

云计算关键领域安全指南 v4.0 的官方网址是：

英文版：

<https://cloudsecurityalliance.org/document/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v4-0/>

中文版：<https://www.c-csa.cn>

官方学习指南：



© 2017 Cloud Security Alliance – All Rights Reserved All rights reserved.

你可以下载、存储、显示在你的电脑上,查看,打印, 以及链接到云计算关键领域安全指南 v4.0

<https://cloudsecurityalliance.org/document/V4.0security-guidance-for-critical-areas-of-focus-in-cloud-computing-v4-0/>,

以下主题:(a)报告可用于个人, 信息,非商业用途;(b)报告不得修改或以任何方式改变;(c)报告不得重新分布;(d)商标,版权或其他条款不可被删除。根据美国版权法的合理使用条款, 如果你将引用部分归为云计算关键领域安全指南 v4.0, 那么你可以引用报告的部分内容。

中文版翻译说明

CSA 云计算关键领域安全指南 v4.0 由 CSA 大中华区研究院组织志愿者进行翻译。

参与翻译工作专家名单：

D1 及前面部分由高轶峰、张全伟、洪毅翻译，D2 由王永霞翻译，D3 由刘剑、白阳翻译，D4 由陈皓翻译，D5 由牛志军翻译，D6 由李建民翻译，D7 由孙军、刘永钢、陈光杰翻译，D8 由王红波翻译，D9 由黄远辉翻译，D10 由耿万德翻译，D11 由任兰芳翻译，D12 由姚伟翻译，D13 由黄远辉、马超翻译，D14 由邹荣新翻译。

参与审校工作专家名单：

D1 及前面部分由顾伟、王朝辉审校，D2 由李建民审校，D3 由刘剑、白阳审校，D4 由耿万德审校，D5 由陈皓审校，D6 由王永霞审校，D7 由孙军、刘永钢审校，D8 由姚伟审校，D9 由王红波审校，D10 由牛志军审校，D11 由张全伟审校，D12 由任兰芳审校，D13 由黄远辉审校，D14 由高轶峰审校。

合稿审核：郭剑锋、叶思海、刘文字、李雨航、杨炳年。

全文由郭剑锋、叶思海负责组织和统稿。

在此感谢参与翻译工作的志愿者。由于翻译时间仓促，存在很多不足的地方，请大家批评指正。欢迎大家提供修改意见，可发送邮件到下面邮箱：info@china-csa.org。

前言

欢迎来到云安全联盟关于云计算关键领域安全指南的第四个版本。云计算的兴起是一项不断发展的技术，它带来了许多机遇和挑战。通过这个文档，我们的目标是提供指导和灵感来支持业务目标，同时管理和减轻采用云计算技术相关的风险。

云安全联盟促进了在云计算领域内提供安全保证的最佳实践，并为寻求采用云计算模式的组织提供了一个实用的、可执行的路线图。云计算关键领域安全指南的第四个版本是建立在之前的安全指南、专门地研究、云安全联盟成员、工作组以及我们社区的行业专家的公开参与之上的。该版本集成了云、安全性和支持技术方面的进展，反映了现实世界的云安全实践，集成了最新的云安全联盟研究项目，并为相关技术提供了指导。

安全云计算的发展需要来自广泛的全球分布式利益相关方的积极参与。CSA 汇集了不同的行业合作伙伴、国际机构组织、工作组和个人。我们非常感谢所有为这次发布做出贡献的人。

请访问 cloudsecurityalliance.com，了解您如何与我们合作，确定并促进最佳实践，以确保有一个安全的云计算环境。

Best Regards,

Luciano (J.R.) Santos

Executive Vice President of
Research Cloud Security
Alliance

致谢

Lead Authors

Rich Mogull
James Arlen
Adrian Lane
Gunnar Peterson
Mike Rothman
David Mortman

Editors

Dan Moren
John Moltz

CSA Staff

Jim Reavis
Luciano (J.R.) Santos
Daniele Catteddu
Frank Guanco
Hillary Baron
Victor Chin
Ryan Bergsma
Stephen Lumpe (Design)

编著者

我们谨代表 CSA 董事会和 CSA 执行团队，感谢所有为 CSA 云计算关键领域安全指南提供时间和反馈的个人。我们珍视您的志愿者贡献，相信像您这样的志愿者将继续引领云安全联盟走向未来。

CEO 的来信

我对这个社区的云安全最佳实践的最新贡献感到非常激动，这一实践始于 2009 年 4 月发布的云安全联盟最初的指导文件。我们希望您能仔细研究这里列出的问题和建议，与您自己的经验相比较，并向我们提供您的反馈。非常感谢所有参与这项研究的人。

最近，我有机会与帮助建立云安全联盟的一位行业专家共度一天。他表示，CSA 已经完成了最初的任务，即为了证明云计算可以安全，并提供必要的工具来实现这一目标。CSA 不仅帮助云计算成为信息技术的可靠安全选择，而且今天的云计算已经成为 IT 的默认选择，并且正在以非常深远的方式重塑现代商业世界。

云计算的巨大成功和 CSA 在引领受信任的云生态系统方面的作用，给我们的新使命带来了更大的挑战和紧迫感。云现在已经成为各种计算形式的后端，包括无处不在的物联网。云计算是信息安全行业的基础。集装箱(容器)化和 DevOps 等等在组织内的 IT 新常态，已经与云计算密不可分，加速了我们的变革。在云安全联盟中，我们致力于为您提供在高速发展的 IT 环境中您所需的必要的安全知识，让您保持在新时代质量保证和信任趋势的前沿。总之，我们欢迎你们加入我们的社区。

Best Regards,

Jim Reavis

Co-Founder & CEO

Cloud Security Alliance

目录

D1: 云计算概念和体系架构.....	8
D2: 治理与企业风险管理.....	30
D3: 法律问题，合同和电子举证.....	40
D4: 合规和审计管理.....	55
D5: 信息治理.....	62
D6: 管理平面和业务连续性.....	69
D7: 基础设施安全.....	80
D8: 虚拟化和容器.....	95
D9: 事件响应.....	106
D10: 应用安全.....	113
D11: 数据安全和加密.....	124
D12: 身份、授权和访问管理.....	135
D13: 安全即服务.....	147
D14: 相关技术.....	154

D1: 云计算概念和体系架构

1.1 简介

本域为云计算安全指南的其它所有部分介绍一个概念性的框架。它描述和定义了云计算，设置了我们的基本术语，并详细描述了文档其余部分中使用的总体逻辑和架构框架。

看待云计算有很多不同的方式:它可以是一项技术、一系列的技术、一种运作模式、一种商业模式，这儿仅仅举了几个例子。从本质上来说，这是一场颠覆性的变革。它发展地非常非常快，而且没有放缓的迹象。虽然我们在本指南的第一个版本中包含的参考模型依旧比较准确，但是它们显然已经不再那么完整了。即使这样更新后也不可能解释未来几年的每一个可能的变化。

云计算为敏捷、弹性和经济带来了巨大的潜在收益。组织可以运转地更快(因为他们不需要购买和拨备硬件，所有的都是软件定义的)，减少停机时间(由于固有的弹性和其他云特性)，并且节省资金(由于资本支出减少，需求和能力匹配)。自云服务提供商有重大的经济激励措施来保护消费者以来，我们也看到了安全收益。

然而，这些收益是在您理解并采用原生云模型，并调整您的架构和控制，以适应云平台特性和功能的基础上才会出现。其实，使用现有的应用或资产，并在不进行任何更改的情况下将其移动到云服务提供商，往往会降低敏捷性、弹性，甚至是安全性，同时还增加了成本。

该领域的目的是建立基础，以使文档的其余部分及其建议都基于此。其意图是为信息安全专家提供一种通用语言和对云计算的理解，并开始强调云计算和传统计算之间的区别，以及帮助引导信息安全专家采用原生云方法，从而带来更好的安全性(以及其他收益)，而不是产生更多的风险。

这个领域包括了 4 部分：

- 定义云计算
- 云逻辑模型
- 云概念、架构和参考模型
- 云安全性和合规管理范围、职责和模型

云安全联盟并没有着手创建一个全新的分类法或参考模型。我们的目标是对现有的模型进行提取和协调——最值得注意的是 NIST 的特种文献 800-145, ISO/IEC 17788 and ISO/IEC 17789——关注与信息安全专家最相关的是什么。

1.2 概览

1.1.1 定义云计算

云计算是一种新的运作模式和一组用于管理计算资源共享池的技术。

云计算是一种颠覆性的技术，它可以增强协作、提高敏捷性、可扩展性以及可用性，还可以通过优化资源分配、提高计算效率来降低成本。云计算模式构想了一个全新的世界，组件可以迅速调配、置备、部署和回收，还可以迅速地扩充或缩减，以提供按需的、类似于效用计算的分配和消费模式。

NIST 将云计算定义为：

云计算是一个模式，它是一种无处不在的、便捷的、按需的，基于网络访问的，共享使用的，可配置的计算资源（如：网络、服务器、存储、应用和服务）可以通过最少的管理工作或服务提供商的互动来快速置备并发布。

ISO / IEC 的定义非常相似：

通过自服务置备和按需管理，实现网络可访问、可扩展的、弹性的共享物理或虚拟资源池的范式。

描述云的一种(稍微)简单的方法是，它需要一组资源，比如处理器和内存，并将它们放到一个大的池中(在这种情况下，使用虚拟化)。消费者需要从池中获得需要的东西，比如 8 CPUs 和

16 GB 的内存，而云将这些资源分配给客户端，然后客户端连接到网络并在网络上使用这些资源。当客户端完成时，他们可以将资源放回池中供其他人使用。

云可以由几乎任何计算资源组成，从计算（如处理器和内存）到网络、存储以及更高级别资源（如数据库和应用程序）。例如，在数百个其他组织共享的服务中订阅 500 名员工的客户关系管理应用，与在云主机中启动 100 台远程服务器是一样的。

定义:云用户是请求和使用资源的人或组织，云提供商是分发它的人或组织。我们有时还会使用术语“客户”和“消费者”来指代云用户，用服务或简单的云来描述云提供商。NIST 500-292 使用“cloud actor”这个术语，并增加了云代理、运营商和审计人员的角色。ISO/IEC 17788 使用术语云服务用户、云服务合作伙伴和云服务提供商。

创建云的关键技术是抽象和调配。我们从底层的物理基础设施中抽象出资源来创建我们的池，并使用调配(和自动化)来协调从池分割和分发各种资源到用户。正如您将看到的，这两种技术创造了我们用来定义“cloud”的所有基本特征。

这就是云计算和传统的虚拟化之间的区别;虚拟化技术将资源抽象化，但是它通常缺乏将它们组合在一起并按需分发给用户的调配，而是依赖于手动流程。

云是多租户的。多个不同的消费者共享同一个资源池,但彼此相互隔离和孤立。隔离允许云提供商将资源分配到不同的组,孤立确保他们不能看到或修改对方的资产。多租户不仅应用在不同的组织;它还用于在单个业务或组织中分配不同单元之间的资源。

1.1.2 定义模型

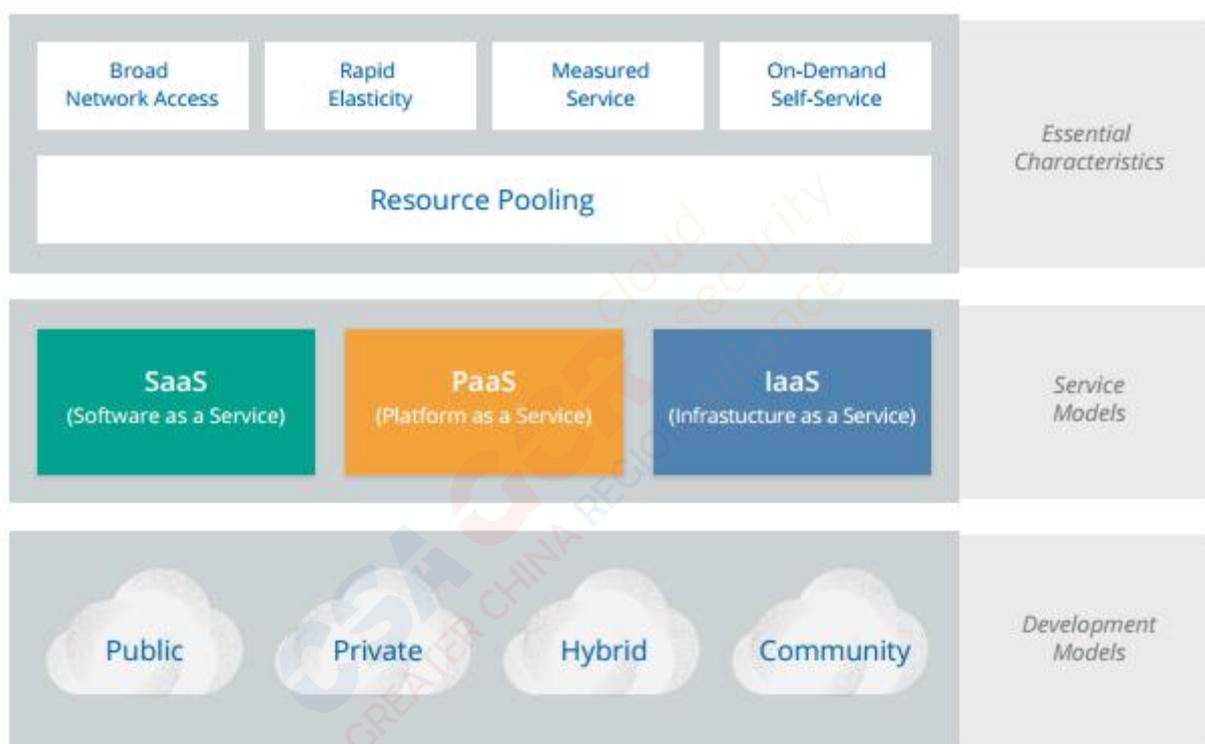
云安全联盟(CSA)使用 NIST model for cloud computing 作为定义云计算的标准。CSA 还支持更深入的 ISO/IEC model，并作为参考模型。在这个领域中，我们将引用两者。

NIST 出版物是被普遍接受的，所以，我们选择与 NIST Working Definition of Cloud Computing (NIST 800-145) 保持一致，这样我们能够集中精力到用例上，而不是细微的语法定义差别上，

同时能保证一致性并获得广泛的共识。

值得注意的是，本指南的目的是使其具有广泛的易用性、适用于全球范围内的组织。虽然 NIST 是美国政府机构，选择此参考模型不应该被解释为是对其它观点或地域的排斥。

在 NIST 对云计算的定义中，包括了五个基本特征、三个云服务模型、以及四个云部署模型。下图对它们进行了形象的汇总，后面会有详细描述。



1.1.2.1 基本特征

以下特性使云成为了云。如果具备以下特征，我们就把它看作是云计算。如果它缺少其中任何一个，它很可能不是一个云。

- 正如上面所讨论的，资源池是最基本的特性。云提供商对资源进行抽象，并将其聚集到一个池中，其中的一部分可以分配给不同的用户(通常是基于策略)。
- 用户自己可以按需自动配置资源，他们自己管理自己的资源，而无需与服务提供商的服务人员互动。
- 广泛的网络访问意味着所有的资源都可以通过网络获得，而不需要直接的实体接取；网络

并不是服务的必须部分。

- 快速弹性允许用户从池中按需使用资源(置备和释放),通常完全自动。这使他们更紧密地匹配资源消耗需求(例如,需求增加时添加虚拟服务器,然后当需求终止时释放它们)。

- 提供可测量的服务,以确保用户只使用他们所分配的东西,如果有必要的话,还可以对他们收取费用。这就是“效用计算”这个术语的由来,因为计算资源现在可以像水和电一样消耗,客户只需要支付他们所使用的东西。

ISO/IEC 17788 列出了六个关键特性,其中前五个特性与 NIST 的特征相同。唯一的补充是多租户,这与资源池是不同的。

1.1.2.2 服务模型

NIST 定义了三个服务模型,它们描述了云服务的不同基础类别:

- 软件即服务 (SaaS)是由服务商管理和托管的完整应用软件。用户可以通过 web 浏览器、移动应用或轻量级客户端应用来访问它。

- 平台即服务(PaaS)抽象并提供开发或应用平台,如数据库、应用平台(如运行 Python、PHP 或其它代码的地方),文件存储和协作,甚至专有的应用处理(例如机器学习、大数据处理或直接 API 访问完整的 SaaS 应用的特性)。关键的区别在于,使用 PaaS,您不需要管理底层的服务器、网络或其他基础设施。

- 基础设施即服务(IaaS)提供了基础性的计算资源,如计算、网络或存储。

我们有时称它们为“SPI”模型。

ISO/IEC 使用了一个更加复杂的定义,它使用了一个与 SPI 模型(软件、基础设施和平台功能类型)密切相关的云功能类型。然后,它扩展到更细粒度的云服务类别,比如计算即服务、存储即服务,甚至还包括 IaaS/PaaS/SaaS。

这些类别具有一定的渗透性:一些云服务跨越了这些模型,而另一些则不完全属于单一的服务模式。实际上,没有理由尝试把所有的东西都分配到这三大类中,甚至是 ISO/IEC 模型中更细粒度的类别。这仅仅是一个有用的描述工具,而不是一个严格的框架。

这两种方法都是同样有效的，但是由于 NIST 的模型更加简洁，并且目前使用得更广泛，所以它是 CSA 研究中主要使用的定义。

1.1.2.3 部署模型

NIST 和 ISO/IEC 都使用相同的 4 个云部署模型。下面描述这些技术是如何部署和使用的，它们适用于整个服务模型的范围：

- 公共云。云基础设施提供服务给一般公众或某个大型行业团体。并由销售云计算服务的组织所有。
- 私有云。云基础设施专为一个单一的组织运作。它可以由该组织或某个第三方管理并可以位于组织内部或外部。
- 社区云。云基础设施由若干个组织共享，支持某个特定有共同关注点的社区。(例如使命、安全要求、政策或合规性考虑等)。它可以由该组织或某个第三方管理并可以位于组织内部或外部。
- 混合云。云基础设施由两个或多个云（私有、社区、或公共）组成，以独立实体存在，但是通过标准的或专有的技术绑定在一起，这些技术促进了数据和应用的可移植性（例如：云间的负载平衡）。混合通常用于描述非云化数据中心与云服务提供商的互联。

部署模型是基于云用户定义的，即使用云的用户。如下图所示，拥有和管理云的组织即使在单个部署模型中也会有所不同。

	Infrastructure Managed By ¹	Infrastructure Managed By ²	Infrastructure Located ³	Accessible and Consumed By ⁴
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/Community				Trusted
Hybrid	<u>Both</u> Organization & Third Party Provider	<u>Both</u> Organization & Third Party Provider	<u>Both</u> On-Premise & Off-Premise	Trusted & Untrusted

¹ 管理包括：治理，运营，安全，合规等

² 基础设施是指物理基础设施，如设施，计算网络和存储设备

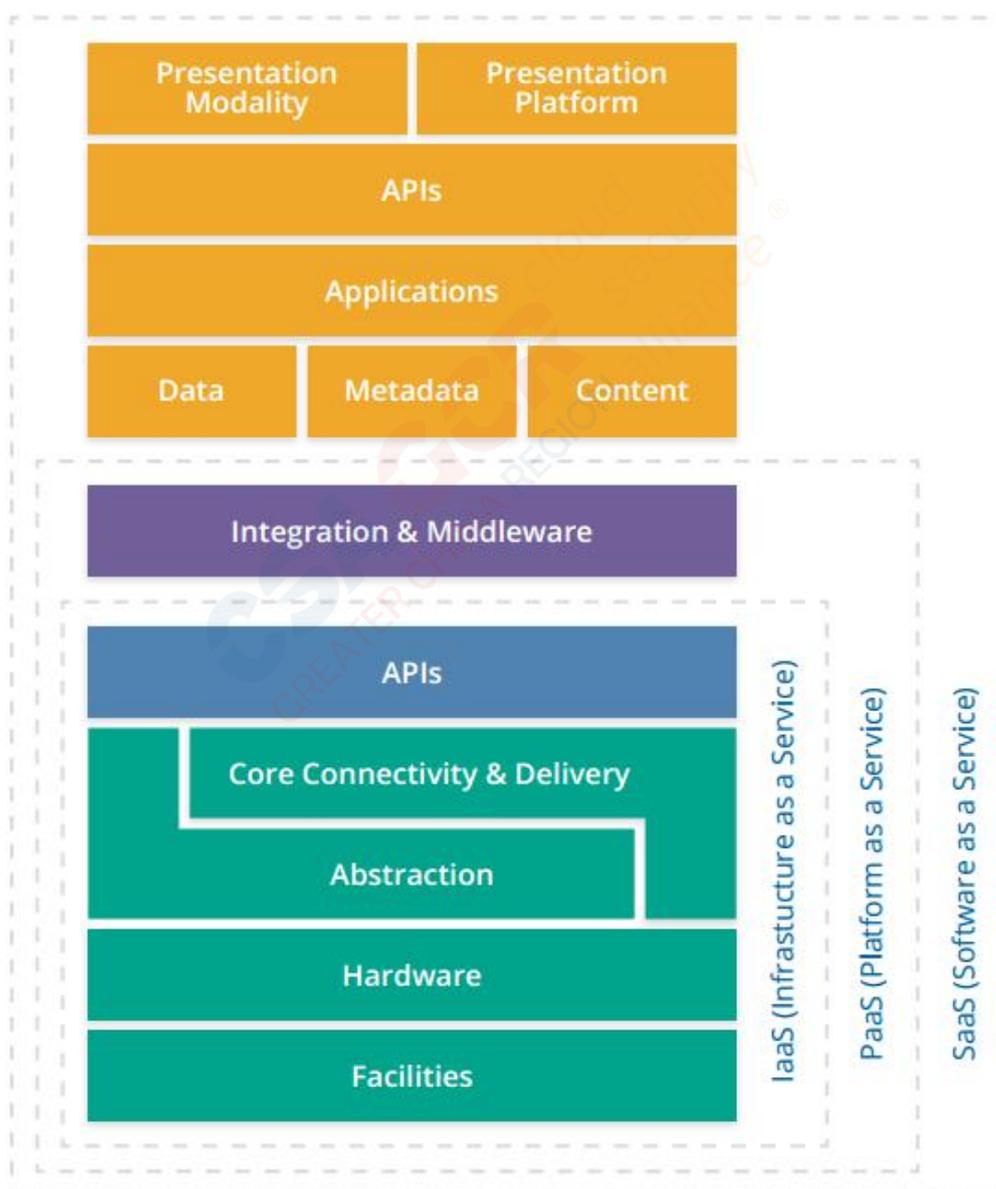
³ 基础设施位置与组织的管理层相比是物理性的，并且与所有权和控制权有关

⁴ 可信用户是那些被认为是组织的合法/合同/政策下的组成部分，包括员工，承包商和业务伙伴。不可信用户是可能被授权使用某些或所有服务的用户，但不属于组织的一部分。

1.1.3 参考和架构模型

现在，在构建云服务方面，有很多不断发展的技术，使得任何单一的引用或架构模型从一开始就过时了。本节的目标是提供一些基础知识，帮助信息安全专家做出明智的决策，以及了解更复杂和新兴模型的基线。对于一个深入的参考架构模型，我们再次推荐 ISO/IEC 17789 和 NIST 500-292，这是 NIST 定义模型的补充。

看待云计算的一种方式是将其视为一个堆栈，SaaS 是位于 PaaS 之上，PaaS 位于 IaaS 之上。这并不是所有(甚至大多数)实际部署的代表，而是作为开始讨论的有用参考。



1.1.3.1 基础设施即服务

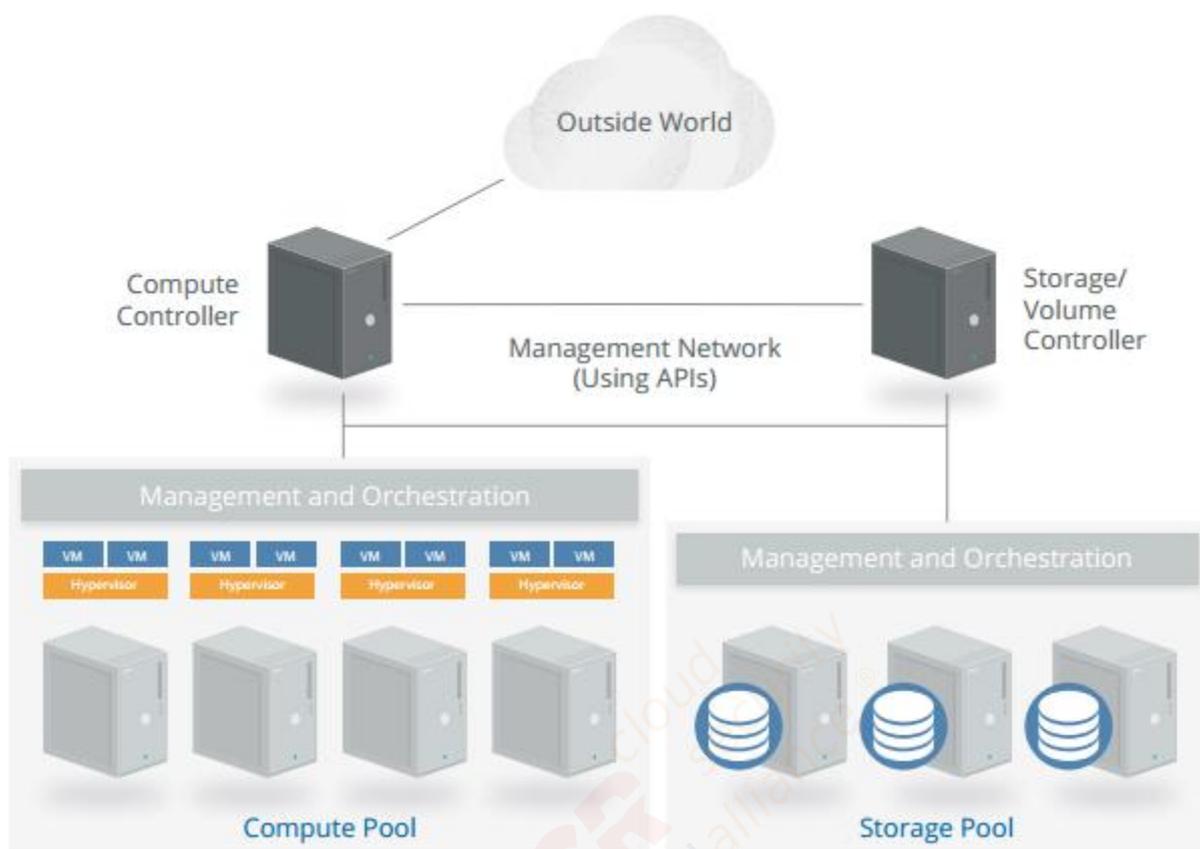
物理设施和硬件基础设施构成 IaaS 的基础。利用云计算，我们将这些资源抽象并集中在一起，但是在最基本的层面上，我们总是需要物理硬件、网络和存储来进行构建。这些资源通过抽象和调配进行汇集。抽象通常通过虚拟化，将资源从物理约束中解放，生成池。然后，一组核心连接和交付工具(编排)将这些抽象资源组合在一起，创建池，并自动化将他们交付给用户。

所有这些都是通过应用程序编程接口(APIs)实现的。APIs 通常是云中组件的底层通信方法，其中一些(或完全不同的集合)公开给云用户，以管理他们的资源和配置。目前大多数云 APIs 都使用 REST(Representational State Transfer)，它在 HTTP 协议上运行，非常适合于 Internet 服务。

在大多数情况下，这些 APIs 都是可以远程访问的，并被封装到基于 web 的用户界面中。这种结合是云管理层面，因为用户使用它来管理和配置云资源，比如启动虚拟机(实例)或配置虚拟网络。从安全的角度来看，这既是与保护物理基础设施最大的区别(因为您不能依赖物理访问作为控制)，也是在设计云安全程序时，需要最优先考虑的问题。如果攻击者进入您的管理平面，他们可能获得您的整个云部署的远程访问完整权限。

因此 IaaS 由设备、硬件、抽象层、编排(核心连接和交付)层组成，将抽象资源绑定在一起，通过 APIs 远程管理资源并将它们交付给用户。

下面是一个 IaaS 平台的简单架构示例:



这是一个非常简单的图表，展示了用于编排的计算和存储控制器，用于抽象的管理程序，以及计算和存储池之间的关系。它省略了许多组件，例如网络管理器。

一系列物理服务器每个运行两个组件：虚拟机管理程序和管理/编排软件，以连接服务器并将它们连接到计算控制器。用户请求一个特定大小的实例(虚拟服务器)，而云控制器确定哪个服务器具有容量，并分配请求的大小的实例。

控制器随后通过请求存储控制器的存储来创建一个虚拟硬盘驱动器，该存储控制器从存储池中分配存储，并通过网络将其连接到适当的主机服务器和实例(用于存储通信的专用网络)。网络，包括虚拟网络接口和地址，也被分配并连接到必要的虚拟网络。

然后，控制器将服务器映像的副本发送到虚拟机中，启动它，并配置它；随着虚拟网络和存储都配置好之后，这就将创建一个在虚拟机中运行的实例。一旦整个过程完成，元数据和连接信息就由云控制器代理，并提供给用户，用户现在就可以连接到实例并登录。

1.1.3.1 平台即服务

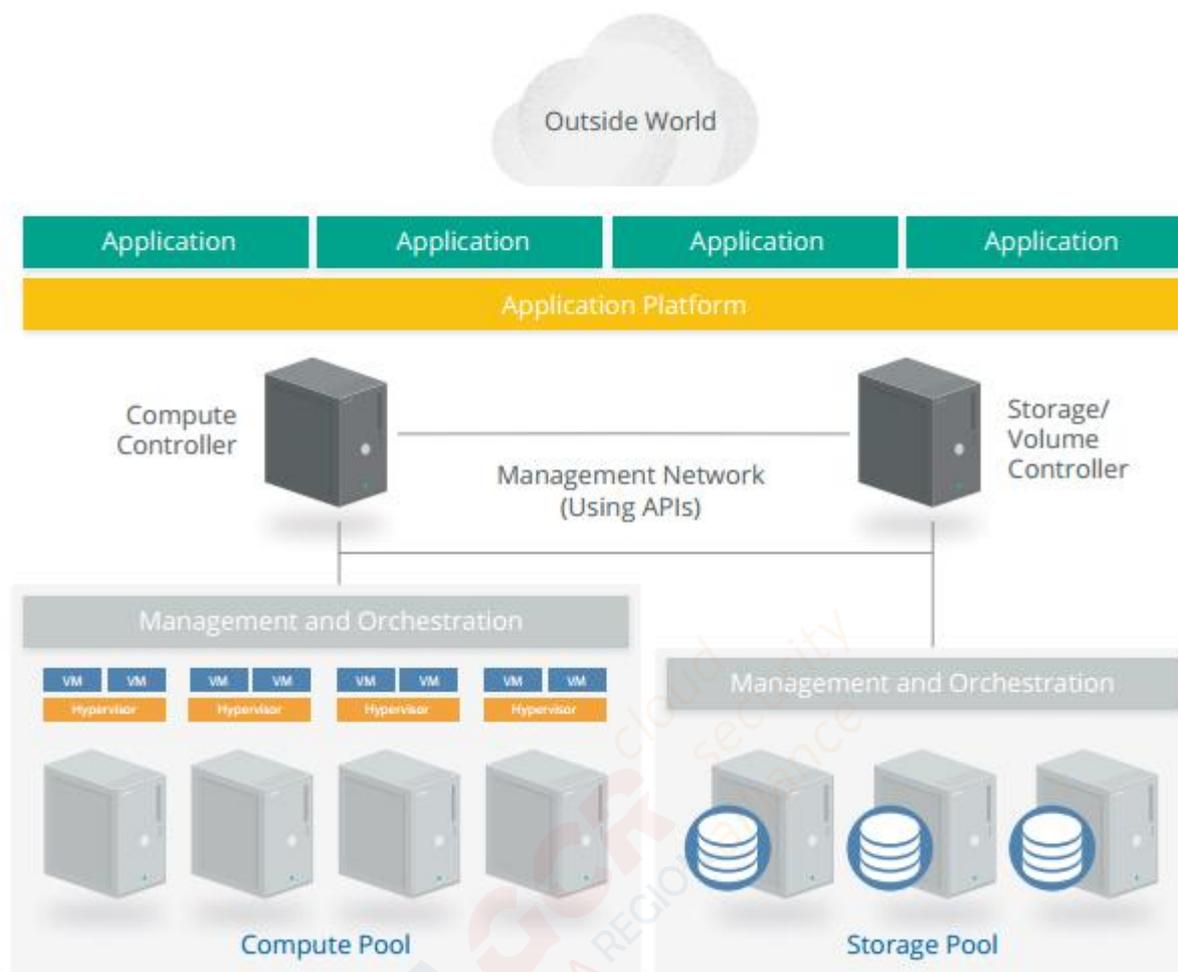
在所有的服务模型中，PaaS 是最难以确定的，因为 PaaS 产品的范围广泛，并且构建 PaaS 服务的方法很多。PaaS 增加了与应用程序开发框架、中间件功能以及数据库、消息传递和队列等功能的集成层。这些服务允许开发人员在平台上构建应用程序，并使用程序支持的编程语言和工具。

在现实世界中经常见到的一个选择，在我们的模型中也可以看到，就是在 IaaS 的基础上构建一个平台。在 IaaS 上构建了集成层和中间件，然后将其汇集在一起，进行编排，并使用 APIs 作为 PaaS 暴露给用户。例如，可以通过在 IaaS 中运行的实例上部署修改后的数据库管理系统软件来构建数据库即服务。用户通过 API(和一个 web 控制台)管理数据库，并通过普通的数据库网络协议访问它，或者通过 API 访问它。

在 PaaS 中，云用户只看到平台，而不是底层的基础设施。在我们的示例中，数据库可根据需要进行伸缩，而不需要管理单个服务器、网络、补丁等。

另一个例子是应用程序部署平台。这使得开发人员可以在不管理底层资源的情况下加载和运行应用程序代码。这种服务使 PaaS 可以运行任何语言编写的任何应用程序，将开发人员从配置和构建服务器中解放出来，让他们与时俱进，或者去操心集群和负载均衡之类的复杂问题。

这个简单架构图展示了一个在 IaaS 架构之上运行的应用平台(PaaS):



PaaS 不一定要建立在 IaaS 之上；没有理由不能自定义设计独立架构。定义的特点是消费者访问和管理平台，而不是底层基础设施（包括云基础设施）。

1.1.3.1 软件即服务

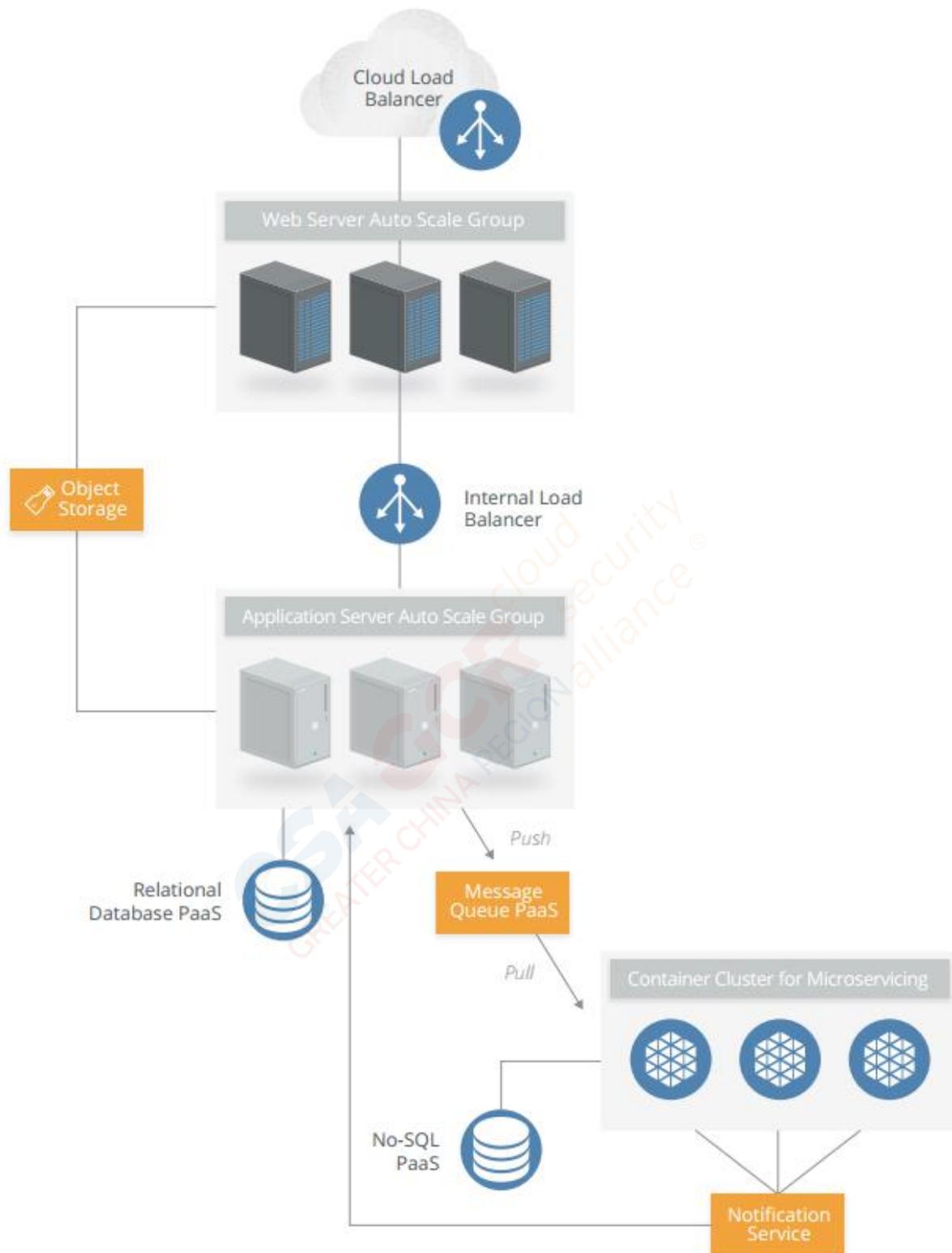
SaaS 服务是完整的、多租户的应用程序，也具有任何大型软件平台的复杂架构。

为了提高敏捷性、弹性和(潜在的)经济利益，许多 SaaS 提供商构建在 IaaS 和 PaaS 之上。

大多数现代云应用程序(SaaS 或其它)都使用 IaaS 和 PaaS 的组合，有时跨不同的云提供商。许多人还倾向于为一些(或全部)功能提供公共 APIs。他们经常需要这些来支持各种各样的客户端，特别是 web 浏览器和移动应用程序。

因此，所有 SaaS 都有一个 API 位于应用程序/逻辑层和数据存储之上。然后有一个或多个表示层，通常包括 Web 浏览器、移动应用程序和公共 API 访问。

下面的简化架构图取自一个真正的 SaaS 平台，但它是通用的，已删除使用中的特定产品的引用：



1.1.4.1 逻辑模型

从宏观上，云计算和传统计算都遵循一种逻辑模型，这种逻辑模型可以基于功能识别不同的层次。

这有助于阐明不同计算模型之间的差异：

- 基础设施：包括计算系统的核心组件：计算机，网络和存储，其他组件设立的基础，移动部件。
- 元结构：提供基础设施层与其他层之间接口的协议和机制，是一种将多种技术紧密联系起来、实现管理与配置的粘合剂
- 信息结构：数据和信息，如数据库中的内容，文件存储等
- 应用结构：部署在云端的应用程序和用于构建它们的底层应用程序服务。例如，PaaS 的功能特性如消息队列，人工智能分析或通知服务

不同的安全性将映射到不同的逻辑层。应用程序安全性映射到应用程序结构，数据安全性映射到信息结构，基础设施的安全性映射到基础设施层。

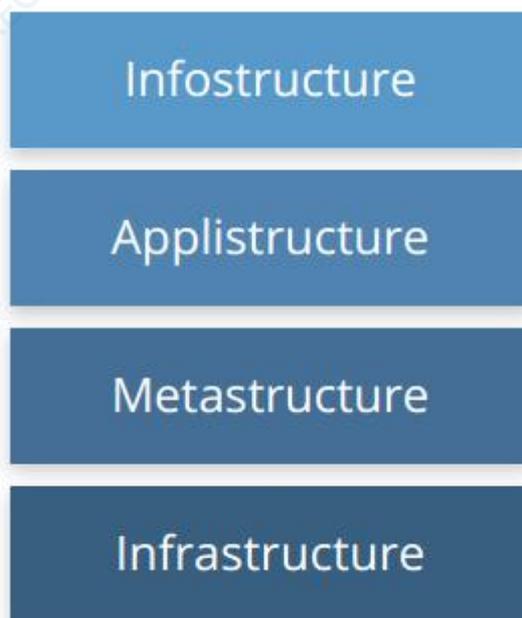
云计算与传统计算的关键区别在于元结构。

云计算元结构包括了可网络接入且远程访问的管理平台组件。

另一个关键的区别在于，在云端，你往往会给每个层次赋予双重的任务。

例如：基础设施包括用于创建云的基础设施以及云消费者使用和管理的虚拟基础架构。

在私有云中，同一个组织可能需要同时管理上述两种基础设施；在公有云中，提供商管理物理基础设施，而消费者管理其部分虚拟基础架构。



正如我们稍后要讨论的那样，这对谁是负责人，及管理、安全性有着深刻的影响。这些层次往往也映射到常见的 IT 组织中的不同专业和技术团队。

尽管最明显且最直接的安全管理差异在于元结构，但云与传统计算在每一个层次都有很大的差异。差异的规模不仅取决于云平台，更取决于云消费者如何利用云平台。

例如，一个极大程度基于云提供商的 PaaS 产品所实现的云应用程序，相比一个仅为了迁移至 IaaS 平台进行细小变更的应用程序而言，具有更多应用程序结构的差异。

1.2 云安全范围、职责和模型

1.2.1 云安全与合规性范围和职责

这听起来也许很简单，但是云安全和合规性包含了一个安全团队在当前应当负责的所有职责。虽然延续了所有传统安全领域，但是其风险、角色和职责的性质，以及控制点的实施时常有着巨大的变化。

虽然云安全和合规性的总体范围没有变化，但是任何一个云服务参与者都应当承担起相应的职责。可以这样想：云计算是一种共享技术模式，不同的组织通常会承担实施和管理不同部分的责任。因此，安全职责也由不同的组织分担，所有的组织都包含在其中。

这通常被称为共享责任模型，它是依赖于特定的云提供商和功能/产品，服务模型和部署模型的责任矩阵。

从宏观上讲，安全职责是与任何角色对于架构堆栈的控制程度相对应的：

- 软件即服务：云服务提供商负责几乎所有的安全性，因为云消费者只能访问和管理其使用的应用程序，并且无法更改应用程序。例如，SaaS 提供商负责周边安全，日志/监控/审计和应用安全性，而消费者可能只能够管理授权和权利。
- 平台即服务：云服务提供商负责平台的安全性，而消费者负责他们在平台上所部署的应用，包括所有安全配置。因此两者职责几乎是平均分配的。例如，使用一个数据库作为服务时，提供商管理基本的安全，修复和核心配置，而云消费者则对其他负责，包括数据库要使用的安全功能，管理账户，甚至是身份验证方法。

- 基础设施即服务：类似 PaaS，云服务提供商负责基本的安全，而云消费者负责他们建立在该基础设施上的其它安全，不同于 PaaS，IaaS 的消费者承担更多的责任。例如，IaaS 的提供商将可能监视他们的网络边界所受到的攻击，但消费者在服务商提供的工具基础上，全权负责如何定义和实现自己的虚拟网络安全。



这些角色在使用云服务中介或其他中介机构和合作伙伴时就变得更加复杂。

最重要的安全性考虑是确切地知道谁负责特定的云计算项目。如果任何特定的云提供商提供了特殊的安全控制，且你清楚地知道他们提供了什么以及如何运作，这一点相对而言就没有那么重要。消费者可以选择通过自身控制来消除控制的差异，或是选择不同的云提供商。当选择 IaaS 时，云消费者的责任就很高，而如果选择 SaaS 则相对较低。

这是云服务提供商和消费者的安全关系的本质。提供商应当做什么？消费者应当做什么？云供应商是否给使用者提供了他们需要的服务？合同中担保了哪些责任和服务水平协议，以及技术文档和细则包含了什么技术？

与这种共享责任模式相关的，有如下两条建议：

- 云服务提供商应该清楚地记录其内部的安全控制和客户的安全功能，因此云消费者能够做出明智的决定。提供商也应正确地设计和实施这些控制。
- 无论是什么云项目，云消费者应建立一个责任矩阵，以确定由谁及如何实施控制。这也应该与所有必要的合规标准相一致。

云安全联盟提供了两个工具，以帮助满足这些要求：

- 共识评估问卷 (CAIQ)，为云服务提供商提供的标准模板以记录他们的安全与合规控制。
- 云控制矩阵 (CCM)，其中列出了云计算的安全控制，并将它们映射到多个安全和合规标准。该矩阵还可以用来记录安全责任。

这两份文件需要根据具体的组织和项目要求进行调整，但它提供了一个全面的初始模板，并确保满足合规要求。

1.2.2 云安全模型

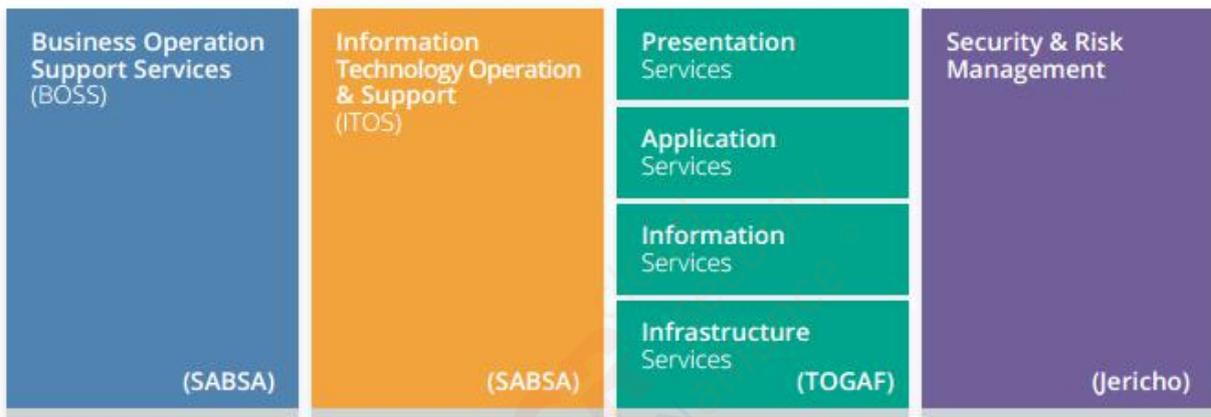
云安全模型是一个协助指导安全决策的工具。“模型”这个词可能有些模糊，所以为了明确我们的目的，我们分解出以下类型：

- **概念模型或框架**，包括用于解释云安全概念和原理的可视化效果和描述，如本文提到的 CSA 逻辑模型。
- **控制模型或框架**，对特定的云安全控制或控制类别进行分类和细化，如 CSA CCM。
- **参考架构**是指实现云安全的模板，这个架构通常是具有普遍性的（例如 IaaS 安全参考架构）。它们可以是非常抽象的，与概念相关，或者相当详细，与特定的控制和功能相关。
- **设计模式**是针对特定问题的可重复使用的解决方案。在安全方面，IaaS 日志管理即其中一个例子。与参考架构一样，它们可能或多或少是抽象的或具体的，甚至是特定云平台上的常见实现模式。

这些模型之间的划分往往是模糊和重叠的，这取决于模型开发人员的目标，甚至将它们中的一些称为“模型”也可能不够准确，但是由于我们看到这些术语在不同来源之间可互换使用，所以将它们分组是合乎情理的。

CSA 已经审查并推荐以下模型：

- CSA [企业架构](#)
- CSA [云控制矩阵 \(CCM\)](#)
- NIST [云计算安全参考架构草案 \(NIST 500-299 号特刊\)](#)，其中包括概念模型，参考架构和控制框架。
- ISO / IEC [FDIS 27017 信息技术 - 安全技术 - 基于 ISO / IEC 27002 的云服务信息安全控制实践守则](#)。



在本指南中，我们还提及其他领域特定的模型。

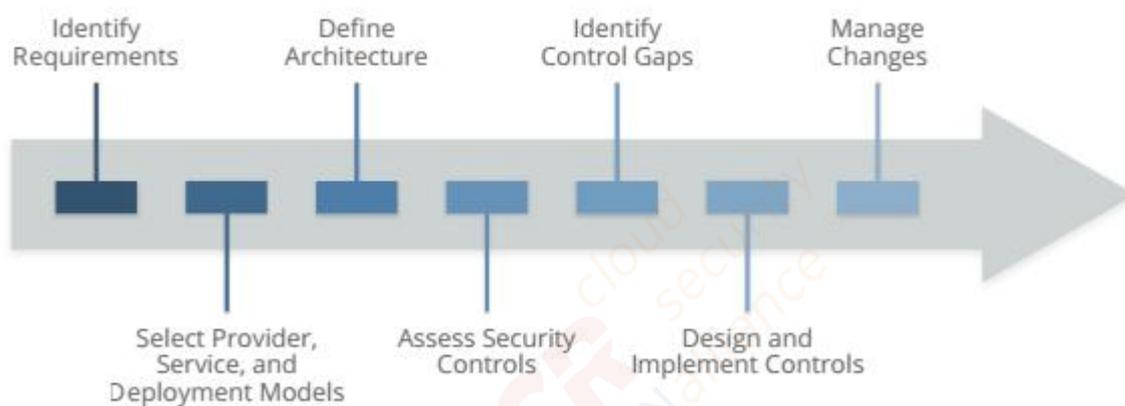
1.2.2.1 一个简单的云安全流程模型

虽然实施细节、必要的控制、具体过程以及各种参考架构和设计模型会根据具体的云项目有很大的不同，但是仍会有一个相对简单的高级流程来管理云安全：

- 确定必要的安全和合规要求以及任何现有的控制点。
- 选择云提供商、服务和部署模型。
- 定义架构。
- 评估安全控制。
- 确定控制差距。
- 设计和实施控制以弥补差距。
- 持续管理变更。

由于不同的云计算项目，即使是同一个云提供商，也可能会采用完全不同的配置和技术，每个项目都应该根据自己的情形进行评估。例如，针对某一供应商部署在 IaaS 上的应用程序所适用的安全控制，与这家供应商部署在 PaaS 的类似项目所适用的安全控制相比，可能看起来区别很大。

关键在于识别需求、设计架构，然后根据底层云平台的功能来识别差距。这就是为什么在将安全需求转化为控制之前，您需要了解云供应商和云架构。



1.3 重点关注领域

组成 CSA 指南的其它 13 个领域着重介绍了云计算安全的关注领域，以解决云计算环境中战略和战术安全的“痛点”（pain points），从而可应用于各种云服务和部署模式的组合。

这些域分成了两大类：治理（governance）和运行（operations）。治理域范畴很广，解决云计算环境的战略和策略问题，而运行域则更关注于战术性的安全考虑以及在架构内的实现。

1.3.1 治理域

领域	名称	描述
D2	治理和企业风险管理	组织治理和度量云计算带来的企业风险的能力。 例如违约的判决先例，用户组织充分评估云提供商风险的能力，当用户和提供商都有可能出现故障时保护敏感数据的责任，及国际边界对这些问题有何影响等都是关注点。
D3	法律问题：合同和电子举证	使用云计算时潜在的法律问题。 本节涉及的的问题包括信息和计算机系统的保护要求、安全漏洞信息披露的法律、监管要求，隐私要求和国际法等。
D4	合规性和审计管理	保持和证明使用云计算的合规性。 本节涉及评估云计算如何影响内部安全策略的合规性、以及不同的合规性要求（规章、法规等）。同时还提供在审计过程中证明合规性的一些指导。
D5	信息治理	治理云中的数据。 本节涉及云中数据的识别和控制；以及可用于处理数据迁移到云中时失去物理控制这一问题的补偿控制。也提及其它项，如谁负责数据机密性、完整性和可用性等。

1.3.2 运行域

领域	名称	描述
D6	管理平面和业务连续性	保护访问云时使用的管理平台和管理结构，包括 Web 控制台和 API。确保云部署的业务连续性。
D7	基础设施安全	核心云基础架构安全性，包括网络、负载安全和混合云安全考虑。该领域还包括私有云的安全基础。
D8	虚拟化及容器（Container）技术	虚拟化管理系统、容器和软件定义的网络的安全性。
D9	事件响应、通告和补救	适当的和充分的事件检测、响应、通告和补救。尝试说明为了启动适当的事件处理和取证，在用户和提供商两边都需要满足的一些条目。本域将会帮助您理解云给您现有的事件处理程序带来的复杂性。
D10	应用安全	保护在云上运行或在云中开发的应用软件。包括将某个应用迁移到或设计在云中运行是否可行，如果可行，什么类型的云平台是最合适的（SaaS, PaaS, or IaaS）。
D11	数据安全和加密	实施数据的安全和加密控制，并保证可扩展的密钥管理
D12	身份、授权和访问管理	管理身份和利用目录服务来提供访问控制。关注点是组织将身份管理扩展到云中遇到的问题。本节提供洞察评估一个组织准备就绪进行基于云的身份、授权和访问管理（IdEA）。
D13	安全即服务	提供第三方促进安全保障、事件管理、合规认证以及身份和访问监督。
D14	相关技术	与云计算有着密切关系的已建立的新兴技术，包括大数据，物联网和移动计算

1.4 建议

- 理解云计算与传统基础设施或虚拟化之间的差异，以及抽象化和自动化对安全性的影响
- 熟悉 NIST 云计算模型和 CSA 参考架构
- 使用工具，如 CSA 的共识评估问卷（CAIQ），来评估和比较云服务提供商。
- 云提供商应清楚地记录其安全控制和功能，并使用类似 CSA CAIQ 的工具进行发布。
- 使用工具，如 CSA 云控制矩阵（CCM），来评估和记录云项目安全性和合规性要求和控制，以及每一个控制点的负责人。
- 使用云安全流程模型来选择提供商，设计架构，识别控制差距，以及实施安全性和合规性控制。

1.5 参考文献

- Rich Mogull
- 基于 Christofer Hoff 的参考模型和逻辑结构

D2: 治理与企业风险管理

2.0 简介

治理与企业风险管理都是被广泛涉及的主题。本指南集中讨论它们在云计算环境下的不同之处。而不是也不应被看做是与云计算无关的环境下的应用探讨。

对安全专家来说，云计算对治理与企业风险管理带来的影响主要有以下四个方面：

- 治理包括组织运作中的策略、流程、以及内控措施。涉及到组织架构和领导层明确的方针，以及任何管理机制。

关于治理更多的信息，请参考：

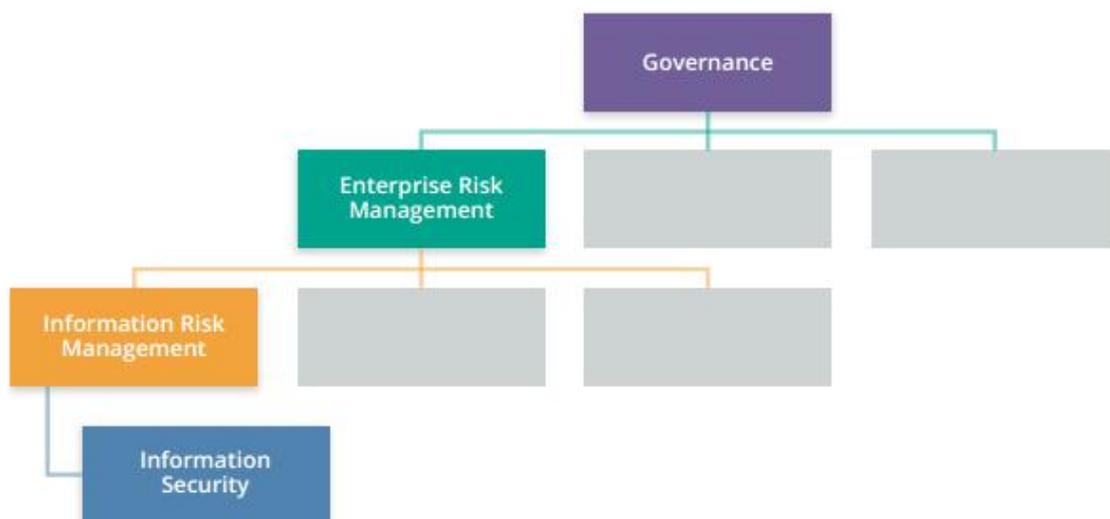
- ❖ ISO/IEC 38500:2015 信息技术 组织 IT 治理
- ❖ ISACA - COBIT - 企业 IT 治理与管理的业务框架
- ❖ ISO/IEC 27014:2013 信息技术 安全技术 信息安全治理

- 企业风险管理包括组织全面的风险管理，与组织的治理和风险容忍度相一致。企业风险管理包括所有类型的风险，不仅仅是技术相关的风险。

- 信息风险管理包括涉及信息本身的风险管理，以及信息技术风险管理。组织面对各种风险，从财务到物理等涉及各个领域，信息仅仅是组织需要管理的一类资产而已。

- 信息安全是管理信息相关风险的工具和实践。信息安全并不是管理信息风险的全部和终结，政策、合同、保险和其他机制也发挥作用（包括非电子数据信息的物理安全等）。然而，信息安全的主要作用是对电子信息以及我们访问电子信息的系统，提供管理流程和控制措施。

在如下图一个简化的层次结构中，信息安全是信息风险管理的工具，信息风险管理进而是企业风险管理的工具，企业风险管理又是企业治理的工具。这四个层次是密切相关的，但需要关注各自的重点、流程和工具。



2.1 一个简单的风险和治理的等级关系

法律问题和合规分别涵盖在域3和域4中。信息风险管理和数据治理在域5中进行说明。信息安全基本上在本指南的其余所有部分都有涉及。

2.1 概述

2.1.1 治理

云计算影响治理关系，因为它要么引入对第三方过程管理（在公共云或托管私有云的情况下），或在私有云的情况下可能改变内部的治理结构。管理云计算时要记住的首要问题是，一个组织永远不能外包治理的责任，即使是使用外部供应商的情况下。无论采用云计算或不采用云计算服务，这都是正确的。但需要理解的是，在云计算环境下的共同责任模式的概念，是非常有用的。

云服务提供商通常会试图利用规模经济来管理成本和提供云计算服务的能力。这意味着需要提供标准化的服务（包括合同和服务水平协议），对所有客户都是一致的。对待云服务提供商，组织的治理模式不一定能像对待其他专用的外部服务提供商一样，专用的外部服务提供商他们通常为每个客户定制自己的产品，包括法律协议。

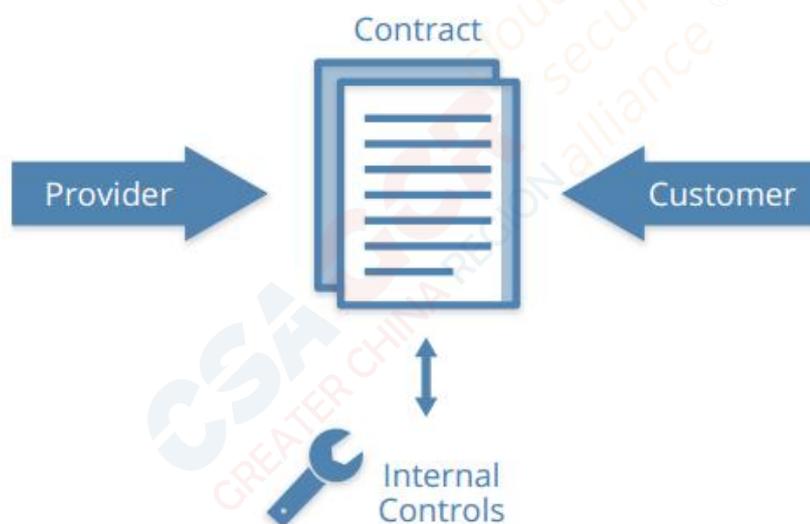
云计算改变了实施管理和治理的职责与机制。如任何业务关系一样，需要在合同中定义治

理的职责和机制。如果关注的领域不在合同中明确，就没有可实施的保障机制，并且存在治理缺口。治理缺口不一定意味着需要排除使用外部供应商，但他们确实要求客户调整自己的流程以减少差距，或接受相关的风险。

2.1.1.1 云治理的工具

与任何其他领域一样，也有用于治理的特定管理工具。此列表更侧重于外部云服务提供者的管理工具，但这些工具通常也可以运用在在内部私有化部署的环境下：

- **合同：**管理的主要工具是云提供商和云客户之间的合同（对公有云和私有云都一样）。合同是把一切都变成法律条款，从而保障任何服务水平或承诺不会违约的唯一方式。合同是将治理扩展到业务合作伙伴和服务提供者的主要工具。



合同定义供应商和客户之间的关系，也是客户向他们的供应商扩展治理措施的主要工具。

- **供应商（云提供商）评估：**这些评估是云客户利用可用的信息和允许的流程/技术，来对潜在的云提供商进行考核的方法。这综合了合同和手册的研究，与第三方认证（法律条款上通常明确要求评估或审计的结果），以及技术研究等各个方面。与任何供应商的评估都非常相似，包括财务上的可行性，历史，特色产品，第三方认证的结果，来自同行的反馈等等。更多关于评估的详细信息在此域和域 4 中描述。
- **合规报告：**合规报告包括供应商内部（即自身）和外部合规评估的所有文件。它们是一个

组织执行自己的内部控制措施情况的审计报告，客户可以选择对提供商进行审计（虽然这通常不是云服务的选项之一），或者由可信的第三方执行。第三方审核和评估通常是首选的，因为他们可以提供具有独立性的验证（假设你信任第三方）。

合规报告往往提供给云服务的潜在客户和已有的客户，但是往往需要签署 NDA 或服务合同。这往往需要是执行公司审计的要求，并不一定能由云服务提供商控制。

评估和审计应根据现有的标准（实际上有非常多的参考标准），关键是需要要了解标准的应用范围，而不仅仅是标准本身。像 SSAE 16 标准具有明确的适用范围，包括评估对象（例如，供应商的服务有哪些）以及相关控制措施的实施评估。因此，一个云服务提供者“通过”了一个审计，不一定包含所有的安全控制措施，这对安全和风险管理人员来说可能是不够的。需要同时考虑第三方的评估，等同于你在做自己评估时，可能进行的活动。并非所有的审计公司（或审计师）都是一致的，公司的经验、历史和资格应包括在你的治理决策中。

云安全联盟明 STAR 注册，可以用来做是一种保证程序，它提供了一系列文件注册表信息，供云提供商基于 CSA 的云控制矩阵（CCM）和（CAIQ）开展通用评估的报告。一些云服务提供商还披露额外的认证信息和评估文件（包括自我评估）。

2.1.2 企业风险管理

企业风险管理（ERM）是组织对所有类型风险的全面管理。与治理一样，合同定义了云服务提供商和云客户之间的风险管理的角色和职责。而且，与治理一样，你永远不能外包你的整体责任，你必须承担对外部供应商的风险管理的职责。

对风险管理，更多的信息可以参考：

- ❖ ISO 31000:2009 风险管理-原则和指南
 - ❖ ISO/IEC 31010:2009 风险管理-风险评估技术
- 【 NIST Special Publication 800-37 版本 1 】（ 2014 年 6 月 5 日 发布 ）
(<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf>)

在云环境下，风险管理是基于责任共享模型的（这是我们最经常讨论的参考安全模型）。对某些风险来说，云提供商承担一定的责任，而云客户要承担比这个范围更大的风险责任。考虑到不同云服务模式之间的差异性，某些情况下这种情况特别明显。在 SaaS 情况下，云服务提供

商承担更多的风险，而在 IaaS 情况下，云客户承担更多的风险。但是，需要再次强调，云客户对风险的所有权负责，他们只是向云服务提供商的传递了一些风险管理的要求。这在私有云情况下，也是一样的；在这种情况下，一个组织单位把一些风险管理的要求传递给了内部的云服务提供商，而不是外部服务提供商，内部的 SLA 和程序取代了和外部的合同。

ERM 依赖于良好的合同和文件，明确的责任划分，以及应对潜在的、未经处理的风险的方式。鉴于治理几乎完全依赖于合同，风险管理可以根据云提供商的文档，深入挖掘他们的技术和流程的能力。例如，合同很少定义网络安全实际上是如何实现的。通过审查供应商的文件，可以提供更多的信息，以帮助做出有效的风险决策。

风险容忍度是指组织的领导和利益相关方愿意接受的风险总量和等级。它会基于资产而变化，你不应该对某个特定的云提供商做一个基准一致的风险决策，相反，风险评估应该与所涉及的资产的价值和要求相一致。因为公有云服务商是外部的，云客户可能会关注一些共享基础设施的资产情况，并不意味着它对所有资产的风险接受程度是一致的。随着时间的推移，你应该建立一个矩阵跟踪表，来描述一系列的云服务以及哪些类型的资产与这些服务相关。迁移到云端不会改变你的风险承受能力，它只是改变了管理风险的方式。

2.1.3 服务模式和部署方式的影响

不仅需要考虑选择不同的云服务提供商，而且在云服务的交付模式上，也必须注意不同的服务模式和部署模式是如何影响风险的管理、治理和能力的。

2.1.3.1 服务模式

软件即服务 SAAS

在大多数情况下，合同谈判的重要性都是 SaaS 服务最明显的例子。好的服务合同将保护风险治理或验证某些情况下风险控制的能力，例如，数据的存储，处理和传输，以及在应用中的情况。SaaS 供应商的规模大小和能力水平，往往分布在两个极端；对一个小型 SaaS 提供商时，谈判合同的可能性要高得多。但不幸的是，许多小型 SaaS 提供商无法在复杂的环境下满足或超

过客户治理和风险管理的的能力要求。具体而言，对 SaaS 应用的基础设施的实际操作来说，整个风险水平的可视性仅限于暴露在由云提供商开发的用户界面而已。

平台即服务 PAAS

这种服务模式可以更加明确要求的细节（同时相关的自我管理和治理风险问题的能力也提升了）。但是完整地沟通合同的可能性比任何其他的服务模式都要低。这是因为大多数 PaaS 的核心驱动力是在提供一个单一的能力，效率会非常高。

PaaS 通常提供丰富的 API，许多 PaaS 提供商也可以收集一些必要的的数据来证明符合 SLAs 要求的达成情况。也就是说，客户必须在确定云服务商的合同约定方面，有效地提出了控制或支持所需的水平能力，以满足治理或风险管理的要求。

基础设施即服务 IAAS

基础设施即服务的云模式最接近传统的数据中心服务（甚至就是一个传统的外包管理数据中心服务）；好消息是对绝大多数现有的风险管理活动，组织已经建立或可以直接利用。然而，对一些新的复杂的业务流程和相关的管理层，如域 1 中描述的，基础设施方面的要求，往往被忽视。

在许多方面，这种模式的业务流程和管理层的风险治理和管理与传统的数据中心的基础设施（网络、电源、暖通、空调等）是一致的。类似的风险治理和管理的问题也是同样存在的，但这些系统对云客户来说可控程度是完全不同的，因此改变现有的管理过程是必需的。例如，控制可以改变网络配置的权限，以及利用云管理工具的界面控制设施管理权限。

2.1.3.2 部署模式

公有云

在公有云这种模式下，云客户对云提供商的管理能力降低了，因为云提供商负责管理和治理云基础设施、相关的人员和其他的一切。并且，云客户也降低了跟云提供商谈判合同的能

力，这必将会影响云客户将自己的治理模式扩展到云端的能力。以同样的合同模板应对多租户的需求是公有云的自然属性：云供应商不能调整为每一个云客户运行使用一套流程，定制一组资源的合同和操作。适应不同的客户需求，是会增加成本的；云供应商需要权衡，而且这往往是使用公有云和私有云之间的分界线。托管私有云的模式下，允许全定制，但由于规模经济损失增加了成本。

这并不意味着你不该尝试谈判你的合同要求，但应认识到对一个云提供商这而言并非普遍可行的，因此你需要选择不同的云提供商（这可能也会造成不太安全的情况），或调整您的需求，并使用替代的风险治理机制，从而减轻这方面的压力。

这种情况非常类似航运服务。当你使用一个普通的运营商/供应商，你无法定义他们的业务模式。而你需要把你的敏感文件包委托给他们交付，希望他们履行安全义务，并满足预期的服务水平协议要求。

私有云

公共云并不是影响风险治理的唯一模式，私有云也会产生影响。如果一个组织允许第三方拥有和/或管理私有云（这是很常见的），这种情况下的风险治理情况与任何其他的外包供应商都是类似的。通过合同中规定双方的义务和责任是非常重要的。

虽然你可能对合同条款有更多的控制权，但确保它们覆盖所需的治理机制仍然很重要。对公共服务提供商，往往通过多种奖励的证据来承诺其服务的能力，而托管的私有云则可以提供其他额外的性能、特定的功能水平和竞争力，但是在合同中也会有额外的费用产生。这必须在合同谈判中考虑，通过条款明确保证该平台的能力。例如，通过要求供应商对私有云平台在一定的时间内始终保持最新的版本，解除合同后关闭相关的服务。

组织内部的私有云的治理模式一般是通过内部服务水平协议（企业或其他组织单位）并提供访问云服务和计费的模式。

混合云

在考虑混合云环境时，治理策略必须考虑由云提供商的合同和该组织的内部治理策略共同组成的最小的公共控制措施集。云消费者同时采用两个云环境或数据中心的服务。在这两种情况下，整体治理是这两种模式的交集。例如，如果您将您的数据中心通过专用的网络链接连接到您云端，您需要解决跨越两个环境的治理问题。

由于社区云是多个组织共享的不对外开放的平台，它的治理延伸到各个社区成员之间的关系，而不仅仅是云供应商和云客户。混合了公有云和托管私有云的治理要求，可以利用合同和其他治理工具，参考一定规模的公有云提供商的模式，但是基于社区的方式进行调整，如托管私有云模式。这也包括社区成员关系，财务关系，以及如何响应成员离开社区时的控制方式。

2.1.3.3 云风险管理的权衡

云计算在企业风险管理方面有利有弊。这些因素包括如下事项，包括公有云和托管私有云等各种情况带来的风险：

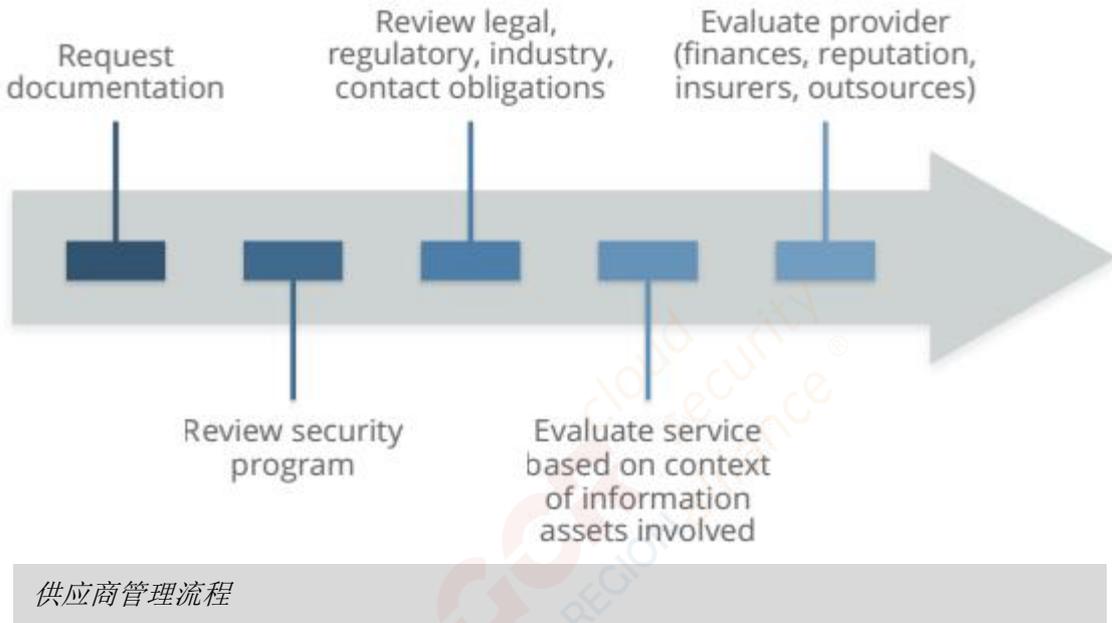
- 对资产和相关流程的物理控制较少，您不实际控制基础设施或云计算提供者的内部流程。
- 由于缺乏日常的可视性或管理方法，对合同、审计和评估有更大的依赖性。
- 这就建立了对关系的积极管理和遵守合同的严格要求。云提供商还不断发展他们的产品和服务，保持竞争力，这些持续的创新可能会超过最初的合同范围，对合同带来变化，或没有包括在现有的协议和评估范围中。
- 云客户和云提供商，通过责任共享模型来管理风险，云客户有可能会减少需求（和相关的成本降低），要求云提供商接受风险。云客户没有外包管理风险的责任，但可以外包一些风险管理措施的实施。

2.1.3.4 云风险管理的工具

下面的过程有助于在云计算部署中提供风险管理的基础。风险管理的核心方法依然是管理、转移、接受或规避风险。但一切都应从正确的评估开始：

供应商评估为云风险管理计划奠定了基础：

- 请求或获取文件。
- 审查其安全方案和文件。
- 审查供应商和相关的任何法律、法规、合同和管辖要求。（见域 3：合法性）。
- 在你的信息资产范围内评估合同中的服务要求。
- 评估云提供商的整体情况，如财政稳定，信誉，和外包商管理等。



定期对供应商审查和评估，以确保它们的输出都是最新的：

- 不要假定来自某一特定提供商的所有服务都符合相同的审核/评估标准。它们是会变化的。
- 如果可能的话，应定期安排评估或采取自动评估的方式。

在审查和理解云提供商管理风险的能力之后，余下的就是残余风险。残余风险通常可以由您实现的控制措施（例如加密）来管理。风险控制的可能性和具体的实现方式，在云提供商、特定服务/特性、服务模型和部署模型上差别很大。如果你开展了所有的评估和执行你自己能采取的控制，仍然有参与的风险，你唯一的选择是转移风险、接受风险、或者规避风险。

风险转移通常是由保险来实现的，但是它是一种不完善的机制，特别是信息风险。它可以弥补一些与一次损失事件相关的财务损失，但对二次损失事件（如客户损失）没有帮助，特别是无形资产损失或难以量化的损失，如声誉损失。从保险运营商的角度来看，网络保险也是一

个新兴的领域，但是还没有在其他形式保险中广泛采用的精算表的深度运用，如火灾或洪水的保险，甚至经济补偿也可能与主要损失事件相关的所需的费用是不匹配的。

2.2 推荐

- 根据选定的云部署和服务模型确定安全和风险管理责任共担模型。参考相关行业最佳实践、国际标准和法规，开发一个云治理框架/模型，例如 CSA CCM、COBIT 5、NIST RMF、ISO / IEC 27017、HIPAA、PCI DSS、欧盟 GDPR 等。
- 了解合同是如何影响您的治理框架/模型的。
 - 在签订协议之前获得和审查合同（以及任何参考文件）。
 - 不要假设您可以有效地与云提供商协商合同，但这也不一定阻止您使用该提供商。
 - 如果合同不能有效协商，并且你认为具有无法接受的风险，那么考虑采用其他机制来管理这种风险（例如监控或加密）。
- 开发云供应商评估的过程。
- 这应包括：
 - 合同审查。
 - 供应商自我评估报告。
 - 遵守文件和政策的程度。
 - 现有审计和评估。
 - 符合客户要求的服务评审。
 - 强有力的变更管理政策，以监测组织使用云服务的变化。
- 云提供商再评估应如期进行，并尽可能自动化。
- 云提供商应提供云客户所需的文档和报告。
 - 例如，CSA STAR 注册表。
- 风险要求应与所涉及的具体资产和这些资产的风险承受能力相一致。
- 建立一种具体的风险管理和风险接受/缓解方法，以评估每个解决方案的风险。
- 控制剩余风险。
- 如果仍然存在剩余风险，选择接受或规避风险。
- 基于资产类型（例如与数据分类相关联）、云的使用情况和管理情况，使用工具跟踪已批准的供应商。

D3: 法律问题，合同和电子举证

3.1 简介

本域着重介绍由云计算所引起的一些法律方面的问题，提供了法律要求方面的一般性背景，包括将数据迁移到云上可能引发法律问题、在云服务协议中要考虑的一些问题，以及在诉讼体系内电子举证所要求的特殊问题。

本域仅就有选择性的问题提出了概述，并不能对所有潜在问题提供足够的细节。对您面临的特定问题，您应咨询你准备参与运营所在的司法管辖区或（和）你客户所在司法管辖区的法律顾问。更进一步要求，应注意法律法规的变化，并在真实环境应用之前，验证和更新本域的参考资料或有关信息。

本域包括如下主题：

法律问题

- 云服务协议（合同）
- 第三方访问存储在云上电子文档的问题

尽管本域包括了数据治理和数据审计/合规方面的一些内容，但相关内容的深入剖析在域 D4 和 D5 两部分。

因为自己部署的私有云的运营与目前大多数现存 IT 的运营相当，本域主要关注公有云或第三方托管私有云的法律问题。

3.2 概述

3.1.1 数据保护/隐私权的法律框架

纵观全球，众多国家有着不计其数的法律、法规以及其它的要求，它们要求公共组织和私营机构要保护个人数据的隐私性、信息和计算机系统的安全性。这些法律部分是依据经合组织（Organization for Economic Cooperation and Development，简称 OECD）的隐私及安全指导意见，以及亚太经合组织（Asia Pacific Economic Cooperation，简称 APEC）的隐私框架。

横跨多个区域的云提供商和云用户，将会面临各种不同司法管辖区域的法律和法规所构成的矩阵，影响因素如下：

- 云提供商所在的区域
- 云用户所在的区域
- 数据主体所在的区域
- 合同适用的法律管辖区域，可能与某些股东不同。
- 这些不同区域之间的互认条约或其他的法律文书。



适用的法律要求应针对不同司法管辖区域，最广泛的吸收多种法律主体和框架

例如，在亚太地区、日本、澳大利亚、新西兰以及许多国家已经通过数据保护法律，这些

法律要求数据的控制人采用合理的技术、物理和管理措施来防范个人数据遭受丢失、滥用或是篡改。

在日本，个人信息保护法案要求私营企业保护个人信息以及数据的安全。在不同领域还有很多特定的法案，例如在医疗行业特定的法律有《医疗从业者法案》、《公共健康护士法案》、《助产士和护士法案》以及《药剂师法案》，这些法案要求注册的医疗职业人员对病人的信息保守秘密。

在澳大利亚，在使用云服务时有两个关键的用于保护客户的法律：《隐私法》（the Privacy Act 1988）和《澳大利亚消费者权益法》（ACL, Australian Consumer Law）。《隐私法》明确了个人信息必须被良好的保持，以确保和个人相关的信息和意见受到保护，并确保在数据和人之间没有关联。《澳大利亚消费者权益法》保护客户免受来自供应商错误或误导合同条款和不良行为的侵害。《隐私法》适用于所有澳大利亚的客户，即使云服务供应商在海外，以及合同中约定适用他国法律的情况。

在欧洲经济区(EEA)，历史上有两个主要的欧盟指令阐明了数据保护方面有关的要求（注：EU Directives，欧盟指令，是一种欧盟法律，要求欧盟的成员国家在其本国的法律中贯彻执行），包括 1995 年欧盟的《数据保护指令》（Data Protection Directive）以及 2002 年的《电子隐私指令》（E-Privacy Directive，2009 年修订版）。这些指令包括包含安全的组成部分，并必须将提供充分安全的职责传递给分包商。其它与欧洲经济区有紧密联系的国家，例如非洲的摩洛哥和突尼斯、中东的以色列和阿联酋也已通过遵循同样准则的类似法律。

包括 1995 年的《数据保护指令》和 2002 年/2009 年的《电子隐私指令》都在逐渐被淘汰或被相关法规替代。在 2016 年 5 月 4 日，欧盟发布了新的《通用数据保护法案》（GDPR），不同于指令，法案对各成员国有直接的约束，不需要各成员国内额外的法律授权程序。GDPR 将在 2018 年 5 月 25 日正式生效（有个相关的指令，要求各个成员国在 2018 年 5 月 6 日前生效）。《通用数据保护法案》将取代 1995 年的《数据保护指令》。用于取代 2002 年《电子隐私指令》，新的《电子隐私法案》草案初稿已经发布，其内容将很快定稿，在其正式实施后可作为 GDPR 的补充。

因此，根据“指令”的要求，在成员国内，当某公司违反其所在国家的数据保护规定，将依照成员国的法律和法规，施以强制性的制裁措施，而新的《通用数据保护法案》将直接约束所有与欧盟公民数据处理有关的公司，争议将由与争议双方的个人或实体关系最密切的数据监管机构或成员国法庭直接裁决。

北美、中美以及南美国家也正在以快速的步伐通过数据保护法律。这些国家的法律都包括安全方面的要求，并且将确保个人数据防护和安全的重担放在了数据保管人身上。无论这些数据位于何处，特别是当向第三方传输时。譬如，除了加拿大、阿根廷以及哥伦比亚的数据保护法律已经出台多年外，墨西哥、乌拉圭和秘鲁也全都通过了数据保护法律。这些法律都主要受到欧洲模式的启发，并且也可能包括对亚太经合组织隐私框架的引用。

在美国开展业务的组织可能受制于一个或多个数据保护法律。这些法律要求组织为他们分包商的行为负责。譬如，金融服务现代化法案（Gramm-Leach-Bliley Act (GLBA) 13）或是 1996 年发布的医疗保险及责任法案（Health Insurance Portability and Accountability Act，简称 HIPAA）要求相关的组织以书面合同的形式迫使他们的分包商采用合理的安全措施，并且遵守数据隐私条款。根据合同执行的一些行业标准，例如《支付行业数据安全标准》（Payment Card Industry PCI Data Security Standards，简称 PCI DSS），也包括对分包商类似的安全要求。

除了这些知名法律法规的示例，美国还有众多小的法律和法规可能影响存储和使用个人信息。这些数据隐私条款常常被嵌入到与某个行业活动相关的一系列法规中（例如，美国联邦法规第 21 章就是关注信息被提交给食品药品监督管理局或被其收集的隐私条例）。还有政府机构，例如联邦贸易委员会（Federal Trade Commission，简称 FTC）或是各州总检察长，无论是否存在特定的隐私法律的影响，他们一般情况下拥有隐私和安全要求的强制权。在 FTC 与温德姆酒店集团（Wyndham）的司法判例中（FTC v. Wyndham, 799 F.3d 236 (3d. Cir. 2015)），法院支持 FTC 以“商业上合理的安全”为由于干预企业在个人隐私方面的错误，并支持其作为一个不公平的贸易惯例（隐私落入了 FTC 管辖范围）。

一般来说，大多数有较强数据隐私法律要求的国家都把他们的法规关注到数据主体即数据所有者上。这些规则保护数据，无论谁持有他们。美国的隐私法案关注谁持有数据，例如，HIPAA 保护法案只应用于由健康计划、医疗保健机构、医疗服务提供者以及他们的代理人（即那些被 HIPAA 视为商业伙伴的人）持有的数据；其他可以收集和使用健康数据的实体有可能不遵守 HIPAA。大多数其他美国联邦隐私法律和法案都与此相同。

除联邦法律和法规外，在美国大多数州都有，至少在违约会导致财务数据丢失方面都有与数据隐私和/或数据安全相关的法律。无论数据存于美国的哪里，这些法律适用于任何在美国的公司（不仅是该法律所在的特定的州）。有些州的法律只适用于他们自己公民的数据，有些州的法律即适用于他们自己公民的数据，还适用于其他缺乏自己数据隐私法的州的公民的数据（参见德克萨斯州法律：Tex. Bus. & Com. Code § 521.053(b).）。这些法律中，有的是特别普遍性的描述，有的则参照特定标准（例如 PCI-DSS，如上文述）并在合规基础上分配责任（例如华盛顿州法律：RCW 19.255.020(2)(b).）。

以下部分就个人数据被传输到云中、或是在云中处理时可能引发与之相关的法律问题提供一些例子。

发行物	描述
美国联邦法	美国是没有全国性数据保护且适用于所有类型个人资料的法律的少数国家之一。美国依赖的是联邦法、州法，甚至地方法混合的法律体系。美国众多的联邦法律以及相关的规定，例如 GLBA、HIPAA、1998 年的儿童在线隐私保护法案（Children’s Online Privacy Protection Act，简称 COPPA），它们与由联邦贸易委员会发布的命令共同要求公司在处理数据时采取专门的隐私和安全措施。在他们与第三方服务提供商的合同中也要求类似的预防措施。根据联邦贸易委员会法第 5 条，联邦贸易委员会在执行案件中签发了众多的法令，各州的总检察长基于该州不公平和欺骗法的要求，在调查公司是否采用“商务上合理的措施”，以保障足够的隐私和安全的进程中，也会签发类似的法令（如适用）。例如，在 FTC 与温德姆酒店集团（Wyndham）的司法判决中要求 Wyndham 公司在处理数据时采用“商业上合理的安全措施”。
美国州法	美国众多的州法也要求公司有义务为个人数据提供充分的隐私保护或安全保护，并要求他们的服务提供商做同样的事情。解决信息安全问题的州法通常至少要求公司与服务提供商的书面合同里有合理的安全措施条款。例如，可参见马萨诸塞州的《联邦居民个人信息保护标准（201 CMR 17.00）》的扩展要求。

标准	<p>例如像 PCI DSS、或是 ISO 27001 这样的标准也引发类似联邦法以及州法那样的多米诺骨牌效应。受制于 PCI DSS、或是 ISO 27001 标准的公司必须遵守特定的标准，并同时会将类似的义务传达给他们的分包商以便满足受制约的这些标准。</p>
非美国法规	<p>许多国家已经通过遵循欧盟模式、经合组织或亚太经合组织模式的数据保护法律。在这些法律下，数据的控制人（通常是与个人有主要关系的法律主体）被禁止收集和处理个人数据，除非如下的要求被满足：例如，如果数据主体同意对其数据收集及对该数据用途的提议。这些法律规定了访问个人数据的实体的若干义务，如某些保密性和安全义务。他们赋予个人一系列权利，使他们可以对抗任何持有其个人资料的实体。当委托一个第三方代表数据的控制人（数据处理人）处理数据时，第三方也对收集和处理个人数据保有责任。数据的控制人被要求确保任何代表它处理个人数据的第三方采取充分的技术、组织架构上的安全措施来保护数据。</p>
合同责任	<p>即使未被规定要采取具体的活动，公司合同上可能有责任保护他们的顾客、联系人或是雇员的个人信息，以确保这些数据未被挪作他用、以及未泄漏给第三方。譬如，这个责任可能来自公司在其 Web 站点上发布的、或是公司已与第三方签订并执行的合同中约定的条款、条件和隐私声明。例如数据处理人可能受其服务协议条款的约束，只针对某一特定目的处理个人数据。</p> <p>此外，公司可能与它的客户签订合同（例如服务协议），在合同中对数据保护（个人或公司的数据）、使用限制、确保安全性、使用加密等做出具体的承诺。组织必须确保当由其监管的数据位于云中时，它会具备持续的能力满足在隐私性通告、或其它合同内所做出的许诺和承诺。例如，公司或许已经同意数据只能用于特定的用途。在云中的数据必须只能用于它们被收集的目的。</p> <p>如果隐私性通告允许这些个人数据的主体访问他们的个人数据、修改或是删除信息，云服务提供商也必须允许其与在非云服务关系下同程度地行使访问、修改和删除的权利。</p>
针对跨国界数据传输的禁令	<p>在全世界有许多法律禁止、或是限制信息传出该国。在有些情况下（例如欧盟的情况），只有当接收信息的国家提供对个人信息、以及隐私权充分的保护时才允许信息传输。该充分保护要求的目的在于：确保那些跨国界被传输到别国数据的个人数据主体可以享有类似的、或是不低于数据传输前所在国家能够提供的隐私权利和隐私保护。或者，有必要在数据输入人和输出人之间签订一个合同，合同约定一旦完成向输入人传输数据，数据主体的权利会确定得到保护。</p> <p>因此对于云计算用户来说，知晓其雇员、客户以及其他人的个人数据将位于何处是重要的，以便能解决国外的数据保护法律可能施加给其的特定限制。</p> <p>依国家而定，确保该充分保护的要求可能是复杂的和严格的。在某些情况下，可能需要首先获得当地数据保护专员的许可。在其他国家（典型的是那些对信息流有限制的国家）则简单禁止把居民的数据传输到国外。</p>

3.1.2 合同与供应商选择

当数据被传输到云中后，保护数据以及确保其安全通常是数据收集人或保管人的职责，即使在某些情况下这个责任可能与他人共享。当数据的保管人依赖第三方来持有或是处理数据时，其对于任何数据的丢失、损坏或滥用仍然承担责任。数据的保管人与云服务提供商签署一份书面的（法律）协议是慎重的，该协议要清晰定义角色、各方的期望和与数据利害攸关的众多职责，这可能是法律或监管上需要的。如该协议还应明确识别允许和禁止使用的数据，以及数据被盗或泄露时应采取的措施。

上述讨论的法律、法规、标准以及相关的最佳实践也要求数据保管人进行尽职调查（在执行合同前）或安全审计（在合同履行期间），以确保这些责任得到履行。

3.1.2.1 内部应尽职调查

公司是委托给他们的数据的保管人。如上所述，许多法律、法规或合同禁止、约束或限定数据披露或转让给第三方。例如，如果没有对“商业伙伴”施加特定的义务要求的情况下，根据 HIPAA 保护健康信息不能被转移到第三方或“商业伙伴”。如果数据源于国外，跨国界转接数据，而不提供“适当的保护”的隐私权和个人资料，很可能是有重大障碍。

在进入云计算之前，公司应该评估自己的实践、需求和限制，目的确定云计算交易相关的法律障碍和合规性要求。例如，应该确定其业务模式是否允许使用，以及在何种条件下使用云计算服务”和“其业务性质可能是放弃对公司数据的控制受到法律限制的。

公司应调查是否存在保密协议或数据使用协议，用于限制传输数据给第三方，即使这第三方是服务提供商。如果公司已签署保密协议，以保护个人信息或商业秘密，没有数据所有者的事先许可，此协议可能禁止雇用分包商。如果公司计划将客户数据处理分包给第三方，则该公司使用的数据可能需要当事人，即客户的同意。这种限制大多数情况适用于转移到云服务提供商。在这种情况下，没有客户的事先许可（数据所有者），迁移数据到云将导致违反与该客户之间的数据使用协议。

在其他情况下，公司处理的数据可能是敏感或保密，数据不应该被转移到云，或转移可能

需要显著的预防措施。存在这样的可能情况，例如与高风险项目有关的文件，如研发路线图，或即将上市、合并或收购的计划。

此外，普通法的观念中如“谨慎义务”或“责任能力”可能会要求公司对云服务提供商进行尽职调查是一个重要因素，以确定服务方是否可以继续有这方面能力保护其资产。

3.1.2.2 监控、测试和更新

云环境不是静态的。它在不断进化并且各方必须与之适应。建议对云服务进行定期的监控、测试和评估，以确保服务提供商采取了要求的隐私及安全措施，并且流程和策略得到遵循。如果没有这种定期测试，控制效果可能会受到一种未被监测到的方式的损害。

此外，公司所处的法律、法规以及技术的形势很可能以快节奏发生变化。必须及时地解决新兴的安全威胁、新出现的法律和合规要求。各方必须与法律、法规、合同要求和其它要求齐头并进，并且确保运营保持在遵守可适用的法律和法规之下；而且随着新的技术和法律浮现，要确保也有不断随之进化的到位的安全措施。

3.1.2.3 外部尽职调查

在签订任何合同之前，尽职调查的关键部分必须是要求和审查对方业务的所有相关方面 - 在此，另一方指拟定的云提供商和云供应商。云服务的购买者需要确保其了解其正考虑购买的特定应用程序或服务。外部尽职调查的程度和投入的时间取决于实际情况。该过程可能需要一天、一个星期，或一个月取决于客户的具体需求、要处理的数据的性质、处理的灵敏度和强度、和其他的因素使一个特定的操作“常规”或“高度敏感”。

因此，根据拟建项目的性质，尽职调查可能涉及评估所提供服务的性质和完整性，服务质量 and 稳定性的信誉”，支持或维护的可用性，客户服务的响应速度，网络的速度，或数据中心的位置。了解客户可能提供深度价值说明。审查针对云提供商提起诉讼的报告可能会很有启发。检查参考资料并进行在线搜索，以评估供应商的声誉可能也是非常有价值的。

在大多数情况下，云的客户将至少要评估可适用的服务水平、最终用户、和法律协议，隐私政策，安全的披露，与适用法律符合的证据（如注册要求）确保云提供商提供的条件适合其组织。根据尽职调查预期的深度和强度，需要调查的问题可能包括：

- 该服务将是可靠的，易于使用？

- 服务器将如何处理数据？
- 服务将如何运作和提供？
- 数据是否与其他客户的数据相匹配？
- 如何将数据保护免受入侵或灾害。
- 价格如何随时间演变？
- 云供应商将满足公司的计算和访问需求吗？
- 云供应商将在未来几年保持业务吗？其财务状况如何？
- 将提供哪些服务水平？
- 使用什么安全措施？
- 在破坏安全的情况下会发生什么？

对于任何新的项目，好的尽职调查要审查所有的云服务协议的条款和条件（包括所有附件，时间表和附录）。这对于云计算尤其重要，因为一些供应商的条款和条件是不可谈判的。在这些情况下，公司将需要准备和装备，以作出明智的决定使用或不使用该供应商。

3.1.2.4 合同谈判

云合同的目的是准确地描述各方的理解。众多的注意事项和措施可以减少当事人使用云服务中暴露在法律，商业接触，和声誉风险的不利影响。

建议合同应始终仔细审查，即使被告知内容是不可协商的。一方面，合同实际上可能是谈判而变化。即使不可能做到这一点，每个云服务的购买者应该理解合同协议的后果和影响。不能协商的合同很可能缺乏特定类型客户所需的某些保护”。在这种情况下，客户应权衡上述保护与承诺的利益之间的风险。

3.1.2.5 依赖于第三方的审核和认证

审计和合规在第 4 域中被更详细地介绍，但两个因素可能影响合同和法律/法规要求。云计算中的第三方审核或认证经常被用来保证与云提供商的基础设施方面的合规性，它允许一个云客户在云平台之上建立自己的标准服务。对于供应商需要发布和客户需要评估的以下因素是至关重要：

- 评估范围。
- 评估中包含哪些特定功能/服务。

例如，云服务提供商的最新存储产品可能不符合 HIPAA（因此供应商可能不愿意签署覆盖它的业务合作协议（HIPAA Business Associate Agreement，BAA）），尽管服务商的其他的许多服务

都能够符合 HIPAA 的要求。

3.1.3 电子举证

本节讨论了美国诉讼的独特要求。围绕“发现”的美国规则，在诉讼中对方当事人可以获取私人文件，这涵盖广泛的潜在文件。特别是，在法庭文件中发现不限于那些在起初就被认为是证据的文件；相反，发现将适用于所有文件的合理预判为证据（证据相关的和证明是证据）。参见联邦民事诉讼规则（Federal Rules of Civil Procedure，FRCP）规则 26。

近年来，已经有不少诉讼当事人被指控自行删除、丢失、或修改不利于自己的重要证据。在这些情况下，联邦民事诉讼规则（Federal Rules of Civil Procedure）认可，资金被认为是无责任的破坏；在某些情况下，陪审团可以给予一个“逆向推理指令”（如法官或陪审团的指示来假定证据被销毁，最坏的可能是其中拥有方摧毁了它）。参见 FRCP 规则 37。由于在这方面进行的诉讼，FRCP 已改为明确各方当事人的责任，特别是在电子化存储信息的情况下（electronically stored information，ESI）。

由于云计算将成为诉讼或调查中所需要的电子化存储信息的仓库，云服务提供商和他们的客户必须仔细规划如何识别案件涉及的所有文档，为了能够满足联邦民事诉讼规则中电子证据发现条款的严格要求，各州也要与这些法律条款相吻合。

在这点上，云服务的客户和供应商需要考虑下列问题，当面对一个客户的“发现”请求，并且可能相关的数据存在于云服务提供商。

3.1.3.1 资产、保管和控制

在美国的大多数司法管辖区，各方有义务生成相关信息，限于其所拥有、保管或控制的文档和数据。托管在第三方的相关的数据，即使是云服务提供商，一般也不会为一方当事人生成信息的义务，尽管有法律权限去查阅或获得这些数据。然而，并非所有托管在云服务提供商的数据会在客户的控制下（例如，灾难恢复系统，云服务提供商用于运行环境创建和维护的某些元数据）。区分哪些数据提供或不提供给客户可能牵涉到客户和供应商的利益。云服务提供商作为信息生成的云数据处理者，其法律程序方面的义务是每个司法管辖区亟待解决的遗留问题。

3.1.3.2 相关的云应用和环境

有时，实际的云应用程序或云环境本身可能与解决争议有关。在这种情况下，云应用程序和云环境可能超出客户的控制，则要求传票或其他发现程序直接送达到提供商。

3.1.3.3 可搜索性和电子取证工具

由于在云环境中，客户可能无法和在自己的环境中一样申请或使用电子取证工具。此外，客户可能没有能力或管理权限搜索或访问托管在云中的数据。例如，客户可以立即访问在自己服务器上的员工的电子邮件帐户，但不具备访问托管在云中的员工电子邮件帐户的能力。因此，客户需要考虑导致受限访问潜在的额外的时间和费用。在一定程度上，客户能够通过协商或补充云服务协议，这个问题可以提前解决。否则，云客户可能没有其他选择，具体解决这个问题时，用户可能需要支付云提供商额外的服务费用，以执行所需的搜索。

3.1.3.4 保存

一般来说，在美国一方有义务采取合理的措施，对其拥有、保管、或控制其所知道的或理应知道的数据和信息，防止数据或信息因销毁或更改而被破坏或修改，这与悬而未决的或合理预期的诉讼或政府调查相关（这在文档销毁上也通常被成为“诉讼保留”）。根据客户使用的云服务和云部署模式，客户在云中保存与在其他 IT 基础设施中保存可以非常类似，也可以更复杂。

在欧盟，信息保存由欧洲议会和欧盟理事会 2006 年 3 月 15 日的指令 2006/24/EC 管辖，日本，韩国，新加坡也有类似的数据保护措施。在南美，巴西和阿根廷分别有阿泽雷多条例草案（Azeredo Bill），阿根廷数据保留法 2004（Argentina Data Retention Law 2004），以及 2004 年 2 月 6 号的 25.873 号法令。在美国，尽管适用于潜在当事人的管辖权裁决多种多样，这些关注内容在联邦民事诉讼法第 37 条得到了广泛的解决。

3.1.3.5 数据保存发法律和记录保持义务

除了源于美国法律关于电子证据的数据保存义务，公司可能需要知道某些数据保留法规的影响。数据保留法要求相关机构“在一定时间周期内保留数据。”

成本和存储：保存可以要求延长大规模数据的保留期。根据服务等级协议（service level agreement，SLA）这样的后果是什么？如果保持要求超出服务等级协议的条款，会发生什么情况？如果客户继续保持数据，谁支付延时存储，以及以怎样的代价？客户是否有在服务等级协议下的存储容量？客户是否能在取证的方式下有效地下载数据，从而可以离线或近端保持数据？所有这些问题都应该被视为转移到云端的一部分。

保存范围：请求方仅有权访问托管在云中包含相关信息的数据，该数据包含或可被合理计算出需要处理问题的与相关、可提供证据的信息，而不享有在云中或在应用程序中的所有数据访问权。（确切限制的问题，很可能在诉讼中得到解决。”）然而，如果客户没能以粒度方式保持相关信息或数据，可能需要过度保持（over-preserve）作为合理的保护，这取决于诉讼或调查。

（然后，在取证过程中，这些信息作用被应确定哪些应该必须和不应作为移交的一部分。这个过程，称为文件审查或特权审查，可以由有偿律师工作人员，或在某些情况下，由专家系统进行。如何对调查产生的越来越多的信息分类，这是一个在法律和技术研究不断前行的领域。）

动态和共享存储：如果客户有空间来容纳数据，数据相对静止，访问的人有限的并且知道如何保存数据，则在云中保存数据的负担可能相对较小。然而，在云环境中以编程方式修改或删除数据，或与没有意识到数据需要保持的人共享，保持变得更加困难。当客户明确这些数据是相关的，而且需要保村的，客户可能需要与供应商合作，以确定合理的方式来保持这些数据。

3.1.3.6 收集

由于可能缺乏管理控制，客户收集来自云中的数据比收集防火墙后面的数据更困难，更耗时，更昂贵。特别是客户对其云中的数据可能不具有相同的能见度水平，将已经收集到的数据与云计算中的数据进行比较，以确定输出的完整性和准确性，可能会更加困难。

访问和带宽：在大多数情况下，客户访问其在云中的数据将取决于服务等级协议。这可能会限制其快速、以取证的方式收集大量数据的能力（即，与所有合理相关的元数据保持一致）。客户和云服务提供商尽早地考虑了这个问题，在诉讼和调查允许收集的情况下，为额外的访问建立协议（和成本）。如果没有这些协议，当请求方和法院交涉时，客户应考虑在云中收集带来

额外的时间和成本。注意，依据 FRCP 26 (B) (2) (B)，因过度的负担或成本，诉讼当事人能够证明信息请求是不合理的。然而，即使是证明是有效的，法院可以命令从这些来源的取证，如果请求方能够证明这些信息为什么是需要，否则也许不能获得。

取证：“云”数据源的位逐位镜像通常是困难或不可能的。为了安全起见，供应商不愿允许访问他们的硬件，特别是在多租户环境中客户能访问到其他客户的数据。即使在私有云中，取证也非常困难，客户可能需要将这些限制通知对方律师或法院。(此外，FRCP 26(b)(2)(b)可以解除这种不适当的负担。)幸运的是，取证在云计算中很少批准，由于数据结构的组成通常是数据分层或虚拟化，本身不能提供有效的额外相关信息进行按位分析。

合理的完整性：客户面对请求发现应采取合理的措施以验证其从云供应商的收集是完整和准确的，尤其在普通业务流程不可获得和诉讼的具体措施被用来获取信息。这个过程与在云中的数据是准确的、经过验证的或可接受的校验是分开的。

无法合理的访问：由于客户存储的数据及客户的访问权限和特权存在差异，存在一些案例显示云中的客户并非可访问所有存储在云中数据。当响应请求发现时，云用户和云的供应商应该分析信息的要求和关联性、重要性、均衡性或可访问性的相关数据结构。

3.1.3.7 直接访问

在云环境外，请求方对相应方的 IT 环境的直接访问是不支持的。(尽快这种事件只是有时发生；事实上，在民事案件中，一些法院已经允许没有通知下查封 IT 设备，为了保全证据，包括就业纠纷。)在云环境中，直接访问甚至不受欢迎，甚至更不被支持，可能和取证分析一样不太可能。重要的是，由于硬件和设施不在其拥有、保管或控制之内，可能无法提供客户直接访问，请求方需要与供应商直接协商以获得此类访问。

3.1.3.8 本地生成

云服务提供商通常把数据存储于云中不受客户控制的高度专有的系统和应用程序中。通常

情况下，ESI 预计将制定的标准格式（如 PDF 的电子文件），除非与此争议相关的转化数据（如元数据）而信息丢失。在这种情况下，云本地生成的原始格式的数据对请求方可能是无用的，因为他们将无法理解所产生的信息。在这种情况下，可能最好的是要求所有有关方，包括生产方和供应商，相关信息的接口使用云计算环境中标准报告或接口协议，应妥善保管有关资料。

3.1.3.9 认证

在这种情况下下的认证是指司法鉴定的数据被接纳为证据。这不应该被混淆为用户身份认证，用户身份认证只是身份管理的一个组成部分。将数据存储云中不影响数据认证，以确定数据是否应被接纳为证据。现在的问题是文档是否是它所声称的。例如，电子邮件不能因为它是存储在公司防火墙后面或存储在云中而被认为更可信或更不可信。问题是它是否被完整的存储，以及法院能否相信从它被创建后没有被改变。在没有其他证据情况下，如篡改或黑客攻击，只是因为被创建或存储在云中，文件不应该被或多或少地认为可接受的或可信的。

3.1.3.10 在电子取证方面供应商和客户之间的合作

供应商和客户最好从合作的一开始就考虑（电子）发现导致的复杂度并在服务等级协议中说明，这符合他们的共同利益。供应商可能要考虑设计包括发现服务的优秀云产品来吸引客户（“设计取证”）。无论如何，客户和供应商应该考虑包含一项协议，是对任何合理的取证请求事件相互配合。

3.1.3.11 传票或搜查令

云服务提供商可能被第三方以传票、搜查令或法院形式的命令要求其提供信息，获得对客户数据的访问请求。客户可能希望能对抗访问请求，确保数据的保密性和秘密性要求。为此，云服务协议应要求云服务供应商把收到传票的信息通知公司，并给公司时间来对抗此类访问请求。

云服务提供商可能会试图通过开放其设施，并向请求者提供访问请求中标识的任何信息来响应请求。在这样做之前，云服务提供商应确保与法律顾问磋商，请求要求是在良好的秩序下，

并采用适当的法律方法。云服务提供商在披露其保管的信息前应认真地分析请求，并考虑是否可以通过发布信息来满足其客户。在某些情况下，服务商可以更好的满足客户的需求，因为它可以满足太宽泛或有问题的需求。

3.1.3.12 更多的信息

关于取证和电子存储信息的更多阅读资料，有各种各样的来源。比较重要的一个是塞多纳会议（**Sedona Conference**），该组织围绕 ESI 的处理提出有影响力建议已经好几年了，他们反过来又在影响这一新兴的法律领域。然而，请注意，他们的建议本身并不具有法律效力。

D4: 合规和审计管理

4.1 介绍

当组织将其业务从传统数据中心迁移至云计算数据中心之时就将面临新的安全挑战。其中最大的挑战之一即遵从众多监管条例对交付、度量和通信的合规约束。云服务的客户和供应商都需要理解和掌握这些不同的条例上的区别，包括在监管上的区别，以及对已经存在的合规和审计标准、过程和实践的区别。而云计算所拥有的分布式和虚拟化的特性，使得原本基于确定目标和物理实体的信息和过程的监管方法需要进行重大的框架调整。

除了云服务供应商和用户之外，监管和审计机构也需要针对云计算这一新领域进行调整。现行的法律法规在编写时，很少考虑到虚拟化环境或者云上的部署。这会导致云计算用户在面对组织合规性的外部审计时面临很大挑战。正因如此，理解云计算与监管环境的相互关系将是任何“云”战略的关键因素。云计算用户、审核机构和供应商务必考虑并且理解以下几点：

- 针对特定的云服务或者服务提供商的监管的影响，对适用跨境或者多管辖权的事例给予特别关注。云服务提供商和用户的合规责任分配，包括间接提供商（如：你所采用云服务提供商的云服务提供商）。这包括合规继承的概念，其中提供商可能有他们服务的一部分被认证为合格，这部分可以从客户的审核范围中剔除，但客户仍然对建立在顶层的供应商的合规性负责。
- 云服务提供商证明其合规的能力，包括及时的文档生成，证据产生以及过程合规性。

一些附加的云服务特定的问题需要特别关注，包括以下几点：

- 供应商审核和认证的作用以及如何影响客户审核（或评估）范围。
- 了解云提供商的哪些功能和服务属于审核和评估的范围。
- 随着时间的推移管理合规性和审计。
- 与可能缺乏云计算技术经验的监管和审核机构合作。
- 与可能缺乏审核或合规性经验的供应商合作。

4.1 概览

用大量的现代法规和标准实现并保持合规性是大多数信息安全团队的核心工作，也是治理和风险管理的重要工具。以致于该领域的工具和团队有自己的缩写：GRC，即治理（Governance），风险（Risk）和合规性（Compliance）。虽然 GRC 与审计密切相关。纵然审计是一种支持，确保和证明合规性的关键机制。但合规性不止于审计，而审计也不止于确保合规性。于我们而言：

- 合规性确保公司义务的认识和遵守（例如，企业社会责任，道德，适用法律，法规，合同，战略和政策）。合规过程评估认识和合规的状态，进一步评估不符合成本的风险和潜在成本，将其与实现合规所需的成本进行比较，并以此为依据来对必要的补偿性措施来进行优先级规划，资金支持和项目启动。
- 审计是证明（或反驳）合规性的关键工具。同时，审计和评估也被用于支持不合规风险决策。

本节将单独讨论这些相关的领域，以便更好地专注云计算对其各自的影响。

4.1.1 合规

云服务（或任何地方）的信息技术越来越受到政府、行业团体、业务相关方和其他利益相关者的政策和法规的影响。合规性管理是一种治理工具；它是关于一个组织如何评估，采取补救措施，和证明它满足这些内部和外部合约的工具。

特别是法规通常对信息技术和信息治理有很强影响，尤其是在监控，管理，保护和公开披露方面。许多规章制度和义务都要求一定等级的安全性，这就是为什么信息安全与合规性紧密结合的原因。因此，安全控制是一个确保合规性的重要工具，并且这些控制的评价和测试是安全专业人员的核心工作。甚至专门的内部或外部审计师执行评估本身也是评估的内容。

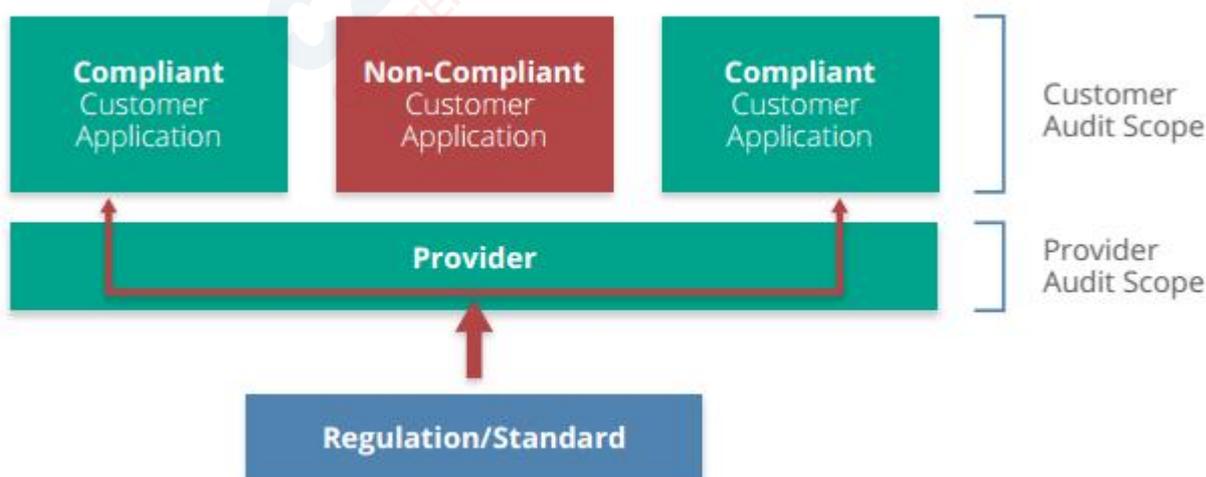
4.1.1.1 云如何改变合规

与安全性一样，合规性在云服务中是一个共享责任模式。云服务供应商和客户都有责任，但客户始终对自己的合规性负责。这些责任是通过合同，审核/评估，和具体的合规性要求的细节来确定的。

所有云客户，尤其是公有云的客户，必须更多地依赖于供应商的第三方认证来了解他们的合规性和差距。由于公有云提供商依赖于规模经济来管理成本，他们往往不会让客户来进行审计。相反，类似于公开上市公司的财务审计，他们与第三方的公司执行审计和颁发认证。因此，云的用户通常不会自己定义审计的范围或者自行执行审计。他们往往需要依靠这些报告和认证来决定服务是否符合他们的合规性责任。

许多云供应商被各种法规和行业要求认证，如 PCI DSS, SOC1, SOC2, HIPAA, 最佳实践/框架如 CSA CCM 和全球/区域法规如 EU GDPR。这些有时被称为准入型审计 (pass-through audit)。准入型审计是合规性继承的一种形式。在这个模型中，云供应商的所有或者某些基础设施和服务依照合规标准进行审核。供应商承担这些认证的成本并维护认证。对供应商进行审计，包括准入型审计，都需要了解其局限性：

- 这些审计证明供应商是合规的。
- 在云服务上建立合规的应用程序和服务仍然是客户的责任。
- 这意味着供应商的基础设施/服务不在客户审核/评估范围之内。但客户建立自己的一切仍在审计范围内。
- 客户为他们自己所建立和维护的，承担最终的合规责任。例如，如果一个 IaaS 供应商获得 PCI DSS 认证，客户可以在该平台上建立自己的 PCI 合规的服务，而供应商的基础设施和运营应在客户的评估范围之外。然而，如果客户没有对在云服务中运行的应用程序进行适当的设计，那么将会极易与 PCI 规则产生冲突从而造成评估失败。



根据合规继承，云供应商的基础架构在客户合规审计范围之外，但是客户配置和在认证的服务之上建立的一切依然在审计范围内

云服务合规性问题不仅仅是准入型审计；云服务的特质也创建了额外的差异性。

许多云供应商提供全球分布式数据中心运行的中央管理控制台/平台。但管理和理解在哪里部署数据并保持其在全国和国际司法管辖区的法律合规性仍然是客户的责任。

在传统计算中组织有同样的责任，但云计算大大减少了这些潜在的国际部署时候的冲突。比如，如果没有启用适当的控制来防止这种情况，开发人员可能在无需请求国际数据中心并签署多级合同的情况下，就可以在不符合规定的国家/地区部署受管制数据。

并不是一个给定的云服务供应商的所有功能和服务必须符合和认证/审核的所有法规和标准。云供应商有责任清晰的说明认证和证书，让客户了解认证的范围和局限性。

4.1.2 审计管理

合适的组织治理结构自然包括审计和保证。审计必须独立进行，并应被稳健的设计从而反映最佳的实践、适当的资源和测试协议和标准。在深入研究云服务影响之前，我们需要定义有关信息安全的审计管理的范围。

审计和保证是证明符合内部或外部要求（或识别缺陷）的合规性的机制。报告需要包括合规性测定，以及确定的问题、风险和补偿建议的清单。审计和保证不仅限于信息安全，也包括那些与信息安全相关的方面，通常集中在评估安全管理和控制的有效性。大多数组织受内部和外部审计和评估的混合管制以确保符合内部和外部要求。

所有审核有可变范围和适用性声明，它定义了评价对象（如所有系统与财务数据）和控制范围（如行业标准，自定义范围，或两者都有）。认证是来自第三方的法律声明，可以作为审计结果声明。认证是对云供应商进行评价和采纳使用的一个关键的工具，因为云客户不总是可以自己的云供应商进行评估。

审计管理包括对审计和评估相关的所有活动的管理，如确定需求、范围、进度和职责。

4.1.2.1 云如何改变审计管理

一些云客户可能习惯了去审计第三方供应商，但云计算的性质和与云供应商的合同往往会对于部署地点现场的审计形成障碍。客户应该了解的是，云供应商在同时给多个租户提供服务的时候，会（并且通常应该）将部署地点现场审计视为一种安全风险。来自大量客户的多个部署地现场审计会呈现明显的逻辑性和安全性挑战，特别是当供应商使用一组共享资产来给客户创建资源池时。

客户与这些供应商的工作将会不得不依赖第三方认证而不是他们自己执行的审计。根据审计标准，实际审计结果只有在保密协议（NDA）的约束下才可以给用户查看，这意味着客户在获得风险评估或其他评价的结果之前，需要遵守相关基本的法律协议。这往往是由于法律或审计公司的合同要求，而非出于云供应商混淆视听的意愿。

云供应商应该理解，客户仍然需要确保供应商履行合同及监管义务，因此应提供细致的第三方认证来证明他们履行自己的义务，尤其是当供应商不允许客户直接对其进行评估时。这些认证应基于行业标准，要有明确的界定范围和具体的被评估的控制列表。发布证书和认证（在法律允许的程度）将大大帮助客户评估云供应商。云安全联盟星级登记处（Cloud Security Alliance STAR registry）为供应商提供了一个中央库，以便供应商公开发布这些文件。

一些标准是用于证明文档所述的控制达到了需求和设计的要求，如 SSAE 16。这个标准不必明确控制的范围，所以都需要进行完整的评价。同时，认证和证明不一定适用于云服务供应商提供的所有服务。供应商应该明确哪些服务和功能被覆盖，客户有责任注意并了解对自己所使用的供应商的影响。

某些类型的客户技术评估和审计（如脆弱性评估）在供应商的服务条款内或许会被限制，又或许需要许可。这通常帮助供应商区分合法评估和攻击。

重要的是要记住认证和证明是基于某个时间点的行为。认证是一个“一段时间”的评估，并可能在未来任何时间点无效。供应商必须保持现有的任何已发布的结果，否则有可能使客户面临不合规的风险。根据合同，这甚至可能造成供应商的法律风险。同时，客户也有责任确保

他们所依赖的认证结果，并且在供应商的情况随时间变化时及时跟踪。



证据 (Artifacts) 是日志、文件和其他在审计和证明合规性所需的材料的集合；他们是支持合规活动的证据。供应商和客户都有责任制定和管理各自的证据。客户最终要对证据负责以支持自己的审计，因此需要知道供应商提供什么，并创建自己的证据来弥补之间的差距。例如，由于在 PaaS 上的服务器日志可能无法获得，所以需要在应用程序中构建更强大的登录日志进行补偿。

4.2 推荐

- 合规、审核和保证应该是持续性的。以上程序不应被视作某个时间点上的行为，许多标准和法规正朝着这个模式发展。尤其是在云计算中，供应商和客户的情况往往会更加频繁地进行变化，几乎不会处于静态的情况。
- 云供应商应该：
 - 要清楚地传达他们的审计结果、认证和证明，特别注意：
 - ◆ 评估的范围。
 - ◆ 不同地点和管辖区内所覆盖的特定特征/服务。
 - ◆ 客户如何部署合规的应用程序和云服务。
 - ◆ 任何额外的客户责任和限制。
 - 云供应商必须随时间变化维护其认证/证明并主动沟通任何状态变化。
 - 云供应商应参与持续遵守措施，避免为客户造成任何差距，从而暴露风险。
 - 为客户提供通常需要的合规所需的证据及文件，如客户不能自行收取的管理活动日志。

- 云客户应该：
 - 在部署、迁移或开发云技术之前，明确全部合规义务。
 - 评估提供商的第三方认证和认证，并将其与合规性要求保持一致。
 - 了解评估和认证的范围，包括涵盖的控制和系统特性/服务。
 - 尝试选择具有云计算经验的审核人员，尤其是当准入型审计和认证会被用于客户审计范围的情况下。
 - 确保他们了解供应商提供的合规性证据，并有效地收集和管理这些证据。
 - ◆ 当供应商的证据不充足时，创建和收集自己的证据。
 - 云安全联盟云控制矩阵可以支持提供云供应商的注册表、相关的遵从性要求以及当前的状态。

D5: 信息治理

5.1 介绍

信息安全的主要目标是保护系统和应用程序的基本数据。随着企业向云计算过渡，传统的数据安全方法受到基于云架构的挑战。弹性、多租户、新的物理和逻辑架构和被分离的控制，需要新的数据安全策略。在众多云部署中，用户甚至将数据转移到外部环境甚至公共环境中，这是几年前不可想象的。

在云计算时代管理信息是一项艰巨的挑战，它影响到所有组织，不仅需要新的技术保护，而且需要新的基本治理方法。虽然云计算几乎对信息治理的所有领域都有一些影响，但由于与第三方合作和管理管辖边界的复杂性增加，它特别影响到适用性、隐私和公司策略。

信息/数据治理的定义：

确保数据和信息的使用遵循组织的策略、标准和战略 — 包括监管、合同和商业目标

我们的数据总是服从一系列的要求。一些要求是由其他人附加给我们的，如监管机构、客户和合作伙伴—他们基于我们的风险承受能力或者只是我们想如何管理操作而自定义的。信息治理包括确保我们按照我们的目标和要求处理数据的企业架构和控制。

存储在云中的数据在信息和数据治理需求方面遇到的影响来自很多方面

- **多租户：**当数据存储在与其它不可信的租户共享基础设施的公共云上，多租户提出了复杂的安全需求。即使在私有云环境中，对不同的业务单元共享的基础设施的存储和管理，可能也有不同的管理需求。
- **共享的安全责任：**更大的共享环境带来更大的共享的安全责任。现在数据更可能是由不同的团队甚至组织所有和管理。因此，识别数据的管理者和所有者非常重要。

- 所有权，顾名思义，是关于谁拥有数据的。它并不总是完全清楚的。假如客户提供给你数据，你可能拥有它，或者他们可能仍然合法拥有它，这取决于法律、合同和策略。如果您在公共云提供商托管数据，您应该拥有它，但这可能又取决于合同。
- 保管是指谁是管理数据。如果一个客户向你提供他们的个人信息，同时你没有拥有它的权利，你仅仅是保管者。这意味着你只能以被认可的方式使用它。如果你使用公共云提供商，他们同样成为数据保管者，虽然你也有依赖于自我执行和自我管理实现的适度的保管责任。托管不能转移你的责任。基本上，所有者定义规则（有时是间接地控制）和保管者执行规则。所有者与保管者之间的角色和台词，受云基础设施的影响，特别是在公共云的情况下。

在云中托管客户数据，我们将第三方（云提供商）引入治理模型。

- 管辖边界和数据主权：由于云按定义实现了广泛的网络访问，它增加了在更多地点（司法管辖区）托管数据的机会，并减少了迁移数据的摩擦。一些供应商可能不会让数据的物理位置易于识别，而在某些情况下可能需要额外的控制来限制特定地点的数据。
- 适用性规则和隐私政策：所有这些可能受到云适用的第三方提供者和管辖权变化的组合所影响。例如，您的客户协议可能不允许您共享/使用云提供商上的数据，或者可能有某些安全要求（如加密）。
- 销毁和删除数据：这与云平台的技术能力有关。您能确保根据策略销毁和删除数据了吗？

当迁移到云时，把云作为重新审视信息架构的机会。我们今天的许多信息体系架构是相当破碎的，因为它们在几十年的时间内基于不断变化的技术实现的。迁移到云端创造了一个绿色领域的机会来重新审视如何管理信息并找到改进工作的方法。不要搁置和平移现存的问题。

5.2 概要

数据/信息治理意味着确保使用数据和信息遵循组织策略、标准和战略。这包括监管、合同和商业需求和目标，信息和数据是不同的，但是我们倾向于交替使用它们。信息是有价值的数。为了我们的目的，我们使用这两个术语表示相同的事物，因为这是很常见的。

5.1.1 云信息治理领域

我们将不会覆盖所有的数据治理领域，但是我们将聚焦于托管在云端对数据治理的影响。云计算对数据治理的很多领域产生了影响：

- 信息分级。它经常与适用性有关，并影响云的目标和处理需求。不是每个人都一定有一个数据分级方案，如果你有，您需要因云计算而调整它。
- 信息管理策略。分级和云的关系需要增补，如果你有。他们还应该覆盖不同的 SPI 层，由于发送数据到一个 SaaS 供应商与建设自己的 IaaS 应用程序是非常不同的。你需要确定，什么可以上云？什么产品和服务？有什么安全要求？
- 属地和管辖政策。这些都有非常直接的云含义。任何外包必须符合属地和司法管辖要求。可以理解内部策略能够因云计算而改变，但法律要求是硬性约束。（请参阅法律领域以获取更多关于这方面的信息）确保您理解合同和法律可能产生冲突，您需要与您的法律部门合作，处理控制数据，以确保您最大限度的合规。
- 授权。云计算需要对授权进行最小的更改，但请参见数据安全生命周期以了解云的影响。
- 所有权。您的组织对数据和信息的责任，不会因迁移到云而废止。
- 保管。您的云提供商可能会成为保管者。托管的数据，除了完全加密的，仍然在保管者控制之下。
- 隐私。隐私是监管要求、合同义务和对顾客承诺的总和（例如公开声明）。您需要了解总体需求，并确保信息管理和安全策略一致。
- 合同控制。这是将治理需求扩展到第三方（如云提供商）的法律工具。
- 安全控制。安全控制是执行数据治理的工具。它们在云计算中明显的变化了。请看数据安全安全和加密领域。

5.1.2 数据安全生命周期

虽然信息生命周期管理是一个相当成熟的领域，但它并不能很好地映射安全专业需求。数据安全生命周期不同于信息生命周期。

因管理、顾及安全受众的不同需求。这里只是生命周期的一个概要，完整的版本在 <http://www.securosis.com/blog/data-security-lifecycle-2.0>。它只是一个帮助理解数据安全边界和控制的工具。它不应该被用来作为适用于所有类型数据的一种严格的工具。它是一种从高层次帮助评估数据安全并找到重点的建模工具。

生命周期包括从创造到废弃的六个阶段。虽然它被显示为一个线性的过程，一旦创建，数据可以在两个阶段之间不受限制地转换，并且可能不会经过所有的阶段（例如，不是所有的数据最终都会被销毁）。



创建。创建是新的数字内容的生成，或变更/更新/修改现有的内容。

保存。保存是将数字数据提交给某种存储库的行为，通常与创建几乎同时发生。

使用。数据在某种活动中被查看、处理或以其他方式使用，不包括修改。

共享。信息可以被其他人访问，比如用户之间、客户之间以及合作伙伴之间。

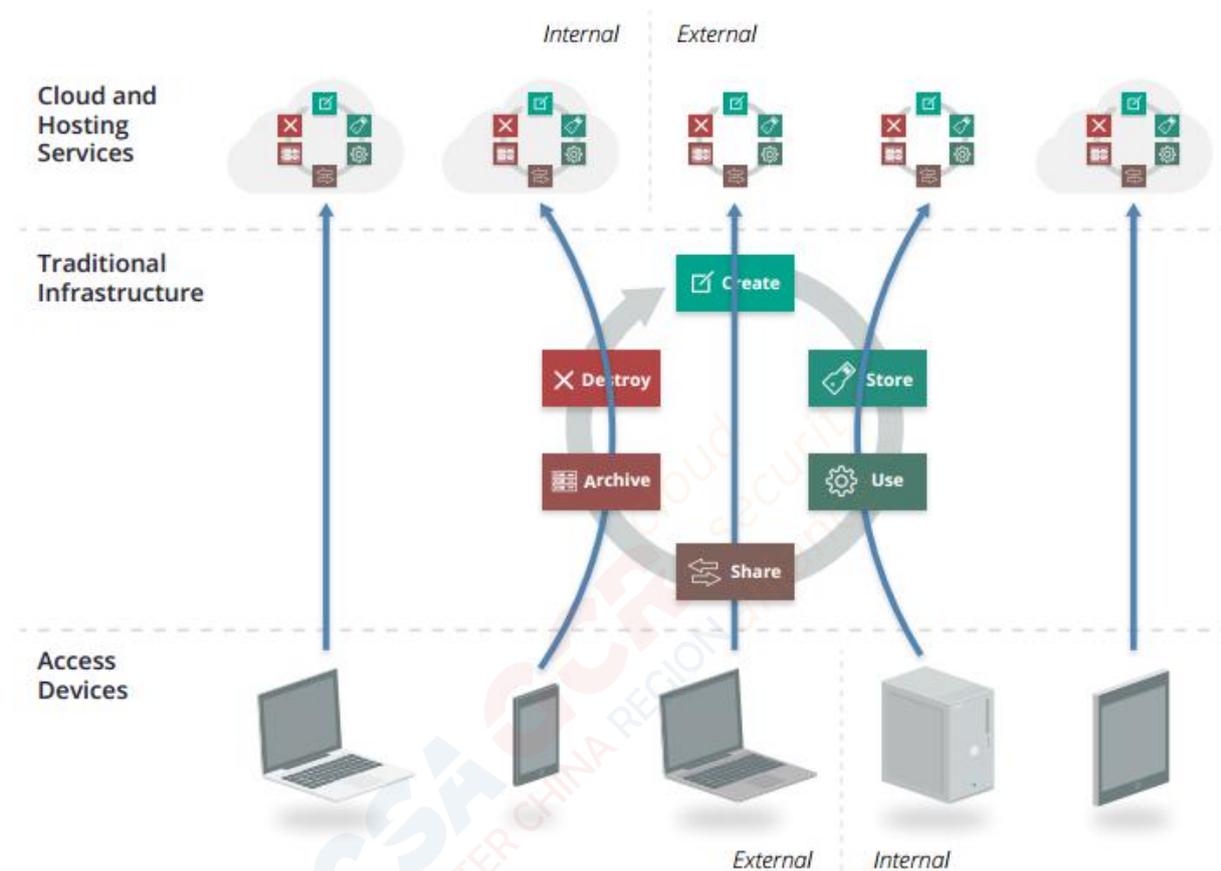
归档。数据离开活跃使用，进入长期存储。

销毁。通过物理或数字的方法，数据被永久性的破坏（例如，基于加密的切碎）。

5.1.2.1 位置和授权

生命周期表示信息传递所处的阶段，但不表明它所在的位置或如何访问它。

位置：可以通过生命周期思想，而不是作为一个单一的、线性的操作来说明，但可以作为一系列更小的周期在不同的操作环境中运行。几乎任何阶段，数据可以在这些环境之间进出。



数据被访问并存储在多个位置，每个都有自己的生命周期。

由于所有潜在的监管、合同和其他管辖问题，理解数据的逻辑和物理位置非常重要。

授权：当用户知道数据在何处以及如何移动时，他们需要知道谁访问它，以及如何访问它。这里有两个因素

- 谁访问了数据？
- 他们怎么访问它的（设备 & 渠道）？

今天的数据被各种不同的设备访问使用。这些设备具有不同的安全特性，可以使用不同的应用

程序或客户端。

5.1.2.1 功能、参与者和控制

下一步确定数据可以实现由设定的参与者（个人或系统）和特定位置确定的功能。

功能：我们可以基于一个设定的基准做三项工作：

- **读**。查看/读取数据，包括创建、复制、文件传输、传播和其他信息交换。
- **过程**。执行一笔数据事务：更新它；在业务处理事务中使用它，等等。
- **存储**。保存数据（在文件、数据库里，等等）。

下表展示生命周期各阶段的功能映射：

	Create	Store	Use	Share	Archive	Destroy
Read	X	X	X	X	X	X
Process	X		X			
Store		X			X	

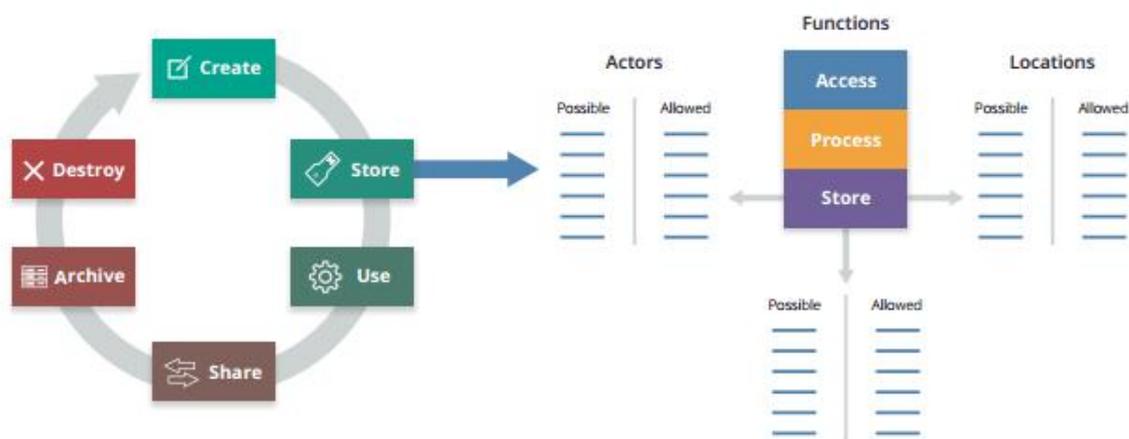
表1—信息生命周期阶段

参与者（个人、应用程序、系统/进程，而不是访问设备）在一个位置完成每一项功能。

控制：限制将一系列可能的行为降级为允许的行为。下表展示了一种用户罗列控制矩阵的可行的方法。

Function		Action		Location	
Possible	Allowed	Possible	Allowed	Possible	Allowed

生命周期功能和控制矩阵



生命周期功能和控制矩阵

5.3 推荐

- 在计划向云过渡之前，确定信息的治理需求。包括法律和监管要求、合同义务和其它公司策略。您的公司策略和标准可能需要更新，以允许第三方处理数据。
- 确保信息治理策略和实践扩展到云端。这将通过合同和安全控制来完成。
- 在需要时，使用数据安全生命周期帮助数据处理和控制进行建模。
- 利用迁移到云的机会，对现有基础设施曾使用的断裂的方法，进行重新思考和重新构建，而不是搁置和平移现有的信息架构，不要养成坏习惯。

D6: 管理平面和业务连续性

6.1 介绍

管理平面是传统基础架构和云计算之间唯一最重大的安全差异。这不是全部元结构（在域 1 中定义），它是连接元结构并完成云的大部分配置工作的界面。

我们通常都会有一个管理平面，我们用它来管理基础架构、平台及应用的工具和接口，但云对资源管理进行了抽象化和集中化。如今早已不再是通过线缆和控制盒来管理数据中心的配置了，而是通过 API 接口和网络控制台。

因此获得了管理平面访问权限就像获得毫无限制地访问您的数据中心的权限一样，除非您已经采取了适当的安全控制措施以限制哪些人可以访问管理平面及可以在上面执行哪些操作。

出于安全的考虑，管理平面将很多我们以前通过不同的系统和工具管理的对象整合到一起管理，然后通过一套授权证书使得它们可以通过互联网被访问。这对安全来说不一定是降低保障，它可能也是有收益的，但它是绝对不同的，在我们需要如何评估和管理安全等方面影响着我们。

集中化也带来安全收益。没有隐匿未知的资源，在任何时候你都知道你拥有什么资源、它们在哪里、如何配置的。这对宽带接入和计量服务的新兴属性。云控制器总是需要知道资源池中资源的进出、分派。

这并不意味着您纳入云管的所有资产都被平等地管理。云控制器无法窥视运行中的服务器里的内容，也无法打开锁定的文件，更无法了解您的特定数据和信息意味着什么。

最后，这是第一域和本指南中讨论的责任共享模式的延伸。云管理平面负责管理资源池中的资产，而云消费者负责配置他们的资产和部署到云端的资产。

- 云提供方负责确保管理平面的安全，并把必要的安全工作开放给云消费者，例如具有管理平面访问权限的某个角色可以在平台上做什么事情的授权颗粒度。
- 云消费者负责正确配置他们所使用的管理平面，保护和管理其授权证书。

6.1.1 云上的业务连续性和容灾

业务连续性/容灾的重要性在云上和非云环境一样重要。 既应考虑与第三方提供方的潜在关联导致的差异（我们在 BC / DR 中通常会处理的事项），还应考虑其他的由于使用共享资源导致的某些固有差异。

云上的业务连续性/容灾主要关注以下三方面：

- 在某一既定的云提供方内确保连续性和恢复。 这些是最优构建云部署以保持运行状态的工具和技术，以应对部署中断或部分云提供程序中断的情况。
- 对云提供方可能出现的中断进行准备和管理。 中断的范围会比较广，小至包括职责内应解决的、可以在单一服务提供方内应对的中断，大至超过了固有的容灾控制措施的能力、会导致云提供方的部分甚至全部服务停掉的大中断。
- 考虑一些选项以实现可移植性，以备您需要对云提供方或平台进行迁移的情形。这个不同寻常的特征是为应对云全部功能丧失的情况，例如云提供方停业或双方有了法律纠纷。

6.1.1.1 失败架构

云平台具有难以置信的弹性，但单一的云资产通常比传统基础设施的弹性更小。这是因为运行在复杂度高的环境中的虚拟化资源的自身脆弱性更大。

这主要适用于计算、网络和存储等资源，因为它们可以采用更底层访问，而且云提供方可以为运行在 IaaS 上的平台和应用程序提供额外的弹性技术。

然而，这意味着云提供方倾向于提供一些能提高弹性的选项，这是传统基础设施在同等成本下无法实现的。 例如您可以把多个物理数据中心的资源分区，把虚拟机部署在分区上并设置可

以自动扩展，以实现高可用。这样您的应用程序可以跨区负载均衡地运行，即便某个分区整个宕掉，您的应用程序仍能正常运行。这在传统的数据中心实现起来相当困难，因为在多个物理隔离区域上跨区部署负载均衡、支持容错自动切换的应用程序的成本是相当高的。

但是，只有您设计了这种云架构，才能利用这些能力才能实现额外的弹性。如果将应用程序全部部署在一个分区内，甚至在单个分区的单个虚拟机上，它的弹性还比不上运行在妥善维护的物理服务器上的弹性。

这就是为什么将现有应用程序以不改变架构、“升层和转换”整体迁移的方式会降低弹性。现有的应用程序很少有采用这种弹性的方式进行架构和部署的，因此不做改变而直接虚拟化或迁移到云上会增加单个故障的发生几率。

IaaS 的管理能力更高，而 SaaS 的管理能力要低得多，就像安全性一样。对于 SaaS，您依靠云提供方保障整个应用程序的服务运行。使用 IaaS，您可以设计您的应用程序的架构以应对故障，将更多责任掌握在手中。如以往一样，PaaS 处在前两者中间 - 一些 PaaS 可能具有可配置的弹性选项，而其他平台完全由提供方掌握。

总体而言，基于风险的方式是关键，因为：

- 不是所有的资产都需要同样级别的连续性
- 在对云提供方可能的中断策划完整的应对方案时不要涵盖所有可感知的损失，会把自己逼疯。查看一下历史的绩效信息。
- 努力设计与传统基础设施相当的 RTO 和 RPO

6.1.1.1 访问管理平面

管理平台通常是通过 API 和 Web 控制台来实现。应用程序接口允许对云的可程式管理。它们是将云的组件保持在一起并实现其编排的粘合剂。由于不是每个人都想通过编程来管理他的云，所以 Web 控制台提供了可视化界面。在许多情况下，Web 控制台只是调用了与您可以直接调用的 API。

云提供方和平台通常还会提供软件开发套件（SDK）和命令行界面（CLI）的方式，使其与 API 的集成更加容易。

- Web 控制台由云提供方管理。可为某组织设置其专用的 Web 控制台（通常使用 DNS 重定向绑定到联盟身份的 DNS 重定向）。例如，当您连接到您的云端文件共享应用程序时，您将在登录后被重定向到您自己的“版本”应用程序。此版本将具有与其相应的自己的域名，且可以更容易地集成联盟身份（例如登录到“your-organization.application.com”，而不是登录到“application.com”）。

如前所述，大多数 Web 控制台提供了用户访问界面调用 API。但是因为平台不同或云提供方的开发过程，有时您会遇到 Web 控制台端特征与 API 调用不匹配的情况。

API 是典型 REST 风格云服务，因为 REST 可以通过 Internet 轻松实现。由于是通过 HTTP/S 运行且可以在各种环境中良好运行，REST API 已经成为 Web 服务的标准。

由于在 REST 中没有单一的身份验证标准，所以可以使用各种身份验证机制。HTTP 请求签名和 OAuth 是最常见的方式；这两者都利用加密技术来验证身份验证请求。

仍然经常会看到在请求中嵌入密码的服务。这不太可靠，暴露认证证书的风险较高。在较早版本或设计不佳的 Web 平台中经常看到首先构建 Web 接口，然后再添加消费者 API。如果您遇到这种情况，如果可能的话您需要使用专门账号来访问 API，以减少认证证书外泄的机会。

6.1.1.1 保障管理平面的安全

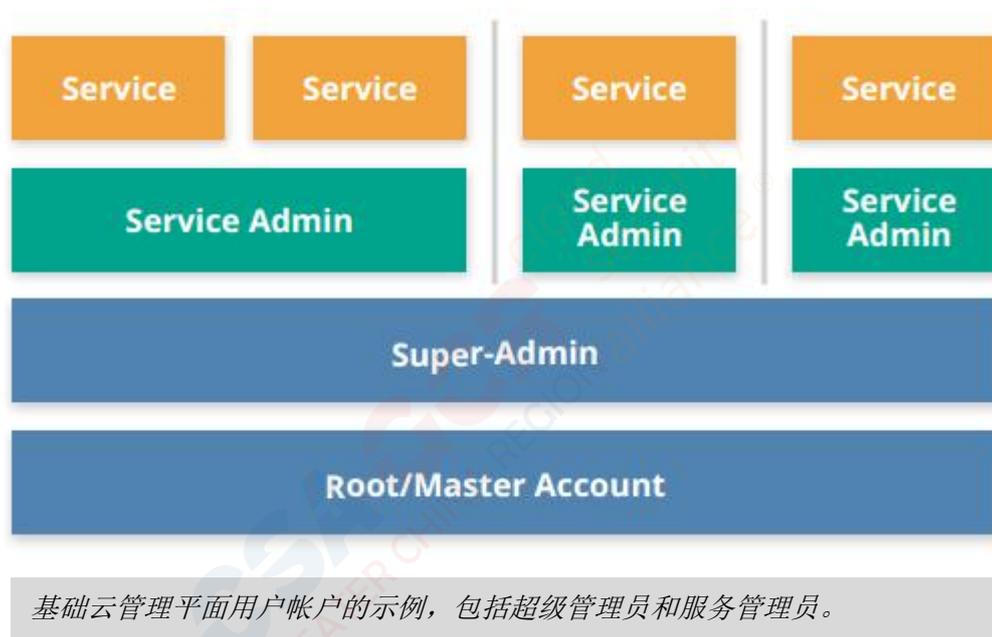
身份识别和访问权限管理（IAM）包括身份识别、身份验证和授权（包括访问权限管理）。这是确定谁可以在您的或提供方的云平台内做什么的管理方式。

特定的选项、配置甚至概念在云提供方和平台之间差异很大。每方都有其自己的实现方式，甚至可能不采用相同的定义，例如“组”和“角色”。

无论是平台或提供方，总会有个账户拥有超级管理员权限，用于管理整个配置。这个账户应该是企业所有（而不是个人所有），严密锁起来，而且几乎从未使用。

与超级管理员帐户分离，您通常还可以创建单个管理员使用的超级管理员帐户。应谨慎使用这些特权；这也应该是一个较小的组织，因为这些帐户中的任意一个的泄露或滥用都可能导致某人能够改变或访问所有的东西。

您的平台或提供方可能会支持只能管理部分服务的较低级别的管理帐户。我们有时称这些“服务管理员”或“日常管理员”。这些帐户被滥用或泄露的话不一定会暴露全部部署，因此更适合日常使用。这有助于区分单个会话，因此允许单个管理员访问多个服务管理员帐户（或角色）的情况并不罕见，这样他们只需用执行某特定操作所需的权限登录即可，而不至于暴露更广的授权。



提供方和消费者都应该始终只允许用户、应用程序和其他管理平面所需的最少特权。

所有特权用户帐户都应使用多因子身份验证（MFA）。如果可能，所有云帐户（甚至个人用户帐户）都应使用 MFA。它是防范广泛攻击的单一最有效的安全控制之一。无论服务模式如何，MFA 对于 SaaS 和 IaaS 而言都同样重要。

（可参阅 IAM 域获取 IAM 的更多信息，以及联邦角色和强身份验证等广泛用于云管理平面的内容。）

6.1.1.1 建立/提供云服务时的管理平面安全

当您负责构建和维护管理平面时，例如部署私有云等情况，将增加您的责任。当您使用云时您只需配置供应商向您开放的管理平面的部分；但是当您是云提供方时，显然需对所有内容负责。

了解实施细则超出了本指南的范围，总体来说在建立和管理安全管理平面上有五方面内容：

- **边界安全：**防止针对管理平面的组件本身（如 Web 和 API 服务器）的攻击。它包括较低级别的网络防御以及针对应用程序攻击的更高级别的防御。
- **客户认证：**使用安全机制授权客户访问管理平面。应使用加密的、文件化的现有标准（如 OAuth 或 HTTP 请求签名）。客户认证应支持 MFA 作为可选项或要求。
- **内部认证和凭证传递：**您的内部员工使用这种机制来连接并访问管理平面中不面向客户的部分。它还包括客户的身份验证和任何内部 API 请求之间的翻译。云提供方应总是强制在云管理认证中使用多因子认证。
- **授权和权利：**此种授权方式可用于客户授权和对内部管理员授权。细颗粒度的授权更能让客户安全地管理自己的用户和管理员。在内部，细颗粒度的授权可以减少管理员帐户泄露的影响或员工滥用的影响。
- **日志，监控和告警：**对于有效的安全性和合规性，强大的日志记录和管理监控至关重要。这既适用于对客户用自己的帐户做了什么的管理，也适用于对员工日常服务管理中的工作。对异常事件发出告警是确保监控是对操作有前瞻指导性的重要安全控制措施，而不仅仅是事后的查看活动而已。理想情况下，云客户应该能够通过 API 或其他机制在平台中访问自己活动的日志，以便与自己的安全日志记录系统进行集成。

6.1.2 业务连续性和容灾

像安全和合规一样，业务连续性和灾难恢复（BC / DR）是双方共担的责任。云提供方应管理其职责内的方面，云客户也应承担云服务如何使用和管理的最终责任。特别是在规划云提供方（或云提供方的部分服务）的中断时尤其如此。

和安全性类似，客户在 IaaS 中拥有更多的控制和责任，SaaS 中的少些，PaaS 中的处在中间水平。

BC / DR 必须采用基于风险的方法。许多业务连续性选项在云中可能成本高昂，也可能不是必需的。这与传统的数据中心没有什么不同，但是在丧失物理控制时要想过度补偿并不罕见。例如，一家主要的 IaaS 供应商停产或改变其整个业务模式的可能性很低，但对于一家小型的风投支持 SaaS 提供方来说，这并不罕见。

- 要求供应商提供一段时期内的宕机时间的统计数据，因为这有助于您的风险决策。
- 不同的供应商能力也有所不同。在供应商流程中应包括相应内容。

6.1.2.1 云提供方内部的业务连续性

当部署资产到云上时，您不能假定云将永存或总是以您期望的方式运行。虽然云提供方可以采用一些机制来增强应用程序的弹性，云可以整体来说更具弹性。但和其他任何一种技术一样，云中断和问题很常见。

一个要花点时间强调的要点是：正如我们在几个地方提到的，将单个资源虚拟化到池中通常会降低这个资源（例如一个虚拟机）的弹性。而从另一方面来看，通过软件抽取资源和管理所有内容可以更灵活地实现弹性功能，如长期存储和跨地域的负载平衡。

这里有很多选项，并不是所有的提供方或平台都是平等创建的，但是您不应想当然地认为只要是云就或多或少地比传统基础设施更具弹性。有时云好些、有时差些。您只有通过风险评估和知道未来将如何使用云服务后，才能知道这些差异是什么。

这就是为什么在迁移到云之前通常要重新构建部署架构的原因。弹性本身，以及确保弹性的基本机制在变化。直接“升层和转换”的迁移方式不太可能解决故障，也不可能通过利用平台和服务的特定能力来实现潜在的改进。

重点是理解和巧妙利用平台的业务连续性/容灾的特性。一旦您决定部署到云中，那么您希望在通过第三方工具添加任何其他功能之前先优化您对包含的业务连续性/容灾功能的使用。

BC / DR 必须考虑整个逻辑栈：

- **元结构**：因为云的配置由软件控制着，所以这些配置应可备份、可恢复。但有时不可行，在 SaaS 中是相当少见，在 IaaS 平台（包括第三方）中经常利用工具的软件定义基础设施的功能来实现它。

软件定义基础架构的方式允许您创建基础架构模板来配置云部署的部分甚至全部方面。然后，这些模板由云平台本机翻译或解释 API 调用，以实现整体协调所有的配置。

这不仅仅包括架构、网络设计或服务配置等，还将包括诸如 IAM 和日志记录等控制措施。

- **基础架构**：如前所述，任何提供方都力争在同样成本下提供功能以支持相对于传统数据中心而言的更高的可用性。但这只有在调整您的架构后才能实现。不做架构调整或重构就直接上云的应用的可用性通常会降低。

确保并了解这些功能的成本模型，特别是在提供方的物理位置/区域实施这些功能，成本可能很高。某些资产和数据必须转换为跨云位置/区域工作，例如用于启动服务器的自定义机器映像。这些资产需包含在计划中。

- **信息架构**：即使实际的存储成本是可管理的，数据同步通常也是跨多点管理中的难题之一。这是由于数据集的大小（与基础架构配置相关）和保持数据在多点间和服务之间的同步。即使在单个存储位置/系统中，这也通常是困难的。

- **应用结构**：应用结构除了包括以上所有内容，还包括代码、消息队列等应用程序资产。当云消费者构建自己的云应用程序时，通常建立在 IaaS 和/或 PaaS 之上，因此弹性和容灾自然地就绑定在那些层上。应用架构包括应用程序中的全部内容。

了解 PaaS 的限制和锁定，以及 PaaS 组件的宕机计划。平台服务包括我们用于在应用程序中手动实现的一系列功能，从身份验证系统到消息队列和通知。现代的应用程序甚至经常将这些来自多个不同云提供方的服务整合起来，创建一个复杂的网络。

与供应商讨论组件/服务的可用性是合理的。例如，来自基础架构提供方的数据库服务可能与其虚拟机托管的性能和可用性是不同的。

当不可能实时切换时，设计您的应用程序以在服务中断时能够按部就班地失效。有很多自动化技术来支持这个。例如，如果您的队列服务宕了，那么应该触发挂起前端，这样消息就不会丢失。

计划内的宕机时间通常是一个选项。您并不总是需要完美的可用性。但如果您打算接受宕机，您应该至少确保您能按部就班地宕机，同时拥有相应的通知计划和应急响应。使用冷备设备和 DNS 重定向技术可以实现这个需求。

“混沌工程”通常用于帮助构建弹性云部署。因为所有的云都是基于 API 的，所以混沌工程使用工具来选择性地降低云的某一部分，以持续测试业务连续性。

这不仅仅是测试环境中做，通常也会在生产环境中完成，并且迫使工程师承担故障而不仅仅将其视为一个可能的事件。通过设计失败的系统，您可以更能承受单个组件的故障。

6.1.2.2 业务连续性应对云提供方损失

通常单个云提供方、或其基础设施（如一个特定地理位置）的主要部分的服务可能会中断。对云提供方的中断进行应对策划通常是很困难，因为一旦选用它就没法做什么改变。有时您可以迁移到其他服务的其他部分。但在一些情况下，内部迁移不是一个可选项，也许你已完全被“禁闭”了。

依据供应商的历史绩效及其内部可用性的能力，接受此风险通常是个合法的选择。

宕机时间可能是另一个可选方式，但这取决于您的恢复时间目标（RTO）。通过 DNS 重定向应该可以启用某些冷备的资源。如果您采用 API 的方式，则完整的事件响应方案中还应包括对 API 调用失败的响应。

如果容灾地点的服务也可能依赖于相同的提供方的话，要谨慎考虑选择其他提供方或服务。如果备份存储提供方和主地点的基础架构提供方是同一家，对您不会有任何好处。

在提供方之间移动数据可能是困难的。但与移动虚拟资源架构、安全控制、日志等内容（可能会在跨平台间不兼容）相比，这相对是容易的。

由于完全依赖提供方，SaaS 通常是提供方中断时的最大忧虑。定期的数据提取和归档可能是您在接受宕机之外的唯一业务连续选项。将数据提取和归档到另一个云服务，特别是 IaaS /

PaaS 上，可能比将其移动到本地/本地存储更好。再次强调，要采用基于风险的方法，其中包括您提供方的真实历史信息。

即使你有数据，你也必须有一个备用的应用程序可供数据迁移。如果您无法使用数据，那么您就没有可行的恢复策略。

测试、测试、再测试。这通常比传统的数据中心容易些，因为您不受物理资源的限制，而只需支付测试期间的某些资产的使用费即可。

6.1.2.1 私有云和云提供方的业务连续性

这完全在由提供方来承担，业务连续/容灾包括所有物理设施的宕机。因为如果云宕了，一切就都宕了，RTO 和 RPO 将是严格的。

如果您正在向他人提供服务，在建立业务连续性计划时要注意合同要求，包括数据留存相关的内容。例如，在容灾情况下数据拷到实行不同司法制度的其他地区可能会违反合同或当地法律。

6.2 建议

- 管理平面（元架构）的安全
 - 确保 API 网关和 Web 控制台的边界安全。
 - 使用强身份验证和多因子认证。
 - 确保对主账户持有人/根帐户授权证书的严格控制，并考虑对它们的访问的双重认证。
 - ◆ 与您的云提供方建立多帐户将有助于细化账户的细粒度、并限制权限范围（IaaS 和 PaaS）。
 - 使用单独的超级管理员和日常管理员帐户，而不是根/主帐户持有人证书。
 - 对元结构访问要坚持使用最低权限帐户。
 - ◆ 这就是为什么要求云提供方将开发和测试帐户分离的原因。
 - 只要可行，尽量使用多因子认证方式。
- 业务连续性

- 容错架构
- 采取基于风险的方法。即使您认为已到了最坏的情况，这时也不意味您在这种情况下应该或需要保持完整的可用性。
- 和云提供方一起设计高可用性。在 IaaS 和 PaaS 中，这通常比传统基础设施中的同等情况更容易、成本效益更高。
 - ◆ 充分利用提供方的特质。
 - ◆ 了解供应商的历史绩效、能力和限制。
 - ◆ 宜始终考虑多地点，但应注意成本决定于可用性要求。
 - 还应确保将镜像介质和资产 ID 转换为在不同位置工作的内容。
 - ◆ 元架构的业务连续性与资产在业务连续性一样重要。
- 准备当云提供方发生中断时可以按部就班宕机的步骤。
 - ◆ 这可以是一些计划,包括与其他云提供方或当前云提供方的其他区域进行协同或执行迁移。
- 对于超高可用性应用程序，在尝试跨区域的业务连续性，然后再考虑跨供应商的业务连续性。
- 云提供方，包括私有云，必须向客户/用户提供最高级别的可用性和相关机制，以供其管理自身可用性的相关方面。

D7: 基础设施安全

7.0 简介

基础设施安全是在云中安全运行的基础。“基础设施”是计算机和网络的粘合剂，一切都建立在其之上。就本指南而言，我们从计算和网络安全开始，其中还包括负载和混合云。虽然存储安全也是基础设施的核心，但是关于存储安全更全面和深入的内容将在第 11 个域：数据安全和加密中涵盖。本知识域还包括私有云计算的基本原理。本部分并不包括传统数据中心安全中的那些已经很好地被现有标准和指南所涵盖的内容。

基础设施安全包括最底层的安全，从物理设施到用户的配置和基础设施组件的实现。这些是云计算中所有其他内容的基本组成部分，包括计算（负载）、网络和存储安全。

CSA 指南的目的是将重点放在与云相关的基础设施安全方面。数据中心安全方面的知识体系和行业标准已经非常强大，云服务提供商和私有云部署可以参考。因此，本指南把重点放在那些广泛的已有材料之上。具体来说，本域讨论了两个方面的问题：底层基础设施方面云的关注点，以及虚拟网络和负载的安全性。

7.1 概述

在云计算中，基础设施有两个大的层面：

- 汇集在一起用来构建云的基础资源。这层是用于构建云资源池的原始的、物理的和逻辑的计算（处理器、内存等）、网络和存储资源。例如，这包括用于创建网络资源池的网络硬件和软件的安全性。
- 由云用户管理的虚拟/抽象基础设施。这层是从资源池中使用的计算、网络和存储资产。例如，由云用户定义和管理的虚拟网络的安全性。

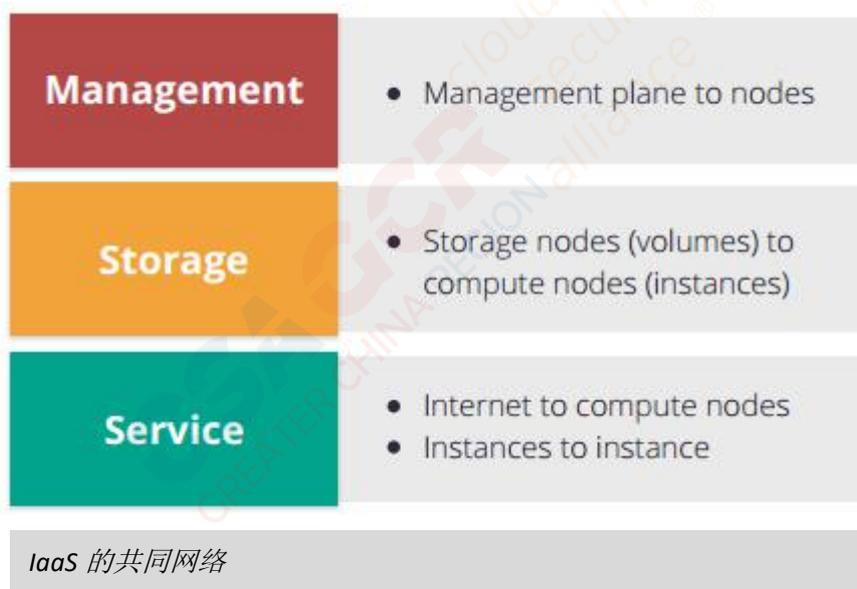
在本域中，信息和建议主要集中在第二层，即云用户的基础设施安全。基础设施安全对于云提供商更为重要，包括那些管理私有云的供应商，这与现有数据中心的安全标准是一致的。

7.2 云网络虚拟化

所有云都利用某种形式的虚拟网络来抽象物理网络并创建网络资源池。通常，云用户从这个池中获取所期望的网络资源，然后这些资源可以在其所使用的虚拟化技术的范围内进行配置。例如，一些云平台只支持特定子网中的 IP 地址分配，而另一些云平台允许云用户具备提供整个 B 类虚拟网络并完全定义子网结构的能力。

如果您是云提供商（包括私有云管理者），出于操作和安全的原因，将云的网络进行物理隔离都是非常重要的。我们通常看到至少有三个不同的网络被隔离到专用硬件上，而相互之间没有功能或业务重叠：

- 虚拟机和互联网之间通信的服务网络为云用户构建了网络资源池。
- 存储网络连接虚拟存储与虚拟机。
- 用于管理和 API 流量的管理网络。



虽然这不是构建私有云网络架构的唯一方法，但它是一个共同的基线，特别是对于不处理大规模云计算的私有云提供商，仍然需要平衡性能和安全性。

目前在云计算中常见的网络虚拟化有两大类：

- VLAN（虚拟局域网）：VLAN 利用现有的网络技术在大多数网络硬件实现。VLAN 在企业网络中是非常普遍的，即使没有云计算。

它们被设计用于单租户网络（企业数据中心），以分离不同的业务单元、功能部门等（如来宾网络）。VLAN 并不适用于大规模虚拟化或安全性，就 VLAN 本身而言，不应该作为一个网络隔离的有效的安全控制手段来考虑。VLAN 也不是物理网络隔离的替代品。

- 软件定义网络（SDN）：在顶部的一个更完整的网络硬件抽象层，SDN 将网络控制平面从数据平面解耦（你可以在维基百科词条阅读更多关于 SDN 原则的资料）。这使得我们可以摆脱传统局域网的局限性，对网络进行抽象。

SDN 有多种实现方式，包括基于标准的和专有的选项。根据实现方案的不同，SDN 可以提供更高的灵活性和隔离性。例如，在同一物理网络上的虚拟网络的多个隔离的重叠 IP 范围。不像标准的 VLAN，如果实施得当，SDN 可提供有效的安全隔离边界。SDN 通常还提供软件定义的任意 IP 范围，使客户能够更好地扩展其现有的网络到云。如果客户需要 10.0.0.0/16 范围的 IP，SDN 可以支持它，而不管底层网络寻址。它甚至可以使用相同的内部网络 IP 地址段支持多个客户。

从表面上看，SDN 对云用户可能像一个普通的网络，但作为一个更完整的抽象将在表面下起着非常不同的作用。SDN 的底层技术和管理将与云用户访问的方式完全不同，并且会有相当多的复杂性。例如，SDN 可以使用包封装，以便虚拟机和其他“标准”资产不需要对其基础网络堆栈进行任何更改。虚拟化堆栈接收来自标准操作系统的数据包，通过虚拟网络接口连接，然后封装这些包以在实际网络中传输它们。虚拟机不需要对兼容虚拟网络接口的 SDN 有任何了解，该虚拟网络接口是由虚拟机管理程序提供的。

7.3 云网络带来的安全变化

对云消费者和提供者来说，由于缺乏对底层物理网络的直接管理，导致了通常的网络实践的改变。最常用的网络安全模式依赖于物理通信路径的控制和安全设备的插入。对于云客户来说，这是不可能的，因为它们只在虚拟层运行。

传统的网络入侵检测系统（NIDS），主机之间的通信都被虚拟的或物理的入侵检测系统所镜像和监视，这些在云环境中都不支持。客户的安全工具需要依赖于内嵌的虚拟装置或安装在实例中的软件代理。这会创建一个阻塞点或增加处理器的开销，所以务必在实施之前确认你真的需要这种水平的监测。一些云提供商可能提供某种级别的内置网络监控（在私有云平台上有更多的选择），但这并不能达到直接嗅探物理网络时那样相同程度的效果。

7.3.1 虚拟设备的挑战

云环境中，由于物理设备不能插入（除云提供商之外），如果仍然需要，则必须用虚拟设备替换它们，如果云网络支持必要的路由。这也带来了与插入虚拟设备用于网络监控一样的关注：

- 虚拟设备因此成为瓶颈，因为它们不能失败，必须拦截所有的流量。
- 虚拟设备可能占用大量资源并增加成本以满足网络性能要求。
- 使用时，虚拟设备应该支持自动缩放以匹配它们保护的资源的弹性。根据产品的不同，如果供应商不支持与自动缩放相兼容的弹性许可证，这可能会导致问题。

虚拟设备还应该考虑到在云中的操作，以及实例在不同地理区域和可用区域之间移动的能力。云网络的变化速度比物理网络要快，需要设计工具来处理这个重要的差异。

云应用程序组件趋向于分布式以提高弹性，而由于自动缩放，虚拟服务器可能寿命更短、产量更高。这将改变安全策略需要如何设计。

- 这导致了安全工具必须能够管理非常高的变化率（例如，使用寿命不到一小时的服务器）。
- IP 地址将比传统网络更快地改变，安全工具必须考虑到。理想情况下，它们应该通过唯一 ID 标识网络上的资产，而不是 IP 地址或网络名称。

资产不太可能使用静态 IP 地址。不同的资产可以在短时间内共享相同的 IP 地址。告警和事件响应生命周期可能必须进行修改，以确保告警在这种动态环境中是可操作的。单个应用程序层中的资产常常位于多个子网上以恢复弹性，从而使基于 IP 的安全策略更加复杂。由于自动缩放，资产也可能是短暂的，存在数小时甚至几分钟。从另一方面看，云架构偏向于每个服务器更少的服务，这提高了您定义限制性防火墙规则的能力。不象单个虚拟机上的一堆服务（比如在物理服务器上，您需要最大限度地硬件中进行资本投资），在虚拟机上运行更小的一组服务，甚至是一

个服务，这是很常见的。

7.3.2 SDN 的安全优势

从积极的方面来说，软件定义的网络支持新类型的安全控制，常常使它成为网络安全整体增益：

- 隔离更容易。这使得不受物理硬件的限制，构建出尽可能多的隔离网络成为可能。例如，如果你使用相同的地址段运行多个网络，由于地址冲突，没有逻辑的方式可以使他们直接通信。SDN 是隔离不同安全上下文的应用程序和服务的好方法。我们将在下面更详细地讨论这个。
- SDN 防火墙（例如，安全组）可用于比基于硬件的防火墙更灵活标准的资产，因为它们不受物理拓扑的限制。（注意，许多类型的软件防火墙是这样的，但与硬件防火墙不同）。SDN 防火墙通常是一组策略，它定义了可以应用于单个资产或资产组的入口和出口规则，而不管网络位置（在给定的虚拟网络中）。例如，您可以创建一组防火墙规则，该规则适用于具有特定标记的任何资产。请记住这一点很难讨论，因为不同的平台使用不同的术语，并有不同的能力来支持这种能力，所以我们试图把事情保持在概念的层次上。
 - 与云平台的编排层相结合，使用传统的硬件或基于主机的方法，可以使用较少的管理开销实现非常动态和粒度化的组合和策略。例如，如果在自动伸缩组中的虚拟机被自动部署在多个子网并实现负载均衡，那么你可以创建一个防火墙规则适用于这些情况，不管他们的子网或 IP 地址。这是安全云网络的一个关键功能，它使用的架构与传统计算截然不同。
 - 默认拒绝通常是起点，您需要从那里打开连接，这与大多数物理网络相反。
 - ◆ 将其视为主机防火墙的粒度，具有更好的网络设备可管理性。主机防火墙有两个问题：首先，在规模上很难管理，如果它们所在的系统受到破坏，它们很容易被改变和失效。另一方面，通过网络防火墙路由所有内部流量，甚至在子网之间的路由是成本高昂的。软件防火墙，如安全组，在系统之外进行管理，但仍然适用于每个系统，不需要额外的硬件成本或复杂的配置。因此，诸如在同一个虚拟子网上隔离每一个虚拟机，这样做是很平常的。
 - ◆ 正如前面提到的，防火墙规则可以基于其他条件，如标签。请注意，虽然有潜

力，但实际能力取决于平台。如果仅仅因为云网络是基于 SDN 的，并不意味着它实际上传递了任何安全利益。

- ◆ 很多网络攻击都是默认被消除的（取决于你的平台），如 ARP 欺骗和其他低级别的漏洞，不仅仅是消除嗅探。这是由于 SDN 固有的特性，以及在数据包上应用更多基于软件的规则和分析。
- ◆ 可以加密包，因为它们是封装的。
- ◆ 与安全组一样，其他路由和网络设计可以是动态的、与云的业务流程层相关联，如桥接虚拟网络或连接到内部的 PaaS 服务。
- ◆ 附加的安全功能可以原生添加。

7.3.3 微分段和软件定义的边界

微分段（有时也被称为 hypersegregation）利用虚拟网络拓扑来运行更多、更小，更加孤立的网络，而不用增加额外的硬件成本，使得以前的那种模式成为的历史。由于整个网络是在软件中定义的，没有许多传统的寻址问题，运行这些多功能的软件定义的环境更为可行。

利用此功能的一个常见的实用示例是在自己的虚拟网络上运行大多数（如果不是全部）应用程序，并且只在需要时连接这些网络。如果攻击者破坏单个系统，这将大大降低爆炸半径。攻击者不能再利用此立足点扩展整个数据中心。

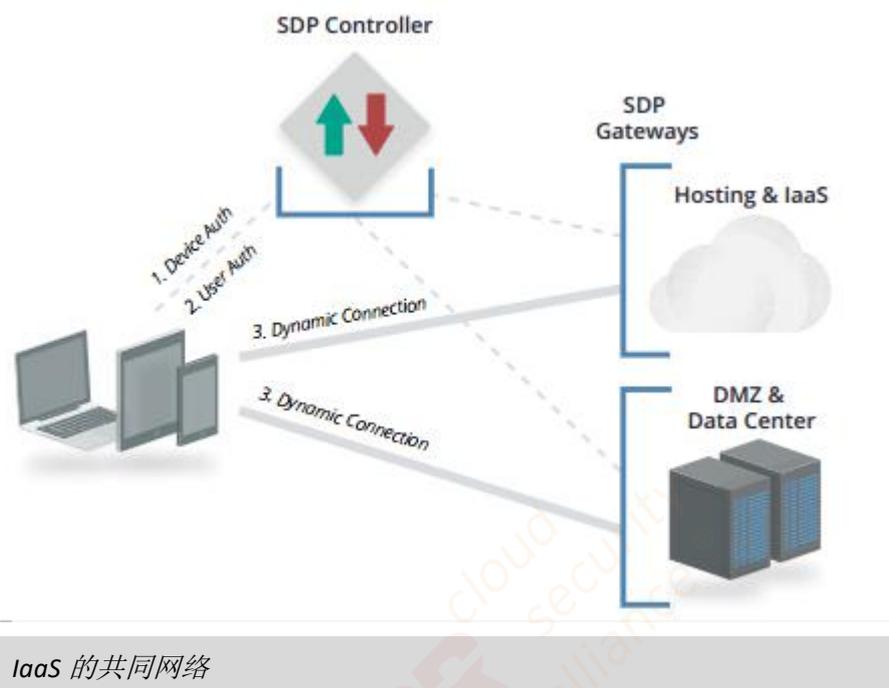
虽然基于软件配置的微分区不会导致固定投资支出的增加，但在管理多个重叠网络和连接时会导致运行费用支出的增加。

云安全联盟软件定义边界（SDP，Software Defined Perimeter）工作组开发了一种模型和规范，它结合了设备和用户身份验证，动态地提供对资源的网络访问和增强安全性。

SDP 包括三个组件：

- 连接资产的 SDP 客户机（例如膝上型电脑）
- SDP 控制器，用于验证和授权 SDP 客户机并配置与 SDP 网关的连接。
- SDP 网关，终止 SDP 客户机网络流量，在与 SDP 控制器通信时强制执行策略。

因此，网络安全决策可以在更广泛的标准范围内进行，而不仅仅是 IP 数据包。特别是结合了 SDN 这个潜在的为不断变化的网络拓扑结构提供了更多灵活性和安全性的技术。



更多关于 SPD 的信息请到 CSA 的以下链接获取：

https://cloudsecurityalliance.org/group/software-defined-perimeter/#_overview

7.3.4 云提供商或私有云的其他注意事项

供应商必须维护物理/传统网络的核心安全性，平台在其之上构建。根网络上的安全故障可能危及所有客户的安全。对任意通信和多租户来说，这种安全性必须是可被管理的，其中一些必须考虑对抗性。

保持多租户环境的分区和隔离是绝对必要的。因此，正确地启用、配置和维护 SDN 安全控件，必然将带来额外的成本开销。虽然看起来 SDN 一旦启动和运行就提供了所需的隔离功能，但为了处理潜在的敌对租户，花费额外的时间来妥善设置一切是非常重要的。我

们并不是说你的用户必然是敌对的，但可以肯定的是，在某个时刻，网络上的某些东西将会被破坏并用于进一步的攻击。

供应商还必须向云用户暴露安全控制措施，以便他们能够正确配置和管理其网络安全性。

最后，云服务提供者负责实现保护环境的边界安全，但最大限度地减少对客户负载的影响。例如，在影响云用户之前，DDOS 和基线 IPS 过滤掉敌对流量。另一个要考虑的是确保当实例被释放回到虚拟机管理程序时，任何潜在的敏感信息是被擦除了的，以确保当磁盘空间被重新分配后信息不能够被另一个客户读取。

7.3.5 混合云的考虑

正如在域 1 中提到的，混合云将企业私有云或数据中心连接到公共云提供商，通常使用专用 WAN 链路或 VPN。理想情况下，混合云将支持任意网络寻址，以帮助无缝扩展云用户的网络。如果云使用与您的内部资产相同的网络地址段，则它实际上无法使用。

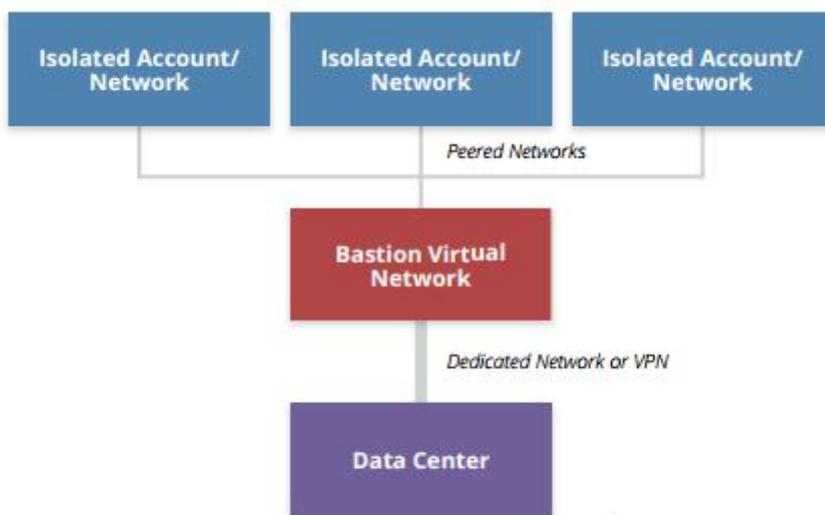
如果私有网络不在同等的安全级别，则混合连接可能会降低云网络的安全性。如果你在数据中心运行一个扁平的网络，与雇员的系统隔离很小，有人可能会危及员工的笔记本电脑，然后用它来扫描整个混合云部署。混合连接不能有效地简化两个网络的安全性。应该通过路由、访问控制，甚至防火墙或两个网络之间的额外网络安全工具来实现隔离。

出于管理和安全方面的原因，通常最好将混合连接最小化。连接多个不同的网络是复杂的，特别是当其中一个网络是软件定义的，另一个由硬件限制的时候。混合连接通常仍然是必要的，但不要假设它们是必需的。由于协调安全控制的需要，它们可能会增加路由复杂度，降低运行多个重叠 IP 段的云网络的能力，并使双方的安全性复杂化。

一种新兴的混合云连接架构是“堡垒”或“中转”虚拟网络：

- 此场景允许您使用单一的混合连接将多个不同的云网络连接到数据中心。云用户为混合连接建立一个专用的虚拟网络，然后通过指定的堡垒网络与任何其他网络进行通信。

- 二级网络通过“堡垒”网络连接到数据中心，但由于它们彼此不相互对等，无法相互交谈，因此可以有效隔离。另外，您可以在堡垒网络部署不同的安全工具、防火墙规则集和访问控制列表等来进一步保护进出混合连接的流量。



更灵活的混合云架构“堡垒”或“传输”网络

7.4 云计算与负载安全

负载作为一个处理单元，可以在虚拟机、容器或者其他的抽象中。负载始终运行在处理器上并占用内存。负载包括多种多样的处理任务，从运行在虚拟机标准操作系统上的传统应用到基于 GPU 或 FPGA 的特殊任务。基本上所有的这些负载任务都能以某些形式在云计算中被支持。

对于云提供商来说，维持每一个运行在硬件栈上的云负载及其硬件的完整性都是非常关键的。不同的硬件栈也支持不同的运行隔离方式和信任链选项。这些选项可以包括运行在主处理器、安全运行环境、加密和密钥管理区域以及其他更多的基于硬件的监视器和监控进程。由于

这些选项的范围广泛并且变化快速，在此时提供预防指导超出了我们的能力，但是从一般意义上来说，安全性的很大部分可能归功于正确选择和利用硬件的这些高级功能。

以下是一些计算抽象类型，每一个都有不同程度的隔离性：

- **虚拟机**：虚拟机是最广为人知的计算抽象形式，所有的 IaaS 提供商都可以提供。从基础镜像创建(或克隆)出来的虚拟机在云计算中一般被称之为实例。虚拟机管理程序(hypervisor)理论上也是底层硬件之上的操作系统。现在的 hypervisor 可以被嵌入到底层硬件功能中并且通常应用在标准服务器上(以及工作站)，在提供高性能运算的同时加强隔离。虚拟机有遭到内存攻击的可能性，但由于软硬件的不断改进使得隔离逐步加强，现在变得越来越难。在现在的 hypervisor 上运行的虚拟机通常受到了有效的安全控制，并且针对虚拟机和安全运行环境的硬件隔离不断增强也将会不断提升这些控制能力。
- **容器**：容器是运行在操作系统上的代码执行环境(目前)，共享并充分利用操作系统的资源。虚拟机是操作系统的一个完整抽象，容器是一个受限区域，它使用操作系统的内核以及操作系统其他能力的运行着被隔离的进程。多个容器可以在同一个虚拟机上运行，也可以完全不使用虚拟机直接在硬件上运行。容器提供了一个受限的代码运行环境，只允许代码访问容器的配置定义的进程和功能。由于容器的平台依赖性，其隔离功能不会与平台产生差异。容器也随着不同的管理系统、底层操作系统和容器技术而快速发展。D8 将会更加深入的讨论容器。
- **基于平台的负载**：基于平台的负载是一个更加复杂的类别，其运行在除虚拟机和容器之外的共享的平台上，如运行在共享数据库平台上的逻辑/过程。假设一个存储过程在一个多租户数据库中运行，或者一项机器学习任务在一个机器学习 PaaS 平台上运行。平台提供商需要对其隔离性和安全性负全部责任，尽管提供商可能公开某些安全选项和控件。
- **无服务器计算**：无服务器是一个广泛的类别，主要是指云用户不需要管理任何底层硬件或虚拟机的场景，只需要访问公开的功能。例如，有一些无服务器平台可以直接执行应用程序代码。但是在后台，这些功能仍然容器、虚拟机或其他专业硬件平台的能力。从安全角

度上看，无服务器只不过是一个包含容器和基于平台负载的组合项，由云提供商管理所有的底层，包括基础的安全功能和控制项。

7.4.1 云对负载安全的改变

所有的处理器和内存几乎都始终要运行多个负载，负载经常来自不同的租户。多个租户很可能共享同一个物理计算节点，不同的物理栈上会有一系列的隔离能力。维持负载的隔离应该是云提供商的首要的责任之一。

有些环境中，专用/私有租用是可能的，但是通常成本更高。使用这种模式只能让指定的负载运行在指定的物理服务器上。将硬件从通用资源池中取出，将会提高公有云用户的使用成本，和使用私有云一样，内部资源的使用率将会降低。

尽管有的平台支持指定负载运行在特定的硬件池或通用位置来提供可用性、合规性和其他需求，但是不管使用哪种部署模型，云用户都很少能够控制负载的物理的运行位置。

7.4.2 不可变负载增强安全性

动态启用基于镜像创建的实例，部署在容器中，可自动扩展，是最佳的工作状态，这些实例可以在其功能不再需要的时候被关闭，并且不会破坏应用程序栈。这是云环境中弹性计算的核心。因此你不再需要为正在运行的负载打补丁或者做其他修改，因为这也不会改变镜像，而且新的实例将会与正在运行且被人工修改过的实例不同步。我们称这些虚拟机是不可变的。

重新配置或修改不可变的实例需要更新底层镜像，然后通过关闭旧的实例并在其位置运行新实例的方式轮流替换。

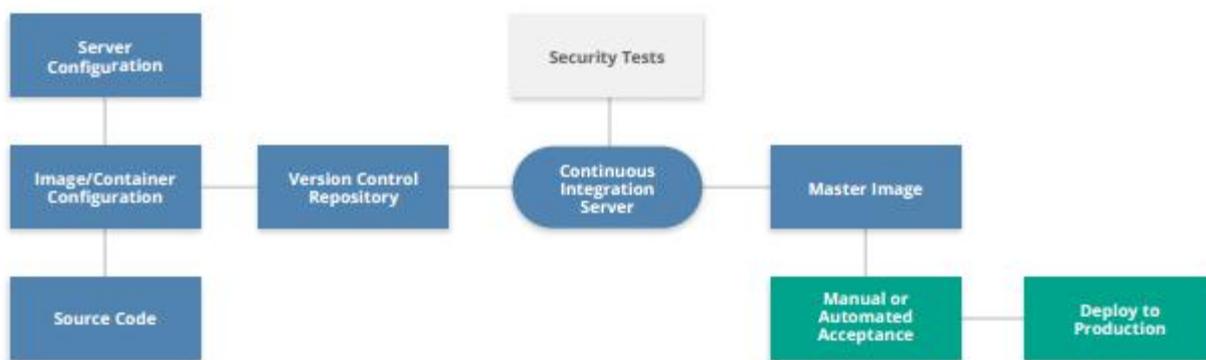
不可变性是有不同程度的。单纯的定义是使用新的实例完全替换正在运行的实例。事实上，有的组织仅使用推送新镜像的方式更新操作系统，仅使用替换部署技术向正在运行的虚拟机中推送代码。虽然从技术上说并不是完全不可变的，但对于实例的更改，这些推送坚持完全使用自动操作，而不再是人工登录系统来进行本地更改。

不可变负载能够给安全性带来显著提升：

- 不用对正在运行的系统打补丁，也不用担心依赖关系、中断的补丁进程等。可以使用新的正式版直接替换。
- 可以也应该禁止远程登录正在运行的负载（如果登录仍然是一个选项）。这是一个操作要求，用于防止修改而导致栈中的实例不一致，这也给安全性带来显著提升。
- 更快地推出更新版本，应用程序必须设计个别节点下线的处理方式（这是所有自动扩展基本原则）。可以更少的遇到修复一个正在运行的系统在复杂性和脆弱性上的限制。即使某些部分崩溃，也可以直接替换掉。
- 由于实例不能更改，禁用服务和应用白名单程序/进程将更容易实现。
- 大多数的安全性测试可以在镜像创建阶段进行管理，从而减少了对运行中的负载进行脆弱性评估的需求，因为在创建过程中负载的特性应该已经是完全已知的。但这并不能取消对生产负载的所有安全测试，这只是一种分流大量测试的方式。

不可变性增加了一些需求：

- 需要一个一致的镜像创建流程和自动化程序来支持部署更新。这些新镜像必须基于补丁描述和恶意软件更新定期生成。
- 安全性测试必须集成到镜像创建和部署过程中，包括源代码测试和漏洞评估（如果使用的是虚拟机和标准容器）。
- 镜像配置需要一些机制，在部署镜像并将其应用在生产的虚拟机之前禁用登录和限制其服务。
- 对于某些负载，可能需要一个进程来启用负载的登录功能，当负载在应用程序栈中不可用时可以用来排除故障。这样可以把负载从群组中提取出来，但允许让负载继续隔离运行。或者（而且通常是首选），发送充分而详细的日志到外部收集器，这样就不再需要登录负载。
- 如果需要在指定的时间创建几十个甚至数百个镜像，将会增加服务目录管理工作的复杂性。



不可变的虚拟机或容器创建镜像的部署流程

7.4.3 云对标准负载安全控制的影响

有些标准负载的控制措施对于云负载来说是不可行的（例如在某些类型的容器中运行防病毒软件）。有些控制措施不是必须的或者是需要进行深度定制来维持其在云计算环境中的有效性。

- 在非基于 VM 的负载中运行代理可能是不可行的，例如在某些运行在“无服务器”供应商管理容器上的负载。
- ”传统”的代理可能对云造成大量性能损耗，具有较低计算需求的轻量级代理允许负载更好的分布和资源更有效的使用。不是为云计算设计的代理假设的底层计算能力可能与云部署设计的不一致。在特定的云项目中，开发人员可能会假设代理运行在一群轻量、单用途的虚拟机上。不适应这种环境的安全代理可能会显著的增加处理开销，并需要更多的虚拟机类型和成本。
- 云环境中运行的代理也需要支持动态的云负载和部署模式，如自动伸缩。它们不能直接（以及在代理或管理系统中）依赖于静态 IP 地址。虽然有的云资产运行在静态地址上，但更常见的是在运行时通过动态分配 IP 地址来实现其弹性。因此代理必须具有发现管理/控制平台的功能，并且通过管理/控制平台确定代理所运行的负载类型和位置。
- 代理的管理平台自身的运行也需要以同样的速度支持自动伸缩和弹性（例如可以支持大规模的动态 IP 寻址、支持在一个小时内让多个负载使用相同的 IP）。传统的工具一般不是以这种速度来设计的，这和我们讨论网络安全以及防火墙是一样的问题。
- 代理不该因为通讯/网络或其他需求增加了受攻击面。诚然，代理在云中有很大的可能

性因为以下原因产生安全风险：

- 运行不可变系统需要更大的权限，而一个代理，就像任何软件一样，会打开额外的攻击面，特别是如果它的配置改变和签名可以被用作攻击向量的话。
 - 即使在云中我们也常常于对少量的个别服务以最小网络端口的方式在特定的虚拟机（或容器）中运行，就像在物理服务器上一样。但有的代理需要打开额外的防火墙端口，因而增加了网络受攻击面。
 - 这不意味着代理始终会引起新的安全风险，但在简单地假设使用代理将会提升安全性之前，需要对收益进行平衡。
- 文件完整性监控是检测正在运行的不可变实例遭到未授权更改的一个有效手段。由于不可变的负载的硬件化特性，因此通常更少需要额外的安全工具。不可变负载相比普通服务器更加固定，并且常常运行一套更小的服务。文件完整性监控也变得更加轻量，由于不可变负载不被改变的特性，文件完整性监控应该具有零误报的优点，能对不可变负载实现良好的安全控制。
 - 仍然使用标准安全控制措施并长期运行的虚拟机可以在网络上进行隔离，并改变其被管理的方式。但将管理工具连接到虚拟机所运行的私有网络子网时可能会遇到困难。即使技术上允许在相同的子网中运行管理工具，但这也会明显的增加成本和管理难度。
 - 由于隔离运行的云负载的抽象化，其通常比运行在物理基础设施上更有弹性。这对于灾难恢复是非常重要的。

7.4.4 负载安全监控和日志的变化

安全日志/监控在云计算中更加复杂：

- 日志中的 IP 地址并不一定反映一个特定的工作流，因为多个虚拟机可能在一段时间内共享相同的 IP 地址，而且一些负载，如容器和无服务器负载可能根本没有可识别的 IP 地址。因此需要在日志中收集一些其他的唯一标识符来确保能够知道日志条目的真实来源。这些唯一标识符需要代表短暂存在的系统，即使负载可能只在很短的时间内有效。
- 由于云具有更快的变化速度，日志也需要在外部更快地被卸载和收集。在自动伸缩组中，不再需要的实例的日志如果没有在云控制器将实例关闭之前被收集，无疑将被丢

失。

- 日志的结构需要考虑云存储和网络消耗。例如，由于额外的存储和额外的网络费用，在公有云中发送实例的所有日志到本地的 SIEM 将产生很高的成本。

7.4.5 脆弱性评估的改变

在云计算中实施脆弱性评估需要考虑架构和合同的限制：

- 云所有者（公有或私有）通常需要评估通知和评估真实的限制范围。这是因为他们可能无法在没有事先预警的前提下从真实攻击中将评估区分出来。
- 默认拒绝网络进一步限制了自动网络评估的潜在效果，就像任何的防火墙一样。为了支持评估除非打开通道或者在实例上使用代理，否则评估只能知道大量的测试被防火墙规则所阻断。
- 不可变负载的评估可以在镜像创建过程中进行。由于这些负载还未投入生产，并且创建过程是自动化的，因此评估可以在更少的网络限制下进行，从而增加评估面。
- 由于渗透测试依然使用与攻击者相同的范围，其受到的影响较小。第 D10 中会更详细地讨论渗透测试。

7.4.6 云存储安全

云存储虽然是基础设施的一部分，但在 D11 会更深入的讨论存储和数据安全。

7.5 建议

- 了解提供商或平台的基础设施安全。
 - 在共享安全模型中，提供者（或私有云平台的维护者）有确保云的物理底层、抽象层和业务流程层安全的责任。
 - 复查合规证书和认证。
 - ◆ 定期检查行业标准和行业特定的合规证书和认证，确保服务提供商遵循云基础设置的最佳实践和规则。

- 网络
 - 优先选用 SDN
 - 在多个虚拟网络和多个云帐号/业务中使用 SDN 功能可以增强网络隔离
 - ◆ 与传统的数据中心相比，使用独立的帐号和虚拟网络有效限制了影响范围
 - 实施默认拒绝策略的云防火墙
 - 基于每一个负载实施云防火墙，而不是基于每一个网络
 - 只要环境允许，建议始终使用云防火墙（安全组）策略限制同一个虚拟子网中负载之间的流量
 - 减少对限制弹性或引起性能瓶颈的虚拟设备的依赖
- 计算/负载
 - 尽量使用不可变负载
 - ◆ 禁用远程访问
 - ◆ 将安全测试集成到镜像创建过程中
 - ◆ 实现文件完整性监控告警
 - ◆ 基于镜像更新的方式打补丁，而不是基于运行的实例
 - ◆ 如有必要使用安全代理，选择适配云环境并且对性能影响最小的
 - 维持长期运行的负载的安全控制，但需要使用云适配的工具
 - 将日志存储到负载之外
 - 了解和遵守云服务提供商的对漏洞评估和渗透测试的规定

D8: 虚拟化和容器

8.0 简介

虚拟化不只是一个创建虚拟机的工具—它是云计算能力的核心技术。我们使用的虚拟化都

是通过计算能力实现，从完整的虚拟机到 Java 虚拟机这样的虚拟可执行环境，以及存储、网络，诸如此类。

云计算基本上构建于资源池之上，而虚拟化技术用于将修正后的基础设施转化为资源池。虚拟化为资源池提供所需抽象，然后用协调器管理。

如上所述，虚拟化涵盖了极其广阔的不同技术；任何时间我们创建抽象，实质上就是在使用虚拟化。对云计算来说，我们倾向于聚焦一些用于创建资源池虚拟化的特定方面，尤其是：

- 计算
- 网络
- 存储
- 容器

上述不是虚拟化仅有的类别，而是和云计算最为相关的内容。

了解虚拟化对安全性的影响是正确构建和实施云安全的基础。资源池提供的虚拟资产看起来就像它们用来替代的物理资产一样，不过这种看法不过是帮助我们更好理解和管理我们所见虚拟资产的工具而已。这也是应用这种现有技术（如操作系统）的有效方式，而无需从头开始完全重写。在这种情况下，这些虚拟资产的工作方式和抽象出它们的资源截然不同。

8.1 概述

最基本的，虚拟化从底层的物理资产中抽取资源。从完整的计算机到网络以及代码，你几乎可以将所有东西用技术手段虚拟化。如引言所述，云计算基本上是基于虚拟化：我们抽取资源以创建资源池。没有虚拟化，就没有云。

许多安全过程被设计出来以期对底层基础设施进行物理控制。尽管云计算不会消失，虚拟化为安全控制增加了两个新的层次：

- 虚拟化技术本身的安全性。例如：保护管理程序。

- 虚拟资产的安全控制。在许多情况下，必须用相应物理设备不同的方式实现。例如，如同第七章所讨论，虚拟防火墙和物理防火墙不同，单纯地物理防火墙抽象道虚拟机可能仍然无法满足部署或安全要求。

云计算中的虚拟化安全依然遵循共享的责任模型。云提供商始终负责保护物理基础设施及虚拟平台本身。同时，在云提供商实现和管理的基础上，云客户负责合理地实施有效的虚拟安全控制并了解潜在风险。例如，决定何时加密虚拟化存储，正确配置虚拟网络及防火墙，或者决定何时使用专用主机与共享主机。

由于许多控件涉及其他云安全领域（如数据安全），因此这一章我们将重点放在具体虚拟化问题上。然而，这条边界线并非总是清晰，大部分云安全控制在本指南的其他章节阐述的更加深入，如第七章（D7）：基础设施安全广泛地集中在虚拟网络和负载上。

8.1.1 与云计算相关的主要虚拟化类别

8.1.1.1 计算

计算虚拟化从底层硬件抽象出代码运行（包含操作系统），而不是直接从硬件运行。代码运行于抽象层之上可以实现更灵活的应用，例如在同一硬件（虚拟机）上运行多个操作系统。这是一个简化，如果你有兴趣了解更多，我们建议对虚拟机管理器和管理程序进一步研究。

计算最常用的是虚拟机，但这正在快速改变，在很大程度上是由于技术改变和容器的采用引起。

容器和某些类型的无服务器基础设施也是抽象计算。这些是和创建代码执行环境不同的抽象，但它不会像虚拟机一样抽象出完整的操作系统。（下面详细介绍了容器）

云提供者责任

云提供商在计算虚拟化中的主要安全责任是强制隔离并维护安全的虚拟化基础设施。

- 隔离确保一个虚拟机/容器中的计算过程或内存对另一个虚拟机/容器不可见。即使在同一个物理硬件上运行进程，我们会据此隔离不同的租户。
- 云提供商还负责保护底层基础设施和虚拟化技术以免外部攻击和内部滥用。这意味着使用经过适当加固和支持补丁程序和最新的管理程序，以便随时间变化更新和保护进程。无法通过云部署修补管理程序，可能导致在新的技术漏洞被发现时创建了一个在基本上不安全的云。

云提供商也要支持云端消费者的虚拟化安全使用。这意味着从镜像（或其他源）创建安全的进程链，通过安全且完整的引导程序运行虚拟机。这确保租户不能际遇通过他们不应该访问的镜像（比如属于其他租户的）启动虚拟机，并且运行的虚拟机（或其他进程）是客户期望运行的虚拟机或进程。

此外，云提供商需要确保可变内存在未许可的监控中是安全的。因为如果是另一个租户、恶意雇员甚至于攻击者能访问运行中的内存，重要的数据可能被暴露。

云消费者责任

同时，云消费者的主要责任是正确实施部署在虚拟环境中的所有安全措施。由于计算虚拟化的主要责任在云提供商，所以客户趋于只拥有虚拟化负载的少数选项。更多的负载保护在第七章会有涵盖。

也就是说，云端消费者可以在安全实施中解决一些虚拟化有关的差异。首先，云端消费者应该利用安全控制管理虚拟基础设施，这将基于云平台而有所不同，通常包括：

- **安全设置**，比如虚拟资源的身份管理。这不是像操作系统登录凭据这样资源内部的身份管理，而是被允许访问云资源管理者的身份管理—例如，停止或更改虚拟机的配置。查阅第六章以获取管理器安全的详细信息。
- **监控和日志**。第七章涵盖了负载的监控和日志，包含如何处理来自容器虚拟器的系统日志，但云平台可能在虚拟化级别提供额外的日志和监控。这可以包含虚拟机状态、管理事件、性能等。

- **镜像资产管理。** 云计算部署基于主镜像—无论是虚拟机、容器还是其他代码—然后在云上运行。相比于传统计算主镜像，这往往是高度自动化并且导致产生更多基于资产的镜像。管理这些—包含哪些满足安全要求，部署在哪里，以及谁可以访问—是一个重要的安全责任。
- **使用专用主机。** 如果有的话，基于资源安全上下文使用专用主机。在某些情况下，你可以指定资产运行在你专属的硬件之上（成本更高），即使在多租户的云上。

其次，云消费者还对虚拟化资源的安全控制负责。

- 这包含负载的所有标准化安全性，无论是虚拟主机、容器还是应用代码。这些都被安全标准最佳实践和第七章（D7）中的附加指导所涵盖。
- 值得一提的是确保只有安全的配置文件被部署（例如修补的、更新的虚拟镜像）。由于云计算的自动化，很容易部署上那些没有加固或者进行适当安全设定的旧配置。

其他常见计算安全性问题包括：

- 虚拟资源更加短暂并且快速变化。任何相应的安全措施（例如监控），必须跟上这个速度。再次强调，这些细节在第七章（D7）有更深入的介绍。
- 主机级监控/日志可能不适用，尤其是无服务器部署。可能需要实施备选日志方法。例如，在无服务器部署中，不太可能查看底层平台的系统日志，需要通过编写更强大的应用日志代码来解决。

8.1.2 网络

有多种虚拟网络，从基本的虚拟局域网（VLANs）到完全软件定义网络（SDN）。作为云基础设施安全的核心，在本章和第七章都会有涵盖。

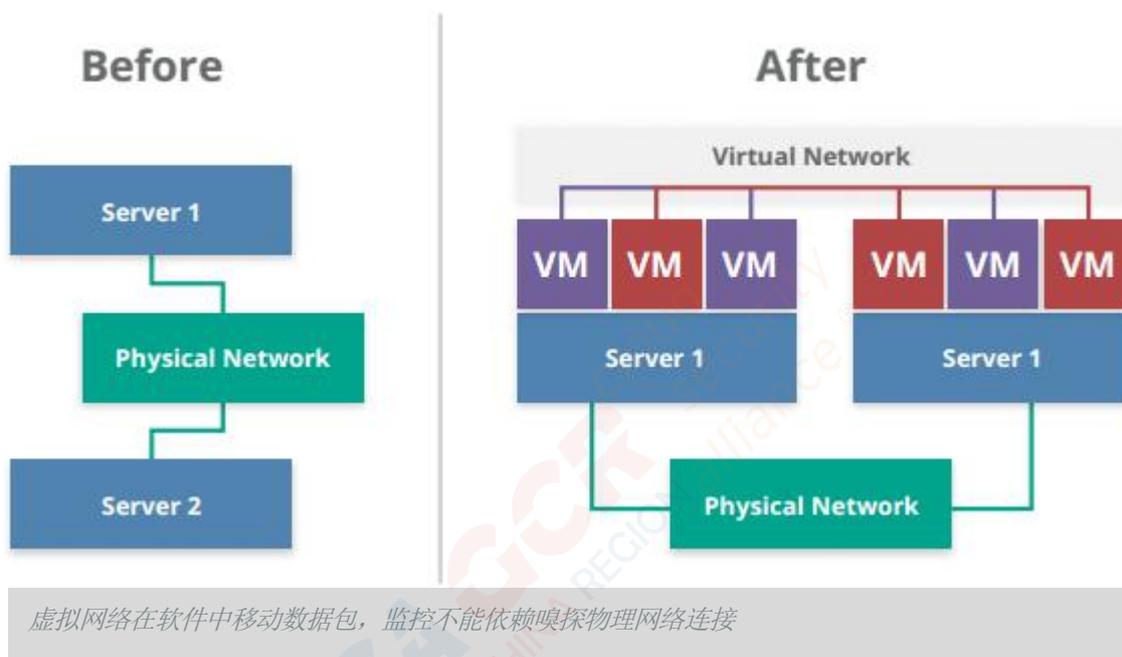
回顾一下，当今的大多数云计算使用 SDN 虚拟化网络。（VLANs 通常不适合云部署，因为对多租户缺乏重要的隔离能力。

SDN 从底层物理设施中抽象出网络管理器，消除了许多典型的网络约束。例如，即使是地址范围完全重叠的虚拟网络，你也可以通过相同的硬件覆盖多个虚拟网络，并将流量分离和隔离。SDN 也可以用软件设置和 API 调用定义，支持编排性和敏捷性。

虚拟网络和物理网络完全不同。他们在物理网络上运行，但抽象允许对影响很多安全进程和技术的网络行为进行深度修改。

8.1.2.1 监控和过滤

特别的是，由于数据包在虚拟网络移动方式差异，监控和过滤（包含防火墙）变化很大。资源可以在物理服务器上交互，而不用通过物理网络传输。例如，如果两个虚拟机位于相同的物理机器上，则没有理由将机箱内的网络流量路由到网络之上。因此，他们可以直接通讯，并且在网络上（或附加在路由器/交换机硬件）的监控和过滤工具永远看不到流量。



作为补偿，你可以将流量路由到同一硬件（包含网络安全产品的虚拟机版本）上的虚拟网络监控或过滤工具。你也可以将流量桥接到网络，或路由到相同虚拟网络的网络设施上。这些方法每一种都有缺点，因为它们产生瓶颈和低效能路由。

云平台/提供商可能不支持直接访问网络监控。由于复杂性和成本，公有云提供商很少允许客户进行全面数据包网络监控。因此，你无法设想除非你自己在主机中或通过虚拟设备收集，将无法访问原始数据包数据。

特别是公有云中，一些云服务间的通讯会发生在提供商的网络中。客户监控和过滤该流量是不可能的（并且会为提供商增加安全风险）。例如，如果将无服务器的应用连接到云提供商的

存储对象、数据库平台、消息队列或其他 PaaS 产品，则此流量会在服务商网络运行，而不一定在客户管理的虚拟网络中。随着我们走出简单的基础设施虚拟化，客户管理网络的概念开始消失。

然而，所有现代云平台提供内置防火墙，可能比相应的物理防火墙更有优势。这些软件防火墙可能在 SDN 或管理程序中运行。它们通常提供比现代专用下一代防火墙更少的功能，但由于云提供商提供的其他固有安全性，这些功能并非总是必需。

8.1.2.2 管理基础设施

云计算的虚拟网络始终支持远程管理，因此，保护管理器/元结构至关重要。有时，可以通过少量 API 调用或者 Web 控制台的几次点击创建和销毁整个复杂的网络。

云提供商责任

云提供商主要负责建立安全的网络基础设施并正确配置。隔离和独立网络流量，以防止租户访问其他用户的流量，这是绝对最高优先级的安全性。这是任何多租户网络最基础的安全控制。

云提供商应该禁用数据包嗅探或其他会在租户间暴露数据或配置的元数据泄露。即使租户自己的虚拟网络中，跟非虚拟网络常用技术一样，数据包嗅探也应该禁用以削弱攻击者破坏单个节点进而监控网络的能力。标签或其他 SDN 级元数据不能暴露在管理器之外，否则被攻陷的主机可能被用于跨越 SDN 本身。

所有虚拟网络都应该为云用户启用内置防火墙功能，而不用主机防火墙或外部产品。云提供商也有责任检测并阻止来自底层物理网络和虚拟平台的攻击。这包含云本身的周边安全。

云用户责任

云消费者主要负责合理配置虚拟网络的部署，尤其是虚拟防火墙。

网络架构可以在虚拟网络安全中发挥更大的作用，因为我们不受物理连接和路由的限制。由于虚拟网络是软件结构，多个独立的虚拟网络可以提供传统物理网络不能做到的广泛的区域隔离优势。你可以在各自虚拟网络中运行应用程序栈，这样在恶意角色获得切入点时能明显降低被攻击面。物理网络上对应的的架构成本十分高昂。

可以使用软件模板在一些云平台定义不可变网络，这能帮助实施已知很好的配置。可以用模板定义所有已知良好的网络状态，而不用手工设置所有配置。除了具有安全基线创建多个网络的能力外，还能用于检测并在某些情况下恢复与正常状态的偏差。

再次强调，云消费者负责管理器暴露控制正确权限管理及配置。当虚拟防火墙和/或监控不满足安全需求时，云消费者可能需要用虚拟安全设备或主机安全代理进行补偿。这属于云基础设施安全并在第七章有深入介绍。

8.1.2.3 云覆盖网络

云覆盖网络是跨越多个“基础”网络创建网络的一种特殊 WAN 虚拟化技术。例如，覆盖网络可能跨越物理和云位置或多个云网络，甚至可能在不同的云提供商。完整的讨论超出本指南的范围，核心安全建议也是如此。

8.1.3 存储

存储虚拟化已经在大多数组织中很常见。SAN 和 NAS 都是存储虚拟化的常见形式—存储安全性在第 11 章有更详细的讨论。

大多数虚拟化存储是可靠的，并且在不同的地方保存了多个数据副本，因此驱动器故障不太可能导致数据丢失。加密这些驱动器减少了驱动器交换（一种很常见的行为）带来数据暴露的担忧。

然而，这种加密不能保护任何虚拟层中的数据；只能保护物理存储中的数据。根据存储类型，云提供商可能（或反而）在虚拟层加密数据，但这样无法保护客户数据免受云提供商的影响。因此，应使用第 11 章的建议提供任意额外保护。

8.1.4 容器

容器是高度可移植代码执行环境。为了简化，虚拟机是具有独立内核的完整操作系统，容器是虚拟执行环境，具有独立的用户空间，但使用共享内核。完整的讨论超出了本指南范围，可以通过维基百科获得更多软件容器信息。

容器可以直接构建于物理机器之上，也可以在虚拟机运行。当前实现依赖于已有内核/操作系统，这也是为什么即使管理程序不支持嵌套虚拟化，容器也可以在虚拟机运行。（软件容器依赖于完全不同的管理器技术）

软件容器系统总是包含三个关键组件：

- 容器执行环境。
- 自动协调及调度控制器（可以是多个工具集合）。
- 容器镜像或代码的可执行仓库。
- 这些都是运行东西的地方，运行的东西以及管理系统将他们结合在一起。

不拘泥受限于技术平台，容器安全性包含：

- 确保底层物理基础设施（计算，网络，存储）安全性。这和其他形式的虚拟化没什么区别，但它延伸到容器运行环境所在的底层操作系统。
- 确保管理器安全性，这种情况下，它是协调者和调度者。
- 妥善保护镜像仓库。镜像库应该位于经过适当访问控制配置的安全位置。这既是防止容器镜像和定义文件的丢失或篡改，也是防止篡改文件导致敏感数据泄露。容器如此容易运行，以至于镜像只能被部署在正确安全上下文的环境中也很重要。
- 将安全性构建到容器内运行的任务/代码中。仍然可能在容器内运行易受攻击的软件，在某些情况写，这可能暴露来自其他容器的操作系统或数据。例如，可以配置一些容器不仅允许访问文件系统上的容器数据，也可以根文件系统。也有可能允许了过多的

网络访问。这些都是特定于特殊容器平台，因此需要安全地配置容器环境和镜像/容器本身。

容器快速发展，使得安全性的某些方面复杂化，但并不表示容器是不安全的。

容器不一定提供完整的安全性隔离，但一定提供任务隔离。也就是说，虚拟机通常提供安全性隔离。因此你可以将同等安全性上下文的任务放在相同的物理或虚拟主机容器，以提供更大的安全性隔离。

根据你选用的产品不同，容器管理系统和镜像仓库也具有不同安全功能。安全部门需要学习和理解它们要支持的产品功能。产品最少要支持基于角色的访问控制和强大的身份认证。还应该支持安全配置，例如文件系统，进程和网络访问隔离。

对容器安全的深度理解有赖于深度理解操作系统内部结构，例如名字空间、网络端口映射、内存和存储访问。

不同的主机操作系统和容器技术提供不同的安全功能。该评估结论可以适用于任意容器平台选型。

一个要保护的关键区域就是，镜像/任务/代码被允许的特定执行环境。具有适当容器管理和调度的安全仓库将实现这一点。

8.3 建议

- 云提供商要：
 - 永久地保护用于虚拟化的任意底层物理设施。
 - 聚焦于确保租户间的安全隔离。
 - 在虚拟化层提供充分的安全功能，以使云消费者合理地保护其资产。
 - 有力地保护物理基础设施和虚拟化平台，使之避免被攻击或内部妥协。
 - 使用默认安全配置实现所有客户管理虚拟化特性。

- 具体优先事项:
 - ◆ 计算
 - 使用安全管理程序并实现管理补丁进程，使之保持最新。
 - 配置管理程序以隔离虚拟主机。
 - 实现内部进程和技术安全性控制，以免管理员/非租户访问到运行中的虚拟机或可变内存。
 - ◆ 网络
 - 实现必要的周边安全防护，以免底层网络受到攻击，并尽可能在物理层和虚拟网络层检测和防护攻击。虚拟网络层不能直接自我保护。
 - 即使这些网络被相同消费者控制，也要确保虚拟网络的隔离性。
 - 除非消费者有意连接独立的虚拟网络。
 - 实施内部安全控制和策略，以免消费者网络被篡改和未经允许或合约之外的流量监控。
 - ◆ 存储
 - 如果底层存储没有在其他层级进行加密，则加密所有底层存储，以免驱动器更换时数据泄露。
 - 从数据管理功能隔离加密，以免客户数据未经批准被访问。
- 云消费者应该:
 - 确保他们理解云提供商提供的功能及所有安全漏洞。
 - 根据云提供商和其他行业最佳实践合理地配置虚拟化服务。
 - ◆ 大部分基本的虚拟化安全依赖于云提供商，这就是为什么大多数针对云消费者的安全建议涵盖在本指南的其他章节。
 - 对于容器:
 - ◆ 了解已选容器平台和底层操作系统的安全隔离功能，然后选择合适的配置。
 - ◆ 使用物理或虚拟主机在同一物理或虚拟主机提供相同的安全性上下文的容器隔离和容器组。
 - ◆ 确保只能部署批准的、已知且可靠的容器镜像或代码。
 - ◆ 适当地保护容器协调器/管理程序及调度者软件栈。
 - ◆ 为所有容器和管理程序仓库实现适当的基于角色的访问控制，以及强大的认证功能。

D9: 事件响应

9.0 介绍

事件响应（IR - Incident Response，下同）在任何信息安全计划中都是十分关键的一方面。预防性安全措施已经证明无法完全消除关键数据被破坏的可能性。大多数组织都已经有一些事件响应计划来管理他们将如何调查安全攻击，但由于云计算在获取司法数据和政府监管方面存在明显的差异，组织必须考虑在云计算中他们的事件响应流程如何改变。

这部分旨在识别由云计算独有特征产生的事件响应的差异。在事件响应生命周期准备阶段制定事件响应计划和进行其他活动时，安全行业人员可以将此作为参考。这部分根据被普遍采用的美国国家标准与技术研究所《计算机安全事件处理指南》（NIST 800-61rev2 08/2012）[1]中所描述的事件响应生命周期进行组织。其他国际事件响应的标准框架包括《ISO/IEC 27035 信息技术—安全技术—安全事件管理》和欧洲网络与信息安全局(ENISA)的《事件响应与网络危机合作策略》。

在描述了 NIST 800-61rev2 规定的事件响应生命周期，每个后续部分分别讨论了生命周期的一个阶段，并探讨了在云环境中事件响应人员需要关注的地方。

9.1 概述

9.1.1 事件响应生命周期

事件响应周期在 NIST 800-61rev2 文档中有明确的定义。它包括以下阶段和主要活动：



事件响应生命周期

- **准备：“建立事件响应能力，使组织对事件响应作好充分准备”。**
 - 处理事件的流程。
 - 通讯和设施的处理人员。
 - 事件分析硬件和软件。
 - 内部文档及数据（端口列表、资产清单、网络拓扑图、当前网络流量基线）。
 - 确定相关培训。
 - 评估基础设施（通过主动扫描和网络监控，漏洞评估和开展风险评估）。
 - 订阅第三方威胁情报服务。
- **检测与分析**
 - 警报（端点保护、网络安全监控、主机监控、帐号创建、特权提升、其他入侵指标、SIEM、安全分析（基线和异常检测）和用户行为分析）。
 - 验证警报信息（减少误报）和升级。
 - 分析事件的范围。
 - 分配一位事件经理（事件负责人），协调进一步行动。
 - 指定一位人员，向高级管理层传达事件遏制和恢复状态。
 - 建立攻击时间表。
 - 分析潜在数据丢失的程度。
 - 通知和协调活动。
- **遏制、根除和恢复**
 - 遏制：使系统脱机。权衡数据丢失与服务可用性。确保系统在检测到时不会自毁。
 - 消除与恢复：清理受影响的设备并将系统恢复正常操作。确认系统运行恢复正常，实

施措施以防止类似事件。

- 记录事件和收集证据（证据保管链）。

- **总结**

- 哪些方面可以做得更好？能否更快地发现攻击？有什么额外的数据有助于更快地隔离攻击？事件响应流程需要改进吗？如果需要，如何改进？

9.1.2 云计算如何影响事件响应

在云部署中，事件响应生命周期的每个阶段都会受到不同程度的影响。有些阶段与需要和第三方协调的外包环境中的事件响应类似。其他差异则与云的抽象和自动化特性有关。

9.1.2.1 准备

当准备云事件响应时，有一些主要考虑因素：

- **SLA 和治理：**使用公有云或托管提供商的任何事件都需要了解服务水平协议（SLA），并可能需要与云提供商协调。请记住，根据您与提供商的关系，您可能没有直接的提供商联络点，并可能会受限于通过标准支持提供的任何服务内容。通过在第三方数据中心定制私有云与通过网站注册并点击许可协议获取 SaaS 应用程序建立的关系有很大的区别。

关键问题包括：

- 您的组织做什么业务？云服务提供商（CSP）负责什么？谁是联络点？预期的响应时间是多少？事件升级程序是怎样的？您是否有带外通信方式（如果网络受到影响）？交接工作如何开展？您将访问什么数据？

如果可能，必须与云服务提供商对事件响应流程进行联合测试。验证事件响应流程升级程序和角色/责任是否清晰明确。确保当云服务提供商检测到事件时，有联系人通知您，以及这些通知被集成到您的流程中。对于通过点击注册购买的服务，通知将可能会发送到您的注册电子邮箱；这些应由企业控制并连续监测。确保为您的云服务提供商指定联系人，包括带外通信方式并对其进行测试。

- IaaS / PaaS 与 SaaS: 在多租户环境中, 如何提供您云中的特定数据进行调查? 对于每个主要服务, 您应该了解并记录对事件响应有用的数据和日志。不要假设您可以在事件之后联系提供商收集通常不可获取的数据。

“云应急工具包”: 这些是在远程位置进行调查所需的工具 (正如基于云的资源)。例如, 您有从云平台收集日志和元数据的工具吗? 您能解释信息吗? 您如何获取运行虚拟机的镜像以及您可以访问哪种数据: 磁盘存储或易失性存储器?

- 构建能够使检测、调查和响应 (遏制和可恢复性) 更快速的云环境架构。这意味着确保您具有正确的配置和架构, 可支持事件响应:
- 启用各种工具手段, 例如云端 API 日志, 并确保日志存储在安全的地方, 以便在发生事件时可提供给调查人员。
- 利用隔离措施确保攻击不会传播并影响整个应用程序。
- 尽可能使用不可变 (同一配置的) 服务器。如果检测到问题, 将负载 (业务) 从受影响的设备迁移到已知良好状态的新实例。同时, 也需要更多关注文件完整性监控和配置管理。
- 实施应用程序堆栈映射图, 以了解数据所存储的位置, 以便在监视和数据捕获时考虑到地理差异。
- 开展威胁建模和桌面演练非常有用, 可确定云堆栈中针对不同组件的不同类型攻击的最有效的遏制措施。
- 包括对 IaaS / PaaS / SaaS 事件响应的差异。

9.1.2.2 检测与分析

在云环境中的检测和分析可能看起来几乎相同 (对于 IaaS) 和完全不同 (对于 SaaS)。无论在哪种情况下, 监控范围都必须覆盖云管理平面 (整个云平台的资产), 而不仅仅是已部署的资产。

您可以利用云内监控和警报启动自动化事件响应工作流程, 以加快事件响应过程。一些云服务提供商在云平台中提供这些功能, 也有一些第三方监控工具可以选择使用。这些可能不是专门用于安全的: 许多云平台 (IaaS, 可能也有 PaaS) 都会出于性能和操作原因而公开各种实时和准实时的监控指标。在安全上, 也可以利用这些来实现安全需求。

云平台还提供各种日志, 这些日志有时可以整合到现有的安全操作/监控中。这些日志可能

包括操作日志和 API 调用或管理活动的完整日志。请记住，这些并不适用于所有提供商；与 SaaS 相比，通常 IaaS 和 PaaS 会提供更多。当日志源不可用时，您可以使用云端控制台来识别环境/配置变更情况。

事件响应中，云事件的数据源可能与传统计算的有所不同。也存在很多重叠的地方，例如系统日志，但是在如何收集数据以及新来源方面（例如日志源来源于云管理平面）存在差异。

如上所述，云平台日志可能是一个选项，但它们不是普遍可用的。理想情况下，它们应该显示所有管理平面活动。了解记录的内容和可能影响事件分析的差距很重要。是否记录所有管理活动？是否包括自动化系统活动（如自动扩展）或云提供商管理活动？在发生严重事件的情况下，提供商可能会有其他通常不会向客户提供的日志。

收集信息的一个挑战可能是有限的网络可视化程度。来自云提供商的网络日志通常是流水记录，而不是捕获的完整原始数据包。

在有差距的地方您可以为技术栈提供自己的日志记录。这可以在实例、容器和应用程序代码中有效运用，以获得对于调查很重要的遥测数据。特别注意在 PaaS 和无服务器应用架构，您可能需要添加自定义应用程序级日志记录。

外部威胁情报也可能与本地事件响应一样有用，以帮助确定攻击的指标并获取对手信息。需要注意的是，当云服务提供商提供的信息面临证据保管链问题时，这将是潜在的挑战。在这一点上还没有可靠的先例。

除了了解数据来源的变化之外，取证和调查支持也需要作出改变。

始终需要关注云服务提供商可以提供什么以及所提供的是否符合证据保管链要求。并不是每一起事件都会导致法律诉讼，但与您的法律团队合作是十分重要的，以了解法律界线以及在何处会产生证据保管链的问题。

由于云环境的动态性和更高速的特点，自动运行很多取证/调查流程有更大的必要性。例如，由于正常的自动扩展活动或管理员决定终止运行需要调查的虚拟机，证据可能会丢失。您可以自动执行一些任务，包括：

- 虚拟机的存储快照。
- 在警报时捕获任何元数据，以便根据基础架构当时的状态进行分析。
- 如果您的提供商支持，可以“暂停”虚拟机，这将保存易失性存储器状态。

您还可以利用云平台的功能来确定潜在的受攻击的程度：

- 分析网络流量来检查网络隔离是否持续有效。您还可以使用 API 调用快速复制网络和虚拟防火墙规则状态，这可以让您在事件发生时准确了解整个技术栈。
- 检查配置数据以检查其他类似实例是否可能受到同样的攻击。
- 查看数据访问日志（对于基于云的存储，如有）和管理平面日志，以查看事件是否影响或跨越云平台。
- 无服务器和基于 PaaS 的架构将需要额外的跨云平台的相关性和任何自身应用程序日志。

9.1.2.3 遏制、根除和恢复

始终确保云管理平面/元结构远离攻击者。这通常将涉及调用破坏程序来访问云帐户的根或主认证凭证，确保攻击者活动未对于较低级别的管理员帐户隐藏。记住：如果攻击者还处于管理平面，则不能遏制攻击。对云资产的攻击（如虚拟机）有时可能会泄露管理平面的凭据，然后将其用于范围更大、更严重的攻击。

在这一阶段的响应中，云环境通常会提供更多的灵活方案，特别是对于 IaaS。软件定义的基础架构允许您在干净的环境中快速重建业务，而对于比较孤立的攻击，固有的云特性（例如自动扩展组，用于更改虚拟网络或机器配置的 API 调用以及快照）可以加速隔离、根除和恢复过程。例如，在许多平台上，您可以通过将实例移出自动扩展组、通过虚拟防火墙将其隔离、并将其替换以即时隔离虚拟机。

这也意味着，由于新的基础设施/实例是干净的，因此在确定其攻击原理和破坏范围之前，不必立即“消除”攻击者。相反，你可以简单地隔离它们。但是，您仍然需要确保漏洞利用路径已关闭，不能用于渗透其他生产资产。如果担心管理平面被入侵，请确保确认新的基础设施/

应用程序的模板或配置尚未被入侵。

也就是说，这些功能并非总是普遍的：对于 SaaS 和一些 PaaS 可能非常有限，因此需要更多地依靠云提供商。

9.1.2.4 总结

如对于任何攻击一样，应与内部响应团队和提供商合作，以确定响应计划哪些工作有效和哪些无效，然后确定任何需要改进的地方。应特别注意收集的数据的局限性，并努力找出解决这些问题的方法。

变更 SLA 是相当困难的，但如果商定的响应时间，数据或其他支持不能满足需要，应当尝试重新协商 SLA。

9.2 建议

- SLA 和围绕客户和提供者职责确定期望是基于云资源的事件响应的关键。明确角色/责任的沟通以及实践响应和交接是至关重要的。
- 云客户必须建立与提供者沟通的适当路径，以便在事件发生时使用。现有的开放标准可以促进事件沟通。
- 云客户必须了解云提供商所提供的用于分析目的数据的内容和格式，并评估现有的取证数据是否满足司法证据保管链要求。
- 云客户应该采用持续和无服务器的方式监控云资源，才能比传统的数据中心更早地发现潜在的问题。
 - 数据源应存储或复制到在事件期间仍可保持可用性的位置。
 - 如果需要和可能，还应该妥当处理它们以保持适当的保管链。
- 基于云的应用程序应利用自动化和业务流程来简化和加速响应，包括遏制和恢复。
- 对于使用的每个云服务提供商，必须在企业事件响应计划中规划和描述用于检测和处理涉及该供应商托管资源的事件的方法。
- 每个云服务提供商的 SLA 必须保证对事件处理提供支持，以有效地执行企业事件响应计划。这必须涵盖事件处理过程的每个阶段：检测、分析、遏制、根除和恢复。
- 事件响应计划至少每年或每当应用架构有重大变化时进行测试。客户应尽可能地将其测试程序与供应商（和其他合作伙伴）的测试程序进行最大程度的整合。

D10: 应用安全

10.0 介绍

应用安全包含了一个非常复杂和庞大的知识体系：从早期设计和威胁建模去维护和防卫生产应用程序。随着应用程序开发实践的不断进步和采用新的流程、模式和技术，应用安全也在以难以置信的速度发展。云计算是这些进步的最大驱动因素之一，它会产生相应的压力，使应用安全的状态发生变化，以确保这种进展尽可能安全地继续下去。

本部分指南旨在为希望在云计算环境中安全的构建和部署应用程序，特别是 PaaS 和 IaaS 的软件开发和 IT 团队准备。（本节中的许多技术也用于支持安全的 SaaS 应用程序）。它主要关注：

- 云计算中应用安全的不同；
- 回顾安全软件开发基础知识以及云计算中的变化；
- 利用云功能实现更安全的云应用。

我们无法涵盖所有可能的开发和部署选项——即使只是与云计算直接相关的选项——因此侧重点放在有助于指导大多数情况下的安全的重要领域。该章节还引入了 DevOps 的安全基础知识，DevOps 也正迅速成为云应用开发的主导力量。

云计算主要为应用程序带来安全优势，但与大多数云技术领域一样，它需要对不在云中运行的现有实践、流程和技术进行相应的更改。在高层次上，这种机会和挑战的平衡包括：

机会

- **更高的安全基线** 云服务提供商，尤其是主要的 IaaS 和 PaaS 提供商，比大多数组织有更显著的经济动机去维持更高的基线安全性。在云环境中，主要的基线安全失效，削弱了公有云提供商为保持与客户关系所需的信任。云服务提供商也应该遵守更广泛的安全要求，以满足从这些垂直领域吸引客户所需的所有监管和行业合规基线。这些结合在一起，激励着云提供商保持极高的安全性。
- **响应能力** 与传统的基础设施相比，API 和自动化提供了广泛的可使用性，以更低的成本，构建响应性更高的安全程序。例如更改防火墙规则或使用更新后的代码部署新服务器，就可以通过一些 API 调用或自动化来处理。
- **隔离环境** 云应用还可以利用虚拟网络和其他结构（包括 PaaS）来实现高度隔离的环境。

例如，无需额外的成本，就可以在完全独立的虚拟网络上部署多个应用程序堆栈，从而消除了攻击者使用一个受到攻击的应用程序，攻击周边防火墙后面的其他应用程序的能力。

- **独立的虚拟机** 通过使用微服务架构进一步增强安全性。由于云不需要使用者来优化物理服务器的使用，所以通常会存在单个系统上部署多个应用程序组件和服务的需求，因此开发人员可以部署更多、更小的虚拟机，每个虚拟机专用于一个功能或服务。这就减少了各个虚拟机的攻击面，并支持更精细的安全控制。
- **弹性** 弹性可以更好地利用不变的基础设施。当使用弹性工具(例如 auto-scale groups) 时，每个生产系统将基于基线图像动态启动，并且可能在无需人工交互的情况下自动取消配置。因此，对于核心业务需求，意味着您不希望管理员登录系统并进行更改，因为它们会在正常的自动调度活动期间消失。这允许使用远程管理是完全禁用的不可变服务器。我们在第 7 章中更详细地描述了不可变的服务器和基础设施。
- **DevOps** DevOps 是一种新的应用程序开发方法和哲学，主要关注应用程序开发和部署的自动化。DevOps 为提高代码的安全性、变更管理和生产应用程序安全性提供了许多机会，甚至增强安全性操作。
- **统一接口** 与那些由不同组管理的传统异构系统和设备(负载均衡器、服务器、网络设备、防火墙、ACL 等)相比，用于基础设施和应用服务(使用 PaaS)的统一接口(管理接口和 API)，提供了更全面的视图和更好的管理。这就创造了减少由于缺乏通信或全栈可见性而导致的安全性故障。

挑战

- 详细的可见性受限 监控和日志的可见性和可用性受到了影响，需要新的方法来收集与安全相关的数据。在使用 PaaS 时尤其如此。通常可用的日志(如系统或者网络日志)将无法从云客户获取。
- 增加应用范围 管理平台/元结构安全性，直接影响与该云帐户相关联的任何应用程序的安全性。开发商和运营商也可能需要访问管理平台，而不是总是沟通不同的团队。数据和敏感信息也可能在管理平台内暴露。最后，现代云应用程序常常与管理平台连接，以触发各种自动化操作，尤其是在涉及到 PaaS 的情况下。基于以上所有原因，管理平台的安全性现在已经在应用程序的安全性范围之内，任何一方的失败都可能与其他安全漏洞挂钩。
- 不断变化的威胁模型 云提供商的关联和共享安全模型，以及任何操作和事件响应计划，需要包含在威胁模型中。威胁模型还需要对云提供程序或平台的技术问题进行调整。。
- 降低透明度 在应用程序中，可能会有更少的透明度，特别是与外部服务集成在一起。例如，您很少知道与应用程序集成的外部 PaaS 服务的整套安全控制。

总体而言，由于共享安全模型，应用安全性将会发生变化。其中一些与管理 and 操作直接相关，但是应用程序的安全方面，需要考虑和规划的问题还有很多。

10.1 概述

由于应用安全的广泛性，以及应用安全中涉及到许多不同的技能和角色，这一章节被分为以下主要方面：

- 安全软件开发生命周期：从设计到部署，计算如何影响应用安全。
- 设计和架构：为云计算设计应用程序的趋势，甚至可以提高安全性。
- DevOps 和持续集成/持续部署（CI / CD）：DevOps 和 CI / CD 在云应用程序的开发和部署中经常被使用，并迅速成为主导模式。它们引入了新的安全考虑，通过更多的手动开发和部署模式（如瀑布）来提高安全性。

10.1.1 安全软件开发生命周期和云计算简介

安全软件开发生命周期(SSDLC)描述了在应用程序开发、部署和操作的各个阶段中的一系列安全活动。行业中使用了多种框架，包括：

- 微软的安全开发生命周期
- NIST 800-64
- ISO/IEC 27034
- 其他组织，包括 OWASP 和各种应用程序安全供应商，也发布了他们自己的生命周期和安全活动指南。

由于框架的范围和术语的不同，云安全联盟将其分为更大的“元阶段”，以帮助描述整个框架中看到的相对标准的活动。这并不意味着取代正式的方法，而只是提供一个描述性的模型，我们可以使用它来处理主要的活动，而不用管一个组织会按照什么生命周期进行标准化。

- 安全的设计和开发：从培训和制定组织范围的标准到实际编写和测试代码。
- 安全部署：将代码从孤立的开发环境转移到生产中时的安全和测试活动。
- 安全操作：保护和维持生产应用程序，包括外部防御，如 Web 应用程序防火墙和持续的漏洞评估。

无论您使用哪种特定的 SSDLC，云计算都将影响 SSDLC 的每个阶段。结合（在公共云端）强大的外部供应商，这是云计算抽象和自动化的直接结果。尤其是：

- 共享的责任模式意味着，即使在基于 IaaS 的裸机应用程序中，云设备一直依赖于安全性的某些方面。您采用 PaaS 和提供商特定功能越多，安全责任的划分就越高。它可以像使用云端负载均衡器一样简单，供应商完全负责保护安全，云计算使用者负责处理和正确使用。
- 在本指南的几乎每个领域都有所讨论，可见性和控制权的变化很大。当主要在 IaaS 上运行时，可能只是缺少网络日志，但是当您进入 PaaS 时，可能意味着服务器和服务日志的丢失。它会根据供应商和技术的不同而变化。
- 不同的云提供商在特性、服务和安全性方面具有不同的功能，这些功能必须在整体应用安全计划中加以考虑。
- 管理平台和元结构现在可能在应用安全范围内，特别是当应用程序组件与云服务直接通信时。
- 有新的和不同的架构选项，特别是在您使用 PaaS 时。
- DevOps 的兴起和影响，我们稍后将在这个章节中介绍。

10.1.2 安全设计与开发

安全应用程序设计和开发有五个主要阶段，所有这些都是云计算所支持的：



安全的应用设计和开发阶段

训练： 三种不同的角色需要两种新的训练类别。所有的开发，运营和安全都应该接受关于云安全基础（不是特定供应商）的额外培训，以及针对项目所使用的特定云提供商和平台的适当的技术安全培训。开发人员和运营人员通常会参与直接构建和管理云基础设施，因此基准安全性培训对于他们将使用的工具具有重要意义。

定义： 云使用者决定了提供商的认可架构或功能/工具、安全标准和其他要求。这可能与合规性

要求紧密相关，例如列出哪些云服务（包括较大提供商中的单独服务）允许哪种类型的数据。在这一步骤中，部署过程也应该被定义，尽管这有时在项目后期完成。安全标准应该包括允许在云提供商中管理哪些服务的初始授权，这些服务通常独立于实际的应用程序架构。它还应该包括预先批准的工具、技术、配置，甚至是设计模式。

设计: 在应用程序设计过程中，特别是在涉及 PaaS 的时候，云安全的重点是架构、云提供商的基准能力、云提供商的功能，以及自动化和管理部署和操作的安全性。我们发现，将安全性整合到应用程序架构中往往具有重要的安全优势，因为有机会利用提供商自己的安全功能。例如，插入无服务器负载均衡器或消息队列可能会完全阻止某些网络攻击路径。这也是您进行威胁建模的地方，这也必须是云和提供商/平台的具体规范。

开发: 开发人员可能需要具有对云管理平台的管理访问权限的开发环境，以便它们可以对网络、服务和其他设置进行配置。这绝不应该是生产环境，也不应该保留生产数据。开发人员还可能使用必须保护的 CI / CD 管道，特别是代码存储库。如果使用 PaaS，则开发人员应该建立日志记录到他们的应用程序，以尽可能的弥补网络，系统或服务日志的任何丢失。

测试: 应将安全测试整合到部署过程和管道中，测试往往跨越这些和安全部署阶段，但倾向于安全单元测试，安全功能测试，静态应用程序安全测试 (SAST) 和动态应用程序安全测试 (DAST)。由于重复内容，我们将在下一节中更深入地讨论云计算的问题。组织还应该更多地依赖于云中的自动化测试。由于基础设施本身是通过模板和自动化实现的，所以基础设施更常用于应用程序测试。作为安全测试的一部分，请考虑为安全敏感的功能要求灵活的功能，这可能需要更深入的安全审查，例如身份验证和代码加密。

10.1.3 安全部署

由于部署自动化在云环境中往往更加突出，因此通常还会在设计和开发阶段包含某些安全活动。自动化的安全性测试非常频繁的集成到部署管道中，并且在直接开发人员控制之外执行。这本身就是偏离许多本地开发项目，但测试本身也需要适应云计算。

有多种应用安全性测试可能会潜在的集成到开发和部署中：

代码审查: 这是一个手动活动，不一定集成到自动化测试中，但 CI/CD 管道可能把它强化为手动控制过程。审查本身并不一定会因云而发生变化，但有特定的领域需要更多的关注。任何与管理层的应用程序通信 (例如对云服务的 API 调用，其中一些可以更改基础设施) 都应该被仔细检查，特别是在项目的早期。除了查看代码本身之外，安全团队还可以专注于确保在应用程序的这一部分中只启用最少的权限，然后使用管理平台的说明来验证它们。与认证和加密相关的任何内容对于额外的审查也很重要。然后可以自动部署过程以通知安全性，如果对可能需要手动批准的这些代码部分进行任何修改，或者只是事后更改审核。

单元测试, 回归测试和功能测试: 这些是开发人员在其正常进程中使用的标准测试。安全测试可以并且应该集成在这些中，以确保应用程序中的安全功能继续按预期运行。测试本身可能需要更新以考虑在云中运行，包括任何 API 调用。

静态应用安全测试 (SAST): 在正常测试范围之外，这些应该理想的包括对云服务的 API 调用的检查。他们还应该寻找这些 API 调用的任何静态嵌入式凭据，这是一个日益严重的问题。

动态应用安全测试 (DAST): DAST 测试运行应用程序，并包括测试，如 Web 漏洞测试和模糊。由于云服务提供商的服务条款 DAST 可能受到限制和/或需要提供商的预测许可。使用云和自动化部署管道，可以使用基础设施作为代码来站起来完全功能的测试环境，然后在批准生产变更之前进行深入评估。

10.1.3.1 对脆弱性评估的影响

脆弱性评估可以集成到 CI / CD 管道中，并且相当容易地在云中实现，但它几乎总是需要遵守提供商的服务条款。

我们通常看到两种具体的模式。第一个是针对镜像或容器进行完整的评估，作为您为此目的而定义的云的特定测试区域 (虚拟网络的一个部分) 的一部分。只有通过这个测试，镜像才会被批准用于生产部署。我们看到了一个类似的模式，它通过使用基础设施作为代码构建一个测试环境来测试整个基础结构。

在这两种情况下，生产测试较少或根本不被测试，因为它应该是不可变的，完全类似于测

试环境（都基于相同的定义）。组织还可以使用基于主机的漏洞评估工具，该工具在虚拟机中本地运行，因此不需要与云提供商协调或许可。

10.1.3.2 对渗透测试的影响

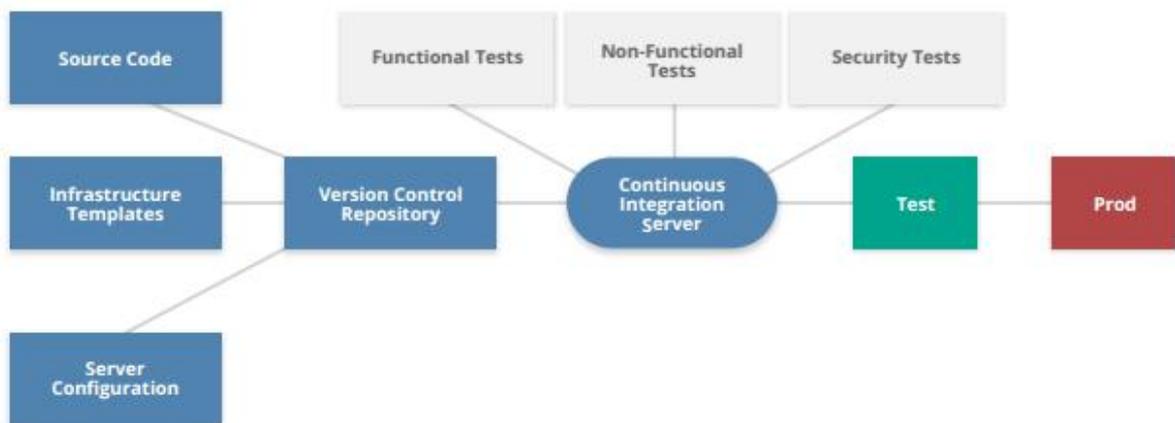
与脆弱性评估一样，未经云提供商的许可，几乎肯定会有渗透测试的限制。CSA 建议使用以下准则来适应云的渗透测试：

- 使用在部署应用程序上有云服务经验的测试公司。
- 包括测试范围内的开发人员和云管理员。许多云漏洞攻击云端维护者，而不是云端的应用，包括云管理平台。
- 如果应用程序是一个多用户的应用程序，那么允许渗透测试人员作为用户授权访问，以确定他们能否破坏用户的隔离性，并利用其访问权限获取另一个用户的环境或数据。

10.1.3.3 部署管道安全

通过支持不可变的基础设施(减少对生产环境的手工更改)、自动化安全性测试，以及当这些更改通过管道运行时，应用程序和基础设施的大量日志记录可以增强安全性。配置正确后，日志可以跟踪每个代码、基础架构和配置更改，并将它们与提交更改的提交人和批准的人联系起来；它们还将包括任何测试结果。

管道本身需要得到严密的保护。考虑在一个严格限制访问的、专用的云环境中存储管道，或者用基础设置存储管道部件。



部署管道的流程

10.1.3.4 基础架构作为代码和不可变的影响

大多时候，我们将基础架构称为代码。由于云的虚拟和软件定义的性质，通常可以使用由工具（提供商或第三方）转换为自动构建环境的 API 调用的模板来定义整个环境。一个基本示例是从模板构建服务器配置。更复杂的实施可以构建整个云应用程序堆栈，直到网络配置和身份管理。

由于这些环境是由一组源文件定义自动构建的，所以它们也可以是不可变的。如果系统或环境是由一个模板自动构建的，很可能来自于一个 CI/CD 管道，那么在生产中所做的任何更改都将被下一个代码或模板更改所覆盖。因此，生产环境可以比非云应用程序部署中通常可能的更紧密，其中大部分基础架构都手动配置为规范。当安全性正常进行时，使用基础设施作为代码和不可变的部署可以显着提高安全性。

10.1.4 安全操作

当应用程序部署到生产中时，安全活动将继续。本章节涵盖许多其他章节内容，特别是在第 7 章（基础架构）、第 8 章（容器）、第 11 章（数据）和第 12 章（身份和访问管理）中。本节包含更直接适用于应用程序的附加指南：

- 生产环境的管理平台应该比开发环境更严格的锁定。如前所述，如果应用程序直接访问托管环境的管理平台，那么这些特权应该被限定在最小可能的范围内。我们建议为每个应用程序服务使用多组凭证，以便进一步划分权限。
- 即使使用不可变的基础设施，仍应该积极监控通过基线的生产环境的变化和偏差。这可以并且应该通过使 API 调用云的代码（或工具）自动化，以定期评估配置状态。

在某些云平台上，可能会使用内置的评估和配置管理功能。根据平台和变更的性质，也可以自动修复未经批准的更改。例如，代码可以自动还原任何未被安全认证的防火墙规则的变动。

- 即使部署后，甚至使用不可变的基础架构，也不要忽视正在进行的应用程序测试和评估。在公共云场景中，这可能需要与云提供商协调或许可，以避免违反服务条款，就像任何其他漏洞评估一样。
- 变更管理不仅包括应用程序，还包括任何基础架构和云管理平台。
- 有关事件响应的信息，请参见第 9 章；有关业务连续性和管理平台安全性的更多信息，

请参见第 6 章。

10.1.5 云如何影响应用程序设计和架构

云的本质就是在首选应用设计、体系结构和模式中创造了变化。其中一些与安全无直接关系，但以下趋势有助于减少常见安全问题：

- **默认隔离：** 应用程序可以轻松地在自己的隔离的云环境中运行。根据提供者的不同，可能是一个单独的虚拟网络或账户/子账户。使用账户或者子账户结构可以有助于实现管理平台隔离。组织可以在开通高度限制性的生产账户的同时开通更广泛的开发账户权限。
- **不可变的基础设施：** 如上所述，由于操作的原因，不可变的基础设施在云中变得越来越普遍。安全性可以通过禁用远程登录到不可变的服务器/容器，添加文件完整性监控以及将不可变技术集成到事件恢复计划中来扩展这些优点。
- **增加使用微服务：** 在云计算中，更容易将不同的服务隔离到不同的服务器(或容器)中，因为一方面，您不再需要最大化地利用物理服务器，另一方面，即使在使用较小的计算机节点来处理负载时，自动伸缩组也可以确保应用程序的可伸缩性。因为每个节点都做得更少，所以更容易锁定并最小化运行在它上的服务。虽然这提高了每个负载的安全性(当使用正确时)，但为了确保所有微服务之间的通信，确保任何服务代理、调度和路由都是安全配置的，也确实增加了一些开销。
- **PaaS 和“无服务器”体系结构：** 通过 PaaS 和“无服务器”设置（直接在云提供商的平台上运行负载，而不用管理底层服务和操作系统），极大的降低了攻击面。只有当云提供商承担平台/无服务器设置的安全性并满足您的要求时，才会这样做。无服务器可以带来一些优势。首先，对于供应商来说，有很大的经济动机来维持极高的安全级别，并保持他们的环境更新。这就消除了将这些安全与云消费者保持一致的日常责任，但永远不会消除其对安全性的最终责任。与可靠的云提供商合作，具有良好的业绩记录至关重要。

接下来，无服务器平台可以在提供商的网络上运行，通过 API 或 HTTPS 流量与消费者的组件通信。这就消除了直接网络攻击路径，即使攻击者破坏了服务器或容器。攻击者仅限于尝试 API 调用或 HTTPS 传输，无法端口扫描识别其他服务器或使用其他常用技术。

- **软件定义安全：** 安全团队可以利用所有相同的工具和技术自动化许多安全操作，甚至将它们与应用程序堆栈进行整合。常见的例子包括自动化云事件响应，对权限进行动态更改、以及对未经批准的基础设施的修正。
- **事件驱动安全：** 某些云提供商支持事件驱动的代码执行。在这些情况下，管理平台会

检测到各种各样的活动（比如将文件上载到指定的对象存储位置，或者对网络或身份管理进行配置更改），从而可以通过通知消息触发代码执行，或者通过服务器托管代码执行。安全性可以为安全操作定义事件，并使用事件驱动的功能来触发自动通知、评估、补救或其他安全流程。

10.1.6 云提供商的其他注意事项

所有服务类型的云提供商需要特别注意其应用服务的某些方面，如果存在安全问题，可能会为其客户带来非常大的问题：

- 需要对 API 和 WEB 服务进行广泛的强化，并假设来自身份验证和未验证的对手的攻击。这包括使用专门为 API 设计的行业标准认证。
- 应监测 API 的滥用和异常活动。
- 服务应经过广泛的设计和测试，以防止攻击或不当/意外的跨租户访问。

10.1.7 DevOps 的崛起和作用

DevOps 指的是开发和运营团队通过更好的协作和通信进行更深入的整合，重点是自动化应用程序部署和基础架构运作。有多种定义，但总体思路包括文化，哲学，流程和工具。

10.1.7.1 安全意义和优势

- 标准化：使用 DevOps，任何投入生产的产品都是由 CI / CD 管道在批准的代码和配置模板上创建的。开发/测试/产品都是基于完全相同的源文件，消除了与已知的良好标准的偏差。
- 自动化测试：如所讨论的，可以将多种安全测试集成到 CI / CD 管道中，并根据需要添加手动测试以进行补充。
- 不可变：CI / CD 管道可以快速可靠的为虚拟机、容器和基础架构堆栈生成主映像。这实现了自动化部署和不可变基础架构。
- 改进审计和变更管理：CI/CD 管道可以跟踪所有的内容，甚至是与提交更改的人相关的源文件中的单个字符更改，以及存储在版本控制存储库中的应用程序堆栈（包括基础设施）的整个历史记录，提供了一个相当可观的审计和变更追踪的便利。
- SecDevOps/DevSecOps 和 Rugged DevOps：这两个术语正在形成，用来描述将安全活动整合到 DevOps 的过程。SecDevOps / DevSecOps 有时指的是使用 DevOps 自动化技术

来改进安全操作。Rugged DevOps 指的是将安全测试整合到应用程序开发过程中，以产生更加坚固，更安全，更具弹性的应用程序。

10.2 建议

- 了解云提供商的安全功能，不仅仅是他们的基准，还有各种平台和服务。
- 将安全性构建到初始设计过程中。云部署更多的是“绿地”，为早期的安全提供了新的机会。
- 即使您没有正式的 SDLC，也可以考虑进行连续部署，并将安全性自动化到部署管道中。
- 威胁建模、SAST 和 DAST (带有模糊的) 都应该被集成起来。应将测试配置为在云环境中工作，但也要测试特定于云平台的问题，比如存储的 API 凭证。
- 了解云中的新架构选项和要求。更新您的安全策略和标准以支持它们，而不仅仅是试图在完全不同的计算模型上强制实施现有标准。
- 将安全测试集成到部署过程中。
- 使用软件定义的安全性来自动执行安全控制。
- 使用事件驱动的安全性（如果可用）自动检测和修复安全问题。
- 使用不同的云环境来更好地隔离管理平台访问，并自由的为开发人员提供配置开发环境，同时也锁定生产环境。

D11: 数据安全和加密

11.0 引言

数据安全是信息和数据治理的关键执行工具。与云安全所有领域一样，由于数据安全并不适合对所有内容提供同等保护，所以应基于风险应用数据安全。

无论是否涉及云，这对数据安全都是成立的。然而，许多组织不习惯于将大量敏感数据（如果不是全部）委托并信任第三方，或将其所有内部数据混合到共享资源池中。因此，我们本能地可能会为“云中的任何事物”制定一个严密的安全政策，而不是坚持以风险为基础的方法，而这将更加安全和高效经济。

例如，加密 SaaS 中的所有内容可能是因为你完全不信任 SaaS 服务提供商。这意味着在最开始你就不应该使用该服务。但加密所有内容并不是灵丹妙药，可能导致虚假的安全感，例如，在不确保设备本身的安全性的情况下加密数据流量。

还有一些人认为，信息安全就是数据安全，但就我们的目的而言，这个域将集中在那些与保护数据本身相关的控制，其中加密是最重要的一种控制手段。

11.1 概述

11.1.1 数据安全控制

数据安全控制往往分为以下三个部分：

- 控制什么数据进入云端（以及进入到哪里）。
- 保护和管理云中的数据。关键的控制和过程是：
 - 访问控制
 - 加密
 - 架构
 - 监控/告警（使用情况、配置、生命周期状态等）

- 附加控制，包括云提供商相关的具体产品/服务/平台，DLP 以及企业权限管理。
- 执行信息生命周期管理安全：
 - 管理数据位置/归属地
 - 确保合规性，包括人工审计（日志，配置）
 - 备份和业务连续性，在第六章（D6）中会有描述。

11.1.2 云数据存储类型

由于云存储是虚拟化的，它支持不同于传统存储技术的不同数据存储类型。在虚拟化层之下，可能使用常见的数据存储机制，但云端消费者接入的云存储虚拟化技术将会有所不同。常见的存储类包括：

对象存储：对象存储类似于文件系统。“对象”通常是文件，使用云平台特定机制进行存储。大多数访问通过 API，而不是标准的文件共享协议，即便云提供商可能也提供支持这些协议的前端接口。

卷存储：这实质上是实例或虚拟机的虚拟硬盘。

数据库：云平台和提供商可以支持各种不同类型的数据库，包括现有的商业和开源选择以及自己的专有系统。专有数据库通常使用自己的 API。商业或开源数据库由提供商托管，通常使用现有的连接标准。这些可以是关系的或非关系的，后者包括 NoSQL 和其他键/值存储系统，或者基于文件系统的数据库（例如 HDFS）。

应用程序/平台：如，内容分发网络（CDN），存储在 SaaS 中的文件、缓存和其他新颖选项中。

大多数云平台也使用冗余持久的存储机制，这些机制经常使用数据分散（有时也称为分位数据碎片）。此过程需要大量数据，将其分解，然后将多个副本存储在不同的物理存储上，以提供高持久性。以这种方式存储的数据是物理分散的。例如，单个文件不会存储在单个硬盘驱动器上。

11.1.3 管理数据迁移

在保护云中数据的安全之前，大多数组织都需要一些管理手段来管理存储在私有云和公有云服务商中的数据。相比安全，合规性更为至关重要。

首先，定义不同的策略-允许存储的数据类型和存储位置，然后将这些策略与基本安全需求相结合。例如，“假设符合 y 加密和访问控制要求，那么在 x 服务上允许使用 PII”。

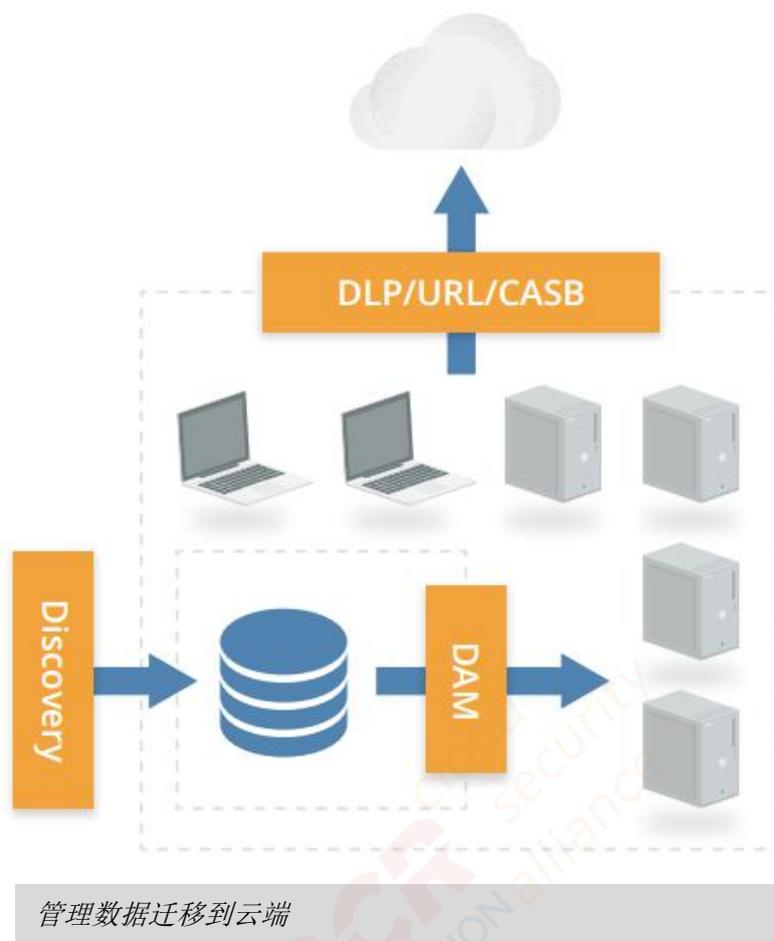
然后识别关键的数据存储。使用数据库活动监视工具或文件活动监视工具监视数据存储的大量迁移/活动。这基本上是在为大型数据传输建立“早期警告系统”，但它也是重要的数据安全控制，可以检测各种主要违规行为和滥用情况。

检测实际迁移监视云使用情况和任何数据传输。您可以借助以下工具来执行此操作：

CASB: 云访问和安全代理（也称为云安全网关）使用各种机制发现云服务的内部使用，如网络监控，集成现有网络网关或监控工具，甚至通过监控 DNS 查询。发现用户在连接哪些服务后，大部分产品通过可用的 API 或者内联截获（中间人监控）提供对核准服务的活动的监控。支持 DLP 和其他安全告警，甚至提供更好的控制手段来管理云服务（SaaS /PaaS / IaaS）中敏感数据的使用。

URL 过滤: 虽然 URL 过滤器/网关不如 CASB 那么强大，但可以帮助了解用户使用（或尝试使用）哪些云服务。

DLP: 如果监视 Web 流量（并查看 SSL 连接），则 DLP 工具还可以帮助检测数据迁移到云服务。但是，一些云 SDK 和 API 可能会加密部分数据和流量，则 DLP 工具无法解开，因此将无法正确识别载荷。



11.1.3.1 保护云数据传输安全

确保在数据移动到云端的过程中采取数据保护措施。这需要理解供应商的数据迁移机制，因为促使供应商机制比“手动”数据传输方法（比如 SFTP）要更安全更具有成本效益。例如，通过 API 将数据发送到提供商的对象存储中，很可能比在同一供应商的虚拟机上设置自己的 SFTP 服务器更可靠和安全。

根据云平台支持的内容，有几种可用于中转加密的选项。一种方法是在发送到云端之前进行加密（客户端加密）。网络加密（TLS / SFTP / 等）是另一种选择。大多数云提供商 API 默认使用 TLS；如果不是，选择不同的提供商，因为这是一个基本的安全功能。基于代理的加密可能是第三个选项，将加密代理放置在云消费者和云提供商之间的可信区域中，代理在将数据传输到提供商之前负责加密。

在某些情况下，可能需要接受公共的或不受信任的数据。如果允许合作伙伴或公众向您发送数据，请确保具备相应的安全机制，以便在处理或混合现有数据之前对其进行清理。在集成之前，请务必隔离并扫描此数据。

11.1.4 保护云中数据

访问控制和加密是重要的数据安全控制技术。

11.1.4.1 云数据访问控制

访问控制至少可以在三个层面执行：

- **管理平面：**这些是用于管理直接访问云平台管理平面的用户访问的控制。例如，登录到 IaaS 服务的 Web 控制台将允许该用户访问对象存储中的数据。幸运的是，大多数云平台和提供商默认策略是拒绝访问控制。
- **公共和内部共享控制：**如果数据是对无法直接访问云平台的公众或合作伙伴提供外部共享，则此访问将会有第二层控件。
- **应用程序级别控制：**在云平台上构建自己的应用程序时，设计和实现自己的控件来管理访问。

访问控制选项将根据云服务模型和提供商特定功能而有所不同。基于平台特定的功能创建一个权限矩阵。授权矩阵记录用户、组和角色应该访问哪些资源和功能。

Entitlement	Super-Admin	Service-Admin	Storage-Admin	Dev	Security-Audit	Security-Admin
Volume Describe	X	X		X	X	X
Object Describe	X		X	X	X	X
Volume Modify	X	X		X		X
Read Logs	X				X	X

经常（理想的是连续地）验证控制措施是否满足您的要求，特别注意任何公开场景。考虑为所有新公开共享或更改允许公开访问权限设置告警。

细粒度访问控制和权利映射

技术之间潜在权利的深度将会有很大差异。一些数据库可能支持行级的安全性，而其他数据库可能不仅仅是广泛的访问。有些将允许您将权限绑定到云平台内置的身份和执行机制，而其其它则完全依赖于仅在虚拟机中运行的存储平台本身。

了解您的选择，将其映射出来并构建矩阵很重要。当然，这不仅适用于文件访问；它也适用于数据库和所有云存储数据。

11.1.4.2 存储（At-Rest）加密和令牌

基于服务模型、提供商和应用/部署细节，加密选项差异很大。密钥管理与加密一样重要，因此在后续部分中将会涉及。

加密和标记化是两种独立的技术。加密通过应用数学算法来保护数据，数学算法“加扰”数据，然后只能通过使用相应的密钥进行解扰（解密）过程来复原数据。结果是一串密文。另一方面，令牌取代数据并用随机值替换它，然后将原始和随机版本存储在安全数据库中，以备以后恢复。

当数据的格式很重要时（例如更换现有系统中信用卡号需要相同格式的文本字符串），通常会使用令牌化。格式保存加密使用密钥加密数据，但也保持与标记化相同的结构格式，但它可能不会像加密那样安全。

加密系统有三个组成部分：数据，加密引擎和密钥管理。数据当然是您要加密的信息。引擎是加密的数学过程。最后，密钥管理器处理加密密钥。系统的整体设计重点聚焦于每个部件放在哪里。

设计加密系统时，应该从威胁模型开始。例如，您是否信任云提供商来管理您的密钥？密钥怎么泄露的？您应该在哪里找到加密引擎来管理您所关心的威胁？

IaaS 加密

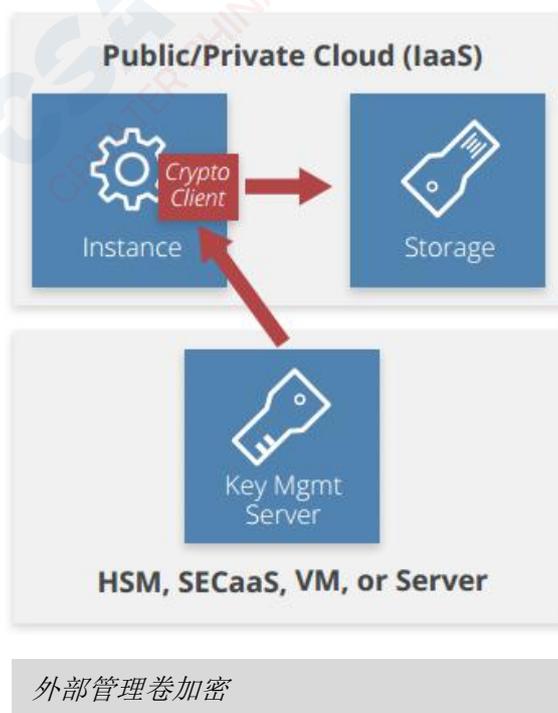
根据您的数据，可以使用不同的方法对 IaaS 卷进行加密。

卷存储加密

- 实例管理的加密：加密引擎在实例中运行，密钥存储在卷中，但受密码短语或密钥对保护。
- 外部管理加密：加密引擎在实例中运行，但密钥由外部管理，并根据请求发送给实例。

对象和文件存储

- 客户端加密：当对象存储用作应用程序（包括移动应用程序）的后端时，使用嵌入在应用程序或客户端中的加密引擎对数据进行加密。
- 服务器端加密：数据在传输后在服务器（云）端进行加密。云提供商可以访问密钥并运行加密引擎。
- 代理加密：在此模型中，将卷连接到特殊实例或设备/软件，然后将实例连接到加密实例。代理处理所有加密操作，并且可以将密钥保存在内部或外部。



外部管理卷加密

PaaS 加密

由于有不同的 PaaS 平台，PaaS 加密区别非常大。

- **应用层加密：**数据在 PaaS 应用程序或访问平台的客户端进行加密。
- **数据库加密：**数据库使用内置的加密技术在数据库中进行加密，并由数据库平台（如透明数据库加密（TDE））或现场级别支持。
- **其他：**这些是应用程序中的供应商管理层，如消息队列。当用于底层存储时，还有 IaaS 选项。

SaaS 加密

SaaS 提供商可以使用之前讨论的任何选项。建议在可能的情况下每个客户端使用不同密钥，以便更好地实施多租户隔离。以下选项适用于 SaaS 消费者：

- **提供商管理的加密：**数据在 SaaS 应用程序中加密，一般由提供商管理。
- **代理加密：**在发送到 SaaS 应用程序之前，数据通过加密代理。

11.1.4.3 密钥管理（包括客户管理的密钥）

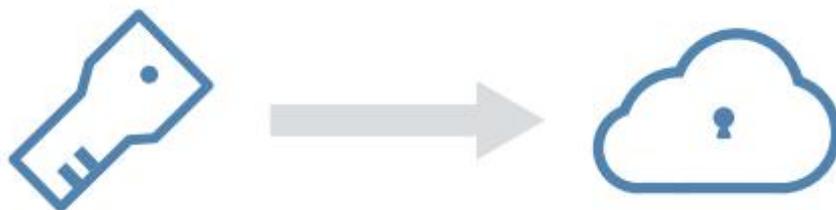
密钥管理的主要考虑因素是性能、可访问性、延迟和安全性。您是否将正确的密钥在正确的时间放在合适的位置，同时满足您的安全和合规要求？

处理密钥管理有四个潜在的选择：

- **HSM /设备：**使用传统的硬件安全模块（HSM）或基于设备的密钥管理器，这通常需要在本地进行，并通过专用连接将密钥提供给云。
- **虚拟设备/软件：**在云中部署虚拟设备或基于软件的密钥管理器。
- **云提供商服务：**这是云提供商提供的关键管理服务。在选择此选项之前，请确保您了解安全模型和 SLA 以了解您的密钥是否会被暴露。
- **混合：**您还可以使用组合，例如使用 HSM 作为密钥的信任根，然后将特定于应用程序的密钥提供给位于云中的虚拟设备，并仅管理其特定上下文的密钥。

客户管理的密钥

客户管理的密钥允许云客户在提供商管理加密引擎时管理自己的加密密钥。例如，使用您自己的密钥来加密 SaaS 平台中的 SaaS 数据。许多提供商默认加密数据，使用他们自己完全控制的密钥。有些可能允许您替换自己的密钥与他们的加密系统集成。确保您的供应商的做法符合您的要求。



客户管理密钥

一些提供商可能会要求您使用提供商内的服务来管理密钥。因此，尽管密钥是由客户管理的，但它仍然可被供应商获得。这并不一定意味着它是不安全的：由于密钥管理和数据存储系统可以分开，所以需要供应商的多个员工的勾结才可能危害数据。然而，根据当地的法律，政府的要求仍然可能暴露钥匙和数据。您可能可以在提供商的外部存储密钥，并且只能在每个请求的基础上传递它们。

11.1.5 数据安全架构

应用架构影响数据安全。云提供商提供的功能可以减少攻击面，但确保要求强大的元结构安全性。例如，通过在提供商的网络上通信使用云存储或队列服务而不是在你自己的虚拟网络来隔离网络。因为网络攻击路径关闭，所以迫使攻击者只能攻击云提供商或将其限制于应用级攻击。

一个例子是使用对象存储进行静态实例的数据传输和批处理，而不是 SFTP-ing。另一个例子是不同虚拟网络上的消息队列间隔运行应用程序组件，这些组件只能通过云提供商的消息队列服务传递数据来桥接。这消除了从应用程序的一部分到另一部分的网络攻击。

11.1.6 监控、审计和告警

这些应该与整体云监控相结合。（请参阅 D3、D6 和 D7）识别（并提醒）对敏感数据的任何公共访问权限或权利变更。可用时使用标记来支持警报。

您需要监控 API 和存储访问，因为数据可能会通过任一种方式公开 - 换句话说，通过 API 调用或通过公共共享 URL 访问对象存储中的数据。活动监视，包括数据库活动监视，可能是一个选项。确保将您的日志存储在安全的位置，如专用日志记录帐户。

11.1.7 其他数据安全控制

11.1.7.1 云平台/提供商特有的控制

云平台或提供商可能具有不在本域其他地方覆盖的数据安全控制。虽然通常它们将是某种形式的访问控制和加密，但本指南无法涵盖所有可能的选项。

11.1.7.2 数据丢失防护

数据丢失防护（DLP）是通过监视本地系统、网络、电子邮件和其他流量来监控和保护员工访问的数据的方法。它通常不会在数据中心内使用，因此比通常未部署 DLP 的 PaaS 或 IaaS 它更适用于 SaaS。

- **CASB（云访问和安全代理）**：一些 CASB 包括其保护的受制裁服务的基本 DLP 功能。例如，您可以设置信用卡号码从未存储在特定云服务中的策略。有效性在很大程度上取决于特定工具，云服务以及 CASB 如何集成进行监控。一些 CASB 工具还可以将流量路由到专用 DLP 平台，以便提供比 CASB 的 DLP 功能更强大的分析。
- **云提供商功能**：云提供商本身可以提供 DLP 功能，例如云文件存储和协作平台，可以扫描上传的内容文件并应用相应的安全策略。

11.1.7.3 企业权力管理

与 DLP 一样，这通常是一种员工安全控制，并不总是适用于云。由于所有 DRM / ERM 都基于加密，现有的工具可能会破坏云的功能，特别是在 SaaS 中。

- **完全 DRM:** 这是使用现有工具的传统全数字版权管理。例如，在将文件存储在云服务中之前对文件应用权限。如上所述，除非有某种集成（在撰写本文时很少见），否则可能会破坏云端服务器的功能，例如浏览器预览或协作。
- **基于提供者的控制:** 通过使用本地功能，云平台可能能够强制执行与完全 DRM 相似的控制。例如，用户/设备/视图与编辑：仅允许某些用户在 Web 浏览器中查看文件的策略，而其他用户可以下载和/或编辑内容。有些平台甚至可以将这些策略绑定到特定的设备上，而不仅仅是在用户层面上。

11.1.7.4 数据屏蔽和测试数据生成

这些是保护在开发和测试环境中使用的数据的技术，或限制对应用程序中数据的实时访问。

- **测试数据生成:** 这是创建一个基于“真实”数据库的非敏感测试数据的数据库。它可以使用加扰和其他随机化技术来创建类似于大小和结构的源，但缺少敏感数据的数据集。
- **动态屏蔽:** 动态屏蔽通常使用代理机制即时重写数据，以掩盖传递给用户的全部或部分数据。它通常用于保护应用程序中的一些敏感数据，例如呈现给用户时，屏蔽掉除最后一位数字外的其他信用卡号码。

11.1.8 执行生命周期管理安全

- **管理数据位置/驻留:** 在某些时候，您需要禁用不必要的位置。使用加密来强制访问容器或对象级别。然后，即使数据移动到未经批准的位置，数据仍然受到保护，除非密钥和它一起移动。
- **确保合规性:** 您不仅需要实施控制来维护合规性，您需要记录和测试这些控制。这些是“合规的工件”；这包括您将拥有的任何审计工件。
- **备份和业务连续性**（见 D6 章）

11.2 建议

- 了解您正在使用的云平台的具体功能。
- 不要关闭云提供商的数据安全性。在许多情况下，它比建立自己的安全性更低，成本更低。
- 创建用于确定访问控制的授权矩阵。执行将根据云提供商的功能而有所不同。
- 考虑 CASB 来监控流入 SaaS 的数据。对于一些 PaaS 和 IaaS 可能仍然有帮助，但更多

地依赖现有的策略和数据存储库安全性来进行这些大型迁移。

- 根据数据、业务和技术要求的威胁模型，使用适当的加密选项。
- 考虑使用由供应商管理的加密和存储选项。在可能的情况下，使用客户管理的密钥。
- 利用架构来提高数据安全性。不要完全依赖访问控制和加密。
- 确保 API 和数据级监控都已到位，并且该日志符合合规性和生命周期策略要求
- 利用现有标准帮助建立良好的安全性和正确使用加密和密钥管理技术和流程。特别是，NIST SP-800-57 和 ANSI X9.69 和 X9.73。

D12: 身份、授权和访问管理

12.0 介绍

身份、权利以及访问管理（IAM）深受云计算的影响。不管是公有云还是私有云都需要在不损害安全的前期下进行身份访问（IAM）管理。本章关注的焦点是我们需要调整云的哪些身份管理机制。当我们回顾一些基本概念时，关注点是云计算如何改变我们的身份管理，以及我们需要做什么。

云计算的出现，对于内部系统的传统 IAM 管理引入了许多变化。这并不是说这些都是新闻

题，但在处理云的 IAM 管理时是更大的问题。

关键的区别是云提供商和云消费者之间的关系，即便在私有云。IAM 不能仅仅由一方或另一方来管理，因此需要建立信任关系，通过责任指定和技术机制来实现，通常情况下，我们将这种方式归结为联邦。这加剧了一个事实，即大多数组织有许多（有时数百）不同的云供应商，因此迫切需要扩展他们的 IAM。

云也在发生快速的变化，变得更为分布式（包括穿越了不同的法律管辖的边界），增加了管理界面的复杂性，也更加依赖（通常来说是唯一）于网络通信，也相当于对网络攻击打开了基础设施的管理权限。同时，在供应商之间以及在不同的服务和部署模式之间都存在着广泛的差异。

此域主要侧重于组织和云提供商之间或云提供商和服务之间的 IAM。它不讨论在云应用程序中管理 IAM 的所有方面，例如在 IaaS 上运行的企业应用程序的内部 IAM。这些问题与在传统基础设施中建立类似的应用和服务非常相似。

12.0.1 云上 IAM 的差异

身份和访问管理总是复杂的。最核心的一点是，我们将某种形式的实体（人、系统、代码等）映射到与各种相关联的可验证身份属性（可以根据当前情况改变），然后根据授权决定他们能做什么或不能做什么。即使你控制整个链条的所有过程，对不同的系统和技术采用安全和可验证的方式管理 IAM 仍然是一个挑战，特别是在大规模应用的场景下。

在云计算中，最基本的问题是，多个组织正在对资源的身份识别和访问进行管理，这一点显著的复杂化了管理过程。举例来说，想象一下要统一在几十个或者几百上千个不同的云服务上规范同一个用户的行为。联邦制将作为管理这个问题的主要工具，通过建立组织之间的相互

信任关系以及在组织间强制使用标准化的技术。

联邦制以及其他的 IAM 技术在计算机出现之前就已经存在了，随着时间的推移，组织也随着 IT 的发展对他们的 IAM 系统进行修修补补。云计算是一个强制因素，自从使用了云以后，快速的推动了企业去面对其 IAM 实践，针对与云的差异之处进行升级。这既带来了机遇也带来了挑战。

在更高层次上，向云迁移是建立基于现代架构和标准的新基础设施与流程的机会。多年来 IAM 已经取得了巨大的进步，但由于预算和遗留基础设施的限制，许多组织只能在有限的案例中实施。采用云计算，无论是一个小型项目还是整个数据中心迁移，通常意味着在基于最新的 IAM 实践的新基础架构上构建新系统。

这些转变也带来挑战。考虑到涉及的所有变量，与多个内部和外部各方一起转移到联邦制可能是复杂和难以管理的。不同系统和技术中决定和实施属性和授权会带来流程和技术问题。即使基础架构决策也可能受到云提供商和平台之间支持的广泛变化的阻碍。

IAM 跨越本文档中的每个域。本节首先对并非所有读者都熟悉的一些核心术语进行快速回顾，然后再深入了解云对身份管理的影响，阐述对访问和权利管理的影响。

12.1 概览

IAM 是一个广泛的实践领域，有其自身的专用术语，对于那些不是该领域的专业人士来说可能会令人困惑，特别是因为某些术语在不同的语境中有不同的含义（在 IAM 以外的领域中使用）。术语“IAM”不是通用的，并且通常被称为身份管理（IdM）。

Gartner 将 IAM 定义为“确保适当的个人能够以正确的理由在正确的时间访问正确的资源的安全规则”。在我们阐述细节之前，以下为我们在云计算中讨论 IAM 时最为相关的高层次术语定义：

- 实体：具有身份的人或“事物”。它可以是个人，系统，设备或应用程序代码。

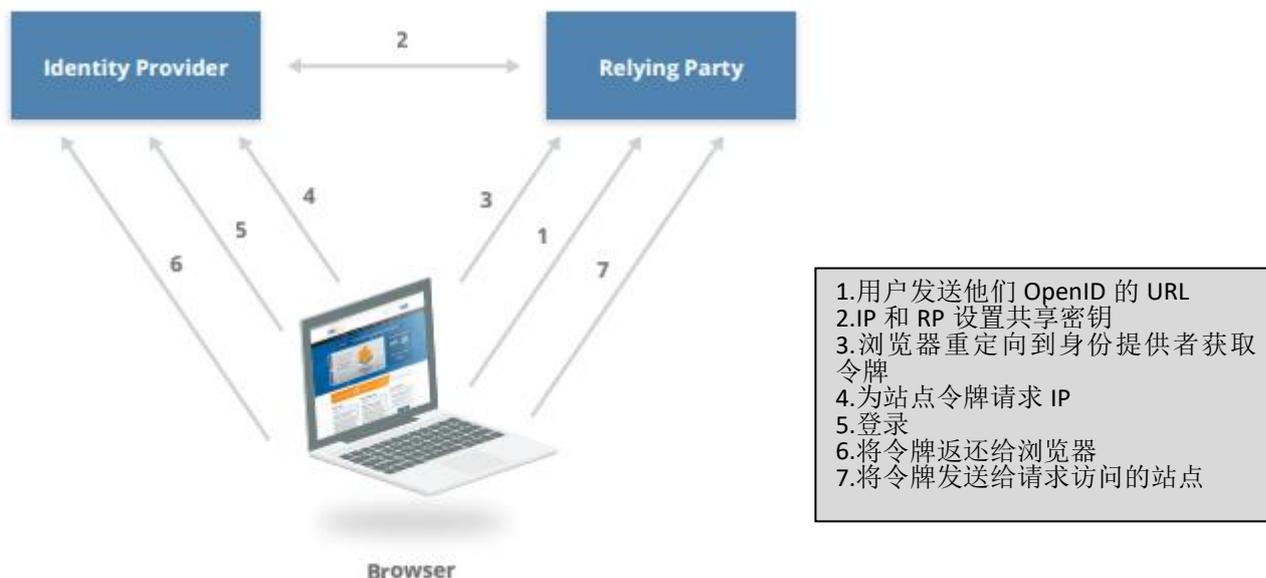
- **身份**：一个实体在给定命名空间内的唯一标识。实体可以具有多个数字身份，一个实体可以具有工作身份（或取决于系统的多个身份），社交媒体身份和个人身份。例如，如果您是单个目录服务器中的单个条目，则这就是您的身份。
- **标识符**：可以鉴别身份的方式。对于数字身份，这往往是一个密码令牌。在现实世界中，这可能是你的护照。
- **属性**：身份各个方面。属性可以相对静态（如组织单位）或高度动态（IP 地址，正在使用的设备，用户使用 MFA 进行身份验证，位置等）。
- **人物角色**：具有语义指向的属性身份的一种表示。例如，开发人员登录工作，然后连接到云环境作为特定项目的开发人员。身份仍然是个人，人物角色是该项目背景下的个人。
- **角色**：在不同的语义中，身份可以有多个角色。“角色”是一个以许多不同的方式被混乱和滥用的术语。出于我们自身考虑，我们会将其视为与人物角色相似，或作为人物角色的子集。例如，给定项目中的给定开发人员可能具有不同的角色，例如“超级管理员”和“开发者”，然后用于进行访问决策。
- **认证**：确认身份的过程。当您登录到您所在的系统时用户名（标识符）和密码（我们称为身份验证因子的属性）。也称为 Authn。
- **多因素认证 (MFA)**：在认证中使用多个因素。常用选项包括通过物理或虚拟设备/令牌（OTP）生成的一次密码，通过文本消息发送的 OTP 进行的带外验证方式，或来自移动设备，生物识别或插件令牌的确认。
- **访问控制**：限制对资源的访问。访问管理是管理资源访问的流程。
- **授权**：允许一个身份访问某些内容（例如数据或功能）。也称为 Authz。
- **权利**：将身份（包括角色，人物角色和属性）映射到授权。权利是他们被允许做的，处于文档化的考虑，我们将它们以权利矩阵的形式体现。
- **联邦身份管理**：跨不同系统或组织鉴别身份的过程。这是单点登录的关键推动者，也是在云计算中管理 IAM 的核心。
- **授权源**：身份的“根”源，例如管理员工身份的目录服务器。
- **身份提供者**：联邦中的身份来源。身份提供者并不总是授权源，但有时可以依赖于授权源，尤其是当它作为该进程的代理时。
- **依赖方**：依赖于身份提供者进行身份鉴别的系统。

以下相关章节将涵盖更多的术语，包括主要的 IAM 标准。此外，虽然这部分看起来可能过分关注公有云，但相同的原则同样适用于私有云；然而，因为组织可能对整个情况有更多的控制权，范围将会减少。

12.1.1 云计算的 IAM 标准

目前已有很多身份和访问管理标准，其中许多可以用于云计算。尽管标准的选择范围广泛，但行业正趋向于一个核心集合，在各种部署中最常见，并且得到大多数提供商的支持。还有一些有希望但尚未广泛使用的标准。以下列表并不代表任何特定的推荐，也并非所有选项，而只是代表受到供应商最广泛、最常支持的选项：

- 安全鉴别标记语言（SAML）2.0 是联合身份管理的 OASIS 标准，支持身份验证和授权。它使用 XML 来在身份提供者和依赖方之间做出鉴别。鉴别声明可以包含身份验证声明，属性声明和授权决策声明。企业工具和云提供商都非常广泛地支持 SAML，但是初始配置可能很复杂。
- OAuth 是一种非常广泛用于 Web 服务的 IETF 授权标准（包括消费者服务）。OAuth 旨在通过 HTTP 进行工作，目前版本为 2.0，与 1.0 版不兼容。给混合使用带来了一些不便，OAuth 2.0 更多的是框架，而不像 OAuth 1.0 是一些刚性要求，这意味着实施上可能存在不兼容的情况。最常用于在服务之间委派访问控制/授权。
- OpenID 是联邦认证非常广泛支持的 Web 服务标准。它是基于 URLs 的 HTTP 对身份提供商和用户/身份进行识别。目前的版本是 1.0，它是消费服务场景中很常见。
- 可扩展访问控制标记语言（XACML）是用于定义基于属性的访问控制/授权的标准。它是一种策略语言，用于在策略决策点定义访问控制，然后将其传递到策略执行点。它可以与 SAML 和 OAuth 一起使用，因为它解决了问题的不同部分——即决定一个实体允许使用一组属性，而不是处理登录或授权。
- 跨域身份管理系统（SCIM）是域之间交换身份信息的标准。它可以用于外部系统中的账户配置和取消以及交换属性信息。



联邦身份管理如何运作：当其与依赖方建立信任关系后，联邦会引入身份提供者做出鉴别。核心是建立信任关系和交换凭证的一系列加密操作。一个实际的例子是用户登录到他们的工作网络，它承载账户的目录服务器。然后，该用户打开连接到 SaaS 应用程序的浏览器。在登录行为的背后隐藏了一系列的后台操作，身份提供者（内部目录服务器）鉴别用户的身份，用户的身份以及任意属性得到认证。依赖方信任这些鉴别申明，而不需要用户输入任何凭据来进行登录。事实上，依赖方甚至没有该用户的用户名或密码；它依赖于身份提供者来证实身份验证成功。假如用户通过内部目录成功进行身份验证，就可以直接访问 SaaS 应用程序的网站并登录。

这并不意味着在云计算中不再使用其他身份识别，验证和授权的技术或标准。大多数云提供商，特别是 IaaS 提供商，都有自己内部 IAM 系统，但可能不使用任何这些标准，或连接到使用这些标准的组织。例如，HTTP 请求签名常用于 REST API 的身份验证，由云提供商端的内部策略进行授权决定。请求签名仍然可以通过 SAML 支持单点登录，或 API 可能完全基于 OAuth，或使用自己的令牌机制。所有这些都是常见的，但大多数企业级云提供商都提供某种联合支持。

身份协议和标准本身并不代表完整的解决方案，但它们是一种手段。选择身份协议时的必要的概念是：

- 没有解决所有身份和访问控制问题的协议。
- 身份协议必须在用例的上下文进行分析。例如，基于浏览器的单点登录，API 密钥或移动端到云验证等方式可以引导公司采用不同的方法。
- 运营的关键假设就是身份本身就是一个边界，就像一个 DMZ。因此，任何身份识别协议都必须从可以穿越危险领域并抵御恶意的角度来选择和设计。

12.1.2 管理云计算的用户和身份

身份管理的“身份”部分重点关注注册，配置，传播，管理和取消配置身份的流程和技术。在系统中管理和配置身份是信息安全数十年来致力于解决的问题。不久之前，IT 管理员仍需要在每个不同的内部系统中单独配置用户。即使在今天，通过集中式目录服务器和一系列标准，真正的单点登录仍然比较少见；用户仍然管理一组凭据，尽管比过去的规模小得多。

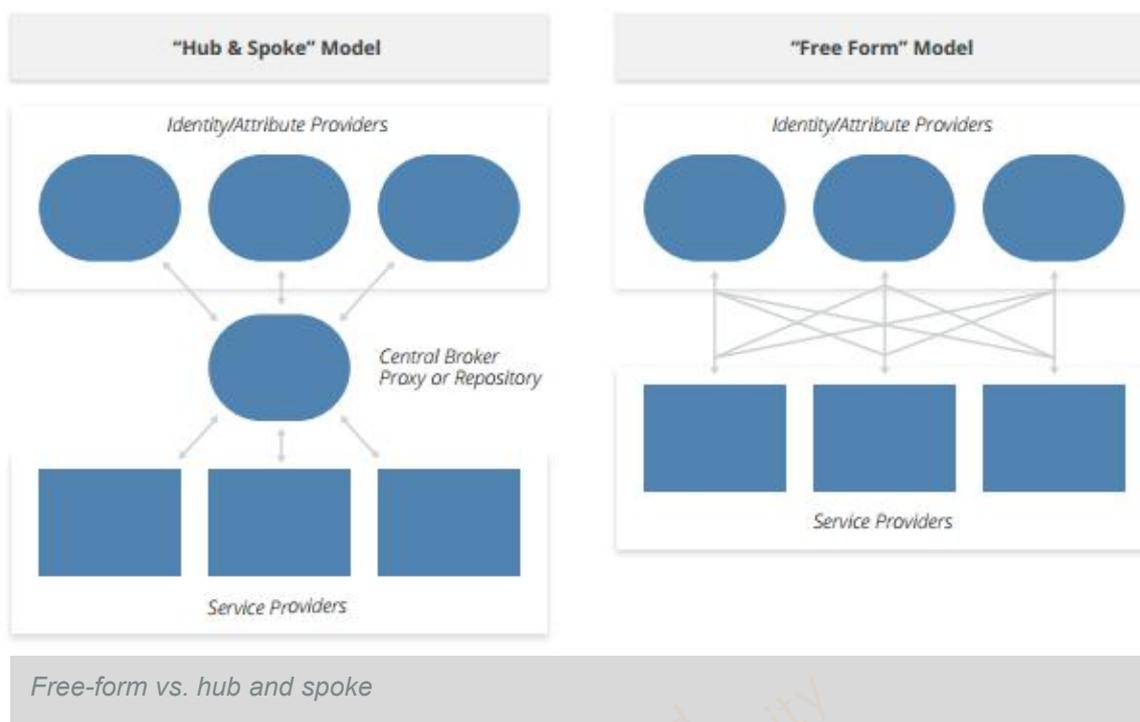
关于范围的说明：本节中所描述的方法是通用的，但是倾向于针对用户管理。相同的原则适用于服务，设备，服务器，代码和其他实体的身份管理，但这些过程和细节可能更复杂，并与应用程序安全性和体系结构紧密相关。出于同样的原因，该域也仅包括对云提供商的所有内部身份管理问题的有限讨论。并不是说这些领域不那么重要，在许多情况下，它们更重要，但它们也带来了在本指南的限定范围内所不能完全涵盖的复杂性。

云提供商和云消费者需要从如何管理身份的基本决定开始：

- 云提供商需要几乎总是支持直接访问服务的用户的内部身份，标识符和属性，同时还支持联邦，以便组织不必手动配置和管理供应商系统中的每个用户，并颁发每个人的独立凭据。
- 云消费者需要决定他们希望在哪些地方管理自己的身份，以及他们希望支持哪些架构模型和技术，并与云提供商集成。

作为云消费者，您可以登录云提供商并在其系统中创建你所需要的所有身份。这对于大多数组织来说是不可扩展的，这就是为什么大多数组织转向联邦。需要记住的一点是，将所有或部分身份与云提供商隔离看似有道理，但可能会存在例外的情况，例如用于调试联合身份连接问题的备份管理员帐户。

当使用联邦时，云消费者需要确定持有可用来联合的唯一身份标识的授权源。通常来说是内部的目录服务器，下一个决定就是是否直接使用授权源作为身份提供方，或使用一个不同的身份来源，抑或集成一个身份代理。有两种可能的架构：



- **Free-form:** 内部身份提供者/来源（通常是目录服务器）直接连接到云提供商。
- **Hub and Spoke:** 内部身份提供者/来源与集中代理进行通信，然后作为云提供商的联邦身份提供方。

直接联合内部目录服务器的自由格式模型带来了以下问题：

- 目录需要 Internet 访问。这可能是一个问题，取决于现有的拓扑结构，或者它可能违反安全策略。
- 在访问云服务之前，可能需要用户将 VPN 重新连接到公司网络。
- 根据现有的目录服务器，特别是如果您在不同的组织孤岛中有多个目录服务器，则与外部提供商可能采用联邦形式会比较复杂且技术上难以实现。
- 身份代理处理身份提供商和依赖方之间的联盟（可能并不总是云服务）。它们可以位于网络边缘甚至云端，以便启用 web-SSO。
- 身份提供者不仅仅需要位于内部，许多云提供商现在支持基于云的目录服务器，以支持内部联盟和其他云服务。例如，更复杂的体系结构可以通过身份代理将内部目录的组织身份的一部分进行同步或联合，然后再将其作为其他联盟连接的身份提供者。

在确定大型模型之后，仍然需要在实施时进行所需流程和架构的决策：

- 如何管理应用程序代码，系统，设备和其他服务的身份识别。您可以利用相同的模型和标

- 准，或决定对云上的部署以及应用程序采用不同方法。例如，上面的描述倾向于用户访问服务，但可能不适用于服务与服务、系统或设备的通信服务或 IaaS 部署中的应用程序组件。
- 定义身份配置过程以及如何将其集成到云部署过程中。尽管目标应该是尽可能建立一个统一的流程，但是对于不同的用例也可能有多个不同的配置过程。
 - 如果组织对传统基础设施已有有效的配置流程，则应将其理想地扩展到云部署中。然而，如果现有的内部流程是有问题的，那么组织应借迁移到云计算上的机遇，作为建立新的、更有效的流程。
 - 配置和支持单个云服务提供商并进行相应部署。应建立新提供商引入到 IAM 基础设施的正式流程。这包括建立任何所需联邦连接的流程，以及：
 - 对身份提供者和依赖方之间的属性（包括角色）进行映射。
 - 启用所需的监控/记录，包括身份相关的安全监控，如行为分析。
 - 建立一个权力矩阵(下一节详细讨论)。
 - 记录任何破解/修复情况，以防任何用于关系的联盟（或其他技术）出现技术故障。
 - 确保存在潜在账户被盗用的事件响应机制，包括特权账号的盗用。
 - 对身份以及云服务提供商实施配置或权利变更的管理流程。如通过联邦形式，则需要两端都进行相应的工作。

最后，云提供商需要确定他们希望支持的身份管理标准。一些提供商只支持联邦，而其他提供商则支持多个 IAM 标准和自己的内部用户/账户管理。为企业市场服务的供应商将需要支持联邦身份识别，比如 SAML 协议。

12.1.3 认证以及凭证

认证是证明或确认身份的过程。在信息安全中认证通常指的是用户登录的行为，但实际上也指实体在任何时点证明自己是其所声称的那个身份。认证是身份提供方的责任。

云计算对身份验证的最大影响是使用多因素强身份验证的强烈需求。这有两方面原因：

- 广泛的网络访问意味着云服务总是通过网络访问，并经常通过互联网访问。凭证的丢失可能导致账户被攻击者利用，从而使得攻击不再受限于本地网络。
- 更多地使用联邦单点登录意味着一组凭证可能使更多的云服务暴露在潜在的危險中。

多因素认证为减少账户的恶意利用提供了最好的选择。这不是灵丹妙药，但在云服务上使用

用单一因素（如密码）进行认证存在很大的风险。当在联邦上使用 MFA 与时，身份提供方可以并且应该将 MFA 状态作为属性传递给依赖方。

MFA 有多种选择，包括：

- 硬件令牌是物理设备，可产生一次性密码供人输入或需要插入读卡器。当需要最高级别的安全性时，这些是最好的选择。
- 软令牌的工作方式类似于硬件令牌，但通过手机或电脑上的软件应用程序来运行。软令牌也是一个很好的选择，但是如果用户的设备受到攻击，则可能会受到影响，并且在任何威胁模型中都需要考虑此风险。
- 带外密码是发送到用户手机（通常）的文本或其他消息，然后像令牌生成的任何其他一次性密码一样进行输入。虽然也是一个很好的选择，但任何威胁模型必须考虑消息拦截，特别是短信信息。
- 生物识别技术随着生物识别技术的普及，在移动手机上得到越来越多的应用。对于云服务，生物特征是本地保护手段，不向云提供商发送生物特征信息，而是可以发送给提供商的属性。因此，需要考虑本地设备的安全性和所有权。

对于客户来说，FIDO 是可以简化针对消费者的更强认证方式，同时减少摩擦的一个标准。

12.1.4 授权和访问管理

权利、授权、以及访问控制这些术语在含义上都有些重叠，根据上下文语义进行不同的理解。虽然在本节的前面已经进行了定义，我们这里做一个快速回顾。

授权是被允许做某事——访问某个文件或网络的权限，或在特定资源上执行特定函数，例如调用一个 API。

访问控制作为授权允许或拒绝的一种表现，它确保用户在被允许访问之前有经过相应的认证。

权利将身份映射到授权和任何必需的属性（例如，当 z 属性为设定值时，允许用户 x 访问资源 y ）。我们通常将这些权利的映射引用为权利矩阵。权利通常被编码为分发和执行的技术策略。

这只是这些术语某一方面的定义，你可能会发现在其他文档中使用场景不一样。类似地，我们使用 IAM 中的“A”表示访问管理，涉及到定义、传播、强制授权等整个流程。

Entitlement	Super-Admin	Service-1 Admin	Service-2 Admin	Dev	Security-Audit	Security-Admin
Service 1 List	X	X		X	X	X
Service 2 List	X		X	X	X	X
Service 1 Modify Network	X	X		X		X
Service 2 Modify Security Rule	X	X				X
Read Audit Logs	X				X	X

授权矩阵样例

这里我们举一个真实情况下的云的案例。云提供商提供了一个用于启动新虚拟机的 API，该 API 有一个相应的授权，允许启动新的虚拟机，但需要额外的授权选项明确用户可以在哪个虚拟网络中启动虚拟机。云管理员创建了一个权利，在开发组中的用户可以在他们的项目网络中，经过多因素认证后，可以创建虚拟机。该组和使用 MFA 进行认证是该用户身份的属性。该权利作为一个政策被写入到云提供商的系统中强制执行。

云以多种方式影响权利、授权和访问管理：

- 云提供商和平台，像任何其他技术一样，具有一套自身的潜在授权机制。除非提供者支持 XACML（少见），否则云消费者通常需要在云平台上直接配置权利。
- 云提供商负责强制授权和访问控制。
- 云消费者负责定义权利并在云平台中正确配置它们。
- 云平台倾向于对基于属性的访问控制模型提供更大的支持，对于 IAM，它比基于角色的访问控制模型提供更大的灵活性和安全性。RBAC 是传统的模型，用于执行授权，通常依赖于一个单一的属性（定义的角色）。ABAC 允许更细的颗粒度以及结合语境的多属性决策，如角色、位置、认证方法等。
 - ABAC 是基于云的访问管理的首选模式。
- 当使用联邦时，云消费者负责向云提供商提供映射属性，包括角色和组，并确保这些在认证过程中得到合理沟通。

- 云提供商负责支撑细粒度属性以及授权以确保 ABAC 以及云消费者的有效安全。

12.1.4 特权用户管理

在控制风险方面，没有什么事情比特权用户管理更重要。前面所提到的强认证方式应该作为特权用户管理重点考虑的一点。此外，应该实施账户和会话记录以推动特权用户的审计和透明度。在某些情况下，使用一个更高水平保证措施，如凭证控制，数字证书，物理和逻辑上独立的访问控制点，以及堡垒机等单独严格控制的系统，对特权用户的登录行为进行控制更为有益。

12.2 建议

- 组织应制定一个全面和正式的计划和管理云服务的身份和授权。
- 当连接到外部云服务提供商时，如果可能，使用联邦来扩展现有的身份管理。尽量减少云提供商中与身份不一致的身份信息。
- 酌情考虑适当的使用身份代理。
- 云消费者负责维护身份提供者并定义身份和属性。
 - 这些应以授权源为基础。
 - 当内部部署选项不可用或不符合要求时，分布式组织应考虑使用云托管目录服务器。
- 云消费者对所有外部云帐户应优先选择 MFA，并发送 MFA 状态作为联合身份验证时的属性。
- 特权身份应始终使用 MFA。
- 为每个云提供商和项目制定权利矩阵，重点是元结构和/或管理界面的访问。
- 当云提供商或平台支持时，将权利矩阵转换为技术策略。
- 对于云计算，相对 RBAC，应优先考虑 ABAC。
- 云提供商应使用开放标准提供内部和联邦身份。
- 没有魔术协议：首先选择您的场景和约束条件，然后找到正确的协议。

D13: 安全即服务

13.0 介绍

虽然本指南的大部分内容是关注保护云平台 and 云部署，但本域内容将转移到涵盖从云端提供的安全服务。这些服务（通常是 SaaS 或 PaaS 服务）不一定只用于保护云部署；他们同样有可能帮助保护传统的本地部署的基础设施。

安全即服务（SecaaS）提供商提供安全能力作为云服务。这包括专门的安全即服务提供商以及通用云计算提供商自带的安全特性。安全即服务涵盖了广泛的各种可能的技术，但必须符合以下标准：

- SecaaS 包括通过云服务方式提供的安全产品或服务。
- 要被视为 SecaaS，其服务必须满足域 1 中提及的美国国家标准与技术研究院（NIST）的云计算基本特性。

本节重点介绍市场上一些更常见的安全即服务类别，但 SecaaS 正在不断发展，以下描述和列表不应被视为规范。本文档中没有涵盖的示例和服务，将不断地进入市场。

13.1 概述

13.1.1 SecaaS 的潜在优势和问题

在深入了解不同的主要 SecaaS 类别的细节之前，了解 SecaaS 与本地部署安全、自我管理安全的区别是非常重要的。通过这样思考分析 SecaaS 潜在的好处和问题。

13.1.1.1 潜在优势

- **云计算优势。** 云计算的通常潜在优势（例如降低资本成本、敏捷性、冗余性、高可用性和弹性）都适用于 SecaaS。与任何其他云提供商一样，这些优势的大小取决于安全提供商的定价、执行和能力。
- **人员配置和专业知识。** 许多组织尽力地雇用、培训和保留安全相关领域的专业人士。

由于当地市场的局限性，专家的高昂成本以及日常需求的平衡，这种情况可能会加剧攻击者的创新。因此，SecaaS 提供商带来了广泛的领域知识和研究的好处，对于不仅只专注于安全性或特定安全领域的许多组织而言，这些领域知识和研究可能无法获得。

- **智能共享。** SecaaS 提供商同时保护多个客户，将有机会在客户相互间共享信息情报和数据。例如，在一个客户端中发现恶意软件样本允许提供商立即将其添加到其防御平台，从而保护所有其他客户。实际上这不是一个魔术棒，因为效果会有所不同，但是由于情报分享是内置在服务中的，所以具有潜在的好处。
- **部署灵活性。** SecaaS 可能会更好地支持不断发展的工作场所和云迁移，因为它本身就是使用互联网访问和弹性的云计算模式提供的。服务通常可以处理更灵活的部署模式，例如支持分布式位置而不需要复杂的多站点硬件安装。
- **客户无感知。** 在某些情况下，SecaaS 可以在组织受到攻击之前直接拦截攻击，例如，垃圾邮件过滤和基于云的 Web 应用程序防火墙部署在攻击者和组织之间。他们可以在达到客户资产之前处理某些攻击。
- **伸缩和成本。** 云模式为消费者提供了“按您的成长付费”模式，这也有助于组织专注于其核心业务，并将安全问题留给专家。

13.1.1.2 潜在问题

- **能见度不足。** 由于安全即服务的运行是从客户中迁移过来的，因此与运行自己的操作相比，它们往往提供较少的可见性或数据。SecaaS 提供商可能不会公开如何实现自身安全和管理自己的环境的细节。根据服务和提供商的不同，可能会导致数据源以及可获得的内容（如监视和事件）的细节程度的差异。客户的一些信息可能通常看起来有所不同、有差距或根本无法获取。合规性的实际证据和痕迹以及其他调查数据可能无法满足客户的目标。所有这都可以并且应该在达成任何协议之前确定。
- **监管差异。** 鉴于全球监管要求，SecaaS 供应商可能无法实现以确保组织在所有司法管辖区的合规。
- **处理监管的数据。** 客户还需要保证根据任何合规性要求处理任何受管制数据（这些数据可能被抽取作为常规安全扫描或安全事件的一部分）；这也需要遵守上述国际司法管辖权差异。例如，欧洲的员工监督比美国的监管更加严格，甚至基本的安全监控做法也可能违反该地区的工人权利。同样，如果 SecaaS 提供商迁移其业务，由于数据中心迁移或负载均衡，可能会违反在数据居住地区有限制的规定。
- **数据泄漏。** 与其它任何云计算服务或产品一样，一直存在数据从一个云消费者泄漏到另一个云消费者的顾虑。这种风险并不是 SecaaS 所特有的，但是安全性数据（以及安全扫描或事件中潜在的其他受监管数据）的高度敏感性确实意味着 SecaaS 提供商应该被保留多租户隔离和分段的最高标准。安全相关数据也可能涉及诉讼、执法调查和其他出示证据的情况。当这些情况涉及服务中的其它客户时，客户希望确保他们自身的数据不被暴露。

- **更换供应商。**虽然简单地切换 SecaaS 提供商比替换本地部署的硬件和软件可能在表面上更容易，但组织可能需要关注因锁定效应而丢失对数据的访问，包括遵守或调查支持所需的历史数据。
- **迁移到 SecaaS。**对于已经具有安全操作和本地部署的传统安全控制解决方案的组织，迁移到 SecaaS 以及任何内部 IT 部门和 SecaaS 提供商之间的边界和接口，必须进行良好的计划、实施和维护。

13.1.2 现提供的安全即服务主要分类

现在有大量的产品和服务都称为安全即服务。虽然以下不是一份权威的列表，但它描述了许多在写这篇文章时看到的更常见的类别：

13.1.1.1 身份，授权和访问管理服务

身份即服务是涵盖可能组成一个身份生态系统的一个或多个服务的通用术语，例如策略执行点（PEP-as-a-service）、策略决策点（PDP-as-a-service）、策略接入点（PAP-as-a-ervice）、为实体提供身份的服务、提供属性的服务（例如多因素身份验证），以及提供信誉的服务。

在云安全中大量使用的知名类别之一是联合身份代理（Federated Identity Brokers）。这些服务帮助组织在现有身份提供商（内部或云托管目录）与组织使用的许多不同云服务之间建立 IAM。他们可以提供基于 Web 的单点登录（SSO），这有助于降低连接到使用不同联盟配置的各种外部服务的一些复杂性。

云部署中还有其他两个常见的类别。强身份验证服务使用应用程序和基础设施来简化各种强身份验证选项（包括移动设备应用程序和多因素访问令牌）的集成。在云中，另一个类别是作为组织身份提供者的主机目录服务器。

13.1.1.2 云访问安全代理（CASB，又称云安全网关）

此类产品拦截直接连接或通过 API 连接到云服务的通信，以便监视活动、执行策略、以及检测和/或防止安全问题。它们最常用于管理组织的授权和未经授权 SaaS 服务。虽然有本地部署的 CASB 方案，但它也经常提供为云托管服务。

CASB 还可以连接到本地工具以帮助组织检测、评估和可能阻止云服务使用和未经批准的服务。许多这些工具包括风险评估功能，可帮助客户了解和分类数百或数千个云服务。评级是基于供应商评估的组合，可以加权并与组织的优先级相结合。

大多数提供商还为覆盖的云服务提供基本的数据防丢失功能，内置地或通过与其他服务的合作和集成。

根据组织现在讨论的“CASB”，该术语有时也用于包括联合身份代理。这可能令人困惑：虽然“安全网关”和“身份代理”功能的组合是可能的并确实存在，但市场仍然主要以独立服务提供这两个功能。

13.1.1.3 Web 安全（Web 安全网关）

Web 安全包括实时保护，通过软件和/或设备安装提供本地化部署或者通过将 Web 流量代理或重定向（或两者混合）到云提供商来提供服务。这为其他保护提供了一层额外的保护，例如防恶意程序软件以防恶意程序通过诸如网页浏览入侵企业。此外，它还可以强制执行关于 Web 访问类型和允许访问的时间段的策略规则。应用程序授权管理可以为 Web 应用程序提供更多级别的细粒度和上下文的安全执行机制。

13.1.1.4 电子邮件安全

电子邮件安全应该提供对进站和出站电子邮件的控制，保护组织免受网络钓鱼和恶意附件等风险的影响，并实施可接受的使用和垃圾邮件防范等公司政策，并提供业务连续性选项。

此外，该解决方案还可以支持基于策略的电子邮件加密以及与各种电子邮件服务器解决方案的集成。许多电子邮件安全解决方案还提供一些功能特性，如类似实现身份识别和不可否认性的数字签名功能。该类别包括全面的服务，从简单的反垃圾邮件功能到全面集成的电子邮件安全网关（具有高级恶意程序和网络钓鱼保护）。

13.1.1.5 安全评估

安全评估是通过云方式提供对云服务的第三方或客户驱动的审核或对本地部署系统的评估的解决方案。基础设施、应用程序和合规性审核的传统安全评估有明确的定义和各种标准的支持（如 NIST、ISO 和 CIS）。相对成熟的工具集已经出现，并且一些使用 SecaaS 为交付模式的工具已经实现。使用该模式，用户获得了云计算的典型优势：多样化的弹性、可忽略不计的部署时间、管理费用低，以及初次投资低的付费方式。

安全评估有三大类：

- 在云中部署的资产的传统安全/漏洞评估（例如虚拟机/实例的补丁和漏洞）或本地化部署。
- 应用安全评估，包括 SAST、DAST 和 RASP 的管理。
- 通过 API 直接与云服务连接的云平台评估工具，不仅可以评估部署在云中的资产，还可以评估云配置。

13.1.1.6 Web 应用程序防火墙（WAF）

在基于云的 Web 应用程序防火墙（WAF）中，在将流量传递到目标 Web 应用程序之前，客户先将流量（使用 DNS）重定向到分析和过滤流量的服务。许多云 WAF 还包括反 DDoS 功能。

13.1.1.7 入侵检测/防御（IDS / IPS）

入侵检测/防御系统使用基于规则、启发式或行为模型来检测可能对企业造成风险的异常活动。使用 IDS / IPS 作为服务，信息将提供给服务提供商的管理平台，而不是由客户自己负责事件分析。云 IDS / IPS 可以使用本地化安全的现有硬件、云中的虚拟设备（有关限制请参阅域 7）或基于主机的代理。

13.1.1.8 安全信息与事件管理（SIEM）

安全信息和事件管理（SIEM）系统聚合（通过推或拉机制）来自虚拟和物理网络、应用程序和系统的日志和事件数据。然后将该信息去噪并分析，以提供可能需要人工干预或其他类型的响应的信息或事件的实时报告和警报。云 SIEM 通过云服务收集这些数据，而不是由客户管理的本地系统。

13.1.1.9 加密和密钥管理

加密和密钥管理服务提供加密数据和/或加密密钥管理服务。它们可能由云服务提供以支持客户管理的加密和数据安全。它们可能仅限于保护该特定云提供商中的资产，或者可以跨多个提供商访问（甚至通过 API 本地化部署）进行更广泛的加密管理。该类别服务还包括用于拦截 SaaS 流量来加密离散数据的 SaaS 加密代理。

然而，在 SaaS 平台之外加密数据可能会影响平台利用相关数据的能力。

13.1.1.10 业务连续性和灾难恢复

云业务连续性和灾难恢复服务提供商将数据从单个系统、数据中心或云服务备份到云平台，而不是依赖本地存储或运送磁带。客户可以使用本地网关来加速数据传输和本地恢复，使用此类云服务作为最坏灾难情况或存档目的的最终存储库。

13.1.1.11 安全管理

这些服务将传统的安全管理功能（如终端保护、代理管理、网络安全、移动设备管理等）集成到单个云服务中。这减少或消除了对本地管理服务器的需求，并且可能特别适合于分布式组织。

13.1.1.12 分布式拒绝服务保护

大多数 DDoS 保护本质上都是基于云的。它们通过将流量重定向路由到 DDoS 服务来实现，以便在影响客户自己的基础架构之前吸收攻击。

13.2 建议

- 在确定 SaaS 提供商之前，请务必了解数据处理（和可用性）、调查和合规性支持的任何安全性要求。
- 特别注意处理受监管的数据，如个人身份信息保护（PII）。
- 了解您的数据保留需求，并选择支持输入的数据不会产生锁定情况的提供商。

- 确保 SecaaS 服务与您当前和未来的计划兼容，例如其支持的云（和本地部署）平台、接受的工作站和移动操作系统等。

CSA GCR cloud security
GREATER CHINA REGION alliance®

D14: 相关技术

14.0 简介

在本指南中我们专注于提供直接保护云计算的背景信息和最佳实践。但作为一项基础技术，还有各种其他相关技术也会带来各自特有的安全问题。

尽管描述云计算所有的潜在用途已经远远超出了本文的范围，但是云安全联盟认为云计算相关关键技术的背景和建议是非常重要的。例如 **Container** 容器技术和软件定义网络技术（SDN）等与云计算紧密相关的内容，我们将分别在本指南中的其他章节中描述。本章更多的是关注那些与现有章节不紧密相关的其他技术。

把这些技术放在单独的章节有助于在这些技术的使用发生变化和拥有新特性时更新、添加和删除相关内容。

14.1 概要

相关技术可分为两大类：

- 几乎完全依赖云计算来操作的技术。
- 不一定依赖云，但在云部署中常见的技术。

这并不是说这些技术在没有云的情况下无法工作，只是它们经常是搭接或依赖于云部署，因此它们对大多数云安全专业人员都有影响。

当前列表内容包括：

- 大数据
- 物联网(IOT)
- 移动设备
- 无服务器计算

目前，云安全联盟的其他工作组有多个正在进行的项目和出版物中包含了这些技术：

- 大数据工作组
- 物联网工作组
- 移动工作组

14.1.1 大数据

大数据包括用于解决传统数据处理工具无法处理的超大数据集的一组技术，它不是任何单一的技术，而通常指的是分布式的集合、存储和数据处理框架。

Gartner 将其定义为：“大数据是需要新处理模式才能具有更强决策力、洞察发现力和流程优化能力来适应海量、高增长率和多样化的信息资产。”

“3Vs” 尽管有很多的解释，但通常被认为是大数据的核心定义：

- 高海量化：记录或属性的数据体量非常大。
- 高快速化：数据的快速生成和处理，例如实时数据或流数据。
- 高多样性：结构化、半结构化或非结构化数据。

云计算由于它的弹性和巨大的存储能力，经常出现在部署大数据项目的地方。大数据并不是云计算的专有技术，但大数据技术通常被集成到云计算应用中，并由云服务提供商以 IaaS 或 PaaS 的形式提供服务。

如不考虑具体的工具集，大数据有三个共同的组成部分：

- 分布式数据收集：用于摄取大量数据的机制，通常是流媒体的性质。这可能是“轻量级”的，如 web 点击流分析；也可能是复杂的，如高度分布式的科学成像或传感器数据。并非所有的大数据都依赖于分布式或流媒体数据收集，但它是一项核心的大数据技术。
- 分布式存储：在分布式文件系统(如 Google 文件系统、Hadoop 分布式文件系统等)或数据库(通常是 NoSQL)中存储大型数据集的能力，由于非分布式存储技术的局限性，这种能力通常是必需的。
- 分布式处理：用于有效地分析单个源处理无法处理的、大规模且快速变化的数据集，且拥有分布式处理作业能力的工具（如 MapReduce, Spark 等）。

14.1.1.1 安全性和隐私方面的考虑

由于大数据应用（数据收集、存储和处理均分布在不同的节点中）的高度分布性质，可能存在大量潜在的敏感信息。安全和隐私通常是最先考虑的，但却需要接受不同工具和平台的挑战。

14.1.1.2 数据收集

数据收集机制可能会使用需要适当保护的中间存储，该存储是将数据从收集转移到存储的一部分。即使主存储是安全的，对中间存储的检测依旧很重要，就像处理节点上的交换空间一样简单。例如，如果数据收集机制在容器或虚拟机中运行，则确保底层存储得到适当的保护。分布式分析/处理节点也可能使用某种需要额外安全保护措施的中间存储。例如，这可能是运行处理作业实例的卷存储。

14.1.1.3 密钥管理

由于分布式节点的特性，依赖于特定机制的密钥存储管理将变的非常复杂。现有的一些技术能够对大部分的大数据存储层进行恰当加密，这些技术与本指南中的 11 章“数据安全和加密”一致。复杂的因素是密钥管理需要解决将密钥发布到多存储和分析节点上的问题。

14.1.1.4 安全功能

并不是所有的大数据技术都有强大的安全能力。在某些情况下，云服务提供商的安全功能可以帮助弥补大数据技术的局限性。所有安全体系中都应该包含上述两者，而具体细节取决于所选技术的组合。

14.1.1.5 身份识别和访问管理

身份识别和访问管理（IAM）很可能出现在云计算和大数据工具级别，这可能会使授权矩阵复杂化。

14.1.1.6 PaaS

许多云服务提供商正在通过机器学习和其他平台扩展大数据支持，这是一种依赖于企业数据访问的服务选项。如果不完全了解潜在的数据泄露、合规性和隐私含义，就不应该使用这些数据。例如，如果机器学习在提供商的基础架构中作为 PaaS 运行，提供商的员工可以在技术上访问它，这是否会产生合规的风险？

这并不意味着您不应该使用服务，它只是意味着您需要了解隐含的含义并作出适当的风险决策。机器学习和其他分析服务并不一定是不安全的，也不一定违反隐私和合规承诺。

14.1.2 物联网(IoT)

物联网是使用互联网连接的物理世界中使用的非传统计算设备的总称。它包括了从互联网支持的运营技术(如电力和水)到健身追踪器、联网灯泡、医疗设备等等。这些技术越来越多地部署在企业环境中，例如：

- 供应链的数字跟踪。
- 实体物流的数字跟踪。
- 市场、零售和客户关系的管理。
- 为员工或客户提供相关的健康生活的应用。

这些设备中很大一部分连接到云计算基础设施，用于后端处理和数据存储。与物联网相关的关键云安全问题包括：

- 数据收集和清理的安全。
- 设备注册、身份验证和授权。当前遇到的一个常见问题是使用存储凭据对后端云服务提供程序进行直接的 API 调用。一些已知的案列表明，攻击者会对应用程序或设备软件进行反编译，然后使用这些凭证进行恶意攻击。
- 从设备到云服务基础设施的连接的 API 安全性。除了刚刚提到的存储凭证问题，API 本身可以被解码并用于对云服务基础设施的攻击。
- 加密通信。许多当前设备使用的是弱的、过时的加密方式或者不加密的方式，将数据和设备置于危险境地。
- 能够修补和更新设备，这样他们就不会成为妥协的焦点。目前，设备按原样发送，从来没有收到操作系统或应用程序的安全更新。这已经引起了许多重大的、广泛关注的

安全事件，例如基于受损的物联网设备的大规模僵尸网络攻击。

14.1.3 移动

移动计算既不是云计算的新技术，也不是云计算的专有技术，但很大一部分的移动应用程序都会连接到云计算平台用于后端处理。云可以作为支持移动计算的一个理想平台，因为云服务提供商是异地分布的，并且为移动应用程序中常见的高度动态的负载设计。本节不讨论所有的移动安全性，只讨论影响云安全的部分。

移动计算(在云环境中)的主要安全问题与物联网非常相似，除了移动电话或平板电脑也是一般用途的计算机：

- 设备注册、身份验证和授权是一个常见的问题源。特别是(再次)使用存储凭证，当移动设备直接连接到云服务提供商的基础架构/API 时尤为如此。众所周知，攻击者可以对移动应用程序进行反编译，以显示存储的凭据，这些凭据随后被用于直接操作或攻击云基础设施。存储在设备上的数据也应该受到保护，假设设备的使用者可能是一名恶意攻击者。
- 应用程序 API 也是缺陷的潜在来源。攻击者可以嗅探 API 连接，在某些情况下，使用本地代理将自己的设备重定向，然后反编译(可能是未加密的)API 调用，并发现它们的安全弱点。设备应用程序内的证书锁定/验证可以帮助降低这种风险。

关于移动和云计算安全的更多建议，请参见 CSA 移动工作组的最新研究。

14.1.4 无服务器计算

无服务器计算是对特定 PaaS 功能的广泛使用，以至于所有或部分应用程序堆栈都在云服务提供商的环境中运行，而不需要任何客户管理的操作系统，甚至是容器。

“无服务器计算”有点用词不当，因为总有一个服务器在某个地方运行负载，但是这些服务器及其配置和安全性完全对云计算用户隐藏。使用者只管理服务的设置，而不是任何底层的硬件和软件栈。

无服务器计算包括如下服务:

- 对象存储
- 云负载均衡器
- 云数据库
- 机器学习
- 消息队列
- 通知服务
- 代码执行环境(这些通常是受限制的容器,用户可以在其中运行上传的应用程序代码。)
- api 网关
- web 服务器

无服务器计算功能可能会被云服务提供商深度集成,并与事件驱动的系统、集成的 IAM 和消息传递绑定在一起,以支持复杂应用程序的构建,而客户无需对服务器、容器或其他基础设施进行任何管理。

从安全的角度来看,关键问题包括:

- 无服务器给云服务提供商带来了更高的安全负担。选择好您的云服务提供商并理解好安全性 SLA 和能力是非常重要的。
- 使用无服务器的云用户将无法访问常用的监视和日志记录级别,例如服务器或网络日志。应用程序需要集成更多的日志记录,云服务提供商应该提供必要的日志以满足核心安全和合规性需求。
- 尽管提供者的服务可以通过认证或测试来满足不同的合规性
- 需求不一定是每个服务都能匹配每个潜在的规则。提供者需要保持最新的合规性映射,并且客户需要确保他们只在他们的合规范围内使用服务。
- 由于这是集成和使用无服务器能力的唯一方法,所以对云服务提供商的管理层的访问将会非常高。
- 无服务器可以显著减少攻击的表面和路径,集成无服务器组件可能是在攻击链中断开链接的一种很好的方式,即使整个应用程序堆栈不是没有服务器的。
- 任何漏洞评估或其他安全测试都必须符合提供者的服务条款。云消费者可能不再有能直接测试应用程序,或者必须用更少的范围进行测试,因为提供者的基础架构现在已经承载了所有的东西,并且不能区分合法的测试和攻击。
- 事件响应可能也很复杂,并且肯定需要在过程和工具上进行更改,以管理基于服务器的事件。

14.2 建议

- 大数据
 - 尽可能利用云服务提供商的能力，即使它们与大数据工具安全功能有重叠。这将确保您在云的元结构和特定应用程序堆栈中有适当的保护。
 - 对数据收集和数据存储层中的主存储、中间存储和备份存储进行加密。
 - 在项目授权矩阵中包括大数据工具和云平台身份识别和访问管理（IAM）。
 - 充分理解使用云机器学习或分析服务的潜在好处和风险。特别注意隐私和合规性的含义。
 - ◆ 云服务提供商应采取管理和技术控制来确保客户数据不暴露给自己的员工或其他管理员。
 - ◆ 云服务提供商应该清楚地发布他们的分析和机器学习服务遵循的遵从标准(对于他们的客户)。
 - ◆ 当考虑到不符合安全性、隐私或合规性要求的服务时，云用户应该考虑使用数据屏蔽或混淆。
 - 遵循其他大数据安全最佳实践，包括工具供应商(或开放源码项目)和云安全联盟提供的那些最佳实践。
- 物联网
 - 确保设备可以进行修补和升级。
 - 不要将静态凭据存储在可能导致云应用程序或基础设施受损的设备上。
 - 遵循安全设备注册和对云应用程序的身份验证的最佳实践，通常使用联合身份标准。
 - 加密通信。
 - 使用安全的数据收集管道并进行数据清理，以防止通过对数据收集管道进行攻击从而利用云应用和云基础设施。
 - 假设所有 API 请求都是怀有恶意的。
 - 遵循由 CSA 物联网工作组发布的更多、更详细的指南。
- 移动
 - 在设计一个直接连接到云基础设施的应用程序时，请遵循您的云服务提供商的指导，以正确的身份验证和授权移动设备。
 - 使用行业标准，通常是联合身份，将移动设备应用程序连接到云托管的应用程序。
 - 不要在因特网上传输未加密的密钥或凭证。
 - 测试所有的 API 时都应该假设恶意攻击者具有身份验证、未加密的访问权限
 - ◆ 在移动应用程序中考虑证书固定和验证。

- ◆ 验证所有 API 数据并进行清理以确保安全。
 - ◆ 为恶意的 API 活动实现服务器/云端安全监视。
 - 确保存储在设备上的所有数据都是安全的和加密的。
 - 那些可能由于应用程序栈受攻击而导致泄露的敏感信息不能存储在本地设备上，因为恶意用户很可能访问到这些数据。
 - 遵循 CSA 移动工作组的更详细的建议和研究。
- 无服务器计算
 - 云服务提供商必须清楚地说明哪些 PaaS 服务是根据哪些法规遵循需求或标准进行评估的。
 - 云使用者必须只使用符合其合规性和治理义务的无服务器服务。
 - 考虑使用架构的方式将无服务器组件注入到应用程序栈中，以减少或消除攻击面和/或网络攻击路径。
 - 了解无服务器对安全评估和监控的影响。
 - ◆ 云用户需要更多地依赖于应用程序代码扫描和日志记录，而较少依赖于服务器和网络日志。
 - 云用户必须更新针对服务器部署的事件响应流程。
 - 尽管云服务提供商负责无服务器平台级别以下的安全，但云计算用户仍然需要正确配置和使用产品。