使用 VMware Cloud Services 控制台

VMware Cloud services

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

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

威睿信息技术（中国）有限公司
北京办公室
北京市海淀区
科学院南路 2 号
融科资讯 C 座南楼 1 层
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

版权所有 © 2023 VMware, Inc. 保留所有权利。 版权和商标信息

目录

什么是 Cloud Services Console

1

通过 VMware Cloud Services 控制台，可以跨混合和原生公有云管理整个 VMware Cloud services 组合。

要了解如何管理用户和组、将角色分配给组织的资源和服务，以及查看有权访问您组织的 OAuth 应用程序，请参见身份与访问管理文档。

查找有关当前成本和上次结账单的信息？是否需要管理付款方式或更改默认付款方式？是否需要有关添加优惠额度和承付的信息？请参见我们的《计费和订阅》文档。

要了解如何管理组织、在组织中创建 OAuth 应用程序，并在您属于多个组织的情况下在组织之间切换，请参见管理组织。

是否要更改语言和区域格式、使用 MFA 保护您的帐户、生成 API 令牌，以及编辑您的用户配置文件？不进一步查看！请参见如何管理帐户。

如何注册 VMware Cloud Services 2

不管您需要迁移到云、统一多云操作、按需缩放还是构建现代应用程序，在 VMware Cloud 上都已涵盖。

可以通过多种方法开始使用 VMware Cloud services。作为新的或现有的 VMware Cloud services 用户，您可以通过执行以下操作之一来载入服务：

- 从 VMware 营销网站购买服务。
- 从 VMware 营销网站注册免费服务或试用服务。
- 从 VMware Sales 购买服务。
- 从 VMware 合作伙伴代理商处购买服务。

根据您要载入的服务不同，载入工作流可能会有所不同。

如果您的企业已使用 VMware Cloud services，您可以通过请求访问现有组织来将自己加入到该组织。请求和接收对 VMware Cloud services 组织的首次访问的过程可能因您的帐户而异。

- 如果您的帐户未联合，请参见如何作为 VMware Cloud Services 中的用户加入。
- 如果您的帐户已联合，请参见如何作为具有联合帐户的用户加入。

通过服务上线注册 VMware Cloud services 的典型步骤顺序如下所示：

步骤

1 从服务注册或您的邀请链接启动加入过程。

2 如果您没有 VMware 帐户，请按照以下步骤创建一个帐户。

3 如果您已有 VMware 帐户，请登录到 VMware Cloud Services。

4 创建或选择要载入服务的 VMware Cloud services 组织。

5 在组织中载入服务后，您将成为组织所有者，可以邀请其他用户以及授予对组织及其服务的访问权限：

   a 从左侧主菜单中，选择**身份与访问权限 > 活跃用户**。

   b 单击**添加用户**。

   c 加入要邀请的用户的电子邮件地址。

d 选择组织角色和服务角色。

e 选中要发送给新用户的电子邮件邀请的复选框，然后单击**添加**。

用户会收到一封邀请电子邮件，其中包含一个链接，供用户用于将自己以您为其分配的角色加入到组织中。

后续步骤

有关不同服务上线工作流的详细信息和详细过程，请参见 VMware Cloud Services 入门指南。

如何作为 VMware Cloud Services 中的用户加入

要开始以无权访问任何组织和非联合帐户的新用户身份使用 VMware Cloud Services，首先必须从**组织所有者**用户处获得对组织和服务的访问权限。

请求对 VMware Cloud Services 的初始访问权限是一个脱机过程，可由您或**组织所有者**启动。通常，在**组织所有者**向您授予组织中的组织角色和服务角色后，您会收到一封电子邮件，其中包含组织的链接。

1 单击**查看我的角色**链接可访问该组织。

2 如果您没有 VMware 帐户，系统会提示您创建一个帐户。

3 如果您已有 VMware 帐户，则可以登录到该组织，并根据您获得的组织角色和服务访问权限开始使用服务。

如果要请求获得组织中的其他角色，请参见如何请求其他角色。

如何作为具有联合帐户的用户加入

作为联合域的非组织用户，首次使用企业帐户登录到 VMware Cloud services 时会启动加入工作流。

在加入过程中，您可以自行选择组织、服务、组织角色和服务角色，以请求访问权限。您的请求必须经过**组织所有者**批准，这可能需要一些时间。

可在加入工作流中选择的组织是企业联合域中已激活身份监管和管理 (IGA) 的组织。如果您必须获取对未激活 IGA 的组织的访问权限，则需要从**组织所有者**向您发送邀请链接才能加入。

步骤

1 转到 https://cloud.vmware.com/，然后单击**登录**。

2 在 VMware Cloud services 欢迎屏幕中，键入您的企业帐户凭据。

加入工作流的第一步会显示与企业关联且激活了 IGA 的组织列表。

3 选择您要访问的组织，然后单击**继续**。

4 在所选组织中选择您的角色。

您的组织角色决定了您在组织中拥有的访问级别和权限。使用联合帐户加入时，只能请求默认的**组织成员**角色。载入后，可以请求其他角色。有关详细信息，请参见如何在激活了监管的组织中请求角色。

5 单击**继续**。

工作流的**选择服务角色**步骤会显示所选组织中可用的服务。

6 对于要作为**组织成员**访问的每个服务，请使用下拉列表选择服务角色。

注 服务角色特定于服务。如果不确定您需要哪些服务角色，请查看要访问的服务的文档。

7 单击**继续**。

8 在载入工作流的**完成请求**步骤中，定义服务访问请求的时间段。

9 在**业务理由**文本框中，键入要发送给**组织所有者**的消息，然后单击**继续**。

您的请求会显示在**挂起的请求**列表中，等待**组织所有者**批准。

10 要请求访问联合域中另一个激活了 IGA 的组织，请单击**提交新请求**。

11 重复步骤 3 到 9。

后续步骤

可能需要一些时间才会收到所请求的组织角色和服务角色的批准。此时您才能访问 Cloud Services 控制台，以检查所提交请求的状态，取消您创建的请求或创建新请求。

如何登录 Cloud Services 控制台

3

作为 VMware Cloud Services 用户，您可以使用 VMware 帐户凭据登录 Cloud Services 控制台。如果您的帐户已联合，则可以使用企业帐户凭据登录。

当用户登录 VMware Cloud Services 时，在成功进行身份验证后，将为该用户的登录会话生成访问令牌和刷新令牌。这两个令牌都使用 OAuth2.0 应用程序在后台生成，并具有默认的生存时间 (TTL) 值：

- 访问令牌的 TTL 为 30 分钟。
- 刷新令牌的 TTL 为 24 小时。

这意味着，成功登录后，访问令牌的有效期仅为 30 分钟。之后，该令牌将变为无效，可以使用刷新令牌重新生成访问令牌，以便用户可以继续登录会话。24 小时后，刷新令牌将过期，用户需要重新登录。

目前，无法修改访问令牌和刷新令牌的默认 TTL 值。

前提条件

- 您必须在一个或多个 VMware Cloud Services 组织中具有组织角色。

步骤

1. 打开浏览器窗口，并转到 https://console.cloud.vmware.com/。
2. 输入您的帐户电子邮件地址，然后单击**下一步**。
3. 键入密码，然后单击**登录**。

结果

成功登录后，VMware Cloud Services 主页将显示组织中可用的服务。

什么是 Cloud Services 组织

4

VMware Cloud 使用组织提供对一个或多个服务的受控访问。

作为使用多个云服务的企业，组织提供了一种简单的方法用于将业务组和流程映射到不同的组织。

可以使用 Cloud Services 控制台管理您的组织及其资源，例如：

- 用户和组角色和权限。
- 载入其他服务。
- 获取计费和订阅信息。
- 查看组织服务的使用情况数据。
- 在组织中设置身份验证策略。
- 审核事件日志。
- 获取支持。

您在组织中分配的组织角色决定了您对 Cloud Services 控制台中各功能的访问权限。您在组织中拥有的服务角色决定了您可以访问组织中的哪些可用 VMware Cloud services。您可以在多个组织中具有不同的角色。

如何使用 Cloud Services 目录

5

VMware Cloud Services 目录提供了一种简单的方法来查看、浏览、搜索或筛选满足特定条件的服务。

服务目录是在您登录到 Cloud Services 控制台时打开的第一个页面。每个目录项都由一个显示服务相关信息的单独卡视图表示。如果组织中有可用的服务，您可以单击服务卡视图上的链接来请求访问权限。

位置	可以执行的操作
服务 > **组织**选项卡	■ 在页面的**我的服务**部分下，您可以找到已为您分配其服务角色的所有服务。单击某个服务卡视图可启动该服务。 ■ **其他服务**部分提供了组织中没有为您分配其服务角色的所有服务的列表。 所有访问请求都必须由**组织所有者**批准。有关提交服务角色访问请求的信息，请参见如何请求其他角色。
服务 > **推荐**选项卡	请参见基于当前服务订阅的服务推荐列表。
服务 > **全部**选项卡	浏览或筛选完整的 VMware Cloud Services 目录。您可以按类别和定价模型筛选服务目录。
服务下的任何页面	使用页面右上角的**搜索服务**框按关键字查找相关服务。

请阅读以下主题：

- 我可以使用哪些服务目录操作
- 如何请求其他角色

我可以使用哪些服务目录操作

您可以直接从 VMware Cloud services 目录中的服务卡视图管理对 VMware Cloud services 的访问权限。可对给定服务执行哪些操作取决于您在组织中的角色以及要访问的服务类型。对于免费、试用和付费服务，可执行不同的操作。

组织成员操作

如果您有权访问...	且服务为...	您可以执行的操作是...	此操作的结果是...
服务	免费、活动试用或付费	**启动服务**	服务在 Cloud Services Console 中启动
	免费、活动试用或一个或多个服务实例付费	通过工具提示**启动服务**（如果有一个服务实例）	所选服务实例在 Cloud Services Console 中启动
		通过下拉菜单**启动服务**（如果有多个服务实例）	
组织，但无权访问服务	免费、活动试用或付费	**请求角色**	系统提示您为服务请求角色
无权访问服务，并且服务不在您的组织中	免费、活动试用或付费	**访问**	系统提示您启用服务
		了解更多	启动服务详细信息页面
	试用已过期	**了解更多**	打开服务详细信息或购买信息页面

组织所有者操作

如果您有权访问...	且服务为...	您可以执行的操作是...	此操作的结果是...
服务	免费或付费	**启动服务**	服务在 Cloud Services Console 中启动
	活动试用	**启动服务**	服务在 Cloud Services Console 中启动
		省略号图标 (•••) 中的**查看试用详细信息**	打开服务试用详细信息页面
		省略号图标 (•••) 中的**购买服务**	打开包含购买信息的页面
组织，但无权访问服务	免费、活动试用或付费	**访问**	系统提示您通过编辑角色来获取对服务的访问权限
		了解更多	启动服务详细信息页面
无权访问服务，并且服务不在您的组织中	免费、付费或试用付费	**访问**	系统提示您启用服务
	试用已过期 根据组织设置，将显示四个操作之一。	**购买服务**	打开包含购买信息的页面

如果您有权访问...	且服务为...	您可以执行的操作是...	此操作的结果是...
		确认付款方式	打开 Cloud Services Console 中的**确认付款方式**页面
		添加付款方式	打开 Cloud Services Console 中的**付款信息**页面，并提示您为组织添加付款方式详细信息

如何请求其他角色

作为**组织成员**用户，您可以通过**组织所有者**用户的邀请或提交自助服务请求来访问组织中可用的 VMware Cloud services。

自助服务请求无需等待**组织所有者**发送邀请，并可让您确定想要在组织内访问的服务和角色，以及所请求访问权限的时间段。

注 **组织所有者**可以自行分配额外的组织角色和服务角色。有关详细信息，请参阅如何管理角色和权限。

要提交自助服务请求，请浏览服务目录，以查找要为其请求其他角色的服务。只需单击服务卡视图中的**请求访问权限**链接。将打开一个弹出窗口，您可以在其中使用下拉菜单选择新的服务角色。

所有请求都会提交给**组织所有者**，组织所有者可以批准请求，也可以在批准之前拒绝或修改请求。处理请求后，您会收到电子邮件通知。

如何查看我提交的自助服务请求?

您可以随时在**我的帐户** > **我的角色**页面上的**我的请求历史记录**部分中查看挂起的服务请求和过去的服务请求。

我能否取消创建的自助服务请求?

只能取消处于挂起状态的自助服务请求。打开**我的角色**页面，然后单击要删除的请求对应的**取消**链接。

为什么在服务图标中看不到**请求访问权限**链接?

在联合域中激活了身份监管和管理 (IGA) 的组织中，可能已取消激活用于请求其他服务角色的选项。在这种情况下，需要**组织所有者**向您发送邀请。

如何管理 Cloud Services 帐户

6

VMware Cloud services 帐户是管理个人资料的位置。选择语言和区域格式首选项、安全设置（如密码和 MFA 设置），并生成和管理 API 令牌。您还可以查看您在组织中拥有的角色。

要访问您的帐户，请单击您的用户名，然后单击**我的帐户**。

请阅读以下主题：

如何查看用户配置文件

您的用户配置文件包含您在创建 VMware 客户帐户时提供的详细信息。能够编辑用户配置文件取决于您的客户配置文件。

注 无法更改注册时使用的电子邮件地址。

您可以在 Cloud Services 控制台中查看自己的个人资料，也可以登录到自己的 My VMware 帐户 (https://customerconnect.vmware.com/) 进行查看。

如果您的帐户未联合，则可以在 Cloud Services 控制台中修改个人资料详细信息，所做的更改将保存到您的 VMware 帐户，反之亦然。

如果您的帐户已联合，则可使用的编辑选项是有限的。例如，您无法更改配置文件名称，只能查看 VMware ID 详细信息。

步骤

1 在 Cloud Services 控制台工具栏上，单击您的用户名，然后选择**我的帐户**。

2 在**配置文件**页面上进行相应更改，然后单击**保存**。

如何重置密码

您的 VMware Cloud services 与 VMware ID 使用相同的密码。

您可以在 VMware Cloud services 平台中重置 VMware ID，也可以登录到 VMware Customer Connect 帐户 (https://customerconnect.vmware.com/) 执行此操作。

步骤

1 在 Cloud Services 控制台工具栏上，单击您的用户名，然后选择**我的帐户 > 安全**。

2 输入信息以更改您的密码，然后单击**更改密码**。

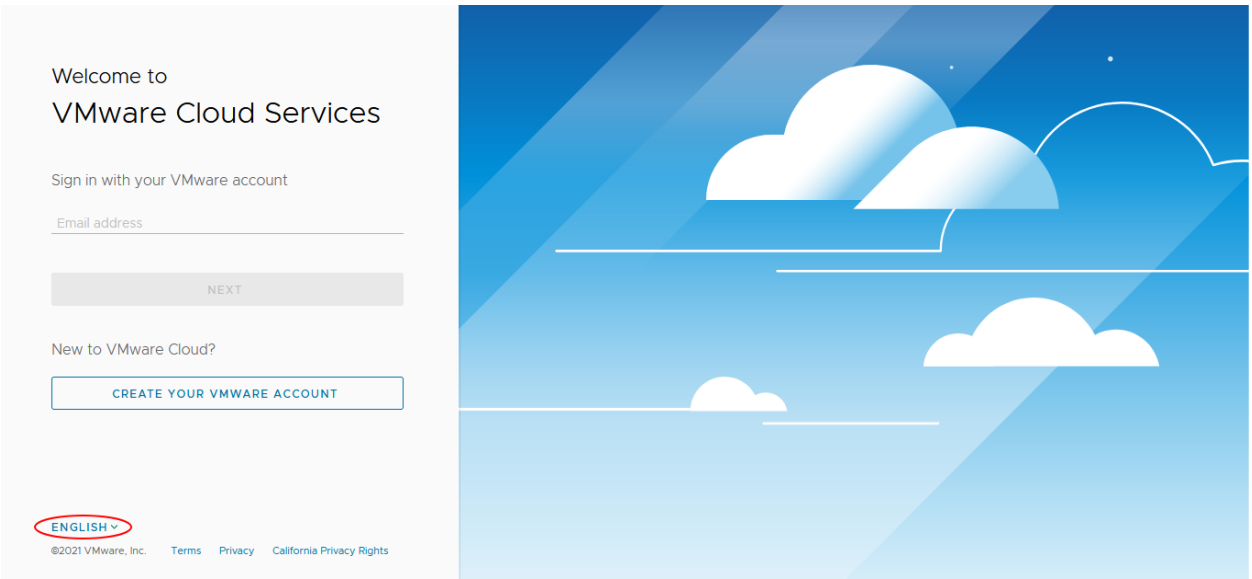
您的 VMware ID 已重置。

如何更改语言和区域格式

您可以在使用云服务之前将语言更改为您的首选语言，也可以在帐户设置中设置区域格式。

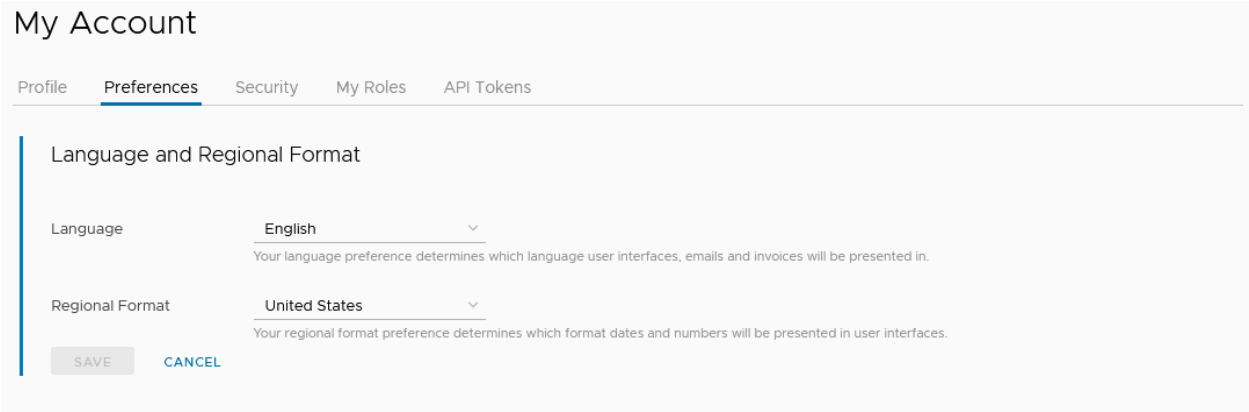
选择首选语言

如果您尚未登录 VMware Cloud services，可在登录之前选择首选语言。我们支持您在浏览器中设置的区域格式。



更改语言和区域格式

登录后，如果要在任意时间更改语言和区域格式，请在菜单栏中单击您的用户名，并选择**我的帐户 > 首选项**。然后单击**编辑**。



如果要更改语言，请注意，并非所有页面都能以所选语言显示。此外，有些表单仅支持英文字符。别担心，我们会告知您在何种情况下仅支持英文。

是否可以设置与语言不同的区域格式

如果设置的区域格式与首选语言不同，则所选语言的默认区域格式可能会覆盖选定区域格式。显示某些电子邮件、报表和发票时可能会出现这种情况。例如，如果选择“英语”作为首选语言，而选择“日语”作为区域格式，某些通信可能会以 US 区域格式显示。下面列出了各种语言及其默认区域格式。

语言	默认区域格式
English	US
简体中文	CN
繁体中文	TW
Español	ES
意大利语	IT
Français	FR
日语	JP
Deutsch	DE
한국어	KR

如何使用多因素身份验证保护我的帐户

多因素身份验证 (MFA) 是一项安全增强功能，要求您在登录时提供两项证据 (即凭据)。这些凭据可以是您已有的信息，例如密码，也可以是诸如生成一次性通行码的应用程序。MFA 通过添加额外的安全层来帮助保护数据和应用程序访问。

您可能已通过某种形式使用 MFA。例如，您登录的网站向您的移动设备发送代码，然后您使用此代码获取帐户的访问权限。

注 如果您的 VMware Cloud Services 帐户已联合，则 MFA 由您的企业安全团队管理。

要使用 MFA 保护您的 VMware Cloud Services 帐户，请在您的移动设备中下载身份验证应用程序。这将创建一个虚拟 MFA 设备。该应用程序会生成与基于时间的一次性密码标准兼容的六位数身份验证代码。您可以结合使用此代码与 VMware ID 以及密码登录到云服务。

为您的帐户设置 MFA 时，您将收到一组 10 个恢复代码。将这些代码保存到安全位置。如果您附近没有 MFA 设备或者 MFA 设备已丢失，则需要使用这些代码登录。

如何执行以下操作?	
激活我的 MFA 设备。	1 在菜单上单击您的用户名，然后选择**我的帐户 > 安全**。 2 单击**激活 MFA 设备**，然后按照说明设置您的设备。 3 MFA 将自动启用。下次登录时，需要使用 VMware ID 和密码以及该应用程序生成的身份验证代码。
禁用 MFA，以便仅使用 My VMware ID 和密码登录。	1 在菜单上单击您的用户名，然后选择**我的帐户 > 安全**。 2 单击 **MFA 已启用**切换键。
取消激活我的 MFA 设备。	1 在菜单上单击您的用户名，然后选择**我的帐户 > 安全**。 2 单击**取消激活 MFA 设备**。
重新生成恢复代码	可以随时通过访问**我的帐户 > 安全**来重新生成一组新的恢复代码。

可以使用哪种双因素身份验证应用程序?

VMware Cloud services 支持以下双因素身份验证应用程序。

通过单击下面相应的链接，可以下载适用于您设备的身份验证程序。

设备	身份验证应用程序
iOS	■ Google Authenticator。请参见 https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8。 ■ Duo Mobile。请参见 https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile。
Android	■ Google Authenticator。请参见 https://support.google.com/accounts/answer/1066447?hl=en。 ■ Duo Mobile。请参见 https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile。
Windows phone	■ Authenticator。请参见 https://www.microsoft.com/en-us/store/p/authenticator/9wzdncrfj3rj?rtc=1。 ■ Duo Mobile。请参见 https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile。
Blackberry	Google Authenticator 请参见 https://support.google.com/accounts/answer/1066447。

有关虚拟 NUMA 应用程序的详细信息，请参见 https://tools.ietf.org/html/rfc6238。

无法通过 MFA 登录时可以采取的操作

在 VMware Cloud services 中激活 MFA 时，您将收到一组 10 个恢复代码。可以复制这些代码，进行下载，甚至还可以进行打印，但必须保存到安全位置。

无法登录时如何排除 MFA 故障

在 VMware Cloud services 中激活 MFA 时，您将收到一组 10 个恢复代码。可以复制这些代码，进行下载，甚至还可以进行打印，但必须保存到安全位置。

如果登录 VMware Cloud services 时遇到问题，可以使用恢复代码。

如果...	执行操作
我无权访问我的 MFA 设备或设备已丢失	在 VMware Cloud Services 登录页面上，单击**解决 MFA 问题**链接。出现提示时，输入其中一个恢复密钥。
找不到恢复代码	通过拨打支持电话号码或访问 VMware Customer Connect 上的登录聊天支持来联系 VMware 技术支持团队。

如何生成 API 令牌

建立授权 API 连接时，需要使用 API 令牌对自己进行身份验证。以前称为 OAuth 刷新令牌的 API 令牌用于交换访问令牌，并按组织授权访问。您可以从 Cloud Services 控制台 中的帐户页面或通过 VMware Cloud Services 生成 API 令牌。

令牌是使用可提取字母数字字符的特殊算法生成的。每个令牌都是一个唯一的 65 个字符的组合。生成令牌时，您可以确定令牌的持续时间和范围：

- 令牌的生存时间 (TTL) 范围可以是几分钟到几个月，也可以设置为永不过期。默认持续时间为六个月。
- 范围提供了一种方法，可对令牌有权访问组织中的哪些区域实施控制，即组织中的哪些角色以及哪些服务和权限级别。

前提条件

确保 API 令牌的存储位置安全且受保护。

步骤

1 在 Cloud Services 控制台工具栏上，单击您的用户名，然后选择**我的帐户 > API 令牌**。

2 单击**生成新的 API 令牌**链接。

3 输入令牌的名称。

4 指定令牌的所需使用期限。

注 如果遭到入侵，不会过期的令牌可能会带来安全风险。如果发生这种情况，必须撤销令牌。

5 定义令牌的范围。您的选择必须基于您的用户帐户支持的角色。

范围	描述
组织角色	组织角色决定了用户对组织资源的访问权限。 ■ 为您的 API 令牌选择一个或多个组织角色。
服务角色	服务角色内置在授予对 VMware Cloud services 的访问权限的预定义权限集中。 ■ 使用服务名称旁边的箭头图标可展开可用于该服务的角色，然后为您的 API 令牌选择一个或多个服务角色。
权限	某些服务支持为服务角色分配一组有限的可用权限，从而进行更精细的选择。 ■ 选择服务角色时，可用权限将显示在表的右侧。为您的 API 令牌选择相关的服务权限。

如果需要，您可以选择**所有角色**，并授予您对所有组织角色和服务角色的令牌访问权限。

注 即使您为令牌分配**所有角色**访问权限，该令牌也只有您的用户帐户支持的访问角色。要查看您拥有的组织角色和服务角色，请从**我的帐户**页面中选择**我的角色**选项卡。

6 （可选）选中 **Open ID** 复选框以检索具有扩展用户详细信息的 Open ID 合规令牌。

7 （可选）设置电子邮件首选项，以便在令牌即将过期时接收提醒。

8 单击**生成**。

9 将令牌凭据保存到安全位置，以便可以检索供以后使用。

出于安全原因，在生成令牌后，我们仅在“API 令牌”页面上显示令牌的名称，而不是令牌凭据。这意味着您无法再通过复制此页面中的凭据来重用令牌。

10 单击**继续**。

除了 API 令牌之外，您还可以使用 OAuth 应用程序对应用程序进行身份验证。要了解何时使用 OAuth 应用程序，而不使用 API 令牌，请参见 OAuth 应用程序与 API 令牌的区别。

示例： 使用 API 令牌与 VMware Cloud Services API 交互

通过将 API 令牌交换为身份验证令牌可以使用 API 令牌与我们的 API 进行交互。

1 生成 API 令牌。

2 对 https://console.cloud.vmware.com/csp/gateway/am/api/auth/api-tokens/authorize 执行 `POST`。

3 在标头中，包括以下请求：

- accept: `application/json`
- content type: `application/x-www-form-urlencoded`/

4 在正文中，包括 `refresh_token={token value}` 请求。

5 执行脚本的 HTTP 调用时，在 `csp-auth-token` 标头中使用身份验证令牌。

如何管理我的 API 令牌

作为 API 令牌的唯一所有者，您有责任安全地存储、备份和管理这些令牌。

要查看和管理您的 API 令牌，请单击您的用户名，然后选择**我的帐户 > API 令牌**。

- 要重新生成令牌，请单击**生成**。这会将现有令牌替换为新令牌。要继续调用 API，您必须在 API 调用中更新令牌。
- 要停用令牌，请单击**撤销**。这将撤销 API 令牌和关联的访问令牌。
- 为防止对组织的资源进行未经授权的访问，强烈建议您将生成的 API 令牌保留在安全且受保护的位置。VMware Cloud Services 不会检查拥有证明，但在以下情况下捕获令牌使用情况审核事件：
  - 用户生成 API 令牌
  - 用户撤销一个或所有个人令牌
  - 用户尝试通过 API 令牌刷新生成访问令牌，但未成功

  注 要在 VMware Cloud Services 中查看审核事件日志，您必须具有**组织所有者**角色。
- 要为 API 添加额外的安全层，您可以为 API 令牌添加多因素身份验证。有关详细信息，请参见如何使用多因素身份验证保护我的 API 令牌。
- 如果您的 API 令牌因违反组织中设置的任何策略或不遵守组织的标准而由**组织所有者**取消激活，您将收到一封来自 VMware Cloud Services 的电子邮件通知。在**我的帐户 > API 令牌**页面上，已停用令牌将带有标签 Deactivated 。

下表汇总了最常见的 API 令牌自助式管理任务：

如果要...	执行操作
延长已过期 API 令牌的有效性。	您必须重新生成令牌。
重新生成有效的 API 令牌。	可以随时重新生成令牌。如果重新生成令牌，则会撤销先前令牌的所有实例。如果您已使用令牌（例如，在您的一个脚本中使用了令牌），请记得将其替换为新生成的令牌。
替换被盗用的 API 令牌。	如果觉得令牌可能被盗用，您可以撤销令牌以防止未经授权的访问。生成新令牌可以续订授权。
销毁仍然有效的 API 令牌。	通过撤销有效 API 令牌可以销毁该令牌。
恢复丢失的 API 令牌。	无法恢复丢失的令牌。您必须撤销丢失的令牌并生成新的令牌。
重新激活**组织所有者**取消激活的 API 令牌	如果已取消激活的令牌仍然有效，则必须联系**组织所有者**并要求重新激活。

如何使用多因素身份验证保护我的 API 令牌

如果使用 API 令牌访问 VMware Cloud Services API，则可以通过在 API 令牌上激活多因素身份验证 (MFA) 来添加额外的安全层。

这样，即使您的 API 令牌受到某些破坏，您的数据和应用程序也会受到保护，使其免去未经授权的访问。激活 MFA 后，您尝试交换 VMware Cloud Services API 访问令牌的任何令牌都需要 MFA 身份验证。

要使用 MFA 保护您的 VMware Cloud Services API 帐户，请在您的移动设备中下载身份验证应用程序。这将创建一个虚拟 MFA 设备。该应用程序会生成与基于时间的一次性密码标准兼容的六位数身份验证代码。要访问 VMware Cloud Services API，必须提供从注册的 MFA 设备生成的六位数令牌。

如何执行以下操作?	
激活我的 MFA 设备。	1 在菜单上单击您的用户名，然后选择**我的帐户 > API 令牌 > MFA**。 2 单击**激活 MFA 设备**，然后按照说明设置您的设备。 3 MFA 将自动启用。下次使用 API 令牌获取访问令牌时，您将需要使用应用程序生成的身份验证代码。
禁用 MFA。	1 在菜单上单击您的用户名，然后选择**我的帐户 > API 令牌 > MFA**。 2 单击 **MFA 已启用**切换键。 **重要说明** 如果您的组织强制对 API 令牌使用 MFA，则无法禁用 MFA。即使您可以生成 API 令牌，也无法将它们交换为访问令牌，除非您从注册的 MFA 设备提供六位数的密码。
取消激活我的 MFA 设备。	1 在菜单上单击您的用户名，然后选择**我的帐户 > API 令牌 > MFA**。 2 单击**取消激活 MFA 设备**。

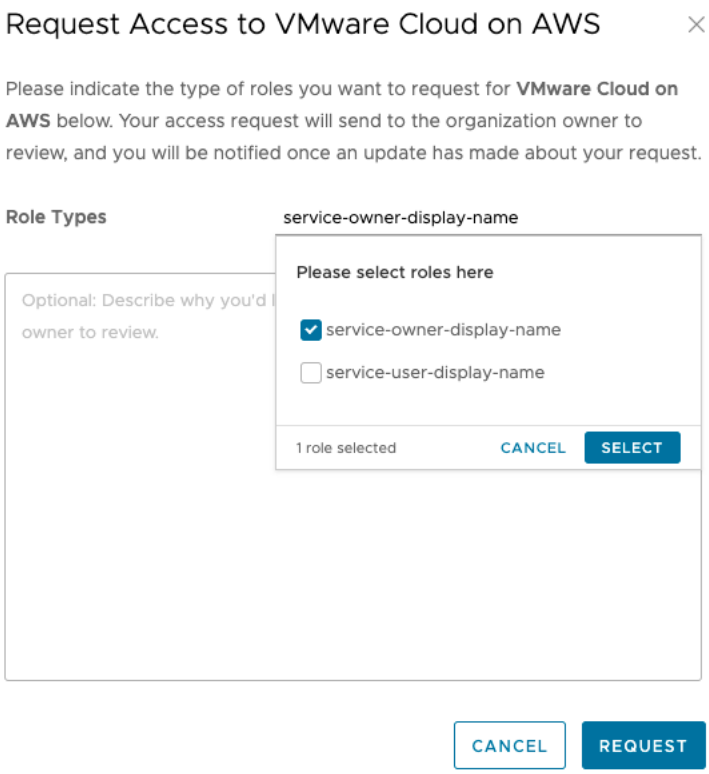
如何管理组织中的角色

角色由具有**组织所有者**角色的用户分配。您通常将拥有组织中的角色以及一个或多个组织服务中的角色。作为**组织成员**用户，您可以请求组织中可用服务的其他服务角色，并且可以删除已分配给您的角色。要获取其他服务角色访问权限，您的请求必须经过**组织所有者**批准。

有关组织角色的详细信息，请参见如何管理角色和权限。

下面介绍了如何管理您在组织中的服务角色：

- 要查看您的角色，查看您具有服务的哪些访问权限以及请求其他角色，请单击您的用户名，然后选择**我的帐户 > 我的角色**。
- 要删除不再需要的服务角色或其他组织角色，请单击服务名称以展开您拥有的该服务的所有角色。找到要移除的服务角色后，单击**删除角色**。您的角色删除请求必须由**组织所有者**批准后才会生效。
- 要查看过去的角色请求，请向下滚动到页面的**我的请求历史记录**部分。
- 要请求组织中已有服务的其他服务角色，请单击**请求角色**并做出选择。



如果您是激活了身份监管和管理 (IGA) 的组织的成员，则也可以选择请求新的组织角色。有关详细信息，请参见如何在激活了监管的组织中请求角色。

如何在激活了监管的组织中请求角色

激活了身份监管和管理的组织的**组织所有者**可以允许**组织成员**提交自助服务访问请求，而不是通过邀请授予访问权限。如果此选项在组织中可用，您可以直接从 Cloud Services 控制台请求其他角色。

步骤

1 登录到 VMware Cloud Services，然后导航到**我的帐户 > 我的角色**页面。

2 单击**添加服务访问权限**链接。

> **注** 如果您看不到**添加服务访问权限**链接，则说明自助服务请求选项已取消激活，您只能通过**组织所有者**向您发送的邀请获取其他访问权限。

3 选择要请求的其他组织角色和服务角色。

4 单击**提交**。

结果

您的请求已创建并提交审批。**组织所有者**处理请求后，您将收到通知。

如何管理 Cloud Services 组织 7

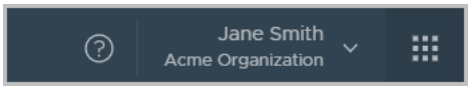
您的 VMware 帐户可以与一个或多个 VMware Cloud services 组织相关联。VMware Cloud 使用组织提供对一个或多个服务的受控访问。要访问 Cloud Services，您必须属于某个组织。

如果您是**组织所有者**用户，您可以访问组织中的所有资源。您可以将 Cloud Services 添加到组织，然后邀请用户加入。您可以管理组织付款方式和用户访问权限。如果您拥有**组织成员**用户角色，则对组织资源的访问权限有限。

要了解您的角色可在组织中执行的操作，请参见如何管理角色和权限。

活动组织

登录到 VMware Cloud services 时，您所登录的组织将在 Cloud Services 控制台菜单栏上显示在您的用户名下。



如果您属于多个组织，可以在任意给定时间从活动组织切换到其他组织。您也可以选择登录时默认显示的组织。

查看组织 ID

每个组织都有一个唯一的 ID。与外部命令行界面（如 VMware Container Engine CLI）交互时，您可能需要使用此 ID。单击您的用户名，可以查看组织 ID。组织名称下会显示简短 ID。要显示完整的组织 ID，请单击短 ID。

显示组织设置

通过单击您的用户名并选择**查看组织**，可以显示组织名称和 ID。

如果您是**组织所有者**，您可以更改组织的显示名称。

您还可以查看和编辑国家/地区和邮政编码，以及添加或编辑在查询 VMware API 时使用的标记，具体取决于您的客户配置文件。

请阅读以下主题：

- 如何访问另一个组织

如何访问另一个组织

如果您属于多个组织，可以在任意给定时间从活动组织切换到其他组织。

登录到 VMware Cloud Services 时，将显示您的活动组织。可以在 VMware Cloud Services 菜单上您的用户名下看到活动组织的名称。

步骤

1 在 VMware Cloud Services 菜单上，单击您的用户名旁边的箭头。

2 在菜单中，单击组织名称旁边的箭头。

将出现一个下拉列表，其中显示了您所在组织的名称。

3 选择要显示的组织。

如何指定默认组织

如果您属于多个组织，则可以选择您登录时默认显示的组织。

默认情况下，活动组织是您受邀加入的组织，或者您注销 VMware Cloud Services 时显示的组织。

步骤

1 在 VMware Cloud Services 菜单上，单击您的用户名旁边的箭头。

2 单击**设置默认组织**。

将显示您所在组织的列表。

3 选择要在您登录时显示的组织。

如何自定义 VMware Cloud Services 标头

作为**组织所有者**用户，您可以对 VMware Cloud Services 标题进行品牌标识和自定义，以反映您公司的品牌。

在此任务中创建的自定义 VMware Cloud Services 标题仅对访问此特定组织的**组织成员**可见。

前提条件

- 您必须具有**组织所有者**角色。
- 您必须熟悉贵公司的品牌准则。

步骤

1 登录到 Cloud Services 控制台，导航到**组织 > 详细信息**。

2 在组织详细信息页面的**组织自定义**部分中，单击**编辑**。

3 在**标题显示名称**文本框中，键入要在组织中显示而不是在 VMware Cloud Services 中显示的名称。

4 要对**浅色主题**上载组织徽标，请单击**浏览**，然后从本地计算机中选择图像文件。

注 只能为徽标图像上载 `.svg` 文件。

默认情况下，**深色主题**的标题徽标设置为**与浅色主题相同**。要为 **深色主题**上载其他图像文件，请取消选中**与浅色主题相同**复选框，单击**浏览**并从本地计算机中选择图像。

预览部分将刷新，以显示您所做的新颜色更改。您可以通过单击**还原默认值**来恢复所做的更改。

5 要对**浅色主题**和**深色主题**修改组织标题的调色板，请执行以下操作：

a 单击**标题背景颜色**，然后单击**标题文本颜色**文本字段。

b 使用颜色选择工具为每个条目定义颜色。

6 单击**保存**。

预览部分将刷新，以显示新的标题徽标。

7 刷新服务页面以查看所做的更改。

下载云服务的软件二进制文件时涉及的内容

8

某些 VMware Cloud services 需要使用与服务分开下载和安装的其他软件二进制文件。

您可以通过单击 Cloud Services 控制台菜单上的**下载**来下载其他软件。此选项适用于组织中的以下角色：

- **组织所有者**；
- 具有**软件安装者**角色的**组织管理员**。
- 具有**软件安装者**角色的**组织成员**。

在**下载**页面中，可以一站式获取组织中您具有服务访问权限的所有服务所需的软件二进制文件，同时可以下载其他软件。

如果...	执行操作
如果看不到**下载**菜单链接	请求组织中的**组织所有者**或**软件安装者**角色。 根据您的组织，您可以通过**组织所有者**的邀请或通过提交自助服务请求来执行此操作。有关详细信息，请参见如何请求其他角色。
如果可以打开**下载**页面，但看不到需要为其下载其他软件的服务	为服务请求角色。有关详细信息，请参见如何管理组织中的角色。 **注** 如果您在组织中分配了服务角色，但仍然没有看到任何适用于该服务的软件二进制文件可供下载，这意味着在 VMware Cloud Services 中没有与该服务关联的二进制文件或软件包 .
如果您是若干 VMware Cloud Services 组织的成员	切换到您具有组织角色和服务角色的组织，以便您可以访问需要下载的软件二进制文件。有关详细信息，请参见如何访问另一个组织。

请阅读以下主题：

- 如何下载 VMware Cloud Services 的其他软件

如何下载 VMware Cloud Services 的其他软件

需要为服务下载的其他软件二进制文件和软件包可以从 Cloud Services 控制台 中的**下载**页面访问。

前提条件

要下载其他软件二进制文件和软件包，您必须：

- 具有**组织所有者**角色或**软件安装者**权限（如果您是组织中的**组织管理员**或**组织成员**）；
- 对于要为其下载其他软件的服务，为您分配了服务角色；
- 对于要为其下载其他软件的服务，您的组织具有该服务的有效订阅。

步骤

1. 登录到 Cloud Services 控制台。
2. 从主菜单中，单击**下载**。

   将打开**产品资源管理器**。它显示了您有权访问的服务的列表，同时还提供了其他软件供下载。
3. 要查看服务的软件二进制文件，请单击服务名称。

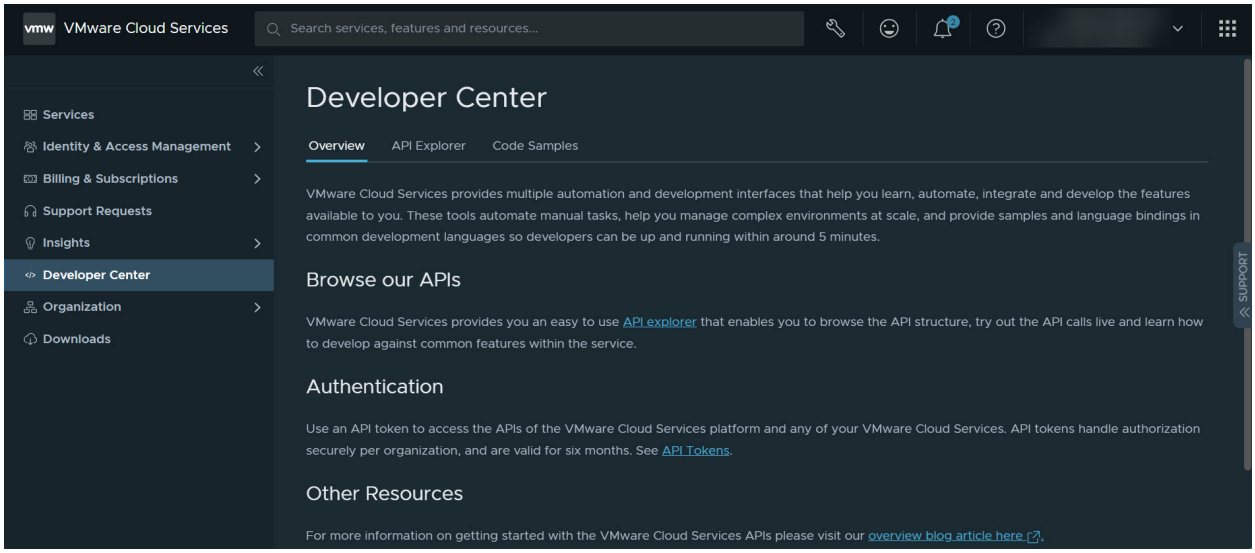
   产品资源管理器的右侧窗格显示与所选服务关联的下载项二进制文件。
4. 浏览可用的软件下载：
   a. 单击**阅读更多**可查看特定软件二进制文件的详细信息。
   b. 单击**下载**可在本地计算机上下载软件二进制文件。

如何使用 VMware Cloud Services 中的“开发人员中心”

9

VMware Cloud Services 中的**开发人员中心**提供了 API 接口，可帮助您自动执行、集成和开发 Cloud Services 控制台中可用的功能。

可以从 Cloud Services 控制台中的主菜单访问**开发人员中心**。要使用**开发人员中心**，您必须具有**组织所有者**角色。



在**开发人员中心**的 **API 资源管理器**页面中，可以与可用的 VMware Cloud Services API 进行交互。有关详细信息，请参见需要了解有关 API 资源管理器的哪些内容。

在**开发人员中心**的**代码示例**页面上，可以浏览和下载社区编写的示例。使用这些示例可帮助您快速开始执行自动化、管理或集成任务。

请阅读以下主题：

- 需要了解有关 API 资源管理器的哪些内容
- 开发人员中心提供哪些 API
- 如何在开发人员中心尝试 API

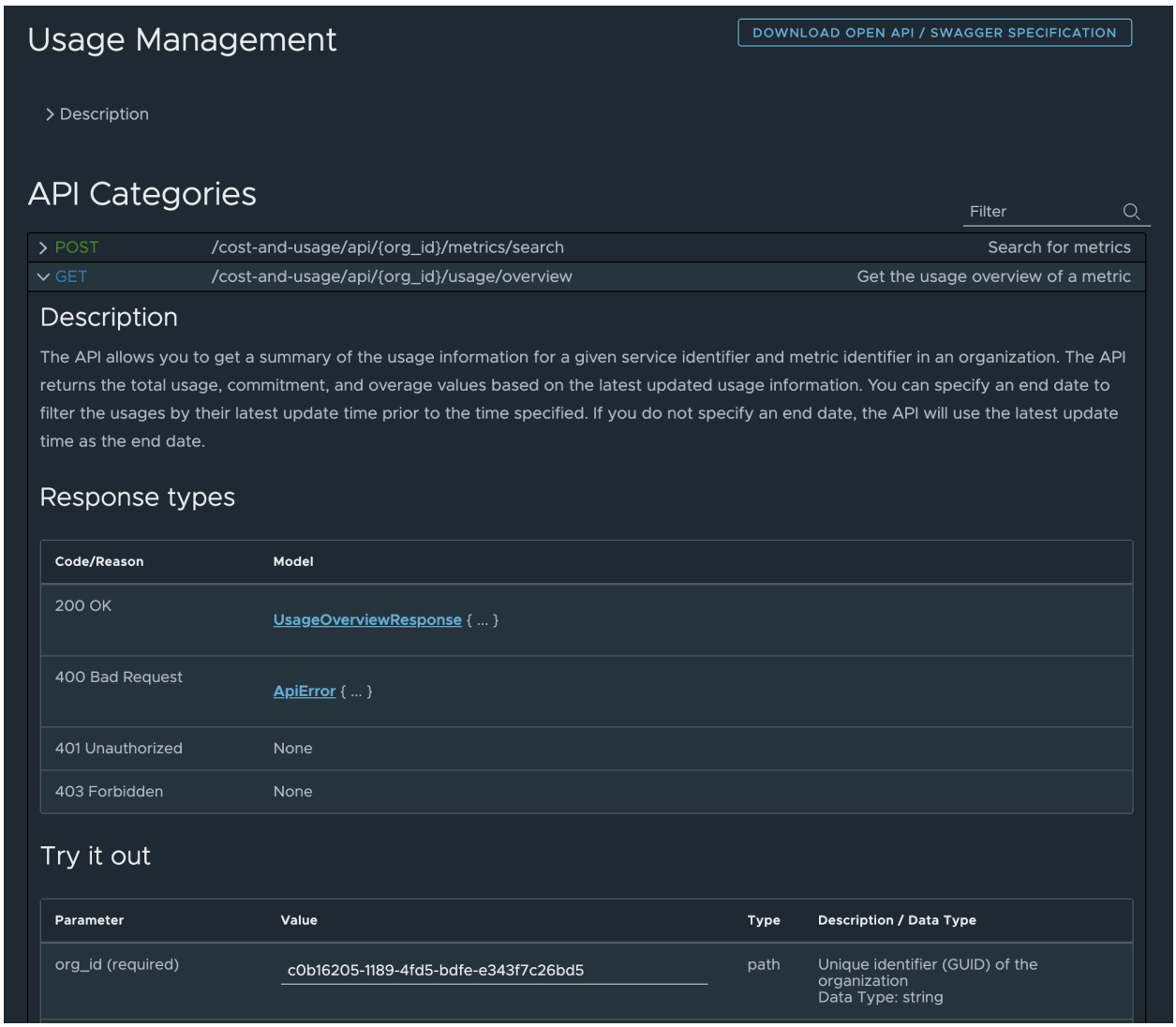
需要了解有关 API 资源管理器的哪些内容

作为**组织所有者**，您可以在 Cloud Services 控制台中访问 **API 资源管理器**，查找组织中可用的所有 VMware Cloud services API。

您可以：

- 直接从 Cloud Services 控制台调用 API。
- 浏览 API 结构。
- 实时试用 API 调用，了解如何针对服务中的常见功能进行开发。

要开始与 API 交互，请登录到 Cloud Services 控制台，然后导航到**开发人员中心 > API 资源管理器**。



如上面的屏幕截图所示，**API 资源管理器**页面分为多个部分，用于选择可用的 API、复制组织的环境和服务信息以及与所选 API 进行交互。

可用的 API

在 **API 资源管理器**页面的**可用的 API** 部分中，可以浏览组织环境中的 API。单击页面左侧的任意 API 链接，可以查看：

- 有关相应类别中特定 API 的信息。
- 可能作为所选类别中显示的任何 API 的一部分返回的对象模型/数据结构列表。该列表还包括在 API 调用的响应中可能找到的内容详细信息。

有关 API 类别的详细信息，请参见开发人员中心提供哪些 API。

环境

在 **API 资源管理器**页面的**环境**部分中，可以查看和复制某些 API 上通常需要的参数，例如：

- **组织名称**：您登录的组织的名称。
- **组织 ID**：您登录的组织的 ID。
- **身份验证令牌**：与持有者令牌结合使用，可以在 API 调用的身份验证标头中使用。
- **服务**：从下拉列表中选择服务并单击复制图标时，将复制选定的服务 ID。

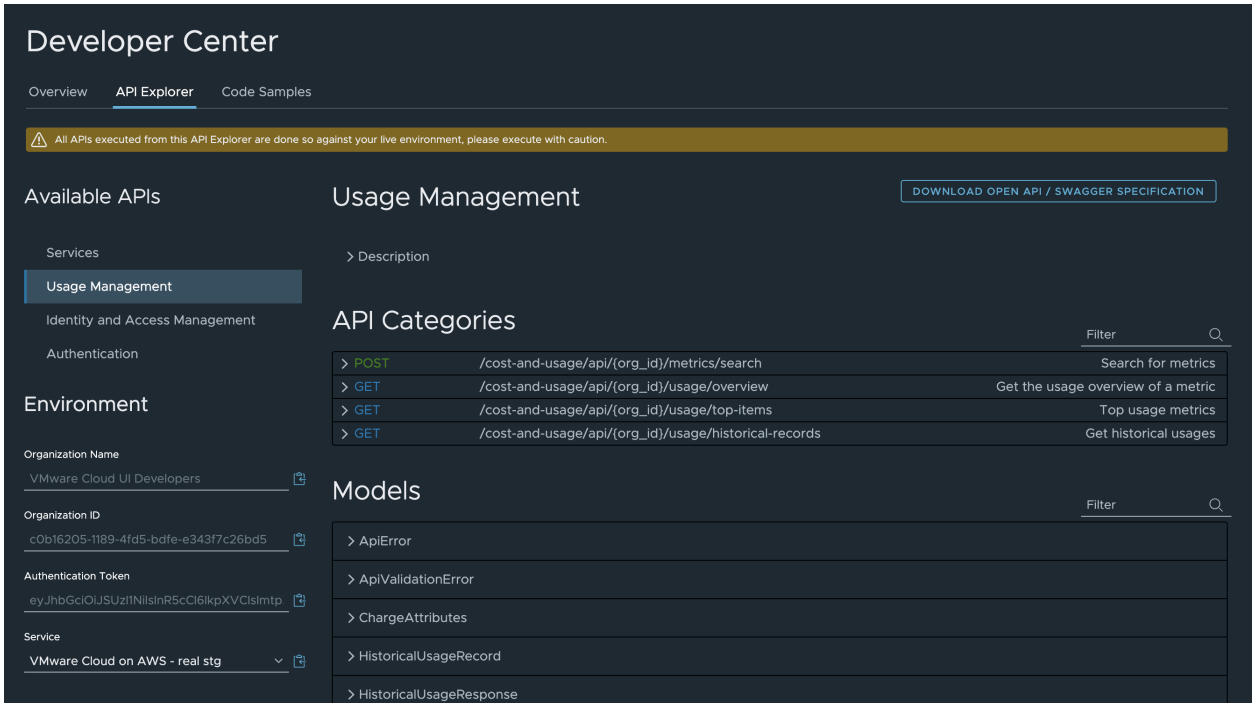
服务信息

从**可用的 API** 列表中选择一个 API 时，将显示**服务信息**部分。在该部分中，可以查看和复制基本 URL，以便在调用给定 API 类别中的 API 时使用。

开发人员中心提供哪些 API

作为**开发人员中心**的用户，您可以通过在 Cloud Services 控制台中打开**开发人员中心 > API 资源管理器**页面，与可用的 VMware Cloud Services API 进行交互。

此页面中列出的 API 用作 VMware Cloud Services 中组织和组织用户的主要身份验证和管理点。**可用的 API** 菜单中的每个链接表示一个特定类别或 API 组。



API 类别	描述
服务	包含组织中所有服务的 API 列表、其显示名称和图标。
使用情况管理	这组 API 可帮助您查找有关组织中当前和历史使用情况的数据，包括按类型和区域进行搜索。 可以在 Developer Portal (https://developer.vmware.com/apis/cost-and-usage-management/latest/) 上找到详细的使用情况管理 API 文档。
身份与访问管理	您可以使用这组 API 管理组织中的用户和组。 可以在 Developer Portal (https://developer.vmware.com/apis/csp/csp-iam/latest/) 上找到详细的身份与访问管理 API 文档。
身份验证	如果要自动执行与 Cloud Services 控制台交互的流程，可以使用这组中的 API。在连接到其他 API 之前，必须在 Cloud Services 控制台中进行身份验证。为此，请先创建 API 令牌。有关详细信息，请参见 如何生成 API 令牌。

如何在开发人员中心尝试 API

可以直接从 Cloud Services 控制台中的 **API 资源管理器**页面试用组织中可用的任何 API。

前提条件

您必须在组织中具有**组织所有者**角色。

步骤

1 在 Cloud Services 控制台中登录到您的组织。

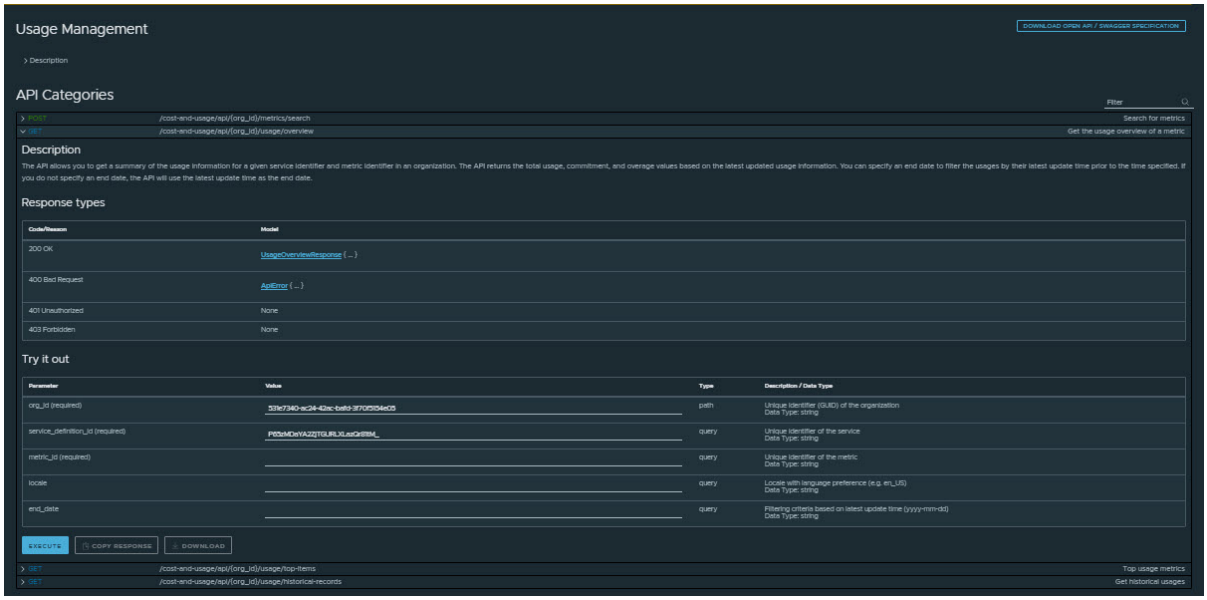
2 导航到**开发人员中心 > API 资源管理器**。

3 从 **API 资源管理器**页面上的**可用的 API** 菜单中选择一个 API 类别。

该页面将刷新以显示所选类别中的所有可用 API。

4 使用箭头图标展开 API 的内容。

5 向下滚动到**试用**部分。



6 要创建 API 调用，请填写所需的属性。

尽可能根据页面右侧显示的环境详细信息预填充属性。

在本地构建或使用 API 集成或服务器调用时，您可能会使用 API 规范示例片段。一种简单的方法是单击位于 **API 资源管理器**页面顶部和底部的**下载 Open API/Swagger 规范**按钮。规范文件包含示例调用和预期响应。

7 单击**执行**。

注 从 **API 资源管理器**进行的所有 API 调用都将针对您的实时环境执行。使用**试用**功能时务必小心谨慎。

结果

执行 API 调用时，页面将刷新，以在 **API 资源管理器**页面**试用**部分的正下方显示响应。您可以与模型响应交互，以文本格式查看负载，也可以复制或下载响应。

示例：

在此示例中，将使用“身份与访问管理”类别中的 API 获取有关**主体用户**（即当前登录到组织的用户）的信息。

1 打开 **API 资源管理器**。

2 从**可用的 API** 列表中选择**身份与访问管理**。

3 在显示的 **API 类别**列表中，单击**主体用户**。

4 单击 `GET /am/api/loggedin/user`。

5 单击**执行**。

对所创建 API 调用的响应将显示在页面的**响应**部分中，返回了用于登录到组织的用户信息。

身份与访问管理

10

作为**组织所有者**用户，您可以控制用户和组对组织及其资源的访问权限。

请阅读以下主题：

- 如何管理角色和权限
- 如何管理组织中的用户
- 如何使用组
- 如何在我的组织中设置身份验证策略
- 企业联合的含义及其在 VMware Cloud Services 中的运作方式
- 身份监管和管理的含义及其在 VMware Cloud Services 中的运作方式
- 如何使用 OAuth 2.0 对应用程序进行身份验证
- 如何在 VMware Cloud Services 中审核事件日志
- 如何在 VMware Cloud Services 中创建 NIST 登录前通知
- 如何使用数据见解仪表板
- 在 Cloud Services 控制台中使用项目涉及哪些内容

如何管理角色和权限

作为**组织所有者**用户，您可以在邀请 VMware Cloud Services 用户加入组织时授予他们基于角色的访问权限。

您可以从 Cloud Services 控制台中的**身份与访问管理 > 活跃用户**菜单查看和管理您组织中的用户角色。

组织角色和权限

对组织资源的访问权限由分配给组织中每个用户的角色决定。可以为每个用户分配组织中的以下一个或多个角色：

- **组织所有者**
- **组织成员**
- **组织管理员**

要了解每个组织角色的权限，请参阅 VMware Cloud Services 中提供哪些组织角色。

服务角色和权限

VMware Cloud services 附带一组预定义的内置服务角色，可以分配给组织中的用户。**组织所有者**用户可以根据每个云服务提供的角色授予组织中的其他用户访问云服务的权限。有关内置服务角色的详细信息，请参阅相关 VMware Cloud 服务的文档。

VMware Cloud Services 中提供哪些组织角色

VMware Cloud Services 用户可以在任何组织中具有以下任何组织角色：**组织成员**、**组织管理员**或**组织所有者**。

组织角色和权限

每个组织的权限级别各不相同：

- **组织所有者**角色对组织中的所有资源具有完全管理访问权限。**组织所有者**用户也可以为自己分配角色。
- **组织管理员**角色具有有限的管理访问权限。**组织管理员**用户可以将服务角色分配给任何组织角色，但只能管理具有相同或更低管理权限角色的用户、组和 OAuth 应用程序。

  例如，**组织管理员**用户可以为在组织中具有**组织成员**或**组织管理员**角色的其他用户和组授予或管理访问权限，但不能管理分配了**组织所有者**角色的用户、组或资源。
- **组织成员**角色对组织资源具有只读访问权限。

以下是您需要了解的有关 VMware Cloud Services 中这三个组织角色的权限信息。如果为用户分配的角色相互冲突，则会将具有较大权限的角色分配给用户。

权限	组织所有者	组织管理员	组织成员
属于一个或多个组织	☑	☑	☑
访问您的其他组织	☑	☑	☑
指定登录时显示的组织。	☑	☑	☑
查看和修改组织设置。	☑	☑ 仅查看。	☑ 仅查看。
在组织中添加/移除用户	☑	☑ 仅限具有**组织成员**或**组织管理员**角色的用户。	
管理组织中用户的服务访问权限和角色。	☑	☑	
管理并查看付款方式和计费。	☑	☑ 当**计费只读**复选框处于选中状态时，此角色将提供对计费相关信息的只读访问权限以及用于生成使用情况报告的选项。	☑ 当**计费只读**复选框处于选中状态时，此角色将提供对计费相关信息的只读访问权限以及用于生成使用情况报告的选项。
提交和管理支持请求。	☑	☑ 当**支持用户**复选框处于选中状态时。	☑ 当**支持用户**复选框处于选中状态时。

权限	组织所有者	组织管理员	组织成员
查询云服务 API 以获取客户使用情况和数据。 此权限仅限特定客户配置文件。	☑	☑ 当**托管服务提供商**复选框处于选中状态时。	☑ 当**托管服务提供商**复选框处于选中状态时。
创建和管理 OAuth 应用程序，以授权第三方应用程序访问受保护资源。	☑	☑ 仅限组织中的用户创建的 OAuth 应用程序。	☑ 当**开发人员**复选框处于选中状态时。
在组织的关联 vRealize Log Insight Cloud 服务实例中访问组织的所有审核数据。	☑	☑ 当**访问日志审核员**复选框处于选中状态时。	☑ 当**访问日志审核员**复选框处于选中状态时。
访问 Cloud Services 的其他软件二进制文件和软件包下载链接。	☑	☑ 当**软件安装者**复选框处于选中状态时。	☑ 当**软件安装者**复选框处于选中状态时。
创建、修改和管理对项目及其资源的访问权限。	☑	☑ 当**项目管理员**复选框处于选中状态时。	☑ 当**项目管理员**复选框处于选中状态时。

如何管理组织中的用户

如果您是**组织所有者**用户，则可以管理用户访问权限，并确定授予组织中用户和组的服务级别和组织级别权限。

您可以使用 Cloud Services 控制台中的**身份与访问管理**菜单邀请组织中的用户、分配组织角色和服务角色、更改用户角色或从组织中移除用户。

注 对用户角色的更改可能需要长达 30 分钟才能在组织中生效。

邀请用户加入您的组织时，您可以分配两种基于角色的访问权限：

- 访问组织的一个或多个云服务。可以通过向用户分配服务提供的一个或多个角色，向用户授予对该服务的访问权限。有关详细信息，请参见相关 VMware Cloud Services 的文档。
- 对组织的基于角色的访问权限。作为具有完全访问权限的**组织所有者**用户或具有只读访问权限的**组织成员**用户。

将访问权限分配给组比一次将同一权限分配给单个用户更高效。作为**组织成员**，您可以确定构成组的用户以及为其分配的角色和权限。

如何向我的组织添加用户

作为**组织所有者**，您可以邀请用户加入组织并向其授权访问与组织关联的服务。您还可以跟踪您发送的邀请。邀请有效期最多为七天。如果发错了邀请，可以撤销该邀请。

您邀请的用户可以拥有多个角色：

- 组织中的角色 - **组织所有者**或**组织成员**。要查看分配给每个角色的权限，请参见 VMware Cloud Services 中提供哪些组织角色

- 您邀请用户加入的云服务中的角色。每个云服务都有其自身特定的角色。有关详细信息，请参见相关 VMware Cloud services 的文档。
- 根据您的客户配置文件，您还可以查看托管服务提供商角色，该角色允许用户查询云服务 API 来获取客户使用情况和数据。如果将此角色分配给租户组织的用户，他们将有权访问组织中的所有数据。

步骤

1 在 Cloud Services 控制台工具栏中，单击 **VMware Cloud Services** 图标，然后选择**身份与访问管理 > 活跃用户**。

2 单击**添加用户**。

3 在**添加新用户**页面上，输入以下信息：

a 在**用户**文本框中，输入要添加到组织的用户的电子邮件地址。

可以通过以下方法一次添加多个用户：以逗号分隔电子邮件地址或在单独的一行中输入每个电子邮件地址。

b 在**分配组织角色**部分中，分配用户将在组织中具有的角色。

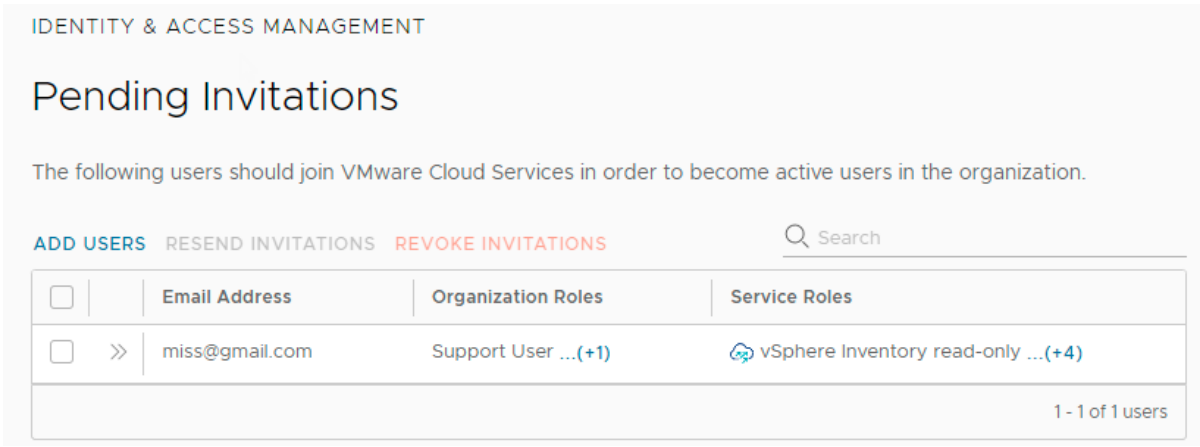
组织所有者角色具有完全管理访问权限。如果为新用户选择**组织成员**角色，请考虑通过在**其他角色**部分中选择一个或多个角色来添加其他访问权限。

c 要为用户分配组织中的服务角色，请单击**添加服务访问权限**，然后使用下拉菜单进行选择。

d 再次单击**添加服务访问权限**，以授予用户访问其他服务的权限。

4 单击**添加**可向用户发送邀请。

您发送的邀请有效期为七天。可以在**身份与访问管理 > 待定邀请**选项卡上查看邀请的状态。



5 如果发错了邀请，可以撤销该邀请。选中邀请旁边的复选框，然后单击**撤销邀请**。

电子邮件中的激活链接将被撤销，收到该邮件的用户将无法登录到该服务。

如何从我的组织中移除用户

作为**组织所有者**，您可以从组织中移除用户。已移除的用户将无法访问组织及其服务。

步骤

1 打开 Cloud Services 控制台，然后选择**身份与访问管理 > 活跃用户**。

2 选择一个或多个用户，然后单击**移除用户**。

3 单击**移除**，从您的组织中永久移除用户。

如何更改用户角色

当用户加入您的组织时，他们会获得**组织所有者**直接授予的组织角色和服务角色访问权限，或者他们作为组成员继承这些访问权限。作为**组织所有者**，您可以从 Cloud Services 控制台查看和编辑用户角色。

下面介绍了在您编辑用户角色时需要了解的相关信息。

- 用户可以具有多种角色的组合，这些角色包括直接分配给他们的角色以及从组中继承的角色。例如，直接为支持用户分配的角色以及一些从组中继承的角色，例如开发人员和 VMware Cloud on AWS 管理员。
- 如果为用户分配的角色相互冲突，则会将具有较大权限的角色分配给用户。例如，如果为用户分配了只读角色和管理员角色，则用户会获得管理员角色。

步骤

1 在 Cloud Services 控制台工具栏中，单击 **VMware Cloud Services** 图标，然后选择**身份与访问管理 > 活跃用户**。

2 单击用户名旁边的双箭头图标 (») 以查看其角色以及是否属于组。

对此用户的角色进行的更改可能会替代其通过组分配的角色。

3 选中某个用户旁边的复选框，然后单击**编辑角色**。

4 根据需要更改此用户的组织角色和服务角色。

5 单击**保存**。

如何使用组

将角色分配给组比一次将同一权限分配给单个用户更高效。作为**组织所有者**用户，您可以创建组并确定构成组的成员以及为其分配的角色。

此外，您还可以在创建或添加组后对其进行编辑。随着组织的扩展和变革，可以在组中添加或移除成员。

VMware Cloud services 中有两种类型的组 - 自定义组和企业组。可以与其他组织共享自定义组。企业组可以嵌套在自定义组中。

自定义组

可以通过输入名称和描述，添加成员，然后为组织及其资源分配角色，创建自定义组。例如，可以创建一个自定义组，并为其授予组织的**组织成员**角色和支持角色，以及对组织中特定服务的只读访问权限。自定义组还可以包括企业组。

对于自定义组，您可以编辑名称和描述，添加或移除成员，以及更改组的角色分配。

共享组

创建自定义组时，可以确定是否要使其共享。作为**组织所有者**，您可以将共享组与其他组织关联，从而能够为共享组的成员分配关联组织中的角色，并且他们无需**组织所有者**的邀请即可访问服务。

分配给共享组的服务角色特定于组织。关联组织的**组织所有者**导入共享组，并为组分配其自己组织内的角色。要导入共享组，**组织所有者**必须知道该组的名称或 ID。

只有源组织（创建共享组的组织）的**组织所有者**才能修改组的成员或移除组。从关联组织中移除共享组不会删除该共享组，并且稍后可以重新添加。请参见如何如何管理共享组。

企业组

企业组是从企业域同步的组。使用 VMware Cloud services 联合企业域后，您的企业组将可供您在组织中使用。请参见如何如何将角色分配给企业组。

对于企业组，只能更改组的角色分配。您无法在 VMware Cloud services 的企业组中添加或移除成员，但您可以为组织及其资源分配角色，并将其添加到自定义组。

嵌套组

将组添加到其他组称为嵌套。以下是您需要了解的有关嵌套组的信息：

- 您可以将企业组嵌套在自定义组中。
- 嵌套组可以包含角色的组合：直接分配给企业组的角色和通过自定义组分配的角色。
- 您可以编辑嵌套企业组的角色或添加其他角色，但无法移除从自定义组继承的角色。
- 不能将自定义组嵌套在另一个自定义组中。

作为**组织所有者**，您还可以在创建或添加组后对其进行编辑。对于自定义组，您可以编辑名称和描述，添加或移除成员，以及更改组的角色分配。对于企业组，只能更改组的角色分配。

作为**组织所有者**，您可以创建组，管理组，以及随着组织的扩展和变革，添加或移除组成员。

注 对组进行更改后，可能需要长达 30 分钟更改才会在组织中生效。

如何创建新组

作为**组织所有者**用户，您可以在组织中创建新组，并为组分配组织角色和服务角色。这些组称为自定义组。

有关为每个组织角色分配的权限的信息，请参见如何管理角色和权限。有关为服务角色分配的权限的信息，请参见服务对应的文档。

步骤

1 在 Cloud Services 控制台上，选择**身份与访问管理 > 组**。

2 单击**添加组**。

3 选择**创建新组**，然后单击**继续**。

4 输入组的名称和描述。

5 如果要与其他组织共享组，请单击**添加组织**。

a 选择要共享组的组织：键入每个组织的组织 ID，或者从弹出窗口中显示的组织列表中进行选择。

b 单击**添加**。

注 创建共享的自定义组时，关联组织的**组织所有者**可以为组织中的组分配角色。

6 单击**添加成员**将成员添加到您的组，然后单击**添加**。

成员可以是企业组和用户。您可以选择跳过此步骤并在创建组后添加成员。

7 通过选择组织角色为组分配对组织的访问权限。

8 为组分配对服务访问权限：单击**添加服务访问权限**，然后选择服务以及要分配给组的此服务的角色。

9 要添加对其他服务的访问权限，请单击**添加服务访问权限**。

10 单击**创建**。

该组将添加到**身份与访问管理**页面上的组列表中。

如何将角色分配给企业组

如果使用 VMware Cloud services 联合您的域，则可以从企业源域选择组，并为其分配组织中的角色。这些组称为企业组。

企业组是从企业域同步的组。可以同时为多个企业组分配角色，并查看所选组中的成员。

您分配的组成员可以拥有多个角色：

- 组织角色：组织中的角色 - **组织所有者**或**组织成员**。要查看分配给每个角色的特权，请参见如何管理角色和权限。
- 服务角色：一个或多个 VMware Cloud services 中的角色。每个云服务都有其自身特定的角色。有关详细信息，请参见相关 VMware Cloud Service 的文档。
- 根据您的客户配置文件，您还可以查看托管服务提供商角色，该角色允许用户查询云服务 API 来获取客户使用情况和数据。如果将此角色分配给租户组织的成员，他们将有权访问组织中的所有数据。

步骤

1 从 Cloud Services 控制台主菜单中，选择**身份与访问管理 > 组**。

2 单击**从源域中选择组**，然后单击**继续**。

3 搜索要向其分配角色的企业组。

4 向组分配组织角色。

请参阅上面的链接以查看每个角色的权限。

5 选择一个服务，然后向组分配服务中的一个或多个角色。

选择服务时，将显示服务默认角色。单击角色可选择其他角色。

6 要向组授予对其他服务的访问权限，请单击**添加服务访问权限**并分配角色。

7 单击**添加**。

要向具有**组织成员**角色的用户发送电子邮件，请选中对应的复选框。将自动向具有**组织所有者**和支持用户角色的用户发送一封电子邮件。

如何管理共享组

当**组织所有者**用户创建自定义组并将其与其他组织相关联时，该组将变为共享组。目标组织的**组织所有者**会收到源**组织所有者**发送的电子邮件邀请，邀请其导入共享组并分配服务角色。

作为受邀导入在其他组织中创建的共享组的**组织所有者**，您可以在将共享组导入到组织中时为其分配服务角色。

您可以通过标签 

区分导入的共享组和在组织中创建的共享组。

导入的共享组的用户可根据分配给组的角色访问组织中的服务。这允许跨组织访问组级别的服务，也无需向每个用户单独发送邀请。

重要说明 无法编辑从其他组织导入的共享组。您可以编辑分配给共享组的角色，也可以从组织中移除组。

前提条件

您必须知道创建要添加的共享组的源组织的名称或组织 ID。

步骤

1 在 Cloud Services 控制台上，选择**身份与访问管理 > 组**。

2 单击**添加组**。

3 选择**从其他组织导入组**，然后单击**继续**。

4 从下拉菜单中，选择创建共享组的源组织。

5 选择要导入的共享组。

6 选择一个组织角色，为选定的组分配对组织的访问权限。

7 单击**添加服务访问权限**，将服务角色分配给选定的组：

a 使用下拉菜单选择您希望共享组访问的组织中服务。

b 单击角色框，然后选择要分配给共享组的服务角色。

c 定义访问的时间段。您可以选择结束日期，或提供不过期访问权限。

8 要添加对其他服务的访问权限，请单击**添加服务访问权限**，然后重复步骤 7.a 到 7.c。

9 如果您希望共享组的所有用户收到访问服务的邀请，请保持选中**向所有受邀用户发送电子邮件，告知此角色分配**。

10 单击**导入**。

结果

共享组将作为自定义远程组添加到组织。

如何在我的组织中设置身份验证策略

作为**组织所有者**用户，您可以为用户访问 VMware Cloud services 组织设置身份验证策略，如多因素身份验证、IP 身份验证首选项以及域级别的用户访问。

可从 Cloud Services 控制台中的**组织 > 身份验证策略**页面创建和管理组织的身份验证策略设置。

重要说明 可能需要长达 30 分钟新策略或策略更改才会生效。

如果为您的组织设置了多个身份验证策略，则将根据所有策略依次验证每次用户登录。如果违反了任何策略，则不允许用户访问组织。

如何设置多因素身份验证

实施多因素身份验证 (MFA) 后，除登录凭据外，您组织中的所有用户还需要提供六位数的身份验证代码。为提供代码，他们必须向 VMware Cloud Services 注册 MFA 设备。无法提供有效 MFA 代码的组织用户将拒绝访问组织。

如果您是联合域的**组织所有者**，则无法控制组织的 MFA。联合域的 MFA 在公司正在使用的身份提供程序上由**企业管理员**配置。此过程仅适用于非联合域。

前提条件

- 您必须在组织中具有**组织所有者**角色。
- 您必须已在 VMware Cloud Services 中注册 MFA 设备，以便在实施 MFA 后不会出现无法访问自己组织的情况。有关详细说明，请参阅如何使用多因素身份验证保护我的帐户。

步骤

1 登录到 Cloud Services 控制台，然后单击**组织 > 身份验证策略**。

2 在**多因素身份验证**部分中，单击切换按钮，使其颜色变为绿色。

结果

现在已实施 MFA，您组织的所有用户都需要注册 MFA 设备并在登录时提供 MFA 令牌。

注 策略可能需要长达 30 分钟才会在组织中生效。

如何定义 IP 身份验证首选项

作为**组织所有者**，您可以通过定义 IP 地址或 IP 范围来阻止或允许用户从特定 IP 进行访问，从而管理对组织的访问。

为此，您可以通过应用身份验证首选项来阻止或允许用户从 IP 范围或特定 IP 地址进行访问。如果为 IP 范围定义了身份验证首选项，则您可以为该范围内的特定 IP 设置例外。例如，如果将阻止身份验证应用于 IP 范围，则您可以为该范围内的一个或多个 IP 设置例外，以允许这些 IP 访问 VMware Cloud services。

注 输入的 IP 地址必须遵循 IPv4 和 IPv6 IP 地址的 CIDR 表示法。

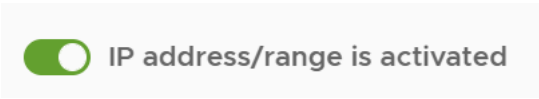
您可以定义两个身份验证首选选项：

- **阻止 IP**：将阻止从特定 IP 地址/范围登录的用户访问组织。
- **允许 IP**：将允许从特定 IP 地址/范围登录的用户访问组织。

您只能在组织中激活一个首选项。您可以在这两个首选项之间切换，但不能同时激活这两个首选项。

要在组织中设置或修改 IP 身份验证首选项，请登录到 Cloud Services 控制台，然后导航到**组织 > 身份验证策略 > IP 地址/范围**。

注 您的策略设置可能需要长达 30 分钟才能在组织中生效。

目的	执行操作
为组织设置 IP 身份验证首选项	1 如果首次设置 IP 身份验证首选项，请选择一个选项，然后单击**激活**。 此时会显示策略设置页面，指示您的组织中已激活 IP 地址/范围。  2 单击**添加**，并键入 IP 地址或范围。 3 再次单击**添加**。 您输入的地址或范围将添加到为您的组织指定的阻止或允许的地址和范围的列表中。
向身份验证首选项添加例外	您可以为已在允许 IP 列表或阻止 IP 列表上定义的 IP 范围中的 IP 地址定义例外规则。 1 在 **IP 地址/范围**页面的**例外**部分中，单击**添加例外**。 2 在打开的弹出窗口中，键入要作为例外添加到组织中的身份验证策略的 IP 地址。 如果激活了**允许 IP** 首选项，则系统会拒绝用户从例外列表上的 IP 访问 VMware Cloud services。相反，如果激活了**阻止 IP** 首选项，则系统会允许用户从例外列表上的 IP 访问 VMware Cloud services。

目的	执行操作
修改身份验证首选项的 IP 地址、范围或例外	激活 IP 身份验证策略后，您可以添加其他 IP、IP 范围和例外。您还可以从策略中修改或移除现有的 IP 和范围。 ■ 要进行更改，首先请从列表中选择 IP 地址或范围，然后应用相应的操作。
更改 IP 身份验证首选项	如果要将组织中的身份验证首选项从**阻止 IP** 切换至**允许 IP**（反之亦然），则必须先移除为当前身份验证首选项指定的所有 IP 地址和范围。 1 在 **IP 地址/范围**页面上，选择当前定义的所有 IP 地址和范围。 2 单击**移除**。 3 单击“用户 IP 身份验证首选项”选项旁边的**更改**链接。 4 在打开的弹出窗口中，选择新选项，然后单击**保存**。 5 要为新选择的策略设置定义新的 IP 地址或范围，请单击**添加**。

我意外将自己添加到阻止列表，并想要取消阻止我的 IP

如果意外将 IP 添加到组织的**阻止 IP** 列表，则必须提交支持请求才能取消阻止。由于您无法登录到组织并在 Cloud Services 控制台中使用**支持中心**，因此，您可以通过致电 VMware 技术支持团队来完成该操作。

在我的组织中阻止用户 IP 地址是否会阻止用户访问所属的其他组织

如果用户属于多个组织，并且其中一个组织实施了基于 IP 的策略，则不允许用户访问该特定组织。然后，用户可以在登录时选择切换到其他组织。

如何在域级别管理用户访问权限

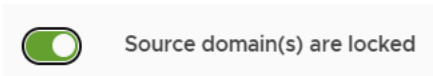
作为**组织所有者**用户，您可以决定允许访问您的 VMware Cloud Services 组织的域。

激活源域身份验证策略后，只有您指定的域中的用户才能访问您的组织。来自所有其他域的访问将会锁定，即使在组织中添加或邀请了组和用户也是如此。

步骤

1 登录到 Cloud Services 控制台，然后导航到**组织 > 身份验证策略 > 源域**。

2 要激活策略，请单击滑块并更改其位置以显示源域已锁定。



3 输入您允许访问组织的域名。

4 要将更多域和子域添加到允许的域列表中，请单击**添加域**链接。

5 单击**保存**。

结果

现在，为指定的域和子域激活了源域。只有从允许的域登录的组织成员才能访问您的组织。从其他域登录的用户的访问权限将锁定。

注 您的策略可能需要长达 30 分钟才能在组织中生效。

如果您或其他**组织所有者**意外地未将您的域包含到允许访问组织的源域列表中，从而导致您无法访问组织，请提交帮助支持请求。

企业联合的含义及其在 VMware Cloud Services 中的运作方式

作为使用 VMware Cloud services 的企业，您可以对多个企业域设置联合。通过联合企业域，您可以为企业中的用户激活单点登录。使用 VMware Cloud services 的企业联合是通过自助服务工作流设置的，并支持与基于 SAML 2.0 的身份提供程序集成。

通过为企业中的 VMware Cloud services 用户和组织采用联合身份访问，您可以激活以下内容：

- 您企业中的所有用户都可以使用其企业帐户访问 VMware Cloud services。
- **组织所有者**可以通过将组织角色和服务角色分配给从企业目录同步的组来控制对组织和服务的身份验证。
- 您的安全团队可以为 VMware Cloud services（包括多因素身份验证）设置和实施企业级安全和访问策略。

作为未联合域的**组织所有者**，您可以为整个企业域启动自助服务联合工作流。在完成设置后，企业联合可用于企业域中的所有用户，并应用于所有组织中的所有服务。

注意 您的企业必须拥有要联合以获得 VMware Cloud services 访问权限的域，并且您必须在自助服务工作流的第一步中验证所有权。您无法联合属于服务提供程序的域。

有关通过自助服务联合工作流设置企业联合的详细说明，请参阅《使用 VMware Cloud Services 设置企业联合指南》。

联合身份验证和未联合身份验证有什么区别?

如果您的企业域未联合，则对 VMware Cloud services 的访问将通过 VMware ID 帐户进行身份验证。如果您不熟悉 VMware Cloud services，请访问 my.vmware.com 以创建 VMware ID。

如果您的企业域已联合，则对 VMware Cloud services 的访问将通过您的企业账户进行身份验证。托管 Workspace ONE Access 租户将用作身份代理，以便使用身份提供程序设置联合。托管租户已配置为通过您的企业身份提供程序和 Active Directory 进行验证。通过配置 Workspace ONE Access Connector，可以管理用户和组对 VMware Cloud services 的访问，以便从企业 Active Directory 同步用户和组。仅将部分必需的个人资料属性（例如 `username`、`firstname`、`lastname` 和电子邮件地址）配置为同步。您可以稍后添加更多属性。

注 永远不会同步或缓存用户密码。

.

是否可以撤消企业域的联合?

如果您决定为最初配置的任何联合企业域撤消联合设置或撤消联合，则必须提交支持请求。

为企业域设置企业联合时涉及的内容

为企业域设置企业联合是一个自助服务过程，涉及多个步骤、用户和角色。

下面是使用 VMware Cloud services 联合企业域所涉及的人员和问题。

组织所有者

未联合域的**组织所有者**用户可以从 Cloud Services 控制台启动联合设置。任何**组织所有者**都可以启动自助服务联合过程，并分配一个或多个**企业管理员**来完成设置。

在企业中担任系统管理员角色并充分了解企业目录服务和身份提供程序配置的**组织所有者**，可以充当联合设置的**企业管理员**。

企业管理员

企业管理员是属于企业中央安全团队的系统管理员，负责管理目录服务和身份提供程序。作为为企业域设置企业联合的指定人员，**企业管理员**完成自助服务设置过程的配置和验证步骤。设置企业联合可能会涉及不同安全团队的代表。指定的**企业管理员**可以邀请其他管理员帮助进行设置。

企业联合组织

当**组织所有者**通过邀请一个或多个**企业管理员**为企业域启动自助服务联合工作流时，可以使用一个特殊的联合组织进行设置。参与自助服务联合过程的每个人都会收到一封电子邮件通知，其中包含访问特殊联合组织的链接。此组织的目的是为企业域设置企业联合并修改初始设置。

将企业帐户链接到 VMware ID

帐户已联合的现有 VMware Cloud services 用户必须将其企业帐户链接到其 VMware ID 帐户，才能访问组织中的服务。激活了为其域设置的联合后加入 VMware Cloud services 的新用户无需创建 VMware ID，除非他们需要查看计费信息或提交支持请求。

如果 VMware Cloud services 用户联系 VMware 以查看计费信息和获得支持，VMware 要求这些用户拥有 VMware ID，并将其企业帐户与 VMware ID 相关联。

VMware Workspace ONE Access 租户

设置联合身份管理要求客户配置和管理 VMware Workspace ONE Access 租户。租户是在自助服务联合过程中创建的。Workspace ONE Access 租户充当身份提供程序的身份代理（服务提供程序），并且不参与实际的用户身份验证。

自助服务联合设置工作流

自助服务联合设置涉及多个步骤，这些步骤可由不同的**企业管理员**在不同的时间执行。该工作流会从上次离开的位置恢复。参与设置的**企业管理员**必须具有包含 VMwareID 的 VMware Cloud services 帐户。联合设置中的所有步骤均通过特殊联合组织的**设置企业联合**工作流完成。

为什么需要链接 My VMware ID

如果您是**组织所有者**或具有联合帐户的**支持用户**，仍需要将 VMware ID 链接到您的企业帐户，以便访问计费信息和客户支持。

为什么看不到所有云服务?

您必须将 VMware ID 帐户链接到您的联合帐户，才能看到 VMware ID 帐户下的所有服务。如果您有任何令牌，系统会自动传输它们。

如何链接我的 Cloud Services 帐户?

通过在 Cloud Services 控制台上单击**我的帐户 > 配置文件**来链接您的帐户。

如果创建 VMware ID 时使用了企业电子邮件地址，请单击 Cloud Services 控制台横幅中的**链接 VMware ID** 按钮。如果在链接帐户之前关闭横幅，则可以稍后通过在 Cloud Services 控制台上单击**我的帐户 > 配置文件**来链接您的帐户。

您可以在“配置文件”页面中查看链接帐户的详细信息。

这对组织所有者或具有支持角色的用户有何影响?

如果您是**组织所有者**或具有**支持用户**角色，则必须链接 VMware ID 帐户才能继续访问计费信息和客户支持。链接帐户后，将收到客户编号。此后，如果创建新组织，您可以在设置组织时链接 VMware ID 帐户。

在哪里查看我的客户编号?

作为**组织所有者**或**支持用户**，您需要客户编号。链接帐户后，客户编号将在**用户/组织设置**菜单中您的名字下面显示。

您还可以在“配置文件”页面上查看客户编号和链接帐户的其他详细信息。

OAuth 客户端会出现什么情况?

OAuth 客户端用于将第三方应用程序与 VMware Cloud services 集成。

如果联合帐户的用户名与 VMware ID 的用户名相同，例如，都是 joe@acme.com，则使用此 VMware ID 登录时创建的任何 OAuth 客户端都会在链接此 VMware ID 时转移到您的联合帐户。

如果 VMware ID 的用户名与联合帐户的用户名不同，例如，分别为 joe@gmail.com 和 joe@acme.com，则您的客户端不会转移到联合帐户，您应创建新客户端。

有关创建 OAuth 客户端的详细信息，请参见如何使用 OAuth 2.0 对应用程序进行身份验证。

为什么需要链接企业身份提供程序

如果您的域已联合，则可以使用身份监管和管理 (IGA) 高级功能轻松地将非组织用户加入 VMware Cloud services。

激活 IGA 的一种方法是，请求**企业管理员**在“企业联合”组织仪表板中进行更改。另一种方法是将您的组织链接到身份提供程序 (IdP)。只有联合域的**组织所有者**才能将组织链接到其 IdP。

1 登录到 Cloud Services 控制台，然后单击**组织 > 详细信息**。

2 在**链接到身份提供程序的域**部分中，单击**链接身份提供程序**。

此时将打开一个弹出窗口，其中显示了与您组织关联的 IdP 和域。

3 单击**链接**，然后单击**继续**。

有关 IGA 功能的详细信息，请参见身份监管和管理的含义及其在 VMware Cloud Services 中的运作方式。

身份监管和管理的含义及其在 VMware Cloud Services 中的运作方式

身份监管和管理 (IGA) 是一种服务，通过该服务，您的企业可获取审核记录和认证的数据，并帮助**组织所有者**用户实时管理自助服务访问请求、批准、违规行为和 API 令牌。

IGA 服务具有两组功能：基本和高级。它仅适用于具有联合域的组织。

- 要开始使用基本 IGA 功能，**组织所有者**必须通过单击**身份与访问管理 > 监管**页面上的**开始**链接来激活 IGA 服务。
- 要开始使用高级 IGA 功能，请参见如何在我的组织中激活身份监管和管理高级功能。

通过在组织中使用 IGA 服务，VMware Cloud Services 用户可以执行以下操作：

作为	使用基本 IGA	使用高级 IGA
组织所有者用户	■ 从 Cloud Services 控制台 中的**身份与访问管理 > 监管**页面访问 IGA 仪表板。 ■ 激活或取消激活**组织成员**提交旨在申请其他角色的自助服务请求的功能。 ■ 通过管理入站组织和服务角色请求，监管对组织中服务的访问权限。 ■ 监控违规情况并立即响应威胁。	■ 在链接到企业身份提供程序的任何激活了监管的组织中载入服务。
组织成员	■ （如果已在组织中激活）提交自助服务访问请求，申请其他组织角色和服务角色。请参见如何在激活了监管的组织中请求角色。	■ 在链接到企业身份提供程序的任何激活了监管的组织中自行载入。请参见如何作为具有联合帐户的用户加入。

如何在我的组织中激活身份监管和管理高级功能

如果您的域已联合，则可以为联合域中的所有组织激活其他身份监管和管理 (IGA) 高级功能。

激活组织中的高级 IGA 功能需要满足以下条件：

- 联合域中的**组织所有者**必须将企业身份提供程序链接到 VMware Cloud Services。请参见为什么需要链接企业身份提供程序。
- **企业管理员**必须为链接到其企业身份提供程序的部分或全部 VMware Cloud services 组织启用高级 IGA 功能。有关详细信息，请参见为联合域启用高级 IGA 功能。

有关企业联合的详细信息，请参见企业联合的含义及其在 VMware Cloud Services 中的运作方式。

激活高级 IGA 功能后，非组织用户可以在加入期间请求链接组织中的组织和服务角色访问权限。要详细了解此功能，请参见如何作为具有联合帐户的用户加入。

如何管理对其他角色的自助服务请求

作为激活了身份监管和管理 (IGA) 的组织的**组织所有者**用户，您可以通过 Cloud Services 控制台中的**监管 > 请求**页面管理组织角色和服务角色请求。

只有在组织中激活了用于提交自助服务请求的选项时，**组织成员**用户才能使用此选项。

如果已激活对其他角色的请求，组织成员用户可通过以下方法请求访问权限...	如果未激活对其他角色的请求...
单击 Cloud Services 目录中服务图标上的**请求访问权限**链接。	无法单击服务图标上的**请求访问权限**链接。
单击**我的帐户 > 我的角色**页面上的**请求角色**链接。	**我的帐户 > 我的角色**页面上不显示**请求角色**链接。

如何激活或停用自助服务请求

要激活或取消激活对组织中其他角色的自助服务请求，请执行以下操作：

1 转到**监管 > 请求**，然后单击**设置**。

2 单击**对其他角色的请求**滑块以激活或取消激活该设置。

3 单击**保存**。

如何处理挂起的请求?

组织角色和服务角色访问权限的所有入站请求都列在**挂起的请求**部分中。通过**过去的请求**，可以查看在组织中创建的所有请求的历史数据。

要批准或拒绝请求，请在**挂起的请求**列表中选择一个或多个条目，然后单击相应的按钮。在请求获得批准或拒绝时，请求角色访问权限的用户将收到电子邮件通知。

是否可以在批准前修改访问请求?

作为**组织所有者**，您可以修改**组织成员**请求的服务角色访问权限的时间段。单击**请求 ID** 链接可查看原始请求的时间段。要更改请求的时间段，请单击**批准**，然后选择**批准并修改**。更改设置并提交所做更改。

注 **批准并修改**选项仅适用于服务角色访问请求，不适用于组织角色。

组织所有者无法修改**组织成员**最初请求的服务或角色访问权限。如果您希望向请求者提供有关您愿意批准的适当访问级别的指导，可以选择在拒绝请求时包含一条消息。请求者会收到电子邮件通知，并可以提交包含适当组织角色和服务角色的新访问请求。

如何监控组织中违反策略的行为

作为激活了身份监管和管理 (IGA) 的组织中的**组织所有者**用户，您可以监控组织中的用户登录以及使用 OAuth 应用程序和 API 令牌进行登录的访问违规行为。您可以定义和修改触发违规的策略。

通过为 OAuth 应用程序和 API 令牌激活各种触发器（例如非活动 API 令牌、非活动 OAuth 所有者、广泛的服务范围、不安全或未获批准的 OAuth 应用程序 URI），可以为激活了 IGA 的组织中的登录设置违规策略。

注 如果激活了“源域”身份验证策略，则对于从策略设置不允许的域执行的所有登录尝试，都会捕获用户访问违规行为。

步骤

1 使用企业帐户登录到 Cloud Services 控制台。

2 导航到**身份与访问管理 > 监管 > 违规**。

3 单击**设置**。

4 在打开的**违规设置**页面中，根据需要修改 OAuth 应用程序和 API 令牌的设置。

5 单击**保存**。

结果

违规仪表板将刷新，以根据新设置显示违规行为。

该仪表板上的信息每天更新一次。

如何对组织中违反策略的行为采取措施

作为激活了身份监管和管理 (IGA) 的组织中监控违规行为的**组织所有者**用户，您可以针对在组织中发现的违规行为采取措施。您可以通过导航到**身份与访问管理 > 监管 > 违规**，访问完整的违规行为列表。

在组织中捕获的违规行为按登录 VMware Cloud Services 时使用并触发违规的身份验证方法类型进行分组。单击相应的选项卡可查看完整列表以及您可以对违规行为采取的可行应对措施。

- **OAuth 应用程序**选项卡显示触发违规的应用程序的名称、严重性、描述以及创建 OAuth 应用程序的组织用户的电子邮件。
- **API 令牌**选项卡显示触发违规的 API 令牌的名称、严重性、描述以及创建 API 令牌的组织用户的电子邮件。
- **用户访问**选项卡显示登录尝试触发违规的组织用户的电子邮件、严重性、违规发生的日期以及违规发生的源域。对于从“源域”身份验证策略不允许的任何域进行的登录尝试，将捕获用户访问冲突。有关详细信息，请参见如何在域级别管理用户访问权限。

下表介绍了可对组织中的违规行为采取的措施。

目标	执行以下操作
更改违规行为的可见性	此操作会将违规行为的可见性状态从活动更改为隐藏。此操作不会删除违规行为，且是可恢复的。 1 找到要隐藏的违规行为，然后单击相应的双箭头 (») 以展开其详细信息。 2 选中要隐藏的活动违规行为旁边的复选框。 3 单击**隐藏**。 该违规行为不再显示在详细信息部分中。
显示已隐藏的违规行为	此操作将显示状态为隐藏的违规行为。 ■ 展开违规行为的详细信息部分，然后打开**全部显示**开关。将显示已隐藏的所有违规行为。
从组织中移除 OAuth 应用程序	此操作将移除 OAuth 应用程序，并阻止其访问组织。OAuth 应用程序不会删除，但不会进一步报告此应用程序的违规行为。移除操作无法从**违规**页面恢复 - 要监控此 OAuth 应用程序的违规行为，必须再次将其添加到组织。 1 在**违规**页面上，打开 **OAuth 应用程序**选项卡。 2 找到要移除的应用程序。 3 选中名称旁边的复选框。 4 单击**移除**。
编辑违规行为的严重性	根据您组织的需求，可以为任何违规条件定义严重性。 1 在**违规**页面上，单击**设置**。 2 使用**严重性**下拉菜单更改要修改的每个违规条件的设置。 3 单击**保存**。

如何管理组织中的 API 令牌

作为激活了身份监管和管理 (IGA) 的组织中的**组织所有者**用户，您可以监控在组织中创建的 API 令牌，并为所有新创建的令牌设置空闲和最长生存时间 (TTL) 限制。

要访问 **API 令牌**仪表板，请打开 Cloud Services 控制台，然后导航到**身份与访问管理 > 监管 > API 令牌**。打开的仪表板将列出组织中的用户创建的所有 API 令牌。

对于每个 API 令牌，您都可以查看详细信息，例如令牌名称、创建 API 令牌的组织用户的名称、创建日期和过期日期、上次使用令牌的日期以及令牌的范围（分配给令牌的组织角色）。

如果违反了组织的 TTL 策略，**API 令牌**仪表板列表将显示警示图标 (⚠)。为您的组织设置的 TTL 策略将应用于组织中的用户创建的所有新 API 令牌。如果更改 TTL 策略，则会在将违反新设置的所有先前创建的 API 令牌旁边显示一个警示图标。

您可以激活、停用或修改两个 TTL 策略设置：

- **空闲令牌 TTL**。

  此设置定义 API 令牌在违反策略之前允许的空闲生存时间。

- **最大令牌 TTL**。

  此设置定义在组织中创建的任何 API 令牌允许的最长生存时间。组织用户无法生成最大令牌 TTL 大于此设置定义的值的 API 令牌。

如果 API 令牌违反组织中的任何策略或准则，该怎么办

如果 API 令牌违反组织中的 TTL 策略，或者看似可疑，则可以从 **API 令牌**仪表板取消激活该令牌。这样，将无法使用该令牌访问组织中的资源。

1 在 **API 令牌**仪表板上，选择要取消激活的 API 令牌。

2 单击**取消激活**链接。

该 API 令牌的状态将从“已激活”更改为“已取消激活”。该 API 令牌的所有者将收到一封来自 VMware Cloud Services 的电子邮件通知，通知他们用于访问组织的令牌已由**组织所有者**取消激活。

要重新激活已取消激活的 API 令牌，请在仪表板上选择该 API 令牌，然后单击**激活**链接。该 API 令牌的所有者将收到一封确认重新激活的电子邮件通知。

如何更改组织中 API 令牌的 TTL 策略

要修改 API 令牌 TTL 策略，请执行以下操作：

1 在 **API 令牌**仪表板上，单击**设置**。

目标	执行操作
激活或停用策略。	使用**策略状态**滑块。
更改 TTL 设置	在相应的 TTL 设置部分中输入一个新值，然后从下拉列表中选择一个时间单位。时间单位可以是分钟、小时或天。

2 单击**保存**。

根据策略对现有令牌运行的验证每 24 小时进行一次。这意味着，由于您所做的更改，**API 令牌**仪表板违规列表可能需要一些时间才能更新。

如何在组织中分配默认角色

作为激活了身份监管和管理 (IGA) 的组织中的**组织所有者**用户，您可以通过设置策略为组织中的用户分配默认的组织角色和服务角色。

通过该策略授予的默认角色将应用于从指定联合域登录组织的所有用户，并且无法在用户级别进行编辑。要更改默认角色授权，必须修改策略。

重要说明 存在一个已知问题：作为**组织所有者**，您无法查看组织中已根据策略获得默认角色的用户以及在组织中没有其他角色的用户。除非这些用户请求获得其他角色且请求获得批准，否则这些用户不会显示在 Cloud Services 控制台 的**活跃用户**列表中。具有默认角色的用户获得组织中的其他角色后，这些用户将显示在**活跃用户**列表中，作为**组织所有者**，您可以向他们授予其他角色。

前提条件

- 您的企业身份提供程序已链接到 VMware Cloud Services。
- 组织中已激活高级 IGA 功能。
- 您在组织中具有**组织所有者**角色。

步骤

1 使用企业帐户登录到 Cloud Services 控制台。

2 导航到**身份与访问管理 > 监管 > 请求**。

3 单击**设置**。

4 在页面的**授予默认角色**部分中，单击**添加域策略**链接。

5 输入新策略的名称和描述。

6 选择要将策略应用到的域。

7 选择要自动分配给从指定域登录到组织的所有用户的组织角色和服务角色。

8 单击**保存**。

结果

您指定的角色将在用户登录到 VMware Cloud Services 时可供指定域中的所有用户使用。

如何使用 OAuth 2.0 对应用程序进行身份验证

VMware Cloud Services 控制台使用 OAuth 2.0，以便您可以为应用程序授予对组织中受保护资源进行安全委派访问的权限。VMware Cloud Services 支持 Web 应用程序访问（应用程序的用户授予访问权限）和服务器到服务器交互（直接向您的应用程序程序发出访问令牌）。

什么是 OAuth 2.0

OAuth 2.0 是一种授权协议，支持为您的应用程序授予对资源的安全访问权限。您的客户端通过访问令牌获得授权。访问令牌具有一个范围，用于定义令牌可以访问哪些资源。有关 OAuth 2.0 的信息，请参见 OAuth 规范（网址：https://tools.ietf.org/html/rfc6749#page-8），或阅读博客文章 OAuth 2.0 Simplified（网址：https://aaronparecki.com/oauth-2-simplified/）。

OAuth 2.0 如何与 VMware Cloud Services 配合使用

VMware Cloud services 涵盖利用不同授权类型（如 `client credentials`、`authorization code` 和 `public client` 与 `authorization code`）的应用程序授权的几个用例。根据您的目标，您可以选择创建三种类型的 OAuth 应用程序之一，分别对应于每个授权类型（服务器到服务器应用程序、Web 应用程序以及本机/移动应用程序）。

假设您是**组织所有者**，有权访问 VMware Cloud on AWS。您开发了一个可帮助您进行股票交易的应用程序。您将该应用程序称为 `Trading 1.0`。您想在 vCenter Server 管理的虚拟机上运行该应用程序，但首先需要使用 VMware Cloud on AWS 授权该应用程序。

1 您在 Cloud Services 控制台中创建 OAuth 2.0 应用程序。可以将其视为注册 `Trading 1.0` 应用程序的一种方式。您可以通过在**组织 > OAuth 应用程序**菜单中单击**创建应用程序**来启动应用程序创建，然后执行一系列步骤。在该过程结束时，我们以应用程序 ID 和应用程序密钥形式发出客户端凭据，该凭据用于向 API 标识客户端。将这些凭据粘贴到您的脚本中。

2 已在组织中创建应用程序，但尚未授予其访问权限。您可以通过将应用程序添加到组织来授予其访问权限。这将允许应用程序访问您在创建应用程序时定义的组织中的服务和资源。只有服务器到服务器应用程序类型的应用程序才需要执行此步骤，此步骤不适用于 Web 和本机/移动应用程序。

3 运行 `Trading 1.0` 客户端应用程序时，它会从授权服务器请求访问令牌。获得授权后，授权服务器会将访问令牌发送到 API，您的客户端即获得访问权限。

谁可以创建和管理 OAuth 应用程序

作为**组织所有者**用户或具有**开发人员**角色的**组织成员**用户，您可以创建和管理 OAuth 应用程序。

您还可以管理组织中的其他**组织所有者**创建或添加的 OAuth 应用程序。

是否可以重新生成应用程序密钥

可以，作为**组织所有者**，您可以重新生成组织中 OAuth 应用程序的应用程序密钥。如果创建 OAuth 应用程序的**组织所有者**离开您的公司，而您想继续运行该应用程序，此方法会非常有用。

是否可以使用 API 令牌身份验证，而不使用 OAuth 应用程序

可以，如果 API 在授权过程中要求用户是经身份验证的实体，则必须改用 API 令牌。要了解何时使用 OAuth 应用程序与 API 令牌，请参见 OAuth 应用程序与 API 令牌的区别。

如何管理 OAuth 2.0 应用程序

作为**组织所有者**用户，您可以创建、查看和修改组织中 OAuth 2.0 应用程序的详细信息。

您还可以：

- 管理组织中的其他**组织所有者**用户创建或添加的 OAuth 应用程序；
- 授予对在您拥有**组织所有者**角色的任何组织中创建的应用程序的访问权限。

目标	执行操作
查看有权访问您组织的 OAuth 应用程序。	单击**身份与访问管理 > OAuth 应用程序**。 您可以在此处查看在其他组织中创建并有权访问您组织的应用程序。
添加在其他组织中创建的 OAuth 应用程序。	1 单击**身份与访问管理 > OAuth 应用程序**。 2 单击**添加应用程序**。 3 要确定需要添加的 OAuth 应用程序，请选择以下选项之一： ■ **输入应用程序 ID** ■ **按组织搜索** 4 单击**继续**。 5 如果选择了使用 OAuth 应用程序的 ID 确定 OAuth 应用程序，系统会提示您输入 OAuth 应用程序 ID。 6 如果选择了通过创建 OAuth 应用程序的组织确定 OAuth 应用程序，则系统会提示您先从下拉菜单中选择组织名称，然后从该组织中可用的 OAuth 应用程序列表中选择 OAuth 应用程序。 **组织**下拉菜单仅显示您具有**组织所有者**访问权限的组织。 7 查看应用程序详细信息，然后单击**添加**。
移除在其他组织中创建并有权访问您组织的 OAuth 应用程序。	1 单击**身份与访问管理 > OAuth 应用程序**。 2 从显示的 OAuth 应用程序列表中，选择要阻止其访问您组织的应用程序。 3 单击**移除**。
查看在您的组织中创建的应用程序。	单击**组织 > OAuth 应用程序**。 您可以在此处查看在您的组织中创建的所有应用程序。 ■ 修改应用程序。如果更改应用程序的范围，则位于其他组织中的应用程序实例不会包含所做的更改。要更新范围，**组织所有者**用户必须从其组织中移除该应用程序，然后重新添加该应用程序，或者编辑该应用程序以反映更新的范围。 ■ 从组织中移除应用程序。 ■ 添加已在组织中创建但尚未获得组织访问权限的应用程序。 ■ 创建应用程序。

目标	执行操作
在您的组织中创建新的 OAuth 应用程序。	1 单击**组织 > OAuth 应用程序**。 2 选择要添加的应用程序类型： ■ 对于服务器到服务器应用程序，请参见如何对服务器到服务器应用程序使用 OAuth 2.0 ■ 对于 Web 应用程序，请参见如何对 Web 应用程序使用 OAuth 2.0 ■ 对于本机/移动应用程序，请参见如何对本机应用程序和移动应用程序使用 OAuth 2.0
管理在您的组织中创建的 OAuth 应用程序。	单击**组织 > OAuth 应用程序**，然后选择要管理的应用程序： ■ 要修改 OAuth 应用程序，请单击**编辑**。 **注** 如果更改应用程序的范围，则位于其他组织中的应用程序实例不会包含所做的更改。要更新范围，**组织所有者**用户必须从其组织中移除该应用程序，然后重新添加该应用程序，或者编辑该应用程序以反映更新的范围。 ■ 要移除应用程序，请单击**删除**。 **注** 此操作无法恢复。使用这些客户端凭据的任何应用程序将无法再访问受保护的资源，且凭据将失效。 ■ 要添加已在组织中创建但尚未授予组织访问权限的服务器到服务器应用程序，请单击**添加到组织**。

如何对服务器到服务器应用程序使用 OAuth 2.0

如果您的应用程序需要直接访问另一台服务器，而无需用户授权，您可以创建 `Server to server app`。此选项基于 OAuth 2.0 `client credentials` 授权类型。在此流程中，您的应用程序使用其 OAuth 凭据检索访问令牌。

范围在服务器到服务器应用程序中特别重要。范围提供了一种方法，可对客户端有权访问组织中的哪些区域实施控制，即组织中的哪些角色以及哪些服务和权限级别。作为**组织所有者**用户，您可以向任何组织添加服务器到服务器应用程序。因此，虽然您可以为应用程序指定许多云服务的广泛访问权限，但访问权限最终由组织中包含的服务决定。向其添加 OAuth 应用程序的组织不包含应用程序范围所含的服务时，您会收到通知。

前提条件

- 您具有在此组织中添加和管理 OAuth 应用程序所需的权限。请参见 VMware Cloud Services 中提供哪些组织角色。

步骤

1. 登录到 Cloud Services 控制台。
2. 单击**组织 > OAuth 应用程序**，然后单击**创建新的 OAuth 应用程序**。
3. 选择**服务器到服务器应用程序**。
4. 通过输入名称和描述来注册客户端。

5 为新 OAuth 应用程序设置**访问令牌 TTL** 值。

访问令牌生存时间 (TTL) 定义了令牌的有效时间段。

- 默认访问令牌 TTL 时间为 30 分钟；
- 可以设置的最长访问令牌 TTL 时间为 300 分钟（5 小时）；
- 可以设置的最短访问令牌 TTL 时间为 1 分钟。

6 定义范围。

范围提供了一种方法，可对客户端有权访问组织中的哪些区域实施控制，即组织中的哪些角色以及哪些服务和权限级别。

7 单击**创建**以生成客户端凭据。

8 在**已创建 OAuth 应用程序**弹出窗口中，复制凭据或下载 JSON 文件，然后单击**继续**。

您应将凭据存储在一个安全的位置。

9 （可选）将应用程序添加到活动组织。

您可以跳过此步骤，稍后将应用程序添加到此组织和其他组织。请参见 如何管理 OAuth 2.0 应用程序。

后续步骤

将凭据粘贴到您的脚本。

如何对 Web 应用程序使用 OAuth 2.0

如果您的应用程序是在服务器上运行的常规 Web 应用程序并且需要用户授权，则可以创建 `Web app`。此选项基于 OAuth 2.0 `authorization code` 授权类型。在此流程中，用户在您的应用程序访问任何资源之前对其进行授权，并且应用程序会检索访问令牌和（可选）刷新令牌。

前提条件

- 您具有在此组织中添加和管理 OAuth 应用程序所需的权限。请参见 VMware Cloud Services 中提供哪些组织角色。

步骤

1 登录到 Cloud Services 控制台。

2 单击**组织 > OAuth 应用程序**，然后单击**创建新的 OAuth 应用程序**。

3 选择 **Web 应用程序**，然后单击**继续**。

4 输入应用程序详细信息以注册您的应用程序：

   a 键入新 Oauth 应用程序的名称和描述。

   b 至少输入一个重定向 URI。

   用户对您的客户端进行授权后，授权服务器会将用户重定向回您的客户端以访问通过访问令牌指定的 URI。最好添加多个 URI。使用格式 http://acme.com。

   c 指定访问令牌的时间范围。

   默认访问令牌生存时间 (TTL) 设置为 30 分钟。可以设置的最大值为 300 分钟（5 小时）。可以设置的最小值为 1 分钟。

   d 如果您希望访问令牌持续授权请求，请选择**发出刷新令牌**并设置**刷新令牌 TTL** 值。

   默认刷新令牌 TTL 为 30 分钟。可以设置的最大值为 300 分钟（5 小时）。可以设置的最小值为 1 分钟。

5 定义范围。

   范围提供了一种方法，可对客户端有权访问组织中的哪些区域实施控制，即哪些服务和权限级别。

6 选中**请求 ID** 复选框，获取有关授权您应用程序的用户的信息。

7 单击**创建**以生成客户端凭据。

8 复制凭据或下载包含您凭据的 JSON 文件。您应将凭据存储在一个安全的位置。

9 单击**继续**。

后续步骤

将凭据粘贴到您的脚本。

如何对本机应用程序和移动应用程序使用 OAuth 2.0

诸如原生应用和移动应用之类的公用客户端无法维护客户端密钥的机密性。将 OAuth 2.0 用于原生应用和移动应用时，我们会生成应用 ID，并使用用于代码交换的公钥 (PKCE) 提供额外的验证。

PKCE 是一种保护未使用客户端密钥的公用客户端的技术。有关将 PKCE 与移动应用配合使用的详细信息，请参见此博客。

前提条件

- 您具有在此组织中添加和管理 OAuth 应用程序所需的权限。请参见 VMware Cloud Services 中提供哪些组织角色。

步骤

1 单击您的用户名并选择**查看组织 > OAuth 应用程序**，然后单击**创建新的 OAuth 应用程序**。

2 选择**原生/移动应用**，然后单击**继续**。

3 输入应用程序详细信息以注册您的应用程序：

a 键入新 Oauth 应用程序的名称和描述。

b 至少输入一个重定向 URI。

用户对您的客户端进行授权后，授权服务器会将用户重定向回您的客户端以访问通过访问令牌指定的 URI。最好添加多个 URI。使用格式 http://acme.com。

c 指定访问令牌的时间范围。

默认访问令牌生存时间 (TTL) 设置为 30 分钟。可以设置的最大值为 300 分钟（5 小时）。可以设置的最小值为 1 分钟。

d 如果您希望访问令牌持续授权请求，请选择**发出刷新令牌**并设置**刷新令牌 TTL** 值。

默认刷新令牌 TTL 为 30 分钟。可以设置的最大值为 300 分钟（5 小时）。可以设置的最小值为 1 分钟。

4 定义范围。

范围提供了一种方法，可对客户端有权访问组织中的哪些区域实施控制，即哪些服务和权限级别。

5 选中**请求 ID** 复选框，获取有关授权您应用程序的用户的信息。

6 单击**创建**以生成客户端凭据。

7 复制应用程序 ID 或下载包含应用程序 ID 的 JSON 文件。您应将这些凭据存储在一个安全的位置。

8 单击**继续**。

后续步骤

将凭据粘贴到您的脚本。

OAuth 应用程序与 API 令牌的区别

您可以使用 OAuth 应用程序和 API 令牌与 VMware Cloud Services API 进行交互。

API 令牌由组织中的用户颁发，并与用户的帐户以及从中生成 API 令牌的组织相关联。OAuth 应用程序由组织中的用户创建后，将充当服务器到服务器交互中的实体，并可在多个组织中使用。只有创建 API 令牌的用户才能执行 API 令牌管理。OAuth 应用程序的所有者是创建该应用程序的组织，可由作为**组织所有者**或具有**开发人员**角色的**组织成员**的用户进行管理。

您可以使用 OAuth 应用程序和 API 令牌自动处理与 VMware Cloud Services 交互的进程。不同之处在于，API 令牌在访问令牌中包含用户帐户，而 OAuth 应用程序在执行授权时无需用户帐户。选择使用 API 令牌或 OAuth 应用程序进行 API 调用时，必须考虑交互中涉及的 API 服务的特定要求。一些 API 要求用户帐户为经身份验证的实体，而其他一些 API 则不作要求。例如，如果您在 VMware Cloud Services 中调用 API 以获取组织的计费和订阅信息，则可以使用服务器到服务器类型的 OAuth 应用程序或 API 令牌调用 API 服务，因为它不要求通过用户凭据进行身份验证，并且也接受客户端凭据。如果组织的用户使用 API 更新其密码，则该 API 要求用户充当身份验证实体。

重要说明 使用服务器到服务器类型的 OAuth 应用程序自动调用 Cloud Services 之前，必须先查阅相关的 API 文档。

如何在 VMware Cloud Services 中审核事件日志

通过使用 VMware Aria Operations for Logs 的关联实例，您可以监控在执行用户登录、用户管理、API 令牌、OAuth 应用程序和计费等活动时组织用户触发的事件。

VMware Aria Operations for Logs 是一项 VMware Cloud 服务，您需要付费或试用订阅才能使用。有关不同订阅选项的信息，请参见 VMware Aria Operations for Logs (SaaS) 订阅和计费。

通过使用 VMware Aria Operations for Logs 服务，您可以使用各种审核功能，例如日志筛选、存档和转发。通过在 Cloud Services 控制台中启动 VMware Aria Operations for Logs 服务，可以访问您组织的审核数据。您可以打开 **VMware Cloud Services 的审核事件**仪表板，在其中直观了解组织中的事件。如果默认情况下未激活该仪表板，请从**仪表板**页面的**内容包仪表板**选项卡中选择该仪表板以进行查看。

有关使用 VMware Aria Operations for Logs 的详细信息，请参阅使用 VMware Aria Operations for Logs (SaaS)。

注 如果您的组织没有 VMware Aria Operations for Logs 服务订阅，但您希望查看当前或过去一段时间内的 VMware Cloud services 日志事件，要解决此需求，可以通过第 12 章 我如何获取支持获取审核报告。您将在创建支持请求后的 48 小时内通过电子邮件收到指定时间段的报告且报告采用加密的 CSV 文件格式。

谁可以在 VMware Aria Operations for Logs 中查看审核数据

组织中具有 **VMware Aria Operations for Logs 用户**或 **VMware Aria Operations for Logs 管理员**服务角色的所有用户都可以在关联的 VMware Aria Operations for Logs 服务实例中访问组织的所有审核数据。

VMware Cloud Services 捕获哪些审核事件

事件日志提供有关用户操作的信息，如事件名称、触发事件的用户以及事件的时间和位置。作为**组织所有者**用户，您可以使用 VMware Aria Operations for Logs 的关联实例查看您组织的审核事件。

VMware Cloud services 捕获 Cloud Services 控制台中与访问和帐户管理、计费和订阅用户活动相关的一系列审核事件。如果使用自动化功能管理组织中的某些资源，则某些事件可能由调用方（而不是用户）触发。

搜索和筛选 VMware Cloud Services 审核事件

您可以通过以下两种方式搜索和筛选组织的日志事件：使用 **VMware Cloud Services 的审核事件**内容包中已保存的查询；创建自定义查询。

您可以从 vRealize Log Insight Cloud 实例的**内容包**菜单中访问内容包。有关详细信息，请参见使用内容包。

您可以通过自定义查询 VMware Cloud Services 审核事件，在 vRealize Log Insight Cloud 服务的**浏览日志**页面中搜索和筛选日志事件。要仅查看 VMware Cloud Services 审核事件，作为搜索条件，请选择 **log_type**，然后选择 **Contains**，并输入 **`csp-audit`**。要搜索特定事件，请创建一个包含事件类型的查询。

VMware Cloud Services 的审核事件

表 10-1. 帐户管理

审核事件名称	事件类型	描述
UserLogin	csp__user_login	用户登录成功。
UserLogout	csp__user_logout	用户注销成功。
GenerateApiToken	csp__generate_api_token	用户生成了个人 API 令牌。
RevokeApiToken	csp__revoke_api_token	用户撤销了个人 API 令牌。
RevokeAllApiTokens	csp__revoke_all_api_tokens	用户撤销了所有个人 API 令牌。
RefreshTokenExchangeFailed	csp__refresh_token_exchange_failed	用户尝试通过 API 令牌刷新生成访问令牌，但未成功。
FirstLogin	csp__first_login	用户首次登录时分配了邀请中的角色。
LinkAccount	csp__link_account	用户将其企业联合帐户链接到了其 VMware ID 帐户。此操作允许用户使用其企业凭据登录 VMware Cloud Services。
UnlinkAccount	csp__unlink_account	用户更改了链接到其 VMware ID 的帐户。
CreateOrgOAuthApp	csp__create_org_o_auth_app	调用方在组织中创建了 OAuth 应用程序。
UpdateOrgOAuthApp	csp__update_org_o_auth_app	调用方在组织中更新了 OAuth 应用程序。
DeleteOrgOAuthApp	csp__delete_org_o_auth_app	调用方在组织中删除了 OAuth 应用程序。
OrgOAuthAppNewSecretRotation	csp__org_o_auth_app_new_secret_rotation	调用方在组织中轮换了 OAuth 应用程序的密钥。
ActivateMfa	csp__activate_mfa	具有 VMware ID 的用户激活了 MFA 设备。

表 10-1. 帐户管理 （续）

审核事件名称	事件类型	描述
DeactivateMfa	csp__deactivate_mfa	具有 VMware ID 的用户取消激活了 MFA 设备。
TurnOnMfa	csp__turn_on_mfa	具有 VMware ID 的用户为其帐户启用了多因素身份验证。
TurnOffMfa	csp__turn_off_mfa	具有 VMware ID 的用户为其帐户禁用了多因素身份验证。
RegenerateMfaRecoveryCodes	csp__regenerate_mfa_recovery_codes	具有 VMware ID 的用户重新生成了一组新的恢复代码以进行多因素身份验证。
UpdateMfaAttributes	csp__update_mfa_attributes	具有 VMware ID 的用户更新了其帐户的 MFA 设置。
GenerateNewMfaActivationSecret	csp__generate_new_mfa_activation_secret	具有 VMware ID 的用户生成了新的激活密钥，以便为其帐户设置 MFA。
InvitationSentAck	csp__invitation_sent_act	向用户发送邀请时创建了内部通知。
CreateMspInvitation	csp__create_msp_invitation	载入新提供商组织的电子邮件邀请发送给了新的服务提供商。
UpdateMspInvitation	csp__update_msp_invitation	载入新提供商组织的更新电子邮件邀请发送给了新的服务提供商。
DeleteMspInvitation	csp__delete_msp_invitation	撤销了发送给新服务提供商的载入新提供商组织电子邮件邀请。

表 10-2. 组织管理

审核事件名称	事件类型	描述
CreateOrganization	csp__create_org	用户创建了一个新组织。
UpdateOrganization	csp__update_org	用户更新了现有组织。
DeleteOrganization	csp__delete_org	用户删除了现有组织。
InviteExistingUserToOrganization	csp__invite_existing_user_to_org	现有用户已添加到组织。
RemoveUserFromOrganization	csp__remove_user_from_org	现有用户已从组织中移除。
UpdateUserRolesOnOrganization	csp__update_user_roles_on_org	现有用户的角色已更新。
InviteNonExistingUserToOrganization	csp__invite_non_existing_user_to_org	电子邮件邀请发送给了新用户。
RevokeUserInvitations	csp__revoke_user_invitations	撤销了通过电子邮件发送给用户的邀请。
RemoveClientFromOrganization	csp__remove_client_from_org	用户移除了分配给组织的 OAuth 应用程序。该操作不会删除 OAuth 应用程序。

表 10-2. 组织管理 （续）

审核事件名称	事件类型	描述
AssignRolesToClientOnOrganization	csp__assign_roles_to_client_on_org	调用方将服务/组织角色分配给了组织中的客户端。该操作指示首次分配给以前从未分配过角色的客户端。
UpdateClientRolesOnOrganization	csp__update_client_roles_on_org	调用方将服务/组织角色更新到了组织中的客户端。
UpdateUserDefaultOrganization	csp__update_user_default_org	用户更新了对其帐户显示的默认组织。此操作仅适用于属于多家组织的成员的用户。

表 10-3. 组

审核事件名称	事件类型	描述
RemoveGroupFromOrganization	csp__remove_group_from_org	用户从组织中移除了现有组。
AssignRolesToGroupOnOrganization	csp__assign_roles_to_group_on_org	用户将组织和服务角色分配给了组织中新创建的组。
UpdateGroupRolesOnOrganization	csp__update_group_roles_on_org	用户更新了组织中现有组的角色分配。
CustomGroupAddClients	csp__custom_group_add_clients	用户将新成员添加到了组织中的自定义组。
CustomGroupRemoveClients	csp__custom_group_remove_clients	用户从组织中的自定义组中移除了现有成员。

表 10-4. 计费和订阅

审核事件名称	事件类型	描述
CreateSubscription	csp__create_subscription	用户为新服务或现有服务创建了订阅。
AddOrgPaymentMethod	csp__add_org_payment_method	用户将新付款方式添加到了其组织。
RemoveOrgPaymentMethod	csp__remove_org_payment_method	用户从其组织中移除了付款方式。
UpdateOrgDefaultPaymentMethod	csp__update_org_default_payment_method	用户更新了组织的默认付款方式。
AddDetailsToOrg	csp__add_details_to_org	用户将公司地址和/或其他“计费和订阅”详细信息添加到了组织。
UpdateOrgAddress	csp__update_org_address	用户在其组织的“计费和订阅”详细信息中更新了公司地址。
UpdateOrgCommerceData	csp__update_org_commerce_data	用户更新了其组织的“计费和订阅”详细信息（货币、年度计费日期等）
UpdateOrgTaxId	csp__updated_org_tax_id	用户在其组织的“计费和订阅”详细信息中更新了税务 ID。

表 10-4. 计费和订阅 （续）

审核事件名称	事件类型	描述
UpdateOrgPoReferenceNumber	csp__update_org_po_reference_number	用户设置了新的组织 PO 参考编号。
IncomingOrder	csp__incoming_order	调用方创建了服务订阅订单。

表 10-5. 身份监管和管理

审核事件名称	事件类型	描述
ApproveDenyEntitlementRequest	csp__iga_entitlements_requests_approval	授权请求通过了**组织所有者**批准或被拒。
CreateEntitlementRequest	csp__iga_register_entitlements_request	用户创建了授权请求。
CreateEntitlementRequestForNonOrgMember	csp__iga_register_entitlements_request_non_org_member	新的非组织用户创建了授权请求。
CancelEntitlementRequest	csp__iga_delete_entitlement_request	用户取消了授权请求。
CancelEntitlementRequestForNonOrg	csp__iga_delete_entitlement_request_non_org_member	新的非组织用户取消了已由同一用户提交的授权请求。
EnablingGovernance	csp__iga_status_change	为组织激活了身份监管和管理。
UpdateGovernancePolicies	csp__iga_update_governance_policies_request	用户已更新身份监管和管理策略。

如何在 VMware Cloud Services 中创建 NIST 登录前通知

为了满足 NIST 800-53 AC-8 审核要求，您必须能够向访问您组织的**组织成员**用户显示登录前通知。

NIST 通知将应用于用户从其登录到 VMware Cloud Services 的域，而与用户所属的组织无关。当用户从创建了 NIST 通知的域登录到组织时，他们会看到一个对话框，要求他们阅读并接受通知条款，然后再进入密码输入页面。

作为**组织所有者**，您可以通过在 VMware Customer Connect 上提交支持请求来请求自定义 NIST 800-53 AC-8 通知消息。需要在支持请求中包含以下信息：

- 要为其应用 NIST 通知的企业域；
- 希望在 NIST 通知对话框中显示的文本；
- 所有所需语言的文本本地化版本；
- 您的 VMware Cloud Services 组织的名称。

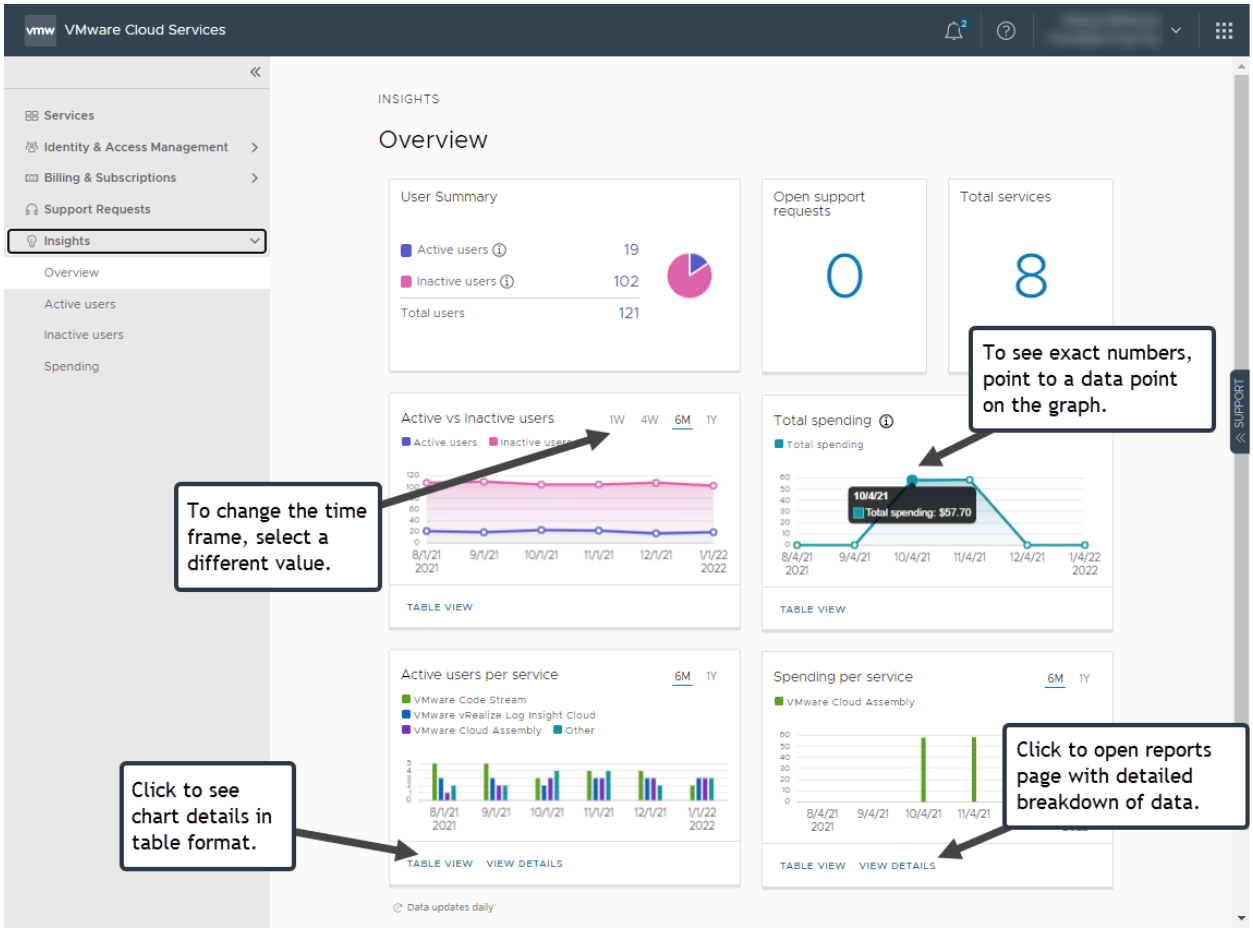
NIST 通知由 VMware 技术支持在验证您的**组织所有者**状态和域后手动实施。

如何使用数据见解仪表板

作为**组织所有者**用户，您可以通过 Cloud Services 控制台中的**见解**仪表板查看一段时间内组织中的服务使用情况。

要访问**见解**仪表板，请选择**见解 > 概览**。

见解仪表板简要显示了您组织中的用户在预定义时间段内的活动级别信息。您可以获取以下信息：组织中的活跃用户总数和非活跃用户总数、每个服务的活跃用户数和非活跃用户数、所有服务的总支出以及每个服务的支出明细。



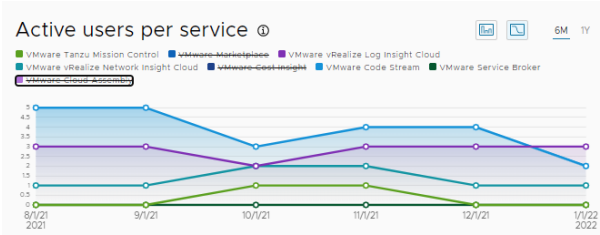
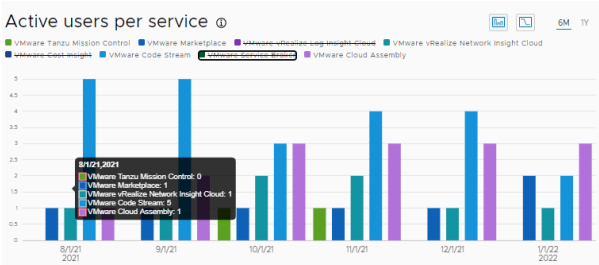
见解仪表板上的数据每天更新一次。

使用数据见解仪表板还可以执行哪些操作

作为**组织所有者**用户，您可以通过访问**活跃用户**、**非活跃用户**和**支出**仪表板获取服务、使用情况和成本的详细数据细目。您可以筛选数据以查看每个选项卡上显示的部分信息。

“活跃用户”仪表板

活跃用户仪表板显示有关组织中每个服务的所有活跃用户的信息。活跃用户是指在 60 天内至少登录过 VMware Cloud services 一次的那些用户。

目标	执行操作
在数据的图形视图和图表视图之间切换	单击仪表板右上角的图形 ( ) 或图表 ( ) 图标。
要更改数据报告的时间段，请执行以下操作：	通过单击仪表板右上角的相应图标选择不同的时间段。可以在六个月和一年之间选择。
按特定服务筛选活跃用户	单击要从视图中排除的服务的名称。  排除的服务名称显示已划掉。要在数据视图中重新包含服务，请单击其名称。
查看特定月份中的每服务活跃用户细目	指向图表或图形中的数据点。 
在表格视图中查看图表详细信息	单击**在表视图中显示详细信息**链接。
查看活跃用户详细信息	数据图表下方的表提供了有关组织中所有活跃用户的详细信息，例如名称、电子邮件和自上次登录以来的天数。 通过单击后退和前进图标滚动表中的页面。

“非活跃用户”仪表板

非活跃用户仪表板显示有关组织中每个服务的所有非活跃用户的信息。非活跃用户是指过去 60 天内未登录过 VMware Cloud services 的那些用户。

目标	执行操作
在数据的图形视图和图表视图之间切换	单击仪表板右上角的图形 ( ) 或图表 ( ) 图标。
要更改数据报告的时间段，请执行以下操作：	通过单击仪表板右上角的相应图标选择不同的时间段。可以在六个月和一年之间选择。
按服务筛选非活跃用户	单击要从视图中排除的服务的名称。
查看特定月份中的每服务非活跃用户细目	指向图表或图形中的数据点。
在表格视图中查看图表详细信息	单击**在表视图中显示详细信息**链接。

目标	执行操作
查看非活跃用户详细信息	数据图表下方的表提供了有关组织中非活跃用户的详细信息，例如名称、电子邮件、自上次登录以来的天数以及上次操作的日期。 通过单击后退和前进图标滚动表中的页面。
从组织中移除非活跃用户	选中用户名旁边的复选框，然后单击**从组织中移除**

“每服务开支”仪表板

此仪表板显示组织中一段时间内每个服务的每月支出。您看到的成本值以您组织的默认货币形式表示。

目标	执行操作
在数据的图形视图和图表视图之间切换	单击仪表板右上角的图形 () 或图表 () 图标。
要更改数据报告的时间段，请执行以下操作：	通过单击仪表板右上角的相应图标选择不同的时间段。可以在六个月和一年之间选择。
筛选显示支出的服务	单击要从视图中排除的服务的名称。
查看特定月份中服务的成本细目	指向图表或图形中的数据点。
在表格视图中查看图表详细信息	单击**在表视图中显示详细信息**链接。

在 Cloud Services 控制台中使用项目涉及哪些内容

VMware Cloud Services 使用项目作为一种方法，将组织的资源分组到不同的段，并为用户和组分配对每个段中资源的访问权限。这样，**组织所有者**能够以逻辑方式组织、映射和跟踪其云服务资源的使用情况。

当您考虑 VMware Cloud Services 中的资源时，请想象一下特定服务的预定义、可衡量和逻辑部分。通过在项目中组织服务资源，**组织所有者**用户可以跨部门或成本中心衡量和跟踪企业中云服务的使用情况

重要说明 到目前为止，只有少数 VMware Cloud services 已启用，可以使用 Cloud Services 控制台中的项目功能。要了解您正在使用的服务是否可以利用项目进行资源分组，请查阅该服务的文档或联系 VMware 技术支持。

假设您的组织中有两个项目 - 项目 1 和项目 2，以及三个服务 - 服务 A、服务 B 和服务 C。

- 为项目 1 启用服务 A 和 B。
- 为项目 2 启用服务 B 和 C。

通过对已启用的服务进行资源分组，服务 B 的资源可以在两个项目中使用，而服务 A 和服务 C 的资源分别在一个项目中使用。

如何在 Cloud Services 控制台中创建项目

要设置和管理项目，您必须在组织中具有**组织所有者**或**项目管理员**角色。可以从 Cloud Services 控制台中的**身份与访问管理 > 项目**设置新项目。

设置新项目涉及三个步骤：

1 定义新项目的名称。

新项目将保持为空，直到启用您计划与其配合使用的服务。

2 查看项目的已启用服务和资源。

如果服务列在**已启用服务**部分下，并且资源列在**资源**表中，您便知晓已为您的项目启用了该服务。

3 为用户和/或组分配对新项目的访问权限。

如何从我的组织中删除项目

仅当满足以下两个条件时，才能删除项目：

- 项目没有与其关联的已启用服务和资源。
- 用户和/或组未分配有项目的访问权限。

计费和订阅

11

具有**组织所有者**角色的 VMware Cloud Services 用户可以查看计费和订阅详细信息，并管理其组织的付款方式。具有额外**计费只读**角色的**组织成员**用户可以查看其组织的计费和订阅详细信息，但无法管理付款方式。

VMware Cloud Services 中的每个组织都与一个计费帐户相关联。

您可以按需使用 VMware Cloud services，也可以通过购买 1 年期或 3 年期订阅进行使用。采购订单概述了订阅中承诺的容量、条款开始和结束日期以及协商价格。VMware Cloud Services 根据采购订单中列出的条款向您计费。

您每月会收到一张发票或业务明细报表，其中包括组织通过 VMware 购买的服务所产生的所有成本。

如果您的组织从多个卖方购买了服务，则**计费和订阅**页面将显示所有卖方的信息。但是，通过非 VMware 卖方购买的服务的应计成本和服务费用信息无法通过 Cloud Services 控制台 查看。请与相应卖方联系以获取此信息。

请阅读以下主题：

- VMware Cloud Services 计费和订阅入门
- 如何管理组织的付款方式
- 如何使用 VMware Cloud Services 订阅和承付
- 如何使用“使用情况管理”仪表板
- 如何查看帐单和发票

VMware Cloud Services 计费和订阅入门

首次购买 VMware Cloud Services 订阅时，您会收到一封电子邮件，其中包含用于打开 VMware Cloud Services 上线工作流的链接。

作为首次用户和**组织所有者**，您可以在设置组织时提供地址和默认付款方式。VMware Cloud Services 根据在上线期间设置的计费详细信息对每个组织进行计费：

- 您企业的**地址**决定了组织可用的销售单位、货币选项、税费和付款方式。

  例如，美国地址以美元计费并征收销售税，英国地址以英镑计费并征收增值税。此外，在欧盟注册的每个组织都可以选择输入税务 ID。

- 组织的**付款时使用的货币**由销售单位决定，销售单位派生自业务地址所在的国家/地区。每家组织可以具有默认货币，以及根据组织的地址预先批准的例外货币。不同的销售单位可以与一种或多种货币相关联。要了解更多信息,请参见如何确定付款货币
- **默认付款方式**可以是 VMware 预付资金帐户、信用卡或按发票付款 (PBI)。您的组织在上线时可以选择的默认付款方式因您的计费帐户而异。

  例如，某些用户只能选择 PBI 作为付款方式，而其他用户可以选择 VMware 资金帐户和信用卡。

前提条件

- 您要在 VMware Cloud Services 的新组织中载入付费云服务。

步骤

1 在服务上线工作流的**创建组织**步骤中，提供您组织的计费详细信息：

  a 输入组织的名称。

  b 提供企业的地址。

  重要说明 在此步骤中提供的业务地址必须通过地址验证检查并符合验证规则。要了解更多信息,请参见需要了解有关地址验证的哪些内容

  c 如果有多个货币选项可用，请选择将用于向您的组织进行计费的货币。

  d 选择默认付款方式。

  注 在组织中载入服务后，**组织所有者**用户随时可以如何更改组织的默认付款方式。无法在 Cloud Services 控制台中更改用于向组织进行计费的货币。要切换到其他货币，必须提交支持票证。

2 单击**完成**。

结果

您的组织计费帐户现已创建。现在，您可以从 Cloud Services 控制台 中的**计费和订阅**菜单中获取计费信息，以及管理付款方式和服务订阅。

需要了解有关地址验证的哪些内容

VMware Cloud Services 会对为您组织提供的业务地址应用验证标准。

作为**组织所有者**，您在服务上线期间设置组织时或者向现有组织添加新服务或订阅时，会输入业务地址。要通过验证，组织地址必须包含有关街道地址、邮政编码、城市、州或省（如果适用）以及国家/地区的正确信息。在以下情况下，将自动执行验证检查：

- 在服务/订阅上线期间输入或更新业务地址。
- 从**组织 > 详细信息**页面更新业务地址。

下表详细介绍了可能的验证检查结果以及需要时可以采取的操作。

如果...	则...
组织地址验证成功。	继续执行服务/订阅上线工作流的下一步。
组织地址不符合验证规则。提供了符合要求的建议地址。	打开**编辑或选择地址**弹出窗口，其中显示了原始地址以及符合验证规则的建议地址。 ■ 如果选择建议的地址，则继续执行工作流的下一步。 ■ 如果决定保留原始地址，则必须承认该地址不符合验证规则，并同意授权 VMware 对该地址进行所有必要的更改，以使其符合要求。为此，请选中**编辑或选择地址**弹出窗口上的相应复选框。 ■ 要修改为组织提供的原始地址，请单击**编辑地址**按钮。这将返回到“组织资料”页面，可以在其中进行必要的更改。
无法验证组织地址。未提供符合要求的建议地址。	当地址验证失败且没有建议替代地址时，将打开一个弹出窗口，提示您执行以下操作之一： ■ 编辑地址。 ■ 选中相应的复选框，同意授权 VMware 对组织地址进行所有必要的更改，以使其符合验证规则。只有在接受同意后，才能继续执行服务/订阅上线工作流。
VMware 在**组织所有者**同意后更新了组织地址。	当您以**组织所有者**身份登录 VMware Cloud Services 时，将打开一个弹出窗口，其中显示了更新的地址。 ■ 如果接受经过验证的新地址，则将替换现有的组织地址。所有**组织所有者**用户都将收到有关更改的应用程序内通知。 ■ 如果取消经过验证的新地址，则每当打开服务/订阅上线工作流时，都会提示您更改地址以符合验证规则。

如何使用 VMware Cloud Services 中的计费和订阅页面

Cloud Services 控制台中的**计费和订阅**部分包含几个基本页面，可帮助您查看组织的活动并管理用于服务和订阅的付款方式。

概览	**概览**页面显示过去一个月组织使用的所有服务的当前应计成本和费用。如果通过多个卖方购买了订阅，则可从此页面访问查看每个卖方的详细信息。 要了解更多信息，请参见如何获取组织的计费信息
管理付款方式	在**管理付款方式**页面中，可以将新的付款方式添加到组织并更改默认付款方式。 要了解更多信息，请参见如何管理组织的付款方式
订阅	**订阅**页面显示组织中购买的所有 VMware Cloud Services 订阅的详细信息。 要了解更多信息，请参见如何使用 VMware Cloud Services 订阅和承付
优惠额度	**优惠额度**页面显示可用的优惠额度，您可以根据组织的每月费用应用和兑换这些优惠额度。 要了解更多信息，请参见如何使用优惠额度付款
发票和帐单	在**发票和帐单**页面中，可以查看和下载组织的业务明细报表和发票。 要了解更多信息，请参见如何查看帐单和发票

如何获取组织的计费信息

可以从 Cloud Services 控制台中**计费和订阅**菜单下的**概览**页面查看组织的计费信息。

作为**组织所有者**用户或具有额外**计费只读**角色权限的**组织成员**用户，您可以查看从 VMware 购买的所有服务的以下计费信息：

- 从 VMware 购买的所有服务的当前计费周期内应计成本和费用；
- 应用于当前成本的优惠额度；
- 从 VMware 购买的所有服务的上一个计费周期内付款和未结余额；
- 按月列出的所有服务的所有采购、收费、折扣等详细说明。

注 对于通过卖方所购买服务的计费信息，您必须访问卖方的计费控制台。要了解更多信息,请参见如何查看卖方信息

您当前的成本

当前成本部分反映您从 VMware 购买的服务的成本。例如，每个 CPU 每小时的私有云使用情况。这些都是应计成本，反映了从当前计费周期开始直到查看当日（包括查看日）这段时间服务的使用情况。应计成本仅反映组织中服务的按需使用情况，不包括承付成本。此信息每天刷新一次。

当前成本部分还提供了有关您可能已从 VMware 折扣计划收到的任何优惠额度和折扣的信息。

您的上一个计费周期

在**上次帐单**部分中，可以查看上一个计费周期产生的费用。计费周期由在组织中设置第一个服务的日期决定，且为期一个月。例如，如果**组织所有者**在 15 日启用组织的第一个服务，那么该组织所有服务的计费周期为当月 15 日至下个月的 14 日。

上次帐单部分提供上一个计费周期收取的按需服务和承付服务费用摘要。要查看、下载并打印上一个计费周期的详细业务明细报表文件，请单击**上次帐单**部分底部的**查看帐单 (PDF)** 链接。

要查看并打印任何最近 15 个业务明细报表、按需发票和年度承付发票，请单击**所有帐单**链接。有关详细信息，请参见如何查看帐单和发票。

有些情况下，云服务可能会在非计费周期开始日期的其他日期估算某些使用项目的当前成本。在这种情况下，使用发生时间与帐单上显示的时间之间可能会存在时间延迟。有关云服务如何估算当前成本的详细信息，请参见如何估算我的当前成本。

如何估算我的当前成本

计费概览中的**当前成本**部分反映了组织中的服务在任意给定时间的成本。此部分显示的成本仅针对从 VMware 购买的服务。这些都是应计成本，反映了从定义的周期开始所用服务的使用情况。此定义的周期可能不同于计费周期。

要了解云服务如何估算其当前成本以及这些成本对计费周期产生的影响，请参见下表。

VMware Cloud Services	如何估算当前成本
VMware Cloud on AWS	VMware Cloud on AWS 的主机使用情况跟踪与计费周期一致。帐单上显示的主机使用情况是在计费期间发生的整个主机使用情况。 其他类型的使用情况（包括传出数据、IP 地址使用情况和重新映射以及 EBS 使用情况）在每月 5 日发送给您，包括直到上个月最后一天的使用情况。对于这些类型的使用情况，使用发生时间与帐单上显示的时间之间可能会存在时间延迟。延迟时间量取决于计费周期开始日期相对于当月 5 日的时间差。 有关详细信息，请参见 VMC 计费信息。

如何确定付款货币

VMware Cloud services 支持使用信用卡、资金帐户和优惠额度以各种货币支付服务费用。付款货币在设置组织时从选项列表中选择。

设置组织时，您输入的业务地址决定了在载入工作流的**组织和付款**步骤中提供给您的货币选项。组织可以使用默认货币付款，可以使用预先批准的例外货币付款，还可以使用美元（如果选择了**全球美元**选项）付款。有关服务上线的详细信息，请参阅 VMware Cloud Services 入门指南。

如果需要将付款货币更改为不同于组织中已定义的选项，可以随时进行此更改。请参见如何更改组织中的付款货币。

VMware Cloud services 支持两种销售单位：一种适合美国客户，一种适合非美国客户。美国客户只按美元结算，非美国销售单位中的国家/地区可按各种货币结算。这可能会对您造成哪些影响？

- 组织地址还决定了税收类型，例如销售税或增值税。税务 ID 用于帮助管理地方税。如果您具有免税资格或类似资格，您可能希望输入税务 ID。您可以在设置组织时输入税务 ID。也可以稍后在“组织”页面上通过单击您的用户名并选择**查看组织**来输入。
- 您可以使用任意帐单地址的任意信用卡支付服务费用。如果组织的付款货币不同于信用卡货币，您的信用卡提供商可能会向您收取境外交易费。
- 如果要更改您组织的地址，新地址必须与原始地址位于相同的销售单位。此外，您不能将地址更改为与原始地址使用不同货币的国家/地区。请参见下表，了解更多信息。

  如果需要更改为位于不同销售单位或具有不同货币的国家/地区的地址，请提交支持请求。

  如果需要将付款货币更改为不同于为组织设置的货币，则必须创建支持请求。要了解如何创建支持请求，请参见 第 12 章 我如何获取支持。
- 您可以使用任意资金帐户作为组织的付款方式，但前提是资金帐户的货币与组织的货币相同且属于同一销售单位。要使用资金帐户付款，计费帐户货币必须与资金帐户货币匹配，并且资金帐户货币必须与订单订阅货币匹配。

VMware Cloud Services 销售单位

可以使用下表中的信息确定支付服务费用时使用的货币。

表 11-1. 适用于非美国客户的销售单位国际汇兑

如果您组织的地址位于以下国家/地区...	您的默认付款货币为...
阿富汗、阿尔及利亚、美属萨摩亚、安哥拉、安圭拉、南极、安提瓜和巴布达、阿根廷、亚美尼亚、阿鲁巴、阿塞拜疆、巴哈马、巴林、孟加拉、巴巴多斯、白俄罗斯、伯利兹、贝宁、百慕大、不丹、玻利维亚、博奈尔岛、圣尤斯特歇斯和塞巴、博茨瓦纳、布韦岛、巴西、英属印度洋领地、文莱达鲁萨兰、布基纳法索、布隆迪、柬埔寨、喀麦隆、加拿大、佛得角群岛、开曼群岛、中非共和国、乍得、智利、哥伦比亚、科摩罗、刚果、库克群岛、哥斯达黎加、科特迪瓦、古巴、库腊索、吉布提、多米尼加、多米尼加共和国、东帝汶、厄瓜多尔、埃及、萨尔瓦多、赤道几内亚、厄立特里亚、爱沙尼亚、埃塞俄比亚、福克兰群岛、法罗群岛、斐济、芬兰、法属圭亚那、法属波利尼西亚、法国南部领土、加蓬、冈比亚、乔治亚、加纳、格林纳达、瓜德罗普岛、关岛、危地马拉、几内亚、几内亚比绍、圭亚那、海地、赫德岛和麦克唐纳群岛、洪都拉斯、香港特别行政区、印度、印度尼西亚、伊朗、伊拉克、以色列、牙买加、约旦、哈萨克斯坦、肯尼亚、基里巴斯、韩国、科威特、吉尔吉斯斯坦、老挝、黎巴嫩、莱索托、利比里亚、利比亚、中国澳门、马达加斯加、马拉维、马来西亚、马尔代夫、马里、马绍尔群岛、马提尼克、毛里塔尼亚、毛里求斯、马约特岛、墨西哥、密克罗尼西亚、摩尔多瓦、蒙特塞拉特、摩洛哥、莫桑比克、缅甸、纳米比亚、瑙鲁、尼泊尔、荷属安的列、新喀里多尼亚、新西兰、尼加拉瓜、尼日尔、尼日利亚、纽埃、朝鲜民主主义人民共和国、北马里亚纳群岛、阿曼、巴基斯坦、帕劳、被占的巴勒斯坦领土、巴拿马、巴布亚新几内亚、巴拉圭、秘鲁、菲律宾、皮特凯恩、波多黎各、卡塔尔、留尼汪、俄罗斯、卢旺达、圣巴托洛缪、圣赫勒拿、圣基茨和尼维斯、圣卢西亚、圣马丁、圣皮埃尔和密克隆群岛、圣文森特和格林纳丁斯、萨摩亚、圣多美和普林西比、沙特阿拉伯、塞内加尔、塞舌尔、塞拉利昂、新加坡、所罗门群岛、索马里、南非、南乔治亚和南桑威奇群岛、苏丹南部、斯里兰卡、苏丹、苏里南、斯瓦尔巴群岛和扬马延岛、斯威士兰、叙利亚、中国台湾、托塔吉克斯坦、坦桑尼亚、泰国、东帝汶、多哥、托克劳、汤加、特立尼达和多巴哥、突尼斯、土耳其、土库曼斯坦、特克斯和凯科斯群岛、图瓦卢、乌干达、乌克兰、阿拉伯联合酋长国、美属离岛、乌拉圭、乌兹别克斯坦、瓦努阿图、委内瑞拉、越南、维尔京群岛、瓦利斯和富图纳群岛、西撒哈拉、也门	USD
阿尔巴尼亚、安道尔、奥地利、比利时、波斯尼亚和黑塞哥维那、保加利亚、克罗地亚、塞浦路斯、捷克共和国、丹麦、法国、德国、希腊、格陵兰、匈牙利、冰岛、爱尔兰、意大利、拉脱维亚、列支敦士登、立陶宛、卢森堡、马其顿、马耳他、摩纳哥、黑山、挪威、波兰、葡萄牙、罗马尼亚、圣马力诺、塞尔维亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典、瑞士、荷兰、梵蒂冈、南斯拉夫、赞比亚、津巴布韦、奥兰群岛	EUR
直布罗陀、格恩西岛、马恩岛、泽西管区、英国	GBP
日本	JPY
中国、蒙古	CNY
澳大利亚、圣诞岛、科科斯群岛、诺福克岛	AUD

表 11-2. 适用于美国客户的销售单位 US

如果您组织的地址位于以下国家/地区	付款货币
United States of America	USD

如何更改组织中的付款货币

设置组织时，将在服务上线工作流中确定付款货币。设置组织的**组织所有者**用户可以选择默认货币，也可以选择预先批准的例外货币。

您组织的付款货币可以是以下货币之一：

- 基于业务地址的默认货币。

- 全球美元。
- 预先批准的其他货币。

前提条件

要更改组织中的付款货币，您必须在 VMware Customer Connect 中创建支持请求。组织所有者可以随时通过 Cloud Services 控制台发起更改请求。

.

步骤

1 登录到 Cloud Services 控制台，然后选择**计费和订阅 > 管理付款方式**。

2 单击**更改货币**按钮。

3 在打开的对话框窗口中，单击**创建支持请求**。

这将打开 VMware Customer Connect 上的 VMware 技术支持页面。

4 在**非技术支持**下，单击**获得指导性支持**。

5 在 **Cloud Services** 下，单击**计费和使用情况**，然后按照提示创建请求。

如何查看卖方信息

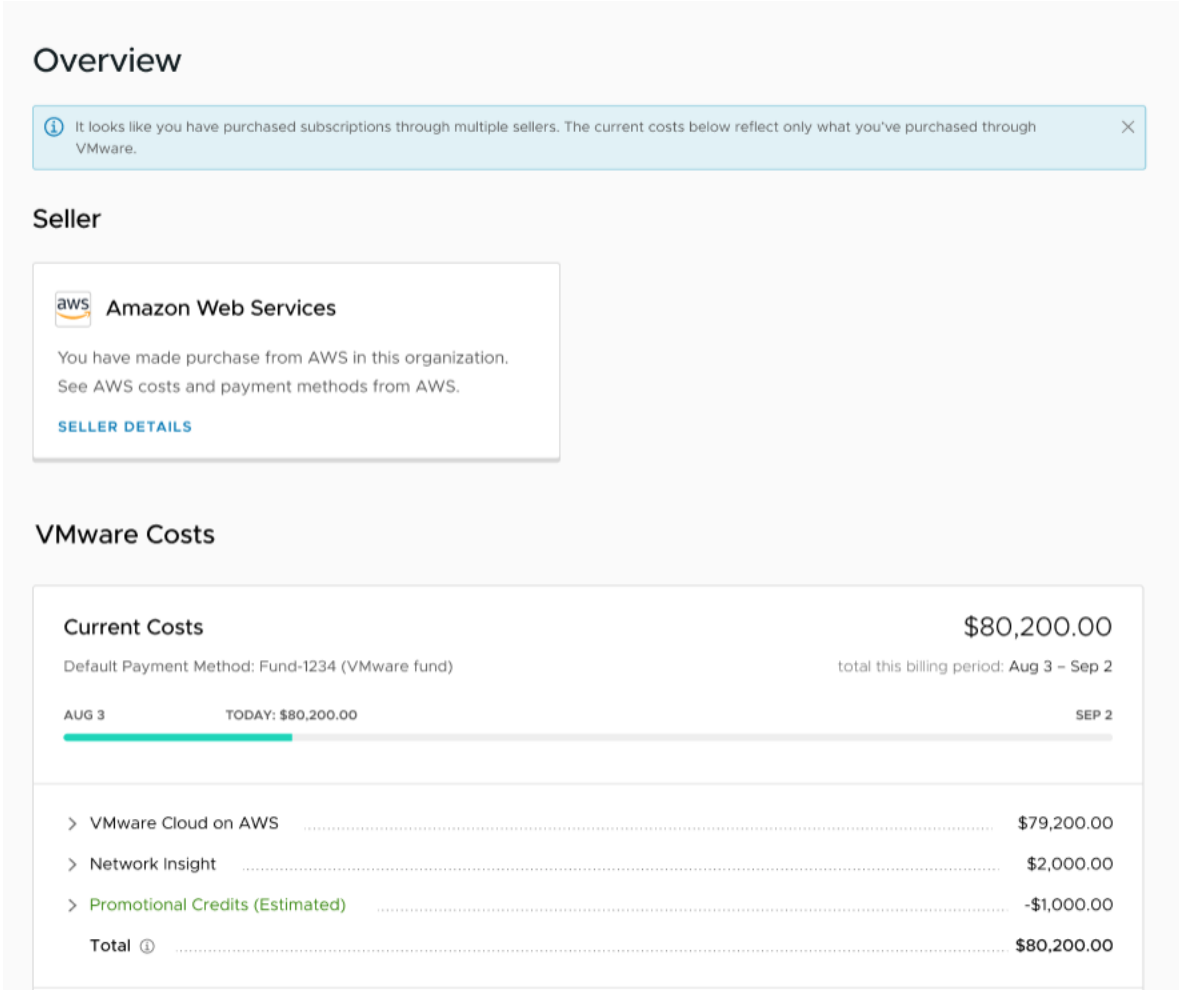
仅当您的组织拥有从一个或多个 VMware 合作伙伴购买的服务和订阅时，才会显示卖方信息。

组织中的每个卖方都由一个单独的图块表示。

步骤

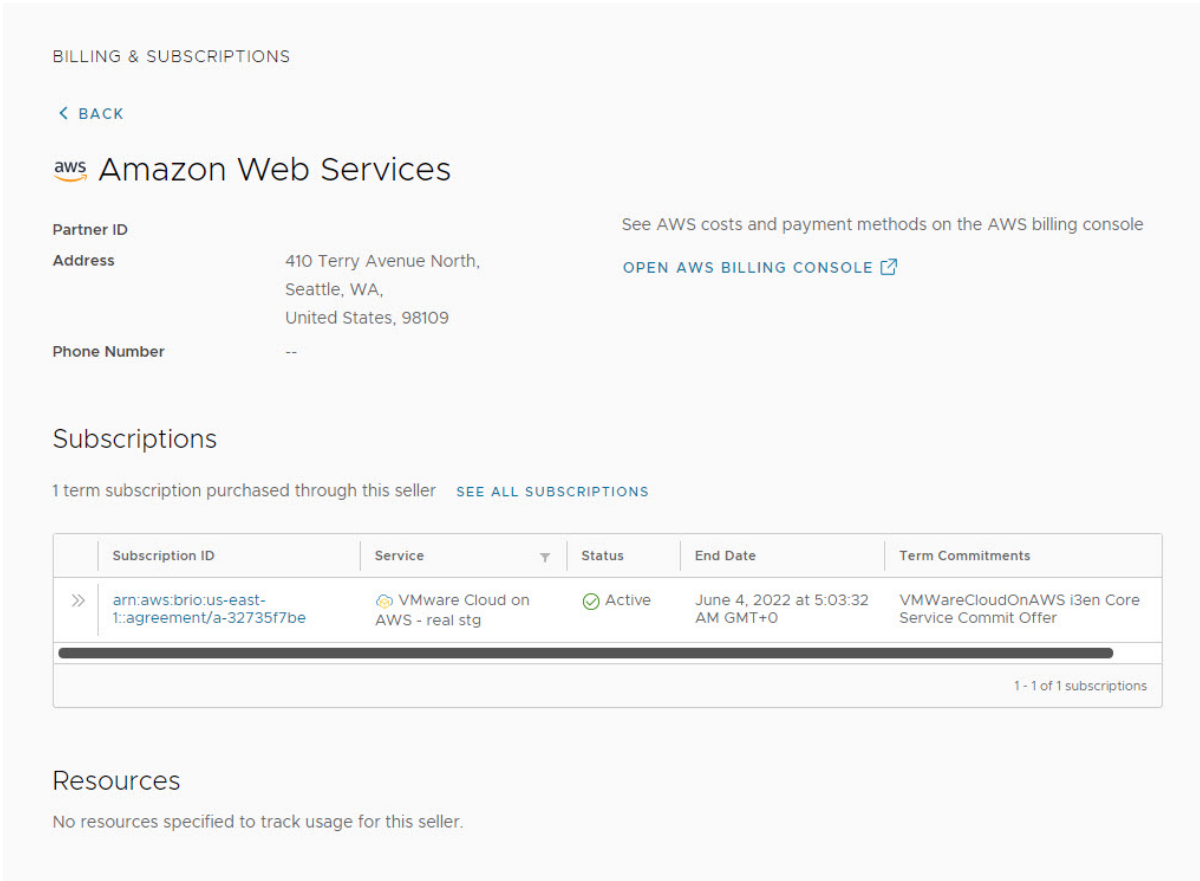
1 登录到 Cloud Services 控制台，然后选择**计费和订阅 > 概览**。

卖方部分列出了您的组织从其购买过服务的卖方。例如，如果组织从 VMware 和 Amazon Web Services 购买了服务，您将看到两个卖方。


Overview
It looks like you have purchased subscriptions through multiple sellers. The current costs below reflect only what you've purchased through VMware.
Seller
aws
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
$80,200.00
Default Payment Method: Fund-1234 (VMware fund)
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

2 要查看组织中从任何 VMware 合作伙伴卖方购买的服务和订阅，请单击其相应图块中的**卖方详细信息**链接。

此时将打开卖方的详细信息页面。



3 要查看与此卖方关联的成本和付款方式，请单击指向其计费控制台的链接。

4 要查看从此卖方所购买订阅的详细信息，请单击**订阅 ID** 链接。

这将打开订阅详细信息页面，您可以在其中查看其他详细信息，例如期限承付、订阅开始日期和结束日期、付款方式、订阅历史记录等。

后续步骤

如果您没有将 VMware 添加为您组织中的卖方，请了解如何将 VMware 添加为卖方，以便可以直接购买云服务。

如何向 VMware Cloud Services 注册合作伙伴卖方合同代码

通过非 VMware 合作伙伴卖方购买订阅时，您的订单可能包含折扣。作为**组织所有者**用户，在组织中载入服务后，您必须向 Cloud Services 控制台登记合作伙伴卖方提供的合同代码。

通过将合同代码与 VMware Cloud Services 中的卖方档案相关联，您可以确保订单中的折扣将体现在帐单中。

前提条件

- 您在组织中具有**组织所有者**角色。
- 您具有通过合作伙伴卖方购买的订阅的合同编号。
- 您已载入服务，并且卖方位于组织中。

步骤

1 登录到 Cloud Services 控制台，然后选择**计费和订阅 > 概览**。

页面的**卖方**部分列出了您的组织从其购买过服务的卖方。

2 单击卖方详细信息图标或页面中的**添加合同**链接。

3 在打开的弹出窗口中，键入合同编号，然后单击**提交**。

结果

合同代码现已与您的组织相关联，并将应用所有相关折扣。

您还能够为相关服务单独创建订阅。

如何将 VMware 添加为卖方

如果您的组织从非 VMware 卖方购买了 VMware Cloud services，则可以在载入服务时添加 VMware，也可以稍后添加。这样，您可以直接从 VMware 购买 VMware Cloud services，也可以从现有卖方购买。

将 VMware 作为卖方添加到组织中意味着您必须通过 VMware 创建计费帐户，并填写组织的档案。您可以通过添加组织的业务地址和首选付款方式来创建计费帐户。

前提条件

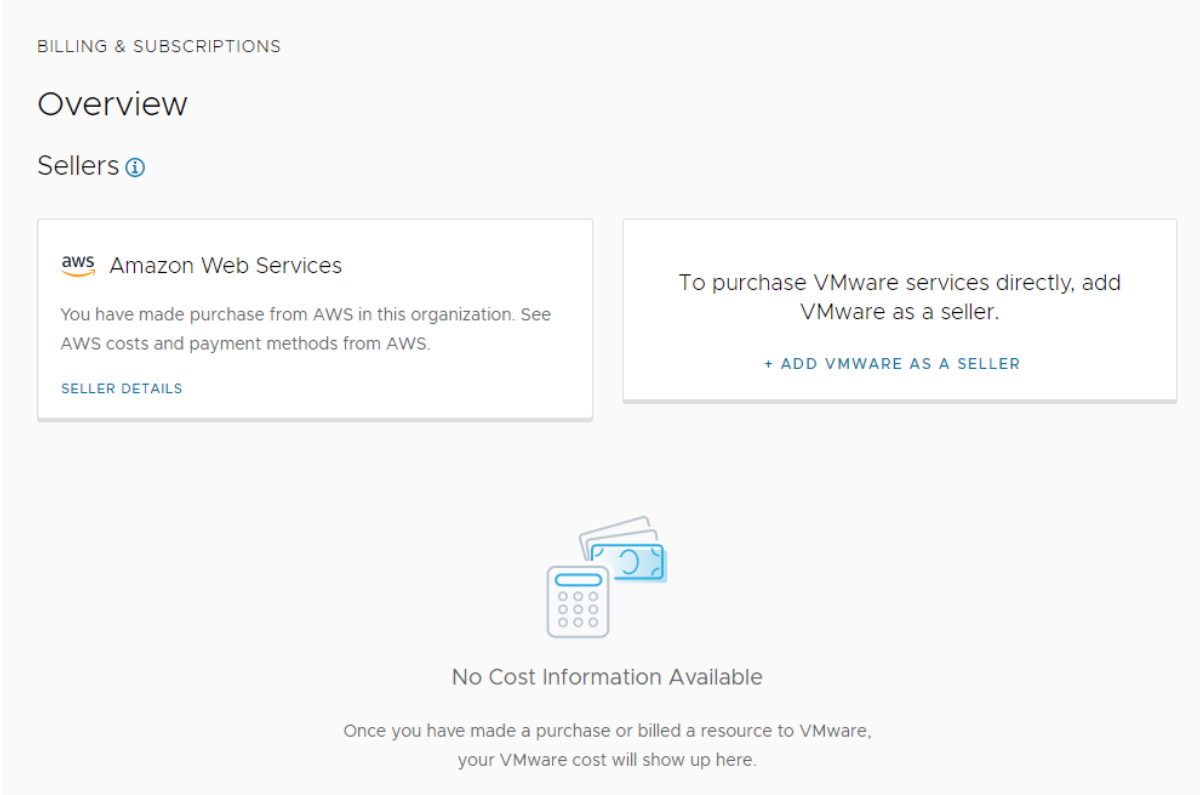
要在 Cloud Services 控制台中将 VMware 添加为卖方，您必须具有**组织所有者**角色，并且您的组织必须从非 VMware 卖方购买过服务。

步骤

1 使用您的 My VMware 帐户登录到 Cloud Services 控制台。

2 转到**计费和订阅 > 概览**。

卖方部分显示您组织中的非 VMware 卖方。



3 单击**将 VMware 添加为卖方**链接。

4 填写组织的档案：输入帐单地址并选择货币和付款方式。

> **注** 要在创建计费帐户后更改组织的货币，您必须提交支持请求。

5 查看并同意**服务条款**。

6 单击**完成**。

结果

VMware 现已添加为您组织中的卖方。

如何管理组织的付款方式

您的计费帐户决定了您的组织可以使用的付款方式。您可以使用资金帐户、信用卡或链接无限制按发票付款帐户。

资金帐户

要使用某个 VMware 资金帐户支付组织的费用，请将资金帐户链接到您的组织，然后将其中一个设置为默认付款方式。这样，您可以在所有组织中使用同一个资金帐户。您可以使用任意资金帐户，前提是它位于与 VMware Cloud services 关联的 VMware 授权帐户中且与组织使用同一种货币。有关详细信息，请参见如何使用资金帐户付款。

信用卡

除非您所在的国家/地区对信用卡使用没有任何限制，则可以使用信用卡支付服务费用。有关详细信息，请参见使用信用卡作为付款方式有哪些限制。

如果组织的付款货币不同于信用卡货币，您的信用卡提供商可能会向您收取境外交易费。有关详细信息，请参阅如何使用信用卡付款。

按发票付款帐户

如果新服务的销售订单与按发票付款 (PBI) 帐户相关联，则在服务上线期间它显示为付款方式。在这种情况下，PBI 付款方式受到限制，只能应用于包含在销售订单中的订阅，而不能作为默认付款方式添加到组织中。

如果要使用 PBI 帐户作为默认付款方式，用于支付组织产生的任何购买、资源和超额费用，您必须为组织中的所有服务激活无限制 PBI 以进行付款授权。启用无限制 PBI 需完成脱机批准过程，您可以通过提交支持请求来开始该过程。有关详细信息，请参阅如何使用发票付款。

您可以根据需要向组织中添加任意数量的付款方式，但只能将其中一个设置为默认付款方式。

如何添加新的付款方式

作为**组织所有者**用户，您可以向组织添加新的付款方式。在组织级别定义的付款方式可供所有**组织所有者**用户使用。

步骤

1 打开 Cloud Services 控制台，然后导航到**计费和订阅 > 管理付款方式**。

2 在页面的**其他付款方式**区域中，单击**添加付款方式**。

3 选择要添加的付款方式类型。

目的	执行操作
链接按发票付款帐户	选择一个或多个要添加的按发票付款帐户，然后单击**链接帐户**。 **注** 只能在组织级别将无限制 PBI 帐户添加为付款方式。如果要添加的 PBI 帐户受到限制，则必须先通过提交支持请求来激活无限制 PBI。
链接 VMware 资金帐户	选择要添加为付款方式的 VMware 资金帐户，然后单击**链接资金帐户**。
添加信用卡	添加信用卡详细信息，然后单击**添加卡**。 **注** 通过单击**添加卡并设为默认值**，您将更改组织的默认付款方式，这将影响使用默认付款方式的所有服务和订阅。

什么是默认付款方式

注册 VMware Cloud services 时，可以添加要用于支付组织费用的付款方式。这种付款方式将成为组织的默认付款方式，组织内的所有**组织所有者**用户都可以使用这种付款方式。

除非您为购买指定其他付款方式，否则默认付款方式将应用于支付组织中的所有购买、资源和超额费用。您可以在 Cloud Services 控制台的**计费和订阅 > 管理付款方式**选项卡中，为组织添加新的付款方式或更改默认付款方式。

您可以在组织中添加资金帐户、信用卡或链接无限制按发票付款帐户作为付款方式，但只能将其中一个设置为默认付款方式。

设置组织时，组织的地址将决定支付组织服务费用时使用的货币。有关付款方式和货币的详细信息，请参见如何确定付款货币。

当订阅其他服务、购买加载项并将承付应用于您的组织时，您的销售订单可以为订阅或期限承付确定不同的付款方式，该付款方式仅适用于该特定购买。稍后可以更改订阅的付款方式。有关详细信息，请参阅如何更改订阅付款方式。

如何更改组织的默认付款方式

作为**组织所有者**用户，您可以更改组织的默认付款方式。

Cloud Services 控制台的**管理付款方式**页面的**其他付款方式**部分中列出了您的组织可用的所有付款方式。如果要将组织的默认付款方式更改为未列出的新付款方式，则必须先添加该付款方式。

步骤

1 打开 Cloud Services 控制台，然后导航到**计费和订阅 > 管理付款方式**。

2 在页面的**默认付款方式**区域中，单击“更改默认付款方式”。

3 从显示的可用付款方式列表中，选择要使用的付款方式。

4 单击**确认**。

将立即应用新的默认付款方式。

如何更改订阅付款方式

当您在组织中载入新服务或向现有服务添加新订阅时，可以选择默认付款方式，也可以为新订阅添加不同的付款方式。稍后，您可以更改组织中任何订阅的付款方式。

更改当前订阅的付款方式不会影响组织的默认付款方式。默认付款方式仍应用于使用它的其他采购和资源。新定义的付款方式将仅用于支付当前订阅的费用，直到**组织所有者**用户更改该付款方式为止。

步骤

1 打开 Cloud Services 控制台，然后转到**计费和订阅 > 订阅**。

2 从组织的订阅列表中，单击要更改的订阅的**订阅 ID** 链接。

此时将打开**订阅详细信息**页面。

3 在此页面的**付款方式**区域中，单击**更改**。

4 从组织中的可用付款方式列表中，选择订阅的新付款方式。

5 单击**确认**。

结果

订阅的详细信息页面将刷新以显示您选择的新付款方式。

如何使用发票付款

作为**组织所有者**用户，如果激活了无限制 PBI，您可以将组织的默认付款方式更改为按发票付款 (PBI)。启用无限制 PBI 需完成脱机批准过程，您可以通过提交支持请求来开始该过程。

激活后，PBI 可以作为默认付款方式应用于组织的所有服务和订阅。您还可以应用无限制 PBI 作为当前订阅的付款方式。

步骤

1 在 Cloud Services 控制台 上，选择**支持中心**，然后单击**创建支持请求**。

2 在**类别**文本框中，选择 **VMware Cloud Services - 计费和使用情况**。

3 在**主题**文本框中，输入**激活无限制 PBI**。

4 输入支持请求详细信息，然后单击**创建支持请求**。

VMware Cloud Services 代表将就您的请求与您联系。激活无限制 PBI 后，您会收到一条通知。

如何使用信用卡付款

VMware Cloud services 支持使用各种信用卡支付。您可以使用个人或公司 Mastercard、Visa、American Express、Discover、JCB 和 Diners Club 信用卡。您还可以使用 Mastercard、Visa 或 American Express 借记卡。

如果要使用信用卡支付服务费用，请注意：

- 您的信用卡限制和支付平台决定了您的交易金额。您的单次交易可支付的最高金额为 25000 美元。有关信用卡限制的详细信息，请联系发卡银行。
- 组织地址决定了结算货币。有关国家/地区及其相关货币的列表，请参见如何确定付款货币。
- 根据组织地址和信用卡的帐单地址，使用信用卡时存在某些使用信用卡作为付款方式有哪些限制。

  重要说明 如果您组织的帐单地址位于欧洲经济区 (EEA) 的成员国家/地区或合作国家/地区，则您的信用卡支付将受欧盟第二个支付服务指令 (2015/2366 PSD2) 的影响。PSD2 要求通过双因素身份验证对电子交易进行强客户身份验证 (SCA)。如果需要，将在结帐流程中显示 SCA 提示，要求您提供其他安全信息，然后由银行或信用卡发卡机构进行验证。

- 将信用卡添加为付款方式时，我们不会从您的卡中扣费，但我们会检查您的信用卡是否有效。有效性检查可能包括由银行机构发出的预授权请求。您可能会在帐单中看到 1.00 美元或等额的待处理授权请求。预授权不是费用，不会从您的帐户中扣款。

您可以在载入云服务时添加信用卡作为付款方式，也可以稍后通过在 Cloud Services 控制台中选择**计费和订阅 > 管理付款方式**执行此操作。

有关详细信息，请参见如何更改组织的默认付款方式。

使用信用卡作为付款方式有哪些限制

出于风险和欺诈考虑，可对信用卡付款方式应用某些限制。这些限制基于组织的地址或信用卡的帐单地址。

应用信用卡限制的国家/地区列表

如果您所在的国家/地区在限制使用信用卡之列，则会在 VMware Cloud Services 中停用该付款方式。

在以下情况下，无法使用信用卡作为付款方式...	
您组织的地址位于以下国家/地区之一：	阿富汗、荷属安的列斯、安哥拉、波斯尼亚和黑塞哥维那、孟加拉、布基纳法索、巴林、巴西、白俄罗斯、刚果民主共和国、喀麦隆、中国、古巴、佛得角群岛、塞浦路斯、厄立特里亚、福克兰群岛、法属圭亚那、瓜德罗普岛、关岛、海地、马恩岛、伊拉克、伊朗、韩国、科威特、老挝、蒙古、马里、马提尼克、蒙特塞拉特、墨西哥、尼日利亚、尼泊尔、被占的巴勒斯坦领土、苏丹、塞内加尔、叙利亚、土库曼斯坦、东帝汶、乌克兰、梵蒂冈、委内瑞拉、马约特岛、津巴布韦。
信用卡的帐单地址位于以下国家/地区之一：	阿富汗、荷属安的列斯、安哥拉、南极、奥兰群岛、波斯尼亚和黑塞哥维那、孟加拉、布基纳法索、巴林、圣巴托洛缪、博奈尔岛、圣尤斯特歇斯和塞巴、巴西、布韦岛、白俄罗斯、科科斯、刚果民主共和国、中非共和国、喀麦隆、中国、古巴、佛得角群岛、库腊索、圣诞岛、塞浦路斯、西撒哈拉、厄立特里亚、福克兰群岛、法属圭亚那、瓜德罗普岛、南乔治亚岛和南桑威奇群岛、关岛、香港特别行政区、赫德岛和麦克唐纳群岛、海地、马恩岛、印度、英属印度洋领地、伊拉克、基里巴斯、韩国、科威特、老挝、立陶宛、卢森堡、拉脱维亚、圣马丁、马里、蒙特塞拉特、墨西哥、马来西亚、诺福克岛、尼日利亚、挪威、尼泊尔、瑙鲁、纽埃、皮特凯恩、被占的巴勒斯坦领土、卢旺达、苏丹、瑞典、新加坡、斯瓦尔巴和扬马延、塞内加尔、索马里、苏丹南部、圣多美和普林西比、叙利亚、乍得、法国南部领土、泰国、托克劳、土库曼斯坦、东帝汶、土耳其、图瓦卢、美国边远岛屿、梵蒂冈、委内瑞拉、马约特岛、津巴布韦

如何使用优惠额度付款

如果您有优惠额度适用于任何 VMware Cloud services，可以将优惠额度应用于任意一个组织，然后兑换额度用来抵扣组织的每月费用。

优惠额度可以是特定于服务的，也就是说您可以使用其抵扣某特定服务、一组服务的每月费用，也可以应用于所有服务。请务必注意优惠额度的过期日期，并在过期前进行兑换。

优惠额度可以兑换为 VMware Cloud Services 支持的任何货币。首次启用某项服务时，有时可以享有优惠额度。启用服务时，可以兑换这些额度。

步骤

1 在 Cloud Services 控制台上，单击**计费和订阅 > 优惠额度**。

可以在组织中应用的所有优惠额度会显示在**可用优惠额度**选项卡上。

2 要兑换优惠额度，请单击其详细信息图块上的**激活**链接。

此额度将在下一个帐单期间兑换。您可以随时通过导航到**计费和订阅 > 优惠额度 > 激活的优惠额度**来检查优惠额度余额。

需要了解有关 VMware 资金帐户的哪些内容

VMware 资金帐户是特定于 VMware 的付款方式，可用于购买服务或产品。每个资金帐户由一笔或多笔存款组成。

当您想要向资金帐户充值时，您可以与销售人员合作并购买新的存款。存款由“优惠额度”组成，即您可用于购买 VMware 服务和产品的资金。

可以在需要访问权限的 VMware Connect 门户上通过资金帐户管理平台查看链接资金帐户的详细信息和管理其设置。有关详细信息，请参见“我的资金帐户”页面、“资金帐户详细信息”页面和导航概述。

要使用 VMware 资金帐户支付云服务和订阅费用，必须将每个资金帐户作为付款方式链接到 VMware Cloud services 组织。可以将资金帐户链接为组织和订阅的默认付款方式，也可以链接为一次性付款方式。还可以使用资金帐户直接从 Cloud Services 控制台支付未结发票金额。要使用链接的资金帐户支付组织费用，这些资金帐户的余额必须为正且具有足够的“资金”。

请注意，要在 Cloud Services 控制台 中链接资金帐户：

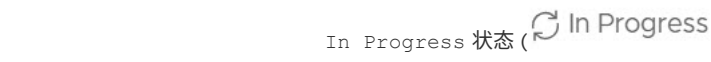
- 您必须在要链接资金帐户的组织中具有**组织所有者**角色。
- 只有 VMware 授权帐户内的资金帐户可以与 VMware Cloud services 组织相关联。
- 资金帐户的货币和销售单位必须与组织的货币和销售单位相匹配。

如果用作组织中默认付款方式的链接资金帐户用完、过期或处于孤立状态，则必须将该资金帐户替换为另一个资金帐户（称为正常运行的资金帐户），或替换为其他付款方式。孤立资金帐户是中断付款流的空资金帐户组，必须立即替换。

为便于**组织所有者**用户及时管理其资金帐户，VMware Cloud Services 会发送电子邮件和应用程序内通知，告知其组织中资金帐户的状态和更改。有关详细信息，请参见如何在 VMware Cloud Services 中管理 VMware 资金帐户。

如何使用资金帐户付款

作为**组织所有者**用户，您可以使用链接 VMware 资金帐户支付服务的费用。除了在组织中使用资金帐户作为默认付款方式外，还可以直接从 Cloud Services 控制台支付未结发票金额。

目标	执行操作
将链接 VMware 资金帐户设置为组织中的默认付款方式。	请参见如何更改组织的默认付款方式
将链接 VMware 资金帐户设置为活动订阅的付款方式。	请参见如何更改订阅付款方式
支付未结超额费用或期限承付发票金额。	1 登录到 Cloud Services 控制台，然后导航到**计费和订阅 > 发票和帐单 > 发票**。 2 找到要支付的未付发票，然后单击垂直省略号图标 ⋮。 3 单击**立即支付**链接。 4 在打开的弹出窗口中，查看发票详细信息，然后选择要用于此付款的资金帐户。 **注** **付款方式**下拉列表仅显示链接到组织且余额为正的资金帐户。 5 单击**立即支付**。 将提交付款，刷新**发票**页面，并在所支付的发票旁边显示 `In Progress` 状态（  ）。 交易完成后，您将收到电子邮件通知。交易可能会立即完成，也可能需要几个小时才能完成。只有在交易完成后，发票余额才会更新。 第一笔部分付款正在进行时，可以追加付款。更新后的发票将反映付款情况和更新后的余额。
通过 Cloud Services 控制台 查看使用资金帐户支付的发票的付款历史记录	1 转到**计费和订阅 > 发票和帐单 > 发票**。 2 找到要检查付款情况的发票，然后单击垂直省略号图标 ⋮。 3 单击**付款历史记录**链接。 **付款历史记录**部分显示所选发票的付款方式、状态和已付金额。

如何在 VMware Cloud Services 中管理 VMware 资金帐户

作为**组织所有者**用户，您可以在 Cloud Services 控制台中将 VMware 资金帐户链接为组织的付款方式和取消链接。只能将链接到组织的资金帐户设置为默认付款方式，或用于支付未结超额费用和期限承付发票金额。

注 在 Cloud Services 控制台中，您只管理资金帐户与组织的链接。可以通过需要访问权限的 VMware Connect 门户管理实际资金帐户。

有关对组织中 VMware 资金帐户所做更改的通知将通过电子邮件和应用程序自动发送给所有**组织所有者**用户以及组织中具有**计费只读**角色的**组织成员**用户。

下表介绍了如何在 VMware Cloud Services 组织中使用 VMware 资金帐户付款方式。

目标	执行操作
将 VMware 资金帐户链接为组织中的付款方式。	您可以使用任意资金帐户，前提是它位于与 VMware Cloud services 关联的 VMware 授权帐户中且与组织使用同一种货币。 1 登录到 Cloud Services 控制台，然后导航到**计费和订阅 > 管理付款方式**。 2 在页面的**其他付款方式**部分中，单击**添加付款方式**。 3 选择**链接 VMware 资金帐户**，然后单击**继续**。 4 从显示的可用 VMware 资金帐户列表中，选择要链接为组织中的付款方式的资金帐户。 **注** 此列表将仅显示链接到 VMware 帐户的 VMware 资金帐户。 5 链接您选择的资金帐户： ■ 要将资金帐户链接为组织中的默认付款方式，请单击**链接资金帐户并设为默认值**。 ■ 要链接资金帐户并将其作为组织中的付款方式提供，请单击**链接资金帐户**。
取消链接已链接为组织中的付款方式的资金帐户。	组织中的付款方式可供所有**组织所有者**用户使用。如果要从组织中移除活动资金帐户，请执行以下操作： 1 打开**管理付款方式**页面。 2 单击资金帐户名称旁边的水平省略号图标 (•••)，然后选择**取消链接资金帐户**
查看已链接为组织中的付款方式的资金帐户的详细信息。	1 转到**计费和订阅 > 管理付款方式**。 2 单击资金帐户名称旁边的水平省略号图标 (•••)，然后选择**在 MyVMware 上查看详细信息**。 这将打开 VMware Customer Connect 网站，您可以在使用 VMware 帐户登录后在其中查看资金帐户的详细信息。
管理已链接为组织中的默认付款方式的已过期资金帐户。	如果您将资金帐户用作组织中的默认付款方式，则会在过期日期之前收到一封电子邮件通知。对于即将过期的资金帐户，您可以执行以下操作之一： ■ 将组织的默认付款方式更改为组织中链接的另一个活动资金帐户。 ■ 将默认付款方式更改为信用卡或 PBI。 ■ 如果您还有其他未在组织中链接的活动资金帐户，则可以将其链接到组织，然后将其设置为默认付款方式。

目标	执行操作
管理用完的资金帐户	如果用作默认付款方式或用于发票付款的资金帐户没有足够的“资金”来支付全部发票金额，则发票将显示为部分付款。必须使用具有足够“额度”的其他资金帐户或其他付款方式支付剩余费用。
管理链接为组织中的默认付款方式的孤立资金帐户	资金帐户可能会由于以下原因之一变为孤立状态： ■ 更改资金帐户所有者 ■ 资金帐户合并 ■ 更改**组织所有者** ■ **组织所有者**不再是资金帐户用户 发生这种情况时，VMware Cloud Services 会通知**组织所有者**用户已变为孤立状态的资金帐户，并将孤立资金帐户替换为正常运行的资金帐户。另外，还会向所有**组织所有者**用户发送有关更新默认付款方式的通知。如果需要进一步更改付款，请参见如何管理组织的付款方式。

如何使用 VMware Cloud Services 订阅和承付

VMware Cloud services 订阅允许您承诺以一年或三年的预定义费率（以降低或协商费率）购买一定量的容量，从而节省成本。

您可以按需使用 VMware Cloud services，也可以通过购买 1 年期或 3 年期订阅进行使用。按需服务使用情况按较高费率计费，而服务订阅以折扣费率计费。您将通过订阅购买计划 (SPP) 或按发票付款购买订阅。

您可以为订阅中的每个服务购买并使用多个承付。每个承付期限的开始日期和结束日期可能会有所不同。采购订单概要说明了承付的容量、期限和商定的价格。

VMware Cloud Services 根据服务订阅承付中规定的条款向您计费。

对于未涵盖在承付期限内的任何额外使用，将基于您注册服务时商定的按需定价扣费。

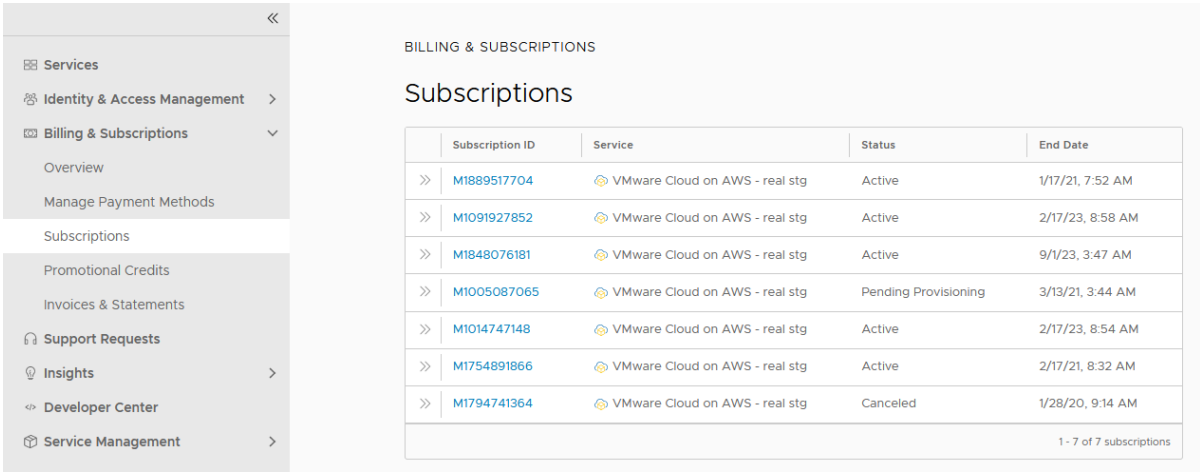
如何查看组织中服务的订阅详细信息

要查看组织中的订阅详细信息，您必须具有**组织所有者**角色或具有**计费只读**权限的**组织成员**角色。

步骤

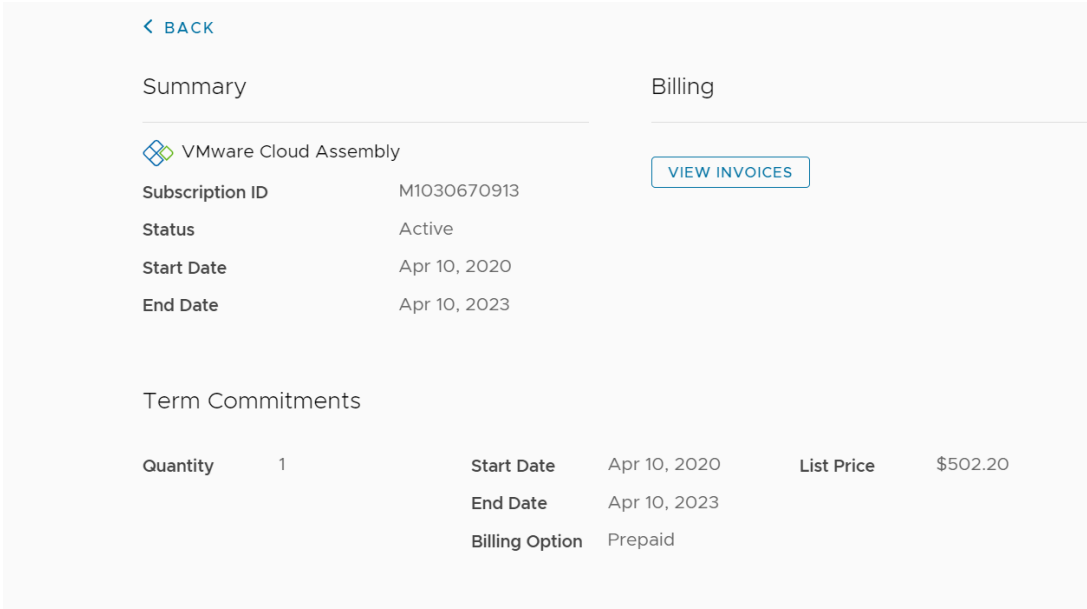
1 在 Cloud Services 控制台 中，导航到**计费和订阅 > 订阅**。

打开的表格提供了有关组织中所有订阅的信息。它列出了每个订阅的 ID、购买其订阅的 VMware Cloud services 以及订阅中包含的期限承付。



2 要查看特定订阅的更多详细信息，请找到要查看的订阅，然后单击其**订阅 ID** 链接。

打开的页面将显示有关订阅以及随订阅一起购买的期限承付的其他详细信息。



3 (可选) 要查看并下载发票，请单击页面的**计费**部分中的**查看发票**。

如何设置承付

如果您是**组织所有者**用户，请联系您的 VMware 销售代表协商报价和安排承付的付款。

购买完成后，您将收到通知电子邮件，说明您的承付处于活动状态。对于每个承付，您都将收到包含唯一链接的电子邮件。

1 要将承付应用于当前的某个组织或新组织，请单击电子邮件中的链接。

2 按照服务上线工作流中的步骤执行操作。

有关承付的详细信息，请参见为什么需要将承付应用于组织。

有关载入工作流的详细信息，请参见如何载入通过 VMware Sales 购买的付费云服务。

如何购买订阅

VMware Cloud Services 提供了针对选定服务和卖方自助购买订阅的选项。

注 自助订阅购买选项当前仅适用于从 VMware 购买的 VMware Tanzu Service Mesh。

可以在 Cloud Services 控制台中从**计费和订阅 > 订阅**页面或从云服务目录中的服务图标中对上面列出的服务发起订阅购买订单。

前提条件

您必须在要购买新订阅的组织中具有**组织所有者**角色。

步骤

1 登录到 Cloud Services 控制台，然后导航到**计费和订阅 > 订阅**。

2 单击**创建订阅**。

此时将打开**创建订阅**工作流的第一步。

3 在**服务**工作流步骤的**选择服务**部分中，使用下拉菜单选择服务或服务包以及要从其购买新订阅的卖方。

4 单击**下一步**。

如果您的组织没有有效的地址，或者组织的默认付款方式未定义，则打开的下一步是**计费信息**。

5 在工作流的**计费信息**步骤中，指定组织的地址并选择默认付款方式。

6 单击**下一步**。

7 在工作流的**配置**步骤中，为订阅选择配置选项。根据要订阅的解决方案或服务，订阅配置步骤可能会要求您选择以下选项：

- 版本和/或区域。
- 承付数量、计费频率和承付期限。

该页面的**订单摘要**部分将根据您的最新选择显示订阅的信息和成本。

8 订阅配置准备就绪后，单击**保存**。

9 如果要更改或删除订阅配置，可以使用**配置**步骤**报价**部分中的**修改**或**移除**按钮执行此操作。

10 要继续处理购买订单，请单击**下一步**。

11 在工作流的最后一步中，查看购买订单摘要和付款摘要，然后选择付款方式。

12 单击**创建订阅**。

13 在打开的弹出窗口中，单击**创建**以确认购买。

结果

屏幕上将显示订阅订单购买请求的确认信息。可能需要一些时间才能处理购买订单并激活新订阅。之后，可以在组织的**订阅**页面上查看订阅的详细信息。

如何扩展订阅

作为**组织所有者**，您可以扩展组织中所选订阅的容量。

注 目前，只有 VMware Tanzu Service Mesh 正在使用此功能，并且仅当您从 VMware 购买订阅时，此功能才可用。

前提条件

- 您已购买要从 VMware 扩展的订阅。
- 您在组织中具有**组织所有者**角色。

步骤

1 登录到 Cloud Services 控制台，然后导航到**计费和订阅 > 订阅**。

2 找到要扩展的订阅，单击订阅 ID 前面的垂直省略号图标 (⋮)，然后单击**扩展**。

3 输入订阅的新数量，然后单击**保存**。

订单摘要部分将根据您的最新选择显示订阅的信息和成本。

4 如果要更改所选数量，请单击**修改**并输入新值。

5 要确认您的订阅扩展，请单击**下一步**。

6 在工作流的最后一步中，查看购买订单摘要和付款摘要，然后选择付款方式。

7 单击**创建订阅**。

结果

屏幕上将显示订阅订单购买请求的确认信息。可能需要一些时间才能处理购买订单并激活对订阅的更改。之后，可以在组织的**订阅**页面上查看订阅的详细信息。

为什么需要将承付应用于组织

您可以为不同的 VMware Cloud Services 购买多个订阅，并为每个订阅购买多个期限承付。每个订阅可以在一个组织中使用。如果您有多个 VMware Cloud services 组织，则可以将新购买的承付应用于您选择的组织。

购买承付时，销售产品会概要说明容量、期限和商定的价格。作为**组织所有者**用户，您可以在完成购买后将承付应用于新组织或现有组织。为此，请打开新承付的链接并按照工作流中的步骤进行操作。

与特定组织关联后，该组织的成员可以使用该承付，直到其期限到期为止。

如何更改订阅续订首选项

作为**组织所有者**用户，您可以从 Cloud Services 控制台中的**订阅详细信息**页面管理订阅续订。

组织中的每个订阅都有一个默认续订首选项，可以在订阅过期前 30 天内进行更改。

重要说明 **订阅详细信息**页面仅显示所购买订阅支持的续订首选项。如果下面列出的任何续订首选项缺失，则表示该首选项当前不可用于您的订阅。

如果您的续订首选项设置为...	则...
自动续订	您的订阅将自动续订，您无需额外输入。
手动续订	客户经理将在续订日期之前与您联系，讨论续订详细信息。 您还可以提交支持请求以询问续订选项。
您也可以在续订之前取消订阅，只需将续订首选项更改为**取消续订**即可。	您也可以在续订订阅之前取消订阅。在这种情况下，您的组织将在订阅过期日期后失去对订阅的授权。

前提条件

您必须具有**组织所有者**角色。

步骤

1 登录到 Cloud Services 控制台，然后导航到**计费和订阅 > 订阅**。

2 从显示的订阅列表中，单击订阅的 ID。

这会打开**订阅详细信息**页面。

3 在**续订首选项**部分中，单击**更改**。

4 为订阅选择新的默认续订首选项，然后单击**确认**。

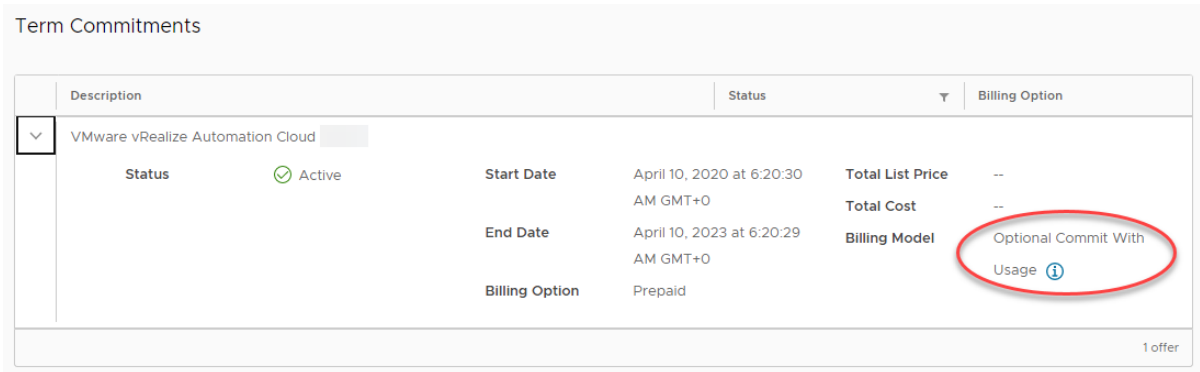
什么是计费模式

VMware Cloud Services 使用三种不同的计费模式。订阅的计费模式决定了如何对组织内购买和使用的服务和承付收取组织费用。

计费模式信息显示为订阅的**期限承付**详细信息的一部分。

1 登录到 Cloud Services 控制台，然后转到**计费和订阅 > 订阅**。

2 单击订阅的 ID 以打开其详细信息页面，然后展开**期限承付**部分。



注 您只能查看通过 VMware 购买的订阅的计费模式。

下表介绍了三种计费模式之间的差异。

	仅承付	可选承付及使用量	强制承付及使用量
描述：	您必须购买订阅才能使用服务。	无需订阅即可开始使用服务，但可能产生按需使用量。	必须购买订阅才能使用服务，并且可能会因超额使用量而付费。
默认付款方式：	不需要	必需	不需要
成本由以下因素决定：	承付	承付 + 按需使用量（如果有）	承付 + 超额使用量（如果有）

如何使用“使用情况管理”仪表板

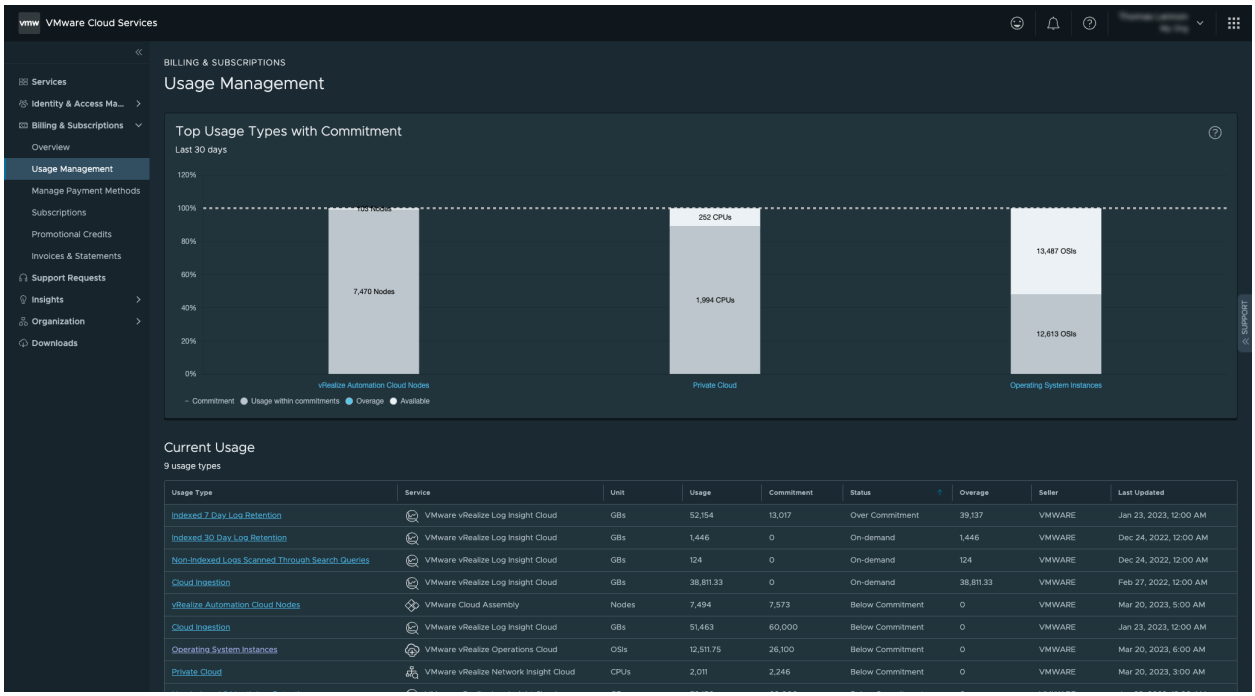
作为**组织所有者**用户，您可以通过 Cloud Services 控制台中的**使用情况管理**仪表板根据使用情况类型跟踪一段时间内组织中的服务使用情况。

注 使用情况管理并非适用于所有 VMware Cloud services。当前提供使用情况数据的一些服务包括 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 Platform。

可以观看以下视频，大概了解“使用情况管理”功能：

(Cloud Services 控制台使用情况管理讲解示范)

可以通过导航到**计费和订阅 > 使用情况管理**，访问**使用情况管理**仪表板。

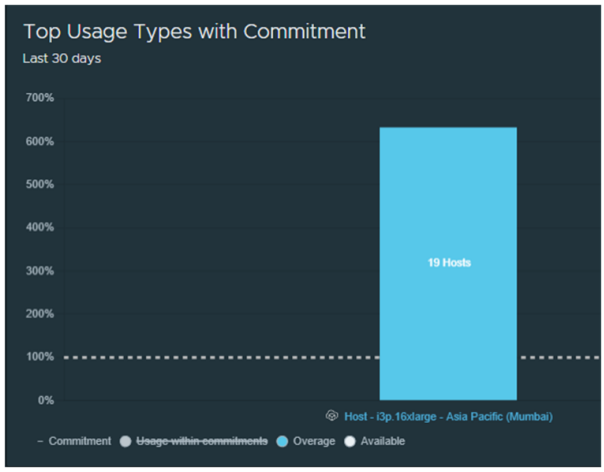
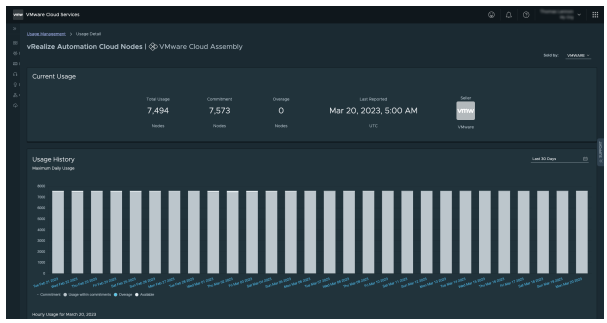


使用情况数据分为两个部分：一个图表，展示过去 30 天内组织中的前几种使用情况类型；一个表，详细展示组织中所有使用情况类型的当前使用情况。

VMware Cloud services 使用许多使用情况类型。使用情况类型基于组织中置备的特定服务，包括用于衡量服务承付容量的单位。最常用的单元是内核、主机、vCPU、CPU 和 OSI。以下是一些使用情况类型示例：

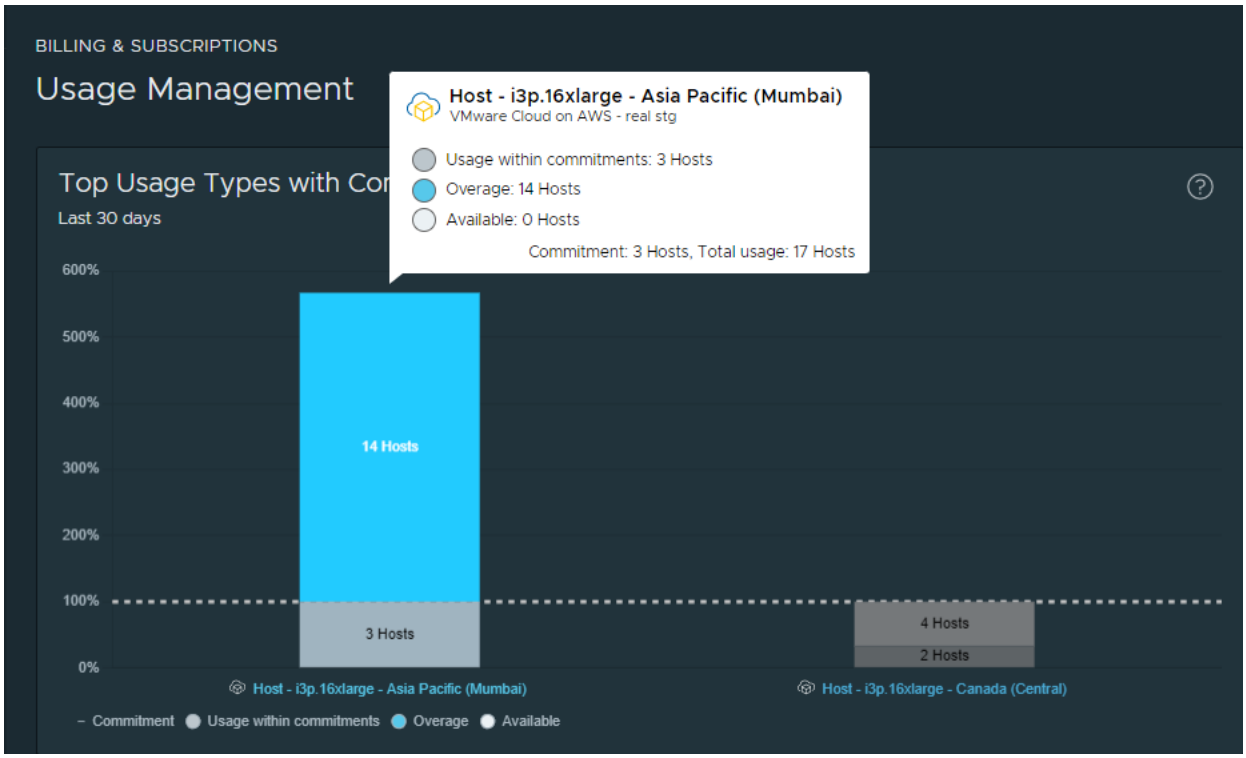
- `Operating System Instances`
- `Cloud Director Cores`
- `Host - r.5metal - Europe (Ireland)`

目标	执行操作
了解有关使用前几种使用情况类型的更多信息。	请参见需要了解有关“包含承付的前几种使用情况类型”图表的哪些内容。
了解有关使用当前使用情况的更多信息。	请参见需要了解有关“当前使用情况”表的哪些内容。

目标	执行操作
根据容量（如包含承付的使用情况、超额或可用承付）筛选使用情况。	在**使用情况管理**仪表板的**包含承付的前几种使用情况类型**部分中，单击图表下要从视图中排除的信息对应的标签。 例如，如果要仅查看前几种使用情况类型的超额，请单击**包含承付的使用情况**标签。当该标签划掉时，视图将刷新以仅显示超额的使用情况类型。 
查看每种使用情况类型的当前和历史使用情况	单击要查看当前和历史使用情况详细信息的使用情况类型链接。如果使用情况类型包含在**包含承付的前几种使用情况类型**部分中，则链接位于图表中相应条形的正下方。如果使用情况类型在**当前使用情况**部分中列出，则会在“使用情况类型”列中找到链接。 将打开一个页面，其中显示了所选使用情况类型的当前和历史使用情况视图。  要了解有关当前和历史使用情况的更多信息，请参见需要了解有关当前和历史使用情况详细信息的哪些内容。

需要了解有关“包含承付的前几种使用情况类型”图表的哪些内容

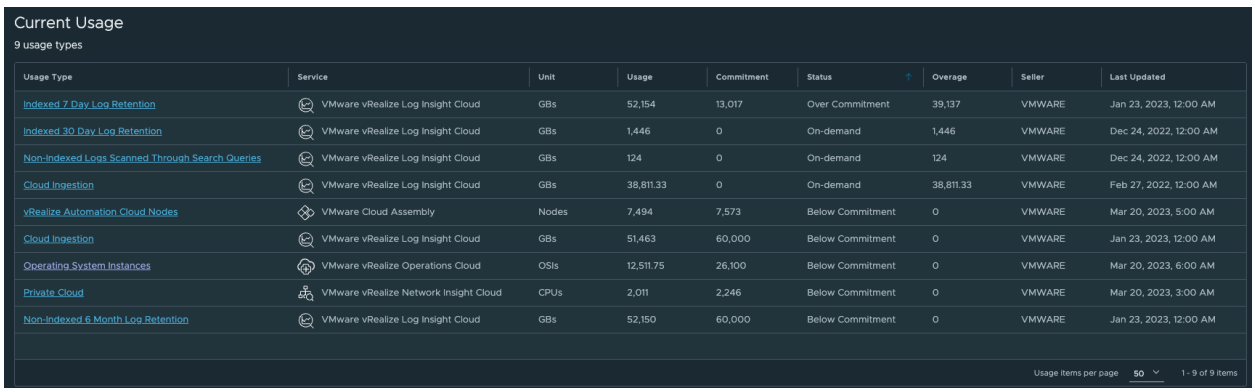
使用情况管理仪表板中的**包含承付的前几种使用情况类型**图表显示过去 30 天内您组织中前几种使用情况类型的使用情况高水位线摘要，按承付百分比排序。



承付是指组织通过订阅购买的单位数量。水平虚线表示 100% 承付级别。低于这条线的条形表示此服务和使用情况类型未充分利用。条形的蓝色部分表示您已超出承付，可以考虑减少使用量或购买更多承付。在该图表中，组织使用情况超出承付的单位数量显示为超额。

需要了解有关“当前使用情况”表的哪些内容

当前使用情况表位于 Cloud Services 控制台 中**使用情况管理**仪表板的主要部分**包含承付的前几种使用情况类型**下。



该表简要说明了组织中所置备服务的使用情况类型的使用情况详细信息。下面详细介绍了可以在每个表列中找到的信息：

列	描述
使用情况类型	组织中置备的特定服务的使用情况以及用于衡量该服务承付容量的单位。例如，`Host - r5.metal - US West Oregon`。 使用情况类型显示为链接。单击该链接将打开一个详细信息页面，其中显示了所选使用情况类型的当前和历史使用情况。
服务	特定使用情况类型相关联的云服务。例如，VMware Cloud on AWS。
单位	表示特定使用情况类型的测量单位。例如，主机、内核、GB（存储）、IP/EIP、CPU/vCPU 等。
使用情况	表示报告时正在使用的实际使用情况：当前正在使用的单位数量。
承诺	组织通过订阅购买的单位数量。
状态	表示使用情况状态摘要。选项如下所示： ■ 高于承付：使用情况超过承付时。 ■ 按需：对某个使用情况类型有使用但无承付时。 ■ 等于或低于承诺：某些服务在使用情况达到或低于承付时没有数据。此状态表示消耗的使用量没有超过购买的承付量。不显示使用的具体数量。
超额	表示使用情况超过承付的程度。
卖方	表示您从其购买订阅的卖方。可以显示可能针对使用情况计费的过度消耗。
上次更新时间	表示上次获取数据的时间戳。

如何下载当前使用情况数据

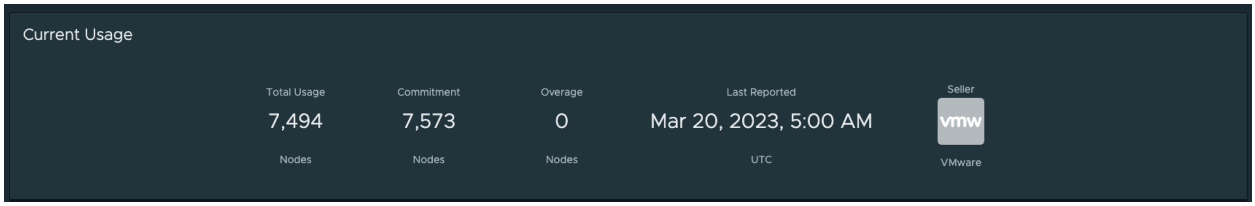
可以通过单击**当前使用情况**表左上角的**导出**按钮，下载包含组织当前使用情况数据的 CSV 文件。

需要了解有关当前和历史使用情况详细信息的哪些内容

对于组织中的**使用情况管理**仪表板中显示的每种使用情况类型，都可以查看当前和历史使用情况详细信息。要打开详细信息，请单击使用情况类型链接。

当前使用情况

当前使用情况仪表板概要显示一些基本详细信息。

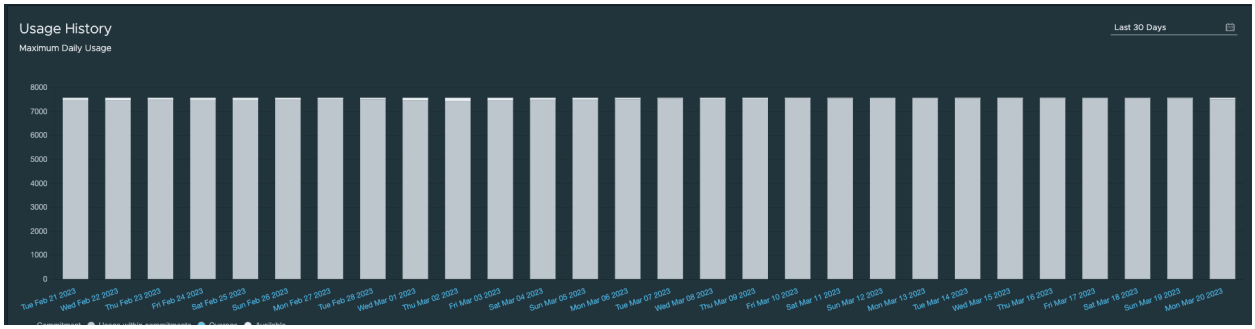


- **总使用量**显示总使用量和使用情况衡量指标类型。例如，`7,494 Nodes`。
- **承付**显示特定服务订阅承付使用情况单位数量。例如，`7,573 Nodes`。

- **超额**显示如果实际使用情况超过承付使用情况，则由单位数量值反映出差额。
- **上次报告时间**显示上次更新当前使用情况类型详细信息时的时间戳。
- **卖方**表示订阅使用情况类型的卖方。

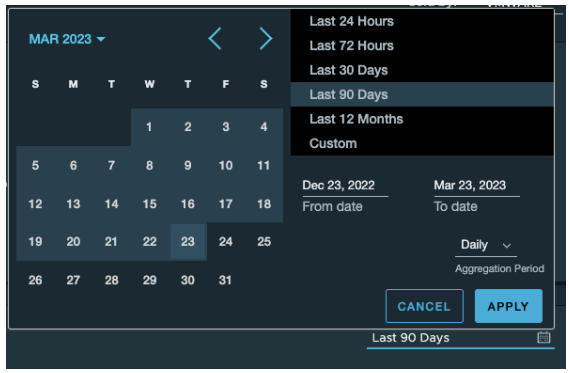
使用情况历史记录

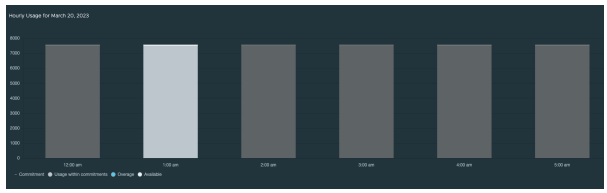
使用情况历史记录视图显示预定义时间段内的每日最大使用量，以及特定日期的每小时使用情况。



- **每日最大使用量**视图中的垂直轴表示使用情况衡量指标和单位数量。
- 水平轴表示图表上所显示数据的时间范围。

如何使用当前和历史使用情况视图

目标	执行操作
查看有关使用情况的更多详细信息。	将鼠标悬停在图表柱条上。您会发现： ■ 图表的时间戳。 ■ 承付内的使用情况：当时正在使用的承付所提供的单位数量。 ■ 超额：当时导致超额的单位数量，超额的百分比结果。 ■ 可用：当时可供使用的单位数量。
修改**每日最大使用量**图表时间段。	1 单击**每日最大使用量**图表右上角的日历图标。 此视图的默认时间段为 30 天。可以筛选每日最大使用量数据的最短时间段为 24 小时。最长时间段为 2 年。  2 更改时间段设置，然后单击**应用**。

目标	执行操作
查看特定日期的**每小时使用情况**图表。	单击**每日最大使用量**图表中的任意日期条。**每小时使用情况**图表将刷新，显示所选日期的每小时使用情况细目。  **注** 每小时使用情况仅显示过去 30 天的数据。
以表格格式查看每小时使用情况。	可以在**每小时使用情况**图表正下方的表中查看每小时使用情况细目。  单击任意日期旁边的双箭头图标，可获得展开的每小时使用情况视图，该视图按以下列进行组织： ■ 时间：数据所引用的一天中的具体时间。 ■ 承付：表示您的组织在订阅中承付的数量。 ■ 承付内的使用情况：表示视为在组织承付范围内的实际使用情况。 ■ 超额使用量：表示超出组织承付并视为超额的使用量。 ■ 总使用量：表示包括组织承付内的任何使用量以及任何超额的总使用量。 ■ 单位：适用于所选使用情况类型的衡量指标，即主机/IP/EIP/CPU/vCPU 等

以下视频展示了如何使用缩放功能。

(Cloud Services 控制台 - 使用情况管理缩放功能)

使用情况管理常见问题解答

本主题介绍了有关 Cloud Services 控制台中**使用情况管理**仪表板的常见问题解答 (FAQ)。

问：为什么我的购买没有显示在“使用情况管理”页面中？

答：所有使用情况数据每天进行处理。根据您使用服务的时间，可能需要长达 48 小时才会显示在此报告中。请注意，某些服务按月提供数据。

问：为什么我的使用情况延迟了？

答：所有使用情况数据每天进行处理。根据您使用服务的时间，可能需要长达 48 小时才会显示在此报告中。请注意，某些服务按月提供数据。

问：如何查找成本信息？

答：可以通过查看业务明细报表来查看服务的费用。有关详细信息，请参阅 如何阅读我的业务明细报表。

问：我看不到使用情况数据。为什么？

答：使用情况管理并非适用于所有 VMware Cloud services。当前提供使用情况数据的一些服务包括 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 Platform。如果您的服务受支持，则根据您使用服务的时间，可能需要长达 48 小时才会显示在此报告中。请注意，某些服务按月提供数据。

问：可以查看多久以前的使用情况数据?

答：仪表板中显示的默认时间段为 30 天。可以筛选每日最大使用量数据的最短时间段为 24 小时。最长时间段为两年。请注意，在任何给定时间，图表显示最长一年期的数据。

问：我看不到任何每小时数据。为什么？

答：仅可以查看过去 30 天的每小时数据。除此之外，还可以查看每日数据。

问：我的使用情况数据不反映我的帐单。为什么？

答：大多数服务根据计费周期内发生的每小时超额总和进行计费。在此图表中，您将看到给定小时的实际使用情况，以及给定一天的最大使用情况。

问：我看不到“前几种使用情况”图表。为什么？

答：**前几种使用情况**图表仅显示您所承付服务在过去 30 天内的使用情况。如果任何服务的使用情况都不符合要求，则根本不显示该图表。您可能看不到使用情况的几种原因如下：

- 所有使用情况都是有关按需服务的使用情况。按需使用情况不会显示在“前几种使用情况”图表中。
- 您使用的服务不提供使用情况数据。
- 您的使用发生在过去 30 天以前。

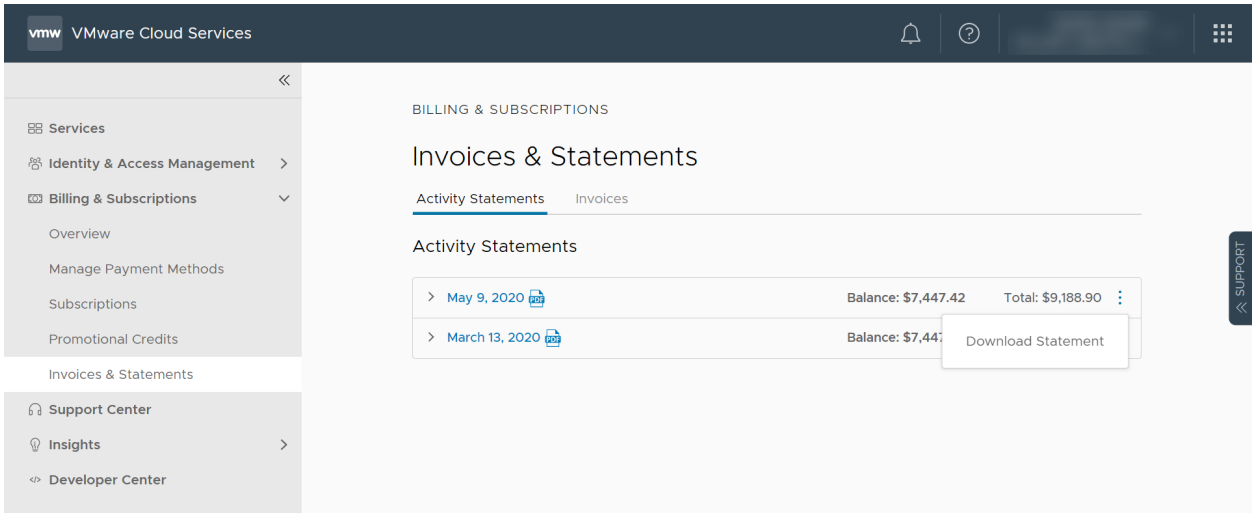
如何查看帐单和发票

作为**组织所有者**用户，您可以查看并打印最近的 15 个业务明细报表、按需发票和年度承付发票。

在 Cloud Services 控制台 中选择**计费和订阅 > 发票和帐单**可查看结账单和发票。

您的业务明细报表

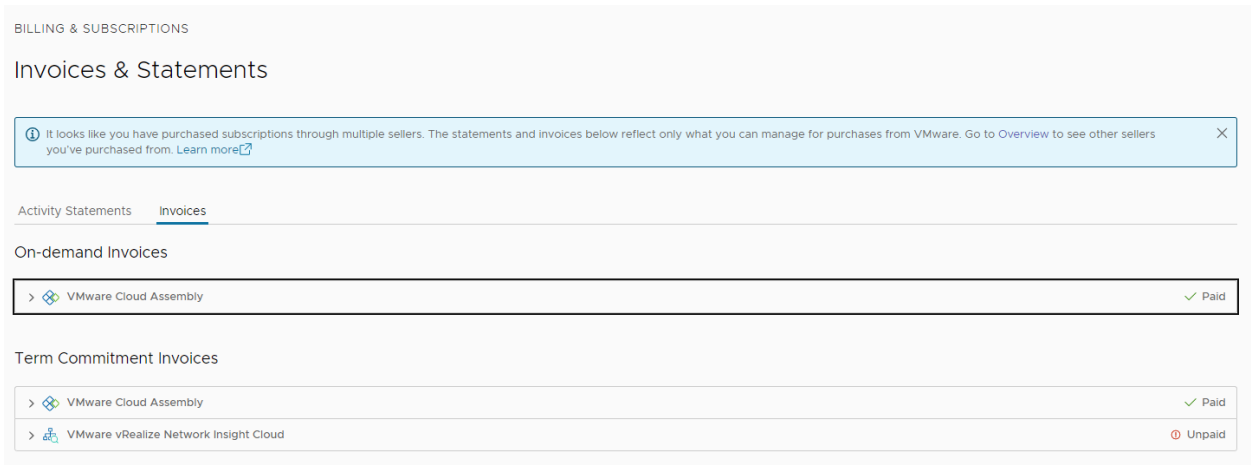
业务明细报表页面显示给定计费周期内使用的所有服务的月度摘要。每个业务明细报表都提供相关费用、优惠额度和余额的付款摘要。通过单击其链接，或者从旁边的垂直省略号图标中选择一个选项，可以查看和下载业务明细报表。



您的发票

要访问发票，请单击**发票和帐单**页面上的**发票**选项卡。

- 页面的**按需发票**部分会列出按需订阅的计费成本。
- **期限承付发票**部分列出了订阅期限承付的发票。



您可以通过单击发票链接或从旁边的垂直省略号图标 (⋮) 菜单中选择**下载**来下载发票。

如何阅读我的业务明细报表

作为**组织所有者**用户，您可以在给定计费周期的业务明细报表中查看有关组织在该计费周期内使用的所有服务的详细信息。业务明细报表不是发票。

业务明细报表中包含的内容

每个业务明细报表都提供计费周期内应计的所有服务费用的摘要和明细，以及根据服务费用支付的款项。

计费周期摘要

“计费周期摘要”是计费周期内总费用、优惠额度、折扣、调整和付款的概览。“余额”的金额显示当前周期内的未付费用，而“未结余额”显示上一计费周期内的未支付余额。

注 在业务明细报表的生成日期之后支付的款项不反映在其中。

费用细目

“费用细目”部分为您组织中的每个服务的应计费用提供了一个直观的饼图表示形式。针对每个服务显示的金额是扣除所有折扣、促销和调整后的所有费用的净金额。仅当您的组织为多个服务付费时，才会填充此图表。

费用历史记录

如果您的组织在一个以上计费周期内发生了费用，“费用历史记录”部分将显示一个折线图，并列出最长 12 个月内各项服务的费用历史记录。针对每个服务显示的金额是扣除所有折扣、促销和调整后的所有费用的净金额。

服务费用

“服务费用”部分包括计费周期内发生的费用和使用的优惠额度，以及针对这些费用支付的所有款项。积分包括每项服务的所有折扣、促销和调整，并在金额前显示一个减号。服务费用可用于具有承付的服务、按需使用的服务以及与服务使用相关的其他费用。“期限承诺”、“按需使用”和“其他费用小计”按行显示，后跟付款和当前余额。付款包括每项服务的所有折扣、优惠和调整。

按需使用详细信息

您组织使用的按需服务的所有费用都反映在“按需使用详细信息”部分中。仅当您的组织使用按需服务且仅在使用这些服务时，才会产生费用。

其他费用详细信息

您的组织产生的任何其他费用（如数据传输、Direct Connect、EBS、弹性 IP 费用和注册额度）将显示在其他费用下。这些费用按唯一区域和 SID（订阅 ID）汇总。

业务明细报表中使用的缩写术语表

您的业务明细报表显示了成本计算所涉及的产品、服务和测量单位的缩写。下面的术语表提供了可帮助您理解业务明细报表的快速参考。

表 11-3. VMware Cloud Services 缩写术语表

产品名称	测量单位	测量单位描述
vRealize Automation Cloud	EA	每个
	NDH	每小时节点数
vRealize Log Insight Cloud	EA	每个
	NDH	每小时节点数
	GB	千兆字节
vRealize Network Insight Cloud	CPU	中央处理单元

表 11-3. VMware Cloud Services 缩写术语表 （续）

产品名称	测量单位	测量单位描述
	GB	千兆字节
	EA	每个
	VCP	虚拟中央处理单元
NSX Cloud	CRM	每月内核数
	EA	每个
Tanzu Application Catalog	EA	每个
Tanzu Application Service	COH	计算单位小时
	EA	每个
VMware Cloud Director	CRM	每月内核数
	EA	每个
VMware SD-WAN by VeloCloud	EA	每个
VMware Learning Platform	ALH	活动实验室小时
	BIH	自备云
	COH	计算单位小时
	EA	每个
	STH	存储单位小时
	WIH	Windows 单位小时
VMware Cloud on AWS	ATG	每 GB 连接数
	ATH	每小时连接数
	EA	每个
	GB	千兆字节
	GBM	每月千兆字节
	HST	主机
	HPH	每小时主机数
	IPR	每小时 IP 地址数
	IP	IP 地址
	VMH	每小时虚拟机数
VMware Cloud on AWS GovCloud (US)	EA	每个

表 11-3. VMware Cloud Services 缩写术语表 （续）

产品名称	测量单位	测量单位描述
	HPH	每小时主机数
	IP	IP 地址
	VMH	每小时虚拟机数
	ATH	每小时连接数
	ATG	每千兆字节连接数
	IPR	每小时 IP 地址数
	GB	千兆字节
VMware Cloud on DELL EMC	EA	每个
	NDM	每月节点数
	EDM	每月 Edge 数
vRealize Operations Cloud	EA	每个
	OSI	操作系统实例

如何在发票中插入 PO 号

要处理发票付款，您可能需要包含其他信息，例如发票中的 PO 号。您可以从 Cloud Services 控制台 中的**发票**页面添加参考信息，并重新打印发票。

前提条件

您必须在生成发票的组织中具有**组织所有者**角色。

步骤

1 登录到 Cloud Services 控制台，然后导航到**计费和订阅 > 发票和帐单 > 发票**。

2 找到要重新打印的发票，然后单击旁边的垂直省略号 (⋮) 图标。

3 从打开的菜单中，选择**插入参考编号**。

> **注** 仅当发票作为可下载 PDF 提供、尚未支付且付款方式不是信用卡时，**插入参考编号**链接才可用。如果发票已提交进行重新打印，但更新的发票尚不可下载，则该链接不可用。

4 在打开的弹出窗口中，输入要包含在发票中的 PO 编号，然后单击**提交**。

> **重要说明** 重新生成新发票可能需要长达 24 小时。在重新打印发票后，您会收到一封电子邮件通知。

我如何获取支持

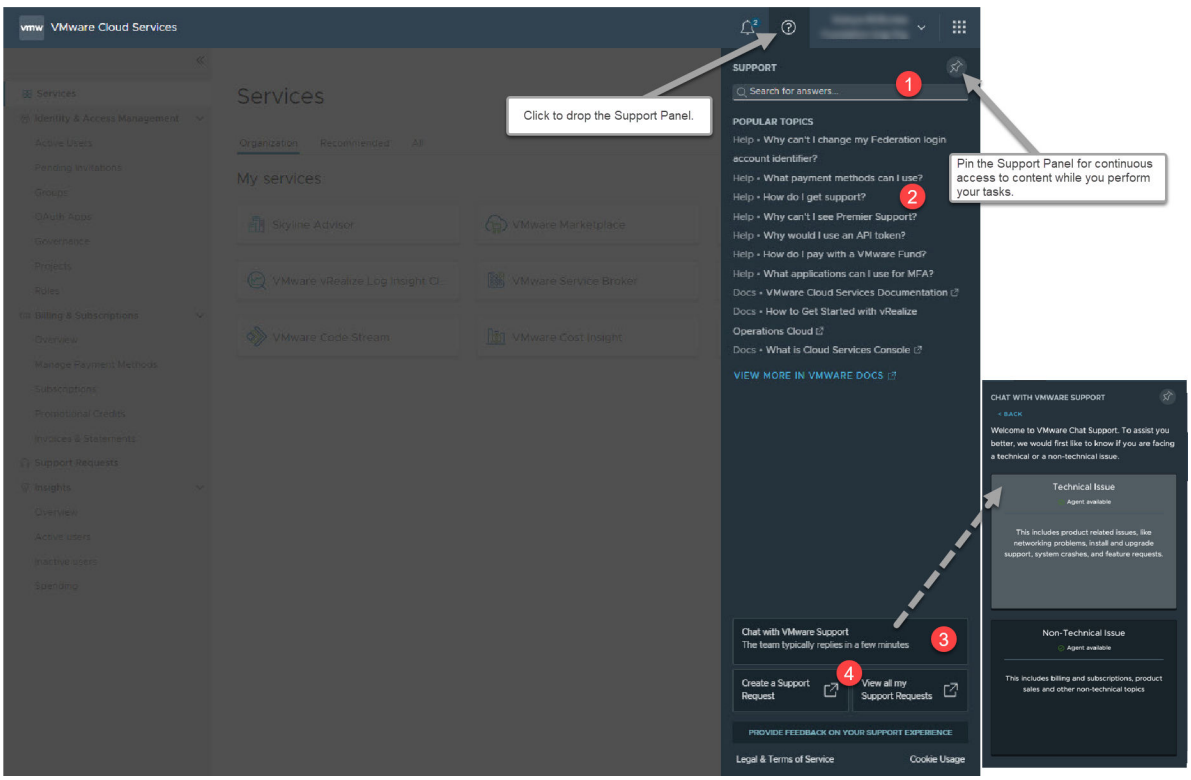
12

欢迎体验 VMware Cloud services 产品内支持服务。在此，您可以查看上下文帮助内容以便快捷地执行任务，搜索问题答案，以及与我们的客户支持团队进行交流。

我们会不断针对所有云服务推出的新功能提升您的使用体验。目前，在“支持”面板中可查看以下部分或全部功能。

步骤

1 通过单击菜单上的**问号**图标或单击窗格右侧的**支持**选项卡打开“支持”面板。



2 访问所需的支持服务。

支持面板不仅提供上下文帮助内容，还提供强大的搜索功能，可帮助发现更多内容和回答问题，您无需联系技术支持即可执行所有这些操作。当您与客户支持代表聊天时，可以继续操作云服务。

访问此支持功能...	可帮助您...
1. 智能搜索。	搜索内容，查找问题答案。我们会搜索文档、专门编写的帮助主题、社区和知识库文章。
2. 页面相关内容。	执行您的任务。打开**支持**面板时，将看到页面相关帮助主题，其中包含的信息足以帮助您完成任务。当您执行任务，从一个页面转至另一个页面时，帮助内容会相应地发生变化。内容列表还会显示您的搜索结果。搜索结果中包含更多帮助主题、知识库文章、文档中心的内容以及社区中的内容。 如果找不到要查找的内容，请单击**在 VMware Docs 中查看更多信息**以执行与您正在查看的页面相关的搜索，或者如果您键入了搜索项，会执行与该搜索项相关的搜索。搜索结果显示在文档中心内。
3. 咨询 VMware 技术支持团队。	联系我们的支持工程师和客户支持代表。 以下是您需要了解的有关实时支持聊天的信息： ■ 发起与 VMware 技术支持聊天与上下文相关。这意味着，当您从 Cloud Services 控制台发起与 VMware 技术支持聊天时，可以获得有关 Cloud Services 控制台问题的帮助。要针对某项服务获得聊天支持，请确保在登录到该服务后发起聊天。 ■ 与我们的客户支持工程师进行交流时，您可以继续使用 Cloud Services 控制台或使用 Cloud Services 控制台。您始终可以通过以下方式返回聊天功能：单击浏览器窗口右侧的**支持**按钮  ，然后单击**返回到聊天**图标  。 ■ 客户支持工程师还可以帮助您提交支持请求。 ■ 根据为您的浏览器和 VMware Cloud Services 配置文件配置的语言设置，您将获得英语或日语在线支持。 ■ 在 Cloud Services 控制台中使用实时支持聊天时： ■ 必须先选择要寻求帮助的问题是技术问题还是非技术问题。这可确保您的请求发送给正确的客户支持代表。 ■ 不能同时进行多个支持聊天。要打开新聊天以咨询新问题，必须关闭当前聊天。 ■ 在聊天过程中，可以选择直接从聊天窗口向客户支持代表发送文件或屏幕截图。 **注** 为避免在活动聊天会话期间出现任何超时问题，建议在前台保持浏览器窗口/选项卡打开。
4. 创建支持请求/查看所有支持请求。	打开 VMware Customer Connect，可在其中创建和管理支持请求。

3 要管理支持请求，请单击 Cloud Services 控制台菜单中的**支持请求**链接。

所有与支持相关的功能现在均可通过 VMware Customer Connect 门户进行访问。

a 单击**创建支持请求**。

此时将在 Customer Connect 上打开 **VMware 技术支持**页面。有关创建新支持请求的详细说明，请参见如何在 Customer Connect 中以及通过 Cloud Services 门户提交支持请求。

在打开支持请求之前，您可能需要其他与服务相关的信息。例如，在 VMC on AWS 中，您可能需要 SDDC 的支持信息。

b 要访问您的组织的所有未解决和已解决的支持请求，请单击**查看支持请求历史记录**。

此时将在 Customer Connect 上打开**支持请求历史记录**页面。

然后，您可以按组织、类型和时间段筛选支持请求。您还可以对数据进行排序和导出。

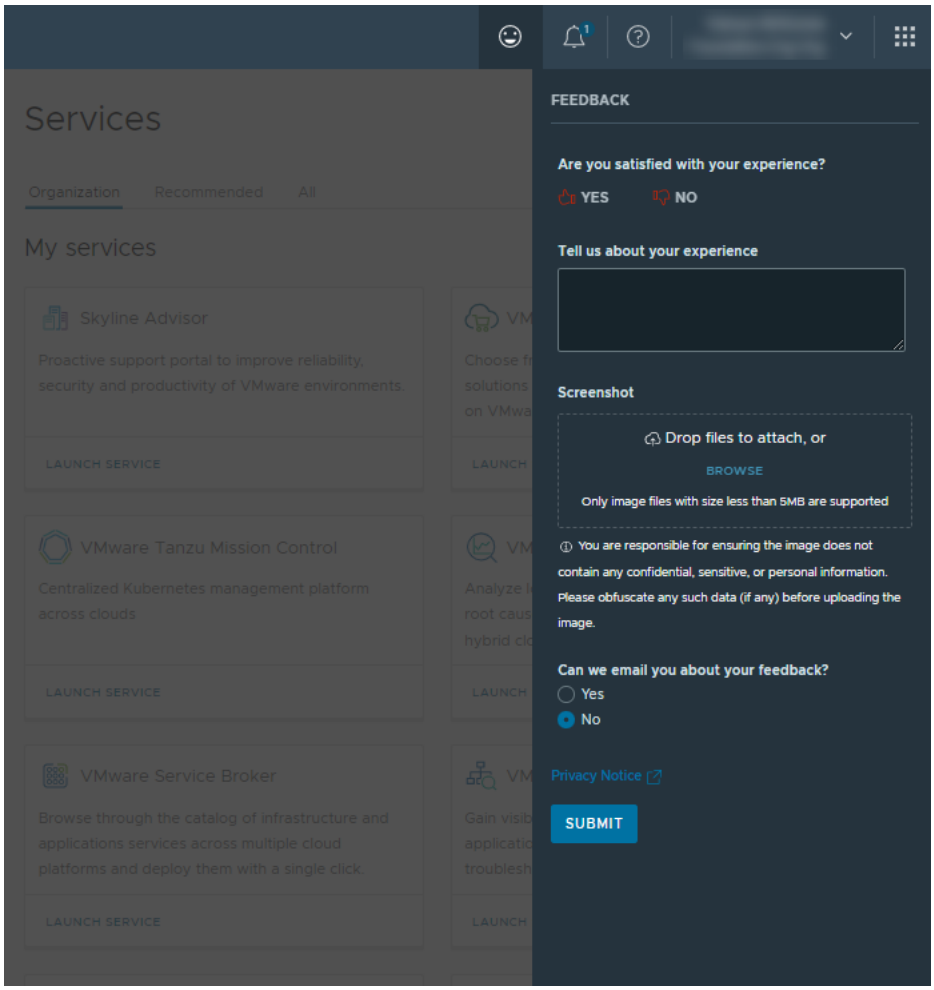
如何提供反馈

13

反馈有助于我们改进产品。您可以直接从产品中提交有关 Cloud Services 控制台 的反馈。

1 在 Cloud Services 控制台 的水平菜单中，单击**反馈**图标（ ）。

此时将打开反馈面板。



2 使用一个或多个可用选项提供反馈：

- 使用拇指向上或拇指向下图标可传达您对使用 Cloud Services 控制台 的满意度。
- 使用文本字段更详细地描述您的体验。

- 如果要直观地增强反馈消息，请通过单击**浏览**或者将图像拖放到指定的字段来附加屏幕截图。
- 请告知您是否要进一步与 VMware Cloud Services 控制台 团队就您的反馈进行接洽。

3 单击**提交**。