

VMware Cloud Services 콘 솔 사용

VMware Cloud services

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 Cloud Services Console란? 6
- 2 VMware Cloud Services에 등록하는 방법 7
 - VMware Cloud Services에서 사용자로 온보딩하는 방법 8
 - 페더레이션된 계정이 있는 사용자로 온보딩하는 방법 8
- 3 Cloud Services 콘솔에 로그인하는 방법 10
- 4 Cloud Services 조직이란? 11
- 5 Cloud Services 카탈로그를 사용하는 방법 12
 - 내가 사용할 수 있는 서비스 카탈로그 작업 12
 - 추가 역할을 요청하는 방법 14
- 6 내 Cloud Services 계정을 관리하는 방법 15
 - 내 사용자 프로필을 보는 방법 15
 - 내 암호를 재설정하는 방법 16
 - 언어 및 국가별 형식을 변경하는 방법 16
 - 다단계 인증을 사용하여 내 계정을 보호하는 방법 17
 - 사용할 수 있는 2단계 인증 애플리케이션 18
 - 로그인할 수 없는 경우 MFA 문제를 해결하는 방법 19
 - API 토큰을 생성하는 방법 19
 - 내 API 토큰을 관리하는 방법 21
 - 다단계 인증을 사용하여 API 토큰을 보호하는 방법 22
 - 조직에서 내 역할을 관리하는 방법 23
 - 거버넌스가 활성화된 조직에서 역할을 요청하는 방법 24
- 7 내 Cloud Services 조직을 관리하는 방법 25
 - 내 조직 중 다른 조직에 액세스하는 방법 26
 - 기본 조직을 지정하는 방법 26
 - VMware Cloud Services 헤더를 사용자 지정하는 방법 26
- 8 내 클라우드 서비스용 소프트웨어 바이너리 다운로드와 관련된 사항 28
 - VMware Cloud Services용 추가 소프트웨어를 다운로드하는 방법 29
- 9 VMware Cloud Services 개발자 센터에서 작업하는 방법 30
 - API 탐색기에 대해 알아두어야 할 사항 31

- 개발 센터에서 사용할 수 있는 API 32
- 개발자 센터에서 API를 시도하는 방법 33

10 ID 및 액세스 관리 36

- 역할 및 사용 권한을 관리하는 방법 36
 - VMware Cloud Services에서 사용할 수 있는 조직 역할 37
- 내 조직의 사용자를 관리하는 방법 38
 - 내 조직에 사용자를 추가하는 방법 39
 - 내 조직에서 사용자를 제거하는 방법 40
 - 사용자 역할을 변경하는 방법 40
- 그룹을 사용하는 방법 41
 - 새 그룹을 생성하는 방법 42
 - 엔터프라이즈 그룹에 역할을 할당하는 방법 43
 - 공유 그룹을 관리하는 방법 44
- 내 조직에서 인증 정책을 설정하는 방법 45
 - 다단계 인증을 설정하는 방법 45
 - IP 인증 기본 설정을 정의하는 방법 46
 - 도메인 수준에서 사용자 액세스를 관리하는 방법 48
- 엔터프라이즈 페더레이션 소개 및 VMware Cloud Services에서 작동하는 방식 48
 - 회사 도메인에 대한 엔터프라이즈 페더레이션 설정과 관련된 사항 49
 - 내 VMware ID를 연결해야 하는 이유 51
 - 회사 ID 제공자를 연결해야 하는 이유 52
- ID 거버넌스 및 관리 소개 및 VMware Cloud Services에서 작동하는 방식 52
 - 내 조직에서 고급 ID 거버넌스 및 관리를 활성화하는 방법 53
 - 추가 역할에 대한 셀프 서비스 요청을 관리하는 방법 53
 - 내 조직에서 정책 위반을 모니터링하는 방법 54
 - 내 조직에서 정책 위반에 대해 조치를 취하는 방법 55
 - 조직에서 API 토큰을 관리하는 방법 56
 - 조직에서 기본 역할을 할당하는 방법 57
- OAuth 2.0으로 애플리케이션을 인증하는 방법 58
 - OAuth 2.0 애플리케이션을 관리하는 방법 60
 - 서버 대 서버 애플리케이션에 OAuth 2.0을 사용하는 방법 61
 - 웹 애플리케이션에 OAuth 2.0을 사용하는 방법 63
 - 네이티브 및 모바일 애플리케이션에 OAuth 2.0을 사용하는 방법 64
 - OAuth 애플리케이션과 API 토큰의 차이점 65
- VMware Cloud Services의 감사 이벤트 로그 작동 방식 65
 - VMware Cloud Services에서 캡처되는 감사 이벤트 66
- VMware Cloud Services에서 NIST 로그인 전 알림을 생성하는 방법 70
- 데이터 인사이트 대시보드를 사용하는 방법 71
 - 데이터 인사이트 대시보드에서 수행할 수 있는 기타 작업 71

11 청구 및 구독 75

VMware Cloud Services 청구 및 구독 시작 75

주소 유효성 검사에 대해 알아두어야 할 사항 76

VMware Cloud Services에서 청구 및 구독 페이지를 사용하는 방법 77

조직에 대한 청구 정보를 가져오는 방법 78

내 현재 비용이 계산되는 방식 79

지불 통화가 결정되는 방식 79

판매자 정보를 보는 방법 82

VMware를 판매자로 추가하는 방법 85

내 조직의 지불 방법을 관리하는 방법 86

새 지불 방법을 추가하는 방법 87

기본 지불 방법 소개 88

송장으로 지불하는 방법 89

신용 카드로 지불하는 방법 90

프로모션 크레딧으로 지불하는 방법 91

VMware 펀드에 대해 알아두어야 할 사항 92

VMware Cloud Services 구독 및 약정을 사용하는 방법 95

조직의 서비스에 대한 구독 세부 정보를 보는 방법 95

약정을 설정하는 방법 96

구독을 구매하는 방법 97

조직에 약정을 적용해야 하는 이유 98

구독 갱신 기본 설정을 변경하는 방법 99

청구 모델이란? 99

[사용량 관리] 대시보드를 사용하는 방법 100

[상위 약정 사용량 유형] 차트에 대해 알아두어야 할 사항 102

현재 사용량 테이블에 대해 알아두어야 할 사항 103

현재 사용량 및 기간별 사용량 세부 정보에 대해 알아두어야 할 사항 104

사용량 관리 FAQ 107

명세서 및 송장을 보는 방법 108

내 사용 명세서를 읽는 방법 110

송장에 PO 번호를 삽입하는 방법 112

12 지원을 받는 방법 114

13 피드백을 제공하는 방법 117

Cloud Services Console란?

1

VMware Cloud Services 콘솔을 사용하면 하이브리드 및 네이티브 공용 클라우드 전반에 걸쳐 전체 VMware Cloud services 포트폴리오를 관리할 수 있습니다.

사용자 및 그룹을 관리하고, 사용자 및 그룹에게 조직 리소스 및 서비스에 대한 역할을 할당하고, 조직에 액세스할 수 있는 OAuth 앱을 보는 데 대한 자세한 내용은 [ID 및 액세스 관리](#) 설명서를 참조하십시오.

현재 비용 및 마지막 청구 내역에 대한 정보를 찾으십니까? 지불 방법을 관리하거나 기본 지불 방법을 변경해야 합니까? 프로모션 크레딧 및 약정 추가에 대한 정보를 원하십니까? [청구 및 구독](#) 설명서를 참조하십시오.

조직을 관리하고, 조직에 OAuth 애플리케이션을 생성하고, 둘 이상의 조직에 속하는 경우 조직 간에 전환하는 데 대한 자세한 내용은 [조직 관리](#)를 참조하십시오.

언어 및 국가별 형식을 변경하고, MFA로 계정을 보호하고, API 토큰을 생성하고, 사용자 프로파일을 편집하시겠습니까? 여기에서 모두 제공됩니다! [계정을 관리](#)하는 방법을 확인하십시오.

VMware Cloud Services에 등록하는 방법

2

VMware Cloud에서는 클라우드로 마이그레이션하거나, 멀티 클라우드 작업을 수행하거나, 요청 시 확장하거나, 현대적인 앱을 구축하는 등의 다양한 작업이 가능합니다.

VMware Cloud services 사용을 시작하는 방법에는 여러 가지가 있습니다. 신규 또는 기존 VMware Cloud services 사용자는 다음 중 하나를 수행하여 서비스를 온보딩할 수 있습니다.

- VMware 마케팅 웹 사이트에서 서비스를 구매합니다.
- VMware 마케팅 웹 사이트에서 무료 또는 평가판 서비스에 등록합니다.
- VMware Sales에서 서비스를 구매합니다.
- VMware 파트너 리셀러에서 서비스를 구매합니다.

온보딩하는 서비스에 따라 온보딩 워크플로에 차이가 있을 수 있습니다.

귀사에서 VMware Cloud services를 이미 사용하는 경우에는 조직에 대한 액세스를 요청하여 기존 조직에서 직접 온보딩할 수 있습니다. VMware Cloud services 조직에 대한 최초 액세스 권한을 요청하고 받는 절차는 계정에 따라 다를 수 있습니다.

- 계정이 페더레이션되지 않은 경우 VMware Cloud Services에서 **사용자로 온보딩하는 방법** 항목을 참조하십시오.
- 계정이 페더레이션된 경우 **페더레이션된 계정이 있는 사용자로 온보딩하는 방법** 항목을 참조하십시오.

서비스 온보딩을 통해 VMware Cloud services에 등록하는 일반적인 단계의 순서는 다음과 같습니다.

절차

- 1 서비스 가입 또는 초대 링크에서 온보딩 프로세스를 시작합니다.
- 2 VMware 계정이 없으면 단계에 따라 계정을 생성합니다.
- 3 VMware 계정이 이미 있으면 VMware Cloud Services에 로그인합니다.
- 4 서비스를 온보딩할 VMware Cloud services 조직을 생성하거나 선택합니다.
- 5 조직에서 서비스를 온보딩하면 다른 사용자를 초대하고 조직 및 해당 서비스에 대한 액세스를 허용할 수 있는 조직 소유자가 됩니다.
 - a 기본 왼쪽 메뉴에서 **ID 및 액세스 > 활성 사용자**를 선택합니다.
 - b **사용자 추가**를 클릭합니다.

- c 초대하려는 사용자의 이메일 주소를 입력합니다.
- d 조직 및 서비스 역할을 선택합니다.
- e 새 사용자에게 보낼 이메일 초대의 확인란을 선택하고 **추가**를 클릭합니다.

할당된 역할로 조직에서 직접 온보딩할 수 있는 링크가 포함된 초대 이메일을 사용자가 받게 됩니다.

다음에 수행할 작업

다양한 서비스 온보딩 워크플로에 대한 자세한 내용 및 자세한 절차는 [VMware Cloud Services 시작 가이드](#)를 참조하십시오.

VMware Cloud Services에서 사용자로 온보딩하는 방법

조직에 대한 액세스 권한이 없고 페더레이션되지 않은 계정에 대한 액세스 권한이 없는 새 사용자로 VMware Cloud Services를 사용하려면 먼저 **조직 소유자**인 사용자로부터 조직 및 서비스 액세스 권한을 얻어야 합니다.

VMware Cloud Services에 대한 초기 액세스 요청은 오프라인 프로세스이며 사용자 또는 **조직 소유자**가 시작할 수 있습니다. 일반적으로 **조직 소유자**가 조직에서 사용자에게 조직 및 서비스 역할을 부여하면 사용자는 조직에 대한 링크가 포함된 이메일을 받게 됩니다.

- 1 **내 역할 보기** 링크를 클릭하여 조직에 액세스합니다.
- 2 VMware 계정이 없으면 계정을 생성하라는 메시지가 나타납니다.
- 3 이미 VMware 계정이 있으면 조직에 로그인하고 부여받은 조직 역할 및 서비스 액세스 권한에 따라 서비스 사용을 시작할 수 있습니다.

조직에서 추가 역할을 요청하려면 [추가 역할을 요청하는 방법](#) 항목을 참조하십시오.

페더레이션된 계정이 있는 사용자로 온보딩하는 방법

페더레이션된 도메인을 사용하는 조직 이외의 사용자인 경우 회사 계정으로 VMware Cloud services에 처음 로그인하면 온보딩 워크플로가 열립니다.

온보딩 프로세스 중에 조직, 서비스, 조직 및 서비스 역할을 자체적으로 선택하여 액세스를 요청합니다. **조직 소유자**가 요청을 승인해야 하며 시간이 걸릴 수 있습니다.

온보딩 워크플로에서 선택 가능한 조직은 IGA(ID 거버넌스 및 관리)가 활성화된 엔터프라이즈 페더레이션된 도메인의 조직입니다. IGA가 활성화되지 않은 조직에 대한 액세스 권한을 얻어야 하는 경우 온보딩할 **조직 소유자**로부터 초대 링크를 받아야 합니다.

절차

- 1 <https://cloud.vmware.com/> 항목으로 이동하고 **로그인**을 클릭합니다.
- 2 VMware Cloud services 시작 화면에서 회사 계정 자격 증명을 입력합니다.
온보딩 워크플로의 첫 번째 단계에서는 엔터프라이즈와 연결된 IGA가 활성화된 조직 목록이 표시됩니다.
- 3 액세스하려는 조직을 선택하고 **계속**을 클릭합니다.

4 선택한 조직에서 역할을 선택합니다.

조직 역할에 따라 조직의 액세스 및 사용 권한 수준이 결정됩니다. 페더레이션된 계정으로 온보딩하는 경우 기본 **조직 멤버** 역할만 요청할 수 있습니다. 온보딩 후 추가 역할을 요청할 수 있습니다. 자세한 내용은 [거버넌스가 활성화된 조직에서 역할을 요청하는 방법](#)의 내용을 참조하십시오.

5 **계속**을 클릭합니다.

워크플로의 **서비스 역할 선택** 단계에는 선택한 조직에서 사용 가능한 서비스가 표시됩니다.

6 **조직 멤버**로 액세스하려는 각 서비스에 대해 드롭다운 목록을 사용하여 서비스 역할을 선택합니다.

참고 서비스 역할은 서비스별로 다릅니다. 필요한 서비스 역할이 확실하지 않은 경우 액세스하려는 서비스에 대한 설명서를 참조하십시오.

7 **계속**을 클릭합니다.

8 온보딩 워크플로의 **요청 마무리** 단계에서 서비스 액세스 요청에 대한 기간을 정의합니다.

9 **비즈니스 근거** 텍스트 상자에 **조직 소유자**에게 보낼 메시지를 입력한 다음 **계속**을 클릭합니다.

요청은 **보류 중인 요청** 목록에 표시되며 **조직 소유자**의 승인을 기다립니다.

10 페더레이션된 도메인의 다른 IGA가 활성화된 조직에 대한 액세스를 요청하려면 **새 요청 제출**을 클릭합니다.

11 3~9단계를 반복합니다.

다음에 수행할 작업

요청한 조직 및 서비스 역할에 대한 승인을 받는 데 다소 시간이 걸릴 수 있습니다. 그때까지 Cloud Services 콘솔에 액세스하여 제출한 요청의 상태를 확인하거나, 생성한 요청을 취소하거나, 새 요청을 생성할 수 있습니다.

Cloud Services 콘솔에 로그인하는 방법

3

VMware Cloud Services 사용자는 VMware 계정 자격 증명을 사용하여 Cloud Services 콘솔에 로그인합니다. 계정이 페더레이션된 경우 회사 계정 자격 증명을 사용하여 로그인합니다.

사용자가 VMware Cloud Services에 로그인하고 인증에 성공하면 사용자의 로그인 세션에 대한 액세스 및 새로 고침 토큰이 생성됩니다. 두 토큰 모두 OAuth2.0 애플리케이션을 사용하여 백그라운드에서 생성되며 기본 TTL(Time to Live) 값은 다음과 같습니다.

- 액세스 토큰의 경우 30분 TTL.
- 새로 고침 토큰의 경우 24시간 TTL.

즉, 로그인에 성공한 후 액세스 토큰은 30분 동안만 유효합니다. 그 후에는 유효하지 않게 되며 사용자가 로그인 세션을 계속할 수 있도록 새로 고침 토큰을 사용하여 액세스 토큰을 다시 생성합니다. 24시간 후에는 새로 고침 토큰이 만료되므로 사용자가 다시 로그인해야 합니다.

현재 액세스 토큰과 새로 고침 토큰의 기본 TTL 값은 수정할 수 없습니다.

사전 요구 사항

- 하나 이상의 VMware Cloud Services 조직에서 조직 역할이 있어야 합니다.

절차

- 1 브라우저 창을 열고 <https://console.cloud.vmware.com/> 사이트로 이동합니다.
- 2 계정 이메일을 입력한 후 다음을 클릭합니다.
- 3 암호를 입력한 다음 **로그인**을 클릭합니다.

결과

로그인에 성공하면 조직에서 사용할 수 있는 서비스가 VMware Cloud Services 홈 페이지에 표시됩니다.

Cloud Services 조직이란?

4

VMware Cloud는 조직을 사용하여 하나 이상의 서비스에 대한 제어된 액세스를 제공합니다.

여러 클라우드 서비스를 사용하는 엔터프라이즈인 조직은 비즈니스 그룹 및 프로세스를 다른 조직에 쉽게 매핑할 수 있는 방법을 제공합니다.

Cloud Services 콘솔을 사용하여 조직 및 다음과 같은 리소스를 관리합니다.

- 사용자 및 그룹 역할과 사용 권한.
- 추가 서비스를 온보딩합니다.
- 청구 및 구독 정보를 가져옵니다.
- 조직의 서비스에 대한 사용량 데이터를 확인합니다.
- 조직에서 인증 정책을 설정합니다.
- 이벤트 로그를 감사합니다.
- 지원을 받습니다.

조직에서 할당 받은 조직 역할에 따라 Cloud Services 콘솔의 기능에 대한 액세스 권한이 결정됩니다. 조직 내에서 보유하고 있는 서비스 역할에 따라 조직에서 액세스할 수 있는 VMware Cloud services가 결정됩니다. 여러 조직에서 서로 다른 역할을 가질 수 있습니다.

Cloud Services 카탈로그를 사용하는 방법

5

VMware Cloud Services 카탈로그를 사용하면 특정 조건을 충족하는 서비스를 쉽게 보거나, 찾아보거나, 검색하거나, 필터링할 수 있습니다.

서비스 카탈로그는 Cloud Services 콘솔에 로그인할 때 열리는 첫 번째 페이지입니다. 각 카탈로그 항목은 서비스에 대한 정보를 표시하는 별도의 카드로 표시됩니다. 조직에서 서비스를 사용할 수 있으면 서비스 카드의 링크를 클릭하여 액세스를 요청할 수 있습니다.

다음 위치에서	가능한 작업
서비스 > 조직 탭	<ul style="list-style-type: none"> ■ 페이지의 내 서비스 섹션에서는 내게 서비스 역할이 이미 할당된 모든 서비스를 찾을 수 있습니다. 서비스를 시작하려면 서비스 카드를 클릭합니다. ■ 기타 서비스 섹션에는 내게 할당된 서비스 역할이 없는 조직의 모든 서비스 목록이 제공됩니다. <p>모든 액세스 요청은 조직 소유자의 승인을 받아야 합니다. 서비스 역할에 대한 액세스 요청 제출에 대한 자세한 내용은 추가 역할을 요청하는 방법 항목을 참조하십시오.</p>
서비스 > 권장 탭	현재 서비스 구독을 기반으로 하는 서비스 권장 사항 목록을 확인합니다.
서비스 > 모두 탭	전체 VMware Cloud Services 카탈로그를 찾아보거나 필터링합니다. 범주 및 가격 책정 모델을 기준으로 서비스 카탈로그를 필터링할 수 있습니다.
서비스 아래 모든 페이지	페이지의 오른쪽 상단 모서리에 있는 서비스 검색 상자를 사용하여 키워드로 관련 서비스를 찾습니다.

다음으로 아래 항목을 읽으십시오.

- [내가 사용할 수 있는 서비스 카탈로그 작업](#)
- [추가 역할을 요청하는 방법](#)

내가 사용할 수 있는 서비스 카탈로그 작업

VMware Cloud services 카탈로그의 서비스 카드에서 직접 VMware Cloud services에 대한 액세스를 관리할 수 있습니다. 지정된 서비스와 관련하여 수행할 수 있는 작업은 조직에서의 역할 및 액세스하려는 서비스 유형에 따라 다릅니다. 무료, 평가판 및 유료 서비스에 대해 다양한 작업을 사용할 수 있습니다.

조직 멤버 작업

다음에 액세스할 수 있고...	서비스가 다음에 해당하면...	수행할 수 있는 작업...	이 작업의 결과...
서비스	무료, 활성 평가판 또는 유료	서비스 시작	Cloud Services Console에서 서비스가 시작됨
	무료, 활성 평가판 또는 유료(하나 이상의 서비스 인스턴스 포함)	서비스 시작 - 서비스 인스턴스가 하나인 경우 도구 설명 포함 서비스 시작 - 서비스에 대해 여러 인스턴스가 있는 경우 드롭다운 메뉴 사용	선택한 서비스 인스턴스가 Cloud Services Console에서 시작됨
조직(단, 서비스에 대해서는 없음)	무료, 활성 평가판 또는 유료	역할 요청	서비스에 대한 역할을 요청하라는 메시지가 표시됨
서비스에 대한 액세스 권한이 없고 서비스가 조직에 없는 경우	무료, 활성 평가판 또는 유료	액세스	서비스를 온보딩하라는 메시지가 표시됨
		자세한 정보	서비스 세부 정보 페이지가 시작됨
	만료된 평가판	자세한 정보	서비스 세부 정보 또는 구매 정보 페이지가 열림

조직 소유자 작업

다음에 액세스할 수 있고...	서비스가 다음에 해당하면...	수행할 수 있는 작업...	이 작업의 결과...
서비스	무료 또는 유료	서비스 시작	Cloud Services Console에서 서비스가 시작됨
	활성 평가판	서비스 시작	Cloud Services Console에서 서비스가 시작됨
		말줄임표 아이콘(☰)에서 평가판 세부 정보 보기 말줄임표 아이콘(☰)에서 서비스 구매	서비스 평가판 세부 정보 페이지가 열림 구매 정보가 있는 페이지가 열림
조직(단, 서비스에 대해서는 없음)	무료, 활성 평가판 또는 유료	액세스	역할을 편집하여 서비스에 대한 액세스 권한을 얻으라는 메시지가 표시됨
		자세한 정보	서비스 세부 정보 페이지가 시작됨
서비스에 대한 액세스 권한이 없고 서비스가 조직에 없는 경우	무료, 유료 또는 평가 후 유료로 전환	액세스	서비스를 온보딩하라는 메시지가 표시됨
	만료된 평가판 조직 설정에 따라 네 가지 작업 중 하나가 표시됨	서비스 구매	구매 정보가 있는 페이지가 열림

다음에 액세스할 수 있고...	서비스가 다음에 해당하면...	수행할 수 있는 작업...	이 작업의 결과...
		지불 방법 확인	에서 지불 방법 확인Cloud Services Console 페이지가 열림
		지불 방법 추가	Cloud Services Console에서 지불 정보 페이지가 열리고 조직에 대한 지불 방법 세부 정보를 추가하라는 메시지가 표시됨

추가 역할을 요청하는 방법

조직 **멤버인** 사용자는 **조직 소유자인** 사용자의 초대를 통해 또는 셀프 서비스 요청을 제출하여 조직에서 사용할 수 있는 VMware Cloud services에 액세스할 수 있습니다.

셀프 서비스 요청을 사용하면 **조직 소유자**의 초대를 기다리지 않아도 되고 조직 내에서 액세스하려는 서비스 및 역할과 요청된 액세스에 대한 기간을 결정할 수 있습니다.

참고 **조직 소유자**는 추가적인 조직 및 서비스 역할을 자신에게 직접 할당할 수 있습니다. 자세한 내용은 [역할 및 사용 권한을 관리하는 방법](#) 항목을 참조하십시오.

셀프 서비스 요청을 제출하려면 서비스 카탈로그에서 추가 역할을 요청하려는 서비스를 찾습니다. 서비스 카드에서 **액세스 요청** 링크를 클릭하기만 하면 됩니다. 드롭다운 메뉴를 사용하여 새 서비스 역할을 선택할 수 있는 팝업창이 열립니다.

모든 요청은 승인하기 전에 요청을 승인, 거부 또는 수정할 수 있는 **조직 소유자**에게 제출됩니다. 요청이 처리되면 이메일 알림을 받게 됩니다.

직접 제출한 셀프 서비스 요청을 보는 방법

보류 중인 서비스 요청과 과거 서비스 요청은 **내 계정 > 내 역할** 페이지의 **내 요청 기록** 섹션에서 언제든지 볼 수 있습니다.

직접 생성한 셀프 서비스 요청을 취소할 수 있습니까?

보류 중 상태의 셀프 서비스 요청만 취소할 수 있습니다. **내 역할** 페이지를 열고 삭제하려는 요청에 대한 **취소** 링크를 클릭합니다.

서비스 타일에 **액세스 요청** 링크가 표시되지 않는 이유는 무엇입니까?

페더레이션된 도메인이 있는 IGA(ID 거버넌스 및 관리)가 활성화된 조직에서 추가 서비스 역할을 요청하는 옵션이 비활성화되어 있을 수 있습니다. 이런 경우 **조직 소유자**의 초대가 필요합니다.

내 Cloud Services 계정을 관리하는 방법

6

사용자 프로파일은 VMware Cloud services 계정에서 관리합니다. 언어 및 국가별 형식 기본 설정, 암호 및 MFA 설정과 같은 보안 설정을 선택하고 API 토큰을 생성하고 관리합니다. 조직에서 자신이 보유하고 있는 역할도 볼 수 있습니다.

계정에 액세스하려면 사용자 이름을 클릭한 다음 **내 계정**을 클릭합니다.

다음으로 아래 항목을 읽으십시오.

- 내 사용자 프로파일을 보는 방법
- 언어 및 국가별 형식을 변경하는 방법
- 다단계 인증을 사용하여 내 계정을 보호하는 방법
- API 토큰을 생성하는 방법
- 조직에서 내 역할을 관리하는 방법
- 거버넌스가 활성화된 조직에서 역할을 요청하는 방법

내 사용자 프로파일을 보는 방법

사용자 프로파일은 VMware 고객 계정을 생성할 때 제공한 세부 정보로 구성됩니다. 고객 프로파일에 따라 사용자 프로파일을 편집할 수 있을 수도 있습니다.

참고 등록된 이메일 주소는 변경할 수 없습니다.

Cloud Services 콘솔에서 또는 <https://customerconnect.vmware.com/>에서 My VMware 계정에 로그인하여 사용자 프로파일을 볼 수 있습니다.

계정이 페더레이션되지 않은 경우 Cloud Services 콘솔에서 프로파일 세부 정보를 수정할 수 있습니다. 변경한 내용은 VMware 계정에 저장되며 그 반대의 경우도 마찬가지입니다.

계정이 페더레이션된 경우 편집 옵션이 제한됩니다. 예를 들어 프로파일 이름을 변경할 수 없으며 VMware ID 세부 정보만 볼 수 있습니다.

절차

- 1 Cloud Services 콘솔 도구 모음에서 사용자 이름을 클릭하고 **내 계정**을 선택합니다.
- 2 **프로파일** 페이지에서 변경하고 **저장**을 클릭합니다.

내 암호를 재설정하는 방법

VMware Cloud services 암호는 VMware ID와 동일한 암호입니다.

VMware Cloud services 플랫폼에서 또는 <https://customerconnect.vmware.com/>에서 VMware Customer Connect 계정에 로그인하여 VMware ID를 재설정할 수 있습니다.

절차

- 1 Cloud Services 콘솔 도구 모음에서 사용자 이름을 클릭하고 **내 계정 > 보안**을 선택합니다.
- 2 정보를 입력하여 암호를 변경하고 **암호 변경**을 클릭합니다.

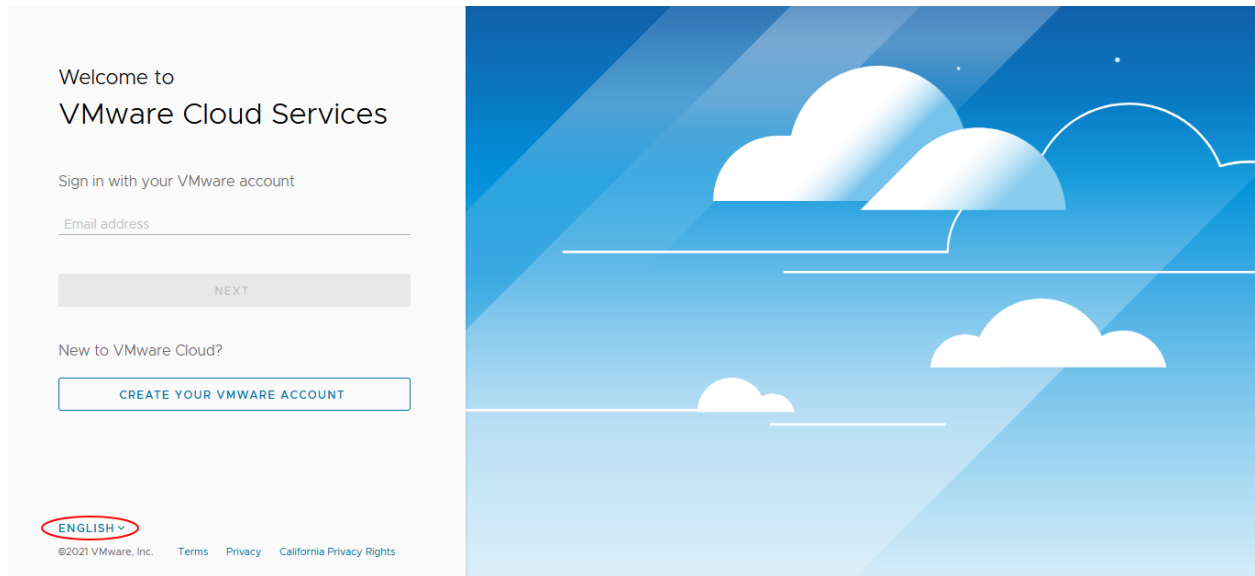
VMware ID가 재설정됩니다.

언어 및 국가별 형식을 변경하는 방법

클라우드 서비스를 등록하기 전에 표시 언어를 기본 설정 언어로 변경하거나 계정 설정에서 국가별 형식을 설정할 수도 있습니다.

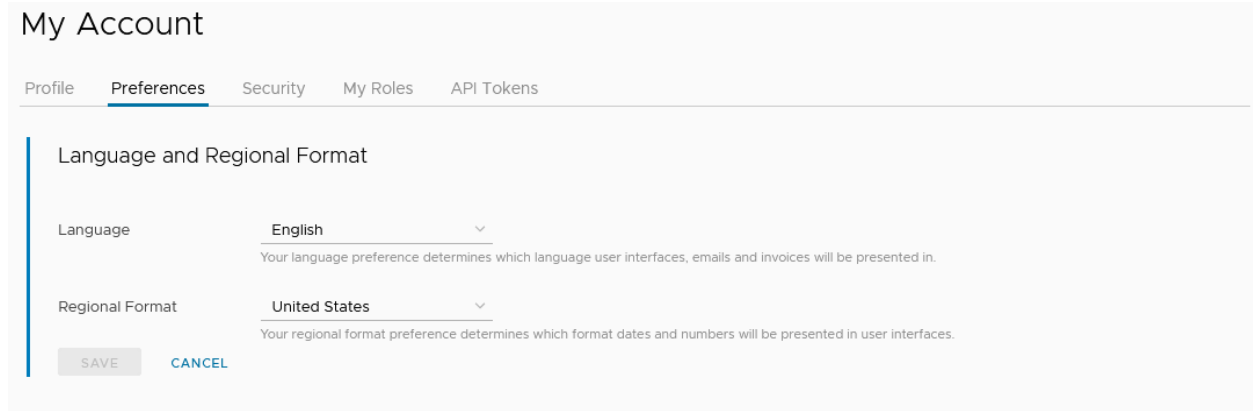
기본 설정 언어로 등록 경험

VMware Cloud services를 아직 등록하지 않은 경우 로그인하기 전에 기본 설정 언어를 선택할 수 있습니다. 브라우저에서 국가별 형식 설정을 지원합니다.



언어 및 국가별 형식 변경

로그인한 후 언제든지 언어 및 국가별 형식을 변경하려면 메뉴 모음에서 사용자 이름을 클릭하고 **내 계정 > 기본 설정**을 선택합니다. 그런 다음, **편집**을 클릭합니다.



언어를 변경하는 경우 모든 페이지가 선택된 언어로 표시는 것은 아닙니다. 영어 문자만 지원하는 일부 양식도 있습니다. 영어만 지원되는 경우에는 알려 드리므로 걱정하지 않으셔도 됩니다.

언어와 다른 국가별 형식 설정

기본 설정 언어와 다른 국가별 형식을 설정하면 선택한 언어에 대한 기본 국가별 형식이 선택된 국가별 형식을 재정의하는 경우가 있을 수 있습니다. 이 현상은 특정 이메일, 청구서 및 송장을 표시할 때 발생할 수 있습니다. 예를 들어 영어를 기본 설정 언어로 선택하고 일본어를 국가별 형식으로 선택하면 일부 커뮤니케이션이 미국 국가별 형식으로 표시될 수 있습니다. 언어와 기본 국가별 형식 목록은 다음과 같습니다.

언어	기본 국가별 형식
English	US
중국어 간체	CN
중국어 번체	TW
Español	ES
이탈리아어	IT
Français	FR
일본어	JP
Deutsch	DE
한국어	KR

다단계 인증을 사용하여 내 계정을 보호하는 방법

MFA(다단계 인증)는 로그인할 때 2개의 증거 조각(자격 증명)을 제공해야 하는 보안 향상 기능입니다. 이러한 자격 증명은 암호처럼 알고 있는 정보이거나 1회용 암호를 생성하는 애플리케이션처럼 가지고 있는 정보일 수 있습니다. MFA를 사용하면 별도의 보안 계층을 추가하여 데이터 및 애플리케이션에 대한 액세스를 보호할 수 있습니다.

일부 양식 등에서 MFA를 이미 사용했을 수 있습니다. 예를 들어 계정에 대한 액세스 권한을 얻는 데 사용되는 코드를 모바일 디바이스로 전송하는 웹 사이트에 로그인한 경우입니다.

참고 VMware Cloud Services 계정이 페더레이션되면 엔터프라이즈 보안 팀에서 MFA를 관리합니다.

MFA를 사용하여 VMware Cloud Services 계정을 보호하려면 모바일 디바이스에 인증 애플리케이션을 다운로드합니다. 이 경우 가상 MFA 디바이스가 생성됩니다. 이 애플리케이션은 시간 기반 1회용 암호 표준과 호환되는 6자리 인증 코드를 생성합니다. 이 코드를 VMware ID 및 암호와 함께 사용하여 클라우드 서비스에 로그인합니다.

계정에 대해 MFA를 설정하면 10개의 복구 코드 집합이 수신됩니다. 이러한 코드를 안전한 위치에 저장합니다. 근처에 MFA 디바이스가 없거나 이를 잃어버린 경우 로그인해야 합니다.

수행하려는 작업	
MFA 디바이스를 활성화합니다.	<ol style="list-style-type: none"> 1 메뉴에서 사용자 이름을 클릭하고 내 계정 > 보안을 선택합니다. 2 MFA 디바이스 활성화를 클릭하고 지침에 따라 디바이스를 설정합니다. 3 MFA가 자동으로 설정됩니다. 다음에 로그인할 때 VMware ID 및 암호, 애플리케이션에서 생성된 인증 코드를 사용합니다.
MFA를 해제하여 VMware ID 및 암호로만 로그인합니다.	<ol style="list-style-type: none"> 1 메뉴에서 사용자 이름을 클릭하고 내 계정 > 보안을 선택합니다. 2 MFA가 설정됨 토크 키를 클릭합니다.
MFA 디바이스를 비활성화합니다.	<ol style="list-style-type: none"> 1 메뉴에서 사용자 이름을 클릭하고 내 계정 > 보안을 선택합니다. 2 MFA 디바이스 비활성화를 클릭합니다.
내 복구 코드를 재생성합니다.	언제든지 내 계정 > 보안 에 액세스하여 새로운 복구 코드 집합을 재생성할 수 있습니다.

사용할 수 있는 2단계 인증 애플리케이션

VMware Cloud services는 다음과 같은 2단계 인증 애플리케이션을 지원합니다.

아래의 적절한 링크를 클릭하여 디바이스에 대한 인증자를 다운로드할 수 있습니다.

디바이스	인증 애플리케이션
iOS	<ul style="list-style-type: none"> ■ Google Authenticator. https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8의 내용을 참조하십시오. ■ Duo Mobile. https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile의 내용을 참조하십시오.
Android	<ul style="list-style-type: none"> ■ Google Authenticator. https://support.google.com/accounts/answer/1066447?hl=en의 내용을 참조하십시오. ■ Duo Mobile. https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile의 내용을 참조하십시오.

디바이스	인증 애플리케이션
Windows phone	<ul style="list-style-type: none"> Authenticator. https://www.microsoft.com/en-us/store/p/authenticator/9wzdncrfj3rj?rtc=1의 내용을 참조하십시오. Duo Mobile. https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile의 내용을 참조하십시오.
Blackberry	Google Authenticator https://support.google.com/accounts/answer/1066447 의 내용을 참조하십시오.

가상 MFA 애플리케이션에 대한 자세한 내용은 <https://tools.ietf.org/html/rfc6238> 항목을 참조하십시오.

MFA를 사용하여 로그인할 수 없는 경우 수행할 수 있는 작업

VMware Cloud services에서 MFA를 활성화하면 10개의 복구 코드 집합이 수신됩니다. 이러한 코드를 복사하고 다운로드하고 인쇄할 수 있지만 안전한 위치에 저장해야 합니다.

로그인할 수 없는 경우 MFA 문제를 해결하는 방법

VMware Cloud services에서 MFA를 활성화하면 10개의 복구 코드 집합이 수신됩니다. 이러한 코드를 복사하고 다운로드하고 인쇄할 수 있지만 안전한 위치에 저장해야 합니다.

VMware Cloud services에 로그인하는 데 문제가 있는 경우 복구 코드를 사용할 수 있습니다.

조건...	수행할 단계
MFA 디바이스에 액세스할 수 없거나 디바이스를 분실했음	VMware Cloud Services 로그인 페이지에서 MFA 문제 해결 링크를 클릭합니다. 메시지가 표시되면 복구 키 중 하나를 입력합니다.
복구 코드를 찾을 수 없음	지원 전화 번호 로 전화하거나 VMware Customer Connect에서 로그인 채팅 지원 에 액세스하여 VMware 지원에 문의하십시오.

API 토큰을 생성하는 방법

API 토큰을 사용하면 승인된 API 연결을 생성할 때 자신을 인증할 수 있습니다. 이전에 OAuth 새로 고침 토큰이라고 했던 API 토큰은 액세스 토큰으로 교환되며 조직별로 액세스 권한을 부여합니다. Cloud Services 콘솔의 계정 페이지에서 또는 VMware Cloud Services를 통해 API 토큰을 생성합니다.

토큰은 영숫자를 선택하는 특수 알고리즘을 사용하여 생성됩니다. 각 토큰은 고유한 65자 조합입니다. 토큰을 생성할 때 해당 기간 및 범위를 결정합니다.

- 토큰의 TTL(Time to Live)은 몇 분에서 몇 개월까지 설정하거나 만료되지 않도록 설정할 수 있습니다. 기본 기간은 6개월입니다.
- 범위는 토큰이 액세스할 수 있는 조직의 영역, 특히 조직 내 역할 및 서비스 그리고 권한 수준을 제어할 수 있도록 구현하는 방법을 제공합니다.

사전 요구 사항

API 토큰을 위한 안전하고 보호된 스토리지 위치를 확인합니다.

절차

- 1 Cloud Services 콘솔 도구 모음에서 사용자 이름을 클릭하고 **내 계정 > API 토큰**을 선택합니다.
- 2 **새 API 토큰 생성** 링크를 클릭합니다.
- 3 토큰의 이름을 입력합니다.
- 4 원하는 토큰의 수명을 지정합니다.

참고 만료되지 않는 토큰은 손상될 경우 보안 위험을 초래할 수 있습니다. 이러한 상황이 발생하는 경우 토큰을 해지해야 합니다.

- 5 토큰의 범위를 정의합니다. 사용자 계정에서 지원하는 역할을 기반으로 선택해야 합니다.

범위	설명
조직 역할	조직 역할은 조직의 리소스에 대한 사용자의 액세스 권한을 결정합니다. <ul style="list-style-type: none"> ■ API 토큰에 대해 하나 이상의 조직 역할을 선택합니다.
서비스 역할	서비스 역할은 VMware Cloud services에 대한 액세스 권한을 부여하는 미리 정의된 기본 제공 사용 권한 집합입니다. <ul style="list-style-type: none"> ■ 서비스 이름 옆에 있는 화살표 아이콘을 사용하여 해당 서비스에 사용할 수 있는 역할을 확장한 다음 API 토큰에 대한 서비스 역할을 하나 이상 선택합니다.
사용 권한	일부 서비스에서는 서비스 역할에 사용할 수 있는 제한된 사용 권한 집합을 할당하여 더 세분화된 선택을 할 수 있습니다. <ul style="list-style-type: none"> ■ 서비스 역할을 선택하면 사용 가능한 권한이 테이블 오른쪽에 표시됩니다. API 토큰에 대한 관련 서비스 사용 권한을 선택합니다.

필요한 경우 **모든 역할**을 선택하여 모든 조직 및 서비스 역할에 대한 액세스 권한을 토큰에 부여할 수 있습니다.

참고 토큰에 **모든 역할** 액세스 권한을 할당하더라도 토큰은 사용자 계정이 지원하는 액세스 역할만 가지게 됩니다. 보유하고 있는 조직 및 서비스 역할을 보려면 **내 계정** 페이지에서 **내 역할** 탭을 선택합니다.

- 6 (선택 사항) 확장된 사용자 세부 정보가 포함된 OpenID 규격 토큰을 검색하려면 **OpenID** 확인란을 선택합니다.
- 7 (선택 사항) 토큰이 곧 만료되는 경우 미리 알림을 받도록 이메일 기본 설정을 지정합니다.
- 8 **생성**을 클릭합니다.
- 9 나중에 검색할 수 있도록 토큰 자격 증명을 안전한 장소에 저장합니다.

보안상의 이유로 토큰을 생성한 후에는 [API 토큰] 페이지에 토큰 자격 증명이나 토큰의 이름만 표시됩니다. 즉, 이 페이지에서 더 이상 토큰을 자격 증명을 복사하여 재사용할 수 없게 됩니다.

10 계속을 클릭합니다.

API 토큰 외에도 OAuth 애플리케이션을 사용하여 애플리케이션을 인증할 수 있습니다. API 토큰 대신 OAuth 애플리케이션을 사용하는 시기를 확인하려면 [OAuth 애플리케이션과 API 토큰의 차이점](#)을 참조하십시오.

예제: API 토큰을 사용하여 VMware Cloud Services API와 상호 작용

API 토큰을 사용하여 인증 토큰을 교환하면 API와 상호 작용할 수 있습니다.

- 1 API 토큰을 생성합니다.
- 2 <https://console.cloud.vmware.com/csp/gateway/am/api/auth/api-tokens/authorize>에 대해 POST를 수행합니다.
- 3 헤더에 다음 요청을 포함합니다.
 - `accept: application/json`
 - `content type: application/x-www-form-urlencoded/`
- 4 본문에 `refresh_token={token value}` 요청을 포함합니다.
- 5 스크립트 HTTP 호출의 `csp-auth-token` 헤더에 인증 토큰을 사용합니다.

내 API 토큰을 관리하는 방법

API 토큰을 안전하게 저장, 백업 및 관리할 책임은 API 토큰의 단독 소유자에게 있습니다.

API 토큰을 보고 관리하려면 사용자 이름을 클릭한 다음 **내 계정 > API 토큰**을 선택합니다.

- 토큰을 재생성하려면 **재생성**을 클릭합니다. 그러면 기존 토큰이 새 토큰으로 바뀝니다. API 호출을 계속하려면 API 호출에서 토큰을 업데이트해야 합니다.
- 토큰을 비활성화하려면 **해지**를 클릭합니다. 그러면 API 토큰과 연결된 액세스 토큰이 모두 해지됩니다.
- 조직의 리소스에 대한 무단 액세스를 방지하려면 생성한 API 토큰을 안전하고 보호된 위치에 보관하는 것이 좋습니다. VMware Cloud Services는 소유 증명을 확인하지 않지만 다음과 같은 경우 토큰 사용 감사 이벤트를 캡처합니다.
 - 사용자가 API 토큰을 생성함
 - 사용자가 개인 토큰을 하나 또는 모두 해지함
 - 사용자가 API 토큰 새로 고침으로 액세스 토큰을 생성하지 못함

참고 VMware Cloud Services에서 감사 이벤트 로그를 보려면 **조직 소유자** 역할이 있어야 합니다.

- API에 추가 보안 계층을 추가하기 위해 API 토큰에 대한 다단계 인증을 추가할 수 있습니다. 자세한 내용은 [다단계 인증을 사용하여 API 토큰을 보호하는 방법](#)의 내용을 참조하십시오.

- 조직에 설정된 정책을 위반하거나 조직의 표준을 준수하지 않아서 **조직 소유자**가 API 토큰을 비활성화한 경우에는 VMware Cloud Services로부터 이메일 알림을 받게 됩니다. **내 계정 > API 토큰** 페이지에서 비활성화된 토큰은 **Deactivated** 레이블로 표시됩니다.

다음 표에는 가장 일반적인 API 토큰 셀프 서비스 관리 작업이 요약되어 있습니다.

원하는 작업...	수행할 단계
만료된 API 토큰의 유효성을 확장합니다.	토큰을 재생성해야 합니다.
유효한 API 토큰을 재생성합니다.	언제든지 토큰을 재생성할 수 있습니다. 토큰을 재생성하는 경우 이전 토큰의 모든 인스턴스를 해지합니다. 예를 들어 스크립트 중 하나에서 토큰을 사용한 경우에는 새로 생성된 토큰으로 교체해야 합니다.
손상된 API 토큰을 교체합니다.	토큰이 손상되었다고 생각되면 토큰을 해지하여 무단 액세스를 방지할 수 있습니다. 새 토큰을 생성하여 인증을 갱신합니다.
아직 유효한 API 토큰을 삭제합니다.	유효한 API 토큰을 해지하여 삭제합니다.
손실된 API 토큰을 복구합니다.	손실된 토큰은 복구할 수 없습니다. 손실된 토큰을 해지하고 새 토큰을 생성해야 합니다.
조직 소유자 가 비활성화한 API 토큰 재활성화	비활성화된 토큰이 아직 유효하면 조직 소유자 에 연락하여 재활성화를 요청해야 합니다.

다단계 인증을 사용하여 API 토큰을 보호하는 방법

API 토큰을 사용하여 VMware Cloud Services API에 액세스하는 경우 API 토큰에서 MFA(다단계 인증)를 활성화하여 추가 보안 계층을 추가할 수 있습니다.

이렇게 하면 API 토큰이 손상되더라도 데이터와 애플리케이션을 무단 액세스로부터 보호할 수 있습니다. MFA를 활성화하면 VMware Cloud Services API에 대한 액세스 토큰으로 교환하려는 모든 토큰에 MFA 인증이 필요합니다.

MFA를 사용하여 VMware Cloud Services API 토큰을 보호하려면 모바일 디바이스에 인증 애플리케이션을 다운로드합니다. 이 경우 가상 MFA 디바이스가 생성됩니다. 이 애플리케이션은 시간 기반 1회용 암호 표준과 호환되는 6자리 인증 코드를 생성합니다. VMware Cloud Services API에 액세스하려면 등록된 MFA 디바이스에서 생성된 6자리 토큰을 제공해야 합니다.

수행하려는 작업	
MFA 디바이스를 활성화합니다.	<ol style="list-style-type: none"> 1 메뉴에서 사용자 이름을 클릭하고 내 계정 > API 토큰 > MFA를 선택합니다. 2 MFA 디바이스 활성화를 클릭하고 지침에 따라 디바이스를 설정합니다. 3 MFA가 자동으로 설정됩니다. 다음에 API 토큰을 사용하여 액세스 토큰을 가져올 때 애플리케이션에서 생성된 인증 코드가 필요합니다.
MFA를 해제합니다.	<ol style="list-style-type: none"> 1 메뉴에서 사용자 이름을 클릭하고 내 계정 > API 토큰 > MFA를 선택합니다. 2 MFA가 설정됨 토글 스위치를 클릭합니다. <p>중요 조직에서 API 토큰에 MFA를 사용하도록 한 경우에는 MFA를 해제할 수 없습니다. API 토큰을 생성할 수 있더라도 등록된 MFA 디바이스에서 생성된 6자리 암호를 제공하지 않으면 액세스 토큰으로 교환할 수 없습니다.</p>
MFA 디바이스를 비활성화합니다.	<ol style="list-style-type: none"> 1 메뉴에서 사용자 이름을 클릭하고 내 계정 > API 토큰 > MFA를 선택합니다. 2 MFA 디바이스 비활성화를 클릭합니다.

조직에서 내 역할을 관리하는 방법

역할은 **조직 소유자** 역할을 맡은 사용자가 할당합니다. 일반적으로 조직에서의 역할과 하나 이상의 조직 서비스에서의 역할을 맡게 됩니다. **조직 멤버인** 사용자는 조직에서 사용할 수 있는 서비스에 대해 추가 서비스 역할을 요청할 수 있으며 이미 할당된 역할을 삭제할 수 있습니다. 추가적인 서비스 역할 액세스 권한을 얻으려면 **조직 소유자**가 요청을 승인해야 합니다.

조직 역할에 대한 자세한 내용은 [역할 및 사용 권한을 관리하는 방법](#) 항목을 참조하십시오.

조직에서 서비스 역할을 관리하는 방법은 다음과 같습니다.

- 역할을 보고, 서비스에 대해 보유한 액세스 권한을 보고, 추가 역할을 요청하려면 사용자 이름을 클릭하고 **내 계정 > 내 역할**을 선택합니다.
- 더 이상 필요하지 않은 서비스 역할 또는 추가 조직 역할을 삭제하려면 서비스 이름을 클릭하여 해당 서비스에 대해 보유하고 있는 모든 역할을 확장합니다. 제거하려는 서비스 역할을 찾은 후 **역할 삭제**를 클릭합니다. 삭제가 적용되려면 역할 삭제 요청이 **조직 소유자**의 승인을 받아야 합니다.
- 지난 역할 요청을 보려면 페이지의 **내 요청 기록** 섹션까지 아래로 스크롤합니다.
- 조직에서 이미 사용 가능한 서비스에 대한 추가 서비스 역할을 요청하려면 **역할 요청**을 클릭하고 항목을 선택합니다.

Request Access to VMware Cloud on AWS ×

Please indicate the type of roles you want to request for **VMware Cloud on AWS** below. Your access request will send to the organization owner to review, and you will be notified once an update has made about your request.

Role Types

Optional: Describe why you'd like to request access to the organization owner to review.

service-owner-display-name

Please select roles here

service-owner-display-name

service-user-display-name

1 role selected CANCEL SELECT

CANCEL
REQUEST

IGA(ID 거버넌스 및 관리)가 활성화된 조직의 멤버인 경우 새 조직 역할을 요청할 수 있는 추가 옵션이 있습니다. 자세한 내용은 [거버넌스가 활성화된 조직에서 역할을 요청하는 방법](#)을 참조하십시오.

거버넌스가 활성화된 조직에서 역할을 요청하는 방법

ID 거버넌스 및 관리가 활성화된 조직의 **조직 소유자**는 초대를 통해 액세스 권한을 부여하는 대신 **조직 멤버**가 셀프 서비스 액세스 요청을 제출하도록 허용할 수 있습니다. 조직에서 이 옵션을 사용할 수 있는 경우 Cloud Services 콘솔에서 추가 역할을 직접 요청할 수 있습니다.

절차

- 1 VMware Cloud Services에 로그인하고 **내 계정 > 내 역할** 페이지로 이동합니다.
- 2 **서비스 액세스 추가** 링크를 클릭합니다.

참고 서비스 액세스 추가 링크가 표시되지 않으면 셀프 서비스 요청 옵션이 비활성화되었음을 의미하며 **조직 소유자**가 보낸 초대를 통해서만 추가 액세스 권한을 얻을 수 있습니다.

- 3 요청하려는 추가 조직 및 서비스 역할을 선택합니다.
- 4 **제출**을 클릭합니다.

결과

승인을 위해 요청이 생성 및 제출됩니다. **조직 소유자**가 요청을 처리하면 알림을 받게 됩니다.

내 Cloud Services 조직을 관리하는 방법

7

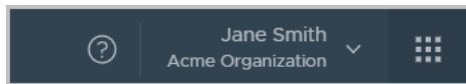
VMware 계정은 하나 이상의 VMware Cloud services 조직과 연결될 수 있습니다. VMware Cloud는 조직을 사용하여 하나 이상의 서비스에 대한 제어된 액세스를 제공합니다. 클라우드 서비스에 액세스하려면 조직에 속해야 합니다.

조직 소유자인 사용자는 조직의 모든 리소스에 대한 액세스 권한이 있습니다. 조직에 클라우드 서비스를 추가한 다음 가입하도록 사용자를 초대합니다. 조직 지불 방법 및 사용자 액세스를 관리합니다. **조직 멤버**인 사용자 역할을 보유한 경우 조직의 리소스에 대한 제한된 액세스 권한을 갖습니다.

현재 역할로 조직 내에서 수행할 수 있는 작업을 확인하려면 **역할 및 사용 권한을 관리하는 방법** 항목을 참조하십시오.

활성 조직

VMware Cloud services에 로그인하면 현재 로그인된 조직이 Cloud Services 콘솔 메뉴 표시줄의 사용자 이름 아래에 표시됩니다.



둘 이상의 조직에 속한 경우 언제든지 활성 조직에서 다른 조직으로 전환할 수 있습니다. 로그인하면 기본적으로 표시되는 조직을 선택할 수도 있습니다.

조직 ID 보기

각 조직은 고유한 ID가 있습니다. VMware Container Engine CLI와 같은 외부 명령줄 인터페이스와 상호 작용할 때 이 ID를 사용해야 할 수 있습니다. 사용자 이름을 클릭하여 조직 ID를 볼 수 있습니다. 조직 이름 아래에 단축된 버전의 ID가 표시됩니다. 전체 조직 ID를 표시하려면 짧은 ID를 클릭합니다.

조직 설정 표시

사용자 이름을 클릭하고 **조직 보기**를 선택하여 조직 이름 및 ID를 표시할 수 있습니다.

조직 소유자는 조직의 표시 이름을 변경할 수 있습니다.

고객 프로파일에 따라 국가 및 우편 번호를 보거나 편집하고 VMware API를 쿼리할 때 사용할 태그를 추가하거나 편집할 수도 있습니다.

다음으로 아래 항목을 읽으십시오.

- 내 조직 중 다른 조직에 액세스하는 방법
- 기본 조직을 지정하는 방법
- VMware Cloud Services 헤더를 사용자 지정하는 방법

내 조직 중 다른 조직에 액세스하는 방법

둘 이상의 조직에 속한 경우 언제든지 활성 조직에서 다른 조직으로 전환할 수 있습니다.

VMware Cloud Services에 로그인하면 활성 조직이 표시됩니다. VMware Cloud Services 메뉴의 사용자 이름을 아래에서 활성 조직의 이름을 확인할 수 있습니다.

절차

- 1 VMware Cloud Services 메뉴에서 사용자 이름 옆의 화살표를 클릭합니다.
- 2 메뉴에서 조직 이름 옆의 화살표를 클릭합니다.
조직 이름을 표시하는 드롭다운 목록이 나타납니다.
- 3 표시할 조직을 선택합니다.

기본 조직을 지정하는 방법

둘 이상의 조직에 속한 경우 로그인할 때 기본적으로 표시되는 조직을 선택할 수 있습니다.

활성 조직은 기본적으로 초대받은 조직이거나 VMware Cloud Services에서 로그아웃했을 때 표시된 조직입니다.

절차

- 1 VMware Cloud Services 메뉴에서 사용자 이름 옆의 화살표를 클릭합니다.
- 2 **기본 조직 설정**을 클릭합니다.
조직 목록이 표시됩니다.
- 3 로그인할 때 표시할 조직을 선택합니다.

VMware Cloud Services 헤더를 사용자 지정하는 방법

조직 소유자인 사용자는 회사의 브랜드를 반영하도록 VMware Cloud Services 헤더를 브랜딩하고 사용자 지정할 수 있습니다.

이 작업에서 생성하는 사용자 지정 VMware Cloud Services 머리글은 이 특정 조직에 액세스하는 **조직 멤버**에게만 표시됩니다.

사전 요구 사항

- **조직 소유자** 역할이 있어야 합니다.
- 회사 브랜딩 지침을 잘 알고 있어야 합니다.

절차

- 1 Cloud Services 콘솔에 로그인하고 **조직 > 세부 정보**로 이동합니다.
- 2 조직 세부 정보 페이지의 **조직 사용자 지정** 섹션에서 **편집**을 클릭합니다.
- 3 **머리글 표시 이름** 텍스트 상자에 VMware Cloud Services 대신 조직에 표시할 이름을 입력합니다.
- 4 **밝은 테마**에 대한 조직 로고를 업로드하려면 **찾아보기**를 클릭하고 로컬 시스템에서 이미지 파일을 선택합니다.

참고 로고 이미지에는 `.svg` 파일만 업로드할 수 있습니다.

어두운 테마의 머리글 로고는 기본적으로 **밝은 테마와 동일**로 설정되어 있습니다. **어두운 테마**에 대해 다른 이미지 파일을 업로드하려면 **밝은 테마와 동일** 확인란의 선택을 취소하고 **찾아보기**를 클릭하여 로컬 시스템에서 이미지를 선택합니다.

미리 보기 섹션이 새로 고쳐지고 변경한 새 색상이 표시됩니다. **기본값 복원**을 클릭하여 변경한 내용을 되돌릴 수 있습니다.

- 5 **밝은 테마** 및 **어두운 테마** 모두에 대한 조직 머리글의 색상표를 수정하려면 다음을 수행합니다.
 - a **머리글 배경색** 및 **머리글 텍스트 색** 텍스트 필드를 클릭합니다.
 - b 색상 선택 도구를 사용하여 각 항목의 색상을 정의합니다.
- 6 **저장**을 클릭합니다.

미리 보기 섹션이 새로 고쳐지고 새 머리글 로고가 표시됩니다.
- 7 변경한 내용을 보려면 서비스 페이지를 새로 고칩니다.

내 클라우드 서비스용 소프트웨어 바이너리 다운로드와 관련된 사항



일부 VMware Cloud services에는 서비스와 별도로 다운로드하여 설치하는 추가 소프트웨어 바이너리를 사용해야 합니다.

추가 소프트웨어는 Cloud Services 콘솔 메뉴에서 **다운로드**를 클릭하여 다운로드합니다. 이 옵션은 조직의 다음 역할에 사용할 수 있습니다.

- **조직 소유자**
- **소프트웨어 설치 관리자** 역할이 있는 **조직 관리자**
- **소프트웨어 설치 관리자** 역할이 있는 **조직 멤버**

다운로드 페이지 한 곳에서 서비스 액세스 권한이 있는 조직의 모든 서비스에 필요한 소프트웨어 바이너리를 구하는 동시에 다운로드할 추가 소프트웨어를 제공할 수 있습니다.

조건...	수행할 단계
다운로드 메뉴 링크가 표시되지 않는 경우	조직에서 조직 소유자 또는 소프트웨어 설치 관리자 역할을 요청합니다. 이 작업은 조직에 따라 조직 소유자 의 초대를 통해 또는 셀프 서비스 요청을 제출하여 수행합니다. 자세한 내용은 추가 역할을 요청하는 방법 의 내용을 참조하십시오.
다운로드 페이지를 열 수 있지만 추가 소프트웨어를 다운로드해야 하는 서비스가 표시되지 않는 경우	서비스에 대한 역할을 요청합니다. 자세한 내용은 조직에서 내 역할을 관리하는 방법 의 내용을 참조하십시오. 참고 조직에서 할당 받은 서비스 역할이 있어도 해당 서비스에 대해 다운로드할 소프트웨어 바이너리를 볼 수 없다면 VMware Cloud Services의 서비스와 연결된 바이너리 또는 패키지가 없음을 의미합니다.
여러 VMware Cloud Services 조직의 멤버인 경우	다운로드해야 하는 소프트웨어 바이너리에 액세스할 수 있는 조직 및 서비스 역할이 있는 조직으로 전환합니다. 자세한 내용은 내 조직 중 다른 조직에 액세스하는 방법 의 내용을 참조하십시오.

다음으로 아래 항목을 읽으십시오.

- [VMware Cloud Services용 추가 소프트웨어를 다운로드하는 방법](#)

VMware Cloud Services용 추가 소프트웨어를 다운로드하는 방법

서비스를 위해 다운로드해야 하는 추가 소프트웨어 바이너리 및 패키지는 Cloud Services 콘솔의 **다운로드** 페이지에서 액세스할 수 있습니다.

사전 요구 사항

추가 소프트웨어 바이너리 및 패키지를 다운로드하려면 다음이 필요합니다.

- 조직에서 **조직 관리자** 또는 **조직 멤버**인 경우 **조직 소유자** 역할 또는 **소프트웨어 설치 관리자** 사용 권한이 있어야 합니다.
- 추가 소프트웨어를 다운로드하려는 서비스에 대해 서비스 역할을 할당 받았습니다.
- 조직에 추가 소프트웨어를 다운로드하려는 서비스에 대한 활성 구독이 있습니다.

절차

1 Cloud Services 콘솔에 로그인합니다.

2 기본 메뉴에서 **다운로드**를 클릭합니다.

제품 탐색기 페이지가 열립니다. 액세스 권한이 있는 서비스 목록과 함께 다운로드할 추가 소프트웨어가 표시됩니다.

3 서비스에 대한 소프트웨어 바이너리를 보려면 서비스 이름을 클릭합니다.

제품 탐색기의 오른쪽 창에는 선택한 서비스와 연결된 다운로드 바이너리가 표시됩니다.

4 사용 가능한 소프트웨어 다운로드를 살펴봅니다.

a 특정 소프트웨어 바이너리에 대한 세부 정보를 보려면 **자세히 읽기**를 클릭합니다.

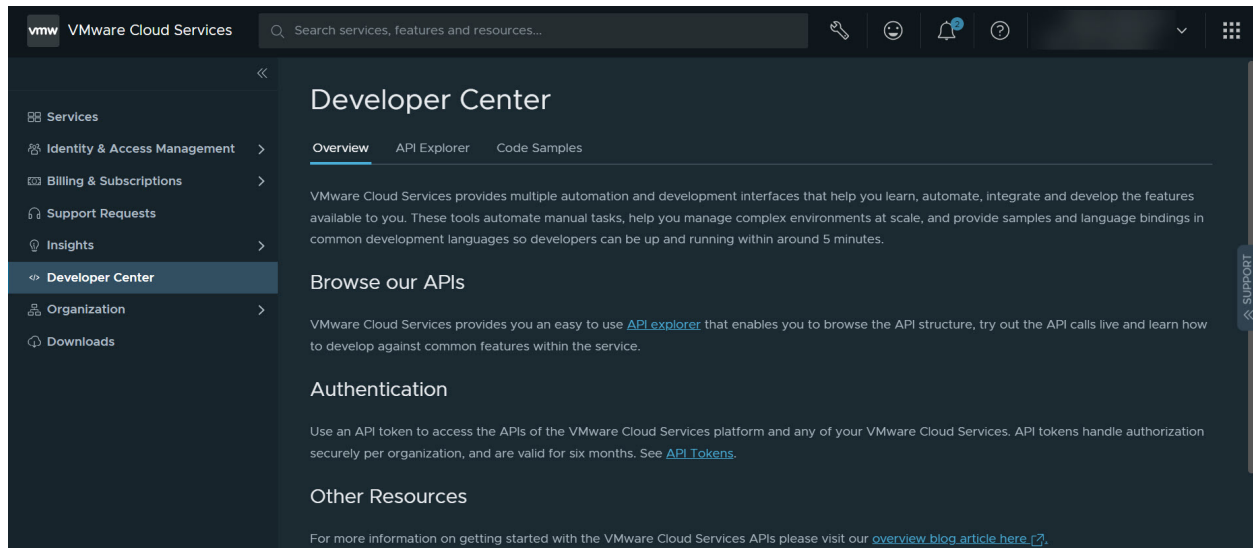
b 로컬 시스템에 소프트웨어 바이너리를 다운로드하려면 **다운로드**를 클릭합니다.

VMware Cloud Services 개발자 센터에서 작업하는 방법

9

VMware Cloud Services의 **개발자 센터**는 Cloud Services 콘솔에서 사용할 수 있는 기능을 자동화, 통합 및 개발하는 데 도움이 되는 API 인터페이스를 제공합니다.

개발자 센터는 Cloud Services 콘솔의 기본 메뉴에서 액세스할 수 있습니다. **개발자 센터**를 사용하려면 **조직 소유자** 역할이 있어야 합니다.



개발자 센터의 API 탐색기 페이지에서는 사용 가능한 VMware Cloud Services API와 상호 작용할 수 있습니다. 자세한 내용은 **API 탐색기에 대해 알아두어야 할 사항**의 내용을 참조하십시오.

개발자 센터의 코드 샘플 페이지에서는 커뮤니티에서 작성한 샘플을 찾아보고 다운로드할 수 있습니다. 샘플을 사용하여 자동화, 관리 또는 통합 작업을 시작하십시오.

다음으로 아래 항목을 읽으십시오.

- **API 탐색기에 대해 알아두어야 할 사항**
- **개발 센터에서 사용할 수 있는 API**
- **개발자 센터에서 API를 시도하는 방법**

API 탐색기에 대해 알아두어야 할 사항

조직 소유자는 Cloud Services 콘솔의 **API 탐색기**에 액세스하여 조직에서 사용할 수 있는 모든 VMware Cloud services API를 찾습니다.

다음을 수행할 수 있습니다.

- Cloud Services 콘솔에서 직접 API를 호출합니다.
- API 구조를 찾습니다.
- API 호출을 라이브로 사용해 보고 서비스 내에서 일반적인 기능을 개발하는 방법을 알아봅니다.

API와 상호 작용을 시작하려면 Cloud Services 콘솔에 로그인한 후 **개발자 센터 > API 탐색기**로 이동합니다.

Usage Management DOWNLOAD OPEN API / SWAGGER SPECIFICATION

> Description

API Categories

Filter

- > **POST** /cost-and-usage/api/{org_id}/metrics/search Search for metrics
- ▼ **GET** /cost-and-usage/api/{org_id}/usage/overview Get the usage overview of a metric

Description

The API allows you to get a summary of the usage information for a given service identifier and metric identifier in an organization. The API returns the total usage, commitment, and overage values based on the latest updated usage information. You can specify an end date to filter the usages by their latest update time prior to the time specified. If you do not specify an end date, the API will use the latest update time as the end date.

Response types

Code/Reason	Model
200 OK	UsageOverviewResponse { ... }
400 Bad Request	ApiError { ... }
401 Unauthorized	None
403 Forbidden	None

Try it out

Parameter	Value	Type	Description / Data Type
org_id (required)	<u>c0b16205-1189-4fd5-bdfe-e343f7c26bd5</u>	path	Unique identifier (GUID) of the organization Data Type: string

위의 스크린샷에 설명된 것처럼 **API 탐색기** 페이지는 사용 가능한 API를 선택하고, 조직에 대한 환경 및 서비스 정보를 복사하고, 선택한 API와 상호 작용할 수 있는 여러 섹션으로 나뉘어 있습니다.

사용 가능한 API

API 탐색기 페이지의 **사용 가능한 API** 섹션에서는 조직 환경의 API를 찾아볼 수 있습니다. 페이지 왼쪽의 API 링크를 클릭하여 다음을 확인합니다.

- 각 범주의 특정 API에 대한 정보.
- 선택한 범주에 표시된 API의 일부로 반환될 수 있는 개체 모델/데이터 구조의 목록. 이 목록에는 API 호출의 응답에서 찾을 수 있는 항목에 대한 세부 정보도 포함되어 있습니다.

API 범주에 대한 자세한 내용은 [개발 센터에서 사용할 수 있는 API](#)의 내용을 참조하십시오.

환경

API 탐색기 페이지의 **환경** 섹션에서는 다음과 같이 일부 API에 일반적으로 필요한 매개 변수를 보고 복사할 수 있습니다.

- **조직 이름:** 로그인한 조직의 이름입니다.
- **조직 ID:** 로그인한 조직의 ID입니다.
- **인증 토큰:** 보유자 토큰과 결합하여 API 호출의 인증 헤더에서 사용할 수 있습니다.
- **서비스:** 드롭다운에서 서비스를 선택하고 복사 아이콘을 클릭하면 선택한 서비스 ID가 복사됩니다.

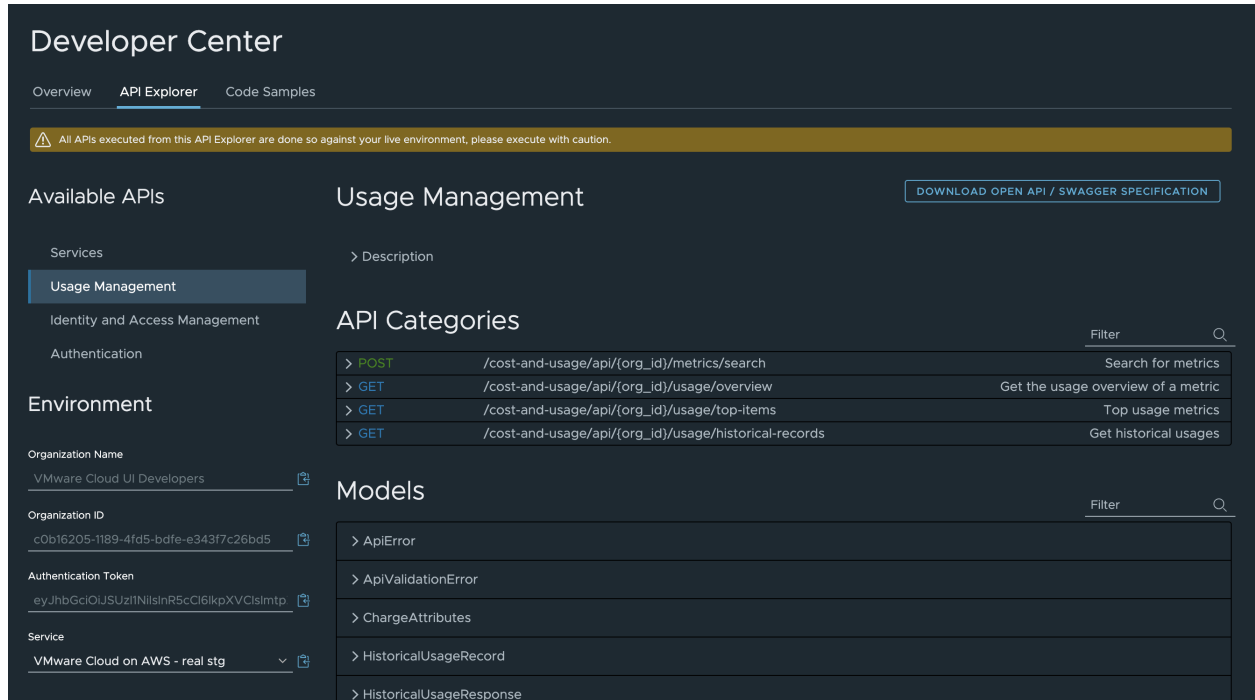
서비스 정보

서비스 정보 섹션은 **사용 가능한 API** 목록에서 API를 선택할 때 표시됩니다. 이 섹션에서는 지정된 API 범주에서 API를 호출할 때 사용할 기본 URL을 보고 복사할 수 있습니다.

개발 센터에서 사용할 수 있는 API

개발자 센터 사용자는 Cloud Services 콘솔에서 **개발자 센터 > API 탐색기** 페이지를 열어 VMware Cloud Services와 상호 작용합니다.

이 페이지에 나열된 API는 VMware Cloud Services 조직 및 조직 사용자의 기본 인증 및 관리 지점 역할을 합니다. **사용 가능한 API** 메뉴의 각 링크는 특정 범주 또는 API 그룹을 나타냅니다.



API 범주	설명
서비스	조직의 모든 서비스에 대한 API 목록과 표시 이름 및 아이콘을 포함합니다.
사용량 관리	이 API 그룹은 유형 및 지역별 검색을 포함하여 조직의 현재 및 기간별 사용량에 대한 데이터를 찾을 수 있도록 도와줍니다. 개발자 포털(https://developer.vmware.com/apis/cost-and-usage-management/latest/)에서 자세한 사용량 관리 API 설명서를 찾을 수 있습니다.
ID 및 액세스 관리	이 API 그룹을 사용하여 조직의 사용자 및 그룹을 관리합니다. 개발자 포털(https://developer.vmware.com/apis/csp/csp-iam/latest/)에서 자세한 ID 및 액세스 관리 API 설명서를 찾을 수 있습니다.
인증	Cloud Services 콘솔과 상호 작용하는 프로세스를 자동화하려는 경우 이 그룹의 API를 사용합니다. 다른 API에 연결하기 전에 Cloud Services 콘솔에서 인증해야 합니다. 이를 위해 우선 API 토큰을 생성해야 합니다. 자세한 내용은 API 토큰을 생성하는 방법 항목을 참조하십시오.

개발자 센터에서 API를 시도하는 방법

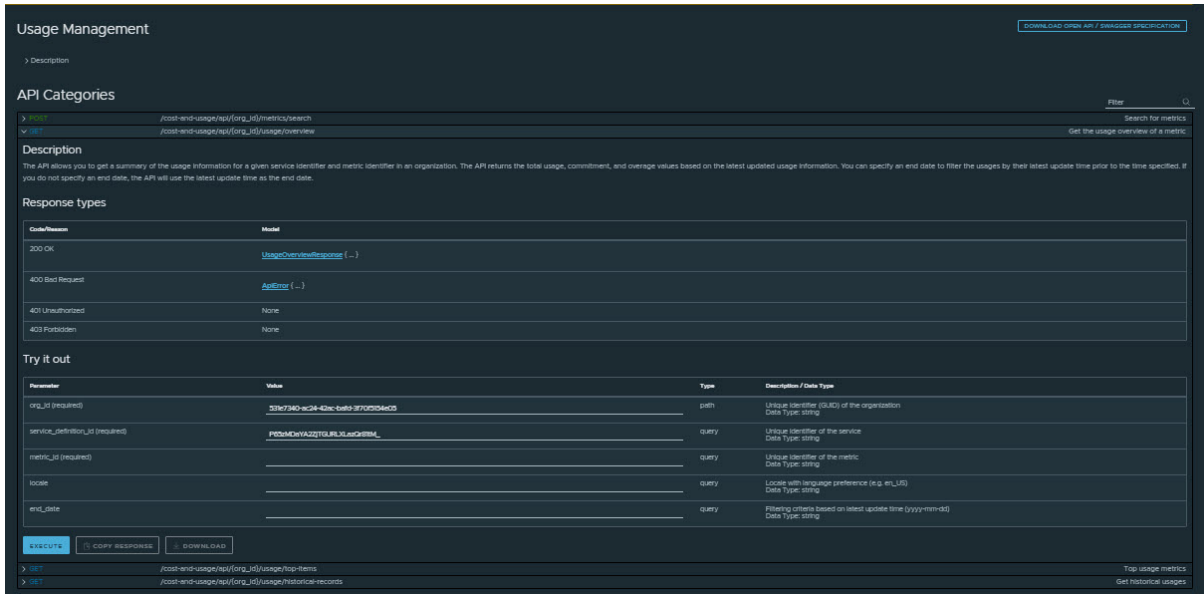
Cloud Services 콘솔의 **API 탐색기** 페이지에서 직접 조직에서 사용할 수 있는 모든 API를 사용해 볼 수 있습니다.

사전 요구 사항

조직에서 **조직 소유자** 역할이 있어야 합니다.

절차

- 1 Cloud Services 콘솔에서 자신의 조직에 로그인합니다.
- 2 개발자 센터 > API 탐색기로 이동합니다.
- 3 API 탐색기 페이지의 **사용 가능한 API** 메뉴에서 API 범주를 선택합니다.
페이지가 새로 고쳐지면서 선택한 범주에서 사용할 수 있는 모든 API가 표시됩니다.
- 4 화살표 아이콘을 사용하여 API의 콘텐츠를 확장합니다.
- 5 아래로 스크롤하여 **평가판 사용** 섹션으로 이동합니다.



- 6 API 호출을 생성하려면 필요한 속성을 입력합니다.
속성은 가능한 경우 페이지 오른쪽에 표시된 환경 세부 정보를 기반으로 미리 채워집니다.
API 통합 또는 서버 호출을 로컬로 구축하거나 사용할 때 API 규격 샘플의 조각을 사용할 수 있습니다. **API 탐색기** 페이지의 위쪽과 아래쪽에 있는 **Open API/Swagger 규격 다운로드** 버튼을 클릭하면 이 작업을 쉽게 수행할 수 있습니다. 규격 파일에는 샘플 호출 및 예상 응답이 포함되어 있습니다.
- 7 **실행**을 클릭합니다.

참고 API 탐색기에서 수행하는 모든 API 호출이 라이브 환경에 대해 실행됩니다. **평가판 사용** 기능을 사용할 때는 항상 주의를 기울여야 합니다.

결과

API 호출을 실행하면 페이지가 새로 고쳐지면서 **API 탐색기** 페이지의 **평가판 사용** 섹션 바로 아래에 응답이 표시됩니다. 모델 응답과 상호 작용하고 페이로드를 텍스트 형식으로 보고, 응답을 복사하거나 다운로드할 수 있습니다.

예제:

이 예에서는 [ID 및 액세스 관리] 범주의 API를 사용하여 현재 조직에 로그인한 사용자인 **주체 사용자**에 대한 정보를 가져옵니다.

- 1 **API 탐색기**를 엽니다.
- 2 **사용 가능한 API** 목록에서 **ID 및 액세스 관리**를 선택합니다.
- 3 표시되는 **API 범주** 목록에서 **주체 사용자**를 클릭합니다.
- 4 `GET /am/api/loggedin/user`을 클릭합니다.
- 5 **실행**을 클릭합니다.

생성한 API 호출에 대한 응답은 페이지의 **응답** 섹션에 표시되며 조직에 로그인하는 데 사용한 사용자 정보를 반환합니다.

ID 및 액세스 관리

10

조직 소유자인 사용자는 조직 및 해당 리소스에 대한 사용자 및 그룹 액세스를 제어합니다.

다음으로 아래 항목을 읽으십시오.

- 역할 및 사용 권한을 관리하는 방법
- 내 조직의 사용자를 관리하는 방법
- 그룹을 사용하는 방법
- 내 조직에서 인증 정책을 설정하는 방법
- 엔터프라이즈 페더레이션 소개 및 VMware Cloud Services에서 작동하는 방식
- ID 거버넌스 및 관리 소개 및 VMware Cloud Services에서 작동하는 방식
- OAuth 2.0으로 애플리케이션을 인증하는 방법
- VMware Cloud Services의 감사 이벤트 로그 작동 방식
- VMware Cloud Services에서 NIST 로그인 전 알림을 생성하는 방법
- 데이터 인사이트 대시보드를 사용하는 방법
- Cloud Services 콘솔에서 프로젝트 작업과 관련된 사항

역할 및 사용 권한을 관리하는 방법

조직 소유자인 사용자는 조직에 가입하도록 초대할 때 VMware Cloud Services 사용자에게 역할 기반 액세스 권한을 부여합니다.

Cloud Services 콘솔의 **ID 및 액세스 관리 > 활성 사용자** 메뉴에서 조직의 사용자 역할을 보고 관리할 수 있습니다.

조직 역할 및 사용 권한

조직의 리소스에 대한 액세스 권한은 조직의 각 사용자에게 할당된 역할에 따라 결정됩니다. 각 사용자는 조직에서 다음 역할 중 하나 이상을 할당받을 수 있습니다.

- 조직 소유자
- 조직 멤버

■ **조직 관리자**

각 조직 역할에 대한 사용 권한을 보려면 VMware Cloud Services에서 사용할 수 있는 **조직 역할** 항목을 참조하십시오.

서비스 역할 및 사용 권한

VMware Cloud services에는 조직의 사용자에게 할당할 수 있는 미리 정의된 기본 제공 서비스 역할 집합이 제공됩니다. **조직 소유자**인 사용자는 조직 내 다른 사용자에게 각 클라우드 서비스가 제공하는 역할에 따라 클라우드 서비스에 대한 액세스 권한을 부여합니다. 기본 제공 서비스 역할에 대한 자세한 내용은 관련 VMware Cloud 서비스의 설명서를 참조하십시오.

VMware Cloud Services에서 사용할 수 있는 조직 역할

VMware Cloud Services 사용자는 조직에서 **조직 멤버**, **조직 관리자** 또는 **조직 소유자**와 같은 조직 역할을 가질 수 있습니다.

조직 역할 및 사용 권한

각 조직의 사용 권한 수준은 다음과 같이 다양합니다.

- **조직 소유자** 역할은 조직의 모든 리소스에 대한 전체 관리 액세스 권한을 갖습니다. **조직 소유자**인 사용자는 자신에게 역할을 직접 할당할 수도 있습니다.
- **조직 관리자** 역할에는 제한된 관리 액세스 권한이 있습니다. **조직 관리자**인 사용자는 조직 역할에 서비스 역할을 할당할 수 있지만 관리 권한이 같거나 더 낮은 역할이 있는 사용자, 그룹 및 OAuth 애플리케이션만 관리할 수 있습니다.

예를 들어, **조직 관리자**인 사용자는 조직에서 **조직 멤버** 또는 **조직 관리자** 역할을 가진 다른 사용자 및 그룹에 대한 액세스 권한을 부여하거나 관리할 수 있지만 **조직 소유자** 역할이 할당된 사용자, 그룹 또는 리소스는 관리할 수 없습니다.

- **조직 멤버** 역할에는 조직 리소스에 대한 읽기 전용 액세스 권한이 있습니다.

다음은 VMware Cloud Services에서 세 가지 조직 역할의 사용 권한에 대해 알고 있어야 하는 내용입니다. 사용자에게 서로 충돌하는 역할이 할당되면 사용자는 사용 권한이 더 큰 역할을 받게 됩니다.

사용 권한	조직 소유자	조직 관리자	조직 멤버
하나 이상의 조직에 속해 있습니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
기타 조직 중 하나에 액세스합니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
로그인할 때 표시되는 조직을 지정합니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
조직 설정을 보고 수정합니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 보기 전용.	<input checked="" type="checkbox"/> 보기 전용.
조직에서 사용자를 추가/제거합니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 조직 멤버 또는 조직 관리자 역할이 있는 사용자만 해당됩니다.	

사용 권한	조직 소유자	조직 관리자	조직 멤버
조직에서 사용자의 서비스 액세스 및 역할을 관리합니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
지불 방법 및 청구서를 관리하고 봅니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 청구 읽기 전용 확인란을 선택한 경우, 이 역할은 청구 관련 정보에 대한 읽기 전용 액세스 권한 및 사용량 소비 보고서를 생성하는 옵션을 제공합니다.	<input checked="" type="checkbox"/> 청구 읽기 전용 확인란을 선택한 경우, 이 역할은 청구 관련 정보에 대한 읽기 전용 액세스 권한 및 사용량 소비 보고서를 생성하는 옵션을 제공합니다.
지원 티켓을 제출 및 관리합니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 지원 사용자 확인란이 선택된 경우.	<input checked="" type="checkbox"/> 지원 사용자 확인란이 선택된 경우.
고객 사용량 및 데이터에 대해 클라우드 서비스 API를 쿼리합니다. 이 사용 권한은 특정 고객 프로파일에 대해서만 사용할 수 있습니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 관리 서비스 제공자 확인란이 선택된 경우.	<input checked="" type="checkbox"/> 관리 서비스 제공자 확인란이 선택된 경우.
타사 앱이 보호된 리소스에 액세스하도록 인증하기 위해 OAuth 앱을 생성하고 관리할 수 있습니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 조직의 사용자가 생성한 OAuth 애플리케이션에만 해당됩니다.	<input checked="" type="checkbox"/> 개발자 확인란이 선택된 경우.
조직의 연결된 vRealize Log Insight Cloud 서비스 인스턴스에서 조직에 대한 모든 감사 데이터에 액세스합니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 액세스 로그 감사자 확인란이 선택된 경우.	<input checked="" type="checkbox"/> 액세스 로그 감사자 확인란이 선택된 경우.
클라우드 서비스에 대한 추가 소프트웨어 바이너리 및 패키지 다운로드 링크에 액세스합니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 소프트웨어 설치 관리자 확인란이 선택된 경우.	<input checked="" type="checkbox"/> 소프트웨어 설치 관리자 확인란이 선택된 경우.
프로젝트 및 해당 리소스에 대한 액세스를 생성, 수정 및 관리합니다.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 프로젝트 관리자 확인란이 선택된 경우.	<input checked="" type="checkbox"/> 프로젝트 관리자 확인란이 선택된 경우.

내 조직의 사용자를 관리하는 방법

조직 소유자인 사용자는 사용자 액세스를 관리하고 조직의 사용자 및 그룹에 부여되는 서비스 및 조직 수준 사용 권한을 결정합니다.

Cloud Services 콘솔의 **ID 및 액세스 관리** 메뉴를 사용하여 조직에 사용자를 초대하고 조직 및 서비스 역할을 할당하고 사용자 역할을 변경하거나 조직에서 사용자를 제거합니다.

참고 사용자 역할에 변경한 사항이 조직에 적용되는 데 최대 30분이 걸릴 수 있습니다.

사용자를 조직에 초대할 때 다음과 같은 두 가지 유형의 역할 기반 액세스 권한을 할당합니다.

- 조직의 클라우드 서비스 중 하나 이상에 대한 액세스 권한. 서비스에서 제공하는 역할을 하나 이상 할당하여 사용자에게 서비스에 대한 액세스 권한을 부여합니다. 자세한 내용은 관련 VMware Cloud Service의 설명서를 참조하십시오.
- 조직에 대한 역할 기반 액세스 권한. 전체 액세스 권한이 있는 **조직 소유자**인 사용자 또는 읽기 전용 액세스 권한이 있는 **조직 멤버**인 사용자.

그룹에 액세스 권한을 할당하는 것은 한 번에 하나씩 개별 사용자에게 동일한 사용 권한을 할당하는 것보다 효율적입니다. **조직 멤버**는 그룹을 구성하는 사용자와 이들에게 할당된 역할 및 사용 권한을 결정합니다.

내 조직에 사용자를 추가하는 방법

조직 소유자는 사용자를 조직에 초대하여 연결된 서비스에 대한 액세스 권한을 부여합니다. 전송한 초대를 추적할 수도 있습니다. 초대는 최대 7일 동안 유효합니다. 초대를 잘못 전송한 경우 해당 초대를 취소할 수 있습니다.

초대된 사용자는 다음과 같이 여러 역할을 보유할 수 있습니다.

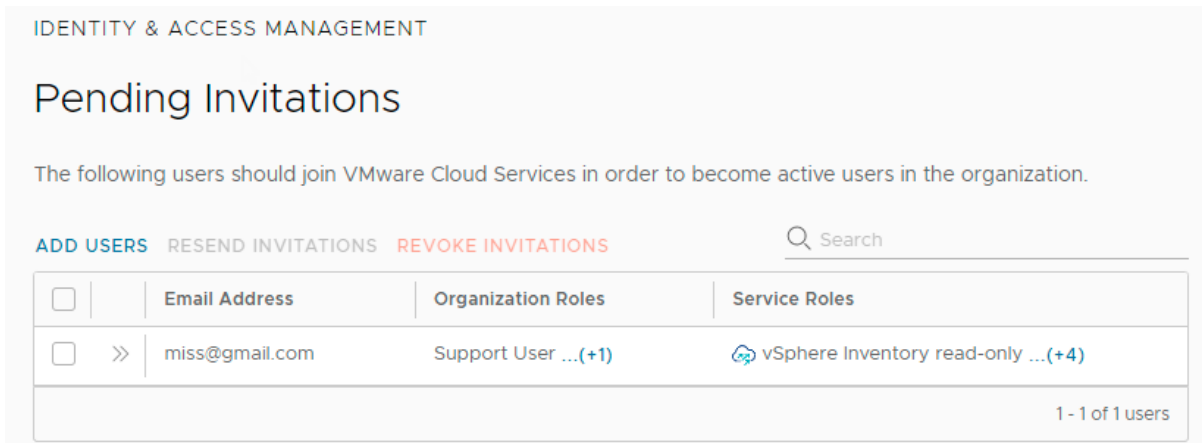
- 조직 내의 역할 - **조직 소유자** 또는 **조직 멤버**. 이러한 각 역할에 할당된 사용 권한을 보려면 [VMware Cloud Services에서 사용할 수 있는 조직 역할](#) 항목을 참조하십시오.
- 사용자를 초대하는 클라우드 서비스 내의 역할. 각 클라우드 서비스에는 고유한 특정 역할이 있습니다. 자세한 내용은 관련 VMware Cloud services의 설명서를 참조하십시오.
- 고객 프로파일에 따라 사용자가 고객 사용량 및 데이터에 대해 클라우드 서비스 API를 쿼리하도록 허용하는 관리 서비스 제공자 역할을 볼 수도 있습니다. 이 역할을 테넌트 조직의 사용자에게 할당하는 경우 해당 사용자는 조직 내의 모든 데이터에 대한 액세스 권한을 갖습니다.

절차

- 1 Cloud Services 콘솔 도구 모음에서 **VMware Cloud Services** 아이콘을 클릭하고 **ID 및 액세스 관리 > 활성 사용자**를 선택합니다.
- 2 **사용자 추가**를 클릭합니다.
- 3 **새 사용자 추가** 페이지에서 다음 정보를 입력합니다.
 - a **사용자** 텍스트 상자에 조직에 추가할 사용자의 이메일 주소를 입력합니다.
이메일 주소를 쉼표로 구분하거나 각 이메일 주소를 별도의 줄에 입력하여 한 번에 둘 이상의 사용자를 추가할 수 있습니다.
 - b **조직 역할 할당** 섹션에서 사용자가 조직에서 갖게 될 역할을 할당합니다.
조직 소유자 역할에는 전체 관리 액세스 권한이 있습니다. 새 사용자에게 대한 **조직 멤버** 역할을 선택하는 경우 **추가 역할** 섹션에서 하나 이상의 역할을 선택하여 다른 액세스 권한을 추가하는 것이 좋습니다.
 - c 조직에서 사용자 서비스 역할을 할당하려면 **서비스 액세스 추가**를 클릭하고 드롭다운 메뉴를 사용하여 항목을 선택합니다.
 - d **서비스 액세스 추가**를 다시 클릭하여 사용자에게 다른 서비스에 대한 액세스 권한을 부여합니다.

4 **추가**를 클릭하여 사용자에게 초대를 전송합니다.

전송한 초대는 7일 동안 유효합니다. **ID 및 액세스 관리 > 보류 중인 초대** 탭에서 초대의 상태를 볼 수 있습니다.



5 초대를 잘못 전송한 경우 해당 초대를 취소할 수 있습니다. 초대 옆의 확인란을 선택하고 **초대 취소**를 클릭합니다.

이메일의 활성화 링크가 해지되고 메일의 전송 대상으로 지정된 사용자가 서비스에 로그인할 수 없습니다.

내 조직에서 사용자를 제거하는 방법

조직 소유자는 조직에서 사용자를 제거할 수 있습니다. 제거된 사용자는 조직 및 해당 서비스에 액세스할 수 없습니다.

절차

- 1 Cloud Services 콘솔을 열고 **ID 및 액세스 관리 > 활성 사용자**를 선택합니다.
- 2 하나 이상의 사용자를 선택하고 **사용자 제거**를 클릭합니다.
- 3 **제거**를 클릭하여 조직에서 사용자를 영구적으로 제거합니다.

사용자 역할을 변경하는 방법

사용자가 조직에 가입하면 사용자는 **조직 소유자**가 직접 부여한 조직 및 서비스 역할 액세스 권한을 받거나 그룹의 멤버로 상속합니다. **조직 소유자**는 Cloud Services 콘솔에서 사용자 역할을 보고 편집할 수 있습니다.

사용자 역할 편집과 관련하여 다음 내용을 알아두어야 합니다.

- 사용자는 역할의 조합, 즉 자신들에게 직접 할당된 역할과 그룹에서 상속된 역할을 보유할 수 있습니다. 예를 들어 지원 사용자에게 대한 직접 역할 할당과 개발자 및 VMware Cloud on AWS 관리자와 같이 그룹에서 상속된 일부 역할이 있습니다.
- 사용자에게 서로 충돌하는 역할이 할당되면 사용자는 사용 권한이 더 큰 역할을 받게 됩니다. 예를 들어 사용자에게 읽기 전용 역할과 관리자 역할이 할당되면 사용자는 관리자 역할을 받습니다.

절차

- 1 Cloud Services 콘솔 도구 모음에서 **VMware Cloud Services** 아이콘을 클릭하고 **ID 및 액세스 관리 > 활성 사용자**를 선택합니다.
- 2 사용자 이름 옆에 있는 이중 화살표 아이콘(»)을 클릭하여 해당 역할을 보고 해당 역할이 그룹에 속하는지 확인합니다.
사용자의 역할을 변경하는 경우 그룹에서 할당된 역할이 재정의될 수 있습니다.
- 3 사용자 옆의 확인란을 선택하고 **역할 편집**을 클릭합니다.
- 4 사용자의 조직 역할과 서비스 역할을 필요에 맞게 변경합니다.
- 5 **저장**을 클릭합니다.

그룹을 사용하는 방법

그룹에 역할을 할당하는 것은 한 번에 하나씩 개별 사용자에게 동일한 사용 권한을 할당하는 것보다 효율적입니다. **조직 소유자**인 사용자는 그룹을 생성하고 그룹을 구성하는 멤버와 할당된 역할을 결정합니다.

또한 그룹이 생성되거나 추가된 후 그룹을 편집할 수도 있습니다. 조직이 확장되고 변경될 때 그룹에서 멤버를 추가하거나 제거합니다.

VMware Cloud services에서 사용 가능한 두 가지 유형의 그룹은 사용자 지정 그룹 및 엔터프라이즈 그룹입니다. 사용자 지정 그룹은 다른 조직과 공유할 수 있습니다. 엔터프라이즈 그룹은 사용자 지정 그룹에 중첩될 수 있습니다.

사용자 지정 그룹

이름과 설명을 입력하고 멤버를 추가한 다음 조직과 리소스에 대한 역할을 할당하여 사용자 지정 그룹을 생성합니다. 예를 들어 사용자 지정 그룹을 생성하고 조직에 **조직 멤버** 역할, 지원 역할 및 조직의 특정 서비스에 대한 읽기 전용 액세스 권한을 부여할 수 있습니다. 사용자 지정 그룹에는 엔터프라이즈 그룹도 포함될 수 있습니다.

사용자 지정 그룹의 경우 이름 및 설명을 편집하고, 멤버를 추가 또는 제거하고, 그룹의 역할 할당을 변경할 수 있습니다.

공유 그룹

사용자 지정 그룹을 생성할 때 그룹을 공유로 만들지 여부를 결정할 수 있습니다. **조직 소유자**는 공유 그룹을 다른 조직과 연결하여 공유 그룹의 멤버에게 연결된 조직의 역할을 할당하고 **조직 소유자**의 초대 없이 서비스에 액세스하도록 허용할 수 있습니다.

공유 그룹에 할당된 서비스 역할은 조직별로 다릅니다. 연결된 조직의 **조직 소유자**는 공유 그룹을 가져오고 자신의 조직 내에서 그룹에 역할을 할당합니다. 공유 그룹을 가져오기 위해 **조직 소유자**는 그룹의 이름 또는 ID를 알고 있어야 합니다.

소스 조직(공유 그룹이 생성된 조직)의 **조직 소유자**만 그룹의 멤버를 수정하거나 제거할 수 있습니다. 공유 그룹은 연결된 조직에서 제거해도 삭제되지 않으며 나중에 다시 추가할 수 있습니다. [공유 그룹을 관리하는 방법](#) 방법을 참조하십시오.

엔터프라이즈 그룹

엔터프라이즈 그룹은 회사 도메인에서 동기화된 그룹입니다. 회사 도메인을 VMware Cloud services와 페더레이션하면 조직에서 사용할 수 있는 엔터프라이즈 그룹이 제공됩니다. [엔터프라이즈 그룹에 역할을 할당하는 방법](#)하는 방법을 참조하십시오.

엔터프라이즈 그룹의 경우 그룹의 역할 할당만 변경할 수 있습니다. VMware Cloud services의 엔터프라이즈 그룹에서 멤버를 추가하거나 제거할 수 없지만, 이러한 멤버에게 조직 및 해당 리소스에 대한 역할을 할당하고 사용자 지정 그룹에 추가할 수 있습니다.

중첩된 그룹

그룹을 다른 그룹에 추가하는 것을 중첩이라고 합니다. 다음은 중첩된 그룹에 대해 알고 있어야 하는 내용입니다.

- 엔터프라이즈 그룹을 사용자 지정 그룹에 중첩할 수 있습니다.
- 중첩된 그룹은 엔터프라이즈 그룹에 직접 할당된 역할 및 사용자 지정 그룹을 통해 할당된 역할의 조합을 보유할 수 있습니다.
- 중첩된 엔터프라이즈 그룹의 역할을 편집하거나 다른 역할을 추가할 수 있지만, 사용자 지정 그룹에서 상속한 역할은 제거할 수 없습니다.
- 사용자 지정 그룹은 다른 사용자 지정 그룹에 중첩할 수 없습니다.

조직 소유자는 그룹이 생성되거나 추가된 후에도 그룹을 편집할 수 있습니다. 사용자 지정 그룹의 경우 이름 및 설명을 편집하고, 멤버를 추가 또는 제거하고, 그룹의 역할 할당을 변경할 수 있습니다. 엔터프라이즈 그룹의 경우 그룹의 역할 할당만 변경할 수 있습니다.

조직 소유자는 그룹을 생성하고, 그룹을 관리하고, 조직의 확장 및 변경에 따라 그룹에서 멤버를 추가하거나 제거합니다.

참고 그룹을 변경하면 변경 내용이 조직에 적용되는 데 최대 30분이 걸릴 수 있습니다.

새 그룹을 생성하는 방법

조직 소유자인 사용자는 조직에서 새 그룹을 생성하고 그룹에 조직 및 서비스 역할을 할당할 수 있습니다. 이러한 그룹을 사용자 지정 그룹이라고 합니다.

각 조직 역할에 할당된 사용 권한에 대한 자세한 내용은 [역할 및 사용 권한을 관리하는 방법](#) 항목을 참조하십시오. 서비스 역할에 할당된 사용 권한에 대한 자세한 내용은 해당 서비스 설명서를 참조하십시오.

절차

- 1 Cloud Services 콘솔에서 **ID 및 액세스 관리 > 그룹**을 선택합니다.
- 2 **그룹 추가**를 클릭합니다.

- 3 새 그룹 생성을 선택하고 **계속**을 클릭합니다.
- 4 그룹의 이름과 설명을 입력합니다.
- 5 그룹을 다른 조직과 공유하려면 **조직 추가**를 클릭합니다.
 - a 그룹을 공유할 조직을 선택합니다. 각 조직의 조직 ID를 입력하거나 팝업 창에 표시된 조직의 목록에서 선택합니다.
 - b **추가**를 클릭합니다.

참고 공유되는 사용자 지정 그룹을 생성하면 연결된 조직의 **조직 소유자**가 조직의 그룹에 역할을 할당할 수 있습니다.

- 6 **멤버 추가**를 클릭하여 그룹에 멤버를 추가하고 **추가**를 클릭합니다.
 멤버는 엔터프라이즈 그룹 및 사용자일 수 있습니다. 이 단계를 건너뛰고 그룹을 생성한 후에 멤버를 추가하도록 선택할 수 있습니다.
- 7 조직 역할을 선택하여 그룹에 조직에 대한 액세스 권한을 할당합니다.
- 8 **서비스 액세스 추가**를 클릭하고 서비스 및 이 서비스에 대해 그룹에 할당하려는 역할을 선택하여 그룹에 서비스에 대한 액세스 권한을 할당합니다.
- 9 추가 서비스에 대한 액세스 권한을 추가하려면 **서비스 액세스 추가**를 클릭합니다.
- 10 **생성**을 클릭합니다.
 그룹이 ID 및 액세스 관리 페이지의 그룹 목록에 추가됩니다.

엔터프라이즈 그룹에 역할을 할당하는 방법

도메인이 VMware Cloud services와 페더레이션된 경우 회사 소스 도메인에서 그룹을 선택하고 조직에서 역할을 할당할 수 있습니다. 이러한 그룹을 엔터프라이즈 그룹이라고 합니다.

엔터프라이즈 그룹은 회사 도메인에서 동기화된 그룹입니다. 한 번에 2개 이상의 엔터프라이즈 그룹에 역할을 할당할 수 있으며 선택된 그룹의 멤버를 볼 수 있습니다.

할당하는 그룹의 멤버는 다음과 같이 여러 역할을 보유할 수 있습니다.

- 조직 역할: 조직 내의 역할 - **조직 소유자** 또는 **조직 멤버**. 이러한 각 역할에 할당된 권한을 보려면 **역할 및 사용 권한을 관리하는 방법** 항목을 참조하십시오.
- 서비스 역할: 하나 이상의 VMware Cloud services 내에 있는 역할입니다. 각 클라우드 서비스에는 고유한 특정 역할이 있습니다. 자세한 내용은 관련 VMware Cloud Service의 설명서를 참조하십시오.
- 고객 프로파일에 따라 사용자가 고객 사용량 및 데이터에 대해 클라우드 서비스 API를 쿼리하도록 허용하는 관리 서비스 제공자 역할을 볼 수도 있습니다. 이 역할을 테넌트 조직의 멤버에게 할당하는 경우 해당 사용자는 조직 내의 모든 데이터에 대한 액세스 권한을 갖습니다.

절차

- 1 Cloud Services 콘솔 기본 메뉴에서 **ID 및 액세스 관리 > 그룹**을 선택합니다.

2 **소스 도메인에서 그룹 선택**을 클릭한 후 **계속**을 클릭합니다.

3 역할을 할당할 엔터프라이즈 그룹을 검색합니다.

4 그룹에 조직 역할을 할당합니다.

각 역할의 사용 권한을 보려면 위의 링크를 참조하십시오.

5 서비스를 선택한 다음 그룹에 서비스의 하나 이상의 역할을 할당합니다.

서비스를 선택하면 서비스 기본 역할이 나타납니다. 역할을 클릭하여 다른 역할을 선택합니다.

6 그룹에 다른 서비스에 대한 액세스 권한을 부여하려면 **서비스 액세스 추가**를 클릭하고 역할을 할당합니다.

7 **추가**를 클릭합니다.

조직 멤버 역할이 있는 사용자에게 이메일을 전송하려면 확인란을 선택합니다. **조직 소유자** 및 지원 사용자 역할이 있는 사용자에게 이메일이 자동으로 전송됩니다.

공유 그룹을 관리하는 방법

조직 소유자인 사용자가 사용자 지정 그룹을 생성하고 이를 다른 조직과 연결하면 해당 그룹이 공유됩니다. 대상 조직의 **조직 소유자**는 소스 **조직의 소유자**로부터 이메일 초대를 받아 공유 그룹을 가져오고 서비스 역할을 할당합니다.

다른 조직에서 생성된 공유 그룹을 가져오기 위한 초대를 받는 **조직 소유자**는 공유 그룹을 조직으로 가져오는 동안 공유 그룹에 대한 서비스 역할을 할당합니다.

가져온 공유 그룹과 조직에서 생성된 공유 그룹은 레이블(**Custom | remote**)로 구분할 수 있습니다.

가져온 공유 그룹의 사용자는 그룹에 할당된 역할에 따라 조직의 서비스에 액세스할 수 있습니다. 이에 따라 그룹 수준의 서비스에 대한 조직 간 액세스가 허용되고 각 사용자에게 개별 초대를 보낼 필요가 없습니다.

중요 다른 조직에서 가져온 공유 그룹은 편집할 수 없습니다. 공유 그룹에 직접 할당한 역할을 편집하거나 조직에서 그룹을 제거할 수 있습니다.

사전 요구 사항

추가할 공유 그룹을 생성한 소스 조직의 이름 또는 조직 ID를 알고 있어야 합니다.

절차

1 Cloud Services 콘솔에서 **ID 및 액세스 관리 > 그룹**을 선택합니다.

2 **그룹 추가**를 클릭합니다.

3 **다른 조직에서 그룹 가져오기**를 선택하고 **계속**을 클릭합니다.

4 드롭다운 메뉴에서 공유 그룹을 생성한 소스 조직을 선택합니다.

5 가져올 공유 그룹을 선택합니다.

6 선택한 그룹 액세스를 조직에 할당할 조직 역할을 선택합니다.

- 7 선택한 그룹에 서비스 역할을 할당하려면 **서비스 액세스 추가**를 클릭합니다.
 - a 드롭다운 메뉴를 사용하여 공유 그룹에서 액세스할 조직의 서비스를 선택합니다.
 - b 역할 상자를 클릭하고 공유 그룹에 할당할 서비스 역할을 선택합니다.
 - c 액세스 기간을 정의합니다. 종료 날짜를 선택하거나 만료되지 않은 액세스를 제공할 수도 있습니다.
- 8 추가 서비스에 대한 액세스 권한을 추가하려면 **서비스 액세스 추가**를 클릭하고 7.a~7.c 단계를 반복합니다.
- 9 공유 그룹의 모든 사용자가 서비스에 액세스할 수 있는 초대를 받도록 하려면 **초대된 모든 사용자에게 이 역할 할당을 알리는 이메일 보내기**를 선택한 상태로 둡니다.
- 10 **가져오기**를 클릭합니다.

결과

공유 그룹이 조직에 사용자 지정 원격 그룹으로 추가됩니다.

내 조직에서 인증 정책을 설정하는 방법

조직 소유자인 사용자는 도메인 수준에서 VMware Cloud services 조직에 대한 사용자 액세스(예: 다단계 인증, IP 인증 기본 설정 및 사용자 액세스) 인증 정책을 설정합니다.

조직에 대한 인증 정책 설정은 Cloud Services 콘솔의 **조직 > 인증 정책** 페이지에서 생성 및 관리합니다.

중요 새 정책 또는 정책 변경 사항을 적용하는 데 최대 30분이 걸릴 수 있습니다.

조직에 여러 인증 정책이 설정되어 있으면 각 사용자 로그인에 모든 정책에 대해 순서대로 검증됩니다. 어느 정책 이든 위반하면 사용자는 조직에 액세스할 수 없습니다.

다단계 인증을 설정하는 방법

MFA(다단계 인증)가 적용되면 조직의 모든 사용자는 로그인 자격 증명 외에 6자리 인증 코드를 제공해야 합니다. 코드를 제공하려면 MFA 디바이스를 VMware Cloud Services에 등록해야 합니다. 유효한 MFA 코드를 제공하지 못한 조직 사용자는 조직에 대한 액세스가 거부됩니다.

페더레이션된 도메인의 **조직 소유자**인 경우 조직의 MFA를 제어하지 않습니다. 페더레이션된 도메인에 대한 MFA는 회사에서 사용 중인 ID 제공자의 **엔터프라이즈 관리자**가 구성합니다. 이 절차는 페더레이션되지 않은 도메인에 만 적용됩니다.

사전 요구 사항

- 조직에서 **조직 소유자** 역할이 있어야 합니다.
- MFA를 적용한 후에 조직에서 자신을 잠그지 않도록 VMware Cloud Services에 MFA 디바이스가 등록되어 있어야 합니다. 자세한 지침은 **다단계 인증을 사용하여 내 계정을 보호하는 방법**의 내용을 참조하십시오.

절차

- 1 Cloud Services 콘솔에 로그인하고 **조직 > 인증 정책**을 클릭합니다.

2 **다단계 인증** 섹션에서 토글 버튼을 클릭하여 버튼 색상을 녹색으로 바꿉니다.

결과

이제 MFA가 적용됩니다. 조직의 모든 사용자는 MFA 디바이스를 등록해야 하며 로그인 시 MFA 토큰을 제공해야 합니다.

참고 정책이 조직에 적용되는 데 최대 30분이 걸릴 수 있습니다.

IP 인증 기본 설정을 정의하는 방법

조직 소유자는 특정 IP에서 사용자 액세스를 차단하거나 허용하도록 IP 주소 또는 IP 범위를 정의하여 조직에 대한 액세스를 관리할 수 있습니다.

이렇게 하려면 인증 기본 설정을 적용하여 IP 범위 또는 특정 IP 주소에서의 사용자 액세스를 차단하거나 허용합니다. 인증 기본 설정이 IP 범위에 대해 정의된 경우 범위 내의 특정 IP에 대한 예외를 설정할 수 있습니다. 예를 들어 IP 범위에 블록 인증을 적용하는 경우 해당 범위 내에 있는 하나 이상의 IP에 대해 예외를 설정하여 VMware Cloud services에 대한 액세스를 허용할 수 있습니다.

참고 입력한 IP 주소는 IPv4 및 IPv6 IP 주소에 대한 CIDR 표기법을 따라야 합니다.

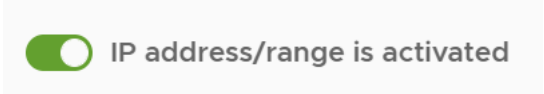
다음 두 가지 인증 기본 설정 옵션을 정의할 수 있습니다.

- **IP 차단:** 특정 IP 주소/범위의 사용자 로그인은 조직에 대한 액세스가 차단됩니다.
- **IP 허용:** 특정 IP 주소/범위의 사용자 로그인은 조직에 대한 액세스가 허용됩니다.

조직에서 기본 설정을 하나만 활성화할 수 있습니다. 두 기본 설정 사이를 전환할 수 있지만 두 가지 기본 설정을 동시에 활성화할 수는 없습니다.

조직에서 IP 인증 기본 설정을 지정하거나 수정하려면 Cloud Services 콘솔에 로그인하고 **조직 > 인증 정책 > IP 주소/범위**로 이동합니다.

참고 정책 설정이 조직에 적용되는 데 최대 30분이 걸릴 수 있습니다.

수행할 작업	절차
조직에 대한 IP 인증 기본 설정 지정	<ol style="list-style-type: none"> 1 IP 인증 기본 설정을 처음으로 설정하는 경우 옵션을 선택하고 활성화를 클릭합니다. 정책 설정 페이지가 표시되고 IP 주소/범위가 조직에서 활성화 되었음을 나타냅니다.  2 추가를 클릭하고 IP 주소 또는 범위를 입력합니다. 3 다시 추가를 클릭합니다. 입력한 주소 또는 범위가 조직에 대해 지정된 차단된 주소 또는 허용된 주소 및 범위 목록에 추가됩니다.
인증 기본 설정에 예외 추가	<p>허용되거나 차단된 IP 목록에 이미 지정된 IP 범위의 IP 주소에 대한 예외 규칙을 정의합니다.</p> <ol style="list-style-type: none"> 1 IP 주소/범위 페이지의 예외 섹션에서 예외 추가를 클릭합니다. 2 팝업 창이 열리면 조직의 인증 정책에 예외로 추가할 IP 주소를 입력합니다. IP 허용 기본 설정을 활성화한 경우 예외 목록에 있는 IP에서 VMware Cloud services에 액세스하는 사용자는 액세스가 거부됩니다. 반대로 IP 차단 기본 설정을 활성화한 경우 예외 목록에 있는 IP에서 VMware Cloud services에 액세스하는 사용자는 액세스가 허용됩니다.
인증 기본 설정에 대한 IP 주소, 범위 또는 예외 수정	<p>IP 인증 정책을 활성화한 후에는 IP, IP 범위 및 예외를 더 추가할 수 있습니다. 정책에서 기존 IP 및 범위를 수정하거나 제거할 수도 있습니다.</p> <ul style="list-style-type: none"> ■ 변경하려면 먼저 목록에서 IP 주소 또는 범위를 선택한 다음 적절한 작업을 적용합니다.
IP 인증 기본 설정 변경	<p>조직의 인증 기본 설정을 IP 차단에서 IP 허용으로 또는 그 반대로 전환하려면 먼저 현재 인증 기본 설정에 지정된 IP 주소 및 범위를 모두 제거해야 합니다.</p> <ol style="list-style-type: none"> 1 IP 주소/범위 페이지에서 현재 정의된 모든 IP 주소 및 범위를 선택합니다. 2 제거를 클릭합니다. 3 [사용자 IP 인증 기본 설정] 옵션 옆에 있는 변경 링크를 클릭합니다. 4 팝업 창이 열리면 새 옵션을 선택한 다음 저장을 클릭합니다. 5 새로 선택한 정책 설정에 대해 새 IP 주소 또는 범위를 정의하려면 추가를 클릭합니다.

실수로 자신을 차단하여 내 IP 차단 해제

실수로 조직에 대한 **IP 차단** 목록에 IP를 추가한 경우 차단 해제하려면 지원 티켓을 제출해야 합니다. 조직에 로그인하여 Cloud Services 콘솔의 **지원 센터**를 사용할 수 없으므로 VMware 지원에 연락하여 이 작업을 수행할 수 있습니다.

내 조직의 사용자 IP 주소를 차단하면 해당 사용자가 멤버인 다른 조직에 액세스하지 못하게 차단

사용자가 여러 조직에 속하고 IP 기반 정책이 이러한 조직 중 하나에서 적용될 경우 해당 특정 조직에 대한 액세스가 허용되지 않습니다. 그런 다음 로그인 시 다른 조직으로 전환할 수 있는 옵션이 제공됩니다.

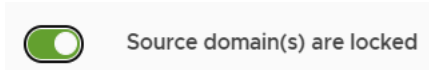
도메인 수준에서 사용자 액세스를 관리하는 방법

조직 소유자인 사용자는 VMware Cloud Services 조직에 액세스할 수 있는 도메인을 결정할 수 있습니다.

소스 도메인 인증 정책이 활성화되면 지정한 도메인의 사용자만 조직에 액세스할 수 있습니다. 다른 모든 도메인의 액세스는 그룹 및 사용자가 조직에 추가되거나 초대된 경우에도 잠겨 있습니다.

절차

- 1 Cloud Services 콘솔에 로그인하고 **조직 > 인증 정책 > 소스 도메인**으로 이동합니다.
- 2 정책을 활성화하려면 슬라이더를 클릭하고 소스 도메인이 잠겨 있음을 표시하도록 위치를 변경합니다.



- 3 조직에 대한 액세스를 허용할 도메인 이름을 입력합니다.
- 4 허용된 도메인 목록에 도메인 및 하위 도메인을 더 추가하려면 **도메인 추가** 링크를 클릭합니다.
- 5 **저장**을 클릭합니다.

결과

지정한 도메인 및 하위 도메인에 대해 이제 소스 도메인이 활성화되었습니다. 허용된 도메인에서 로그인하는 조직 멤버만 조직에 액세스할 수 있습니다. 다른 도메인에서 로그인하는 사용자의 액세스가 잠깁니다.

참고 조직에 정책이 적용되는 데 최대 30분이 걸릴 수 있습니다.

사용자 또는 다른 **조직 소유자**가 실수로 조직에 대한 액세스가 허용되는 소스 도메인 목록에 사용자 도메인을 포함시키지 않아 조직에 액세스할 수 없게 된 경우에는 도움말 지원 티켓을 엽니다.

엔터프라이즈 페더레이션 소개 및 VMware Cloud Services에서 작동하는 방식

VMware Cloud services를 사용하는 엔터프라이즈는 여러 회사 도메인과 페더레이션을 설정할 수 있습니다. 회사 도메인을 페더레이션하여 엔터프라이즈의 사용자에 대해 Single Sign-On을 활성화할 수 있습니다. VMware Cloud services와의 엔터프라이즈 페더레이션은 셀프 서비스 워크플로를 통해 설정되며 SAML 2.0 기반 ID 제공자와의 통합을 지원합니다.

엔터프라이즈의 VMware Cloud services 사용자 및 조직에 대해 페더레이션된 ID 액세스를 채택하여 다음을 활성화합니다.

- 엔터프라이즈의 모든 사용자가 회사 계정을 사용하여 VMware Cloud services에 액세스합니다.

- **조직 소유자**가 회사 디렉토리에서 동기화된 그룹에 조직 및 서비스 역할을 할당하여 조직 및 서비스에 대한 인증을 제어할 수 있습니다.
- 보안 팀이 다단계 인증을 포함하여 VMware Cloud services에 대한 엔터프라이즈 수준 보안 및 액세스 정책을 설정하고 적용할 수 있습니다.

페더레이션되지 않은 도메인의 **조직 소유자**는 전체 엔터프라이즈 도메인에 대한 셀프 서비스 페더레이션 워크플로를 시작합니다. 설정을 완료하면 회사 도메인의 모든 사용자가 엔터프라이즈 페더레이션을 사용할 수 있게 되고 엔터프라이즈 페더레이션이 모든 조직의 모든 서비스에 적용됩니다.

주의 엔터프라이즈는 VMware Cloud services 액세스를 위해 페더레이션할 도메인을 소유해야 하며 셀프 서비스 워크플로의 첫 번째 단계에서 소유권을 확인해야 합니다. 서비스 제공자에 속하는 도메인은 페더레이션할 수 없습니다.

셀프 서비스 페더레이션 워크플로를 통한 엔터프라이즈 페더레이션 설정에 대한 자세한 지침은 [VMware Cloud Services](#)와 [엔터프라이즈 페더레이션 설정 가이드](#)를 참조하십시오.

페더레이션된 인증과 페더레이션되지 않은 인증 간의 차이점은 무엇입니까?

회사 도메인이 페더레이션되지 않은 경우 VMware Cloud services에 대한 액세스가 VMware ID 계정을 통해 인증됩니다. VMware Cloud services 사용이 처음이라면 my.vmware.com을 방문하여 VMware ID를 생성합니다.

회사 도메인이 페더레이션된 경우 VMware Cloud services에 대한 액세스가 회사 계정을 통해 인증됩니다. 호스팅된 Workspace ONE Access 테넌트가 ID 브로커로 사용되어 ID 제공자와 페더레이션을 설정합니다. 호스팅된 테넌트는 회사 ID 제공자 및 Active Directory를 통한 검증을 위해 구성됩니다. 회사 Active Directory의 사용자 및 그룹을 동기화하도록 Workspace ONE Access 커넥터를 구성하여 VMware Cloud services에 대한 사용자 및 그룹 액세스를 관리합니다. `username`, `firstname`, `lastname` 및 이메일 주소와 같은 일부 필수 사용자 프로파일 특성만 동기화되도록 구성됩니다. 나중에 특성을 더 추가할 수 있습니다.

참고 사용자 암호는 동기화되지 않으며 캐시되지 않습니다.

회사 도메인에 대한 페더레이션을 실행 취소할 수 있습니까?

페더레이션 설정을 실행 취소하거나 처음 구성한 페더레이션된 회사 도메인에 대해 페더레이션을 실행 취소하기로 결정한 경우 지원 티켓을 제출해야 합니다.

회사 도메인에 대한 엔터프라이즈 페더레이션 설정과 관련된 사항

회사 도메인에 대한 엔터프라이즈 페더레이션 설정은 여러 단계, 사용자 및 역할이 포함된 셀프 서비스 프로세스입니다.

다음은 회사 도메인을 VMware Cloud services와 페더레이션하는 작업에 관여하는 사람과 관련 내용에 대한 설명입니다.

조직 소유자

페더레이션되지 않은 도메인의 **조직 소유자** 사용자는 Cloud Services 콘솔에서 페더레이션 설정을 시작할 수 있습니다. 모든 **조직 소유자**는 셀프 서비스 페더레이션 프로세스를 시작하고 **엔터프라이즈 관리자**를 한 명 이상 할당하여 설정을 완료할 수 있습니다.

해당 엔터프라이즈에 대한 시스템 관리자 역할을 보유하고 있고 엔터프라이즈 디렉토리 서비스 및 ID 제공자 구성에 대한 충분한 지식이 있는 **조직 소유자**는 페더레이션 설정과 관련하여 **엔터프라이즈 관리자** 역할을 수행할 수 있습니다.

엔터프라이즈 관리자

엔터프라이즈 관리자는 엔터프라이즈의 중앙 보안 팀에 속해 있고 디렉토리 서비스와 ID 제공자를 관리하는 시스템 관리자입니다. **엔터프라이즈 관리자**는 회사 도메인에 대해 엔터프라이즈 페더레이션을 설정하도록 지정된 사람으로서 셀프 서비스 설정 프로세스의 구성 및 검증 단계를 완료합니다. 엔터프라이즈 페더레이션을 설정하는 데에는 여러 보안 팀의 담당자가 필요할 수 있습니다. 지정된 **엔터프라이즈 관리자**는 다른 관리자를 초대하여 설정에 도움을 받을 수 있습니다.

엔터프라이즈 페더레이션 조직

조직 소유자가 하나 이상의 **엔터프라이즈 관리자**를 초대하여 회사 도메인에 대한 셀프 서비스 페더레이션 워크플로를 시작하는 경우 해당 설정에서 특수 페더레이션 조직을 사용할 수 있게 됩니다. 셀프 서비스 페더레이션 프로세스에 관련된 모든 사용자는 특수 페더레이션 조직 액세스를 위한 링크가 포함된 이메일 알림을 받습니다. 이 조직의 목적은 회사 도메인에 대한 엔터프라이즈 페더레이션을 설정하고 초기 설정을 수정하는 것입니다.

VMware ID에 회사 계정 연결

계정이 페더레이션된 VMware Cloud services의 기존 사용자는 회사 계정을 VMware ID 계정에 연결해야 조직의 서비스에 액세스할 수 있습니다. 도메인에 대한 페더레이션이 설정이 활성화된 후 VMware Cloud services에 온보딩한 새 사용자는 청구 정보를 보거나 지원 티켓을 제출해야 하는 경우가 아니면 VMware ID를 생성할 필요가 없습니다.

청구 및 지원 목적으로 VMware를 이용하는 VMware Cloud services의 사용자에게는 VMware ID가 있어야 하며 회사 계정을 VMware ID와 연결해야 합니다.

VMware Workspace ONE Access 테넌트

페더레이션된 ID 관리를 설정하려면 고객이 VMware Workspace ONE Access 테넌트를 구성하고 관리해야 합니다. 테넌트는 셀프 서비스 페더레이션 프로세스의 일부로 생성됩니다. Workspace ONE Access 테넌트는 ID 제공자에 대한 ID 브로커(서비스 제공자) 역할을 하며 실제 사용자 인증에는 관여하지 않습니다.

셀프 서비스 페더레이션 설정 워크플로

셀프 서비스 페더레이션 설정에는 서로 다른 **엔터프라이즈 관리자**가 다양한 시간대에 수행할 수 있는 여러 단계가 포함됩니다. 워크플로는 마지막 종료 위치에서 재개됩니다. 설정에 관여하는 **엔터프라이즈 관리자**에게는 VMware ID가 있는 VMware Cloud services 계정이 있어야 합니다. 페더레이션 설정의 모든 단계는 특수 페더레이션 조직의 **엔터프라이즈 페더레이션 설정** 워크플로를 통해 완료됩니다.

내 VMware ID를 연결해야 하는 이유

페더레이션된 계정이 있는 **조직 소유자** 또는 **지원 사용자**인 경우에도 청구 정보 및 고객 지원 액세스를 위해 회사 계정에 연결된 VMware ID가 있어야 합니다.

내 클라우드 서비스가 모두 표시되지 않는 이유

귀하의 VMware ID 계정에서 모든 서비스에 액세스하려면 VMware ID 계정을 페더레이션된 계정에 연결해야 합니다. 토큰이 있는 경우 자동으로 전송됩니다.

내 클라우드 서비스 계정을 연결하는 방법

Cloud Services 콘솔에서 **내 계정 > 프로파일**을 클릭하여 계정을 연결합니다.

VMware ID를 생성할 때 회사 이메일 주소를 사용한 경우 Cloud Services 콘솔 배너에서 **VMware ID 연결** 버튼을 클릭합니다. 계정을 연결하기 전에 배너를 닫은 경우 Cloud Services 콘솔 콘솔에서 **내 계정 > 프로파일**을 클릭하여 나중에 계정을 연결할 수 있습니다.

[프로파일] 페이지에서 연결된 계정의 세부 정보를 볼 수 있습니다.

이 작업이 조직 소유자 및 지원 역할이 있는 사용자에게 미치는 영향

조직 소유자이거나 **지원 사용자** 역할을 보유한 경우에는 청구 정보 및 고객 지원에 계속 액세스할 수 있도록 VMware ID 계정을 연결해야 합니다. 계정을 연결한 후 고객 번호를 받습니다. 앞으로 새 조직을 만들면 조직을 설정할 때 VMware ID 계정을 연결하게 됩니다.

내 고객 번호를 볼 수 있는 위치

조직 소유자 또는 **지원 사용자**는 고객 번호가 필요합니다. 계정을 연결한 후 **사용자/조직 설정** 메뉴에서 귀하의 이름 아래에 고객 번호가 표시됩니다.



[프로파일] 페이지에서 연결된 계정의 기타 세부 정보 및 고객 번호를 볼 수도 있습니다.

내 OAuth 클라이언트 처리 방법

OAuth 클라이언트는 타사 애플리케이션을 VMware Cloud services와 통합하는 데 사용됩니다.

페더레이션된 계정의 사용자 이름이 VMware ID와 동일한 경우(예: example joe@acme.com)에는 VMware ID를 연결하면 VMware ID로 로그인하여 생성한 OAuth 클라이언트가 페더레이션된 계정으로 전송됩니다.

VMware ID의 사용자 이름이 페더레이션된 계정과 같지 않은 경우(예: joe@gmail.com 및 joe@acme.com)에는 페더레이션된 계정으로 클라이언트가 전송되지 않으며 새 클라이언트를 생성해야 합니다.

OAuth 클라이언트 생성에 대한 자세한 내용은 [OAuth 2.0으로 애플리케이션을 인증하는 방법](#)의 내용을 참조하십시오.

회사 ID 제공자를 연결해야 하는 이유

도메인이 페더레이션되면 고급 IGA(ID 거버넌스 및 관리) 기능을 사용하여 비조직 사용자를 VMware Cloud services로 쉽게 온보딩할 수 있습니다.

IGA를 활성화하는 한 가지 방법은 [엔터프라이즈 관리자](#)에게 엔터프라이즈 페더레이션 조직 대시보드에서 변경하도록 요청하는 것이며, 또 다른 방법은 조직을 IdP(ID 제공자)에 연결하는 것입니다. 페더레이션된 도메인의 **조직 소유자**만 조직을 해당 IdP에 연결할 수 있습니다.

- 1 Cloud Services 콘솔에 로그인하고 **조직 > 세부 정보**를 클릭합니다.
- 2 **ID 제공자에 연결된 도메인** 섹션에서 **ID 제공자 연결**을 클릭합니다.
조직과 연결된 IdP 및 도메인이 팝업 창에 표시됩니다.
- 3 **연결**을 클릭한 다음 **계속**을 클릭합니다.

IGA 기능에 대한 자세한 내용은 [ID 거버넌스 및 관리 소개 및 VMware Cloud Services에서 작동하는 방식](#) 항목을 참조하십시오.

ID 거버넌스 및 관리 소개 및 VMware Cloud Services에서 작동하는 방식

IGA(ID 거버넌스 및 관리)는 엔터프라이즈에서 감사 추적 및 인증을 위한 데이터를 얻고 **조직 소유자**인 사용자가 셀프 서비스 액세스 요청, 승인, 위반 및 API 토큰을 실시간으로 관리할 수 있는 서비스입니다.

IGA 서비스에는 두 가지(기본 및 고급) 기능 집합이 포함되어 있습니다. 페더레이션된 도메인이 있는 조직에서만 사용할 수 있습니다.

- 기본 IGA 기능을 사용하려면 **조직 소유자**가 **ID 및 액세스 관리 > 거버넌스** 페이지에서 **시작** 링크를 클릭하여 IGA 서비스를 활성화해야 합니다.
- 고급 IGA 기능 사용을 시작하려면 **내 조직에서 고급 ID 거버넌스 및 관리를 활성화하는 방법** 항목을 참조하십시오.

조직에서 IGA 서비스를 사용하면 VMware Cloud Services 사용자가 다음을 수행할 수 있습니다.

역할	기본 IGA 사용 시	고급 IGA 사용 시
조직 소유자 사용자	<ul style="list-style-type: none"> Cloud Services 콘솔의 ID 및 액세스 관리 > 거버넌스 페이지에서 IGA 대시보드에 액세스합니다. 추가 역할에 대한 셀프 서비스 요청을 제출할 수 있는 조직 멤버의 기능을 활성화하거나 비활성화합니다. 들어오는 조직 서비스 역할 요청을 관리하여 조직의 서비스에 대한 액세스를 제어합니다. 위반을 모니터링하고 위협에 즉시 대응합니다. 	<ul style="list-style-type: none"> 회사 ID 제공자에 연결된 거버넌스가 활성화된 조직에서 서비스를 온보딩합니다.
조직 멤버	<ul style="list-style-type: none"> 조직에서 활성화된 경우 추가 조직 및 서비스 역할에 대한 셀프 서비스 액세스 요청을 제출합니다. 거버넌스가 활성화된 조직에서 역할을 요청하는 방법을 참조하십시오. 	<ul style="list-style-type: none"> 회사 ID 제공자에 연결된 거버넌스가 활성화된 조직에서 자신을 온보딩합니다. 페더레이션된 계정이 있는 사용자로 온보딩하는 방법의 내용을 참조하십시오.

내 조직에서 고급 ID 거버넌스 및 관리를 활성화하는 방법

도메인이 페더레이션된 경우 페더레이션된 도메인의 모든 조직에 대해 추가 고급 IGA(ID 거버넌스 및 관리) 기능을 활성화할 수 있습니다.

조직에서 고급 IGA 기능을 활성화하려면 다음이 필요합니다.

- 페더레이션된 도메인의 **조직 소유자**는 회사 ID 제공자를 VMware Cloud Services에 연결해야 합니다. [회사 ID 제공자를 연결해야 하는 이유](#)의 내용을 참조하십시오.
- 엔터프라이즈 관리자**는 해당 회사 ID 제공자에 연결된 일부 또는 모든 VMware Cloud services 조직에 대해 고급 IGA 기능을 활성화해야 합니다. 자세한 내용은 [페더레이션된 도메인에 대해 고급 IGA 기능 사용](#)을 참조하십시오.

엔터프라이즈 페더레이션에 대한 자세한 내용은 [엔터프라이즈 페더레이션 소개 및 VMware Cloud Services에서 작동하는 방식](#)을 참조하십시오.

고급 IGA 기능이 활성화되면 비조직 멤버는 온보딩 중에 연결된 조직에서 조직 및 서비스 역할 액세스를 요청할 수 있습니다. 이 기능에 대해 자세히 알려면 [페더레이션된 계정이 있는 사용자로 온보딩하는 방법](#)의 내용을 참조하십시오.

추가 역할에 대한 셀프 서비스 요청을 관리하는 방법

IGA(ID 거버넌스 및 관리)가 활성화된 조직의 **조직 소유자**인 사용자는 Cloud Services 콘솔의 **거버넌스 > 요청** 페이지를 통해 조직 및 서비스 역할 요청을 관리합니다.

셀프 서비스 요청을 제출하는 옵션은 조직에서 이 옵션이 활성화된 경우에만 **조직 멤버**인 사용자가 사용할 수 있습니다.

추가 역할 요청이 활성화된 경우 조직 멤버인 사용자가 액세스를 요청하는 방법:	추가 역할 요청이 활성화되지 않은 경우:
Cloud Services 카탈로그의 서비스 타일에서 액세스 요청 링크를 클릭합니다.	서비스 타일의 액세스 요청 링크를 클릭할 수 없습니다.
내 계정 > 내 역할 페이지에서 역할 요청 링크를 클릭합니다.	내 계정 > 내 역할 페이지에 역할 요청 링크가 표시되지 않습니다.

셀프 서비스 요청을 활성화 또는 비활성화하는 방법

조직의 추가 역할에 대한 셀프 서비스 요청을 활성화하거나 비활성화하려면 다음을 수행합니다.

- 1 **거버넌스 > 요청**으로 이동하여 **설정**을 클릭합니다.
- 2 **추가 역할 요청** 슬라이더를 클릭하여 설정을 활성화하거나 비활성화합니다.
- 3 **저장**을 클릭합니다.

보류 중인 요청을 처리하는 방법은 무엇입니까?

조직 및 서비스 역할 액세스에 대한 모든 수신 요청은 **보류 중인 요청** 섹션에 나열됩니다. **과거 요청**을 사용하면 조직에서 생성된 모든 요청에 대한 기간별 데이터를 볼 수 있습니다.

요청을 승인하거나 거부하려면 **보류 중인 요청** 목록에서 하나 이상의 항목을 선택하고 해당하는 버튼을 클릭합니다. 역할 액세스를 요청하는 사용자는 요청이 승인되거나 거부되면 이메일 알림을 받습니다.

액세스 요청을 승인하기 전에 수정할 수 있습니까?

조직 소유자는 **조직 멤버**가 요청한 서비스 역할 액세스에 대한 기간을 수정할 수 있습니다. **요청 ID** 링크를 클릭하여 원래 요청의 기간을 볼 수 있습니다. 요청된 기간을 변경하려면 **승인**을 클릭한 다음 **수정하여 승인**을 선택합니다. 설정을 변경하고 변경을 제출합니다.

참고 **수정하여 승인** 옵션은 서비스 역할 액세스 요청에만 사용할 수 있으며 조직 역할에는 적용되지 않습니다.

조직 소유자는 **조직 멤버**가 원래 요청한 서비스 또는 역할 액세스를 수정할 수 없습니다. 승인하려는 적절한 액세스 수준에 대한 지침을 요청자에 제공하려는 경우 요청을 거부할 때 메시지를 포함할 수 있습니다. 요청자는 이메일 알림을 받고 적절한 조직 및 서비스 역할로 새 액세스 요청을 제출할 수 있습니다.

내 조직에서 정책 위반을 모니터링하는 방법

IGA(ID 거버넌스 및 관리)가 활성화된 조직의 **조직 소유자**인 사용자는 조직에서 사용자 로그인 그리고 OAuth 애플리케이션 및 API 토큰을 사용한 로그인에 대한 액세스 위반을 모니터링합니다. 위반 트리거에 대한 정책을 정의하고 수정합니다.

비활성 API 토큰, 비활성 OAuth 소유자, 광범위한 서비스 범위, OAuth 애플리케이션에 대한 안전하지 않거나 승인되지 않은 URI와 같이 OAuth 애플리케이션과 API 토큰에 대한 다양한 트리거를 활성화하여 IGA가 활성화된 조직의 로그인에 대한 위반 정책을 설정합니다.

참고 소스 도메인 인증 정책이 활성화되면 정책 설정에서 허용하지 않는 도메인에서 시작된 모든 로그인 시도에 대해 사용자 액세스 위반이 캡처됩니다.

절차

- 1 회사 계정으로 Cloud Services 콘솔에 로그인합니다.
- 2 **ID 및 액세스 관리 > 거버넌스 > 위반**으로 이동합니다.
- 3 **설정**을 클릭합니다.
- 4 **위반 설정** 페이지가 열리면 OAuth 애플리케이션 및 API 토큰에 대한 설정을 적절히 수정합니다.
- 5 **저장**을 클릭합니다.

결과

위반 대시보드가 새로 고쳐지며 새 설정에 따라 위반을 표시합니다.

대시보드의 정보는 매일 업데이트됩니다.

내 조직에서 정책 위반에 대해 조치를 취하는 방법

위반을 모니터링하는 IGA(ID 거버넌스 및 관리)가 활성화된 조직의 **조직 소유자**인 사용자는 조직에서 검색된 위반 사항에 대해 조치를 취할 수 있습니다. **ID 및 액세스 관리 > 거버넌스 > 위반**으로 이동하여 위반의 전체 목록에 액세스할 수 있습니다.

조직에서 캡처된 위반은 위반을 트리거한 VMware Cloud Services에 로그인하는 데 사용된 인증 방법의 유형별로 그룹화됩니다. 전체 목록과 위반에 대응하기 위해 수행할 수 있는 가능한 작업을 보려면 해당 탭을 클릭합니다.

- **OAuth 애플리케이션** 탭에는 위반을 트리거한 애플리케이션의 이름, 심각도, 설명 및 OAuth 애플리케이션을 생성한 조직 사용자의 이메일이 표시됩니다.
- **API 토큰** 탭에는 위반을 트리거한 API 토큰의 이름, 심각도, 설명 및 API 토큰을 생성한 조직 사용자의 이메일이 표시됩니다.
- **사용자 액세스** 탭에는 로그인 시도로 인해 위반이 트리거된 조직 사용자의 이메일, 심각도, 위반이 발생한 날짜 및 위반이 발생한 소스 도메인이 표시됩니다. 소스 도메인 인증 정책에서 허용하지 않는 도메인에서 로그인을 시도하면 사용자 액세스 위반이 캡처됩니다. 자세한 내용은 [도메인 수준에서 사용자 액세스를 관리하는 방법](#)의 내용을 참조하십시오.

조직의 위반 사항에 대응하여 취할 수 있는 조치는 다음 표에 설명되어 있습니다.

원하는 작업	절차
위반의 가시성 변경	<p>이 작업은 위반의 가시성 상태를 활성화에서 숨겨짐으로 변경합니다. 위반은 삭제되지 않으며 되돌릴 수 있습니다.</p> <ol style="list-style-type: none"> 1 숨기려는 위반 사항을 찾고 해당하는 이중 화살표(>>)를 클릭하여 세부 정보를 펼칩니다. 2 숨기려는 활성화 위반 옆의 확인란을 선택합니다. 3 숨기기를 클릭합니다. <p>위반이 세부 정보 섹션에 더 이상 표시되지 않습니다.</p>
숨겨진 위반 표시	<p>이 작업은 숨겨짐 상태인 위반을 표시합니다.</p> <ul style="list-style-type: none"> ■ 위반 사항의 세부 정보 섹션을 확장하고 모두 표시 토글을 켭니다. 숨겨진 모든 위반이 표시됩니다.
조직에서 OAuth 애플리케이션을 제거	<p>이 작업은 OAuth 애플리케이션을 제거하고 조직에 액세스하지 못하도록 차단합니다. OAuth 애플리케이션이 삭제되지는 않지만 이 애플리케이션에서 추가 위반이 보고되지 않습니다. 제거 작업은 위반 페이지에서 되돌릴 수 없습니다. 이 OAuth 애플리케이션에서 위반을 모니터링하려면 조직에 다시 추가해야 합니다.</p> <ol style="list-style-type: none"> 1 위반 페이지에서 OAuth 애플리케이션 탭을 엽니다. 2 제거할 애플리케이션을 찾습니다. 3 이름 옆에 있는 확인란을 선택합니다. 4 제거를 클릭합니다.
위반의 심각도 편집	<p>조직의 요구 사항에 따라 위반 기준에 대한 심각도를 정의할 수 있습니다.</p> <ol style="list-style-type: none"> 1 위반 페이지에서 설정을 클릭합니다. 2 심각도 드롭다운 메뉴를 사용하여 수정하려는 각 위반 기준에 대한 설정을 변경합니다. 3 저장을 클릭합니다.

조직에서 API 토큰을 관리하는 방법

IGA(ID 거버넌스 및 관리)가 활성화된 조직의 **조직 소유자**인 사용자는 조직에서 생성된 API 토큰을 모니터링하고 새로 생성된 모든 토큰의 유효 및 최대 TTL(Time to Live)에 대한 제약 조건을 설정합니다.

API 토큰 대시보드에 액세스하려면 Cloud Services 콘솔을 열고 **ID 및 액세스 관리 > 거버넌스 > API 토큰**으로 이동합니다. 대시보드가 열리면 조직의 사용자가 생성한 모든 API 토큰 목록이 제공됩니다.

각 API 토큰에 대해 토큰 이름, API 토큰을 생성한 조직 사용자의 이름, 생성 및 만료 날짜, 토큰이 마지막으로 사용된 날짜, 토큰의 범위(토큰에 할당된 조직 역할)와 같은 세부 정보를 볼 수 있습니다.

조직의 TTL 정책을 위반한 경우 **API 토큰** 대시보드 목록에 경고 아이콘(⚠️)이 표시됩니다. 조직에 대해 설정된 TTL 정책은 조직의 사용자가 생성한 모든 새 API 토큰에 적용됩니다. TTL 정책을 변경하면 새 설정을 위반하는 이전에 생성된 모든 API 토큰 옆에 경고 아이콘이 나타납니다.

활성화, 비활성화 또는 수정할 수 있는 두 가지 TTL 정책 설정이 있습니다.

- **유효 토큰 TTL.**

이 설정은 정책을 위반하기 전에 API 토큰에 대해 허용되는 유효 TTL(Time to Live)을 정의합니다.

■ 최대 토큰 TTL.

이 설정은 조직에서 생성된 모든 API 토큰에 대해 허용되는 최대 TTL(Time to Live)을 정의합니다. 조직 사용자는 최대 토큰 TTL이 이 설정에 정의된 것보다 큰 API 토큰을 생성할 수 없습니다.

API 토큰이 조직의 정책 또는 지침을 위반한 경우 취할 수 있는 조치

API 토큰이 조직의 TTL 정책을 위반하거나 어떤 식으로든 의심스러워 보이는 경우에는 **API 토큰** 대시보드에서 토큰을 비활성화할 수 있습니다. 그러면 조직의 리소스에 액세스하는 데 사용할 수 없습니다.

1 **API 토큰** 대시보드에서 비활성화할 API 토큰을 선택합니다.

2 **비활성화** 링크를 클릭합니다.

API 토큰 상태가 [활성화됨]에서 [비활성화됨]으로 변경됩니다. API 토큰 소유자는 VMware Cloud Services로부터 조직에 액세스하는 데 사용했던 토큰을 **조직 소유자**가 비활성화했다는 이메일 알림을 받습니다.

비활성화된 API 토큰을 다시 활성화하려면 대시보드에서 API 토큰을 선택한 다음 **활성화** 링크를 클릭합니다. API 토큰 소유자는 재활성화를 확인하는 이메일 알림을 받습니다.

조직에서 API 토큰에 대한 TTL 정책을 변경하는 방법

API 토큰 TTL 정책을 수정하려면 다음을 수행합니다.

1 **API 토큰** 대시보드에서 **설정**을 클릭합니다.

원하는 작업	수행할 단계
정책을 활성화하거나 비활성화.	정책 상태 슬라이더를 사용합니다.
TTL 설정 변경	해당 TTL 설정 섹션에 새 값을 입력하고 드롭다운 목록에서 시간 단위를 선택합니다. 시간 단위는 분, 시간 또는 일일 수 있습니다.

2 **저장**을 클릭합니다.

정책에 대한 기존 토큰의 유효성 검사 실행은 24시간에 한 번씩 수행됩니다. 따라서 변경 사항으로 인해 **API 토큰** 대시보드의 위반 목록이 업데이트되려면 다소 시간이 걸릴 수 있습니다.

조직에서 기본 역할을 할당하는 방법

IGA(ID 및 액세스 거버넌스)가 활성화된 조직의 **조직 소유자**인 사용자는 정책을 설정하여 조직의 사용자에게 기본 조직 및 서비스 역할을 할당할 수 있습니다.

해당 정책을 통해 부여된 기본 역할은 지정된 페더레이션된 도메인에서 조직에 로그인하는 모든 사용자에게 적용되며 사용자 수준에서 편집할 수 없습니다. 기본 역할 사용 권한을 변경하려면 정책을 수정해야 합니다.

중요 조직 소유자는 정책에 따라 기본 역할이 부여되고 조직에서 다른 역할이 없는 조직의 사용자를 볼 수 없다는 알려진 문제가 있습니다. 이러한 사용자는 추가 역할을 요청하고 요청이 승인되지 않는 한 Cloud Services 콘솔의 **활성 사용자** 목록에 표시되지 않습니다. 기본 역할이 있는 사용자가 조직에서 추가 역할을 맡으면 **활성 사용자** 목록에 표시되며 **조직 소유자**가 사용자에게 추가 역할을 부여할 수 있습니다.

사전 요구 사항

- 회사 ID 제공자가 VMware Cloud Services에 연결되어 있습니다.
- 조직에서 고급 IGA 기능이 활성화되어 있습니다.
- 조직에서 **조직 소유자** 역할이 있습니다.

절차

- 1 회사 계정으로 Cloud Services 콘솔에 로그인합니다.
- 2 **ID 및 액세스 관리 > 거버넌스 > 요청**으로 이동합니다.
- 3 **설정**을 클릭합니다.
- 4 페이지의 **기본 역할 부여** 섹션에서 **도메인 정책 추가** 링크를 클릭합니다.
- 5 새 정책의 이름과 설명을 입력합니다.
- 6 정책을 적용할 도메인을 선택합니다.
- 7 지정된 도메인에서 조직에 로그인하는 모든 사용자에게 자동으로 할당할 조직 및 서비스 역할을 선택합니다.
- 8 **저장**을 클릭합니다.

결과

지정한 역할은 지정된 도메인의 모든 사용자가 VMware Cloud Services에 로그인하면 사용할 수 있게 됩니다.

OAuth 2.0으로 애플리케이션을 인증하는 방법

VMware Cloud Services 콘솔에서는 애플리케이션에 조직의 보호된 리소스에 대한 위임된 보안 액세스를 제공할 수 있도록 OAuth 2.0을 사용합니다. VMware Cloud Services는 애플리케이션 사용자가 액세스 권한을 부여하는 웹 애플리케이션 액세스 및 액세스 토큰이 애플리케이션에 직접 발행되는 서버 간 상호 작용을 지원합니다.

OAuth 2.0이란?

OAuth 2.0은 애플리케이션에 리소스에 대한 보안 액세스 권한 부여할 수 있는 권한 부여 프로토콜입니다. 클라이언트는 액세스 토큰을 통해 권한이 부여됩니다. 액세스 토큰에는 토큰이 액세스할 수 있는 리소스를 정의하는 범위가 있습니다. OAuth 2.0에 대한 자세한 내용은 <https://tools.ietf.org/html/rfc6749#page-8>에서 OAuth 규격을 참조하거나 <https://aaronparecki.com/oauth-2-simplified/>에서 OAuth 2.0 Simplified라는 블로그를 살펴보십시오.

VMware Cloud Services에서 OAuth 2.0의 작동 방식

VMware Cloud services는 다양한 권한 부여 유형(예: `client credentials`, `authorization code` 및 `authorization code`가 있는 `public client`)을 사용하는 애플리케이션 권한 부여에 대한 여러 사용 사례를 다루고 있습니다. 목표에 따라 각 권한 부여 유형에 해당하는 세 가지 유형의 OAuth 애플리케이션(서버 간 애플리케이션, 웹 애플리케이션 및 네이티브/모바일 애플리케이션) 중 하나를 생성하도록 선택할 수 있습니다.

VMware Cloud on AWS에 액세스할 수 있는 **조직 소유자**라고 가정해보겠습니다. 주식 거래에 도움이 되는 애플리케이션을 개발했습니다. 애플리케이션을 `Trading 1.0`이라고 하겠습니다. vCenter Server를 통해 관리되는 가상 시스템에서 애플리케이션을 실행하려고 하지만 우선 VMware Cloud on AWS API를 통해 애플리케이션에 권한을 부여해야 합니다.

- 1 Cloud Services 콘솔에서 OAuth 2.0 애플리케이션을 생성합니다. 이것은 `Trading 1.0` 애플리케이션을 등록하는 방법으로 생각할 수 있습니다. **조직 > OAuth 애플리케이션** 메뉴에서 **애플리케이션 생성**을 클릭하고 일련의 단계를 진행하여 애플리케이션 생성을 시작합니다. 이 과정의 끝 부분에서, API를 사용하여 클라이언트를 식별하는 데 사용되는 애플리케이션 ID 및 애플리케이션 암호의 형태로 클라이언트 자격 증명을 발행합니다. 이러한 자격 증명을 스크립트에 붙여넣습니다.
- 2 애플리케이션이 조직에서 생성되었지만 액세스 권한이 아직 부여되지 않았습니다. 애플리케이션을 조직에 추가하여 액세스 권한을 부여합니다. 그러면 애플리케이션을 생성할 때 정의한 조직의 서비스와 리소스에 애플리케이션이 액세스할 수 있습니다. 이 단계는 서버 간 애플리케이션 유형의 애플리케이션에만 필요하며 웹 및 네이티브/모바일 애플리케이션에는 적용되지 않습니다.
- 3 `Trading 1.0` 클라이언트 애플리케이션을 실행하면 권한 부여 서버에 액세스 토큰을 요청합니다. 권한이 부여된 경우, 권한 부여 서버가 API에 액세스 토큰을 보내고 클라이언트에 액세스 권한이 부여됩니다.

OAuth 애플리케이션을 생성 및 관리할 수 있는 사람

조직 소유자인 사용자 또는 **개발자** 역할을 가진 **조직 멤버**인 사용자는 OAuth 애플리케이션을 생성하고 관리합니다.

조직에 있는 다른 **조직 소유자**가 생성하거나 추가한 OAuth 애플리케이션을 관리할 수도 있습니다.

애플리케이션 암호를 다시 생성할 수 있습니까?

예, **조직 소유자**는 조직에 있는 OAuth 애플리케이션의 애플리케이션 암호를 다시 생성할 수 있습니다. 이 기능은 OAuth 애플리케이션을 생성한 **조직 소유자**가 더 이상 비즈니스 엔터프라이즈에 근무하지 않는 경우 애플리케이션을 계속 실행하려고 할 때 유용합니다.

OAuth 애플리케이션 대신 API 토큰 인증을 사용할 수 있습니까?

예, API가 인증 프로세스에서 사용자가 인증된 엔티티일 것을 요구하는 경우 API 토큰을 대신 사용해야 합니다. OAuth 애플리케이션과 API 토큰의 사용 시기를 확인하려면 [OAuth 애플리케이션과 API 토큰의 차이점](#)을 참조하십시오.

OAuth 2.0 애플리케이션을 관리하는 방법

조직 소유자인 사용자는 조직에서 OAuth 2.0 애플리케이션의 세부 정보를 생성하고 보고 수정합니다.

다음 작업도 가능합니다.

- 조직에 있는 다른 **조직 소유자**인 사용자가 생성하거나 추가한 OAuth 애플리케이션을 관리합니다.
- **조직 소유자** 역할을 맡고 있는 조직에서 생성된 애플리케이션에 대한 액세스 권한을 부여합니다.

원하는 작업	수행할 단계
조직에 액세스할 수 있는 OAuth 애플리케이션을 확인합니다.	<p>ID 및 액세스 관리 > OAuth 애플리케이션을 클릭합니다.</p> <p>여기에서 조직에 대한 액세스 권한이 있는 다른 조직에서 생성된 애플리케이션을 볼 수 있습니다.</p>
다른 조직에서 생성된 OAuth 애플리케이션을 추가합니다.	<ol style="list-style-type: none"> 1 ID 및 액세스 관리 > OAuth 애플리케이션을 클릭합니다. 2 애플리케이션 추가를 클릭합니다. 3 추가하려는 OAuth 애플리케이션을 식별하려면 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> ■ 애플리케이션 ID 입력 ■ 조직으로 검색 4 계속을 클릭합니다. 5 해당 ID를 사용하여 OAuth 애플리케이션을 식별하도록 선택한 경우 OAuth 애플리케이션 ID를 입력하라는 메시지가 표시됩니다. 6 OAuth 애플리케이션이 생성된 조직을 통해 해당 애플리케이션을 식별하도록 선택한 경우 먼저 드롭다운 메뉴에서 조직 이름을 선택한 다음 해당 조직에서 사용할 수 있는 OAuth 애플리케이션 목록에서 OAuth 애플리케이션을 선택하라는 메시지가 표시됩니다. <p>조직 드롭다운 메뉴에는 조직 소유자 액세스 권한이 있는 조직만 표시됩니다.</p> 7 애플리케이션 세부 정보를 검토하고 추가를 클릭합니다.
조직에 액세스할 수 있는 다른 조직에서 생성된 OAuth 애플리케이션을 제거합니다.	<ol style="list-style-type: none"> 1 ID 및 액세스 관리 > OAuth 애플리케이션을 클릭합니다. 2 표시되는 OAuth 애플리케이션 목록에서 조직에 액세스하지 못하게 하려는 애플리케이션을 선택합니다. 3 제거를 클릭합니다.

원하는 작업	수행할 단계
조직에서 생성된 애플리케이션을 봅니다.	<p>조직 > OAuth 애플리케이션을 클릭합니다.</p> <p>그러면 조직에서 생성된 모든 애플리케이션을 볼 수 있습니다.</p> <ul style="list-style-type: none"> ■ 애플리케이션 수정. 애플리케이션의 범위 지정을 변경하는 경우 변경 내용이 다른 조직에 있는 애플리케이션의 인스턴스에 포함되지 않습니다. 범위 지정을 업데이트하려면 조직 소유자인 사용자가 해당 조직에서 애플리케이션을 제거하고 다시 추가하거나, 업데이트된 범위 지정을 반영하도록 애플리케이션을 편집해야 합니다. ■ 조직에서 애플리케이션 제거. ■ 조직에서 생성되었지만 조직에 대한 액세스가 아직 부여되지 않은 애플리케이션 추가. ■ 애플리케이션 생성.
조직에서 새 OAuth 애플리케이션을 생성합니다.	<ol style="list-style-type: none"> 1 조직 > OAuth 애플리케이션을 클릭합니다. 2 추가할 애플리케이션 유형을 선택합니다. <ul style="list-style-type: none"> ■ 서버 대 서버 애플리케이션은 서버 대 서버 애플리케이션에 OAuth 2.0을 사용하는 방법 항목을 참조하십시오. ■ 웹 애플리케이션의 경우 웹 애플리케이션에 OAuth 2.0을 사용하는 방법 항목을 참조하십시오. ■ 네이티브/모바일 애플리케이션의 경우 네이티브 및 모바일 애플리케이션에 OAuth 2.0을 사용하는 방법 항목을 참조하십시오.
조직에서 생성된 OAuth 애플리케이션을 관리합니다.	<p>조직 > OAuth 애플리케이션을 클릭하고 관리할 애플리케이션을 선택합니다.</p> <ul style="list-style-type: none"> ■ OAuth 애플리케이션을 수정하려면 편집을 클릭합니다. <p>참고 애플리케이션의 범위 지정을 변경하는 경우 변경 내용이 다른 조직에 있는 애플리케이션의 인스턴스에 포함되지 않습니다. 범위 지정을 업데이트하려면 조직 소유자인 사용자가 해당 조직에서 애플리케이션을 제거하고 다시 추가하거나, 업데이트된 범위 지정을 반영하도록 애플리케이션을 편집해야 합니다.</p> ■ 애플리케이션을 제거하려면 삭제를 클릭합니다. <p>참고 이 작업은 되돌릴 수 없습니다. 이러한 클라이언트 자격 증명을 사용하는 모든 애플리케이션은 더 이상 보호된 리소스에 액세스할 수 없으며 자격 증명이 무효화됩니다.</p> ■ 조직에서 생성되었지만 아직 조직에 대한 액세스 권한이 부여되지 않은 서버 대 서버 애플리케이션을 추가하려면 조직에 추가를 클릭합니다.

서버 대 서버 애플리케이션에 OAuth 2.0을 사용하는 방법

애플리케이션이 사용자 권한 부여 없이 다른 서버에 직접 액세스해야 하는 경우에는 `Server to server app`을 생성합니다. 이 옵션은 `OAuth 2.0 client credentials` 권한 부여 유형에 기반합니다. 이 흐름에서 애플리케이션은 OAuth 자격 증명을 사용하여 액세스 토큰을 검색합니다.

범위 지정은 서버 대 서버 애플리케이션에서 특히 중요합니다. 범위는 클라이언트가 액세스할 수 있는 조직의 영역, 특히 조직 내 역할 및 서비스 그리고 권한 수준을 제어할 수 있도록 구현하는 방법을 제공합니다. **조직 소유자**인 사용자는 원하는 조직에 서버 대 서버 애플리케이션을 추가할 수 있습니다. 따라서 많은 클라우드 서비스에서 애플리케이션에 대한 광범위한 액세스 권한을 지정할 수 있지만, 결국 액세스 권한은 조직에 포함된 서비스에 의해 결정됩니다. 애플리케이션 범위에 포함된 서비스를 포함하지 않는 조직에 OAuth 애플리케이션을 추가하면 알림을 받게 됩니다.

사전 요구 사항

- 이 조직에서 OAuth 애플리케이션을 추가하고 관리하는 데 필요한 사용 권한이 있습니다. [VMware Cloud Services에서 사용할 수 있는 조직 역할](#)의 내용을 참조하십시오.

절차

- 1 Cloud Services 콘솔에 로그인합니다.
- 2 **조직 > OAuth 애플리케이션**을 클릭한 다음 **새 OAuth 애플리케이션 생성**을 클릭합니다.
- 3 **서버 대 서버 애플리케이션**을 선택합니다.
- 4 이름과 설명을 입력하여 클라이언트를 등록합니다.
- 5 새 OAuth 애플리케이션에 대한 **액세스 토큰 TTL** 값을 설정합니다.
액세스 토큰 TTL(Time to Live)은 토큰이 유효한 기간을 정의합니다.
 - 기본 액세스 토큰 TTL 시간은 30분입니다.
 - 설정할 수 있는 최대 액세스 토큰 TTL 시간은 300분(5시간)입니다.
 - 설정할 수 있는 최소 액세스 토큰 TTL 시간은 1분입니다.
- 6 범위를 정의합니다.
범위는 클라이언트가 액세스할 수 있는 조직의 영역, 특히 조직 내 역할 및 서비스 그리고 권한 수준을 제어할 수 있도록 구현하는 방법을 제공합니다.
- 7 **생성**을 클릭하여 클라이언트 자격 증명을 생성합니다.
- 8 **OAuth 애플리케이션 생성됨** 팝업 창에서 자격 증명을 복사하거나 JSON 파일을 다운로드하고 **계속**을 클릭합니다.
자격 증명을 안전한 장소에 저장하는 것은 사용자의 책임입니다.
- 9 (선택 사항) 애플리케이션을 활성 조직에 추가합니다.
이 단계를 건너뛰고 나중에 이 조직 및 다른 조직에 애플리케이션을 추가할 수 있습니다. [OAuth 2.0 애플리케이션을 관리하는 방법](#)의 내용을 참조하십시오.

다음에 수행할 작업

자격 증명을 스크립트에 붙여넣습니다.

웹 애플리케이션에 OAuth 2.0을 사용하는 방법

애플리케이션이 서버에서 실행되고 사용자 권한 부여가 필요한 일반 웹 애플리케이션이면 web app을 생성합니다. 이 옵션은 OAuth 2.0 authorization code 권한 부여 유형에 기반합니다. 이 흐름에서는 애플리케이션이 리소스에 액세스하기 전에 사용자가 애플리케이션에 권한을 부여하고, 애플리케이션이 액세스 토큰과 새로 고침 토큰(선택적으로)을 검색합니다.

사전 요구 사항

- 이 조직에서 OAuth 애플리케이션을 추가하고 관리하는 데 필요한 사용 권한이 있습니다. VMware Cloud Services에서 사용할 수 있는 조직 역할의 내용을 참조하십시오.

절차

- 1 Cloud Services 콘솔에 로그인합니다.
- 2 **조직 > OAuth 애플리케이션**을 클릭한 다음 **새 OAuth 애플리케이션 생성**을 클릭합니다.
- 3 **웹 애플리케이션**을 선택하고 **계속**을 클릭합니다.
- 4 애플리케이션 세부 정보를 입력하여 애플리케이션을 등록합니다.
 - a 새 OAuth 애플리케이션의 이름과 설명을 입력합니다.
 - b 리디렉션 URI를 하나 이상 입력합니다.

사용자가 클라이언트에 권한을 부여한 후, 권한 부여 서버는 사용자를 클라이언트에서 액세스 토큰으로 지정한 URI로 다시 리디렉션합니다. URI를 둘 이상 추가하는 것이 가장 좋습니다. http://acme.com 형식을 사용하십시오.
 - c 액세스 토큰에 대한 시간 범위를 지정합니다.

기본 액세스 토큰 TTL(Time to Live) 설정은 30분입니다. 설정할 수 있는 최대값은 300분(5시간)입니다. 설정할 수 있는 최소값은 1분입니다.
 - d 액세스 토큰이 요청에 지속적으로 권한을 부여하도록 하려면 **새로 고침 토큰 발행**을 선택하고 **새로 고침 토큰 TTL** 값을 설정합니다.

기본 새로 고침 토큰 TTL은 30분입니다. 설정할 수 있는 최대값은 300분(5시간)입니다. 설정할 수 있는 최소값은 1분입니다.
- 5 범위를 정의합니다.

범위는 클라이언트가 액세스할 수 있는 조직의 영역, 특히 서비스 종류와 권한 수준을 제어할 수 있도록 구현하는 방법을 제공합니다.
- 6 **Open ID** 확인란을 선택하여 애플리케이션을 인증하는 사용자에게 대한 정보를 가져옵니다.
- 7 **생성**을 클릭하여 클라이언트 자격 증명을 생성합니다.
- 8 자격 증명을 복사하거나 자격 증명을 포함하는 JSON 파일을 다운로드합니다. 자격 증명을 안전한 장소에 저장하는 것은 사용자의 책임입니다.

9 계속을 클릭합니다.

다음에 수행할 작업

자격 증명을 스크립트에 붙여넣습니다.

네이티브 및 모바일 애플리케이션에 OAuth 2.0을 사용하는 방법

네이티브 및 모바일 애플리케이션과 같은 공용 클라이언트는 클라이언트 암호의 기밀성을 유지할 수 없습니다. 네이티브 및 모바일 애플리케이션에 OAuth 2.0을 사용하면 애플리케이션 ID를 생성하고 PKCE(코드 교환용 공용 키)를 사용하여 추가적인 인증을 제공합니다.

PKCE는 클라이언트 암호를 사용하지 않는 공용 클라이언트를 보호하는 기술입니다. 모바일 애플리케이션에서 PKCE를 사용하는 방법에 대한 자세한 내용은 이 [블로그](#)를 참조하십시오.

사전 요구 사항

- 이 조직에서 OAuth 애플리케이션을 추가하고 관리하는 데 필요한 사용 권한이 있습니다. [VMware Cloud Services에서 사용할 수 있는 조직 역할](#)의 내용을 참조하십시오.

절차

- 1 사용자 이름을 클릭하고 **조직 보기 > OAuth 애플리케이션**을 선택한 다음, **새 OAuth 애플리케이션 생성**을 클릭합니다.
- 2 **네이티브/모바일 애플리케이션**을 선택하고 **계속**을 클릭합니다.
- 3 애플리케이션 세부 정보를 입력하여 애플리케이션을 등록합니다.
 - a 새 OAuth 애플리케이션의 이름과 설명을 입력합니다.
 - b 리디렉션 URI를 하나 이상 입력합니다.

사용자가 클라이언트에 권한을 부여한 후, 권한 부여 서버는 사용자를 클라이언트에서 액세스 토큰으로 지정한 URI로 다시 리디렉션합니다. URI를 둘 이상 추가하는 것이 가장 좋습니다. http://acme.com 형식을 사용하십시오.
 - c 액세스 토큰에 대한 시간 범위를 지정합니다.

기본 액세스 토큰 TTL(Time to Live) 설정은 30분입니다. 설정할 수 있는 최대값은 300분(5시간)입니다. 설정할 수 있는 최소값은 1분입니다.
 - d 액세스 토큰이 요청에 지속적으로 권한을 부여하도록 하려면 **새로 고침 토큰 발행**을 선택하고 **새로 고침 토큰 TTL** 값을 설정합니다.

기본 새로 고침 토큰 TTL은 30분입니다. 설정할 수 있는 최대값은 300분(5시간)입니다. 설정할 수 있는 최소값은 1분입니다.
- 4 범위를 정의합니다.

범위는 클라이언트가 액세스할 수 있는 조직의 영역, 특히 서비스 종류와 권한 수준을 제어할 수 있도록 구현하는 방법을 제공합니다.

- 5 **Open ID** 확인란을 선택하여 애플리케이션을 인증하는 사용자에게 대한 정보를 가져옵니다.
- 6 **생성**을 클릭하여 클라이언트 자격 증명을 생성합니다.
- 7 애플리케이션 ID를 복사하거나 애플리케이션 ID가 포함된 JSON 파일을 다운로드합니다. 자격 증명을 안전한 장소에 저장하는 것은 사용자의 책임입니다.
- 8 **계속**을 클릭합니다.

다음에 수행할 작업

자격 증명을 스크립트에 붙여넣습니다.

OAuth 애플리케이션과 API 토큰의 차이점

VMware Cloud Services API와의 상호 작용에는 OAuth 애플리케이션과 API 토큰이 모두 사용됩니다.

API 토큰은 조직의 사용자가 발행하며 사용자의 계정과 API 토큰을 생성한 조직과 연결됩니다. 조직의 사용자가 생성한 OAuth 애플리케이션은 서버 대 서버 상호 작용에서 엔티티로 작동하며 여러 조직에서 사용될 수 있습니다. API 토큰은 토큰을 생성한 사용자만 관리할 수 있습니다. OAuth 애플리케이션의 소유자는 애플리케이션을 생성한 조직이며, **개발자** 역할이 있는 **조직 소유자** 또는 **조직 멤버**인 사용자가 관리할 수 있습니다.

OAuth 애플리케이션과 API 토큰을 모두 사용하여 VMware Cloud Services API와 상호 작용하는 프로세스를 자동화할 수 있습니다. 차이점은 API 토큰은 사용자 계정을 액세스 토큰에 통합하지만 OAuth 애플리케이션은 사용자 계정 없이 인증을 수행한다는 것입니다. API 토큰 또는 OAuth 애플리케이션을 사용하여 API 호출을 수행하도록 선택하는 경우 상호 작용에 관련된 API 서비스의 특정 요구 사항을 고려해야 합니다. 일부 API는 사용자 계정이 인증된 엔티티여야 하지만 다른 API는 그렇지 않습니다. 예를 들어 API를 호출하여 조직에 대한 청구 및 구독 정보를 VMware Cloud Services로 가져오는 경우 서버 대 서버 유형의 OAuth 애플리케이션을 사용하거나 API 토큰을 사용하여 API 서비스를 호출할 수 있습니다. 사용자 자격 증명을 통한 인증이 필요하지 않고 클라이언트 자격 증명도 수락하기 때문입니다. 조직의 사용자가 API를 사용하여 암호를 업데이트하는 경우 API를 사용하면 사용자가 인증 엔티티로 작동해야 합니다.

중요 VMware Cloud Services에 대한 자동화된 호출을 위해 서버 대 서버 유형의 OAuth 애플리케이션을 사용하려면 먼저 관련 API 설명서를 참조해야 합니다.

VMware Cloud Services의 감사 이벤트 로그 작동 방식

VMware Aria Operations for Logs의 연결된 인스턴스를 사용하여 사용자 로그인, 사용자 관리, API 토큰, OAuth 애플리케이션, 청구 등의 작업으로 조직 사용자가 트리거한 이벤트를 모니터링할 수 있습니다.

VMware Aria Operations for Logs는 VMware Cloud Services로서, 사용하려면 유료 또는 평가판 구독이 필요합니다. 다양한 구독 옵션에 대한 자세한 내용은 [VMware Aria Operations for Logs\(SaaS\) 구독 및 청구](#)를 참조하십시오.

VMware Aria Operations for Logs 서비스를 사용하여 로그 필터링, 아카이브 및 전달과 같은 다양한 감사 기능을 얻을 수 있습니다. Cloud Services 콘솔에서 VMware Aria Operations for Logs 서비스를 시작하여 조직에 대한 감사 데이터에 액세스합니다. 이러한 방법으로 조직의 이벤트에 대한 시각적 개요를 볼 수 있는 **VMware Cloud Services 감사 이벤트** 대시보드를 엽니다. 대시보드가 기본적으로 활성화되어 있지 않은 경우 대시보드를 보려면 **대시보드** 페이지의 **컨텐츠 팩 대시보드** 탭에서 대시보드를 선택합니다.

VMware Aria Operations for Logs 사용에 대한 자세한 내용은 [VMware Aria Operations for Logs\(SaaS\) 사용을 참조하십시오](#).

참고 조직에 VMware Aria Operations for Logs 서비스 구독이 없고 현재 또는 과거 기간에 대한 VMware Cloud services 로그 이벤트를 계속 보려는 경우 해결 방법으로 [장 12 지원을 받는 방법](#)하여 감사 보고서를 얻습니다. 지원 요청 생성 시점으로부터 48시간 내에 지정된 기간에 대한 암호화된 CSV 파일 형식의 보고서를 이메일로 받습니다.

VMware Aria Operations for Logs의 감사 데이터를 볼 수 있는 사람

VMware Aria Operations for Logs 사용자 또는 VMware Aria Operations for Logs 관리자 서비스 역할이 있는 조직의 모든 사용자는 연결된 VMware Aria Operations for Logs 서비스 인스턴스에서 조직의 모든 감사 데이터에 액세스할 수 있습니다.

VMware Cloud Services에서 캡처되는 감사 이벤트

이벤트 로그는 이벤트 이름, 이벤트를 트리거한 사용자, 이벤트의 시간 및 위치와 같은 사용자 작업에 대한 정보를 제공합니다. **조직 소유자**인 사용자는 VMware Aria Operations for Logs의 연결된 인스턴스를 사용하여 조직에 대한 감사 이벤트를 검토합니다.

VMware Cloud services는 액세스 및 계정 관리, 청구 및 구독을 통해 Cloud Services 콘솔의 사용자 활동에 대한 다양한 감사 이벤트를 캡처합니다. 자동화를 사용하여 조직의 일부 리소스를 관리하는 경우 일부 이벤트가 사용자 대신 호출자에 의해 트리거될 수 있습니다.

VMware Cloud Services 감사 이벤트 검색 및 필터링

VMware Cloud Services **감사 이벤트** 컨텐츠 팩에서 저장된 쿼리를 사용하거나 사용자 지정 쿼리를 생성하여 조직에 대한 로그 이벤트를 검색하고 필터링할 수 있습니다.

vRealize Log Insight Cloud 인스턴스의 **컨텐츠 팩** 메뉴에서 컨텐츠 팩에 액세스합니다. 자세한 내용은 [컨텐츠 팩 사용](#)을 참조하십시오.

VMware Cloud Services 감사 이벤트에 대한 사용자 지정 쿼리를 사용하여 vRealize Log Insight Cloud 서비스의 **로그 탐색** 페이지에서 로그 이벤트를 검색하고 필터링할 수 있습니다. VMware Cloud Services에 대한 감사 이벤트만 보려면 검색 조건으로 **log_type**, **포함**을 차례로 선택하고 **csp-audit**을 입력합니다. 특정 이벤트를 검색하려면 이벤트 유형이 포함된 쿼리를 생성합니다.

VMware Cloud Services 감사 이벤트

표 10-1. 계정 관리

감사 이벤트 이름	이벤트 유형	설명
UserLogin	csp__user_login	사용자가 로그인했습니다.
UserLogout	csp__user_logout	사용자가 로그아웃했습니다.
GenerateApiToken	csp__generate_api_token	사용자가 개인 API 토큰을 생성했습니다.
RevokeApiToken	csp__revoke_api_token	사용자가 개인 API 토큰을 해지했습니다.
RevokeAllApiTokens	csp__revoke_all_api_tokens	사용자가 모든 개인 API 토큰을 해지했습니다.
RefreshTokenExchangeFailed	csp__refresh_token_exchange_failed	사용자가 API 토큰 새로 고침으로 액세스 토큰을 생성하지 못했습니다.
FirstLogin	csp__first_login	처음 로그인할 때 초대를 통해 사용자에게 역할이 할당되었습니다.
LinkAccount	csp__link_account	사용자가 회사의 페더레이션된 계정을 자신의 VMware ID 계정에 연결했습니다. 이 작업을 통해 사용자는 회사 자격 증명을 사용하여 VMware Cloud Services에 로그인할 수 있습니다.
UnlinkAccount	csp__unlink_account	사용자가 자신의 VMware ID에 연결된 계정을 변경했습니다.
CreateOrgOAuthApp	csp__create_org_o_auth_app	호출자가 조직에서 OAuth 애플리케이션을 생성했습니다.
UpdateOrgOAuthApp	csp__update_org_o_auth_app	호출자가 조직에서 OAuth 애플리케이션을 업데이트했습니다.
DeleteOrgOAuthApp	csp__delete_org_o_auth_app	호출자가 조직에서 OAuth 애플리케이션을 삭제했습니다.
OrgOAuthAppNewSecretRotation	csp__org_o_auth_app_new_secret_rotation	호출자가 조직에서 OAuth 애플리케이션의 암호를 변경했습니다.
ActivateMfa	csp__activate_mfa	VMware ID가 있는 사용자가 MFA 디바이스를 활성화했습니다.
DeactivateMfa	csp__deactivate_mfa	VMware ID가 있는 사용자가 MFA 디바이스를 비활성화했습니다.
TurnOnMfa	csp__turn_on_mfa	VMware ID가 있는 사용자가 자신의 계정에 대해 다단계 인증을 설정했습니다.
TurnOffMfa	csp__turn_off_mfa	VMware ID가 있는 사용자가 자신의 계정에 대해 다단계 인증을 해제했습니다.
RegenerateMfaRecoveryCodes	csp__regenerate_mfa_recovery_codes	VMware ID가 있는 사용자가 다단계 인증을 위해 새 복구 코드 집합을 재생성했습니다.

표 10-1. 계정 관리 (계속)

감사 이벤트 이름	이벤트 유형	설명
UpdateMfaAttributes	csp__update_mfa_attributes	VMware ID가 있는 사용자가 자신의 계정에 대한 MFA 설정을 업데이트했습니다.
GenerateNewMfaActivationSecret	csp__generate_new_mfa_activation_secret	VMware ID가 있는 사용자가 자신의 계정에 대해 MFA를 설정하기 위해 새로운 활성화 암호를 생성했습니다.
InvitationSentAck	csp__invitation_sent_act	사용자에게 초대를 보낼 때 내부 알림이 생성되었습니다.
CreateMspInvitation	csp__create_msp_invitation	새 서비스 제공자에게 새 제공자 조직 온보딩을 위한 이메일 초대를 보냈습니다.
UpdateMspInvitation	csp__update_msp_invitation	새 서비스 제공자에게 새 제공자 조직 온보딩을 위한 업데이트된 이메일 초대를 보냈습니다.
DeleteMspInvitation	csp__delete_msp_invitation	새 서비스 제공자에게 보낸 새 제공자 조직 온보딩을 위한 이메일 초대가 취소되었습니다.

표 10-2. 조직 관리

감사 이벤트 이름	이벤트 유형	설명
CreateOrganization	csp__create_org	사용자가 새 조직을 생성했습니다.
UpdateOrganization	csp__update_org	사용자가 기존 조직을 업데이트했습니다.
DeleteOrganization	csp__delete_org	사용자가 기존 조직을 삭제했습니다.
InviteExistingUserToOrganization	csp__invite_existing_user_to_org	기존 사용자가 조직에 추가되었습니다.
RemoveUserFromOrganization	csp__remove_user_from_org	기존 사용자가 조직에서 제거되었습니다.
UpdateUserRolesOnOrganization	csp__update_user_roles_on_org	기존 사용자의 역할이 업데이트되었습니다.
InviteNonExistingUserToOrganization	csp__invite_non_existing_user_to_org	새 사용자에게 이메일 초대를 보냈습니다.
RevokeUserInvitations	csp__revoke_user_invitations	사용자에게 이메일로 보낸 초대가 취소되었습니다.
RemoveClientFromOrganization	csp__remove_client_from_org	사용자가 조직에 할당된 OAuth 애플리케이션을 제거했습니다. 이 작업으로 OAuth 애플리케이션은 삭제되지 않았습니다.
AssignRolesToClientOnOrganization	csp__assign_roles_to_client_on_org	호출자가 조직의 클라이언트에 서비스/조직 역할을 할당했습니다. 이 작업은 이전에 역할이 할당되지 않았던 클라이언트에 처음으로 역할이 할당되었음을 나타냅니다.

표 10-2. 조직 관리 (계속)

감사 이벤트 이름	이벤트 유형	설명
UpdateClientRolesOnOrganization	csp__update_client_roles_on_org	호출자가 조직의 클라이언트에 대한 서비스/조직 역할을 업데이트했습니다.
UpdateUserDefaultOrganization	csp__update_user_default_org	사용자가 계정에 대해 표시된 기본 조직을 업데이트했습니다. 이 작업은 둘 이상의 조직에 속한 사용자에게만 적용됩니다.

표 10-3. 그룹

감사 이벤트 이름	이벤트 유형	설명
RemoveGroupFromOrganization	csp__remove_group_from_org	사용자가 조직에서 기존 그룹을 제거했습니다.
AssignRolesToGroupOnOrganization	csp__assign_roles_to_group_on_org	사용자가 조직에서 새로 생성된 그룹에 조직 및 서비스 역할을 할당했습니다.
UpdateGroupRolesOnOrganization	csp__update_group_roles_on_org	사용자가 조직의 기존 그룹에 대한 역할 할당을 업데이트했습니다.
CustomGroupAddClients	csp__custom_group_add_clients	사용자가 조직의 사용자 지정 그룹에 새 멤버를 추가했습니다.
CustomGroupRemoveClients	csp__custom_group_remove_clients	사용자가 조직의 사용자 지정 그룹에서 기존 멤버를 제거했습니다.

표 10-4. 청구 및 구독

감사 이벤트 이름	이벤트 유형	설명
CreateSubscription	csp__create_subscription	사용자가 새 서비스 또는 기존 서비스에 대한 구독을 생성했습니다.
AddOrgPaymentMethod	csp__add_org_payment_method	사용자가 자신의 조직에 새 지불 방법을 추가했습니다.
RemoveOrgPaymentMethod	csp__remove_org_payment_method	사용자가 자신의 조직에서 지불 방법을 제거했습니다.
UpdateOrgDefaultPaymentMethod	csp__update_org_default_payment_method	사용자가 조직의 기본 지불 방법을 업데이트했습니다.
AddDetailsToOrg	csp__add_details_to_org	사용자가 회사 주소 및/또는 기타 청구 및 구독 세부 정보를 조직에 추가했습니다.
UpdateOrgAddress	csp__update_org_address	사용자가 자신의 조직에 대한 청구 및 구독 세부 정보에서 회사 주소를 업데이트했습니다.
UpdateOrgCommerceData	csp__update_org_commerce_data	사용자가 자신의 조직에 대한 청구 및 구독 세부 정보(통화, 연간 청구 날짜 등)를 업데이트했습니다.
UpdateOrgTaxId	csp__updated_org_tax_id	사용자가 자신의 조직에 대한 청구 및 구독 세부 정보에서 세금 ID를 업데이트했습니다.

표 10-4. 청구 및 구독 (계속)

감사 이벤트 이름	이벤트 유형	설명
UpdateOrgPoReferenceNumber	csp__update_org_po_reference_number	사용자가 새 조직 PO 참조 번호를 설정했습니다.
IncomingOrder	csp__incoming_order	호출자가 서비스 구독에 대한 주문을 생성했습니다.

표 10-5. ID 거버넌스 및 관리

감사 이벤트 이름	이벤트 유형	설명
ApproveDenyEntitlementRequest	csp__iga_entitlements_requests_approval	조직 소유자가 자격 요청을 승인 또는 거부했습니다.
CreateEntitlementRequest	csp__iga_register_entitlements_request	사용자가 자격 요청을 생성했습니다.
CreateEntitlementRequestForNonOrgMember	csp__iga_register_entitlements_request_non_org_member	새 비조직 사용자가 자격 요청을 생성했습니다.
CancelEntitlementRequest	csp__iga_delete_entitlement_request	사용자가 자격 요청을 취소했습니다.
CancelEntitlementRequestForNonOrg	csp__iga_delete_entitlement_request_non_org_member	새 비조직 사용자가 동일 사용자가 이미 제출한 자격 요청을 취소했습니다.
EnablingGovernance	csp__iga_status_change	조직에 대해 ID 거버넌스 및 관리가 활성화되었습니다.
UpdateGovernancePolicies	csp__iga_update_governance_policies_request	사용자가 ID 거버넌스 및 관리 정책을 업데이트했습니다.

VMware Cloud Services에서 NIST 로그인 전 알림을 생성하는 방법

NIST 800-53 AC-8 감사 요구 사항을 충족하려면 조직에 액세스하는 조직 멤버인 사용자에게 로그인 전 알림을 표시할 수 있어야 합니다.

NIST 알림은 사용자가 속한 조직에 관계없이 사용자가 VMware Cloud Services에 로그인하는 도메인에 적용됩니다. 사용자가 NIST 알림이 생성된 도메인에서 조직에 로그인할 때 암호 입력 페이지로 이동하기 전에 알림 조건을 읽고 수락할지 묻는 대화상자가 표시됩니다.

조직 소유자는 [VMware Customer Connect](#)에서 지원 요청을 열어서 사용자 지정 NIST 800-53 AC-8 알림 메시지를 요청합니다. 지원 요청에는 다음 정보를 포함합니다.

- NIST 알림을 적용하려는 엔터프라이즈 도메인
- NIST 알림 대화상자에 표시할 텍스트
- 필요한 모든 언어로 지역화된 텍스트 버전
- VMware Cloud Services 조직의 이름

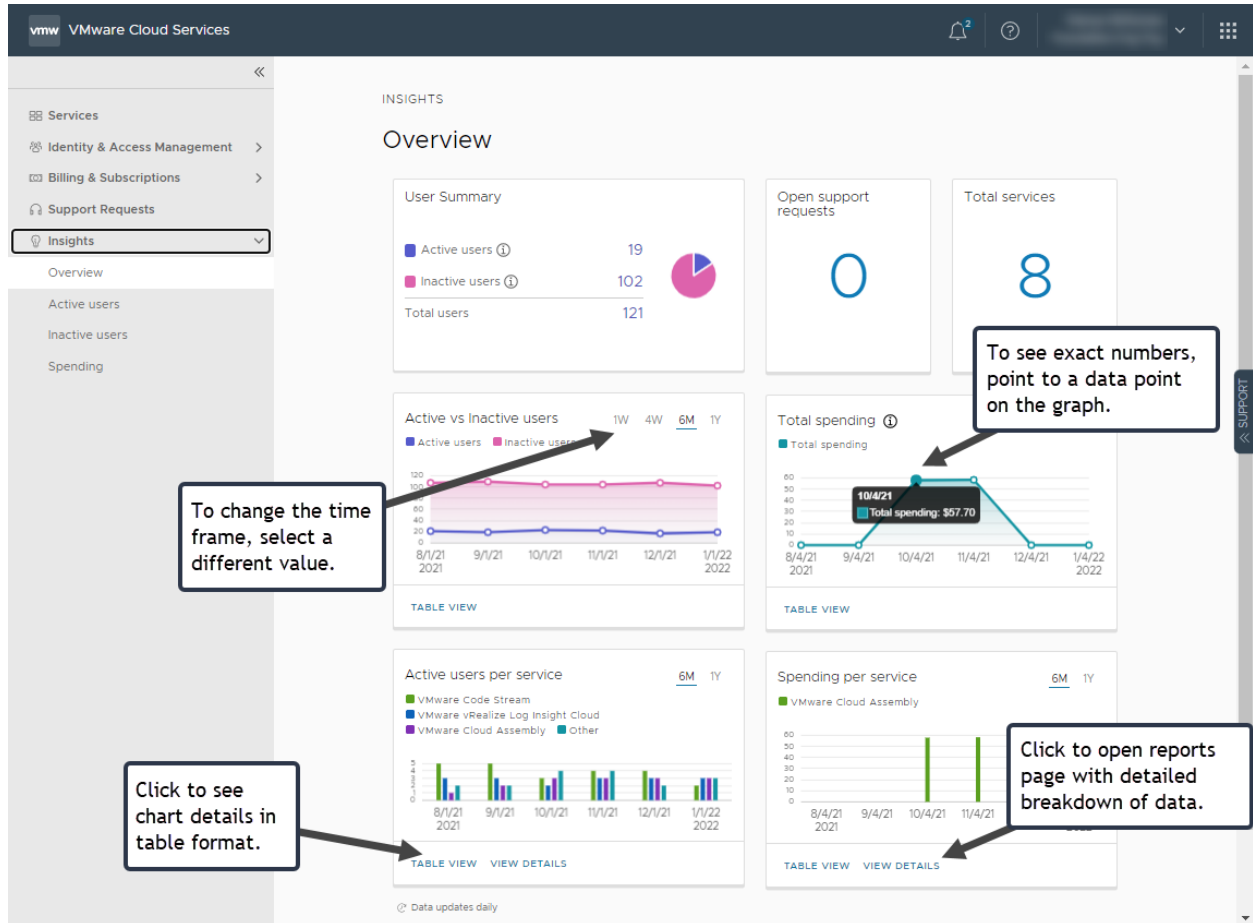
NIST 알림은 **조직 소유자** 상태 및 도메인이 확인된 후 VMware 기술 지원에서 수동으로 구현됩니다.

데이터 인사이트 대시보드를 사용하는 방법

조직 소유자인 사용자는 Cloud Services 콘솔의 **인사이트** 대시보드를 통해 조직의 서비스가 시간에 따라 어떻게 사용되는지 볼 수 있습니다.

인사이트 대시보드에 액세스하려면 **인사이트 > 개요**를 선택합니다.

인사이트 대시보드에는 미리 정의된 기간 동안 조직 사용자의 작업 수준에 대한 시각적 스냅샷이 표시됩니다. 조직의 총 활성 사용자 수와 비활성 사용자 수, 서비스당 활성 및 비활성 사용자 수, 모든 서비스에 대한 총 지출 및 서비스당 지출에 대한 분석 정보를 가져옵니다.





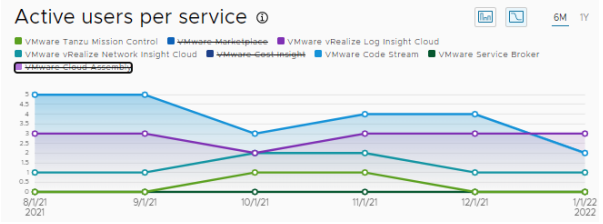
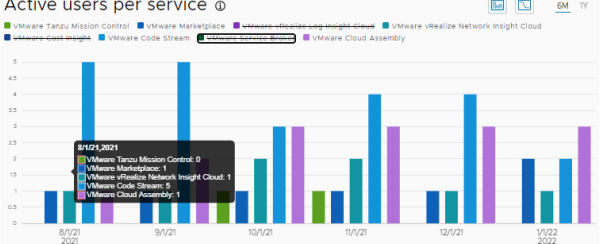
인사이트 대시보드의 데이터는 매일 업데이트됩니다.

데이터 인사이트 대시보드에서 수행할 수 있는 기타 작업

조직 소유자인 사용자는 **활성 사용자**, **비활성 사용자** 및 **지출** 대시보드에 액세스하여 서비스, 사용량 및 비용 데이터에 대한 세부적인 분석을 얻을 수 있습니다. 데이터를 필터링하여 각 탭에 표시되는 정보의 하위 집합을 볼 수 있습니다.

활성 사용자 대시보드

활성 사용자 대시보드에는 조직의 모든 서비스당 활성 사용자에 대한 정보가 표시됩니다. 활성 사용자는 60일 동안 VMware Cloud services에 한 번 이상 로그인한 사용자입니다.

원하는 작업	수행할 단계
데이터의 그래프 보기와 차트 보기 간 전환	대시보드의 오른쪽 상단에서 그래프() 또는 차트() 아이콘을 클릭합니다.
데이터 보고서의 기간 변경	대시보드의 오른쪽 상단에 있는 해당 아이콘을 클릭하여 다른 기간을 선택합니다. 6개월과 1년 중에서 선택할 수 있습니다.
특정 서비스당 활성 사용자 필터링	보기에서 제외할 서비스의 이름을 클릭합니다.  <p>Active users per service</p> <p>VMware Tanzu Mission Control, VMware Marketplace, VMware vRealize Log Insight Cloud, VMware vRealize Network Insight Cloud, VMware Cost Insight, VMware Code Stream, VMware Service Broker</p> <p>9/2/21, 9/9/21, 10/7/21, 11/4/21, 12/2/21, 12/30/21, 1/1/22</p>
특정 월의 서비스당 활성 사용자 분석 보기	차트 또는 그래프에서 데이터 지점을 가리킵니다.  <p>Active users per service</p> <p>VMware Tanzu Mission Control, VMware Marketplace, VMware vRealize Log Insight Cloud, VMware vRealize Network Insight Cloud, VMware Cost Insight, VMware Code Stream, VMware Cloud Assembly</p> <p>8/2/21, 8/9/21, 8/16/21, 8/23/21, 8/30/21, 9/6/21, 9/13/21, 9/20/21, 9/27/21, 10/4/21, 10/11/21, 10/18/21, 10/25/21, 11/1/21, 11/8/21, 11/15/21, 11/22/21, 11/29/21, 12/6/21, 12/13/21, 12/20/21, 12/27/21, 1/3/22, 1/10/22, 1/17/22, 1/24/22, 1/31/22</p>
테이블 보기에서 차트 세부 정보 보기	테이블 보기에 세부 정보 표시 링크를 클릭합니다.
활성 사용자 세부 정보 보기	데이터 차트 아래의 테이블은 조직의 모든 활성 사용자에 대한 세부 정보(예: 이름, 이메일 및 마지막 로그인 이후 일 수)를 제공합니다. 앞뒤 아이콘을 클릭하여 테이블의 페이지를 스크롤합니다.

비활성 사용자 대시보드

비활성 사용자 대시보드에는 조직의 모든 서비스당 비활성 사용자에 대한 정보가 표시됩니다. 비활성 사용자는 60일이 지나도록 VMware Cloud services에 로그인하지 않은 사용자입니다.

원하는 작업	수행할 단계
데이터의 그래프 보기와 차트 보기 간 전환	대시보드의 오른쪽 상단에서 그래프() 또는 차트() 아이콘을 클릭합니다.
데이터 보고서의 기간 변경	대시보드의 오른쪽 상단에 있는 해당 아이콘을 클릭하여 다른 기간을 선택합니다. 6개월과 1년 중에서 선택할 수 있습니다.

원하는 작업	수행할 단계
서비스당 비활성 사용자 필터링	보기에서 제외할 서비스의 이름을 클릭합니다.
특정 월의 서비스당 비활성 사용자 분석 보기	차트 또는 그래프에서 데이터 지점을 가리킵니다.
테이블 보기에서 차트 세부 정보 보기	테이블 보기에 세부 정보 표시 링크를 클릭합니다.
비활성 사용자 세부 정보 보기	데이터 차트 아래의 테이블은 조직의 비활성 사용자에 대한 세부 정보(예: 이름, 이메일, 마지막 로그인 이후 일 수 및 마지막 작업 날짜)를 제공합니다. 앞뒤 아이콘을 클릭하여 테이블의 페이지를 스크롤합니다.
조직에서 비활성 사용자 제거	사용자 이름 옆의 확인란을 선택하고 조직에서 제거 를 클릭합니다.

서비스당 지출 대시보드

이 대시보드에는 일정 기간 동안 조직의 서비스당 월별 지출이 표시됩니다. 비용 값은 조직의 기본 통화로 표시됩니다.

원하는 작업	수행할 단계
데이터의 그래프 보기와 차트 보기 간 전환	대시보드의 오른쪽 상단에서 그래프() 또는 차트() 아이콘을 클릭합니다.
데이터 보고서의 기간 변경	대시보드의 오른쪽 상단에 있는 해당 아이콘을 클릭하여 다른 기간을 선택합니다. 6개월과 1년 중에서 선택할 수 있습니다.
지출이 표시되는 서비스 필터링	보기에서 제외할 서비스의 이름을 클릭합니다.
특정 월의 서비스에 대한 비용 분석 보기	차트 또는 그래프에서 데이터 지점을 가리킵니다.
테이블 보기에서 차트 세부 정보 보기	테이블 보기에 세부 정보 표시 링크를 클릭합니다.

Cloud Services 콘솔에서 프로젝트 작업과 관련된 사항

VMware Cloud Services는 조직의 리소스를 별개의 버킷으로 그룹화하고 각 버킷의 리소스에 대한 사용자 및 그룹 액세스를 할당하는 방법으로 프로젝트를 사용합니다. 이를 통해 **조직 소유자**는 클라우드 서비스 리소스의 사용량을 논리적으로 구성, 매핑 및 추적할 수 있습니다.

VMware Cloud Services의 리소스를 생각할 때 특정 서비스의 미리 정의되고 측정 가능한 논리적 세그먼트라고 가정합니다. 프로젝트에서 서비스 리소스를 구성하면 **조직 소유자**인 사용자가 부서 또는 비용 센터 전체에서 엔터프라이즈의 클라우드 서비스 사용량을 측정하고 추적할 수 있습니다.

중요 Cloud Services 콘솔의 프로젝트 기능을 사용하기 위해 지금까지 몇 가지 VMware Cloud services만 사용하도록 설정되었습니다. 사용 중인 서비스가 리소스 그룹화에 프로젝트를 활용할 수 있는지 알아보려면 해당 서비스에 대한 설명서를 참조하거나 VMware 지원에 문의하십시오.

조직에 프로젝트 1과 프로젝트 2라는 두 개의 프로젝트와 서비스 A, 서비스 B 및 서비스 C라는 세 개의 서비스가 있다고 가정해 보겠습니다.

- 서비스 A와 B는 프로젝트 1에 대해 사용하도록 설정되었습니다.
- 서비스 B와 C는 프로젝트 2에 대해 사용하도록 설정되었습니다.

사용하도록 설정된 서비스의 리소스 그룹화를 사용하면 서비스 B의 리소스를 두 프로젝트 모두에서 사용할 수 있지만, 서비스 A 및 서비스 C의 리소스는 각각 하나의 프로젝트에서 사용할 수 있습니다.

Cloud Services 콘솔에서 프로젝트를 생성하는 방법

프로젝트를 설정하고 관리하려면 조직에서 **조직 소유자** 또는 **프로젝트 관리자** 역할이 있어야 합니다. 새 프로젝트는 Cloud Services 콘솔의 **ID 및 액세스 관리 > 프로젝트**에서 설정합니다.

새 프로젝트를 설정하는 데는 세 가지 단계가 있습니다.

- 1 새 프로젝트의 이름을 정의합니다.

새 프로젝트는 프로젝트와 함께 사용하려는 서비스가 사용되도록 설정될 때까지 비어 있는 상태로 유지됩니다.

- 2 프로젝트에 사용되도록 설정된 서비스 및 리소스를 살펴봅니다.

서비스가 **사용하도록 설정된 서비스** 섹션에 나열되어 있고 리소스가 **리소스** 테이블에 나열되어 있다면 된 경우 서비스가 프로젝트에 대해 사용되도록 설정된 것입니다.

- 3 새 프로젝트에 대한 사용자 및/또는 그룹 액세스 권한을 할당합니다.

내 조직에서 프로젝트를 삭제하는 방법

다음 두 조건이 충족되는 경우에만 프로젝트를 삭제할 수 있습니다.

- 프로젝트에 연결된 서비스 및 리소스가 사용하도록 설정되어 있지 않습니다.
- 사용자 및/또는 그룹에 프로젝트에 대해 할당된 액세스 권한이 없습니다.

조직 소유자 역할이 있는 VMware Cloud Services 사용자는 청구 및 구독 세부 정보를 보고 조직의 지불 방법을 관리할 수 있습니다. 추가적인 **청구 읽기 전용** 역할이 있는 **조직 멤버인** 사용자는 지불 방법을 관리하는 옵션 없이 조직의 청구 및 구독 세부 정보를 볼 수 있습니다.

VMware Cloud Services의 각 조직은 청구 계정과 연결됩니다.

VMware Cloud services는 주문형으로 사용하거나 1년 또는 3년의 구독 기간을 구매하여 사용할 수 있습니다. 구매 주문에는 구독 약정의 용량, 기간 시작 및 종료 날짜, 협상 가격이 요약됩니다. VMware Cloud Services는 구매 주문에 제시된 조건에 따라 청구합니다.

VMware를 통해 구매한 조직의 서비스로 인해 발생한 모든 비용에 대해 하나의 월별 송장 또는 활동 명세서를 받게 됩니다.

조직이 여러 판매자로부터 서비스를 구매한 경우 **청구 및 구독** 페이지에 모든 판매자에 대한 정보가 표시됩니다. 하지만 VMware 이외의 판매자를 통해 구매한 서비스에서 발생한 비용 및 서비스 요금 정보는 Cloud Services 콘솔에서 확인할 수 없습니다. 이 정보를 얻으려면 판매자에게 문의하십시오.

다음으로 아래 항목을 읽으십시오.

- VMware Cloud Services 청구 및 구독 시작
- 내 조직의 지불 방법을 관리하는 방법
- VMware Cloud Services 구독 및 약정을 사용하는 방법
- [사용량 관리] 대시보드를 사용하는 방법
- 명세서 및 송장을 보는 방법

VMware Cloud Services 청구 및 구독 시작

VMware Cloud Services 구독을 처음으로 구매하면 VMware Cloud Services 온보딩 워크플로를 여는 링크가 포함된 이메일을 받게 됩니다.

처음 사용자와 **조직 소유자**는 조직을 설정할 때 주소 및 기본 지불 방법을 제공합니다. VMware Cloud Services는 온보딩 중에 설정된 청구 세부 정보를 기반으로 각 조직에 청구합니다.

- 엔터프라이즈의 **주소**는 조직에서 사용할 수 있는 판매 단위, 통화 옵션, 과세 및 지불 방법을 결정합니다.

예를 들어 미국 주소는 미국 달러로 청구되고 판매세가 부과되며 영국 주소는 영국 파운드르 청구되고 VAT가 부과됩니다. 또한 유럽 연합에 등록된 각 조직은 세금 ID 입력 옵션이 있습니다.

- 조직의 **지불 시 사용할 통화**는 비즈니스 주소가 있는 국가에서 파생된 판매 단위에 의해 결정됩니다. 각 조직에는 조직의 주소를 기반으로 기본 통화 및 사전 승인된 예외 통화가 있을 수 있습니다. 다른 판매 단위는 하나 이상의 통화와 연결될 수 있습니다. 자세한 내용은 [지불 통화가 결정되는 방식](#)에서 참조하십시오.
- **기본 지불 방법**은 VMware 선불 펀드, 신용 카드 또는 PBI(송장으로 지불)일 수 있습니다. 온보딩 시 조직에서 사용할 수 있는 기본 지불 방법은 청구 계정에 따라 달라집니다.

예를 들어 일부 사용자는 PBI만 지불 방법으로 선택할 수 있으며 기타 사용자는 VMware 펀드 및 신용 카드를 선택할 수 있습니다.

사전 요구 사항

- VMware Cloud Services의 새 조직에서 유료 클라우드 서비스를 온보딩하고 있습니다.

절차

- 1 서비스 온보딩 워크플로의 **조직 생성** 단계에서 조직에 대한 청구 세부 정보를 제공합니다.
 - a 조직의 이름을 입력합니다.
 - b 엔터프라이즈 주소를 제공합니다.

중요 이 단계에서 제공하는 사업장 주소는 주소 유효성 검사를 통과하고 유효성 검사 규칙을 준수해야 합니다. 자세한 내용은 [주소 유효성 검사에 대해 알아두어야 할 사항](#)에서 참조하십시오.

- c 여러 통화 옵션을 사용할 수 있는 경우 조직에 청구되는 통화를 선택합니다.
- d 기본 지불 방법을 선택합니다.

참고 조직에 서비스가 온보딩되면 **조직 소유자**인 사용자는 언제든지 송장을 처리하는 데 사용되는 **조직의 기본 지불 방법을 변경하는 방법**할 수 있습니다. 조직에 청구되는 통화는 Cloud Services 콘솔에서 변경할 수 없습니다. 다른 통화로 전환하려면 지원 티켓을 제출해야 합니다.

- 2 **완료**를 클릭합니다.

결과

이제 조직 청구 계정이 생성되었습니다. 이제 Cloud Services 콘솔의 **청구 및 구독** 메뉴에서 청구 정보를 얻고 지불 방법 및 서비스 구독을 관리할 수 있습니다.

주소 유효성 검사에 대해 알아두어야 할 사항

VMware Cloud Services는 조직에 제공된 사업장 주소에 유효성 검사 기준을 적용합니다.

조직 소유자는 서비스 온보딩 중에 조직을 설정할 때 또는 기존 조직에 새 서비스 또는 구독을 추가할 때 사업장 주소를 입력합니다. 유효성 검사를 통과하려면 조직의 주소에 도로 주소, 우편 번호, 구/군/시, 시/도(해당하는 경우) 및 국가에 대한 정확한 정보가 포함되어야 합니다. 유효성 검사는 다음과 같은 경우 자동으로 수행됩니다.

- 서비스/구독 온보딩 중에 사업장 주소를 입력하거나 업데이트합니다.

- **조직 > 세부 정보** 페이지에서 사업장 주소를 업데이트합니다.

다음 표에는 유효성 검사의 가능한 결과와 필요한 경우 수행할 수 있는 작업에 대한 세부 정보가 제공됩니다.

조건...	결과...
조직 주소 유효성 검사에 성공했습니다.	서비스/구독 온보딩 워크플로의 다음 단계로 진행합니다.
조직 주소가 유효성 검사 규칙을 준수하지 않습니다. 규칙을 준수하는 주소가 제안됩니다.	<p>주소 편집 또는 선택 팝업 창이 열리고 원래 주소와 유효성 검사 규칙을 준수하는 제안된 주소가 표시됩니다.</p> <ul style="list-style-type: none"> ■ 제안된 주소를 선택하면 워크플로의 다음 단계로 진행합니다. ■ 원래 주소를 유지하기로 결정한 경우 해당 주소가 유효성 검사 규칙을 준수하지 않음을 인정하고 규칙을 준수하도록 주소에 필요한 모든 변경을 수행할 수 있는 권한을 VMware에 부여하는 데 동의해야 합니다. 이렇게 하려면 주소 편집 또는 선택 팝업 창에서 해당 확인란을 선택합니다. ■ 조직에 제공된 원래 주소를 수정하려면 주소 편집 버튼을 클릭합니다. 그러면 필요한 사항을 변경할 수 있는 [조직 프로필] 페이지로 돌아갑니다.
조직 주소의 유효성을 검사할 수 없습니다. 규칙을 준수하는 주소는 제안되지 않습니다.	<p>주소 유효성 검사가 실패하고 대체 주소가 제안되지 않으면 팝업 창이 열리고 다음 중 하나를 수행하도록 요청합니다.</p> <ul style="list-style-type: none"> ■ 주소를 편집합니다. ■ 해당 확인란을 선택하여 유효성 검사 규칙을 준수하도록 주소에 필요한 모든 변경을 수행할 수 있는 권한을 VMware에 부여하는 데 동의합니다. 동의를 수락한 후에만 서비스/구독 온보딩을 진행할 수 있습니다.
조직 소유자가 동의한 후 VMware에서 조직 주소가 업데이트됩니다.	<p>VMware Cloud Services에서 조직 소유자로 로그인하면 업데이트된 주소를 보여주는 팝업 창이 열립니다.</p> <ul style="list-style-type: none"> ■ 유효성이 검사된 새 주소를 수락하면 기존 조직 주소가 대체됩니다. 모든 조직 소유자 사용자는 변경에 대한 애플리케이션 내 알림을 받게 됩니다. ■ 유효성이 검사된 새 주소를 무시하면 온보딩 서비스/구독 워크플로를 열 때마다 유효성 검사 규칙을 준수하도록 주소를 변경하라는 메시지가 표시됩니다.

VMware Cloud Services에서 청구 및 구독 페이지를 사용하는 방법

Cloud Services 콘솔의 **청구 및 구독** 섹션에는 조직의 활동을 확인하고 서비스 및 구독에 사용되는 지불 방법을 관리하는 데 도움이 되는 기본 페이지가 포함되어 있습니다.

개요	<p>개요 페이지는 조직의 모든 서비스에 대해 지난 달에 발생한 현재 비용과 청구 금액을 표시합니다. 여러 판매자를 통해 구독을 구매한 경우 이 페이지에서 각 판매자에 대한 세부 정보에 액세스할 수 있습니다.</p> <p>자세한 내용은 조직에 대한 청구 정보를 가져오는 방법에서 참조하십시오.</p>
지불 방법 관리	<p>지불 방법 관리 페이지에서는 조직에 새 지불 방법을 추가하고 기본 지불 방법을 변경할 수 있습니다.</p> <p>자세한 내용은 내 조직의 지불 방법을 관리하는 방법에서 참조하십시오.</p>

<p>구독</p>	<p>구독 페이지에는 조직에서 구매한 모든 VMware Cloud Services 구독에 대한 세부 정보가 표시됩니다.</p> <p>자세한 내용은 VMware Cloud Services 구독 및 약정을 사용하는 방법에서 참조하십시오.</p>
<p>프로모션 크레딧</p>	<p>프로모션 크레딧 페이지에는 조직의 월별 비용에 적용하고 사용할 수 있는 프로모션 크레딧이 표시됩니다.</p> <p>자세한 내용은 프로모션 크레딧으로 지불하는 방법에서 참조하십시오.</p>
<p>송장 및 청구서</p>	<p>송장 및 청구서 페이지에서는 조직의 활동 명세서 및 송장을 보고 다운로드할 수 있습니다.</p> <p>자세한 내용은 명세서 및 송장을 보는 방법에서 참조하십시오.</p>

조직에 대한 청구 정보를 가져오는 방법

조직의 청구 정보는 Cloud Services 콘솔의 **청구 및 구독** 메뉴 아래에 있는 **개요** 페이지에서 볼 수 있습니다.

추가적인 **청구 읽기 전용** 역할 사용 권한이 있는 **조직 소유자**인 사용자 또는 **조직 멤버**인 사용자는 VMware에서 구매한 모든 서비스에 대해 다음과 같은 청구 정보를 볼 수 있습니다.

- VMware에서 구매한 모든 서비스에 대한 현재 청구 기간의 누적 비용 및 요금
- 현재 비용에 적용된 프로모션 크레딧
- VMware에서 구매한 모든 서비스에 대한 지난 청구 기간의 지불 및 미결제 잔액
- 모든 월별 서비스에 대한 모든 구매, 요금, 할인 등의 세부 계정

참고 판매자를 통해 구매한 서비스에 대한 청구 정보를 보려면 판매자의 청구 콘솔에 액세스해야 합니다. 자세한 내용은 [판매자 정보를 보는 방법](#)에서 참조하십시오.

현재 비용

현재 비용 섹션에는 VMware에서 구매한 서비스의 비용이 반영됩니다. 예를 들어, CPU당 사설 클라우드의 시간 별 사용량이 있습니다. 이러한 비용은 누적 비용이며, 현재 청구 기간의 처음부터 사용자가 이를 보는 날짜까지(당일 포함) 서비스의 사용량을 반영합니다. 누적 비용은 조직 내 서비스의 주문형 사용량만 반영하며 약정 비용은 포함하지 않습니다. 이 정보는 매일 새로 고쳐집니다.

현재 비용 섹션에는 VMware 할인 프로그램을 통해 받은 할인과 프로모션 크레딧에 대한 정보도 제공됩니다.

마지막 청구 기간

마지막 청구서 섹션에서 이전 청구 기간 동안 누적된 항목별 요금을 볼 수 있습니다. 청구 기간은 조직에서 첫 번째 서비스가 설정된 날짜에 따라 결정되고 한 달 간 지속됩니다. 예를 들어 **조직 소유자**가 15일에 조직의 첫 번째 서비스를 온보딩한 경우 조직 내 모든 서비스의 청구 기간은 이달 15일에서 다음 달 14일까지입니다.

마지막 청구서 섹션에서는 지난 청구 기간 동안 누적된 주문형 서비스와 약정 서비스에 대한 요금의 요약을 제공합니다. 지난 청구 기간에 대한 자세한 사용 명세서 파일을 보고 다운로드하고 인쇄하려면 **마지막 청구서** 섹션의 맨 아래에 있는 **청구서 보기(PDF)** 링크를 클릭합니다.

마지막 15개의 사용 명세서, 요청 시 송장 및 연 단위 약정 송장을 보고 인쇄하려면 **모든 청구서** 링크를 클릭합니다. 자세한 내용은 **명세서 및 송장을 보는 방법**의 내용을 참조하십시오.

클라우드 서비스가 특정 항목에 대한 현재 사용 비용을 청구 기간의 시작 날짜와는 다른 날짜에 계산하는 경우가 있을 수 있습니다. 이 경우 사용량이 청구서에 표시되는 시기와 사용량이 발생하는 시기 사이에 시간 차이가 있을 수 있습니다. 클라우드 서비스가 현재 비용을 예상하는 방법에 대한 자세한 내용은 **내 현재 비용이 계산되는 방식**을 참조하십시오.

내 현재 비용이 계산되는 방식

청구 개요의 **현재 비용** 섹션에는 언제든지 조직의 서비스에 대한 비용이 반영됩니다. 이 섹션에 표시되는 비용은 VMware에서 구매한 서비스에만 해당하는 비용입니다. 이는 누적 비용이며 정의된 기간의 처음부터 서비스에 대한 사용량이 반영됩니다. 정의된 기간은 청구 기간과 다를 수 있습니다.

클라우드 서비스에서 현재 비용이 계산되는 방식과 비용이 청구 주기에 어떤 영향을 미치는지 보려면 다음 표를 참조하십시오.

VMware Cloud Services	현재 비용이 계산되는 방식
VMware Cloud on AWS	<p>VMware Cloud on AWS에 대한 호스트 사용량은 청구 주기에 맞춰 추적됩니다. 청구서에 표시되는 호스트 사용량은 청구 기간 중 전체 호스트 사용량입니다.</p> <p>데이터 전송, IP 주소 사용 및 다시 매핑, EBS 사용을 비롯한 다른 유형의 사용량은 매월 5일에 전송되며 지난 달 마지막 날까지의 사용량이 포함됩니다. 이러한 유형의 사용량은 사용량이 발생한 시기와 이것이 청구서에 표시되는 시기 사이에 시간 차이가 있습니다. 시간 차이가 얼마나 될지는 해당 월의 5일과 비교하여 청구 주기가 언제 시작되는지에 따라 달라집니다.</p> <p>자세한 내용은 VMC 청구 정보를 참조하십시오.</p>

지불 통화가 결정되는 방식

VMware Cloud services에서는 신용 카드, 펀드 및 프로모션 크레딧을 사용하여 다양한 통화로 서비스에 대한 비용을 지불할 수 있습니다. 지불 통화는 조직 설정 중에 옵션 목록에서 선택됩니다.

조직을 설정할 때 입력하는 사업장 주소에 따라 온보딩 워크플로의 **조직 및 지불** 단계에 표시되는 통화 옵션이 결정됩니다. 조직은 기본 통화로 지불하거나, 사전 승인된 예외 통화로 지불하거나, **Global USD** 옵션이 선택된 경우 USD로 지불할 수 있습니다. 서비스 온보딩에 대한 자세한 내용은 [VMware Cloud Services 시작 가이드](#)를 참조하십시오.

지불 통화를 조직에 이미 정의된 옵션에서 다른 옵션으로 변경해야 하는 경우 언제든지 변경할 수 있습니다. **내 조직의 지불 통화를 변경하는 방법**의 내용을 참조하십시오.

VMware Cloud services는 미국 고객용 판매 단위 및 미국 외 지역 고객용 판매 단위라는 두 가지 판매 단위를 지원합니다. 미국 고객에게는 미국 달러로만 비용이 청구되고 미국 외 판매 단위에 속하는 국가에서는 다양한 통화로 비용이 청구됩니다. 이것이 미치는 영향은 무엇일까요?

- 조직의 주소에 따라 세금 유형(예: 판매세 또는 VAT)도 결정됩니다. 지방세의 관리를 용이하게 하기 위해 납세 ID가 사용됩니다. 세금 면제 또는 이와 유사한 지위가 있는 경우 납세 ID를 입력하는 것이 좋습니다. 납세 ID는 조직을 설정할 때 입력할 수 있습니다. 나중에 조직 페이지에서 사용자 이름을 클릭하고 **조직 보기**를 선택하여 입력할 수도 있습니다.
- 신용카드를 사용하여 서비스에 대한 비용을 지불할 경우 청구 주소에는 제한이 없습니다. 조직의 지불 통화가 카드 통화와 다른 경우 신용카드 제공사에 의해 해외 거래 비용이 발생할 수 있습니다.
- 조직의 주소를 변경하려는 경우 새 주소의 위치는 원래 주소와 판매 단위가 동일해야 합니다. 또한 원래 주소와는 다른 통화가 사용되는 국가의 거주지로 주소를 변경할 수 없습니다. 자세한 내용을 보려면 아래 표를 참조하십시오.

다른 판매 단위 또는 다른 통화를 사용하는 국가에 있는 주소로 변경해야 하는 경우 지원 요청을 제출합니다.

지불 통화를 조직에 대해 설정된 통화에서 다른 통화로 변경해야 하는 경우 지원 티켓을 생성해야 합니다. 방법을 알아보려면 [장 12 지원을 받는 방법](#)의 내용을 참조하십시오.

- 펀드의 통화가 조직의 통화와 동일하고 동일한 판매 단위에 속하는 경우에는 해당 펀드를 조직의 지불 방법으로 사용할 수 있습니다. 펀드로 지불하려면 청구 계정 통화가 펀드 통화와 일치해야 하며 펀드 통화가 구독 주문 통화와 일치해야 합니다.

VMware Cloud Services 판매 단위

다음 표의 정보를 사용하여 서비스에 대한 비용이 청구되는 통화를 확인하십시오.

표 11-1. 미국 외 지역 고객용 판매 단위 국제환

조직의 주소가 다음 국가에 해당되는 경우...	기본 지불 통화
아프가니스탄, 알제리, 미국령 사모아, 앙골라, 앵귤라, 남극 대륙, 안티가 바부다, 아르헨티나, 아르메니아, 아루바, 아제르바이잔, 바하마, 바레인, 방글라데시, 바베이도스, 벨로루시, 벨리즈, 베냉, 버뮤다, 부탄, 볼리비아, 보네르, 신트위스타티우스 및 사바, 보츠와나, 부베섬, 브라질, 영국령 인도양 지역, 브루나이, 부르키나 파소, 부룬디, 캄보디아, 카메룬, 캐나다, 케이프 베르데, 케이맨 제도, 중앙 아프리카 공화국, 차드, 칠레, 콜롬비아, 코모로, 콩고, 쿡 제도, 코스타리카, 코트디부아르, 쿠바, 쿠라사오, 지부티, 도미니카, 도미니카 공화국, 동티모르, 에콰도르, 이집트, 엘살바도르, 적도 기니, 에리트레아, 에스토니아, 에티오피아, 포클랜드 제도, 페로 제도, 피지, 핀란드, 프랑스령 기아나, 프랑스령 폴리네시아, 프랑스어 남부 지방, 가봉, 감비아, 조지아, 가나, 그레나다, 과들루프, 괌, 과테말라, 기니, 기니비사우, 가이아나, 아이티, 허드 섬 및 맥도널드 제도, 온두라스, 홍콩, 인도, 인도네시아, 이란, 이라크, 이스라엘, 자메이카, 요르단, 카자흐스탄, 케냐, 키리바시, 대한민국, 쿠웨이트, 키르기스스탄, 라오스, 레바논, 레소토, 라이베리아, 리비아, 마카오, 마다가스카르, 말라위, 말레이시아, 몰디브, 말리, 마셜 제도, 마르티니크, 모리타니, 모리셔스, 마요트, 멕시코, 마이크로네시아, 몰도바, 몬트세랫, 모로코, 모잠비크, 미얀마, 나미비아, 나우루, 네팔, 네덜란드령 앤티리스, 뉴칼레도니아, 뉴질랜드, 니카라과, 니제르, 나이지리아, 니우에 섬, 북한, 북마리아나 제도, 오만, 파키스탄, 팔라우, 팔레스타인 자치구역, 파나마, 파푸아 뉴기니, 파라과이, 페루, 필리핀, 피지, 푸에르토리코, 카타르, 리유니언, 러시아, 르완다, 생바르텔레미, 세인트 헬레나, 세인트 키츠 네비스, 세인트루시아, 세인트 마틴, 생피에르 미클롱, 세인트빈센트그레나딘, 사모아, 상투메 프린시페, 사우디아라비아, 세네갈, 세이셸, 시에라 리온, 싱가포르, 솔로몬 제도, 소말리아, 남아프리카공화국, 사우스 조지아 및 사우스 샌드위치 군도, 남부 수단, 스리랑카, 수단, 수리남, 스발바르 및 얀마옌, 스와질란드, 시리아, 대만, 타지키스탄, 탄자니아, 태국, 동티모르, 토고, 토켈라우, 통가, 트리니다드 토바고, 튀니지, 터키, 투르크메니스탄, 터크스 케이커스 제도, 투발루, 우간다, 우크라이나, 아랍 에미리트, 미국령 해외 제도, 우루과이, 우즈베키스탄, 바누아투, 베네수엘라, 베트남, 버진 아일랜드, 왈리스 및 푸투나, 서사하라, 예멘,	USD
알바니아, 안도라, 오스트리아, 벨기에, 보스니아 헤르체고비나, 불가리아, 크로아티아, 키프로스, 체코 공화국, 덴마크, 프랑스, 독일, 그리스, 그린란드, 헝가리, 아이슬란드, 아일랜드, 이탈리아, 라트비아, 리히텐슈타인, 리투아니아, 룩셈부르크, 마케도니아, 몰타, 모나코, 몬테네그로, 노르웨이, 폴란드, 포르투갈, 루마니아, 산마리노, 세르비아, 슬로바키아, 슬로베니아, 스페인, 스웨덴, 스위스, 네덜란드, 바티칸 시국, 유고슬라비아, 잠비아, 짐바브웨, 올란드 제도	EUR
지브롤터, 건지 섬, 맨섬, 저지, 영국	GBP
일본	JPY
중국, 몽골	CNY
오스트레일리아, 크리스마스 섬, 코코스(킬링) 제도, 노퍽 섬	AUD

표 11-2. 미국 고객용 판매 단위 US

조직의 주소가 다음 국가에 해당되는 경우	청구되는 통화
United States of America	USD

내 조직의 지불 통화를 변경하는 방법

지불 통화는 조직을 설정할 때 서비스 온보딩 워크플로의 일부로 결정됩니다. 조직을 설정하는 조직 소유자인 사용자가 기본 통화 또는 사전 승인된 예외 통화를 선택했습니다.

조직 지불 통화는 다음 중 하나일 수 있습니다.

- 사업장 주소를 기반으로 하는 기본 통화.
- Global USD.

■ 사전 승인된 다른 통화.

사전 요구 사항

조직의 지불 통화를 변경하려면 VMware Customer Connect에서 지원 티켓을 생성해야 합니다. 조직 소유자는 Cloud Services 콘솔을 통해 언제든지 변경을 시작할 수 있습니다.

.

절차

- 1 Cloud Services 콘솔에 로그인하고 **청구 및 구독 > 지불 방법 관리**를 선택합니다.
- 2 **통화 변경** 버튼을 클릭합니다.
- 3 대화상자 창이 열리면 **지원 요청 생성**을 클릭합니다.
그러면 VMware Customer Connect의 **VMware 지원** 페이지가 열립니다.
- 4 **비기술 지원**에서 **안내식 지원 받기**를 클릭합니다.
- 5 **클라우드 서비스**에서 **청구 및 사용량**을 클릭하고 안내 메시지에 따라 요청을 생성합니다.

판매자 정보를 보는 방법



조직에 하나 이상의 VMware 파트너로부터 구매한 서비스 및 구독이 있는 경우에만 판매자 정보를 사용할 수 있습니다.

조직의 각 판매자는 별도의 타일로 표시됩니다.


절차

- 1 Cloud Services 콘솔에 로그인하고 **청구 및 구독 > 개요**를 선택합니다.
판매자 섹션에는 조직에서 서비스를 구매한 판매자가 나열됩니다. 예를 들어 조직이 VMware 및 Amazon Web Services에서 서비스를 구매한 경우 두 판매자가 표시됩니다.

Overview

 It looks like you have purchased subscriptions through multiple sellers. The current costs below reflect only what you've purchased through VMware. 

Seller

 **Amazon Web Services**

You have made purchase from AWS in this organization.
 See AWS costs and payment methods from AWS.

[SELLER DETAILS](#)

VMware Costs

Current Costs

Default Payment Method: Fund-1234 (VMware fund)

\$80,200.00

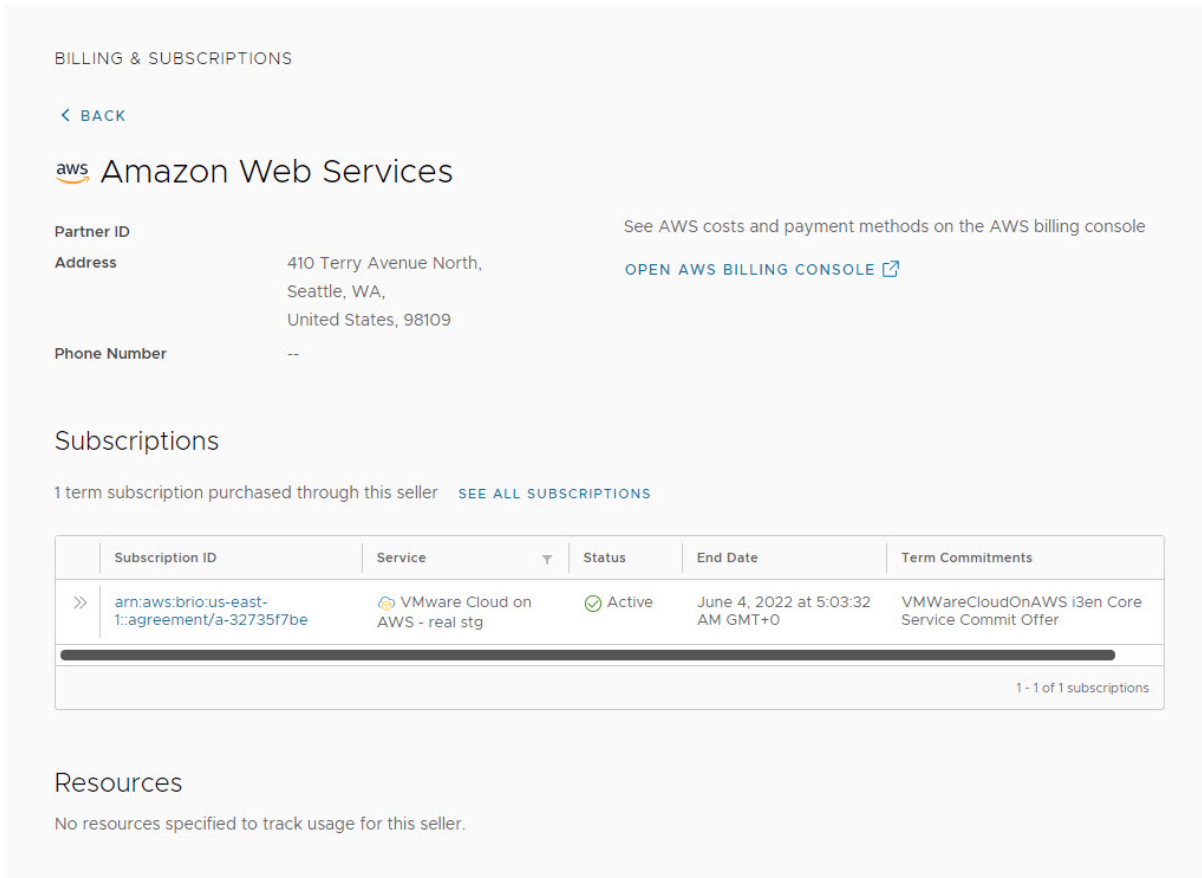
total this billing period: Aug 3 - Sep 2

AUG 3 TODAY: \$80,200.00 SEP 2

>	VMware Cloud on AWS	\$79,200.00
>	Network Insight	\$2,000.00
>	Promotional Credits (Estimated)	-\$1,000.00
	Total ⓘ	\$80,200.00

- 조직의 VMware 파트너 판매자로부터 구매한 서비스 및 구독을 보려면 각 타일에서 **판매자 세부 정보** 링크를 클릭합니다.

판매자의 세부 정보 페이지가 열립니다.



- 이 판매자와 연결된 비용 및 지불 방법을 보려면 해당 청구 콘솔에 대한 링크를 클릭합니다.

- 이 판매자로부터 구매한 구독에 대한 세부 정보를 보려면 **구독 ID** 링크를 클릭합니다.

그러면 기간 약정, 구독 시작 및 종료 날짜, 지불 방법, 구독 기록 등과 같은 추가 세부 정보를 볼 수 있는 구독 세부 정보 페이지가 열립니다.

다음에 수행할 작업

조직에 VMware를 판매자로 등록하지 않은 경우 클라우드 서비스를 직접 구매할 수 있도록 **VMware를 판매자로 추가하는 방법**을 알아보십시오.

VMware Cloud Services에 파트너 판매자 계약 코드를 등록하는 방법

VMware 파트너가 아닌 판매자를 통해 구독을 구매하는 경우 주문에 할인이 포함될 수 있습니다. **조직 소유자인** 사용자는 조직에 서비스가 온보딩된 후 파트너 판매자가 제공하는 계약 코드를 Cloud Services 콘솔에 등록해야 합니다.

VMware Cloud Services의 판매자 프로필과 계약 코드를 연결하여 주문 할인이 청구서에 반영됩니다.

사전 요구 사항

- 조직에서 **조직 소유자** 역할이 있습니다.
- 파트너 판매자를 통해 구매한 구독에 대한 계약 번호가 있습니다.
- 서비스를 온보딩했으며 판매자가 조직에 있습니다.

절차

- 1 Cloud Services 콘솔에 로그인하고 **청구 및 구독 > 개요**를 선택합니다.
페이지의 **판매자** 섹션에는 조직에서 서비스를 구매한 판매자가 나열됩니다.
- 2 판매자 세부 정보 타일 또는 페이지에서 **계약 추가** 링크를 클릭합니다.
- 3 팝업 창이 열리면 계약 번호를 입력한 다음 **제출**을 클릭합니다.

결과

이제 계약 코드가 조직과 연결되어 모든 관련 할인이 적용됩니다.
또한 관련 서비스에 대한 구독을 독립적으로 생성할 수 있습니다.

VMware를 판매자로 추가하는 방법

조직이 VMware 이외의 판매자로부터 VMware Cloud services를 구매한 경우 해당 서비스로 온보딩할 때 또는 나중에 VMware를 추가할 수 있습니다. 이러한 방식으로 기존 판매자와 함께 VMware에서 직접 VMware Cloud services를 구매할 수 있습니다.

조직에 VMware를 판매자로 추가하는 것은 VMware로 청구 계정을 생성하고 조직에 대한 프로파일을 작성해야 함을 의미합니다. 조직의 비즈니스 주소와 기본 지불 방법을 추가하여 청구 계정을 생성합니다.

사전 요구 사항

Cloud Services 콘솔에서 VMware를 판매자로 추가하려면 **조직 소유자** 역할이 있어야 하며 조직이 VMware 이외의 판매자로부터 서비스를 구매해야 합니다.


절차

- 1 My VMware 계정으로 Cloud Services 콘솔에 로그인합니다.
- 2 **청구 및 구독 > 개요**로 이동합니다.
판매자 섹션에는 조직에 있는 VMware 이외의 판매자가 표시됩니다.

BILLING & SUBSCRIPTIONS

Overview

Sellers ⓘ


 Amazon Web Services

You have made purchase from AWS in this organization. See AWS costs and payment methods from AWS.

[SELLER DETAILS](#)

To purchase VMware services directly, add VMware as a seller.

[+ ADD VMWARE AS A SELLER](#)



No Cost Information Available

Once you have made a purchase or billed a resource to VMware, your VMware cost will show up here.

- 3 **VMware를 판매자로 추가** 링크를 클릭합니다.
- 4 청구 주소를 입력하고 통화 및 지불 방법을 선택하여 조직의 프로파일을 작성합니다.

참고 청구 계정을 생성한 후 조직의 통화를 변경하려면 지원 티켓을 제출해야 합니다.

- 5 **서비스 약관**을 검토하고 이에 동의합니다.
- 6 **완료**를 클릭합니다.

결과

이제 VMware가 조직의 판매자로 추가되었습니다.

내 조직의 지불 방법을 관리하는 방법

청구 계정은 조직에서 사용 가능한 지불 방법을 결정합니다. 펀드, 신용 카드를 사용하거나 무제한 PBI(송장으로 지불) 계정을 연결할 수 있습니다.

펀드

VMware 펀드 중 하나를 사용하여 조직의 비용을 처리하려면 펀드를 조직에 연결하고 펀드 중 하나를 기본 지불 방법으로 설정합니다. 이러한 방식으로 모든 조직 전체에서 동일한 펀드를 사용할 수 있습니다. VMware Cloud services와 연결된 VMware 사용 권한 계정 내에 있으며 조직에서 사용되는 동일한 통화인 경우 어느 펀드든 사용할 수 있습니다. 자세한 내용은 [펀드로 지불하는 방법](#)의 내용을 참조하십시오.

신용 카드

해당 국가에서 신용 카드 사용에 대한 제한이 없는 한 신용 카드를 사용하여 서비스 비용을 지불할 수 있습니다. 자세한 내용은 [신용 카드를 지불 방법으로 사용하는 경우 제한 사항](#)의 내용을 참조하십시오.

조직의 지불 통화가 카드 통화와 다른 경우 신용 카드 제공자에 의한 해외 거래 수수료가 발생할 수 있습니다. 자세한 내용은 [신용 카드로 지불하는 방법](#)을 참조하십시오.

송장으로 지불 계정

새 서비스에 대한 판매 주문이 PBI(송장으로 지불) 계정과 연결된 경우 서비스 온보딩 중에 지불 방법으로 표시됩니다. 이 경우 PBI 지불 방법은 제한되어 판매 주문에 포함된 구독에만 적용할 수 있고 기본 지불 방법으로 조직에 추가할 수 없습니다.

PBI 계정을 기본 지불 방법으로 사용하여 조직에서 발생한 구매, 리소스 및 초과를 커버하려면 조직의 모든 서비스에 대한 지불 승인을 위해 무제한 PBI를 활성화해야 합니다. 무제한 PBI를 사용하도록 설정하려면 지원 요청을 제출하여 시작하는 오프라인 승인 프로세스를 수행해야 합니다. 자세한 내용은 [송장으로 지불하는 방법](#)을 참조하십시오.

조직에 원하는 만큼 지불 방법을 추가할 수 있지만 그 중 하나만 기본 지불 방법으로 설정할 수 있습니다.

새 지불 방법을 추가하는 방법

조직 소유자인 사용자는 새 지불 방법을 조직에 추가할 수 있습니다. 조직 수준에서 정의된 지불 방법은 모든 **조직 소유자인** 사용자가 사용할 수 있게 됩니다.

절차

- 1 Cloud Services 콘솔을 열고 **청구 및 구독 > 지불 방법 관리**로 이동합니다.
- 2 페이지의 **기타 지불 방법** 영역에서 **지불 방법 추가**를 클릭합니다.

3 추가할 지불 방법 유형을 선택합니다.

수행할 작업	절차
송장으로 지불 계정 연결	<p>추가할 송장으로 지불 계정을 하나 이상 선택하고 계정 연결을 클릭합니다.</p> <p>참고 무제한 PBI 계정은 조직 수준에서만 지불 방법으로 추가할 수 있습니다. 추가하려는 PBI 계정이 제한된 경우 먼저 지원 티켓을 제출하여 무제한 PBI를 활성화해야 합니다.</p>
VMware 펀드 연결	<p>지불 방법으로 추가할 VMware 펀드를 선택한 다음 펀드 연결을 클릭합니다.</p>
신용 카드 추가	<p>신용 카드 세부 정보를 추가하고 카드 추가를 클릭합니다.</p> <p>참고 카드 추가 및 기본값으로 설정을 클릭하면 조직의 기본 지불 방법이 변경되고, 이는 기본 지불 방법을 사용하는 모든 서비스 및 구독에 영향을 줍니다.</p>

기본 지불 방법 소개

VMware Cloud services에 가입할 때 조직의 비용을 처리하는 데 사용할 지불 방법을 추가합니다. 이 지불 방법은 조직의 기본 지불 방법이 되며 조직 내의 **조직 소유자**인 모든 사용자가 사용할 수 있습니다.

구매에 대해 다른 지불 방법을 지정하지 않는 한 기본 지불 방법이 조직의 모든 구매, 리소스 및 초과에 적용됩니다. Cloud Services 콘솔의 **청구 및 구독 > 지불 방법 관리** 탭에서 새 지불 방법을 추가하거나 조직의 기본 지불 방법을 변경할 수 있습니다.

조직의 기본 지불 방법으로 펀드, 신용 카드를 추가하거나 무제한 PBI(송장으로 지불) 계정을 연결할 수 있지만 그 중 하나만 기본 지불 방법으로 설정할 수 있습니다.

조직을 설정할 때 조직의 주소에 따라 조직의 서비스에 대해 지불하는 통화가 결정됩니다. 지불 방법 및 통화에 대한 자세한 내용은 **지불 통화가 결정되는 방식** 항목을 참조하십시오.

추가 서비스를 구독하고 추가 기능을 구매하고 조직에 약정을 적용할 때 판매 주문이 해당 특정 구매에만 적용되는 구독 또는 기간 약정에 대해 다른 지불 방법을 결정할 수 있습니다. 나중에 구독에 대한 지불 방법을 변경할 수 있습니다. 자세한 내용은 **구독 지불 방법을 변경하는 방법**을 참조하십시오.

조직의 기본 지불 방법을 변경하는 방법

조직 소유자인 사용자는 조직의 기본 지불 방법을 변경할 수 있습니다.

조직에서 사용할 수 있는 모든 지불 방법은 Cloud Services 콘솔의 **지불 방법 관리** 페이지에서 **기타 지불 방법** 섹션에 나열됩니다. 조직에 대한 기본 지불 방법을 나열되지 않은 새 지불 방법으로 변경하려는 경우 먼저 지불 방법을 추가해야 합니다.

절차

- 1 Cloud Services 콘솔을 열고 **청구 및 구독 > 지불 방법 관리**로 이동합니다.
- 2 페이지의 **기본 지불 방법** 영역에서 [기본 지불 방법 변경]을 클릭합니다.

- 3 표시되는 사용 가능한 지불 방법 목록에서 사용할 지불 방법을 선택합니다.
- 4 **확인**을 클릭합니다.

새 기본 지불 방법이 즉시 적용됩니다.

구독 지불 방법을 변경하는 방법

조직에서 새 서비스를 온보딩하거나 기존 서비스에 새 구독을 추가하는 경우 기본 지불 방법을 선택하거나 새 구독에 대해 다른 지불 방법을 추가할 수 있습니다. 나중에 조직의 모든 구독에 대한 지불 방법을 변경할 수 있습니다.

현재 구독에 대한 지불 방법을 변경해도 조직의 기본 지불 방법에는 영향을 주지 않습니다. 기본 지불 방법은 이 지불 방법을 사용하는 다른 구매 및 리소스에 계속 적용됩니다. 새로 정의된 지불 방법은 **조직 소유자**인 사용자가 변경할 때까지 현재 구독의 비용을 지불하는 데에만 사용됩니다.

절차

- 1 Cloud Services 콘솔을 열고 **청구 및 구독 > 구독**으로 이동합니다.
- 2 조직의 구독 목록에서 변경할 구독의 **구독 ID** 링크를 클릭합니다.
구독 세부 정보 페이지가 열립니다.
- 3 페이지의 **지불 방법** 영역에서 **변경**을 클릭합니다.
- 4 조직의 사용 가능한 지불 방법 목록에서 구독에 대한 새 지불 방법을 선택합니다.
- 5 **확인**을 클릭합니다.

결과

구독 세부 정보 페이지가 새로 고쳐지면서 선택한 새 지불 방법이 표시됩니다.

송장으로 지불하는 방법

조직 소유자인 사용자는 무제한 PBI가 활성화된 경우 조직의 기본 지불 방법을 PBI(송장으로 지불)로 변경할 수 있습니다. 무제한 PBI를 사용하도록 설정하려면 지원 요청을 제출하여 시작하는 오프라인 승인 프로세스를 수행해야 합니다.

활성화되면 PBI를 조직 전반의 모든 서비스 및 구독에 대한 기본 지불 방법으로 적용할 수 있습니다. 무제한 PBI를 현재 구독에 대한 지불 방법으로 적용할 수도 있습니다.

절차

- 1 Cloud Services 콘솔에서 **지원 센터**를 선택하고 **지원 요청 생성**을 클릭합니다.
- 2 **범주** 텍스트 상자에서 **VMware Cloud Services - 청구 및 사용량**을 선택합니다.
- 3 **제목** 텍스트 상자에서 **무제한 PBI 활성화**를 입력합니다.
- 4 지원 요청 세부 정보를 입력하고 **지원 요청 생성**을 클릭합니다.

VMware Cloud Services 담당자가 귀하에게 해당 요청과 관련해 연락합니다. 무제한 PBI가 활성화되면 알림을 받게 됩니다.

신용 카드로 지불하는 방법

VMware Cloud services는 다양한 신용 카드를 사용한 지불을 지원합니다. 개인 또는 회사 Mastercard, Visa, American Express, Discover, JCB, Diners Club 신용 카드를 사용할 수 있습니다. Mastercard, Visa 또는 American Express 직불 카드를 사용할 수도 있습니다.

신용 카드를 사용하여 서비스에 대해 지불하려는 경우:

- 신용 카드 한도 및 지불 프로세서가 거래 규모를 결정합니다. 단일 거래에서 소비할 수 있는 최대 금액은 25,000달러입니다. 신용 한도에 대한 자세한 내용은 발급 은행에 문의해야 합니다.
- 조직의 주소가 청구되는 통화를 결정합니다. 국가 및 관련 통화 목록은 [지불 통화가 결정되는 방식](#) 항목을 참조하십시오.
- 조직의 주소 및 신용 카드의 청구 주소를 기반으로 신용 카드 사용에 대한 특정 [신용 카드를 지불 방법으로 사용하는 경우 제한 사항](#)이 있습니다.

중요 조직의 청구 주소가 EEA(유럽 경제 지역) 회원국 또는 협력 국가인 경우 신용 카드 지불은 유럽 연합의 PSD2(Second Payment Service Directive, 2015/2366)의 영향을 받습니다. PSD2에서는 전자 거래에 2단계 인증을 통한 SCA(Strong Customer Authentication)를 요구합니다. 필요한 경우 결제 과정 중에 추가 보안 정보를 제공하라는 SCA 프롬프트가 표시되고 이러한 정보는 나중에 은행 또는 카드 발급자가 확인하게 됩니다.

- 신용 카드를 지불 방법으로 추가하면 해당 카드에 대해 비용을 청구하지는 않지만 카드가 유효한지 확인합니다. 유효성 검사에는 금융기관에 의한 사전 인증 요청이 포함될 수 있습니다. 청구서에서 1.00달러 또는 등가의 보류 중인 인증 요청을 확인할 수 있습니다. 사전 인증은 요금이 아니며 계좌에서 펀드가 인출되지 않습니다.

클라우드 서비스를 온보딩할 때 또는 나중에 Cloud Services 콘솔에서 [청구 및 구독 > 지불 방법 관리](#)를 선택하여 신용 카드를 지불 방법으로 추가할 수 있습니다.

자세한 내용은 [조직의 기본 지불 방법을 변경하는 방법](#)의 내용을 참조하십시오.

신용 카드를 지불 방법으로 사용하는 경우 제한 사항

위험 및 사기에 대한 고려 사항으로 인해 신용 카드를 지불 방법으로 사용하는 경우 특정 제한 사항이 적용될 수 있습니다. 이러한 제한 사항은 조직의 주소 또는 신용 카드의 청구 주소를 기반으로 합니다.

신용 카드 사용 제한이 적용되는 국가 목록

국가가 신용 카드 사용 제한에 해당하는 경우에는 VMware Cloud Services에서 지불 방법이 비활성화됩니다.

다음과 같은 경우 신용 카드를 지불 방법으로 사용할 수 없습니다.

<p>조직의 주소가 다음 국가 중 하나에 해당합니다.</p>	<p>아프가니스탄, 네덜란드령 앤티리스, 앙골라, 보스니아 헤르체고비나, 방글라데시, 부르키나파소, 바레인, 브라질, 벨로루시, 콩고 민주 공화국, 카메룬, 중국, 쿠바, 카보베르데, 키프로스, 에리트레아, 포클랜드 제도, 프랑스령 기아나, 과들루프, 괌, 아이티, 맨 섬, 이라크, 이란, 한국, 쿠웨이트, 라오스, 몽골, 말리, 마르티니크, 몬트세라트, 멕시코, 나이지리아, 네팔, 팔레스타인 점령 지역, 수단, 세네갈, 시리아, 투르크메니스탄, 동티모르, 우크라이나, 바티칸, 베네수엘라, 마요트, 짐바브웨.</p>
<p>신용 카드의 청구 주소가 다음 국가 중 하나에 해당합니다.</p>	<p>아프가니스탄, 네덜란드령 앤티리스, 앙골라, 남극 대륙, 올란드 제도, 보스니아 헤르체고비나, 방글라데시, 부르키나파소, 바레인, 세인트 바셀레미, 보네르, 신트외스타티위스 및 사바, 브라질, 부베이 섬, 벨로루시, 코코스, 콩고 민주 공화국, 중앙 아프리카 공화국, 카메룬, 중국, 쿠바, 카보베르데, 쿠라카오, 크리스마스 섬, 키프로스, 서사하라, 에리트레아, 포클랜드 제도, 프랑스령 기아나, 과들루프, 사우스 조지아 및 사우스 샌드위치 제도, 괌, 홍콩, 허드 섬 및 맥도널드 제도, 아이티, 맨 섬, 인도, 영국령 인도양 식민지, 이라크, 키리바시, 한국, 쿠웨이트, 라오스, 리투아니아, 룩셈부르크, 라트비아, 세인트 마틴, 말리, 몬트세라트, 멕시코, 말레이시아, 노퍽 섬, 나이지리아, 노르웨이, 네팔, 나우루, 니우에, 핏케언, 팔레스타인 점령 지역, 르완다, 수단, 스웨덴, 싱가포르, 스발바르 및 얀마센, 세네갈, 소말리아, 남수단, 상투메 프린시페, 시리아, 차드, 프랑스 남쪽 영역, 태국, 토켈라우, 투르크메니스탄, 동티모르, 터키, 투발루, 미국령 군소 제도, 바티칸, 베네수엘라, 마요트, 짐바브웨.</p>

프로모션 크레딧으로 지불하는 방법

VMware Cloud services에 대해 프로모션 크레딧이 있는 경우 이를 조직 중 하나에 적용하고 조직의 월별 비용에 대해 사용할 수 있습니다.

프로모션 크레딧은 특정 서비스에만 적용되거나(특정 서비스의 월별 비용에 대해 사용할 수 있음), 서비스 그룹에 적용되거나, 모든 서비스에 적용될 수 있습니다. 크레딧의 만료 날짜를 확인하고 만료되기 전에 사용해야 합니다.

프로모션 크레딧은 모든 VMware Cloud Services 지원 통화에 대해 사용할 수 있습니다. 프로모션 크레딧은 당사의 서비스 중 하나를 처음 온보딩할 때 경우에 따라 부여됩니다. 해당 크레딧은 서비스를 온보딩할 때 사용됩니다.

절차

- 1 Cloud Services 콘솔에서 **청구 및 구독 > 프로모션 크레딧**을 클릭합니다.

조직에서 적용할 수 있는 모든 프로모션 크레딧이 **사용 가능한 크레딧** 탭에 표시됩니다.

2 프로모션 크레딧을 사용하려면 세부 정보 타일에서 **활성화** 링크를 클릭합니다.

크레딧은 다음 청구 기간 동안 사용됩니다. **청구 및 구독 > 프로모션 크레딧 > 활성화된 크레딧**으로 이동하면 언제든지 프로모션 크레딧의 잔액을 확인할 수 있습니다.

VMware 펀드에 대해 알아두어야 할 사항

VMware 펀드는 서비스 또는 제품을 구매하는 데 사용할 수 있는 VMware 관련 지불 방법입니다. 각 펀드는 하나 이상의 예금으로 구성됩니다.

펀드에 "금액"을 추가하려는 경우 영업 담당자를 통해 새로운 예금을 구매할 수 있습니다. 예금은 VMware 서비스 및 제품에 대해 지출할 수 있는 금액인 "크레딧"으로 구성됩니다.

액세스 권한이 필요한 VMware Connect 포털의 펀드 관리 플랫폼을 통해 세부 정보를 보고 연결된 펀드의 설정을 관리합니다. 자세한 내용은 [내 펀드 페이지](#), [펀드 세부 정보 페이지](#) 및 [탐색의 개요](#)를 참조하십시오.

VMware 펀드를 사용하여 클라우드 서비스 및 구독 비용을 지불하려면 각 펀드를 VMware Cloud services 조직에 지불 방법으로 연결해야 합니다. 펀드를 조직 및 구독에 대한 기본 지불 방법 또는 일회성 지불 방법으로 연결할 수 있습니다. 또한 Cloud Services 콘솔에서 미결 송장을 직접 지불하는 데 사용할 수도 있습니다. 연결된 펀드로 조직의 비용을 충당하려면 펀드에 잔액이 있어야 하며 해당 "금액"이 충분해야 합니다.

Cloud Services 콘솔에서 펀드를 연결하려면 다음에 유의하십시오.

- 펀드를 연결하려는 조직에서 **조직 소유자** 역할이 있어야 합니다.
- VMware 사용 권한 계정 내에 있는 펀드만 VMware Cloud services 조직과 연결할 수 있습니다.
- 펀드의 통화 및 판매 단위가 조직의 통화 및 판매 단위와 일치해야 합니다.

조직에서 기본 지불 방법으로 사용 중인 연결된 펀드의 잔액이 부족하거나 펀드가 만료 또는 분리된 경우라면 펀드를 다른 펀드(생존 펀드라고 함)로 바꾸거나 다른 지불 방법으로 바뀌어야 합니다. 분리된 펀드는 빈 펀드 그룹으로 지불 흐름을 중단시키므로 즉시 바뀌어야 합니다.

VMware Cloud Services는 **조직 소유자**인 사용자가 적시에 펀드를 관리할 수 있도록 이메일 및 애플리케이션 내 알림을 통해 조직의 펀드 상태와 펀드에 대한 변경 내용을 알립니다. 자세한 내용은 [VMware Cloud Services에서 VMware 펀드를 관리하는 방법](#)의 내용을 참조하십시오.

펀드로 지불하는 방법

조직 소유자인 사용자는 연결된 VMware 펀드를 사용하여 서비스 비용을 충당할 수 있습니다. 조직의 기본 지불 방법으로 펀드를 사용하는 것 외에도 Cloud Services 콘솔에서 직접 미결 송장을 지불할 수 있습니다.

원하는 작업	수행할 단계
연결된 VMware 펀드를 조직의 기본 지불 방법으로 설정합니다.	조직의 기본 지불 방법을 변경하는 방법 의 내용을 참조하십시오.
연결된 VMware 펀드를 활성 구독에 대한 지불 방법으로 설정합니다.	구독 지불 방법을 변경하는 방법 의 내용을 참조하십시오.

원하는 작업	수행할 단계
<p>미결 초과분 송장 또는 기간 약정 송장을 지불합니다.</p>	<ol style="list-style-type: none"> 1 Cloud Services 콘솔에 로그인하고 청구 및 구독 > 송장 및 청구서 > 송장으로 이동합니다. 2 지불하려는 미지불 송장을 찾은 후 세로 줄임표 아이콘  을 클릭합니다. 3 지금 지불 링크를 클릭합니다. 4 팝업 창이 열리면 송장 세부 정보를 검토하고 이 지불에 사용할 펀드를 선택합니다. <hr/> <p>참고 지불 방법 드롭다운은 조직에 연결되어 있고 잔액이 남아 있는 펀드만 표시합니다.</p> <ol style="list-style-type: none"> 5 지금 지불을 클릭합니다. <p>지불이 제출되고 송장 페이지가 새로 고쳐지면서 지불한 송장 옆에 In Progress 상태()가 표시됩니다.</p> <p>거래가 완료되면 이메일 알림을 받게 됩니다. 거래는 즉시 완료되거나 몇 시간이 걸릴 수 있습니다. 송장 잔액은 거래 완료 후에만 업데이트됩니다.</p> <p>첫 번째 부분 지불이 진행 중인 동안 추가 지불을 할 수 있습니다. 업데이트된 송장에는 지불 및 업데이트된 잔액이 모두 반영됩니다.</p>
<p>Cloud Services 콘솔을 통해 펀드로 지불된 송장에 대한 지불 내역을 보려는 경우</p>	<ol style="list-style-type: none"> 1 청구 및 구독 > 송장 및 청구서 > 송장으로 이동합니다 2 지불을 확인하려는 송장을 찾은 다음 세로 줄임표 아이콘  을 클릭합니다. 3 지불 내역 링크를 클릭합니다. <p>지불 내역 섹션에는 선택한 송장에 대한 지불 방법, 상태 및 지불 금액이 표시됩니다.</p>

VMware Cloud Services에서 VMware 펀드를 관리하는 방법

조직 소유자인 사용자는 Cloud Services 콘솔에서 조직의 지불 방법으로 VMware 펀드를 연결 및 연결 해제할 수 있습니다. 조직에 연결된 펀드만 기본 지불 방법으로 설정하거나 미결 초과분 송장 및 기간 약정 송장을 지불하는 데 사용할 수 있습니다.

참고 Cloud Services 콘솔에서 조직에 대한 펀드 연결만 관리합니다. 액세스 권한이 필요한 VMware Connect 포털을 통해 실제 펀드를 관리합니다.

조직의 VMware 펀드에 대한 변경 관련 알림은 조직에서 **청구 읽기 전용** 역할이 있는 **조직 멤버**인 사용자 및 모든 **조직 소유자**인 사용자에게 이메일을 통해 그리고 애플리케이션 내 알림으로 자동 전송됩니다.

다음 표에서는 VMware Cloud Services 조직에서 VMware 펀드 지불 방법을 사용하는 방법을 설명합니다.

원하는 작업	수행할 단계
<p>VMware 펀드를 조직의 지불 방법으로 연결하려는 경우.</p>	<p>VMware Cloud services와 연결된 VMware 사용 권한 계정 내에 있으며 조직에서 사용되는 동일한 통화인 경우 어느 펀드든 사용할 수 있습니다.</p> <ol style="list-style-type: none"> 1 Cloud Services 콘솔에 로그인하고 청구 및 구독 > 지불 방법 관리로 이동합니다. 2 페이지의 기타 지불 방법 섹션에서 지불 방법 추가를 클릭합니다. 3 VMware 펀드 연결을 선택하고 계속을 클릭합니다. 4 사용 가능한 VMware 펀드 목록이 표시되면 조직의 지불 방법으로 연결할 펀드를 선택합니다. <hr/> <p>참고 이 목록에는 VMware 계정에 연결된 VMware 펀드만 표시됩니다.</p> <ol style="list-style-type: none"> 5 선택한 펀드를 연결합니다. <ul style="list-style-type: none"> ■ 펀드를 조직의 기본 지불 방법으로 연결하려면 펀드를 연결하고 기본값으로 설정을 클릭합니다. ■ 펀드를 연결하고 조직의 지불 방법으로 사용할 수 있도록 하려면 펀드 연결을 클릭합니다.
<p>조직의 지불 방법으로 이미 연결되어 있는 펀드의 연결을 해제하려는 경우.</p>	<p>조직의 지불 방법은 모든 조직 소유자인 사용자가 사용할 수 있습니다. 조직에서 활성 펀드를 제거하려면 다음을 수행합니다.</p> <ol style="list-style-type: none"> 1 지불 방법 관리 페이지를 엽니다. 2 펀드 이름 옆의 가로 줄임표 아이콘(***)을 클릭하고 펀드 연결 해제를 선택합니다.
<p>조직의 지불 방법으로 이미 연결되어 있는 펀드에 대한 세부 정보를 보려는 경우.</p>	<ol style="list-style-type: none"> 1 청구 및 구독 > 지불 방법 관리로 이동합니다. 2 펀드 이름 옆의 가로 줄임표 아이콘(***)을 클릭하고 MyVMware에 대한 세부 정보 보기를 선택합니다. <p>그러면 VMware Customer Connect 웹 사이트가 열립니다. 여기에서 VMware 계정으로 로그인하면 펀드의 세부 정보를 볼 수 있습니다.</p>
<p>조직의 기본 지불 방법으로 이미 연결되어 있는 만료된 펀드를 관리하려는 경우.</p>	<p>조직의 기본 지불 방법으로 펀드를 사용하는 경우 만료 날짜 전에 이메일 알림을 받게 됩니다. 만료를 보류 중인 펀드의 경우 다음 작업 중 하나를 수행할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 조직의 기본 지불 방법을 조직에 연결된 다른 활성 펀드로 변경합니다. ■ 기본 지불 방법을 신용 카드 또는 PBI로 변경합니다. ■ 조직에 연결되지 않은 다른 활성 펀드가 있는 경우 해당 펀드를 조직에 연결한 다음 기본 지불 방법으로 설정할 수 있습니다.

원하는 작업	수행할 단계
잔액이 부족한 펀드를 관리하려는 경우	기본 지불 방법으로 사용 중이거나 송장 지불에 사용하는 펀드에 전체 송장 금액을 충당하기에 충분한 "금액"이 없는 경우 송장은 부분적으로 지불된 것으로 표시됩니다. 남은 비용을 충당하려면 충분한 "크레딧"이 있는 다른 펀드나 다른 지불 방법을 사용해야 합니다.
조직의 기본 지불 방법으로 연결되어 있는 분리된 펀드를 관리하려는 경우	<p>다음과 같은 이유 중 하나로 펀드가 분리될 수 있습니다.</p> <ul style="list-style-type: none"> ■ 펀드 소유자 변경 ■ 펀드 병합 ■ 조직 소유자 변경 ■ 조직 소유자가 펀드 사용자에서 제외됨 <p>이러한 경우 VMware Cloud Services에서는 조직 소유자인 사용자에게 펀드가 분리되었음을 알리고 이 분리된 펀드를 생존 펀드로 바꿉니다. 업데이트된 기본 지불 방법에 대한 추가 알림이 모든 조직 소유자인 사용자에게 전송됩니다. 지불에 대한 추가 변경이 필요한 경우 내 조직의 지불 방법을 관리하는 방법 항목을 참조하십시오.</p>

VMware Cloud Services 구독 및 약정을 사용하는 방법

VMware Cloud services 구독을 사용하면 미리 정의된 기간(1년 또는 3년) 동안 감소 또는 협상된 요금으로 특정 용량을 구입하도록 약정하여 비용을 절약할 수 있습니다.

VMware Cloud services는 주문형으로 사용하거나 1년 또는 3년의 구독 기간을 구매하여 사용할 수 있습니다. 주문형 서비스 사용량은 더 높은 요금으로 청구되는 반면 서비스 구독은 할인된 요금으로 청구됩니다. 구독은 SPP(구독 구매 프로그램) 또는 송장으로 지불을 통해 구매합니다.

구독의 각 서비스에 대해 여러 약정을 구매하고 사용할 수 있습니다. 각 약정 기간의 시작 날짜와 종료 날짜는 다를 수 있습니다. 구매 주문에는 약정의 용량, 기간 및 협상 가격이 요약됩니다.

VMware Cloud Services는 서비스 구독에 대한 약정에 제시된 조건에 따라 청구합니다.

약정 기간에서 커버되지 않은 추가 사용량은 해당 서비스에 가입할 때 동의한 주문형 가격 책정을 기반으로 청구됩니다.

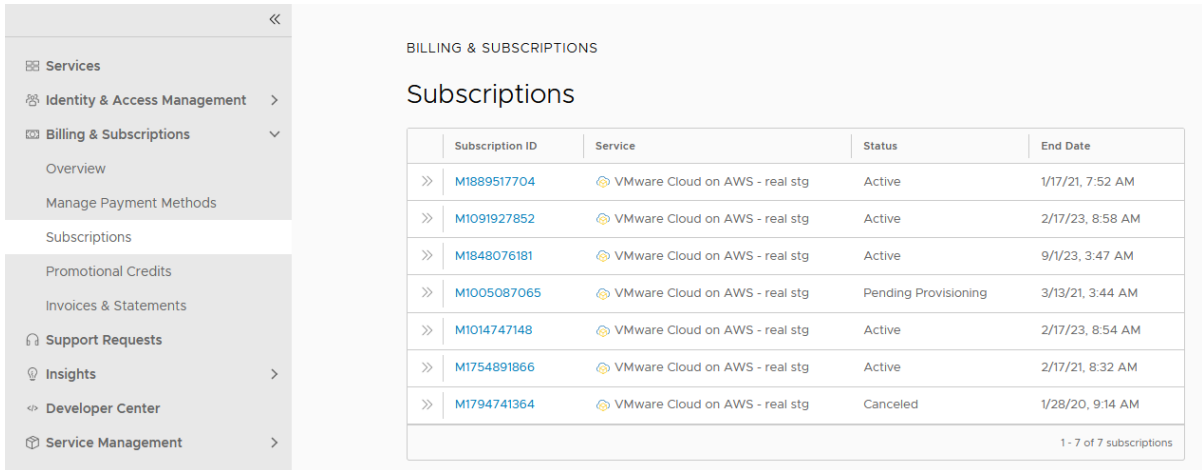
조직의 서비스에 대한 구독 세부 정보를 보는 방법

조직의 구독 세부 정보를 보려면 **청구 읽기 전용** 사용 권한이 있는 **조직 멤버** 역할 또는 **조직 소유자** 역할이 있어야 합니다.

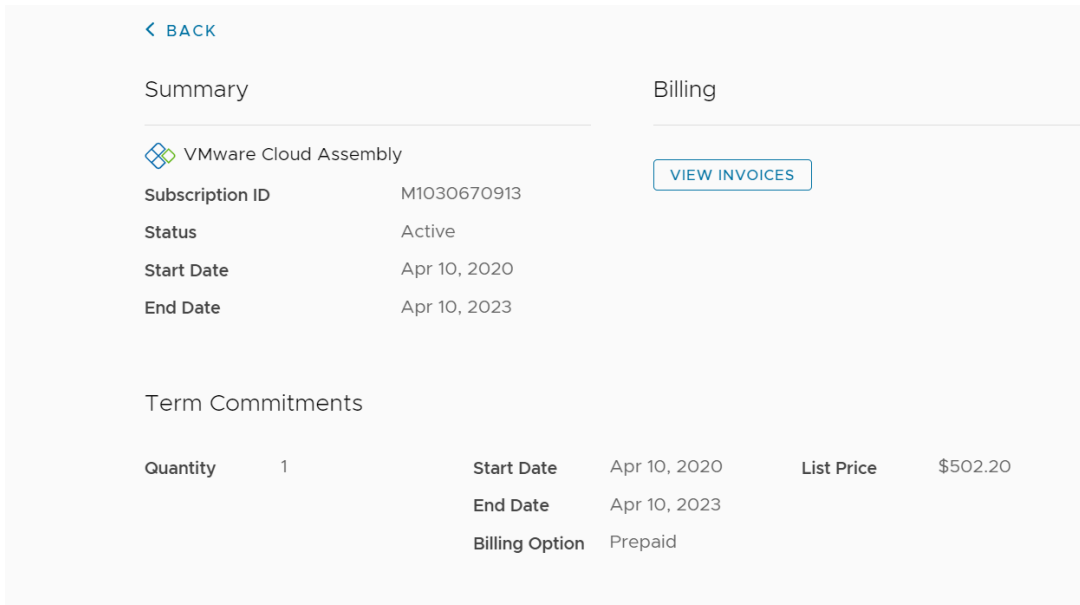
절차

- 1 Cloud Services 콘솔에서 **청구 및 구독 > 구독**으로 이동합니다.

조직의 모든 구독에 대한 정보가 들어 있는 표가 열립니다. 여기에는 각 구독의 ID, 구독을 구매한 VMware Cloud services 및 구독에 포함된 기간 약정이 나열되어 있습니다.



- 2 특정 구독에 대한 자세한 정보를 보려면 보려는 구독을 찾고 해당 **구독 ID** 링크를 클릭합니다. 페이지가 열리면서 구독 및 구독과 함께 구매한 기간 약정에 대한 추가 세부 정보가 표시됩니다.



- 3 (선택 사항) 송장을 보고 다운로드하려면 페이지의 **청구** 섹션에서 **송장 보기**를 클릭합니다.

약정을 설정하는 방법

조직 소유자 사용자인 경우 VMware 영업 담당자에게 문의하여 견적을 협상하고 약정에 대한 지불을 마련합니다. 구매가 완료되면 약정이 활성임을 나타내는 알림 이메일이 수신됩니다. 각 약정에 대해 고유한 링크가 포함된 이메일이 수신됩니다.

- 1 현재 조직 중 하나 또는 새 조직에 약정을 적용하려면 이메일의 링크를 클릭합니다.
- 2 서비스 온보딩 워크플로의 단계를 따릅니다.

약정에 대한 자세한 내용은 **조직에 약정을 적용해야 하는 이유** 항목을 참조하십시오.

온보딩 워크플로에 대한 자세한 내용은 [VMware Sales](#)를 통해 구매한 유료 클라우드 서비스를 온보딩하는 방법을 참조하십시오.

구독을 구매하는 방법

VMware Cloud Services에는 선택된 서비스 및 판매자를 위한 셀프 서비스 구독 구매 옵션이 있습니다.

참고 셀프 서비스 구독 구매 옵션은 현재 VMware에서 구매한 VMware Tanzu Service Mesh에만 사용할 수 있습니다.

청구 및 구독 > 구독 페이지 또는 Cloud Services 콘솔의 Cloud Services 카탈로그에 있는 서비스 타일에서 위에 나열된 서비스에 대한 구독 구매 주문을 시작할 수 있습니다.

사전 요구 사항

새 구독을 구매할 조직에서 **조직 소유자** 역할이 있어야 합니다.

절차

- 1 Cloud Services 콘솔에 로그인하고 **청구 및 구독 > 구독**으로 이동합니다.
- 2 **구독 생성**을 클릭합니다.
구독 생성 워크플로의 첫 번째 단계가 열립니다.
- 3 **서비스** 워크플로 단계의 **서비스 선택** 섹션에서 드롭다운 메뉴를 사용하여 서비스/서비스 번들 및 새 구독을 구매할 판매자를 선택합니다.
- 4 **다음**을 클릭합니다.
조직에 유효한 주소가 없거나 조직에 대한 기본 지불 방법이 정의되지 않았다면 다음 단계로 **청구 정보**가 열립니다.
- 5 워크플로의 **청구 정보** 단계에서는 조직의 주소를 지정하고 기본 지불 방법을 선택합니다.
- 6 **다음**을 클릭합니다.
- 7 워크플로의 **구성** 단계에서는 구독에 대한 구성 옵션을 선택합니다. 구독하는 솔루션 또는 서비스에 따라 구독 구성 단계에서 다음을 선택하도록 요청할 수 있습니다.
 - 버전 및/또는 지역.
 - 약정 수량, 청구 빈도 및 약정 기간.
페이지의 **주문 요약** 섹션에는 최근 선택 사항을 기반으로 구독의 정보와 비용이 표시됩니다.
- 8 구독 구성을 완료했으면 **저장**을 클릭합니다.
- 9 구독 구성을 변경하거나 삭제하려면 **구성** 단계의 **제공** 섹션에서 **수정** 또는 **제거** 버튼을 사용하여 해당 작업을 수행할 수 있습니다.
- 10 구매 주문을 진행하려면 **다음**을 클릭합니다.
- 11 워크플로의 마지막 단계에서 구매 주문 요약 및 지불 요약을 검토하고 지불 방법을 선택합니다.

12 구독 생성을 클릭합니다.

13 팝업 창이 열리면 생성을 클릭하여 구매를 확인합니다.

결과

화면에 구독 주문 구매 요청 확인이 표시됩니다. 구매 주문이 처리되고 새 구독이 활성화될 때까지 다소 시간이 걸릴 수 있습니다. 그 후에는 조직의 **구독** 페이지에서 구독 세부 정보를 볼 수 있습니다.

구독을 확장하는 방법

조직 소유자는 조직에서 선택한 구독의 용량을 확장할 수 있습니다.

참고 현재 VMware Tanzu Service Mesh만 이 기능을 사용하고 있으며 VMware 구독을 구매한 경우에만 사용할 수 있습니다.

사전 요구 사항

- 확장할 구독을 VMware에서 구매했습니다.
- 조직에서 **조직 소유자** 역할이 있습니다.

절차

- 1 Cloud Services 콘솔에 로그인하고 **청구 및 구독 > 구독**으로 이동합니다.
- 2 확장할 구독을 찾고 구독 ID 앞에 있는 세로 말줄임표 아이콘(⋮)을 클릭한 다음 **확장**을 클릭합니다.
- 3 구독에 대한 새 수량을 입력하고 **저장**을 클릭합니다.
주문 요약 섹션에는 최근 선택 사항을 기반으로 구독의 정보와 비용이 표시됩니다.
- 4 선택한 수량을 변경하려면 **수정**을 클릭하고 새 값을 입력합니다.
- 5 구독 확장을 확인하려면 **다음**을 클릭합니다.
- 6 워크플로의 마지막 단계에서 구매 주문 요약 및 지불 요약을 검토하고 지불 방법을 선택합니다.
- 7 **구독 생성**을 클릭합니다.

결과

화면에 구독 주문 구매 요청 확인이 표시됩니다. 구매 주문이 처리되고 구독 변경이 활성화될 때까지 다소 시간이 걸릴 수 있습니다. 그 후에는 조직의 **구독** 페이지에서 구독 세부 정보를 볼 수 있습니다.

조직에 약정을 적용해야 하는 이유

서로 다른 VMware Cloud Services에 대해 여러 구독을 구매하고 각 구독에 대해 여러 기간 약정을 구매할 수 있습니다. 각 구독은 하나의 조직에서 사용할 수 있습니다. 둘 이상의 VMware Cloud services 조직이 있는 경우 새로 구매한 약정을 원하는 조직에 적용할 수 있습니다.

약정을 구매하는 경우 판매 제안에 용량, 기간 및 협상 가격이 요약됩니다. **조직 소유자**인 사용자는 구매가 완료된 후 새 조직 또는 기존 조직에 약정을 적용합니다. 이렇게 하려면 새 약정에 대한 링크를 열고 워크플로의 단계를 따릅니다.

특정 조직과 연결되면 해당 기간이 만료될 때까지 해당 조직의 멤버가 약정을 사용할 수 있습니다.

구독 갱신 기본 설정을 변경하는 방법

조직 소유자인 사용자는 Cloud Services 콘솔의 **구독 세부 정보** 페이지에서 구독에 대한 갱신을 관리합니다.

조직의 각 구독에는 구독이 만료되기 최대 30일 전에 변경할 수 있는 기본 갱신 기본 설정이 있습니다.

중요 **구독 세부 정보** 페이지에는 구매한 구독에서 지원하는 갱신 기본 설정 옵션만 표시됩니다. 아래에 나열된 갱신 기본 설정 중 하나라도 누락된 경우에는 현재 구독에 사용할 수 없다는 의미입니다.

갱신 기본 설정 상태	결과...
자동 갱신	구독이 자동으로 갱신되며 추가 입력이 필요하지 않습니다.
수동 갱신	갱신 날짜 전에 고객 영업 담당자가 연락을 드려서 갱신 세부 사항을 논의합니다. 지원 요청을 제출하여 갱신 옵션에 대해 문의할 수도 있습니다.
갱신 기본 설정을 갱신 취소 로 변경하여 구독이 갱신되기 전에 구독을 취소할 수도 있습니다.	구독이 갱신되기 전에 취소할 수도 있습니다. 이 경우 만료 날짜가 지나면 조직은 구독에 대한 사용 권한을 상실합니다.

사전 요구 사항

조직 소유자 역할이 있어야 합니다.

절차

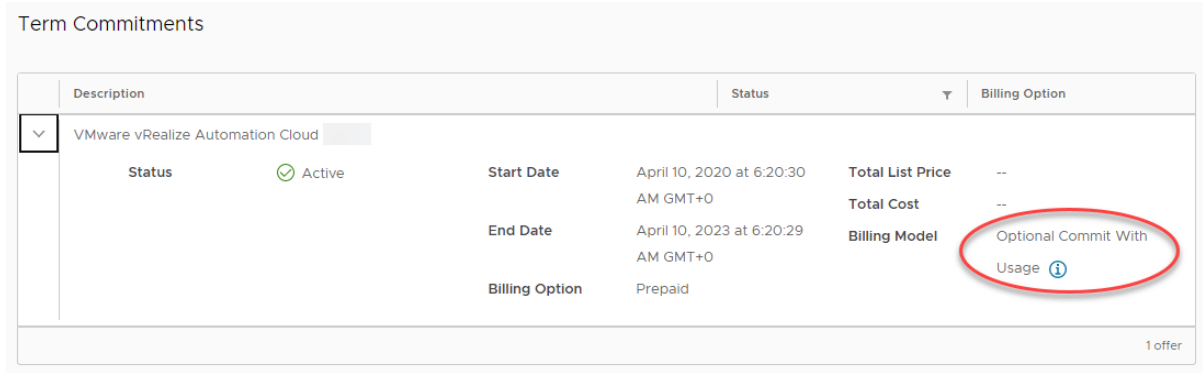
- 1 Cloud Services 콘솔에 로그인한 다음 **청구 및 구독 > 구독**으로 이동합니다.
- 2 표시되는 구독 목록에서 구독 ID를 클릭합니다.
그러면 **구성 세부 정보** 페이지가 열립니다.
- 3 **갱신 기본 설정** 섹션에서 **변경**을 클릭합니다.
- 4 구독에 대한 새 기본 갱신 기본 설정을 선택하고 **확인**을 클릭합니다.

청구 모델이란?

VMware Cloud Services는 세 가지 다른 청구 모델을 활용합니다. 구독에 대한 청구 모델은 조직 내에서 구매하고 사용하는 서비스 및 약정에 대해 조직에 요금이 부과되는 방식을 결정합니다.

청구 모델 정보는 구독에 대한 **기간 약정** 세부 정보의 일부로 표시됩니다.

- 1 Cloud Services 콘솔에 로그인하고 **청구 및 구독 > 구독**으로 이동합니다.
- 2 구독의 ID를 클릭하여 세부 정보 페이지를 연 다음 **기간 약정** 섹션을 확장합니다.



참고 VMware를 통해 구매한 구독에 대해서만 청구 모델을 볼 수 있습니다.

다음 표에는 세 가지 청구 모델 간의 차이점이 설명되어 있습니다.

	약정 전용	선택적 사용량 약정	필수 사용량 약정
설명:	서비스를 활용하려면 구독을 구매해야 합니다.	서비스 사용을 시작하기 위해 구독이 필요하지 않지만 주문형 사용량이 발생할 수 있습니다.	서비스를 활용하려면 구독을 구매해야 하며 초과 사용량에 대해 요금이 부과될 수 있습니다.
기본 지불 방법:	필요하지 않음	필수	필요하지 않음
비용 결정 기준:	약정	약정 + 주문형 사용량(있는 경우)	약정 + 초과 사용량(있는 경우)

[사용량 관리] 대시보드를 사용하는 방법

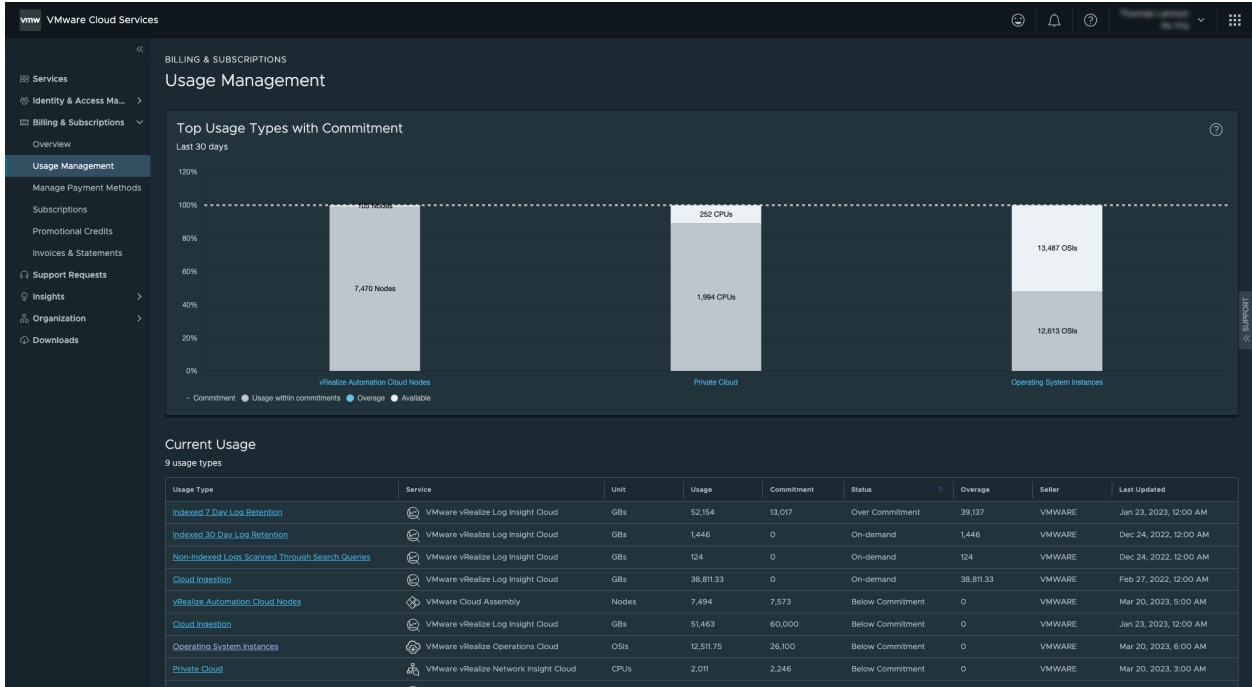
조직 소유자인 사용자는 Cloud Services 콘솔의 **사용량 관리** 대시보드를 통해 조직의 서비스가 시간대별로 사용 유형에 따라 어떻게 사용되는지 추적할 수 있습니다.

참고 일부 VMware Cloud services에서는 사용량 관리를 사용할 수 없습니다. 현재 사용량에 대한 데이터를 제공하는 서비스에는 VMware Cloud on AWS, VMware Aria Operations for Networks, VMware Aria Operations, VMware Aria Operations for Logs, VMware Aria Automation, VMware Cloud Disaster Recovery, VMware Cloud Director, VMware Lab Platform이 있습니다.

다음 비디오에서 사용량 관리 기능에 대한 개요를 볼 수 있습니다.



청구 및 구독 > **사용량 관리**로 이동하여 **사용량 관리** 대시보드에 액세스합니다.

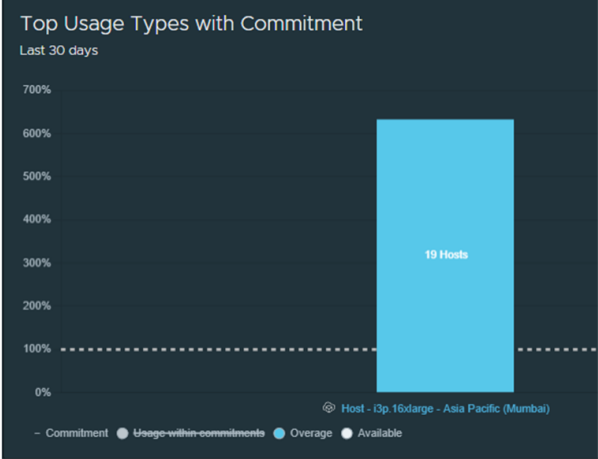
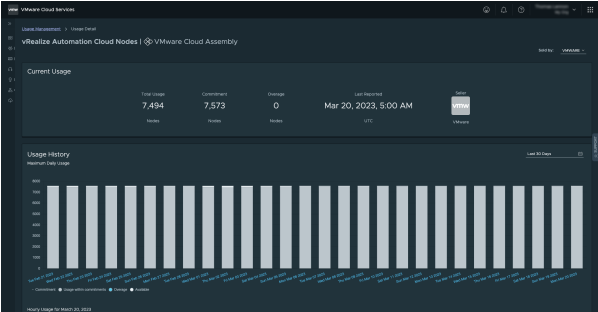


사용량 데이터는 두 가지 섹션 즉, 지난 30일 동안 조직의 상위 사용량 유형을 보여주는 차트와 조직 내 모든 사용 유형의 현재 사용량에 대한 세부 정보를 보여주는 테이블로 구성됩니다.

VMware Cloud services는 다양한 사용 유형을 사용합니다. 사용 유형은 조직에 프로비저닝된 특정 서비스를 기반으로 하며 서비스에 대한 약정된 용량을 측정하는 데 사용되는 단위를 포함합니다. 가장 일반적으로 사용되는 단위는 코어, 호스트, vCPU, CPU 및 OS입니다. 다음은 사용 유형의 몇 가지 예입니다.

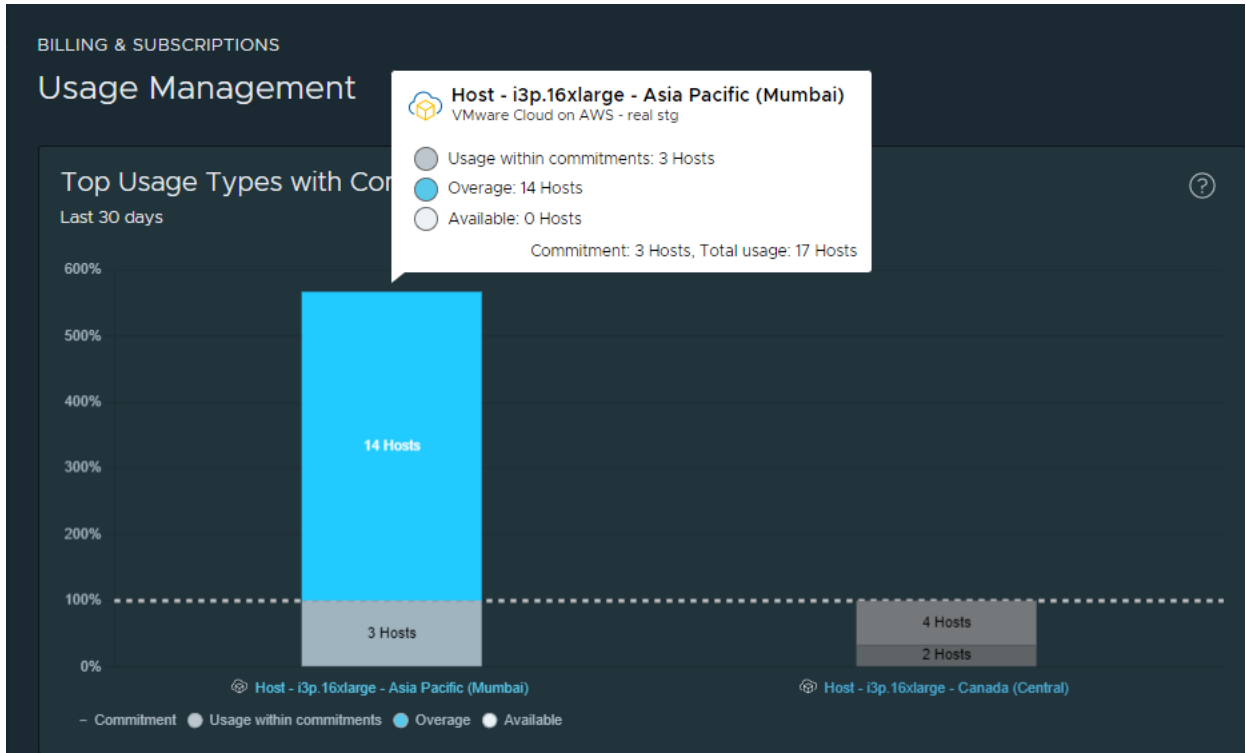
- Operating System Instances
- Cloud Director Cores
- Host - r.5metal - Europe (Ireland)

원하는 작업	수행할 단계
상위 사용량 유형 작업에 대해 자세히 알아봅니다.	[상위 약정 사용량 유형] 차트에 대해 알아두어야 할 사항의 내용을 참조하십시오.
현재 사용량 작업에 대해 자세히 알아봅니다.	현재 사용량 테이블에 대해 알아두어야 할 사항의 내용을 참조하십시오.

원하는 작업	수행할 단계
<p>용량을 기준으로 사용량을 필터링합니다(예: 약정 사용량, 초과분 또는 사용 가능한 약정).</p>	<p>사용량 관리 대시보드의 상위 약정 사용량 유형 섹션에서 보기에서 제외하려는 정보에 해당하는 차트 아래의 레이블을 클릭합니다. 예를 들어 상위 사용량 유형에 대한 초과분만 보려면 약정 사용량 레이블을 클릭합니다. 레이블에 줄이 그어지면 보기가 새로 고쳐지고 초과분의 사용 유형만 표시됩니다.</p> 
<p>사용 유형별 현재 사용량 및 기간별 사용량을 봅니다.</p>	<p>현재 사용량 및 기간별 사용량 세부 정보를 보려는 사용 유형 링크를 클릭합니다. 사용 유형이 상위 약정 사용량 유형 섹션에 있는 경우 링크가 그래프의 해당 막대 바로 아래에 있습니다. 사용 유형이 현재 사용량 섹션에 나열되면 사용 유형 열에서 링크를 찾을 수 있습니다. 선택한 사용 유형에 대한 현재 사용량 및 기간별 사용량 보기를 보여주는 페이지가 열립니다.</p>  <p>현재 사용량 및 기간별 사용량에 대해 자세히 알아보려면 현재 사용량 및 기간별 사용량 세부 정보에 대해 알아두어야 할 사항에서 참조하십시오.</p>

[상위 약정 사용량 유형] 차트에 대해 알아두어야 할 사항

사용량 관리 대시보드의 **상위 약정 사용량 유형** 차트에는 지난 30일 동안 조직 내 상위 사용량 유형에 대한 최고 사용량 요약이 약정 백분율로 정렬하여 표시됩니다.



약정은 구독을 통해 조직에서 구매한 단위 수입니다. 수평 점선은 100% 약정 수준을 표시합니다. 이 선 아래의 막대는 해당 서비스 및 사용량 유형에 대한 활용도가 낮다는 것을 나타냅니다. 막대의 파란색 부분은 약정을 초과하여 사용량을 줄이거나 추가 약정 구매를 고려할 수 있음을 나타냅니다. 차트에서 조직의 사용량이 약정을 초과한 단위 수는 초과로 표시됩니다.

현재 사용량 테이블에 대해 알아두어야 할 사항

현재 사용량 테이블은 Cloud Services 콘솔에서 사용량 관리 대시보드의 기본 상위 약정 사용량 유형 섹션 아래에 있습니다.

Usage Type	Service	Unit	Usage	Commitment	Status	Overage	Seller	Last Updated
Indexed 7 Day Log Retention	VMware vRealize Log Insight Cloud	GBs	52,154	13,017	Over Commitment	39,137	VMWARE	Jan 23, 2023, 12:00 AM
Indexed 30 Day Log Retention	VMware vRealize Log Insight Cloud	GBs	1,446	0	On-demand	1,446	VMWARE	Dec 24, 2022, 12:00 AM
Non-Indexed Logs Scanned Through Search Queries	VMware vRealize Log Insight Cloud	GBs	124	0	On-demand	124	VMWARE	Dec 24, 2022, 12:00 AM
Cloud Ingestion	VMware vRealize Log Insight Cloud	GBs	38,811.33	0	On-demand	38,811.33	VMWARE	Feb 27, 2022, 12:00 AM
vRealize Automation Cloud Nodes	VMware Cloud Assembly	Nodes	7,494	7,573	Below Commitment	0	VMWARE	Mar 20, 2023, 5:00 AM
Cloud Ingestion	VMware vRealize Log Insight Cloud	GBs	51,463	60,000	Below Commitment	0	VMWARE	Jan 23, 2023, 12:00 AM
Operating System Instances	VMware vRealize Operations Cloud	OSs	12,511.75	26,100	Below Commitment	0	VMWARE	Mar 20, 2023, 6:00 AM
Private Cloud	VMware vRealize Network Insight Cloud	CPUs	2,011	2,246	Below Commitment	0	VMWARE	Mar 20, 2023, 3:00 AM
Non-Indexed 6 Month Log Retention	VMware vRealize Log Insight Cloud	GBs	52,150	60,000	Below Commitment	0	VMWARE	Jan 23, 2023, 12:00 AM

이 테이블에는 조직에 프로비저닝된 서비스의 사용 유형에 대한 개략적인 사용량 세부 정보가 제공됩니다. 다음은 각 테이블 열에서 찾을 수 있는 정보에 대한 자세한 설명입니다.

범	설명
사용 유형	조직에서 프로비저닝된 특정 서비스에 대한 사용량 및 해당 서비스의 약정된 용량을 측정하는 데 사용되는 단위입니다. 예: Host - r5.metal - US West Oregon 사용 유형은 링크로 표시됩니다. 링크를 클릭하면 선택한 사용 유형에 대한 현재 사용량 및 기간별 사용량을 보여주는 세부 정보 페이지가 열립니다.
서비스	특정 사용 유형이 연결된 클라우드 서비스입니다. 예: VMware Cloud on AWS.
단위	특정 사용 유형에 대한 측정 단위를 나타냅니다. 예를 들어 호스트, 코어, GB(스토리지), IP/EIP, CPU/vCPU 등이 있습니다.
사용	보고 시점에 사용 중인 실제 사용량을 나타냅니다. 현재 사용 중인 단위 수입입니다.
약정	조직에서 구독을 통해 구매한 단위 수입입니다.
상태	사용량 상태에 대한 요약을 나타냅니다. 옵션은 다음과 같습니다. <ul style="list-style-type: none"> ■ 약정 초과: 사용량이 약정을 초과하는 경우. ■ 요청 시: 약정이 없는 사용 유형에 대한 사용량이 있는 경우. ■ 약정과 동일 또는 약정 미만: 일부 서비스는 사용량이 약정 이하일 때 데이터가 없습니다. 이 상태는 구매 용량 이하로 소비하고 있음을 나타냅니다. 사용 중인 구체적인 수량은 표시되지 않습니다.
초과	사용량이 약정을 얼마나 초과했는지 나타냅니다.
판매자	구독을 구매한 판매자를 나타냅니다. 사용량에 대해 청구될 수 있는 초과 소비를 표시할 수 있습니다.
마지막 업데이트 날짜	데이터를 마지막으로 가져온 시점의 타임 스탬프를 나타냅니다.

현재 사용량 데이터를 다운로드하는 방법

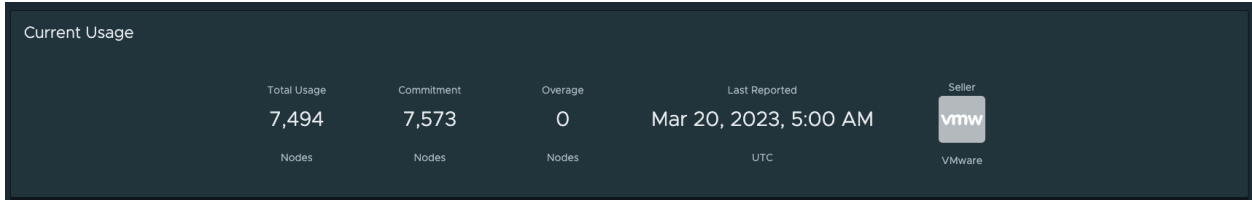
현재 사용량 테이블의 왼쪽 상단에서 **내보내기** 버튼을 클릭하여 조직의 현재 사용량 데이터가 포함된 CSV 파일을 다운로드할 수 있습니다.

현재 사용량 및 기간별 사용량 세부 정보에 대해 알아두어야 할 사항

조직의 **사용량 관리** 대시보드에 표시된 각 사용 유형에 대해 현재 사용량 및 기간별 사용량 세부 정보를 볼 수 있습니다. 세부 정보를 열려면 사용 유형 링크를 클릭합니다.

현재 사용량

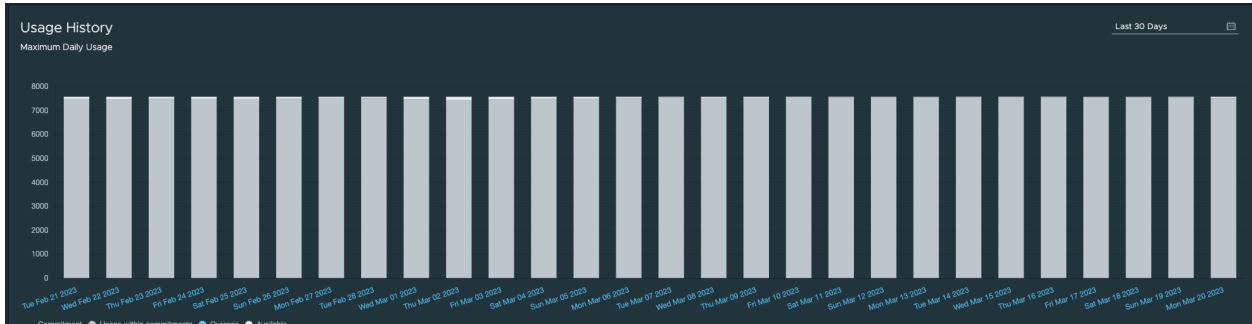
현재 사용량 대시보드에는 몇 가지 기본 세부 정보에 대한 개략적인 보기가 표시됩니다.



- **총 사용량**은 총 사용량 단위 및 사용량 메트릭 유형을 표시합니다. 예: 7,494 Nodes
- **약정**은 특정 서비스 구독의 사용량에 약정된 단위를 표시합니다. 예: 7,573 Nodes
- **초과**는 실제 사용량이 약정 사용량을 초과하는 경우 표시되며 그 차이가 단위 값으로 반영됩니다.
- **마지막 보고**는 현재 사용 유형 세부 정보가 마지막으로 업데이트된 타임 스탬프를 표시합니다.
- **판매자**는 구독 사용 유형의 판매자를 나타냅니다.

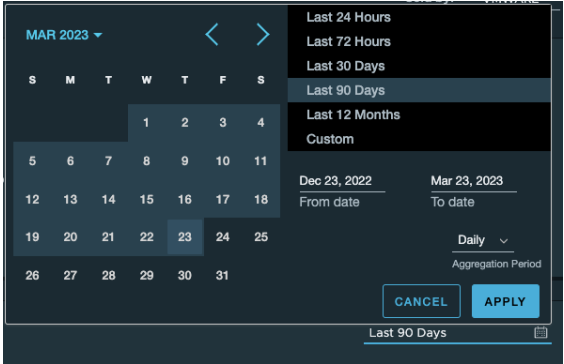
사용량 기록

사용량 기록 보기에는 미리 정의된 기간 동안의 최대 일별 사용량과 특정 날짜의 시간별 사용량이 표시됩니다.



- **최대 일별 사용량** 보기의 세로 축은 사용량 메트릭과 단위 양을 나타냅니다.
- 가로 축은 차트에 표시되는 데이터의 시간 프레임을 나타냅니다.

현재 사용량 및 기간별 사용량 보기로 작업하는 방법

원하는 작업	수행할 단계
<p>사용량에 대한 자세한 정보를 봅니다.</p>	<p>차트 막대 위로 마우스 커서를 가져갑니다. 볼 수 있는 항목:</p> <ul style="list-style-type: none"> ■ 차트의 타임 스탬프. ■ 약정 내 사용량: 당시 사용하던 약정을 통해 사용 가능한 단위 수입니다. ■ 초과: 해당 시점에 초과가 발생한 단위 수, 초과액 백분율 결과입니다. ■ 사용 가능: 해당 시점에 사용할 수 있는 단위 수입니다.
<p>최대 일별 사용량 차트 기간을 수정합니다.</p>	<p>1 최대 일별 사용량 차트의 오른쪽 상단 모서리에 있는 일정 아이콘을 클릭합니다.</p> <p>이 보기의 기본 기간은 30일입니다. 최대 일별 사용량 데이터를 필터링할 수 있는 최소 기간은 24시간입니다. 최대 기간은 2년입니다.</p>  <p>2 기간 설정을 변경하고 적용을 클릭합니다.</p>

원하는 작업	수행할 단계
<p>특정 날짜에 대한 시간별 사용량 차트를 봅니다.</p>	<p>최대 일별 사용량 차트에서 날짜 표시줄을 클릭합니다. 시간별 사용량 차트가 새로 고쳐지고 선택한 날짜의 사용량에 대한 시간별 분석이 표시됩니다.</p>  <p>참고 시간별 사용량 데이터는 지난 30일에 대해서만 제공됩니다.</p>
<p>시간별 사용량을 테이블 형식으로 봅니다.</p>	<p>시간별 사용량 차트 바로 아래에 있는 테이블에서 시간별 사용량에 대한 분석을 볼 수 있습니다.</p>  <p>날짜 옆에 있는 이중 화살표 아이콘을 클릭하면 확장된 시간별 사용량 보기가 다음 열 아래에 구성되어 표시됩니다.</p> <ul style="list-style-type: none"> ■ 시간: 데이터가 참조하는 하루 중 특정 시간입니다. ■ 약정: 조직이 구독을 통해 약정한 수량을 나타냅니다. ■ 약정 내 사용량: 조직 약정의 일부로 간주되는 실제 사용량을 나타냅니다. ■ 초과 사용량: 조직의 약정을 벗어나 초과분으로 간주되는 사용량을 나타냅니다. ■ 총 사용량: 조직의 약정 내 사용량과 초과분을 모두 합친 전체 사용량을 나타냅니다. ■ 단위: 선택한 사용 유형(예: 호스트/IP/EIP/CPU/vCPU 등)에 적용 가능한 메트릭입니다.

다음 비디오는 확대/축소 기능을 사용하는 방법을 보여 줍니다.



(Cloud Services 콘솔 - 사용량 관리 확대/축소 기능)

사용량 관리 FAQ

이 항목에서는 Cloud Services 콘솔의 **사용자 관리** 대시보드 관련 FAQ(자주 묻는 질문)에 대해 설명합니다.

Q: 내 구매가 [사용량 관리] 페이지에 표시되지 않는 이유는 무엇입니까?

A: 모든 사용량 데이터는 매일 처리됩니다. 서비스 사용이 발생한 시점에 따라 이 보고서에 표시되는 데 최대 48시간이 걸릴 수 있습니다. 일부 서비스는 월별로 데이터를 제공합니다.

Q: 사용량이 지연되는 이유는 무엇입니까?

A: 모든 사용량 데이터는 매일 처리됩니다. 서비스 사용이 발생한 시점에 따라 이 보고서에 표시되는 데 최대 48시간이 걸릴 수 있습니다. 일부 서비스는 월별로 데이터를 제공합니다.

Q: 비용 정보를 찾으려면 어떻게 합니까?

A: 사용 명세서를 통해 서비스에 대한 요금을 볼 수 있습니다. 자세한 내용은 [내 사용 명세서를 읽는 방법](#)의 내용을 참조하십시오.

Q: 내 사용량 데이터를 볼 수 없습니다. 이유

A: 일부 VMware Cloud services에서는 사용량 관리를 사용할 수 없습니다. 현재 사용량에 대한 데이터를 제공하는 서비스에는 VMware Cloud on AWS, VMware Aria Operations for Networks, VMware Aria Operations, VMware Aria Operations for Logs, VMware Aria Automation, VMware Cloud Disaster Recovery, VMware Cloud Director, VMware Lab Platform이 있습니다. 서비스가 지원되는 경우 서비스 사용이 발생한 시점에 따라 이 보고서에 표시되는 데 최대 48시간이 걸릴 수 있습니다. 일부 서비스는 월별로 데이터를 제공합니다.

Q: 사용량 데이터를 볼 수 있는 기간은 얼마나 됩니까?

A: 대시보드에 표시되는 기본 기간은 30일입니다. 최대 일별 사용량 데이터를 필터링할 수 있는 최소 기간은 24시간입니다. 최대 기간은 2년입니다. 차트는 지정된 시간에 최대 1년 동안의 데이터를 표시합니다.

Q: 시간별 데이터가 표시되지 않습니다. 이유

A: 시간별 데이터는 지난 30일에 대해서만 제공됩니다. 그 이전에 대해서는 일별 데이터만 사용할 수 있습니다.

내 사용량 데이터와 청구서가 일치하지 않습니다. 이유

A: 대부분의 서비스 청구는 청구 기간 동안 발생한 시간 단위 초과분의 합계를 기반으로 합니다. 이 차트에는 지정된 시간의 실제 사용량과 지정된 날짜의 최대 사용량이 표시됩니다.

Q: 상위 사용량 차트가 표시되지 않습니다. 이유

A: **상위 사용량** 차트는 약정이 있는 서비스에 대해 지난 30일 동안 발생한 사용량만 표시합니다. 적격 사용량이 있는 서비스가 없으면 차트가 아예 표시되지 않습니다. 사용량이 표시되지 않을 수 있는 이유에는 몇 가지가 있습니다.

- 모든 사용량이 주문형 서비스에 대한 것입니다. 주문형 사용량은 상위 사용량 차트에 표시되지 않습니다.
- 사용량이 사용량 관련 데이터를 제공하지 않는 서비스에 대한 것입니다.
- 사용량이 발생한지 30일이 넘었습니다.

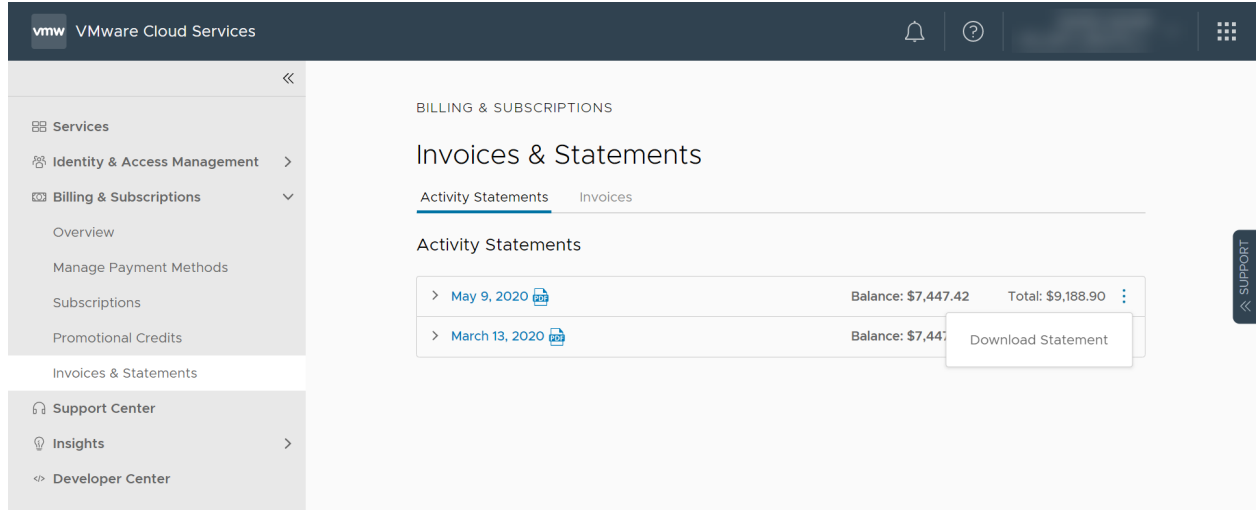
명세서 및 송장을 보는 방법

조직 소유자인 사용자는 마지막 15개의 사용 명세서, 요청 시 송장 및 연 단위 약정 송장을 보고 인쇄할 수 있습니다.

Cloud Services 콘솔에서 **청구 및 구독 > 송장 및 청구서**를 선택하여 청구서 및 송장을 봅니다.

사용 명세서

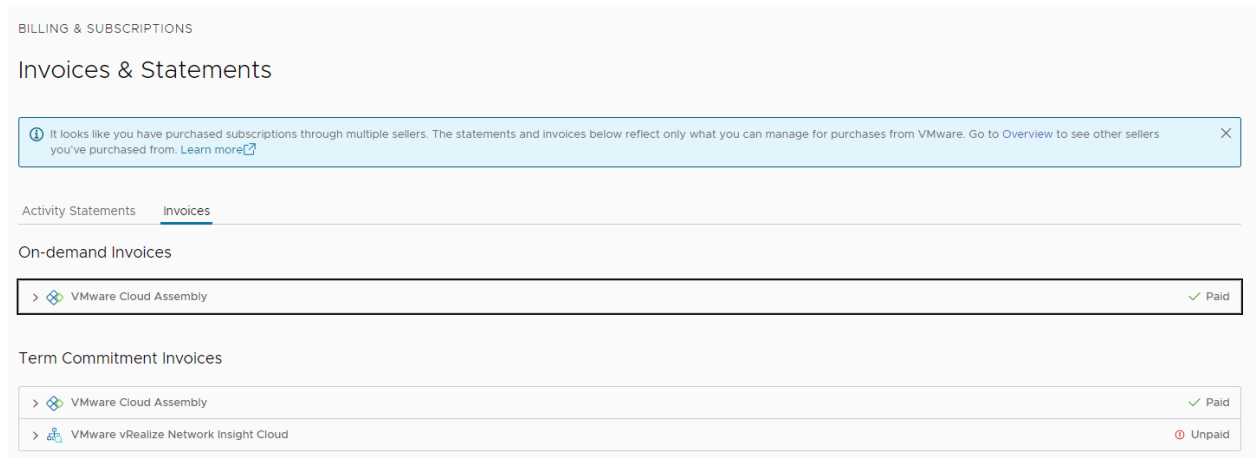
사용 명세서 페이지에는 주어진 청구 기간 동안 소비된 모든 서비스에 대한 월별 요약이 표시됩니다. 각 사용 명세서는 청구 금액에 대한 지불 내역, 프로모션 크레딧 및 잔고에 대한 요약을 제공합니다. 해당 링크를 클릭하거나 옆에 있는 세로 말줄임표 아이콘에서 옵션을 선택하여 사용 명세서를 보고 다운로드합니다.



송장

송장에 액세스하려면 **송장 및 청구서** 페이지에서 **송장** 탭을 클릭합니다.

- 페이지의 **요청 시 송장** 섹션에는 주문형 구독에 대한 청구 비용이 나열됩니다.
- **기간 약정 송장** 섹션에는 구독의 기간 약정에 대한 송장이 나열됩니다.



송장 링크를 클릭하거나 옆에 있는 세로 줄임표 아이콘(⋮) 메뉴에서 **다운로드**를 선택하여 송장을 다운로드합니다.

내 사용 명세서를 읽는 방법

조직 소유자인 사용자는 특정 청구 기간에 대한 사용 명세서에서 해당 청구 기간 동안 조직에서 사용한 모든 서비스에 대한 세부 정보를 볼 수 있습니다. 사용 명세서는 송장이 아닙니다.

사용 명세서에 포함된 내용

각 사용 명세서는 청구 기간에 발생한 모든 서비스 요금과 서비스 요금에 대한 지불 내역에 대한 요약 및 세부적인 분석을 제공합니다.

청구 기간 요약

[청구 기간 요약]은 청구 기간에 대한 총 요금, 크레딧, 할인, 조정 및 지불에 대한 개요입니다. [잔액]은 현재 기간에 지불되지 않은 요금을 표시하며 [미결 잔액]은 이전 청구 기간에 지불되지 않은 잔액을 표시합니다.

참고 사용 명세서의 명세서 생성 날짜 이후에 이루어진 지불은 사용 명세서에 반영되지 않습니다.

요금 분석

[요금 분석] 섹션에서는 조직의 각 서비스에 대해 발생한 요금을 시각적인 원형 차트로 표시합니다. 각 서비스에 대해 표시되는 금액은 요금에서 할인, 프로모션 및 조정 금액을 모두 공제한 후의 순 금액입니다. 이 차트는 조직에서 둘 이상의 서비스에 대해 요금이 부과된 경우에만 채워집니다.

요금 기록

둘 이상의 청구 기간에 걸쳐 요금이 부과된 경우, 최대 12개월 동안의 서비스별 요금 내역이 포함된 선형 그래프가 [요금 기록] 섹션에 표시됩니다. 각 서비스에 대해 표시되는 금액은 요금에서 할인, 프로모션 및 조정 금액을 모두 공제한 후의 순 금액입니다.

서비스 요금

[서비스 요금]에는 청구 기간 내에 발생한 요금 및 크레딧과 해당 요금에 적용되는 모든 지불이 포함됩니다. 크레딧에는 각 서비스에 대해 이루어진 모든 할인, 프로모션 및 조정이 포함되며 금액 앞에 빼기 기호가 표시됩니다. [서비스 요금]은 기간 약정이 있는 서비스, 주문형 서비스 및 서비스 사용량과 관련하여 추가 요금이 있는 서비스에 대한 것일 수 있습니다. 기간 약정, 주문형 사용량 및 기타 요금 소계는 라인별로 표시되고, 그 뒤에 지불 및 현재 잔액이 표시됩니다. 지불에는 모든 할인, 프로모션 및 서비스별 조정이 포함됩니다.

주문형 세부 정보

조직에서 사용하는 주문형 서비스에 대한 모든 요금은 [주문형 세부 정보] 섹션에 반영됩니다. 요금은 조직에서 주문형 서비스를 사용한 경우에 한하여 사용된 시간에 대해서만 발생합니다.

기타 요금 세부 정보

조직에서 발생하는 데이터 전송, Direct Connect, EBS, Elastic IP 요금 및 가입 크레딧과 같은 추가 요금은 기타 요금 아래에 표시됩니다. 요금은 고유 지역 및 SID(구독 ID)별로 집계됩니다.

사용 명세서에 사용되는 약어 용어집

사용 명세서에는 비용 계산에 영향을 주는 제품, 서비스 및 측정 단위의 약어가 표시됩니다. 아래 용어집은 명세서를 읽을 때 도움이 되는 빠른 참조를 제공합니다.

표 11-3. VMware Cloud Services 약어 용어집

제품 이름	측정 단위	측정 단위 설명
vRealize Automation Cloud	EA	각
	NDH	시간당 노드
vRealize Log Insight Cloud	EA	각
	NDH	시간당 노드
	GB	기가바이트
vRealize Network Insight Cloud	CPU	중앙 처리 장치
	GB	기가바이트
	EA	각
	VCP	가상 중앙 처리 장치
NSX Cloud	CRM	월별 코어
	EA	각
Tanzu Application Catalog	EA	각
Tanzu Application Service	COH	계산 단위 시간
	EA	각
VMware Cloud Director	CRM	월별 코어
	EA	각
VMware SD-WAN by VeloCloud	EA	각
VMware Learning Platform	ALH	활성 랩 시간
	BIH	Bring Your Own Cloud
	COH	계산 단위 시간
	EA	각
	STH	스토리지 장치 시간
	WIH	Windows 장치 시간
VMware Cloud on AWS	ATG	GB당 첨부 파일
	ATH	시간당 첨부 파일

표 11-3. VMware Cloud Services 약어 용어집 (계속)

제품 이름	측정 단위	측정 단위 설명
	EA	각
	GB	기가바이트
	GBM	기가바이트 월
	HST	호스트
	HPH	시간당 호스트
	IPR	시간당 IP 주소
	IP	IP 주소
	VMH	시간당 가상 시스템
VMware Cloud on AWS GovCloud (US)	EA	각
	HPH	시간당 호스트
	IP	IP 주소
	VMH	시간당 가상 시스템
	ATH	시간당 첨부 파일
	ATG	기가바이트당 첨부 파일
	IPR	시간당 IP 주소
	GB	기가바이트
VMware Cloud on DELL EMC	EA	각
	NDM	월별 노드
	EDM	월별 Edge
vRealize Operations Cloud	EA	각
	OSI	운영 체제 인스턴스

송장에 PO 번호를 삽입하는 방법

송장에 대한 지불을 처리하려면 PO 번호와 같은 추가 정보를 송장에 포함해야 할 수도 있습니다. Cloud Services 콘솔의 **송장** 페이지에서 참조 정보를 추가하고 송장을 재인쇄합니다.

사전 요구 사항

송장이 생성된 조직에서 **조직 소유자** 역할이 있어야 합니다.

절차

- 1 Cloud Services 콘솔에 로그인하고 **청구 및 구독 > 송장 및 청구서 > 송장**으로 이동합니다.
- 2 재인쇄할 송장을 찾아서 옆에 있는 세로 줄임표(⋮) 아이콘을 클릭합니다.
- 3 메뉴가 열리면 **참조 번호 삽입**을 선택합니다.

참고 참조 번호 삽입 링크는 송장이 다운로드 가능한 PDF로 제공되고 아직 지불되지 않았으며 지불 방법이 신용 카드가 아닌 경우에만 사용할 수 있습니다. 송장이 재인쇄를 위해 이미 제출되었지만 업데이트된 송장을 아직 다운로드할 수 없는 경우에는 사용할 수 없습니다.

- 4 팝업 창이 열리면 송장에 포함하려는 PO 번호를 입력한 다음 **제출**을 클릭합니다.

중요 새 송장을 재생성하는 데 최대 24시간이 걸릴 수 있습니다. 송장이 재인쇄되면 이메일 알림을 받게 됩니다.

지원을 받는 방법

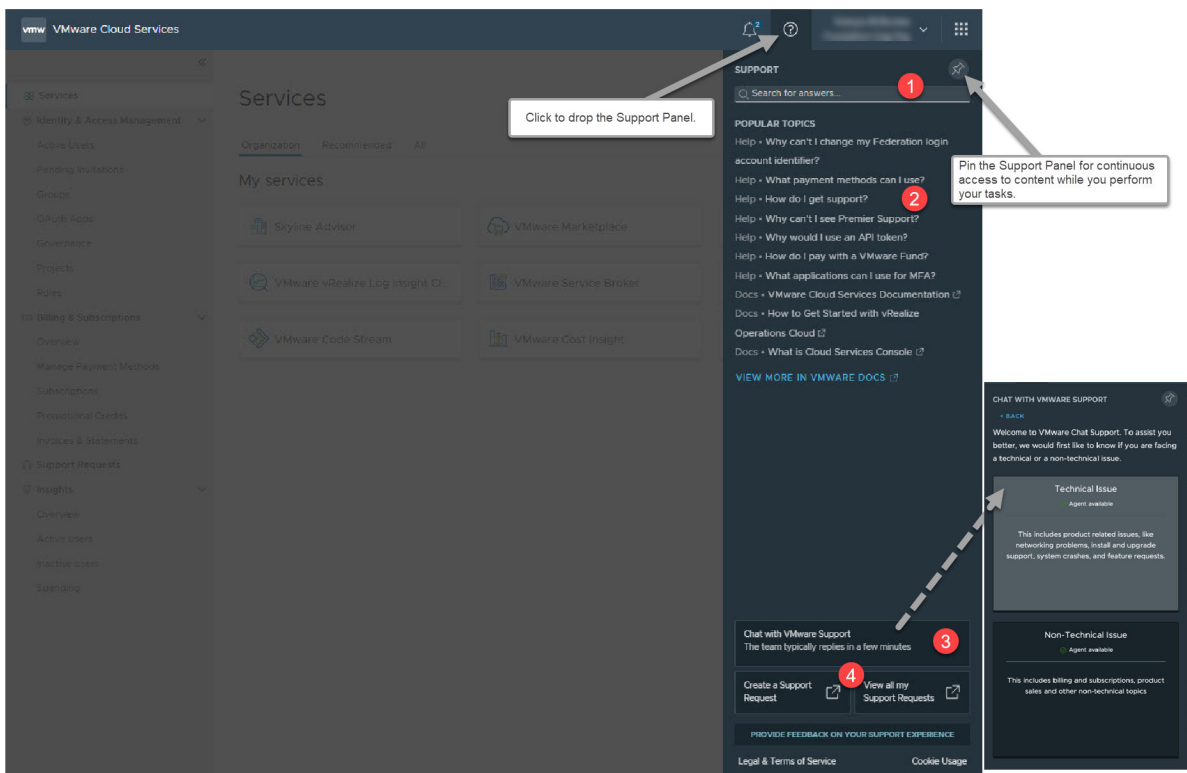
12

VMware Cloud services 제품 내 지원 환경에 오신 것을 환영합니다. 이 환경에서는 작업 수행에 도움이 되는 상황에 맞는 도움말 콘텐츠를 볼 수 있고, 질문에 대한 답변을 검색할 수 있고, 채팅을 원하는 경우에는 고객 지원 팀의 멤버에게 문의할 수 있습니다.

당사의 지원 환경은 모든 클라우드 서비스에 롤아웃되고 있는 새로운 기능을 통해 계속해서 진화하고 있습니다. 현재 지원 패널에서 다음 기능 중 일부 또는 전부를 볼 수 있습니다.

절차

- 1 메뉴에서 **물음표** 아이콘을 클릭하거나 창의 오른쪽에 있는 **지원** 탭을 클릭하여 지원 패널을 엽니다.



- 2 필요한 지원 수준에 액세스합니다.

지원 패널에는 상황에 맞는 도움말 콘텐츠와 강력한 검색 기능이 제공되기 때문에 지원 팀에 문의하지 않고도 많은 콘텐츠를 검색하고 질문에 답변할 수 있습니다. 고객 지원 담당자와 채팅하고 싶은 경우, 채팅하는 동안에도 클라우드 서비스와 계속 상호 작용할 수 있습니다.

액세스할 수 있는 지원 기능	도움 내용
1. 인텔리전트 검색.	질문에 대한 답을 찾기 위해 당사의 콘텐츠를 검색합니다. 당사의 설명서, 특별히 작성된 도움말 항목, 커뮤니티 및 기술 자료 문서를 검색합니다.
2. 페이지 관련 콘텐츠.	<p>작업을 수행하는 데 도움을 받을 수 있습니다. 지원 패널을 열면 작업에 도움이 되는 정보가 충분히 포함된 페이지 관련 도움말 항목을 볼 수 있습니다. 원하는 방식으로 작업을 진행하는 동안 페이지를 이동하면 그에 따라 도움말 콘텐츠도 변경됩니다. 콘텐츠 목록에는 검색 결과도 표시됩니다. 검색 결과에는 더 많은 도움말 항목, 기술 자료 문서, 설명서 센터의 콘텐츠 및 커뮤니티의 콘텐츠도 포함됩니다.</p> <p>원하는 항목을 찾을 수 없는 경우 VMware Docs에서 더 보기를 클릭하면 보고 있는 페이지와 관련된 검색 또는 검색 항목을 입력한 경우 해당 항목과 관련된 검색을 수행할 수 있습니다. 검색 결과는 설명서 센터에 표시됩니다.</p>
3. VMware 지원과 채팅	<p>당사의 지원 엔지니어 및 고객 지원 담당자에게 문의할 수 있습니다. 다음은 실시간 지원 채팅에 대해 알고 있어야 하는 내용입니다.</p> <ul style="list-style-type: none"> ■ VMware 지원과 채팅을 시작하면 상황에 맞게 지원이 제공됩니다. 즉, Cloud Services 콘솔에서 VMware 지원과 실시간 채팅을 시작하면 Cloud Services 콘솔 관련 문제에 대한 도움을 받을 수 있습니다. 특정 서비스에 대한 채팅 지원에 액세스하려면 해당 서비스에 로그인한 후 채팅을 시작해야 합니다. ■ 고객 지원 엔지니어와 채팅하는 동안 Cloud Services 콘솔 또는 Cloud Services 콘솔과 계속 상호 작용할 수 있습니다. 브라우저 창의 오른쪽 모서리에 있는 지원 버튼(🔍)을 클릭한 다음 채팅으로 돌아가기 아이콘(🗨️)을 클릭하면 언제든지 채팅으로 돌아갈 수 있습니다. ■ 고객 지원 엔지니어는 지원 요청을 여는 데 도움을 줄 수도 있습니다. ■ 브라우저 및 VMware Cloud Services 프로파일에 대해 구성된 언어 설정에 따라 영어 또는 일본어로 온라인 지원을 받게 됩니다. ■ Cloud Services 콘솔에서 실시간 지원 채팅을 사용하는 경우: <ul style="list-style-type: none"> ■ 먼저 도움이 필요한 문제가 기술적 문제인지 아니면 비기술적 문제인지 선택해야 합니다. 이렇게 하면 적합한 고객 지원 담당자에게 요청을 전달할 수 있습니다. ■ 동시에 여러 지원 채팅을 사용할 수 없습니다. 새 문제에 대한 새 채팅을 열려면 현재 채팅을 닫아야 합니다. ■ 채팅 중에 채팅 창에서 직접 고객 지원 담당자에게 파일이나 스크린샷을 보낼 수 있는 옵션이 있습니다. <p>참고 활성 채팅 세션 중에 시간 초과 문제를 방지하려면 브라우저 창/탭을 포그라운드에서 열어 두는 것이 좋습니다.</p>
4. 지원 요청 생성/내 모든 지원 요청 보기.	지원 요청을 생성하고 관리할 수 있는 VMware Customer Connect 를 엽니다.

3 지원 요청을 관리하려면 Cloud Services 콘솔 메뉴에서 **지원 요청** 링크를 클릭합니다.

이제 VMware Customer Connect 포털을 통해 모든 지원 관련 기능을 사용할 수 있습니다.

a **지원 요청 생성**을 클릭합니다.

Customer Connect의 **VMware 지원** 페이지가 열립니다. 새 지원 요청 생성에 대한 자세한 지침은 [Customer Connect에서](#) 그리고 [Cloud Services 포털을 통해 지원 요청을 제출하는 방법을 참조하십시오](#).

지원 요청을 열기 전에 추가 서비스 관련 정보가 필요할 수 있습니다. 예를 들어 VMC on AWS에서 [SDDC에 대한 지원 정보가 필요할 수 있습니다](#).

b 조직에 대해 열려 있거나 닫힌 모든 지원 요청에 액세스하려면 **지원 요청 기록 보기**를 클릭합니다.

Customer Connect에서 **지원 요청 기록** 페이지가 열립니다.

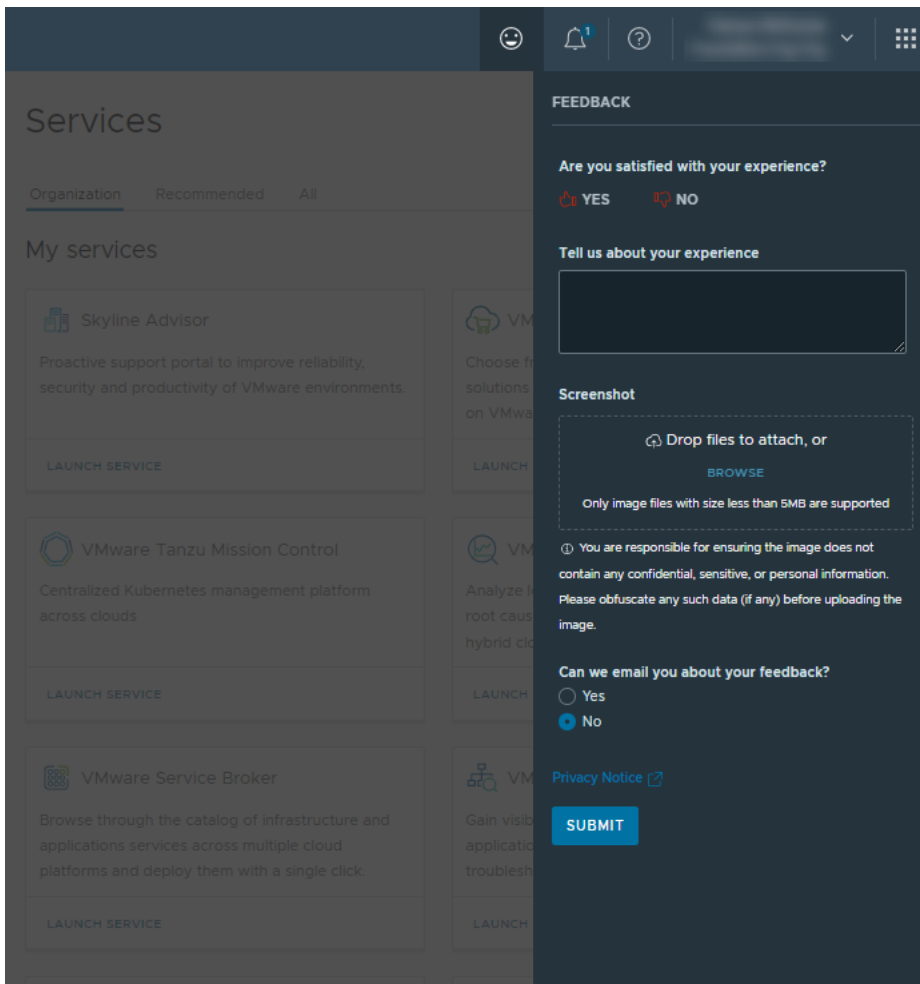
그러면 조직, 유형 및 기간별로 지원 요청을 필터링할 수 있습니다. 데이터를 정렬하고 내보낼 수도 있습니다.

피드백을 제공하는 방법

13

피드백은 제품을 개선하는 데 도움이 됩니다. 제품에서 직접 Cloud Services 콘솔에 대한 피드백을 제출할 수 있습니다.

- 1 Cloud Services 콘솔의 가로 메뉴에서 **피드백 제안** 아이콘(☺)을 클릭합니다.
피드백 패널이 열립니다.



- 2 사용 가능한 옵션 중 하나 이상을 사용하여 피드백을 제공합니다.
 - '좋아요' 또는 '싫어요' 아이콘을 사용하여 Cloud Services 콘솔 사용에 대한 만족도를 전달합니다.

- 텍스트 필드를 사용하여 경험을 좀 더 자세히 설명합니다.
- 피드백 메시지를 시각적으로 향상시키려면 **찾아보기**를 클릭하거나 지정된 필드에 이미지를 끌어다 놓아 스크린샷을 첨부합니다.
- 피드백과 관련하여 VMware Cloud Services 콘솔 팀과 더 연락을 원하시는지 알려주십시오.

3 **제출**을 클릭합니다.