

VMware Cloud Director 10.1 릴리스 정보

VMware Cloud Director 10.1 | 2020년 4월 9일 | 빌드 15967253(설치된 빌드 15967236)

이러한 릴리스 정보의 추가 사항 및 업데이트 사항을 확인하십시오.

이 문서에 포함된 내용

- [이 릴리스의 새로운 기능](#)
- [보안](#)
- [제품 지원 고지 사항](#)
- [이전 릴리스에서 업그레이드](#)
- [시스템 요구 사항 및 설치](#)
- [해결된 문제](#)
- [알려진 문제](#)

이 릴리스의 새로운 기능

- 이 릴리스의 새로운 기능 및 업데이트된 기능에 대한 자세한 내용은 VMware 기술 백서 [VMware vCloud Director 10.1의 새로운 기능](#)을 참조하십시오.

- HTML5 UI에서 변경된 동작:

이전 VMware Cloud Director 버전에서는 HTML UI의 vApp 작업 메뉴를 사용하여 vApp을 중지하거나 전원을 끌 수 있습니다. 두 전원 작업 모두 vApp 배포를 해제하지만 vApp에 다르게 영향을 미칩니다. 전원 끄기 작업은 vApp의 가상 시스템에 대한 [시작 및 중지 순서] 설정을 따르지 않습니다. 또한 전원 끄기 작업은 조직 VDC 네트워크에서 모든 VM NIC 연결을 끊고 vApp에 대해 배포된 Edge 게이트웨이를 제거하여 vApp 네트워크 배포를 해제합니다.

VMware Cloud Director 10.1에서, 실행 중인 vApp에서 전원 끄기 작업을 수행하면 vApp 및 여기에 포함된 가상 시스템 배포를 해제하지 않고 vApp에 있는 모든 가상 시스템의 전원이 꺼집니다. 가상 시스템의 NIC는 각 네트워크에 연결된 상태로 유지되며 vApp Edge 게이트웨이는 배포된 상태로 유지됩니다. vApp 및 vApp의 가상 시스템이 배포된 상태로 유지됩니다. vApp의 개별 가상 시스템 각각에 대한 전원 끄기 작업은 활성 상태로 유지되며 이를 사용하여 가상 시스템의 전원을 끌 수 있습니다. 이렇게 하면 가상 시스템 배포가 해제됩니다.

vApp의 전원을 끄면 [전원 끄기] 작업은 [시작 및 중지 순서] 설정에 정의한 시작 순서를 따릅니다. 그 결과, 시작을 위해 구성된 순서의 역순으로 가상 시스템의 전원이 꺼집니다. [전원 끄기] 작업 중에는 [중지 대기] 설정이 적용되지 않습니다. vApp의 전원을 끄면, 여기에 포함된 가상 시스템의 전원 상태에서 파생된 vApp의 전원 상태가 [전원 꺼짐]으로 표시됩니다.

- VMware Cloud Director API 34.0 스키마에 numberOfCpus 및 MemoryAllocationMB 특성에 대한 정의가 포함됩니다.

보안

- **경고:** 버전 10.1로 업그레이드한 후 VMware Cloud Director는 연결된 모든 인프라 끝점에 대한 인증서를 항상 확인합니다. 이는 VMware Cloud Director가 SSL 인증서를 관리하는 방식이 변경되었기 때문입니다. 업그레이드 전에 인증서를 VMware Cloud Director로 가져오지 않으면 SSL 확인 문제로 인해 vCenter Server 및 NSX 연결에 실패한 연결 오류가 표시될 수 있습니다. 이 경우 업그레이드 후 다음 두 가지 옵션이 제공됩니다.
 1. 셸 관리 도구 trust-infra-certs 명령을 실행하여 중앙 집중식 인증서 저장소에 자동으로 연결하고 vCenter Server 및 NSX Manager 인스턴스에 대한 모든 인프라 끝점의 인증서를 검색합니다. [vSphere 리소스에서 끝점 인증서 가져오기](#)를 참조하십시오.
 2. 서비스 제공자 관리자 포털 UI에서 각 vCenter Server 및 NSX 인스턴스를 선택하고 인증서를 수락하는 동안 자격 증명을 다시 입력합니다.
- 버전 10.1부터 서비스 제공자 및 테넌트는 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고, SSL 핸드셰이크의 일부로 서버 ID를 확인할 수 있습니다. VMware Cloud Director 네트워크 연결을 보호하려면 연결 테스트를 위해 VMware Cloud Director API를 사용하는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성합니다. VMware Cloud Director 설치 또는 업그레이드 후 그리고 VMware Cloud Director에 대한 액세스 권한을 테넌트에 부여하기 전에 거부 목록을 구성합니다. [테스트 연결 거부 목록 구성](#)을 참조하십시오.
- VMware Cloud Director 10.1은 모든 SSL 인증서를 신뢰하는 동작을 더 이상 사용하지 않습니다. 이 릴리스에서는 vCenter Server 및 NSX 연결이 이 옵션을 지원하지 않습니다. 다른 모든 연결의 경우에도 모든 인증서 신뢰가 더 이상 사용되지 않으며 VMware Cloud Director 10.1 이후 지원되지 않습니다. 시스템 관리자는 이러한 전환에 대비해야 합니다.
 - VMware Cloud Director 시스템 조직에 대해 LDAP를 사용하는 경우 UI에서 최초 사용 시 신뢰 대화 상자를 사용하거나 API를 사용하여 인증서를 업로드할 수 있습니다.
 - 이 옵션의 모든 사용을 감사하고 UI 또는 API를 사용하여 적절한 인증서를 제공합니다.
 - 테넌트에 변경 내용을 전달합니다. **모든 인증서 수락** 옵션이 사용되도록 설정된 사용자 지정 LDAP를 사용하는 모든 테넌트가 이 구성으로부터 전환해야 합니다. 테넌트는 UI에서 최초 사용 시 신뢰 대화 상자를 사용하거나 API를 통해 인증서를 업로드할 수 있습니다.

오픈 소스 패키지가 업데이트됨

- jackson-databind가 버전 2.9.10.1로 업데이트되었습니다.
- jre가 버전 1.8.0u231로 업데이트되었습니다.
- openssl이 버전 1.0.2u로 업데이트되었습니다.
- xstream이 버전 1.4.11.1로 업데이트되었습니다.

제품 지원 고지 사항

VMware Cloud Director 10.1은 vSphere 7.0 및 NSX-T Data Center 3.0을 지원하지 않습니다. 상호 운용성 인증이 진행 중이며 vSphere 7.0 및 NSX-T Data Center 3.0은 VMware Cloud Director 10.1의 부 패치 릴리스에서 지원될 예정입니다.

NSX-T Data Center의 VRF-lite tier-0 게이트웨이로 지원되는 외부 네트워크는 지원되지 않습니다.

수명 종료 및 지원 종료 경고

- SQL Server 데이터베이스는 더 이상 지원되지 않습니다. PostgreSQL 데이터베이스만 지원됩니다.
- Oracle Linux는 VMware Cloud Director 애플리케이션을 설치하는 호스트 운영 체제로 더 이상 지원되지 않습니다.
- VMware Cloud Director API 버전 20 이하는 지원되지 않습니다.
- VMware Cloud Director API 버전 27.0-29.0은 폐기되며 VMware Cloud Director 10.1 이후에는 지원되지 않을 예정입니다.
- VMware Cloud Director API 버전 30.0은 더 이상 사용되지 않습니다.
- Flex 기반 UI는 제품에서 제거되었으며 더 이상 지원되지 않습니다.
- /api/sessions API 로그인 끝점은 VMware Cloud Director API 버전 33.0/VMware Cloud Director 10.0에서 더 이상 사용되지 않으며 향후의 VMware Cloud Director 릴리스에서 지원되지 않습니다. 서비스 제공자 및 테넌트의 VMware Cloud Director 액세스에 대해 별도의 VMware Cloud Director OpenAPI 로그인 끝점을 사용할 수 있습니다.
- API /cloud/server_status는 HTTP 및 HTTPS 프로토콜 모두에서 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다. HTTP 및 HTTPS 프로토콜에 대해 /api/server_status를 사용해야 합니다.
- 재설정 작업 /ldap/action/resetLdapCertificate 및 /ldap/action/resetLdapKeyStore는 VMware Cloud Director 10.1이 SSL 인증서를 저장하고 처리하는 방식으로 인해 VMware Cloud Director API 버전 34.0에서 제거되었습니다. 인증서에 대한 신뢰를 취소하려면 /cloudapi/1.0.0/ssl/trustedCertificates 끝점을 사용해야 합니다.
- 업데이트 작업 /ldap/action/updateLdapCertificate 및 /ldap/action/updateLdapKeyStore는 더 이상 사용되지 않으며 향후 릴리스에서 지원되지 않습니다. VMware Cloud Director에서는 LDAP 인증서의 신뢰를 위해 새로운 끝점 /cloudapi/1.0.0/ssl/trustedCertificates를 도입했습니다.
- vSphere는 vSphere SSO를 SAML IDP로 더 이상 사용하지 않습니다. vSphere SSO를 SAML IDP로 사용하도록 구성된 모든 VMware Cloud Director 배포는 다른 외부 SAML IDP로 마이그레이션해야 합니다. 향후 vSphere 및 VMware Cloud Director 릴리스에서는 이 IDP 사용이 지원되지 않습니다.
- 사용 가능한 권장 암호 그룹이 없기 때문에 DSA 및 DSS 인증서가 더 이상 지원되지 않습니다.

예정된 지원 종료 알림

- VMware Cloud Director API 34.0(VMware Cloud Director 10.1)에는 점차 폐기되고 있으며 향후 릴리스에서 제거될 API가 포함되어 있습니다. [VMware Cloud Director API 프로그래밍 가이드](#)를 참조하십시오.

이전 릴리스에서 업그레이드

VMware Cloud Director 10.1로의 업그레이드, 업그레이드/마이그레이션 경로 및 워크플로에 대한 자세한 내용은 [VMware Cloud Director 장치 업그레이드 및 마이그레이션](#) 또는 [Linux에서 vCloud Director 업그레이드](#)를 참조하십시오.

시스템 요구 사항 및 설치

포트와 프로토콜

VMware Cloud Director 10.1에서 사용하는 네트워크 포트 및 프로토콜에 대한 자세한 내용은 [VMware Ports and Protocols](#)를 참조하십시오.

호환성 매트릭스

다음에 대한 최신 정보는 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

- 다른 VMware 플랫폼과의 VMware Cloud Director 상호 운용성
- 지원되는 VMware Cloud Director 데이터베이스

지원되는 VMware Cloud Director 서버 운영 체제

- CentOS 6
- CentOS 7
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7

지원되는 AMQP 서버

VMware Cloud Director는 AMQP를 사용하여 확장 서비스, 개체 확장 및 알림에 사용되는 메시지 버스를 제공합니다. 이 VMware Cloud Director 릴리스에는 RabbitMQ 버전 3.7.9 또는 3.8.2가 필요합니다.

자세한 내용은 VMware Cloud Director 설치, 구성 및 업그레이드 설명서를 참조하십시오.

이전 메트릭 데이터를 저장하기 위해 지원되는 데이터베이스

가상 시스템 성능 및 리소스 사용에 대해 VMware Cloud Director가 수집하는 메트릭을 저장하도록 VMware Cloud Director 설치를 구성할 수 있습니다. 이전 메트릭에 대한 데이터는 Cassandra 데이터베이스에 저장됩니다. VMware Cloud Director는 Cassandra 버전 3.x를 지원합니다.

자세한 내용은 VMware Cloud Director 설치, 구성 및 업그레이드 설명서를 참조하십시오.

디스크 공간 요구 사항

설치 및 로그 파일 용도로 VMware Cloud Director 서버 각각에 약 2100MB의 여유 공간이 필요합니다.

메모리 요구 사항

메모리 요구 사항은 *VMware Cloud Director 설치, 구성 및 업그레이드 설명서*를 참조하십시오.

CPU 요구 사항

VMware Cloud Director는 CPU 기반 애플리케이션입니다. 사용 중인 vSphere 버전의 CPU 오버 커밋 지침을 따라야 합니다. 가상화된 환경에서는, VMware Cloud Director에 사용할 수 있는 코어의 수에 관계없이 vCPU와 물리적 CPU의 비율이 합리적인 수준이어야 과도한 오버 커밋이 발생하지 않습니다.

필수 Linux 소프트웨어 패키지

VMware Cloud Director 서버 각각에는 몇 가지 일반적인 Linux 소프트웨어 패키지가 설치되어 있어야 합니다. 대개 이러한 패키지는 운영 체제 소프트웨어와 함께 기본적으로 설치됩니다. 누락된 패키지가 있으면 진단 메시지와 함께 설치 관리자가 실패합니다.

alsa-lib	libICE	module-init-tools
bash	libSM	net-tools
chkconfig	libstdc++	pciutils
coreutils	libX11	procps
findutils	libXau	redhat-lsb
glibc	libXdmcp	sed
grep	libXext	tar
initscripts	libXi	wget
krb5-libs	libXt	which
libgcc	libXtst	

설치 관리자에 필요한 패키지 이외에 네트워크 연결을 구성하고 SSL 인증서를 생성하는 몇 가지 절차에서 Linux nslookup 명령(Linux bind-utils 패키지에 있음)을 사용해야 합니다.

지원되는 LDAP 서버

다음 LDAP 서비스에서 사용자 및 그룹을 VMware Cloud Director로 가져올 수 있습니다.

플랫폼	LDAP 서비스	인증 방법
Windows Server 2012	Active Directory Simple	Simple SSL
Windows Server 2016	Active Directory Simple	Simple SSL
Linux	OpenLDAP	Simple, Simple SSL

지원되는 보안 프로토콜 및 암호 그룹

VMware Cloud Director에서는 클라이언트 연결이 안전해야 합니다. SSL 버전 3 및 TLS 버전 1.0 및 1.1에는 심각한 보안 취약성이 있는 것으로 발견되었기 때문에, 서버가 클라이언트 연결 시 사용하도록 제공하는 기본 프로토콜 집합에 더 이상 포함되지 않습니다. 시스템 관리자는 더 많은 프로토콜과 암호 그룹을 사용하도록 설정할 수 있습니다. *VMware Cloud Director 설치, 구성 및 업그레이드 설명서*에서 "셸 관리 도구" 섹션을 참조하십시오. 다음의 보안 프로토콜이 지원됩니다.

- TLS 버전 1.2

- TLS 버전 1.1(기본적으로 사용하지 않도록 설정됨)
- TLS 버전 1.0(기본적으로 사용하지 않도록 설정됨)

지원되는 암호 그룹은 기본적으로 사용되도록 설정됩니다.

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

시스템 관리자는 셸 관리 도구를 사용하여 기본적으로 사용되지 않도록 설정된 지원되는 다른 암호 그룹을 명시적으로 사용하도록 설정할 수 있습니다.

참고: vCenter Server 5.5-update-3e 이전 릴리스 및 ovftool 4.2 이전 버전과 상호 운용하려면 VMware Cloud Director에서 TLS 버전 1.0을 지원해야 합니다. 지원되는 SSL 프로토콜 또는 암호 집합은 셸 관리 도구를 사용하여 재구성할 수 있습니다. *VMware Cloud Director 설치, 구성 및 업그레이드 설명서*에서 "셸 관리 도구" 섹션을 참조하십시오.

지원되는 브라우저

VMware Cloud Director는 다음 브라우저의 현재 및 이전의 주요 릴리스와 호환됩니다.

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Microsoft Internet Explorer 11

지원되는 게스트 운영 체제 및 가상 하드웨어 버전

VMware Cloud Director는 각 리소스 풀을 뒷받침하는 ESXi 호스트에서 지원하는 모든 게스트 운영 체제 및 가상 하드웨어 버전을 지원합니다.

VMware Cloud Director WebMKS 2.1.1

VMware Cloud Director WebMKS 2.1.1 콘솔은 다음을 추가적으로 지원합니다.

- Windows용 Mozilla Firefox 및 Google Chrome의 PrintScreen 키.
- Windows 및 macOS의 Windows 키. Windows 키 누르기를 시뮬레이션하려면 Windows OS에서 Ctrl+Windows 또는 macOS에서 Ctrl+Command 키를 누릅니다.
- Google Chrome 및 Mozilla Firefox에서 자동 키보드 레이아웃 감지.

해결된 문제

- **두 개의 VMware Cloud Director 장치 사이트를 연결하면 개체가 사이트 전체에 표시되지 않음**
사이트 연결을 설정하고 사이트에 개체(예: 조직, 조직 VDC, vApp, VM 등)가 있는 경우 현재 사이트에서 해당 개체를 볼 수 없습니다. HTML 5 UI는 연결된 다른 사이트의 개체만 표시합니다. 이 문제는 다중 사이트 팬아웃 통신 중에 발생합니다. VMware Cloud Director 장치의 /etc/hosts 파일에 올바른 콘텐츠가 없기 때문입니다.
- **메모리 할당 오류로 인해 VM 크기 조정 정책 업데이트가 실패함**
할당 풀 VDC를 Flex 조직 VDC로 변환하면, vCloud Director는 변환 전에 할당 풀 VDC의 최대 정책 정보를 유지합니다. 할당 풀 VDC에 정의된 예약보다 높은 CPU 또는 메모리 예약 보장은 가상 시스템 예약, 제한 또는 할당을 설정이 잘못되었습니다. 오류가 발생하면서 실패합니다.
- **다중 셀 환경에서 기본 셀을 중지 또는 일시 중지할 때 정기 작업이 보조 셀에서 다시 시작되지 않음**
다중 셀 환경에서 기본 셀을 중지하거나 일시 중지할 때 기본 셀의 백그라운드에서 실행 중인 정기 작업이 보조 셀에서 시작되지 않습니다.
- **데이터 서비스가 사용되도록 설정된 호스트 기반 스토리지 정책의 VM을 다른 호스트 기반 스토리지 정책이 있는 VM으로 복제하면 작업이 실패하고 오류가 발생함**
IOPS 또는 VM 암호화와 같은 호스트 기반 규칙이 사용되도록 설정된 스토리지 정책에 있는 VM을 생성하는 경우 VM을 복제하고 대상 VM의 스토리지 정책을 변경하려고 하면 복제 작업 중에는 데이터 서비스 기능이 포함된 VM 스토리지 정책 변경 또는 적용이 허용되지 않습니다. 오류가 발생하며 작업이 실패합니다. 데이터 서비스 기능이 포함된 VM 스토리지 정책은 복제 작업이 완료된 후 그리고 VM의 전원이 켜지기 전에 프로비저닝된 VM에 할당될 수 있습니다.
- **글로벌 테넌트 역할 vApp 작성자에게 템플릿과 미디어에 대한 업로드 권한과 생성 권한이 없는데도 이러한 작업을 수행할 수 있음**
글로벌 테넌트 역할 vApp 작성자에게는 기본적으로 내 클라우드의 vApp 추가 권한이 있습니다. 이 권한 및 템플릿/미디어: 생성/업로드 권한이 단일 작업을 공유하기 때문에 VMware Cloud Director가 템플릿/미디어: 생성/업로드 권한도 vApp 작성자 역할에 잘못 부여합니다.

이 문제는 해결되었습니다. vApp 작성자 역할에 템플릿/미디어: 생성/업로드 권한을 계속해서 포함하려는 경우 서비스 제공자가 해당 권한을 vApp 작성자 글로벌 역할에 추가하고 조직에 게시할 수 있습니다.
- **새로 생성된 가상 시스템이 조직 VDC 기본 스토리지 정책에 배포됨**
vCloud Director 테넌트 포털에서 독립형 가상 시스템을 새로 생성할 때 스토리지 정책을 지정하는 옵션이 없습니다. 따라서, 생성된 가상 시스템이 조직 VDC의 기본 스토리지 정책으로 배포됩니다.

알려진 문제

- **새로운 항목 Microsoft Internet Explorer 11을 사용하는 경우 VM 웹 콘솔을 열 수 없음**
Microsoft Internet Explorer 11을 사용하여 VM 콘솔에 연결하면 흰색 빈 창이 열리고 VM 콘솔에 액세스할 수 없습니다.

해결 방법: 없음.

- **새로운 항목** 예약 풀 VDC를 Flex 조직 VDC로 변환한 후 VM이 비준수 상태가 됨
예약 풀 할당 모델을 사용하는 조직 VDC에서 일부 VM에 CPU 및 메모리에 대한 예약이 0이 아닌 경우, CPU 및 메모리에 대한 무제한 구성(또는 둘 다)이 있는 경우 Flex 조직 VDC로 변환한 후 이러한 VM은 비준수 상태가 됩니다. VM을 다시 준수 상태로 만들려고 하면 시스템에서 예약 및 제한에 대해 잘못된 정책이 적용되고 CPU 및 메모리 예약이 0으로 설정되고 제한이 **무제한**으로 설정됩니다.

해결 방법:

1. 시스템 관리자가 올바른 구성으로 VM 크기 조정 정책을 만들어야 합니다.
 2. 시스템 관리자가 변환된 Flex 조직 VDC에 새 VM 크기 조정 정책을 게시해야 합니다.
 3. 테넌트는 VMware Cloud Director API 또는 VMware Cloud Director 테넌트 포털을 사용하여 Flex 조직 VDC의 기존 가상 시스템에 VM 크기 조정 정책을 할당할 수 있습니다.
- **새로운 항목** 테넌트 포털 UI에서 선호도 또는 반선호도 규칙을 생성할 때 [필수] 확인란을 선택 취소해도 규칙 구성이 영향을 받지 않음
테넌트 포털 UI에서 선호도 또는 반선호도 규칙을 생성할 때 [필수] 확인란을 선택 취소해도 규칙 구성이 영향을 받지 않습니다. 선호도 및 반선호도 규칙은 항상 필수입니다. 즉, 규칙이 충족되지 않으면 규칙에 추가된 VM의 전원이 켜지지 않습니다.

해결 방법: 없음.

- **새로운 항목** VMware Cloud Director API를 사용하여 vApp을 쿼리하면 numberOfCpus 및 MemoryAllocationMB 특성에 대해 빈 필드가 반환됨
VMware Cloud Director API 33.0 또는 이전 버전을 사용하여 vApp REST API 쿼리를 실행하는 경우 REST API 응답 본문의 numberOfCpus 및 MemoryAllocationMB 특성에 빈 필드가 반환됩니다. 이 문제는 numberOfCpus 및 MemoryAllocationMB 특성에 대한 정의가 API 스키마에 포함되어 있지 않기 때문에 발생할 수 있습니다.

해결 방법: VMware Cloud Director API 34.0을 사용하여 vApp을 쿼리합니다.

- **새로운 항목** NSX-T Edge 게이트웨이에 NAT 규칙을 추가하려고 하면 실패함
NSX-T Edge 게이트웨이에 NAT 규칙을 추가하려고 하면 실패하고 다음 오류 메시지가 표시됩니다. "재배포를 위해 새 값 및 폐기된 값이 업데이트되었습니다. 오류 코드 503266".

해결 방법: NSX-T Data Center 정책 API를 사용하여 NSX-T Edge 게이트웨이가 연결된 외부 네트워크의 재배포 구성을 업데이트합니다.

1. NSX-T Edge 게이트웨이가 연결된 외부 네트워크를 지원하는 Tier-0 라우터의 ID를 적어둡니다.
 - GET 요청을 수행하여 작업 환경에서 Tier-0 라우터 목록을 가져옵니다.
GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s
 - 목록을 검토하여 VMware Cloud Director UI에서 외부 네트워크에 대한 [일반 정보] 탭의 Tier-0 라우터 이름과 일치하는 표시 이름으로 Tier-0을 식별합니다.
2. 외부 네트워크(Tier-0 게이트웨이)를 수동으로 업데이트합니다.
 - GET 요청을 수행하여 라우터에서 localeServices 목록을 가져옵니다.
GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services
응답은 로케일 서비스 하나를 반환합니다.

- localeService ID를 복사하고 GET 요청을 수행하여 검사합니다.

GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services/<LocaleServiceId>.

응답은 로케일 서비스에 대한 속성 목록을 반환합니다.

```
{
  "route_redistribution_config": {
    "bgp_enabled": true,
    "enabled": true,
    "redistribution_rules": [
      {
        "name": "some-name",
        "route_redistribution_types": [
          "TIER1_DNS_FORWARDER_IP",
          "TIER1_NAT",
          "TIER1_STATIC"
        ]
      }
    ]
  },
  ...
}
```

- 다음과 같이 응답을 수정합니다.

```
{
  "route_redistribution_config": null,
  "route_redistribution_types": [
    "TIER1_DNS_FORWARDER_IP",
    "TIER1_NAT",
    "TIER1_STATIC"
  ],
  ...
}
```

- 수정된 속성으로 PUT 요청을 수행하여 Tier-0 라우터의 localeService를 업데이트합니다.

- **새로운 항목** 대상 스토리지 컨테이너가 데이터스토어 클러스터인 경우 가상 시스템을 다른 클러스터로 재배포하면 실패함

가상 시스템을 다른 클러스터로 재배포하려는 작업을 수행하는 경우 대상 스토리지 컨테이너가 데이터스토어 클러스터이면, 마이그레이션이 실패하고 NO_FEASIBLE_PLACEMENT_SOLUTION 오류가 표시됩니다. VMware Cloud Director 로그에 invalidProperty = spec.host가 포함된 Storage DRS 호출 오류가 표시됩니다.

해결 방법:

1. vSphere Client를 사용하여 대상 데이터스토어 클러스터에서 Storage DRS를 사용하지 않도록 설정하거나 VMware Cloud Director API를 사용하여 재배포 대상 스토리지를 데이터스토어로 변경합니다.

2. 실패한 작업을 다시 시도합니다.

- **새로운 항목** 처음 로그인 시 루트 암호가 만료되도록 하는 설정을 활성화하면 VMware Cloud Director 장치 배포가 실패함

처음 로그인 시 루트 암호 만료 설정이 활성화된 장치를 배포하려고 하면 배포가 실패하고 /opt/vmware/var/log/firstboot 로그 파일에 다음과 같은 오류가 표시됩니다.

[ERROR] postgresauth script failed to execute.

해결 방법: **처음 로그인 시 루트 암호 만료** 설정을 비활성화하고, 대문자 1개, 소문자 1개, 숫자 1개, 특수 문자 1개를 포함하는 8자 이상의 초기 루트 암호를 지정합니다.

- **새로운 항목** vApp 사용자가 템플릿에서 vApp을 생성하려고 할 때 "작업이 거부됨" 메시지가 나타날 수 있음

할당된 사용자 역할이 vApp 사용자일 때 템플릿에서 vApp을 생성하려고 시도하고 vApp의 가상 시스템에 대해 VM 크기 조정 정책을 사용자 지정하면 "작업이 거부됨" 메시지가 나타납니다. 이 문제는 vApp 사용자 역할로 템플릿에서 vApp을 인스턴스화할 수 있지만 가상 시스템의 메모리, CPU 또는 하드 디스크를 사용자 지정할 수 있는 권한은 이 역할에 포함되지 않기 때문에 발생합니다. 크기 조정 정책을 변경하면 가상 시스템 메모리 또는 CPU를 변경할 수 있습니다.

해결 방법: 없음.

- **새로운 항목** NFS 다운타임으로 인해 VMware Cloud Director 장치 클러스터 기능이 오작동할 수 있음

NFS 공유가 켜져 있거나 읽기 전용 전환 등으로 NFS를 사용할 수 없는 경우에는 장치 클러스터 기능이 오작동할 수 있습니다. NFS가 다운되었거나 NFS에 연결할 수 없으면 HTML5 UI가 응답하지 않습니다. 실패한 기본 셀 펜싱, 전환, 대기 셀 승격 등과 같은 기능도 영향을 받을 수 있습니다. NFS 공유 스토리지를 올바르게 설정하는 방법에 대한 자세한 내용은 [VMware Cloud Director 장치의 전송 서버 스토리지 준비](#)를 참조하십시오.

해결 방법:

- 읽기 전용이 되지 않도록 NFS 상태를 수정합니다.
- NFS 공유가 켜진 경우 NFS 공유를 정리합니다.

- **새로운 항목** 다중 사이트 환경에서 vCenter Server 및 NSX 리소스를 추가하는 동안 끝점을 신뢰할 경우 해당 끝점이 중앙 집중식 인증서 스토리지 영역에 추가되지 않음

다중 사이트 환경에서 HTML5 UI를 사용하는 동안 vCloud Director 10.0 사이트에 로그인했거나 vCenter Server 인스턴스를 vCloud Director 10.0 사이트에 등록하려는 경우 VMware Cloud Director가 끝점을 중앙 집중식 인증서 스토리지 영역에 추가하지 않습니다.

해결 방법:

- API를 사용하여 VMware Cloud Director 10.1 사이트로 인증서를 가져옵니다.
- 인증서 관리 기능을 트리거하려면 VMware Cloud Director 10.1 사이트의 SP 관리자 포털로 이동하고 서비스의 **편집** 대화 상자로 이동한 후 **저장**을 클릭합니다.

- **새로운 항목** vCenter Server 6.5 이하 버전에서 명명된 디스크를 암호화하려고 하면 오류와 함께 실패함

vCenter Server 인스턴스 6.5 이하 버전에서 새로운 또는 기존의 명명된 디스크를 암호화 지원 정책에 연결하려고 하면 작업이 실패하고 이 vCenter Server 버전에서는 명명된 디스크 암호화가 지원되지 않습니다. 오류가 표시됩니다.

해결 방법: 없음.

- **새로운 항목** VMware Cloud Director 버전 10.0 및 10.1을 사용하는 혼합된 다중 사이트 환경에서, vCenter Server 및 NSX 연결에 대한 인증서 신뢰가 로컬 사이트의 개체에 대해서만 작동함
VMware Cloud Director 버전 10.0과 10.1이 서로 연결되어 있는 다중 사이트 환경을 사용하는 경우, 이러한 사이트 중 하나에 로그인하면 다른 사이트에서 vCenter Server 또는 NSX Manager 인스턴스를 등록할 수 없습니다.

해결 방법: vCenter Server 또는 NSX Manager 인스턴스를 등록하려는 사이트에 로그인하고 등록 프로세스를 시작합니다.

- **새로운 항목** VMware Cloud Director 테넌트 포털에서 [애플리케이션] 탭의 가상 시스템에 대한 고급 필터링 옵션을 통해 데이터 센터별로 VM을 필터링할 수 없음

VMware Cloud Director 테넌트 포털에서 위쪽 탐색 모음의 [애플리케이션] 탭 아래 가상 시스템으로 이동하여, 고급 필터링 옵션에서 데이터 센터별로 가상 시스템을 필터링하면 다음 오류가 발생합니다. 잘못된 요청: 알 수 없는 속성 이름 vdcName입니다..

해결 방법: 위쪽 탐색 모음에서 데이터 센터를 선택하고 데이터 센터를 선택하여 가상 시스템을 봅니다.

- **새로운 항목** 확장 서비스가 VMware Cloud Director의 RabbitMQ 메시지를 처리할 수 없음

RabbitMQ에 의존하는 확장 서비스가 메시지의 notification.type 헤더를 가져올 수 없습니다. 헤더에 새 임시 이름이 있기 때문입니다. VMware Cloud Director 10.1.0의 헤더 이름은 notification.operationType입니다.

해결 방법: 확장 서비스에서 VMware Cloud Director의 RabbitMQ 메시지를 처리하고 notification.type 메시지 헤더를 사용하는 경우 이를 변경해야 합니다. notification.type 헤더를 사용할 수 없는 경우 확장 서비스는 헤더 notification.operationType에서 값을 가져와야 합니다. 이 변경은 버전 10.1.0에만 필요합니다.

- **VMware Cloud Director 서비스 제공자 관리자 포털에서, 조직 가상 데이터 센터 삭제가 실패하고 오류가 발생함**

VMware Cloud Director 서비스 제공자 관리자 포털에서 조직 VDC에 Edge 게이트웨이를 추가하고 게이트웨이가 VMware Cloud Director 분산 라우팅을 제공하도록 설정한 경우, 조직 VDC를 삭제하려고 하면 실패하고 조직 VDC 네트워크를 삭제할 수 없습니다. 오류 메시지가 표시됩니다.

해결 방법:

1. API를 사용하여 조직 VDC 네트워크 및 조직 VDC와 연결된 Edge 게이트웨이를 삭제합니다.
2. API를 사용하여 조직 VDC를 삭제합니다.

- **제공자가 레거시 API 로그인 끝점에 액세스할 수 없도록 설정하면, 시스템 관리자 로그인에 의존하는 모든 API 통합이 작동을 멈춤(예: vCloud Usage Meter 및 vCloud Availability for VMware Cloud Director)**

vCloud Director 10.0부터는 서비스 제공자와 테넌트가 VMware Cloud Director에 액세스하는 데 별도의 VMware Cloud Director OpenAPI 로그인 끝점을 사용할 수 있습니다. 서비스 제공자가 레거시 /api/sessions 끝점에 액세스할 수 없도록 설정되면 VMware Cloud Director와 통합된 제품(예: vCloud Usage Meter 및 vCloud Availability for VMware Cloud Director)이 작동을 중지합니다. 이러한 제품을 계속 작동하려면 패치가 필요합니다.

이 문제는 시스템 관리자에게만 영향을 줍니다. 테넌트 로그인에 영향을 받지 않습니다.

해결 방법: 셸 관리 도구를 사용하여 서비스 제공자가 레거시 `/api/sessions` 끝점에 액세스할 수 있도록 다시 설정합니다.

- **VDC의 예약 보장 값을 변경하는 경우, 재부팅 후에도 기존 VM이 그에 따라 업데이트되지 않음**
시스템 기본 정책을 사용하는 Flex 조직 VDC가 있고 이 VDC의 전원이 켜진 가상 시스템에 기본 크기 조정 정책을 사용하는 경우, VDC의 리소스 보장 값을 늘리면 기존 VM에 대한 리소스 예약이 업데이트되지 않고 비준수로 표시도 되지 않습니다. 이 문제는 레거시 VDC 할당 모델을 Flex 할당 모델로 변환하고 기존 VM이 변환 후 Flex 조직 VDC의 새로운 기본 정책을 준수하지 않는 상태가 되어도 발생합니다.

해결 방법:

1. VM 식별자를 찾으려면 VMware Cloud Director 테넌트 포털에서 VM의 세부 정보 페이지로 이동합니다. URL에 식별자가 표시됩니다.
`https://Cloud_Director_IP_address_or_host_name/tenant/.../vm-Identifier/general`
2. VMware Cloud Director UI에서 비준수 VM을 표시하려면 VMware Cloud Director API를 사용하여 VM에 대해 명시적인 규정 준수 검사를 수행합니다.
POST: `https://VCD_IP_Address/api/vApp/vm-Identifier/action/checkComputePolicyCompliance`
3. VMware Cloud Director 테넌트 포털에서 정책을 다시 적용하고 리소스 예약을 다시 구성하려면 비준수 VM에 대해 **VM이 규정을 준수하도록 설정**을 클릭합니다.

- **전용 vCenter Server 인스턴스에서 실행 중인 VM, 총 VM, CPU 및 메모리 통계에 대한 정보가 VMware Cloud Director에 잘못 표시됨**

전용 vCenter Server 인스턴스 버전이 6.0 업데이트 3i 이하, 6.5 업데이트 2 이하 또는 6.7 업데이트 1 이하인 경우에는 vCenter Server 인스턴스에서 실행 중인 VM, 총 VM과 CPU 및 메모리 통계에 대한 정보가 VMware Cloud Director에 잘못 표시됩니다. 테넌트 포털의 전용 vCenter Server 타일과 서비스 제공자 관리 포털의 전용 vCenter Server 정보는 실행 중인 VM과 총 VM 모두에 대해 0을 표시하며, vSphere 환경에 가상 시스템이 있는 경우에도 마찬가지입니다.

해결 방법: vCenter Server 인스턴스를 버전 6.0 업데이트 3j, 6.5 업데이트 3, 6.7 업데이트 2 이상으로 업그레이드합니다.

- **전원이 켜진 VM의 계산 정책 변경이 실패할 수 있음**

전원이 켜진 VM의 계산 정책을 변경하려고 할 때 새 계산 정책이 VM 그룹 또는 논리적 VM 그룹이 있는 제공자 VDC 계산 정책과 연결된 경우 오류가 발생합니다. 오류 메시지는 다음이 포함됩니다. 기본 시스템 오류: `com.vmware.vim.binding.vim.fault.VmHostAffinityRuleViolation`.

해결 방법: VM의 전원을 끈 후 작업을 다시 시도합니다.

- **Firefox에서 VMware Cloud Director 서비스 제공자 관리자 포털을 사용하는 경우 테넌트 네트워킹 화면을 로드할 수 없음**

Firefox에서 VMware Cloud Director 서비스 제공자 관리자 포털을 사용하는 경우 테넌트 네트워킹 화면(예: 조직 가상 데이터 센터에 대한 **방화벽 관리** 화면)이 로드되지 않을 수 있습니다. 이 문제는 Firefox 브라우저가 타사 쿠키를 차단하도록 구성된 경우에 발생합니다.

해결 방법: 타사 쿠키를 허용하도록 Firefox 브라우저를 구성합니다.

- **VMware Cloud Director 10.1이 vRealize Orchestrator 워크플로의 입력 매개 변수 목록만 지원함**
VMware Cloud Director 10.1은 vRealize Orchestrator 워크플로의 다음 입력 매개 변수를 지원합니다.

- boolean
- sdkObject
- secureString
- number
- mimeTypeAttachment
- properties
- date
- composite
- regex
- encryptedString
- array

해결 방법: 없음

- **VMware VAAI(vSphere Storage APIs Array Integration) 지원 NFS 어레이 또는 VVols(vSphere Virtual Volumes)에 생성된 빠른 프로비저닝 가상 시스템을 통합할 수 없음**

네이티브 스냅샷을 사용하는 경우 빠른 프로비저닝 가상 시스템의 인플레이스 통합이 지원되지 않습니다. 네이티브 스냅샷은 VVols뿐 아니라 VAAI 지원 데이터스토어에서도 항상 사용됩니다. 빠른 프로비저닝 가상 시스템이 이러한 스토리지 컨테이너 중 하나에 배포되는 경우 해당 가상 시스템을 통합할 수 없습니다.

해결 방법: VAAI 지원 NFS 또는 VVols를 사용하는 조직 VDC에 빠른 프로비저닝을 사용하도록 설정하지 마십시오. VAAI 또는 VVol 데이터스토어에서 가상 시스템을 스냅샷과 통합하려면 가상 시스템을 다른 스토리지 컨테이너로 재배포합니다.

- **VMware Cloud Director API를 사용하여 템플릿에서 VM을 생성하고 기본 스토리지 정책을 지정하지 않은 경우 템플릿에 대해 설정된 기본 스토리지 정책이 없으면 새로 생성된 VM은 소스 템플릿 자체의 스토리지 정책을 사용하려고 시도함**

VMware Cloud Director API를 사용하여 템플릿에서 VM을 생성하고 기본 스토리지 정책을 지정하지 않은 경우 템플릿에 대해 설정된 기본 스토리지 정책이 없으면 새로 생성된 VM은 배포 중인 조직 VDC의 스토리지 정책을 사용하는 대신 소스 템플릿 자체의 스토리지 정책을 사용하려고 시도합니다.

해결 방법: 없음.