹을 대상 **VMware Identity Manager**로 마이그레이션

소스 환경의 모든 사용자 지정 그룹을 대상 배포의 vIDM(VMware Identity Manager)으로 마이그레이션해야 합니다.

사용자 지정 그룹을 마이그레이션하기 위한 이 절차를 완료합니다.

사전 요구 사항

- 해당 테넌트에 대한 로컬 사용자 계정 생성.
- vRealize Automation 가상 장치에서 Horizon Workspace 서비스가 실행 중인지 확인합니다.

절차

- 1 vRealize Automation 가상 장치에서 SSH 세션을 시작합니다.
- 2 명령 프롬프트에서 vRealize Automation 가상 장치를 설치할 때 생성한 암호를 사용하여 **root**로 로그인합니다.
- 3 다음 명령을 실행합니다.

```
vcac-config migrate-custom-groups
```

- 마이그레이션이 완료되면 사용자 지정 그룹의 마이그레이션이 완료되었습니다! 메시지가 표시됩니다.
- 소스 환경에 사용자 지정 그룹이 없는 경우 vRA 데이터베이스에서 사용자 지정 그룹을 찾을 수 없습니다. 마이그레이션 프로세스를 건너뛵니다. 메시지가 표시됩니다.

참고 사용자 지정 그룹 마이그레이션이 실패하는 경우 `/var/log/vmware/vcac/vcac-config.log`의 로그 파일에서 자세한 내용을 확인하십시오.

여러 테넌트 및 IaaS 관리자 마이그레이션

테넌트 또는 IaaS 관리자가 있는 각 vRealize Automation 테넌트에 대해 각 관리자를 수동으로 삭제하고 복원해야 합니다.

vRealize Automation 콘솔에서 각 테넌트에 대해 다음 절차를 수행합니다.

사전 요구 사항

업그레이드된 가상 장치에서 vRealize Automation 콘솔에 로그인합니다.

- 1 업그레이드된 가상 장치에서 해당하는 정규화된 도메인 이름(https://va-hostname.domain_name/vcac)을 사용하여 vRealize Automation 콘솔을 엽니다.

분산 환경의 경우, 마스터 가상 장치에서 콘솔을 엽니다.

- 2 **vsphere.local** 도메인을 선택합니다.
- 3 **administrator**라는 사용자 이름과 가상 장치를 배포할 때 입력한 암호를 사용하여 로그인합니다.

절차

- 1 **관리 > 테넌트**를 선택합니다.
- 2 테넌트 이름을 클릭합니다.
- 3 **관리자**를 클릭합니다.
- 4 각 테넌트 및 IaaS 관리자 이름 및 사용자 이름이 포함된 목록을 만듭니다.
- 5 각 관리자를 가리킨 후 삭제 아이콘(✖)을 클릭합니다. 모든 관리자를 삭제할 때까지 이 작업을 반복합니다.
- 6 **완료**를 클릭합니다.
- 7 [테넌트] 페이지에서 테넌트 이름을 다시 클릭합니다.
- 8 **관리자**를 클릭합니다.
- 9 앞서 삭제한 각 사용자의 이름을 적절한 검색 상자에 입력하고 **Enter** 키를 누릅니다.
- 10 검색 결과에서 적절한 사용자의 이름을 클릭하여 해당 사용자를 관리자로 다시 추가합니다.
작업을 마치면 테넌트 관리자 및 IaaS 관리자 목록이 삭제했던 관리자 목록과 동일하게 됩니다.
- 11 **완료**를 클릭합니다.

다음에 수행할 작업

보조 장치를 업그레이드합니다. [추가 vRealize Automation 장치에 업데이트 설치](#) 항목을 참조하십시오.

추가 vRealize Automation 장치에 업데이트 설치

고가용성 환경에서 마스터 가상 장치는 마스터 모드에서 포함된 PostgreSQL 데이터베이스를 실행하는 노드입니다. 환경의 다른 노드는 포함된 PostgreSQL 데이터베이스를 복제 모드에서 실행합니다. 업그레이드 중, 복제 가상 6.2.5 장치에는 데이터베이스 변경이 필요하지 않습니다.

업데이트를 설치하는 동안 vRealize Automation 장치 관리 인터페이스를 닫지 마십시오.

사전 요구 사항

- 가상 장치 업데이트를 다운로드했는지 확인합니다. [vRealize Automation 장치 업데이트 다운로드](#) 항목을 참조하십시오.

- jdbc:postgresql 데이터베이스 연결이 마스터 PostgreSQL 노드의 외부 IP 주소를 가리키는지 확인합니다.
 - a vRealize Automation 장치에서 새 명령 프롬프트를 엽니다.
 - b `/etc/vcac/server.xml`로 이동하여 `server.xml` 파일을 백업합니다.
 - c `server.xml` 파일을 엽니다.
 - d 필요한 경우 사용하려는 PostgreSQL 데이터베이스를 나타내도록 `server.xml` 파일 항목 `jdbc:postgresql`을 편집합니다.
 - 외부 PostgreSQL 데이터베이스의 경우 마스터 PostgreSQL 노드의 외부 IP 주소를 입력합니다.
 - 포함된 PostgreSQL 데이터베이스의 경우 마스터 가상 장치의 IP 주소를 입력합니다.
- 예: `jdbc:postgresql://198.15.100.60:5432/vcac`

절차

- 1 업그레이드를 위해 vRealize Automation 장치 관리 인터페이스를 엽니다.
 - a 각 보조 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
 - b **업데이트**를 클릭합니다.
- 2 **설정**을 클릭합니다.
- 3 [업데이트 저장소] 섹션에서 VMware 저장소 또는 CDROM 중 하나를 선택하여 업데이트를 다운로드합니다.
- 4 **상태**를 클릭합니다.
- 5 **업데이트 확인**을 클릭하여 업데이트가 있는지 확인합니다.
- 6 **업데이트 설치**를 클릭합니다.
- 7 **확인**을 클릭합니다.
업데이트가 진행 중임을 알리는 메시지가 나타납니다.
- 8 (선택 사항) 디스크 1GB의 크기를 50GB로 수동 조정하지 않았다면 다음 단계를 수행합니다.
 - a 가상 장치를 재부팅하라는 메시지가 나타나면 **시스템**을 클릭하고 **재부팅**을 클릭합니다.
재부팅하는 동안 시스템에서 업데이트에 필요한 디스크 1의 공간이 조정됩니다.
 - b 시스템이 재부팅되었으면 로그아웃했다가 vRealize Automation 장치 관리 인터페이스에 다시 로그인하고 **업데이트 > 상태**를 선택합니다.
 - c **업데이트 확인** 및 **업데이트 설치**를 클릭합니다.
- 9 업그레이드가 성공적으로 처리되었는지 확인하려면 로그 파일을 엽니다.
 - `/opt/vmware/var/log/vami/vami.log`

- /opt/vmware/var/log/vami/updatecli.log
- /var/log/vmware/horizon/horizon.log
- /var/log/bootstrap/*.log

업그레이드 프로세스 중에 로그아웃했다가 로그인하는 경우 계속하여 로그 파일 /opt/vmware/var/log/vami/updatecli.log의 업데이트 진행률을 따를 수 있습니다.

환경에 따라 업데이트를 완료하는 데 소요되는 시간이 다릅니다.

- 10 업데이트가 완료되면 vRealize Automation 장치 관리 인터페이스에서 로그아웃하고 웹 브라우저 캐시를 지운 다음 vRealize Automation 장치 관리 인터페이스에 로그인합니다.
- 11 가상 장치를 재부팅합니다.
 - a 시스템을 클릭합니다.
 - b 재부팅을 클릭하고 선택을 확인합니다.
- 12 가상 장치가 재부팅되면 복제 vRealize Automation 장치 관리 인터페이스에 로그인합니다.
- 13 클러스터를 선택합니다.
- 14 마스터 vRealize Automation 장치 사용자 이름 및 암호를 입력합니다.
- 15 클러스터에 가입을 클릭합니다.
- 16 서비스를 클릭하고 iaas-service를 제외한 각 서비스가 [등록됨]으로 나열되었는지 확인합니다.

다음에 수행할 작업

[vRealize Automation 업그레이드 후 IaaS 서버 구성 요소 업그레이드.](#)

vRealize Automation 업그레이드 후 IaaS 서버 구성 요소 업그레이드

vRealize Automation 6.2.5에서 업그레이드한 후 시스템 관리자가 Microsoft SQL Server 데이터베이스를 포함한 IaaS 서버 구성 요소를 업그레이드합니다.

IaaS 서버 구성 요소를 업그레이드하기 위한 2개의 옵션이 있습니다.

- 자동화된 IaaS 업그레이드 셸 스크립트를 사용합니다.
- 대상 vRealize Automation 릴리스와 함께 제공된 vRealize Automation IaaS 설치 관리자 실행 파일을 사용합니다.

공통 구성 요소 카탈로그 구성 요소가 설치된 경우 업그레이드하기 전에 해당 구성 요소를 제거해야 합니다. 업그레이드를 완료한 후 적절한 버전의 구성 요소를 다시 설치할 수 있습니다. 자세한 내용은 "공통 구성 요소 카탈로그 설치 가이드"를 참조하십시오. 이 가이드를 사용할 수 없으면 [vRealize Automation 업그레이드 검사 목록](#)에 나와 있는 대체 절차를 사용하십시오.

업그레이드 셸 스크립트를 사용하여 IaaS 구성 요소 업그레이드

vRealize Automation 6.2.5 장치를 대상 vRealize Automation 릴리스로 각각 업데이트한 후 업그레이드 셸 스크립트를 사용하여 IaaS 구성 요소를 업그레이드합니다.

업데이트된 기본 또는 마스터 vRealize Automation 장치에는 각 IaaS 노드 및 구성 요소를 업그레이드하는 데 사용하는 셀 스크립트가 포함됩니다.

가상 시스템을 위한 vSphere 콘솔을 사용하거나 SSH 콘솔 세션을 사용하여 업그레이드 스크립트를 실행할 수 있습니다. vSphere 콘솔을 사용하는 경우 스크립트 실행을 중단시킬 수 있는 간헐적인 네트워크 연결 문제를 피합니다.

스크립트가 구성 요소를 업그레이드하는 중에 스크립트를 중지할 경우, 스크립트는 구성 요소 업그레이드가 완료될 때까지 실행됩니다. 노드에 업그레이드되지 않은 구성 요소가 있는 경우에는 스크립트를 다시 실행해야 합니다.

업그레이드가 완료되면 `/usr/lib/vcac/tools/upgrade/upgrade.log`에서 업그레이드 로그 파일을 열어 업그레이드 결과를 검토할 수 있습니다.

사전 요구 사항

- 모든 vRealize Automation 장치의 성공적인 업데이트를 확인합니다.
- 모든 vRealize Automation 장치를 업데이트한 후 IaaS 서버를 재부팅하는 경우 IaaS Windows 서비스를 중지해야 합니다. IaaS 구성 요소를 업그레이드하기 전에 관리 에이전트 서비스를 제외한 모든 IaaS Windows 서비스를 서버에서 중지합니다.
- 마스터 또는 기본 vRealize Automation 장치 노드에서 업그레이드 셀 스크립트를 실행하기 전에 각 서비스가 [등록됨] 상태인지 확인합니다.
 - a vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
 - b **서비스**를 클릭합니다.
 - c `iaas-service`를 제외한 각 서비스가 [등록됨] 상태인지 확인합니다.
- 각 vRealize Automation IaaS 가상 시스템에서 관리 에이전트를 업그레이드합니다.
 - a 브라우저를 열고 vRealize Automation 장치의 [IaaS 설치] 페이지로 이동합니다.
`https://vrealize-automation-appliance-FQDN:5480/installer`
 - b **관리 에이전트 설치 관리자**를 클릭합니다.
기본적으로 설치 관리자는 [다운로드] 폴더에 다운로드됩니다.
 - c 각 vRealize Automation IaaS 가상 시스템에 로그인한 후 **관리 에이전트 설치 관리자** 파일을 사용하여 관리 에이전트를 업그레이드합니다.
- Model Manager 데이터가 설치되어 있는 기본 IaaS 웹 사이트 노드에 JAVA SE Runtime Environment 8, 64비트, 업데이트 161 이상이 설치되어 있는지 확인합니다. Java를 설치한 후 환경 변수 `JAVA_HOME`을 새 버전으로 설정해야 합니다.
- 각 IaaS 웹 사이트 노드에 로그인하고 생성 날짜가 `web.config` 파일의 수정된 날짜 이전인지 확인합니다. `web.config` 파일의 생성 날짜가 수정된 날짜와 같거나 이후인 경우 **IaaS 웹 사이트 구성 요소에 대한 업그레이드 실패**의 절차를 수행합니다.

- 각 IaaS 노드에서 다음 단계를 수행하여 해당 IaaS 노드에 업그레이드된 IaaS 관리 에이전트가 있는지 확인합니다.
 - a vRealize Automation 장치 관리 인터페이스에 로그인합니다.
 - b 클러스터를 선택합니다.
 - c 각 IaaS 노드에서 설치된 모든 구성 요소 목록을 확장하고 IaaS 관리 에이전트를 찾습니다.
 - d 관리 에이전트 버전이 최신인지 확인합니다.
 - 롤백해야 하는 경우 IaaS Microsoft SQL Server 데이터베이스 백업에 액세스할 수 있는지 확인합니다.
 - 분리된 모든 IaaS 노드를 삭제합니다. vRealize Automation에서 분리된 노드 삭제 항목을 참조하십시오.
 - 해당 배포의 IaaS 서버 스냅샷이 사용 가능한지 확인합니다.
- 업그레이드가 실패하면 스냅샷 및 데이터베이스 백업으로 되돌리고 다른 업그레이드를 시도합니다.

절차

- 1 기본 또는 마스터 vRealize Automation 장치 노드에서 새 콘솔 세션을 열고 루트 계정으로 로그인합니다.
- SSH를 사용하여 업그레이드 스크립트를 실행하려면 SSH 콘솔 세션을 엽니다.
- 2 디렉토리를 `/usr/lib/vcac/tools/upgrade/`로 변경합니다.
 - 3 프롬프트에서 이 명령을 실행하여 `upgrade.properties` 파일을 생성합니다.
- ```
./generate_properties
```
- 4 `upgrade.properties` 파일을 열고 모든 필수 값을 입력합니다.
- 이 테이블은 환경에 따라 다른 필수 값을 보여 줍니다. 예를 들어 DEM 작업자 또는 Orchestrator가 포함된 노드에서는 DEM 자격 증명이 필요합니다.

| 필수 값         | 설명                                                            | 자격 증명 형식    | 예제 값               |
|--------------|---------------------------------------------------------------|-------------|--------------------|
| web_username | 기본 웹 노드에 대한 사용자 이름입니다. 한 번만 필요합니다.                            | Domain\User | iaasDomain\webuser |
| web_password | 기본 웹 노드에 대한 암호입니다. 한 번만 필요합니다.                                | 암호          | pa\$\$w0rd!        |
| dem_username | DEM 작업자 또는 DEM 조정자에 대한 사용자 이름입니다. DEM 구성 요소가 설치된 각 노드에 필요합니다. | Domain\User | iaasDomain\demuser |
| dem_password | DEM 작업자 또는 DEM 조정자에 대한 암호입니다. DEM 구성 요소가 설치된 각 노드에 필요합니다.     | 암호          | pa\$\$w0rd!        |

| 필수 값                | 설명                                                                | 자격 증명 형식      | 예제 값                  |
|---------------------|-------------------------------------------------------------------|---------------|-----------------------|
| agent_username      | vSphere 에이전트와 같은 에이전트에 대한 사용자 이름입니다. 에이전트 구성 요소가 설치된 각 노드에 필요합니다. | Domain\User   | iaasDomain\agent_user |
| agent_password      | vSphere 에이전트와 같은 에이전트에 대한 암호입니다. 에이전트 구성 요소가 설치된 각 노드에 필요합니다.     | 암호            | pa\$\$w0rd!           |
| vidm_admin_password | VIDM 관리자 암호입니다. vRealize Automation 6.2.5에서 업그레이드할 때만 필요합니다.      | VIDM_password | pa\$\$w0rd!           |

보안상의 이유로 업그레이드 셸 스크립트를 실행할 때 **upgrade.properties** 파일이 제거됩니다. 파일의 속성은 IaaS 관리 에이전트를 통해 나오는 각 IaaS 구성 요소에 대한 정보를 사용하여 정의됩니다. **./generate\_properities** 또는 **./upgrade\_from\_62x** 셸 스크립트를 실행하기 전에 모든 IaaS 관리 에이전트가 업그레이드되고 정상 상태여야 합니다. 업그레이드 셸 스크립트를 실행할 때 IaaS 관리 에이전트에 문제가 있는 경우 [업데이트를 통한 관리 에이전트 업그레이드 실패](#) 항목을 참조하십시오. **upgrade.properties** 파일을 다시 생성하려면 2단계와 3단계를 반복합니다.

## 5 업그레이드 스크립트를 실행합니다.

a 명령 프롬프트에서 **./upgrade\_from\_62x**를 입력합니다.

b Enter 키를 누릅니다.

스크립트는 각 IaaS 노드와 해당 노드에 설치된 모든 구성 요소를 표시합니다. 스크립트는 업그레이드를 설치하기 전에 각 구성 요소를 검증합니다. **upgrade.properties** 파일에 잘못된 값이 있는 경우 스크립트가 실패합니다.

첫 번째 IaaS 서버 구성 요소를 완료하는 데 30분 이상 소요될 수 있습니다. 업그레이드 중에 **Upgrading server components for node web1-vra.mycompany.com**과 유사한 메시지가 표시됩니다.

업그레이드 셸 스크립트가 실패한 경우 **upgrade.log** 파일을 검토합니다.

문제를 해결한 후 업그레이드 스크립트를 다시 실행할 수 있습니다. 업그레이드 스크립트를 다시 실행하기 전에 **upgrade.properties** 파일을 다시 생성하고 연 후 모든 필수 값을 입력합니다.

## 6 (선택 사항) 자동 Manager Service 페일오버를 사용하도록 설정합니다. [업그레이드 후 자동 Manager Service 페일오버를 사용하도록 설정](#) 항목을 참조하십시오.

다음에 수행할 작업

기본 제공 vRealize Orchestrator 제어 센터에 대한 액세스 복원.

## IaaS 설치 관리자를 사용하여 IaaS 구성 요소 업그레이드

vRealize Automation 6.2.5를 대상 vRealize Automation 릴리스로 업그레이드한 후 이 대체 방법을 사용하여 IaaS 구성 요소를 업그레이드할 수 있습니다.

## laaS 설치 관리자를 다운로드하여 laaS 구성 요소 업그레이드

vRealize Automation 6.2.5에서 업그레이드한 후 업그레이드할 laaS 구성 요소가 설치되어 있는 가상 시스템에 laaS 설치 관리자를 다운로드합니다.

이 절차를 진행하는 중에 인증서 경고가 표시될 수 있습니다. 이 경고는 무시해도 됩니다.

---

**참고** Manager Service의 패시브 백업 인스턴스를 제외하고, 업그레이드 프로세스 중 모든 서비스에 대한 시작 유형은 [자동]으로 설정되어야 합니다. 서비스를 [수동]으로 설정하는 경우 업그레이드 프로세스가 실패합니다.

---

### 사전 요구 사항

- laaS 설치 가상 시스템에 Microsoft .NET Framework 4.5.2 이상이 설치되어 있는지 확인합니다. VMware vRealize Automation laaS 설치 페이지에서 .NET 설치 관리자를 다운로드할 수 있습니다. 서비스를 종료한 후 .NET을 4.5.2로 업데이트하는 경우 가상 시스템은 설치의 일부로 다시 시작될 수 있습니다. 이 경우 관리 에이전트를 제외하고 수동으로 가상 시스템의 모든 laaS 서비스를 중지해야 합니다.
- Internet Explorer를 사용하여 다운로드하는 경우 보안 강화 구성 설정을 사용하지 말아야 합니다. 검색 창에 `res://iesetup.dll/SoftAdmin.htm`을 입력하고 Enter 키를 누릅니다.
- 업그레이드하려는 하나 이상의 laaS 구성 요소가 설치되어 있는 Windows Server에 로컬 관리자로 로그인합니다.

### 절차

- 1 브라우저를 열고 기본 또는 마스터 vRealize Automation 장치의 [laaS 설치] 페이지로 이동합니다.  
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 2 **laaS 설치 관리자**를 클릭합니다.
- 3 메시지가 표시되면 `setup__vrealize-automation-appliance-FQDN@5480.exe`를 데스크톱에 저장합니다.

파일 이름을 변경하지 마십시오. 이 이름은 설치를 올바른 vRealize Automation 장치에 연결합니다.

### 다음에 수행할 작업

- 외부 vRealize Orchestrator 장치 클러스터가 있는 경우 다음 항목을 참조하십시오.
- [vRealize Automation 업그레이드 후 laaS 구성 요소 업그레이드](#) 항목을 참조하십시오.

## vRealize Automation 업그레이드 후 laaS 구성 요소 업그레이드

vRealize Automation 6.2.5를 업그레이드한 후에는 SQL 데이터베이스를 업그레이드하고 laaS 구성 요소가 설치된 모든 시스템을 구성해야 합니다. 최소 설치와 분산 설치를 위해 이러한 단계를 사용할 수 있습니다.

---

**참고** laaS 설치 관리자는 업그레이드할 laaS 구성 요소가 있는 가상 시스템에 있어야 합니다. 웹 노트에서 원격으로도 업그레이드할 수 있는 Microsoft SQL 데이터베이스를 제외하고 외부 위치에서는 설치 관리자를 실행할 수 없습니다.

---

해당 배포의 IaaS 서버 스냅샷이 사용 가능한지 확인합니다. 업그레이드가 실패하면 해당 스냅샷으로 되돌리고 다른 업그레이드를 시도할 수 있습니다.

서비스가 다음 순서로 업그레이드되도록 업그레이드를 수행합니다.

## 1 IaaS 웹 사이트

로드 밸런서를 사용 중인 경우 기본이 아닌 모든 노드에 대해 트래픽을 사용하지 않도록 설정합니다.

웹 사이트 서비스를 실행 중인 다음 서버를 업그레이드하기 전에 현재 서버에 대한 업그레이드를 완료합니다. Model Manager Data 구성 요소가 설치되어 있는 것부터 시작합니다.

외부 Microsoft SQL 데이터베이스에 대한 수동 업그레이드를 수행 중인 경우 웹 노드를 업그레이드하기 전에 외부 SQL을 업그레이드해야 합니다. 웹 노드에서 외부 SQL을 원격으로 업그레이드할 수 있습니다.

## 2 Manager Service

패시브 Manager Service를 업그레이드하기 전에 액티브 Manager Service를 업그레이드합니다.

SQL 인스턴스에서 SSL 암호화를 사용하도록 설정하지 않은 경우 [IaaS 업그레이드 구성] 대화상자에서 **SSL 암호화**를 선택 해제합니다.

## 3 DEM 조정자 및 DEM 작업자

모든 DEM 조정자 및 DEM 작업자를 업그레이드합니다. 다음 서버를 업그레이드하기 전에 현재 서버에 대한 업그레이드를 완료합니다.

## 4 에이전트

에이전트를 실행 중인 다음 서버를 업그레이드하기 전에 현재 서버에 대한 업그레이드를 완료합니다.

## 5 관리 에이전트

업그레이드 프로세스의 일부로 업데이트됩니다.

한 서버에서 서로 다른 서비스를 사용 중인 경우 업그레이드하면 적절한 순서로 서비스가 업데이트됩니다. 예를 들어 사이트의 동일한 서버에 웹 사이트와 Manager Service가 있는 경우 모두 업데이트하도록 선택합니다. 업그레이드 설치 관리자가 적절한 순서로 업데이트를 적용합니다. 한 서버에 대한 업그레이드를 완료한 후에 다른 서버에 대한 업그레이드를 시작해야 합니다.

---

**참고** 배포에서 로드 밸런서를 사용하는 경우 업그레이드하려는 첫 번째 장치를 로드 밸런서에 연결해야 합니다. 캐시 오류를 피하려면 업그레이드를 적용하기 전에 로드 밸런서 트래픽에 대해 vRealize Automation 장치의 다른 모든 인스턴스를 사용하지 않도록 설정해야 합니다.

---

### 사전 요구 사항

- 기존 vRealize Automation 6.2.5 환경을 백업합니다.
- 모든 vRealize Automation 장치를 업데이트한 후 IaaS 서버를 재부팅하는 경우 IaaS Windows 서비스를 중지해야 합니다. IaaS 구성 요소를 업그레이드하기 전에 관리 에이전트 서비스를 제외한 모든 IaaS Windows 서비스를 서버에서 중지합니다.



- **IaaS 설치 관리자를 다운로드하여 IaaS 구성 요소 업그레이드.**
- Model Manager 데이터가 설치되어 있는 기본 IaaS 웹 사이트 노드에 올바른 Java 버전이 설치되어 있는지 확인합니다. JAVA SE Runtime Environment 8, 64비트, 업데이트 161 이상이 설치되어 있어야 합니다. Java를 설치한 후 환경 변수 JAVA\_HOME을 새 버전으로 설정합니다.
- 생성 날짜가 web.config 파일의 수정된 날짜 이전인지 확인합니다. web.config 파일의 생성 날짜가 수정된 날짜와 같거나 이후인 경우 **IaaS 웹 사이트 구성 요소에 대한 업그레이드 실패**의 절차를 수행합니다.
- vRealize Automation 6.2.5에서 업그레이드 중이고 외부 Microsoft SQL 데이터베이스가 있는 경우 올바른 관리 에이전트 버전이 설치되어 있어야 합니다. IaaS 웹 사이트 업그레이드를 실행하기 전에 외부 데이터베이스의 관리 에이전트는 버전 7.0 이상이어야 합니다. 외부 SQL 가상 시스템의 제어판에서 관리 에이전트 버전을 확인할 수 있습니다. 관리 에이전트의 버전이 7.0 이상이 아닌 경우 다음 단계를 완료하여 관리 에이전트를 업그레이드합니다.
  - a 브라우저에서 [IaaS 설치] 페이지로 이동합니다.  
<https://vrealize-automation-appliance-FQDN:5480/installer>
  - b **관리 에이전트 설치 관리자**를 클릭합니다.  
 기본적으로 설치 관리자는 [다운로드] 폴더에 다운로드됩니다.
  - c 외부 데이터베이스에 로그인하여 **관리 에이전트 설치 관리자** 파일로 관리 에이전트를 업그레이드한 후 Windows 관리 에이전트 서비스를 다시 시작합니다.
- 공통 구성 요소 카탈로그 구성 요소가 설치된 경우 업그레이드하기 전에 해당 구성 요소를 제거해야 합니다. 자세한 내용은 "공통 구성 요소 카탈로그 설치 가이드"를 참조하거나 **vRealize Automation 업그레이드 검사 목록**에 제공된 단계를 따르십시오.

#### 절차

- 1 로드 밸런서를 사용하고 있는 경우 환경을 준비합니다.
  - a Model Manager Data가 포함된 IaaS 웹 사이트 노드가 로드 밸런서 트래픽에 대해 사용되도록 설정되었는지 확인합니다.  
 vCAC Folder\Server\ConfigTool 폴더가 있는지 여부로 이 노드를 식별할 수 있습니다.
  - b 로드 밸런서 트래픽에 대해 기본이 아닌 Manager Service 및 기타 모든 IaaS 웹 사이트를 사용하지 않도록 설정합니다.
- 2 setup\_\_vrealize-automation-appliance-FQDN@5480.exe 설치 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 3 **다음**을 클릭합니다.
- 4 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 5 [로그인] 페이지에서 현재 배포에 대한 관리자 자격 증명을 입력합니다.  
 사용자 이름은 **root**이고 암호는 장치를 배포할 때 입력한 암호입니다.

6 인증서 수락을 선택합니다.

7 설치 유형 페이지에서 **업그레이드**가 선택되었는지 확인합니다.

**업그레이드**가 선택되지 않았다면 이 시스템의 구성 요소가 이미 이 버전으로 업그레이드된 것입니다.

8 다음을 클릭합니다.

9 업그레이드 설정을 구성합니다.

| 옵션                                                           | 작업                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Model Manager Data를 업그레이드하는 경우</b>                        | [vCAC 서버] 섹션에서 <b>Model Manager Data</b> 확인란을 선택합니다.<br>이 확인란은 기본적으로 선택되어 있습니다. Model Manager Data는 한 번만 업그레이드합니다. 분산 설치를 업그레이드할 때, 웹 서버와 Model Manager Data 간에 버전 불일치가 있으면 웹 서버가 작동을 중지합니다. Model Manager Data 업그레이드가 완료되면 웹 서버가 정상적으로 작동합니다.                                                                                                                                                                                                      |
| <b>Model Manager Data를 업그레이드하지 않는 경우</b>                     | [vCAC 서버] 섹션에서 <b>Model Manager Data</b> 확인란을 선택 해제합니다.                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>사용자 지정 워크플로를 Model Manager Data에서 최신 버전으로 유지하려는 경우</b>    | Model Manager Data를 업그레이드하는 경우 [확장성 워크플로] 섹션에서 <b>내 최신 워크플로 버전 유지</b> 확인란을 선택합니다.<br>이 확인란은 기본적으로 선택되어 있습니다. 사용자 지정 워크플로는 항상 유지됩니다. 확인란 선택은 버전 순서만 결정합니다. Model Manager에서 워크플로를 사용자 지정한 경우 가장 최신의 워크플로가 업그레이드 후 가장 최신 버전으로 유지되도록 하려면 이 옵션을 선택하십시오.<br>이 옵션을 선택하지 않으면 vRealize Automation Designer와 함께 제공된 각 워크플로의 버전이 업그레이드 후 가장 최신이 되며 업그레이드 전 가장 최신이었던 버전은 두 번째로 최신인 버전이 됩니다.<br>vRealize Automation Designer에 대한 자세한 내용은 "수명 주기 확장성" 항목을 참조하십시오. |
| <b>Distributed Execution Manager 또는 프록시 에이전트를 업그레이드하는 경우</b> | [서비스 계정] 섹션에 관리자 계정의 자격 증명을 입력합니다.<br>업그레이드하는 모든 서비스는 이 계정으로 실행됩니다.                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Microsoft SQL Server 데이터베이스를 유지하려는 경우</b>                 | Model Manager Data를 업그레이드하는 경우 <b>서버</b> 텍스트 상자에 데이터베이스 서버와 데이터베이스 인스턴스의 이름을 입력합니다. <b>데이터베이스 이름</b> 텍스트 상자에 데이터베이스 서버 이름의 FQDN(정규화된 도메인 이름)을 입력합니다.<br>데이터베이스 인스턴스가 기본이 아닌 SQL 포트에 있는 경우 서버 인스턴스 규격에 포트 번호를 포함합니다. Microsoft SQL 기본 포트 번호는 1433입니다.<br>관리자 노드를 업그레이드하는 경우 기본적으로 MSSQL SSL 옵션이 선택되어 있습니다. 해당 데이터베이스가 SSL을 사용하지 않는 경우 <b>데이터베이스 연결에 SSL 사용</b> 을 선택 해제합니다.                                                                           |

10 다음을 클릭합니다.

11 업그레이드하려는 모든 서비스가 [업그레이드 준비 완료] 페이지에 나타나는지 확인하고 **업그레이드**를 클릭합니다.

[업그레이드] 페이지와 진행률 표시기가 나타납니다. 업그레이드 프로세스가 완료되면 **다음** 버튼이 활성화됩니다.

12 다음을 클릭합니다.

**13 완료**를 클릭합니다.

**14** 모든 서비스가 다시 시작되었는지 확인합니다.

**15** 설명된 순서에 따라 배포의 각 IaaS 서버에 대해 이러한 단계를 반복합니다.

**16** 모든 구성 요소가 업그레이드되면 vRealize Automation 장치 관리 인터페이스에 로그인하고 이제 IaaS를 포함한 모든 서비스가 등록되어 있는지 확인합니다.

## 결과

선택된 모든 구성 요소는 새 릴리스로 업그레이드됩니다.

다음에 수행할 작업

- 기본 제공 vRealize Orchestrator 제어 센터에 대한 액세스 복원.
- 배포에서 로드 밸런서를 사용하는 경우 각 로드 밸런서 노드를 업그레이드하여 vRealize Automation 상태 점검을 사용하고 연결되지 않은 노드에 대해 로드 밸런서 트래픽을 다시 사용하도록 설정합니다. 이전 배포에서 로드 밸런싱된 포함된 PostgreSQL 데이터베이스를 사용한 경우 PostgreSQL 풀의 모든 노드가 필요하지 않으므로 이를 사용하지 않도록 설정합니다. 편리한 시간에 풀을 삭제합니다.

자세한 내용은 vRealize Automation 제품 설명서의 "로드 밸런서 문서" 섹션에서 "vRealize Automation 로드 밸런싱" 을 참조하십시오.

- (선택 사항) 자동 Manager Service 페일오버를 사용하도록 설정합니다. 업그레이드 후 자동 Manager Service 페일오버를 사용하도록 설정 항목을 참조하십시오.

## 기본 제공 vRealize Orchestrator 제어 센터에 대한 액세스 복원

IaaS 서버 구성 요소를 업그레이드한 후에는 vRealize Orchestrator에 대한 액세스를 복원해야 합니다.

vRealize Automation 6.2.5를 업그레이드할 때 역할 기반 액세스 제어 기능을 수용하려면 이 절차를 수행해야 합니다. 이 절차는 고가용성 환경에서 사용할 수 있습니다.

## 사전 요구 사항

vRealize Automation 환경에 대한 스냅샷을 생성합니다.

## 절차

**1** vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

`https://vrealize-automation-appliance-FQDN:5480`

**2** 클러스터를 선택합니다.

**3** 마스터 노드와 복제 노드를 식별합니다.

**4** 각 복제 노드에서 SSH 세션을 열고 관리자로 로그인한 후 다음 명령을 실행합니다.

```
service vco-server stop && service vco-configurator stop
```

**5** 마스터 노드에서 SSH 세션을 열고 관리자로 로그인한 후 다음 명령을 실행합니다.

```
rm /etc/vco/app-server/vco-registration-id
```

- 6 마스터 노드에서 디렉토리를 `/etc/vco/app-server/`로 변경합니다.
- 7 `sso.properties` 파일을 엽니다.
- 8 속성 이름 `com.vmware.o11n.sso.admin.group.name`에 공백이 있거나 Bash 명령에서 특수 문자로 인정될 수 있는 아포스트로피(') 또는 달러 기호(\$)와 같은 기타 Bash 관련 문자가 포함되어 있는 경우 다음 단계를 완료합니다.
  - a `com.vmware.o11n.sso.admin.group.name` 속성이 포함된 줄을 복사하고 값에 대해 AdminGroup을 입력합니다.
  - b `com.vmware.o11n.sso.admin.group.name` 속성이 포함된 원래 줄의 맨 앞에 #을 추가하여 줄에 주석 처리를 합니다.
  - c `sso.properties` 파일을 저장하고 닫습니다.
- 9 다음 명령을 실행합니다.
 

```
vcac-vami vco-service-reconfigure
```
- 10 8단계를 완료했다면 `sso.properties` 파일을 열고 다음 단계를 완료합니다.
  - a `com.vmware.o11n.sso.admin.group.name` 속성이 포함된 원래 줄의 맨 앞에서 #을 제거하여 줄에서 주석 처리를 제거합니다.
  - b `com.vmware.o11n.sso.admin.group.name` 속성이 포함된 줄의 사본을 제거합니다.
  - c `sso.properties` 파일을 저장하고 닫습니다.
- 11 다음 명령을 실행하여 vco-server 서비스를 다시 시작합니다.
 

```
service vco-server restart
```
- 12 다음 명령을 실행하여 vco-configurator 서비스를 다시 시작합니다.
 

```
service vco-configurator restart
```
- 13 vRealize Automation 장치 관리 인터페이스에서 **서비스**를 클릭하고 마스터 노드의 모든 서비스가 [등록됨] 상태가 될 때까지 기다립니다.
- 14 모든 서비스가 등록되면 vRealize Automation 복제 노드를 vRealize Automation 클러스터에 가입시켜 vRealize Orchestrator 구성을 동기화합니다.

다음에 수행할 작업

[vRealize Automation을 업그레이드한 후 외부 vRealize Orchestrator 마이그레이션.](#)

## vRealize Automation을 업그레이드한 후 외부 vRealize Orchestrator 마이그레이션

vRealize Orchestrator 7.5부터는 외부 vRealize Orchestrator 환경을 더 이상 업그레이드할 수 없습니다. 외부 vRealize Orchestrator 환경을 최신 버전으로 이동하려면 마이그레이션해야 합니다.

**참고** vRealize Automation에 내장된 vRealize Orchestrator 인스턴스는 vRealize Automation 업그레이드를 통해 자동으로 업그레이드됩니다. 내장된 vRealize Orchestrator만 사용하면 작업이 필요하지 않습니다.

vRealize Orchestrator 마이그레이션은 워크플로, 동작, 구성 및 리소스 요소, 패키지, 작업, 정책, 인증서, 플러그인 및 기타 기존 요소를 모두 덮어써서 외부 소스 vRealize Orchestrator 구성을 새로 구성된 vRealize Orchestrator 7.5 환경으로 전송합니다.

최신 vRealize Automation 릴리스로 업그레이드하는 경우 외부 vRealize Orchestrator 마이그레이션에는 두 가지 옵션이 있습니다.

- 외부 vRealize Orchestrator를 다른 외부 vRealize Orchestrator 인스턴스로 마이그레이션합니다. vRealize Orchestrator 설명서에서 [외부 Orchestrator 서버를 외부 vRealize Orchestrator 7.5로 마이그레이션](#)을 참조하십시오.
- 외부 vRealize Orchestrator 서버를 vRealize Automation에 내장된 vRealize Orchestrator 인스턴스로 마이그레이션합니다. vRealize Orchestrator 설명서에서 [외부 Orchestrator 서버를 vRealize Orchestrator 7.5로 마이그레이션](#)을 참조하십시오.

**참고** 내장된 vRealize Orchestrator 인스턴스를 외부 vRealize Orchestrator 환경으로 마이그레이션하는 기능은 지원되지 않습니다.

## Active Directory 연결에 사용자 또는 그룹 추가

기존 Active Directory 연결에 사용자 또는 그룹을 추가할 수 있습니다.

디렉토리 관리 사용자 인증 시스템은 그룹 및 사용자를 추가할 때 Active Directory에서 데이터를 가져옵니다. 데이터 전송 속도는 Active Directory 기능에 의해 제한됩니다. 따라서 추가되는 그룹 및 사용자 수에 따라 작업에 오랜 시간이 소요될 수 있습니다. 문제를 최소화하려면 그룹 및 사용자를 vRealize Automation 작업에 필요한 그룹 및 사용자로만 제한합니다. 문제가 발생하면 불필요한 애플리케이션을 닫고 배포에 Active Directory에 할당된 적절한 메모리가 있는지 확인합니다. 문제가 계속되면 Active Directory 메모리 할당을 늘립니다. 사용자 및 그룹 수가 많은 배포의 경우, Active Directory 메모리 할당을 24GB 정도까지 늘려야 할 수도 있습니다.

vRealize Automation 배포를 많은 사용자 및 그룹과 동기화할 때 SyncLog 세부 정보를 사용할 수 있게 되기까지 지연이 있을 수 있습니다. 로그 파일의 타임 스탬프는 콘솔에 표시된 완료된 시간과 다를 수 있습니다.

그룹 구성원이 [사용자] 목록에 없는 경우 Active Directory의 그룹을 추가하면 구성원이 목록에 추가됩니다. 그룹을 동기화할 때 Active Directory에서 [도메인 사용자]가 기본 그룹으로 포함되어 있지 않은 사용자는 동기화되지 않습니다.

**참고** 동기화 작업은 시작한 이후에 취소할 수 없습니다.

## 사전 요구 사항

- **Connector**를 설치하고 활성화 코드를 활성화합니다. [사용자 특성] 페이지에서 필요한 기본 특성을 선택하고 추가 특성을 추가합니다.
- **Active Directory**에서 동기화할 **Active Directory** 그룹 및 사용자의 목록.
- [LDAP를 통한 Active Directory]의 경우 필요한 정보에는 기본 DN, Bind DN, Bind DN 암호가 포함됩니다.
- [Active Directory(Windows 통합 인증)]의 경우 필요한 정보에는 도메인의 Bind 사용자 UPN 주소 및 암호가 포함됩니다.
- SSL을 통해 Active Directory에 액세스하는 경우에는 SSL 인증서의 사본이 필요합니다.
- Windows 인증과 통합된 다중 포리스트 Active Directory가 있으며 도메인 로컬 그룹에 다른 포리스트의 구성원이 포함되어 있는 경우 다음을 수행합니다. Bind 사용자를 도메인 로컬 그룹의 관리자 그룹에 추가합니다. Bind 사용자가 추가되지 않으면 이러한 구성원은 도메인 로컬 그룹에서 누락됩니다.
- **테넌트 관리자**로 vRealize Automation에 로그인합니다.

## 절차

- 1 **관리 > 디렉토리 관리 > 디렉토리**를 선택합니다.
- 2 원하는 디렉토리 이름을 클릭합니다.
- 3 **동기화 설정**을 클릭하여 동기화 옵션이 포함된 대화 상자를 엽니다.
- 4 사용자 또는 그룹 구성을 변경할지 여부에 따라 적합한 아이콘을 클릭합니다.

그룹 구성을 편집하려면:

- 그룹을 추가하려면 **+** 아이콘을 클릭하여 그룹 DN 정의에 대한 줄을 추가하고 적합한 그룹 DN을 입력합니다.
- 그룹 DN 정의를 삭제하려면 원하는 그룹 DN에 대한 **x** 아이콘을 클릭합니다.

사용자 구성을 편집하려면:

- ◆ 사용자를 추가하려면 **+** 아이콘을 클릭하여 사용자 DN 정의에 대한 줄을 추가하고 적합한 사용자 DN을 입력합니다.

사용자 DN 정의를 삭제하려면 원하는 사용자 DN에 대한 **x** 아이콘을 클릭합니다.

- 5 **저장**을 클릭하여 업데이트를 즉시 동기화하지 않고 변경 내용을 저장합니다. **저장 및 동기화**를 클릭하여 변경 내용을 저장하고 업데이트를 즉시 동기화합니다.

## 로드 밸런서 사용

배포가 로드 밸런서를 사용하는 경우 보조 노드 및 상태 점검을 다시 사용하도록 설정하고 로드 밸런서 시간 초과 설정을 되돌립니다.

vRealize Automation의 상태 점검은 버전에 따라 다릅니다. 자세한 내용은 [VMware vRealize Automation 설명서](#)에서 "vRealize Automation 로드 밸런싱 구성 가이드" 항목을 참조하십시오.

로드 밸런서 시간 초과 설정을 10분에서 다시 기본값으로 변경합니다.

## vRealize Automation 업그레이드를 위한 사후 업그레이드 작업

vRealize Automation 6.2.5에서 업그레이드한 후에는 필요한 모든 사후 업그레이드 작업을 수행합니다.

### 고가용성 배포를 위한 포트 구성

고가용성 배포에서 업그레이드를 완료한 후에는 포트 8444의 트래픽을 vRealize Automation 장치에 전달하도록 로드 밸런서를 구성하여 원격 콘솔 기능을 지원해야 합니다.

자세한 내용은 [vRealize Automation 설명서](#)에서 "vRealize Automation 로드 밸런싱 구성 가이드"를 참조하십시오.

### 소비자에 대해 Remote Console에 연결 작업 사용

vRealize Automation에서 vSphere가 프로비저닝한 장치에 대해 소비자에 대한 원격 콘솔 작업이 지원됩니다.

릴리스를 업그레이드한 후 Blueprint를 편집하고 **작업** 탭에서 **원격 콘솔에 연결**을 선택합니다.

자세한 내용은 [기술 자료 문서 2109706](#)을 참조하십시오.

### 외부 워크플로 시간 초과 파일 복원

업그레이드 프로세스에서 xmldb 파일을 덮어쓰기 때문에 vRealize Automation 외부 워크플로 시간 초과 파일을 재구성해야 합니다.

#### 절차

- 1 시스템의 다음 디렉토리에서 외부 워크플로 구성(xmldb) 파일을 엽니다.

`\VMware\VCAC\Server\ExternalWorkflows\xmldb\.`

- 2 xmldb 파일을 마이그레이션 전에 백업한 파일로 바꿉니다. 백업 파일이 없는 경우 외부 워크플로 시간 초과 설정을 재구성합니다.
- 3 설정을 저장합니다.

### 대상 vRealize Automation에서 포함된 vRealize Orchestrator 인프라 끝점 재구성

vRealize Automation 6.2.5 환경에서 마이그레이션하는 경우에는 내장형 대상 vRealize Orchestrator 서버를 가리키는 인프라 끝점의 URL을 업데이트해야 합니다.

#### 사전 요구 사항

- vRealize Automation의 대상 vRealize Automation 릴리스로 마이그레이션을 완료합니다.
- 대상 vRealize Automation 콘솔에 로그인합니다.
  - a 대상 가상 장치의 정규화된 도메인 이름(<https://vra-vd-hostname.domain.name/vcac>)을 사용하여 vRealize Automation 콘솔을 엽니다.

고가용성 환경인 경우, 대상 가상 장치 로드 밸런서의 정규화된 도메인 이름(<https://vra-vd-lb-hostname.domain.name/vcac>)을 사용하여 콘솔을 엽니다.

- b IaaS 관리자 사용자로 로그인합니다.

절차

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.
- 2 [끝점] 페이지에서 vRealize Orchestrator 끝점을 선택하고 **편집**을 클릭합니다.
- 3 [주소] 텍스트 상자에서 vRealize Orchestrator 끝점 URL을 편집합니다.
  - 최소 환경으로 마이그레이션한 경우, vRealize Orchestrator 끝점 URL을 `https://vra-va-hostname.domain.name:443/vco`으로 바꿉니다.
  - 고가용성 환경으로 마이그레이션한 경우, vRealize Orchestrator 끝점 URL을 `https://vra-va-lb-hostname.domain.name:443/vco`으로 바꿉니다.
- 4 **확인**을 클릭합니다.
- 5 vRealize Orchestrator 끝점에서 데이터 수집을 수동으로 실행합니다.
  - a [끝점] 페이지에서 vRealize Orchestrator 끝점을 선택합니다.
  - b **작업 > 데이터 수집**을 선택합니다.

데이터 수집이 완료되었는지 확인합니다.

승인 정책을 포함하는 업그레이드된 워크플로 스크립트 수정

vRealize Automation 승인 정책을 호출하는 vRealize Orchestrator 6.x에 워크플로 스크립트가 있는 경우, vRealize Automation 7.0 이상의 변경 사항을 수용하도록 스크립트를 수정해야 합니다.

승인 서비스를 호출하여 승인 클라이언트를 호출하는 대신 승인 클라이언트를 직접 호출해야 합니다.

절차

- 1 vRealize Orchestrator 6.x에서 다음 예제와 유사한 스크립트가 있는 경우.

```
var service = vcacHost.createApprovalClient().getApprovalApprovalInfoService();
System.log("got the service");
var approvalInfo = service.getApprovalInfo(approvalId);
var approvalPolicy = approvalInfo.getPolicy();
```

- 2 이 예제와 비슷한 스크립트로 대체합니다.

```
var approvalClient = vcacHost.createApprovalClient();

var vars = [
 approvalId
];

var approvalInfo = approvalClient.getWithVariables("/info/approvals/{0}", vars);
var approvalPolicy = new vCACCAFEApprovalDescriptiveReference() ;
approvalPolicy.setId(approvalInfo.getProperty("policy").getProperty("id"));
approvalPolicy.setName(approvalInfo.getProperty("policy").getProperty("name"));
approvalPolicy.setDescription(approvalInfo.getProperty("policy").getProperty("description"));
```



## app.config 파일에 로깅 변경 내용 복원

업그레이드 프로세스에서는 구성 파일에서 로깅과 관련하여 변경한 내용을 덮어씁니다. 업그레이드를 완료했으면 업그레이드하기 전에 변경한 내용을 **app.config** 파일에 복원해야 합니다.

사전 요구 사항 작업 중에 백업한 **laaS** 서버에 대해 병합을 수행하거나 \*.exe.config 파일(예: managerservice.exe.config)의 수정 사항을 덮어쓰지 않고 변경 내용을 복원할 수 있습니다.

## 업그레이드 후 자동 Manager Service 페일오버를 사용하도록 설정

vRealize Automation을 업그레이드하면 자동 Manager Service 페일오버는 기본적으로 사용하지 않도록 설정됩니다.

업그레이드 후 자동 Manager Service 페일오버를 사용하도록 설정하려면 다음 단계를 완료합니다.

### 절차

- 1 vRealize Automation 장치에서 루트로 명령 프롬프트를 엽니다.
- 2 디렉토리를 `/usr/lib/vcac/tools/vami/commands`로 변경합니다.
- 3 자동 Manager Service 페일오버를 사용하도록 설정하려면 다음 명령을 실행합니다.

```
python ./manager-service-automatic-failover ENABLE
```

laaS 배포 전체에서 자동 페일오버를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

```
python ./manager-service-automatic-failover DISABLE
```

## 자동 Manager Service 페일오버 정보

기본 Manager Service가 중지되면 백업으로 자동 페일오버되도록 vRealize Automation laaS Manager Service를 구성할 수 있습니다.

vRealize Automation 7.3부터 기본 또는 백업 역할을 할 호스트를 제어하기 위해 이제 더 이상 각 Windows Server에서 Manager Service를 수동으로 시작 또는 중지할 필요가 없습니다. 업그레이드 셀 스크립트 또는 laaS 설치 관리자 실행 파일을 사용하여 laaS를 업그레이드하는 경우에는 자동 Manager Service 페일오버가 기본적으로 사용하지 않도록 설정됩니다.

자동 페일오버를 사용하도록 설정하면 백업을 포함한 모든 Manager Service 호스트에서 Manager Service가 자동으로 시작됩니다. 자동 페일오버 기능을 사용하면 호스트가 서로를 투명하게 모니터링하고 필요한 경우 페일오버할 수 있지만 모든 호스트에서 Windows 서비스가 실행되고 있어야 합니다.

---

**참고** 자동 페일오버를 사용하지 않아도 됩니다. 자동 페일오버를 사용하지 않도록 설정하고 Windows 서비스를 계속 수동으로 시작하고 중지하여 기본 또는 백업 역할을 할 호스트를 제어할 수 있습니다. 수동 페일오버 방식을 사용하는 경우 한 번에 하나의 호스트에서만 서비스를 시작해야 합니다. 자동 페일오버가 사용되지 않도록 설정된 상태로 여러 laaS 서버에서 동시에 서비스를 실행하면 vRealize Automation을 사용할 수 없게 됩니다.

---

자동 페일오버를 선택적으로 사용 또는 사용하지 않도록 설정하지 마십시오. 자동 페일오버는 laaS 배포의 모든 Manager Service 호스트에서 설정되거나 해제된 상태로 항상 동기화되어야 합니다.

## 연결 테스트 실행 및 업그레이드된 끝점 확인

이전 vRealize Automation 릴리스에서 업그레이드하면 대상 환경에서 특정 끝점이 변경됩니다.

vRealize Automation으로 업그레이드한 후에는 적용 가능한 모든 끝점에 대해 **연결 테스트** 작업을 사용해야 합니다. 업그레이드된 일부 끝점을 수정해야 할 수도 있습니다. 자세한 내용은 [업그레이드 또는 마이그레이션된 끝점 사용 시 고려 사항](#)을 참조하십시오.

업그레이드 또는 마이그레이션된 끝점의 기본 보안 설정은 신뢰할 수 없는 인증서를 허용하지 않는 것입니다.

신뢰할 수 없는 인증서를 사용하고 있는 경우에는 이전 버전의 vRealize Automation 설치에서 업그레이드 또는 마이그레이션한 후 인증서 검증을 사용하도록 모든 vSphere 및 NSX 끝점에 대해 다음 단계를 수행해야 합니다. 그렇지 않으면 인증서 오류가 발생하고 끝점 작업이 실패합니다. 자세한 내용은 <http://kb.vmware.com/kb/2150230>의 VMware 기술 자료 문서 "vRA 7.3으로 업그레이드 후 끝점 통신이 끊김 (2150230)" 및 <http://kb.vmware.com/kb/2108294>의 "웹 브라우저 인증서 주의를 방지하도록 vCenter Server 루트 인증서를 다운로드 및 설치하는 방법(2108294)"을 참조하십시오.

- 1 업그레이드 또는 마이그레이션 후에 vRealize AutomationvSphere 에이전트 시스템에 로그인하고 **서비스** 탭을 사용하여 vSphere 에이전트를 다시 시작합니다.  
마이그레이션이 모든 에이전트를 다시 시작하지 못할 수 있으므로 필요한 경우 에이전트를 수동으로 다시 시작합니다.
- 2 적어도 하나 이상의 ping 보고가 완료될 때까지 기다립니다. ping 보고가 완료되려면 1~2분 정도가 소요됩니다.
- 3 vSphere 에이전트가 데이터 수집을 시작하면 vRealize Automation에 IaaS 관리자로 로그인합니다.
- 4 **인프라 > 끝점 > 끝점**을 클릭합니다.
- 5 vSphere 끝점을 편집하고 **연결 테스트**를 클릭합니다.
- 6 인증서 프롬프트가 표시되면 **확인**을 클릭하여 인증서를 수락합니다.  
인증서 프롬프트가 표시되지 않으면 현재 끝점에 대한 Windows 시스템 호스팅 서비스의 신뢰할 수 있는 루트 인증 기관(예: 프록시 에이전트 시스템 또는 DEM 시스템)에 인증서가 올바르게 저장되어 있을 수 있습니다.
- 7 **확인**을 클릭하여 인증서 수락을 적용하고 끝점을 저장합니다.
- 8 각 vSphere 끝점에 대해 이 절차를 반복합니다.
- 9 각 NSX 끝점에 대해 이 절차를 반복합니다.
- 10 **인프라 > 계산 리소스**로 이동하여 **vCenter 계산** 리소스를 마우스 오른쪽 버튼으로 클릭하고 **데이터 수집**을 실행합니다.

**연결 테스트** 작업이 성공해도 일부 데이터 수집 또는 프로비저닝 작업이 실패하면 끝점 역할을 하는 모든 에이전트 시스템과 모든 DEM 시스템에 동일한 인증서를 설치할 수 있습니다. 또는 기존 시스템에서 인증서를 제거하고 실패한 끝점에 대해 이전 절차를 반복할 수 있습니다.

## DynamicTypes 가져오기

DynamicTypes 플러그인을 사용하고 업그레이드 전에 구성을 패키지로 내보낸 경우 다음 워크플로를 가져와야 합니다.

- 1 대상 환경에서 동적 유형 구성을 가져옵니다.
  - a Java Client에 관리자 로 로그인합니다.
  - b **워크플로** 탭을 선택합니다.
  - c **라이브러리 > 동적 유형 > 구성**을 선택합니다.
  - d **패키지에서 구성 가져오기** 워크플로를 선택하고 실행합니다.
  - e **가져올 구성 패키지**를 클릭합니다.
  - f 내보낸 패키지 파일을 찾아 **파일 첨부**를 클릭합니다.
  - g 패키지에 연결된 네임스페이스에 대한 정보를 검토하고 **제출**을 클릭합니다.
- 2 **인벤토리 > 동적 유형**을 선택하여 동적 유형 네임스페이스를 가져왔는지 확인합니다.

## vRealize Automation 업그레이드 문제 해결

업그레이드 문제 해결 항목에서는 vRealize Automation 6.2.5에서 업그레이드할 때 발생할 수 있는 문제에 대한 해결 방법을 제공합니다.

### 로드 밸런서 시간 초과 오류와 함께 설치 또는 업그레이드가 실패함

로드 밸런서가 있는 분산 배포의 vRealize Automation 설치 또는 업그레이드가 503 서비스 사용 불가 오류를 표시하며 실패합니다.

#### 문제

로드 밸런서 시간 초과 설정에서 작업을 완료할 시간이 충분히 허용되지 않아서 설치 또는 업그레이드가 실패합니다.

#### 원인

로드 밸런서 시간 초과 설정이 충분하지 않아서 실패가 발생할 수 있습니다. 로드 밸런서 시간 초과 설정을 100초 이상으로 늘리고 작업을 다시 실행하여 문제를 수정할 수 있습니다.

#### 해결책

- 1 로드 밸런서 시간 초과 값을 100초 이상으로 늘리십시오.
- 2 설치 또는 업그레이드를 다시 실행하십시오.

### IaaS 웹 사이트 구성 요소에 대한 업그레이드 실패

IaaS 업그레이드가 실패하고 업그레이드를 계속할 수 없습니다.

## 문제

웹 사이트 구성 요소에 대해 IaaS 업그레이드가 실패합니다. 다음 오류 메시지가 설치 관리자 로그 파일에 표시됩니다.

- System.Data.Services.Client.DataServiceQueryException:  
An error occurred while processing this request. --->  
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- <b> Description: </b>An application error  
occurred on the server. The current custom error settings for this application  
prevent the details of the application error from being viewed remotely (for  
security reasons). It could, however, be viewed by browsers running on the  
local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files  
(x86)\VMware\VCAC\Server\Model Manager Data\DeployRepository.xml"  
(InstallRepoModel target(s)) -- FAILED.

다음 오류 메시지가 저장소 로그 파일에 표시됩니다.

- [Error]: [sub-thread-Id="20"  
context="" token=""] Failed to start repository service. Reason:  
System.InvalidOperationException: Configuration section encryptionKey is not  
protected  
at  
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration  
config)  
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)  
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2  
decryptFunc)  
at  
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object  
sender, ObjectMaterializedEventArgs e)  
at  
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()

```

at
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
at
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(CoreModelEntities
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().

```

#### 원인

IaaS 업그레이드는 **web.config** 파일의 생성 날짜가 수정된 날짜와 같거나 이후인 경우에 실패합니다.

#### 해결책

- 1 IaaS 호스트에서 Windows에 로그인합니다.
- 2 Windows 명령 프롬프트를 엽니다.
- 3 vRealize Automation 설치 폴더로 디렉토리를 변경합니다.
- 4 **관리자 권한으로 실행** 옵션으로 기본 텍스트 편집기를 시작합니다.
- 5 **web.config** 파일을 찾아 선택하고 파일을 저장하여 해당 파일 수정 날짜를 변경합니다.
- 6 **web.config** 파일 속성을 검사하여 파일 수정 날짜가 생성 날짜 이후인지 확인합니다.
- 7 IaaS를 업그레이드합니다.

**Manager Service가 런타임 중에 SSL 검증 오류로 인해 실행되지 못함**

Manager Service가 SSL 검증 오류로 인해 실행되지 못합니다.

#### 문제

Manager Service가 로그의 다음 오류 메시지와 함께 실패합니다.

[Info]: Thread-Id="6" - context="" token="" 핵심 데이터베이스에 연결하지 못함, 00:00:05  
 이내에 재시도함, 오류 세부 정보: 서버에 연결했지만 로그인하는 동안 오류가 발생했습니다. (제  
 공자: SSL 제공자, 오류: 0 - 인증서 체인이 신뢰할 수 없는 기관으로부터 발급되었습니다.)

## 원인

런타임 중에 Manager Service가 SSL 검증 오류로 인해 실행되지 못합니다.

## 해결책

- 1 ManagerService.config 구성 파일을 엽니다.
- 2 다음 줄에서 **Encrypt=False**를 업데이트합니다.

```
<add name="vcac-repository" providerName="System.Data.SqlClient" connectionString="Data
Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated Security=True;Pooling=True;Max
Pool Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

## 업그레이드 후 로그인 실패

동기화되지 않은 사용자 계정을 사용하는 세션에 대한 업그레이드 후에는 브라우저를 종료하고 다시 로그인해야 합니다.

## 문제

vRealize Automation을 업그레이드한 후 로그인할 때 시스템에서 동기화되지 않은 사용자 계정에 대한 액세스를 거부합니다.

## 해결책

브라우저를 종료하고 vRealize Automation을 다시 시작합니다.

## 업그레이드 후 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없음

최신 버전의 vRealize Automation으로 업그레이드한 후 이전 버전의 특정 속성 정의를 사용하는 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없습니다.

## 문제

6.2.x 이전 버전에서 업그레이드했고 다음 제어 유형 또는 특성이 포함된 속성 정의가 있는 경우, 해당 특성이 속성 정의에서 누락되고 해당 정의를 사용하는 모든 카탈로그 항목이 업그레이드하기 전의 방식으로 작동하지 않습니다.

- 제어 유형. 확인란 또는 링크.
- 특성. 관계, 정규식 또는 속성 레이아웃.

## 원인

vRealize Automation 7.0 이상에서는 속성 정의에서 더 이상 해당 특성을 사용하지 않습니다. 속성 정의에서 포함된 제어 유형 또는 특성을 사용하지 않고 대신 vRealize Orchestrator 스크립트 작업을 사용하여 속성 정의를 구성하거나 속성 정의를 다시 생성해야 합니다.

스크립트 작업을 사용하여 제어 유형 또는 특성을 vRealize Automation 7.x로 마이그레이션합니다.

## 해결책

- 1 vRealize Orchestrator에서 속성 값을 반환하는 스크립트 작업을 생성합니다. 작업은 단순 유형을 반환해야 합니다. 예를 들어 문자열, 정수 또는 지원되는 다른 유형을 반환합니다. 작업은 해당 작업이 종속된 다른 속성을 입력 매개 변수로 사용할 수 있습니다.
- 2 vRealize Automation 콘솔에서 제품 정의를 구성합니다.
  - a **관리 > 속성 사전 > 속성 정의**를 선택합니다.
  - b 속성 정의를 선택하고 **편집**을 클릭합니다.
  - c [권장 사항 표시] 드롭다운 메뉴에서 **드롭다운**을 선택합니다.
  - d [값] 드롭다운 메뉴에서 **외부 값**을 선택합니다.
  - e 스크립트 작업을 선택합니다.
  - f **확인**을 클릭합니다.
  - g 스크립트 작업에 포함된 입력 매개 변수를 구성합니다. 기존 관계를 유지하려면 매개 변수를 다른 속성에 바인딩합니다.
  - h **확인**을 클릭합니다.

## 외부 PostgreSQL 데이터베이스 병합 실패

외부 PostgreSQL 데이터베이스와 포함된 PostgreSQL 데이터베이스 병합이 실패합니다.

## 문제

외부 PostgreSQL 데이터베이스 버전이 포함된 PostgreSQL 데이터베이스 버전보다 최신이면 병합이 실패합니다.

## 해결책

- 1 외부 PostgreSQL 데이터베이스의 호스트에 로그인합니다.
- 2 `psql --version` 명령을 실행합니다.  
외부 데이터베이스의 PostgreSQL 버전을 기록해 둡니다.
- 3 포함된 PostgreSQL 데이터베이스의 호스트에 로그인합니다.
- 4 `psql --version` 명령을 실행합니다.  
포함된 데이터베이스의 PostgreSQL 버전을 기록해 둡니다.

## 해결책

외부 PostgreSQL 버전이 포함된 PostgreSQL 버전보다 최신인 경우 외부 PostgreSQL 데이터베이스를 병합하려면 지원 부서에 도움을 요청하십시오.

고가용성 환경을 업그레이드한 후 클러스터에 가입 명령이 실패함

보조 클러스터 노드의 vRealize Automation 장치 관리 인터페이스에서 **클러스터에 가입**을 클릭했을 때 진행률 표시기가 사라집니다.

#### 문제

업그레이드 후 vRealize Automation 장치 관리 인터페이스를 사용하여 기본 노드에 보조 클러스터 노드를 가입시키면 진행률 표시기가 사라지고 오류 또는 성공 메시지가 표시되지 않습니다. 이 동작은 간헐적으로 발생하는 문제입니다.

#### 원인

진행률 표시기가 사라지는 이유는 일부 브라우저가 서버의 응답 대기를 중지하기 때문입니다. 이 동작으로 클러스터에 가입 프로세스가 중지되지는 않습니다. `/var/log/vmware/vcac/vcac-config.log`에서 로그 파일을 확인하여 클러스터에 가입 프로세스가 성공했는지 확인할 수 있습니다.

루트 파티션에 사용 가능한 공간이 충분하지 않으면 업그레이드가 실패함

vRealize Automation 장치 호스트의 루트 파티션에 사용 가능한 공간이 충분하지 않으면 업그레이드를 계속할 수 없습니다.

이 절차는 vRealize Automation 장치 호스트의 디스크 1 루트 파티션에서 사용 가능한 공간을 늘립니다. 분산 배포에서 이 절차를 수행하여 각 복제 노드에서 사용 가능한 공간을 순차적으로 늘린 다음 master 노드에서 사용 가능한 공간을 늘립니다.

**참고** 이 절차를 수행할 때 다음과 같은 경고 메시지가 표시될 수 있습니다.

- **WARNING: Re-reading the partition table failed with error 16:**  
Device or resource busy. The kernel still uses the old table. The new table will be used at the next reboot or after you run `partprobe(8)` or `kpartx(8)` Syncing disks.
- **Error: Partition(s) 1 on /dev/sda have been written, but we have been unable to inform the kernel of the change, probably because it/they are in use. As a result, the old partition(s) will remain in use. You should reboot now before making further changes.**

추가 변경하기 전에 지금 재부팅해야 합니다. 라는 메시지를 무시하십시오. 10단계 이전에 시스템을 재부팅하면 업그레이드 프로세스에 문제가 발생합니다.

#### 해결책

- 1 vRealize Automation 장치 호스트 가상 시스템의 전원을 켜고 보안 셸 연결을 사용하여 루트 사용자로 로그인합니다.
- 2 다음 명령을 실행하여 서비스를 중지합니다.
  - a `service vcac-server stop`
  - b `service vco-server stop`
  - c `service vpostgres stop`



- 3 다음 명령을 실행하여 스왑 파티션을 마운트 해제합니다.

```
swapoff -a
```

- 4 다음 명령을 실행하여 기존의 디스크 1 파티션을 삭제하고 44GB의 루트 파티션과 6GB의 스왑 파티션을 생성합니다.

```
(echo d; echo 2; echo d; echo 1; echo n; echo p; echo ; echo ; echo '+44G'; echo n; echo p; echo ; echo ; echo ; echo w; echo p; echo q) | fdisk /dev/sda
```

- 5 다음 명령을 실행하여 스왑 파티션 유형을 변경합니다.

```
(echo t; echo 2; echo 82; echo w; echo p; echo q) | fdisk /dev/sda
```

- 6 다음 명령을 실행하여 디스크 1에 부팅 가능 플래그를 설정합니다.

```
(echo a; echo 1; echo w; echo p; echo q) | fdisk /dev/sda
```

- 7 다음 명령을 실행하여 파티션 변경 내용을 Linux 커널에 등록합니다.

```
partprobe
```

추가 변경하기 전에 재부팅하라는 메시지가 표시되면 메시지를 무시합니다. 10단계 이전에 시스템을 재부팅하면 업그레이드 프로세스에 문제가 발생합니다.

- 8 다음 명령을 실행하여 새 스왑 파티션을 포맷합니다.

```
mkswap /dev/sda2
```

- 9 다음 명령을 실행하여 스왑 파티션을 마운트합니다.

```
swapon -a
```

- 10 vRealize Automation 장치를 재부팅합니다.

- 11 장치를 재부팅한 후 다음 명령을 실행하여 디스크 1 파티션 테이블의 크기를 조정합니다.

```
resize2fs /dev/sda1
```

- 12 디스크 확장에 성공했는지 확인하려면 **df -h**를 실행하고 **/dev/sda1**의 사용 가능한 디스크 공간이 30GB보다 큰지 확인합니다.

### .xml 파일 백업 복사본으로 인한 시스템 시간 초과

vRealize Automation은 확장명이 .xml인 모든 파일을 \VMware\vCAC\Server\ExternalWorkflows\xmlldb\ 디렉토리에 등록합니다. 이 디렉토리에 확장명이 .xml인 백업 파일이 포함되어 있으면 시스템 시간 초과를 유발하는 중복 워크플로가 실행됩니다.

해결 방법: 이 디렉토리에 파일을 백업하는 경우에는 해당 백업을 다른 디렉토리로 이동하거나 백업 파일의 확장명을 .xml이 아닌 값으로 변경하십시오.

### vRealize Automation에서 분리된 노드 삭제

분리된 노드는 호스트에서 보고되었지만 호스트에 없는 중복된 노드입니다.

## 문제

각각의 IaaS 및 가상 장치 노드가 정상 상태인지 확인할 때 호스트에 하나 이상의 분리된 노드가 있는 것을 발견할 수도 있습니다. 분리된 노드는 모두 삭제해야 합니다.

## 해결책

- 1 기본 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

`https://vrealize-automation-appliance-FQDN:5480`

- 2 클러스터를 선택합니다.

- 3 테이블에 표시된 각 분리된 노드에 대해 **삭제**를 클릭합니다.

vRealize Automation에서 새 디렉토리를 생성할 수 없음

첫 번째 동기화 커넥터가 있는 새 디렉토리를 추가하려는 시도가 실패합니다.

## 문제

이 문제는 `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`에 있는 잘못된 `config-state.json` 파일로 인해 발생합니다.

이 문제를 해결하는 방법에 대한 자세한 내용은 [기술 자료 문서 2145438](#)을 참조하십시오.

업그레이드 시 일부 가상 시스템의 배포가 생성되지 않음

업그레이드할 때 누락된 상태의 가상 시스템에 대해서는 해당하는 배포가 대상 환경에 생성되지 않습니다.

## 문제

업그레이드 시 소스 환경에서 가상 시스템이 누락된 상태인 경우, 해당하는 배포가 대상 환경에 생성되지 않습니다. 업그레이드 이후에 가상 시스템이 더 이상 누락된 상태가 아니면 대량 가져오기를 사용하여 시스템을 대상 배포로 가져올 수 있습니다.

인증서를 신뢰할 수 없음 오류

vRealize Automation 장치 콘솔에서 인프라 [로그 뷰어] 페이지를 확인할 때, **Certificate is not trusted** 메시지가 포함된 끝점 연결 장애 보고서가 표시될 수 있습니다.

## 문제

vRealize Automation 장치 콘솔에서 **인프라 > 모니터링 > 로그**를 선택합니다. [로그 뷰어] 페이지에 다음과 유사한 보고서가 표시될 수 있습니다.

끝점에 연결하지 못했습니다. 이 끝점에 대해 보안 연결을 설정할 수 있는지 검증하려면 [끝점] 페이지에서 vSphere 끝점으로 이동한 후 [연결 테스트]를 클릭합니다.

내부 예외: 인증서를 신뢰할 수 없습니다(RemoteCertificateChainErrors). 주체: C=US, CN=vc6.mycompany.com 지문: DC5A8816231698F4C9013C42692B0AF93D7E35F1

## 원인

vRealize Automation의 이전 릴리스에서 업그레이드하면 원래 환경의 끝점이 변경됩니다. vRealize Automation 업그레이드 후 IaaS 관리자는 보안 **https** 연결을 사용하는 업그레이드된 각 끝점을 검토해야 합니다. 끝점에 **Certificate is not trusted** 오류가 있으면 해당 끝점이 제대로 작동하지 않습니다.

## 해결책

- 1 인프라 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 2 **인프라 > 끝점 > 끝점**을 선택합니다.
- 3 보안 연결을 사용하는 각 끝점에 대해 다음 단계를 완료합니다.
  - a **편집**을 클릭합니다.
  - b **연결 테스트**를 클릭합니다.
  - c 인증서 세부 정보를 검토한 후, 인증서를 신뢰할 수 있으면 **확인**을 클릭합니다.
  - d 이 끝점에 사용되는 모든 IaaS 프록시 에이전트에 대한 Windows 서비스를 다시 시작합니다.
- 4 인프라 [로그 뷰어] 페이지에 **Certificate is not trusted** 오류가 더 이상 표시되지 않는지 확인합니다.

사전 요구 사항 수정을 적용하는 동안 vRealize Automation 설치 또는 업그레이드 실패  
vRealize Automation 설치 또는 업그레이드가 실패하고 로그 파일에 오류 메시지가 나타납니다.

## 문제

vRealize Automation 설치 또는 업그레이드 시 해당 절차가 실패합니다. 일반적으로 이 문제는 설치 또는 업그레이드 중에 수정이 제대로 적용되지 않은 경우에 발생합니다. 로그 파일에 **Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped**와 유사한 오류 메시지가 나타납니다.

## 원인

Windows 환경에 [사용]으로 설정된 PowerShell 스크립트 실행에 대한 그룹 정책이 있습니다.

## 해결책

- 1 Windows 호스트 시스템에서 **gpedit.msc**를 실행하여 로컬 그룹 정책 편집기를 엽니다.
- 2 왼쪽 창의 **컴퓨터 구성** 아래에서 확장 버튼을 클릭하여 **관리 템플릿 > Windows 구성 요소 > Windows PowerShell**을 엽니다.
- 3 **스크립트 실행 설정**의 경우 상태를 **Enabled**에서 **Not Configured**로 변경합니다.

## 업데이트를 통한 관리 에이전트 업그레이드 실패

vRealize Automation 장치 관리 인터페이스 [업데이트 상태] 페이지에서 **업데이트 설치**를 클릭하면 관리 에이전트에 대한 오류 메시지가 표시됩니다.

## 문제

업그레이드 프로세스가 실패했습니다. 다음 메시지가 나타납니다. 노드 **x**에서 관리 에이전트를 업그레이드할 수 없습니다. 메시지가 두 개 이상의 노드를 나열하는 경우가 종종 있습니다.

## 원인

이 문제는 여러 가지 상황에 의해 발생할 수 있습니다. 오류 메시지는 영향을 받은 시스템의 노드 ID만 식별합니다. 자세한 정보는 명령이 실패한 시스템의 관리 에이전트에 대한 **All.log** 파일에서 찾을 수 있습니다.

상황에 따라 영향을 받는 노드에 대해 다음 작업을 수행하십시오.

## 해결책

- ◆ 관리 에이전트 서비스가 실행 중이 아닌 경우 서비스를 시작하고 가상 장치에서 업그레이드를 다시 시작합니다.
- ◆ 관리 에이전트 서비스가 실행 중이고 관리 에이전트가 업그레이드된 경우 가상 장치에서 업그레이드를 다시 시작합니다.
- ◆ 관리 에이전트 서비스가 실행 중이지만 관리 에이전트가 업그레이드되지 않은 경우 수동 업그레이드를 수행합니다.
  - a 브라우저에서 [IaaS 설치] 페이지로 이동합니다.  
<https://vrealize-automation-appliance-FQDN:5480/installer>
  - b 관리 에이전트 설치 관리자를 다운로드하고 실행합니다.
  - c 관리 에이전트 시스템을 재부팅합니다.
  - d 가상 장치에서 업그레이드를 다시 시작합니다.

## 관리 에이전트 업그레이드 실패

vRealize Automation 업그레이드 중에 관리 에이전트 업그레이드가 실패합니다.

## 문제

페일오버 문제로 인해 기본 및 보조 관리 에이전트 호스트가 전환된 경우 자동화된 업그레이드 프로세스가 필요한 호스트를 찾지 못해 업그레이드가 실패합니다. 관리 에이전트가 업그레이드되지 않은 각 IaaS 노드에서 이 절차를 수행합니다.

## 해결책

- 1 관리 에이전트 로그 폴더(C:\Program Files (x86)\VMware\VCAC\Management Agent\Logs\))에서 All.log를 엽니다.

설치 폴더의 위치가 기본 위치와 다를 수 있습니다.

- 2 로그 파일에서 오래되거나 전원이 꺼진 가상 장치에 관한 메시지를 검색합니다.

예: INNER EXCEPTION: System.Net.WebException: 원격 서버에 연결할 수 없습니다. ---> System.Net.Sockets.SocketException: 연결된 대상이 일정 시간 이후에 제대로 응답하지 않아 연결 시도가 실패했거나 연결된 호스트가 응답하지 않아 설정된 연결이 실패했습니다.  
IP\_Address: 5480

- 3 C:\Program Files (x86)\VMware\VCAC\Management Agent \VMware.IaaS.Management.Agent.exe.config에 있는 관리 에이전트 구성 파일을 편집하여 기존 alternativeEndpointaddress 값을 기본 가상 장치 끝점의 URL로 바꿉니다.

설치 폴더의 위치가 기본 위치와 다를 수 있습니다.

VMware.IaaS.Management.Agent.exe.config에 있는 alternativeEndpointaddress의 예.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="thumbprint number" />
```

- 4 관리 에이전트 Windows 서비스를 다시 시작하고 All.log 파일을 검토하여 작동 중인지 확인합니다.  
5 기본 vRealize Automation 장치에서 업그레이드 절차를 실행합니다.

기본 시간 초과 설정 때문에 vRealize Automation 업데이트가 실패함

사용자 환경에서 데이터베이스 동기화를 위한 기본 설정이 너무 짧은 경우 업데이트를 위한 시간 설정을 늘릴 수 있습니다.

문제

데이터베이스 동기화가 3600초의 기본값보다 오래 걸리는 일부 환경에서는 Vcac-Config SynchronizeDatabases 명령에 대한 시간 초과 설정이 충분하지 않습니다.

Vcac-Config.exe.config 파일의 cafeTimeoutInSeconds 및 cafeRequestPageSize 속성 값은 API와 Vcac-config.exe 유틸리티 도구 간의 통신을 제어합니다. 해당 파일은 IaaS 설치 위치\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config에 있습니다.

다음 선택적 매개 변수에 대해 값을 제공하여 SynchronizeDatabases 명령에 대해서만 기본 시간 초과 값을 재정의할 수 있습니다.

매개 변수	짧은 이름	설명
--DatabaseSyncTimeout	-dstm	초 단위로 SynchronizeDatabases 전용 http 요청 시간 초과 값을 설정합니다.
--DatabaseSyncPageSize	-dsps	예약 또는 예약 정책 동기화 전용 동기화 요청 페이지 크기를 설정합니다. 기본값은 10입니다.

이러한 매개 변수가 Vcac-Config.exe.config 파일에 설정되지 않은 경우 시스템은 기본 시간 초과 값을 사용합니다.

## 고가용성 환경에서 IaaS 업그레이드 실패

로드 밸런싱을 사용하도록 설정하고 기본 웹 서버 노드에서 IaaS 업그레이드 프로세스를 실행하면 실패합니다. 다음과 같은 오류 메시지가 표시될 수 있습니다. "System.Net.WebException: 작업이 시간 초과됨" 또는 "401 - 승인되지 않음: 잘못된 자격 증명으로 인해 액세스가 거부되었습니다."

### 문제

로드 밸런싱을 사용하도록 설정한 상태에서 IaaS를 업그레이드하면 간헐적으로 장애가 발생할 수 있습니다. 이러한 문제가 발생하면 로드 밸런싱을 사용하지 않도록 설정하고 vRealize Automation 업그레이드를 다시 실행해야 합니다.

### 해결책

- 1 환경을 업데이트 전 스냅샷으로 되돌립니다.
- 2 기본 IaaS 웹 서버 노드에 대한 원격 데스크톱 연결을 엽니다.
- 3 Windows hosts 파일이 있는 위치(c:\windows\system32\drivers\etc)로 이동합니다.
- 4 hosts 파일을 열고 웹 서버 로드 밸런서를 생략하도록 이 줄을 추가합니다.  
*IP\_address\_of\_primary\_iaas\_website\_node vrealizeautomation\_iaas\_website\_lb\_fqdn*  
예:  
10.10.10.5 vra-iaas-web-lb.domain.com
- 5 hosts 파일을 저장하고 vRealize Automation 업데이트를 다시 시도합니다.
- 6 vRealize Automation 업데이트가 완료되면 hosts 파일을 열고 4단계에서 추가한 줄을 제거합니다.

### 업그레이드 후 지연된 스토리지

예약 탭에 스토리지가 표시되지 않습니다.

업그레이드 후 [예약] 탭에 스토리지가 표시되지 않으면 모든 노드에서 vcac-server를 다시 시작해야 합니다. [예약] 탭의 [리소스] 섹션에 스토리지가 표시되려면 최대 1시간이 걸릴 수 있습니다.

### 업그레이드 문제 해결

업그레이드 문제를 해결하기 위해 업그레이드 프로세스를 수정할 수 있습니다.

vRealize Automation 환경 업그레이드에 문제가 발생하는 경우 이 절차를 사용하여 사용 가능한 플러그 중 하나를 선택하여 업그레이드 프로세스를 수정할 수 있습니다.

### 해결책

- 1 기본 vRealize Automation 장치 노드에 대한 보안 셸 연결을 엽니다.
- 2 명령 프롬프트에서 다음 명령을 실행하여 전환 파일을 생성합니다.

**touch available\_flag**

예: **touch /tmp/disable-iaas-upgrade**

표 1-70. 사용 가능한 플래그

플래그	설명
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> <li>가상 장치가 다시 시작된 후 IaaS 업그레이드 프로세스를 차단합니다.</li> <li>관리 에이전트 업그레이드를 차단합니다.</li> <li>자동 사전 요구 사항 확인 및 수정을 차단합니다.</li> <li>IaaS 서비스 중지를 차단합니다.</li> </ul>
/tmp/do-not-upgrade-ma	관리 에이전트 업그레이드를 차단합니다. 이 플래그는 관리 에이전트가 수동으로 업그레이드되는 경우에 적합합니다.
/tmp/skip-prereq-checks	자동 사전 요구 사항 확인 및 수정을 차단합니다. 이 플래그는 자동 사전 요구 사항 수정에 문제가 있으며 수정이 대신 수동으로 적용된 경우에 적합합니다.
/tmp/do-not-stop-services	IaaS 서비스 중지를 차단합니다. 업그레이드가 Manager Service, DEM 및 에이전트와 같은 IaaS Windows 서비스를 중지하지 않습니다.
/tmp/do-not-upgrade-servers	데이터베이스, 웹 사이트, WAPI, 리포지토리, Model Mfrontanager 데이터 및 Manager Service와 같은 모든 서버 IaaS 구성 요소의 자동 업그레이드를 차단합니다.  <b>참고</b> 이 플래그는 Manager Service 자동 패일오버 모드 사용도 차단합니다.
/tmp/do-not-upgrade-dems	DEM 업그레이드를 차단합니다.
/tmp/do-not-upgrade-agents	IaaS 프록시 에이전트 업그레이드를 차단합니다.

### 3 선택한 플래그에 대한 작업을 완료합니다.

표 1-71. 추가 작업

플래그	작업
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> <li>수동으로 관리 에이전트를 업그레이드합니다.</li> <li>수동으로 필수 IaaS 사전 요구 사항을 적용합니다.</li> <li>IaaS 서비스를 수동으로 중지합니다. <ul style="list-style-type: none"> <li>a IaaS Windows Server에 로그인합니다.</li> <li>b 시작 &gt; 관리 도구 &gt; 서비스를 선택합니다.</li> <li>c 다음과 같은 순서로 이러한 서비스를 중지합니다. <ul style="list-style-type: none"> <li><b>참고</b> IaaS Windows Server를 종료하지 않습니다.</li> </ul> </li> </ul> </li> </ul>
/tmp/do-not-upgrade-ma	<ul style="list-style-type: none"> <li>a 각 VMwarevRealize Automation 프록시 에이전트.</li> <li>b 각 VMware DEM 작업자.</li> <li>c VMware DEM 조정자.</li> <li>d VMware vCloud Automation Center 서비스.</li> </ul> <ul style="list-style-type: none"> <li>가상 장치 업그레이드가 완료된 후 수동으로 IaaS 업그레이드를 시작합니다.</li> </ul>
/tmp/do-not-upgrade-ma	수동으로 관리 에이전트를 업그레이드합니다.

표 1-71. 추가 작업 (계속)

플래그	작업
/tmp/skip-prereq-checks	수동으로 필수 IaaS 사전 요구 사항을 적용합니다.
/tmp/do-not-stop-services	IaaS 서비스를 수동으로 중지합니다. 1 IaaS Windows Server에 로그인합니다. 2 시작 > 관리 도구 > 서비스를 선택합니다. 3 다음과 같은 순서로 이러한 서비스를 중지합니다.  <b>참고</b> IaaS Windows Server를 종료하지 않습니다. a 각 VMwarevRealize Automation 프록시 에이전트. b 각 VMware DEM 작업자. c VMware DEM 조정자. d VMware vCloud Automation Center 서비스.
/tmp/do-not-upgrade-servers	
/tmp/do-not-upgrade-dems	
/tmp/do-not-upgrade-agents	

- 4 기본 vRealize Automation 장치 관리 콘솔에 액세스하고 기본 vRealize Automation 장치를 업데이트합니다.

**참고** 각 플래그는 제거될 때까지 활성 상태로 유지되기 때문에 업그레이드 후에  
**rm /flag\_path/flag\_name** 명령을 실행하여 선택한 플래그를 제거합니다. 예:  
**rm /tmp/disable-iaas-upgrade.**

#### IaaS 사전 요구 사항 검사 중 가상 장치 업그레이드가 실패함

IaaS 사전 요구 사항 검사를 통해 사용자 지정 IIS 웹 사이트 이름으로 구성된 환경의 유효성을 검사할 수 없습니다. 자동화된 IaaS 업그레이드를 사용하지 않도록 설정하면 문제가 해결됩니다.

#### 문제

설치 전 스크립트 및 설치 후 스크립트를 실행하면서 IaaS 사전 요구 사항을 검사하는 동안 가상 장치 업그레이드가 실패합니다.

Error: Unrecognized configuration path MACHINE/WEBROOT/APPHOST/Default Web Site can not find path IIS:\Sites\Default Web Site because it does not exist.

오류가 발생하면 다음과 유사한 오류 메시지가 표시됩니다. Applying automatic fix for <사전 요구 사항 검사 이름> prerequisite failed.

#### 원인

IaaS 사전 요구 사항 검사를 통해 사용자 지정 IIS 웹 사이트 이름으로 구성된 환경의 유효성을 검사할 수 없습니다. 자동화된 IaaS 업그레이드 사전 요구 사항 검사를 사용하지 않도록 설정하면 문제가 해결됩니다.



## 해결책

- 1 자동화된 IaaS 업그레이드 사전 요구 사항 검사 및 수정을 사용하지 않도록 설정합니다.
- 2 vRealize Automation 업그레이드를 실행합니다. [업그레이드 문제 해결](#)을 참조하십시오.
- 3 업그레이드 프롬프트를 따릅니다. vRealize Automation을 재부팅하라고 프롬프트에 표시되면 IaaS 설치 관리자를 사용하여 충족되지 않은 IaaS 사전 요구 사항을 검색하고 수동으로 수정할 수 있습니다.

---

**참고** IaaS 사전 요구 사항 유효성 검사를 완료할 때까지 장치를 다시 시작하지 마십시오.

---

- 4 모든 IaaS 웹 사이트 노드에 대해 다음 단계를 사용합니다.
  - a IaaS 설치 관리자를 다운로드합니다. [vRealize Automation 장치를 업그레이드한 후 IaaS 구성 요소 업그레이드를 위해 IaaS 설치 관리자 다운로드](#)를 참조하십시오.
  - b IaaS 설치 관리자를 처음 초기화하면 확장명이 `.exe.config`인 새 구성 파일이 동일한 디렉토리에 생성됩니다.
  - c IaaS 설치 관리자를 닫고 구성 파일의 `<appSettings>` 섹션에 다음 키를 추가합니다. 이 키는 사용자 지정 웹 사이트 이름을 IaaS 사전 요구 사항 검사기로 전달합니다.
 

```
<add key="PreReqChecker.Default.DefaultWebSite" value="custom_web_site_name"/>
```
  - d 구성 파일을 저장하고 IaaS 설치 관리자를 다시 실행합니다. 사전 요구 사항 유효성 검사가 완료될 때까지 화면에 나타나는 지침을 따릅니다. 실패한 사전 요구 사항이 있으면 수동으로 해결합니다.
- 5 IaaS 설치 관리자를 닫고 업그레이드된 vRealize Automation 장치를 재부팅하여 IaaS 자동 업그레이드를 활성화합니다.

---

**참고** IaaS 설치 관리자를 사용하여 수동으로 IaaS 업그레이드를 계속하려면, 먼저 업그레이드된 vRealize Automation 장치를 재부팅하고 모든 서비스가 등록될 때까지 기다립니다. IaaS 구성 요소가 설치되어 있는 모든 시스템을 업그레이드하고 구성해야 합니다. 자세한 내용은 [vRealize Automation을 대상 릴리스로 업그레이드한 후 IaaS 구성 요소 업그레이드](#)를 참조하십시오.

---

## vRealize Automation 마이그레이션

마이그레이션을 사용하여 현재 vRealize Automation 환경을 최신 vRealize Automation 버전으로 병존 업그레이드할 수 있습니다.

이 정보는 마이그레이션을 사용하여 vRealize Automation을 7.5로 업그레이드하는 것과 관련됩니다. 지원되는 다른 업그레이드 경로에 대한 자세한 내용은 [vRealize Automation 제품 설명서](#)에서 "vRealize Automation 6.2.5에서 업그레이드" 또는 vRealize Automation 7.1 이상에서 업그레이드를 참조하십시오.

## vRealize Automation 마이그레이션

마이그레이션을 사용하여 현재 vRealize Automation 환경의 병존 업그레이드를 수행할 수 있습니다.

마이그레이션은 테넌트와 ID 저장소를 제외한 모든 데이터를 현재 vRealize Automation 소스 환경에서 vRealize Automation 최신 버전이 있는 대상 배포로 이동합니다. 또한 마이그레이션은 포함된 vRealize Orchestrator 7.x의 모든 데이터를 대상 배포로 이동합니다.

마이그레이션은 데이터를 수집하여 대상 환경에 안전하게 복사하는 데 필요한 시간 동안 vRealize Automation 서비스를 중지하는 것 외에는 소스 환경을 변경하지 않습니다. 소스 vRealize Automation 데이터베이스의 크기에 따라 마이그레이션에 몇 분에서 몇 시간까지 소요될 수 있습니다.

최소 배포로 또는 고가용성 배포로 소스 환경을 마이그레이션할 수 있습니다.

마이그레이션 후 대상 환경을 운영 환경에서 사용하려면 소스 환경을 다시 활성화하지 마십시오. 마이그레이션 이후의 소스 환경 변경 내용은 대상 환경에 동기화되지 않습니다.

소스 환경이 vCloud Air 또는 vCloud Director와 통합되거나 물리적 끝점을 포함하는 경우에는 마이그레이션을 사용하여 업그레이드를 수행해야 합니다. 마이그레이션은 대상 환경에서 이러한 끝점 및 끝점과 연결된 모든 항목을 제거합니다. 또한 마이그레이션을 수행하면 vRealize Automation 6.2.5에서 지원된 VMware vRealize Application Services 통합도 제거됩니다.

**참고** 마이그레이션하기 전에 vRealize Automation 가상 시스템을 준비하기 위한 추가적인 작업을 완료해야 합니다. 마이그레이션하기 전에 기술 자료 문서 [51531](#)을 검토하십시오.

vRealize Automation 6.2.5에서 마이그레이션하는 경우 문제가 발생할 수 있습니다. 자세한 내용은 [마이그레이션 시나리오](#)를 참조하십시오.

## 마이그레이션 검사 목록

이 검사 목록을 사용하여 vRealize Automation 마이그레이션 중 및 전과 후에 작업을 추적합니다.

**참고** 운영 마이그레이션 전에 [테스트 마이그레이션 실행](#)을 실행하여 프로비저닝 사용 사례를 테스트하고 마이그레이션 중 발생할 수 있는 문제에 플래그를 설정합니다.

표 1-72. 마이그레이션 전

단계	참조
vRealize Automation 설치 배포	vRealize Automation <a href="#">엔터프라이즈 배포</a> 를 위한 설치 마법사 사용을 참조하십시오.
현재 설치 백업	시스템 백업 및 복원에 대한 자세한 내용은 <a href="#">기존 vRealize Automation 6.2.5 환경 백업</a> 을 참조하십시오. 일반 정보는 <a href="#">Symantec Netbackup을 사용하여 백업 및 복원 구성</a> 을 참조하십시오.
모든 사전 요구 사항 검증	<a href="#">마이그레이션 사전 요구 사항</a> 을 참조하십시오.
마이그레이션 전 작업을 사용하여 대상 준비	<a href="#">사전 마이그레이션 작업</a> 을 참조하십시오.
테스트 마이그레이션 실행	<a href="#">테스트 마이그레이션 실행</a> 을 참조하십시오.

표 1-73. 마이그레이션

단계	참조
마이그레이션 실행	테스트 마이그레이션이 검증되고 성공하면 <a href="#">마이그레이션 절차</a> 에 따라 운영 마이그레이션을 실행합니다.

표 1-74. 마이그레이션 후

단계	참조
마이그레이션 후 작업	마이그레이션이 완료되면 <a href="#">사후 마이그레이션 작업</a> 을 수행합니다.
마이그레이션된 환경 검증	<a href="#">대상 vRealize Automation 환경 검증</a> 을 참조하십시오.
6.2.x 마이그레이션 시나리오에 대한 검사	6.2에서 7.x로 마이그레이션하는 경우 <a href="#">마이그레이션 시나리오</a> 를 검토하여 차이점을 식별하십시오.

## 테스트 마이그레이션 실행

운영 환경을 마이그레이션하기 전에 프로비저닝 사용 사례의 유효성을 검사하기 위해 테스트 마이그레이션을 실행하는 것이 중요합니다. 이후 버전의 설계가 개선되면서 변경되었을 수도 있는 **Blueprint**, 워크플로 또는 스크립트를 다시 작업하려면 마이그레이션 테스트가 필요합니다. 관리되는 워크로드에 원치 않는 변경을 방지하려면 테스트 시 vRealize Automation 관리자의 주의가 필요합니다.

### 절차

- 1 vRealize Automation의 최소 설치를 배포합니다.
- 2 마이그레이션이 완료되면 대상에 다음 항목을 설정합니다.
  - a 마이그레이션 후에는 프록시 에이전트를 중지하고 이메일 알림을 일시 중단합니다.
  - b 만료 예정인 워크로드를 등록 취소하거나 리스를 연장합니다.
  - c 대상에서 프록시 에이전트 DoDeletes를 false로 설정합니다. 이벤트가 만료되면 대상에서 워크로드를 제거하지 않습니다.
  - d 대상 시스템의 리스를 모니터링하여 소스 시스템과 일치시킵니다. 리스를 동기화된 상태로 유지하여 시스템 만료를 방지합니다.
  - e 프로비저닝을 테스트하고 네트워크 파일을 사용하려면 예약에서 네트워크 프로파일을 제거합니다. 파일을 제거하면 소스와 대상의 IP 주소가 중복되지 않습니다.
- 3 vRealize Orchestrator 및 vRealize Automation에 대한 테스트 마이그레이션을 실행합니다.
- 4 유효성을 검사하고 소스 환경을 대상과 비교합니다. 변경이 필요한 영역을 확인합니다.
- 5 6.2.x에서 최신 버전으로 마이그레이션하는 경우 vRealize Production Test 업그레이드 지원 도구의 출력을 참조합니다. 이 도구는 워크플로 개선이 필요한 부분을 식별합니다.

도구에 대한 자세한 내용은 [vRealize Automation 제품 설명서](#)에서 "vRealize Automation Production Test"를 참조하십시오.

- 6 수정된 정보와 워크플로를 저장하고 기록하면 운영 마이그레이션으로 손쉽게 가져오고 전송할 수 있습니다.
- 7 운영 마이그레이션이 완료되면 테스트 마이그레이션 환경의 전원을 끕니다. 두 vRealize Automation 시스템의 장기 실행은 지원되는 구성이 아닙니다.

## vRealize Automation 환경 사용자 인터페이스

몇 가지 인터페이스로 vRealize Automation 환경을 사용하고 관리합니다.

### 사용자 인터페이스

다음 테이블은 vRealize Automation 환경을 관리하는 데 사용하는 인터페이스를 설명합니다.

표 1-75. vRealize Automation 관리 콘솔

용도	액세스	필요한 자격 증명
vRealize Automation 콘솔을 사용하여 다음과 같은 시스템 관리자 작업을 수행합니다.	1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 장치 시작 페이지를 엽니다.	시스템 관리자 역할을 가진 사용자여야 합니다.
<ul style="list-style-type: none"> <li>■ 테넌트를 추가합니다.</li> <li>■ vRealize Automation 사용자 인터페이스 사용자 지정합니다.</li> <li>■ 이메일 서버를 구성합니다.</li> <li>■ 이벤트 로그를 봅니다.</li> <li>■ vRealize Orchestrator를 구성합니다.</li> </ul>	2 <b>vRealize Automation 콘솔</b> 을 클릭합니다.  다음 URL을 사용하여 vRealize Automation 콘솔을 열 수도 있습니다. <a href="https://vrealize-automation-appliance-FQDN/vcac">https://vrealize-automation-appliance-FQDN/vcac</a>	
	3 로그인합니다.	

표 1-76. vRealize Automation 테넌트 콘솔. 이 인터페이스는 서비스와 리소스를 생성하고 관리하는 데 사용되는 기본 사용자 인터페이스입니다.

용도	액세스	필요한 자격 증명
vRealize Automation을 사용하여 다음과 같은 작업을 수행합니다.	1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름과 테넌트 URL 이름을 사용하여 테넌트의 URL을 입력합니다.	다음 역할 중 하나 이상을 가진 사용자여야 합니다.
<ul style="list-style-type: none"> <li>■ 새 IT 서비스 Blueprint를 요청합니다.</li> <li>■ 클라우드 및 IT 리소스를 생성하고 관리합니다.</li> <li>■ 사용자 지정 그룹을 생성하고 관리합니다.</li> <li>■ 비즈니스 그룹을 만들고 관리합니다.</li> <li>■ 사용자에게 역할을 할당합니다.</li> </ul>	2 로그인합니다.	<ul style="list-style-type: none"> <li>■ 애플리케이션 설계자</li> <li>■ 승인 관리자</li> <li>■ 카탈로그 관리자</li> <li>■ 컨테이너 관리자</li> <li>■ 컨테이너 설계자</li> <li>■ 상태 소비자</li> <li>■ 인프라 설계자</li> <li>■ 소비자 보안 내보내기</li> <li>■ 소프트웨어 설계자</li> <li>■ 테넌트 관리자</li> <li>■ XaaS 설계자</li> </ul>

표 1-77. vRealize Automation 장치 관리 인터페이스.

용도	액세스	필요한 자격 증명
<p>vRealize Automation 장치 관리를 사용하여 다음과 같은 작업을 수행합니다.</p> <ul style="list-style-type: none"> <li>■ 등록된 서비스의 상태를 봅니다.</li> <li>■ 시스템 정보를 보고 장치를 재부팅하거나 종료합니다.</li> <li>■ 고객 환경 향상 프로그램에 대한 참여를 관리합니다.</li> <li>■ 네트워크 상태를 봅니다.</li> <li>■ 업데이트 상태를 보고 업데이트를 설치합니다.</li> <li>■ 관리 설정을 관리합니다.</li> <li>■ vRealize Automation 호스트 설정을 관리합니다.</li> <li>■ SSO 설정을 관리합니다.</li> <li>■ 제품 라이선스를 관리합니다.</li> <li>■ vRealize Automation Postgres 데이터베이스를 구성합니다.</li> <li>■ vRealize Automation 메시징을 구성합니다.</li> <li>■ vRealize Automation 로깅을 구성합니다.</li> <li>■ IaaS 구성 요소를 설치합니다.</li> <li>■ 기존 vRealize Automation 설치에서 마이그레이션합니다.</li> <li>■ IaaS 구성 요소 인증서를 관리합니다.</li> <li>■ Xenon 서비스를 구성합니다.</li> </ul>	<ol style="list-style-type: none"> <li>1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 장치 시작 페이지를 엽니다.  <code>https://vrealize-automation-appliance-FQDN</code></li> <li>2 <b>vRealize Automation 장치 관리</b>를 클릭합니다.  다음 URL을 사용하여 vRealize Automation 장치 관리 인터페이스를 열 수도 있습니다. <code>https://vrealize-automation-appliance-FQDN:5480</code></li> <li>3 로그인합니다.</li> </ol>	<ul style="list-style-type: none"> <li>■ 사용자 이름: root</li> <li>■ 암호: vRealize Automation 장치를 배포할 때 입력한 암호.</li> </ul>

표 1-78. vRealize Orchestrator 클라이언트

용도	액세스	필요한 자격 증명
<p>vRealize Orchestrator 클라이언트를 사용하여 다음과 같은 작업을 수행합니다.</p> <ul style="list-style-type: none"> <li>■ 작업을 개발합니다.</li> <li>■ 워크플로를 개발합니다.</li> <li>■ 정책을 관리합니다.</li> <li>■ 패키지를 설치합니다.</li> <li>■ 사용자 및 사용자 그룹 사용 권한을 관리합니다.</li> <li>■ URI 개체에 태그를 연결합니다.</li> <li>■ 인벤토리를 봅니다.</li> </ul>	<ol style="list-style-type: none"> <li>1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 시작 페이지를 엽니다.  <code>https://vrealize-automation-appliance-FQDN</code></li> <li>2 로컬 컴퓨터에 client.jnlp 파일을 다운로드하려면 <b>vRealize Orchestrator Client</b>를 클릭합니다.</li> <li>3 client.jnlp 파일을 마우스 오른쪽 버튼으로 클릭하고 <b>시작</b>을 선택합니다.</li> <li>4 [계속하시겠습니까?] 대화 상자에서 <b>계속</b>을 클릭합니다.</li> <li>5 로그인합니다.</li> </ol>	<p>vRealize Orchestrator 제어 센터 인증 제공자 설정에 구성된 vcoadmins 그룹에 속하거나 시스템 관리자 역할이 있는 사용자여야 합니다.</p>

표 1-79. vRealize Orchestrator 제어 센터

용도	액세스	필요한 자격 증명
vRealize Orchestrator 제어 센터를 사용하여 vRealize Automation에 내장된 기본 vRealize Orchestrator 인스턴스의 구성을 편집합니다.	<ol style="list-style-type: none"> <li>1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름을 사용하여 vRealize Automation 장치 시작 페이지를 엽니다.  https://vrealize-automation-appliance-FQDN</li> <li>2 <b>vRealize Automation 장치 관리</b>를 클릭합니다.  다음 URL을 사용하여 vRealize Automation 장치 관리 인터페이스를 열 수도 있습니다. https://vrealize-automation-appliance-FQDN:5480</li> <li>3 로그인합니다.</li> <li>4 <b>vRA &gt; Orchestrator</b>를 클릭합니다.</li> <li>5 <b>Orchestrator 사용자 인터페이스</b>를 선택합니다.</li> <li>6 <b>시작</b>을 클릭합니다.</li> <li>7 Orchestrator 사용자 인터페이스 URL을 클릭합니다.</li> <li>8 로그인합니다.</li> </ol>	<p>사용자 이름</p> <ul style="list-style-type: none"> <li>■ 역할 기반 인증이 구성되지 않은 경우 <b>root</b>를 입력합니다.</li> <li>■ 역할 기반 인증에 대해 구성된 경우 vRealize Automation 사용자 이름을 입력합니다.</li> </ul> <p>암호</p> <ul style="list-style-type: none"> <li>■ 역할 기반 인증이 구성되지 않은 경우 vRealize Automation 장치를 배포했을 때 입력한 암호를 입력합니다.</li> <li>■ 사용자 이름이 역할 기반 인증에 대해 구성된 경우 사용자 이름에 대한 암호를 입력합니다.</li> </ul>

표 1-80. Linux 명령 프롬프트

용도	액세스	필요한 자격 증명
호스트(예: vRealize Automation 장치 호스트)에서 Linux 명령 프롬프트를 사용하여 다음과 같은 작업을 수행합니다. <ul style="list-style-type: none"> <li>■ 서비스 중지 또는 시작</li> <li>■ 구성 파일 편집</li> <li>■ 명령 실행</li> <li>■ 데이터 검색</li> </ul>	<ol style="list-style-type: none"> <li>1 vRealize Automation 장치 호스트에서 명령 프롬프트를 엽니다.  로컬 컴퓨터에서 명령 프롬프트를 여는 한 가지 방법은 PuTTY와 같은 애플리케이션을 사용하여 호스트에서 세션을 시작하는 것입니다.</li> <li>2 로그인합니다.</li> </ol>	<ul style="list-style-type: none"> <li>■ 사용자 이름: root</li> <li>■ 암호: vRealize Automation 장치를 배포할 때 생성한 암호.</li> </ul>

표 1-81. Windows 명령 프롬프트

용도	액세스	필요한 자격 증명
호스트(예: IaaS 호스트)에서 Windows 명령 프롬프트를 사용하여 스크립트를 실행할 수 있습니다.	<ol style="list-style-type: none"> <li>1 IaaS 호스트에서 Windows에 로그인합니다.  로컬 컴퓨터에서 로그인하는 한 가지 방법은 원격 데스크톱 세션을 시작하는 것입니다.</li> <li>2 Windows 명령 프롬프트를 엽니다.  명령 프롬프트를 여는 한 가지 방법은 호스트에서 [시작] 아이콘을 마우스 오른쪽 버튼으로 클릭하고 <b>명령 프롬프트</b> 또는 <b>명령 프롬프트(관리자)</b>를 선택하는 것입니다.</li> </ol>	<ul style="list-style-type: none"> <li>■ 사용자 이름: 관리자 권한이 있는 사용자.</li> <li>■ 암호: 사용자의 암호.</li> </ul>

## 마이그레이션 사전 요구 사항

마이그레이션 사전 요구 사항은 대상 환경에 따라 다릅니다.

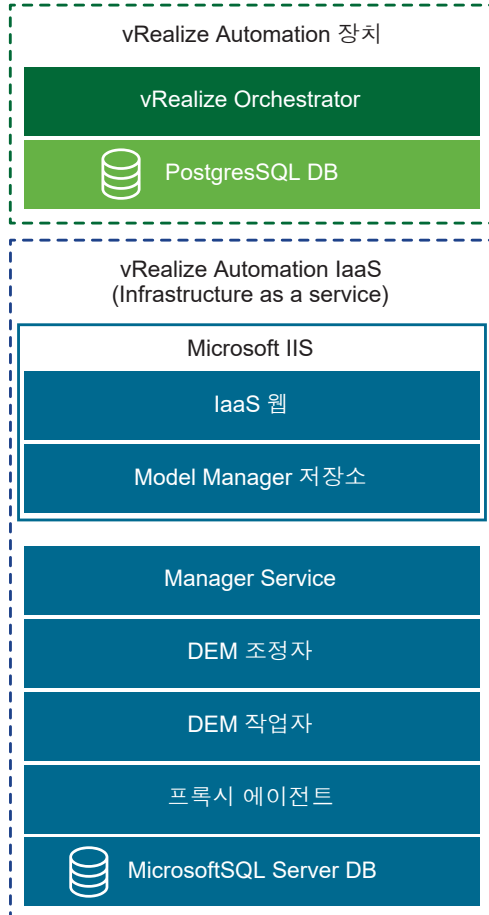
최소 환경 또는 고가용성 환경으로 마이그레이션할 수 있습니다.

#### 최소 환경으로 마이그레이션하기 위한 사전 요구 사항

최소 환경으로 성공적으로 마이그레이션하기 위해 다음 사전 요구 사항을 검토합니다.

최소 배포에는 IaaS 구성 요소를 호스팅하는 하나의 Windows Server와 하나의 vRealize Automation 장치가 포함됩니다. 최소 배포에서 vRealize Automation SQL Server 데이터베이스는 IaaS 구성 요소와 동일한 IaaS Windows Server 또는 별도의 Windows Server에 있을 수 있습니다.

그림 1-16. vRealize Automation 최소 배포



#### 사전 요구 사항

- 새로운 vRealize Automation 대상 환경이 있는지 확인합니다.

- 다음 요구 사항에 따라 대상 환경에 관련 프록시 에이전트를 설치합니다.
  - vSphere, Hyper-V, Citrix XenServer 및 테스트 프록시 에이전트에 대해 대상 프록시 에이전트 이름과 소스 프록시 에이전트 이름이 일치해야 합니다.

---

**참고** 다음 단계를 완료하여 에이전트 이름을 가져옵니다.

- 1 IaaS 호스트에서 **관리자** 권한이 있는 로컬 사용자로 Windows에 로그인합니다.
  - 2 Windows 탐색기를 사용하여 에이전트 설치 디렉토리로 이동합니다.
  - 3 VRMAgent.exe.config 파일을 엽니다.
  - 4 serviceConfiguration 태그 아래에서 agentName 특성의 값을 찾습니다.
- 

- 기술 자료 문서 [51531](#)을 검토합니다.
- vSphere, Hyper-V, Citrix XenServer 및 테스트 프록시 에이전트에 대해 대상 프록시 에이전트 끝점 이름과 소스 프록시 에이전트 끝점 이름이 일치해야 합니다.
- 대상 환경에서 vSphere, Hyper-V, Citrix XenServer 또는 테스트 프록시 에이전트에 대해 끝점을 생성하지 마십시오.
- 대상 vRealize Automation 장치의 vRealize Automation 구성 요소에 대한 버전 번호를 검토합니다.
  - a 대상 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **루트**로 대상 vRealize Automation 장치 관리에 로그인합니다.
  - b **클러스터**를 선택합니다.
  - c 삼각형을 클릭하여 호스트/노드 이름 레코드를 확장합니다.

vRealize AutomationIaaS 구성 요소의 버전 번호가 일치하는지 확인합니다.

- vRealize Automation 대상 IaaS 데이터베이스의 대상 Microsoft SQL Server 버전이 2012, 2014 또는 2016인지 확인합니다.
- 소스 및 대상 vRealize Automation 환경 사이에 포트 22가 열려 있는지 확인합니다. 소스 가상 장치와 대상 가상 장치 사이에 SSH(보안 셸) 연결을 설정하려면 포트 22가 필요합니다.
- 끝점 vCenter에 마이그레이션을 완료하기에 충분한 리소스가 있는지 확인합니다.
- 대상 vRealize Automation 환경 시스템 시간이 Cafe와 IaaS 구성 요소 간에 동기화되었는지 확인합니다.
- 대상 환경의 IaaS 서버 노드에 Java SE Runtime Environment(JRE) 8, 64비트, 업데이트 181 이상이 설치되어 있는지 확인합니다. JRE를 설치한 후 JAVA\_HOME 환경 변수가 각 IaaS 노드에 설치한 Java 버전을 가리키는지 확인합니다. 필요한 경우 경로를 수정합니다.
- 각 IaaS 노드에 PowerShell 3.0 이상이 설치되어 있는지 확인합니다.
- 소스 및 대상 vRealize Automation 환경이 실행되고 있는지 확인합니다.
- 소스 vRealize Automation 환경에서 실행 중인 사용자 작업 및 프로비저닝 작업이 없는지 확인합니다.



- 대상 vRealize Automation 환경의 IaaS 노드에 운영 체제와 상호 작용할 수 있는 바이러스 백신 또는 보안 소프트웨어가 실행 중인지 확인하고 해당 구성 요소가 올바르게 구성되었는지 또는 이러한 구성 요소가 사용되지 않도록 설정되었는지 확인합니다.
- 보류 중인 Windows 설치 업데이트로 인해 IaaS Web Service 및 Model Manager를 다시 시작할 필요가 없는지 확인합니다. 업데이트가 보류 중이면 마이그레이션이 World Wide Web 게시 서비스를 시작하거나 종료하지 못할 수 있습니다.

다음에 수행할 작업

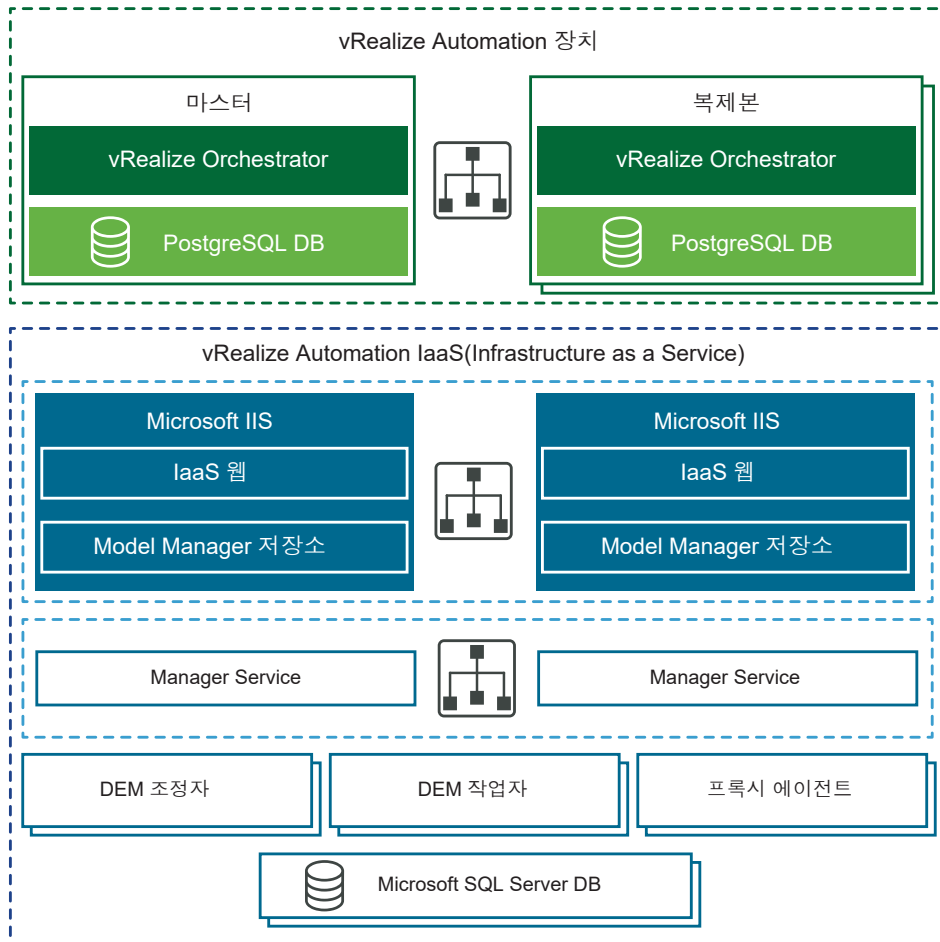
사전 마이그레이션 작업.

고가용성 환경으로 마이그레이션하기 위한 사전 요구 사항

고가용성 환경으로 성공적으로 마이그레이션하기 위해 다음 사전 요구 사항을 검토합니다.

고가용성 환경의 크기는 다양할 수 있습니다. 기본 분산 배포는 별도의 Windows Server에서 IaaS 구성 요소를 호스팅하는 방법으로 간단하게 vRealize Automation의 성능을 향상시킬 수 있습니다. 많은 고가용성 환경은 더 나아가 중복 장치, 중복 서버 및 더 많은 용량을 위한 로드 밸런싱을 구현합니다. 대규모 분산 배포는 확장성, 고가용성 및 재해 복구 기능을 향상시킵니다.

그림 1-17. vRealize Automation 고가용성 환경



## 사전 요구 사항

- 고가용성을 위해 구성된 마스터 장치와 복제 가상 장치가 있는 새로운 vRealize Automation 대상 설치가 있는지 확인합니다. [vRealize Automation 고가용성 구성 고려 사항](#) 항목을 참조하십시오.
- 모든 vRealize Automation 가상 장치가 루트 사용자에게 대해 동일한 암호를 사용하는지 확인합니다.
- 다음 요구 사항에 따라 대상 환경에 관련 프록시 에이전트를 설치합니다.
  - vSphere, Hyper-V, Citrix XenServer 및 테스트 프록시 에이전트에 대해 대상 프록시 에이전트 이름과 소스 프록시 에이전트 이름이 일치해야 합니다.

---

**참고** 다음 단계를 완료하여 에이전트 이름을 가져옵니다.

- 1 IaaS 호스트에서 **관리자** 권한이 있는 로컬 사용자로 Windows에 로그인합니다.
  - 2 Windows 탐색기를 사용하여 에이전트 설치 디렉토리로 이동합니다.
  - 3 VRMAgent.exe.config 파일을 엽니다.
  - 4 serviceConfiguration 태그 아래에서 agentName 특성의 값을 찾습니다.
- 
- vSphere, Hyper-V, Citrix XenServer 및 테스트 프록시 에이전트에 대해 대상 프록시 에이전트 끝점 이름과 소스 프록시 에이전트 끝점 이름이 일치해야 합니다.
  - 대상 환경에서 vSphere, Hyper-V, Citrix XenServer 또는 테스트 프록시 에이전트에 대해 끝점을 생성하지 마십시오.
  - 대상 vRealize Automation 장치의 vRealize Automation 구성 요소에 대한 버전 번호를 확인합니다.
    - a 대상 vRealize Automation 환경에서, vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.  
`https://vrealize-automation-appliance-FQDN:5480`
    - b **클러스터**를 선택합니다.
    - c 호스트/노드 이름 레코드를 확장하여 구성 요소를 보려면 확장 버튼을 클릭합니다.  
 모든 가상 장치 시스템 노드에서 vRealize Automation 구성 요소의 버전 번호가 일치하는지 확인합니다.  
 모든 IaaS 노드에서 vRealize AutomationIaaS 구성 요소의 버전 번호가 일치하는지 확인합니다.
  - 기술 자료 문서 [51531](#)을 검토합니다.
  - 이러한 단계를 수행하여 트래픽을 마스터 노드에만 연결합니다.
    - a 모든 중복 노드를 사용하지 않도록 설정합니다.
    - b 로드 밸런서 설명서에 따라 이러한 항목에 대한 상태 모니터를 제거합니다.
      - vRealize Automation 가상 장치
      - IaaS 웹 사이트
      - IaaS Manager Service

- vRealize Automation 대상 IaaS 데이터베이스의 대상 Microsoft SQL Server 버전이 2012, 2014 또는 2016인지 확인합니다.
- 소스 및 대상 vRealize Automation 환경 사이에 포트 22가 열려 있는지 확인합니다. 소스 가상 장치와 대상 가상 장치 사이에 SSH(보안 셸) 연결을 설정하려면 포트 22가 필요합니다.
- 끝점 vCenter에 마이그레이션을 완료하기에 충분한 리소스가 있는지 확인합니다.
- 기본값에서 최소 10분으로 로드 밸런서 시간 초과 설정을 변경했는지 확인합니다.
- 대상 vRealize Automation 환경 시스템 시간이 Cafe와 IaaS 구성 요소 간에 동기화되었는지 확인합니다.
- 대상 환경의 IaaS Web Service 및 Model Manager 노드가 Java Runtime Environment 권한을 가지고 있는지 확인합니다. Java SE Runtime Environment(JRE) 8, 64비트, 업데이트 181 이상이 설치되어 있어야 합니다. JAVA\_HOME 시스템 변수가 각 IaaS 노드에 설치한 Java 버전을 가리키는지 확인합니다. 필요한 경우 경로를 수정합니다.
- 각 IaaS 노드에 PowerShell 3.0 이상이 설치되어 있는지 확인합니다.
- 소스 및 대상 vRealize Automation 환경이 실행되고 있는지 확인합니다.
- 소스 vRealize Automation 환경에서 실행 중인 사용자 작업 및 프로비저닝 작업이 없는지 확인합니다.
- 대상 vRealize Automation 환경의 IaaS 노드에 운영 체제와 상호 작용할 수 있는 바이러스 백신 또는 보안 소프트웨어가 실행 중인지 확인하고 해당 구성 요소가 올바르게 구성되었는지 또는 이러한 구성 요소가 사용되지 않도록 설정되었는지 확인합니다.
- 보류 중인 Windows 설치 업데이트로 인해 IaaS Web Service 및 Model Manager를 다시 시작할 필요가 없는지 확인합니다. 업데이트가 보류 중이면 마이그레이션이 World Wide Web 게시 서비스를 시작하거나 종료하지 못할 수 있습니다.

다음에 수행할 작업

사전 마이그레이션 작업.

## 사전 마이그레이션 작업

마이그레이션하기 전에 몇 가지 사전 마이그레이션 작업을 수행해야 합니다.

소스 vRealize Automation 환경 데이터를 대상 vRealize Automation 환경에 마이그레이션하기 전에 수행하는 사전 마이그레이션 작업은 소스 환경에 따라 다릅니다.

### vRealize Automation 마이그레이션을 통해 도입되는 변경 사항 검토

vRealize Automation 7.1 이상에서는 업그레이드 프로세스 진행 중과 완료 후에 다양한 기능이 변경됩니다. vRealize Automation 6.2.5 환경에서 업그레이드하는 경우 업그레이드 프로세스를 시작하기 전에 이러한 변경 사항을 검토합니다.

vRealize Automation 6.2.5와 7.1 이상의 차이점에 대한 자세한 내용은 [vRealize Automation 마이그레이션을 통해 도입되는 변경 사항 검토](#) 항목을 참조하십시오.

**참고** vRealize Production Test Upgrade Assist Tool은 vRealize Automation 6.2.5 환경을 분석하여 업그레이드 문제를 일으킬 수 있는 기능 구성을 파악하고 환경이 업그레이드할 준비가 되었는지 확인합니다. 이 도구 및 관련 설명서를 다운로드하려면 [VMware vRealize Production Test Tool](#) 제품 다운로드 페이지로 이동하십시오.

vRealize Automation 6.2.5에서 최신 버전으로 마이그레이션한 후 이러한 속성 정의를 사용하는 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없습니다.

- 제어 유형: 확인란 또는 링크.
- 특성: 관계, 정규식 또는 속성 레이아웃.

vRealize Automation 7.1 이상에서는 속성 정의에서 더 이상 이러한 요소를 사용하지 않습니다. 속성 정의에서 포함된 제어 유형 또는 특성을 사용하지 않고 대신 vRealize Orchestrator 스크립트 작업을 사용하도록 속성 정의를 구성하거나 속성 정의를 다시 생성해야 합니다. 자세한 내용은 [마이그레이션 후 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없음](#) 항목을 참조하십시오.

#### 소프트웨어 에이전트 패치 적용

vRealize Automation 7.1.x 또는 7.3.x에서 마이그레이션하려면 소프트웨어 에이전트를 TLS 1.2로 업그레이드할 수 있도록 먼저 소스 장치에 핫 픽스를 적용해야 합니다.

TLS(전송 계층 보안) 프로토콜은 브라우저와 vRealize Automation 간의 데이터 무결성을 제공합니다. 이 핫 픽스를 적용하면 소스 환경의 소프트웨어 에이전트를 TLS 1.2로 업그레이드할 수 있게 됩니다. 이 업그레이드는 최고 수준의 보안을 보장하며 vRealize Automation 7.1.x 또는 7.3.x에 필요합니다. 각 버전에는 고유한 핫 픽스가 있습니다.

#### 사전 요구 사항

실행 중인 vRealize Automation 7.1.x 또는 7.3.x 소스 vRealize Automation 환경입니다.

#### 절차

- ◆ 마이그레이션을 시작하기 전에 소스 vRealize Automation 7.1.x 또는 7.3.x 장치에 이 핫 픽스를 적용합니다. [기술 자료 문서 52897](#)을 참조하십시오.

#### 다음에 수행할 작업

[vSphere 에이전트에서 DoDeletes 설정을 False로 변경](#).

#### vSphere 에이전트에서 DoDeletes 설정을 False로 변경

vRealize Automation 6.2.x 환경에서 마이그레이션하는 경우에는 마이그레이션하기 전에 대상 vSphere 에이전트에서 DoDeletes 값을 **true**에서 **false**로 변경해야 합니다.

#### 사전 요구 사항

마이그레이션 위한 사전 요구 사항을 완료합니다.

## 절차

1 DoDeletes 값을 **false**로 변경합니다.

이렇게 하면 소스 환경에서 가상 시스템이 삭제되는 것을 방지합니다. 소스와 대상 환경은 병렬로 실행됩니다. 프로덕션 마이그레이션을 확인한 후 리스 불일치가 발생할 수 있습니다.

2 프로덕션 마이그레이션을 검증하고 소스 환경을 종료한 후에는 DoDeletes 값을 **true**로 설정합니다.3 vSphere 에이전트 구성 절차의 단계에 따라 DoDeletes를 **false**로 설정합니다.

다음에 수행할 작업

마이그레이션을 위해 vRealize Automation 가상 시스템 준비.

## vRealize Automation 소스 환경에서 템플릿 확인

vRealize Automation 마이그레이션 이전에 가상 시스템 템플릿을 살펴보고 모든 템플릿의 최소 메모리 설정이 4MB 이상인지 확인해야 합니다.

vRealize Automation 소스 환경에 있는 가상 시스템 템플릿의 메모리가 4MB 미만이면 마이그레이션에 실패합니다. 소스 환경에 메모리가 4MB 미만인 Blueprint가 있는지 확인하려면 이 절차를 완료하십시오.

사전 요구 사항

## 절차

## 1 SQL Server 데이터베이스를 호스팅하는 Windows Server에 로그인합니다.

## 2 SQL Server Management Studio를 열고 vRA 데이터베이스에 연결합니다.

## 3 다음 스크립트를 실행하여 메모리가 4MB 미만으로 지정된 Blueprint가 있는지 확인합니다.

```
select VirtualMachineTemplate set MemoryMB = 4 where IsHidden = 0 and MemoryMB < 4;
```

여기서 vCAC는 데이터베이스 이름입니다.

## 4 스크립트를 통해 메모리가 4MB 미만으로 지정된 Blueprint를 찾으면 다음 스크립트를 실행하여 메모리를 4MB 이상으로 업데이트합니다.

```
update [vCAC].[dbo].[VirtualMachineTemplate] set MemoryMB = 4 where IsHidden = 0 and MemoryMB < 4;
```

여기서 vCAC는 데이터베이스 이름입니다.

다음에 수행할 작업

마이그레이션을 위해 vRealize Automation 가상 시스템 준비.

## 마이그레이션을 위해 vRealize Automation 가상 시스템 준비

vRealize Automation 6.2.x 가상 시스템 마이그레이션에 대한 알려진 문제 때문에 마이그레이션 후에 문제가 발생할 수 있습니다.

기술 자료 문서 000051531을 검토하고 마이그레이션하기 전에 환경에서 모든 관련 수정을 수행해야 합니다.

다음에 수행할 작업

마이그레이션에 필요한 정보 수집.

마이그레이션에 필요한 정보 수집

다음 테이블을 사용하면 소스 및 대상 환경에서 마이그레이션하는 데 필요한 정보를 기록할 수 있습니다.

사전 요구 사항

상황에 맞는 사전 요구 사항 확인을 완료합니다.

- 최소 환경으로 마이그레이션하기 위한 사전 요구 사항.
- 고가용성 환경으로 마이그레이션하기 위한 사전 요구 사항.

예

표 1-82. 소스 vRealize Automation 장치

옵션	설명	값
호스트 이름	소스 vRealize Automation 장치 관리에 로그인합니다. 시스템 탭에서 호스트 이름을 찾습니다. 호스트 이름은 FQDN(정규화된 도메인 이름)이어야 합니다.	
루트 사용자 이름	root	
루트 암호	소스 vRealize Automation 장치를 배포할 때 입력한 루트 암호입니다.	
마이그레이션 패키지 위치	마이그레이션 패키지가 생성되는 소스 vRealize Automation 6.2.x 또는 7.x 장치의 기존 디렉토리에 대한 경로입니다. 디렉토리의 사용 가능한 공간은 vRealize Automation 데이터베이스 크기의 두 배만큼 커야 합니다. 기본 위치는 /storage입니다.	

표 1-83. 대상 vRealize Automation 장치

옵션	설명	값
루트 사용자 이름	root	
루트 암호	대상 vRealize Automation 장치를 배포할 때 입력한 루트 암호입니다.	
기본 테넌트	vsphere.local	
관리자 사용자 이름	관리자	
관리자 암호	대상 vRealize Automation 환경을 배포할 때 입력한 administrator@vsphere.local 사용자 암호입니다.	

표 1-84. 대상 IaaS 데이터베이스

옵션	설명	값
데이터베이스 서버	복제된 데이터베이스가 있는 Microsoft SQL Server 인스턴스의 위치입니다. 명명된 인스턴스와 기본이 아닌 포트가 사용되는 경우 SERVER,PORT\INSTANCE-NAME 형식으로 지정합니다.	
복제된 데이터베이스 이름	마이그레이션에 대해 복제된 소스 vRealize Automation 6.2.x/7.x IaaS Microsoft SQL 데이터베이스의 이름입니다.	
인증 모드	Windows 또는 SQL Server를 선택합니다. SQL Server를 선택하는 경우 로그인 이름과 암호를 입력해야 합니다.	
로그인 이름	복제된 IaaS Microsoft SQL 데이터베이스에 대해 db_owner 역할을 가진 SQL Server 사용자의 로그인 이름입니다.	
암호	SQL Server 사용자의 암호입니다.	
원본 암호화 키	소스 환경에서 검색한 원본 암호화 키입니다. <a href="#">소스 vRealize Automation 환경에서 암호화 키 가져오기</a> 항목을 참조하십시오.	
새 암호	새 암호화 키를 생성하는 데 사용되는 일련의 단어입니다. 대상 vRealize Automation 환경에서 새 IaaS 구성 요소를 설치할 때마다 이 암호를 사용합니다.	

다음에 수행할 작업

[소스 vRealize Automation 환경에서 암호화 키 가져오기](#).

소스 vRealize Automation 환경에서 암호화 키 가져오기

마이그레이션 절차의 일부로 소스 vRealize Automation 환경의 암호화 키를 입력해야 합니다.

사전 요구 사항

소스 환경에서 액티브 Manager Service 호스트 가상 시스템에 대해 관리자 권한을 갖고 있는지 확인합니다.

절차

- 1 소스 환경에서 액티브 Manager Service를 호스팅하는 가상 시스템에서 관리자 명령 프롬프트를 열고 다음 명령을 실행합니다.

```
"C:\Program Files (x86)\VMware\VCAC\Server\ConfigTool\EncryptionKeyTool\DynamicOps.Tools.EncryptionKeyTool.exe" key-read -c "C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config" -v
```

설치 디렉토리가 기본 위치(C:\Program Files (x86)\VMware\VCAC)가 아닌 경우 실제 설치 디렉토리로 경로를 편집합니다.

2 명령을 실행한 후에 표시되는 키를 저장합니다.

이 키는 다음 예와 유사한 긴 문자열입니다.

```
NRH+f/B1nCB6yvasLS3sxespgdkcFWAEuyV0g4lfryg=.
```

다음에 수행할 작업

- vRealize Automation 6.2.x 환경에서 마이그레이션하는 경우: [소스 vRealize Automation 환경에서 대상 환경으로 각 테넌트 추가](#)
- vRealize Automation 7.x 환경에서 마이그레이션하는 경우: [소스 vRealize Automation 6.2.x 환경의 테넌트 및 IaaS 관리자 나열](#)

소스 vRealize Automation 6.2.x 환경의 테넌트 및 IaaS 관리자 나열

vRealize Automation 6.2.x 환경을 마이그레이션하려면 먼저 각 테넌트에 대해 테넌트 관리자와 IaaS 관리자의 목록을 만들어야 합니다.

소스 vRealize Automation 콘솔에서 각 테넌트에 대해 다음 절차를 수행합니다.

---

**참고** vRealize Automation 7.x 환경에서 마이그레이션한 경우에는 이 절차를 수행하지 않아도 됩니다.

---

사전 요구 사항

소스 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **관리자**로 소스 vRealize Automation 콘솔에 로그인합니다.

---

**참고** 고가용성 환경인 경우, 소스 가상 장치 로드 밸런서의 정규화된 도메인 이름(<https://vra-vb-lb-hostname.domain.name/vcac>)을 사용하여 콘솔을 엽니다.

---

절차

- 1 **관리 > 테넌트**를 선택합니다.
- 2 테넌트 이름을 클릭합니다.
- 3 **관리자**를 클릭합니다.
- 4 각 테넌트 및 IaaS 관리자 사용자 이름이 포함된 목록을 만듭니다.
- 5 **취소**를 클릭합니다.

다음에 수행할 작업

[소스 vRealize Automation 환경에서 대상 환경으로 각 테넌트 추가](#).

소스 vRealize Automation 환경에서 대상 환경으로 각 테넌트 추가

소스 환경에 있는 각 테넌트의 이름을 사용하여 대상 환경에 테넌트를 추가해야 합니다.



마이그레이션이 성공하려면 소스 환경의 각 테넌트를 대상 환경에 생성해야 합니다. 또한 소스 환경의 테넌트 URL 이름을 사용하여 추가하는 각 테넌트에 대해 테넌트별 액세스 URL을 사용해야 합니다. 마이그레이션하지 않을 미사용 테넌트가 소스 환경에 있는 경우에는 마이그레이션 전에 해당 테넌트를 소스 환경에서 삭제해야 합니다.

**참고** 마이그레이션을 검증하면 사전 요구 사항에 따라 소스에 구성된 동일한 테넌트 수 이상의 테넌트가 대상 시스템에 있는지 확인할 수 있습니다. 마이그레이션 검증은 테넌트 이름이 아니라 대/소문자를 구분하는 테넌트 URL 이름을 기준으로 테넌트 비교를 수행합니다.

소스 환경의 각 테넌트에 대해 이 절차를 수행합니다.

- vRealize Automation 6.2.x 환경에서 마이그레이션할 때는 소스 환경에 있는 기존 SSO2 테넌트와 ID 저장소를 대상 환경의 VMware Identity Manager로 마이그레이션합니다.
- vRealize Automation 7.x 환경에서 마이그레이션할 때는 소스 환경에 있는 기존 VMware Identity Manager 테넌트와 ID 저장소를 대상 환경의 VMware Identity Manager로 마이그레이션합니다.

사전 요구 사항

- [마이그레이션에 필요한 정보 수집](#).
- 대상 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **관리자**로 대상 vRealize Automation 콘솔에 로그인합니다.

**참고** 고가용성 환경인 경우, 대상 가상 장치 로드 밸런서의 정규화된 도메인 이름(<https://vra-vb-hostname.domain.name/vcac>)을 사용하여 콘솔을 엽니다.

절차

- 1 **관리 > 테넌트**를 선택합니다.
- 2 **새로 만들기** 아이콘()을 클릭합니다.
- 3 **이름** 텍스트 상자에 소스 환경의 테넌트 이름과 일치하는 테넌트 이름을 입력합니다.  
예를 들어 소스 환경의 테넌트 이름이 DEVTenant이면 **DEVTenant**를 입력합니다.
- 4 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.
- 5 **URL 이름** 텍스트 상자에 소스 환경의 테넌트 URL 이름과 일치하는 테넌트 URL 이름을 입력합니다.  
이 URL 이름은 vRealize Automation 콘솔 URL에 테넌트 관련 식별자를 추가하는 데 사용됩니다.  
예를 들어 소스 환경의 DEVTenant에 대한 URL 이름이 dev인 경우 **dev**를 입력하여 <https://vra-vb-hostname.domain.name/vcac/org/dev> URL을 생성합니다.
- 6 (선택 사항) **연락처 이메일** 텍스트 상자에 이메일 주소를 입력합니다.
- 7 **제출하고 다음 단계로 진행**을 클릭합니다.

다음에 수행할 작업

추가된 각 테넌트에 대해 관리자 생성.

### 추가된 각 테넌트에 대해 관리자 생성

대상 환경에 추가한 각 테넌트에 대해 관리자를 생성해야 합니다. 관리자를 생성하려면 로컬 사용자 계정을 생성한 후 이 계정에 테넌트 관리자 권한을 할당합니다.

대상 환경의 각 테넌트에 대해 이 절차를 수행합니다.

사전 요구 사항


- **소스 vRealize Automation 환경에서 대상 환경으로 각 테넌트 추가.**
- 대상 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **관리자**로 대상 vRealize Automation 콘솔에 로그인합니다.

---

**참고** 고가용성 환경인 경우, 대상 가상 장치 로드 밸런서의 정규화된 도메인 이름(<https://vra-vb-lb-hostname.domain.name/vcac>)을 사용하여 콘솔을 엽니다.

---

절차

- 1 **관리 > 테넌트**를 선택합니다.
- 2 추가한 테넌트를 클릭합니다.  
예를 들어 DEVTenant의 경우 **DEVTenant**를 클릭합니다.
- 3 **로컬 사용자**를 클릭합니다.
- 4 **새로 만들기** 아이콘()을 클릭합니다.
- 5 **사용자 세부 정보**에 요청된 정보를 입력하여 테넌트 관리자 역할을 할당할 로컬 사용자 계정을 생성합니다.  
로컬 사용자 이름은 기본 로컬 디렉토리인 **vsphere.local**에서 고유해야 합니다.
- 6 **확인**을 클릭합니다.
- 7 **관리자**를 클릭합니다.
- 8 **테넌트 관리자** 검색 상자에 로컬 사용자 이름을 입력하고 Enter 키를 누릅니다.
- 9 사용자를 테넌트 관리자 목록에 추가하려면 검색 결과에서 적절한 이름을 클릭합니다.
- 10 **완료**를 클릭합니다.
- 11 콘솔에서 로그아웃합니다.

다음에 수행할 작업

- 최소 배포의 경우: **최소 환경으로 마이그레이션하기 전에 Active Directory 링크의 사용자와 그룹 동기화.**

- 고가용성 배포의 경우: **고가용성 환경으로 마이그레이션하기 전에 Active Directory 링크의 사용자와 그룹 동기화.**

최소 환경으로 마이그레이션하기 전에 **Active Directory** 링크의 사용자와 그룹 동기화

사용자와 그룹을 vRealize Automation의 최소 배포로 가져오기 전에 대상 vRealize Automation을 Active Directory 링크에 연결해야 합니다.

각 테넌트에 대해 이 절차를 수행합니다. 테넌트에 **Active Directory**가 두 개 이상 있는 경우에는 테넌트에서 사용하는 **Active Directory** 각각에 대해 이 절차를 수행합니다.

사전 요구 사항

- **추가된 각 테넌트에 대해 관리자 생성.**
- **Active Directory에 대한 액세스 권한이 있는지 확인합니다.**
- **테넌트 관리자**로 vRealize Automation에 로그인합니다.

절차

- 1 **관리 > 디렉토리 관리 > 디렉토리**를 선택합니다.
- 2 **디렉토리 추가** 아이콘(+)을 클릭하고 **LDAP/IWA를 통한 Active Directory 추가**를 선택합니다.
- 3 **Active Directory 계정 설정**을 입력합니다.

◆ 비네이티브 Active Directory

옵션	샘플 입력
디렉토리 이름	고유한 디렉토리 이름을 입력합니다. 비네이티브 Active Directory를 사용하는 경우 <b>LDAP를 통한 Active Directory</b> 를 선택합니다.
이 디렉토리는 <b>DNS 서비스 위치를 지원</b> 합니다.	이 옵션을 선택 해제합니다.
기본 DN	서버가 검색하는 디렉토리에 대한 시작점의 DN(고유 이름)을 입력합니다. 예를 들어 <b>cn=users,dc=rainpole,dc=local</b> 을 입력합니다.

옵션	샘플 입력
<b>Bind DN</b>	사용자를 검색할 권한이 있는 Active Directory 사용자 계정의 CN(일반 이름)을 포함하여 전체 DN(고유 이름)을 입력합니다. 예를 들어 <b>cn=config_admin infra,cn=users,dc=rainpole,dc=local</b> 을 입력합니다.
<b>Bind DN 암호</b>	사용자를 검색할 수 있는 계정의 Active Directory 암호를 입력하고 <b>연결 테스트</b> 를 클릭하여, 구성된 디렉토리에 대한 연결을 테스트합니다.

◆ 네이티브 Active Directory

옵션	샘플 입력
<b>디렉토리 이름</b>	고유한 디렉토리 이름을 입력합니다. 네이티브 Active Directory를 사용하는 경우 <b>Active Directory(Windows 통합 인증)</b> 를 선택합니다.
<b>도메인 이름</b>	가입할 도메인의 이름을 입력합니다.
<b>도메인 관리자 사용자 이름</b>	도메인 관리자의 사용자 이름을 입력합니다.
<b>도메인 관리자 암호</b>	도메인 관리자의 암호를 입력합니다.
<b>Bind 사용자 UPN</b>	도메인에서 인증될 수 있는 사용자의 이름을 이메일 주소 형식을 사용하여 입력합니다.
<b>Bind DN 암호</b>	사용자를 검색할 수 있는 계정에 대한 Active Directory Bind 계정 암호를 입력합니다.

4 저장 및 다음을 클릭합니다.

도메인 선택에 도메인 목록이 표시됩니다.

5 기본 도메인 설정을 수락하고 다음을 클릭합니다.

6 특성 이름이 올바른 Active Directory 특성에 매핑되어 있는지 확인하고 다음을 클릭합니다.

7 동기화할 그룹과 사용자를 선택합니다.

a 새로 만들기 아이콘(+ )을 클릭합니다.

b 사용자 도메인을 입력하고 그룹 찾기를 클릭합니다.

예를 들어 **dc=vcac,dc=local**을 입력합니다.

c 동기화할 그룹을 선택하려면 선택을 클릭하고 다음을 클릭합니다.

d 사용자 선택에서 동기화할 사용자를 선택하고 다음을 클릭합니다.

vRealize Automation을 사용해야 하는 사용자 및 그룹만 추가합니다. 중첩 구조의 모든 그룹에서 vRealize Automation을 사용해야 하는 경우가 아니면 중첩된 그룹 동기화를 선택하지 마십시오.

8 디렉토리에 동기화 중인 사용자 및 그룹을 검토하고 디렉토리 동기화를 클릭합니다.

디렉토리 동기화에 시간이 걸리며 백그라운드에서 실행됩니다.

다음에 수행할 작업

### 소스 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행

고가용성 환경으로 마이그레이션하기 전에 **Active Directory** 링크의 사용자와 그룹 동기화

사용자와 그룹을 고가용성 vRealize Automation 환경으로 가져오기 전에 **Active Directory** 링크에 연결해야 합니다.

- 각 테넌트에 대해 1~8단계를 수행합니다. 테넌트에 **Active Directory**가 두 개 이상 있는 경우에는 테넌트에서 사용하는 **Active Directory** 각각에 대해 이 절차를 수행합니다.
- 테넌트에 연결된 각 ID 제공자에 대해 9~10단계를 반복합니다.

사전 요구 사항

- 추가된 각 테넌트에 대해 관리자 생성.
- **Active Directory**에 대한 액세스 권한이 있는지 확인합니다.
- **테넌트 관리자**로 vRealize Automation에 로그인합니다.

절차

- 1 **관리 > 디렉토리 관리 > 디렉토리**를 선택합니다.
- 2 **디렉토리 추가** 아이콘(+)을 클릭하고 **LDAP/IWA를 통한 Active Directory 추가**를 선택합니다.
- 3 **Active Directory** 계정 설정을 입력합니다.

#### ◆ 비네이티브 Active Directory

옵션	샘플 입력
디렉토리 이름	고유한 디렉토리 이름을 입력합니다. 비네이티브 Active Directory를 사용하는 경우 <b>LDAP를 통한 Active Directory</b> 를 선택합니다.
이 디렉토리는 DNS 서비스 위치를 지원 합니다.	이 옵션을 선택 해제합니다.
기본 DN	서버가 검색하는 디렉토리에 대한 시작점의 DN(고유 이름)을 입력합니다. 예를 들어 <b>cn=users,dc=rainpole,dc=local</b> 을 입력합니다.

옵션	샘플 입력
<b>Bind DN</b>	사용자를 검색할 권한이 있는 Active Directory 사용자 계정의 CN(일반 이름)을 포함하여 전체 DN(고유 이름)을 입력합니다. 예를 들어 <b>cn=config_admin infra,cn=users,dc=rainpole,dc=local</b> 을 입력합니다.
<b>Bind DN 암호</b>	사용자를 검색할 수 있는 계정의 Active Directory 암호를 입력하고 <b>연결 테스트</b> 를 클릭하여, 구성된 디렉토리에 대한 연결을 테스트합니다.

#### ◆ 네이티브 Active Directory

옵션	샘플 입력
<b>디렉토리 이름</b>	고유한 디렉토리 이름을 입력합니다. 네이티브 Active Directory를 사용하는 경우 <b>Active Directory(Windows 통합 인증)</b> 를 선택합니다.
<b>도메인 이름</b>	가입할 도메인의 이름을 입력합니다.
<b>도메인 관리자 사용자 이름</b>	도메인 관리자의 사용자 이름을 입력합니다.
<b>도메인 관리자 암호</b>	도메인 관리자 계정의 암호를 입력합니다.
<b>Bind 사용자 UPN</b>	도메인에서 인증될 수 있는 사용자의 이름을 이메일 주소 형식을 사용하여 입력합니다.
<b>Bind DN 암호</b>	사용자를 검색할 수 있는 계정에 대한 Active Directory Bind 계정 암호를 입력합니다.


#### 4 저장 및 다음을 클릭합니다.

**도메인 선택** 페이지에 도메인 목록이 표시됩니다.

#### 5 기본 도메인 설정을 수락하고 다음을 클릭합니다.

#### 6 특성 이름이 올바른 Active Directory 특성에 매핑되어 있는지 확인하고 다음을 클릭합니다.

#### 7 동기화할 그룹과 사용자를 선택합니다.

a **새로 만들기** 아이콘 을 클릭합니다.

b 사용자 도메인을 입력하고 **그룹 찾기**를 클릭합니다.

예를 들어 **dc=vcac,dc=local**을 입력합니다.

c 동기화할 그룹을 선택하려면 **선택**을 클릭하고 **다음**을 클릭합니다.

d **사용자 선택** 페이지에서 동기화할 사용자를 선택하고 **다음**을 클릭합니다.

vRealize Automation을 사용해야 하는 사용자 및 그룹만 추가합니다. 중첩 구조의 모든 그룹에서 vRealize Automation을 사용해야 하는 경우가 아니면 **중첩된 그룹 동기화**를 선택하지 마십시오.

#### 8 디렉토리에 동기화 중인 사용자 및 그룹을 검토하고 **디렉토리 동기화**를 클릭합니다.

디렉토리 동기화에 시간이 걸리며 백그라운드에서 실행됩니다.

**9 관리 > 디렉토리 관리 > ID 제공자**를 선택하고 새 ID 제공자를 클릭합니다.

예: **WorkspaceIDP\_\_1**.

**10** 선택한 ID 제공자에 대한 페이지에서 각 노드에 커넥터를 추가합니다.

- a 커넥터 추가에 대한 지침을 따릅니다.
- b vRealize Automation 로드 밸런서의 FQDN(정규화된 도메인 이름)을 가리키도록 **IdP 호스트 이름** 속성의 값을 업데이트합니다.
- c **저장**을 클릭합니다.

다음에 수행할 작업

[소스 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행.](#)

소스 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행

마이그레이션하기 전에 소스 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행해야 합니다.

이 데이터 수집은 7.1.x 이상에서 마이그레이션하는 경우 vRealize Automation에서 로드 밸런서 재구성 작업을 수행하는 데 필요합니다.

---

**참고** vRealize Automation 6.2.x에서 마이그레이션할 때 소스 환경에서 이 데이터 수집을 실행할 필요가 없습니다. vRealize Automation 6.2.x는 [로드 밸런서 재구성] 작업을 지원하지 않습니다.

---

절차

- ◆ vRealize Automation 마이그레이션 이전에 소스 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행합니다. 자세한 내용은 [끝점 데이터 수집 수동 시작](#) 항목을 참조하십시오.

다음에 수행할 작업

[수동으로 소스 vRealize AutomationIaaS Microsoft SQL 데이터베이스 복제.](#)

수동으로 소스 vRealize AutomationIaaS Microsoft SQL 데이터베이스 복제

마이그레이션을 시작하기 전에 vRealize Automation 소스 환경의 IaaS Microsoft SQL 데이터베이스를 백업한 후 vRealize Automation 대상 환경에 새로 생성된 빈 데이터베이스에 복원해야 합니다.

사전 요구 사항

- [소스 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행.](#)
- SQL Server 데이터베이스 백업 및 복원에 대한 정보를 가져옵니다. 전체 SQL Server 데이터베이스 백업을 생성하고 SQL Server 데이터베이스를 새 위치에 복원하는 데 대한 문서를 [Microsoft Developer Network](#)에서 검색합니다.

## 절차

- ◆ 소스 vRealize AutomationlaaS Microsoft SQL 데이터베이스의 전체 백업을 생성합니다. 이 백업을 사용하여 대상 환경의 새로 생성된 빈 데이터베이스에 SQL 데이터베이스를 복원합니다.

다음에 수행할 작업

대상 vRealize Automation 환경의 스냅샷 생성.

### 대상 vRealize Automation 환경의 스냅샷 생성

각 대상 vRealize Automation 가상 시스템의 스냅샷을 생성합니다. 마이그레이션이 실패하면 가상 시스템 스냅샷을 사용하여 마이그레이션을 다시 시도할 수 있습니다.

자세한 내용은 vSphere 설명서를 참조하십시오.

사전 요구 사항

수동으로 소스 vRealize AutomationlaaS Microsoft SQL 데이터베이스 복제.

다음에 수행할 작업

다음 절차 중 하나를 수행합니다.

- vRealize Automation 소스 데이터를 vRealize Automation 최소 환경으로 마이그레이션.
- vRealize Automation 소스 데이터를 vRealize Automation 고가용성 환경으로 마이그레이션.

### Postgres 데이터베이스 정리

업그레이드 또는 마이그레이션을 위해 Postgres 데이터베이스를 준비하려면 데이터베이스 정리를 수행하십시오.

로그 및 원격 분석 번들을 저장하는 pg\_largeobject 테이블의 큰 개체와 애플리케이션 개체는 업그레이드 또는 마이그레이션을 느리게 하거나 중지할 수 있습니다. 업그레이드 또는 마이그레이션을 시도하기 전에 vacuum 데이터베이스 정리를 수행하여 Postgres 데이터베이스를 준비할 수 있습니다.

---

**참고** 서비스가 실행 중일 때는 데이터베이스 정리를 수행할 수 없습니다.

---

## 절차

- 1 VAMI의 클러스터 페이지에서 Postgres 데이터베이스 덤프를 생성하거나 마스터 가상 장치의 백업/스냅샷을 생성하여 장치 백업부터 시작합니다.
- 2 vRA VAMI에서 복제를 동기화에서 비동기로 전환합니다.
- 3 마스터 vRA의 Postgres 사용자(su-postgres)로, 데이터베이스에 vacuum을 실행하여 로그 항목을 제거합니다.

```
su - postgres -c "/opt/vmware/vpostgres/current/bin/vacuumlo -v -p 5432 vcac"
```

```
su - postgres -c "/opt/vmware/vpostgres/current/bin/vacuumdb -f -p 5432 -t pg_largeobject -t pg_largeobject_metadata vcac"
```



**4** 데이터베이스 공간을 회수하려면 `vacuum full` 명령을 사용합니다.

```
psql -d vcac
vacuum full
vacuum analyze
```

중복된 테넌트 이름이 있는 개체 정리

vRealize Automation 7.x로 마이그레이션하기 전에 중복된 테넌트 이름이 있는 개체를 정리해야 합니다.

중복된 테넌트 이름이 있는 개체를 정리하려면 [KB 58002](#)에 설명된 단계를 따르십시오.

중복된 vRealize Orchestrator 리소스 및 데이터베이스 항목 정리

vRealize Automation 7.x로 마이그레이션하기 전에 중복된 vRealize Orchestrator 리소스 및 데이터베이스 항목을 정리해야 합니다.

중복된 vRealize Orchestrator 리소스 및 데이터베이스 항목을 정리하려면 [KB 54987](#)에 설명된 단계를 따르십시오.

**vRealize Automation 대상에서 HF 테이블 백업**

vRealize Automation 7.x로 마이그레이션하기 전에 vRealize Automation 대상 환경에서 HF 테이블을 백업해야 합니다.

vRealize Automation 7.x 환경에 HF를 적용한 경우 마이그레이션 전에 HF 테이블을 백업하고 마이그레이션 후 복원해야 합니다.

다음은 수행하여 HF 테이블을 백업합니다.

```
mkdir /tmp/hf_tables
/opt/vmware/vpostgres/current/bin/pg_dump -U postgres --data-only -d vcac -t public.hf_patch > /tmp/hf_tables/hf_patch.sql
/opt/vmware/vpostgres/current/bin/pg_dump -U postgres --data-only -d vcac -t public.hf_patch_execution > /tmp/hf_tables/hf_patch_execution.sql
/opt/vmware/vpostgres/current/bin/pg_dump -U postgres --data-only -d vcac -t public.hf_patch_nodes > /tmp/hf_tables/hf_patch_nodes.sql
cd /tmp/hf_tables/
zip -r /tmp/hf_tables.zip ./
```

새로 생성된 `hf_tables.zip` 파일을 백업합니다.

마이그레이션 후 HF 테이블 복원에 대한 자세한 내용은 [vRealize Automation 대상에서 HF 테이블 복원](#) 항목을 참조하십시오.

## 마이그레이션 절차

소스 vRealize Automation 환경 데이터를 마이그레이션하기 위해 수행하는 절차는 최소 환경으로 마이그레이션하는지 아니면 고가용성 환경으로 마이그레이션하는지에 따라 다릅니다.

## vRealize Automation 소스 데이터를 vRealize Automation 최소 환경으로 마이그레이션

현재 vRealize Automation 환경 데이터를 새로운 vRealize Automation 릴리스로 마이그레이션할 수 있습니다.

소스 시스템의 모든 테넌트는 대상에서 다시 생성해야 하고 ID 저장소 마이그레이션 절차를 수행해야 합니다. 자세한 내용은 [ID 저장소를 VMware Identity Manager로 마이그레이션](#) 항목을 참조하십시오.

### 사전 요구 사항

- [마이그레이션에 필요한 정보 수집](#).
- 소스 vRealize Automation 환경에서 암호화 키 가져오기.
- 소스 vRealize Automation 환경에서 대상 환경으로 각 테넌트 추가.
- 추가된 각 테넌트에 대해 관리자 생성.
- 최소 환경으로 마이그레이션하기 전에 [Active Directory 링크의 사용자와 그룹 동기화](#).
- 수동으로 소스 vRealize AutomationIaaS Microsoft SQL 데이터베이스 복제.
- 대상 vRealize Automation 환경의 스냅샷 생성.
- 대상 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 루트로 대상 vRealize Automation 장치 관리에 로그인합니다.

### 절차

- 1 마이그레이션을 선택합니다.
- 2 소스 vRealize Automation 장치에 대해 정보를 입력합니다.

옵션	설명
호스트 이름	소스 vRealize Automation 장치의 호스트 이름입니다.
루트 사용자 이름	root
루트 암호	vRealize Automation 장치를 배포할 때 입력한 루트 암호입니다.
마이그레이션 패키지 위치	마이그레이션 패키지가 생성되는 소스 vRealize Automation 장치의 기존 디렉토리 경로입니다.

- 3 대상 vRealize Automation 장치에 대해 정보를 입력합니다.

옵션	설명
루트 사용자 이름	root
루트 암호	대상 vRealize Automation 장치를 배포할 때 입력한 루트 암호입니다.
기본 테넌트	vsphere.local 이 필드를 수정할 수 없습니다.

옵션	설명
관리자 사용자 이름	관리자 이 필드를 수정할 수 없습니다.
관리자 암호	대상 vRealize Automation 환경을 배포할 때 입력한 administrator@vsphere.local 사용자 암호입니다.

#### 4 대상 IaaS 데이터베이스 서버에 대한 정보를 입력합니다.

옵션	설명
데이터베이스 서버	복원된 vRealize Automation IaaS Microsoft SQL 데이터베이스가 상주하는 Microsoft SQL Server의 위치입니다. 명명된 인스턴스와 기본이 아닌 포트가 사용 되는 경우 <code>SERVER,PORT\INSTANCE-NAME</code> 형식으로 입력합니다. AAG(AlwaysOn 가용성 그룹)를 사용하도록 대상 Microsoft SQL Server를 구성하 는 경우, 포트 또는 인스턴스 이름 없이 대상 SQL Server를 AAG 수신기 이름으로 입력해야 합니다.
복제된 데이터베이스 이름	소스에서 백업하고 대상 환경에서 복원한 소스 vRealize Automation IaaS Microsoft SQL 데이터베이스의 이름입니다.
인증 모드	<div> <div>■ Windows</div> <div>Windows 인증 모드를 사용하는 경우 IaaS 서비스 사용자에게는 SQL Server db_owner 역할이 있어야 합니다. SQL Server 인증 모드를 사용할 때 동일한 사용 권한이 적용됩니다.</div> </div> <div> <div>■ SQL Server</div> <div>SQL Server에 로그인 이름 및 암호 텍스트 상자가 열립니다.</div> </div>
로그인 이름	복제된 IaaS Microsoft SQL 데이터베이스에 대해 db_owner 역할을 가진 SQL Server 사용자의 로그인 이름입니다.
암호	복제된 IaaS Microsoft SQL 데이터베이스에 대해 db_owner 역할을 가진 SQL Server 사용자의 암호입니다.
원본 암호화 키	소스 환경에서 검색한 원본 암호화 키입니다. <a href="#">소스 vRealize Automation 환경에서 암호화 키 가져오기</a> 항목을 참조하십시오.
새 암호	새 암호화 키를 생성하는 데 사용되는 일련의 단어입니다. 대상 vRealize Automation 환경에서 새 IaaS 구성 요소를 설치할 때마다 이 암호를 사용합니다.

#### 5 검증을 클릭합니다.

이 페이지는 검증 진행률을 표시합니다.

- 항목 검증에 실패할 경우 IaaS 노드에서 오류 메시지와 검증 로그 파일을 확인합니다. 로그 파일  
위치는 [마이그레이션 로그 위치](#) 항목을 참조하십시오. **설정 편집**을 클릭하고 문제 항목을 편집합  
니다.

#### 6 마이그레이션을 클릭합니다.

이 페이지는 마이그레이션 진행률을 표시합니다.

- 마이그레이션이 성공한 경우 모든 마이그레이션 작업이 완료된 것으로 페이지에 표시됩니다.

- 마이그레이션이 실패한 경우 가상 장치 및 IaaS 노드에서 마이그레이션 로그 파일을 검사합니다. 로그 파일 위치는 [마이그레이션 로그 위치](#) 항목을 참조하십시오.

마이그레이션을 다시 시작하기 전에 다음 단계를 완료합니다.

- a 마이그레이션 전에 스냅샷을 생성할 때 캡처한 상태로 대상 vRealize Automation 환경을 되돌립니다.
- b 소스 IaaS 데이터베이스의 백업을 사용하여 대상 IaaS Microsoft SQL 데이터베이스를 복원합니다.

다음에 수행할 작업

[사후 마이그레이션 작업](#).

**vRealize Automation 소스 데이터를 vRealize Automation 고가용성 환경으로 마이그레이션**

현재 vRealize Automation 환경 데이터를 고가용성 환경으로 구성된 새로운 vRealize Automation 릴리스로 마이그레이션할 수 있습니다.

소스 시스템의 모든 테넌트는 대상에서 다시 생성해야 하고 ID 저장소 마이그레이션 절차를 수행해야 합니다. 자세한 내용은 [ID 저장소를 VMware Identity Manager로 마이그레이션](#) 항목을 참조하십시오.

사전 요구 사항

- 마이그레이션에 필요한 정보 수집.
- 소스 vRealize Automation 환경에서 암호화 키 가져오기.
- 소스 vRealize Automation 환경에서 대상 환경으로 각 테넌트 추가.
- 추가된 각 테넌트에 대해 관리자 생성.
- 고가용성 환경으로 마이그레이션하기 전에 Active Directory 링크의 사용자와 그룹 동기화.
- 수동으로 소스 vRealize Automation IaaS Microsoft SQL 데이터베이스 복제.
- 대상 vRealize Automation 환경의 스냅샷 생성.
- 대상 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 루트로 대상 vRealize Automation 장치 관리에 로그인합니다.

절차

- 1 **마이그레이션**을 선택합니다.
- 2 소스 vRealize Automation 장치에 대한 정보를 입력합니다.

옵션	설명
호스트 이름	소스 vRealize Automation 장치의 호스트 이름입니다.
루트 사용자 이름	root
루트 암호	소스 vRealize Automation 장치를 배포할 때 입력한 루트 암호입니다.

### 3 소스 vRealize Automation 장치의 마이그레이션 패키지 위치에 대한 정보를 입력합니다.

옵션	설명
마이그레이션 패키지 위치	마이그레이션 패키지가 생성되는 소스 vRealize Automation 장치의 기존 디렉토리 경로입니다.

### 4 대상 vRealize Automation 장치에 대해 정보를 입력합니다.

옵션	설명
루트 사용자 이름	root
루트 암호	대상 vRealize Automation 장치를 배포할 때 입력한 루트 암호입니다.
기본 테넌트	vsphere.local
관리자 사용자 이름	관리자
관리자 암호	대상 vRealize Automation 환경을 배포할 때 입력한 administrator@vsphere.local 사용자 암호입니다.

### 5 대상 IaaS 데이터베이스 서버에 대한 정보를 입력합니다.

옵션	설명
데이터베이스 서버	복원된 vRealize AutomationIaaS Microsoft SQL 데이터베이스가 상주하는 Microsoft SQL Server 인스턴스의 위치입니다. 명명된 인스턴스와 기본이 아닌 포트가 사용되는 경우 <code>SERVER,PORT\INSTANCE-NAME</code> 형식으로 입력합니다. AAG(AlwaysOn 가용성 그룹)를 사용하도록 대상 Microsoft SQL Server를 구성하는 경우, 포트 또는 인스턴스 이름 없이 대상 SQL Server를 AAG 수신기 이름으로 입력해야 합니다.
복제된 데이터베이스 이름	소스에서 백업하고 대상 환경에서 복원한 소스 vRealize AutomationIaaS Microsoft SQL 데이터베이스의 이름입니다.
인증 모드	<div> <div>■ Windows</div> <div>Windows 인증 모드를 사용하는 경우 IaaS 서비스 사용자에게는 SQL Server db_owner 역할이 있어야 합니다. SQL Server 인증 모드를 사용할 때 동일한 사용 권한이 적용됩니다.</div> </div> <div> <div>■ SQL Server</div> <div>SQL Server에 로그인 이름 및 암호 텍스트 상자가 열립니다.</div> </div>
로그인 이름	복제된 IaaS Microsoft SQL 데이터베이스에 대해 db_owner 역할을 가진 SQL Server 사용자의 로그인 이름입니다.
암호	복제된 IaaS Microsoft SQL 데이터베이스에 대해 db_owner 역할을 가진 SQL Server 사용자의 암호입니다.
원본 암호화 키	소스 환경에서 검색한 원본 암호화 키입니다. <a href="#">소스 vRealize Automation 환경에서 암호화 키 가져오기</a> 항목을 참조하십시오.
새 암호	새 암호화 키를 생성하는 데 사용되는 일련의 단어입니다. 대상 vRealize Automation 환경에서 새 IaaS 구성 요소를 설치할 때마다 이 암호를 사용합니다.

## 6 검증을 클릭합니다.

이 페이지는 검증 진행률을 표시합니다.

- 항목 검증에 실패할 경우 IaaS 노드에서 오류 메시지와 검증 로그 파일을 확인합니다. 로그 파일 위치는 [마이그레이션 로그 위치](#) 항목을 참조하십시오. **설정 편집**을 클릭하고 문제 항목을 편집합니다.

## 7 마이그레이션을 클릭합니다.

이 페이지는 마이그레이션 진행률을 표시합니다.

- 마이그레이션이 성공한 경우 모든 마이그레이션 작업이 완료된 것으로 페이지에 표시됩니다.
- 마이그레이션이 실패한 경우 가상 장치 및 IaaS 노드에서 마이그레이션 로그 파일을 검사합니다. 로그 파일 위치는 [마이그레이션 로그 위치](#) 항목을 참조하십시오.

마이그레이션을 다시 시작하기 전에 다음 단계를 완료합니다.

- 마이그레이션 전에 스냅샷을 생성할 때 캡처한 상태로 대상 vRealize Automation 환경을 되돌립니다.
- 소스 IaaS 데이터베이스의 백업을 사용하여 대상 IaaS Microsoft SQL 데이터베이스를 복원합니다.

다음에 수행할 작업

[사후 마이그레이션 작업](#).

## 사후 마이그레이션 작업

vRealize Automation을 마이그레이션한 후에 상황과 관련된 마이그레이션 후 작업을 수행합니다.

---

**참고** ID 저장소를 마이그레이션한 후 vRealize Code Stream의 사용자는 수동으로 vRealize Code Stream 역할을 재할당해야 합니다.

---

### vRealize Automation 표준 시간대 변경 안 함

vRealize Automation 장치 관리 인터페이스에 표준 시간대를 변경할 수 있는 옵션이 제공되지만, vRealize Automation 표준 시간대는 항상 Etc/UTC로 설정해 두어야 합니다.

Etc/UTC 이외의 표준 시간대를 사용하면 실패한 마이그레이션 및 모든 vRealize Automation 노드의 항목이 포함되지 않은 로그 번들 등과 같은 비정상적인 오류가 발생하는 것으로 알려져 있습니다.

피해야 하는 vRealize Automation 장치 관리 인터페이스 옵션은 **시스템 > 표준 시간대** 아래에 있습니다.

### 소스 vRealize Automation 6.2.x 환경의 테넌트 및 IaaS 관리자 추가

마이그레이션 후 각 테넌트의 vRealize Automation 6.2.x 테넌트 관리자를 삭제하고 복원해야 합니다.

대상 vRealize Automation 콘솔에서 각 테넌트에 대해 다음 절차를 수행합니다.

---

**참고** vRealize Automation 7.x 환경에서 마이그레이션한 경우에는 이 절차를 수행하지 않아도 됩니다.

---

## 사전 요구 사항

- vRealize Automation의 최신 버전으로 마이그레이션을 완료합니다.
- 대상 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **관리자**로 대상 vRealize Automation 콘솔에 로그인합니다.

## 절차

- 1 **관리 > 테넌트**를 선택합니다.
- 2 테넌트 이름을 클릭합니다.
- 3 **관리자**를 클릭합니다.
- 4 각 테넌트 관리자 이름 및 사용자 이름이 포함된 목록을 만듭니다.
- 5 각 관리자를 가리킨 후 삭제 아이콘([삭제])을 클릭합니다. 모든 관리자를 삭제할 때까지 이 작업을 반복합니다.
- 6 **완료**를 클릭합니다.
- 7 [테넌트] 페이지에서 테넌트 이름을 다시 클릭합니다.
- 8 **관리자**를 클릭합니다.
- 9 앞서 삭제한 각 사용자의 이름을 적절한 검색 상자에 입력하고 **Enter** 키를 누릅니다.
- 10 검색 결과에서 적절한 사용자의 이름을 클릭하여 해당 사용자를 관리자로 다시 추가합니다.  
작업을 마치면 테넌트 관리자 목록이 삭제한 관리자 목록과 동일하게 보입니다.
- 11 **완료**를 클릭합니다.

## 연결 테스트 실행 및 마이그레이션된 끝점 확인

vRealize Automation 마이그레이션 시 대상 vRealize Automation 환경에서 끝점이 변경됩니다.

vRealize Automation 마이그레이션 이후에는 적용 가능한 모든 끝점에 대해 **연결 테스트** 작업을 사용해야 합니다. 마이그레이션된 일부 끝점을 수정해야 할 수도 있습니다. 자세한 내용은 [업그레이드 또는 마이그레이션된 끝점 사용 시 고려 사항](#)을 참조하십시오.

업그레이드 또는 마이그레이션된 끝점의 기본 보안 설정은 신뢰할 수 없는 인증서를 허용하지 않는 것입니다.

신뢰할 수 없는 인증서를 사용하고 있는 경우에는 이전 버전의 vRealize Automation 설치에서 업그레이드 또는 마이그레이션한 후 인증서 검증을 사용하도록 모든 vSphere 및 NSX 끝점에 대해 다음 단계를 수행해야 합니다. 그렇지 않으면 인증서 오류가 발생하고 끝점 작업이 실패합니다. 자세한 내용은 <http://kb.vmware.com/kb/2150230>의 VMware 기술 자료 문서 "vRA 7.3으로 업그레이드 후 끝점 통신이 끊김(2150230)" 및 <http://kb.vmware.com/kb/2108294>의 "웹 브라우저 인증서 주의를 방지하도록 vCenter Server 루트 인증서를 다운로드 및 설치하는 방법(2108294)"을 참조하십시오.

- 1 업그레이드 또는 마이그레이션 후에 vRealize Automation vSphere 에이전트 시스템에 로그인하고 **서비스** 탭을 사용하여 vSphere 에이전트를 다시 시작합니다.

마이그레이션이 모든 에이전트를 다시 시작하지 못할 수 있으므로 필요한 경우 에이전트를 수동으로 다시 시작합니다.

- 2 적어도 하나 이상의 ping 보고가 완료될 때까지 기다립니다. ping 보고가 완료되려면 1~2분 정도가 소요됩니다.
- 3 vSphere 에이전트가 데이터 수집을 시작하면 vRealize Automation에 IaaS 관리자로 로그인합니다.
- 4 **인프라 > 끝점 > 끝점**을 클릭합니다.
- 5 vSphere 끝점을 편집하고 **연결 테스트**를 클릭합니다.
- 6 인증서 프롬프트가 표시되면 **확인**을 클릭하여 인증서를 수락합니다.  
인증서 프롬프트가 표시되지 않으면 현재 끝점에 대한 Windows 시스템 호스팅 서비스의 신뢰할 수 있는 루트 인증 기관(예: 프록시 에이전트 시스템 또는 DEM 시스템)에 인증서가 올바르게 저장되어 있을 수 있습니다.
- 7 **확인**을 클릭하여 인증서 수락을 적용하고 끝점을 저장합니다.
- 8 각 vSphere 끝점에 대해 이 절차를 반복합니다.
- 9 각 NSX 끝점에 대해 이 절차를 반복합니다.
- 10 **인프라 > 계산 리소스**로 이동하여 **vCenter 계산** 리소스를 마우스 오른쪽 버튼으로 클릭하고 **데이터 수집**을 실행합니다.

**연결 테스트** 작업이 성공해도 일부 데이터 수집 또는 프로비저닝 작업이 실패하면 끝점 역할을 하는 모든 에이전트 시스템과 모든 DEM 시스템에 동일한 인증서를 설치할 수 있습니다. 또는 기존 시스템에서 인증서를 제거하고 실패한 끝점에 대해 이전 절차를 반복할 수 있습니다.

#### 대상 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행

마이그레이션 후 대상 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행해야 합니다.

이 데이터 수집은 마이그레이션 후 대상 vRealize Automation 환경에서 로드 밸런서 재구성 작업을 수행하는 데 필요합니다.

---

**참고** vRealize Automation 6.2.x에서 마이그레이션한 경우에는 이 데이터 수집을 수행할 필요가 없습니다.

---

#### 사전 요구 사항

- **소스 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집 실행.**
- **대상 vRealize Automation 환경으로 마이그레이션을 완료합니다**

.



## 절차

- ◆ vRealize Automation로 마이그레이션하기 전에 대상 vRealize Automation 환경에서 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행합니다. 자세한 내용은 "vRealize Automation 관리"에서 [끝점 데이터 수집 수동 시작](#) 항목을 참조하십시오.

## 고가용성 환경으로 마이그레이션한 후 로드 밸런서 재구성

고가용성 환경으로 마이그레이션할 때는 마이그레이션을 완료한 후 각 로드 밸런서에 대해 이러한 작업을 수행해야 합니다.

## 사전 요구 사항

[vRealize Automation 소스 데이터](#)를 vRealize Automation 고가용성 환경으로 마이그레이션.

## 절차

- 1 다음 항목에 대해 로드 밸런서를 구성하여 복제 노드가 수신 트래픽을 수용하도록 원래 상태 점검 설정을 복원합니다.
  - vRealize Automation 장치
  - Model Manager를 호스팅하는 IaaS 웹 서버
  - Manager Service
- 2 로드 밸런서 시간 초과 설정을 다시 기본값으로 변경합니다.

## 외부 vRealize Orchestrator 서버를 대상 vRealize Automation으로 마이그레이션

기존 외부 vRealize Orchestrator 서버를 vRealize Automation에 포함된 vRealize Orchestrator 인스턴스로 마이그레이션할 수 있습니다.

## 사전 요구 사항

vRealize Automation의 대상 버전으로 마이그레이션을 완료합니다.

관련 정보는 [vRealize Orchestrator 제품 설명서](#)에서 "vRealize Automation에 외부 Orchestrator 서버 마이그레이션"을 참조하십시오.

## 대상 vRealize Orchestrator에서 vRealize Automation 끝점 재구성

포함된 대상 vRealize Orchestrator에서 vRealize Automation 끝점을 재구성하려면 다음 절차를 따릅니다.

## 사전 요구 사항

- vRealize Automation의 최신 버전으로 마이그레이션을 완료합니다.
- vRealize Orchestrator 클라이언트를 사용하여 대상 vRealize Orchestrator에 연결합니다. 자세한 내용은 [vRealize Orchestrator 설명서](#)에서 "VMware vRealize Orchestrator Client 사용" 항목을 참조하십시오.

## 절차

- 1 상단 드롭다운 메뉴에서 **설계**를 선택합니다.
- 2 **인벤토리**를 클릭합니다.
- 3 **vRealize Automation**을 확장합니다.
- 4 최소 환경에서 마이그레이션한 경우 소스 vRealize Automation 장치 호스트의 FQDN(정규화된 도메인 이름)이 포함된 끝점을 식별합니다. 고가용성 환경에서 마이그레이션한 경우라면 소스 장치 로드 밸런서의 FQDN이 포함된 끝점을 식별합니다.

FQDN이 포함된 끝점을 찾았다면 다음 단계를 완료합니다.	FQDN이 포함된 끝점을 찾지 못했다면 다음 단계를 완료합니다.
<ol style="list-style-type: none"> <li>1 워크플로를 클릭합니다.</li> <li>2 확장 버튼을 클릭하고 <b>라이브러리 &gt; vRealize Automation &gt; 구성</b>을 선택합니다.</li> <li>3 다음 단계 중 하나를 수행합니다. <ul style="list-style-type: none"> <li>■ 최소 환경에서 마이그레이션한 경우 소스 vRealize Automation 장치 호스트의 FQDN을 포함하는 모든 끝점에 대해 <b>vRA 호스트 제거</b> 워크플로를 실행합니다.</li> <li>■ 고가용성 환경에서 마이그레이션한 경우 소스 장치 로드 밸런서의 FQDN을 포함하는 모든 끝점에 대해 <b>vRA 호스트 제거</b> 워크플로를 실행합니다.</li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li>1 <b>리소스</b>를 클릭합니다.</li> <li>2 상단 도구 모음에서 업데이트 아이콘을 클릭합니다.</li> <li>3 확장 버튼을 클릭하고 <b>라이브러리 &gt; vCACCAFE &gt; 구성</b>을 선택합니다.</li> <li>4 다음 단계 중 하나를 수행합니다. <ul style="list-style-type: none"> <li>■ 최소 환경에서 마이그레이션한 경우 소스 vRealize Automation 장치 호스트의 FQDN을 포함하는 URL 속성을 가진 각 리소스를 삭제합니다.</li> <li>■ 고가용성 환경에서 마이그레이션한 경우 소스 vRealize Automation 장치 로드 밸런서의 FQDN을 포함하는 URL 속성을 가진 각 리소스를 삭제합니다.</li> </ul> </li> </ol>

- 5 워크플로를 클릭합니다.
- 6 확장 버튼을 클릭하고 **라이브러리 > vRealize Automation > 구성**을 선택합니다.
- 7 대상 vRealize Automation 장치 호스트 또는 고가용성 배포로 마이그레이션한 경우 로드 밸런싱된 호스트를 추가하려면 **구성 요소 레지스트리를 사용하여 vRA 호스트 추가** 워크플로를 실행합니다.

## 대상 vRealize Orchestrator에서 vRealize Automation 인프라 끝점 재구성

포함된 대상 vRealize Orchestrator에서 vRealize Automation 인프라 끝점을 재구성하려면 다음 절차를 따릅니다.

## 사전 요구 사항

- vRealize Automation의 최신 버전으로 마이그레이션을 완료합니다.
- vRealize Orchestrator 클라이언트를 사용하여 대상 vRealize Orchestrator에 연결합니다. 자세한 내용은 [vRealize Orchestrator 설명서](#)에서 "VMware vRealize Orchestrator Client 사용" 항목을 참조하십시오.

## 절차

- 1 상단 드롭다운 메뉴에서 **설계**를 선택합니다.
- 2 **인벤토리**를 클릭합니다.

### 3 vRealize Automation 인프라를 확장합니다.

- 4 최소 환경에서 마이그레이션한 경우 소스 vRealize Automation 인프라 호스트의 FQDN(정규화된 도메인 이름)이 포함된 끝점을 식별합니다. 고가용성 환경에서 마이그레이션한 경우라면 소스 장치 로드 밸런서의 FQDN이 포함된 끝점을 식별합니다.

FQDN이 포함된 끝점을 찾았다면 다음 단계를 완료합니다.	FQDN이 포함된 끝점을 찾지 못했다면 다음 단계를 완료합니다.
<ol style="list-style-type: none"> <li>1 워크플로를 클릭합니다.</li> <li>2 확장 버튼을 클릭하고 라이브러리 &gt; vRealize Automation &gt; 인프라 관리 &gt; 구성을 선택합니다.</li> <li>3 다음 단계 중 하나를 수행합니다. <ul style="list-style-type: none"> <li>■ 최소 환경에서 마이그레이션한 경우 소스 vRealize Automation 인프라 호스트의 FQDN을 포함하는 모든 끝점에 대해 <b>IaaS 호스트 제거</b> 워크플로를 실행합니다.</li> <li>■ 고가용성 환경에서 마이그레이션한 경우 소스 vRealize Automation 인프라 호스트 로드 밸런서의 FQDN을 포함하는 모든 끝점에 대해 <b>IaaS 호스트 제거</b> 워크플로를 실행합니다.</li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li>1 리소스를 클릭합니다.</li> <li>2 상단 도구 모음에서 업데이트 아이콘을 클릭합니다.</li> <li>3 확장 버튼을 클릭하고 라이브러리 &gt; vCAC &gt; 구성을 선택합니다.</li> <li>4 다음 단계 중 하나를 수행합니다. <ul style="list-style-type: none"> <li>■ 최소 환경에서 마이그레이션한 경우 소스 vRealize Automation 인프라 호스트의 FQDN을 포함하는 host 속성을 가진 각 리소스를 삭제합니다.</li> <li>■ 고가용성 환경에서 마이그레이션한 경우 소스 vRealize Automation 인프라 호스트 로드 밸런서의 FQDN을 포함하는 host 속성을 가진 각 리소스를 삭제합니다.</li> </ul> </li> </ol>

### 5 워크플로를 클릭합니다.

### 6 확장 버튼을 클릭하고 라이브러리 > vRealize Automation > 구성을 선택합니다.

- 7 대상 vRealize Automation 인프라 호스트를 추가하려면 또는 고가용성 배포 로드 밸런싱된 호스트로 마이그레이션한 경우 **vRA 호스트의 IaaS 호스트 추가** 워크플로를 실행합니다.

### vRealize Orchestrator 사용자 지정 설치

사용자 지정된 상태 변경 워크플로 스텝과 vRealize Orchestrator 메뉴 작업 워크플로를 설치하는 워크플로를 실행할 수 있습니다.

자세한 내용은 [vRealize Orchestrator 사용자 지정 설치](#) 항목을 참조하십시오.

### 사전 요구 사항

vRealize Automation의 최신 버전으로 마이그레이션을 완료합니다.

### 대상 vRealize Automation에서 포함된 vRealize Orchestrator 인프라 끝점 재구성

vRealize Automation 6.2.5 환경에서 마이그레이션하는 경우에는 내장형 대상 vRealize Orchestrator 서버를 가리키는 인프라 끝점의 URL을 업데이트해야 합니다.

### 사전 요구 사항

- vRealize Automation의 대상 vRealize Automation 릴리스로 마이그레이션을 완료합니다.
- 대상 vRealize Automation 콘솔에 로그인합니다.
  - a 대상 가상 장치의 정규화된 도메인 이름(<https://vra-va-hostname.domain.name/vcac>)을 사용하여 vRealize Automation 콘솔을 엽니다.

고가용성 환경인 경우, 대상 가상 장치 로드 밸런서의 정규화된 도메인 이름(<https://vra-vb-hostname.domain.name/vcac>)을 사용하여 콘솔을 엽니다.

- b laaS 관리자 사용자로 로그인합니다.

#### 절차

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.
- 2 [끝점] 페이지에서 vRealize Orchestrator 끝점을 선택하고 **편집**을 클릭합니다.
- 3 [주소] 텍스트 상자에서 vRealize Orchestrator 끝점 URL을 편집합니다.
  - 최소 환경으로 마이그레이션한 경우, vRealize Orchestrator 끝점 URL을 <https://vra-vb-hostname.domain.name:443/vco>으로 바꿉니다.
  - 고가용성 환경으로 마이그레이션한 경우, vRealize Orchestrator 끝점 URL을 <https://vra-vb-lb-hostname.domain.name:443/vco>으로 바꿉니다.
- 4 **확인**을 클릭합니다.
- 5 vRealize Orchestrator 끝점에서 데이터 수집을 수동으로 실행합니다.
  - a [끝점] 페이지에서 vRealize Orchestrator 끝점을 선택합니다.
  - b **작업 > 데이터 수집**을 선택합니다.

데이터 수집이 완료되었는지 확인합니다.

대상 vRealize Automation 환경에서 Microsoft Azure 끝점 재구성

마이그레이션 이후 Microsoft Azure 끝점을 재구성해야 합니다.

Microsoft Azure 끝점 각각에 대해 이 절차를 수행합니다.

#### 사전 요구 사항

- 대상 버전의 vRealize Automation로 마이그레이션을 완료합니다.
- 대상 vRealize Automation 콘솔에 로그인합니다.
  - a 대상 가상 장치의 정규화된 도메인 이름(<https://vra-vb-hostname.domain.name/vcac>)을 사용하여 vRealize Automation 콘솔을 엽니다.
 

고가용성 환경인 경우, 대상 가상 장치 로드 밸런서의 정규화된 도메인 이름(<https://vra-vb-lb-hostname.domain.name/vcac>)을 사용하여 콘솔을 엽니다.
  - b laaS 관리자 사용자로 로그인합니다.

#### 절차

- 1 **관리 > vRO 구성 > 끝점**을 선택합니다.
- 2 Microsoft Azure 끝점을 선택합니다.
- 3 **편집**을 클릭합니다.

- 4 세부 정보를 클릭합니다.
- 5 Azure 환경 드롭다운 메뉴에서 영역을 선택합니다.
- 6 클라이언트 암호 텍스트 상자에 원래 클라이언트 암호를 입력합니다.
- 7 Azure 스토리지 URI 텍스트 상자에 스토리지 URL을 입력합니다.  
예: https://mystorageaccount.blob.core.windows.net
- 8 완료를 클릭합니다.
- 9 각 Azure 끝점에 대해 반복합니다.

#### vRealize Automation 6.2.x Automation Application Services 마이그레이션

VMware vRealize Application Services 마이그레이션 도구를 사용하여 기존 Application Services Blueprint 및 배포 프로파일을 VMware vRealize Application Services 6.2.x에서 대상 vRealize Automation 버전으로 마이그레이션할 수 있습니다.

사전 요구 사항

vRealize Automation의 최신 버전으로 마이그레이션을 완료합니다.

절차

- ◆ VMware vRealize Application Services 마이그레이션 도구를 다운로드하려면 다음 단계를 완료하십시오.
  - a [VMware vRealize Automation 다운로드](#)를 클릭합니다.
  - b **드라이버 및 도구 > VMware vRealize Application Services 마이그레이션 도구**를 선택합니다.

원본 대상 vRealize Automation IaaS Microsoft SQL 데이터베이스 삭제

마이그레이션이 완료되면 원본 IaaS 데이터베이스를 삭제할 수 있습니다.

사전 요구 사항

vRealize Automation의 최신 버전으로 마이그레이션을 완료합니다.

마이그레이션된 환경에서는 대상 vRealize Automation 환경을 설치할 때 생성한 원본 vRealize Automation IaaS Microsoft SQL 데이터베이스를 사용하지 않습니다. 따라서 마이그레이션을 완료한 후에는 이 원본 IaaS 데이터베이스를 Microsoft SQL Server에서 안심하고 삭제할 수 있습니다.

마이그레이션 후 데이터 센터 위치 메뉴 콘텐츠 업데이트

마이그레이션 후에는 누락된 모든 사용자 지정 데이터 센터 위치를 **위치** 드롭다운 메뉴에 추가해야 합니다.

최신 버전의 vRealize Automation으로 마이그레이션한 후에는 [계산 리소스] 페이지의 **위치** 드롭다운 메뉴에 있는 데이터 센터 위치가 기본 목록으로 되돌려집니다. 사용자 지정 데이터 센터 위치는 누락되지만 모든 계산 리소스 구성은 성공적으로 마이그레이션되고 **Vrm.DataCenter.Location** 속성이 영향을 받지 않습니다. **위치** 메뉴에 사용자 지정 데이터 센터 위치를 추가할 수 있습니다.

## 사전 요구 사항

최신 버전의 vRealize Automation으로 마이그레이션합니다.

## 절차

- ◆ 누락된 데이터 센터 위치를 **위치** 드롭다운 메뉴에 추가합니다. **시나리오: 영역 간 배포를 위한 데이터 센터 위치 추가** 항목을 참조하십시오.

## 소프트웨어 에이전트를 TLS 1.2로 업그레이드

vRealize Automation 마이그레이션 이후에는 몇 가지 작업을 수행하여 소스 환경의 소프트웨어 에이전트를 TLS(Transport Layer Security) 1.2로 업그레이드해야 합니다.

vRealize Automation 7.4부터, vRealize Automation 및 브라우저 간 데이터 통신에 지원되는 TLS 프로토콜은 TLS 1.2가 유일합니다. 마이그레이션 후에는 모든 기존 가상 시스템은 물론 vRealize Automation 소스 환경의 기존 가상 시스템 템플릿을 업그레이드해야 합니다.

### 소스 환경 가상 시스템 템플릿 업데이트

마이그레이션을 완료했으면 소프트웨어 에이전트가 TLS 1.2 프로토콜을 사용하도록 마이그레이션된 기존 vRealize Automation 템플릿을 업데이트해야 합니다.

게스트 에이전트와 에이전트 부트스트랩 코드를 소스 환경 템플릿에서 업데이트해야 합니다. 연결된 클론 옵션을 사용 중이라면 새로 생성된 가상 시스템과 해당 스냅샷에 템플릿을 다시 매핑해야 할 수 있습니다.

템플릿을 업그레이드하려면 다음 작업을 완료합니다.

- 1 vSphere에 로그인합니다.
- 2 마이그레이션된 각 vRealize Automation 템플릿을 가상 시스템으로 변환하고 시스템의 전원을 켭니다.
- 3 적절한 소프트웨어 설치 관리자를 가져오고 각 가상 시스템에서 해당 소프트웨어 설치 관리자를 실행합니다.
- 4 각 가상 시스템을 다시 템플릿으로 변환합니다.

Linux 또는 Windows용 소프트웨어 설치 관리자를 찾으려면 이 절차를 사용합니다.

## 사전 요구 사항

- vRealize Automation 7.1.x 이상에서 마이그레이션을 완료합니다.
- **소프트웨어 에이전트 패치 적용**(vRealize Automation 7.1.x 또는 7.3.x에서 마이그레이션한 경우)

## 절차

- 1 브라우저를 시작하고 가상 장치의 정규화된 도메인 이름(<https://vra-va-hostname.domain.name>)을 사용하여 vRealize Automation 장치 시작 페이지를 엽니다.
- 2 **게스트 및 소프트웨어 에이전트 페이지**를 클릭합니다.
- 3 Linux 또는 Windows 소프트웨어 설치 관리자에 대한 지침을 따릅니다.

다음에 수행할 작업

소프트웨어 에이전트 업그레이드가 필요한 가상 시스템 식별.

소프트웨어 에이전트 업그레이드가 필요한 가상 시스템 식별

vRealize Automation 콘솔의 상태 서비스를 사용하여 TLS 1.2로의 소프트웨어 에이전트 업데이트가 필요한 가상 시스템을 식별할 수 있습니다.

종종 vRealize Automation 소스 환경에 적용된 패치가 모든 가상 시스템을 업그레이드하지 않습니다. 상태 서비스를 사용하여 아직 TLS 1.2로의 소프트웨어 에이전트 업데이트가 필요한 가상 시스템을 식별할 수 있습니다. 사후 프로비저닝 절차를 위해 대상 환경의 모든 소프트웨어 에이전트가 업데이트되어야 합니다.

사전 요구 사항

- vRealize Automation 7.1.x 이상을 마이그레이션합니다.
- 소프트웨어 에이전트 패치 적용(vRealize Automation 7.1.x 또는 7.3.x에서 마이그레이션한 경우)
- 기본 가상 장치에서 대상 vRealize Automation 환경에 로그인합니다.

절차

- 1 **관리 > 상태**를 클릭합니다.
- 2 **새 구성**을 클릭합니다.
- 3 [구성 세부 정보] 페이지에 요청된 정보를 입력합니다.

옵션	설명
이름	SW Agent verification을 입력합니다.
설명	선택적 설명(예: Locate software agents for upgrade to TLS 1.2)을 추가합니다.
제품	대상 제품 및 버전(예: vRealize Automation 7.4.0)을 선택합니다.
스케줄	[없음]을 선택합니다.

- 4 **다음**을 클릭합니다.
- 5 [테스트 집합 선택] 페이지에서 **vRealize Automation에 대한 시스템 테스트** 및 **vRealize Automation에 대한 테넌트 테스트**를 선택합니다.
- 6 **다음**을 클릭합니다.

## 7 [매개 변수 구성] 페이지에 요청된 정보를 입력합니다.

표 1-85. vRealize Automation 가상 장치

옵션	설명
공개 웹 서버 주소	<ul style="list-style-type: none"> <li>■ 최소 배포의 경우 vRealize Automation 장치 호스트에 대한 기본 URL입니다. 예: <code>https://va-host.domain/</code></li> <li>■ 고가용성 배포의 경우 vRealize Automation 로드 밸런서에 대한 기본 URL입니다. 예: <code>https://load-balancer-host.domain/</code></li> </ul>
SSH 콘솔 주소	vRealize Automation 장치의 정규화된 도메인 이름입니다. 예: <code>va-host.domain</code>
SSH 콘솔 사용자	<b>root</b>
SSH 콘솔 암호	루트의 암호입니다.
최대 서비스 응답 시간(ms)	허용 기본값: 2000

표 1-86. vRealize Automation 시스템 테넌트

옵션	설명
시스템 테넌트 관리자	관리자
시스템 테넌트 암호	관리자의 암호입니다.

표 1-87. vRealize Automation 디스크 공간 모니터링

옵션	설명
경고 임계값 백분율	허용 기본값: 75
위험 임계값 백분율	허용 기본값: 90

표 1-88. vRealize Automation 테넌트

옵션	설명
테스트 중인 테넌트	테스트를 위해 선택한 테넌트입니다.
패브릭 관리자 사용자 이름	패브릭 관리자 사용자 이름입니다. 예: <code>admin@va-host.local</code>  <b>참고</b> 모든 테스트를 실행하려면 이 패브릭 관리자에게 테넌트 관리자 및 IaaS 관리자 역할도 있어야 합니다.
패브릭 관리자 암호	패브릭 관리자의 암호입니다.

## 8 다음을 클릭합니다.

### 9 [요약] 페이지에서 정보를 검토하고 **완료**를 클릭합니다.

소프트웨어 에이전트 확인 구성이 완료되었습니다.

### 10 소프트웨어 에이전트 확인 카드에서 **실행**을 클릭합니다.



- 11 테스트가 완료되면 소프트웨어 에이전트 확인 카드의 가운데를 클릭합니다.
- 12 소프트웨어 에이전트 확인 결과 페이지에서 테스트 결과 페이지를 넘겨 보고 [이름] 열에서 [소프트웨어 에이전트 버전 확인] 테스트를 찾습니다. 테스트 결과가 실패이면 [원인] 열의 **원인** 링크를 클릭하여 오래된 소프트웨어 에이전트가 포함된 가상 시스템을 확인합니다.

#### 다음에 수행할 작업

오래된 소프트웨어 에이전트가 포함된 가상 시스템이 있는 경우 [vSphere에서 소프트웨어 에이전트 업그레이드](#) 항목을 참조하십시오.

#### vSphere에서 소프트웨어 에이전트 업그레이드

마이그레이션한 후 vRealize Automation 장치 관리를 사용하여 vSphere에서 모든 오래된 소프트웨어 에이전트를 TLS 1.2로 업그레이드할 수 있습니다.

이 절차는 소스 환경의 가상 시스템의 오래된 소프트웨어 에이전트를 TLS 1.2로 업데이트하며 대상 vRealize Automation 릴리스로의 마이그레이션에 필요합니다.

#### 사전 요구 사항

- [소프트웨어 에이전트 패치 적용](#)(vRealize Automation 7.1.x 또는 7.3.x에서 마이그레이션한 경우)
- vRealize Automation 7.1.x 이상에서 마이그레이션을 완료합니다.
- 상태 서비스를 사용하여 오래된 소프트웨어 에이전트가 포함된 가상 장치를 식별했습니다.

#### 절차

- 1 기본 vRealize Automation 장치에서 vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **root**로 vRealize Automation 장치 관리에 로그인합니다.  
고가용성 환경의 경우 마스터 장치에서 장치 관리를 엽니다.
- 2 **vRA > 소프트웨어 에이전트**를 클릭합니다.
- 3 **TLS 1.0, 1.1 전환**을 클릭합니다.  
TLS v1.0, v1.1 상태가 [사용]입니다.
- 4 테넌트 자격 증명의 경우 소스 vRealize Automation 장치에 대한 요청된 정보를 입력합니다.

옵션	설명
테넌트 이름	소스 vRealize Automation 장치의 테넌트 이름입니다.  <b>참고</b> 테넌트 사용자에게 소프트웨어 설계자 역할이 할당되어 있어야 합니다.
Username	소스 vRealize Automation 장치의 테넌트 관리자 사용자 이름입니다.
암호	테넌트 관리자 암호입니다.

**5 연결 테스트**를 클릭합니다.

연결이 설정된 경우 성공 메시지가 표시됩니다.

**6** 소스 장치의 경우 소스 vRealize Automation 장치의 IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.

소스 및 대상 장치가 모두 동일한 테넌트 자격 증명을 사용해야 합니다.

**7 배치 나열**을 클릭합니다.

[배치 선택 목록] 테이블이 표시됩니다.

**8 표시**를 클릭합니다.

오래된 소프트웨어 에이전트가 포함된 가상 시스템 목록을 나열하는 테이블이 표시됩니다.

**9** [업그레이드 가능] 상태에 있는 가상 시스템에 대한 소프트웨어 에이전트를 업그레이드합니다.

- 개별 가상 시스템의 소프트웨어 에이전트를 업그레이드하려면 가상 시스템 그룹에 대해 **표시**를 클릭하고, 업그레이드할 가상 시스템을 식별한 후 **실행**을 클릭하여 업그레이드 프로세스를 시작합니다.
- 가상 시스템 배치에 대해 소프트웨어 에이전트를 업그레이드하려면 업그레이드할 그룹을 식별한 후 **실행**을 클릭하여 업그레이드 프로세스를 시작합니다.

업그레이드할 가상 시스템이 200개가 넘는 경우 다음 매개 변수에 대한 값을 입력하여 배치 업그레이드 프로세스 속도를 제어할 수 있습니다.

옵션	설명
배치 크기	배치 업그레이드에 대해 선택된 가상 시스템의 수입니다. 이 숫자를 변경하여 업그레이드 속도를 조정할 수 있습니다.
대기열 크기	한 번에 수행되는 병렬 업그레이드 실행의 횟수입니다. 예: 20. 이 숫자를 변경하여 업그레이드 속도를 조정할 수 있습니다.
배치 오류	배치 업그레이드 속도 저하를 일으키는 REST 오류 수입니다. 예를 들어 업그레이드의 안정성을 향상시키기 위해 5번의 실패 후 현재 배치 업그레이드를 중지하려는 경우 텍스트 필드에 5를 입력합니다.
배치 실패	배치 처리 속도 저하를 일으키는 실패한 소프트웨어 에이전트 업그레이드 수입니다. 예를 들어 업그레이드의 안정성을 향상시키기 위해 5번의 실패 후 현재 배치 업그레이드를 중지하려는 경우 텍스트 필드에 5를 입력합니다.
배치 폴링	업그레이드 프로세스를 확인하기 위해 업그레이드 프로세스가 폴링되는 간격입니다. 이 숫자를 변경하여 업그레이드 속도를 조정할 수 있습니다.

업그레이드 프로세스가 너무 느리거나 너무 많은 업그레이드 실패를 생성하는 경우 업그레이드 성능을 향상시키기 위해 이러한 매개 변수를 조정할 수 있습니다.

**참고** 새로 고침을 클릭하면 배치 목록이 지워집니다. 업그레이드 프로세스에는 영향을 주지 않습니다. TLS 1.2 설정 여부에 대한 정보도 새로 고치며 또한 새로 고침을 클릭하면 vRealize Automation 서비스의 상태 점검도 수행합니다. 서비스가 실행되고 있지 않은 경우 시스템이 오류 메시지를 표시하며 다른 모든 작업 버튼을 비활성화합니다.

## 10 TLS 1.0, 1.1 전환을 클릭합니다.

TLS v1.0, v1.1 상태가 [사용 안 함]입니다.

Amazon Web Service 또는 Microsoft Azure에서 소프트웨어 에이전트 업그레이드  
AWS(Amazon Web Service) 또는 Microsoft Azure에서 수동으로 오래된 소프트웨어 에이전트를 업그레이드할 수 있습니다.

- 마이그레이션된 vRealize Automation 서버의 예약에 지정된 터널 속성을 업데이트해야 합니다.

**참고** 이 예의 모든 버전 인스턴스를 하면 대상 릴리스의 vRealize Automation 버전 값으로 바꿉니다.

사전 요구 사항

- 소프트웨어 에이전트 패치 적용(vRealize Automation 7.1.x 또는 7.3.x에서 마이그레이션한 경우)
- vRealize Automation 7.1.x 이상에서 마이그레이션을 완료합니다.
- 소프트웨어 터널이 있으며 터널 가상 시스템 IP 주소가 알려져 있습니다.

절차

- 1 업그레이드해야 하는 각 노드에 대해 노드 파일을 생성합니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

- 2 Linux 또는 Windows 가상 시스템에서 소프트웨어 에이전트를 업그레이드하기 위한 계획 파일을 생성합니다.

- Amazon AWS 또는 Microsoft Azure 끝점에 해당하는 개인 IP 주소의 값을 포함하도록 /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}에서 마이그레이션 매개 변수 파일을 수정합니다.

```
"key": "ipAddress",
 "value": {
 "type": "string",
 "value": "<$PrivateIp:$PrivatePort>"
 }
}
```

- Linux 시스템 업데이트에 다음 명령을 사용합니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL
Software.LinuxAgentUpdate74 --source_cloud_provider azure
```

- Windows 시스템 업데이트에 다음 명령을 사용합니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW
Software.WindowsAgentUpdate74 --source_cloud_provider azure
```

- 다음 명령은 계획 파일을 실행합니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/
webapps/ROOT/software/plan
```

- 3** 1단계의 노드 파일 및 2단계의 계획 파일을 사용하여 소프트웨어 에이전트를 업데이트하려면 다음 명령을 사용합니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <
$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux
Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --
plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider
azure --action plan_batch -S <$SourceVRAServer>
```

대안으로 노드 인덱스를 제공하여 노드 파일에서 한 번에 하나의 노드를 실행하도록 다음 명령을 사용할 수 있습니다.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <
$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux
Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --
plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider
azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

이 절차를 수행하면서 vRealize Automation 가상 장치 및 호스트 시스템에서 로그를 추적하여 서버 에이전트 업그레이드 프로세스를 확인할 수 있습니다.

업그레이드한 후 업그레이드 프로세스가 Windows 또는 Linux에 대한 소프트웨어 업데이트 스크립트를 vRealize Automation 가상 장치로 가져옵니다. vRealize Automation 가상 장치 호스트로 로그인하여 소프트웨어 구성 요소를 성공적으로 가져왔는지 확인할 수 있습니다. 구성 요소를 가져온 후 소프트웨어 업데이트가 이전 EBS(Event Broker Service)로 전송되어 소프트웨어 업데이트 스크립트를 식별된 가상 시스템에 릴레이합니다. 업그레이드가 완료되고 새로운 소프트웨어 에이전트가 작동되면 ping 요청을 전송하여 새 vRealize Automation 가상 장치에 바인딩됩니다.

#### 참고 유용한 로그 파일

- 소스 vRealize Automation에 대한 Catalina 출력: `/var/log/vcac/catalina.out`. 이 파일에는 에이전트 마이그레이션이 수행될 때 수행되는 업그레이드 요청이 표시됩니다. 이 작업은 소프트웨어 프로비저닝 요청을 수행하는 것과 동일합니다.
- 대상 vRealize Automation에 대한 Catalina 출력: `/var/log/vcac/catalina.out`. 이 파일에는 마이그레이션된 가상 시스템이 7.4.0-SNAPSHOT 버전 번호를 포함하기 위해 수행한 해당 ping 요청이 보고됩니다. EBS 항목 이름(예: `sw-agent-UUID`)을 비교하여 이를 함께 기록할 수 있습니다.
- 대상 vRealize Automation 시스템 마스터 업그레이드 로그 파일에 대한 에이전트 업데이트 폴더: `/var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`. 이 파일을 추적하여 진행 중인 업그레이드 작업을 확인할 수 있습니다.
- 개별 로그는 테넌트 폴더 `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`에서 확인할 수 있습니다. 개별 노드는 실패 및 진행 중 확장자가 포함된 많은 파일로 여기에 나열됩니다.
- 마이그레이션된 VM: `/opt/vmware-appdirector/agent/logs/darwin*.log`. 수신되고 있는 소프트웨어 업데이트 요청과 `agent_bootstrap` + 소프트웨어 에이전트의 최종적인 다시 시작을 나열하는 이 위치를 불시 점검할 수 있습니다.

### 6.2.5에서 마이그레이션한 이후 속성 사전 설정 변경

vRealize Automation 6.2.x 속성 사전의 **Label** 컨트롤이 vRealize Automation 7.x 속성 사전에는 없습니다.

vRealize Automation 7.4 이전 버전으로 마이그레이션하는 동안, **Label** 컨트롤은 마이그레이션된 속성 사전에서 **TextBox** 제어 유형으로 변환됩니다.

vRealize Automation 7.5 이상 버전으로 마이그레이션하는 동안, **Label** 컨트롤은 마이그레이션된 속성 사전에서 **TextArea** 제어 유형으로 변환됩니다. **TextArea** 제어 유형은 이전 버전의 vRealize Automation 7.x로 마이그레이션할 때 사용되는 **TextBox** 제어 유형보다 긴 레이블 이름을 더 잘 지원합니다.

마이그레이션 후에 영향을 받은 **TextBox** 또는 **TextArea** 제어 유형이 포함된 속성 정의를 재정의할 수 없도록 설정할 수 있으며, 이 설정은 각 **Blueprint**의 vRealize Automation 속성 설정에서 수동으로, 영향을 받은 사용자 지정 속성 정의가 사용된 각 **Blueprint** 구성 요소, 예약, 끝점 등에서 수동으로, 또는 vRealize CloudClient의 내보내기 및 가져오기 기능을 사용하여 프로그래밍 방식으로 수행할 수 있습니다.

## 절차

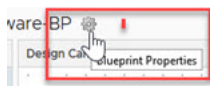
- 1 마이그레이션 후에 어떤 속성 정의에 **Text Box**(7.4 이전) 또는 **TextArea**(7.5 이상) 유형 컨트롤이 사용되는지 확인하기 위해 **관리 > 속성 정의**를 클릭하고 **문자열** 데이터 유형의 각 속성 정의에 대한 **표시 영역** 설정을 살펴봅니다.

이것은 마이그레이션된 vRealize Automation 인스턴스에서 재정의 불가능으로 설정할 속성 정의입니다.

- 2 영향을 받는 사용자 지정 속성을 재정의 불가능으로 설정합니다.

- 전체 Blueprint에 대해 수동으로

- 1 **설계** 탭을 클릭한 후 Blueprint를 엽니다.
- 2 톱니 바퀴 아이콘을 클릭하여 **Blueprint 속성** 페이지를 엽니다.



- 3 **Blueprint 속성** 페이지에서 **속성** 탭을 클릭하고 **사용자 지정 속성**을 클릭합니다.
- 4 **TextBox** 또는 **TextArea** 제어 유형이 포함된 모든 속성 정의에 대해 **재정의 가능**을 꺼짐으로 전환합니다.

- 영향을 받은 사용자 지정 속성이 사용된 각 Blueprint 구성 요소, 예약, 끝점 등에 대해 수동으로

- 1 끝점 및 예약의 경우 **인프라**를 클릭하고 **끝점** 또는 **예약**을 선택합니다.
- 2 각 대상 요소를 열고 해당 [속성] 탭을 사용하여 영향을 받는 **Text Box**(7.4 이전) 또는 **TextArea**(7.5 이상) 유형 컨트롤을 재정의 불가능으로 설정합니다.
- 3 각 Blueprint를 열고 Blueprint 캔버스의 각 시스템, 네트워크 및 기타 구성 요소의 **속성** 탭을 사용하여 영향을 받는 속성 정의를 업데이트합니다.

- 전체 Blueprint에 대해 프로그래밍 방식으로

- 1 vRealize CloudClient 내보내기 명령 시퀀스를 사용하여 Blueprint를 내보냅니다.
- 2 영향을 받는 속성 정의를 재정의 불가능으로 표시합니다. 이 예에서 **TestLabel**은 재정의 불가능으로 설정되고 **TestOverrideLabel**은 요청 양식에서 편집할 수 있는 방식으로 설정됩니다.

```
TestLabel:
 fixed: default test label description at BP
 required: true
 secured: false
 visible: true
TestOverrideLabel:
 default: override this value
 required: true
 secured: false
 visible: true
```

### 3 vRealize CloudClient 가져오기 명령 시퀀스를 사용하여 Blueprint를 가져옵니다.

#### 대상 vRealize Automation 환경 검증

모든 데이터가 대상 vRealize Automation 환경에 성공적으로 마이그레이션되었는지 확인할 수 있습니다.

#### 사전 요구 사항

- 최신 버전의 vRealize Automation으로 마이그레이션합니다.
- 대상 vRealize Automation 콘솔에 로그인합니다.
  - a 대상 가상 장치의 정규화된 도메인 이름(<https://vra-vd-hostname.domain.name/vcac>)을 사용하여 vRealize Automation 콘솔을 엽니다.  
고가용성 환경인 경우, 대상 가상 장치 로드 밸런서의 정규화된 도메인 이름(<https://vra-vd-lb-hostname.domain.name/vcac>)을 사용하여 콘솔을 엽니다.
  - b 테넌트 관리자 사용자 이름과 암호를 사용하여 로그인합니다.

#### 절차

- 1 **인프라 > 관리되는 시스템**을 선택하고 모든 관리되는 가상 시스템이 존재하는지 확인합니다.
- 2 **계산 리소스**를 클릭하고 각 끝점을 선택한 후 **데이터 수집**, **지금 요청** 및 **새로 고침**을 클릭하여 끝점이 작동 중인지 확인합니다.
- 3 **설계**를 클릭하고 **Blueprint** 페이지에서 각 Blueprint의 요소를 확인합니다.
- 4 **XaaS**를 클릭하고 **사용자 지정 리소스**, **리소스 매핑**, **XaaS Blueprint**, **리소스 작업**의 내용을 확인합니다.
- 5 **관리 > 카탈로그 관리**를 선택하고 **서비스**, **카탈로그 항목**, **작업** 및 **사용 권한**의 내용을 확인합니다.
- 6 **항목 > 배포**를 선택하고 프로비저닝된 가상 시스템의 정보를 확인합니다.
- 7 [배포] 페이지에서 전원이 꺼진 프로비저닝된 가상 시스템을 선택하고 **작업 > 전원 켜기**를 선택한 다음 **제출**을 클릭하고 **확인**을 클릭합니다. 가상 시스템 전원이 제대로 켜졌는지 확인합니다.
- 8 **카탈로그**를 클릭하고 새 카탈로그 항목을 요청합니다.
- 9 **일반** 탭에서 요청 정보를 입력합니다.
- 10 시스템 아이콘을 클릭하고 모든 기본 설정을 그대로 선택한 다음 **제출**과 **확인**을 차례로 클릭합니다.
- 11 요청이 완료되는지 확인합니다.

#### vRealize Automation 대상에서 HF 테이블 복원

vRealize Automation 대상에서 HF 테이블을 백업하고 vRealize Automation 7.x로 마이그레이션한 후에는 HF 테이블을 대상 환경에 복원해야 합니다.

HF 테이블 백업에 대한 자세한 내용은 [vRealize Automation 대상에서 HF 테이블 백업](#) 항목을 참조하십시오.

HF 테이블을 대상 환경에 복원하려면 `hf_tables.zip` 파일을 대상 노드의 `/tmp/`에 복사하고 다음 명령을 적용합니다.

```
cd /tmp
unzip ./hf_tables.zip -d ./hf_tables (ignore this command if hf_tables folder is already unzipped)
psql -U postgres -d vcac
\i /tmp/hf_tables/hf_patch.sql
\i /tmp/hf_tables/hf_patch_execution.sql
\i /tmp/hf_tables/hf_patch_nodes.sql
```

## 마이그레이션 문제 해결

마이그레이션 문제 해결 항목은 vRealize Automation을 마이그레이션할 때 발생할 수 있는 문제에 대한 솔루션을 제공합니다.

### PostgreSQL 버전에 따른 오류 발생

업데이트된 PostgreSQL 데이터베이스가 포함된 소스 vRealize Automation 6.2.x 환경에서 관리자 액세스를 차단합니다.

#### 문제

vRealize Automation 6.2.x에서 업그레이드된 PostgreSQL 데이터베이스를 사용하는 경우 관리자는 vRealize Automation에서 이 데이터베이스로의 액세스를 제공하는 항목을 `pg_hba.conf` 파일에 추가해야 합니다.

#### 해결책

- 1 `pg_hba.conf` 파일을 엽니다.
- 2 이 데이터베이스에 대한 액세스 권한을 부여하려면 다음 항목을 추가합니다.

```
host all vcac-database-user vra-va-ip trust method
```

#### 마이그레이션 시 일부 가상 시스템의 배포가 생성되지 않음

마이그레이션할 때 누락된 상태의 가상 시스템에 대해서는 해당하는 배포가 대상 환경에 생성되지 않습니다.

#### 문제

마이그레이션 시 소스 환경에서 가상 시스템이 누락된 상태인 경우, 해당하는 배포가 대상 환경에 생성되지 않습니다.

#### 해결책

- ◆ 마이그레이션 이후에 가상 시스템이 더 이상 누락된 상태가 아니면 대량 가져오기를 사용하여 가상 시스템을 대상 배포로 가져올 수 있습니다.

#### 로드 밸런서 구성 때문에 장기 실행 작업에서 시간 초과 발생

로드 밸런서 시간 초과 설정을 10분으로 변경하면 예기치 않은 연결 종료를 방지하지 못할 수 있습니다.



## 문제

HTTP/HTTPS 요청을 실행하는 동안 연결이 유지되도록 시간 초과를 10분으로 설정하면 마이그레이션 작업을 실행하는 데 시간이 오래 걸릴 경우 예기치 않은 연결 종료를 방지하지 못할 수 있습니다.

## 해결책

- ◆ 마이그레이션 중에 예기치 않은 연결 종료 발생 시, 로드 밸런서의 시간 초과를 10분보다 길게 늘리거나 마이그레이션 기간 동안 적절한 능동 노드를 가리키도록 로드 밸런서 DNS 레코드를 업데이트합니다. 마이그레이션이 완료된 후에는 로드 밸런서 DNS 기록을 되돌립니다.

## 마이그레이션 로그 위치

마이그레이션 프로세스를 기록하는 로그를 확인하여 검증 또는 마이그레이션 문제를 해결할 수 있습니다.

표 1-89. 소스 vRealize Automation 장치

로그	위치
패키지 생성 로그	/var/log/vmware/vcac/migration-package.log

표 1-90. 대상 vRealize Automation 장치

로그	위치
마이그레이션 로그	/var/log/vmware/vcac/migrate.log
마이그레이션 실행 로그	/var/log/vmware/vcac/mseq.migration.log
마이그레이션 실행 출력 로그	/var/log/vmware/vcac/mseq.migration.out.log
검증 실행 로그	/var/log/vmware/vcac/mseq.validation.log
검증 실행 출력 로그	/var/log/vmware/vcac/mseq.validation.out.log

표 1-91. 대상 vRealize Automation 인프라 노드

로그	위치
마이그레이션 로그	C:\Program Files (x86)\VMware\VCAC\InstallLogs-YYYYMMDDHHMMXX\Migrate.log
검증 로그	C:\Program Files (x86)\VMware\VCAC\InstallLogs-YYYYMMDDHHMMXX\Validate.log

마이그레이션 후 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없음

최신 버전의 vRealize Automation으로 마이그레이션한 후 이전 버전의 특정 속성 정의를 사용하는 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없습니다.

## 문제

6.2.x 이전 버전에서 마이그레이션했고 다음과 같은 제어 유형 또는 특성이 포함된 속성 정의가 있는 경우, 이러한 요소가 속성 정의에서 누락되고 해당 정의를 사용하는 모든 카탈로그 항목이 마이그레이션하기 전의 방식으로 작동하지 않습니다.

- 제어 유형. 확인란 또는 링크.
- 특성. 관계, 정규식 또는 속성 레이아웃.

## 원인

vRealize Automation 7.0 이상에서는 속성 정의에서 더 이상 이러한 요소를 사용하지 않습니다. 속성 정의에서 포함된 제어 유형 또는 특성을 사용하지 않고 대신 vRealize Orchestrator 스크립트 작업을 사용하여 속성 정의를 구성하거나 속성 정의를 다시 생성해야 합니다.

스크립트 작업을 사용하여 제어 유형 또는 특성을 vRealize Automation 7.x로 마이그레이션합니다.

## 해결책

- 1 vRealize Orchestrator에서 속성 값을 반환하는 스크립트 작업을 생성합니다. 작업은 단순 유형을 반환해야 합니다. 예를 들어 문자열, 정수 또는 지원되는 다른 유형을 반환합니다. 작업은 해당 작업이 종속된 다른 속성을 입력 매개 변수로 사용할 수 있습니다.
- 2 vRealize Automation 콘솔에서 제품 정의를 구성합니다.
  - a **관리 > 속성 사전 > 속성 정의**를 선택합니다.
  - b 속성 정의를 선택하고 **편집**을 클릭합니다.
  - c [권장 사항 표시] 드롭다운 메뉴에서 **드롭다운**을 선택합니다.
  - d [값] 드롭다운 메뉴에서 **외부 값**을 선택합니다.
  - e 스크립트 작업을 선택합니다.
  - f **확인**을 클릭합니다.
  - g 스크립트 작업에 포함된 입력 매개 변수를 구성합니다. 기존 관계를 유지하려면 매개 변수를 다른 속성에 바인딩합니다.
  - h **확인**을 클릭합니다.

vRealize Automation에서 데이터 수집 라디오 버튼이 사용되지 않도록 설정됨

vRealize Automation 6.2.x에서 7.x로 마이그레이션한 후 대상 vRealize Automation [계산 리소스] 페이지의 [데이터 수집] 아래에 사용되지 않도록 설정된 라디오 버튼이 포함됩니다.

## 원인

소스 환경에 끝점을 가리키는 에이전트를 설치하고 대상 환경에 동일한 끝점을 가리키는 에이전트를 설치했지만 에이전트의 이름이 서로 다른 경우 대상 환경에서 관리자로서 끝점에 대한 테스트 연결을 실행할 수 있습니다. 하지만 패브릭 관리자로서 대상 환경의 vRealize Automation에 로그인하는 경우 [계산 리소스] 페이지의 [데이터 수집] 아래에 있는 라디오 버튼이 사용되지 않도록 설정됩니다.

## 해결책

대상 환경에 설치된 에이전트의 이름을 소스 환경에 설치된 에이전트의 이름과 동일하게 지정하면 이러한 문제를 피할 수 있습니다.

### 소프트웨어 에이전트 업그레이드 문제 해결

vRealize Automation 장치 관리를 사용하여 소프트웨어 에이전트를 업그레이드할 때 발생한 문제의 원인을 식별하기 위해 로그 파일을 검토할 수 있습니다.

#### 문제

소프트웨어 에이전트를 업그레이드할 때 문제가 발생할 수 있습니다. 소프트웨어 에이전트 업그레이드 프로세스 동안 로그 파일을 검토하여 문제가 발생한 위치를 식별할 수 있습니다.

#### 서버 로그

- 서버에서 updateSoftwareAgents.log 파일(/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log)을 검토하여 프로세스를 관찰합니다.
- 대상 장치에서 catalina.out 파일(/var/log/vcac/catalina.out)을 검토하여 성공한 소프트웨어 에이전트를 확인합니다.

version.0-SNAPSHOT에 대해 보고된 "ping"과 같은 문자열을 찾습니다.

다음과 같은 위치에서 추가 정보를 찾을 수 있습니다.

- /var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.plan
- /var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.log
- /var/cache/vcac/agentupdate/sqa/UUID/UUID.log(OS당)

주요 배치 업그레이드를 시작하기 전에 항상 가상 장치 소프트웨어 에이전트에 대한 테스트 업그레이드를 수행해야 합니다. 프로세스 개요는 다음과 같습니다.

- 대상 가상 장치에 대한 첫 번째 요청을 확인하여 에이전트 버전을 식별합니다.
- 업그레이드와 관련한 소스 가상 장치에 대한 요청을 확인합니다.
- 대상 가상 장치에서 해당하는 새로운 버전 값을 보고하는 에이전트를 확인합니다.
- 이러한 이벤트 사이에 updateSoftwareAgents.log 파일(/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log)을 검토합니다.

#### 클라이언트 로그

Linux 에이전트 로그는 appdirector 에이전트 로그 폴더에 있습니다(/opt/vmware-appdirector/agent/logs/\*.log).

다음과 같은 로그 오류를 볼 수 있습니다. 이러한 오류는 업그레이드 프로세스 중에 EBS 대기열이 수시로 변하기 때문에 일시적입니다.

```
Feb 15 2018 16:54:10.105 ERROR [EventPoller-sw-agent-0ad2418d-5b42-4231-a839-a05dd618e43e] []
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler - Error while
polling events for subscription '{}'
```

```
org.springframework.web.client.HttpClientErrorException: 404 Not Found
```

```
org.springframework.web.client.DefaultResponseErrorHandler.handleError(DefaultResponseErrorHa
ndler.java:91) ~[nobel-agent.jar:na]
```

```
org.springframework.web.client.RestTemplate.handleResponse(RestTemplate.java:641) ~[nobel-
agent.jar:na]
```

```
org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-
agent.jar:na]
```

```
org.springframework.web.client.RestTemplate.execute(RestTemplate.java:557) ~[nobel-
agent.jar:na]
```

```
org.springframework.web.client.RestTemplate.exchange(RestTemplate.java:503) ~[nobel-
agent.jar:na]
```

```
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler.pollEvents(RestEv
entSubscribeHandler.java:297) ~[nobel-agent.jar:na]
```

```
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler
$EventPoller.run(RestEventSubscribeHandler.java:329) ~[nobel-agent.jar:na]
```

## 마이그레이션 시나리오

vRealize Automation 6.2.5에서 마이그레이션하는 경우 이러한 문제가 발생할 수 있습니다.

6.2.5의 문제	최신 버전에 대한 해결 방법
<p>vRealize Automation 6.2.5에서 최신 버전으로 마이그레이션한 후 이러한 속성 정의를 사용하는 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없습니다.</p> <ul style="list-style-type: none"> <li>■ 제어 유형: 확인란 또는 링크.</li> <li>■ 특성: 관계, 정규식 또는 속성 레이아웃.</li> </ul> <p>vRealize Automation 릴리스에서, 속성 정의는 더 이상 이러한 요소를 사용하지 않습니다.</p>	<p>속성 정의에서 포함된 제어 유형 또는 특성을 사용하지 않고 대신 vRealize Orchestrator 스크립트 작업을 사용하도록 속성 정의를 구성하거나 속성 정의를 다시 생성해야 합니다. 자세한 내용은 <a href="#">마이그레이션 후 카탈로그 항목이 서비스 카탈로그에 나타나지만 요청할 수 없음</a> 항목을 참조하십시오.</p>
<p>vRealize Automation 6.2.5 드롭다운 메뉴에서 상위-하위 항목 관계를 정의하는 데 사용되는 정규식은 대상 vRealize Automation 릴리스에서 지원되지 않습니다. 6.2.5에서는 정규식을 사용하여 특정 상위 메뉴 항목에만 사용할 수 있는 하나의 하위 메뉴 항목을 정의할 수 있습니다. 상위 메뉴 항목을 선택하면 해당 하위 메뉴 항목만 표시됩니다.</p>	<p>마이그레이션한 후 이전 동작 값을 복원하기 위해 속성 정의를 재생성해야 합니다. 상위 드롭다운 메뉴와 하위 드롭다운 메뉴 간의 상위-하위 관계 생성에 대한 자세한 내용은 <a href="#">vRA 7.2에서 동적 속성 정의를 사용하는 방법</a>을 참조하십시오.</p>
<p>워크플로 스텝을 사용하는 vRealize Orchestrator 워크플로</p>	<p>워크플로 스텝은 마이그레이션 후 이벤트 브로커 구독으로 변환할 수 있습니다.</p> <p>변환 및 변경 단계에 대한 자세한 내용은 "vRealize Automation 확장성 마이그레이션 가이드"를 참조하십시오.</p>

6.2.5의 문제	최신 버전에 대한 해결 방법
Active Directory 통합에 대한 사용자 지정	Active Directory 구성 및 정책은 제품에 내장되어 있습니다. Active Directory 구성에 대한 자세한 내용은 <a href="#">Active Directory 정책 사용</a> 을 참조하십시오.
프로비저닝된 워크로드에 대한 사용자 지정 IPAM 구성	IPAM 구성이 이제 제품에 내장되어 있습니다. IPAM 구성 단계에 대한 자세한 내용은 <a href="#">타사 IPAM 제공자 지원을 제공하기 위한 검사 목록</a> 을 참조하십시오.
속성 사전의 관계형 표현식 사용	관계형 표현식은 속성 사전에서 더 이상 선택 사항이 아닙니다. 다음은 7.x에서 속성 사전 관계를 개발하는 방법의 예입니다. <a href="#">vRA 7의 속성 관계</a>
사용자 지정 호스트 명명	마이그레이션 후 사용자 지정 호스트 명명에는 다양한 옵션이 있습니다. 이러한 옵션에 대한 개요는 <a href="#">vRealize Automation으로 호스트 이름 관리 - 1부: 옵션 이해하기!</a> 를 참조하십시오.
Application Services 기반 Blueprint 사용	Application Services 기반 Blueprint를 마이그레이션하려면 별도의 마이그레이션 단계가 필요합니다. 마이그레이션 단계에 대한 자세한 내용은 "VMware vRealize Application Services 마이그레이션 도구 1.1 사용자 가이드" 참조하십시오.