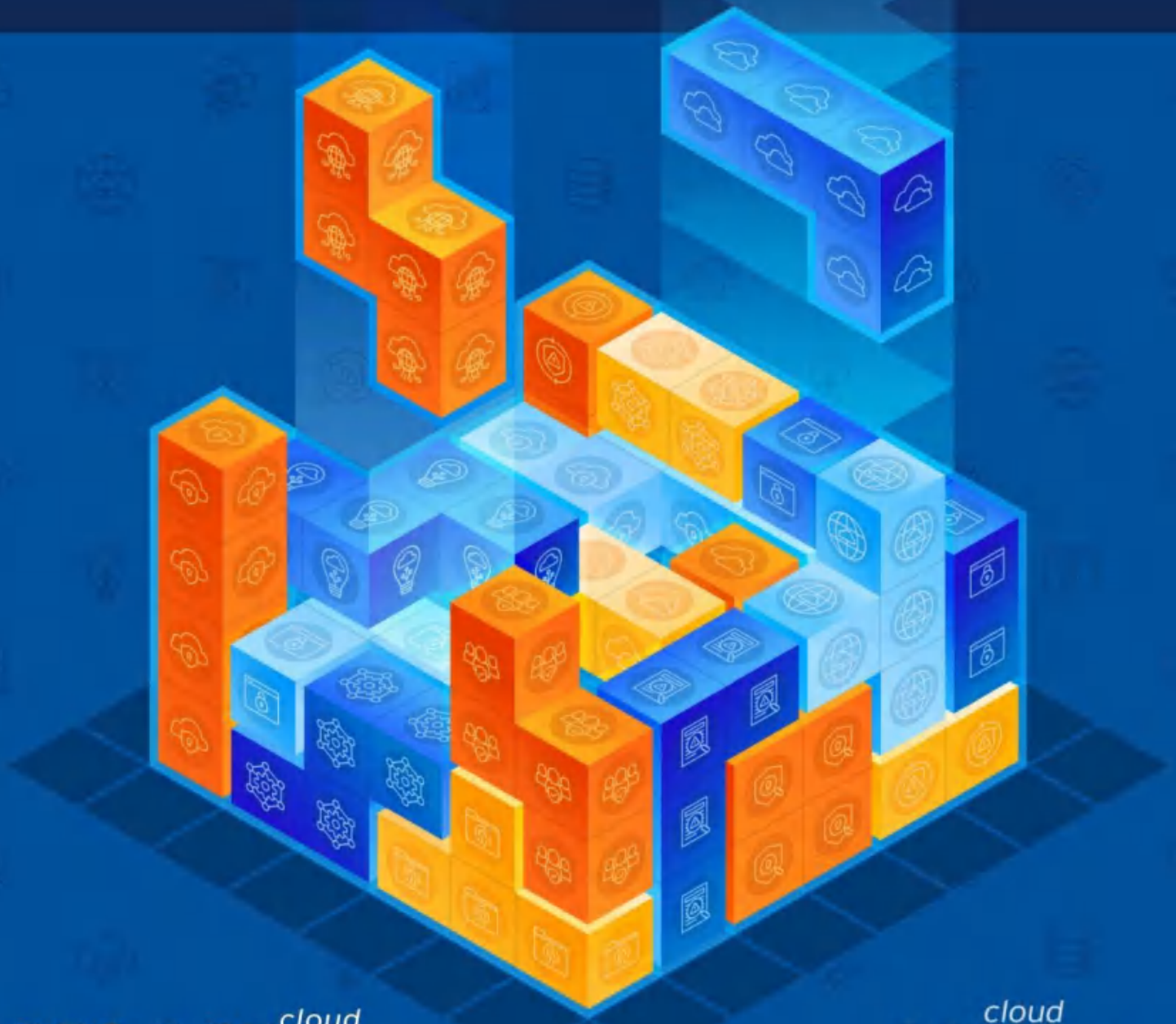
云计算关键领域安全指南v5



CSA GCR cloud security alliance GREATER CHINA REGION

CSA cloud security alliance

云安全知识认证CCSK

Certificate of Cloud Security Knowledge

是国际权威组织云安全联盟于2011年发布的认证项目，旨在为全球范围内的专业人士提供标准化的云安全知识体系。被译成六国语言，在全球广泛推广，被誉为“云计算安全认证之母”。

CCSK作为云计算领域面向个人的首个全球安全认证，全面覆盖了云安全的关键知识点，成为了云安全领域的个人认证基准。《云计算关键领域安全指南》作为 CSA 云安全知识认证（CCSK）国际网络安全认证的官方学习材料，为云计算用户、服务提供商及安全专家提供实用的安全策略，帮助他们在快速变化的云环境中有效地实施安全控制和防护措施。

致谢

《云计算关键领域安全指南 v5 》由 CSA 大中华区组织专家完成翻译并审校，感谢以下专家的贡献：

翻译组

李　岩	卜宋博	沈　勇	贺志生
江　楠	刘　通	米小亮	邢海韬
林　飞	王贵宗	杨　莉	党超辉

审校组

郭鹏程	罗智杰	高林杰	刘广坤
屈　伟	吴　满	马维士	徐　岩
何诣莘	陆　琪	范淑杰	张元恺
刘竞雄	李默涵	赖杨健	丁安安
白黎明	李卓嘉	李晓辉	应天元
夏　威	刘国强	胡志辉	林艺芳
高亚楠	杨喜龙	李来冰	高毅昂
杨天识	廖立澄	周耀明	浦　明
赵晨曦	袁荣婷	赵晨明	闭俊林
易利杰	黄家栋		

英文版编写专家

主要作者

Rich Mogull

Mike Rothman

贡献专家

Jackie Donnelly

Moshe Ferber

Larry Hughes

Michael Roza

Peter van Eijk

审稿人

Mohammad Aamir

Frank Addo

Daniel Adjorlolo

Hafiz Ahmed Sheikh Adnan

Ilango Allikuzhi

Shonnie Almeida J.

Babs Alo

Aakash Alurkar

Agbu Amachundi Enoch

Stephen Amolo

Divya Aradhya

Robyn Bailey

Adeel Bakht

Suramya Bakshi

Mohamed Balushi Al

Vinay Bansal

Robin Basham

Myriam Batista

Allen Baylis

Renu Bedi

Paul Benedek

Bachir Benyammi

Jamie Beth

Shirin Bhambhani

Roberto Bonalumi

Karl Brooks

Jasper Brouwer

Amit Butail

Varun Carlay

Dhanushraj Chandrahasan

Senthilkumar Chandrasekaran

Akshay Chandrasekaran Sekar

Shankar Chebrolu

Anand Chirathadam Abraham

John Chiu

Anand Choksi

Vipul Dabhi

Joseph Dacuma
Michel-Ange Dagrain
Thomas Defise
Neelima Devana
Mankirat Dhodi Singh
Balaram Dhulipudi
Dr. Ivan Djordjevic
Ivan Djordjevic
Moses Dlamini
Keinaz Domingo N.
David Dorsey
Rob Doyon
Vinay Dubey
Swapna Dulganti
Nielet D'Mello
Mohamed Elbashir
Mahmood Elrefai
Joseph Emerick
Dr. Marco Ermini
Kingsley Ezeocha
Ahmed Fawzy
Lorena Ferreyro
Kenneth Ferris
Jonathan Fessenden
Jose Figueredo-Maseda C.
Elaine Flesch
Fernando Fonseca
Park Foreman
Adame Frances
Aadithya Francis
André Gaio Alexandre
Luca Gattobigio
Viktor Gazdag
Jan Gerst
Hussein Ghazy
Tulika Ghosh
Ricardo Giorgi
Andriana Gkaniatsou
Saurabh Goswami
Trevor Gregorio
Nageswara Gude Rao
Madhu Guthikonda
Ahmed Harris
Lyle Hearne
Johnny Hernandez
Dirce Hernandez Eduardo
Aldo Hernández Villaseca
Moreno Hill Sint
Matthew Hoerig
Abdulsalam Ibrahim B.
Ricci Ieong
Frank Iheonu
Arron Johnson
Rahul K
Prasannakumar K G
Patrick Kabongo B.
Nithin Kadumberi Mohan Thattiot
Ruchi Kandpal

Sivakumar Karthikeyan
Shakthi Kathirvelu Priya
Sunil Katwal
Arpitha Kaushik
Alon Kendler
Rohit Khosla
Vana Khurana
Jari Kiero
Brenda Killingsworth L.
Morgan King
Samantha Kloos-Kilkens
Simon Kok
Vivek Krishnan
Sunil Kumar
Francois Laas
Hadir Labib
Daniel Lai
Raymond Lai
Law Lain Chamber
Sundas Latif
Seshagirirao Lekkala
Yutao Ma
Stephen Macomber
Yuvaraj Madheswaran
Niclas Madsen
Ahmed Mahmoud Nabil
Vaibhav Malik
Mohamed Malki
Cecil Martin
Marcus Maxwell
Bilal Mazhar
Mark McDonagh
José Medina Carlos Vargas
Santiago Medranda
Ashish Mehta
Shobhit Mehta
Andre Mess
Enida Metaj
Akhil Mittal
Adeeb Mohammed
Victor Monga
Kenneth Moras
Masahiro Morozumi
Andrew Morrow B.
Venkata Nedunoori
Harry Ngai
Fredrick Ogonda
Esborn Okero
Opeyemi Onifade
Joseph Orsetto
John Oseh B.
Jed Owens
Iyiola Oyinloye
Mayur Pahwa
Govindaraj Palanisamy
Meghana Parwate
Vaibhav Patkar
Martino Pavone

Eric Peeters

Eliza Popa

Kunal Pradhan

Ramon Domingo Quimesó

Adnan Rafique

Sonali Rajesh ZolT R

Marappan Ramiah

Alex Rebo

Aldo Richner

Rangel Rodrigues

Vishakha Sadhwani

Shahid Saleem

Joshua Salvador

Mukund Sarma

Patnana Sayesu

Davide Scatto

Thomas Schmidt

Michael Schmitz

Kg.Seow

Vikrant Shah

Rakesh Sharma

Alex Sharpe

Akshay Shetty

Dr. Ian Silvester

Ryan Simon

Gurpratap Singh

Gaurav Singh

Anamika Singh

Serenity Smile

Heinrich Smit

Jorge Soboredo González

Silvano Sogus

Mikhail Sokolov

Dr. Chantal Spleiss

Dr. Manish Srivastava Kumar

Kevin Stander

Roy Stultiens

Yuanji Sun

Pratibha Swamy

Manjunath T A

Mohammed Tanveer

Billy Teow

Kim Tham Fui

Timothy Thatcher

Michael Theriault

Larry Timmins

Chee Tiong

Ilia Tivin

Wiem Tounsi

Micheal Troutman

Nsikak-Abasi Una Shammah

Pieter VanIperen

Ashish Vashishtha

Peter Ventura

Vaishnav Vijayakumar

Antonio Villamor Magallanes Jr

Alex Webling

Henry Werchan

Udith Wickramasuriya

Pawel Wilczynski

Rini Wilson

Wai Kong Wong

Ben Woods

Ezra Woods

James Yankelvich

Tsutomu Yoneyama

Bader Zyoud

Dennis de Caes

Peter van Loon

Tiaan van Schalkwyk

Cion Mensidor

Hannah Rock

Andy Ruth

Anna Schorr Campbell

Stephen Smith

Adriano Sverko

John Yeoh

CSA 全球员工

Judy Bagwell

Hillary Baron

Marina Bregkou

Josh Buker

Daniele Catteddu

Emily Everett

Ryan Gifford

Frank Guanco

Sean Heide

Erik Johnson

Alex Kaluza

Claire Lehnert

Stephen Lumpe

序言

《云计算关键领域安全指南 v5》由云安全联盟（CSA）于 2009 年首次发布，成为了全球实施云安全的必备手册，为云计算用户、服务提供商及安全专家提供实用的安全策略，帮助他们在快速变化的云环境中有效地实施安全控制和防护措施。作为 CSA 云安全知识认证（CCSK）国际网络安全认证的官方学习材料，云安全指南已被翻译成六种语言，成为全球网络安全从业者的经典教材。

本指南深入探讨了包括云架构、云原生安全、工作负载、虚拟网络、安全数据管理、DevSecOps、零信任模型、生成式 AI 等最新技术领域。它不仅涵盖了当前云环境中的核心安全要素，还提供了关于风险管理、合规性实现、优化组织云安全策略、以及理解责任共担模型等关键问题的宝贵见解。

2024 年，云安全联盟迎来了成立 15 周年的重要里程碑。在过去的 15 年里，CSA 始终致力于推动全球云安全的最佳实践，聚焦云计算领域的安全保障。第五版安全指南不仅进一步夯实了迈向云安全 3.0 时代的坚实基础，也为企业应对最新的云计算安全挑战提供了宝贵指导。

在中国，云计算应用正进入全新的发展阶段，云安全的紧迫性愈加凸显。第五版安全指南将为企业在云安全转型过程中提供切实可行的参考，帮助他们在复杂的云环境中实现安全合规，同时推动创新与业务增长。CSA 期待与更多企业和安全专家携手合作，共同推动云计算安全领域的持续进步，共同构建更加安全、可靠的云计算环境。

李雨航 Yale Li
CSA 大中华区主席兼研究院院长

云安全指南 v5 简介

欢迎阅读云安全联盟（CSA）《云计算关键领域安全指南 v5》（简称“安全指南”）。云计算作为一项不断发展的技术，带来了许多机遇和挑战。通过本文档，我们旨在为企业提供指导和启发，支持业务目标，同时管理和缓解采用云计算技术所带来的风险。

云安全联盟推动在云计算领域实施最佳实践，以提供安全保障，并为那些寻求采用云计算范式的组织提供了切实可行的路线图。第五版安全指南建立在此前版本、安全领域的专门研究以及云安全联盟成员、工作组和业内专家的公开参与基础上。本版本融合了云计算、安全性以及相关技术的最新进展；回顾了实际的云安全实践；整合了最新的云安全联盟研究项目；并为相关技术提供了指导。

迈向安全云计算的进步需要全球范围内各方利益相关者的积极参与。CSA 汇聚了来自不同领域的合作伙伴、国际分会、工作组以及个人。我们深感感激所有为本次发布做出贡献的人们。

请访问 cloudsecurityalliance.com，了解如何与我们合作，识别并推广最佳实践，以确保云计算环境的安全。

此致，

敬礼！

Jim Reavis

云安全联盟首席执行官

Illena Armstrong

云安全联盟总裁

目 录

领域 1：云计算概念和架构

该领域为云安全联盟(CSA) 安全指南的其它章节内容提供了概念性的框架。它描述和定义了云计算，列出了基本术语，并详细说明该文档其余部分所使用的整体控制、部署和架构模型。

云计算可以从多个视角来审视，其可以是一项技术、一组技术的组合、一种运营模式（或模型）、商业模式（或模型），或者是一种经济范式。云计算对传统计算系统具有变革性和颠覆性，它已经成为主导的数字化转型模型。尽管云安全联盟早期版本中的参考模型仍然相关，但它们需要更新以反映持续的进步（例如，来自云服务提供商（CSP）的新工具和技术、零信任、人工智能以及不断发展的实践），随着行业的成熟。这些更新虽然必要，但仍无法完全涵盖未来几年自动化和人工智能能力的快速发展。

云计算可以提供显著的敏捷性、韧性、安全性和经济效益。然而，这些好处只有在正确理解并采用云模型，且云架构和实践与云平台的特点和能力相一致的情况下，才能得以体现。如果云客户（CSC）通过将现有应用程序或资产直接迁移到 CSP（即“重新托管”或“提升和迁移”）而没有任何变更，通常无法提供预期的敏捷性、韧性和安全性，且可能增加成本。简而言之，云计算的好处与正确理解云计算模型、云原生能力和服务的适当使用紧密相关。

本领域旨在建立其余指南和建议的基础。其目的是提供云计算的共同语言和理解，同时突出云计算与传统计算之间的差异。除了已经提到的云计算好处外，本领域还将帮助云安全专业人员及其他相关利益相关者采纳确保更好安全态势的云计算方法。

云安全联盟并不打算创建一个全新的分类法或参考模型。我们的目标是提炼并协调现有的模型——特别是《NIST SP 800-1452》、《ISO/IEC 22123-1:20233》和《ISO/IEC 22123-2:20234》的工作——关注云计算领域专业人员最相关的安全考虑。

为了进一步增强对基本原则的理解，并探讨实施云安全实践的具体主题和实际策略，本指南提供了附加参考资料。

学习目标

在此领域，您将学习：

- 云计算的定义
- 识别云计算模型
- 识别云计算中的参考架构和架构模型
- 了解云安全的范围、责任划分和模型

1.1 定义云计算

云计算是一种运营模型和一组技术，用于通过对计算、网络、存储等资源的抽象来管理共享资源池。云模型设想了一个世界，其中组件和资源可以快速协调、配置、实施、按需扩展或缩小，并且能够退役，从而提供类似公用事业的按需分配和消费模型。其好处包括利益相关者的协作、敏捷性、弹性、可用性、复原力和成本减少。

以下是来自美国国家标准与技术研究院(NIST) 和国际标准化组织(ISO)和国际电工委员会(IEC)关于云计算的定义：

NIST SP 800-145 将云计算定义为一种模型，用于实现对可配置共享计算资源(例如，网络、服务器、存储、应用和服务）池无处不在的、便捷的、按需的网络访问，可以通过最少的管理工作或服务提供商交互来快速供应和释放资源。

ISO/IEC 22123-1:2023 将云计算定义为一种范式，它能够实现通过网络访问可扩展且具弹性的可共享的物理或虚拟资源池，并可按需进行自助式资源调配和管理。

简而言之，云计算将一组资源（如处理器和内存）放入一个大型资源池（通常通过虚拟化技术实现）。云客户（CSC）根据需求（例如：8 个 CPU 和 16GB 内存）从资源池中请求所需的资源。底层的云计算技术将这些资源协调分配给 CSC，后者通过网络连接并使用这些资源。当 CSC 使用完资源后，可以将其释放回资源池供他人使用。

云可以由几乎任何计算资源组成，从处理器、内存和网络等原始基础设施资源，到更高级的软件资源，如数据库和应用程序。例如，为 500 名员工订阅一个客户关系管理（CRM）应用程序，使用一个由成百上千组织共享的服务，这和在计算云上启动 100 台远程服务器一样，都是云计算的一部分。

1.1.1 抽象与编排

云环境的关键概念是抽象和编排。资源从底层物理基础设施中抽象出来，形成资源池；而编排（及自动化）用于协调、分配和交付资源池中的资源给 CSC。内在的标准化水平确保所有 CSC 基本上获得相同的功能服务，并以灵活的方式集成这些服务。如您所见，这两个概念构成了我们定义“云”的所有基本特征。

云本质上是多租户的。多个 CSC 共享同一个资源池，但它们通常在逻辑上，甚至在物理上，彼此隔离。隔离使得 CSP 能够将资源分配给不同的 CSC，并确保它们无法查看或修改彼此的资产，这对于确保 CSC 数据的机密性和完整性至关重要。此外，CSP 能够衡量和约束资源的过度使用，这对于服务的民主化使用和向每个 CSC 提供服务的可用性至关重要。多租户不仅限于跨组织使用，还可以促进在单个组织内不同单位之间的资源分配，这通常被称为“私有云”。

1.2 云计算模型

云安全联盟采用 NIST SP 800-145 模型作为云计算的标准定义。CSA 还支持更详细的 ISO/IEC 22123-1:2023 和 22123-2:2023 模型，它们也作为参考模型。在本领域中，我们将同时引用这两种模型。

NIST 根据五个基本特征、三个云服务模型和四个云部署模型来描述云计算，下面的章节将对这些内容进行总结。

图 1：基于 NIST 和 ISO/IEC 标准的云计算模型概述

1.2.1 云服务模型

NIST 模型通过五个基本特征来描述云，这些特征将云计算与传统托管服务或其它类型的云服务（如托管和虚拟化）区分开来。了解这些特征对于充分利用云计算的潜力和制定云所采用的战略规划至关重要。

以下是 NIST 描述的五个基本特征。

- **资源池化：**云计算通过多租户模型将各种物理和虚拟资源进行池化，用于服务多个 CSC（云客户）。这些资源，例如存储、处理器、内存和网络带宽，会根据需求动态分配和重新分配。
- **广泛的网络访问：**服务可以通过网络访问，并通过 Web 浏览器或专用应用程序进行访问，从而支持多种异构客户端平台（例如服务器、移动电话、笔记本电脑、物联网设备和平板电脑等）。
- **快速弹性：**资源可以快速、弹性地进行配置，在某些情况下，甚至可以自动完成，以便快速向外扩展或收回。对于 CSC 来说，提供的能力通常看起来是无限的，并且可以在任何时候以任意数量购买。

● **计量服务：**云系统通过某种适当的抽象层次自动控制和优化资源使用（例如存储、带宽、活跃用户帐户等）。资源使用可以被度量、监控、控制和报告，提供透明度给 CSP 和 CSC，能够根据使用量进行计费，促进了成本效益和责任感（例如按需付费模式）。

● **按需自助服务：**CSC 可以单方面的按需请求云资源，由 CSP（云服务提供商）自动进行配置，并根据需要提供计算能力，例如 CSC 可自动获得所需计算的运行时间和网络存储量，而无需与每个 CSP 进行人工交互。

ISO/IEC 22123: 2023 列出了六个关键特性，前五个与上面列出的 NIST 特性相同。唯一的新增特性是多租户，它与资源池化不同。

1.2.2 云服务模型

NIST 定义了三种服务模型，分别描述了云服务的不同基础类别：

● **软件即服务 (SaaS)：**是由 CSP 管理和托管的应用程序。CSC 使用Web 浏览器、移动应用程序、应用程序编程接口 (API) 或轻量级客户端应用程序访问它。在此模型中，CSC 只关心应用程序的配置，而不关心底层资源。

● **平台即服务 (PaaS)：**抽象并提供平台，例如应用程序平台（即可执行开发和运行代码的地方）、数据库、文件存储和协作环境。其它示例包括用于机器学习、大数据处理或支持 SaaS 功能的 API 访问的应用程序处理环境。与 SaaS 不同，PaaS 允许 CSC 管理底层平台，但不需要管理虚拟基础设施。

● **基础设施即服务 (IaaS)：**提供对基础计算资源池的访问，例如网络或存储。在 IaaS 中，CSC 负责管理底层虚拟基础设施，如虚拟机、网络、存储和运行的应用程序。

ISO/IEC 22123-3:2023 使用了更复杂的定义，将云能力类型与 SaaS、PaaS 和 IaaS（也称为 SPI）服务模型层（应用、平台和基础设施能力类型）紧密关联。它进一步扩展到云服务类别，如通信即服务（CaaS）、网络即服务（NaaS）、数据存储即服务（DSaaS）和数据恢复即服务等。

这些类别具有一定的渗透性；一些云服务跨越了 SPI 层，而其他云服务则无法严格划分为单一服务模型。实际上，没有必要将所有服务都归入这三大类，或 ISO/IEC 模型中的更细粒度类别。这是一个描述工具，而不是严格的框架。

两种方法都是有效的，但由于 NIST 模型更加简洁且广泛使用，它是 CSA 研究中主要采用的定义。

1.2.3 云部署模型

NIST 和 ISO/IEC 使用相同的四种云部署模型；这些模型描述了技术的部署、消费和应用方式，涵盖了所有服务模型。

- **公有云：**云基础设施向公众或大型行业集团开放，并由 CSP 拥有。
- **私有云：**云基础设施仅供单个组织运营。它可能由组织或第三方管理，并可以位于本地或托管在外。
- **社区云：**云基础设施由多个组织共享，支持具有共同关注点的特定社区（例如，使命、安全要求、政策、合规要求）。它可以由 CSC（或多个 CSC）或第三方管理，且可以位于本地或托管在外。
- **混合云：**云基础设施由两个或多个云（即私有云、社区云或公有云）组成，这些云保持独立的实体，但通过标准化或专有技术绑定在一起，从而实现数据和应用程序的可移植性（例如，云突发以在云之间进行负载均衡）。

其它部署模型：

- **多云：**在多云环境中，CSC 使用来自不同 CSP 的多种云服务（例如应用程序和系统）。通常采用这种方法来减少对单一云提供商的依赖，并在架构设计中构建技术弹性。
- **混合多云：**公有云和私有资源的组合，通常连接到传统数据中心。

1.3 参考和架构模型

有广泛的技术和方法正在发展，用于构建和操作云服务，这些技术和方法可能使任何单一的参考或架构模型过时。本节的目标是提供一些基础知识，并为理解复杂和新兴的模型提供基线，以帮助安全专业人员做出明智的决策。我们推荐 ISO/IEC 22123 和 NIST 500-292 作为深入的参考架构模型，作为 NIST 云计算定义的合理补充。此外，我们建议探索 CSA 企业架构模型，它旨在整合来自四个独立组织架构的特性。

看待云计算的一种方式是将其视为一个堆栈，其中 SaaS 构建在 PaaS 之上，而PaaS 又构建在 IaaS 之上。这并不代表所有（甚至大多数）真实世界的部署模型，但它可以作为有用的参考基线。SPI 堆栈正在不断发展，随着服务提供的不断成熟，我们看到服务模型之间出现重叠，并且彼此的区别也越来越不明显。因此，首先让我们了解一下每个云服务模型的标准架构（即 SPI 堆栈中的层），然后通过一些示例来展示这些界限是如何模糊的。最后，我们以 CSA 企业架构模型作为结束，该模型可以帮助任何正在开发跨平台能力和模式或对集成多云方法感兴趣的人。

1.3.1 基础设施即服务

物理设施和基础设施硬件构成了 IaaS 的基础。借助云计算，我们可以抽象和把资源池化，但在最基本的层面上，我们始终需要物理硬件、网络和存储来构建。这些资源通过抽象和编排汇集在一起。抽象（通常通过虚拟化）将资源从物理限制中解放出来，以实现汇集。然后，一组核心连接和交付工具（编排）将这些抽象的资源绑定在一起，创建资源池，并以自动化的方式将它们分配和交付给 CSC。

编排通常使用API 来实现。API 通常是云中组件的底层通信方法，其中一些组件会暴露给 CSC 来管理资源和配置。如今，大多数云 API 都使用表述性状态转移 (REST)API 的方式实现资源调用，它通过 HTTP 运行，非常适合互联网服务。

在大多数情况下，这些 API 都是远程可访问的，并且包装在基于 Web 的用户界面中。这种组合是云管理或控制平面，因为 CSC 使用它来管理和配置云资源，例如启动虚拟机实例或配置虚拟软件定义网络。从安全角度来看，这与保护本地基础设施的最大不同在于，管理接口现在是通过网络提供的。如果攻击者妥协了管理平面，他们将获得对云基础设施的特权访问。

以下是一个极简化的 IaaS 计算平台架构示例。

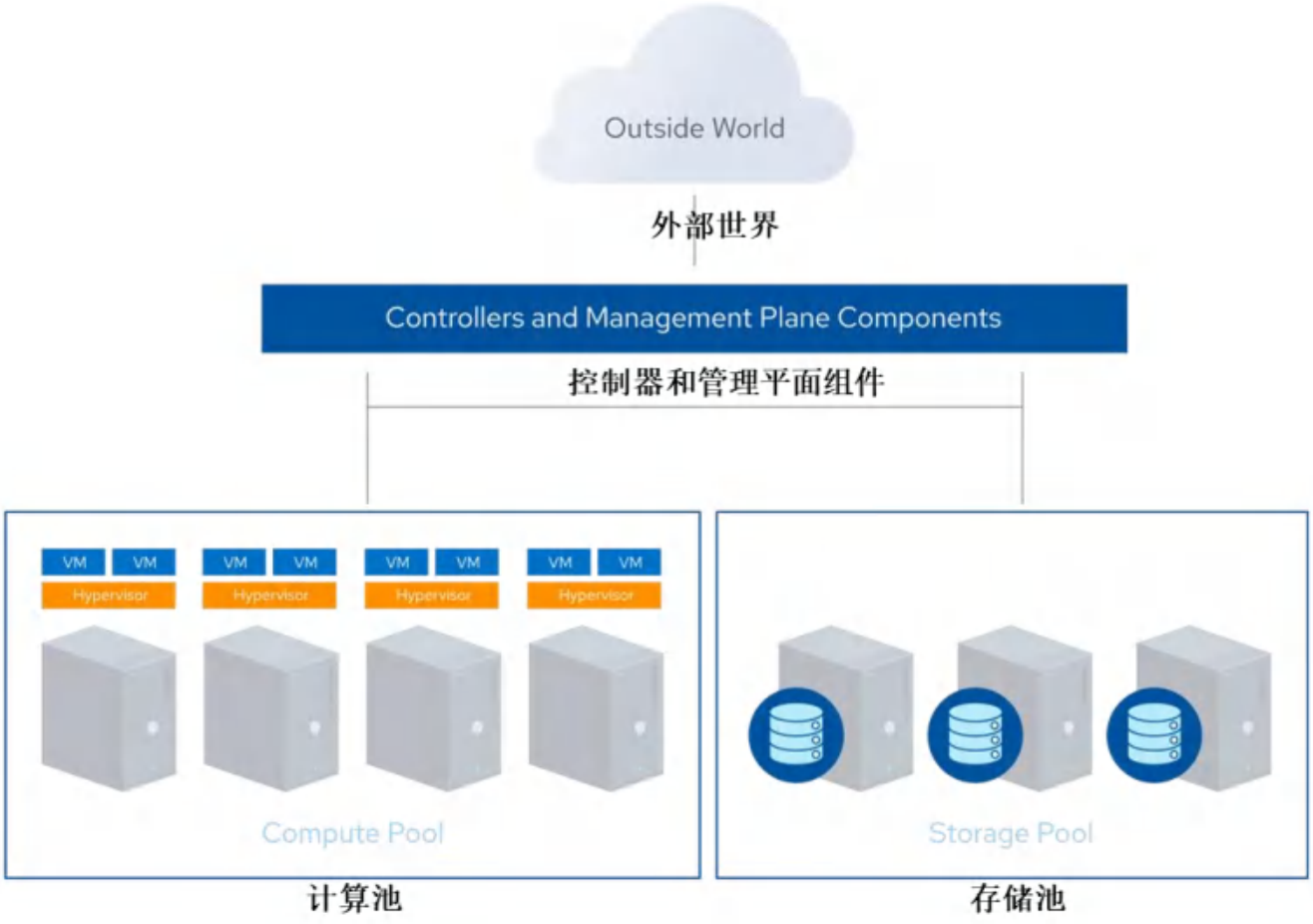


图 2：IaaS 计算平台的简化架构

该示例展示了一个 IaaS 计算平台，具有运行虚拟化管理程序（Hypervisor）和编排软件的物理服务器。云控制器分配资源，创建虚拟实例，配置网络和存储，并为 CSC 提供访问实例的连接信息。

1.3.2 平台即服务

在所有的服务模型中，PaaS 是最难明确描述的，因为 PaaS 的产品种类繁多，方法各异。PaaS 服务通常集成应用程序开发框架、中间件能力以及数据库、消息队列和事件日志等支持服务。这些服务允许开发人员使用该平台所支持的编程语言和工具构建应用程序。

在现实中经常见到的一种选择是构建在 IaaS 之上的平台。例如，集成、持久性和中间件层构建在 IaaS 平台上，然后将其池化、编排，并通过 API 作为 PaaS 服务提供给 CSC。

这可以是使用修改后的数据库管理系统软件实例来构建和部署的数据库即服务 (DBaaS)。CSC 通过 API 和/或 Web 控制台管理数据库，并通过常规数据库网络协议和/或 API 访问数据库。

在 PaaS 中，云用户只能看到平台（或利用平台的应用程序表示层），而看不到底层的基础设施。在我们的示例中，数据库服务会根据实际需要按需扩展或收缩，而CSC 无需管理单个服务器、网络、补丁等。

以下是展示 PaaS 在 IaaS 架构上运行的简化架构。

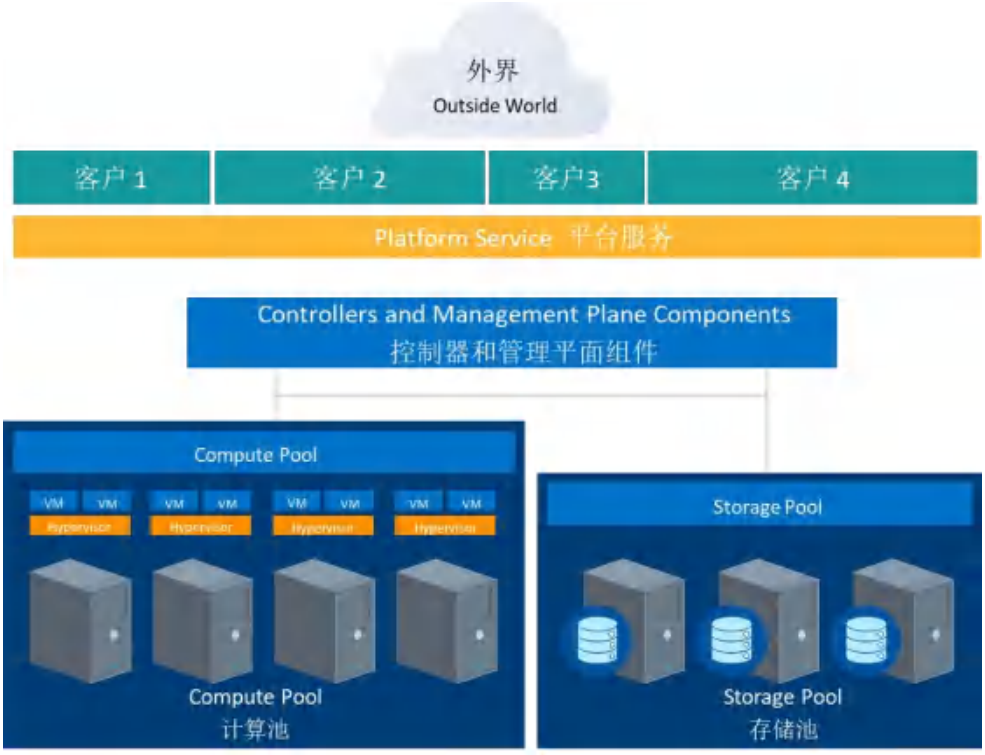


图 3：在 IaaS 上构建的 PaaS 的简化架构

PaaS 不一定需要建立在 IaaS 之上；它也可以是定制的独立架构。其定义特征是 CSC 访问和管理平台，而不是底层云基础设施。一个可能的例子是一个定制的 AI 和机器学习集成服务，支持诸如 AI 驱动的开发工具、机器学习运维 （MLOps）和 AI 生命周期管理等用例。

1.3.3 软件即服务

SaaS 服务是完整的应用程序，涵盖了典型的大型软件平台的所有架构的复杂性。许多 SaaS CSP 基于 IaaS 和 PaaS 构建，原因在于更高的敏捷性、韧性和经济效益。

大多数现代云 SaaS 应用程序结合了 IaaS 和 PaaS，有时还跨不同的 CSP。许多应用程序还提供部分或全部功能的公共 API。它们通常需要支持各种 CSC，尤其是 Web 浏览器、API 和移动应用程序。

SaaS 服务往往具有应用程序/逻辑层和数据存储、API 和表示层服务，通常支持 Web 浏览器和移动应用程序用户接口以及 Internet（互联网）API 访问。

以下是来自实际 SaaS 平台的简化架构，但已去除对具体产品的引用。

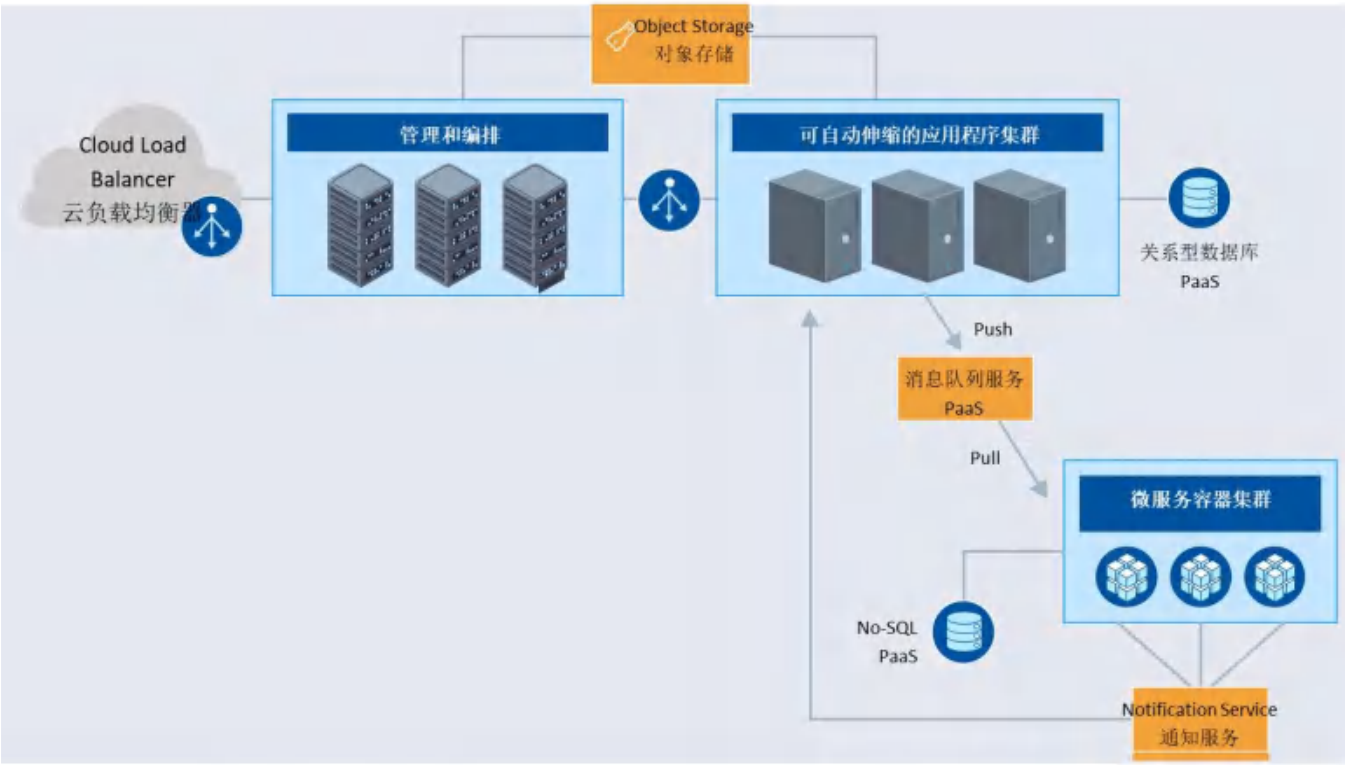


图 4：基于 PaaS 和 IaaS 构建的 SaaS 平台的简化架构

1.3.4 一切皆服务

一切即服务 (XaaS) 是一个广泛的术语，涵盖了通过互联网提供的各种服务的本质，而不是本地或专属的 IDC 数据中心的提供。此模型是云计算的基础，其中“X”可以表示几乎任何以服务的形式提供给用户的服务、应用程序或平台组件，例如安全即服务（Security as a Service）、数据库即服务（DBaaS）、目录即服务（Directory as a Service）、身份即服务（Identity as a Service）、AI 即服务（AI as a Service）。这些几乎总是符合 IaaS/PaaS/SaaS 模型，但在命名上更具描述性和特定性。

1.3.5 重叠的服务模型

虽然 SPI 云服务模型通常以层次结构表示，每一层都建立在其下一层（IaaS、PaaS、SaaS）之上，但这些服务的实施和实际使用方式可以更加灵活。SPI 堆栈是理解不同云服务模型的有用指南。认识到固有的灵活性和重叠层非常重要。SPI 实施不需要建立在严格的层次结构上，模型之间的界限通常很模糊，这被称为重叠服务模型。重叠服务模型不是由严格的层次结构定义的，通常同时封装了多种服务模型的特征。

例如，许多服务同时封装了 SaaS（通过 Web 浏览器提供的完整应用程序）和 PaaS（用于集成平台某些能力的 API）的特征。

1.3.6 CSA 企业架构模型

CSA 企业架构（EA）既是一种方法论，也是一个工具集。它是一个框架，即一种全面的方法，用于构建安全的云基础设施架构。可以用来评估改进机会、创建技术采用路线图、识别可重用的安全模式，并根据一组共同的能力评估不同的云服务提供商（CSP）和安全技术供应商。

为了创建 CSA 企业架构，CSA 研究团队参考了以下四个领域的四个行业标准架构模型：

- **业务运营支持服务（BOSS）** —— Sherwood 应用商业安全架构（SABSA）
- **IT 运营服务（ITOS）** —— IT 基础设施库（ITIL）
- **技术解决方案服务（TSS），包括基础设施（InfraSrv）、信息（InfoSrv）、应用（AS）和展示（PS）服务** —— 开放组应用框架（TOGAF）
- **安全与风险管理 (SRM)** — 开放组织安全论坛（正式的名称为 Jericho 论坛）

图 5： CSA 企业架构的构建模块

CSA 将最好的架构范式结合成一种全面的方法，用于云安全，并结合了业务驱动因素。CSA 企业架构支持云服务在企业商业模型中的价值主张。

CSA 企业架构被 NIST SP 500-292 采纳，进一步巩固了 CSA 方法的重要性。

1.4 云安全范围、责任和模型

云安全和合规性包括安全团队在传统 IT 环境中已经负责的所有任务，只不过这些任务转移到了云端。识别安全需求、选择适当的云服务，并实施控制措施以有效缓解云计算中的风险，是一个迭代的过程，由“共享责任”原则进行划定。我们将基于这一原则描述模型。我们将概述安全责任的划分，其中 CSP 负责基础设施安全，而 CSC 负责他们部署的应用和数据。责任的划分会在不同的服务模型（IaaS、PaaS、SaaS）和 CSP 之间有所不同，这突显了 CSC 理解其职责划分的重要性。

此外，我们还探讨了框架和工具的作用，如 CSA 共识评估倡议问卷（CAIQ）和 CSA 云控制矩阵（CCM），它们有助于促进合规性并与安全标准对齐。所有传统的安全领域依然存在，但风险的性质、角色和责任的分配，以及控制措施的实施，都经常快速变化。

尽管安全和合规性的整体范围没有改变，但任何特定云角色所负责的部分确实发生了变化。可以这样理解：云计算是一种共享的技术模型，不同的组织负责实施和管理堆栈的不同部分。因此，安全责任也在堆栈中分布，并因此在参与的组织之间分配。

这通常被称为“安全责任共担”（SSRM），有时简称为 SRM。可以把它看作是一个责任矩阵，具体取决于特定的云提供商以及特性/产品、服务和部署模型。

1.4.1 责任共担模型

在云计算中，安全是 CSP 和 CSC 共同努力的结果。“责任共担”一词被多个 CSP广泛使用，指的是 CSP 负责安全运营和控制的界限。界限以下是 CSP 的责任；界限以上由 CSC 构建的任何内容都是 CSC 的责任。随着服务模型的改变，这种情况会有很大变化。这个 SSRM 模型概述了 CSP 负责“云”的安全职责，职责包括基础设施、硬件和网络。然而，CSC 负责他们在云中部署的内容。

不同的服务模型下，责任划分会有所不同。无论是 IaaS、PaaS 还是 SaaS，每种服务模型的责任划分都有所不同，而不同的 CSP 之间也可能存在差异。因此，CSC 必须了解这种责任划分，以确保他们对自己的云租户、应用程序和数据等进行适当的保护，并为对 CSP 的问责提供基准。

从高层次来看，安全责任与每个角色在架构堆栈中控制的程度相关。

- **软件即服务（SaaS）**：CSP 负责大部分的安全，因为云用户只能访问和管理他们使用的应用，而不能修改应用的工作方式。即使 CSC 在每个安全领域的责任较小且有限，但通常不会为零。例如，SaaS CSP 负责外部安全、日志记录/监控/审计和应用安全，而 CSC 仍然负责授权和权限的管理。
- **平台即服务（PaaS）**：CSP 负责平台的安全，而 CSC 负责在平台上实施的所有内容，包括如何配置任何提供的安全特性。因此，责任划分更加均衡。例如，使用 DBaaS 时，CSP 管理基础安全、补丁和核心配置，而 CSC 负责其他所有部分，包括使用数据库的哪些安全特性、管理账户或身份验证方法。
- **基础设施即服务（IaaS）**：与 PaaS 类似，CSP 负责基础安全，而 CSC 负责他们在基础设施上构建的所有内容。与 PaaS 不同的是，这将把更多责任放在 CSC 身上。例如，IaaS CSP 可能会监控外围安全，但 CSC 完全负责如何根据服务中提供的工具定义和实施他们的虚拟网络安全。

随着堆栈的逐步向下，CSP 的责任减少，而 CSC 的责任增加。IaaS 模型位于堆栈的较低位置，因此客户需要负责操作系统和应用程序的安全。PaaS 处于中间位置，可能在平台内提供某些安

全功能，但 CSC 仍需在应用程序内进行 API 调用并维持安全配置。SaaS 则不同，因为 CSP 负责整个堆栈，因此他们有责任保护服务中的所有信息。正如你所想象的那样，数据安全对于 SaaS 的 CSP 至关重要，因为一旦发生泄露或故障，可能会引发“银行挤兑”般的事件，甚至危及整个业务。

当使用云代理商或其他中介和合作伙伴时，这些角色会变得更加复杂。理解 CSP 的责任结束的地方和 CSC 的责任开始的地方是至关重要的。云计算不仅仅是利用云服务，更是要通过认识到 CSC 在合作中的角色，确保以安全的方式利用云资源。CSC 必须定期审查和理解他们的责任，尤其是在配置和管理方面，以确保安全策略/措施与组织中所使用数据和资源的敏感性对齐。

下图说明了 SSRM，突出显示了不同服务模型中的 CSP 和 CSC 之间的职责划分。该模型强调了每个参与者对架构堆栈的不同程度的控制和责任：

图 6： 安全责任共担

有效云安全的关键是了解任何云项目中的责任划分。无论 CSP 提供何种具体的安全控制，准确了解谁负责什么至关重要。这种理解使组织能够通过其度量填补控制空白或考虑替换 CSP。对于 IaaS，用户直接控制安全性的能力非常高，而对于 SaaS，则较低。

为了确保云中安全责任的明确分配，我们建议采取以下措施：

●CSP 应彻底记录其内部安全控制和 CSC 特性，以便客户做出知情决策。CSP 还应设计和实施这些控制措施。

●CSC 应建立一个角色与责任矩阵，明确他们在安全方面的责任。该矩阵应记录谁负责实施特定的安全控制，并确保与相关的合规标准对接。

CSA 提供了帮助满足这些要求的工具：

●CAIQ 是一个标准模板，供 CSP 记录其安全和合规控制。

●**CCM** 列出了云安全控制并将其映射到多个安全和合规标准。CCM 也可以用于记录安全责任。

这两份文件需要根据具体的组织和项目需求进行调整，但它们为确保合规性要求提供了全面的起点模板，并且对确保合规性要求至关重要。

关于 SSRM 的更多资源和指南包括：

●**CSA 企业架构：**该框架提供了构建安全云基础设施的全面方法。请参阅上述 CSA 企业架构部分。

●**企业架构与 CCM 责任共担模型：**这一映射帮助用户理解云安全责任，展示了不同服务模型（IaaS、PaaS、SaaS）中 CSP 或 CSC 负责的安全控制。

●**CCM 实施指南：**提供了关于 CSP 和 CSC 在 CCM 中的控制所有权和实施指南。

1.4.2 云安全框架和模式

云安全框架和模式是帮助指导安全决策的工具。“模型”一词可能有些不清楚，因此我们将其分为以下类型：

● 概念模型：或者框架包括用于解释云安全概念和原则的可视化和描述，例如本文档中的 NIST 模型。

- 控制模型：或者框架对特定的云安全控制项或控制类别进行分类和详细说明，例如，CSA CCM。
- 参考架构：是用于实现云安全的模板，通常是通用的。（例如，一个基于 IaaS 的安全参考架构）。它们可以非常抽象，接近概念，也可以非常详细，直至特定的控制和功能。
- 设计模式：是针对特定问题的可重复使用的解决方案。在安全领域，IaaS 的日志管理就是一个例子。与参考架构一样，它们或多或少可以是抽象的或具体的，甚至可以细化到特定云平台上的常见实现模式。

这些模型之间的界限经常模糊和重叠，这取决于模型开发人员的目标。即使将它们归为“模型”一类也可能不准确，但由于我们看到的这些术语在不同来源中交替使用，因此将它们归为一类是有意义的。

CSA 推荐以下几种模型：

- CSA 企业架构（EA）
- CSA 云控制矩阵（CCM）
- ISO/IEC CD 27017.22

ISO/IEC 27017.22 是基于 ISO/IEC 27002 的云服务信息安全控制的实践规范草案，正在开发中，计划取代 ISO/IEC 27017:2015。

1.4.2.1 简单的云安全流程模型

虽然实施细节、必要的控制、具体流程以及各种参考架构和设计模型会根据特定的云实施场景而有很大差异，但有一个相对简单的高级流程来管理云安全。

- 确定必要的安全性和合规性需求以及任何现有的控制措施
- 选择 CSP、服务和部署模型
- 定义架构
- 评估安全控制
- 识别控制差距
- 设计和实施控制措施以填补空白
- 评估控制措施的有效性

- 管理随时间推移的变化

每个云项目，即使是在同一个 CSP 内，也可能需要独特的配置和技术。因此，根据每个项目的具体要求和特点进行评估非常重要。例如，在一个 CSP 中部署在纯 IaaS 上的应用程序的安全控制可能与使用来自同一提供商的更多 PaaS 的类似项目非常不同。

关键在于识别需求、设计架构，然后根据底层云平台的功能确定差距。这就是为什么在实施控制措施以满足安全要求之前，需要了解 CSP 和架构的基本原因。这通常是一个迭代式的流程。了解何时使用原生云服务控制以及何时在外部实施控制以弥补差距是一项重要的考虑因素，可能会对整体安全架构产生重大影响。

总结

组成 CSA 指南其余部分的另外 11 个领域，重点介绍了云计算关注的领域，并针对云环境中的战略和战术安全“痛点”进行了调整，并可应用于任何云服务和部署模型的组合。这些领域分为两大类：治理和运营。治理领域范围广泛，涉及云计算环境中的战略和策略的问题，而运营领域则侧重于架构中更具战术性的安全问题和实施等相关方面。

表 1： 安全指导领域列表

标题	描述
云计算概念和架构	了解面向云安全专业人员的云计算概念和架构。主题包括云模型、安全框架、云原生能力、抽象、编排和多租户，强调敏捷性、弹性和安全性。
云治理	学习以安全性为重点的云治理，涵盖 DevOps、DevSecOps、零信任和 AI/ML 等战略。了解框架、风险管理、合规性，并建立有效的治理结构，如云卓越中心（CCoE）和云注册表。
风险、审计和合规	涵盖云环境中的风险管理、审计流程和合规性。了解云风险评估、合规性要求、法律和审计流程。主题包括合规性继承和利

	用CSP 的合规性来满足监管标准。
组织管理	涵盖使用主要的 CSP 来管理和保护云环境，重点关注组织层次结构、IAM、混合/多云安全性和零信任战略。学习实施有凝聚力的安全控制，并管理不同的云基础架构。
身份和访问管理	涵盖云环境中的身份和访问管理(IAM)，重点关注联合身份、强密码身份验证和授权。学习者将探索高级 IAM 模型、零信任战略和自动化，以增强云安全性和合规性。
云安全监控	涵盖云安全监控挑战和解决方案，包括云遥测、日志、混合/多云设置和高级监控工具。主题包括 SSRM、日志存储、金丝雀、蜜罐令牌以及生成式 AI 在增强云安全方面的作用。
云基础设施和网络	涵盖管理和保护云基础设施，包括安全架构设计、软件定义网络（SDN）、基础设施即代码（IaC）和安全云连接。它强调零信任、安全接入服务边缘（SASE）、容器安全和集成安全度量来保护云资产。
云工作负载安全	涵盖保护云中的工作负载，包括虚拟机、容器、无服务器函数、PaaS 和 AI。学习保护虚拟机镜像、管理容器漏洞以及实施加密、访问控制、运行时保护和 IAM 最佳实践。
云数据安全	涵盖云环境中的数据安全，重点关注数据分类、加密、访问控制和各种云存储类型。它涉及静态、传输和使用中的数据安全，以及 AI 系统安全和未来数据安全技术。
云应用安全	学习云应用安全，专注于保护应用免受外部威胁。了解关于软件开发生命周期（SDLC）、威胁建模、安全编码和测试。主题包括基础设施即代码（IaC）、DevOps、第三方库和新兴的云安全技术。

事件响应与韧性（恢复力）	涵盖云环境中的事件响应和业务恢复能力，这对组织的安全至关重要。了解基于 CSA 和 NIST 指南的 CIR 战略、工具和实践。主题包括准备、检测、遏制、（系统）恢复和（业务）恢复战略。
相关技术与战略	涵盖云安全战略，重点关注零信任、AI 集成以及威胁和漏洞的管理。学习通过多因子身份验证、加密、AI 威胁检测和持续监控来保护云应用、系统和数据。

建议

- 了解云计算之间的差异以及抽象和编排如何影响安全性。
- 熟悉云计算的NIST模型和CSA参考架构。
- 使用SSRM工具在CSC和CSP之间分配和安排安全责任和义务。
- 使用CSA的 CAIQ等工具和文档来评估和比较云提供商。
- 云提供商应记录其安全控制和特性，并使用CSA CAIQ等工具发布它们。
- 使用CSA CCM等工具来评估和记录云项目的安全性和合规性要求和控制，以及每个要求和控制的负责人。
- 使用云安全流程模型来选择提供商、设计架构、识别控制差距并实施安全和合规控制。

其它指导

- CCSK 准备工具包 | CSA
- 云安全联盟词汇表 | CSA
- CSA云控制矩阵 (CCM) | CSA
- CCM-Lite和CAIQ-Lite | CSA
- CCM v4实施指南 | CSA
- CSA企业架构参考指南 | CSA
- 企业架构到CCM责任共担模型 | CSA

领域 2：云治理

此领域关注云治理，重点强调安全的作用。治理是基于由策略、程序和控制构成的框架，旨在促进透明度和对既定标准的问责制。有效的治理实践涉及战略指导、风险管理和缓解措施、合规性监控和补救、预算分配和成本控制。IT 治理确保信息和相关技术能够支持企业战略和目标的实现。

信息系统审计师协会将治理定义为：“治理确保利益相关者的需求、条件和选择得到评估，以确定需要实现的平衡且一致的企业目标；它通过确定优先级和决策来设定方向，并监测绩效和合规性，确保与既定方向和目标的一致性。”

组织可以通过遵循行业特定的治理标准和框架来加强治理实践。例如，ISO/IEC 38500:2024 标准为组织提供了 IT 治理方面的指导。ISACA COBIT 框架为企业 IT 治理和管理提供了全面的实施指南。

关于治理标准的更多信息：

- ISO/IEC 38500:2024 - 信息技术 – 组织 IT 治理
- ISACA - COBIT - 企业 IT 治理和管理的业务框架
- ISO/IEC 27014:2020 - 信息技术 - 安全技术 - 信息安全治理
- 开放群组云治理框架

以下是影响 IT 治理的部分法律法规示例：

- 格雷姆-里奇-比利雷法案 (GLBA)
- 萨班斯-奥克斯利法案 (SOX)
- 健康保险流通与责任法案（HIPAA）
- 通用数据保护条例（GDPR）

学习目标

此领域，您将学习到以下内容：

- 确定云治理的目的。
- 定义云治理中的治理层级体系。
- 探索影响云计算治理的关键战略和概念。

2.1 云治理

云计算的多租户特性、责任共担模型、敏感数据的重新分配、关键应用程序和基础设施的托管，以及安全和隐私问题，迫切需要有效的治理机制。

因为存在各种法规、管辖权、安全和隐私的要求，合规性是业务上云时一个主要的问题。如果没有完善的治理政策，安全问题、财务和风险可能会导致云运营成本急剧增加，并使业务上云成为企业的不明智选择。

成本效益和快速上线是上云的主要驱动因素之一。许多组织认为云计算是一种通过从资本性支出模式转向运营性支出模式（例如，按需付费和基于订阅模式）来实现成本节约的方法。因此，常见的迁移策略是将传统现有的应用程序和基础设施不做任何改变直接迁移到云上。如果这样保持现有体系结构不变直接迁移上云，安全和隐私的治理就成为首要问题，因为转向新技术平台可能会带来新的技术风险。此外，云客户（CSC）还需要与云服务提供商（CSP）责任共担。

战略创新是上云的另一重要驱动因素。许多组织将软件视为可以提供竞争优势的战略资产。云计算提供了快速开发和部署软件的能力，使组织能够快速将新产品和服务推向市场。然而，从治理的角度来看，快速上线也会导致的快速变化的风险，如配置错误和软件供应链等危害。因此，拥有强大的安全设计流程至关重要，以确保云中的软件开发、测试和部署是安全可靠的。

本次讨论的要点包括：

- 上云的驱动因素包括节约成本、运营性支持模型、实现组织目标及战略创新的需求。
- 上云需要考虑的治理因素不仅包括将信息风险（数据、应用程序、主机操作系统、网络和供应链）和物理风险控制在可接受的水平（称为风险偏好）。还需要评估 IT目标是否与业务目标相一致，以及确保遵守法律和法规的要求，包括隐私义务。

● 组织应该根据具体的业务目标来制定迁移战略，确保选择合适的云服务并实施适当的治理策略。

2.1.1 云采用与治理

云计算影响安全治理的主要方式有两种：

1、引入责任共担模式 (SRM)。安全治理责任现在由云服务提供商 CSP 和云客户 CSC 共同承担。更复杂的问题是，在某些情况下第三方服务提供商被引入到供应链中，每个服务提供商都存在自己的安全风险。即使部分责任被转移给这样的第三方，但最终责任仍然由 CSP 或 CSC 承担。

2、由云计算固有特性造成的技术和运营差异。

在云计算出现之前，IT 安全治理在很大程度上依赖于数据中心内运行的固有特性。数据中心的资源是有限的，包括空间、计算、网络等都是有限。而且这些资源都处于相对隔离的物理环境中。组织结构、策略和控制措施都围绕这些资源的稀缺性进行调整。

公有云则完全相反。虽然云提供商的容量也不是无限的，但有充足的容量来满足云客户的需求。云是分散的，不同的团队可以使用登录名和信用卡配置整个资源栈，如果没有有效的治理，这些资源就不会受到集中的管控。

云也从根本上改变了我们管理这些资源的方式。虽然资源可以被分散，但在公有云中，核心管理平面是统一的，并向互联网开放。由于没有物理网络边界，任何拥有正确凭据的人都可以访问管理平面并重构整个虚拟基础设施。这种分布式架构与泛网络管理平面相结合的方式，需要新的、针对云的治理策略。

总之，云计算通过分布式基础设施管理、提供统一的接口实现资源访问的方式，彻底改变了 IT 治理。组织必须在接受这些变化同时确保安全性和控制力，发挥云计算的优势。

2.1.2 云治理的复杂性

随着组织越来越多地采用云服务，它们在新的商业模式、技术和管理方面都面临着独特的治理挑战。这些挑战要求组织更新其治理框架以适应云环境。PaaS、SaaS 和 IaaS 共同的考虑因素包括控制和问责、合法性以及云服务提供商（CSP）和云客户(CSC) 之间的关系。

本节列出了这些考虑因素，强调了为了有效管理云环境所需要调整的治理策略。

以下考虑因素概述了组织在管理云环境时必须解决的关键治理挑战和必要的调整：

控制和问责

● 云计算可能会导致组织失去对 IT 基础设施的直接控制，从而迫使组织采用新的治理框架和流程。

● 使用云解决方案不意味着将控制责任外包给第三方或第四方。

● 云使用多种不同的责任共担模型（SRM），具体取决于云服务提供商（CSP） 和技术栈。同时，这需要在云服务提供商和云客户之间明确分配控制和责任。

● 云客户（CSC） 必须更多地依赖评估活动而不是实际测试。

法律和合规性

● 云服务和数据可能跨越多个司法管辖区，迫使客户遵守更多的法律法规，尤其是有关隐私方面的。

● 数据所有权和分类以及隐私控制可能不是直观清晰的，需要仔细检查。

● 可见性和透明度

● 对于某些云服务，可见性和透明度可能具有挑战性。

定制和标准化

● 云服务提供商可能仅仅提供标准产品，无法根据云客户的具体需求进行定制。

● 云服务提供商可能表现出不同的能力成熟度级别、不同的服务、许可证和模型，想要找到一种适用于所有的云策略是非常困难的。

治理复杂性

● 云服务通常是建立在云服务提供商之上，这使得治理活动的范围具有挑战性（例如，一个运行在另一家 IaaS 提供商的基础设施上的 SaaS 服务）。

● 由于难以明确云服务提供商（CSP）和云客户（CSC）的责任界限，混合云模型可能会使治理变得更加复杂。

CSP 和 CSC 的责任动态变化

● CSPs 可能会迅速变化，这必须在治理模型中加以考虑。

● 使用云服务可能需要额外的、当前 CSC 还不具备的技能，例如云审计能力或云安全能力，以及面向云的安全工具的知识。

下图概述了不同云服务模型相关的特定复杂性，强调了每种模型独特治理挑战和责任。

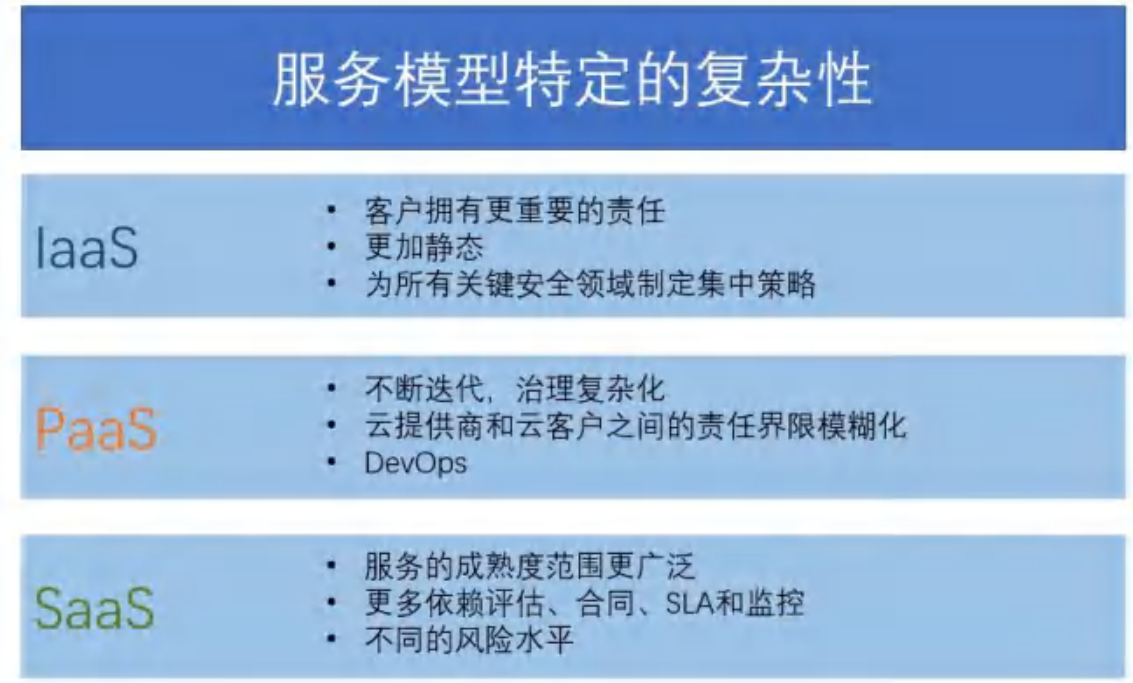


图 7：服务模型特定的复杂性

有效的云治理需要灵活而强大的策略，以应对 IaaS、PaaS 和 SaaS 模型的独特挑战。通过理解和管理这些复杂性，组织可以确保其云环境中的安全性、合规性和运营效率。

2.1.2.1 云治理的复杂性：部署模型

更进一步，还必须考虑与不同云部署模型相关的治理复杂性。以下部分将探讨不同部署模型的治理挑战和责任。

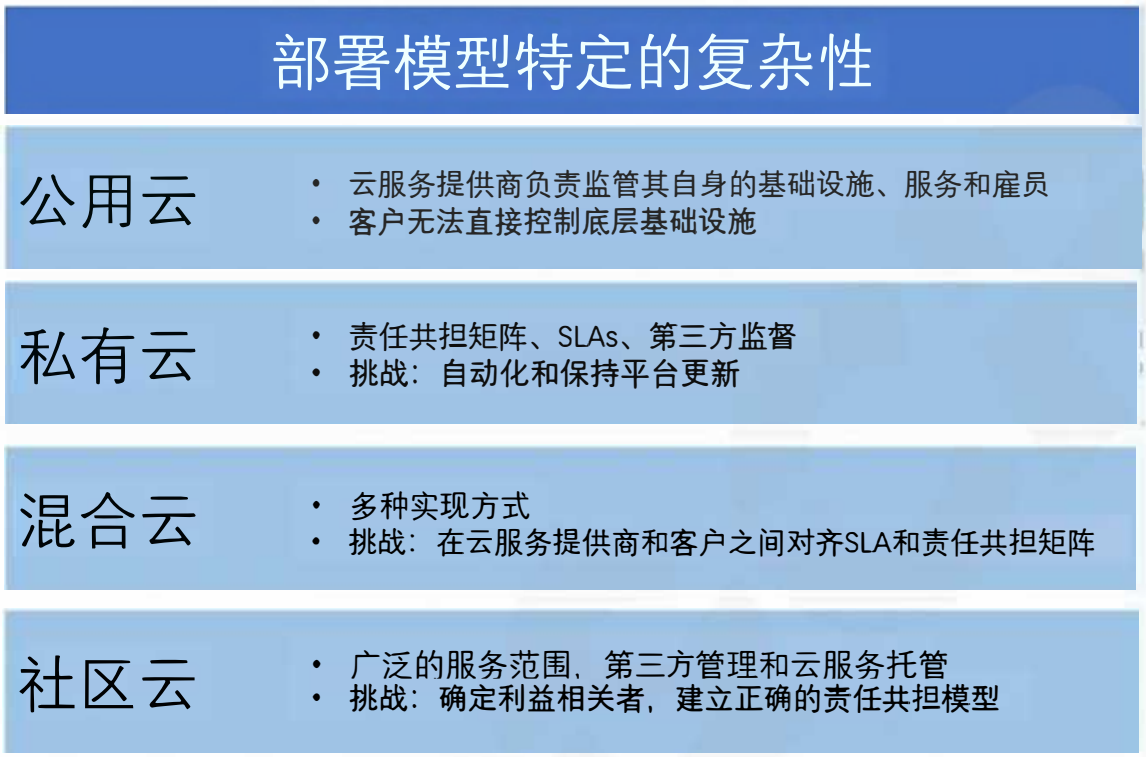


图 8：部署模型特定的复杂性

公有云：公有云是最流行的云部署模型，为所有客户提供标准服务。公有云提供商通常拒绝定制请求，因为这会使治理变得复杂。公有云提供商自己管理的基础设施、服务和雇员。治理挑战来自客户初始配置，并随着时间的推移而逐渐增加，

公有云依赖于多租户架构，因此微隔离成为治理挑战。这通常限制了诸如安全扫描或渗透测试等操作，并降低了对基础设施的可见性。这些挑战需要使用供应商风险管理、服务水平协议(SLA)、第三方审计和合规性报告等新的治理方法。这些方法的有效性是通过衡量减轻了多少云计算风险进行评估的。

私有云：私有云可以由组织或第三方拥有、管理或托管。自我管理的私有云的治理类似于传统的 IT 治理，但也必须解决云特有的问题，如攻击向量、多租户和自动化。由第三方管理的私有云治理方式最接近我们已知的传统外包模式。治理挑战包括理解责任共担矩阵、制定 SLAs 以及构建第三方监控能力以跟踪策略违规和内部威胁。一个重大的挑战是让平台保持最新服务，需要特别关注。

混合云：混合云服务结合了私有云和公有云模型。它们可以通过多种方式实现，从而使策略指南和 责任共担模型（SRM） 变得复杂化。治理挑战包括协调提供商和客户之间的 SLAs 和责任、保护内部边界、扩展安全配置，并解决云安全和成熟度方面的技能差距。

社区云：社区云是指由第三方管理和托管的一系列服务，由多个组织共享但不完全公开，从而降低了多租户的挑战。治理挑战包括识别利益相关者、构建正确的 责任共担模型（SRM）以及专注于使用相同社区云的组织之间的关系和风险。

2.2 有效的云治理

有效的云治理需要建立一个强大的框架和一组策略，以确保有效、安全和合规地使用云资源。它需要实施强大的控制框架和策略来安全、合规和高效地管理云资源。其中包括：

- 定义角色和职责
- 建立云卓越中心或类似机构
- 进行需求收集
- 基于风险的规划
- 风险与补救措施管理
- 数据和数字资产分类
- 遵守法律和监管要求
- 维护云注册表
- 建立治理层级结构
- 利用云特定的安全框架
- 定义云安全策略
- 设定控制目标并指定控制规范

通过实施这些组件，组织可以最大限度地发挥云计算的优势，同时降低潜在风险。下面我们探讨有效云治理的一些关键组件。

2.2.1 云治理实施模型

云卓越中心（CCoE）和云咨询委员会(CAC)模型是实施有效云治理广泛采用的方法。云卓越中心包括工作成员和推广者。云咨询委员会提供高层的赞助和认可。更具体地说：

● 云卓越中心（CCoE）是一个集中式团队或部门，为组织或者其他部门提供上云和使用云的相关指导、最佳实践和支持。CCoE 帮助确保与云客户的目标和标准的一致性。

● CAC 可以包括来自IT、风险管理、合规性、安全和一般业务职能的高级领导小组，负责制定云客户战略和运营的愿景和方向。CAC 在此处不深入介绍，但需要了解它的重要性。

云卓越中心（CCoE）和 CAC 是云客户 IT 治理和安全的推荐组件。它们作为集中化枢纽，负责领导云计算倡议，并推动战略性、安全、合规和有效的上云活动。并非所有云客户都使用相同的术语，但从功能角度来看，这些结构强调了有效云治理所需的关键要素。

2.2.1.1 云卓越中心

云卓越中心（CCoE）的主要功能之一是提供战略指导。它确保云计划与云客户的整体业务目标相一致。通过这种方式，CCoE 确保上云能够支持云客户的目标，并帮助客户取得成功。

CCoE 还可以制定使用云的治理框架。这包括创建符合外部法规和内部最佳实践的策略和标准。CCoE 负责管理风险、确保数据隐私和安全，并维护云环境中的合规性。

CCoE 传播有关云技术和安全措施的知识。它为其他部门提供培训机会和资源，促进了整个组织范围内一致的云技能水平。这确保员工拥有必要的技能和知识，能够有效且安全地利用云服务。

在这些职责中，安全是 CCoE 的主要关注点。它将安全性嵌入到云基础设施中，确保云部署在设计时就处于安全状态。CCoE 确保满足云客户的安全和隐私要求，并应对不断变化的威胁态势。

CCoE 鼓励跨职能部门的协作，包括 IT、安全、合规性和财务等部门。这种协作方法确保云决策的全面性，包括成本、安全性、合规性和业务需求等方面的综合考虑。

CCoE 还促进创新和适应性。鼓励探索新的云服务和技术，并在组织内推广创新文化。同时，CCoE 能够适应技术和业务环境的变化，确保云客户能够有效地利用最新云技术。

最终，CCoE 对于云客户寻求有效且安全地利用云技术的非常有用。它超越了技术范畴，专注于将上云与业务战略相结合，同时确保云环境中的治理、安全性和合规性。下图说明了 CCoE 中的关键角色。

图 9：CCoE 中的关键角色

2.2.2 安全冠军

除了设立云卓越中心（CCoE）之外，云客户还可以在合规、企业风险、法律、人力资源、财务和 IT 等业务部门内任命安全冠军。安全冠军（安全倡导者）了解云安全的重要性，因此可以充当安全倡导者，帮助推动实施安全最佳实践和控制措施。

安全冠军（安全倡导者）应该从团队内部任命，并发挥实际作用。他们通常不是安全组织的成员，而是组织内部团队的成员。这种区别使他们能够专注于在特定团队动态下实施具体的安全措施。组织需要将下列安全角色进行区分：安全冠军、业务信息安全官 (BISO)、首席信息安全官 (CISO) 、信息安全官 (ISO) 。

例如，在 DevOps 团队中，安全冠军的理想候选人通常是团队内的开发人员、系统管理员或 DevOps 平台工程师。他们对团队动态和技术能力有充分的理解，使他们能够有效地倡导安全。他们已经具备了理解云服务和 DevOps 实践中特定安全挑战和解决方案的知识和专业技能。

安全冠军在 DevSecOps 流程中，整合安全实践方面发挥着至关重要的作用。作为安全团队和开发团队之间的联系人，他们在分配权限方面发挥着关键作用。通过在团队内部倡导安全，安全冠军在云和 DevOps/SRE 团队中推广安全文化。安全冠军在开发相关团队中更为普遍，但也可以在其他业务部门中扮演重要角色。

为了培养安全冠军的技能和兴趣，为他们提供有趣且互动的安全培训非常重要。例如，关于道德黑客的研讨会是提高他们实际安全技能的有效方法。然而，重要的是不要强迫安全冠军成为全职的安全专家。他们可以是开发人员或者管理员，只要接受额外的安全培训，就可以担任团队中的联络员和专家。

赋能安全冠军的目标是让他们发挥咨询的作用，而不是让他们承担更多额外职责。避免过度疲劳很重要。通过赋能安全冠军，云客户可以有效地弥合安全与开发之间的差距，培养云和 DevOps 团队中的安全文化。

总之，安全冠军在推广云、DevOps 团队和业务团队内的安全文化方面至关重要。通过赋予他们适当的经验、培训和指导，云客户可以在开发流程中有效地整合安全实践，最终会改进的安全成果。

2.3 治理层级

云治理的一个关键方面是建立治理层级。这涉及定义与云相关问题的决策流程和升级路径。治理层次确保在云客户内在适当级别做出决策，并且有明确的责任和义务。云客户可以利用云特定的安全框架来指导其云治理工作。

信息安全中的治理层级是确保组织系统和数据安全的结构化方法。此层级的顶部是框架，它提供了一套网络安全实践指南。框架的示例包括 NIST 网络安全框架 (CSF)、云控制矩阵 (CCM)、互联网安全中心(CIS) 和 IANS 云安全成熟度模型 (CSMM)。这些框架是组织建立和维护强大网络安全态势的总体结构，可以用来指导企业方针。

策略是治理层级的下一级。它们是叙述性文档，概述了组织的安全要求。策略将框架中的指导方针转化为清晰且可操作的声明，该声明用于指导组织的安全实践活动。框架通常要求组织制定具体策略，以确保符合监管和合规要求。

控制目标比策略更具体，侧重于安全控制的预期结果。它们定义了最小化风险和维护安全环境的目标。例如，控制目标可能会规定所有用户登录云平台必须使用多因素身份验证 (MFA)。控制目标为组织提供了明确的方向，指导完成安全方面的任务。

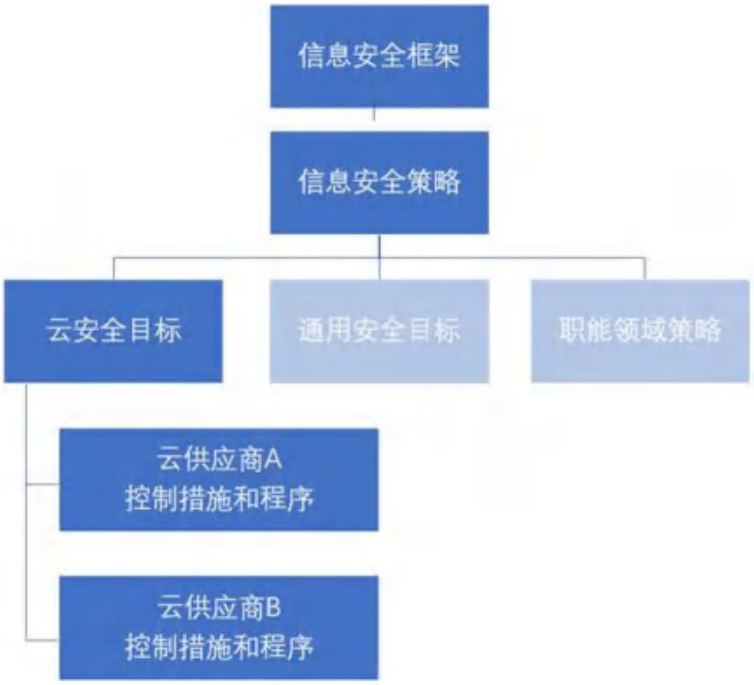


图 10： 结构化安全治理层次结构

控制规范和实施指南是治理层级的基础层。它们是实现控制目标的技术体现。控制规范根据特定的云服务提供商和平台而不同，例如 AWS 或 Azure。它们概述了应采取的技术控制措施，以实现所需的安全结果。例如，为了满足多因素身份验证（MFA）的控制目标，AWS 的控制规范可能要求所有用户都启用MFA 进行控制台访问，并且 IAM(身份和访问管理)的用户需要附加“MFA Required”管理策略才能进行API 访问。通过自动化，控制规范可以验证合规性。值得注意的是，控制目标可能导致多种控制规范，因为云基础设施内的不同环境或技术可能需要量身定制的实现才能满足所需的安全结果。

治理层级为组织提供了一个结构化的信息安全方法，确保安全实践与行业标准、合规性和监管要求相一致。通过遵循治理层次结构，组织可以建立强大的安全策略，并有效地保护其系统和数据。

2.3.1 基本治理原则与指南

为了建立牢固的上云治理框架，第一步就是确定基础治理原则。这些原则将作为指导方针，用于定义策略、标准、控制，目标、控制规范和实施指南，以确保云环境的隐私、安全和合规性。云治理框架应该为上云流程定义关键角色和利益相关者，包括高级管理人员、IT 和技术人员、业务专家和安全利益相关者。治理层级确保与行业标准和监管要求保持一致， 帮助组织建立强大的安全态势。下图说明了云治理流程的关键要素，包括风险容忍度、数据分类和控制目标。

图 11：云治理流程

2.3.1.1 确定风险承受能力

风险容忍度对于理解云环境运营时可接受的风险至关重要。风险容忍度是指云客户在追求其目标的过程中，管理层愿意允许的任何特定风险的可接受程度。这个决定综合考虑了定性和定量因素，例如财务、法律、声誉和运营影响等。

通过评估风险容忍度，云客户可以建立明确的安全态势，并在整个上云过程中做出明智的决策。云卓越中心（CCoE） 或云团队应记录并告知领导层有关上云的风险，并在规定的风险容忍度范围内运营。

风险评估应基于对组织相关的不良网络和运营事件的可能性和重大影响进行分析，可以使用影响可能性矩阵或信息风险因子分析 (FAIR) 等评估方法来实现。

2.3.1.2 数据和资产分类

数据和资产分类是云治理的关键方面。云客户需要根据敏感度、关键性以及与损失相关的潜在影响对数据和资产进行分类。正确的数据分类将有助于选择适当的安全控制措施，并确保符合保护数据的法律、法规和合同要求。

常见的分类可能包括公共数据、内部数据、机密数据和绝密数据。数据和资产的分类会影响它们在云中的存储和处理方式，以及保护它们可能需要的控制措施（法律、监管、组织）。云注册表应记录此分类以供参考。

此外，数据的位置在云计算中是一个关注点，因为数据可能托管在另一个司法管辖区，甚至有时云客户都不知情。一些政府或机构对跨境数据传输有限制，或要求额外的控制，例如欧盟《通用数据保护条例》（GDPR）。

2.3.1.3 识别法律和法规要求

识别适用于不同司法管辖区或行业处理的数据类型的法律法规要求至关重要。例如，如果云客户正在处理欧盟公民的个人数据，则需要遵守 GDPR。同样，如果云客户在美国处理健康信息，则需要必须遵守《健康保险流通与责任法案》(HIPAA)。

除了法律法规的要求外，根据风险评估确定的具体风险项也很重要。这确保了云治理框架的全面性，并与整体风险管理策略保持一致。

2.3.1.4 需求、标准、最佳实践和合同义务

要建立健全的治理框架，必须符合既定的标准、最佳实践和合同义务。这包括遵守 CSA CCM、ISO/IEC 27001、ISO/IEC 27017、NIST CSF 或 CIS Benchmarks 等标准和最佳实践。

了解云服务提供商的合同义务非常重要。这包括确定云客户和云服务提供商之间的共同安全责任，以及他们之间合同中列出的任何具体安全要求。此外，还应考虑与云客户和第三方合作伙伴的合同义务，因为它们可能会影响云计划。在云供应链中，这些组织是云客户和云服务提供商的合作伙伴。

了解当前的最佳实践也很重要。CSP 通常会推荐使用云服务的最佳实践（例如，AWS Well-Architected Framework, Azure Well-Architected Framework, IBM Cloud Well Architected Framework, Google Cloud Architecture Framework）。虽然云客户可能需要根据具体的需求调整这些实践，但最佳实践是建立安全云环境的宝贵参考点。云安全并非一尘不变。它需要根据特定情况进行定制，

包括行业、风险容忍度和法律法规等要求。随着新威胁的出现和法规的演变，持续监控和调整适应是必不可少的。云客户需要确定各个供应商提供的适当服务，并配置这些服务以满足要求和合规标准。

2.3.1.5 咨询关键利益相关者

为了建立强大的上云治理框架，与关键利益相关者进行协商非常重要。这可以确保云安全策略与业务目标保持一致。

此外，为了满足已确定的需求，云客户应制定明确的行动计划，并实施适当的安全、隐私和数据保护的控制措施。该计划应列出实施必要控制措施的具体步骤和时间表，以确保云环境的安全性、隐私和合规性。

2.3.2 云注册表

为了促进有效的云治理，云客户可以建立云部署注册表和云服务注册表。它们在云治理中各自发挥着不同的作用（CSC 可能使用不同的术语）。

从高层次上，云服务注册表是指哪些云平台和服务得到了哪些批准数据类型的列表（例如，SaaS 提供商 X 被批准用于类型 Y 的数据）。

云部署注册表是一种工具，用于维护组织在多个提供商和服务中的云资源清单。这是一个集中式仓库，保存有关组织部署的云资源的信息，包括所有权、使用情况和安全控制等详细信息。此云注册表有助于确保云资源管理的透明度和可问责性。与资产注册表类似，通过拥有全面的云注册表，云客户可以有效地管理和保护其云资源。

一些云客户使用标准风险登记表来跟踪云服务和部署。只要该登记表可供安全和运营团队使用、并保持更新，包含本文所述信息，就是可以接受的。

构建云部署注册表时，包含如下重要的元素：

1、云服务提供商 (CSP)：记录每个帐户的云服务提供商，包括 AWS、Azure 和 GCP 等主要提供商，以及 Salesforce 和 Microsoft 365 等 SaaS 平台。此信息有助于了解所使用的底层基础设施和服务。

2、环境 ID：为每个云环境分配一个唯一标识符，以便于跟踪和管理。此 ID 应出现在日志和其他监控工具中，为每个环境提供精确的参考点。

3、描述性名称：提供一个有意义的名称，准确描述每个云环境的用途或性质。这有助于更容易地识别和理解组织内每个环境的作用。

4、合规分类：根据监管和合规需求（如 PCI DSS、HIPAA、GDPR 等）对每个环境进行分类。正确的分类可确保适当的安全措施和控件被应用，并满足合规性要求。

5、风险分类：评估并标记每个环境的风险级别，以符合云客户的风险管理策略。这有助于采用适度资源和精力处理风险，并确保实施了适当级别的安全控件。

6、环境分类：区分不同类型的环境，例如开发、准备和生产。这样的分类使得每个环境都根据其特定要求进行配置，有助于治理和管理。

7、所有者：确定每个云环境的业务所有者。这确保了决策和资源分配的可问责、责任和清晰的沟通渠道。

8、技术联系人：为每个环境的技术问题和运营管理指定一个联系人。这有助于简化沟通，并确保及时解决技术难题。

9、云服务供应商联系人：客户支持和账户管理的联系信息。此信息对于解决任何与服务相关的问题以及与云服务供应商保持良好关系至关重要。

2.3.2.1 云部署注册表功能

拥有维护良好的云部署注册表可带来多种好处：

● 更好的云资源可见性和控制：全面的注册表允许云客户清楚地了解、记录和跟踪其云资源，从而实现有效的资源管理、优化和变更管理。

● 一致的治理框架应用：通过详细的注册表，云客户可以确保在所有环境中应用适当的治理框架、策略和程序。

● 事件响应支持：云注册表提供所有必要的联系信息，能够在安全事件或运营中断期间快速响应事件并进行有效协调。

● 符合策略和法规：根据合规性需求对环境进行分类，云客户可以确认他们遵守内部策略和外部法规， 从而最大限度地减少不合规的行为。

如果尚未编制云注册表，请先编制云注册表，并确定所有必要元素，收集每个环境所需的信息。根据计划的时间间隔定期审查和更新云注册表。此外，每当业务环境发生重大变化、法律/法规/合同变更、云基础设施发生变化或组织结构发生变化时，都要更新注册表。这可确保注册信息保持准确和最新，从而支持有效的治理和风险管理。

2.3.3 云安全框架

框架的主要目的之一是组织确定安全控制目标的优先级。这些目标代表组织为实现期望的安全结果而设定的具体目标。框架为分类这些目标提供了结构，并帮助组织确定最有效的实施和管理这些目标的方法。通过组织安全控制目标，框架使云客户能够系统性地处理云安全问题，并确保所有必要的控制措施得以落实。

云特有的安全框架是专门为云环境设计的，并考虑了云计算的独特特性。这些框架解决了按需资源分配、责任共担和快速弹性等方面的问题。通过使用特定于云的框架，云客户可以确保其安全程序符合云的具体要求和挑战。

相关云框架的示例如下：

- CSA 云控制矩阵 (CCM)
- ISO/IEC 27017:2015
- BSI 云计算合规标准清单 (C5)
- NIST SP 800-53 Rev.5 - 信息系统和组织的安全和隐私控制
- PCI DSS 支付卡数据安全标准委员会云计算指南

如果云客户已经使用信息安全框架，但该框架未能有效涵盖云的特征，则可以考虑增加云的补充框架。这种理念是将特定于云的安全框架与现有的主框架一起使用。许多现有的安全框架最初并不是为云计算设计的，可能无法充分解决特定于云的活动。通过使用云补充框架，云客户可以专注于云安全活动，同时仍然利用现有框架进行其他安全领域的工作。

2.3.3.1 NIST 网络安全框架

虽然存在多种安全框架，但 NIST 发布的网络安全框架 (CSF)为行业、政府机构和其他组织提供了一种公认的结构化安全方法，即使它不是专门为于云而设计的。该框架也称为 CSF Core，它

提供了高级网络安全结果的六种功能分类，任何组织（无论其规模、部门或成熟度如何）都可以使用它来更好地理解、评估、确定优先级和协商网络安全态势和计划。以下是 CSF 功能，提供了组织网络安全风险管理生命周期的高级策略视图：

- 治理（GV）：建立并监控组织的网络安全风险管理策略、期望和策略。
- 识别(ID)：帮助确定组织当前的网络安全风险。
- 保护（PR）：采取安全措施来防止或降低网络安全风险。
- 检测（DE）：发现并分析可能的网络安全攻击和危害。
- 响应（RS）：对检测到的网络安全事件采取行动。
- 恢复（RC）：恢复受网络安全事件影响的资产和运营。

2.3.3.2 CSA 安全、信任、保证和风险注册

云安全联盟（CSA）有一项 STAR 计划，包括安全、信任、保证和风险。STAR 计划是一项旨在提高云服务的透明度和可信度的计划。该计划为云服务提供商记录其安全实践，并为云客户提供了一个框架来评估云服务提供商的安全态势。

CSA STAR 计划由两个主要部分组成：

1、CSA STAR 证明：在此过程中，云服务提供商会根据 CSA CCM 的安全控制项进行自我评估，并公开其评估结果。这提供了云服务供应商的安全状况透明度，让云客户能够针对是否使用其服务做出明智的决策。

CSA STAR 认证：这需要独立的第三方机构对云服务提供商进行评估，评估标准包括 CSA CCM 和其他公认的行业标准（如 ISO/IEC 27001）。获得 CSA STAR 认证表明云服务提供商已经实施了强有力的安全措施和实践。

通过促进标准化安全评估和提高透明度，CSA STAR 计划使云客户能够评估云服务提供商的安全性、隐私性和合规性。这反过来又有助于云客户在选择和使用云服务时做出明智的决策，从而促进云行业的信任和可靠性。

2.3.3.3 云控制矩阵

CSA CCM v4 包含 17 个控制域。它全面涵盖了从治理和风险

管理到运营安全和数据隐私等各种安全主题。

因此，对于希望增强云安全性的云服务提供商和云客户而言，是一个宝贵的资源。CCM 的主要优势之一是它与 ISO/IEC 27001/27002、PCI DSS、NIST CSF 等领先标准保持一致。通过与这些成熟框架保持协调一致，CCM 确保组织可以在多种标准和法规下实现合规性。这种一致性还扩展到 STAR 计划，进一步提高了其在行业中的可信度和相关性。

CCM 是专为云环境量身定制的，非常适合保护多租户、分布式和动态云系统。与 NIST CSF 等更通用的安全框架不同，它专注于云计算的独特挑战。此外，CCM 允许进行控件定制，使云客户能够根据其特定的云架构、交付模式（IaaS、PaaS、SaaS）和合规需求调整安全控制。

CCM 的另一个重要优势是它支持云治理。它帮助云服务提供商建立和维护可靠的云治理计划，从而有效地管理和监督云风险。这有助于确保云部署与组织目标相一致，并符合相关法规。

CCM 通过不断更新来反映最新的云安全最佳实践。云服务提供商和云客户可以依靠 CCM 作为可靠的资源来满足他们的云安全需求，并维持最新状态。总体而言，云安全框架是云客户建立强大而有效的云安全计划的必备工具。通过选择特定的云框架、附加云安全框架、确认组织安全控制目标，云客户可以全面解决云安全问题，并使其流程与云的独特要求保持一致。

2.3.4 策略

信息安全策略对于建立强大的安全框架非常重要。策略管理着组织信息资产的保护，并概述了必要的控制目标。例如，请参阅 CIS36 发布的 NIST CSF 策略模板指南。

为了确保策略的有效性，建议组织领导层正式批准这些策略。这样的批准赋予策略的权威性，并表明领导层致力于执行这些策略。有了领导层的支持，策略的实施将更加有效。

通常，遵守各种监管和法律框架在信息安全策略的制定中发挥着重要作用，例如数据隐私的 GDPR 或针对财务报告的萨班斯法案 (SOX)。组织需要制定具体策略来满足这些合规标准，这对于确保符合外部要求和避免处罚至关重要。

2.3.4.1 策略类型

组织通常实施的信息安全策略有以下几个示例：

● 信息安全策略是定义信息安全计划应如何运行的最高级别政策。它通常会参考控制目标和其他策略文件，而不是试图包含所有具体的技术要求。

● 可接受使用策略 (AUP)定义了组织 IT 资源的适当用途。

● 远程工作策略概述了远程工作时，要对员工采取的安全措施和行为。

● 云服务使用策略规定了在云中使用数据的要求。

● 数据处理策略描述了数据如何分类、处理、存储和处置，以维护其机密性、完整性和可用性。

信息安全策略是必不可少的可执行文件，它通过为安全实践和行为提供清晰的框架来推动安全实践并加强网络安全文化。它们确保在不同环境中应用适当级别的保护。员工必须熟悉自己特定的信息安全策略，并理解自己在维护这些策略方面的作用，以促进整体安全态势。

2.3.5 云安全控制目标

云安全控制目标是云环境中所需的控制清单。这些目标是面向结果的，这意味着应该优先考虑结果而不是实现方式。这些目标应按照 SMART 原则（具体的、可测量的、可实现的、有时限的）进行衡量。

控制目标应该与平台无关，这意味着没有特定的云服务提供商或技术限制控制目标。这使得控制目标适用于各种云环境，确保其相关性和有效性。

实施的每个安全控制措施都应至少对应一个特定的控制目标。这确保了每项措施都有明确的目的，并有助于实现云环境的总体安全目标。

最后，控制措施应给出明确定义，并专注于实际的安全结果的实现，避免使用模糊指令。目标应详细说明，提供明确的指导方向，但不必过于具体，以免变成按部就班的操作程序。

总之，云安全控制目标指导在云环境下建立强大的安全态势。它们具有适应性、可衡量性和以结果为导向，与云计算的动态特性相一致。组织可以通过遵循这些目标，增强云安全性并降低潜在风险。

2.3.5.1 将控制目标映射到框架

安全计划中的控制目标应该与所使用的框架保持一致。这种结构化方法确保了计划涵盖所有必要的领域。计划的一致性也与大型组织的结构和运营职责相对应。

框架是安全计划的基础，概述了总体结构和方法。另一方面，控制目标定义了期望的结果和目标。将控制目标与框架相关联，可确保计划具有适当的、明确的范围。

值得注意的是，如果控制目标与框架不一致，则表明该战略存在差距。应解决这种不一致问题，以确保该计划的全面有效。同样，在框架中特定类别的控制目标也不足以表明存在需要解决的运营缺陷。

为了保持这种映射关系，建议直接将它包含在控制目标库中。这样可以方便地进行参考，并与文档相一致。CSA CCM 是一个示范框架，具有与相关框架、标准、法律和监管要求的全面映射列表，使其成为进行复杂治理时参考的宝贵资源。

2.3.5.2 控制规范

控制规范是确保云环境安全的重要组成部分。这些规范概述了必须实施的详细技术控制功能，以满足特定安全要求。需要注意的是，控制规范应针对特定供应商和技术，这意味着不同的云服务提供商之间可能存在显著差异。

例如，考虑实施 多因素认证（MFA）的要求。启用 MFA 的技术程序将因云服务提供商而异。每个云服务提供商都有自己独特的配置和实施 MFA 的方式，因此需要创建特定于不同云服务提供商的控制规范。

另一个可能会存在差异的控制规范是网络安全。默认情况下，Azure 将其网络设置为对入站连接开放，这意味着必须配置额外的网络安全组才能确保安全环境。另一方面，AWS 将其网络默认设置为入站连接的最低权限级别，从而提供了更高级别的安全性。此外，Azure支持允许和拒绝网络安全规则设定，而AWS 仅支持允许规则并拒绝所有其他流量。这些差异解释了需要根据特定的云服务提供商定制控制规范。

此外，控制要求可能会根据数据或资源的分类而有所不同。例如，如果云客户处理个人身份信息 (PII)，则默认设置可能会具有更严格的控制要求。另一方面，被视为公开的数据可能具有较少的限制要求。在定义控制规范时，考虑数据或资源的敏感性是非常重要的。

在某些情况下，控制措施无法在云服务提供商的生态系统内完全实施，可能需要第三方工具。这些工具可以提供额外的功能，并增强云环境的安全态势。当使用第三方工具时，定义控制规范非常重要，如：为了满足控制目标和要求，如何配置工具。这确保第三方工具有效地集成到安全策略中。控制规范应随着时间推移而不断发展，以适应技术进步、新产品以及新的威胁和攻击媒介。修订并采用修订后的最新规范具有重要的意义。

2.3.6 责任共担模型

责任共担模型 (SSRM)是一个基本的云安全概念。它规定了云客户和云服务提供商有不同但互补的责任，以确保云服务正常运行并保持安全状态。这种责任共担可以扩展到云服务提供商和云客户之外，涉及其他提供服务的各方，例如支持云服务提供商、代理商和云平台集成商。

就其组织内部透明度而言，云客户需要清楚地了解内部 IT 团队如何在其组织内的不同控制功能中映射责任共担模型。组织需要对其计划部署的工作、负载数量和在云中使用的服务进行适当的探索，例如：需要多少人来操作控制才能使服务值得信赖？某些决定将由此产生：组织是否需要扩大内部规模，如：通过雇用全职员工或与外部顾问合作？在组织内部需要明确责任并反映在企业运营方式中，以避免其责任结束和云服务提供商责任开始之间出现的差距。在双方的协议中描述这些责任并且确切解释会很有益处。

云服务的变化比传统 IT 服务更加迅速，新服务不断发布，旧服务不断被淘汰。因此，随着提供商增加新的服务和升级现有服务，责任共担模型可以随着时间而演变。例如，如果云服务提供商停用某项特定的服务，那么最重要的就是了解谁负责管理数据迁移和转换到新服务的生命周期。因此，所有各方都需要在服务的整个生命周期中考虑各自的责任，而不是在某个时间点。

还值得注意的是，云客户可能会根据云服务的性质增加风险。云中的非核心服务可能面临着被替换或实质性变更的风险。与核心服务形成依赖链可以让它继续存在一段时间，并且对基础服务的变更会给该服务的所有用户带来更高的成本。

总之，责任共担模型划分了安全和治理责任，这些责任根据云服务模型和安全域的不同而有所不同。

2.3.6.1 责任与义务

云客户可能无法完全了解其云服务提供商的基础设施和流程，但仍需对上云进行治理。使用未经授权的云服务（称为“影子 IT”）也会带来额外的内部挑战，即某个员工或部门在 IT 和安全团队不知情的情况下使用云服务。管理这种风险 38 就应设计和实施覆盖影子 IT 及相关风险的认知计划。

2.4 关键战略和概念

本节探讨云计算安全和治理中的重要战略和概念。首先是 DevOps 和 DevSecOps，它们可以帮助使软件开发流程更快、更安全。本节还探讨了零信任安全策略，该策略侧重于不断验证和控制访问以阻止新威胁。最后，本节研究了人工智能 (AI) 和机器学习 (ML) 如何在云安全中用于快速预测和发现问题。总之，本节展示了如何塑造云计算中的安全和治理，使其更易于理解和控制。

2.4.1 DevOps

DevOps 是一组将软件开发 (Dev) 与 IT 运营 (Ops) 相结合的实践，旨在缩短安全软件开发生命周期 (SSDLC39)，同时根据业务目标频繁地提供功能、修复和更新。在云计算中，由于云的敏捷性、可扩展性和灵活性，DevOps方法对于部署和管理应用程序和基础设施至关重要。云客户可以通过自动化将 DevOps方法扩展为更具战略性、更敏捷的组织应用程序开发方法。

2.4.1.1 DevSecOps

DevSecOps 是一种安全方法，它将安全实践集成到整个安全软件开发生命周期中，从初始设计到部署，再到持续监控。通过在每个阶段集成安全实践，DevSecOps 使云客户能够尽早识别和缓解潜在的安全风险和漏洞，从而打造更安全、更具弹性的软件应用程序。

CSA 已经确定了支持安全和高效的 DevSecOps 实施的六个关键支柱，如下图所示。这些支柱与 DevOps 交付流程的五个阶段保持一致，为将安全性纳入软件开发过程打下了全面的基础。

图 12：CSA DevSecOps 的六大支柱

图 13：CSA SSDLC 流水线的五个阶段

通过利用 CSA DevSecOps 交付流程的六大支柱和五个阶段，云客户可以构建安全高效的开发流程，从而创建内置安全的、可靠的高质量应用程序。

2.4.2 零信任安全策略

在当今云计算和远程办公时代，传统的“城堡和护城河”边界安全架构已失效。因为广泛使用互联网连接，日益复杂的威胁善于利用分布式企业网络中任何暴露的技术或人为漏洞。重大的安全漏洞经常被公开报道。这些事件给云客户造成更多的损失，超出了他们实施安全体系结构所花的费用。现代安全体系采用不断成熟的零信任安全策略。

零信任是一种全面的安全策略，包括云/多云、内部和外部合作伙伴/利益相关者、本地/混合系统，并包括运营技术(OT) 和物联网（IoT）。零信任的实施涉及到基于风险设计原则定义企业安全架构，并利用多种产品/服务和已建立的安全原则，例如，因需而知和最小特权。它建议从内向外进行安全设计，而不是从外到内，并增强了可视性和促进自动化、实时响应，使组织能够跟上不断变化的威胁环境。

零信任考虑到越来越复杂和具有攻击性的威胁。这是一种网络安全策略，它基于没有任何用户或资产可以被默认信任的思想。它假设入侵已经发生或将会发生，因此，不应通过在组织边界执行的单一验证授予用户访问敏感信息的权限。相反，每个用户、设备、应用和交易都必须持续验证。零信任的关键设计原则包括：

- 使访问控制更接近组织资源
- 默认拒绝访问
- 持续验证用户和设备的明确授权、细粒度的访问权限
- 实施网络微隔离以限制横向移动
- 密切监视所有访问
- 加密所有网络流量
- 实时分析访问模式，及时发现并应对异常

如果正确实施，零信任策略和架构有可能为业务运营提供更简单、更安全和更灵活的环境。

2.4.3 人工智能与机器学习

在云安全中使用人工智能（AI）或机器学习（ ML） 涉及到使用自动推理。机器学习是人工智能的一个子集，它涉及提取数据和设计算法、从中学习，然后应用所学知识做出明智决策。

云服务提供商通过分析海量数据，再利用人工智能技术来检测安全配置和威胁，而这些数据可能过于复杂，难以依靠人工监管。例如，无监督学习可用于识别某些来自合法访问的威胁，而无需依赖标签。当采用自动化纠错时，这些技术更具威力。

生成式人工智能，包括大语言模型 (LLMs)，从大型数据集中学习模式和结构以生成内容，例如文本、图像和视频。这些人工智能模型通常在云端运行，因为它们需要大量弹性的计算能力和数据存储要求。特别是在处理数据隔离和保护重要的共享资源的时候，更需要考虑在云中运行生成式人工智能引发的数据隐私和应用程序设计方面的问题。

鉴于人工智能和机器学习技术带来的复杂性，NIST 发布了人工智能风险管理框架，旨在改善人工智能系统和模型使用的可信度。该框架本身提供了识别与人工智能系统相关的风险指南，并建议采用四个步骤来管理整个 AI 生命周期中的风险，包括治理、映射、衡量和管理。

图 14：人工智能风险管理框架

与 NIST 框架同步，ISO/IEC 发布了《信息技术-人工智能管理系统》（ISO/IEC 42001:2023），规定了在组织内建立、实施、维护和持续改进人工智能管理系统的要求。它专为提供或利用基于人工智能的产品或服务的实体而设计， 确保负责地开发和使用人工智能系统。它解决了人工智能带来的独特挑战，例如伦理道德考虑、透明度和持续学习。对于组织而言，它提出了一种结构化的方式来管理与人工智能相关的风险和机遇，平衡创新与治理之间的关系。

图 15：ISO/IEC AI 风险管理生命周期

实施 DevSecOps、零信任和人工智能/机器学习 等策略，并遵守 ISO/IEC 42001:2023 等框架，可以确保云环境的稳健和安全。这些实践不仅可以降低风险，还可以提高基于云系统的可信度和可靠性。

总结

有效的云治理是管理云中 IT 基础架构的关键方面，也是有效企业治理不可或缺的一部分。在传统数据中心中，整个 IT 基础设施由集中式团队控制，因此云计算需要采用不同的治理方法。

为了实现有效的云治理，调整组织结构是必不可少的。传统的层级结构可能不再适用。重新评估结构，并建立与云环境相符的角色和职责至关重要。

与此同时，识别和记录风险、监管和安全要求也很重要。在云中，数据可能在多个位置存储和处理，并受到不同法规的监管和合规性标准的约束。识别和记录这些要求对于确保云基础设施保持合规和安全非常必要。

所选治理框架提供了高层的治理要求，并为其余的治理设定了方向。云客户应始终将治理与业务战略保持一致，以确保采用正确的控制措施和指导方针。

云客户应确立明确的角色和职责，建立云卓越中心（CCoE），评估和管理风险，并建立云资产、访问和内部资源治理流程和程序。治理必须包括建立关键指标和测量方法，并定期重新评估组织和云服务提供商的安全状况。

建议

- 了解云计算的技术和运营差异需要新的治理方法来维持有效的安全性。
- 使用云卓越中心（CCoE） 和 云访问控制列表（CACl） 等概念调整组织结构，以提高治理云的能力。
- 实施“安全冠军”计划，更有效地传播安全知识，特别是面向开发团队和云团队。
- 收集并理解您的基础需求，包括您的风险容忍度、合规义务、业务需求和现有的云使用情况。
- 从安全框架入手，安排您的安全策略、控制目标和控制规范，形成明确的治理体系。

- 理解云环境中常见的策略和概念，确定它们对安全和治理产生的影响，包括 DevOps、零信任和人工智能。

补充指南

- 云安全技术参考架构 | CISA
- 零信任的商业价值布道 | CSA
- 零信任指导原则 | CSA
- 面向云客户的 SaaS 治理最佳实践 | CSA
- COBIT 框架 | ISACA
- ISO/IEC TR 3445:2022 信息技术云计算云服务审计

领域 3：风险、审计与合规

此领域专注于云安全的核心方面，因为它们与风险、审计和合规性问题有关。但是，应该注意的是，此领域并不能取代全面的风险、审计和合规性方面的全面培训和经验。对于那些希望深入研究这些主题的人来说，推荐由 CSA 与 ISACA 合作提供的云计算审 计知识证书（CCAK）。

在云风险方面，该领域探讨了评估云服务提供商 (CSP) 的方法。它涵盖了云风险注册中心的建立和审批流程的实施。此外，它还参考了 CSA 的“顶级威胁”提供常见风险的背景信息。

此领域概述了合规性和审计、不同类型的合规性以及合规性继承的概念。为了协助治理、风险和合规性(GRC) 流程，该领域引入了各种工具和技术。这包括策略、程序、控制、自动化的作用、软件物料清单(SBOM) 和相关技术。总的来说，这些组件支持治理框架并帮助管理复杂的云计算风险和合规性要求。

学习目标

在此领域，您将学习：

- 定义、分类和使用工具来管理云风险。
- 确定您的基于云的环境必须接受审核的监管和合规性限制。
- 确定管理 GRC 时使用的一组技术和非技术工具。

3.1 云风险管理

在当今的数字环境中，有效的云风险管理是必不可少的，因为组织越来越依赖云服务。本节深入探讨了了解云风险的重要性，并提供了有关建立云风险概况、评估 CSP、维护云风险注册表以及进行风险评估、威胁情报和威胁建模的见解。通过实施强大的云风险管理实践，组织可以主动识别和减轻潜在风险，确保其云环境的安全性和韧性。

3.1.1 云风险

让我们从一个例子开始。一家公司有一个云存储桶，里面装满了客户的个人信息。我们称之为资产，对于攻击者来说（也称为威胁行为者）是目标。云存储桶的弱点之一是它可能配置错误。我们称之为脆弱性对于攻击者来 说，这意味着攻击向量。

风险：风险在于存储桶中的个人数据泄露，公司因此受到监管机构的罚款。另一个风险在于，由于某些行为，数据变得不可用或损坏。

控制或者对策：是一种降低风险的方法。此处的典型控制措施是任何可防止整个互联网（或更具体地说是威胁行为者）访问这些存储桶的策略。

理想情况下，我们会有足够的控制措施将风险降低到可接受的水平。这包括了解重要的资产和威胁行为者是什么。这个过程称为威胁建模 并在本指南的其他地方进行了讨论，例如应用程序安全。在云世界中，威胁建模首先要确定存储数据的各个位置和云服务，以及数据在它们之间的流动方式。另请参阅 CSA 研究报告《Cloud Threat Modeling》。

以下示例显示了一些最常见的风险因素和类别，包括一般风险和安全风险。我们还建议查看云安全联盟的“顶级威胁研究报告”。在 2024 年版“云计算的 11 类顶级威胁”中，排名前几的类别如下：

- 配置错误与变更控制不足
- 身份与访问管理（IAM）
- 不安全的接口与 APIs
- 云安全策略缺失
- 不安全的第三方资源
- 不安全的软件开发
- 意外的数据泄露
- 系统漏洞
- 云可见性/可观测性不足
- 未验证的资源共享
- 高级持续性威胁 (APT)

还有许多其他云威胁情报来源。请查阅 CSA 网站以获取最新信息。此外 MITRE ATT&CK 框架提供了威胁行为者策略的综合矩阵。

3.1.2 建立云风险概况

对于依赖云服务的组织来说，云风险概况是一项重要的评估。作为网络风险分析师和审计师的基础指南，该概况提供了对 CSC 风险状况的洞察。它使组织能够了解其风险敞口，确保其云战略与业务目标在其风险偏好范围内保持一致。

3.1.2.1 云风险概况入门问题

风险评估的第一步是确定组织的云风险状况，这可以通过风险评估问题来实现。请考虑以下问题作为组织评估其风险状况的起点。它们不一定是详尽无遗的，也不一定是特定云客户 (CSC) 应该使用的确切问题。

- 与业务战略保持一致：
  - 云计算技术如何与整体业务战略相契合？
  - 采用云计算如何支持组织的战略目标？
  - 云计算能为商业模式带来什么好处？如何提升运营效率或市场竞争力？
- 信息安全或网络安全策略：
  - 信息安全或网络安全策略是否已更新以反映云技术管理？
  - 信息安全或网络安全策略多久审查和更新一次以纳入由于采用云计算而产生的变化？
  - 所有相关利益相关者是否都参与审查和更新信息安全或网络安全策略？
- 云计算的第三方风险评估：
  - 第三方风险评估是否包括特定于云计算技术的风险（例如基于数据隐私和安全法）？
  - 第三方风险评估在评估 CSP 方面有多全面
  - 评估是否针对数据隐私、安全法规和行业法规合规性等特定风险？
  - 云风险的评估是否与组织的整体风险偏好和风险承受能力相符？

- 云迁移风险评估：
  - 在云迁移之前是否进行了全面的风险评估，特别关注与云技术相关的风险？
  - 云迁移风险评估结果如何融入整体风险管理计划？
- CSP 和合同档案：
  - 是否有所有 CSP 的集中档案，包括合同、服务水平协议 (SLA) 以及第三方评估或证明报告的详细信息？
  - 如何根据合同监控和审查 CSP 的绩效和合规性？
- 业务连续性/灾难恢复（BC/DR）计划：
  - 组织的 BC/DR 计划是否已更新以反映云的采用？
  - 组织的 BC/DR 计划如何适应云服务？
  - 如果发生云服务故障，是否有针对 BC/DR 的特殊考虑？
  - BC/DR 计划是否记录了 CSP 的职责和依赖关系？
- 云迁移后隐私策略更新：
  - 组织隐私策略是否已更新以包含云采用？
  - 组织隐私策略如何修改以解决云中的数据收集、存储、处理、管理、保留和销毁问题？
  - 更新后的隐私策略是否充分涵盖数据驻留、跨境数据传输和用户同意机制？
- 事件管理策略：
  - 事件管理策略如何更新以包括涉及云服务的事件？
  - 是否有明确的程序来应对涉及基于云的资产的安全漏洞或数据泄露？
  - 是否定义并记录了与 CSP 的事件相关沟通渠道？
- 安全软件开发生命周期 (SSDLC)：
  - 组织的 SSDLC 是否已更新以反映云迁移？
  - SSDLC 如何进行修改以纳入特定于云的安全考虑因素，特别是涉及 API 安全、身份和访问管理以及加密的因素？
  - 云感知安全工具和实践是否集成到 SSDLC 的开发、部署和维护阶段？

3.1.2.2 使用云风险概况

建立云风险概况的结果可用于指导其余的云风险管理流程。目标是确定风险承受能力和当前的云风险状况。云风险概况应该代表 CSC 在风险方面为迁移到云所做的准备程度。

CSC 还应考虑采用云安全框架和标准（例如 CSA 提供的框架和标准），以帮助更详细地对实践进行基准测试并确保云环境中的全面风险管理。

3.1.3 了解云风险管理

了解云风险管理涉及一种结构化的方法来识别、评估和解决与云计算相关的风险。云计算中使用的风险管理和方法与本地环境中采用的风险管理和方法并无不同。然而，在定义范围和环境以及风险评估和处理过程中采取的一些具体行动可能会发生变化。

欧洲网络和信息安全局(ENISA)风险管理流程为组织提供了一个可以有效管理这些风险的框架。此流程旨在集成到 CSC 更广泛的运营流程中，确保采用全面的风险管理方法。以下是此流程关键组件的扩展：

- 企业风险管理策略
    - 包括风险沟通、意识和咨询
- 风险评估
- 风险处理
    - 包括风险接受
- 与其他操作和产品流程的接口
- 监控和审查计划、事件和质量

图 16：综合云风险管理框

3.1.3.1 公司风险管理策略

此阶段旨在创建风险管理环境并制定具体的风险标准来指导评估过程。

● 风险管理范围和框架的定义：为风险管理流程涵盖的内容设定明确的界限，包括云服务和运营的具体方面。

● 外部环境的定义：了解可能影响云运营的外部因素，例如监管要求、市场条件和技术进步。

● 内部环境的定义：评估影响风险管理的内部因素，包括组织结构、文化、风险偏好、风险承受能力和现有控制措施。

● 风险管理背景的生成：创建与组织目标相一致的环境，实现有针对性的、有效的风险管理策略。

● 风险标准的制定：制定适合具体情况的风险评估标准，包括发生的可能性和潜在影响。

● 风险沟通：提高风险意识，咨询相关利益相关者，并确保适当共享有关风险和风险管理活动的信息。

● 风险意识：提高对云风险管理的重要性和正在解决的具体风险的认识。实施有效传播有关风险和风险管理活动信息的机制，以确保所有相关利益相关方都了解情况。

● 咨询：与利益相关者合作以收集见解并确保在风险管理过程中考虑到不同的观点。

3.1.3.2 风险评估

这涉及评估每种风险以确定发生的可能性及其后果的严重性。

- 风险识别：系统地识别与云服务相关的潜在风险，包括安全漏洞、数据丢失和违背合规性。
- 相关风险分析：分析已识别的风险以了解其性质、原因和潜在影响。
- 风险评估：评估每种风险的可能性和影响，并根据其对目标的潜在影响确定其优先次序。

3.1.3.2 风险处理

评估风险后，制定并批准一项行动计划，以缓解、转移、避免或接受每种风险。实施这些行动计划并确定任何剩余（残留）风险：

- 识别选项：探索不同的风险管理策略，例如缓解、转移、避免或接受。
- 制定行动计划：考虑资源和风险偏好，制定具体行动来减轻或解决每个风险。
- 批准行动计划：确保行动计划得到适当的决策者和利益相关者的审查和批准。
- 行动计划实施：在可接受的时间范围内执行已批准的行动来管理已识别的风险。
- 识别剩余风险：评估并记录实施治疗措施后的剩余风险。
- 风险承受能力：如果剩余风险在风险偏好范围内，并且进一步减轻风险的成本大于其影响，则接受剩余风险。
    - 接受风险的决定应该由企业主在充分了解风险的含义和可能的后果之后，进行成本效益分析之后做出。
    - 剩余风险、分析和验收应清晰地记录。
    - 应定期重新评估已接受的风险，以识别风险状况、风险偏好或可用的具有成本效益的缓解措施的任何变化。

3.1.3.4 与其他操作和产品流程的接口

风险管理不应孤立；它应该与其他业务流程相结合，以确保风险考虑贯穿于 CSC 的整个运营和产品生命周期。

3.1.3.5 监控和审查（计划、事件、质量）

持续监控风险管理计划、事件和风险管理活动的质量。定期审查可确保风险管理流程保持有效并适应业务环境的任何变化。

- 持续监控云环境、风险管理计划和实施控制的有效性。
- 定期审查风险管理流程，以确保其在应对不断变化的风险状况和组织变化方面仍然具有相关性和有效性。
- 实施相关指标来评估已实施风险处理的有效性和效率，例如关键控制指标。
- 评估剩余风险，确保其仍在可接受的水平。关键风险指标可以协助及时监控云风险状况。

遵循 ENISA 风险管理流程，CSC 可以建立一个强大的云风险管理框架，并将其与总体风险管理战略和运营实践相结合。这种方法有助于缓解特定的云相关风险，并增强组织在应对云计算环境复杂性方面的弹性和敏捷性。

3.1.4 评估云服务

管理云风险的第一步是建立系统流程来评估 CSP 及其服务产品。此评估应与业务需求和风险承受能力保持一致。评估 CSP 的挑战在于，CSC 很少能够了解所有 CSP 内部运营和技术。CSP 不断改变其服务；在某些情况下，他们可能每周都会增加重大服务变更。CSC 也可能缺乏通过定制 SLA 和合同进行补偿的能力。

以下流程旨在解决这些差异：

- 业务请求
- 查看 CSP 文档
- 审查外部来源
- 映射到合规性要求
- 映射到数据分类
- 定义所需控制和补偿控制
- 审批流程

图 17：评估和批准云服务的系统流程

3.1.4.1 业务需求

CSC 的业务部门请求使用 CSP 和服务（例如，Azure 等大型提供商中的 PaaS 服务）。了解业务需求（包括所需的特定 CSP 和服务）是评估采用特定云解决方案的风险的第一步。

- 了解业务需求：收集业务部门和其他请求云服务的利益相关者的详细要求。其中包括特定功能、性能期望以及监管或数据处理要求。
- 提供商和服务选择：评估潜在的 CSP 及其服务（例如，PaaS、IaaS、SaaS），以确定哪个最适合业务需求。

3.1.4.2 审查云服务提供商（CSP）文档

- 仔细检查 CSP文档。确保其中包含 CSA 共识评估倡议调查问卷（CAIQ）了解安全细节、CSP 持有的任何认证、详细的安全以及隐私策略和服务条款（ToS）。
- CAIQ 和认证：CAIQ 提供了一套全面的问题，CSP 可以通过回答这些问题来披露其安全控制措施。CSP 认证（例如 ISO/IEC 27001、SOC2）可对其安全实践进行第三方验证。
- 安全和隐私文档：审查 CSP 发布的安全性策略、隐私策略和数据处理实践，以确保它们符合相关标准。
- 服务水平协议 (SLA) 和合同：SLA 概述了 CSP 的性能和正常运行时间承诺，而合同则详细说明了服务条款，包括责任和义务。
- 服务条款：了解服务条款对于避免采用后出现法律或运营意外至关重要。这可能是 CSC 和 CSP 之间唯一的合法合同。

3.1.4.3 审查外部来源

除了审查 CSP 文档外，CSC 还可以考虑使用云访问安全代理 (CASB)、云安全态势管理 (CSPM)、云工作负载保护平台 (CWPP) 和 SaaS 安全态势管理 (SSPM) 解决方案等工具进行独立评估。CSC 应该对与 CSP 相关的评论、漏洞和安全事件进行额外研究。这通常也是与提供商一起审查调查结果的好时机，尽管这可能仅限于较大的项目或较小的 CSP。

- 工具：利用工具进行持续的第三方风险监控。
- 研究：调查外部评论、报告的漏洞以及涉及 CSP 的任何过去的安全事件，以评估其安全态势和响应能力。
- 提供商互动：对于重大项目，请考虑直接与 CSP 联系，讨论调查结果和任何疑虑。这可以提供清晰度和保证。

3.1.4.4 合规性映射

在选择 CSP 时，必须使其功能和策略与组织的合规性需求保持一致，例如通用数据保护条例 (GDPR)、健康保险携带与责任法案 (HIPAA) 或支付卡行业数据安全标准 (PCI DSS)。这可确保满足监管要求并确保数据安全。大多数 CSP 都会发布详细的合规性文档，以证明其遵守各种标准和法规。

3.1.4.5 映射到数据分类

并非所有数据都需要相同的风险管理流程。CSP 和服务应根据数据类型进行批准，以便灵活地适应不同的 CSC 需求和要求。例如，使用价值较低或公开的数据且风险较高的服务可能是可以接受的。

- 数据敏感性评估：评估传输中和静止数据的敏感度。并非所有数据都具有相同的风险；因此，并非所有云服务都需要满足最高安全标准。
- 根据数据类型进行服务审批：根据 CSP 处理的数据分类来批准 CSP 及其服务。这种方法可以实现灵活性和资源的有效利用。

3.1.4.6 定义所需补偿控制

在最终批准之前，重要的是选择并记录所需的控制（例如，CSP 内的配置设置）以及任何提供适当安全级别以减轻云风险的补偿控制（例如，第三方工具）。

3.1.4.7 批准数据类型并注册登记

根据收集到的信息和映射，确定 CSP 的服务是否适合预期的数据类型。如果适合，则批准其使用并将其纳入云服务注册表。

3.1.5 云注册表

云注册表是已获批准的 CSP 和服务的中央存储库，以及它们在给定风险级别下获准处理哪些类型的数据。这可以指导内部决策，确定哪些提供商和服务用于哪些项目。它还有助于确保数据仅与合规提供商一起使用。

3.1.5.1 了解云注册表

云注册表是一种战略工具，它记录了 CSC 使用的所有云服务，以及有关其处理的数据类型、评估的风险级别以及何时应审查风险评估的信息。它区分了不同的数据类型（例如，公共、敏感、个人身份信息）并分配风险级别来指导云服务的使用。

3.1.5.2 云注册表的组成部分

云注册表包括服务的 CSP、特定服务本身、允许其处理的数据类型、风险级别（例如，严重、高、中等、低）、到期日期以及风险评估必须重新评估时的其他关键属性。属性可能包括名称、描述、所有者、预期/实际频率、潜在/实际量级、潜在/实际业务影响和处置。

3.1.5.3 云注册表的目的

云注册表简化了审计期间用于评估 CSP 的数据和操作是否符合适用要求的决策流程。它作为一个集中式数据库，列出了已批准的云服务，并根据 CSP 获准处理的数据类型对其进行分类。这不仅可以确保团队符合组织标准和合规性要求，还可以最大限度地减少评估 CSP 的重复工作。通

过查阅注册表，团队可以快速确定哪些服务可用于其特定的数据管理要求，从而加快项目启动并减少管理开销。

3.1.5.4 风险等级和到期日

固有风险和残留风险通常以风险等级表示，例如严重、高、中、低。风险是根据影响和可能性得出的。风险等级决定了审查和审计的频率和强度。例如，处理个人身份信息 (PII) 的服务被归类为严重风险的服务可能会比被归类为中等风险的服务接受更频繁的审查。

表 2：云注册表示例

提供者	服务	数据类型	风险	到期
ABC	对象存储	公开、敏感	低的	年度
ABC	虚拟网络	全部	低的	年度
GHI	CRM 软件即服务	个人身份信息	缓和	季度

这个虚构的例子展示了两个提供商提供的三种特定服务，并列出了允许处理的数据类型。在此基础上，分配风险和所需的审查频率。这使团队能够加快风险评估。

3.1.6 风险评估、威胁情报和建模

将风险评估与威胁情报和建模相结合可改善 CSC 的网络安全态势，尤其是在云计算环境中。随着威胁形势和云技术的发展，这需要不断努力和更新。组织可以通过利用 CSA 和 MITRE 提供的框架并在 SSDLC 中开展全面的威胁建模，更好地准备和降低与云计算相关的风险。这种主动的网络安全方法可确保云部署高效、有效且安全。

- 风险与威胁：
    - 风险是广义的类别，指的是潜在的负面结果，而威胁则代表对手的机会。风险包括威胁行为者利用漏洞或其他安全缺陷而导致资产损失、损坏或毁坏的可能性。
    - 威胁更加具体，代表与旨在利用这些漏洞的对抗性攻击直接相关的风险子集。
- 当前威胁形势：

- 了解云安全领域的最新威胁非常重要，因为威胁形势瞬息万变且不断发展。了解 CSP 及其服务面临的实际威胁是有效评估和降低云部署风险的关键。

- 威胁建模：
  - 威胁建模是 SSDLC 不可或缺的一部分。它是一种结构化方法，可以在保护特定应用程序或系统的背景下识别和缓解潜在威胁，例如结构漏洞或隐私漏洞。

- CSA 的“顶级威胁”：
  - CSA“顶级威胁”经常更新以识别主要的云威胁，并包括特定技术和公共漏洞的示例。

- 其他威胁情报来源：
  - 其他有价值的威胁情报资源包括：
    - MITRE ATT&CK 框架，它提供了全面的策略矩阵。
    - CSA 研究报告《Understanding Cloud Attack Vectors》：由行业为行业创建，对供应商中立且以共识为驱动。

3.2 合规与审计

合规性和审计对于确保信息系统遵守既定的标准、法律、法规和策略以保护数据完整性、可用性和机密性至关重要。这些流程旨在识别漏洞、评估风险并实施控制措施以减轻对信息资产的威胁。

合规性涉及遵守一组管理安全实践的预定义标准或法规。合规性确保组织实施一组规定的安全措施来保护敏感信息和系统。

审计是对记录、操作、流程和控制的独立检查，以确保遵守安全策略、标准和法规。审计有助于发现安全措施中的漏洞并验证实施的控制的有效性。审计可以是内部审计，即由 CSC 自己的审计人员进行，也可以是外部审计，即由独立的第三方进行。定期审计可确保合规性、促进安全态势改善并与客户和合作伙伴建立信任。

3.2.1 合规性类型和云影响

云环境中的合规性是多方面的，包括法律和监管要求、遵守国际、国家、地区和行业标准以及与内部策略和标准的一致性。云计算的动态、分布式和可扩展性为合规性带来了独特的挑战和担忧。下面我们将深入探讨这些方面。

3.2.1.1 合规要求

CSC 必须在利用云服务优势与保持合规性之间取得平衡，以保护其资产并履行其法律和监管义务。以下是影响合规性要求的一些合同要求、标准和内部策略的示例：

- 法律、法规和合同要求：
  - 云服务通常跨多个司法管辖区运营，这些司法管辖区可能有不同的法律和监管要求。跟踪这些变化对于保持合规性至关重要。
  - 合规性继承是指使用已经满足某些合规性标准的云服务。
  - 持续监控存储或处理数据的司法管辖区的法律和监管要求变化。明智地实施合规性继承策略， 利用 CSP 认证，同时确保端到端合规性。
  - 遵守跨境数据传输的法律和监管框架，这对于跨国家运营至关重要。这需要全面遵守国际和地区数据保护法规。
- 国际、国家、行业标准：
  - 收集合规性证据可以手动或通过自动化方式进行。云环境通常有利于自动化，这可能更高效， 但需要适当的工具。
  - 一个重大的挑战是，许多既定的标准尚未更新以反映云计算的特定需求和特点，这可能会留下合规方面的差距。
  - 投资合规性证据收集自动化工具，以提高效率和准确性。积极参与行业论坛或监管机构，倡导并推动制定反映云计算现实的最新标准。
- 内部策略和标准：
  - CSC 可能会发现其现有的内部标准和控制并不完全适合云环境。有必要将这些标准调整到云中，以确保。

3.2.2 云相关法律法规示例

有许多法律法规保护各种数据类型，如个人信息、金融数据和关键的国家基础设施技术。有无数的法规需要掌握，每个 CSC 都有义务了解自己特定的法律和法规要求。以下是通常影响云安全性和遵从性的法规和行业标准的一些代表性示例。

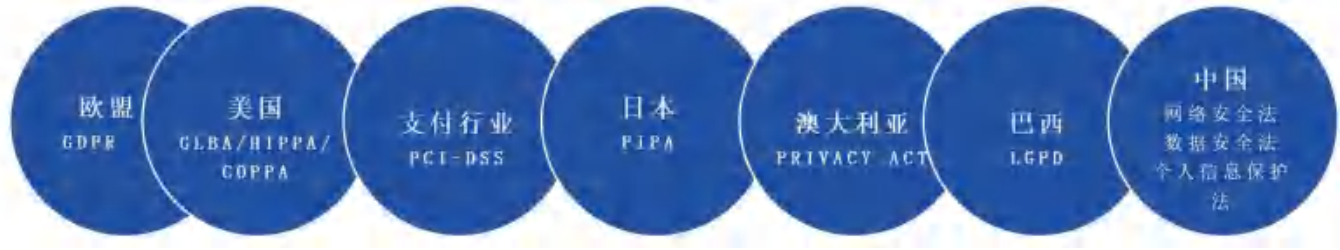


图 18：影响云服务的关键隐私和安全法规

3.2.2.1 隐私法律法规

- 欧盟 GDPR：为数据保护设定了高标准，强调个人对其个人数据的权利，要求数据处理时征得同意，并对不遵守规定的行为施以严厉的处罚。
- 美国法规（CCPA/COPPA）：专注于特定领域，保护
    - 儿童网络隐私保护法（COPPA）
    - 加州消费者隐私法案（CCPA）以及其他类似的州级法案对处理和保护数据都有详细的要求。
- 巴西 LGPD：代表通用个人数据保护法，主要基于欧盟 GDPR。与欧盟法律一样，它也为数据保护设定了高标准，强调个人对其数据的权利，要求在收集和处理数据时征得同意，并对违法行为处以严厉处罚。
- 日本个人信息保护法、澳大利亚隐私法：规范个人信息收集、使用和披露的国家法律，重点关注用户同意、数据准确性和跨境数据流动限制。

3.2.2.2 其他相关法律法规

- 美国法规：

- 《格雷姆-里奇-比利雷法案》（GLBA），该法案规定了美国金融机构保护消费者信息的要求。
- 《健康保险携带与责任法案》（HIPAA）通过制定有关医疗保健提供者、保险公司和其他数据 处理人员如何使用和披露个人健康信息的规定来保护医疗隐私。

● 欧盟法律法规：

- 欧盟数字运营弹性法案 (DORA) 确保在公有云平台上运行的关键金融市场基础设施的运营弹性。
- 欧盟人工智能法案制定了必要的法规，以确保人工智能（AI）系统的可信度。
- NIS 2 是最近实施的网络和信息系统指令的更新版本，加强了欧盟关键服务的网络安全措施。
- 目前正在提议的《欧盟网络安全法》旨在加强欧盟机构自身的数字防御。
- 欧洲银行管理局关于外包安排的 EBA 指南

● 《中华人民共和国网络安全法》：通过概述公司的安全义务、提高公众对网络威胁的认识以及赋予当局监控和管理网络空间的广泛权力，专注于保护在线基础设施和数据。

● PCI DSS：针对处理和加工信用卡持有人信息的组织的跨司法管辖区标准，强调通过全面的安全措施保护财务数据。

3.2.2.3 云端合规性

总体而言，多部法律法规中都存在一些共同的因素：

● 安全处理：确保严格控制对敏感数据的访问，并确保数据处理能够维护其机密性和完整性。

● 安全存储：实施加密和其他保护措施来保护静态和传输中的数据，确保正确的数据保留和删除做法。

● 应尽的注意：遵守行业最佳实践和安全标准，保护数据免受威胁和漏洞的侵害。

● 审计跟踪：维护数据处理活动的全面记录，以证明符合监管要求并方便审计。

3.2.2.4 遵守法规和标准

云提供商通常通过认证、证明和其他形式的授权来符合各种法规、行业和国家标准。这些包括：

- ISO/IEC 27001-2022
- ISO/IEC 27017 云计算服务的信息安全控制
- ISO/IEC 27018 - 保护公有云中的 PII
- 支付卡行业数据安全标准 (PCI DSS)
- 美国注册会计师协会（AICPA）
- 服务组织控制报告（SOC 1 和 SOC 2）
- 云安全联盟的 STAR 认证
- 云安全联盟的 STAR 认可
- 美国联邦风险与授权管理计划 (FedRAMP)
- 新加坡多层云安全标准（MTCS）
- 德国云计算合规标准目录 (C5)
- 健康信息信托联盟 (HITRUST) 通用安全框架 (CSF)
- 《欧盟云行为准则》(EU Cloud CoC)

这些认证、证明和授权对于证明 CSP 致力于维护高标准的安全和数据保护至关重要。

3.2.3 合规继承

合规性继承是云计算中遵守法规的一个重要方面，它为 CSC 提供了一种利用其 CSP 的安全性和合规性状况来满足各种法规和行业标准的方法。这一概念在严格执行数据保护和安全标准的环境中尤其重要，例如金融服务、医疗保健和处理敏感个人数据的行业。

云合规性通常遵循责任共担模型，其中 CSP 和 CSC 分别负责合规性的某些方面。合规性继承旨在减轻 CSC 的一些负担，允许他们从合规的 CSP 那里获得一套控制措施。考虑一个符合 PCI DSS 标准的云基础设施提供商。使用其基础设施服务的 CSC 将继承这套控制措施，并在基础设施级别符合 PCI DSS 标准。但是，CSC 还将负责确保在此基础设施上构建的软件也符合 PCI DSS 标准。

CSP 和 CSC 均接受独立审计，并且各自必须确保其各自的控制符合要求。

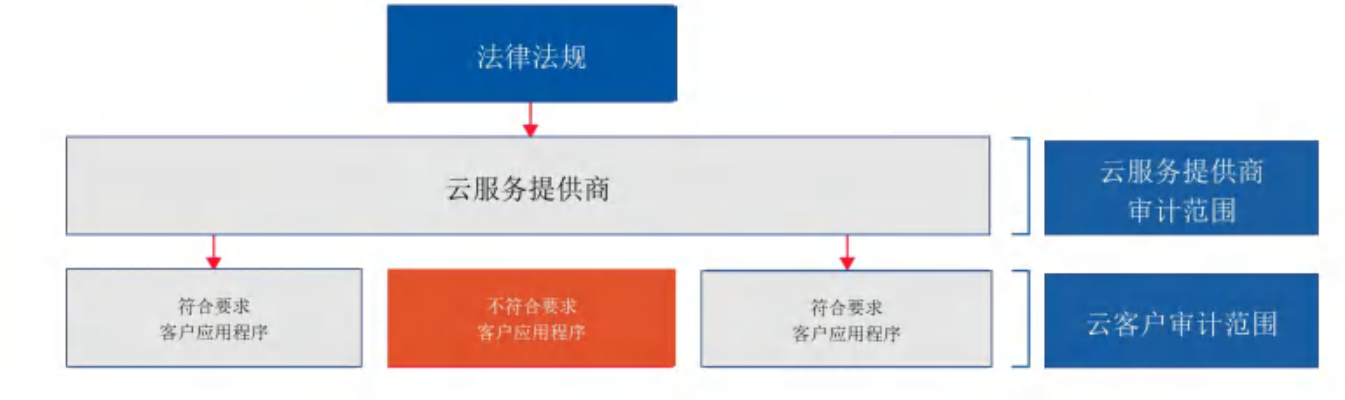


图 19：审计范围：提供商与客户的责任

3.2.3.1 合规性继承限制

合规性继承通常不会转移合规性责任。它仅允许 CSC 利用 CSP 部署的活动和控制。当 CSC 选择依靠 CSP 来全部或部分履行其义务时，它仍然保留整个技术堆栈的合规性责任。在某些标准和框架（例如 ISO 27001 或 SOC 2）中，CSC 必须至少每年采取明确步骤来验证其 CSP 是否继续合规。

- 提供商审计范围：在合规性继承模型中，CSP 的基础设施和服务会接受严格的审核，以确保遵守特定的合规性标准。这些审核通常称为传递式审核，用于验证 CSP 的合规性，从而使 CSC 无需亲自审核 CSP 的基础设施和服务。CSP 负责这些认证的费用和持续维护。
- 客户审核范围：虽然 CSP 可以提供合规的基础设施，但在此基础设施上构建和维护合规应用程序的责任在于 CSC。这种责任划分意味着，尽管 CSP 的服务可能合规，但 CSC 在此基础设施上开发的任何应用程序或服务也必须接受独立合规评估。
    - 符合要求的客户申请：如果 CSC 在符合特定标准或法规（例如 PCI DSS）的 CSP 平台上构建其服务，则 CSP 提供的底层基础设施和操作将被视为合规，并且不在 CSC 的审计范围内。这使得 CSC 能够将合规工作重点放在自己的应用程序和数据管理实践上。
    - 不合规的客户申请：即使使用合规的云基础设施，如果 CSC 的应用程序设计不符合相关标准， 也可能无法满足监管要求。这凸显了 CSC 在确保其应用程序、流程和数据处理实践符合合规要求方面的职责的重要性。

3.2.4 司法管辖区

许多云部署可能跨越不同的法律和监管管辖区。当运营跨越多个地区时，合规性的复杂性会变得更加严重，每个地区都有自己的法律和监管框架来管理数据隐私、安全和其他关键因素。

在多个地区运营的 CSP 和 CSC 将面临适用各种法律法规的司法管辖区。这将受到以下因素的影响：

- CSP 的位置。
- CSC 的位置。
- 数据主体的位置。
- 存储数据的位置。
- CSP/CSC 合同的法律管辖权可能与任何利益相关者的所在地不同。
- 各个地点之间是否存在任何条约或其他法律框架。

一个例子是，即使数据托管在不同的地区，也需要在 CSP 运营所在的国家/地区发布违规通知。

图 20：影响云管辖区合规性的因素

3.2.5 云保障机制

保障是用于验证合规性的过程和方法。保障涵盖了一系列的审计、认证和评估，每种方法都有不同的重点和方法论，这些方法在不同的云服务提供商（CSP）之间可能存在显著差异。这些过程用于验证监管、安全和运营标准的合规性。

表 3：云保证机制：定义和目的

术语	定义	目的	范围	等级保证	重点	举例
审计 Audit	全面地检查 IT 系统、流程和控制	为 IT 控制的有效性和安全性提供合理的保证	关注 IT 系统、安全性和合规性	高. 严格调查和验证 IT 控制	提供关于 IT 遵从标准的独立意见	IT 安全审计评估网络漏洞和访问控制
证明 Attestation	对 IT 实践进行审查，并就情况发表声明	根据既定目的、内部控制或系统评估准确性	可以包括财务报表以外的各种 IT 主题	中等。简化 IT 实践的审计	根据商定的程序验证特定的 IT 控制或信息	SOC 2 报告评估 IT 控制并发布证明声明

保证 Assurance	对 IT 信息进行无偏见的评估，以建立信心。	增强对 IT 流程和系统的信任	不限于具体信息；可以涵盖各种 IT 方面	根据 IT 参与的类型而有所不同	建立对组织 IT 基础设施可靠性和安全性的信心	基于综合评估和审计，增强对 IT 灾难恢复计划有效性的信心
评价 Evaluation	根据标准评价 IT 性能、有效性或结果	衡量成功，确定需要改进的领域，并为 IT 决策提供信息	可以应用于 IT 程序、项目、流程或系统	情境依赖；在 IT 环境中可能并不总是提供保证	评价 IT 方面的价值、有效性或结果	评价 IT 灾难恢复计划或软件开发过程的有效性
评估 Assessment	对 IT 流程、风险或绩效进行全面分析或评估	全面评估和分析 IT 实践、风险和合规性	包括广泛的 IT 相关评估，包括风险评估和合规检查	取决于具体的评估目标和方法	对云迁移策略进行风险评估	评估整体成熟度 IT 治理框架

3.2.5.1 第三方提供商和审计

一些 CSC 可能习惯于审计第三方提供商，但云计算的性质以及与 CSP 签订的合同通常会排除诸如本地审计之类的事情。CSC 应该明白，在提供多租户服务时，CSP 可以（并且通常应该）将本地审计视为安全风险。来自大量客户的多次本地审计带来了明显的后勤和安全挑战，尤其是当提供商依赖共享资产来创建资源池时。

与这些提供商合作的客户将不得不更多地依赖第三方证明，而不是他们自己进行的审计。根据审计标准，实际结果可能只能在保密协议 (NDA) 下发布，这意味着 CSP 必须签订法律协议才能获得用于风险评估或其他评估目的的证明。这通常是由于与审计公司的法律或合同要求，而不是由于 CSP 的任何企图和混淆。

CSPs 应该明白，客户仍然需要确保其满足合同和监管义务，因此应提供严格的第三方证明来证明其满足义务， 尤其是在 CSP 不允许直接进行客户评估的情况下。这些应基于行业标准，明确定义范围并列出评估的具体控制措施。发布认证和证明（在法律允许的范围内）将极大地帮助云客户评估提供商。CSA STAR 注册表为提供商提供一个中央存储库来公开发布这些文档。

3.2.6 合规工件

合规工件是支持合规性活动所需的日志、文档和其他材料。CSP 和 CSC 都有责任制作和管理各自的工件。CSC 最终负责支持其审计所需的工件，因此需要了解 CSP 提供的内容，以便他们可

以创建工件来弥补任何差距（例如，在应用程序中构建更强大的日志记录，因为 PaaS 上的服务器日志可能不可用）。

合规工件表明遵守云环境中的各种法规和安全标准。这些工件在审计期间可作为有形证据，展示组织有效管理和保护数据的能力。

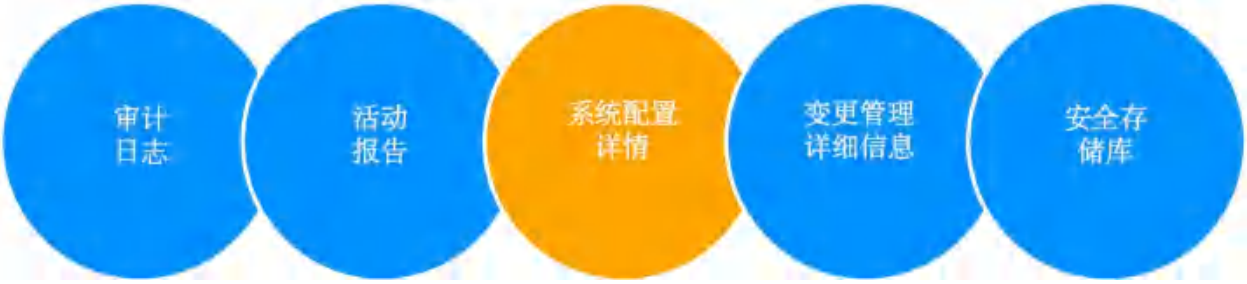


图 21：云环境中的基本合规性构件

以下是合规工件的示例：

- 审计日志：事件、行动和变化的详细记录
- 活动报告：总结用户活动、访问模式和系统交互的报告。活动报告可以帮助识别未经授权的访问、跟踪用户操作并确保操作实践符合合规性要求
- 系统配置详情：系统配置文档，包括网络设置、访问控制和安全措施
- 变更管理详细信息：记录对系统所做的变更，包括更新、修改和补丁。这些详细信息对于确保以维护环境完整性和安全性的方式授权、测试和实施变更至关重要
- 安全存储库：存储合规性工件需要安全、可访问的存储库，以保护数据的完整性和机密性。这些存储库应遵守安全标准，并能够限制只有授权人员才能访问。在某些情况下，管理这些存储库可能会跨越 CSC/CSP 边界，因此需要就访问控制和数据保护措施达成明确的协议。

3.3 治理、风险与合规：工具与技术

GRC工具包中既有技术工具，也有非技术工具。其中包括清晰的职责、合同和存储库文档，用于存储维护的风险注册表和服务注册表。还包括描述已根据其业务环境和 CSC 团队的采用流程进行调整的框架和流程的文档。还有各种各样的技术工具可用于自动执行人工流程无法完成的劳动密集型任务。以下提供了 CSC 可能遇到的不同类型的工具以及每种工具的简要说明。

3.3.1 支持治理、保证和合规的非技术工具

非技术工具在云计算的治理、保证和合规方面发挥着作用，为组织提供管理风险、明确责任和确保遵守监管要求所需的框架和方法。

以下是非技术工具的示例：

- 责任共担模型：
  - 如前所述，责任共担模型描述了 CSP 和 CSC 之间共享的安全责任。在云环境中，了解与安全管理、数据保护和合规义务相关的任务划分至关重要。RACI 图表（负责、负责、咨询和知情）可用于记录角色和职责。
  - 它通过明确定义谁负责特定的安全任务（例如数据加密、网络安全控制和事件响应）来帮助防止安全覆盖范围出现漏洞。
- 合同：
  - 合同规定了云提供商与客户之间关系中的法律角色、责任和期望。其中包括 SLA、数据处理协议和保密条款。
  - 它们确保双方了解各自的义务、合法权利和补救措施，从而为发生纠纷或合规失败时的问责和补救奠定基础。
- 风险注册表：
  - 风险注册表是列出所有已识别风险、其严重程度及其管理措施的文件。
  - 它使组织能够系统地确定风险的优先级并解决风险，从而促进主动风险管理，确保缓解措施与组织的风险偏好相一致。
- 第三方风险管理/提供商/云注册：
  - 保存第三方提供商的登记册并评估其风险，确保所有外部实体都受到评估和监控，以发现潜在的风险和安全隐患。
- 云安全成熟度模型 (CSMM)
  - 它指导组织根据行业基准衡量和改进其整体云安全计划。
  - 它为持续改进云安全提供了路线图，帮助组织识别弱点并随着时间的推移实施更强大的安全措施。
- 服务注册中心：

- 服务注册表是一个包含已部署内部服务信息的数据库。它在云服务中用于管理和发现团队可能集成或使用的动态服务。
- 它允许团队轻松定位和集成现有服务，从而减少冗余并促进重用，从而增强服务互操作性和效率。

- 控制框架：
  - 它包括一组用于管理风险和在组织内实施有效控制的指南或最佳实践。
  - 它使整个组织的风险管理和控制实施标准化，确保一致、有效的治理实践。
- 监测和审计框架：
  - 这些框架用于持续监督，允许检测异常、安全事件并确保控制按预期发挥作用。
  - 它们增强了及时识别和应对潜在安全威胁的能力，确保遵守监管和内部策略。
- 数据/资产分类及目录：
  - 对数据和资产进行系统分类有助于根据敏感性和重要性应用适当的安全控制。
  - 它通过确保对更敏感的资产应用更高级别的安全性来保护关键信息和资源，符合合规性和数据保护要求。
- 用户/实体映射：
  - 将用户和实体映射到其相应的数据访问和处理活动有助于维护数据治理并防止未经授权的访问。
  - 它通过确保只有授权个人才能访问特定数据集来加强数据治理，最大限度地降低数据泄露和违反合规性的风险。

3.3.2支持治理、保证和合规的技术

我们使用一系列技术来帮助我们实现云中的治理、保证和合规性。这些技术有助于实施安全策略、实现合规性的实时监控，并实现云资源管理的自动化，以最大限度地降低人为错误和配置错误带来的风险。

3.3.2.1 云服务提供商策略

CSP 策略是集成在云平台中的一组预防和技术规则，用于控制和管理访问、操作和配置。

制定和执行 CSP 策略需要深入了解组织的安全目标和云环境的功能。CSP 策略应与最佳实践和监管要求保持一致，以确保强大的安全治理。

3.3.2.2 检测与预防控制

云安全信息事件管理 (SIEM)、云安全态势管理 (CSPM)、云原生应用程序保护平台 (CNAPP)、云工作负载保护平台 (CWPP) 和安全服务边缘 (SSE) 等工具提供了对偏离安全和合规基线的监控和管理功能。这些工具可以自动检测错误配置、漏洞和不符合监管标准的情况。

3.3.2.3 软件物料清单

SBOM 是构成软件应用程序的所有组件（包括其开源组件）的综合清单。它对于透明度和跟踪软件依赖关系至 关重要，可确保软件供应链安全合规。实施 SBOM 可让组织跟踪和验证其软件中的组件，确保它们是最新的并且不包含已知漏洞。

3.3.2.4自动化

云部署通常使用自动化来定义和部署，例如标准镜像和 IaC。这些增强了一致性和可审计性。

总结

管理云环境中的风险、审计和合规性对于确保 CSP 和 CSC 的安全性和完整性至关重要。此领域侧重于建立强大的风险管理框架、保持对监管标准的遵守以及利用各种工具和技术进行有效治理。

云风险管理涉及了解和减轻与云服务相关的风险。关键实践包括评估 CSP、维护云注册和实施全面的风险管理策略。这些策略可确保主动识别、评估和管理云风险。

合规性和审计对于遵守标准、法律和法规至关重要。合规性可确保安全措施符合监管要求，而审计可验证这些措施的有效性。云的动态特性要求解决跨多个司法管辖区的法律、监管和合同挑战。组织必须调整其内部策略，以在传统和云环境中保持合规性。

合规性继承利用 CSP 的合规性认证来满足监管标准。这种责任共担模型允许 CSC 从 CSP 继承合规性控制， 同时保持对其应用程序合规性的责任。这种方法简化了合规性管理，但需要持续监控和验证。

GRC 工具和技术支持安全策略和合规性要求的实施。非技术工具（如责任共担模型和风险登记册）以及技术工具（如 SIEM、CSPM 和 SBOM）可增强安全治理。自动化在维护一致且可审计的云部署方面发挥着关键作用。

合规性工件（例如审计日志、活动报告和系统配置）对于证明遵守监管标准至关重要。这些工件的安全存储库可确保其完整性和机密性，从而支持有效的合规性管理。

总之，保护云环境需要全面的风险管理、合规性和持续监控方法。通过利用非技术和技术工具，组织可以有效地管理云风险、确保合规性并维护其云基础设施的安全性和弹性。

建议

合规、审计和保证应该是持续的。它们不应被视为仅仅是某个时间点的活动，许多标准和法规都越来越倾向于这种模式。在云计算领域尤其如此，因为 CSP 和 CSC 都在不断变化。

在云计算中采用持续的合规、审计和保证方法对于应对云服务的复杂性以及确保 CSP 和 CSC 履行其监管和安全义务至关重要。通过遵循这些建议，CSP 和 CSC 可以培育更安全、更合规的云生态系统，有效降低风险并增强对云服务的信任。

云服务提供商

- 透明沟通：传达他们的审计结果、认证和证明，特别注意：
    - 评估范围：明确定义评估云服务的哪些方面，包括具体功能和服务。
    - 覆盖范围详情：指定不同地点和司法管辖区涵盖的服务，帮助 CSC 了解在何处以及如何部署合规应用程序。
    - 部署指南：提供有关 CSC 如何按照相关标准和法规部署应用程序和服务的指导。
    - 客户责任：强调客户需要注意的任何其他责任，包括可能影响合规性的任何服务限制。
- 维护认证：CSP 必须长期维护其认证/证明，并主动通报任何状态变化。

● 持续合规举措：CSP 应参与持续的合规举措，以避免给 CSC 造成漏洞和风险。

● 提供合规工件：向 CSC 提供通常需要的合规证据和成果，例如 CSC 无法自行收集的管理活动日志。

云客户 CSC

● 了解合规义务：CSC 在部署、迁移或在云中开发之前应充分了解其合规义务。这种理解对于选择合适的云服务并根据监管要求进行配置至关重要。

● 评估提供商凭证：根据合规性需求评估 CSP 的第三方证明和认证。确保这些凭证符合特定的合规性义务。

● 评估范围和覆盖范围：清楚了解 CSP 评估和认证的范围，包括涵盖的具体控制措施和服务。这些知识有助于将 CSC 的合规策略与 CSP 的产品保持一致。

● 选择经验丰富的审核员：如果可能的话，选择具有云计算专业知识的审计员，特别是利用通过审计和认证来有效地管理审计范围。

● 管理合规性工件：了解提供商提供的合规性工件，并确保高效收集和管理这些工件。在必要时创建和管理合规性工件，以填补 CSP 留下的任何空白。

● 维护云提供商注册：保留所有使用的 CSP 服务的更新记录，记录相关的合规性要求和每项服务的当前合规性状态。CSA CCM 等工具可以帮助完成此活动，提供一种结构化的方法来管理各种云服务的合规性。

补充指南

- CSA 对云风险管理的看法
- CSA 行为准则差距解决方案和 GDPR 合规性 CSA 行为准则附件 10
- 云计算面临的最大威胁：11 大顶级威胁 深度剖析 | CSA
- 医疗保健领域的第三方供应商风险管理 | CSA
- 减轻混合云风险 | CSA
- 企业资源规划和云采用 | CSA

领域 4：组织管理

组织管理是指云环境的全面管理，它涉及组织和验证云服务提供商 (CSP) 的安全措施，以及保障各个云服务部署的安全。这些关键的安全议题跨越了部署策略，旨在实现结构化的最优“影响半径”控制和安全管理。尽管每个 CSP 的底层技术存在差异，但它们通常提供足够的功能对等性，以实现策略一致的管理实践。

租户管理是多租户环境中资源分配的关键机制，在云环境管理中发挥着至关重要的作用。建立关键控制措施来管理层级结构并解决首要的安全性和合规性问题，对于维护可见性和结构至关重要。

随着企业越来越多地采用多云策略，了解 AWS、Azure 和 Google Cloud 等主流 CSP 使用的层级模型非常重要。本领域探讨了管理和保护多个云部署的各种组织层级结构模型及其功能和最佳实践。通过研究结构差异和标准化方法，云客户 (CSC) 可以实施一致的安全控制和策略，增强其云管理策略并最小化安全风险。

此领域还涉及组织安全管理的细节，包括身份提供商映射、CSP 策略、共享服务，以及混合和多云环境的注意事项。CSC 通常使用多种云服务，包括软件即服务（SaaS）、基础设施即服务（IaaS）和平台即服务（PaaS）。再加上混合连接和并购（M&A），可能导致不受控制的增长或无序的云蔓延，从而增加成本和安全风险。

实现云安全的第一步包括限制不必要的扩展、确定组织占用空间，在跨 CSP 及其内部实施安全控制，以确保单个部署的安全。首要任务是掌握如何将云服务划分成更小的控制单元，并在部署之上建立企业级和租户级的控制措施。

学习目标

在此领域，您将学习：

- 如何管理云服务供应商的组织级安全。

- 如何利用组织层级结构来管理云部署的关键要点。
- 了解混合云/多云部署的安全注意事项。
- 识别不同的云组织层级模型。

4.1 组织层级模型

云环境中采用各种组织层级模型，每种模型在管理不同 CSP 之间的云资源时都有其各自的复杂性。随着云客户（CSC）扩大对云技术的使用，了解 AWS、Azure 和 Google Cloud 等主流 CSP 使用的结构差异和术语至关重要。本节旨在阐明这些概念，并提出一种讨论和实施云中组织结构的标准化方法。通过比较 AWS、Azure 和 Google Cloud 的层级模型，我们提供了有效应用安全控制和策略的洞察，确保跨不同云平台实现统一且安全的云管理策略。

4.1.1 定义

探讨云组织结构的主题可能会很具挑战性，这不仅是因为公司自身技术应用（例如，本地部署、云、OT、ICS）的客观复杂性，还因为不同的云服务供应商（CSP）对于类似的组织结构使用了不同的词汇和术语。例如，亚马逊网络服务（AWS）使用诸如组织、组织单元和账户等术语。相比之下，微软 Azure 将其结构分类为租户、管理组和订阅。谷歌云平台（GCP）将其服务组织成组织、文件夹和项目。

尽管这些术语及其相关功能并不完全相同，但它们有足够的相似之处，可以提取出适用于各种 CSP 的通用安全原则。这些组织的层级化结构将有助于在多个部署中一致地应用安全控制和策略。

为了简化讨论并保持清晰，我们将使用一套标准化的术语：

- 一个“组织”表示 CSP 内的最高层级结构。例如，AWS 和 GCP 中的“组织”，以及 Azure 中的“租户”。
- 一个“组”表示部署的集合。例如，AWS 的“组织单位”、GCP 的文件夹、Azure 的资源组。
- 一个“部署”指的是 CSP 内的隔离环境。例如，AWS 账户、Azure 订阅及 GCP 的项目。

以下是主要 CSP 使用的不同术语的简要概述。

表 4：云服务提供商术语比较

云服务提供者	组织	组	部署
AWS	组织	组织单位	账户
Google Cloud	组织	文件夹	项目
微软 Azure	租户	资源组	订阅

需要注意的是，不同 CSP 所使用的定义术语可能有所不同。例如，“账户”一词通常与身份和访问管理 (IAM) 相关，“订阅”可能指接收定期电子邮件更新，“文件夹”业可以理解为存储文件的地方。

图22：云资源管理的层级结构

采用多种部署是减少不良事件或违规的影响的一种战略方法，有助于遵守 CSP 规定的服务限制，并促进不同技术堆栈的逻辑分离。这种方法强调了采用结构化和分层模型来组织云资源的重要性，从而增强安全性并简化跨云环境的资源管理。

4.1.2 组织安全目标

提供一致的安全方法来保护企业免受内外部恶意行为者的侵害对于创建纵深防御控制非常重要。目标必须是技术导向和业务导向的。成功衡量标准包括降低风险、改善治理和法规遵从性，以及使组织的文化与其领导层的风险偏好保持一致。

4.1.2.1 组织

一个结构良好的部署层级结构是基本要求。它描述了云环境中资源和服务的安排，有助于实现高效管理和运营清晰度。

实施全面的标记策略并维护准确的资源注册表可确保资产易于识别、分类和管理，从而简化部署和维护流程。

4.1.2.2 可见性

维护所有资源配置的清晰视图对于安全性和运营效率至关重要。这种可见性可以快速识别和纠正可能导致漏洞的错误配置。应跟踪服务配置，以确保服务以正确的设置运行并符合安全最佳实践。通过监控整个云环境中的活动，可以检测到可能预示安全威胁的异常或未经授权的操作。

4.1.2.3 治理

强健的身份和访问管理(IAM)实践对于确保只有授权用户才能访问敏感资源并执行其职权范围内的操作至关重要。治理延伸到配置，必须根据定义的标准进行管理，以避免偏离安全基线。

4.1.2.4 一致性

集中式共享安全服务（例如身份提供商和威胁检测系统）可在整个云环境中提供统一的安全覆盖。“账户工厂”可以快速一致地创建符合组织标准和安全要求的云账户，确保部署之间的一致性。账户工厂服务的示例包括 AWS Control Tower、Azure Blueprints 和 Google Cloud Resource Manager。

4.1.3 云服务提供商内的组织能力

所有 IaaS 和 PaaS CSP 都提供分段和隔离的客户环境，这对于实施多租户至关重要。这可确保每个 CSC 都有从 CSP 资源池中分配给自己的安全资源集合。CSC 很快就意识到使用 CSP 进行多个独立部署的好处，即在每个环境中部署不同的应用程序，从而有效地限制任何安全问题的波及范围。这是因为每个部署都与属于不同 CSC 的部署一样独立和隔离，使每个部署都成为一个强大的安全屏障，类似于利用多个隔离的数据中心进行独立部署。

然而，组织和管理这些多重部署带来了挑战，而 CSC 甚至在 CSP 实施之前就已经接受了这一策略。随着时间的推移， CSP 越来越多地引入管理和保护多重部署的功能，并将这种方法确立为最佳实践。

所有主流的云服务提供商都提供四种主要功能，使 CSC 能够显著增强整个组织的安全性：

- 组：允许 CSC 将其部署构建为隔离的层级结构。
- 策略：可应用于组或部署的安全规则集合。这些规则通常具备“启用”和“禁用”功能，可精确到特定的 API 调用或甚至是单个参数。
- IAM ：集中化和/或联动支持 CSC 用户的集中管理。
- 共享安全服务：每个 CSP 都支持自己的一套共享安全服务。这些服务差别很大，但通常包括集中的日志记录。

一些 CSP 还引入了“账户工厂”（又称“登录区”或“账户管理器”）的概念。此功能有助于创建标准化部署，通常利用代码基础设施 (IaC)，配备预装的安全配置和控制基准。这种方法可以便捷地配置账户，尽管在单个策略调整方面可能会灵活性较低。通过这些方法，CSC 可以增强其安全态势，同时有效管理多个部署并保持高水平的安全性和运营效率。

4.1.4 在提供商内部构建层级模型

在云环境中建立部署的总体层级结构时，云客户（CSCs）必须考虑安全性和一般管理因素，例如：

- 该层级结构是否支持有效使用策略？策略定义并限制了在账户内可以执行的操作。大多数 CSCs 支持在组或部署级别应用策略。在组级别应用它们可以为该分支中的所有嵌套组和部署树建立安全措施。
- 该层级结构是否支持身份和访问管理（IAM）要求？在大多数 CSPs 中，CSC 可以在组级别定义用户权限，而不仅仅是在部署内。
- 该层级结构是否与 CSC 的结构兼容，例如业务单位、治理等方面？虽然这不是严格的安全因素，但部署层级结构通常与 IAM 层级结构紧密耦合，并可能影响诸如计费和成本管理等各种资源。

CSC 通常采用三种模型之一来定义其层级结构，每种模型都有各自的优势和操作限制。没有一种模型是普遍优越的，一些 CSC 可以会结合不同模型的元素来最好地反映其操作实际。

- 业务单元和应用导向：在此模型中，以业务单元作为最高层，接着是单元内的应用，然后是环境（例如生产环境与开发环境）。这种模型适合以业务单元为中心的身份访问管理（IAM）层级结构。该模型要求云功能与业务部门和应用程序紧密结合，否则它可能对策略管理效率较低。
- 环境导向：此模型将环境（如开发环境、生产环境、测试环境）置于层级结构的顶部，然后是业务部门或应用程序。这种方法有利于策略管理，允许为不同环境建立基准安全和运营策略。但是，该模型可能与 IAM 层级结构或计费和成本管理的需求不匹配。
- 地理位置导向：对于在全球运营的 CSC，基于地理位置的模型是首选结构。该模型从顶层的地理区域（例如 EMEA、NA 或特定国家/地区）开始。随后，它将业务部门或环境整合到下层级别。该模型通常有利于全球 csc 适配不同地区的安全和监管要求。

多数云客户（CSC）认为在每个云服务供应商（CSP）中维护单一组织是理想的做法，尽管这并非绝对必要。然而，在某些情况下，维护多个组织或租户是必需的，比如为了满足国际监管或安全标准，或者当大型组织的需求超出了 CSP 在一个 CSC 内部署的服务能力限制。通常，层级结构还会包括专门的操作和安全分支，以容纳这些群组在整个基础设施中部署的共享服务。这种战略性的云部署组织结构使得 CSC 能够有效地管理安全性、合规性和运营效率。

在考虑实施零信任架构时，需要整合以上三种模型中的一些要素去适配零信任结构的先进性或最佳成熟度。策略管理和执行层面需要动态地考虑这些模型中的有关要素。

4.2 管理组织级安全

云与传统基础设施之间最显著的区别之一是，在云中，团队通常能够创建和管理他们的虚拟环境，这相当于整个数据中心。以往在物理设施环境中，我们依赖于传统基础设施中的许多传统隔离区域，如网络团队、服务器团队等，而在云中没有固有的需要。尽管如此，所有的云仍然运行在数据中心中，但云客户（CSC）很少看到或与物理层交互，而是通过 Web 界面和 API 调用创建整个网络和应用堆栈。

云安全的目标是在不引入减少或消除云计算好处的摩擦的情况下，保持可接受的风险。在不妨碍业务目标的情况下，保持对云占用空间的控制是很重要的。云服务供应商（CSP）提供了一系列能力来支持网络或应用程序安全等传统安全领域之外的治理和安全。这始于一个明确定义的租户结构，可以通过额外的控制来扩展。

4.2.1 身份提供者和用户/组/角色映射

身份提供商 (IdP) 是一个集中式系统，用于管理用户的身份和身份验证。它独立于单个云部署，允许在不同的云服务（包括 SaaS 平台）中使用单一身份。IdP 和用户/组/角色映射用于定义部署访问权限。这是部署之外的身份和访问管理（IAM），但在部署内部还有额外的 IAM。在组织管理方面，有两个重要因素需要考虑：

- 最小化组织的根目录访问权限。目的是尽可能减少拥有高级访问权限的个人数量，这些权限可能会允许他们变更或访问层级结构中的部署，或变更具有级联效应的共享服务，或潜在地提升对部署的权限。
- 明确谁可以创建部署以及如何创建部署，但要支持相对顺畅的流程，以便团队能够根据策略轻松获取新账户。例如，设置一个账户工厂，在该团队的层级结构分支中创建一个正确配置的请求类型账户（例如开发、沙盒、生产）。

身份提供者（IdP）可以跨多个云服务供应商（CSP）和软件即服务（SaaS）平台使用，即使它仅在其中一个 CSP 内设置。IdP 定义了用户、组和角色映射。这些映射在联合过程中与 CSP 共享，CSP 的 IAM 系统根据这些映射分配权限。此外，可以使用诸如业务单位之类的属性来微调访问控制。根据 CSP 的不同，这些映射可以与组织的层级结构对齐。

4.2.2 云服务提供商（组织）策略

在大多数云服务供应商（CSP）中，组织策略（有时也称为“组织级策略类型”）是一种机制，它允许在部署或组级别启用或禁用特定的部署服务。某些 CSP 还提供侦测或修正策略，这些策略能够识别出策略违规情况，并通过自动恢复到正确的配置来修复它们。在 CSP 的编排引擎中，当需要协调多个步骤来处理多个资源，且单一步骤无法做出决策时，修正和侦测策略尤其有用。例如，创建资源和添加标签可能涉及在提供程序中进行两个或更多的 API 调用。如果标签

未被应用，修正控制可以在资源创建后删除该资源，而预防控制则会失败，因为它无法评估在初始资源创建步骤中是否应用了标签。

策略的一个显著特性是它们能够定义部署的安全参数，同时与部署保持独立。这种外部定位确保了即使拥有完全控制部署权限的管理员也无法修改或删除这些策略。策略适用于各种场景，包括：

- 启用和禁用特定服务，例如禁止使用未经批准的平台服务进行部署。
- 阻止特定的 API 调用以防止未经授权或有害的操作。
- 禁用某些区域以遵守地理监管要求、维护数据属地和主权要求。
- 定义条件，例如只允许来自授权网络源（例如特定的 IP 地址）的特定 API 调用。然而，这需要云服务供应商（CSP）和服务级别的支持，这是不同供应商之间功能最不一致的地方之一。
- 执行身份和访问管理（IAM）的最佳实践，以保护组织级访问和操作工具的安全，包括防止部署管理员限制对关键监控和控制账户的访问（例如，在管理员凭据被泄露的情况下）。

根据 CSP 策略的范围，其可分为三个级别：

1、组织范围的策略：由 CSC 定义并适用于所有部署。通常，此类别包含一组有限的策略，因为在如此广泛的范围内管理例外情况存在挑战。

2、组级策略：涵盖特定组内的所有部署。此级别最常用于策略应用，此级别的策略可以累积并相互加强，尤其是在应用于子组时。CSP 强制执行组合策略集，其中拒绝操作的策略几乎总是优先于更高级别的任何允许策略。

3、部署级别策略：针对单个部署进行量身定制，允许进行精确的安全调整。虽然在组级别应用策略通常被认为是更好的管理实践，但某些场景需要部署级别策略，特别是对于具有特定和细粒度安全要求的部署。

让我们看看如何在层级结构的顶部具体应用策略控制，该策略控制对已添加到主账户的所有用户进行控制。服务控制策略 (SCP) 允许组织指定和控制主账户可以访问和使用哪些服务和功能。（根据 CSP 的不同，这被称为组织或租户。）

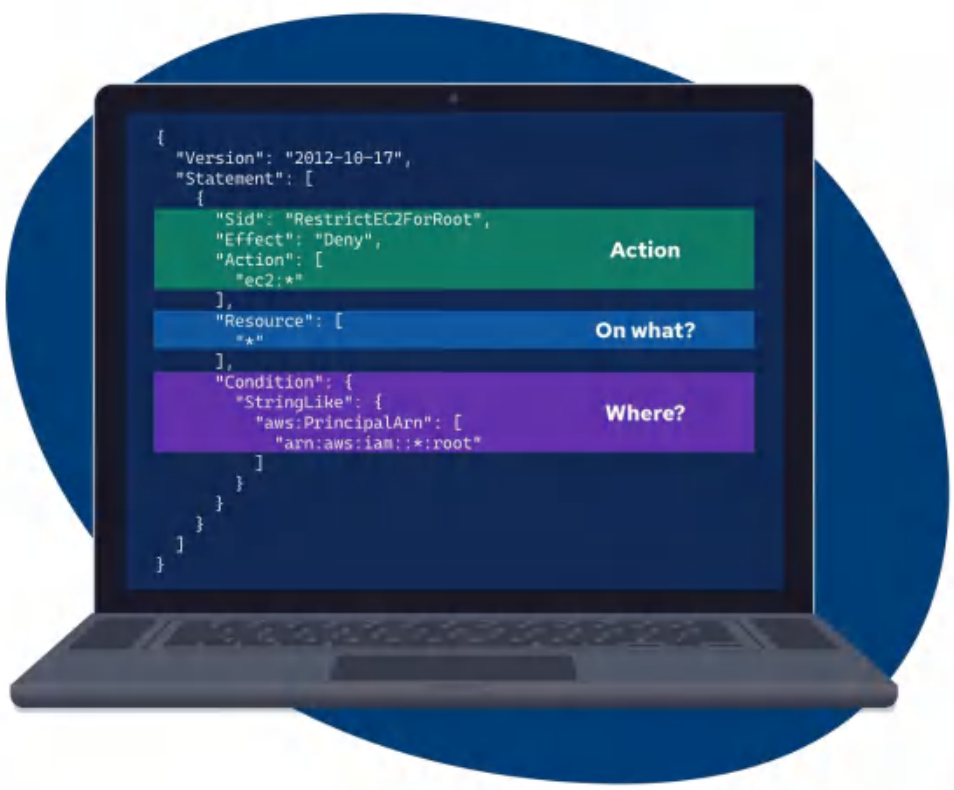


图 23：限制根用户操作的 AWS SCP 示例

在所示示例中，亚马逊网络服务（AWS）的服务控制策略（SCP）应用于 AWS 组织层级结构的顶层，以一致的方式控制所有成员账户的权限。SCP 不会直接向各个账户授予权限。相反，它们定义了账户中可能执行的操作的边界或限制。

SCP 允许集中管理和实施组织内所有部署的安全控制。这些策略提供了一种强大的机制来建立防护措施并确保始终遵守安全标准。具体而言，SCP 具有以下几个关键特征：

- 权限结构：SCP 使用“拒绝列表”方法，明确指定允许的服务和操作，并默认拒绝所有其他服务和操作。
- 执行：服务控制策略（SCPs）在组织级别设置限制，覆盖了附加到个别用户或角色的身份和访问管理（IAM）许可策略。
- 分层：SCP 与 IAM 策略协同工作，定义 CSC 的 AWS 账户的最大权限。
- 常见用例：SCP 通常会执行安全和合规标准，限制整个组织对特定服务或功能的访问。

4.2.3 通用组织共享服务

集中式日志记录和安全遥测支持将所需的安全源收集到单个目的地，而无需从不同部署和区域复杂地手动转发源。这对于有效的安全监控、威胁检测、分析和合规性是必要的。这在将遥测发送到安全信息和事件管理 (SIEM) 平台或安全数据湖时同样有用。

CSP 威胁检测服务（例如 AWS GuardDuty) 提供对云环境中恶意活动和未经授权行为的持续监控。这些服务旨在通过实时识别潜在威胁来保护部署和工作负载，从而能够采取迅速的响应措施来降低风险并保护云资产。

标记策略和标准化通常由成本分配驱动（以确定哪个内部团队应该为资源付费），但也可以作为 IAM 策略的一部分用于实施基于属性的访问控制 (ABAC)。

在这些工具中，每一个都应映射到 CSC 的组织层级结构中，并通过调整以满足组和部署的安全要求。例如，通常对开发和生产环境应用不同的策略，生产环境需要被更严格地锁定，但允许更多暴露在互联网上的资源，而开发环境允许更开放地使用云服务，但严格限制或禁止任何开放面向互联网的资源。

还有以下两种工具不一定是安全控制，但对于实施组织级安全非常有帮助。

- 账户工厂是用于创建新云部署的自动化平台。该术语最初出现在创建 AWS 账户时，即使在与其他 CSP 合作时也仍然常用。账户工厂创建新部署并定义起始配置，这是确保从一开始就实施所需安全控制和配置的强有力安全工具。
- IaC 模板定义从单个服务的配置到整个复杂应用程序堆栈的所有内容。它们通常是账户工厂的核心，但也广泛用于现代的开发和部署流程。安全团队可以利用 IaC 模板来部署他们的堆栈，提供安全的基线配置，并将安全控制集成到项目中。

应最大限度地管理组织/租户根目录之外的组织级安全。日常使用的第三方或云服务供应商（CSP）工具应该被隔离到一个专门的安全部署中。这能减少组织层级结构顶层被破坏并被用来影响所有部署的可能性。

4.2.4 集成云安全和管理平台

云安全态势管理（CSPM）工具通过 API 与云服务供应商（CSP）连接，并评估云资源的当前配置。它们主要在管理平面级别进行态势/配置评估，但不会连接到虚拟机等资源以检查操作系统或内部配置。云工作负载保护平台（CWPP）是使用各种技术来评估工作负载（如虚拟机、容器或无服务器配置）的工具。

云原生应用程序保护平台（CNAPP）结合了 CSPM 和 CWPP 的功能，并可能还包括其他功能，例如基础设施即代码（IaC）代码扫描或云数据存储库（CDR）。

CSPM 的一项基本功能是其库存功能，它涉及识别云环境中每项资产的详细流程。这一流程涵盖各种资源，包括服务器、存储解决方案、数据库和各种服务配置。该流程还可以跟踪和识别资源随时间的变化。下图说明了 CSPM 的核心功能：

图 24：云安全态势管理(CSPM) 的核心功能

CSPM工具执行的下一个重要功能是资源配置评估。这涉及检查云资源的配置，以确保它们符合既定的安全最佳实践和标准。通过将资源设置与公认的行业基准进行比较和特定的内部策略，CSPM工具可以检测错误配置，从而减轻潜在的安全风险。

服务配置监控是对资源配置功能的补充。它侧重于验证云服务的配置是否安全并符合安全性和合规性要求。这一点尤其重要，因为云服务会不断更新和扩展新功能，因此需要定期进行配置审查以维护安全的环境。

检测错误配置是 CSPM 解决方案的一项核心功能，旨在识别可能对云安全构成重大威胁的配置错误。快速检测这些错误配置可让 CSC 及时纠正它们，从而减少对手利用的机会。

下表重点介绍了 CSPM 和 CNAPP 之间的主要区别和用例，展示了它们不同的重点和功能：

表 5：CSPM 与 CNAPP：主要区别和用例

	云安全态势管理（CSPM）	云原生应用程序保护平台（CNAPP）
范围	广泛的云安全方面，包括：	特别关注云原生应用程序，解决以下问题：
	基础设施配置：确保服务器、网络和存储的正确设置	应用程序开发安全：在开发过程中将安全性嵌入到代码中
	访问控制：管理用户权限和身份验证机制	部署安全：确保安全部署和运行时保护
	数据加密：对静态数据和传输中的数据实施加密	威胁情报集成：确定关键漏洞的优先级
	日志记录和监控：设置日志和警报以进行持续监控	集中合规管理：确保遵守标准
	合规性审计：检查是否符合行业标准	权限控制：强制最低特权访问
	IAM：用户身份管理	DevOps安全左移：在流程早期与开发人员开展协作
	网络安全组（NSG）：定义防火墙规则	全面的云工作负载保护：检测漏洞
	机密管理：保护敏感信息	易于使用：简化安全工具堆栈
	补丁管理：保持软件更新	洞察的深度和广度：消除可见性差距
功能	检测错误配置 - 识别暴露的资源 - 管理合规性	从创建到部署保护云原生应用 将云安全态势管理（CSPM）功能与工作负载安全集成 包括持续集成/持续部署（CI/CD）流水线集成

关键差异	专注于基础设施 主要是被动的 侧重于策略执行 可能需要与其他工具集成	以应用为中心 积极主动和预防性 专注于威胁检测和响应 提供更全面、综合的视角
受众	主要是安全团队和合规管理人员	安全、开发及运维团队

合规管理是 CSPM 的另一项关键功能。它使遵守各种标准和监管框架的评估过程自动化。这种自动化大大减少了与合规审计相关的人工工作量，并能够持续监控合规状态。

CWPP 为云环境提供运行时安全，而不仅仅是即时配置检查。通过利用基于主机的传感器，可以查看工作负载，以监控威胁和恶意活动。集成威胁情报可以检测到已知的不良行为者，而防火墙的自动化阻止操作可以防止攻击。在资源规模方面实现持续保护。总体而言，CWPP 通过将配置检查与运行时监控、可见性和响应相结合，为云工作负载提供全生命周期安全。

CNAPP 代表了一种更全面的云安全方法，并结合了多种功能。CNAPP 旨在在整个开发生命周期和跨云基础设施中保护云原生应用程序。它通常将 CSPM 功能与工作负载安全措施和其他功能（例如与 CI/CD 流水线集成）集成在一起。这种方法集中了基于云的内在操作普遍考虑的安全因素。

4.3 混合云和多云部署的注意事项

在当今多样化的 IT 环境中，CSC 通常依赖混合云和多云环境来满足其运营需求。混合云部署将本地数据中心与公有云服务连接起来，增强了灵活性和可扩展性，同时也带来了独特的安全挑战。换句话说，多云策略涉及使用多个 CSP 来以规避供应商锁定并优化性能，但同时也增加了安全管理的复杂性。本节探讨了保护混合云和多云环境的关键考虑因素，重点关注有效的组织管理、IAM、网络安全以及安全工具的战略性使用。了解这些方面对于在跨互连和多样化的云基础设施中保持强大的安全性至关重要。

4.3.1 混合云安全的组织管理

混合云使用虚拟专用网络 (VPN) 或专用网络链路将现有数据中心或设施连接到 CSP。混合云过去仅从网络安全角度考虑，但 CSP 不断扩展其功能。一些示例包括：

1、在专用硬件上将 CSP 服务部署到数据中心。例如，允许虚拟机或数据库使用与 CSP 在其设施中使用的类似或相同的技术堆栈。

2、扩展管理工具，通常通过代理，从云管理平面管理数据中心的资源（虚拟或物理）。

3、扩展身份标识以供在数据中心使用。

作为一种常规策略，强大的云和数据中心安全是实现混合云安全的基础。如果这两个领域中的任何一个存在弱点，应该集中隔离和界定这些弱点，以防止一个领域的安全问题影响到另一个领域。

在混合云安全中，首先需要关注的是身份和访问管理（IAM）和网络安全。身份提供者的损害会影响到两种环境。任何一方网络安全的脆弱性都可能扩大攻击的影响范围。不要误以为云环境是弱点；攻击者现在正在寻找从数据中心到云部署的连接途径。IAM 和云环境是连接这两种环境最常见的接触点。例如，SSH 密钥可能在两种环境中共享，一旦数据中心被攻破，就可能暴露云工作负载，反之亦然。

相反，应避免在不同环境之间标准化安全措施，包括策略和工具，因为这可能是混合云环境中的一个主要缺陷。云环境与传统数据中心使用的技术有本质的不同，试图实施一套统一的控制措施可能会导致安全漏洞和故障。正确使用合适的工具来完成相应的工作至关重要。

云和数据中心环境的不同特性导致了第二个陷阱：混合云蔓延。与传统的公有云服务供应商（CSP）相比，传统基础设施更加僵化，资源相对有限。这并不总是正确的，但对于大多数云客户（CSC）来说，情况通常如此。除了最现代化的数据中心外，大多数数据中心倾向于预设 IP 地址范围、网络架构，并且大量长期运行的工作负载在静态 IP 地址上。另一方面，云环境更短暂，边界更少，在更分散的组织结构中运行，更像是小型数据中心群（根据之前关于组织层级结构的建议）。

混合云蔓延是指将少数数据中心直接连接到大量云部署时产生的复杂性。具体来说，直接连接指的是从给定数据中心到多个云部署的大量 VPN 或专用网络链接。它还包括由于内部 IAM 管

理不善或并购不当造成将多个本地身份提供者连接到多个云部署。这种复杂性带来了额外的安全挑战，而关键的混合云安全策略可以最大限度地减少蔓延。

有效的混合云安全始于在本地和云中建立强大的安全基础，然后仔细梳理和管理环境之间的连接，安全启动，了解接触点，并管理影响范围。

4.3.2 多云安全的组织管理

客户在单个 CSP 的产品完全实现成熟应用之前，迁移到多个基础设施即服务（IaaS）或平台即服务（PaaS）的云服务供应商（CSP），会带来显著的安全挑战。每个 CSP 在最基础的技术层面上都有本质的不同，而有效的安全措施需要深入了解每个 CSP 及其服务的独特性。此外，除了最成熟的云客户（CSC）之外，为多个 CSP 提供统一的安全服务是一项极具挑战性的任务。CSC 不应迁移到第二个 IaaS CSP，除非它已经为主要 CSP 制定了有效且高效的安全计划。

这一建议对于大多数 CSC 来说具有挑战性。即使是那些严格管理且专注于单一 IaaS CSP 的 CSC，也可能因为并购或业务关系/合作伙伴的要求而使用其他 CSP。多云环境的安全挑战极为复杂，但可以通过充足的人员配备、组织管理策略和专为多云环境设计的关键安全共享服务来管理。

对于多云环境，一个常见的误解是，与云无关的容器策略将支持完全可移植的工作负载，允许 CSC 在任何时间点选择任何 CSP，可能是为了动态成本管理。实际上，实现与云无关的实施存在重大障碍。这些挑战既包括运营挑战，也包括安全挑战：

- 容器可以实现工作负载的可移植性，但无法实现管理基础设施的可移植性。构建容器的运行时和编排环境仍然需要相当大的开销。
- 共享服务通常不太便携，除非它们完全无状态且容器化。数据库、消息队列、通知总线和构成现代应用程序的其他服务通常由专用、不可移植资源上的 CSP 提供更好的服务。
- 可能会失去 CSP 的 PaaS 服务提供的经济、安全和运营利益。

4.3.3IaaS/PaaS 多云的组织管理

在应对云基础设施的复杂性时，云客户（CSC）通常会采取不同的策略来利用云服务供应商（CSP）进行基础设施即服务（IaaS）部署。这些策略大致可以分为三种不同的方法，每种方法都体现了 CSC 根据其运营需求、成熟度和战略目标与多个 CSP 的不同合作程度：

实现多云有三种策略：

● 单一模式：CSC 使用一个 CSP 进行 IaaS 部署。如果由于并购而添加了其他 CSP，则该部署将迁移到主 CSP。

● 主从模式：在此模式中，所有新的部署都在主要的 CSP 上进行，这代表了云客户（CSC）的主要云占用情况。次要的 CSP 则用于特定的、有限的或独立的部署，这种情况通常发生在主 CSP 无法满足特定的需求，或是因为合并或收购而引入次要 CSP。对次要 CSP 的使用应严格控制，以降低安全和运营的复杂性。

● 均衡模式：CSC 平等地支持两个或更多个主要 CSP。

理想情况下，CSC 会选择与其成熟度最匹配的策略。它从单一提供商开始，然后根据需要选择性地支持其他 CSP 的隔离部署，直到最终成熟到可以支持多个 CSP。虽然这是我们的建议，但我们也了解到，由于实际情况、内部政策和业务关系等原因，许多 CSC 在达到预期成熟度级别之前就被迫支持多云。

然而，迈向多云采用的旅程并不总是线性的，也并非完全由 CSC 的准备程度驱动。外部因素通常会加速向多云战略的过渡，迫使 CSC 在达到理想的成熟度水平之前应对多云复杂性。这一现实凸显了对适应性强、可扩展的云管理实践以及零信任等安全策略的需求，以适应业务、技术和威胁形势的动态特性。

4.3.3.1IaaS 和 PaaS 多云的工具和人员配备

与混合云一样，多云安全始于每个 CSP 内部的良好安全性，包括使用适当的工具来完成适当的工作。我们在整个领域讨论这些工具，这个子集可以在多云安全中发挥重要作用。

● IAM/SSO/联合身份代理：绝大多数云安全故障都与 IAM 有关。对于多云安全而言，从可靠的身份提供商开始至关重要。根据身份提供商的不同，可能需要联合身份代理来集中和规范单点登录 (SSO) 连接以及与多个提供商和部署的组/角色映射。

● 以云为中心的 SIEM：每个提供商都有自己的安全监测范围，具有多种来源和格式，并且每个 CSP 都不同。为与主要 CSPs 易于集成而设计的工具还包括一系列预构建的威胁检测器，这可以减轻多云支持的负担。

- （CSPM）：CSPM 是一个不断发展的类别，其扩展功能可渗透到其他新的或现有的产品类别中。CSPM 可让您通过一个中央工具监控多个 CSP 的配置、安全性和合规性。

还有许多其他工具将支持安全计划，而这套工具是多云环境的基础。它管理用户与多个云的连接，集中跟踪关键安全监测数据，并提供对多云安全性和合规性配置的可见性。

人员配备比工具配备更具挑战性。市场上不乏安全产品供应商，但熟练的云安全专业人员仍然短缺。许多 CSC 还试图在不增加人员的情况下过渡到云，迫使现有员工在仍支持传统基础设施的同时培养云技能。

每个云服务供应商（CSP）在最基础的技术层面上都存在本质的差异，并且每种服务都需要专门的知识。随着对某一 CSP 提供的服务使用量的增加，保护这些不同服务所需的知识范围也随之扩大。至少，云客户（CSC）应为每个承载任何重要（或关键）业务的云平台配备至少一名领域专家。主要/次要策略有助于减少对每个平台专业人才的需求。

许多 CSC，特别是规模较小的 CSC，尝试将提供足够熟练的员工的责任转移给托管服务提供商(MSP）。虽然在许多情况下这可能是一种可行的策略，但它并不能转移安全和治理的责任。此外，确保托管服务提供商的愿景、战略和能力与 CSC 的期望未来状态保持一致至关重要。

4.3.4SaaS 混合云和多云的组织管理

如今，云客户（CSC）采用多种软件即服务（SaaS）云服务供应商（CSP）来提升其业务运营能力。与基础设施即服务（IaaS）不同,软件即服务（SaaS）通常涉及整合以及 CSC 需要承担更高的灵活性和安全责任，这为 SaaS 领域带来了其特有的挑战。这些挑战包括针对众多业务应用程序的广泛产品、不同的安全成熟度水平以及跨不同 CSP 的多样技术。然而，SaaS 通常要求客户承担较低级别的安全责任。这种多样性源于 SaaS 能够为 CSC 提供有效且具针对性的方法，利用创新来满足其业务需求。

在 CSC 内部，有效的 SaaS 安全管理始于对投资组合的严格管理。在评估 SaaS CSP 是否能够满足业务需求的同时，也应对其安全性和合规性措施进行全面评估。然后，可以根据分类授权他们处理特定类型的数据。这一授权流程以及每个 SaaS CSP 的详细信息应在中央注册表中详细记录和维护。如果业务部门内部提出在已提供服务的类别中采用新的 SaaS CSP，可能需要提供有力的业务理由来支持在已批准的 CSP 之上或与已批准的 CSP 一起添加新的 CSP。

SaaS 解决方案经常需要与其它应用程序集成，无论是混合云模型中的内部应用程序还是其他 SaaS 产品。这些集成促进了应用程序间的数据流动，有时这些流动不会直接关联回单个用户。因此，建立对这些集成的治理有助于维护安全性并控制数据流动。

以下两种类型工具可以帮助管理安全程序中的多个 SaaS CSP：

1、联合身份代理：联合身份代理是身份即服务产品不可或缺的一部分，可用于调解 CSC 身份提供商与其云服务实例之间的联合身份管理连接。联合身份代理为主要 CSP 预先构建集成，并提供统一仪表板供用户访问不同的服务，从而显著简化 CSC 和用户访问和权限的生命周期管理。

2、云访问安全代理(CASB)：CASB 工具用于监管云客户（CSC）的 SaaS 产品组合，提供访问控制和监控功能，并确保只有授权的 SaaS 云服务供应商（CSP）的用户和从授权的位置进行使用。随着 CASB 领域的持续演进，特别是随着零信任安全原则的实施，部分供应商已经开始将关注点扩展到安全配置上，从而催生了 SaaS 安全态势管理（SSPM）的概念。CASB 的核心优势在于提供对 CSC SaaS 使用情况的洞察力和一定程度的控制能力。同时，SSPM 专注于监控和维护安全措施。高级 CASB 解决方案还可能包括实时监控、数据泄露防护（DLP）以及其他功能，以增强 SaaS 的安全性。

通过集成这些工具和策略（理想情况下与零信任安全策略和原则保持一致），CSC 可以更有效地管理其 SaaS 产品组合，帮助确保安全性和合规性，同时利用 SaaS 提供商提供的创新解决方案。

4.3.5 混合云和多云的零信任安全策略

成功的网络攻击通常会利用人们的信任。这使得“信任”成为一个危险的漏洞，应该降低其风险并加以控制。零信任是一种网络安全策略，基于这样一个理念：任何用户或资产都不应该被默认信任。它假设已经发生或将要发生入侵，因此，不应通过在企业边界执行的单次验证授予用户访问敏感信息的权限。相反，每个用户、设备、应用程序和交易都必须持续验证。

零信任是一种企业安全策略，涵盖云/多云、本地和混合系统、内部和外部合作伙伴/利益相关者用户（CSC 管理和自带设备）端点，并包括运营技术 (OT)、工业控制系统 (ICS)、物联网 (IoT) 和物理安全。许多安全专家认为， 对于当前具有大量远程办公和 OT/IoT 组件的分布式企业云/多

云和混合环境，零信任是最佳的企业安全策略。这种策略本质上固守和统一了本地化访问控制类型，支持了前面章节中推荐的环境和应用程序之间的分割和隔离。

总结

利用云环境中的组织或租户层级结构是管理云部署的几个关键方面的战略方法，包括最小化潜在安全事件的影响范围、遵守服务限制以及实现部署的逻辑分离。这种层级结构是协调各种安全控制的基础，强调了深思熟虑和战略性实施的重要性。层级结构不仅有助于有效管理，而且还增强了云部署的安全态势。

身份提供者或目录是管理 CSP 环境中的访问和权限的最前沿。此组件是管理单个权限的初始层，随后在 CSP 的服务中强制执行。CSP 策略作为预防控制措施发挥着关键作用，为整个层级结构的治理提供了强大的机制。这些策略使 CSC 能够控制服务的使用并强制执行特定配置，从而增加额外的安全性和合规性层。

安全信息和事件管理 (SIEM)、安全数据湖和 CSPM 等工具对于在云环境中实现集中可视性必不可少。它们提供对云部署中安全事件、配置和合规性状态的全面洞察，增强 CSC 有效检测和应对潜在安全威胁的能力。

在混合云环境中，重点转向 IAM，尤其是目录和网络连接点。这些组件对于保护本地基础设施和云服务之间的接口、确保不同环境之间的安全访问和数据流至关重要。

对于应对多云战略复杂性的 CSC 来说，最宝贵的资产是足够的专业知识。在特定云平台和服务方面拥有深厚专业知识的个人对于应对多云部署带来的独特挑战和机遇至关重要。他们提供必要的知识和见解，以优化跨不同 CSP 的云服务使用，确保将安全性、合规性和运营效率保持在最高水平。这种强调分层组织、预防性控制、集中可视性和专家指导的云管理战略方法对于实现安全高效的云基础设施至关重要。

建议

云治理和管理

- 创建集中式云部署注册表

- 使用多个部署定义组织层级结构
- 包括特殊用例的例外情况
- 支持创建新部署的顺畅流程
- 使用 CSP 策略管理服务和功能

安全策略和控制

- 采用全局的现代企业安全策略
- 最小化对 CSP 的“根目录”或“全局管理员”凭据的访问
- 使用 CSPM 工具监控和维护安全性和合规性
- 从组织/租户根目录之外的部署运行安全工具
- 为云和数据中心部署制定适当的安全策略
- 关注混合部署中的 IAM 和网络连接
- 正式确定混合连接的要求
- 确保混合/多云环境中容器的安全控制

多云策略

- 除非足够成熟，否则不要轻易在生产中尝试多云
- 建立与云成熟度相对应的多云策略
- 拥有熟悉特定云服务提供商的安全主题专家
- 为多云配备相应充足的安全人员

云安全监控和管理

- 使用支持所有使用的云服务供应商（CSP）的云安全态势管理（CSPM）工具
- 考虑使用 CASB 工具来管理 SaaS 服务
- 考虑使用 SSPM 工具来实现 SaaS 平台可见性

云互操作性和可移植性

- 考虑互操作性和可移植性策略

SaaS 治理

- 维护已批准的 SaaS 平台的注册表

补充指南

- 第三方安全服务的角色和职责 | CSA
- AWS 登陆区
- Azure 登陆区
- 谷歌登陆区
- Oracle 云基础设施 - 登陆区

领域 5：身份与访问管理

身份和访问管理(Identity and Access Management，IAM)确保只有经过授权身份才能访问相应的资源。随着云平台将众多数据中心的管理功能和服务整合到统一的可通过互联网访问的 Web 控制台和应用程序编程接口 (API)中，IAM 成为云原生安全的新防线，保护敏感资源免遭未经授权的访问和滥用。

在公有云和私有云中，云服务提供商(Cloud Service Provider，CSP)和云客户(Cloud Service Customer，CSC)都有责任在可接受的风险容忍度内管理 IAM。虽然我们将回顾基本的 IAM 概念，但重点将放在云中 IAM 的特征和挑战以及确保 IAM 的有效管理。

与本地系统相比，云计算为 IAM 管理引入了新维度。虽然核心安全问题可能并不新鲜，但它们的影响却被放大，并可能在云环境中产生连锁反应。

在云中管理 IAM 与在本地系统管理 IAM 之间的主要区别是：

- 云服务提供商（CSP）与云客户（CSC）之间的关系，以及各自的职责。
- 多个管理接口的整合。
- 这些接口对互联网的暴露，特别是对于公有云环境。

IAM 不能仅由 CSP 或 CSC 管理。它需要双方之间的信任关系、明确的责任划分以及促进 IAM 管理的技术机制。此外，与多个 CSP 打交道的 CSC 还增加了管理多个 IAM 解决方案与每个供应商的独特策略保持一致的复杂性。

本领域主要关注 CSC 和 CSP 之间，或 CSP 和服务之间的 IAM。本领域不讨论在云应用内管理 IAM 的所有方面，例如运行在基础设施即服务(Infrastructure as a Service,IaaS)的企业应用程序的内部 IAM。

学习目标

在本领域，您将学习：

- 定义身份联合及其在身份验证中的作用。
- 区分云环境的 IAM 策略类型。
- 识别身份和访问管理(IAM)的关键组件。
- 在云应用中有效地管理客户身份。

5.1 云中的 IAM 有何不同

IAM 始终很复杂。从本质上讲，某种类型的实体（例如，一个人、一个系统、一段代码）被映射到与各种属性（可以根据当前情况而变化）相关联的可验证身份，然后根据权限决定该实体可以做什么或不能做什么。随着所涉及的不同系统、服务和技术的数量增加，实现这一可验证性的复杂性也会增加。

云计算的 IAM 有三个主要区别：

● IAM 现在可以跨越云计算中的多个组织-任何 CSC 都可以有多个 CSP。这些 CSC 可能使用各种云服务模型中的大量服务。身份联合是处理此问题的主要工具，它通过在组织之间建立信任关系，并通过基于标准的技术来实现这些信任关系。

● CSP 都使用自己私有的 IAM 系统。这些 IAM 系统不仅技术不同，而且整个架构甚至许多术语都不同。CSC 需要学习、理解和实施多种不同的 IAM 模型。虽然传统架构中的不同应用程序和软件堆栈也是如此，但云将这一层异构性添加到整个管理平面甚至连接服务的基础设施中。

● CSP 将管理功能整合到统一的 Web 控制台和 API 中。在公有云，这些管理功能通常暴露于 Internet 上，通常仅使用用户名和密码（以及可能可选的强身份验证或策略条件）进行保护。私有云和容器平台通常会将其管理平面直接或者通过安全配置错误的方式暴露给 Internet。

身份联合和众多 IAM 系统定义了管理云身份和访问的复杂性，而统一管理功能并将其置于互联网上则显著增加了其安全风险临界性。这些问题并非理论上的；绝大多数云原生安全漏洞通常源于 IAM 失效。

迁移到云为 IAM 改进创造了机会。主要供应商通常支持较新的能力，例如基于属性的访问控制(Attribute-Based Access Controls，ABAC)、基于策略的访问控制(Policy-Based Access Controls，PBAC)、基于角色的访问控制 (Role-Based Access Controls(RBAC)、基于风险的身份验证和授权、临

时凭证、密码管理、即时（Just In Time，JIT）访问和其他高级选项。这些能力创造了安全专业人员长期以来一直努力实现的潜在响应能力和控制粒度。

IAM 基本上涵盖了云安全知识认证 (Certification of Cloud Security Knowledge，CCSK)中的每个领域。下一节首先回顾一些并非所有读者都熟悉的基本 IAM 概念和术语，然后深入探讨云的影响-首先是对身份，然后是对访问管理。

5.2 基本术语

IAM（身份识别与访问管理）是一个广阔实践领域，拥有自己的专业术语，然而有些术语可能令人困惑，特别是因为某些术语在不同上下文中具有不同含义（并且在 IAM 之外的领域使用）。甚至“IAM”这个术语都不是通用的，也被称为身份管理 (Identity Management，IdM)。

Gartner 将 IAM 定义为“安全原则，它能使适当的人员能够在适当的时间以适当的理由访问适当的资源。”在我们深入讨论细节之前，以下是与讨论云计算中 IAM 最相关的高级术语：

- 访问控制（Access Control）：基于授予实体的权限来限制对资源的访问。
- 断言（Assertion）：身份提供者(Identity Provider，IdP)向依赖方(Relying Party，RP)发出的包含实体信息的声明。当 IdP 和 RP 不是单一实体或不在共同管理下时，通常会使用联合技术。RP 使用断言中的信息来识别实体，并就其对 RP 所控制资源的访问做出授权决策。
- 属性（Attribute）：实体的特征或性质，用于描述其状态、外观或其他相关方面。属性可以包括各种信息，例如个人详细信息、用户角色、安全许可级别、访问请求的时间或发出请求的位置。
- 基于属性的访问控制（Attribute-Based Access Control，ABAC）：需要特定属性的访问控制或授权，例如多因素认证(MFA)、从被管理系统登录的用户或具有特定标签的目标资源。
- 认证（Authenticate）：验证用户、进程或设备的身份，通常作为允许访问系统资源的先决条件。
- 权威来源（Authoritative Source）：一个受信任的系统，包含关于实体身份属性的最准确和最新信息。其他 IAM 组件会使用此信息执行身份验证和授权等任务。
- 授权（Authorization）：允许或拒绝主体访问系统对象（例如网络、数据、应用程序、服务等）的决策。

● 权利（Entitlement）：将身份映射到具有所需属性的授权（例如，当用户 X 的 Z 属性具有指定值时，允许访问资源 Y）。我们通常将这些权利的映射称为权利矩阵。权利通常被编码为机器可读的策略，以便于分发和执行。

● 实体（Entity）：实体是指计算机系统中唯一的，可识别的参与者。在网络安全领域，实体可以是用户、设备、应用或系统，它们都可被 IAM 系统识别和验证。实体在系统中可以拥有不同的角色和权限，并且通常会记录它们的操作和对资源的访问，以用于审计和安全目的。

● 联合身份管理(Federated Identity Management)：允许用户使用一组凭证访问多个系统或应用，这组凭证通常由身份提供方(IdP)提供。这是单点登录(Single Sign-On，SSO)的关键赋能因素，也是云计算的核心能力。

● IAM 委托人（IAM Principal）：可以请求对 CSP 资源执行操作的用户、角色或其他身份类型。

● 标识符（Identifier）：用于断言身份的制件。它可以是数字的（例如密码令牌），也可以是物理的（例如驾照和护照）。

● 身份（Identity）：给定命名空间内实体的唯一表达。一个实体可以有多个数字身份，例如一个单一个体有工作身份（甚至有多个身份，取决于系统）、社交媒体身份和个人身份。

● 身份提供方(Identity Provider，IdP)：联合中的身份来源。负责执行身份验证策略。IdP 还可以通过将 CSP 角色映射到 IdP 属性，在授权策略中发挥重要作用。IdP 并不总是身份的权威来源，但有时可以依赖身份权威来源。

● 多因素认证（Multi-Factor Authentication，MFA）：一种通过附加因素（例如您知道、拥有或是什么）来验证身份的机制。这是遏制基于身份的攻击（例如被盗的用户 ID/密码等）的重要技术。它通常用于在授予对金融、健康等关键系统的访问权限之前验证身份。该技术还用于有条件的访问，例如从未知设备、未知地点/国家（“不可能的旅行”）登录等。

● 人物角色（Persona）:以用户为中心的视角有助于理解不同用户类型如何与系统交互。它代表具有相似特征的一类用户，并用于开发角色。例如，云系统可以通过描述开发人员、安全分析师、销售代表或内容创建者需要做什么来定义他们的人物角色。这可能导致开发独特的角色和特定的权限。

● 基于策略的访问控制（Policy-Based Access Control，PBAC）：访问需求定义在机器可读的策略文档中，该文档通常提供广泛的灵活性和颗粒度，并支持各种条件和其他变量，例如属性。PBAC 是对 RBAC 和 ABAC 的补充，通常还是定义和管理它们的方式。PBAC 策略文档也使用版本控制存储库和基础设施即代码(Infrastructure as Code，IaC)进行管理，有时被称为条件访问。

● 依赖方(Relying Party，RP)：依靠 IdP 来验证用户身份和访问权限并授予其对自身资源权利的服务。有时被称为服务提供商。

● 角色（Role）：提供以权限为中心的视图，定义用户执行特定任务的访问级别。角色可以是用户独有的，也可以是用户之间共享的。单个用户可能根据其职责拥有多个角色。相反地，如果多个用户具有相同的访问需求，他们可以共享同一角色。例如，每一个定义为“销售代表”的人物角色将拥有相同的权限。

● 基于角色的访问控制（Role-Based Access Control，RBAC）：是一种比 ABAC 更常见的模型，其中访问权限被授予具有给定角色（例如，开发人员或管理员）的所有用户。

下文将介绍其他一些术语，包括主要的 IAM 标准。有关 IAM 的更多定义请参见 CSA 的 IAM 词汇表。

5.3 联合

身份联合（Federation）在处理身份验证的 IdP 与管理授权的 RP 之间建立联系。在云中，RP 通常是一个云服务或应用。因为一个 IdP 可以联合许多 RP，这整合了用户管理（创建、角色分配、属性、身份验证和删除），同时支持分布式系统之间的授权和访问控制。

目前存在不少 IAM 标准和框架，其中很多可以用于云计算。尽管 IAM 可选项的范围很广，云安全行业正在围绕大多数身份提供商共同支持的核心标准集进行整合。

5.3.1 常见联合标准

以下是一些常用的身份联合标准。此列表并不代表任何特定的背书，也不包括所有选项，而只是一些最广泛供应商普遍支持的代表性样本。

● 安全断言标记语言（Security Assertion Markup Language，SAML）是结构化信息标准促进组织（Organization for the Advancement of Structured Information Standards，OASIS）的联合身份

管理标准，支持身份验证和授权。它使用可扩展标记语言（eXtensible Markup Language，XML）在 IdP 和 RP 之间做出断言。断言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 CSP 都广泛支持 SAML，但最初的配置可能是复杂的。SAML 非常适合传统的基于 Web 的客户端-服务器应用程序。

● 开放授权（Open Authorization，OAuth）是互联网工程任务组（Internet Engineering Task Force,IETF）的授权标准，广泛应用于 Web 服务（包括消费者服务）。OAuth 被视为一种授权协议，允许用户授予第三方应用程序有限的资源访问权限，而无需直接与这些应用程序共享其凭据（如密码）。OAuth 常用于授权 API 访问或将第三方连接到应用程序。OAuth 工作在 HTTP 上层，最常用于在服务之间委派访问控制和授权。

● OpenID Connect(OIDC)是 Web 服务广泛支持的联合身份验证标准。它为 OAuth 添加了身份验证层，基于 HTTP 并使用 URL 来识别 IdP 和用户/身份（例如 http://identity.identityprovider.com）。OIDC 1.0 在消费者服务中非常常见，商业产品对它的支持也越来越多。一个例子是单页应用程序（Single Page Application，SPA-例如 Facebook）。OpenID 是一种身份验证标准，与 OIDC 不同。OpenID 2.0 已弃用，并已基本上被 OIDC 取代。

另外两个不太常见但对云计算有用的标准如下所示。

● 可扩展访问控制标记语言（eXtensible Access Control Markup Language，XACML）是定义基于属性的访问控制（ABAC）和授权的标准。XACML 是一种策略语言，用于在策略决策点(Policy Decision Point，PDP)定义访问控制，然后将其传递给策略执行点(Policy Enforcement Point，PEP)。XACML 可以与 SAML 和 OAuth 一起使用，因为它解决了问题的不同部分，即允许实体对一组属性执行什么操作，而不是处理登录或权限授权。

● 跨域身份管理系统（The System for Cross-domain Identity Management，SCIM）是跨域交换身份信息的标准。它可用于在外部系统中配置和取消配置账户以及交换属性信息。

5.3.2 联合身份管理的工作原理

联合身份涉及 IdP 在与 RP 之间建立加密信任关系后向 RP 做出断言。一个实际的例子是用户登录到他们的工作网络，该网络托管账户的目录服务器。IdP 和 RP 共享一个秘钥。当用户打开浏览器连接到 SaaS 应用程序时，不会启动登录过程，而是有一系列幕后操作（图中的步骤 1 到

6），其中 IdP（内部目录服务器）断言用户的身份、对用户进行身份验证，并可能转发任何必要的属性。然后，RP 可以信任这些断言，从而让用户登录，而无需用户输入任何凭据。RP 在其自己的命名空间中不需要该用户的用户名或密码；反而，它依靠 IdP 来断言成功的身份验证。假设用户已成功通过内部目录服务器的身份验证，则用户只需访问 SaaS 应用程序的网站并登录即可。

这并不意味着云计算中没有其他用于身份、身份验证和授权的技术或标准。大多数 CSP，特别是 IaaS 都有内部 IAM 系统，这些系统可能不使用，或者使用这些标准连接到 CSC。例如，HTTP 请求签名通常用于对 REST（Representational State Transfer） API 进行身份验证，以及在 CSP 端使用内部策略来管理授权决策。请求签名可能仍然通过 SAML 支持 SSO，或者 API 可能完全基于 OAuth，或者甚至使用自己的令牌机制。所有这些都很常见，但大多数企业级 CSP 都支持联合。

选择身份协议时的重要理念是：

- 没有一种协议是可以解决所有身份和访问控制问题的万全之策。
- 必须在给定的用例上下文中分析身份协议。例如，基于浏览器的 SSO、API 密钥或移动设备到云的身份验证都可以从不同的方法中受益。
- 关键的假设应该是，身份本身就是一个边界，类似于非军事区。

下图说明了云安全中 OpenID 联合的工作流程，详细描述了从通过 IdP 进行用户身份验证到访问依赖方服务的步骤。

图25：云安全中OpenID联合的工作流程

5.3.3 管理云计算的用户和身份

身份管理中的“身份”部分侧重于注册、配置、传播、管理和取消配置身份的流程和技术。管理身份并在系统中配置身份是信息安全部门几十年来一直在应对的挑战。不久前，IT 管理员需要在每个不同的内部系统中单独配置用户。即使在今天，有了集中式目录服务器和一系列标准，适合一切场景的真正 SSO 仍然相对罕见；用户仍然需要凭证，尽管比过去少了很多。

在决定如何管理云计算的用户和身份时，云服务提供商（CSP）和云客户 CSC 需要从两个关于如何管理身份的基本决策开始。

- CSP 应在其管理的命名空间中支持用户的内部身份、标识符和属性，用户可直接访问服务。此外，他们还应支持联合身份，以防止 CSC 手动配置和管理提供商系统中的每个用户并为每个用户颁发单独的凭证。
- CSC 需要决定管理其身份的最佳位置，并选择适当的架构模型和技术来与 CSP 集成。

CSC 可以登录 CSP 并在其系统中创建所有身份。但是，除了也许最小的 CSC 之外，这种方法对于大多数 CSC 来说都是不可扩展的，这就是大多数 CSC 转向联合身份的原因。在某些例外情况下，将所有或部分身份与 CSP 隔离是有意义的，例如帮助调试联合身份连接问题的备份管理员账户。

在使用联合时，CSC 需要确定唯一身份的权威来源，通常是内部目录服务。接下来，他们必须决定是否直接将此来源用作 IdP，使用由其派生的另一个身份来源（例如来自人力资源系统的目录）,或集成身份代理。联合身份管理有两种主要的架构：

- 中心辐射模式：内部 IdP/来源与中央代理或存储库进行通信，中央代理或存储库充当与 CSP 联合的 IdP。
- 自由组织模式：内部 IdP/来源（通常是目录服务器）直接连接到 CSP。

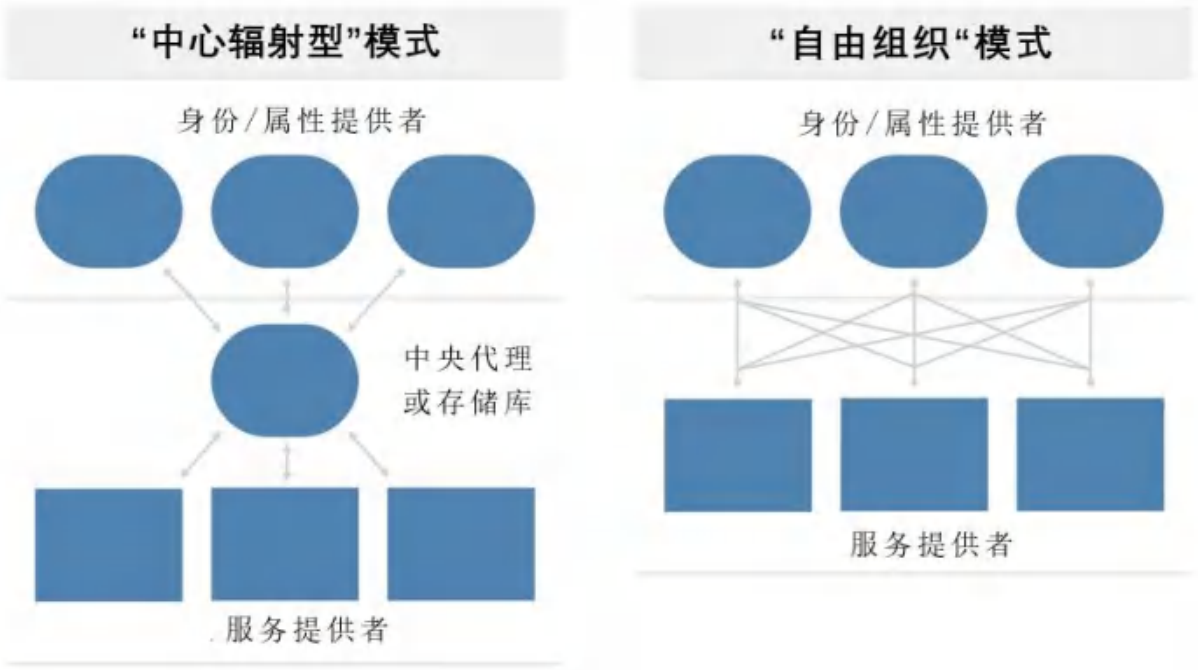


图26：联合身份管理的架构模型：中心辐射型 vs 自由形式

在自由形式模型中直接联合内部目录服务服务器会引发一些问题：

- 该目录需要 Internet 访问。如果违反安全策略，则可能是有问题的。
- 它可能要求用户在访问云服务之前通过 VPN 重新连接到公司网络。
- 根据现有的目录服务服务器，特别是如果不同的组织孤岛中存在多个目录服务服务器，联合到外部提供商可能会是复杂的且技术上很困难。

联合身份代理负责处理 IdP 和 RP 之间的联合。它们可以部署于网络边缘，甚至可以部署于云中，以实现 Web SSO。IdP 不必仅在本地部署，许多 CSP 现在支持基于云的目录服务，这些目录服务既可以在内部也可与其他云服务管理联合。

例如，更复杂的架构可以将 CSC 的部分身份信息从内部目录通过身份代理同步或联合到云托管目录。然后，这个云托管目录可以充当其他联合连接的 IdP。

在实施这些解决方案时，需要考虑几个流程和架构决策：

- 如何管理应用程序代码、系统、设备和其他服务的身份。在云部署和应用软件中，可能利用相同的模型和标准，或者决定采用不同的方法。定义身份配置流程以及如何将其集成到云部署

中。对于不同的用例，可能还有多个配置流程，但目标应该是拥有一个统一的流程。一个常见的例子是员工入职与承包商入职的对比。

- 建立撤消配置流程。适当的治理需要充分且有时迅速地删除身份和访问权限，同时对这些权限的使用情况进行适当的取证跟踪。
    - 如果 CSC 已为传统基础设施制定了有效的配置流程，那么最好将其扩展到云部署中。然而，如果现有的内部流程存在问题，那么 CSC 应该利用迁移到云的机会来构建新的、更有效的流程。
- 配置和支持单个 CSP 和部署。应该有一个将新 CSP 添加到 IAM 基础设施的正式流程。这包括建立任何所需联合连接的过程，以及：
    - 映射 IdP 和 RP 之间的属性（包括角色）。
    - 传递属性以支持 ABAC/PBAC（例如，MFA 状态或用户已进行身份验证的 IP 地址）。
    - 启用所需的监控/日志记录，包括与身份相关的安全监控，例如行为分析。
    - 建立权利矩阵（下一节将进一步讨论）。
    - 记录任何中断/修复场景，以防用于关系的任何联合（或其他技术）出现技术故障。如果 IdP 出现故障，或者与 CSP 的互联网连接出现故障，或者 CSP 的联合支持出现故障，是否有业务连续性计划？
    - 确保针对潜在账户接管的事件响应计划到位。
    - 为身份和 CSP 实施取消配置或权利变更流程。这需要联合关系双方的努力。

最后，CSP 需要确定支持哪些 IdM 标准。一些 CSP 仅支持联合，而另一些 CSP 则支持多种 IAM 标准以及他们自己内部的用户帐户管理。服务于企业市场的 CSP 通常需要支持联合身份，最有可能是 SAML。

5.4 强身份验证和授权

确保强大的身份验证和授权对于云安全至关重要。本节概述保护云访问的关键实践。

认证用于验证用户身份，这对于访问云服务至关重要。多因素认证（MFA）除密码之外增加了额外的安全层，方法包括硬令牌、软令牌和生物识别，每种方法提供不同级别的安全保护。

授权确定用户权限。基于角色的访问控制（RBAC）和基于策略的访问控制（PBAC）等有效模型可管理和执行这些权限，提供细粒度控制。

云服务提供商（CSP）执行这些策略，但云客户（CSC）必须定义和管理它们。基于属性的访问控制（ABAC）等高级模型通过允许上下文感知的访问决策来增强安全。通过实施强壮的身份验证和授权实践，组织可以保护其云资源并确保安全访问。

5.4.1 身份验证和凭证

身份验证是用于验证身份的过程。它不仅对于登录很重要，而且对于必须验证身份并将其与系统或流程内的特定权限或角色相关联的所有场合都很重要。身份提供者（IdP）承担确保可靠身份验证的责任。

云计算对身份验证的最大影响是对强 MFA 的强劲需求，主要有两个原因：

- 广泛的网络接入：云服务始终通过网络访问，通常是通过互联网。这意味着如果凭证丢失或被盗，会更容易导致账户接管，因为攻击并不局限于本地网络。
- 更多地使用联合来实现单点登录（SSO）：对多个云服务使用单独一组凭证意味着，如果这些凭证被泄露，那么大量的服务可能会面临风险。

MFA 是减少账户接管的最强方法之一。虽然它不是万能，但对云服务依赖单一因素（密码）会带来高风险。当使用 MFA 和联合时，IdP 可以而且应当将 MFA 状态作为属性传递给 RP。

MFA 有多种选项，包括：

- 硬令牌是一种物理设备，可生成一次性密码(One-Time Password，OTP)供人工输入或需要插入读卡器。当需要最高级别的安全时，它们是最佳选择。
    - 插入式令牌比用户输入生成 OTP 的令牌更可靠。
    - 有多个用户被网络钓鱼或其他有针对性的攻击诱骗输入或分享 OTP 密码的例子。
- 软令牌的工作原理与硬令牌类似，但由智能手机或计算机上运行的软件应用程序生成。软令牌是一种很好的选择，但如果用户的设备受到攻击，软令牌也可能会被危害，因此任何威胁模型都需要考虑这种风险。

● 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 OTP 一样输入。虽然这也是一个不错的选择，但任何威胁模型都必须考虑消息拦截，尤其是使用短信。由于 SIM 卡交换和针对该基础设施的其他攻击，不再推荐使用 SMS 短信。

● 生物识别逐步成为一种新的选择，因为现在手机上普遍配备了生物识别读取器。对于云服务而言，生物识别是一种本地保护，不会将生物识别信息发送给 CSP，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。

随着组织寻求加强其身份验证机制，人们开始采用传统方法以外的其他方法。这些方法旨在增强安全性，同时提高用户的便利性。

5.4.1.1 其他身份验证方法

无密码身份验证：这种方法利用本地令牌或证书来绕过密码使用，类似于与服务、用户和设备关联的 SSO 令牌。它简化了用户体验，并降低了数据泄露期间网络钓鱼和密码暴露的风险。然而，无密码方法主要用于对消费者应用程序进行用户身份验证, 不推荐用于管理级云服务账户。需要注意的是，无密码系统不应取代 MFA。

快速在线身份验证（Fast IDentity Online，FIDO）：作为当前无密码身份验证的行业标准，FIDO 可能有各种名称，例如“Passkeys”或“Webauthz”，代表着通过提供防网络钓鱼身份验证方法的技术进步。FIDO 允许用户定义可在登录过程中用作身份验证因素的可信设备。FIDO 还可以通过插入或无线连接到访问设备的物理令牌来增强安全。开发无密码身份验证标准的 FIDO 联盟由主流 IT 供应商组成，包括 CSP 和身份和访问管理解决方案提供商。

5.4.2 权利和访问管理

授权和访问控制这两个术语有一定重叠，并且根据上下文有不同的定义。

● 授权是做某事的许可——例如，访问文件或网络，或执行某项功能（如对特定资源的 API 调用）。

● 访问控制允许或拒绝授权的使用，因此它包括在允许访问之前确保用户已经通过身份验证等方面。

● 云权限是指在云环境中授予用户访问特定资源或服务的权限。权限通常决定用户可以对给定资源执行哪些操作，例如读取数据、写入数据、配置设置或管理其他用户。

权限将身份映射到授权和任何需要的属性（例如，当属性 Z 具有指定值时，用户 X 被允许访问资源 Y）。我们通常将这些权限的映射称作权限矩阵。使用 PBAC 时，权限通常被编码为分发和执行的技术策略。

表 6：云访问管理权限矩阵示例

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

云以多种方式影响权限、授权和访问管理：

● CSP 和云平台各自有一套特定的潜在授权机制。除非 CSP 支持 XACML（目前很少见），否则 CSC 用户通常需要直接在云平台内配置权限。

● CSP 负责执行授权和访问控制。

● 云用户负责定义权限并在云平台内正确配置它们。

● 云平台倾向于为 IAM 提供 ABAC 和 PBAC 模型的更大支持，这些模型比 RBAC 模型提供了更大的灵活性和安全性。RBAC 是执行授权的传统模型，通常依赖于单个属性（即定义的角色）。ABAC 通过整合多个属性（例如角色、位置、身份验证方法等）来实现更细粒度和上下文感知的决策。

● 支持 ABAC 的 PBAC 是基于云的访问管理的首选模型。

● 使用联合身份验证时，云用户负责将属性（包括角色和组）映射到 CSP，并确保在身份验证期间正确传达这些信息。

CSP 负责支持细粒度的属性和授权，以便为云用户提供 ABAC 和有效的安全。

这是一个真实的云示例。CSP 有一个用于启动新虚拟机(VM)的 API。该 API 具有相应的授权以允许启动新 VM，并具有用户可在哪个虚拟网络中启动 VM 的附加授权选项。云管理员创建一项权利，规定开发人员组中的用户只能在其项目网络中启动 VM，并且必须通过 MFA 进行身份验证。组和 MFA 的使用是用户身份的属性。该权利以策略的形式编写，并加载到 CSP 的系统中以供执行。

5.4.2.1 资源访问控制和策略

到目前为止，我们主要在 CSP 实体向平台的集中 IAM 管理请求操作的背景下讨论了授权和权限。许多 CSP 还支持应用于单个资源（例如存储位置）的规则和/或策略，并且可以考虑在 CSP 内配置的实体之外的访问。

例如，大多数存储服务允许其他位置的用户通过使用共享链接、IP 限制或临时密码实现对象的直接外部访问。

这些权限是在资源级策略中实现的，可能会绕过中央 IAM 治理。尤其在存储服务中，这是数据泄露的常见来源。甚至可能出现这样的情况：CSC 中的 IAM 用户被明确拒绝访问主 IAM 系统内的资源，但由于资源策略薄弱，仍然可以访问这些资源。

为了降低这种风险，一些 CSP 提供了顶级安全控制来限制外部共享或使用可能允许公共或外部访问的资源策略。CSC 还可以使用自动化来识别和管理这些策略。

5.4.3 条件访问、令牌、会话和 IAM 边界管理

虽然说“IAM 是新的边界”很容易，但准确理解其确切含义很重要。在云中，或者在任何时候通过网络提供服务时，攻击者都可以直接攻击身份。如果攻击者危害身份或 IAM 系统的一部分，他们就可以在不进行网络攻击的情况下破坏资源。随着我们提高保护网络的能力，基于 IAM 的攻击（如网络钓鱼、扫描暴露的凭据或通过恶意软件窃取凭据）有所增加，现在已成为云原生漏洞的最大来源。

IAM 边界包括身份验证和授权、所有类型的实体（用户、系统、代码等），并扩展到联合连接。回顾 IAM 系统，边界是所有可能被访问的接触点，从网络钓鱼用户密码到滥用公开容器定义文件中暴露的凭据。

如上所述，任何联合身份验证操作都会生成一个令牌。此令牌与会话绑定，并具有定义的生存时间(Time To Live，TTL)，该时间与会话时长相对应。IAM 系统可能集成刷新令牌的概念，该令牌在会话到期前自动请求，然后在后台续展或创建新会话。

重要的是要理解令牌是身份验证的产物，可能被窃取和滥用，以提供未经批准的访问，而无需泄露密码。这是一种非常常见的攻击技术。攻击者可以窃取令牌，在许多情况下，甚至可以从他们控制的位于其他地方的系统使用它，直到会话过期或令牌被手动失效。

保护 IAM 边界依赖于 IdP 和 RP 之间划分的多种技术。目标是减少凭证和令牌的泄露和滥用。实现这一点的一项核心技术是有条件访问，它通常使用支持条件声明的 PBAC 策略在云中实现。有条件访问可以在身份验证、授权或两者期间强制执行。

虽然实现将特定于技术，但任何 IAM 边界保护策略都包含几个关键要素：

- 强身份验证（主要是 MFA）是保护 IAM 边界的关键第一步，但它只能处理用户（和某些系统）身份验证，并且仍然暴露于滥用。
- 尽可能使用可自动配置、轮换和取消配置的云提供商托管的访问凭据。所有主要 CSP 都支持此功能，可用于虚拟机、无服务器函数以及访问 CSP 内其他资源或服务的其他资源类型。
- 身份验证期间的设备和位置限制可以限制允许哪些设备以及来自哪些网络位置。虽然这对于去中心化组织中的用户来说可能更难实现，但它仍然可以轻松用于系统/服务身份验证。即使高度分散的 CSC 可以考虑设置 VPN/SASE79（Virtual Private Network/ Secure Access Service Edge）。
- PBAC 系统通常支持对每个授权请求的发起 IP 地址、MFA 状态等的限制性条件。这非常强大，因为每次 API 调用时都会检查授权策略，可以防止滥用被盗令牌。即使攻击者窃取了令牌，如果在授权上实施了 IP 限制，该令牌也无法从外部位置工作。
- 使用 JIT 技术，通过消除静态凭证可以减小滥用的窗口。请求会话访问权限，并获得外部批准，然后在会话结束时撤销。批准步骤是一种双重授权形式，并在会话创建之外管理。一些 CSP 和第三方工具支持此功能。主要好处是减少了攻击面：由于用户没有永久权限，攻击者的机会窗口大大减少。
- 大多数 IaaS 提供商在其网络架构中支持某种形式的内部服务端点，并且可以在 IAM 策略中利用这些端点来确保系统/资源 API 调用仅源自内部网络连接。

● 某些 PBAC 策略支持针对同一人物角色的给定权利有不同授权要求。例如，变更请求可能需要比读取访问权限更严格的一组属性。这将仅允许管理员从公司网络进行网络或 IAM 变更，但允许他们从任何地方访问日志以进行调试。

管理 IAM 边界可能是复杂的，但由于 ABAC 和 PBAC 功能的改进，我们不仅能够更好地根据某人是谁或是什么的静态概念来管理身份，还能够根据他们所在的位置、他们正在使用的设备以及其他持续评估的属性来管理身份。

最终，PBAC 越来越受到基于云的访问管理的青睐。它允许 CSC 实施响应云服务复杂和动态特性的安全策略，确保访问权限足够严格以保护敏感数据，同时又足够灵活以提高生产率。CSP 在支持这些复杂的访问控制机制方面发挥着至关重要的作用，可实现细粒度的属性和授权，从而满足云用户的安全和运营需求。

5.4.4 特权用户管理

想象一下某件东西对于一个国家非常重要-比如储存金银储备的金库-即使国家的主席或总理进入金库，也需要书记官记录进入的日期和时间。这是理解特权身份管理 (Privileged Identity Management，PIM)和特权访问管理(Privileged Access Management，PAM)的起点。

PIM 和 PAM 是组织 IT 环境（尤其是管理平面）安全治理的重要支柱。PIM 涉及监督和控制特权身份——那些拥有访问和修改关键系统或敏感数据的高级权限的用户。PAM 致力于监管和保护访问这些资产和资源的渠道。它涉及决定谁被授予访问权限以及构成该访问权限的方法、时间和活动范围。

PIM 和 PAM 框架固有的一个基本原则是 JIT 访问。JIT 仅在需要的时间段内分配访问权限，同时确保正确记录访问，从而减轻与永久特权和缺乏访问审计相关联的风险。如果不加以约束，永久特权访问将成为一种脆弱性，可通过账户泄露和会话劫持加以利用。

JIT 实践是最小权限原则的实际应用，确保用户仅具备履行其当前工作职责所必需的访问级别。类似，职责分离原则适用于为特权（管理员）和非特权（普通用户）访问提供不同的身份或账户。例如，不应将特权访问权限授予个人用于阅读电子邮件的同一身份/账户。PIM 和 PAM 服务支持的职责分离的另一个重要应用是，它们仅在另一个授权方（例如管理层）批准后才允许访问。一致应用这些原则可以减少对敏感系统的暴露和访问，并改善安全态势。

将 PIM 和 PAM 集成到企业的安全框架中可增强其防御能力。此举通过降低未经授权访问关键资源的可能性来增强整体安全态势。在任何给定时候减少活跃特权账户的数量可以缩小网络犯罪分子可能利用的潜在攻击向量。这种集成可确保遵守监管合规性要求，因为它建立了一个系统，可以监控、记录和审计与特权账户相关联的活动，从而加强 CSC 对敏感操作的控制。

PIM 和 PAM 解决方案具有维护安全合规 IT 环境的几个关键特征。其中最重要的一个特征是凭证的自动轮换，这确保无法通过旧的或泄露的凭证来维持访问，从而消除了系统安全中的一个常见脆弱性。此外，这些解决方案还强制执行 MFA。而且，它们还配备了全面的审计和报告工具。这些工具对于进行详细的取证分析和跟踪对组织策略和监管标准的遵守情况是必不可少的，可提供做出明智安全决策所需的洞察力。

5.5 公有云的 IAM 策略类型

在云计算中，访问控制通过各种策略层进行管理，旨在微调权限并增强安全性。主要策略类型是基于设备、身份、资源、组织或租户的。

基于身份的策略与 IAM 身份相关联。这可以是使用 IdP 获取云环境临时访问权限的联合用户，也可以是 CSC 固有的内部（云原生）IAM 身份。此身份的权限由策略定义，该策略确定允许或禁止的操作，并且可以专门附加到用户、角色或分布到整个组中。尽管不同 CSP 使用的术语各不相同，但基本概念保持一致：这些是附加在个体身份上的权限。

基于设备的策略与设备身份注册和合规状态相关联。设备分为受管设备和非受管设备。敏感信息和资源的访问可以限制在特定级别的设备状态和合规性，例如，设备必须具有更新和打过补丁的操作系统版本，并注册为 CSC 管理的设备。可以允许从较低的合规性状态（例如，来自非受管设备的访问）访问不太敏感的数据和资源。

基于资源的策略与基于设备和身份的策略不同，它们直接与云资源相关联，无论是 S3 存储桶、Lambda 函数或者任何其他服务。此类策略规定谁可以访问资源，并确定其他账户、设备或用户对该资源的允许操作。它们管理跨账户交互并控制对互联网公开资源的访问，包括确保只有授权实体才能对资源执行特定操作。

基于组织或租户的策略具有更广泛的覆盖范围，涵盖 CSC 账户内的整体云部署、跨订阅或整个项目。这些策略对跨越 CSC 的所有云资源实施一致的合规性和安全性标准至关重要。这些

策略通常由云管理员制定，不受制于单个用户或服务的修改，从而在整个部署中保持一致的和安全的基准。

这些策略在应用和范围上各有不同，指导着许多云服务中可能存在的多层访问控制。通过采用 PBAC 模型，CSP 允许遵循最小权限原则的细粒度权限。此模型确保用户和服务仅拥有完成其任务所需的访问权限，从而防止可能导致安全攻击的过多权限。

5.6 最小权限与自动化

最小权限原则是安全的基本原则，其理念是为个体提供履行职责所需的最低访问权限。大规模有效实施这一原则可能极具挑战性。云服务（尤其是 IaaS）提供详细的权限，这些权限可能增强安全态势的同时，也会显著增加复杂性。权限可以理解为一条特定规则：该实体可以具有这些属性在这样的条件下对这些资源执行这些操作。随着选项、实体、资源和条件的增多，管理和预测这些变量变得复杂起来。这种复杂性通常会导致权限过高，带来安全风险，或权限不足，从而阻碍业务运营。

随着基于云的 IAM 规模不断增长，自动化正成为实现有效权限平衡的少数可行策略之一。自动化 IAM 权限没有单一标准；方法取决于所使用的特定技术。不过，某些自动化方法已成功增强云安全性：

- 使用情况追踪：这涉及在一段时间内监控实体在云平台内的活动。然后，系统会分析分配的权限比对实际使用情况。在给定时间范围内未使用的权限将自动撤销，以增强安全性。
- 风险评分：在这种方法中，每个实体和动作都会根据一系列属性（例如 IP 地址或动作时间）分配一个风险分数。然后，这些分数会被输入到策略引擎中，该引擎会允许或拒绝动作-不仅基于预设的权限，还取决于风险级别在给定情况下是否可接受。
- JIT 权限：JIT 权限是根据需要请求和授予的。实体使用模板在指定时间范围内（例如在维护窗口期间）访问特定资源的一组预定权限。如果符合策略约束，则授予 JIT 访问权限，并且可能需要额外授权。当与风险评分系统集成后，JIT 可以得到进一步增强。
- 持续评估：云安全态势管理（Cloud Security Posture Management，CSPM）或以身份为中心的软件等工具，持续评估云环境中的 IAM 配置和实际访问模式，以发现错误配置、不必要的

权限和其他安全漏洞。可以手动或通过自动补救措施解决这些问题。例如，工具可能会扫描大量部署以标记未使用 MFA 管理角色的使用，或识别未经授权的静态访问密钥的存在。

像云身份和权利管理等工具可能会组合并实现这些能力，甚至包括纠正措施等附加选项。

5.6.1 身份与零信任

身份是任何零信任策略的核心要素之一。虽然零信任有多种定义和模型，但它们中的每一个都倾向于共享以下 IAM 原则：

- 访问和连接具有身份感知能力。
- 身份感知扩展到所有实体类型，而不仅仅是人类。
- 跟踪属性并用于为决策提供支持。
- 基于实体、属性、连接、请求的操作和资源的风险评分用于基于策略的决策。

例如，在零信任实施中，用户可能只能在特定时段、启用 MFA 且仅从特定地区访问源自不受信任系统的 Web 邮件，并且禁止附件下载。同一用户只能从官方公司系统访问附件。

零信任符合本领域讨论的许多原则，并且不特定于云，但越来越多地被视为 CSC 实现去中心化和云计算的主要访问策略。零信任也可以成为改进 IAM 边界实施的有力选择。

5.6.2 客户身份

托管在云中的应用软件可能必须管理自己的身份。开发人员有多种选择来处理这一需求，每种选择都有独特的优势和考虑因素。直接在应用软件自己的用户数据库中管理客户身份就是其中一种选择。这种方法需要建立和维护一个安全且可扩展的身份存储，确保用户数据得到安全处理并能快速适应不断增长的需求。

或者，联合可以利用来自外部 IdP（例如 Google、Facebook 或各种企业 SSO 系统）的现有凭据。此方法允许 CSC 使用其现有账户访问服务，从而简化登录过程并提高用户便利性。混合方法结合了两者的优点，提供自我管理身份的灵活性，同时支持联合登录方法。该策略通过适应不同的用户偏好和要求，实现量身定制的用户体验。

当应用软件允许 CSC 直接对云服务进行 API 调用时，保护此类访问就变得至关重要。实施安全的身份验证方法（例如 API 密钥、OAuth 令牌或其他机制）用于控制访问并定义参与者可以执

行的操作范围。确保实施可靠的授权控制，对于根据给定用户的角色标示不同访问级别的权限（例如只读权限、写入权限或完全管理权限）是至关重要的。

CSP，包括提供 AWS Cognito 的 AWS 或提供 B2C 的 Azure，简化了客户身份管理。这些服务提供注册、登录和访问控制等功能，简化了 IdM 的复杂性。第三方身份解决方案进一步扩展了这些功能，增强了用户体验和安全特征，并促进了跨多个平台的更轻松集成。

总结

IAM 极其重要，因为身份已成为管理公有云服务和部署访问的主要手段，超越了传统的网络边界。云安全的一个核心原则是认识到大多数云原生漏洞都可归因为凭证泄露，这强调了采取严格的身份验证措施的重要性。

MFA 被认为是所有云访问的基本要求。此措施通过要求除密码之外的多种验证形式，显著降低了未经授权访问的风险。此外，建议对管理级访问实施 JIT 访问或其他高级特权 IdM 机制，从而确保仅在必要的时间和在所需的持续时间内授予权限。

虽然 CSP 通常提供自己的身份池，但企业采用联合身份管理也有强大的应用场景。联合身份管理允许与现有 IdP 无缝集成，使用户能够使用从其他服务建立的凭证进行身份验证，从而简化用户体验并整合 IdM。

主流 CSP 都已采用 PBAC，该技术能够对访问权限进行细粒度控制。虽然 PBAC 通过详细的策略实施提供了增强的安全性，但它也为 IAM 框架带来了额外的复杂性。

有效的 IAM 策略将安全的 IdP 与强大的身份验证协议相结合。它们注重给予用户完成工作所需的刚好足够访问权限即可。它们根据不同的情况和策略类型使用规则。

在制定全面的 IAM 策略时，重要的是详细记录和阐明那些涵盖云架构各个组件的实践。此类文档应涵盖采用 MFA 背后的逻辑依据、特权账户 JIT 的使用、联合相对于私有身份存储的优势以及 PBAC 系统的复杂性。还应深入研究 IAM 实践与业务目标的一致性、安全措施与用户体验之间的平衡，以及 IAM 应对新兴威胁和技术的持续进化。

建议

身份管理

- 制定全面的策略、计划和流程来管理云服务身份和授权。

- 考虑使用身份代理来加强对身份来源的治理（在适当的情况下）。
- CSP 应当采用开放标准提供内部身份和联合身份。
- 没有特殊的协议：首先选择使用用例和约束，然后找到正确的解决方案。

访问管理

- 连接到外部 CSP 时，尽可能使用联合来扩展现有的 IdM。尽量减少与云 CSC 提供身份无绑定的身份孤岛。
- CSC 负责维护 IdP 并根据权威来源定义身份和属性。
- 云用户应当对所有云访问使用 MFA，并在使用联合身份验证时发送 MFA 状态作为属性。
- 记录符合安全和业务要求的每个云部署的权利矩阵。
- 在 CSP 或平台支持的情况下将权利矩阵转换为技术策略。
- 与 RBAC 相比，优先选择 ABAC 和 PBAC。
- 评估并采用更现代的 IAM 流程和技术，例如改进最小权限的使用情况跟踪，JIT 访问和风险评分。

安全措施

- 考虑实施具有基于位置限制的 IAM 边界，特别是针对敏感资源或管理级的访问，以降低使用被盗凭证或会话令牌进行攻击的风险。
- 尽最大程度可能地消除静态云凭证（如硬编码 API 密钥）的使用。
- 使用自动评估工具来监控 IAM 是否存在配置错误、过度访问、合规性失效和其他问题。考虑对严重违反策略的行为进行自动化补救。
- 记录并监控 IdP 和 RP 上的所有 IAM 变化。

事件响应

- 将失效或限制滥用的 IAM 会话令牌的计划和程序整合到事件响应程序中。

补充指南

- 网络安全和 IAM 中的机器身份 | CSA
- 云的 IAM 是什么？ | CSA

- 身份和访问的零信任原则和指南 | CSA
- 身份和访问管理词汇表 | CSA

领域 6：安全监控

此领域为云环境提出了独特的安全监控挑战和解决方案。它强调了云遥测、管理平面日志、服务和资源日志以及高级监控工具集成的不同方面。它探讨了混合和多云设置的复杂性，包括互操作性和安全性考虑。进一步强调了日志、事件和配置检测在全面安全监控中的关键作用。最后介绍了生成式人工智能(GenAI)，作为增强云安全性和提供多方面保护云基础设施的创新工具。

学习目标

在此领域，您将学习：

- 识别云环境中独特的安全监控挑战。
- 描述云遥测源在监控云环境中的重要性。
- 分析云环境中安全遥测的收集架构。
- 将监控和警报视为云安全的基础组件。
- 实施全面安全监控的检测手段。

6.1 云监控

云基础设施的动态特性为云中的安全监控带来了独特的挑战。警报的时机由于云中变化速度快以及资源分布方式不同，日志也会有所不同。需要专门的策略。此外，安全责任共担 (SSRM) 表明，云客户(CSC) 将负责监控的某些方面，而云服务提供商(CSP) 将负责其他方面。

云通过以下方式增加了安全监控的复杂性：

1. **管理平面：**管理平面控制所有管理操作，就像船长驾驶船只一样。云控制台必须受到密切监控，因为它会做出最关键的决策并授予对云中所有内容的访问权限。
2. **速率因素：**云端的变化速度极快。如此快的速率意味着安全流程必须灵活，并且需要自动响应以应对潜在威胁。

3. **资源分布和隔离：**云资源分散且相互隔离，就像大型仓库的分隔区域一样。适当的分布和隔离可确保一个区域的漏洞不会危及整个系统。也就是说，还需要一定程度的日志集中化，以提供对整个云资产的概览。

4. **云资源分散：**指在 CSC 的云环境中，各种工作负载类型的广泛扩散和多个 CSP 的采用。这种云资产分散在各种平台和服务上的现象使安全监控和管理变得复杂。管理云资源扩散需要全面的策略来解决监控和保护各种云资产的复杂性。

另一方面，云计算也为新的安全监控方法创造了机会。大多数 CSP 服务配置都可以通过简单的API进行审查，这为高级态势管理工具创造了机会，这些工具可以分析配置以获取见解。

6.1.1 日志和事件

日志和事件是安全监控、合规性、问责制以及更广泛的云安全和风险管理实践的基础。它们为云系统、网络和应用程序内发生的活动和行为提供了重要的洞察能力。每个 CSP 的日志和事件都不同。

日志提供相对完整的活动记录（即创建、读取、更新、删除），非常详细，并且通常会持久存储。但是，日志的质量可能因服务而异，并且其批量交付可能会延迟。日志被认为是持久的，通常会保存，有时也会流式传输。

另一方面，事件不同之处在于它们通常仅记录变更（即创建、更新、删除 (C-UD)）。特定条件通常会触发来自Amazon Web Services (AWS) GuardDuty、Microsoft Sentinel 和 Google Cloud Platform (GCP) Security Command Center 等服务的安全警报。与日志不同，事件是短暂的，这意味着除非明确保存，否则不会保留它们。事件可能缺乏日志提供的上下文详细信息，但它们通常速度很快，通常在记录活动后几秒钟内即可获得。

日志提供了调查所需的数据深度，而来自事件的警报提供了对快速响应措施至关重要的及时通知。

日志和事件在以下活动中发挥着重要作用：

- **持续监控和风险管理：**通过实时或近实时监控日志和事件，组织可以增强及时检测和应对安全事件的能力。

● **检测异常和威胁：**使用统计分析、机器学习算法或基于规则的系统评估日志和事件，以检测异常行为，例如异常访问模式、未经授权的配置变更或异常网络流量。异常活动并不是主动威胁的明确指标，而是潜在问题的早期预警。

● **事件响应和取证：**日志和事件提供了事件发生前后活动的详细轨迹，有助于确定根本原因、影响范围和补救措施。

● **合规性和审计要求：**许多监管框架要求收集和保留日志以供审计目的，以确保云安全实践的责任感和透明度。

● **性能和运营洞察：**虽然不是以安全为重点，但监控资源利用率、网络流量模式和应用程序性能指标等可以帮助优化云基础设施并提高整体运营效率。

6.1.2 告警和监控

在云端，更多的攻击可以自动化并快速执行，大大超过传统的检测方法，因为它的功能可以加速攻击的执行。此特性要求警报系统监控云管理平面（也称为控制台），以快速识别和应对威胁。此类系统的基础是维护全面的日志，例如 AWS CloudTrail、Azure Monitor 或 GCP Cloud Monitoring 提供的日志，这些日志可提供对云环境中的资源、用户、API和网络活动的全面可见性。

此外，了解经常针对云环境的各种攻击向量对于设计强大的安全监控策略至关重要。通过检查不同云服务模型（例如 IaaS 和 PaaS 环境）中的常见攻击媒介和利用技术，组织可以更好地理解他们面临的安全风险并相应地调整监控工作。

6.1.3 日志和警报的及时性

云安全的一个关键区别是接收和处理日志和事件数据以及生成相关警报的速度。警报的严重延迟是完全不可接受的，因为云攻击以更快的速度进行，需要同样迅速的响应。此外，由于失去对管理控制台的控制存在很高的风险，警报必须全面覆盖管理平面，以确保立即发现并处理可疑活动。

这需要深入研究日志管理策略，确保以优先及时准确地检测新出现的攻击的方式收集和分析日志。

6.1.4 监测关键指标

监测关键指标指应密切监控关键指标，例如异常的身份和访问管理(IAM)或网络安全活动，尤其是在未使用区域，因为它们通常可以预示网络攻击的初步阶段。MITRE ATT&CK®框架是一种资源，它可以提供哪些指标与哪些攻击策略相关的背景，从而使组织能够专注于与其环境最相关的攻击。

6.2 云遥测源

云遥测源可让组织了解云环境，跟踪从管理操作到单个服务交互和资源性能的所有内容。它们通过不断收集和共享详细信息，提供“看到”和“听到”云环境中正在发生的事情的能力。然后，安全工具、管理员或自动化流程会处理这些信息，以分析和了解 CSC 云环境的运行状况、性能和安全性。请参考下图了解云遥测源的概述，后面几节将详细介绍。

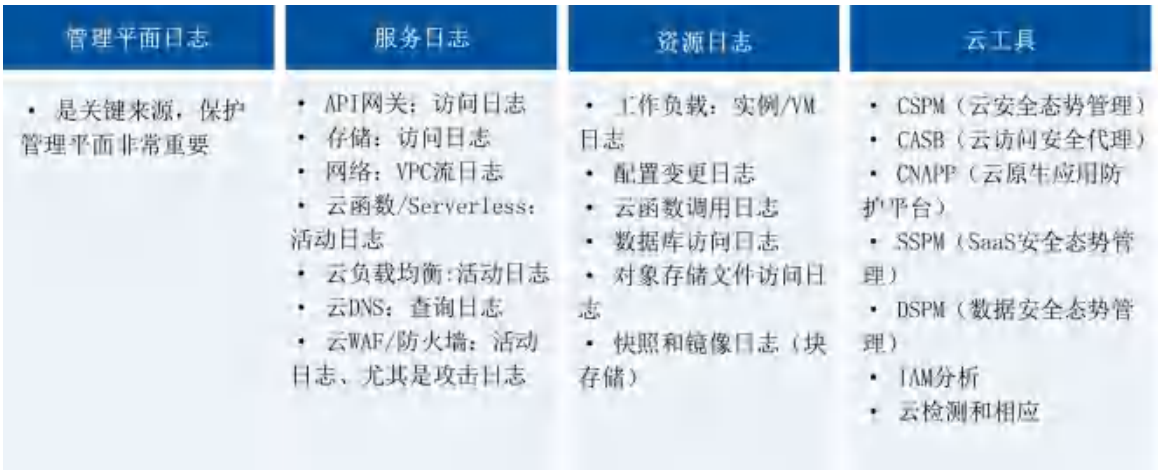


图 27：云遥测源

6.2.1 管理平面日志

管理平面日志类似于日志，详细记录了在云环境中执行的命令和控制。它们提供了有关如何管理云资源的重要见解。通过分析管理平面日志，组织可以了解谁访问了云基础架构、执行了哪些操作以及这些操作何时发生。这种可见性对于维护云环境中的治理、合规性和安全性非常重要。

6.2.2 服务和应用程序日志

服务和应用程序日志就像是单个服务和应用程序的日记，记录每一次交互，例如 API 访问和网络流量，这对于发现可疑活动和取证调查至关重要。这些日志捕获各种活动，包括用户身份验证尝试、网络流量、数据传输和特定于服务的事件。检查服务日志有助于 CSC 监控其云服务的运行状况、性能和安全性。

6.2.3 资源日志

资源日志是虚拟机(VM)、数据库和软件定义网络等资源的专用日志，用于记录每个操作和变更。这些包括资源配置、配置变更、数据访问和传输以及系统级活动等事件。通过分析资源日志，组织可以优化资源利用率、解决问题并检测影响单个云资源的未经授权或异常行为。

6.2.4 云原生工具

云工具是解释日志和自动响应的重要组成部分。它们在解释和利用云遥测源中包含的大量信息方面发挥着关键作用。常用的云工具包括云安全态势管理 (CSPM)、云检测和响应 (CDR)、SaaS 安全态势管理 (SSPM)、数据安全态势管理 (DSPM)、云工作负载保护平台 (CWPP) 和云原生应用保护平台 (CNAPP)。这些工具提供实时威胁检测、合规性监控、配置管理和事件响应自动化等功能。通过将云工具集成到安全运营中，组织可以有效地监控、分析和响应整个云环境中的安全事件。

下面描述了一组专门用于解决云安全和合规管理特定方面的云工具（例如 CSPM、CDR、SSPM、DSPM、CWPP、CNAPP）。

●**云安全态势管理 (CSPM)**是帮助组织持续监控、评估和改善其云基础设施安全状态的工具和实践。它们有助于识别云服务和资源中的错误配置、合规性错误和安全风险。CSPM 工具提供的功能包括持续监控、自动修复和合规性报告，使 CSC 能够加强其整体安全态势并遵守监管 要求。这就像加固堡垒的锁、警报和墙壁，同时确保所有防御都符合设定的标准。

●**云检测与响应 (CDR)**是用于检测和应对云环境中的安全威胁和事件的工具。它们利用高级分析、威胁情报和可能的机器学习算法来识别可疑活动、异常行为和入侵指标。CDR工具有助于快速检测、调查和响应事件，有助于减轻云中安全漏洞和未经授权的访问尝试的影响。

●**SaaS 安全态势管理 (SSPM)**是使组织能够管理和监控 SaaS 应用程序的工具，确保配置和授权正确。这些工具可集中查看多个 SaaS 应用程序的安全控制、配置和合规性状态。SSPM 工具有助于评估 SaaS 安全性的有效性、执行安全策略并确保符合合同义务和监管要求。

●**数据安全态势管理 (DSPM)**是保护敏感数据并确保遵守云环境中数据保护法规的工具。它们提供数据发现、分类、加密策略实施等功能，并确保适当的访问控制，以保护数据免受未经授权的访问、数据泄露和内部威胁。DSPM 工具有助于维护基于云的应用程序、数据库和存储库中的数据隐私、完整性和机密 性。云环境中的 DSPM 工具就像银行的风险管理官。它们确保敏感数据得到良好保护，并且所有处理此问题的方法都是数据符合严格的规定，就像银行保护其资产并遵守金融法规以防止盗窃和确保完整性一样。

●**云工作负载平台保护 (CWPP)**是为跨混合云架构部署的工作负载提供有针对性安全性的工具。这些工具可保护物理服务器、虚拟机、容器和云部署，无论位于何处（本地或公有云）。CWPP 利用持续监控来识别可疑活动和潜在威胁，确保关键工作负载的运行安全性和完整性。

●**云原生应用保护平台（CNAPP）**是专注于在整个云应用程序生命周期内保护云应用程序的工具，通过提供统一的平台来为整个云应用程序堆栈提供全面的安全保护。这些工具集成了 CSPM 和 CWPP 等功能，可全面了解您的应用程序安全状况。这可以实现主动威胁检测、漏洞管理和细粒度权限控制，以保护应用程序。此外，CNAPP 工具通常集成合规性自动化，从而简化对数据保护法规的遵守。

6.2.5 云原生 CSP 安全工具和容器监控

CSP 安全工具和容器监控是我们安全环境的扩展。这些工具发挥着独特但互补的作用。

CSP 提供的云原生安全工具，例如 AWS Security Hub、Azure Defender 或 GCP 安全指挥中心是嵌入在云平台中并集成到云平台中的专业安全服务，可提供内置安全情报。它们既可用作遥测源，又可用作聚合点，并分析数据以提供此类情报。这些工具是云遥测源的重要组成部分，可洞察各种活动，例如用户身份验证尝试、网络流量和特定于服务的事件。然而，由于每个 CSP 都有自己的工具集，因此存在局限性，这会使多云管理变得复杂。因此，收集的遥测数据量必须与分析和关联数据的能力相平衡，以确保可以对最关键的安全警报采取行动。

容器监控工具与 CSP 提供的安全工具和服务（例如 AWS Security Hub、Azure Defender 或 GCP Security Command Center）集成，以下列方式为云原生应用程序提供全面的安全覆盖：

●**数据聚合：**容器监控工具通常与 CSP 提供的安全工具集成，以汇总来自多个来源的数据，包括容器日志、性能指标和安全事件。通过这种集成，可以集中查看整个云环境中与安全相关的活动。

● **关联分析：**通过与 CSP 工具集成，容器监控工具可以将容器特定的数据与更广泛的安全遥测数据关联起来。这种关联能够实现更多通过识别可能表明存在安全漏洞或弱点的模式或异常，实现准确的威胁检测和事件响应。

●**自动修复：**一些容器监控工具可与 CSP 提供的自动化和编排服务集成，以自动执行补救措施来应对安全事件。例如，如果发现容器表现出可疑行为，监控工具可以触发自动操作来隔离容器、阻止网络访问或缩减资源以减轻事件的影响。

容器监控面临的关键挑战包括：

●**数据量：**这需要管理由多个主机上运行的大量容器生成的监控数据量。最佳实践包括实施数据聚合和过滤机制，以优先处理关键事件并减少噪音，以及利用可扩展的存储解决方案来容纳大量监控数据。

●**跨动态环境的可见性：**容器化环境具有高度动态性，容器会根据工作负载需求动态创建、部署和终止。最佳实践包括实施监控解决方案，自动发现和监控新创建的容器并跟踪容器生命周期事件，从而确保跨这些动态环境的可见性。

●**警报和事件响应：**这涉及有效的警报和事件响应，以便及时检测和缓解容器化环境中的安全威胁。最佳实践包括根据预定义阈值或异常检测算法设置警报，建立事件响应程序执行调查和补救安全事件，并定期进行桌面练习或模拟以测试事件响应准备情况。

下表概述了容器监控的主要特性、功能、用例和优势，包括 CWPP 和 CSPM 解决方案。

表 7：CWPP 与 CSPM 之间的概要比较

特性	容器监控工具	CWPP	CSPM
关注点	独立的容器和容器化应用程序	检测云工作负载的漏洞和配置错误，包括容器和无服务器运行时监控	检测云管理平面的云安全态势上的漏洞和错误配置

关键功能	- 监控资源利用率（CPU、内存、网络） - 跟踪健康和性能 - 识别崩溃和错误 - 基本安全功能（漏洞扫描） - 容器日志洞察	- 识别容器镜像和环境中的漏洞 - 配置错误 - 合规性检查 - 运行时异常	- 监控云安全态势 - 检测云服务中的错误配置 - 根据合规性控制测试配置
用例	- 解决容器问题 - 优化容器性能 - 维护应用程序健康	- 保护工作负载抵御漏洞 - 部署安全策略 - 确保检测和补救配置错误	- 主动识别并减轻安全风险 - 确保遵守法规
收益	- 实时了解容器健康状况和性能 - 快速识别和解决容器问题	- 实时洞察工作负载安全性 - 快速识别合规性和漏洞 - 容器化应用程序的高级安全	- 主动云安全管理 - 在被利用之前缓解安全风险 - 合规保证 - 全面了解云安全态势

6.2.6 云遥测限制

遥测系统在分散式网络中共享安全数据方面面临挑战，因为它们难以有效地监控和追踪分散式环境中的数据流。这些限制凸显了全面安全策略的重要性。

一个重大限制是无法捕获未通过传统方式记录的 API 调用，包括监控和收集本地和非云环境中的数据。CSP 经常更新和引入新的 API，其中一些可能没有充分记录或集成到现有的遥测系统中。因此，这些新的和/或未记录的 API 调用可能会被忽视，从而可能导致安全监控和威胁检测出现盲点。

此外，云环境产生的遥测数据量巨大，可能会让监控工具不堪重负，导致无法及时区分合法行为和可疑行为。这种延迟会影响对潜在安全威胁的及时检测和响应。

为了缓解遥测限制，CSC 必须用其他安全控制措施（例如基于主机的安全工具、威胁情报源和 SIEM 平台）来补充云遥测，以确保全面覆盖和有效的威胁检测和响应能力。采用多种先进的威胁检测技术对于有效应对基于云的威胁至关重要。这种方法解决了威胁的多样性和不断演变性，包括那些难以检测的威胁，如内部威胁或复杂的有针对性的攻击。

6.3 采集架构

云计算极大地改变了组织收集安全遥测数据的方式。云部署的分散性（跨越多个数据中心和云提供商）要求采用新的遥测收集方法。推动这些变化的关键因素包括：

1. **去中心化：**与传统的集中式数据中心不同，云部署通常分布在不同位置和提供商，因此需要跨 IaaS、PaaS和 SaaS 模型采用不同的遥测收集方法。

2. **新的遥测来源：**云环境引入了额外的遥测源，例如云管理平面、云事件（通常默认不记录）、云安全工具源和各种特定于服务的日志。

3. **速度变化：**不同日志源生成数据的速度不同，再加上近乎实时的威胁检测和响应的需求，使日志管理变得复杂。

4. **日志存储和分析选项：**组织可以从各种日志存储和分析解决方案（包括安全数据湖）中进行选择，以有效地管理其遥测。

没有单一正确的收集架构；每个提供商和技术堆栈都有独特的要求。本节重点介绍核心原则、各种收集选项以及有效管理云环境中安全遥测的主要架构方法。

6.3.1 日志存储与保留

云计算引入了存储大量数据的新功能，而CSP通常会先将日志保存到自己的存储服务中。云客户需要为这种存储付费，但在将数据导出到其他位置（例如本地 SIEM）时还需要支付数据传输费用。

有效且高效的日志收集架构将考虑移动日志的成本和复杂性。最具成本效益的选择可能是将日志留在CSP的存储服务中，但这可能会给检测、分析和其他活动带来问题。然后，组织可能只能使用与其他安全监控工作不兼容或不满足性能要求的CSP分析工具。将日志移回本地可能会导致数据传输和物理存储要求方面的成本更高。第三方SIEM/分析工具是另一种选择。安全数据湖也是可能的，它是大型存储池，可以接受来自各种来源和格式的日志。

日志保留考虑因素在确保有效监控、故障排除、遵守法规和系统成本方面也发挥着重要作用。确定适当的日志保留期涉及平衡运营需求、监管要求和成本考虑因素。保留足够长的日志时间允许CSC分析历史数据以识别趋势、检测安全事件和排除系统故障。此外，请记住需要将一些日志

事件移动到云外存储以实现弹性和监管目的。但是，延长保留期可能会导致存储成本增加，并可能影响隐私。因此，CSC 必须制定明确的策略，定义要保留哪些日志、保留多长时间以及保留何种级别的访问控制。

以下因素通常会指导您决定在何处存储日志：

- CSP 的默认存储位置
- 默认存储成本
- 与分析工具（CSP 或第三方，例如 SIEM、SOAR）集成 [90] 或 SIEM 即服务）
- 移动日志的数据传输成本
- 移动日志时的目标存储成本
- 能够实施有效的访问控制，这可能需要向云团队提供对其日志的访问权限，但不提供对其他部署日志的访问权限，以满足运营要求。

6.3.2 级联日志架构

级联日志架构是一种分层的日志管理方法。通过这种方法，日志以级联方式收集、汇总和分析，从一层流向另一层，以方便集中监控和分析。级联日志架构本质上并不特定于混合或多云环境，可以在任何需要汇总和分析来自不同基础设施层的多个来源的日志的环境中实施。然而，由于这些架构的分布式特性，以及可能需要从各种本地和基于云的资源收集日志，级联日志在混合或多云环境中可能特别有益。

下图展示了在云环境中管理日志时出于安全目的的合理架构。开发(Dev)、测试(Test) 和生产(Prod)环境各自生成日志，这些日志被发送到与特定项目关联的多个帐户的集中日志管理系统。

图 28：级联日志架构

每个环境（开发、测试、生产）都可以配置为将日志转发到中央存储库。中央日志系统会汇总这些日志，并将与安全相关的日志发送到单个安全/审计环境中，确保它们得到安全保存和整合，这对于有效的安全分析和合规性至关重要。

最后，汇总的日志可以输入数据中心或云 SIEM 系统。SIEM 系统会分析这些日志以识别潜在的安全事件。此架构提供了所有云环境中与安全相关的事件的视图，有助于及时检测和应对威胁。

6.3.3 云安全监控策略指导

在制定监控策略时，要明白将日志整合到一个位置并不总是最佳选择，尤其是在多云环境中。相反，建议采用级联和过滤方法，如上一节所示。

这意味着：

● 构建不同的日志记录和警报路径，考虑到日志生成的速度和源对检测工作的重要性。

● 将所有相关警报和选定的日志转发到安全运营中心(SOC)，同时将大多数原始日志保留在其本地化帐户中，以实现成本效益和资源优化。

● 将利用率较低的日志移动到成本较低的存储环境可以将日志存档以供后人使用，而不会给日志系统增加不必要的规模。

SOC应该首先关注警报，然后深入研究选定的日志以验证事件、对其做出响应并主动搜寻威

胁。

商业工具的选择会影响这种架构的可行性；因此，找到日志数据接近度与分析深度之间的平衡至关重要。这种细致入微的策略有助于有效监控和快速响应事件，这对于维护强大的云安全至关重要。

6.3.3.1 日志处理速度

理解监控的另一个关键概念是区分不同云服务中的日志处理速度。监控和分析通常分为两个独立的轨道：慢速路径和快速路径。慢速路径专门用于日志，可能需要长达15分钟的延迟才能进行分析。快速路径通常用于事件， 但也可以设计用于某些日志，可以近乎实时地分析并生成警报。

这里通过AWS安全工具示例进行了说明：

- “慢速路径”日志，例如来自 CloudTrail 的日志或资源日志（例如，S3 访问日志、ALB日志）通常很详细并用于深入调查，但可能无法立即进行分析。
- 另一方面，CloudWatch 等服务提供的“快速路径”事件旨在快速检测和响应。它们可针对潜在的、影响重大的问题触发快速警报。
- 重要的是要理解这些解决方案并不是互相排斥的并且提供不同的功能，应该串联使用以实现全面的安全监控。
- 快速路径日志对于即时安全事件响应至关重要，而慢速路径日志对于彻底的事后分析和取证很有价值。GuardDuty 等服务、Access Analyzer 和 Security Hub 提供威胁情报和监控，而 Detective 和 Athena 等工具协助分析和应对安全事件。

关键是利用这两种途径来确保及时响应威胁并详细调查安全事件。

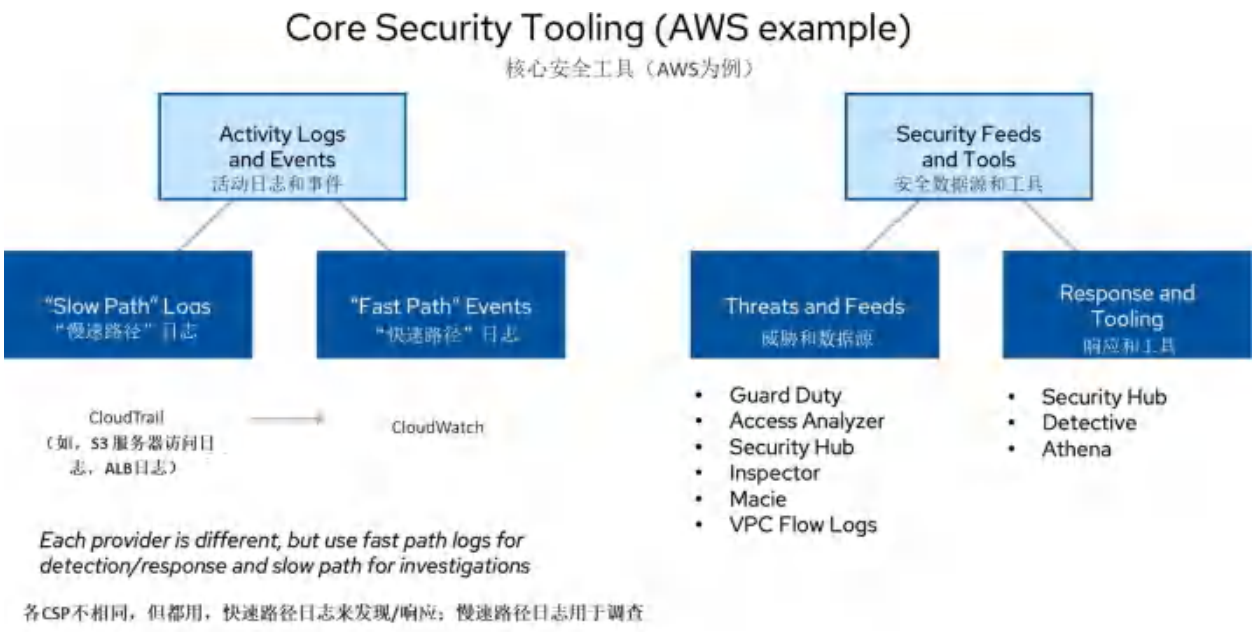


图 29：各种云服务中的日志处理速度，使用AWS 安全工具进行说明

6.3.4 安全数据湖

安全数据湖描述了一个集中式存储库，旨在处理和分析从各种云环境和工具收集的大量相关类型的安全数据。此数据架构应提供可扩展性以管理大量数据，包括结构化和非结构化形式。其灵活性应支持高级分析，使机器学习和人工智能能够从安全数据中提取见解并有效识别威胁。集中和整合安全数据的目的是改进事件检测、分析和响应，并增强整体安全态势。

安全数据湖提供：

- 改进事件响应和取证分析
- 访问全面的历史数据集以进行响应和威胁检测

6.4 检测与安全分析

日志、事件和配置检测路径对于检测和响应各种安全问题的全面监控系统至关重要。

如前所述，日志由于其数量和复杂性而成为慢速路径，需要更多分析时间。但是，它们很全面，可以支持基于随时间变化的模式（例如来自不同 IP 的重复登录尝试）的警报。日志通常使用第三方或内部开发的工具进行分析。

事件代表快速路径，可提供近乎实时的警报。它们可能包含类似于日志的数据，但重点关注C-UD操作在云中。事件通常由CSP安全工具（如AWS GuardDuty、Azure Defender或GCP Security Command Center）生成。虽然很难捕获，但它们确实提供了高价值数据。

配置检测涉及识别云部署中的易受攻击的设置，这些设置可以在日志、事件或 CSPM工具中发现。正确配置后，这些对于识别错误配置和恶意活动至关重要。基础设施即代码 (IaC) 也可以成为配置信息的重要来源，可以在部署前扫描其漏洞。

图 30：云安全中的关键检测路径：日志、事件和配置

6.4.1 比较不同的检测工具

下表是一些云安全监控中使用的流行工具的比较示例，并非以下工具功能的详尽列表。

表 8：云安全监控工具比较

特征	SIEM（安全信息与事件管理）	CSP 警报	CSPM（云安全态势管理）
关注点	● 整体 IT 基础设施	● 特定云问题。	● 连续云监控

数据源	● 来自各种安全来源的日志和事件（例如网络设备、应用程序、云平台	● CSPM 工具生成的警报。 ● 提出一些挑战，因为他们需要动环境特定过滤。 ● 难以汇总，因为警报特定于云且格式和细节差异很大。	● 云资源， 配置，以及活 ● 需要大量调优以确保有效性和准确性
功能	● 汇总、分析和关联安全数据 ● 通常路径较慢，但对于大多数基于日志的分析来说，这是最佳选择	● 提供云端潜在安全问题的通知 ● 需要了解来源/时间（ 告警可能仅当执行特定规则时才产生，例如，规则每 24小时运行一次）	● 监控配置错误， 漏洞，以及合规风险 ● 一些工作与 SIEM 并行补充检测和分析功能

6.4.2 安全监控与分析实践

安全分析中用于检测和应对威胁的一种常见方法是级联和过滤模式，如下所示。它涉及对传入数据流或日志依次应用多种检测机制或过滤器。级联中的每个后续过滤器都会细化和优先处理数据，重点关注特定标准或潜在威胁指标。初始数据流包含各种日志条目或网络流量数据。以下是一个例子：

●级联中的第一个过滤器可能关注可疑活动的高级指标，例如异常登录尝试或异常网络行为。

●后续过滤器逐渐缩小分析范围，重点关注与已知攻击媒介或威胁行为者相关的特定属性或模式。

●如果最终检测到安全威胁，级联中的最后一个过滤器可能会触发警报或响应操作。

●最后，重要的是利用先进的分析技术，例如机器学习和行为分析，来增强级联内检测机制的有效性。

以下是级联过滤模式的示例：

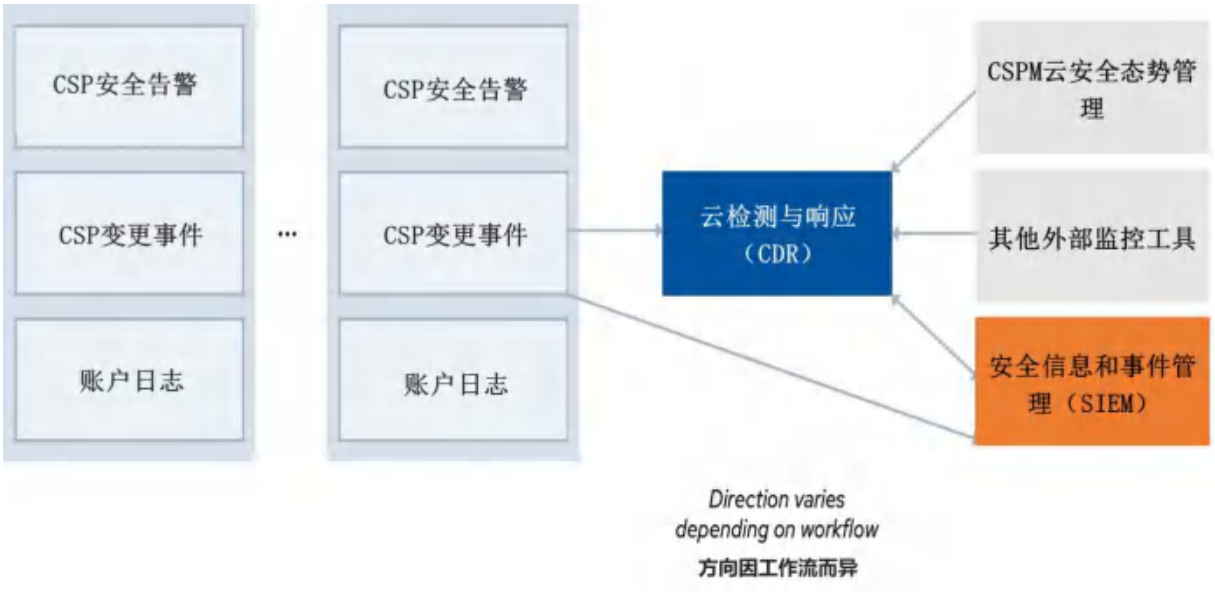


图 31：级联过滤模式示例

在此示例中，从多个帐户收集 CSP 安全警报、变更事件和账户日志。然后对它们进行过滤并发送到适当的工具以采取进一步行动。CDR 路径旨在对已识别的威胁做出即时、自动的响应。CSPM 专注于评估和改善安全态势，通常处理合规性和配置管理。SIEM 系统是一个综合分析平台，可集成来自各种来源的数据以进行深入检查。

关键是要有一个组织良好的检测和响应策略，利用多种工具和途径来确保云环境的安全。了解如何适当地过滤和引导安全信息对于有效的云安全操作至关重要。

6.4.3 云检测与响应

尽管日志聚合是监控的初步步骤，但CDR（云检测与响应）过程通过规则和事件处理实现了更为有效的功能。CDR超越了简单的日志聚合，整合了多项功能，其主要特点包括：

- 过滤数据以消除噪声，并根据已定义的模式检测潜在的威胁。
- 根据上下文丰富日志信息，以帮助进行分析。
- 会通知必要的人员或系统。
- 可能包含安全编排、自动化和响应（SOAR）功能，提供自动响应和调查支持。

在CDR中，云事件被近实时地管理，确保能够及时响应威胁。然而，CDR与SIEM（安全信息

与事件管理）系统的集成可能会有所不同，具体取决于所采用的工具和配置。

6.4.3.1 云检测与响应最佳实践

在思考云攻击检测的最佳实践时，请记住，入侵指标 (IoC)，即使对于虚拟工作负载，其运行方式也与传统工作类似。因此许多相同的检测技术也适用。

应优先考虑最能表明安全问题的特定数据源，例如：

- 来自管理平面的日志。
- IAM 活动。
- 面向公众的资源的变化。
- 结构网络修改。
- 跨账户访问或双向订阅。
- 生产配置改变。

为提升云检测能力，可利用外部威胁情报和先进技术，通过以下两种方式进行安全威胁的早期发现：

- 将威胁情报源集成到云检测系统中。这样，组织就可以随时了解新出现的威胁、攻击媒介和攻击指标 (IoC)。集成威胁情报可以利用外部专业知识和知识来识别和减轻安全风险。
- 利用机器学习算法和高级分析来检测表明存在潜在安全威胁的异常活动。机器学习算法和高级分析可以分析大量数据并识别云环境中的异常活动，从而检测可能预示安全威胁或漏洞的模式和行为。

由于开发（或非生产）环境具有原型（测试）性质，因此监控这些环境可能具有挑战性，因为数据量巨大且可能存在噪音。需要强大的过滤功能来管理噪音。此外，建议使用“我故意这样做”按钮或类似机制来区分有意变更和可能 恶意的变更，通过在云中标记合法活动来充当过滤器，这样就不会浪费时间验证授权变更。

6.4.3.2 检测器示例（CIS 基准）

以下是应监控的云环境中特定活动和变化的列表，以检测潜在的安全威胁。这些指标基于互

联网安全中心(CIS)基准，以及保护IT系统和数据免受攻击的各种最佳实践。

访问管理：

- 未经授权的 API 调用
- 无需 MFA 即可登录管理控制台
- 禁用或安排删除客户管理的密钥
- 任何 IAM 策略变更
- 任何使用root 账户的情况

资源管理：

- 云存储策略变更
- 配置监控变更
- 安全组变更
- 网络访问控制列表 (ACL) 变更
- 网络网关变更
- VPC 变更（例如子网、路由表、服务端点）

日志记录和监控：

- 记录服务配置变更
- 管理控制台身份验证失败

6.4.4 高级监控：金丝雀和蜜罐

虽然在检测攻击方面永远不可能真正做到主动，但有一些方法可以大大缩短攻击与检测之间的时间。这些方法包括“金丝雀”和“蜜罐令牌”，它们是旨在模仿真实资源的诱饵凭证或数据。

金丝雀和蜜罐令牌用于监控未经授权的访问。当攻击者与这些诱饵互动时，会触发警报，表明有人试图或实际入侵。例如，金丝雀可以放置在凭证存储中，以显示为合法的用户数据。蜜罐令牌可以部署在可能吸引攻击者的各种位置，例如数据库或文档。

6.5 生成式 AI 安全监控

生成式人工智能 (GenAI) 具有巨大潜力，可以大幅提高SOC 的效率和有效性，例如自动化日志数据分析、扩展处理数据以及提高恶意活动识别的准确性。

此外，GenAI 还有助于创建模拟攻击场景，这是一种强大的漏洞测试形式。它通过适应观察到的网络行为模式来提高警报的相关性和准确性，并通过广泛的上下文来增强日志数据。这有助于分析师（尤其是经验不足的分析师）了解复杂的安全事件以及攻击可能采取的途径。

此外，GenAI 还提供工作流程建议，为验证和响应警报提供指导，这对于保持有效的安全态势至关重要。这种人工智能驱动的方法越来越多地被云安全工具所利用，并成为云安全基础设施不可或缺的一部分，使团队能够更好地预测、识别和应对威胁。

以下列出了GenAI可能影响的一些事项：

- 通过预测分析模型增强实时威胁检测
- 自动化和扩展日志分析，发现潜在的恶意活动，并提高效率和准确性
- 生成模拟攻击以进行强大的漏洞测试
- 根据学习到的网络行为模式不断改进警报，从而减少警报疲劳
- 丰富日志并为各种安全日志/事件添加广泛的背景信息
- 协助初级分析师理解攻击路径
- 提供工作流程建议，指导分析师验证和响应警报
- 生成模拟真实场景的合成数据，用于测试和训练，这对于在不暴露敏感信息的情况下测试安全模型很有价值

基于GenAI的安全解决方案展现出了安全行业前所未有的创新速度。预计将持续快速创新和能力，以改变SOC的工作方式。

6.5.1 生成式 AI 的挑战与考虑

虽然GenAI在增强云攻击的检测和解决方面前景广阔，但我们必须认识到它带来的潜在挑战和道德困境。需要持续的数据和训练才能保持AI模型的相关性和有效性。然而，这种对大型数据集的必要性可能会引发隐私和数据保护问题，尤其是当大型语言模型 (LLM) 将训练数据纳入其响

应时。

此外，人工智能能力的快速发展需要可扩展的安全解决方案。区分合法活动和人工智能产生的活动也是一个日益严峻的挑战，这可能会误导安全监控工作并在系统中产生更多噪音。

最紧迫的问题之一是对抗性人工智能，这是一种旨在逃避或欺骗安全机制的复杂人工智能系统。同样重要的是人工智能参与人类监视和监控活动的道德考量，这需要符合隐私标准和法规。

采用AI等突破性新技术时，必须采取平衡且深思熟虑的方法。然而，AI融入安全运营似乎是不可避免的，需要从业人员适应以保持稳健且合乎道德的安全实践。

要了解有关GenAI的更多信息，请参阅云安全联盟培训“生成式人工智能与快速工程简介”以及云安全联盟人工智能安全倡议工作组正在开展的工作。

总结

此领域解决独特的云安全监控挑战，重点关注云遥测、管理平面日志、服务/资源日志和高级工具。它涵盖混合/多云复杂性、日志/事件的关键作用以及生成人工智能 (GenAI) 的创新使用。

遥测技术可以查看云环境、跟踪操作和资源性能。但是，遥测技术也面临着 API 调用记录和数据量管理盲点等挑战。有效的策略包括用其他安全控制措施补充遥测技术，以及使用先进的威胁检测技术。

建议采用级联和过滤方法进行日志管理，平衡成本和资源效率。重点是将相关警报转发给SOC，并以经济高效的方式归档较少使用的日志。区分日志处理速度，以便及时响应威胁（快速路径）和深入分析（慢速路径）。

用于处理和分析大量安全数据的集中存储库，支持高级分析以增强事件检测和响应。日志（慢速路径）和事件（快速路径）对于全面监控至关重要。金丝雀和蜜罐等高级监控方法可缩短检测时间。要监控的关键活动包括未经授权的 API 调用、IAM 策略变更和网络配置变更。

GenAI通过自动日志分析、生成模拟攻击、提高警报精度和协助分析师来增强安全性。挑战包括维护隐私、管理数据和处理对抗性AI风险。

建议

监控和警报是云安全的基础组成部分。重要的是：

● 重点关注因自动云攻击而导致的快速检测。

● 监控管理平面。

● 利用日志管理和警报计时策略的组合（例如，利用慢路径日志进行响应和取证，并利用快速路径事件警报来检测高风险活动，包括管理平面）。

● 监控遥测和云工具利用率（例如管理平面日志、服务日志以及 CSPM、CASB 和 CNAPP 的应用），以增强安全监控。

● 战略性地收集和分析日志（例如，考虑部署级联日志架构和选择性警报来管理成本并提高多云环境中的 SOC 效率）。

● 部署金丝雀和蜜罐令牌来提供没有误报的确定性警报，而生成式人工智能则提供了提高威胁检测和响应效率的潜在途径。

补充指南

- 了解云攻击向量 | CSA
- 人工智能安全计划 | CSA
- MITRE ATT&CK 云矩阵

领域 7：云基础设施与网络安全

此领域涵盖管理整体基础设施占用空间和网络安全。它还包括一小部分关于云服务提供商 (CSP) 基础设施安全责任的内容。基础设施即服务 (IaaS) 中的基础设施是指位于云中的计算、网络和存储资源池。

在先前版本的 CSA 安全指南和云安全知识证书 (CCSK) 培训中，我们深入讨论了用于构建和托管公有云或私有云服务的基础设施。由于底层技术的广泛发展，这些内容超出了本培训的范围，本培训面向为云客户(CSC) 而非 CSP 工作的安全专业人员。其他领域涵盖计算（工作负载）和存储（数据）安全问题。

虽然大部分基础设施安全都包含在工作负载、数据和网络部分中，但有一些更高级别的功能涵盖了整个云基础设施选项。这些包括：

- 核心安全技术，如左移、护栏和监控。
- 安全架构，包括完善的架构框架。
- 基础设施即代码（IaC）。
- 不同的云迁移策略（例如，提升和转移）。

此领域专注于网络安全。它从软件定义网络 (SDN) 的概念开始，该概念在每个 IaaS 平台中都有使用。深入研究安全组及其他内容，以及容器网络。然后介绍不同的连接选项，例如连接到 CSC 的数据中心（混合）和工作负载。该领域最后讨论了零信任架构 (ZTA) 和 SASE。SASE 框架正在迅速成为实施云网络的主导模型，并在很大程度上收到安全要求的驱动。

学习目标

在此领域，您将学习：

- 了解保护云基础设施所使用的领域和技术。

- 了解云网络基础知识。
- 管理容器网络。
- 管理云网络安全并设计安全架构。
- 应用零信任技术来保护云基础设施和网络。
- 用于管理安全访问服务边缘 (SASE) 安全性的技术。

7.1 云基础设施安全

云基础设施是指支持通过互联网交付云计算服务和资源所需的硬件、固件和软件组件，例如服务器、存储、网络和虚拟化工具。它使组织能够以可扩展、灵活且经济高效的方式构建、部署和管理应用程序和数据。CSC 应根据 CSP 提供的安全服务来设计和构建其架构。由于 IaaS 和平台即服务 (PaaS) 设计很大程度上依赖于 CSC，因此了解基础设施的正确使用以及如何构建有助于实现云优势的良好架构的实现非常重要。

7.1.1 安全架构：良好架构的支柱

云提供商以略有不同的方式支持的一种架构师方法是遵循良好架构框架的原则。遵循这些支柱，可以指导设计和实施决策，以改善客户用云的效果（例如安全性和成本）。

图 32：良好架构的关键支柱

良好架构有六大支柱：

支柱一：安全

- 保护信息、系统和资产，同时实现商业价值
- 在所有架构层上应用安全性
- 自动执行安全最佳实践、实现可追溯性和管理访问控制

支柱二：卓越运营

- 专注于运行和监控系统以实现商业价值
- 不断改进流程和程序
- 自动执行变更、事件响应并制定管理日常运营的标准

支柱三：可靠性

- 确保工作负载正确且一致地执行其预期功能
- 快速恢复以满足业务和客户需求
- 测试恢复程序，横向扩展以提高可用性，并自动从故障中恢复

支柱四：性能效率

- 高效利用计算资源满足系统要求
- 随着需求变化和技术发展保持效率
- 提高试验频率，使用无服务器架构，并设计实现数分钟内全球化部署的系统

支柱 5：成本优化

- 在最低成本运行系统以实现商业价值
- 使用成本效益高的资源，匹配供需，增强支出意识
- 通过测量、监控和提高资源利用率进行持续优化

支柱六：可持续性

- 最大限度地减少运行云工作负载对环境的影响
- 了解影响并最大限度地利用资源，以最大限度地减少所需资源，并减少对下游的影响

这些支柱有助于开发一种一致的方法来评估架构并实施可扩展、安全且高效的设计。这使 CSC 能够专注于通过其应用程序和服务实现业务价值。

7.1.2 基础设施安全技术

在创建和维护安全基础设施时，需要重点考虑以下四种基础技术。

- **安全架构：**首先要以安全性为主要原则来设计云基础设施。它包括正确隔离资源和网络、实施最小特权访问以及确保存储、通信和服务的配置安全。应建立安全区域和基线配置，以确保所有环境中的安全一致性。IaC 工具可以自动部署安全架构并降低手动配置错误的风险。

- **安全部署和配置：**这涉及配置和/或部署资源和服务，以及加固所有云基础设施组件，包括虚拟机(VM)、容器、存储和网络。它包括应用安全基准和最佳实践，例如互联网安全中心 (CIS) 基准测试，[104] 确保云资产的正确配置。

- **安全左移：**这意味着在开发生命周期的早期嵌入安全控制和测试，而不是事后再考虑。它包括实施代码分析工具、自动化安全测试和持续集成/持续部署 (CI/CD) 流水线安检门。开发人员应接受安全 IaC 编码实践培训，并为其提供工具和框架以在应用程序中构建安全性。

● **持续监控和护栏：**这些措施用于维护安全。它们涉及使用自动化系统来监视云环境并执行策略。它包括使用云安全态势管理 (CSPM) 或云原生应用程序保护平台 (CNAPP) 工具进行日志记录、监视和持续评估，以及实施 AWS Config 规则、服务控制策略或 Azure 策略来执行策略并防止偏离既定标准。定期的安全审核和渗透测试可验证这些措施的有效性。

7.1.3 CSP 基础设施安全责任

基础设施安全始于CSP，这确保了CSC可以在此基础上构建一个安全的平台。在安全责任共担 (SSRM)下，基础设施安全主要是 CSP的责任。CSP基础设施安全责任包括以下内容：

● **设施：**CSP 负责确保云基础设施所在设施的物理安全。这包括访问控制、监控和环境保护等。

● **雇员：**CSP 筛选、培训和管理有权访问云基础设施的员工，帮助维护组织的完整性和可信度。

● **物理网络、存储和计算：**CSP 负责保护并维护云基础设施的底层物理组件，例如服务器、存储设备和网络设备。

● **虚拟化层：**CSP 有责任保护能够在物理基础设施上运行的创建和隔离的虚拟及和容器的虚拟化技术的安全。

● **管理平面：**CSP 保护并控制客户用来管理其云资源和服务的基于 Web 的界面和 API 端点的访问。

PaaS和SaaS服务：CSP提供更高级别的平台和软件服务，控制基于SSRM底层基础设施和应用安全。总之，CSP保护构成云基础设施的物理设施、硬件、虚拟化层和管理接口。CSC专注于保护他们在该基础设施上使用和部署的内容。下图概述了云服务模型（IaaS、PaaS和SaaS）的分层组件，突出显示了提供云服务的各种元素及其集成以提供云服务。

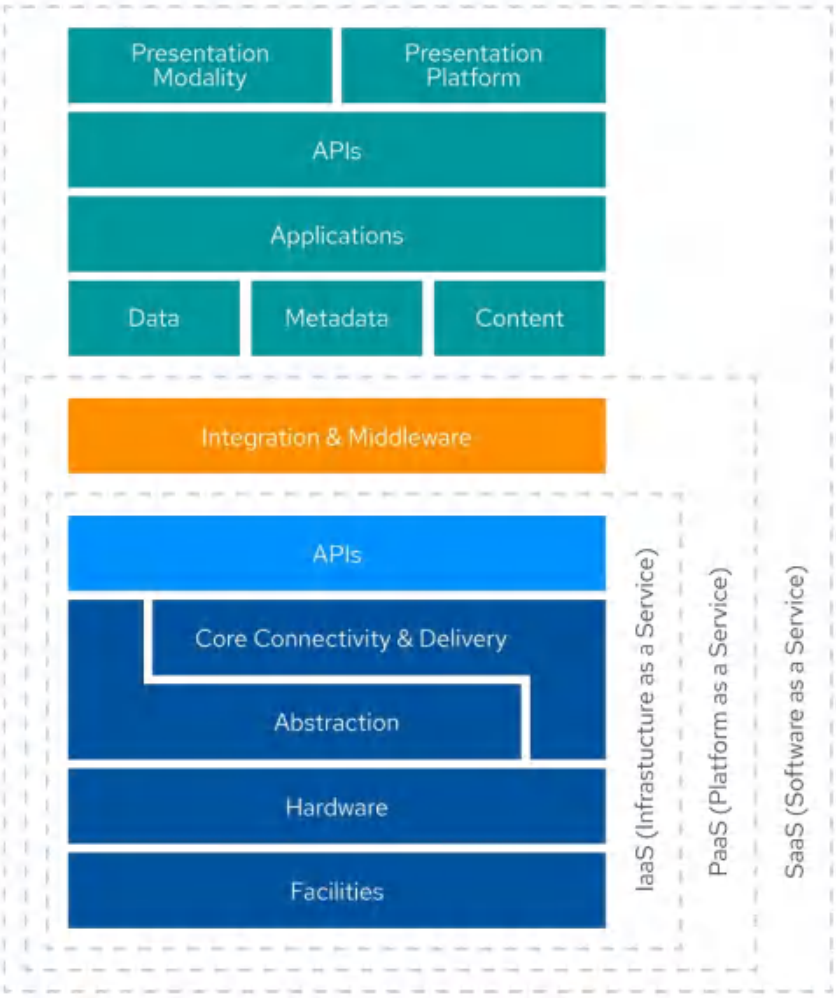


图 33：云服务模型的分层组件：IaaS、PaaS 和 SaaS

7.1.4 基础设施即代码

IaC 在 NIST SP 800-172 中定义为“使用机器可读的配置文件来管理和配置组织 IT 基础设施的过程，而不是采用物理硬件配置或交互式配置工具。”IaC 是部署云资源的主要模型，每个主要提供商都支持该模型。关键的 IaC 概念包括以机器可读的格式定义架构，从底层网络设计到高层应用程序组件，并且通常使用自动化 CI/CD 流水线部署它们。错误配置扫描可以集成到流水线中，并进行完整的版本和控制变更跟踪，确保一致且安全的部署。这种做法称为“左移基础设施安全”，可在开发过程的早期嵌入安全性。本培训的多个领域讨论了IaC，包括应用程序和工作负载安全部分。

IaC提供以下列出的几项安全优势。

1. 一致性和标准化：

●IaC 允许在所有环境中一致地定义和实施安全配置。

●安全最佳实践（例如最小特权访问）可以编入IaC 模板中。

●可以降低错误配置的风险并确保标准化的安全态势。

2. 版本控制和可审计性：

●基础设施代码文件可以存储在版本控制系统中，提供基础设施变更的完整历史记录。

●可以跟踪、审查和审计变更，从而提高可见性和可问责性。

●可以促进基础设施代码的协作和同行评审，以识别和解决安全问题。

3. 自动化安全测试：

●安全扫描和测试可以集成到部署流水线中。

●自动化工具可以在部署之前验证基础设施代码的安全性。

●可以在开发过程早期发现安全问题，降低生产中出现漏洞的风险。

4. 快速、安全的部署：

●IaC 支持基础设施的快速、可重复部署，从而减少所需的时间和精力。

●安全控制可以在部署期间自动应用，确保一致的保护。

●可以通过快速重新部署安全基础设施来实现对安全事件的快速响应。

5. 可扩展性和灵活性：

●IaC 支持根据需求动态扩展和配置资源。

●安全策略和控制可以在新资源创建时自动应用。

●能够在高度动态和分布式的云环境中维护安全性。

通过利用 IaC，CSC 可以将安全性嵌入到其云基础架构的基础中。它提供了一种大规模定义、部署和管理安全和合规基础架构的方法。IaC 有助于将安全性左移、尽早发现问题并确保在整个开发生命周期中始终保持安全的环境。

7.1.5 云迁移架构和安全影响

虽然有些云部署是全新的，但在 IaaS 中，许多部署都是从数据中心甚至其他提供商迁移而来的。在两种完全不同类型的基础设施之间迁移时，迁移不一定是一个简单的过程，因为这两种基础设施具有不同的可用安全功能。有不同的迁移模型，每种模型都有自己的安全性和成本权衡。以下指导注意事项和方法适用于云迁移计划的安全性和架构。

明确的需求定义和对当前安全态势进行全面评估可以指导迁移方法和实施。组织可能需要结合使用多种方法进行云迁移。所采用的不同策略取决于每个应用程序的特定需求和风险。通常，组织可以重新架构/重建、重构或重新托管现有应用程序。

图 34：云迁移策略：重新托管、重构、重新架构

7.1.5.1 重构架构

当应用程序被完全重新架构或从头开始重建为云原生时，这是最耗时和资源密集的方法，可以最大限度地发挥云的优势。这种方法允许 安全设计，在整个开发过程中融入安全控制和实践。通过重建应用程序，它可以充分利用云原生安全功能和自动化。然而，这需要对安全流程、工具和员工技能进行重大改变。确保重建应用程序的安全设计、配置和测试极其重要。

7.1.5.2 重构

当应用程序经过修改和优化以尽可能多地利用云原生服务和功能时，它比重新托管更耗时，但可以提高性能、可扩展性和弹性。它需要更新重构应用程序的安全策略、程序和员工技能。

这种方法提供了将安全最佳实践和控制集成到重构应用程序中并利用IAM、加密和日志记录等 CSP 安全服务的机会。但是，如果架构和配置不当，可能会引入新的风险。

7.1.5.3 重新托管

当应用程序在保留现有架构的情况下以最小的变更迁移到云端时，这是最快的迁移方法，但对云的利用程度最低。在安全考虑方面，由于架构差异，现有的安全控制和问题可能无法有效地转移到云中。此外，现有的安全控制可能无法充分利用云原生安全功能和自动化。这种方法需要调整安全流程和工具以进行云监控和事件响应。

7.2 云网络基础知识

云网络是 SDN。在客户租户环境之间实施强有力隔离是关键。SDN 已成为一项关键技术，彻底改变了网络设计、管理和运营。SDN 将网络控制平面与数据平面分离，允许通过软件的编程方式配置和控制网络。控制平面管理路由、网络/子网定义等，而数据平面在资源和网络之间移动网络流量。从传统的基于硬件的网络向软件定义方法的转变为云环境带来了众多好处。

下图演示了 SDN 环境中的网络控制逻辑，说明了数据包在通过网络控制逻辑在物理主机之间传输时进行封装和解包的过程。

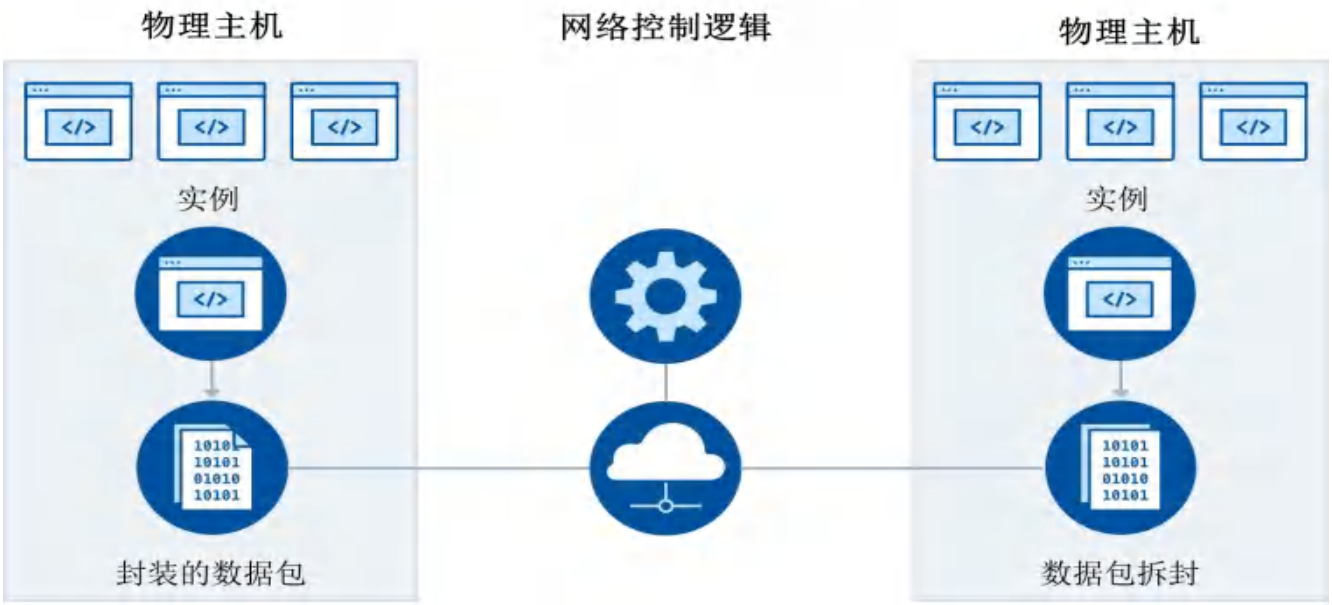


图 35：网络控制逻辑

SDN 的主要优势之一是其增强的灵活性和敏捷性。借助 SDN，网络管理员可以通过软件动态配置和管理网络资源，从而快速配置和修改网络服务。这种灵活性使 CSP 能够快速响应不断变化的 CSC 要求、按需扩展网络资源并根据实时流量模式优化网络性能。SDN 还促进了网络虚拟化的实施，允许在共享物理基础设施之上创建多个逻辑网络。这可以更好地利用网络资源、改进网络分段并更轻松地管理多租户环境。SDN 可以在任何网络上使用，但它是所有 IaaS 平台上的默认设置。

SDN 简化了网络运营和管理。通过集中的网络控制提供统一的网络视图，SDN 降低了管理大型云网络的复杂性。网络管理员可以使用 SDN 控制器和 API 来自动执行网络配置任务、监控网络性能并更高效地解决问题。SDN 还支持将网络服务与云编排平台集成，从而实现网络资源与计算和存储资源的无缝配置和管理。这种集成简化了云应用程序的部署和操作，提高了整体效率并降低了运营成本。

7.2.1 SDN 的安全优势

各大云计算平台所采用的 SDN 虽然各有不同，但都倾向于支持一组核心的强大的安全优势。

- 网络要么默认拒绝，要么可以快速配置为拒绝。这意味着网络结构不会传输数据包，除非有明确的路由和特定的目的地，并且端口/协议得到安全组的批准。（安全组是网络中允许或丢弃流量的规则。）这减少或消除了端口扫描或嗅探等常见的网络攻击技术。
- 基于策略的管理意味着网络通过配置策略进行管理，而不是通过配置不同的技术。这提高了一致性和控制力。
- 细粒度分段比物理网络更容易实现，因为它在 SDN 控制平面中进行管理，不需要物理配置。它非常灵活且功能强大，可以轻松部署特定应用程序所需的网络组件（例如子网）。

安全组（在某些情况下还有其他安全功能）内置于网络结构中。无需防火墙来维护它们。

7.2.2 最小可行网络

SDN 功能支持称为最小可行网络 (MVN) 的概念。在 MVN 中，仅部署最低限度连接所需的网络组件，并且架构中的每一层仅允许应用程序所需的绝对最小路由、端口和协议。这是可执行的每个资源都具有这种能力，并且是网络设计所固有的，从而可以实现并支持微隔离。因此，互联网只能通过 HTTPS 端口 (443) 与负载均衡器通信。Web 服务器将只接受来自指定负载均衡器的连接，并且只接受端口 443 上的连接。应用程序服务器将只允许来自 Web 服务器的预期端口上的入站连接。数据库服务

器只接受认可的应用程序服务器端口的连接。所有这些都是在网络结构中本地强制执行的，无需任何额外的安全工具。例如，攻击者没有途径破坏数据库（应用程序漏洞除外），如果类似的规则适用于出站流量，则没有任何方法可以连接回命令和控制基础设施。

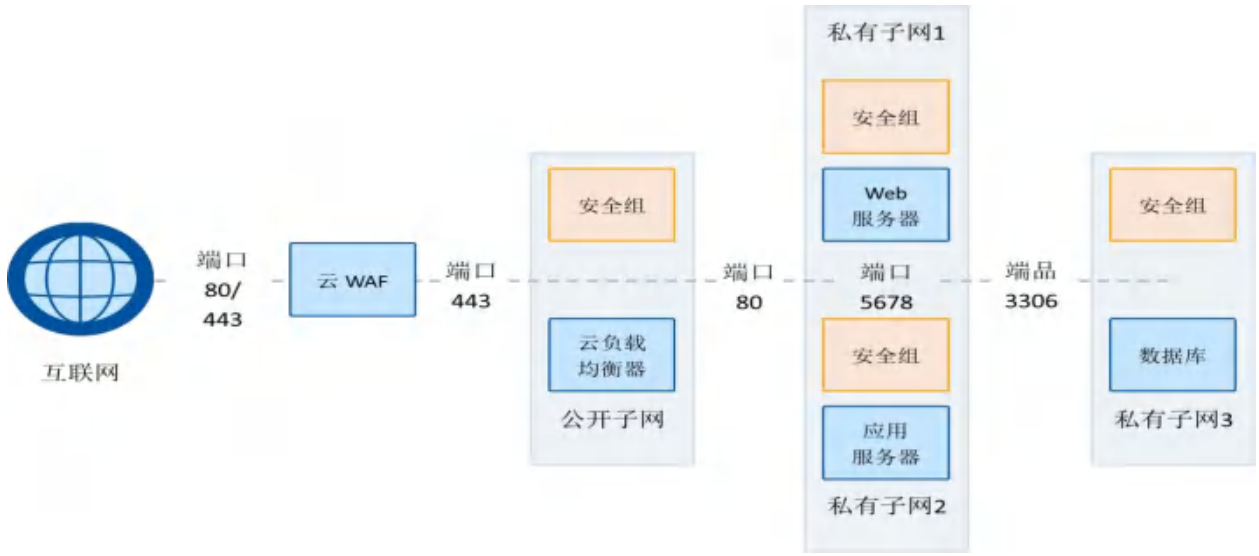


图 36：MVN 中的安全分层架构

在上面的示例中，互联网流量首先由云 Web 应用程序防火墙 (WAF) 接收，该防火墙充当主要入口点。WAF 接受所有传入流量并过滤掉恶意请求，然后将合法流量转发到负载均衡器。反过来，负载均衡器只接受来自 WAF 的流量并将其分发到 Web 服务器层。后续的每层（Web 服务器、应用程序服务器和数据库）只接受来自其上一层的流量，从而创建一个严格控制的类似电路交换的网络。

图中的端口号表示允许各层之间进行通信的特定端口。例如，Web 服务器可以接受来自负载均衡器的端口 80（HTTP）和 443（HTTPS）上的流量，而应用程序服务器可以接受来自 Web 服务器的特定端口（例如 5678） 上的流量。位于独立私有子网中的数据库仅接受来自指定端口上的应用程序服务器的流量。默认情况下，安全组未明确允许的所有其他流量都会被丢弃。

这种 MVN 架构使得攻击者很难侵入系统，因为他们探索网络和直接访问内部组件的能力有限。攻击者本质上仅限于针对应用层漏洞，因为网络端口不会暴露而导致被直接利用。要破坏系统，考虑到有限的攻击面和云平台提供的固有安全控制，攻击者需要成功突破云 WAF、负载均衡器和后续的每层，这是一个重大挑战。

7.2.3 基于 SDN 的常见组件

大多数云网络共享一套一致的基础组件。以下是一些常见的基于 SDN 的云组件。

虚拟网络/虚拟私有云：

- 一些提供商使用虚拟网络 (VNet)，其他提供商使用虚拟私有云 (VPC)
- 在云环境中逻辑隔离虚拟网络
- 使 CSC 能够定义其 IP 地址范围和网络拓扑
- 为云资源提供安全、私密的网络环境

子网（公共和私有）：

- VNet/VPC 内的较小网络段
- 允许进一步细分和组织资源
- 支持应用不同的安全和访问控制策略

路由表：

- 定义如何在 VNet/VPC 内引导网络流量
- 指定子网与外部网络之间的流量路径
- 启用自定义路由配置以获得最佳网络性能

云网络安全组：

- 安全组类似于状态防火墙，但它是在网络结构本身内实现的
- 充当网络接口、实例或子网级别的虚拟防火墙
- 根据 IP 地址、端口、协议和其他标准控制入站和出站流量
- 为单个资源或资源组提供细粒度的安全保护

云网络访问控制列表 (NACL)：

- 通过指定哪些数据包可以通过网络设备和环境，ACL 可以控制入站和出站流量
- ACL 在网络堆栈中的工作位置低于安全组，并且通常是无状态的
- 安全组通常适用于资源（例如实例），而ACL 适用于子网/网络

- 不同的 CSP 上两者的实现有所不同

网络地址转换 (NAT) 网关：

- 允许私有子网中的实例访问 Internet 或其他外部服务
- 将私有 IP 地址转换为公有 IP 地址以用于出站流量
- 对公共互联网隐藏内部 IP 地址来提供一层安全保护

互联网网关：

- 充当 VNet/VPC 中 Internet 流量的入口和出口点
- 允许 VNet/VPC 内的资源与公共 Internet 通信
- 启用云资源的入站和出站 Internet 连接

混合专线：

- 本地基础设施和云之间的专用私有网络连接
- 为混合云环境提供高带宽、低延迟和安全的连接
- 实现本地和云资源的无缝集成
- 示例包括多协议标签交换、AWS DirectConnect 或 Azure ExpressRoute

VPN 网关：

- 在本地网络和云之间建立安全加密的连接
- 允许远程用户或办公室安全地访问云资源
- 为小规模连接提供经济高效的专用租用线路替代方案

服务端点：

- 启用 VNet/VPC 与其他云服务之间的私有连接
- 允许 VNet/VPC 内的资源无需通过公共互联网即可访问云服务
- 通过将流量保持在 CSP 的网络内来增强安全性

对等/传输连接：

- 在同一云区域内的 VNet/VPC 之间建立直接的私有连接

- 使不同 VNet/VPC 中的资源能够相互通信
- 为 VPC 间通信提供经济高效且低延迟的选项

这些元素共同作用，在云中创建一个强大且安全的软件定义网络环境，使客户能够构建可扩展、灵活且可定制的网络架构。

7.2.4 云网络安全组

在 SDN 组件中，云网络安全组是保护云环境中资源的基础。它们是控制实例、VM 或子网级别的入站和出站流量的虚拟防火墙，为单个资源或资源组提供细粒度的安全性。通过定义基于各种参数（例如 IP 地址、端口和协议）允许或拒绝流量的规则来利用安全组。某些提供商（如 AWS）默认拒绝所有策略，CSC 必须创建允许规则。另一方面，Azure 默认采用宽容策略，CSC 可以创建拒绝规则。安全组还可以在内部引用其他安全组，无需在规则中定义 IP 地址。

安全组的关键原则之一是在策略中定义规则。管理员创建安全组策略，其中包含一组管理网络流量的规则。这些规则可以配置为允许或拒绝特定类型的流量，例如安全外壳 (SSH)、远程桌面协议 (RDP) 或 HTTP/HTTPS。通过精心制定这些规则，管理员可以实施最小特权原则，仅授予资源正常运行所需的权限，同时阻止所有其他流 量。

一旦定义了安全组策略，就可以将其应用于云环境中的特定资源。将策略应用于资源可确保在整个基础设施中一致地实施所需的安全措施。安全组可以与单个实例、网络接口或整个子网相关联（取决于 CSP），从而提供灵活性。可以将具有相同安全要求的资源分组并分配到同一个安全组，从而简化管理并减少配置错误的可能性。

安全组的另一个重要原则是，它们由网络结构针对每个资源强制执行。安全组中的每个资源都有一套自己的入站和出站规则。同一安全组内资源之间的流量不会自动被允许。如果需要同一安全组中的资源之间进行通信，则必须定义明确允许该流量的规则。这种明确允许的原则有助于保持严密的安全态势并防止资源之间进行规则之外通 信。

值得注意的是，每个主要的 CSP 都支持安全组。无论使用 AWS、Microsoft Azure、Google Cloud Platform (GCP) 还是任何其他 CSP，CSC 都会发现安全组是一项标准功能。虽然特定术语和配置界面在不同的 CSP 之间可能略有不同，但安全组的核心原则和功能保持一致。这种广泛的适应性使安全组成为跨不同云环境的可靠且可移植的安全机制。

总之，云网络安全组是实施资源级细粒度安全策略的强大工具。安全组通过在策略中定义规则、将这些策略应用于资源并通过网络结构实施这些策略，提供了强大的防御层。同一安全组中的资源之间明确允许的原则进一步增强了安全性。通过跨 CSP 对安全组的一致支持，CSC 可以放心地利用此功能来保护其基于云的资产并保持强大的安全态势。

7.2.5 超越安全组

虽然我们介绍了一些常见的 CSP 云架构工具，但我们还没有讨论其他工具。随着 CSC 获得开发基于云的网络环境的经验，它还将了解推荐的参考架构。无论 CSC 与本地部署进行混合和匹配，重要的是要清楚地了解这些 CSP 服务中的每一个的作用，以及为什么它为所有主要的超大规模提供商和 CSP（例如 AWS、Azure、GCP、IBM、Oracle）构建。

预防性安全措施：

- **CSP 防火墙：**CSP 防火墙（例如 Amazon VPC 防火墙或 Azure 防火墙）内置于云平台中。它们的优势在于无需维护额外的实例或服务器，从而简化了管理并降低了运营开销。但是，与虚拟设备相比，它们在自定义和高级功能方面可能存在局限性。
- **虚拟设备：**虚拟防火墙设备提供了更大的灵活性和对防火墙规则和配置的控制。它们可以部署在负载均衡配置中，以确保高可用性。然而，这种方法增加了复杂性，并且需要持续维护运行防火墙软件的虚拟机或实例。虚拟设备通常用于下一代防火墙 (NGFW) 和入侵检测系统和入侵预防系统 （IDS/IPS）产品。
- **WAF：**WAF 专门保护面向 Web 的应用程序免受 SQL 注入、跨站点脚本 (XSS) 和其他 OWASP Top 10 等常见攻击漏洞。根据 CSP 和 CSC 的要求，WAF 可以部署为云原生服务或虚拟设备。（一些 CSP 将其作为原生服务提供。）
- **出口过滤/管理：**出口过滤控制流向互联网或其他网络的出站流量。可以使用 CSP 防火墙、自托管代理或虚拟设备来实现。不过，需要注意的是，它仅涵盖部署过滤器的特定网络内的资源。

检测性安全措施：

- **流日志和 DNS 日志：**流日志和 DNS 日志提供了对网络流量模式有价值的可见性，并有助于检测异常活动。流日志捕获有关网络流量的源、目的、协议和其他属性的信息，而 DNS 日志记录域名解析请求和响应。这些日志可以帮助识别潜在的安全漏洞、未经授权的访问尝试和数据泄露。

● **流量镜像：**流量镜像允许您复制网络流量以进行监控和分析。但是，网络安全和基础设施安全局(CISA)已将其确定为潜在的安全风险。如果攻击者访问镜像流量，他们可能会拦截敏感数据。为了降低这种风险，建议实施严格的访问控制，加密镜像流量，安全存储，并定期审核配置和访问日志。

PaaS 安全注意事项：

● **API 网关：**API 网关是访问 PaaS 服务的入口点。它们提供身份验证、速率限制和请求/响应转换等功能。有些网关还包含内置安全功能。

● **资源策略：**CSP 提供资源级访问控制策略，例如 AWS IAM 策略或 Azure 基于角色的访问控制（RBAC），用来定义访问 PaaS 服务的细粒度权限的机制。根据最小特权原则正确配置这些策略至关重要。

● **WAF/CDN：**许多 PaaS 服务可以与 WAF 和内容分发网络 (CDN) 服务集成，以增强安全性和性能。WAF 可防御基于 Web 的威胁，而 CDN 则可通过吸收和过滤恶意流量来帮助缓解分布式拒绝服务 (DDoS) 攻击。

● **VPC/VNet 上的服务端点：**服务端点将 PaaS 服务直接连接到 VPC 或 VNet，使 CSC 能够应用一致的安全策略并控制服务和虚拟网络之间的流量。

● **继承网络安全：**PaaS 服务通常会继承通过网络连接时应用于其所关联的 VPC 或 VNet 的网络安全控制。

（许多服务的默认设置是直接 Internet 连接。）这意味着为网络配置的相同防火墙规则、访问控制和监控会扩展到 PaaS 服务，从而在整个云环境中提供一致的安全态势。

7.2.6 容器网络

专用的容器安全控制对于解决容器化的特定漏洞和威胁是必不可少的。容器是短暂的、轻量级的、高度动态的，这使得传统的安全措施效果不佳。由于其更大的攻击面，容器是攻击者的潜在切入点。容器镜像、编排平台或网络配置中的漏洞可被利用来获取未经授权的访问或发起攻击。在部署容器化应用程序时，组织有多种网络堆栈选项，包括Overlay network、主机网络和云原生网络解决方案。每个网络堆栈都有安全隐患和注意事项，强调需要根据所选架构量身定制安全措施。

CSC 不应假设它可以单独管理容器级别的所有网络安全。仍然需要安全组和边界安全来保护容器主机系统。这些措施通常对边界安全更有效，因为它们利用了更有效且可扩展的专用服务或虚拟机。当涉及到容器时，Docker111和 Kubernetes112 有几种主要选项。

Docker 网络选项：

● **桥接网络：**这是 Docker 中的默认网络模式。每个容器都连接到主机上的虚拟桥接网络，允许容器相互通信。桥接网络与主机堆栈隔离，提供网络隔离。

● **主机网络：**在此模式下，容器与主机共享相同的网络堆栈。这意味着容器可以直接访问主机的网络接口并可以绑定到主机端口。

但是这种模式为了简单而舍弃了网络隔离。

● **覆盖网络（Overlay network）：**覆盖网络允许在不同主机上运行的容器无缝通信。这是通过使用虚拟可扩展 LAN (VXLAN) 或 IPSec 隧道在多个主机上创建分布式网络来实现的。覆盖网络通常用于多主机 Docker 部署。

● **Macvlan 网络：**Macvlan 网络为每个容器分配一个唯一的 MAC 地址，使它们在网络上显示为不同的物理设备。容器可以直接连接到物理网络，绕过主机的网络堆栈。当容器需要在物理网络上拥有其 IP 地址时，此模式非常有用。

Kubernetes 网络选项：

● **Pod 网络：**在 Kubernetes 中，pod 是最小的可部署单元，可以包含一个或多个容器。每个 pod 都有自己的 IP 地址，pod 内的容器共享相同的网络命名空间，允许它们使用 localhost 进行通信。Kubernetes 需要容器网络接口 (CNI) 插件来处理 pod 网络。

● **服务网络：**Kubernetes 服务为一组 Pod 提供稳定的 IP 地址和 DNS 名称。服务充当负载均衡器，根据标签和选择器将流量分发到 Pod。服务有多种类型，包括 ClusterIP（集群内部）、NodePort（在每个节点的 IP 上公开）和 LoadBalancer（可通过 CSP 的负载均衡器从外部访问）。

● **入口：**Ingress 是一种 Kubernetes 资源，用于管理集群内服务的外部访问。它充当 HTTP/HTTPS流量的单一入口点，并提供如 URL 路由、SSL 终止和虚拟托管等功能。入口控制器（例如 NGINX）或 Traefik，实施入口规则。

● **网络策略：**Kubernetes 网络策略允许定义规则来控制 Pod 和命名空间之间的流量。CSC 可以根据标签和选择器指定哪些 Pod 可以相互通信。网络策略提供了一种在集群内实施网络分段和限制未经授权访问的方法。

● **容器网络接口插件：**Kubernetes 依靠 CNI 插件来处理 pod 网络。一些流行的 CNI 插件包括：

○ Flannel，一种简单的覆盖网络，它为每个节点分配一个子网，并使用 VXLAN 或 host-gw 进行节点间通信。

○ Calico 是一种高度可扩展且性能卓越的网络解决方案，支持 Overlay 和 non-Overlay 模式以及高级网络策略实施。

○ Weave Net，一种使用Gossip 协议的 Overlay网络 [117] 创建跨多个主机的 VNet，实现自动发现和加密。

这些只是 Docker 和 Kubernetes 中容器网络选项的几个示例。必须在容器和云网络层实施安全性，并且这将根据所选的网络堆栈而有很大差异。

7.3 云连接

NIST 模型中云的一个基本特征是领域 1：云计算概念和架构是广泛的网络访问。即使在私有云中，配置和资源也是通过网络管理和访问的。对于公有云，网络要么是公共互联网，要么是用于创建混合连接的专用线路。

云连接可分为三大类：

● 连接到云中的资源（例如虚拟机）

● 将 CSP 内的独立虚拟网络相互连接

● 从数据中心网络连接到云，或在两个不同的 CSP 之间连接

7.3.1 连接资源

该图概述了安全连接到云中运行的虚拟机或容器等资源的过程。

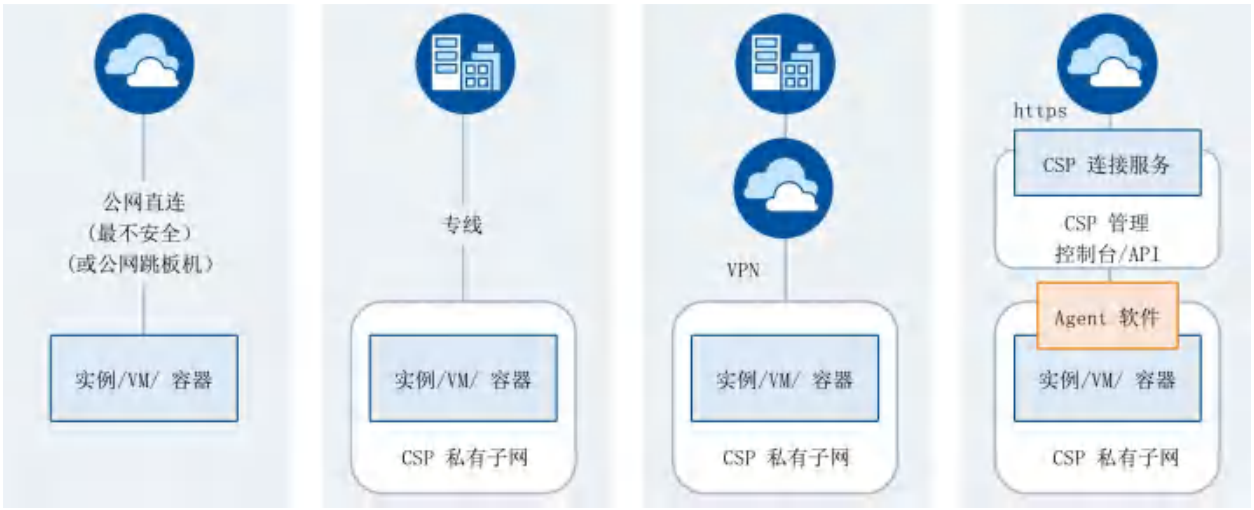


图 37：连接云资源的方式

直接互联网或私有专线

最直接的方法是通过公共互联网进行连接。这也是最不安全的方法。更安全的选择是在本地网络和 CSP 之间建立私有专线。这提供了专用的私有连接。

VPN

另一种常见方法是使用 VPN。VPN 在 CSC 网络和基于云的资源之间通过公共互联网创建加密隧道。

CSP 连接服务

为了访问实际的虚拟机或容器，CSC 需要通过所谓的连接服务，例如 AWS 会话管理器或 Azure 即时 (JIT)，从而通过 Web 控制台或支持端口转发的软件获得访问权限。这项重要的 CSP 服务充当安全网关。它还允许CSC 管理、监控和审计对云资源的访问。一个优点是，这些服务可以使用来自云管理平面的 IAM/RBAC 权限，从而减少或消除对 SSH 密钥或其他凭据的需求。

在图中，请注意虚拟机（基于已批准的安全虚拟机镜像）和实例（由已批准的容器生成）被分组到私有子网中。这些子网提供网络级隔离和安全性。连接服务允许授权用户安全地连接到这些私有子网中的资源，而无需将其暴露给互联网。连接服务通过中央管理控制台和 API 进行管理。这允许 CSC 配置访问策略、监控连接和审计活动。这可以被视为零信任的一种形式，稍后将讨论该主题。

其他选项也在不断发展，包括基于代理的Overlay网络、不同形式的端口隧道，甚至通过队列

管理软件发出异步命令。

总之，使用具有私有网络的连接服务可以提供一种安全的方式来远程管理基于云的资源，同时保持对访问的严格控制和可见性。

7.3.2 连接虚拟网络（在 CSP 内）

为了支持各种企业和应用程序需求，有多种选项和架构可用于连接 CSP 内的不同虚拟网络（例如 VNet 和 VPC）。有些（如服务端点）设计为仅连接到特定服务，即使网络共享重叠的 IP 地址范围。以下是一些用于连接 CSP 内的虚拟网络的示例。

对等连接：

- 在两个虚拟网络 (VNets/VPCs) 之间建立直接的私有连接
- 高度安全，因为流量永远不会穿越公共互联网
- 可快速轻松地为简单架构进行设置
- 随着网络数量的增加，复杂性迅速增涨，导致连接网格变得难以管理和排除故障

传输/网格：

- 提供用于连接虚拟网络的中心辐射模型
- 使用 AWS Transit Gateway 或 Azure Virtual WAN 等托管服务作为中央连接点
- 与复杂的对等网格相比，简化了网络架构和管理
- 更容易在连接的网络间实施一致的安全、监控和路由策略
- 会产生额外的传输服务费用，并且与直接连接相比，有时会略微增加延迟

服务端点：

- 允许将选定的服务投影到虚拟网络中，从而实现私密访问服务
- 例如，无需穿越公共互联网即可将多个应用程序 VPC 连接到共享数据库
- 由于公共端点完全被禁用，因此高度安全，只允许从授权子网进行访问
- 仅限于特定支持服务（因 CSP 而异）
- 对于保护关键数据存储很有用，但不是通用的网络连接解决方案

其他选项：

- 使用软件网关和 SD-WAN Overlay 云网络解决方案实现更高控制力和灵活性

● 共享私有连接（例如 AWS PrivateLink、Azure Private Endpoints），用于跨账户私下访问服务

● 与多个云部署共享单个虚拟网络（使用交叉部署权限）允许不同的组将工作负载部署到同一网络中

正确的选择取决于规模、安全需求、管理开销以及所连接的资源类型。典型的架构结合了多种方法。关键是在安全性、性能、复杂性和成本之间取得适当的平衡。

7.3.2.1 示例：云网络边界整合（云边一体化）

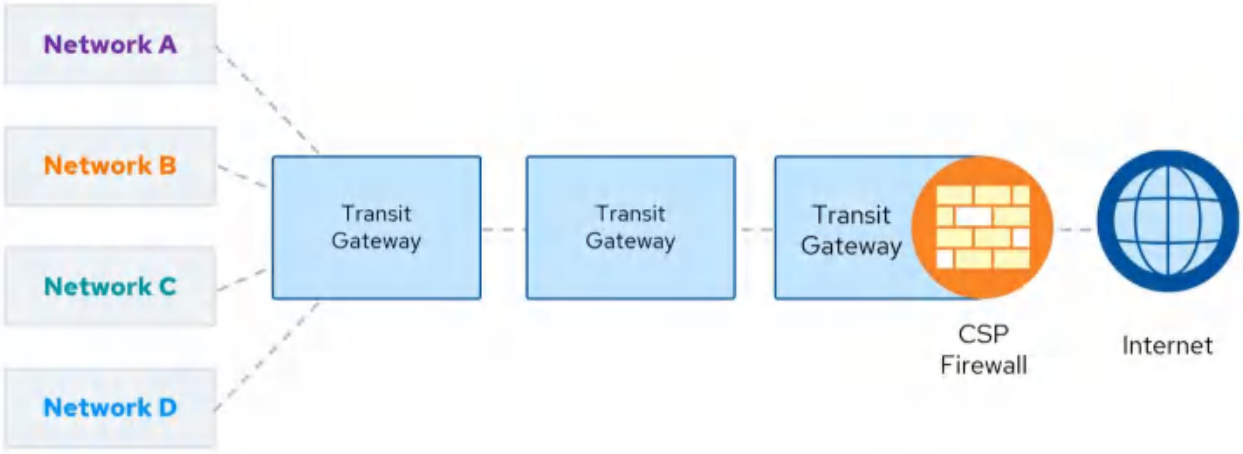


图 38：出站流量的整合云网络边界

在本例中，我们将介绍一个架构框架，该框架旨在通过统一的边缘网络来管理和保护来自几个不同网络（标记为 A、B、C 和 D）的出站互联网流量。此设置采用 CSP 提供的防火墙服务。

在此架构中，网络 A 到 D 连接到中央传输网关。值得注意的是，这些网络的配置没有直接访问互联网。相反，所有互联网流量都通过传输网关汇集，然后定向到专用的边缘网络（例如 VNet 或 VPC）。在此外围网络中，CSP 防火墙（AWS 网络防火墙或 Azure 防火墙）正在运行，检查和过滤合并的流量。

这种设计为所有流向互联网的流量创建了一个单独的、受管控的出口点，而不是允许每个网络自主访问互联网。这种集中式出口过滤方法具有多种优势，包括为所有互联网访问网络建立统一的安全协议，从而简化出站流量的管理和监视。它通过将互联网暴露集中到一个单一的、强化的网络来有效地减少潜在的攻击面，并增强了对离开网络的流量的记录、检查和监督的特异性。

该架构还提供了在边界内集成其他安全功能（如 IDS/IPS、Web 过滤和数据泄露防护 (DLP)）的灵活性。

但是，要优化此架构，必须考虑几个因素。为避免性能瓶颈，正确调整外围网络和防火墙的大小并保持高可用性至关重要。应仔细调整路由和安全协议，以仅允许必要的出站流量。此外，为确保稳健性、弹性和连续性， 建议使用多个帐户或 CSP 以及可用区域来实现冗余和故障转移功能。

7.3.3 连接到数据中心和提供商之间

在创建混合网络（包括多云网络）时，可以使用不同的技术通过互联网或私有主干网传输流量。以下是连接数据中心和 CSP 的一些选项示例。

专线：

- 在本地数据中心和云之间提供专用的、私有的、高速的连接
- 它们的半永久性意味着与部署光纤相比，它们的安装和拆除速度相对较快
- 由于不共享连接，因此速度非常快且性能可预测
- 需要两端兼容的硬件和 IP 寻址，这可能会带来复杂性
- 通常需要连接到网络运营商提供的 Meet-Me 点，然后连接到 CSP 的网络
- 不用于云到云连接，因为 CSP 有自己的互连

VPN：

- 在网络、数据中心和云 VPC/VNet 之间通过互联网建立加密隧道
- 高度灵活，可通过软件配置进行设置和拆除
- 需要两端有适当的硬件（或虚拟设备）来终止 VPN 隧道
- 性能取决于互联网连接的质量。可能会受到 CSC 网络外拥塞的影响
- 通常仍优先选择连接到 CSP 的传输网络（例如 AWS Transit Gateway、Azure Virtual WAN）
- 通常用于备份连接和安全远程访问云资源

混合网格：

- 使用 SD-WAN 或软件网关在本地和多个云之间提供任意到任意的连接

- 在现有连接之上构建 Overlay网络，使用软件和策略定义拓扑和流量流
- 与许多点对点链接相比，提供更大的灵活性和可管理性
- 减少对底层物理网络的依赖可以提高弹性
- 抽象和自动化可以大大减少配置负担和出错的机会
- 由于每跳的流量处理和额外的软件/许可成本，会产生一些性能成本
- 需要维护软件定义策略和网络控制器

上述之间的选择取决于所连接工作负载的规模、关键性和可变性。专线提供最高的性能，但灵活性最低。VPN 快速灵活，但不可预测。SD-WAN 和混合网格为本地和多云中的大规模部署提供了可编程的中间地带。许多 CSC 使用混合方式，例如将专线用于主要数据中心云连接、用于备份和用户访问的 VPN 以及用于统一管理的软件覆盖。关键是了解权衡利弊，并根据业务需求做出选择。

7.3.3.1 示例：转接网关和中心辐射型网络

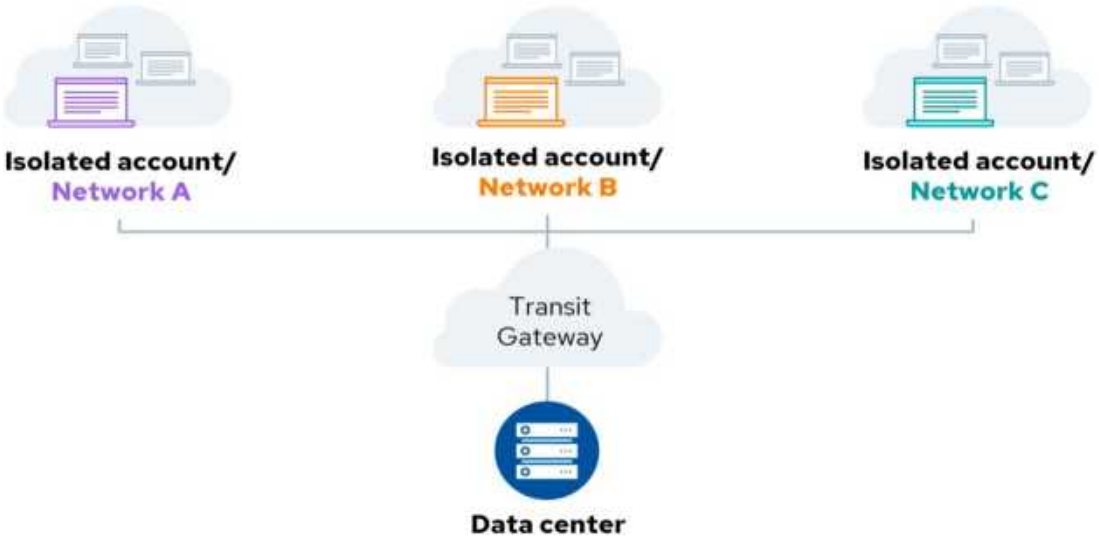


图 39：转接网关和中心辐射型网络 架构

此示例展示了使用传输网关的网络架构，传输网关是一项功能强大的网络服务，可通过集中式数据中心连接隔离网络。具体而言，它概述了传输网关（在 AWS 中称为 Transit Gateway，在 Azure 中称为 Azure WAN）如何充当协调隔离网络之间流量路由的关键枢纽，在图中标记为 A、B 和 C。

该架构由传输网关内的路由表管理，该路由表精确地规定了网络之间允许的流量。路由表指定

- 网络 A 和 C 被授予将其流量路由至数据中心的能力
- 网络 A 被配置来与网络 B 建立通信链路，并且
- 允许网络 B 与网络 C 连接。

重要的是，该架构限制网络 A 与网络 C 建立直接通信路径，同样，禁止网络 B 直接访问数据中心。

在 AWS 环境中，Transit Gateway 通过 Transit Gateway 附件链接到每个帐户中的 VPC。在 Azure 生态系统中，此连接是通过将虚拟网络连接在一起的虚拟 WAN 实现的。

此外，该架构利用专线在本地数据中心和基于云的传输网关之间建立物理连接。通过采用这种中心辐射模型，网络设计成功地分割和管理了多个隔离网络之间的流量。这种配置不仅可以集中执行路由和安全策略，还可以促进数据中心共享服务的可用性。选择性可访问性确保可以从指定网络使用这些服务，从而无需在所有网络段之间进行直接通信。

7.4 零信任和安全访问服务边缘

零信任 (ZT) 坚持不应假设隐含信任的原则，并且对于访问网络的任何用户或设备，始终都需要进行可靠的验证。本节介绍零信任架构框架及其支持技术，例如软件定义边界 (SDP) 和零信任网络访问 (ZTNA)。此外， 它详细介绍了 SASE 如何将各种安全功能集成到统一的云交付服务中，以满足日益分散的环境的需求。SASE 通过合并网络和安全功能来补充这一点，以提供对云服务的安全、可扩展的访问，从而优化分布式环境的性能和安全性。本节探讨了零信任和 SASE 的基本概念、优势和实施策略，详细介绍了它们如何有效地保护云架构和网络。

7.4.1 云基础设施和网络的零信任

零信任作为通用安全策略的讨论领域 2：云治理 CSA 零信任资源中心还提供了很多其他有用的参考资料， 包括 ZT 指导原则文件。

零信任是一种网络安全策略，其前提是不能隐式信任任何用户或资产。它假设已经发生或将发生违规行为，因 此，不应通过在企业边界执行的单次验证授予用户访问敏感信息的权限。相反，必须持续验证每个用户、设备、应用程序和交易。

实施 ZTA 涉及一种全面、全栈、多支柱的安全方法，该方法不假设任何信任，无论是从网络边界内部还是外部请求访问。

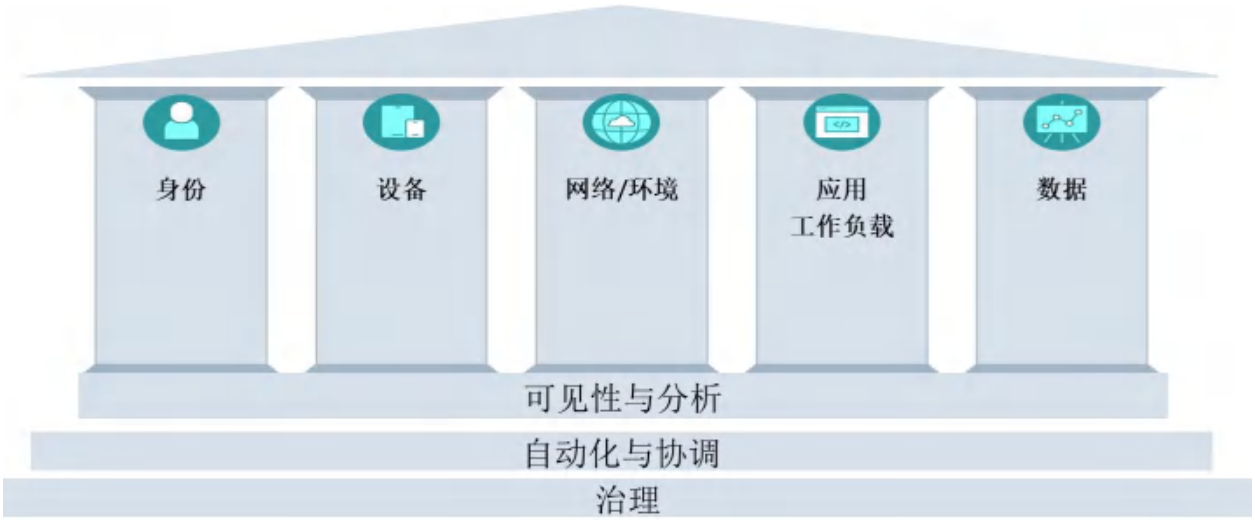


图 40：ZTMM 的五大支柱

7.4.1.1 基础 ZT 概念和能力

零信任是一种安全策略，特别适用于现代云基础设施和网络，在这些基础设施和网络中，业务应用程序和资产通常分布在不同的环境中，用户通常远程访问并频繁通过互联网访问业务系统。通过遵守零信任原则，组织可以增强其云环境的安全态势，降低安全漏洞、未经授权的访问和攻击者横向移动的风险和潜在影响。但是，实施零信任通常需要一种整体的全栈方法，将人员、流程和技术整合到整个云环境中。这可以通过实施以下安全措施的适当定制组合来实现。

持续验证：

● 对所有用户和管理员访问（包括云控制台访问和 API 调用）实施防网络钓鱼的多因素身份验证(MFA)。

● 通过实施基于上下文的访问控制 (CBAC)（可以包括 RBAC 和基于属性的访问控制 (ABAC)），在整个用户会话期间持续验证用户身份、设备姿态和会话上下文。

● 使用安全分析和用户/实体行为分析 (UEBA) 来检测异常和危险行为，特别是对于高度敏感和管理访问。

最低特权访问：

● 遵循最小特权原则，仅向用户和应用程序授予其业务功能所需的最小权限。

● 使用 JIT 访问和有时间限制的凭证来获得提升的权限。

● 定期审查和撤销未使用或过度的权限，并通过访问治理流程及时撤销所有终止用户的访问权限。

微隔离：

● 使用VPC、VNet、虚拟防火墙和类似结构实现网络分段。

● 使用网络安全组 (NSG) 和网络访问控制列表 (NACL) 根据工作负载关键性和安全要求将云网络划分为更小的、隔离的部分。

● 实施细粒度的分段策略并控制分段之间的横向移动。

● 根据最小特权原则限制段和服务之间的通信。

基础设施和工作负载安全：

● 部署 IDS/IPS 来检测和阻止恶意流量。

● 在具有安全边界的专用、隔离环境（例如虚拟机、容器、无服务器功能）中部署工作负载。

● 利用服务网格架构和微服务之间的基于身份的通信。

● 实施工作负载和容器运行时保护、漏洞管理和防火墙。

● 利用硬件安全功能，如加密虚拟机和机密计算区域。

● 使用 DevSecOps 实践自动化漏洞扫描、补丁管理和配置管理等安全流程。

● 采用不可变的基础设施和短暂的工作负载模式来确保安全性和一致性。

● 利用IaC工具安全地配置和配置云资源。

数据安全：

● 使用强加密算法和强大的密钥管理实践对静态数据和传输中数据（例如，通过相互认证的 TLS 连接）进行加密。

● 实施强大的备份和灾难恢复 (DR) 机制，以确保在发生安全漏洞、勒索软件攻击或数据丢失时的业务连续性 (BC)。

● 监控和审核数据访问和使用模式，以防潜在的滥用和泄露企图。

● 实施 DLP 控制和数据屏蔽技术。

监控和日志记录：

● 对云基础设施、网络和工作负载实施集中访问、流量记录和监控。

● 利用云原生日志记录、监控和警报服务收集和分析安全日志、流日志和审计跟踪，以进行威胁检测和事件响应。

● 配置警报和触发器以通知管理员可疑活动或安全漏洞。

● 实施安全信息和事件管理 (SIEM) 系统，用于日志聚合、关联和分析。

● 使用安全编排和自动化 (SOAR) 工具实现安全响应和补救的自动化。

例：零信任针对云中高度敏感信息的细粒度访问控制策略包括几个步骤。首先，验证用户最近的强身份验证。接下来，检查其端点设备的身份和安全卫生。确保他们的网络和地理位置对于所请求的数据和工作负载访问的时间和类型是可接受的。此外，请验证他们没有同时从多个地理位置登录。最后，使用行为分析来确保所请求的访问不符合内部风险访问配置文件。

通过遵循这些准则和原则，CSC 可以基于零信任策略为其云基础设施和网络建立强大的安全态势，帮助降低安全风险并保护敏感数据和资源。

7.4.1.2 零信任概念架构

NIST SP 800-207 零信任架构 (ZTA) 提供了一个组件模型，该模型也在 CSA CCZT 培训中详细介绍，如下图所示。

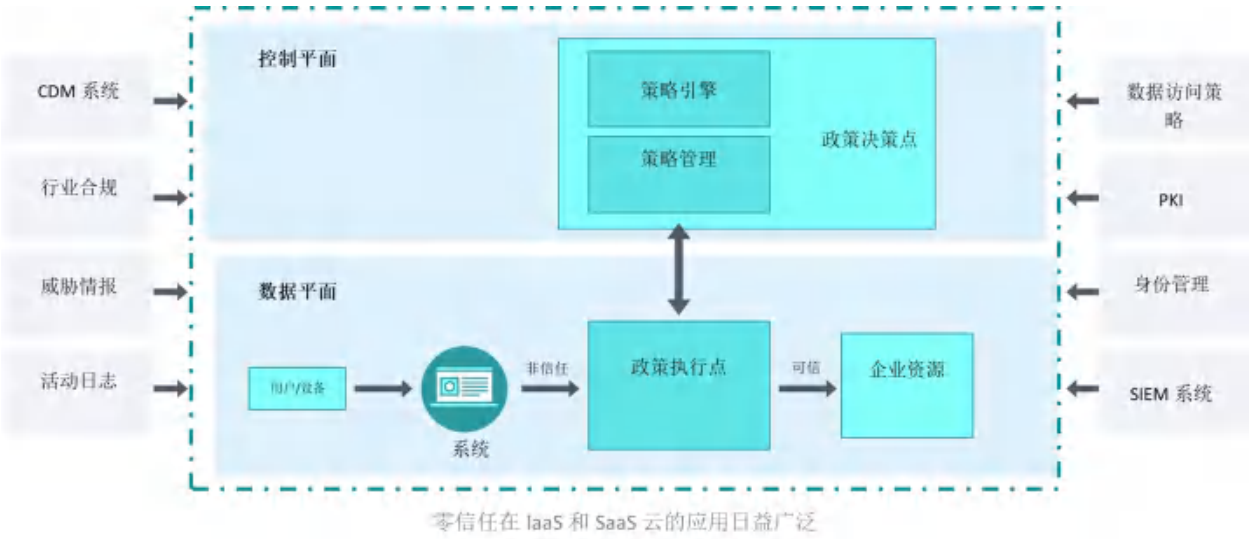


图 41：ZTA 核心逻辑组件（NIST 800-207，第 9 页）

NIST 2020 SP 800-207 提供了 ZTA 关键逻辑组件的简单表示（如上所示）。在 NIST ZT 模型中，使用策略决策点 (PDP) 和策略执行点 (PEP) 定义、管理和执行 ZT 访问策略。PDP 和 PEP 通过将资源访问置于流量访问工作流中来规范资源访问。PDP 包括策略管理员和策略引擎，它们确定规则并将其传递给 PEP。PEP 充当网关，以确保已向正确的实体授予对已批准资源的正确访问权限，并具有正确的访问级别。

NIST 将 PDP 定义为位于控制平面中，是逻辑架构的组件，负责收集、分析数据，并将数据首先转换为情报，然后转换为规则以管理对资源的访问。PEP 位于数据平面中，是 ZT 组件，根据控制平面传递的输入，负责执行规则并提供对资源（数据）的访问。

各种安全相关数据源将信息提供给 PDP，以维护规则并使整个决策过程保持最新。各种情报源将信息输入策略引擎，并支持策略管理员定义和完善访问规则。

7.4.2 软件定义边界和零信任网络访问

实现零信任网络安全的两种关键技术方法是 SDP 和 ZTNA。这些方法并不相互排斥，每种方法的元素都可以组合成量身定制的 ZT 安全实施。

软件定义边界 (SDP)

- 建立一个安全的未经授权的用户和设备看不到的“暗”网，。

- 实施“停电”方法，默认情况下网络不可访问。
- 用户和设备必须经过身份验证并获得授权才能访问受 SDP 保护的资源。
- SDP 利用以身份为中心的控制和微隔离来限制横向移动。

ZTNA

- 用更精细、特定于应用程序的访问控制模型取代传统的 VPN。
- 根据身份、设备、位置和其他环境因素对用户进行验证和授权。
- 提供对特定应用程序或资源的访问权限，而不是授予广泛的网络访问权限。
- ZTNA 解决方案可以是云托管（ZTNA 即服务）或本地托管。

通过实施零信任网络安全原则，组织可以显著增强其整体安全态势，降低数据泄露风险，并在不断演变的网络威胁面前更好地保护其资产。ZTNA 和 SDP 的结合为保护现代、以云为中心和远程访问密集型 IT 环境提供了一个强大的框架。NIST SP 800-215，安全企业网络环境指南 [123] 对这些主题来说是一个很好的参考。

7.4.2.1 软件定义边界

SDP 是一种零信任网络安全架构，旨在提供完整的（OSI 网络）栈安全。SDP 实现会隐藏资产，并在允许任何与隐藏资产的连接之前使用单独的控制平面和数据平面授权访问。SDP 实现了基础零信任原则。

ZT 实施要求在授权之前验证试图访问资产的所有内容。此外，ZT 要求在整个连接期间持续评估会话及其风险级别。使用 SDP 的 ZT 实施使组织能够防御现有网络和基础设施周边中心网络模型中不断出现的旧攻击方法的新变种。实施 SDP 可改善企业的安全态势，这些企业面临着不断适应日益复杂的不断扩大的攻击面的挑战。CSC 必须监控资产的安全状况。SDP 通过启用默认的 drop-all 网关来强制执行此访问管理策略，直到用户/设备经过正确身份验证并被授权访问隐藏资产。通过要求预先审查连接，SDP 可以完全控制谁可以连接、从哪些设备连接到哪些服务和基础设施，以及其他条件和环境因素，例如运营时间和地理位置。

根据SDP架构指南v2的描述，SDP由以下主要组件组成：

● 客户端/发起主机

● 服务/接受主机，也称为 NIST 的 ZTA 模型中的 PEP

●接受主机和发起主机都连接到的 SDP 控制器，也称为 NIST 的 ZTA 模型中的 PDP

● 实现 drop-all 防火墙的 SDP 网关

根据 SDP 架构指南 v2，SDP 的工作方式如下：

● 发起主机上的 SDP 客户端软件会打开与 SDP 的连接。发起主机设备（例如笔记本电脑、平板电脑和智能手机）面向用户，这意味着 SDP 客户端软件在设备本身上运行。网络可能不受运营 SDP 的企业的控制。

● 接受主机设备接收来自发起主机的连接并提供一组 SDP 保护/安全服务。接受主机通常位于 CSC 控制下的网络上（和/或直接代表控制下）[126]）。

● SDP 网关为授权用户和设备提供对受保护进程和服务的访问权限。网关还可以对这些连接进行监控、记录和报告。

发起主机和接受主机设备连接到 SDP 控制器，该控制器是一种设备 / 装置或进程，通过确保以下事项来保护对隔离服务的访问：

1. 用户经过身份验证和授权
2. 设备已验证
3. 建立安全通信
4. 用户和管理流量在网络上保持分离

控制器和接受主机对未经授权的用户和设备不可见且不可访问。SDP 实现可以支持多种不同的连接配置，以适应不同的通信用例。有关详细信息，请参阅软件定义边界 (SDP) 规范 v2.0。

7.4.2.2 零信任网络访问

ZTNA 是零信任安全模型的关键组成部分，专门用于对应用程序和资源进行安全远程访问。ZTNA用更细粒度的规则和特定于应用程序的访问控制模型取代了传统的 VPN。根据身份、设备、位置和其他情境因素，对用户进行验证并授权其访问特定应用程序或资源。

通过实施 ZTNA 原则，组织可以显著减少其攻击面，实施细粒度的访问控制，以减轻未经授权的访问、数据泄露以及网络和应用程序内横向移动的风险。

7.4.3 安全访问服务边缘

SASE（安全访问服务边缘） 是一种新兴的网络安全概念，它将网络安全功能与 WAN 和代理功能相结合，以提供全面的云原生服务。它旨在解决在云优先、移动优先的领域中保护端点设备以及访问应用程序和数据的挑战，在这种领域中，用户和资源越来越多地分布在传统网络边界之外。

7.4.3.1 SASE 框架和架构概述

SASE 是一种将网络和安全功能整合到单一的云交付服务中的框架或架构方法。SASE 旨在为用户提供对应用程序和数据的安全访问，无论他们身在何处，同时确保整个组织网络具备一致的安全策略和控制。

图 42：SASE 框架和架构概述

SASE 在实现云环境中的零信任安全方面发挥着重要作用。零信任是一种安全模型，它不假设任何隐式信任，并持续验证每个访问请求，无论其来自何处。SASE 通过提供一个统一的平台来支持这一点，该平台可在所有用户、设备和应用程序中实施细粒度、上下文感知的访问策略。

它将安全网关、云访问安全代理 (CASB)、ZTNA 和传统防火墙功能等安全功能集成到一个云交付服务中。这使组织能够一致地应用安全策略并监控对云资源的访 问，而不管用户的位置或设备如何。

7.4.3.2 SASE 实施及效益

SASE 集成了网络和应用层安全机制，简化了云环境中零信任的部署和管理。通过将安全性作为云原生服务提供，SASE 减少或消除了需要管理多个单点产品，并使组织能够随着云占用空间的增长快速扩展其安全基础设施。它还提供了一种更加以用户为中心的安全方法，能够根据用户身份、设备状态和应用程序敏感度实施策略。这对于在云中实现最小权限访问至关重要，因为远程用户需要访问特定的应用程序和数据，而不是整个网络。

随着组织持续采用云服务并接受远程工作，SASE 将在实现零信任安全的整体潜力方面发挥重要作用。通过提供统一的云交付平台来保护从任何设备、通过任何网络对任何应用程序的访问，SASE 使组织能够在其整个数字资产（包括云、本地和混合环境）中一致地实施零信任策略。这不仅可以改善整体安全态势，而且在不会损害企业安全的情况下还可以充分利用云的灵活性和可扩展性。

总结

保护云基础设施是一项双重任务，既要保护 CSP 的设置，又要保护 CSC 部署的配置。基础设施安全的核心支柱包括创建安全架构、确保配置从一开始就是安全的、在开发生命周期的早期阶段集成安全性（左移实践）以及通过监控和应用护栏保持警惕。

基于 SDN 原则构建的云网络提供高级安全功能，例如实施默认拒绝策略、根据策略管理访问和规则以及允许进行细粒度的网络分段。这些功能显著的增强了云环境中的安全框架。

融入零信任原则（例如 SDP 和 SASE）对于确保多云连接和实现安全远程访问至关重要。这些模型确保严格控制访问并根据经过验证的身份和上下文提供访问，从而增强分布式环境中的安全性。

容器网络在传统虚拟化云网络之上添加了一个抽象层，从而带来了新的复杂性。这需要在容器和云网络层都应用安全措施，以防止漏洞被利用。

最后，云网络安全不仅限于安全组。它还包括部署防火墙、IDS/IPS 和 WAF 等预防性措施，以及流日志和流量镜像等检测控制。这些元素共同构成了对网络威胁的强大防御措施，确保利用云技术的企业的云基础设施的完整性和弹性。

建议

云基础设施安全

- 遵循良好架构框架或同等原则来指导设计和实施决策，以提高使用云时的安全性和成本效益。
- 左移安全：在开发生命周期的早期嵌入安全控制和测试，而不是事后才考虑。
- 使用 IaC 通过机器可读的配置文件来管理和配置 IT 基础设施。

云网络基础知识

- 实施软件定义网络(SDN)，以提高灵活性、敏捷性并简化网络运营和管理。
- 利用云网络安全组。
- 考虑预防性和检测性安全措施。

云连接

- 使用具有私有网络的连接服务对基于云的资源进行安全的远程管理。
- 考虑使用对等或传输/网格架构来连接 CSP 内的虚拟网络。
- 评估混合网络中连接数据中心和 CSP 之间的不同选项。

零信任和安全访问服务边缘

- 实施零信任：一种网络安全策略，假设没有任何用户或资产是隐式可信的，并要求对每个用户、设备、应用程序和交易进行持续验证。
- 使用 SASE 为用户提供对应用程序和数据的安全访问，无论他们身在何处。

补充指南

- 如何设计安全的无服务器架构 | CSA
- 云操作系统安全规范 v2.0 | CSA
- DevSecOps 的六大支柱：自动化 | CSA

- 软件定义边界作为 DDoS 预防机制 | CSA
- CSA 物联网安全控制框架 | CSA

领域 8：云工作负载安全

该领域涵盖保护云工作负载。云工作负载指在云计算环境中运行的各种任务、应用程序、服务和流程。云工作负载具有可扩展性、灵活性和效率，使企业和个人无需在物理硬件上投入大量资金即可访问和运行应用程序或数据处理任务。云工作负载包含一系列资源，包括虚拟机 (VM)、容器、无服务器功能（也称为功能即服务(FaaS)、AI 和平台即服务(PaaS)。云环境的动态性质及其不断变化和扩展的资源需要与传统方法不同的安全方法。

学习目标

在此领域，您将学习：

- 了解为云安全工作负载创建安全方法的挑战和独特性。
- 了解虚拟机的安全注意事项。
- 了解用于保护容器的安全注意事项。
- 了解安全注意事项以提供 PaaS 安全性。
- 了解保护无服务器或功能即服务工作负载的安全注意事项。
- 了解 AI工作负载的安全注意事项。

8.1 云工作负载安全简介

对于使用云的企业来说，保护这些工作负载不仅仅是为了保护数据，还为了确保其运营能够不间断地持续进行， 并遵守法律法规，包括数据保护和隐私法规。

下面概述了云工作负载和传统环境之间的主要区别：

- **动态和可扩展：**与数据和工作负载相对静态的传统环境不同，云是一个不断演化的动态、可扩展的架构。这种环境的动态性要求采用同样敏捷和弹性的安全方法。对于安全专业人员而言，这意味着重新思考标准安全措施，并适应对抗环境不断变化的环境。

● **复杂性和多样性：**工作负载有很多种类型，每种类型都有各自的要求，因此，一刀切的安全方法是行不通的。

● **完整性、机密性和可用性：**云工作负载安全的核心在于维护数据完整性、机密性和可用性—这些原则是网络安全的基石。在云中，确保数据不被变更（完整性）、仅授权用户可访问（机密性）以及在需要时可用（可用性）至关重要。

8.1.1 云工作负载的类型

云环境中使用各种云工作负载，每种工作负载都有其独特的特性和安全隐患。从管理虚拟实例和保护容器化应用程序，到确保无服务器和人工智能 (AI) 操作的安全，本节提供了在复杂的云安全环境中的基本指导，强调了严格治理和主动安全措施的重要性。

● **虚拟机(VM)和实例：**虚拟机（也称为实例）是云计算的基石。它们通过单独的操作系统和虚拟机管理程序和其他管理平面组件强制执行的安全边界提供隔离。虚拟机管理程序是云服务提供商 (CSP) 维护的关键组件。但是，每个虚拟机内的客户操作系统的安全性通常由云客户(CSC) 处理，需要细致的配置和修补。此外，“虚拟机蔓延”可能带来重大安全风险。此外，管理快照和镜像镜像（文件）对于防止敏感数据泄露至关重要，这凸显了严格治理的必要性。

● **容器：**这些是独立的运行时环境，它们共享主机操作系统的内核，但作为独立的、自包含的进程运行，具有自己的文件系统、库和配置。容器提供了一种轻量级且高效的虚拟机替代方案，但也带来了不同的安全挑战。由于容器共享主机操作系统内核，因此它们本质上提供的隔离性较弱。容器化环境中的安全性取决于正确配置操作系统级控制、维护容器镜像安全性以及确保正确配置容器的运行时环境。尽管 Kubernetes 等编排器在增强安全性方面具有优势，但编排器也带来了额外的复杂性，必须谨慎处理才能防止违规。

● **平台即服务 (PaaS)**: 这些工作负载通过提供一套工具和服务来扩展云平台的功能，从而以更高的效率和更少的开销促进应用程序的开发、部署和管理。这些服务包括数据库和消息传递系统以及内容分发网络(CDN)，它们提出了不同的安全考虑因素。

● **无服务器或函数即服务 (FaaS)**: FaaS 是一种云计算模型，开发人员可以编写和部署单个函数，这些函数会根据事件或请求执行，而无需管理底层基础设施。这种无服务器模型将更多的安全责任委托给 CSP。这种信任重新分配利用了 CSP 的专业安全专业知识和先进的保护措施，

从而最大限度地减少了攻击面。执行环境的短期运行特性，加上 CSP 强制隔离，提供了固有的安全优势。然而，管理机密和以最小特权配置功能对于保护无服务器应用程序免受未经授权的访问和潜在攻击（例如拒绝服务或通过自动扩展造成的财务耗尽）至关重要。

● **AI工作负载**：这些工作负载处理大量数据以进行学习、做出决策或提供预测。因此，它们带来了独特的安全挑战。确保数据的完整性和隐私变得至关重要，特别强调防范对抗性攻击、防止模型盗窃和防止快速注入。尽管存在这些漏洞，但 AI工作负载仍利用了云环境的高级计算资源和可扩展性。

一般来说，当涉及到云工作负载时，管理职责会转向 CSP，尤其是在无服务器计算等模型中。虽然攻击面可能会减少，但可见性、控制和治理挑战仍然存在。因此，安全监控和治理对于在所有云工作负载中保持强大的安全态势至关重要，确保操作能够不间断地继续进行并遵守数据保护法规。

8.1.2 云工作负载：短期和长期运行

短期运行（短暂）VS 长期运行（不可变的)的概念代表了在云工作负载中两种不同的工作负载管理和保护方法。短期运行/短暂方法涉及将工作负载视为可互换和可抛弃的资源。相比之下，长期运行/不可变方法将工作负载视为不可或缺的资源，需要手动维护。传统上，在计算中，基础设施主要使用短期运行模型来处理，但云计算的引入要求我们重新思考我们的方法。这两种模型都对安全性、运营管理和可扩展性有影响，因此了解差异以及何时适合使用每种方法非常重要。

短期运行（短暂）

在云原生架构中，大多数工作负载都采用短期运行模型。这些是临时服务——它们根据需要拉起或销毁，有时只存在很短的一段时间来处理特定任务或工作负载。短期运行工作负载中的安全性是主动且内置的；它是 VM 或容器镜像创建过程的一部分，不需要手动配置或后期部署。使用不可变基础设施意味着无需修补或重新配置，而是启动新的工作负载来替换任何受到损害或有害的工作负载。该模型支持自动扩展和自我修复功能，由于其效率和它提供的增强安全态势，它正在成为现代云原生应用程序架构中的主导模式。

长时间运行（不可变）

相比之下，长期运行的工作负载是经过长期精心培育和维护的工作负载。这些工作负载通常是独一无二的，手动构建和管理，并且手动安装和更新安全软件。这种方法既耗时又容易出现人为错误，从而导致安全实践不一致。长期运行的工作负载通常出现在将传统的本地工作负载迁移到云中而不改变底层管理哲学的场景中（被称为直接迁移（lift and shift“)。虽然长时间运行的工作负载对于某些应用程序（例如需要特别注意的数据库）来说可能是关键，但它们的弹性较差，并且在出现问题时维护成本较高。

云安全中的短期运行负载与长期运行负载对比

在安全性方面，短期运行的工作负载往往比长期运行的工作负载更安全，因为它们的生命周期较短，可以限制受到威胁的可能性，而其配置的自动化特性可确保一致性并减少错误。不可变的基础设施可防止配置漂移和未修补的漏洞，从而更易于维护和扩展安全措施。测试镜像镜像的安全性也比测试长期运行的工作负载更简单。

短期运行模型主张在自动化安全性方面进行前期投资，并将其集成到部署流水线中，这将在规模化方面带来回报。这种策略虽然有效，但可能并不适合所有情况。由于其性质或业务要求，一些短期运行的工作负载仍被视为长期运行的工作负载。这些工作负载应该是例外而不是合理的，应在云环境中受到保护和隔离，以最大限度地降低风险。默认采用短期运行模型，并将长期运行的使用限制在特殊情况下，这被认为是云安全的最佳实践。

对于技术从业者来说，向短暂和不可变的工作负载的转变代表着向使用和替换方法的战略性转变。这是摆脱传统修复和修补模型，转向有利于稳健性和最小化漏洞的运营环境。在这个进化的框架中，云环境成为一个更安全、更可靠、更可预测的虚拟资源托管空间。

8.1.3 对传统工作负载安全控制的影响

对于刚开始接触云技术的人来说，将云工作负载安全视为设置适当的护栏（技术预防控制）有效地监督他们（监控）并定期检查其健康状况和准备情况（评估）。但这样做是在一个非常大且不断变化的虚拟空间中进行的， 其中事物的移动和变化速度比传统计算环境快得多。

以下是云工作负载安全控制的一些重要注意事项。

执行控制：许多组织使用安全代理，像端点保护平台或端点检测和响应 (EDR) 一样，它们可以与云工作负载一起使用。这些工具需要拥抱和支持云的动态和虚拟化特性。代理应该是轻量级的，这样它们就不会显著增加计算成本。它们应该具有云感知能力，而不依赖于固定 IP 地址或其他静态配置。代理应该能够在启动新工作负载时进行自我注册，以使其可用于自动缩放组和不可变场景。这些工具也不应该要求安全组中的入站网络端口，如果攻击者确实进入虚拟网络，这可能会增加攻击面。

监控：通常使用代理来捕获操作系统生成的工作负载日志的工具。由于云资源的瞬时性，这些日志应快速发送到中心位置。在非云环境中，监控代理通常通过网络将日志移动到日志服务器，但在云中，这些日志可以直接保存到本地云存储中，这可能更具成本效益。具有成本效益和灵活性以适应云中不同的存储和计算要求非常重要。日志条目需要丰富以表明工作负载身份，因为 IP 地址或系统名称本身可能指向多个工作负载并且经常变更，并且名称和地址在扩展操作期间或跨不同的云部署重复使用。

评估：漏洞评估（扫描）传统上是通过网络执行的，但这在云端可能并不有效，因为即使是内部网络也有“默认拒绝”控制，安全组也会根据每个工作负载限制连接。不能依赖于将评估服务器放在同一子网上并扫描漏洞。有三种方式更适合云部署。第一种是在部署虚拟机之前评估构建的虚拟机和容器镜像。修复镜像中的漏洞并跟踪镜像的历史记录可防止新虚拟机出现漏洞，并允许快速审核以确定哪些正在运行的虚拟机是易受攻击的版本。其次，组织可以通过创建虚拟机快照并离线评估这些快照来替代运行时漏洞评估，而不会影响正在运行的工作负载。最后，可以选择将漏洞评估代理构建到镜像中。

云工作负载保护平台 (CWPP)：这些是特定于云和容器的工作负载工具，可提供多种工作负载安全功能。它们可以跨云工作负载（例如虚拟机、容器、无服务器）执行深入的漏洞扫描，并根据可利用性和业务影响对发现结果进行优先排序。一些工具还集成了日志和活动收集、额外监控，甚至运行时保护。

8.1.4 软件成分分析

软件成分分析 (SCA) 工具和软件物料清单(SBOM)是镜像流水线中用于提高工作负载安全性的重要工具。这些工具对于管理依赖关系、识别漏洞以及确保跨不同云服务模型的合规性至关重要。

SCA工具对于检查开源和商业组件的云工作负载至关重要。无论是处理虚拟机、容器还是无服务器功能，SCA 都有助于查明这些组件中已知的漏洞和许可问题。通过将SCA集成到持续集成/持续部署(CI/CD) 流水线中，开发人员可以确保在应用程序生命周期的早期解决潜在的安全风险。SCA促进的主动漏洞管理使团队能够检测和解决其依赖项中的漏洞，确保所有组件都符合组织许可策略并降低法律和安全问题的风险。

跨云工作负载的SCA的主要优势包括：

- **主动漏洞管理**：帮助在部署之前识别和纠正漏洞，增强云环境的安全态势。
- **许可证合规性**：确保所有软件组件符合组织的许可协议，从而避免法律问题。
- **风险评估**：为每个已识别的漏洞提供风险评分，帮助根据其潜在影响确定修复的优先顺序。

8.1.5 软件物料清单

SBOM是软件的详细配方，列出了每个组件及其版本以及它在软件环境中的交互方式。这种详细程度对于管理 潜在漏洞和确保所有类型的云工作负载的质量至关重要。生成SBOM 可提供透明度，这对于有效的漏洞管理和法规遵从性至关重要，从而更容易跟踪开源和专有组件的使用和交互。

SBOM 在云工作负载中的重要性包括：

- **增强透明度**：提供所有软件组件的全面细分，有助于更好地治理和控制云工作负载的软件供应链。
- **改进的安全响应**：通过精确定位受影响的组件，有助于更快地识别和修复漏洞。
- **法规遵从性**：协助满足强制披露软件组件的合规性要求，这对于监管要求严格的行业来说至关重要。

总之，将 SCA 和 SBOM 集成到云工作负载（无论是虚拟机、容器还是无服务器架构）的开发和部署过程中，不仅可以增强安全性，还可以确保这些环境的可靠性和合规性。对于希望保护其云运营免受不断变化的网络威胁的组织来说，这些做法是必不可少的。

8.2 虚拟机

VM 是运行在虚拟机管理程序上的整个操作系统。VM（也称为实例）是运行云工作负载的主要方法，因为它们靠近硬件并且被普遍理解。VM 通过虚拟机管理程序强制隔离，在客户内部和客户之间的工作负载之间提供严格的隔离。这种隔离可确保每个 VM 都维护其全栈操作系统。

VM 部署始终从标准化基础镜像开始，为安全配置建立统一的基础。此外，云的自动扩展 VM 功能有助于使用不可变的工作负载，从而提高效率并适应不断变化的需求。

8.2.1 虚拟机挑战与缓解措施

尽管隔离提供了安全性，但在共享物理硬件上运行的虚拟机可能容易受到侧信道攻击（Side Channel Attack）攻击，攻击者可以通过分析硬件行为从虚拟机中推断出信息。为了降低此类风险，每个虚拟机不仅可单独访问，而且还需要从基本虚拟机镜像建立细致的安全配置。这确保保持牢不可破的安全态势，加强虚拟机以防止未经授权的访问，并在整个云基础架构中提供一致的保护层。

虚拟机独特的安全挑战包括：

- **镜像控制：**确保虚拟机镜像安全部署并保持最新是一个挑战，特别是当用户可以提供自己的镜像时。
- **补丁管理：**定期使用最新的安全补丁更新基础镜像至关重要，但可能会耗费大量资源
- **变更管理：**允许 CSC 改变正在运行的虚拟机可能会无意中引入漏洞或导致配置漂移。
- **攻击面管理：**与更精简的工作负载类型（例如容器）相比，虚拟机中的操作系统和应用程序创建的攻击面更大。
- **生命周期管理：**长期运行、手动配置且不经常更换的虚拟机给维持强大的安全态势带来了困难。
- **网络安全：**保护虚拟机网络访问所需的细粒度控制机制，包括安全 shell (SSH)，解决用于访问虚拟机实例的 SSH 私钥被无意泄露的难题。
- **Rootkit 和 bootkit：**使用具有内核级权限的 rootkit 和 bootkit 感染固件和操作系统

有效的虚拟机漏洞管理涉及在安全漏洞被利用之前识别、评估和缓解这些漏洞。强调定期评估、优先级排序、自动化和集成的战略方法对于应对漏洞管理挑战至关重要。虽然管理运行时漏洞非常重要，但缓解镜像中的漏洞始终是优先事项。

为了应对这些挑战，应采取以下措施：

- **安全基础镜像：**从集中管理的目录中强制使用安全的基础 VM 镜像。镜像应在构建后进行版本控制且不可变更。这些镜像通常使用部署流水线创建，这些流水线在自动化时可称为“镜像工厂”。
- **扫描：**在批准使用虚拟机镜像之前，请扫描其中是否存在漏洞和错误配置。
- **最小化攻击面：**删除不必要的操作系统组件并加强操作系统配置。
- **优先级：**关注环境中风险最高的漏洞，考虑可利用性和潜在影响。
- **自动化：**利用自动化进行扫描、修补和报告以提高效率并减少人为错误。
- **集成：**确保漏洞管理工具与现有的安全和 IT 管理系统集成，实现统一的方法。
- **采用短期运行的虚拟机：**在可能的情况下，采用不可变的基础设施方法，其中虚拟机是短暂的和可替换的，从而最大限度地减少难以安全维护的长期运行的虚拟机。
- **配置管理：**使用配置管理和基础设施即代码 (IaC) 来维持所需状态并避免配置漂移。
- **监控和日志记录：**集中收集日志并实施指示入侵企图或可疑活动的指标。有效的监控和日志记录可让您了解虚拟机活动，从而及时检测和响应安全事件。
- **访问控制和最小特权：**授予应用程序和用户最低权限，仅允许其访问与虚拟机关联的授权软件包、库和其他数字资产。实施最小特权原则可减少攻击面并限制安全漏洞的潜在影响。
- **基于主机的防火墙和 SSH 加固：**使用基于主机的防火墙（例如 Linux IP 表防火墙）控制端口、协议和数据包类型，从而限制对 VM 实例的网络访问。通过使用 SSH 配置选项强化所有 VM 实例上的 SSH。
- **安全启动：**防范可能攻击预启动环境以绕过操作系统和防病毒软件的潜在恶意软件。
- **专用安全工具：**实施专为云环境设计的工具，持续监控虚拟机管理程序。此监控功能相当于监控公寓大楼内整个楼层的保安人员，确保虚拟基础设施的安全性和完整性。

适当的虚拟机安全控制和管理可以为云工作负载提供安全灵活的基础。但是，鉴于覆盖面和控制范围的扩大，安全性的责任也更大，并且配置错误的可能性也更大。遵守云安全最佳实践

（例如不可变基础设施、临时工作负载和自动配置管理）可以显著降低这些风险，确保云环境安全、高效且具有弹性。

8.2.2 使用工厂创建安全的虚拟机镜像

创建和管理 VM 镜像对于保护 VM 环境至关重要。此过程涉及从头开始嵌入安全措施。因此，必须建立一套实践来简化 VM 镜像的创建并将安全性无缝集成到每一层。安全 VM 镜像创建的两个关键方面是镜像工厂和镜像源。

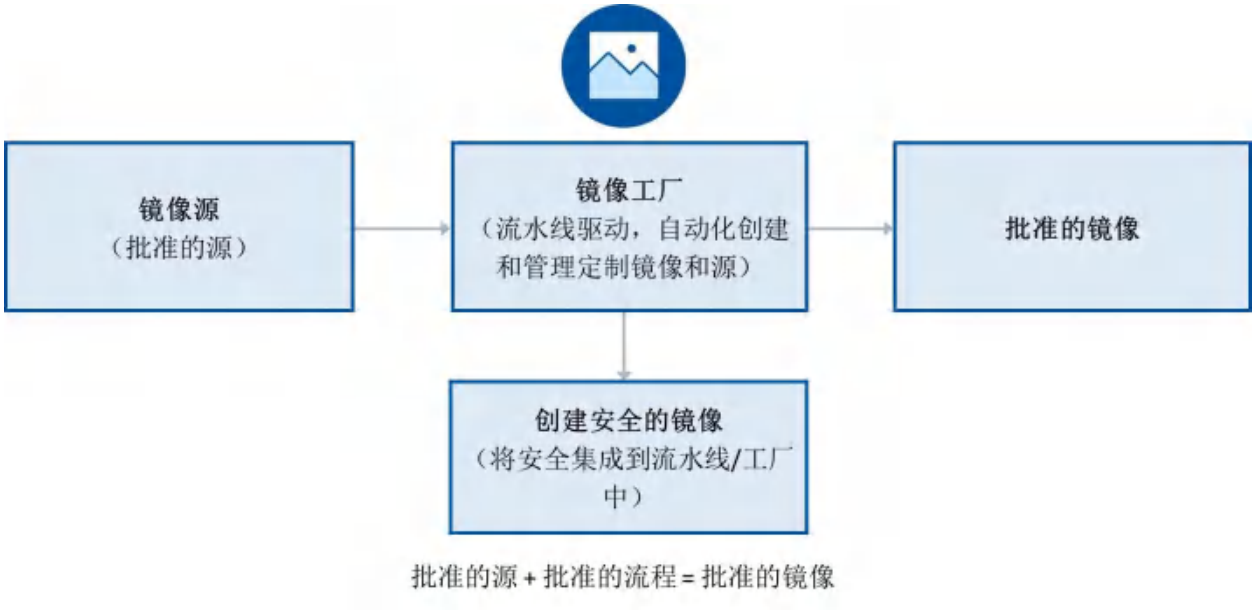


图 43：安全虚拟机镜像创建流程

镜像工厂是用于组装和自定义 VM 镜像的自动化流程和工具。将它们视为厨房，按照菜谱（使用镜像源）创建最终的 VM 镜像（餐点）。镜像工厂确保 VM 创建过程的一致性和可重复性，并高度重视安全性。

镜像工厂充当VM镜像的装配线，一致性、安全性和效率至关重要。这可以包括：

- 构建、测试和微调 VM 镜像以确保跨部署的一致性。
- 尽量减少可能导致安全漏洞的差异。
- 简化安全更新和配置变更的集成。

镜像来源是构建 VM 镜像的起点。它们提供操作系统、应用程序、库和配置文件等核心组件。可以将它们视为 VM 配方的配料。

Image Sources专注于精心管理和维护构成VM镜像的组件，其中包括：

● 保存创建 VM 镜像所必需的源代码和设置库。

● 在构建过程中纳入安全检查。

● 保留全面的版本历史记录，以便在出现问题时轻松回滚。

安全VM镜像创建包含一系列最佳实践，旨在通过以下方式增强VM镜像的安全态势：

● **最小特权：**为了最大限度地减少潜在的漏洞，请仅使用必要的软件和访问权限来设置 VM 镜像。

● **补丁管理：**定期使用最新的安全改进更新 VM 镜像，以防范新的威胁。

● **配置管理：**使用标准化的模板和脚本确保所有 VM 镜像都符合所需的安全标准，从而自动化镜像创建工作流程并减少手动错误。

● **验证和测试：**在使用VM 镜像之前，请彻底检查其是否存在安全漏洞和操作问题，以确保其安全且正常运行镜像 VM 镜像必须始终来自可信来源。

● **使用黄金镜像：**创建“黄金”镜像，这是一个原始的、最小的 VM 镜像，仅包含必要的操作系统和配置设置。此镜像可以作为所有其他 VM 镜像的基础，从而提高一致性并减少蔓延。

总而言之，保护虚拟机镜像就是创建一个一致且可重复的过程，将安全性嵌入到虚拟机的构建中，确保在启动新的虚拟机时，它们已经具备抵御网络威胁的能力。

8.2.2.1 虚拟机的推荐工具和最佳实践

利用正确的工具对于任何漏洞管理计划的成功都至关重要。这些工具提供专门的功能，可满足虚拟机安全的各种需求：

● **云工作负载保护平台 (CWPP)**通常包括跨云工作负载（虚拟机、容器、无服务器）进行深入漏洞扫描的功能，并根据可利用性和业务影响对调查结果进行优先排序。

● **传统漏洞扫描程序**在云端往往不那么有效，但是许多漏洞扫描器现在也支持代理。这些产品可能会更名为 CWPP，具体取决于产品。

● **配置管理工具**自动化补丁部署和配置强化。

● **端点检测和响应 (EDR)**代理执行运行时监控和一些支持漏洞评估。

● **安全信息和事件管理 (SIEM)**进行实时监控和报告。

以下漏洞管理生命周期代表了处理虚拟机漏洞的系统方法，从发现到解决。在云中，此周期

应扩展到涵盖镜像和修补的替代方案，例如用更新的镜像替换正在运行的虚拟机（不变性背后的概念）。该周期包括：

- **识别：**使用自动化工具扫描虚拟机以查找已知漏洞。
- **评估：**分析和评估与已识别漏洞相关的风险，考虑虚拟机的角色以及处理/存储的数据分类，例如数据敏感性。
- **缓解与报告：**应用补丁、配置安全设置并采用变通方法来修复漏洞。
- **文档：**保留漏洞、评估、补救措施的详细记录，以供报告、合规和审计。

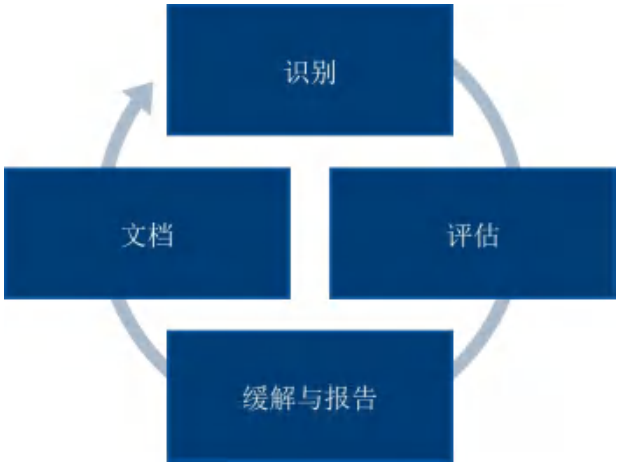


图 44：虚拟机的漏洞管理生命周期

通过将这些策略、工具和实践整合到安全框架中，组织可以显著增强对其虚拟机环境的保护，以抵御当代网络安全环境中威胁数字资产的众多漏洞。

8.2.3 使用部署流水线创建安全镜像

通过部署流水线创建安全镜像（可在镜像工厂内完成）是一个结构化过程，可确保虚拟环境以安全性为核心构建。此方法符合 DevSecOps 原则，将安全性作为开发生命周期的基本组成部分。创建安全镜像不是单一操作，而是部署流水线内一系列精心策划的步骤。

下图说明了安全镜像部署流水线流程，展示了从源代码到生产部署的每个步骤，集成了整个开发生命周期中的安全措施。

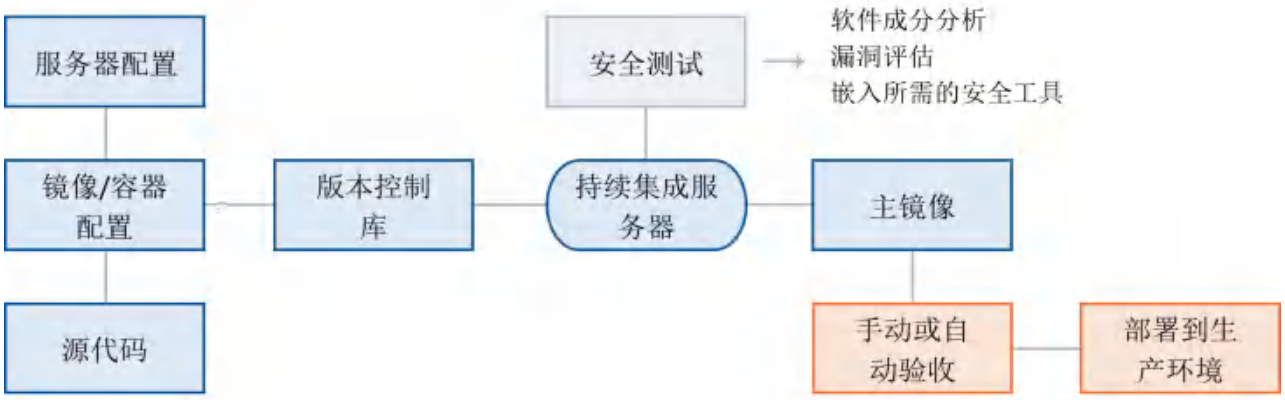


图 45：安全镜像部署流水线流程

步骤如下：

1. **源代码：**任何潜在的源代码都需要在镜像上进行编译和安装。

2. **服务器配置：**安全镜像的基础始于明确定义的服务器配置。利用 IaC，此步骤涉及指定操作系统、网络设置和安全策略，这些将构成服务器环境的基线。

3. **镜像配置：**焦点转移到镜像或容器。此阶段涉及根据预定义的服务器设置，以精简且安全的配置打包应用程序及其依赖项。

4. **版本控制存储库：**镜像配置文件的旅程在它们被签入版本控制系统时继续。使用 Git 存储库或容器注册表等工具，这种做法有助于构建过程中的变更跟踪、协作和问责。

5. **持续集成服务器：**自动化是这里的核心。持续集成服务或服务器从配置文件构建镜像，并在每次提交变更时执行安全检查。

6. **安全测试和执行：**在这里，安全测试成为流水线的集成组件。借助 SCA 和漏洞扫描工具，流水线可以识别和纠正安全问题，在问题扩散之前强化镜像。

7. **主镜像：**一个安全的主镜像就诞生了。这个过程的最终结果是生成一个经过强化、经过审查的主镜像，该镜像被安全存储并准备部署。

8. **手动或自动接受：**此时，镜像将接受严格检查。根据其风险和关键性，它可能通过人工审核或自动验收测试。

9. **部署到生产环境：**主镜像位于生产环境中。镜像向生产的过渡是一致的、安全的，并且使用 IaC和自动化工具进行精确部署。

通过将这些步骤嵌入到实践中，组织可以放心地部署经过仔细审查并针对数字世界的威胁做

好准备的安全镜像。这种方法可以最大限度地减少漏洞，并确保安全性与部署速度保持同步，并在整个环境中有效扩展。随着我们深入研究数据安全，这些实践构成了保护信息和维护云中强大防御的基石。

8.2.4 快照和公开曝光/泄露

快照对于管理虚拟机生命周期至关重要，可提供存储卷的近乎即时的副本以供保存和恢复。快照是虚拟机在特定时刻的保存状态，就像工作区的详细照片一样，可捕获从文件到设置的所有内容。这还包括敏感数据。因此，快照需要谨慎处理，以防止未经授权的访问、无意泄露和数据泄露。

减少公开曝光

虽然快照功能十分有用，但其全面性也带来了风险，尤其是在包含敏感数据时。制定严格的访问控制来管理谁可以创建或检索快照至关重要。想象一下，这些控制相当于一把万能钥匙——只有值得信赖的人员才能拥有这种权限。

快照加密增加了一层必要的安全保护，就像密码一样，可以让非预期的收件人无法读取秘密信息。如果快照无意中公开，加密数据仍将受到保护，没有相应的解密密钥则无法访问。

防止数据泄露

维护快照还涉及定期审查，例如销毁不再需要的敏感文件。此过程通过消除不必要的数据存储来增强安全性并优化云资源消耗。

云安全态势管理(CSPM)等监控工具可充当快照的警卫，仔细检查谁访问或修改了快照。对异常活动实施警报相当于将监控摄像头对准脆弱点，确保快速检测并处理未经授权的尝试。

快照必须具有与其所代表的运行态系统相同的安全级别。由于它们在创建时封装了虚拟机的所有数据和配置，因此如果管理不善，它们可能成为数据泄露的潜在载体。全面的快照安全方法不仅仅是保护数据，还包括确保这些快照不会带来风险或责任。

8.3 容器安全

本节深入探讨了构建安全容器镜像、高效安全地编排容器以及管理容器化环境中出现的无数安全挑战的重要性。它提供了有关保护容器生命周期每个步骤的全面见解，从创建容器镜像到使用 Kubernetes 等系统编排其部署。

8.3.1 容器镜像创建

容器镜像是一种轻量级、独立且可执行的软件包，其中包含运行应用程序所需的一切：代码、运行时、系统工具、库和设置。容器镜像是根据一组指令创建的，这些指令通常在 Dockerfile 中定义，指定基础操作系统、依赖项和应用程序代码。这些镜像可以轻松在不同环境中共享和部署，从而确保应用程序的一致性和可移植性。

容器需要使用安全、经过批准的基础镜像来构建。可以使用评估指令（Dockerfile）的工具添加和评估额外的安全性。确保容器的安全性也很重要。工件存储库，这是容器镜像的注册和存储的地方。

容器本身就支持了不可变基础设施的概念。容器镜像一旦构建并部署，就无法修改；更新和变更是通过用新镜像替换容器来进行的。这相当于用新部件替换机器中出现故障的部件，而不是修理它。

8.3.2 容器网络

容器网络是主机操作系统（通常是 Linux）网络的扩展。

Kubernetes 网络以及网络隔离发生在多个层面，从单个容器到应用程序感知负载均衡器（例如 Ingress Controller）。存在各种用于定义网络策略的技术。同样，其中一些可能是提供商提供的，但也可以是自我管理的。

8.3.3 容器编排与管理系统

容器编排系统已成为管理容器化应用程序复杂生命周期的重要工具。Kubernetes (K8s) 是这些系统中领先的开源平台，因为它具有灵活性和全面的功能集。Kubernetes 协调跨机器集群部署

在容器中的应用程序的部署、扩展和管理，实现无缝自动化和一致操作。容器托管微服务（应用程序组件）并确保组件在一致的环境中运行。

主要的CSP已经采用并调整了Kubernetes，提供针对其云环境的定制版本（例如，亚马逊的EKS、微软的Azure Kubernetes Service、谷歌的GKE）。这些服务在标准 Kubernetes的强大基础上添加了专有功能，为用户提供了熟悉度和提供商特定增强功能的结合。

在使用开源Kubernetes时，务必谨慎使用默认设置，因为它们可能不安全或与您期望的安全态势不一致。这些默认设置可能包括：

- 开放式仪表板，如果没有得到妥善保护，可能会无意中泄露有价值的信息
- 具有广泛权限的默认服务帐户可能会授予不必要的访问权限
- 网络配置未能满足特定部署的严格安全要求

该图展示了一个基本的Kubernetes 架构，其中包含核心管理组件、两个运行容器的“pod”以及用户通过其访问已部署应用程序的负载均衡器。

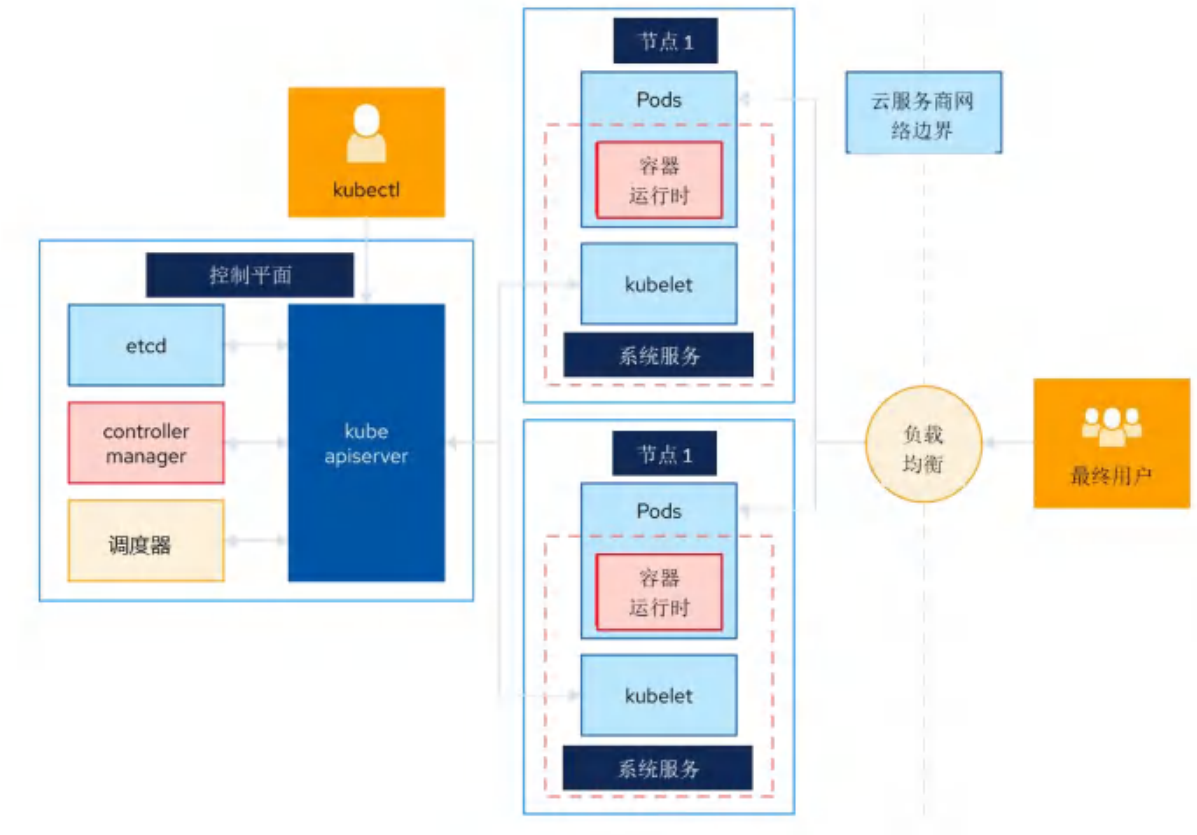


图 46：带有负载均衡器和 Pod 的基本 Kubernetes 设置

8.3.4 容器编排安全

Kubernetes等容器编排平台已成为管理云中容器化工作负载的必备工具。然而，保护这些复杂平台可能颇具挑战性。Kubernetes由多个组件、应用程序编程接口(API)和网络接口组成，如果配置和强化不当，攻击者可能会将其作为攻击目标。配置错误、未修补的漏洞和过于宽松的访问控制可能会导致容器环境遭到破坏和入侵。

最佳实践包括：

● **使用 CSP 服务：**部署容器化应用程序时，最好利用CSP 服务（如果可用）。CSP 通常提供一套旨在实现自动化和增强安全性的工具。这些工具可能包括用于编排的托管服务（如 Kubernetes-as-a- Service），这些服务带有以安全性为重点且符合合规要求的默认配置。

● **强化服务：**服务强化是一种主动方法，可最大限度地减少系统的攻击面。这包括通过禁用不必要的功能来保护编排器，确保最低特权访问，以及实施限制容器之间流量的网络策略和防火墙。强化还应包括使用容器的安全基础镜像，在 Kubernetes 中使用安全上下文设置，以及利用所谓的“准入控制器”来实施良好的安全实践。

● **修补程序/更新：**定期修补和更新容器生态系统中的所有组件至关重要。这不仅包括容器本身，还包括主机、Kubernetes 等编排平台和其他支持服务。补丁管理流程的自动化有助于确保补丁一经发布便立即应用，从而降低漏洞被利用的风险。

● **容器安全策略：**使用 Kubernetes 安全策略、PodSecurityPolicy 和网络策略等工具定义和实施安全策略，以限制和监控 Pod 之间的网络访问。

● **利用安全基准和工具：**标准和标准化工具，例如 CIS 基准 134 对于 Kubernetes，提供一种结构化的方法来检测和纠正不安全的默认值。

● **安全镜像存储库：**安全的镜像存储库是容器安全的核心。使用具有基于角色的访问控制(RBAC) 的私有存储库来管理谁可以推送和拉取镜像。在部署前和生产过程中定期对容器镜像实施扫描和漏洞检测。利用镜像签名建立信任链，以验证镜像从创建到部署期间未被篡改。

● **安全配置：**为了确保容器化环境的完整性和安全性，从强大而安全的配置开始至关重要。这些基础设置涵盖了容器环境的各个方面，是提供安全环境不可或缺的一部分。

○ 集群主机：通过强化主机的操作系统、维护最小安装以及确保主机级安全控制到位来保护集群资源。

○ 存储层：对静态和传输中的数据应用加密，使用访问控制列表 (ACL)或策略来限制对持久卷的访问，并使用日志记录来监控对敏感数据的访问。

○ 网络层：实施网络分段和防火墙来控制服务之间的流量。使用网络策略来强制执行容器之间以及容器与外部网络之间通信的规则。

镜像验证/签名：在 CI/CD 流水线中加入步骤来验证和签名镜像。这可能涉及使用检查已知漏洞的工具，并确保编排器只运行由受信任的机构签名的镜像。

8.3.4.1 安全工件存储库

安全工件存储库充当软件组件（包括容器镜像）的保险库，确保：

● 存储库强制执行数字签名和验证等内容信任机制，以保证容器镜像的真实性和完整性。

● 访问受到严格控制，只允许经过验证的用户推送或拉取镜像，就像银行只允许经过验证的客户进行交易一样。

● 定期对镜像进行扫描以查找漏洞，类似于定期进行健康检查以尽早发现疾病迹象。

● 容器镜像应该是不可变的。

● 镜像的出处得到了彻底的记录和保护，提供了其来源和制作者的清晰信息，类似于保存完好的公共登记处。

● 安全工件存储库与持续集成和部署流水线无缝集成，以在部署之前自动扫描和验证容器镜像。

8.3.4.2 使用安全存储库的最佳实践

保护工件存储库需要采取切实可行的做法，这些做法反映了更广泛的网络安全原则，例如以下原则。

● **仅启用安全源：**就像人们会避免为重要机械使用来源不明的可疑备件一样，开发人员应该只使用来自安全可靠来源的镜像。

● **签名并验证镜像：**数字签名可作为真实性的印章，确认镜像的真实性且未被篡改，类似于历史上信件上的蜡封。

● **扫描漏洞：**在部署之前，镜像应该经过彻底的漏洞扫描，这可以比作对飞机进行全面的飞行前检查。

● **访问控制：**限制存储库访问可确保只有具有合法需要的人才能检索或变更镜像，就像在安全设施中访问敏感信息一样。

● **审计跟踪：**详细记录谁访问或修改了存储库内容至关重要。这提供了透明度并有助于合规性，就像航海日志记录船上发生的事件一样。

● **定期更新：**不断更新和修补存储库软件，以防止已知漏洞并维护存储镜像的安全环境。

保护容器镜像是一项建立坚实基础、执行严格流程、确保完整性和细致记录的工作。通过在容器镜像生命周期的每个阶段嵌入安全性，组织可以加强其容器化应用程序以抵御威胁并满足合规性要求。

8.3.5 管理容器漏洞

保护现代软件部署流程涉及管理容器漏洞。与任何技术一样，容器也存在一系列独特的潜在安全问题，需要系统管理。

以下是管理容器漏洞时的一些关键注意事项：

● **CI/CD 流水线集成：**将漏洞管理工具集成到 CI/CD 流水线中，就像在生产线中嵌入严格的质量保证流程。这种集成可确保容器在开发和部署的每个阶段都经过彻底的安全检查，就像每个产品组件在下线前都要经过的细致检查一样。

● **定期更新：**必须保持容器镜像及其依赖项为最新。

● **不可变容器：**容器管理中的不变性原则是一种重要的防御策略。一旦部署了容器，它就不会被改变；任何必要的更新都会导致部署新的容器。这种方法就像在机器中使用可替换的零件来确保最佳性能，而不是进行临时修复。

● **安全策略执行：**实施和执行安全策略，规定使用预先扫描和批准的镜像进行部署，可以创建一个安全基线，类似于门禁，确保只有经过验证的客人才能进入场地。

● **基于角色的访问控制 (RBAC)：**RBAC 规范对容器管理工具和资源的访问。它保证团队成员只被授予履行其职责所需的访问权限 — 不多也不少。这类似于为安全设施内的不同区域发放不同的钥匙，根据每个人的职责限制访问权限。

● **基于属性的访问控制（ABAC)：**ABAC 提供了一种更精细的方法，特别适合容器化环境，因为容器化环境具有固有的灵活性和动态特性。使用ABAC，除了角色之外，访问决策还考虑属性。这些属性可以包括用户位置、设备类型、存储在容器内的数据分类（例如敏感、公开）信息或其他相关特征。这允许在容器化云环境中实现更灵活和动态的访问控制。

将这些实践嵌入容器的生命周期（从开发开始到部署乃至更远）有助于创建强化的工作流程。它支持了这样一种观点，即安全性不仅仅是事后的想法，而是流程不可或缺的一部分。此外，通过实施RBAC，组织可以维护安全高效的工作流程，同时确保合适的人员始终拥有适当的访问权限。

8.3.6 容器的运行时保护

容器的运行时保护可确保在潜在威胁或故障发生时检测并管理它们，从而保证容器化应用程序的安全并顺利运行。

容器的运行时保护有几个重要方面：

● **实时可见性：**有效的运行时保护始于实时可见性。监控工具就像一双警惕的眼睛，不断观察容器活动，扫描任何可能表明存在安全威胁或操作异常的异常行为。

● **日志记录和审计：**细致的日志记录和审计可以创建容器活动和用户交互的详细日志。日志记录对于事后分析非常有价值，其作用与犯罪调查中的安全摄像机镜头相同。

● **微隔离：**为了最大限度地减少入侵的影响，网络分段被实施，为容器创建隔离隔间，类似于船的防水部分。一旦发生入侵，威胁就会被控制住。

● **容器专用防火墙：**这些防火墙充当流量调节器，建立并执行规则来管理网络流量。它们类似于战略性放置的检查站，控制车辆进出，确保秩序和安全。

● **自动恢复：**最后一个方面是自动响应能力。当检测到威胁时，此紧急协议会立即生效，隔离受感染的容器、拒绝访问或将系统恢复到已知的良好状态，就像无需人工干预即可对入侵做出反应的自动防御系统一样。

运行时保护是需要保持持续警惕的，创建一个强大而响应的系统，监视容器并通过主动和被

动的安全措施快速消除任何威胁，确保容器化应用程序在整个生命周期内的完整性和弹性。

8.4 PaaS 安全

CSP 提供的 PaaS 通常包括替代工作负载组件的服务（例如，消息队列服务取代了服务器上对排队软件的需求）和用于运行工作负载本身的支持性托管平台（如容器）。PaaS 服务自动化和编排虚拟机上的标准软件堆栈并不罕见，例如 SQL Server 或 Oracle 的数据库服务，用于管理底层虚拟机，因此客户只需管理配置设置及其数据库。

换句话说，PaaS 涵盖了非常广泛的选项，从自动化和协调常见软件平台的服务，到托管任意工作负载（如容器或无服务器功能）的服务，再到完全抽象功能（如消息队列）的服务，而客户永远不知道底层运行着什么。

8.4.1 PaaS 的通用安全实践

PaaS 的安全性取决于多层方法，将一般安全实践与针对独特 PaaS 环境组件量身定制的特定措施相结合：

- **安全审计：**定期对 PaaS 组件进行漏洞评估或健康检查对于识别和缓解潜在的安全威胁至关重要。应定期进行这些审核，以适应 PaaS 环境中不断变化的威胁和变化。
- **日志记录和监控：**有效的安全取决于可见性。在 PaaS 平台内实施全面的日志记录和实时活动监控，可以尽早发现可疑行为或潜在违规行为，从而促进快速响应和缓解措施。
- **最小特权：**遵守最小权限原则可最大限度地降低未经授权访问或数据泄露的风险。组织可以通过仅授予用户和服务其角色所需的最低访问级别来显著减少其攻击面。
- **多因子身份认证(MFA)：**使用MFA 加强访问控制可增加一层安全性，使攻击者更难获得未经授权的访问权限。这种方法类似于银行要求同时使用卡和 PIN 进行交易，从而增强了敏感操作的安全性。

访问评审：定期重新评审访问权限可确保只有适当的个人和服务才能访问关键资源。此过程有助于及时撤销不再需要的访问权限，从而进一步加强安全态势。

8.4.2 加密和访问控制

在 PaaS 安全中，管理身份、加密数据和控制访问构成了稳固安全态势的支柱。本节探讨了加密和访问控制在保护 PaaS 环境中所起的重要作用。

加密：通过强大的加密方法保护静态和传输中的数据就像将贵重物品放在保险箱中并提供安全的传输一样。精心管理加密密钥可确保只有授权实体才能访问加密数据。

访问控制：

- **网络分段和防火墙：**实施网络分段和部署防火墙有助于在 PaaS 环境中创建安全区域，控制流量并减少违规的潜在影响。
- **RBAC：**系统根据特定角色分配访问权限，确保个人或服务只能访问其分配功能所需的资源。
- **ABAC：**根据属性分配访问权限，从而允许在云环境中做出更灵活、动态的访问决策。
- **API 网关策略：**API 网关的严格策略控制外部实体如何与 PaaS 交互，类似于俱乐部的保镖管理入口。这些实践意味着为 PaaS 环境构建多层防御策略，以确保它们尽可能地抵御各种安全威胁。

8.4.3 保护特定 PaaS

除了一般的安全措施外，某些 PaaS 平台由于其独特的漏洞而需要专门的保护策略。本节重点介绍保护特定PaaS，例如 CDN、通知服务和消息队列，每种 PaaS 都需要量身定制的安全措施来防范威胁。

- **内容分发网络 (CDN)：**通过 CDN 传输的数据采用安全套接字层 (SSL) 或传输层安全 (TLS) 加密，确保信息保持机密且不会被变更。强大的访问控制和身份验证机制可限制对存储内容的访问。
- **通知服务：**加密通知并使用安全的交付渠道可以保护其中的信息，就像通过受信任的快递员发送敏感文件一样。强大的身份验证方法可以验证有权发送通知的服务和用户的合法性。
- **消息队列：**静态和传输中的消息加密以及安全访问策略和 RBAC 可保护消息队列中的敏感数据。这可确保只有授权实体才能发布或订阅队列，从而保持通信完整性。

必须了解的是，每个 PaaS 组件都有独特的漏洞，需要量身定制的安全措施来保护数据完整性、确保隐私并维持可靠的服务运营。PaaS 的安全性要求采取认真、详细的方法来解决一般和

特定于服务的漏洞。通过实施这些策略，组织可以针对各种安全威胁建立弹性防御，确保其基于云的应用程序和服务的完整性、隐私性和可靠性。

8.5 保护无服务器或函数即服务

无服务器计算，通常也称为函数即服务 (FaaS)，是一种让开发人员编写和部署代码而无需处理底层基础架构的方式。云提供商负责管理服务器，包括配置服务器、扩展服务器以处理不同的负载以及维护服务器。这样一来， 开发人员就可以专注于编码，而不必担心服务器管理的底层工作。

“无服务器”一词有点用词不当，因为服务器仍用于运行应用程序。但是，管理这些服务器并不由应用程序所有者负责。相反，它被CSP抽离了。这种从传统上关注基础设施的转变意味着开发人员只需为他们使用的计算能力付费，通常精确到代码执行的毫秒数。

无服务器计算的主要优势在于其操作简单性。开发人员提供代码，云提供商负责其余工作，包括系统维护和可扩展性等所有操作方面。系统会根据应用程序的需求自动调整计算资源，为希望快速构建和扩展应用程序且开销最小的开发人员提供高度灵活且高效的解决方案。

无服务器中的每个函数通常在轻量级、一次性容器中执行，该容器驻留在一次性虚拟机上。此方法可确保每个函数调用都在明显隔离的环境中运行，从而实现强隔离并防止函数之间的任何干扰。这些执行环境的短暂性大大减少了攻击面，因为没有持久的操作系统需要管理，从而最大限度地降低了潜在的安全风险。此外，此模型通过确保每个函数的执行都是隔离的和瞬时的，从而增强了安全性。

尽管如此，开发人员必须记住，尽管云提供商承担了许多安全责任，但他们仍然必须保护其应用程序代码，有效地管理访问控制，并保护敏感数据。

函数之间相互传输数据。通过正确利用 FaaS，开发人员可以专注于编码，同时依靠云提供商来管理基础设施安全，从而使 FaaS 成为一种安全且可扩展的选项，可以降低操作复杂性并执行应用程序逻辑。

下图说明了FaaS模型中函数、容器、虚拟机的关系：

- 最里面的圆圈代表单独的函数，其中包含应用程序代码。

● 该函数被封装在一个容器内，容器提供了必要的运行环境和依赖项。

● 然后，容器在 CSP 管理的虚拟机上执行。

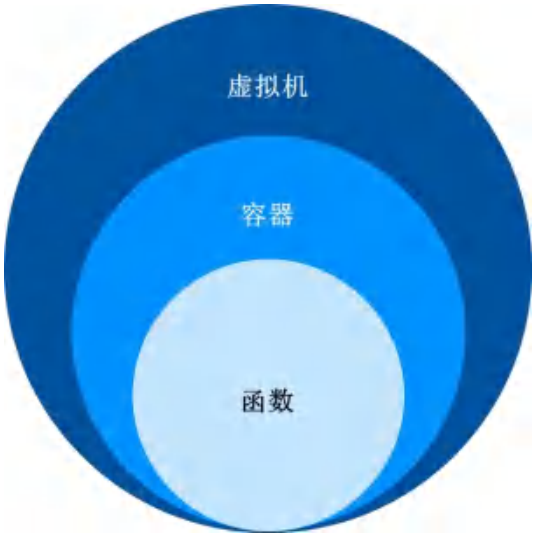


图 47：函数即服务（FaaS）范式

8.5.1 FaaS 安全问题

谈到无服务器计算，需要注意一些常见的安全问题。

● **第三方服务和 API：**造成攻击的可能性。如果这些接口被攻破，攻击者可能会授予它们进行未经授权的配置或监视云环境的权力。

● **易受攻击的依赖项：**无服务器函数通常依赖于外部库，而这些库可能隐藏漏洞或恶意代码。如果不严格检查和更新这些依赖项，它们可能会成为攻击者的后门。

● **配置错误：**不正确或过于宽松的配置可能会无意中打开对无服务器架构内敏感资源的访问权限。必须严格控制与谁可以执行功能以及这些功能可以访问哪些内容相关的安全设置，以限制操作。

● **某个功能的权限过高的 IAM：**当函数被授予过多权限时，会大大增加未经授权访问和潜在数据泄露的风险。此类配置可以允许函数获得不必要的访问权限，从而使攻击者能够利用这些特权进行恶意攻击。

● **直接访问互联网可实现以下功能：**函数可能会在没有适当的网络控制（例如网络分段和 ACL）的情况下直接访问互联网。这种缺乏限制的情况不仅会使函数暴露于外部威胁，而且还会成为外部实体泄露数据的潜在渠道。

上述每个问题都强调了在无服务器模型中采取谨慎的安全实践的必要性，从审查第三方 API 到认真管理依赖项和配置。尽管无服务器模型在可扩展性和成本方面具有优势，但在这些方面保持警惕对于防范漏洞至关重要。此外，独特的无服务器环境会导致特定的安全考虑，而其他工作负载类型则不会出现这些问题。

以下是独特的无服务器安全注意事项：

● **无状态性质：**无服务器函数运行时不会保留内部状态，这极大地改变了安全方法。如果没有持久的服务器环境需要监控，那么人们的注意力就会转向代码本身及其各种依赖项的安全性。这种转变要求彻底了解代码的编写方式、它调用的库以及它处理的数据。开发人员必须确保他们的函数是独立的，并在执行环境中采取所有必要的安全措施。

● **事件驱动的安全性：**无服务器计算的事件驱动特性带来了独特的挑战。无服务器函数通常是响应事件

而执行的，这些事件可能包括用户请求或计划任务。此模型需要对事件进行严格验证，以防止恶意触发。精心设计和验证事件输入对于确保函数仅响应合法和预期的触发至关重要。确保这些事件的安全性涉及仔细检查事件源并在允许函数执行之前执行严格的验证检查。

● **对 CSP 的依赖：**在无服务器架构中，可用的安全措施通常由 CSP 的产品定义。这一限制意味着理解和利用责任共担模型是关键。虽然 CSP 保护云基础设施，但 CSC 必须专注于保护其代码和数据。了解提供商处理哪些安全方面以及哪些责任落在 CSC身上至关重要，例如身份和访问管理 (IAM)、代码安全、数据加密和策略实施。驾驭这种共享环境意味着要随时了解 CSP 的工具和服务并有效地集成它们。

有效地驾驭无服务器安全性需要适应一种模型，在这种模型中，服务器管理不受控制，但保护代码和执行环境的责任仍然存在。这种适应涉及依赖 CSP 的工具并严格遵循最佳配置、事件管理和依赖项安全实践。了解无状态、事件驱动触发器和责任共担模型的细微差别是构建安全的无服务器应用程序的关键。

8.5.2 无服务器的 IAM

IAM是确保无服务器架构安全的基石。由于无服务器应用程序可以跨域集成和与各种服务交互，因此管理信任和访问变得复杂。建立和维护严格的IAM实践以防止未经授权的访问和潜在的违规行为至关重要。

以下是无服务器架构的一些IAM最佳实践：

● **最小特权访问：**在无服务器计算中，必须实施最小特权原则。这意味着为函数提供运行所需的最低访问级别或权限。定期更新这些权限可确保函数没有不必要的访问权限，这可能会使敏感系统或数据面临威胁。

● **细粒度的访问控制：**除了基于预定义角色管理访问权限的 RBAC 之外，无服务器环境还受益于细粒度的访问控制。这种方法可以在单个功能或资源级别精确指定权限，确保最小特权访问并减少攻击面。

● **上下文感知授权：**无服务器架构适合情境感知授权，超越了传统的 RBAC。情境属性（例如用户身份、设备特征、访问时间和环境因素）可以动态影响访问决策。实施情境感知策略可通过根据实时情况调整访问控制来增强安全性。

● **不可变基础设施和密钥管理：**无服务器功能是无状态且短暂的。最佳实践包括利用 CSP 提供的密钥管理服务、定期轮换凭证以及采用不可变基础设施原则来降低凭证泄露的风险。

● **审查并更新 IAM 策略：**定期审查和更新 IAM 策略以确保权限符合当前要求也至关重要。随着无服务器应用程序的发展，其访问需求也在不断变化。定期审核这些策略可确保权限既不会过于宽松也不会过于严格，从而平衡运营效率和安全性。

对于希望保护其无服务器功能的团队，采用这些 IAM 最佳实践并关注新兴的行业解决方案，如每个人的安全生产身份框架 (SPIFFE) 或 SPIFFE 运行时环境 (SPIRE)136至关重要。这些解决方案创建了一个安全、可管理且可靠的无服务器环境，可以安全地跨多个平台和域进行扩展。

8.5.3 网络连接和访问模式

网络设计在无服务器架构的安全性中起着不可或缺的作用。在虚拟网络中隔离无服务器功能可降低未经授权访问的风险，从而增强安全性。可以建立细粒度的访问控制（例如 ACL）来定义谁或什么可以在什么条件下访问这些功能。

确保无服务器功能与其他服务之间的交互安全也至关重要。API 网关通常是传入请求的入口点，必须严格保护。除了确保 API 网关的稳健性之外，对传输中的数据进行加密也至关重要。尽管网络安全在很大程度上由 CSP 控制，但 CSC 必须配置保护应用层数据移动的安全设置。

8.5.4 环境变量和机密信息

在无服务器应用程序中处理敏感信息需要仔细考虑。环境变量应使用变量，而不是将密码或 API 密钥等机密信息硬编码到代码中。这些变量可以在运行时动态管理和注入，从而最大限度地减少敏感信息的泄露。

AWS Secrets Manager 或 Azure Key Vault 等云服务提供了可靠的机密信息管理机制，允许安全地存储、检索和轮换凭证。定期轮换这些机密信息可降低旧的、可能被盗用的凭证被利用的风险。此外，通过 IAM角色控制对这些机密信息的访问可确保只有授权实体才能检索或变更它们。

通过采用这些实践，可以构建一个无服务器环境，从而安全高效地管理网络连接和敏感数据。这有助于维护无服务器应用程序的完整性和机密性，遵守零信任安全模型，在该模型中，信任永远不会被假定，并且必须不断得到验证。

8.6 人工智能工作负载

人工智能站在技术进步的最前沿，改变了我们的生活、工作和互动方式。人工智能工作负载是指构建、交付或利用人工智能功能所涉及的任务、流程或操作。这些工作负载使机器能够从数据中学习、做出预测并在决策过程中模拟人类智能。从根据用户行为推荐产品到自动驾驶汽车，人工智能工作负载涵盖了广泛的复杂性和应用。

AI 工作负载的特点是其对数据的要求高、计算复杂度高。它们需要大量数据集进行模型训练，并需要强大的处理能力，利用图形处理单元 (GPU) 和张量处理单元 (TPU) 等专用硬件来提高效率。此外，这些工作负载必须动态扩展以适应不断变化的需求，这凸显了灵活计算资源（例如云环境提供的资源）的重要性。

AI工作负载的应用范围广泛且多种多样。它们通过自动化任务、增强客户体验以及提供前所未有的复杂问题洞察来重塑行业。随着 AI 技术的发展，理解和管理这些工作负载对于旨在充分利用 AI 潜力的组织来说至关重要。进入 AI 工作负载的旅程不仅要利用计算能力，还要驾驭数据、算法和

实时处理的复杂性，以释放各个行业的创新和价值。

8.6.1 人工智能系统威胁

由于入侵可能造成严重后果，因此人工智能基础设施的安全性是一个关键问题。该基础设施有多个组件，每个组件都面临独特的挑战，需要量身定制的安全措施。通过了解特定威胁并实施适当的缓解策略，可以确保人工智能系统的完整性、机密性和可用性。

以下是按类别分组的一些关键人工智能系统威胁：

数据安全威胁：

● 数据中毒：毒化数据涉及恶意引入虚假信息，导致模型输出不准确。

● 隐私泄露：未经授权访问敏感数据可能导致隐私侵犯和相关的法律问题。

● 数据泄露：模型输出可能会意外泄露训练数据，从而有泄露机密信息的风险。

模型安全威胁：

● 模型盗窃：未经授权复制机器学习模型。这使攻击者能够规避知识产权法，还可能揭示如何欺骗模型，从而加剧风险。

● 对抗性攻击：可以操纵输入来利用设计缺陷并导致错误的预测。

● 模型反转攻击：这些攻击可以从模型输出重建输入数据，威胁训练数据的机密性。

● 提示注入：恶意制作的输入可以利用人工智能模型漏洞触发意外操作或泄露敏感信息，类似于社会工程学诱骗个人危害安全的方式。

基础设施安全威胁：

● 越权存取：对人工智能基础设施的入侵可能导致数据盗窃、恶意变更或有害软件的部署。

● DDoS 攻击：过多的流量可能会造成服务中断。

● 硬件漏洞：针对 GPU 和 TPU 的漏洞可能包括旁道攻击，存在泄露敏感信息的风险。

供应链威胁：

● 软件依赖项：第三方库可能会引入漏洞或恶意代码。

● 第三方服务：依赖外部数据处理和存储服务可能会引入漏洞。

8.6.2 人工智能缓解策略

以下是一些按类别分组的关键 AI 系统迁移策略。

数据安全：

● 加密：在传输和存储过程中保护数据的机密性。

● 差分隐私（Differential Pivacy）：在数据或查询中引入随机性，这样单个记录就无法追溯到某个人。这就像在对话中添加噪音来掩盖私人细节。

● 安全多方计算（multi-party computation）：通过将敏感信息匿名化或标记化作为流程的一部分，处理来自多个来源的数据而不暴露敏感信息。

● 机密计算（Confidential computing）：使用可信执行环境 [138] 在处理过程中保护数据并保护 AI 模型的执行。

模型安全性：

● 模型强化：防御对抗性攻击以增强模型弹性。

● 稳健（鲁棒性）训练：采用技术来提高普遍性并减少过度拟合。

● 对抗训练：通过将操纵的示例纳入训练数据中来增强人工智能模型抵御攻击的能力，增强其弹性，就像战士学习对抗不同的动作一样。

● 模型水印：嵌入唯一标识符以声明所有权并阻止盗窃。

● 输出操作：改变人工智能的反应以掩盖其决策过程可以阻止潜在的窃贼，就像扑克玩家的虚张声势一样。

基础设施安全：

● GPU 和 TPU：为了维护系统完整性，请利用基于硬件的安全功能、定期固件更新和网络安全措施。

● 人工智能服务：遵循云服务的最佳实践，包括访问控制和实时监控。

● 配额和速率限制：应用配额和速率限制来识别和防止 DoS 和 DDoS 攻击。

供应链安全：

●策略：定义并批准供应链的网络安全策略。

●软件供应链风险管理：定期审核和更新第三方依赖项。

●审查第三方服务：集成之前进行安全评估。

●可靠来源：依靠信誉良好的来源获取软件依赖项，维护一份批准列表。

通过采用概述的策略主动应对这些威胁，组织可以加强其人工智能基础设施，以抵御当前和新出现的危险，确保其人工智能系统的弹性。

总结

云工作负载保护是一门不断发展的学科，旨在解决云环境的多样性和动态性所面临的独特安全挑战。传统的安全措施在云中已不够用；因此，需要专门的控制措施来有效保护各种工作负载。对于虚拟机来说，安全性始于镜像级别。虚拟机镜像安全自动化有助于在部署周期的早期嵌入保护措施。实施最小特权原则和优先进行定期漏洞评估等做法是保持对威胁的强大防御的基础。

在使用 Kubernetes 进行容器编排时，自定义配置以增强安全性至关重要。扫描容器镜像中的漏洞并控制谁有权访问和管理这些镜像是至关重要的做法。此外，实施运行时保护机制可确保持续监控容器并防御持续威胁。

无服务器应用程序需要采取有针对性的安全性方法，首先是严格的 IAM 策略。保护 API 端点免受未经授权的访问并严格管理机密是防止漏洞利用的关键。

AI工作负载安全领域发展速度特别快，需要不断学习。为了保护AI工作负载免受攻击，必须采用对抗性训练， 保护AI模型免受未经授权的访问或盗窃，并采用差分隐私等数据隐私技术。

对于 PaaS 环境，定期进行安全审核是识别和修复漏洞的必要条件。静态和传输中的数据加密，以及严格的IAM 控制和安全的通信渠道构成了基础云工作负载保护不是一刀切的解决方案，而是一种适应每种工作负载类型特征的定制方法。了解最新威胁和缓解策略对于维护安全的云生态系统至关重要。

建议

云工作负载管理

● 创建集中式云部署注册表：维护所有云工作负载和部署的综合清单，以便高效跟踪和管理。

● 使用多种部署定义组织层级结构：构建云环境以镜像组织单位，从而实现更好的安全性和管理控制。

● 支持创建新部署的低摩擦流程：简化流程以确保遵守安全策略而不影响运营效率。

虚拟机 (VM) 安全

● 强制使用安全的基本镜像 VM 镜像：对所有部署使用集中管理、版本控制和不可变的基本镜像。

● 实施镜像工厂：自动创建、测试和部署虚拟机镜像，以确保一致性和安全性。

● 扫描虚拟机镜像中的漏洞：定期扫描和更新虚拟机镜像以降低安全风险。

● 采用短期运行的虚拟机：使用不可变基础设施和临时虚拟机来降低与长时间运行实例相关的风险。

● 使用配置管理和基础设施即代码 (IaC)：维持所需状态并防止配置漂移。

● 实施基于主机的防火墙和 SSH 强化：控制网络访问并保护 VM 实例上的 SSH 配置。

容器编排安全

● 使用 CSP 服务进行编排：利用 Kubernetes-as-a-Service 等托管服务来增强安全性。

● 强化编排服务：禁用不必要的功能，确保最小特权访问，并实施网络策略和防火墙。

● 定期修补和更新：自动管理容器、主机和编排平台的补丁。

● 定义和执行安全策略：使用 Kubernetes 安全策略、PodSecurityPolicy 和网络策略等工具。

● 利用安全基准和工具：遵循 Kubernetes 的 CIS 基准以确保安全配置。

● 保护集群主机和存储：强化主机的操作系统，对静态和传输中的数据应用加密，并使用访问控制列表(ACL)。

监测与评估

● 利用 CSPM工具：使用云安全态势管理(CSPM)工具持续监控云安全态势。

● 实施持续监控：使用实时监控工具跟踪工作负载活动并快速检测潜在的安全事件。

● 使用 SCA工具：将软件组合分析(SCA)工具集成到 CI/CD 流水线中，以管理依赖关系并尽早识别漏洞。

● 生成和维护 SBOM：为所有工作负载创建软件物料清单(SBOM)，以增强透明度、安全响应和法规遵从性。

● 端点检测和响应(EDR)代理：执行运行时监控并支持漏洞评估。

● 安全信息和事件管理(SIEM)：提供实时监控和报告。

培训与意识

● 定期进行安全演习：进行基于场景的演习和桌面演练，帮助团队做好应对真实事件的准备。

● 鼓励公正文化：注重系统改进和问责，而不是为安全事件追究不当责任。

PaaS 安全

● 定期安全审计：进行漏洞评估以识别和减轻潜在威胁。

● 全面的日志记录和监控：实施日志记录和实时监控，以检测和应对可疑行为。

● 最小特权原则：仅授予用户和服务必要的最小访问级别。

● 多因素身份验证(MFA)：使用 MFA 增强访问控制。

● 定期访问审查：定期重新评估访问权限以确保适当的访问级别。

确保无服务器或函数即服务 (FaaS) 的安全

● 审查第三方服务和 API：确保它们安全可靠，以避免未经授权的配置或数据泄露。

● 管理易受攻击的依赖项：定期更新并检查外部库是否存在漏洞或恶意代码。

● 纠正错误配置：确保安全设置适当地限制功能的执行和访问。

● 限制功能的 IAM 权限：授予必要的最小权限，以降低未经授权的访问和数据泄露的风险。

● 控制直接互联网访问：实施网络分段和 ACL，以防止功能直接访问互联网。

人工智能缓解策略

● 数据安全：使用加密、差分隐私和安全多方计算来保护数据。

● 模型安全：加强模型以抵御对抗性攻击，使用强大的训练技术，并嵌入唯一标识符以阻止盗窃。

● 基础设施安全：实施配额和速率限制，并遵循云服务的最佳实践。

- 供应链安全：定义网络安全策略，定期审核第三方依赖关系并使用可信来源。

补充指南

- 云工业物联网 (IIoT) - 工业控制系统安全术语表 | CSA
- 实施安全微服务架构的最佳实践 | CSA
- 云对抗载体、漏洞和威胁 (CAVEaT™)：行业协作的新兴威胁矩阵 | CSA
- 集成 SDP 和 DNS：增强零信任策略实施 | CSA
- 医疗云中的勒索软件 | CSA
- 云安全复杂性 | CSA
- 无服务器应用程序面临的 12 个最关键风险 | CSA

领域 9：数据安全

云服务的快速扩展和适应以及网络威胁的日益复杂化要求采取弹性方法来保护信息。数据安全实践对于维护组织完整性、机密性和客户信任以及确保遵守监管要求至关重要。

本领域深入探讨云中数据安全的复杂性，探索组织可以采用的基本策略、工具和实践，以确保其数据在传输和存储时受到保护。从了解数据分类和云存储类型的细微差别到实施高级加密方法和访问控制，本部分提供了探索不断发展的数据安全领域时的指南。本领域也是云存储的入门书。此外，我们将探讨塑造云环境中未来数据保护的关键概念和技术，确保学员了解防止数据泄露和维护数据隐私所需的关键措施。

学习目标

该领域的学习目标旨在为读者提供以下方面的知识：

- 了解数据安全基础知识。
- 数据安全风险分析。
- 数据安全治理体系。
- 数据分类和状态。
- 云存储类型及其相关的安全措施。
- 数据安全技术，例如密钥管理。
- 保护各种类型的计算工作负载。
- 态势管理。
- 先进的数据安全概念。

9.1 数据分类与存储类型

根据数据类型、敏感度和关键性对数据进行分类，组织可以根据数据类型实施适当的安全方法。数据处理不当可能会导致数据泄露、违反合规要求以及数据丢失。从战略角度来看，理解和实施数据分类实践有助于组织保持运营和合规性战略一致。

随着组织需求和监管环境的发展，数据分类必须适应，确保数据治理计划有效并能对事件做出响应。此外，识别不同的数据状态（静止、移动和使用中）需要量身定制的安全措施。除此之外，了解各种云存储类型，例如对象存储、卷存储、数据库存储、软件即服务(SaaS)存储和 PaaS 特定存储，使组织能够根据其特定数据需求和安全要求选择最合适的解决方案。

9.1.1 数据分类

数据分类是一个至关重要的持续过程，涉及根据类型、敏感度、关键性和潜在暴露影响对数据进行分类，同时考虑运营和合规性观点。将数据分类流程纳入组织的数据治理实践对于保护整个数据生命周期至关重要。它可以清晰地划分资产保护优先级。从本质上讲，数据分类为运营安全和合规策略提供信息。

随着组织的发展，运营环境也随之变化，新的法律法规也影响着组织运营的要求。将强大的数据分类策略与明确的资产和数据所有权分配相结合，可使组织能够快速响应事件并成功推动各种数据治理计划。

图 48：数据分类尺度

9.1.2 数据状态

在云安全方面，必须认识到数据会不断在不同状态之间转换，每种状态都需要特定的安全措施。本讨论重点介绍了三种主要数据状态：静态数据（存储中）、动态数据和使用中数据。

静态数据：指以各种形式保存在云环境中的数据。这包括卷中保存的数据，例如虚拟磁盘、对象存储中的文件、数据库、以及平台即服务(PaaS)产品。存储数据的有效安全措施通常包括加密、建立访问控制和维护定期备份以保障数据完整性。

动态数据：指在不同位置之间主动传输或转移的数据。这种移动发生在内部网络、互联网或物理介质（例如 USB 驱动器或外部硬盘驱动器）中。为了保护移动数据的安全，使用加密协议、安全通信通道并确保数据传输过程中的完整性和机密性至关重要。

正在使用的数据：是当前正在由应用程序或服务处理、操纵或交互的数据。这包括应用程序使用的数据、参与 AI 训练和推理的数据或正在进行分析处理的数据。正在使用的数据的安全措施包括实施严格的访问控制、监控用户活动以及在数据处理过程中保护数据的完整性和机密性。

至关重要的是要明白，必须在各个层面和状态下维护数据安全。随着数据在存储、移动和使用之间转换，定制的安全措施对于在整个生命周期内保护数据至关重要。通过了解数据的不同状态并在每个阶段应用有针对性的安全控制，组织可以采用全面的云安全方法，从而保护其敏感数据免遭未经授权的访问、变更或泄露。

9.1.3 云存储类型

了解不同类型的云存储有助于确定最适合特定数据需求的存储解决方案。

不同类型的云存储包括：

- 大量非结构化数据的对象存储
- 类似于虚拟硬盘的低延迟访问卷存储
- 用于管理关系数据和非关系数据的数据库存储
- PaaS 和 SaaS 环境中使用的其他专用存储类型

每个类别都有独特的特点、用例和来自领先云提供商的产品。

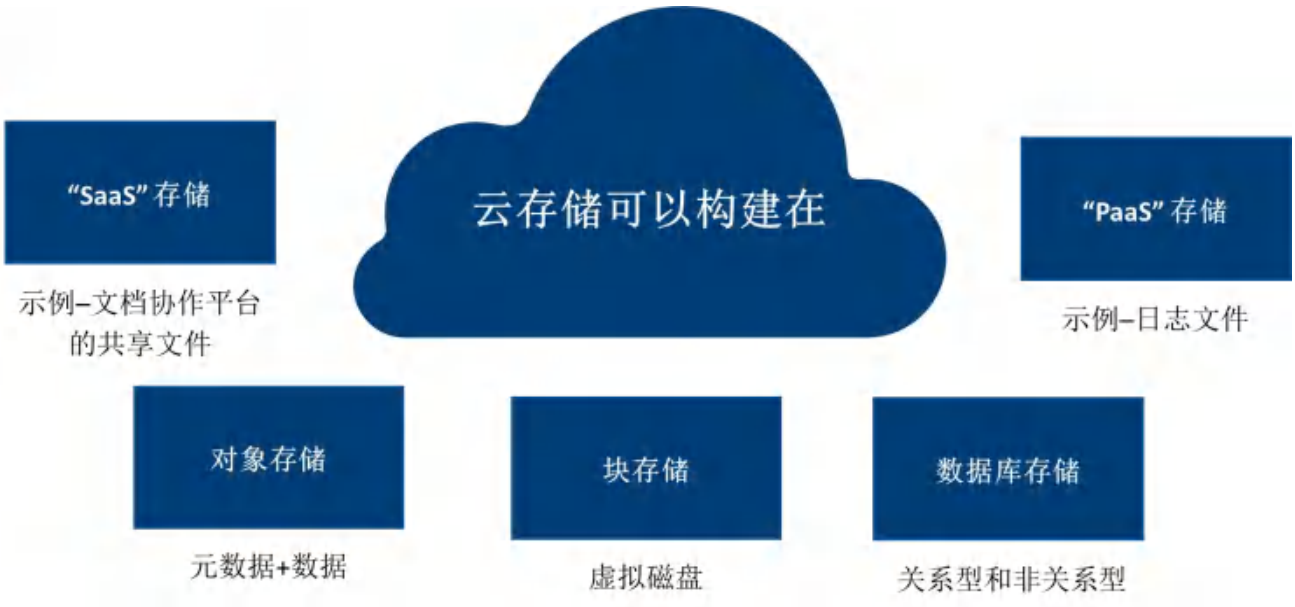


图 49：云存储解决方案的类型

9.1.3.1 对象存储

对象存储旨在存储和检索大量非结构化数据，例如文档、图像、视频和备份。它提供了一个简单的应用程序编程接口(API)，用于存储和访问由唯一键标识的对象。对象存储具有高度可扩展性和耐用性，适用于备份、存档和提供静态网站内容等各种用例。这些类型的存储被归类为基础设施即服务(IaaS)服务，因为云提供商提供了存储基础设施。对象存储服务的示例包括 AmazonS3、GoogleCloudStorage 和 AzureBlobStorage。

9.1.3.2 卷存储

卷存储提供可连接到云中虚拟机的虚拟硬盘。它允许您以类似于传统硬盘的方式存储和访问数据。卷存储通常用于操作系统文件、应用程序数据和其他需要低延迟访问的持久数据。虽然它们的用途与对象存储不同，但此类存储也被视为 IaaS 服务。云提供商提供不同类型的卷存储，例如 AmazonElasticBlockStore(EBS)、GooglePersistentDisk 和 AzureManagedDisks，具有不同的性能特征和定价选项。

9.1.3.3 数据库存储

这包括关系数据库和非关系数据库。云提供商为关系数据库提供托管服务，例如 Amazon Relational Database Service、Google Cloud Structured Query Language(SQL)、Microsoft Azure SQL Database 和 Oracle Database 服务。这些服务提供熟悉的数据库引擎，例如 MySQL、Oracle、PostgreSQL 和 SQLServer。非关系型数据库（也称为 NoSQL 数据库）专为可扩展性和灵活性而设计。示例包括 Amazon DynamoDB、Google CloudDatastore、Oracle NoSQLCloudDB 和 Azure CosmosDB。这些数据库具有高度可扩展性，可以处理大量非结构化数据。

9.1.3.4 其他类型的存储

PaaS 存储是指云平台的各种服务特定存储选项。这些选项包括日志记录服务（例如 Amazon Cloud Watch、Google CloudLogging、Oracle Events 和 Azure Monitor），用于存储和分析来自应用程序和基础设施的日志数据。消息队列支持分布式应用程序组件（例如 Amazon SimpleQueueService(SQS)、Google CloudPub/Sub 和 Azure QueueStorage）之间的可靠通信。Oracle CloudInfrastructure(OCI)Streaming 和其他 PaaS 存储服务可能包括缓存、内存数据库等。云存储也可以作为软件即服务(SaaS)提供，例如 Google Drive、Dropbox、Microsoft OneDrive、Box 等。这些服务使用户能够安全地访问和共享文件和资源，从而实现通过 Internet 的稳健协作。

9.2 保护特定云工作负载类型

每种云工作负载都有其独特的安全需求和挑战。需要不同的工具和技术来有效地解决这些差异。本节探讨了构成保护云中数据存储核心的基本数据安全工具。这些包括用于管理访问的 IAM（身份和访问管理）系统、用于定义权限和网络规则的访问策略，以及用于保护数据完整性和机密性的加密和密钥管理。此外，掩码、标记化和匿名化技术，以及数据泄露防护（DLP）和数据安全态势管理（DSPM）工具，在确保强大的数据安全方面发挥着重要作用。通过实施这些措施，组织可以有效地管理和降低与云数据存储和处理相关的风险。

9.2.1 数据安全工具与技术

尽管从技术上来说，所有信息安全都是数据安全，但这些工具构成了专注于数据存储本身安全的核心工具箱。本领域的剩余部分将提供每个工具的更多细节。

●身份和访问管理（IAM）：IAM 系统管理实体对云环境中特定资源的访问，当进行 API 调用或在用户和数据存在于平台的服务中工作时。这与访问控制不同，访问控制也可以管理外部访问。例如，在 IaaS 和 PaaS 中，访问可以在基于用户的 IAM 策略或附加到存储的资源策略中管理。

●访问策略：访问策略管理资源访问。它们定义了特定资源的访问和允许的操作（即，权限），并确定管理资源之间通信流向的网络规则。资源和网络策略都有助于强化安全边界。

●加密和密钥管理：加密通过将数据转换为不可读的密文来保护数据，只有拥有适当解密密钥的人才能解密。密钥管理系统安全地存储和管理这些加密密钥，确保它们与云服务提供商（CSP）分开存放，无论是在他们的云基础设施内还是在外部密钥管理服务器上。这种组合方法确保了云环境中数据的机密性和完整性。

●掩码：用虚构或部分遮挡的值替换敏感数据的技术，保留格式和长度。例如，仅显示信用卡号的最后四位数字，或为测试环境创建虚假的个人身份信息（PII）数据。

●令牌化：用唯一标识符（标记）替换敏感数据的过程，同时保持引用完整性和安全性。它需要另一个数据库来存储原始数据和相关标记，以将标记转换回原始数据值。

●匿名化：从数据集中移除个人身份信息（PII），使个人无法识别的过程。匿名化技术通常是不可逆的，无法恢复原始数据。

●数据泄露防护（DLP）：DLP 指的是执行策略以保护关键数据，如知识产权和客户信息，并确保数据不会从企业流向未经意的第三方。DLP 解决方案有助于识别、监控和保护敏感数据，包括存储在云环境中的数据。这些解决方案能够发现和分类敏感信息，执行安全策略，并防止未经授权的数据共享或外流。

●数据安全态势管理（DSPM）：DSPM 工具持续评估、监控和修复云数据的安全态势。它们提供对安全事件、配置错误和合规性问题的可见性，使组织能够主动识别和解决安全漏洞，并支持风险管理。

9.2.2 访问控制与策略

在云计算中，管理访问是确保安全和运营完整性的基础。通过 IAM 和 RBAC 等框架实现的访问控制和策略，定义并强制执行跨不同云服务的用户权限。这些机制处理各种访问方法，包括 API 和非 API 交互，并确保权限一致应用，即使资源级策略可能会覆盖它们。访问策略进一步通过为资源上允许的操作设置明确规则，并管理云内的网络交互来支持这些控制。本节将探讨这些机制，并提供实际示例来说明它们在维护云安全中的作用。

9.2.2.1 访问控制

访问控制是云安全的重要组成部分，通常应用于已识别的用户，通常通过 IAM 或 RBAC 策略等机制。这些控制对于管理各种访问方法至关重要，如确保 API 调用的管理、非 API 交互以及其他可能在不同云服务提供商（CSP）中差异显著的其他访问方式。重要的是要注意，如果资源通过 IAM 策略未考虑的渠道访问，基于资源的策略可能会覆盖用户或 IAM 策略的拒绝。例如，用户可能仍然可以通过不涉及 API 调用的 Web 界面或应用程序访问资源。

考虑这个示例：亚马逊网络服务（AWS）IAM 策略已制定，允许'AppRead'角色与'ApplicationData' S3 存储桶交互。此策略使用 JSON 格式，并详细说明各个方面，如策略版本、声明、效果（在这种情况下，是'allow'）、主体（将是'AppRead'角色）、操作（具体来说，'s3:GetObject'和's3:ListBucket'权限）以及指定资源（在 S3 存储桶中被识别为'ApplicationData/*'和'ApplicationData/'）。

此场景突出了 IAM 策略的战略使用，为角色分配精确权限，便于访问指定的 S3 存储桶及其内容。精心规划和执行访问控制对于维护云中资源的完整性和安全性至关重要。

9.2.2.2 访问策略

访问策略管理资源访问。它们定义了特定资源的访问和允许的操作（即，权限），并确定管理资源之间流量流动的网络规则。资源和网络策略都有助于执行安全边界。

资源策略作为直接附加到特定资源的规则集，例如对象存储，使它们可以独立于 API 调用被访问，例如，通过 HTTP。这些策略在 CSP 为不属于您的 IAM 用户组的实体提供资源访问权限的场景中是不可或缺的。此外，它们通常包含网络规则，可以根据 IP 地址施加限制。

重要的是要理解，这些资源策略可以覆盖先前配置中建立的访问控制或基于身份的策略。例如，如果基于身份的策略先前禁止角色访问资源，资源策略可以授予访问权限，因为云提供商通常在直接访问场景中优先评估资源策略而不是身份策略。这种机制对于在维护云平台上的访问灵活性的同时执行安全参数至关重要。

网络策略是一套规则，管理网络上的数据流动，也可以直接应用于该网络内的资源，例如Microsoft Azure。它们主要用于通过 IP 地址或指定的 IP 范围管理访问，建立通信范围，确定谁可以或不能与网络资源交互。

作为一个示例，考虑应用于 S3 存储桶的资源策略，该策略旨在授权来自外部 AWS 账户的角色，授予其从某些批准的 IP 地址访问的权限。此策略将以 JSON 格式表述，指定元素，如策略版本、详细声明和效果，将是'allow'。这里的主体将是 AWS 账户 ID 和特定角色的组合。它将定义操作，如's3:GetObject'和's3:ListBucket'，适用于在 S3 存储桶中被识别为'ApplicationData/*'和'ApplicationData/'的资源。此策略的一个关键部分是指定允许访问的 IP 地址的条件。

这种配置示例说明了云环境中资源策略的灵活性，允许来自不同账户的角色被授权访问，同时实施基于 IP 的限制以增强安全性。资源和网络策略都应该精心制定和执行，以保护云资源，确保它们提供组织所需的确切访问控制和网络安全水平。

9.2.3 云数据加密

该图示说明了数据在云中可以加密的不同层，从最低层（卷或对象存储）开始，一直到应用层。随着您向上移动加密层，您将获得更细粒度的控制和保护您的数据，但它也涉及更复杂的实施和管理。应根据数据的敏感性、合规性要求、性能需求以及所需的控制和管理水平选择适当的加密层。

图 50：云数据加密层

应用层

在应用层加密数据提供业务数据保护和控制。应用程序可以加密特定的敏感数据元素，从而确保更精确级别的保护。然而，与较低层的加密相比，应用层加密需要更多的努力来实施和管理。

数据库层

在数据库层加密数据可以保护数据库及其备份中的所有信息。加密方法提供对哪些数据被加密的详细控制，并有助于满足监管合规要求。

文件/API 层

在文件或 API 级别加密提供比卷或对象存储加密更细粒度的保护。这一层允许加密特定文件或通过 API 访问的数据，提供更有针对性的安全性。

卷或对象存储

在这最低层，数据处于静态加密状态。这一层的加密比更高层的加密更容易管理，性能也更好。然而，数据的保护粒度较小，因为加密是应用于整个卷或对象存储库的。卷加密是一种全磁盘加密形式，对象存储库（例如，存储桶或存储账户）可以设置为加密该存储库中的所有对象。

云服务提供商通常默认加密所有他们的存储，但客户可能能够选择和管理自己的密钥。我们将在本文档后面的“自带密钥加密”部分讨论这一点。

9.2.3.1 云数据加密策略

所有加密系统由三个主要组件组成：

- 要加密的数据
- 加密引擎（加密/解密组件）
- 加密密钥

这些功能组件可以位于不同的位置，这是云加密的核心原则。例如，数据可以位于云服务中，但由客户在存储到服务之前加密，使用存储在第三个位置的密钥（客户端加密版本）。或者，密钥可以由客户持有，在运行时提供给提供商，数据由云服务提供商加密（服务器端加密的一种形式）。最后，密钥可以由服务管理，由客户控制，并用于服务器端加密（自带密钥）。

9.2.3.2 客户端加密

客户端加密是一种安全措施，当云提供商仅存储加密数据时采用。在这个模型中，客户负责在将数据发送到云之前对其进行加密，这保证了云提供商无法访问数据的未加密状态。考虑一个决定使用自有场所的加密工具对其敏感文件进行加密的组织。加密后，他们将这些文件上传到云存储服务，如 Amazon S3 或 Google Cloud Storage。由于加密文件的性质使它们无法用于主动处理，这种方法通常用于备份数据、归档或存储很少访问的、“冷”状态的数据。

9.2.3.3 服务器端加密

服务器端加密是大多数云提供商提供的一种服务，数据使用由提供商自身管理的密钥进行加密。它旨在简化设置，通常不需要客户进行任何特定配置，这可能使其成为可能对安全需求不太严格的组织的有吸引力的选择。服务器端加密的安全性取决于云提供商自己的加密协议及其对加密密钥的管理。这种加密类型的主要保护是针对涉及对存储硬件的物理访问的攻击，例如试图直接访问硬盘驱动器。AWS S3 的默认加密功能就是一个服务器端加密的例子，其中 Amazon 负责管理加密密钥，并在数据处于静态时自动加密所有数据。

9.2.3.4 客户管理的加密密钥

客户管理的加密密钥允许客户通过云提供商的密钥管理服务（KMS）积极参与管理他们的加密密钥。尽管管理密钥，实际的加密过程由云提供商执行。这种方法使客户对加密密钥的生命周期拥有权威，包括它们的创建、轮换和删除。同时，云提供商的基础设施负责执行数据的加密。当正确使用时，客户管理的加密密钥创建了一个清晰的责任分离：客户保持对密钥的控制，而云服务提供商负责加密。通常，这种平衡在保持对密钥的控制和便利性之间，成为许多组织的首选。客户管理的加密密钥的实际应用是在组织使用 Azure Key Vault 等服务进行密钥管理时，这些密钥随后用于加密存储在 Azure 的存储解决方案中的数据，如 Azure Blob Storage 或 Azure File Storage。

9.2.3.5 客户提供的加密密钥

客户提供的加密密钥，也称为自带密钥（BYOK），是一种在数据上传到云后进行加密的模型，云提供商执行加密过程。在这个系统中，客户通常需要向云提供商的 KMS 提供自己的加密密钥。这个过程可能需要将加密密钥转移到 CSP 的 KMS 中，这可能会引入额外的安全风险。这是一种 BYOK 形式，其中密钥由客户自行管理，仅在使用时提供，这与使用 KMS 在云提供商处存储和管理，由客户控制的秘钥是不同的。

虽然这种方法为客户提供了对云服务提供商使用的加密密钥的更大控制权，但它也依赖于 CSP 的加密服务。选择这个解决方案可能会限制 CSP 可以提供的服务或功能范围，因为管理外部密钥所施加的限制。一个常见的场景是，组织将自己的密钥带到 Google Cloud Platform 的 Cloud KMS 中，用于加密存储在 Google Cloud Storage 中的数据。

9.2.3.6 自定义应用级加密

这种方法包括混合情况和应用级加密，客户承担加密和密钥管理的全部责任。它要求客户完全将加密密钥与 CSP 分开，选择通过第三方解决方案或使用具有强大密钥管理功能的行业标准加密库来处理加密过程。

尽管这种策略提供了对加密和密钥的最高控制度，但它相应地增加了客户的复杂性和管理负担。这种方法的一个例子是在自定义应用程序中实施客户端加密，使用 AWS 加密软件开发工具

包（SDK）等工具。在这种情况下，应用程序被设计为在将数据传输到云之前对其进行加密，所有加密密钥都由客户端管理，而不是在云中。

在选择云数据加密策略时，组织应考虑因素，如数据的敏感性、监管要求（例如，PCI-DSS、HIPAA、GDPR）、所需的控制水平，以及安全性、易用性和可用性之间的平衡。适当的策略将取决于每个组织的具体需求和限制。仔细评估每种方法的风险和收益，并选择最符合组织安全目标和资源的策略至关重要。

9.2.3.7 机密计算

机密计算是一种方法，专注于确保敏感数据即使在被处理或分析（使用中的数据）时也保持加密和安全。通过使用基于硬件的 enclave，整个工作负载运行时和内存都被加密，从而在处理堆栈的所有层提供非常严格的安全性。

9.2.4 密钥管理服务和自带密钥

如今，大多数客户提供的加密密钥/BYOK 解决方案都集中在使用 CSP 服务上。客户可能或可能不从外部源带来密钥。这个图示概述了这些加密系统的工作原理，尽管每个 CSP 在技术层面上都会有所不同。

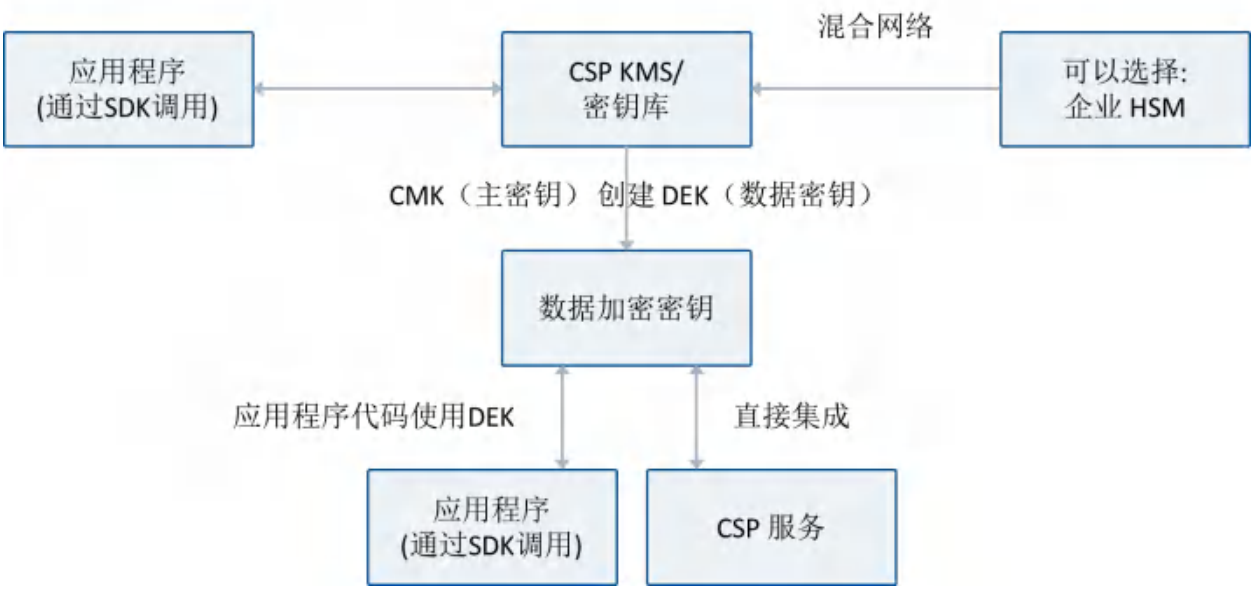


图 51：密钥管理服务和自带密钥加密

CSP 提供密钥管理服务，如 AWS KMS、Google Cloud KMS、Azure Key Vault 和 OCI KMS。这些服务执行各种功能，包括密钥创建、删除、存储、策略和轮换。它们通常作为所有 CSP 客户的多租户系统实施，与传统的硬件安全模块（HSM）相似。此外，一些提供商还提供专用的基于云的 HSM，提供非多租户选项。

客户通常通过使用 CSP 的 KMS 创建客户管理的加密密钥（CMEK）来管理加密。在某些情况下，密钥可能在本地 HSM 中创建，或者 HSM 可能用于生成初始密钥材料。这对于已经在使用数据中心的 HSM 并需要在混合或多云应用程序中同步密钥的客户来说很常见。

CMEK 用于生成单个数据加密密钥（DEK）。CMEK 保留在 KMS 中的标准做法是，DEK 用于实际的加密任务。像 AWS S3 这样的服务可以使用 KMS 密钥来加密客户存储桶中的对象，Azure Key Vault 有能力加密托管存储卷。

对于应用级加密，客户通常使用 DEK，通常通过 CSP 提供的 SDK 来实现，该 SDK 专门设计用于执行加密操作。这允许客户在利用 CSP 提供的强大的加密框架的同时，保持其应用程序的安全性。

一些 KMS 系统提供了一个可选功能，客户可以使用 API 将明文数据发送到服务。然后服务对数据进行加密，返回密文。这个过程有助于防止应用级别的密钥暴露，并且可以作为客户选择企业 HSM 解决方案时的附加安全措施集成。

9.2.5 数据加密建议

在探讨了云环境中数据加密的基础知识之后，以下是增强数据加密的推荐策略，每个策略旨在提高安全性、合规性和云操作的总体数据保护：

●密钥管理服务（KMS）：为了保护云应用程序和服务，建议使用云提供商提供的 KMS。这些服务帮助管理组织的加密密钥。

●SaaS 考虑因素：如果您使用 SaaS，KMS 可能是您唯一的加密选项。SaaS 通常不允许太多定制，因此您将依赖提供商的工具来保护数据。

●默认加密：这通常意味着您的静态数据使用云提供商的密钥进行加密。它通常包含在服务中，不会产生额外成本，并可以满足与数据保护相关的合规性要求。

●服务使用不同的密钥：为不同服务或部署使用不同的加密密钥是一个好习惯。这种方法通过隔离加密域和限制受损密钥的潜在影响来增强安全性。

●密钥上的 IAM 策略：对您的密钥应用 IAM 策略，以执行最小权限原则。这样做确保只有授权的用户和服务可以使用特定密钥，并且您可以定义它们可以使用它执行的操作。

●与威胁模型对齐：确保您的加密策略与您的威胁模型保持一致。例如，如果攻击者可以危及应用程序凭证或数据库管理员的凭证，那么加密数据库的效果就会降低。在这种情况下，攻击者可以通过合法渠道访问或外流加密数据。在这种情况下，攻击者可以通过合法渠道访问或外流加密数据。

9.2.6 云数据泄露防护

云数据泄露防护（DLP）工具用于发现敏感数据，监控使用情况，并防止或警报策略违规。云中的 DLP 由于数据的大规模特性而面临独特的挑战。庞大的数据量和相关成本使得全面的 DLP 扫描变得困难，特别是对于 IaaS 或 PaaS 环境。因此，DLP 往往更多地用于 SaaS 应用程序，而不是 IaaS 或 PaaS。

当 DLP 用于 IaaS 或 PaaS 时，云提供商的本地 DLP 服务通常范围有限。例如，AWS Macie 主要关注 S3 存储。与 IaaS 或 PaaS 集成的外部 DLP 工具通常必须使用数据抽样技术来管理数据量并降低成本。

组织应将 IaaS 或 PaaS DLP 视为类似于“数据中心的 DLP” - 由于复杂性和规模，它们可能没有历史上实施过。相比之下，SaaS 的 DLP 更符合传统的 DLP 实践，重点关注监控用户在电子邮件、Web 浏览和云应用程序使用中的活动。

为了构建有效的云 DLP 策略，组织必须仔细评估其数据全景，优先考虑高风险环境，并平衡使用云原生和第三方 DLP 解决方案。基于风险的方法，结合强大的访问控制，可以帮助管理云 DLP 的挑战，同时仍然保护企业云足迹中的敏感信息。

云 DLP 是云访问安全代理（CASB）的主要能力之一，它通过监控云中的用户操作并根据程序采用定义的策略来提供可见性和安全控制。CASB 整合了多种类型的安全策略执行。示例安全策略包括加密、标记化等。

9.2.7 数据安全态势管理

数据安全态势管理（DSPM）是一个新兴的工具类别，专注于以数据为中心的安全。云安全态势管理（CSPM）管理您的 IaaS 云配置和态势，而 SaaS 安全态势管理（SSPM）管理您的 SaaS 安全，DSPM 则提供数据的可视化和管理能力。

这包括数据发现和分类，也可能包括类似数据泄露防护（DLP）的功能，以帮助您了解数据的位置及其敏感性。DSPM 工具可以拉取并评估所有重叠的访问控制、IAM 策略、资源和网络策略，以评估和可视化谁可以访问数据以及如何访问。这些工具随后提供建议和/或直接管理补救措施或提供具体建议，例如基础设施即代码（IaC）模板或策略。

云数据安全的挑战在于处理所有潜在的重叠控制措施，这些控制措施在不同领域管理，不一定能提供对您的数据使用和暴露的完整视图。DSPM 旨在填补这一空白。

9.3 保护特定存储类型

对象存储服务，如 AWS S3 和 Azure Blob Storage，已成为云服务提供的重要组成部分。网络安全专家认为，这些服务存在显著的组织数据暴露风险。高调事件突显了这些漏洞，通常源于配置错误。通常，云服务提供商默认将存储对象设置为私有，但用户可能会不小心变更这些设置，从而暴露敏感的商业和私人数据。访问设置的复杂性进一步增加了安全性挑战。

为了降低风险，云服务提供商提供了在部署级别阻止公共访问的功能，尽管这有时会干扰合法的数据访问需求。加密数据和使用内容分发网络（CDN）可以增加额外的安全层，下面将讨论这些内容。持续监控和主动的安全策略是避免数据泄露和最小化影响范围的额外保护层。

9.3.1 对象存储安全

对象存储服务，如 AWS S3 和 Azure Blob Storage，对云操作至关重要，但也带来了显著的数据暴露风险。显著事件强调了这些漏洞。通常，云服务提供商默认将存储对象配置为私有设置以保护数据。然而，当用户不小心变更这些设置时，数据泄露事件频繁发生，从而使敏感数据公开可用。

配置错误和对复杂访问设置的误解进一步导致数据暴露。AWS 的细致权限系统，涉及 IAM 角色和策略以及基于资源的策略，正是保护云存储的挑战之一。为了防止意外的公共数据暴露，云服务提供商引入了在部署级别阻止公共访问的能力。例如，AWS 允许用户强制实施账户范围的设置，以防止由于存储桶权限配置错误而导致的数据泄露。

然而，普遍阻止公共访问可能会妨碍合法需要开放数据访问的应用程序。管理这些阻止的例外需要仔细配置，以确保只有必要的数据可以公开访问。通过使用云服务提供商的 KMS 加密数据，提供了额外的安全层，前提是加密密钥与能够变更对象存储权限的身份分开管理。这确保了即使存储容器不小心公开，加密密钥仍然保持安全。

某些应用程序可能会利用 CDN 来分发存储在私有对象存储中的数据，例如与公共 CDN 关联的私有 S3 存储桶。尽管这种设置不会直接暴露存储，但会通过 CDN 导致公共数据访问。使用 CSPM 和数据安全态势管理（DSPM）等工具进行持续监控至关重要。这些工具通过持续监控安全态势，帮助检测和纠正与安全最佳实践的偏差。

在网络安全中，“向左移动”的概念在增强云基础设施的安全性方面发挥着重要作用。它涉及在基础设施即代码（IaC）开发过程中早期检测和防止配置错误，确保最佳实践在开发过程的早期就被整合。这种主动的方法有助于在潜在安全问题成为生产环境中的重大问题之前避免它们。因此，持续监控和主动的安全策略对于维护云基础对象存储中数据的完整性和机密性至关重要。

9.3.2 云数据库安全

在云中部署数据库时，组织主要选择两种方法：

- 传统数据库即服务（DBaaS）
- 云原生数据库

图 52：传统数据库即服务（DBaaS）与云原生数据库对比

传统数据库即服务（DBaaS）

组织可以选择知名的数据库引擎，如 MySQL、PostgreSQL 或 Microsoft SQL Server，这些数据库由云服务提供商提供为托管服务。为了保护这些数据库，建议遵循已建立的最佳实践。这包括采用安全配置，结合强身份验证措施和全面的访问控制。创建安全的数据库用户账户和角色、在私有子网中存储数据，以及对云服务提供商的管理平面 IAM 角色实施最小权限访问原则也很重要。此外，利用云服务提供商的托管备份和快照功能可以增强数据保护，但必须安全维护以防止未经授权的访问，这是数据外泄的常见方式。如果不需要跨区域复制等服务，应该停用这些服务，以符合组织的策略和合规要求。传统 DBaaS 的知名例子包括 Amazon RDS、Azure SQL Database 和 Google Cloud SQL。

云原生数据库

另外，组织可能会考虑专为云平台设计和优化的云原生数据库，具有无服务器操作和自动扩展等功能。为了保护这些数据库，必须首先为管理平面 IAM 角色分配最小权限。数据平面的访问应通过基于资源的策略进行管理，并应禁用公共访问以防止未经授权的数据暴露。在可行的情况下，使用专用私有端点或虚拟私有云（VPC）集成可以为应用程序提供安全的连接路径。利用服务的自动备份和快照功能以及进行安全 API 调用以进行应用集成也是有益的。云原生数据库的例子包括 Amazon DynamoDB、Azure Cosmos DB 和 Google Cloud Firestore。

对于这两种类型的云数据库，至关重要的是：

- 遵循责任共担模型并强化数据库配置。

- 根据需要加密数据以满足合规要求。
- 实施强身份验证措施并保持最小权限原则。
- 积极监控日志并利用云原生威胁检测服务。建议考虑激活数据级日志/事件，这些可能默认未启用。
- 制定和维护全面的备份和恢复计划。

9.3.3 数据湖安全

在大数据时代，数据湖的概念已成为管理和分析来自众多来源的大量数据的关键要素。根据CSA 的数据安全术语表的定义，“数据湖是一个集中式存储库，摄取并以原始形式存储大量数据。然后可以处理这些数据，并作为各种分析需求的基础。由于其开放、可扩展的架构，数据湖可以容纳来自任何来源的所有类型数据，从结构化（数据库表、Excel 表）到半结构化（XML 文件、网页）再到非结构化（图像、音频文件、推文），而不会牺牲保真度。”这一定义概括了数据湖作为全面数据整合点的本质，能够处理和保留各种数据形式的复杂性。

然而，从不同来源整合如此庞大的数据集带来了重大的安全挑战，因为数据湖成为网络威胁的主要目标。因此，部署在数据湖中的安全策略必须是多方面的，以保护敏感信息，同时保持可访问性和实用性。根据敏感性和机密性对数据进行隔离和分区，以及实施强大的访问控制系统，对于维护数据的完整性和安全性至关重要。通过加密、网络安全和持续监控等措施，组织可以努力加强其数据湖的安全性，确保安全有效地使用其整合的数据资源。

为了确保存储在数据湖中的大量多样数据的安全性和完整性，制定了以下策略：

- **数据湖作为数据整合点：**数据湖的强大之处在于它整合了来自众多来源的各种数据，这些数据在敏感性和安全分类上可能差异很大。挑战在于在这一多样化的数据集中保持强大的安全性。
- **安全级别和数据隔离：**鉴于数据湖中数据的多样性，并非所有用户或应用程序都应访问所有数据。一些数据可能是公开的，而其他数据可能是高度机密的。有效隔离这些数据至关重要。
- **通过视图/访问点进行分区：**创建视图或访问点，作为数据湖的窗口，每个视图仅显示特定用户或应用程序可以访问的相关数据。这类似于在数据湖中创建虚拟分区。

9.3.3.1 基线数据安全实践

以下是加强数据环境安全的措施。这些基本措施为抵御漏洞和威胁奠定了基础，为根据需要实施更专业或高级的安全策略做好准备。

- **持续漏洞评估和补救管理：**为了保护免受漏洞影响，确保与数据湖交互的所有组件都及时更新最新的安全补丁。
- **身份和访问管理（IAM）：**实施详细的 IAM 策略。访问应基于最小权限原则，确保用户和应用程序仅拥有执行其功能所需的权限。
- **加密：**在静态、传输和使用时应用加密，以保护数据免受暴露，如果其他控制措施失效。例如，使用 AWS KMS 管理数据湖中 S3 存储桶的加密密钥。
- **网络安全：**利用网络安全措施，如 VPC、安全组和网络访问控制列表，控制数据湖的流入和流出流量。
- **持续日志管理、监控和警报：**持续监控访问模式并审查权限，以确保实施的安全措施随着时间的推移仍然有效。请记住，保护数据湖不是一次性。

9.3.4 人工智能的数据安全

随着人工智能技术变得更加普遍并融入关键业务流程，确保人工智能系统的安全性和完整性至关重要。人工智能的数据安全涉及实施措施保护人工智能系统、算法和数据资产免受各种安全威胁和漏洞的影响。部署人工智能主要有两大方法：人工智能即服务（AIaaS）和自托管/云托管人工智能。

9.3.4.1 人工智能即服务

在 AIaaS 模型中，第三方提供商通过互联网以订阅方式提供人工智能能力和服务。组织可以访问预训练的 AI 模型、API 和工具，将 AI 功能集成到他们的应用程序和工作流程中。例子包括 Anthropic 的 Claude、OpenAI 的 ChatGPT 和 Google Cloud 的 Vertex AI。使用 AIaaS 时，至关重要的是要：

- 理解服务水平协议（SLA），确保提供商满足您的可用性、性能和支持要求。
- 对提供商的数据安全实践进行全面评估，包括加密方法、访问控制和监控能力，以保护数据免受未授权访问。

● 验证提供商是否符合相关法规和标准（如 GDPR、HIPAA 或 SOC 2），以确保敏感数据的保护和遵守行业最佳实践。

● 如果提供商不提供安全区域或专用环境，避免发送专有或敏感数据。

● 与提供商明确数据删除和保留策略，以确保数据生命周期管理满足安全要求。

● 评估提供商的 AI 安全措施，包括针对对抗性攻击（如模型投毒、提示注入等）的保护措施，以确保 AI 驱动的服务和应用程序的完整性和可靠性。

9.3.4.2 自托管/云托管人工智能

在自托管/云托管人工智能方法中，组织在本地或云中开发、部署和管理自己的 AI 模型和基础设施。组织对 AI 开发过程拥有完全控制权，包括数据收集、模型训练、优化和部署。组织对确保 AI 系统的安全负有全部责任。关键考虑因素包括：

● 通过实施访问控制、加密机制和数据治理策略来保护训练数据存储库，以防止敏感数据被未经授权的访问或篡改。

● 建立安全的 AI 系统访问，包括网络分割、防火墙配置和细粒度的 IAM 策略，以控制和限制系统对授权用户和实体的访问。

● 过滤训练数据以防止模型投毒，其目的是操纵 AI 的行为。

● 实施针对提示注入攻击的保护措施，恶意输入尝试通过利用输入机制中的漏洞来绕过 AI 的预期行为。

● 通过部署强大的提示扫描机制来抵御 AI 越狱尝试，该机制检测并阻止 AI 系统内的数据。

● 定期更新和修补 AI 系统以应对新出现的安全隐患。

● 确保 AI 系统遵守相关的 AI 伦理指南和法规，以防止产生偏见或歧视性的输出。

图 53：人工智能即服务（AIaaS）与自托管/云托管人工智能对比

9.3.4.3 其他人工智能考虑因素

为了增强人工智能系统的安全性并确保其安全集成和运行，请考虑以下安全实践。

- 将 AI 系统与其他应用程序集成时采用安全的 API 和加密协议。
- 为与 AI 系统交互的用户实施强有力的身份验证和访问控制。
- 对人工智能系统进行定期审计和安全评估，包括渗透测试和威胁建模。
- 制定并维护事件响应计划，以检测、调查和补救人工智能安全事件或漏洞。
- 培养人工智能安全意识文化并培训开发人员、管理员和用户。

总结

在云服务快速发展和网络威胁日益增加的背景下，该领域满足了云环境中对强大数据安全的需求。它强调了数据安全对于维护组织完整性、机密性、客户信任和法规遵从性的重要性。该领域探讨了数据安全的各个方面，包括数据分类、云存储类型以及针对不同数据状态（静态数据、移动数据和使用数据）的特定安全措施。它涵盖了 IAM、加密和访问控制策略等基本安全工具和技术，为保护云数据提供了全面的指南。总体而言，该领域是希望加强云数据安全实践的组织的基础指南。

建议

- 云安全首先要了解和管理您传输到云的数据并应用访问控制。
- 了解基于 IAM 的访问控制、资源策略和网络策略之间的差异。必须协调一致以防止数据泄露。
- 加密只有在与威胁模型一致且密钥和数据（以及对它们的访问）分离的情况下才能提高安全性。如果攻击者执行SQL 注入攻击并可以通过应用程序获取数据，则加密毫无意义。
- 在 IaaS 或 PaaS 中实现加密时，从 CSP 的 KMS 服务开始。
- IaaS 中的云 DLP 相当于传统数据中心的 DLP。SaaS 的 DLP 相当于电子邮件服务和应用程序的 DLP。
- 通过控制对特定数据的访问（并遵循核心数据存储安全控制）来确保数据湖的安全。
- 人工智能安全应该关注潜在的数据暴露，这取决于你正在审查公共服务还是自托管模型。

补充指南

- 云服务中的密钥管理|CSA
- 具有外部源密钥的云密钥管理系统|CSA
- 使用客户控制密钥存储的建议|CSA
- 云密钥管理基础|CSA
- 云密钥管理基础 II|CSA
- 密钥管理生命周期最佳实践|CSA
- 安全数据湖的敏捷数据原则|CSA
- 了解云数据安全和优先级|CSA

领域 10：应用安全

该领域涵盖应用程序安全性，即使用安全控制保护计算机应用程序免受外部威胁的实践。应用程序安全性包含了非常复杂和庞大的知识体系:从早期设计和威胁建模到维护和保护生产应用程序的所有内容。随着应用程序开发实践的不断进步，应用程序安全性也在快速发展，并采用了新的流程、模式和技术。云计算是其中最大的驱动力之一，也带来了更迫切的稳定、可扩展和安全性要求。

从最初的设计阶段到持续的维护，基于云的应用程序的安全性需要深思熟虑并采取主动措施。云环境(适用于许多私有云和云计算)中应用程序安全性所带来的独特挑战和机遇如下:

- 应用程序通常由微服务和外部服务组成，这需要对攻击面和控制边界进行更详细的分析。
- 攻击面通常包括 API 的大量暴露。
- 在云环境中，应用程序通常使用具有快速功能开发的开发和运营(DevOps)方法进行开发，这既是风险，也是机会。
- 应用程序可以构建在提供商(例如，PaaS 提供商或无服务器)控制的库上，这需要关注责任共担模型。
- 应用程序经常利用第三方库，包括开源组件，引入供应链风险和额外的攻击向量。
- 安全特性，如身份管理、日志记录和监控，通常来自云提供商，这可能与应用程序的需求相匹配，也可能不匹配。
- 应用程序通常部署在可编程的基础设施上(例如：基础设施即代码(IaC)，编排器，Kubernetes 等)。
- 在云环境中大规模运行的应用程序需要对底层基础设施的漏洞有敏锐的认识。无状态架构优先考虑可伸缩性和弹性，通常用于减轻基础设施故障的影响。然而，尽管这些架构提供了灵活性和敏捷性，但它们也引入了可能破坏整体安全态势的复杂性。

学习目标

本领域的学习目标旨在为读者提供以下知识:

- 为创建安全应用程序实施安全开发流程。
- 认识到架构在确保云应用安全方面的关键作用。
- 使用 DevSecOps 在整个安全软件开发生命周期(SSDLC)中自动集成安全性。

10.1 安全开发生命周期

安全的应用程序始于安全的开发过程。安全的应用程序始于安全的开发过程。仅依赖开发团队来创建安全可靠的代码是不够的。为解决这一问题，开发和安全专业领域围绕“软件开发生命周期”（SDLC）流程进行融合，该流程也被称为“安全软件开发生命周期”（SSDLC）。

云在这些流程的各个部分引入了一些新的含义，主要源于应用程序和云基础设施之间更紧密的集成。在云中工作时，开发人员也倾向于使用更新、更快的方法，如 DevOps。最后，基础设施即代码（Infrastructure as code，简称 IaC）和部署流水线是云中的标准实践，但对传统数据中心应用程序的使用程度并不一定相同

10.1.1 CSA 安全开发生命周期

云安全联盟 (CSA) 开发、安全、运营 (DevSecOps)安全开发生命周期（SSDLC）定义了五个阶段，这些阶段与应用程序开发的普遍认可的阶段相对应，每个阶段都确定了成功的 DevSecOps 计划中要实施的关键流程、工具和设计模式。

图 54：安全软件开发生命周期（SSDLC）的阶段

SSDLC 的阶段

1. 安全设计和架构：设计部分参考了可以在产品设计过程中应用的技术和工具。设计是持续的，因此新产品功能和更改将通过设计活动进行。如果在设计阶段不包括安全性，那么以后引

入的安全措施将在部署或运行时产生更高的运营影响和成本。这些安全措施也难以扩展，导致安全瓶颈进而减缓开发速度并影响发布时间表。

2. 安全开发：在开发阶段应用安全编码能力，以确保在构建应用程序时将安全性集成到应用程序中。与人工人工审查相比，自动化工具的编码安全控制可以更好、更一致地识别代码中的弱点和漏洞。如果在开发阶段不包括安全分析和设计，那么在生命周期后期阶段，源代码中的漏洞可能会被识别并部署到生产环境中，修复成本会更高。

3. 持续构建，集成和测试：集成和测试包括对应用程序或产品的功能进行安全测试的工具和过程。如果没有这些工具和方法，安全漏洞和弱点将被利用，并导致数据泄露和可用性问题。

4. 持续交付和部署：部署前的安全检查确保将应用程序或产品部署到安全的基础设施上。如果在部署阶段不包括安全性，则存在漏洞和糟糕的安全性实践削弱应用程序或产品的风险，并利用它在生产环境中进行攻击。

5. 运行时防御和监控：在应用程序或产品发布到生产环境之后可以应用的功能和实践。运行时安全性通过识别效率低下、漏洞和弱点以及启用事件响应来实现持续改进。

10.1.2 安全设计与架构之威胁建模

威胁建模是一种在风险管理中使用的结构化过程，用于识别、评估和纠正可能对组织资产造成安全威胁的潜在问题。它涉及理解系统架构、识别安全目标以及分析可能影响这些目标的潜在威胁。通过执行威胁建模，您可以根据威胁的严重性和可能性对识别出的威胁进行优先排序，并制定策略来减轻或预防相关风险。这一过程通过关注更容易受到攻击的区域来创建更安全的系统设计，并确保安全措施在开发生命周期的早期阶段得到整合。

STRIDE 是一个用于识别和分类安全威胁的框架。它代表了欺骗（Spoofing）、篡改（Tampering）、抵赖（Repudiation）、信息泄露（Information disclosure）、拒绝服务（Denial of Service）和权限提升（Elevation of Privilege）。以下是每种威胁类别的简要概述：

1. **欺骗（Spoofing）：**攻击者假装成其他人，例如用户或系统，以获得未经授权的访问。示例包括网络钓鱼攻击，攻击者模仿合法站点窃取登录凭据。

2. **篡改（Tampering）：**指未经授权变更数据或消息。这可能发生在传输过程中或存储系统中，从而损害数据的完整性。

3. **抵赖（Repudiation）：** 一方在已经采取行动后却否认行为。这破坏了系统将行为归因于正确来源的能力，使问责制复杂化。.

4. **信息泄露（Information Disclosure）：** 这涉及未经授权访问机密信息。技术包括窃听不安全的通信或利用漏洞访问敏感数据。

5. **拒绝服务(Denial of Services)：** 系统资源耗尽导致系统不可用。这将破坏运维并导致严重的停机时间。

6. **权限提升（Elevation of privilege）：** 当攻击者获得比允许的更高的访问级别时，可以绕过访问控制来执行为更高访问权限帐户的操作。

了解这些威胁可以识别系统中的潜在漏洞，并指导开发有效的对策来防止这些安全风险。

10.1.3 安全开发

在云中，架构和应用程序代码之间通常存在更强的耦合。基础设施和服务通常使用 IaC 进行部署，它与应用程序代码完全集成，使用相同的版本控制存储库和持续部署流水线。

云应用程序大量使用来自云服务提供商(CSP)的平台即服务(PaaS)服务，所有这些服务都需要根据应用程序的需求和安全需求进行适当配置。这通常还需要为应用程序代码和服务分配特权，以便进行 API 调用以使用这些服务，从而将潜在的攻击面扩展到管理平面。

- PaaS 服务将更多的安全责任推给了云服务提供商（CSP），并且可以减少或消除客户维护安全，完全修补和配置的服务器或服务的需求。
- 为所有应用组件和 PaaS 服务实现最少特权身份和访问管理(IAM)。
- 使用云服务提供商（CSP）服务，如负载均衡器和高度限制性安全组，以减少面向互联网的风险。

一旦设计完成，就应该遵循标准的安全开发实践。云安全联盟(CSA)建议使用 DevSecOps 流程，这在 10.5 节中有重点介绍。

10.1.4 测试：部署前

部署前测试是在软件投入生产之前确保其安全性和功能性的关键步骤。通过在开发过程的早期，特别是在部署之前集成测试，团队可以节省大量的时间和资源。这种方法允许及早发现和纠正问题，有助于开发更安全、更可靠的软件产品。

以下是一些关键的部署前测试方法。

1. **静态应用程序安全测试(SAST)：**此过程检查应用程序的源代码，以识别现有的安全缺陷或漏洞。它是一种执行安全代码审查的自动化方法，可以集成到持续集成/持续部署(CI/CD)流水线中，或者集成到开发人员的集成开发环境(IDE)中。它专门查找逻辑错误、检查规范实现、检查样式指南和安全缺陷(如 OWASP Top 10 和 SANS Top 25 列出的缺陷)。此外，它扫描硬编码凭据、密钥、令牌和秘密的代码，防止它们进入存储库，并识别其他活动中的潜在泄漏。SAST 可能容易出现误报，这就是为什么它需要调整和优化，以免开发人员排斥。

2. **手动安全代码审查：**在此过程中，经验丰富的开发人员检查提交的每个代码审查以寻找缺陷。自动化过程不会捕获一些重要的错误，例如业务逻辑错误，因此强烈建议进行手动代码审查。这可以通过 Pull Request (PR)流程来实现。最好的方法是将自动流程与手动流程一起运行，因为它们是相互补充的。

3. **软件成分分析(SCA)：** SCA 涉及审计软件所依赖的外部组件，例如库和系统组件。此方法确保这些组件是最新的，并且没有已知的漏洞，并且这些组件的许可类型有助于避免将许可风险带入项目。它对于创建安全的虚拟机(vm)、容器镜像和无服务器函数至关重要。SCA 还可以帮助创建软件物料清单(Software Bill of Materials, SBOM)，为软件中使用的所有组件提供透明性。

4. **静态漏洞扫描：**在云环境中，漏洞扫描对于识别和减轻潜在的安全威胁至关重要。扫描主要有两种类型：静态和动态。静态扫描分析源代码(IaC)和静态配置，包括虚拟机镜像或模板、容器镜像、Dockerfiles、docker-compose 文件、Kubernetes YAMLs、Terraform 或 Cloudformation 文件等文件。这种类型的扫描通常在 SSDLC 的预部署阶段执行，在部署之前检查配置文件、基础结构模板和源代码。静态扫描有助于识别漏洞和配置错误，可以在它们在生产环境中造成问题之前加以解决。

10.1.5 测试：部署后

部署后测试在软件部署后验证其安全性和功能，挑战了在其设计和集成期间所做的假设，特别是对于云应用程序。此阶段确保软件在实际条件下有效运行，对应传统的数据中心测试过程。

以下是一些必要的部署后测试示例。

1. **动态漏洞扫描：**在 SSDLC 中部署后进行动态扫描。它包括主动探测运行环境，模拟真实世界的攻击场景，以识别可能被恶意参与者利用的漏洞。与静态分析不同，静态分析检查静态代码和配置，动态扫描实时评估系统的安全状态，提供对在预部署静态分析期间可能被遗漏的潜在弱点的洞察。通过模拟攻击，动态扫描可以帮助组织了解其系统对各种威胁的弹性，并允许他们在漏洞被利用之前修复漏洞。与静态分析（在部署前识别代码和配置中的漏洞）相结合，动态扫描提供了一种全面的方法来保护云环境，确保应用程序和基础设施免受整个 SSDLC 的潜在威胁。

2. 动态应用程序安全测试(DAST)：DAST 是一种测试方法，测试人员在 web 应用程序运行时检查它，但不了解应用程序、其内部交互或系统级别的设计，也不访问或可见源程序。DAST 也被称为“黑盒”测试，因为它从外部到内部查看应用程序，检查其运行状态，并使用某些技术和测试工具观察其对模拟攻击的响应。应用程序对这些模拟的响应有助于确定应用程序是否容易受到攻击，是否容易受到真正的恶意攻击。

○ **动态分析（模糊测试）：**将不可预测的数据输入到软件中，以识别在运行过程中可能被利用的错误和漏洞。

○ **交互式应用程序安全测试(IAST)：** IAST 是一种应用程序安全测试方法，它在应用程序由自动化测试、人工或任何与应用程序功能交互的活动运行时对应用程序进行测试。IAST 可以被认为是 SAST 和 DAST 的组合，以实现对源代码和运行时执行的问题进行概述的目标。

3. 渗透测试：作为模拟网络攻击，渗透测试旨在利用已知漏洞，测试安全措施的弹性和软件抵御攻击的能力。渗透(渗透)测试可以使用自动化工具或手动工作来应用。从长期来看，建议两者都使用。渗透测试还可以用于测试应用程序组件级别，或在云部署级别执行渗透测试，以识别云配置中的缺陷。

4. **Bug 赏金计划：**这些计划为成功发现并报告实时应用程序中的漏洞或 Bug 的道德黑客提供金钱奖励。漏洞赏金计划允许组织利用道德黑客社区，随着时间的推移改进其系统的安全状态。虽然 Bug 赏金程序并不总是必需的，但它们可以被组织视为其安全策略的一部分。

10.2 安全云应用架构

系统架构在确保云应用程序的安全性方面起着至关重要的作用。它是设计和部署安全的基于云的解决方案的蓝图。通过在体系结构级别集成安全原则和实践，组织可以为保护数据、维护隐私和确保遵守法规标准创建坚实的基础。这包括仔细规划云环境中的组件和交互，以减轻潜在威胁、保护数据传输和有效地管理访问控制。通过移动组件或不实现“功能”，针对特定资产/数据流的威胁可能不再存在。设计良好的架构可以增强云应用的安全性，提高云应用的可扩展性、可靠性和整体性能。

10.2.1 云计算对架构安全的影响

云计算改变了传统软件和基础设施开发的模式，强调一切都是软件。这种转变简化了运维，并将基础设施与应用程序紧密集成，需要一种新的安全方法。

1. **基础设施和应用程序集成：**云将基础设施与应用程序合并，使服务器和数据库等元素成为应用程序功能的组成部分。这种集成可以通过无缝运维增强安全性。然而，它也带来了 IAM 风险，其中不正确的权限可能导致违规。这里的关键是对身份和访问进行细致的管理，以减轻潜在的漏洞。

2. **应用程序组件凭据：**在云中，诸如微服务之类的组件使用通常仅为该服务指定的特定权限和凭据进行通信。暴露或管理不当可能导致重大安全事件。确保安全处理凭证和严格控制访问对于防止违规至关重要。

3. **基础设施即代码和流水线：**通过代码定义基础设施已经成为云实践的一个标志，在部署中提供一致性和效率。然而，这些部署流水线可能会吸引攻击者。流水线的破坏可能会危及整个软件供应链。保护这些流水线可以保护开发和部署过程。

4. **不可变基础设施：**随着虚拟化和基础设施即服务(IaaS)技术的成熟，许多安全专家已经转向一种范式，在这种范式中，机器配置的管理和部署永远不会被维护或篡改。更具体地说，一旦创建了应用程序、服务器或系统配置的实例，就永远不会对其进行修改。相反，如果需要变更，则从公共模板构建新实例并完全替换。这种方法与传统的维护实践(如可变基础结构)形成对比。

总之，向云计算的迁移需要在架构级别重新评估安全性，重点关注集成系统的独特挑战和机遇。早期和前瞻性的安全规划以及对身份和凭证的稳健管理构成了安全的基石。

10.2.2 架构的弹性设计

云环境需要对应用程序的设计和架构进行彻底的变革，强调灵活性、可扩展性和安全性。应在需求构建阶段尽早讨论和规划应用程序安全性。您可以选择参考 SSDLC 的主要框架和指南，例如 NIST 800-64 有关将安全措施融入开发流程的详细指南，或 ISO/IEC 27034 有关如何将安全性融入IT 系统生命周期的指南等。

DAST 测试正在运行的应用程序，包括 Web 漏洞测试和模糊测试等测试。由于与云服务提供商（CSP） 的服务条款，DAST 可能受到限制或可能需要提供商的预测试许可，这对于某些云服务提供商（ CSP） 来说可能非常耗时。借助云和自动化部署流水线，可以使用 IaC 建立完全功能性的测试环境，然后在批准生产变更之前进行深入评估。

以下是针对云环境进行开发、集成和部署的一些最常见的实践：

1. **默认隔离：**云平台允许应用程序在隔离环境中运行，例如单独的虚拟网络或帐户/子帐户。这种隔离通过划分开发和生产环境来提高安全性，并在必要时启用更严格的访问控制。云计算有助于将服务隔离到不同的服务器或容器上，从而提高可扩展性和安全性。这种方法通常涉及微服务，需要仔细管理微服务之间的通信安全性以及服务发现、调度和路由的安全配置。

2. **部署和测试的自动化：**在云平台中，组织希望以比以前更快的速度开发和部署软件。这意味着对于安全和运营团队来说，以前的手动工作（例如部署测试环境或对应用程序代码进行安全测试）应该自动化，以提高效率和速度。自动化需求需要采用新工具并增加其在 CI/CD 流水线中的使用。

3. **不可变的基础架构：**通过禁用远程登录、添加文件完整性监控以及将这些实践纳入事件恢复，不可变基础架构可以降低安全漏洞的风险。

4. **PaaS 和无服务器架构：**PaaS 和无服务器计算将底层服务和运维系统的管理转移给云提供商，从而减少了攻击面。这些架构的安全性很大程度上取决于云提供商对保护平台安全以及满足用户安全要求的承诺。

上述每个方面都强调了根据云计算带来的独特机遇和挑战调整安全策略的重要性。

10.2.3 基础设施即代码和应用程序安全

基础设施即代码（IaC）通过使用配置文件定义和管理资源，彻底改变了 IT 基础设施的设置，类似于根据蓝图自动构建建筑物。

这种方法简化了云资源的部署和管理，显著提高了应用程序的安全性。

1. **自动化遵从性检查：**IaC 促进了针对安全标准和法规的自动验证，确保无论何时配置或修改基础设施都符合要求。这种自动化就像一个无情的检查员，不断地确保遵守安全策略。

2. **一致的安全状态：**通过编写基础设施设置，IaC 保证每个元素（从服务器到数据库）都根据安全最佳实践进行一致的配置。这消除了与手动设置相关的人为错误，检测并消除了配置漂移，并在所有资源之间保持统一的安全级别。重要的是，IaC 还支持通过集中异常管理来管理这些安全策略的异常。例如，由于有效的业务需求，特定资源可能需要偏离标准配置，例如，为公共访问配置简单存储服务（S3）桶。通过在 IaC 框架内记录和管理这些异常，组织可以确保识别、批准和跟踪这些偏差，在支持必要的运维灵活性的同时维护安全监督。

3. **对威胁的快速响应：**IaC 允许对基础设施代码进行快速修改，以响应已识别的漏洞，允许在整个基础设施中进行修补和热修复部署。这种能力类似于远程更新建筑物的安全系统，以解决不需要物理干预的弱点。

4. **快速 CI/CD 回滚：**IaC 支持快速 CI/CD 回滚功能，增强了运维弹性。当对容器或虚拟化环境进行更新时，可以将性能与基准进行统计比较。如果新的自动推出（例如金丝雀版本）无法满足这些基准测试，那么 IaC 允许自动回滚到以前的稳定配置。这不仅可以最大限度地减少停机时间，还可以确保安全性和运维稳定性不受新变更的影响。

下图说明了设计、自动化编码、创建基础架构模板和在安全云架构中部署的迭代过程。

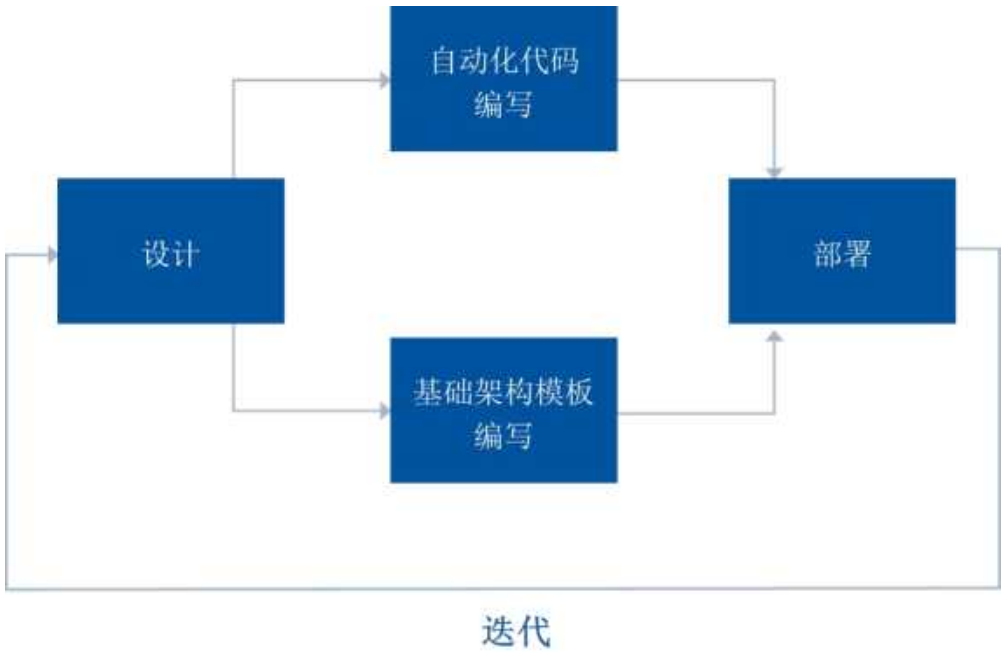


图 55：基础设施即代码：通过自动化增强安全性

组织还应更多地依赖云中的自动化测试。由于 IaC，基础设施更经常成为应用程序测试的范围，其中基础设施本身是通过模板和自动化定义和实施的。利用 IaC 不仅可以提高运营效率，而且通过将安全性嵌入到基础设施的基础中，还可以显著改善基于云的应用程序的安全状况。

10.2.4 安全的最佳实践

当涉及到保护 API 时，有几个选项需要考虑。一种选择是使用 API 网关，它作为管理身份验证、速率限制和传入 API 请求访问控制的集中点。这有助于确保只有经过授权的用户和系统才能访问 API。另一种选择是实现服务网格，其重点是保护应用程序中不同服务之间的通信。服务网格提供内置的加密和身份验证机制，这有助于在服务之间传输敏感数据时保护敏感数据。

除了这些措施之外，仔细定义 API 契约以避免任何潜在的敏感信息泄漏也很重要。API 契约不应该过于宽松，访问应该仅限于必要的数据和功能。此外，您应该将自动化的 API 安全性测试合并到 CI/CD 流水线中。通过这样做，可以在开发过程的早期检测到漏洞，从而及时修复并降低安全破坏的风险。

通过实现这些保护选项并遵循最佳实践，组织可以增强其 API 的安全性，并保护敏感数据免受未经授权的访问或暴露。

10.3 身份和访问管理对应用程序安全的贡献

IAM 在增强应用程序安全性方面发挥着关键作用。它涵盖了用于管理身份和规范组织内用户访问的技术和策略。通过有效地控制谁有权访问哪些资源以及如何授予和撤销访问权限，IAM 系统可确保合适的个人在合适的时间出于合适的原因访问合适的资源。将 IAM 与应用程序安全策略集成对于防止未经授权的访问和保护敏感数据免受潜在威胁至关重要。

10.3.1 设置应用程序组件的权限

将 IAM 想象成您的数字资产的看门人，在授予访问权限之前仔细检查每个实体的凭据。这个系统定义了谁可以进入，并概述了他们在数字领域的能力，类似于俱乐部里保镖的角色。

1. **最小特权原则：**分配访问权限，类似于分发钥匙卡，只为一个角色打开必要的门，最大限度地减少未经授权访问敏感区域的风险。

2. **持续监控：**通过持续监控保持警惕，类似于安全团队监控闭路电视镜头，以及时发现和处理任何异常的访问模式。

3. **职责隔离：**实现多个安全层，如建筑物内的各种检查点，以稀释访问权限的集中，从而避免潜在的滥用或妥协。这也意味着开发人员应该为不同的环境使用不同的权限（例如，Dev vs. Prod）。

4. **联合：**通过实现通用访问协议（很像普遍接受的钥匙卡）来简化跨不同系统或组织的访问，以简化和保护跨平台交互。.

下图描述了 IAM 的过程，说明了用户、身份提供者和服务提供者之间进行认证和授予访问权限的交互过程。

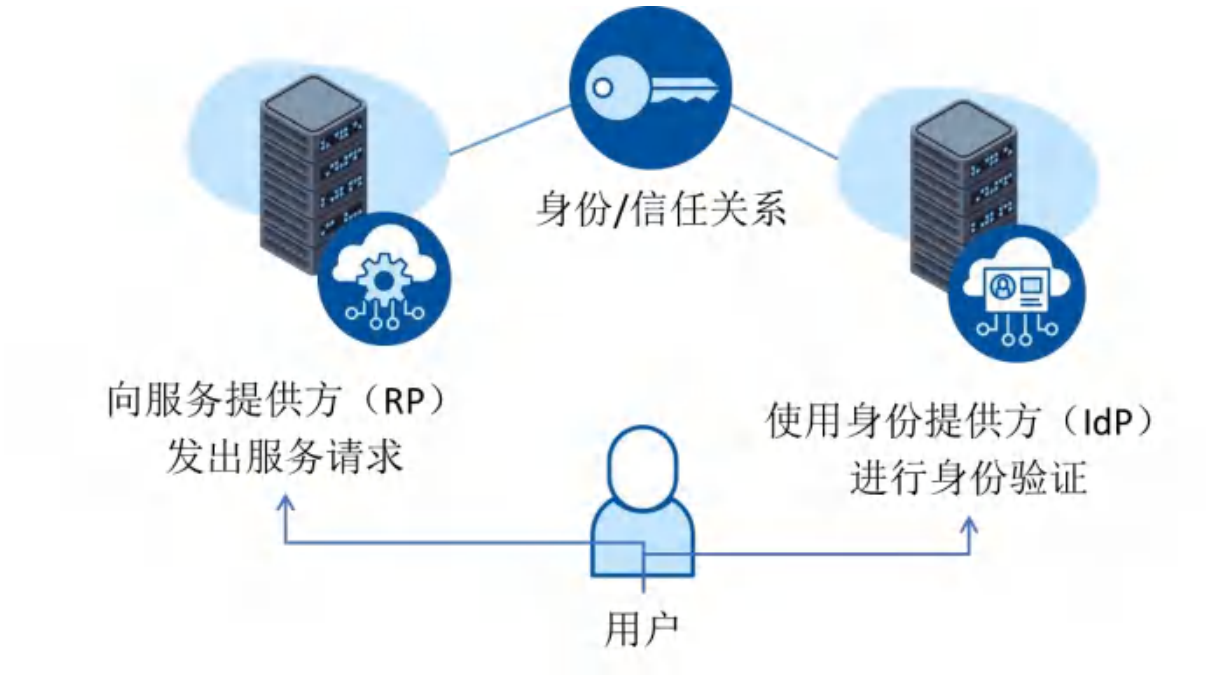


图 56：应用程序安全的 IAM 和机密管理

10.3.2 密钥管理

密钥是数字身份验证凭证（如密码、密钥和令牌），应用程序或基础设施服务使用它们在它们之间或与其他服务进行通信（与人类使用的身份验证凭证相反）。密钥管理是安全处理这些凭证的实践。有效的密钥管理可确保这些敏感元素得到安全的存储、访问和管理，防止未经授权的访问，并降低数据泄露的风险。它涉及系统地创建、分发、轮换和撤销访问凭证的工具和策略，以及秘密泄漏检测，从而保护整个基础设施中数据的完整性和机密性。

以下是密钥管理的一些功能：

● **自动提供凭证：**这就像拥有一个值得信赖的助手，在正确的时间为您提供正确的钥匙，确保服务无需人工干预（和人为错误）即可访问所需的内容。

● **安全存储：**密钥以安全的方式存储，类似于贵重物品存储在银行金库中。

● **与 API 集成：**当应用程序需要验证自己时，密钥会通过安全通道提供给它们，例如在被要求时出示身份证。

● **跨团队共享秘钥：**当团队需要使用相同的凭证时，密钥管理系统允许他们在不看到密钥的情况下这样做，就像共享银行账户一样，你可以在不知道账号的情况下花钱。

密钥管理通常以两种方式之一部署：嵌入式或客户端-服务器。这两种模型都旨在确保机密的安全，同时使应用程序的授权部分可以访问它们。 选择嵌入式和客户端-服务器模型之间的区别通常取决于应用程序的特定需求，例如可扩展性和安全性要求。选择正确的模型对于确保密钥（王国的数字钥匙）在应用程序的生态系统中得到良好保护且正常运行至关重要。

● **嵌入式模型：**在这种模型中，机密管理直接内置于应用程序或系统中一可以将其想象为酒店每个房间都有一个保险箱。它主要出现在 Kubernetes 等容器化环境中，其中应用程序与其所有依赖项（包括机密）一起打包。密钥只使用一次，可以在容器环境中广泛共享，但有时这可能有点过于公开，就像离开房间时忘记锁保险箱。

● **客户端-服务器模型：**此部署模型中的密钥管理更像是具有多个分支机构的银行。您有一个存储所有秘密的中央服务器(主分支)，客户机(其他分支)根据需要请求访问这些秘密。这种设置可以处理大量请求，因为它被设计成将工作负载分散到多个服务器上。此外，它跨不同的服务器复制秘密，以确保它们在需要时始终可用，并在一台服务器出现故障时提供备份。这种方法平衡了安全性和可访问性，确保密钥是安全的，但仍然可以随时获得系统的授权部分。

如今，大多数云提供商都提供静态密钥的替代方案。根据部署方案，可以通过将 IAM 角色/身份分配给服务来避免机密。对于必须使用密钥的场景，所有 IaaS/PaaS 提供商都提供安全存储服务来保证机密的安全。这些服务与 IAM 集成，无需将机密保存在应用程序代码、配置文件或其他不安全的存储中。对于多云和本地部署，也存在第三方服务。

下图说明了生成和管理 X.509 证书的过程，包括创建密钥对、提交证书签名请求 （CSR）以及由证书颁发机构（CA）颁发。

图 57：IAM 和机密管理流程

10.4 DevOps 与 DevSecOps

DevSecOps 是开发、安全和运营的缩写，可自动集成整个 SSDLC 中的安全性。DevSecOps 将“安全性”引入 DevOps 流水线。DevOps 流水线是一组自动化流程和工具，允许开发人员和运营专业人员协作构建代码并将其部署到生产环境并快速生产软件产品。它建立在 CI/CD 模型的概念之上。DevSecOps 通过确保安全性的纳入来增强和强化此 DevOps CI/CD 模型。

- **持续集成（CI）：**开发人员经常将他们的代码变更合并到共享存储库中。这个阶段需要部署前的自动化安全测试（例如 SAST）。
- **持续部署（CD）：**一旦代码通过了 CI 阶段，它就会自动部署到测试或临时环境中。这确保了代码变更能够快速且一致地交付。在这个阶段需要部署后的自动化安全测试（例如 DAST）。

DevSecOps 强调在 CI/CD 流水线的最早阶段就引入安全措施和测试，确保安全考虑是应用程序开发和部署周期的一个组成部分。该方法旨在通过将安全检查、扫描和测试嵌入到 CI/CD 工作流中，从而实现核心安全任务的自动化，从而促进代码变更的快速而安全的交付。

10.4.1 DevSecOps

DevSecOps 将安全性与 DevOps 的敏捷协作和自动化融合在一起，强调了软件开发和部署的整体方法。在本质上，它利用 CI/CD 来自动化和简化流程，使云集成无缝且更安全。采用标准化可以确保从开发到生产的所有环境都是一致的，从而减少出错的机会。自动化测试将安全检查集成到 CI/CD 流水线中，在不牺牲速度的情况下增强了安全性。基础设施中的不变性概念支持自动化部署，并减少与手动变更相关的风险，在基础设施中可以快速可靠地创建环境。

此外，改进的审计和变更管理功能提供了变更的透明性和可追溯性，从而增强了安全性。通过将安全实践集成到 DevOps 中，DevSecOps 优化了运营效率，并显著增强了应用程序和基础设施的安全弹性。

下图说明了 DevSecOps CI/CD 周期，突出了 DevSecOps 阶段的集成，以确保软件的持续和安全交付。

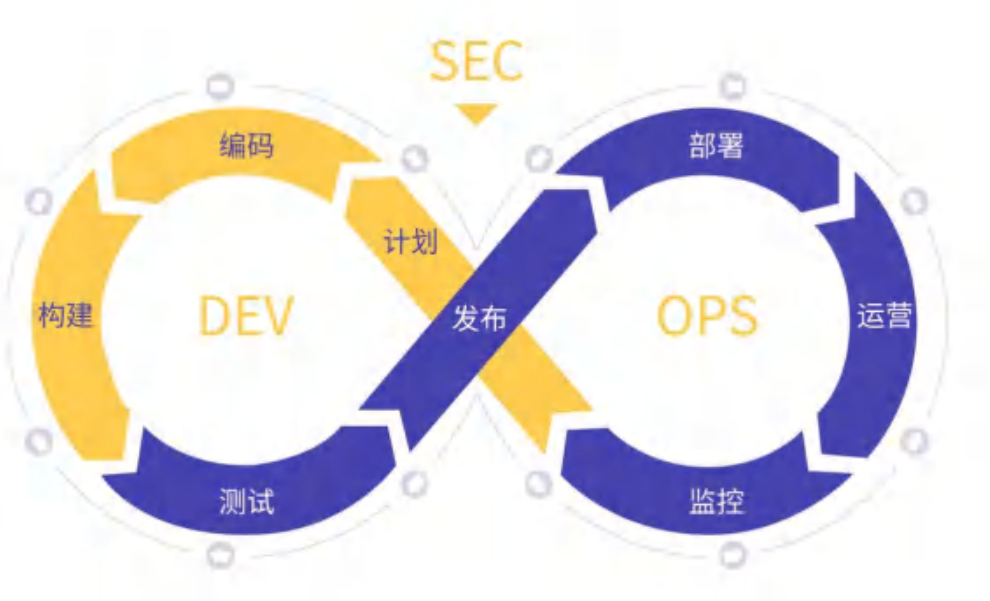


图 58：DevSecOps CI/CD 周期

10.4.2 CSA DevSecOps 的六大支柱

DevSecOps 的六大支柱提供了一个全面的框架，用于将安全性集成到 DevOps 实践的结构中，旨在有效地开发安全的软件。这些支柱强调了共享责任、协作、实用工具、实践选择、协调开发合规性、最小化错误的自动化，以及通过可运维的量度进行持续改进的重要性。

每个支柱都是转换软件开发中使用的文化、过程和工具的基础，确保安全性是从开始到部署的生命周期的一个组成部分。这种整体方法促进了向主动安全实践的转变，其中每个团队成员都被授权为其项目的安全状态做出贡献，弥合了开发、运营和安全团队之间的传统差距。

DevSecOps 的六大支柱:

1. **集体责任**
    a. 安全是所有团队的共同责任。
    b. 培养积极主动、安全意识强的组织文化。
2. **协作与集成**
    a. 跨职能团队合作对 DevSecOps 的成功至关重要。
    b. 弥合知识差距，培养统一的安全意识。
3. **务实的实施**
    a. 选择适合组织需要的工具和实践。
    b. 专注于将安全无缝集成到开发过程中。
4. **建立合规与发展的桥梁**
    a. 通过自动化使遵从性与敏捷实践保持一致。
    b. 在软件生命周期内集成安全措施，以增强风险缓解。
5. **自动化**
    a. 是 DevSecOps 精简流程和减少错误的核心。
    b. 确保高效、一致的安全检查，提高软件质量。
6. **测量、监测、报告和行动**
    a. 为持续改进实施可测量和可运维的度量标准。
    b. 关注部署频率、补丁时间、测试覆盖率和漏洞响应。

该框架强调了将安全性集成到 DevOps 中的综合方法，通过协作、自动化和持续改进来确保安全的软件开发。

10.4.3 DevSecOps 实践

在已经提供的使 DevSecOps 在实践中发挥作用的概念的基础上，我们开发了一种结构化的方法，将安全性无缝地集成到 DevOps 流程中。

● **检测：**实施实时监控系统，像警惕的哨兵一样，尽快扫描和识别安全问题、威胁或错误配置，确保快速响应。

● **自动化：**利用技术自动化重复的安全任务，类似于拥有独立运行的智能系统，从部署补丁到管理配置，确保安全措施始终是最新的，并始终得到执行。

● **交付：**建立高效和直接的通信协议，确保安全警报通过熟悉的工具到达适当的专家，优化团队行动的响应时间和有效性。

● **安全运维：**将安全维护纳入日常工作，将安全问题作为运营的定期和主动的一部分来解决，就像日常清洁将保持餐厅的卫生标准一样。

通过遵循这些关键要求，组织可以在日常运维中嵌入安全性，培养安全和发展齐头并进的文化，以持续维护和改进安全状况。

10.4.3.1 左移与内生安全

如果将 SSDLC 看作是一个水平的步骤过程，那么安全性主要只存在于最后一个步骤，即维护阶段——作为生产应用程序发生安全事件后的反应性措施。左移（Shift-Left）是一个短语，用来表示安全性应该转移到 SSDLC 的早期阶段，以确保设计安全和默认安全的产品。左移（Shift-Left）通过确保 SSDLC 的每个阶段，从开始和规划开始，通过安全的视角来看待，从而实现主动安全。与 SSDLC 后期阶段的补强安全性相比，这种方法也具有成本效益。

下图概述了 DevSecOps 模型中跨不同开发阶段（从架构和开发到生产）的安全性集成，强调了持续的安全性测试和监控。

图 59：DevSecOps:跨开发阶段集成安全性

左移还有助于及早发现漏洞。而不是等待测试完整构建的产品，或者更糟的是，等待攻击者利用漏洞，左移安全工具可以使开发人员尽早识别漏洞并修复它们，从而加强整个开发过程以生产可快速恢复的产品。

下表总结了在 SSDLC 各个阶段应用的主动安全措施，突出了特定安全技术的实施位置及其目的。

表 9：在整个 SSDLC 中采取的主动安全措施

在哪里?	做什么?	为什么?
集成开发环境(IDE)	SAST	检测源代码漏洞并为开发人员提供实时反馈他们编码
存储库	软件组成分析（SCA）	检测脆弱性依赖项和库
构建阶段	安全单元测试	检测模块级安全性漏洞
质量保证阶段	SAST IAST DAST	检测静态代码和运维漏洞
预发布阶段	DAST	检测运维漏洞

运营阶段	Web 应用程序防火墙 (WAF) 运行时应用程序自身保护（RASP）	监控并预防攻击

10.4.3.2 SecOps：Web 应用程序防火墙和 DDoS

即使在部署后，Web 应用程序仍然需要强大的安全措施。实施网关服务、分布式拒绝服务 (DDoS) 保护和 Web 应用程序防火墙(WAF)至关重要。这些工具旨在确保应用程序仍然可供合法用户访问，并能有效管理网络流量的涌入，防止因过载而导致的潜在崩溃。必须强调的是，WAF 是一种预防性控制，不能用作纠正性控制或对开发不良的应用程序的保护。始终记住将安全性放在 SSDLC 的左侧，正如前面所讨论的那样。

IaaS/PaaS 服务中 WAF 和 DDoS 防护的常见部署场景有四种：

1. **代理部署：**当使用 IaaS VM 作为 Web 服务器时，可以在运维系统上安装 WAF 代理。此选项通常不具备 DDoS 缓解功能。

2. **云提供商服务：**IaaS/PaaS 提供商提供集成的 WAF 和 DDoS 防护服务，通常部署在负载均衡器服务上。

3. **第三方市场服务：**IaaS/PaaS 市场提供各种部署在专用虚拟机上的第三方商业 WAF 软件。客户负责部署 WAF 并确保路由、冗余和负载均衡。

4. **SaaS 化的 WAF 和 DDoS 服务：**使用 DNS 重定向，消费者流量被路由到第三方 WAF 服务，经过检查和过滤，然后路由到云提供商环境。

下图说明了 API 网关安全架构，突出显示了 WAF 与 DDoS 防护的集成，以确保安全高效地管理 Web 流量。

图 60：API 网关安全架构

10.5 无服务器和容器化应用程序注意事项

在不断发展的应用程序部署领域，无服务器计算和容器化的重要性日益凸显。无服务器计算使组织无需管理任何底层基础设施即可构建应用程序，从而提供可扩展性和成本效益。同时，容器化将应用程序封装在一致的环境中，从而增强了可移植性。这两种技术都以其独特的优势塑造了现代部署实践，因此有必要了解它们特定的安全影响。我们将在本节中探讨这两种技术。

10.5.1 无服务器和容器对应用程序安全的影响

在不断发展的应用程序部署领域，无服务器和容器技术正在重塑安全实践。安全措施和策略必须适应这些新环境，每个环境都有其独特的考虑因素。随着部署方法的进步，了解这些考虑因素对于维护应用程序安全至关重要。

10.5.1.1 无服务器注意事项

以下是无服务器考虑事项的示例:

● **减少攻击面：**无服务器函数的瞬态特性，即在没有持久存储的情况下执行单一、短暂的运维，本质上限制了攻击的暴露。

● **依赖风险**：依赖外部代码或服务会带来安全风险，类似于在产品制造中使用具有未知安全记录的第三方组件。

● **IAM 复杂性**：无服务器函数的短暂性和分布式特性需要复杂的访问管理，可与在众多不断变化的接入点之间维护安全性相媲美。

10.5.1.2 容器注意事项

以下是容器考虑事项的示例：

● **隔离风险**：集装箱环境中的隔离不足可能导致安全漏洞，类似于连接房间中的屏障不足，可能使入侵者容易通过。

● **不可变基础设施**：容器被设计为在部署后不可变，促进一致性并减少风险，如明显的篡改包装。

● **复杂的配置管理**：随着规模的增加，管理容器的复杂安全配置成为一项挑战，类似于监督跨多个设施的高级安全系统的复杂网络。

下图突出了容器安全性的关键考虑事项，包括代码、运行时、库、环境和配置，这些对于在容器化应用程序中维护健壮的安全性至关重要。

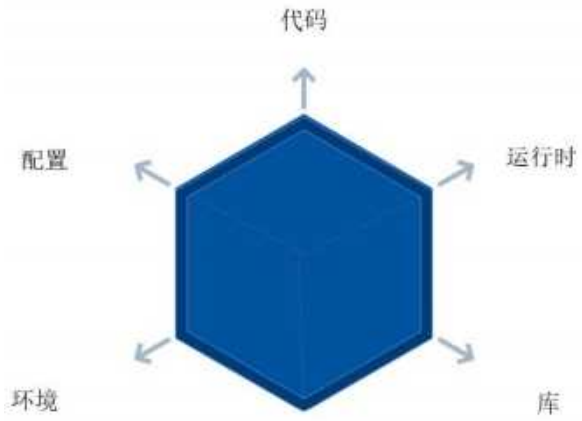


图 61:容器注意事项

总结

云计算是应用程序安全性进步的主要驱动力，它要求进步是稳定的、可扩展的和安全的。安全开发生命周期提供了必要的技术和方法指南，以帮助制作和维护安全的云应用程序。

为了真正加强您的数字生态系统以抵御不断发展的网络威胁，将应用程序安全原则嵌入云计算战略的核心至关重要。这涉及到从初始设计阶段到部署和持续维护的安全性集成。

关键要素包括:

● **安全架构**：通过将安全措施纳入设计阶段，构建安全基础，确保对潜在威胁提供强大的保护。

● **身份和访问管理(IAM)**：实施密钥管理策略以保护应用程序处理的业务数据至关重要。IAM 和秘密管理共同构成了访问控制和数据保护策略的支柱

● **DevSecOps:** DevSecOps 的集成强调了在整个开发生命周期中对应用程序安全性的承诺。这种方法在无服务器计算和容器化等现代部署实践中尤为重要。

● **持续监控和改进**：采用持续监控、威胁建模和自动化安全测试有助于及早识别和减轻漏洞，确保弹性应用程序的安全状态

通过遵循这些指导方针并利用云安全联盟(CSA)的建议，组织可以创建一个安全、有弹性和可扩展的应用程序环境，以应对云计算带来的独特挑战和机遇。

建议

CSA 安全开发生命周期(SSDLC):

● 安全设计和架构：在设计阶段应用技术和工具，尽早集成安全性，避免后期更高的成本和瓶颈。

● 持续构建、集成和测试：在部署之前使用工具和流程来测试漏洞，以防止安全漏洞。

● 持续交付和部署：进行部署前的安全检查，以确保应用程序部署在安全的基础设施上。

● 运行时防御和监控：实施实践，以持续识别和减轻部署后的漏洞和低效率。

采用结构化威胁建模:

● 应用 STRIDE 框架对威胁进行分类：欺骗、篡改、拒绝、信息披露、拒绝服务和特权提升。

关注安全云设计:

● 使用平台即服务(PaaS)和其他云服务提供商（CSP）服务，将安全责任转移给提供商。

● 对所有组件实现最小权限 IAM (Identity and Access Management)。

● 使用云服务提供商（CSP）服务，如负载均衡器和安全组，以尽量减少面对互联网的风险。

集成安全测试方法:

● 静态应用程序安全测试(SAST)：在部署前自动检查代码以识别漏洞和逻辑错误。

● 软件组合分析(SCA)：审计外部组件的漏洞和许可风险，并创建软件材料清单(SBOM)以提高透明度。

进行全面的部署后测试:

● 动态应用程序安全测试(DAST)：执行黑盒测试，从外部角度评估应用程序的安全状态。

● 动态分析(Fuzzing)：输入不可预测的数据，以识别运维过程中的错误和漏洞。

● 交互式应用程序安全测试(IAST)：结合 SAST 和 DAST 来识别代码和运行时的漏洞。

● 渗透测试：进行模拟攻击，利用已知漏洞，测试系统的弹性。

● 漏洞赏金计划：利用道德黑客社区发现和报告漏洞。

加强访问控制:

● 应用最小权限原则，最大限度地减少未授权访问。

● 实施持续监控，以检测和解决异常的访问模式。

● 使用职责隔离来管理访问权限，防止滥用。

● 采用联合简化和安全的跨平台交互。

密钥的管理:

● 自动提供凭据，尽量减少人为错误。

● 安全地存储秘密，类似于金库中的贵重物品。

● 通过安全通道将秘密与 api 集成。

● 促进秘密共享而不暴露秘密，就像共享银行账户一样。

将安全性集成到 CI/CD 流水线中:

● 实现嵌入安全检查的持续集成和部署。

● 在 SSDLC 早期使用左移策略来识别和解决漏洞。

● 自动执行重复的安全任务，以确保一致的执行和及时的更新。

- 促进开发、运营和安全团队之间的协作。

适应现代部署的安全策略:

- 无服务器考虑:
  - 利用瞬时无服务器函数减少的攻击面。
  - 解决依赖风险，管理复杂 IAM 需求。
- 容器注意事项:
  - 确保强大的隔离，以防止漏洞。
  - 使用不可变的基础设施，提高一致性和安全性。
  - 随着容器部署规模的扩大，管理复杂的安全配置。

补充指南

- DevSecOps 的六大支柱| CSA
- 基于自反性安全的信息安全管理| CSA
- 基于 NIST 800-53 R5 控制| CSA 的 faas 无服务器控制框架(集
- DevSecOps 的六大支柱——实用实现| CSA
- 采用云原生密钥管理服务的建议 | CSA
- 提供和使用 API 的安全指南| CSA

领域 11：事件响应与韧性（恢复力）

事件响应（IR，Incident response）是任何信息安全计划的核心环节。云服务用户（CSC，Cloud Service Customer）无论安全防护多么周密，都很难避免出现安全漏洞。虽然许多云服务用户都制定了事件响应计划以应对攻击，但云计算的引入带来了流程、技术和治理上的新挑战，使得事件响应变得更加复杂。

此领域旨在确定和解释云事件响应和韧性（恢复力）的最佳实践，安全专业人员在制定自己的事件计划和流程时可以将其用作参考。此领域的结构遵循 CSA 云事件响应（CIR，Cloud Incident Response）框架 和 NIST 计算机安全事件处理指南（NIST SP 800-61 Rev. 2） 中广泛认可的事件响应生命周期。此外，还包括 CSA 事件响应研究中心以及其他国际标准框架，如 ISO/IEC 27035 和 ENISA 事件响应与网络危机合作策略。安全专业人员可以在制定事件响应计划和执行其他事件响应生命周期活动时参考这些资源。

学习目标

该领域的学习目标旨在为读者提供以下方面的知识：

- 区分事态、事件和事故，并使用响应流程进行应对。
- 准备并响应事件。
- 检测并分析相关数据。
- 遏制、根除与恢复。
- 执行韧性规划以应对失败。

11.1 事件响应与韧性（恢复力）

事件响应（IR）是应对意外事件的过程。它要求清楚地区分事件、事件响应和安全漏洞，每种情况代表不同程度的威胁，并需要量身定制的响应策略。准确识别并分类这些事件是保持云服务的完整性、可用性和机密性的基础，最终也有助于保护数字资产和利益相关者的信任。

在云安全的背景下，事件是指系统或网络中发生的任何可观察到的事件，这些事件可能或可能不表示与安全相关的潜在问题。所有的事件都可能成为事件响应对象，但并非所有事件都构成安全事件，除非它们违反了明示或默示的安全政策，可能会危及正常运营并对云环境造成威胁。事件需要立即处理以防止其升级。最高级别的是安全漏洞，这表示安全防护措施被突破或绕过，导致未经授权的访问或数据泄露。理解事件、事件响应和安全漏洞之间的差异，有助于制定有效的事件响应策略。

11.1.1 事件响应生命周期

事件响应和管理框架已经由许多组织进行开发和文档化。不同的框架有不同的目标和受众。CSA 采用了 NIST 计算机安全事件处理指南（NIST 800-61 Rev 2 08/2012）中普遍接受的事件响应生命周期的术语。

事件响应生命周期是云客户有效准备和管理云事件的指导。NIST 所描述的事件响应生命周期包括以下阶段和主要活动：准备阶段、检测与分析、控制、消除与恢复，以及事后分析。

图 62：云安全中的 IR 生命周期阶段

准备阶段：建立事件响应过程。

- 组建一个有明确角色和责任的团队，包括培训和演练。
- 制定沟通计划和设施。

- 为响应人员提供访问环境和工具的权限，如事件分析服务、硬件和软件。
- 创建内部文档（端口列表、资产列表、网络流量基线）。
- 评估基础设施：主动扫描和监控、漏洞和风险评估。
- 订阅第三方威胁情报服务。
- 评估云服务提供商及其在事件响应方面的能力。
- 审计日志、快照、取证能力和电子发现功能。
- 定期进行备份恢复测试，并至少每年进行一次灾难恢复（DR）测试，以确保事件响应计划的时效性和有效性。

检测与分析阶段：识别安全事件并分析其影响

- 进行检测工程。
- 利用来自云安全态势管理（CSPM）、安全信息与事件管理（SIEM）、工作负载保护和网络安全监控的警报。
- 验证警报以减少误报并避免过度升级。
- 估计事件的范围。
- 指派事件经理协调后续行动。
- 构建攻击的时间轴。
- 确定潜在的数据丢失或影响程度。
- 通知相关渠道并协调活动。
- 向高级管理层通报事件的隔离和恢复状态。

控制、消除与恢复阶段：隔离事件，防止进一步损害并解决根本原因，恢复受影响的系统。

- 控制：包括隔离身份和工作负载，关闭系统或服务，并考虑数据丢失与服务可用性之间的权衡。
- 消除与恢复：清理受损的资产，并将系统和服务恢复到正常运营状态。部署控制措施以防止类似事件的发生。
- 捕获事件数据：记录事件并收集取证证据（如证据链）。

事后分析阶段：从事件中学习，总结经验并改进未来的响应。

- 经验教训：什么可以做得更好？攻击是否能更早检测到？哪些额外的数据能帮助更快地隔离攻击？事件响应过程是否需要改进？如果需要，如何改进？
- 分享经验教训：将学习到的经验与更广泛的安全社区共享。

云计算对所有事件响应生命周期阶段的活动产生影响，带来了新的机遇和挑战。同时，许多事件可能涉及云与传统基础设施和设备，要求事件响应者确保不要因只关注事件的一个方面而忽视整个事件的复杂性。

11.2 准备阶段

准备阶段可分为四个主要类别，以下章节将详细介绍：

- 与云服务提供商的关系所带来的变化
- 响应者培训的变化
- 支持云事件响应（CIR）流程所需的变化
- 支持云事件响应技术所需的变化

准备阶段通常是启动 CIR 程序时最具挑战性的部分。信息安全事件响应的基本原则没有改变，但云计算的技术和操作差异显著影响了这些流程的具体操作。如果在准备阶段未能考虑到这些差异，可能会严重限制有效响应的能力。

以下是一些CIR方面的关键差异：

- 云操作往往更加分布式，各个团队定义并管理自己的基础设施。这会导致访问和遥测数据收集的问题。
- 每个云平台在最基本的技术层面上都存在巨大差异。事件响应需要适当且兼容的工具，并具备深入的专业知识。
- 云攻击可能高度自动化，并且发生得非常迅速。云资源可以通过一次简单的配置更改轻松变为公开或共享。这要求某些事件类型需要非常快速的响应，可能需要流程和技术的改变，以支持并启用全天候的快速响应能力。

● 响应者通常需要对受影响的部署和资源进行广泛的按需访问。仅通过日志访问通常不足以全面分析和响应云事件。分析员和响应者需要迅速理解日志中的上下文，这可能涉及通过 API 或 Web UI 直接查看配置和资源。

11.2.1 事件响应准备和云服务提供商

云事件是共享事件，即使客户拥有所有受影响的资源。任何涉及公有云的事件，都需要理解与云服务提供商的合同协议，包括具体的服务水平协议（SLA）以及提供商所提供的资源。根据与提供商的关系，您可能无法直接联系，并且可能只能通过标准支持渠道获得帮助。许多提供商提供不同级别的支持，您应根据业务关键性的需求选择合适的支持级别（例如，对于任何关键业务部署或包含敏感或受监管数据的部署，选择更快捷的支持渠道和直接联系）。

除了付费支持外，一些提供商会向客户提供一定程度的事件响应协助，无需额外费用。对于与您合作的每个提供商，列出可用的事件支持选项（付费与免费）及其联系方式非常重要，并应将其整合到云部署注册表中。

在某个时刻，您的云服务提供商可能会检测到涉及您资源/部署的事件。因此，确保您的联系信息保持最新并且能够直接发送到您的安全团队是至关重要的。

这些通知通常分为以下几类：

● 滥用通知：当提供商检测到您的资源可能被用于危害他人时。请记住，这些通知不总是准确的，需要进行验证。

● 安全漏洞通知：涉及您资源的安全暴露，比如检测到私密访问凭证被发布到公共代码仓库中。

● 可疑活动通知：可能表明发生了数据泄露或其他攻击的活动。

● 提供商端事件通知：可能会影响您的数据或资源（例如，提供商发生了数据泄露、成功的攻击或数据暴露等）。

● 对于点击式服务，通知通常会发送到您的注册邮箱地址；这些邮箱地址应由企业进行控制并持续监控。

在这个阶段，还需要为那些影响 CSP 且超出 CSC 控制范围的事件制定计划。例如，有记录显示公共漏洞和拒绝服务攻击会影响 CSP。CSC 并非完全无能为力，根据事件的性质，可能可以自

行执行一些响应措施。事件响应团队应该意识到这种风险，并预演一些可能的情景及缓解行动。这通常需要与业务连续性活动进行协调。

11.2.2 云事件响应人员培训

尽管 CIR 实践与传统的事件响应实践共享许多特征和流程，但响应者需要理解这些过程和技术上的差异。

培训和各种演练相结合，可以迅速帮助响应者或团队掌握所需技能，如：

● 通用 CIR 培训帮助构建适用于多个云服务提供商的基础技能。这对于提升云安全意识也是一个良好的选择，即使是那些不会专门从事云事件响应的响应者。

● 针对特定提供商的技术培训对于任何从事主要平台（特别是 IaaS）工作的响应者至关重要。这种培训不仅限于使用提供商提供的 IR 工具，还需要深入了解如何隔离暴露的服务凭证、如何分析日志等。

● 基于场景的演练通过模拟环境帮助练习核心技能，如日志分析、威胁狩猎和资源隔离。

● 完整的演练和红队演习旨在测试整个事件响应流程。

● 面对分布式云团队和领导的桌面演练有助于确保不同团队能够合作协调。桌面演练可能包括大规模事件的模拟，如提供商发生数据泄露。

11.2.3 支持云事件响应流程的更新

事件响应（IR）流程的核心并不会发生根本变化，但 IR 团队将需要调整他们的流程，以适应一些不同的情况。标准的 IR 手册和行动指南并不适用于大多数云事件。它们通常侧重于网络数据包捕获、取证和其他活动，这些活动即使在云环境中需要，也通常是在确保没有发生身份和访问管理（IAM）或管理平面权限提升等更优先事项之后进行的。应该为预期的事件类型创建新的行动指南和手册，这些指南和手册应该是专门针对云环境的。云行动指南和手册应该包括何时邀请非 CIR（Cloud Incident Response）专家参与，并定义对于那些需要两个领域的技能和流程的事件的响应流程，例如，跨越混合连接的云入侵，或针对受损云资源的恶意软件分析。

本地手册和行动指南也应针对两种主要的事件类型进行更新。首先是攻击者在非云环境攻击中获取的云凭证的泄露和滥用。其次是来自已被攻破的资源（如本地服务器或工作站）对云资源

的攻击。作为一个流程，应该有一个要求，即每当出现新的事件类型时，都要为该事件类型创建一个行动指南或手册。除非是严格的云环境，否则您将遇到涉及云和传统基础设施的混合事件，例如涉及员工设备的事件。因此，确保如果您有专门负责云的响应人员，存在处理跨越两种环境的混合事件的流程就显得尤为重要。

如果业务连续性、领导层、法律和合规团队存在，他们需要理解在云事件中的角色，并相应调整他们的流程。云服务提供商泄露了您的客户数据，将涉及不同的危机沟通和法律与合规要求。响应流程，包括行动指南、手册以及整体流程，必须特别关注任何涉及管理平面的云事件的影响。如今，攻击者可能会跨越进入管理平面并提升权限。如果响应人员只关注云资源（例如受损虚拟机），可能会错过攻击中最具破坏性的方面。云事件通常由于攻击者自动化操作而发生得非常迅速。流程必须考虑到这一速度差异。例如，如果事件处理人员依赖的是 15-60 分钟前的日志数据，就无法有效应对实时的云事件。

11.2.3.1 启用响应者访问权限

其他团队和组织在支持 CIR 时需要进行一些关键调整。CIR 团队应具有对所有部署的持续读取权限。没有访问权限去审查相关资源和配置，几乎不可能有效调查一个云事件。所有此类权限的使用都应该被记录并定期审查。根据云服务提供商的能力，应该支持两个级别的访问：

- 对元数据和配置的读取权限（有时称为安全审计）应该是持续的，且是响应人员的默认访问级别。
- 完整的读取权限，允许查看数据，而不仅仅是元数据，通常应该需要多重批准才能使用，并遵循应急访问流程。

更高级别的响应人员应该有权限写入那些需要立即响应的关键情况，例如数据的公开暴露。传统的方法，如通过防火墙阻止访问，在这种情况下可能无法使用。这种权限应受到严格控制，需要批准，并且应使用应急访问流程，但必须在 24/7 时可用。这些响应人员应该非常熟悉云平台，只在最关键的事件中使用该权限。通常，这将涉及高层的批准，因为这授权他们为了安全而交换业务连续性。

在云环境中，分布式团队更可能直接管理自己的基础设施（IaaS/PaaS）。这可能导致许多难以区分攻击的活动。集中式 IR 团队可能缺乏足够的背景知识来理解它们是否是攻击的指示或是

预期的活动。因此，建立清晰的、实时的通信与部署所有者保持联系至关重要，以便将他们纳入 IR 流程。许多组织通过使用 ChatOps 将问题发送到团队，以验证它们是故意的还是潜在的攻击指示。ChatOps 可以以多种方式集成，并允许团队通过点击响应来升级或降级潜在的事件。如果云团队已经使用 ChatOps，这将是一个特别好的选项，因为安全团队可以使用与其他团队相同的通信工具。电子邮件和工单系统也是可选项，但速度较慢，这些时间延迟可能导致响应人员不得不追踪联系人。

IR 团队应该可以访问云部署注册表，并且该注册表应该包含与业务负责人和技术负责人联系的当前信息。事件响应人员可能需要访问持续集成/持续部署（CI/CD）管道、代码库和其他管理和修改云配置的位置。对于隔离、消除和恢复等响应流程，可能需要使用这些资源和服务。这是一个 IR 团队和部署或应用程序所有者必须准备共同工作的场景。

11.2.4 支持云事件响应的技术更新

支持 CIR 的最重要的技术变化是收集所需的安全遥测数据并实施云原生的威胁检测器。本节重点介绍支持 CIR 流程的其他准备性技术变化。

关键技术更新包括：

- 构建事件响应分析环境：这通常是一个部署环境，包含任何需要的分析工具，并能够连接到其他云部署以提取取证数据、日志和其他数据。访问其他账户可能涉及应急访问流程。
- 构建事件响应环境：这个环境通常是一个独立的云部署，配备响应工具，可以修改目标部署中的资源和配置。它可以与 IR 分析环境位于同一部署中，但理想情况下应该是分开的，因为它需要更高权限的访问，如完整的管理员权限。
- 云检测和响应（CDR）：CDR 工具可能与 SIEM 技术重叠，但侧重于处理实时的安全事件数据（而不是日志），路由和分类警报，并自动丰富警报。这些工具通常用于威胁检测，分类、升级、触发自动化的修复/响应。
- 取证：云取证对于虚拟机和容器需要更新的工具，这些工具可能需要在与源资源相同的云提供商中运行。其他取证来源，如源日志文件，可能需要复制和保存，在某些情况下可能只有提供商能够执行。

- 安全编排、自动化和响应（SOAR）：SOAR 工具应支持云操作和自动化，如连接到云服务提供商以丰富和支持分析，自动执行取证成像和其他云操作。
- 其他自动化和响应工具（例如“跳跃工具包”）：大多数云事件响应人员发现自己在使用商业工具、自定义脚本和开源工具的组合来支持调查和响应。这些工具可能与云 SOAR 和 CDR 平台集成，也可能没有集成，这取决于其他可用的工具。即使这些工具没有集成，许多响应人员仍然需要额外的工具来支持不同类型的调查。
- 攻击模拟：帮助响应人员进行培训和红队演练的工具，通过在指定的模拟环境或生产环境中进行故障注入/模拟攻击。这些工具不仅对于培训非常重要，还能验证检测器和遥测是否有效。
- 检测工程：云原生的威胁检测器通常包括日志分析、实时事件监控和配置变化监控等功能。检测工程活动将需要考虑这些新的数据源和活动流，并可能需要技术变更来支持云威胁检测器的生命周期管理。

11.2.4.1 行动指南和手册

行动指南和手册是处理特定事件类型的文档化流程。组织需要为云事件更新这些手册，并为响应新的云事件类型创建新的行动指南/手册。行动指南和手册有不同的定义，但核心目标是相同的。在 IR 上下文中，它们是调查和响应特定事件类型时所采取的步骤系列。

例如，如果检测到潜在的外部滥用凭证事件，来自一个未知的源 IP，行动指南/手册会提供逐步的指导，帮助调查和响应。现代的行动指南通常会在自动化系统（如 SOAR 平台）中实现，这些系统可以通过自动化执行某些步骤，并包含预构建的分析查询。

行动指南和手册是处理特定事件类型的文档化流程。组织需要为云事件更新这些手册，并为响应新的云事件类型创建新的行动指南/手册。行动指南和手册有不同的定义，但核心目标是相同的。在 IR 上下文中，它们是调查和响应特定事件类型时所采取的步骤系列。
例如，如果检测到潜在的外部滥用凭证事件，来自一个未知的源 IP，行动指南/手册会提供逐步的指导，帮助调查和响应。现代的行动指南通常会在自动化系统（如 SOAR 平台）中实现，这些系统可以通过自动化执行某些步骤，并包含预构建的分析查询。
以下是行动指南和手册的重要考虑事项：

● 行动指南和手册的具体性：首先强调，行动指南和手册应根据特定平台和服务进行定制。这可以确保响应对每种情况的独特性相关并有效。

● 版本控制：强调将这些文档保存在版本控制的仓库或 SOAR 系统中的重要性。这种做法有助于跟踪文档变化，确保团队始终使用最新的信息。

● 创建新的行动指南/手册：每当发生新的事件类型时，必须为该事件类型创建相应的行动指南。这种主动的做法可以确保在该类型事件再次发生时，团队能迅速应对。

● 计划 SOAR 系统失败的应对：即便已经部署了 SOAR 系统，仍然需要为其可能发生故障做好应急计划。必须认识到技术可能会失败，因此必须有手动流程或备用计划。

● 自动化集成：讨论如何将自动化融入到 IR 流程中。解释自动化应触发有助于更快解决事件的措施，但也应有检查机制，确保自动化不会干扰或加剧问题。

11.3 检测与分析

事故检测与分析的基本原理在引入云计算后在高层次上不会发生根本变化，但细节上会有显著变化。

云计算的主要差异包括：

● 云计算引入的新的遥测数据，用于检测和分析。

● 管理平面的攻击面必须成为响应过程中主要关注的焦点。

● 云中的活动频率较高，包括攻击者的速度（攻击者高度自动化）以及云环境本身的变化速度。

● 缺乏传统的网络边界，并且增加了身份和访问管理（IAM）的影响半径。

● 云的 API 驱动特性以及资源的短暂性。

● 云和开发团队对基础设施的去中心化管理。

● 自动化、基础设施即代码、无服务器架构及其他云原生技术。

这些差异有时会提高我们检测和分析事故的能力，但也带来了新的挑战。本节的指导内容突出了这些主要差异，并说明了如何调整检测与响应活动。

11.3.1 检测与威胁检测器

有必要为管理平面和 IAM 活动构建威胁检测器。这是最可能发生破坏性活动的地方，因为攻击者有可能直接修改基础设施。这些检测器应专注于活动，而非威胁行为者。云攻击者通常不会通过 IP 列表或连接头出现。活动直接发生在 API 层级，并且通常源自同一云服务提供商中被攻破的环境。例如，一个 API 调用将快照分享给一个未知的部署。

大多数针对云管理平面的攻击依赖于丢失、被盗或被滥用的凭证。来自已知网络和 IAM 边界之外的凭证使用，可能指示潜在的事故发生。由于许多攻击发生时凭证已被攻破，只有行为检测器才能检测到这种入侵。此外，云攻击往往是高度自动化的，并且速度非常快，导致数据在初次被攻破后几秒钟或几分钟内就被外泄甚至公开。对于最关键的活动（例如私人数据变为公开）应尽可能实时工作，或者至少在几分钟内进行检测。这比大多数响应人员在传统基础设施中处理事故的时间框架要紧得多。

配置更改，例如创建新的 IAM 用户或将资源共享给未知账户/订阅/项目，可能是构建云检测器的优秀数据源。这些“配置警报”可以来自直接的仪器化或使用 CSPM 工具（来自云服务提供商（CSP）、第三方、自建或开源）。事故响应人员通常无法知道特定的错误配置是攻击、错误还是该应用堆栈所必需的。这就是为什么与云账户团队的清晰和直接的沟通非常重要，响应人员可以快速判断这是错误还是攻击。一些组织正在采用 ChatOps 或类似的沟通方式，并将警报直接发送给负责的团队，这样他们可以通过应用内的按钮来回应，标明是错误、请求豁免或该活动是意外的，应该上报。

CSP 安全警报通常是检测的优秀数据源，但如果没有调优和过滤，可能会带来问题。例如，在一个锁定的生产环境中，它们可能非常高效，但在开发环境中会导致大量的假阳性。某些警报，如加密货币挖矿和潜在勒索软件的警报，即使在不太结构化的环境中也往往质量较高。其他集中于用户行为的警报则在更动态的非生产环境中效果较差。

检测工程也需要考虑“传统”事件来源，如操作系统受损、Web 攻击和数据库攻击。由于软件定义网络的固有差异，云网络通常不会进行完整的数据包捕获和监控。然而，流量和 DNS 活动可以是构建云原生网络威胁检测器的优秀数据源。

检测器应具有生命周期，最好使用与现代 DevOps/DevSecOps 实践兼容的版本控制和 CI/CD 流水线进行管理。由于被盗用和被滥用的凭证是云漏洞的主要来源，因此使用金丝雀（canaries）和蜜罐（honey tokens）可以成为识别被盗用身份存储库的出色检测工具。

金丝雀和蜜罐应集成到 IR 流程中，并触发立即调查，重点是追踪凭证的获取方式，并以此追踪攻击者。也可以使用蜜罐，蜜罐是基于系统/网络的，而不是以凭证为中心的金丝雀/蜜罐。

11.3.2 云对事件响应分析的影响

由于云计算环境具有短暂性、可扩展性和分散控制的特点，因此必须摆脱传统的 IR 分析。云环境中事件分析的焦点通常是管理平面，它通过日志提供对云活动的全面了解。这些日志对于识别未经授权的访问、错误配置和其他可能表明存在安全事件的异常情况非常有用。

云环境具有动态特性，资源可以快速配置和停用，这要求 IR 团队调整其方法。这包括利用自动化和机器学习来跟上云操作和配置变更的速度。云环境中的分析还优先识别公开暴露的资源，这需要迅速采取行动来缓解潜在的违规或合规性问题。

由于云的性质不同，分析的优先级应该有所改变。主要关注点应该是管理平面活动，而不是资源。攻击者可以根据其访问管理平面的能力造成大规模破坏或数据盗窃。攻击者还会尝试破坏部署中的资源，然后开始尝试使用资源权限进入管理平面。因此，即使是孤立的资源破坏（例如被黑客入侵的虚拟机），如果该资源具有任何内部权限或存储的凭据，也可以向攻击者开放管理平面。

另一个重点是任何公开或意外与来源不明的其他云部署共享的资源。这些都是常见的泄露技术，任何完全公开的资源

显然，暴露问题非常令人担忧。在全面调查事件的其余范围之前，可能需要立即遏制。由于丢失、被盗或滥用的凭证是云原生漏洞最常见的来源，因此分析应侧重于识别帐户中涉及的任何 IAM 实体并确定其权利范围（“IAM 影响半径”）和所有相应活动。指标（例如不同的源 IP 地址）可以帮助辨别这些凭证的预期使用和意外使用。

云管理平面活动日志是追踪攻击的极其强大的工具，因为它们通常显示所有活动，并且攻击者无法修改或删除。即使攻击者可以删除存储的日志，大多数主要云提供商仍会在 API 日志中提

供大约 90 天的活动记录，或者提供日志副本，如果您参与事件支持，这些副本可供检索。一些提供商仅在其 API 日志中记录变更事件，而不会显示读取活动，这消除了跟踪侦察的能力。

当安全遥测数据被输入到中央 SIEM 或安全数据湖时，分析师可能需要使用他们的读取权限直接访问和查看日志的本地版本。他们可能需要在日志被日志平台提取和规范化后查看原始日志，而无需保留原始的完整版本。分析通常需要分析师检查所涉及资源的配置，以便正确处理事件。他们不一定能够仅依靠日志分析。例如，安全组的变更不会帮助他们了解是否有使用该组的暴露资源以及可能的暴露风险是什么。

分析可能仍需要传统技能，因为云漏洞不一定仅限于云平台。例如，云分析师可能会确定凭证是从员工的笔记本电脑中窃取的，或者笔记本电脑本身就是攻击的来源，而无需员工参与。分析师应该让合适的同事具备跨主题域攻击的技能。对于使用 CI/CD 管理的环境，分析应包括流水线，因为这是攻击者的主要目标，也是破坏云应用程序和基础设施的强大载体。

如下图所示，有多个检测点可供执行：

- CDP
- SIEM
- CSPM/云原生应用保护平台（CNAPP）
- CSP/身份提供商 (IdP)

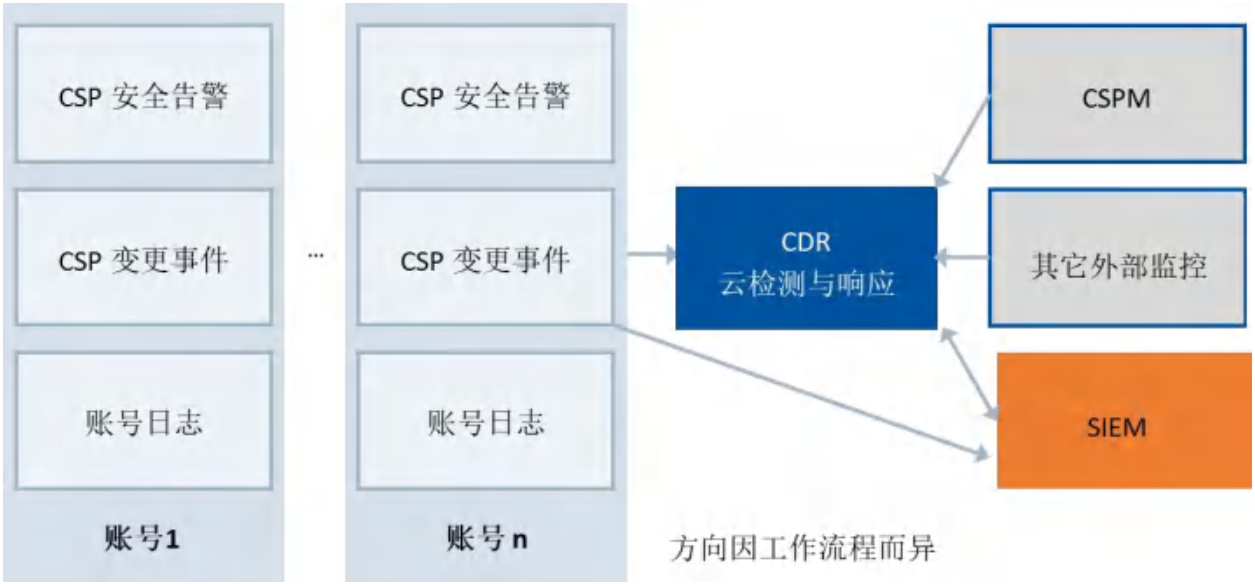


图 63：事件响应分析工作流程

11.3.3 分析优先级：RECIPE PICKS

RECIPE PICKS 是 Securosis 的 Rich Mogull 开发的一种助记符，用于培训云事件响应人员了解他们的初始分析优先级。这些优先级代表了在云管理平面事件期间首先要重点分析的地方，可用于解决大部分事件。

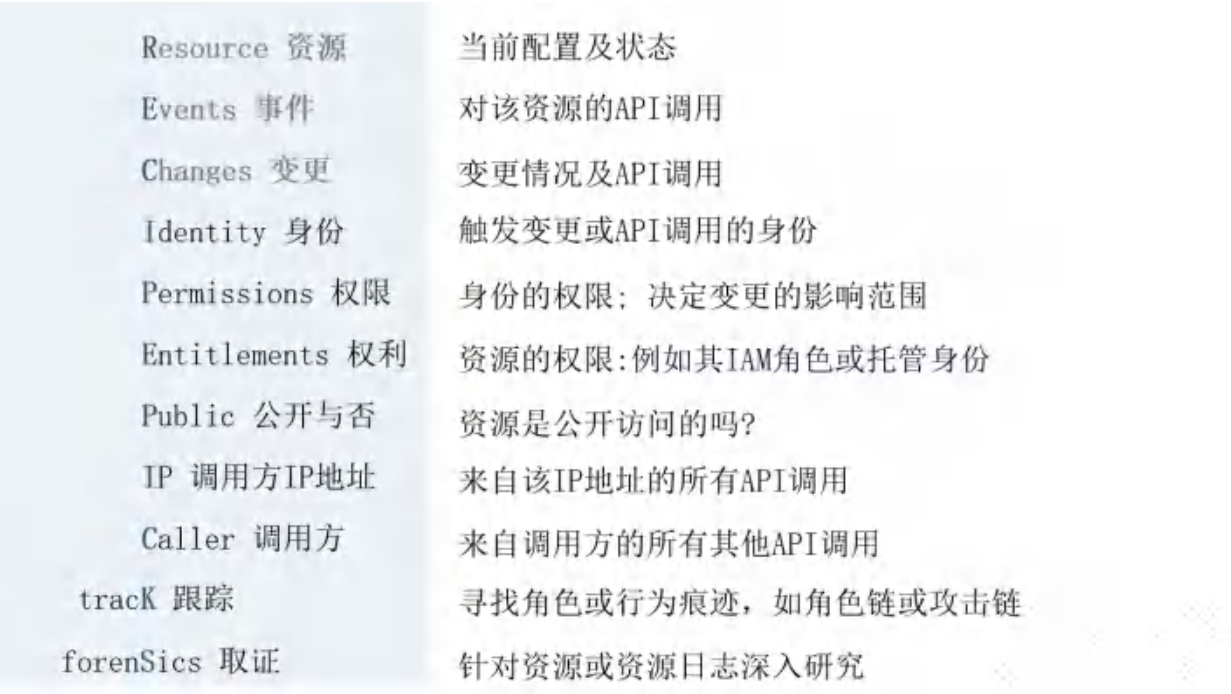


图 64： RECIPE PICKS：IR 分析优先级

注意：顺序无关紧要，除了最后两个（尤其是取证）。更重要的是，所有这些信息都在流程的早期进行收集和分析。

11.3.4 云系统取证

云取证主要分为两大类：管理平面、服务和其他日志的分析，以及虚拟机和容器的系统取证。传统的数字（系统）取证方法通常依赖于对硬件和本地数据存储的物理访问，而这在云中是不可能的。相反，云取证要求 IR 团队在 CSP 提供的约束和功能范围内工作。

云取证的关键方面包括：

● **快照**：几乎所有云提供商和容器管理系统都支持快照，可用于取证分析。了解如何以及为何在检测到事件时立即对存储卷进行快照，以保留虚拟机的状态以供分析。

● **易失性存储器采集：**如果没有检测硬件的能力，如果需要进行内存取证，响应人员将需要安装软件工具，这也会影响系统。

● **日志分析：**即使重点关注虚拟机/容器，管理平面日志以及系统、应用程序和用户活动日志也可用于呈现更全面的事件情况。

例如，它们可以帮助识别获取系统凭证并转向管理平面的攻击者。

● **证据保全：**在云环境中保存数字证据需要彻底了解 CSP 和 CSC 的备份和数据保留策略以及快照的保管链。

以下是使用取证采集和分析环境并从单独部署中受损的工作负载收集存储卷快照的示例。

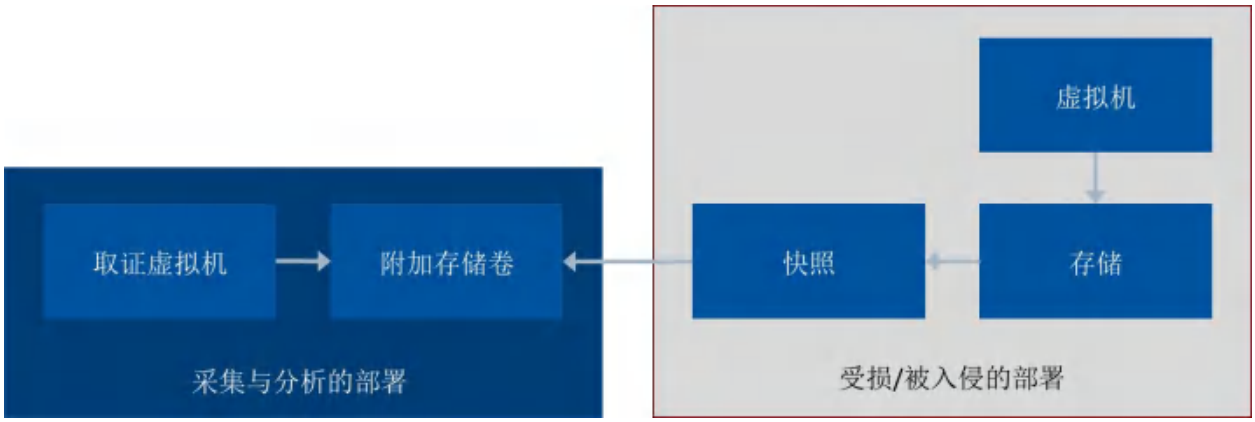


图 65：云取证：快照获取和分析流程

11.3.4.1 云取证：容器和无服务器计算注意事项

容器化和无服务器计算的兴起给云取证带来了额外的复杂性。

以下是容器和无服务器的关键注意事项：

● **容器：**容器天生就具有短暂性，通常只存在很短的时间。这种短暂性给取证数据收集和分析带来了重大挑战。取证策略必须包括捕获容器日志和容器状态快照，以深入了解活动和数据容器流程。因此，强烈建议您将容器日志、VM 日志和每个服务日志重定向到外部日志存储。这种方法的优点是可以将这些日志集成到 SIEM/SOAR 工具中，以改进威胁检测/响应，并由于容器和其他云服务的生命周期很短而提高执行取证分析的可能性。请注意，有时可以暂停并转储正在运行的容器的状态以用于取证目的。

- **无服务器计算：**无服务器架构进一步将执行环境从用户中抽象出来，由 CSP 管理底层基础设施。无服务器环境中的取证分析严重依赖于无服务器函数生成的日志，包括执行日志、访问日志和应用程序日志。理解无服务器函数的调用和执行模式对于重建事件期间的事件至关重要。同样，实施强大的监控也很重要，以便潜在地捕获正在进行的攻击并提供详细的日志以供取证。

11.4 遏制、根除与恢复

在所有的事件响应（IR）活动中，遏制、根除与恢复阶段最受云部署中使用的技术和架构模型的影响。不可变基础设施即代码（IaC）、自动扩展、微服务、身份联合以及底层技术在很大程度上影响这些活动的过程和技术。在许多情况下，与传统数据中心中的响应相比，这些技术带来了显著的优势。

11.4.1 遏制

在可能的情况下，与云和应用所有者合作，帮助确定正确的遏制计划非常重要。由于他们比任何中央事件响应团队更了解自己的部署环境，通常他们也能更好地实施这一计划。身份和访问管理（IAM）以及管理平面的遏制应当是任何安全事件中的首要任务。由于身份认证（AuthN）和授权（AuthZ）机制的分离，IAM 的遏制可能非常困难。云应用依赖于联合身份认证，其中认证和授权是分开进行的，且通常发生在不同的平台上。典型情况下，身份提供者（IdP）会向已认证的用户颁发一个会话令牌，授权方会使用该令牌进行授权。通常，依赖方会在会话令牌的生存时间（TTL）结束前继续接受该令牌，或者直到会话结束为止。即使用户/实体被阻止或从系统中移除，他们仍然可能持有一个有效的会话令牌。依赖方可能会继续接受这个令牌，直到 TTL 过期或者没有触发另一次令牌验证的操作。然而，大多数授权系统会在每次请求时检查授权。因此，遏制可能需要在身份提供者（IdP）和依赖方之间采取不同的措施，其中依赖方需要改变授权（例如，使用拒绝策略）或添加条件（例如，仅接受特定时间后颁发的令牌）。零信任架构建议持续检查授权（例如每 10 分钟一次）。

另一个复杂性出现在服务账户凭证被泄露和滥用时。没有与云或应用所有者进行协调，盲目遏制这些凭证可能会破坏应用功能。此时，响应者可能需要插入条件，例如源 IP 地址限制。此类基于属性的访问控制（ABAC）并非所有云提供商都支持，尤其是 SaaS 提供商。分析必须能够

识别滥用凭证的源，确保攻击者无法重新滥用访问权限并建立新的会话。IAM 的遏制还需要深入了解攻击者是否能够利用其访问权限进行提升或跳跃到不同的身份，这就像我们在网络中追踪攻击者的横向移动一样。如果分析员和响应者是不同的角色，这可能需要紧密协调。

管理平面遏制不仅仅包括 IAM 遏制，还应关注互联服务，识别受影响服务和资源的波及范围。虽然通过审查 IAM 权限通常能清晰显示这一点，但某些云平台中，服务之间可能有内部连接，这些连接只能通过直接查看服务和资源配置才能发现。在云网络中，网络遏制通常更为容易，因为它们依赖于软件定义网络（SDN）。通过 API 调用和 Web 控制台，可以快速且轻松地改变规则。然而，响应者必须了解平台的网络具体情况。例如，与 IAM 一样，某些云提供商中更改网络安全组规则可能不会中断当前的网络会话（因为规则是在连接时评估的，直到会话结束）。

自动扩展机制（如 FaaS、Serverless 等）可以增强遏制效果。响应者或应用所有者可以修改自动扩展组的启动要求，使用修补版本的工作负载，然后将已被妥协的资源隔离，进行进一步分析。遏制活动还应优先考虑任何已公开或与未知目的地共享的资源（例如，未知的云账户、订阅或相同提供商中的项目）。对于关键数据，可能需要冒着暂时破坏应用功能的风险，事件响应者应具备及时向有权作出决策的相关负责人报告和采取行动的通道。在某些情况下，受损的资源（如虚拟机、容器或无服务器代码）可能会让攻击者进入管理平面。分析应识别 IAM 的波及范围，并将其纳入遏制优先事项，特别要关注任何涉及的 CI/CD 流水线。限制攻击者对流水线的访问是首要任务，因为流水线通常拥有完全的管理权限，能够影响部署。

11.4.2 根除

根除通常由云和应用所有者以及他们的管理员和开发人员来执行。与分析和遏制一样，根除的主要重点应当是将攻击者从管理平面中彻底移除，这需要采取永久性措施。此过程可能包括凭证轮换、增加额外的策略条件、实施多因素认证（MFA）或数字证书等技术。只有在确定事件源后，才能锁定源 IAM/访问权限。在事件期间和之后，需要进行分析，以确定攻击者是否能够在管理平面或 IAM 系统内进行横向渗透。

在云环境中，通常替换资源比将攻击者赶出资源更为简便。如果资源是临时性的（如依赖自动扩展或 IaC），更换资源尤其简单。在云原生应用程序中，使用这种方式根除攻击更加容易，而在采用提升与迁移（Lift and Shift）方法部署的应用中则较为困难。根除通常还需要删除旧版

本的镜像、无服务器代码和 IaC。如果攻击者利用这些资源重新入侵部署，尤其是在员工无意中重新部署旧版本的情况下，根除显得尤为重要。根除过程可能还需要对 CI/CD 流水线以及版本控制和工件库中存储的材料进行彻底检查。

11.4.3 恢复

IaC、自动扩展和其他自动化技术在事件恢复中具有强大的功能。它们可以迅速部署硬化版本的应用和基础设施，甚至可以在全新的环境中部署干净的版本。在恢复过程中，所有镜像、资源和模板都应经过分析，以确保根本原因已被根除，且攻击者没有留下任何后门。例如，攻击者可能会通过IAM实体获得访问权限，这个实体看似与事件无关，且未在主要攻击中被使用。或者，攻击者可能会将后门密钥或代码嵌入应用程序或镜像中，以便将来再次访问。

11.5 事后分析

事件响应（IR）中最重要、却常被忽视的阶段之一，是确定从事件中学到的经验教训，并采取积极措施以减少未来类似事件的可能性或影响。这是在事件后分析阶段完成的。在这一阶段，响应者确定事件的根本原因，分析响应过程，并尝试识别改进的领域。这不仅仅是为了归责，而是为了发现任何可以改进的结构性问题，以防止或限制未来的事件。

事件后分析阶段的基本原则对于云环境而言并没有什么不同，但有一些最佳实践值得强调：

- 由于许多云事件涉及与管理云部署的团队合作，因此应将他们纳入任何事件后分析中。
- 响应者应被要求为他们遇到的任何新类型的事件创建新的运行手册/操作手册。
- 许多云安全事件都是由配置错误引起的。云安全联盟建议采用“公正文化”方法，专注于在归咎于个人之前识别任何系统性失败，同时仍然对个人的行为负责。例如，如果过度权限的 IAM 是漏洞的根源，组织可能考虑添加工具来识别潜在的 IAM 问题，安全团队可以提供常见的基准，并与团队合作审查权限，或者组织可以从静态凭证迁移到“即时授权”并结合强认证，但使用不拖慢开发人员工作的无摩擦工具。

11.6 韧性（恢复力）

在云计算领域，韧性指的是应用程序或系统在面对各种类型的中断时，能够继续无缝运行的能力，这些中断从轻微故障到重大停机不等。云韧性的概念是分层的，可以根据服务的关键性和预算约束进行扩展。

在基础层级，单区域韧性是大多数应用程序开始实现韧性的起点。在这种设置中，应用程序托管在单一云提供商的区域内，并采用自动扩展和负载均衡等策略来应对流量的突增，并能够容忍单个组件的故障。备份和恢复策略也已到位，以保护数据。这个基础级别也是最具成本效益的选择，因为它利用了云提供商现有的基础设施和服务，而不需要显著的资源重复。

图 66：全球云弹性战略

然而，单区域部署容易受到区域性故障的影响，尽管这种情况较为罕见，但也可能对应用程序的可用性产生重大影响。为减轻这一风险，组织可以提升到多区域韧性。这包括在同一云提供商的多个区域内运行应用程序的平行部署。虽然这显著提高了容错能力和地理多样性，但也带来了额外的成本。这些成本不仅来自于运行多个应用实例，还来自于跨区域同步数据的需求。此外，跨区域数据传输费用可能会迅速增加，使其成为比单区域部署更昂贵的选择。

最为复杂的云韧性是多个提供商（带来）的韧性。这个层级是通过将应用程序的部署分布在多个云提供商之间来实现的。其目的是保护应用程序免受某个云提供商完全宕机的影响。实现多提供商韧性是复杂的，因为不同云提供商之间存在技术差异。容器化技术通过将应用程序从底层基础设施中抽象出来，可以在一定程度上缓解一些复杂性，但仍然存在挑战。这些挑战包括管理

不同的网络、存储和安全模型，以及在根本不同的环境中协调部署和运维。成本可能会迅速上升，不仅在直接的运营费用方面，还包括设计、开发、测试和持续维护所需的额外开销。尽管成本和复杂性较高，但对于那些对可用性要求极高的关键应用——例如金融交易、医疗服务或全球贸易——多提供商韧性可能是必要的投资。

11.6.1 IaaS/PaaS 韧性工具

IaaS 和 PaaS 的核心依赖于抽象化（虚拟化）和编排。这些额外的层次在裸机硬件之上引入了更多的故障机会。为了应对这一点，CSP 提供了多种工具，帮助客户设计以应对单点故障的韧性。IaaS 和 PaaS 包括多个可以用来提高韧性的工具：

- **架构：**
  - **自动扩展：**利用自动扩展能力，系统可以动态调整资源并在故障时替换它们。
  - **无服务器计算：**无服务器计算具有很高的容错性，因为它本质上设计为根据需求扩展。
  - **平台即服务（PaaS）：**PaaS 提供的服务将操作系统和基础设施管理抽象出来，许多 PaaS 服务有很高的韧性服务级别协议（SLA）。
- **基础设施即代码（IaC）：**
  - **镜像定义：**使用 IaC 定义虚拟机和容器镜像，有助于生成替代品并快速适应。
  - **基础设施定义：**IaC 可以为整个应用堆栈提供可移植性。
- **自动化和备份：**
  - **CI/CD 流水线：**快速自动化修复或将新的堆栈部署到新环境中。
  - **备份：**许多提供商还支持自动备份，特别是他们的 PaaS 服务，如数据库。
- **混沌工程：**
  - **原理和工具：**用于在开发和生产应用程序中注入故障，以持续验证韧性。这指导团队在构建时假设基础设施和服务会发生故障，而不是假设几乎没有停机时间。

11.6.2 SaaS 韧性

当讨论软件即服务（SaaS）应用程序的韧性时，本质上是指服务在面对各种中断时仍能持续运行的能力。在这种背景下，韧性是关于确保业务连续性和灾难恢复（BCP/DR）计划，即使在 SaaS 提供商发生故障或其他问题时也能持续运作。与 IaaS 和 PaaS 不同，使用 SaaS 服务时，客户通常无法管理自己韧性的任何方面。

以下是 SaaS 面临的一些挑战：

● **极其有限的选择：**SaaS 应用程序通常在提供商的基础设施上运行，这意味着对应用程序的弹性和冗余的控制主要掌握在提供商手中，而不是最终用户手中。增强弹性的选项受到提供商提供的内容的限制。因此，对于企业来说，选择提供强大灾难恢复和高可用性功能的 SaaS 提供商非常重要。

● **数据提取/迁移支持：**虽然一些主流平台确实支持数据提取和迁移，但这些功能通常用于切换平台或进行备份，而不是用于实时灾难恢复。该过程不是连续的，并且数据导出之间可能会出现很大的延迟。如果发生中断，可能无法获得最新数据，这对于需要最新数据的操作来说可能会带来问题。

● **定期数据提取：**在许多情况下，企业可用的最佳选择是定期进行数据提取。这包括在可行的情况下进行本地数据同步。虽然这不能提供实时恢复，但它可以降低数据丢失的风险。这些提取的频率取决于业务性质和数据的关键性。对于某些企业来说，每晚备份可能就足够了，而另一些企业可能需要更频繁的备份间隔。

● **检查并了解您的 SaaS SLA：**SLA 是定义您期望从 SaaS 提供商获得的服务水平的重要文件，包括正常运行时间保证和服务中断时提供商的责任。彻底检查这些协议至关重要，以了解承诺的连续性和恢复选项、提供商如何处理数据备份以及如果服务未能达到约定的标准会提供什么补偿。

除了上述几点之外，企业还应考虑以下策略来确保 SaaS 应用程序的连续性：

● **多个提供商：**根据服务的重要性，使用多个 SaaS 提供商来实现冗余可能是值得的。对于对业务运营至关重要的服务尤其如此。

● **混合解决方案：**一些企业可能会选择混合解决方案，其中重要应用程序托管在本地或私有云上，而不太重要的应用程序则托管在 SaaS 提供商上。

● **定期更新的恢复计划：**公司应该有一个记录良好且定期测试的恢复计划。该计划应该根据 SaaS 应用程序及其支持的业务运营的变化进行更新。

● **保险：**一些公司可能还会考虑选择保险来弥补因 SaaS 停机造成的损失，尽管这是一种财务缓冲，而不是连续性解决方案。

● **培训和准备：**确保对员工进行培训，让他们了解如何在停电期间尽可能切换到备用系统或手动流程。

SaaS应用程序的韧性规划要求理解其局限性，并围绕这些局限性进行积极规划，以确保业务运营能够以最小的中断继续进行。

总结

组织应当深入了解云事件响应（CIR）流程及其事件响应（IR）能力，以为可能发生的任何事件做好准备。

本领域探讨了 CIR 框架以及为有效响应事件所需的准备工作。它为 CSP 和 CSC 提供了一种透明、共同的框架，帮助他们共享 CIR 实践，指导 CSC 如何准备并管理云事件，贯穿整个破坏性事件的生命周期。

建立坚实的基础：CIR 框架为组织提供了应对云安全事件的能力。第一阶段是准备阶段，重点是建立坚实的基础。这包括成立专门的云事件响应团队（CIRT）来管理事件。CIRT 随后会制定全面的策略、程序和沟通计划，以指导响应。此外，还需要进行技术准备，以应对云环境中的差异，特别是安全遥测和响应者访问。这包括实施安全工具来进行早期检测，并确保为深入调查提供取证和分析能力。

响应与学习：当发生安全事件时，云事件响应框架将转入检测和分析阶段。在这一阶段，重点是尽早识别事件并理解其根本原因。采用多种检测方法来实现这一目标，并且框架强调根据潜在的业务影响进行快速通知和解决。一旦威胁被遏制，控制、根除与恢复阶段开始发挥作用。这一阶段涉及选择正确的策略来停止攻击者并防止进一步的损害，同时进行调查和取证工作。

持续改进：云事件响应框架的最后阶段是事件后分析阶段。这一阶段对于从经验中汲取教训至关重要。CIRT 分析事件，以识别人员、流程或技术方面的弱点。这些经验教训被反馈到准备阶段，以持续改进组织的事件处理能力。这一循环方法确保了安全态势的不断演进，使组织能够有效应对云环境中不断变化的威胁格局。

协调和信息共享：由于云安全事件的共享特性，有效的沟通至关重要。这包括在CSP与用户之间建立清晰的沟通渠道，定期向受影响的用户提供更新，并促进各方利益相关者之间的信息共享。此外，提前规划与内部IR团队、执法机构和关键合作伙伴的沟通，可以增强整体CIR能力。

建议

事件响应计划

- 制定针对云环境的全面事件响应（IR）计划。
- 成立专门的云事件响应团队（CIRT），并定义各角色和责任。
- 确保响应者能够访问所需的环境和工具，包括事件分析服务、硬件和软件。
- 维护内部文档，如端口列表、资产列表和网络流量基准。

准备阶段

- 执行主动扫描、监控、漏洞和风险评估。
- 订阅第三方威胁情报服务。
- 评估云服务提供商支持 IR 的能力。
- 定期审核日志、快照、取证功能和电子发现功能。
- 定期进行备份恢复和灾难恢复测试。

检测与分析阶段

- 重点关注管理平面和 IAM 活动作为威胁检测的主要领域。
- 实施聚焦活动的威胁检测器，而非聚焦攻击者的检测器。
- 使用配置更改作为云检测的来源，并将其集成到 CSPM 工具中。
- 确保与云账户团队的清晰、直接沟通，以便快速验证事件。
- 使用诱饵和蜜罐令牌来检测被盗身份库，并触发即时调查。
- 利用自动化和机器学习管理云环境的动态性。
- 使用快照保存虚拟机的状态，进行取证分析。

遏制、根除与恢复阶段

- 优先控制 IAM 和管理平面。
- 隔离身份和工作负载，必要时将系统或服务下线。
- 使用自动扩展和基础设施即代码（IaC）替换被攻破的资源。
- 轮换凭证、添加策略条件，并实施多因素认证（MFA）以完成根除。
- 删除旧版本的镜像、无服务器代码和 IaC，防止重新被攻破。

事件后分析阶段

- 遵循“公正文化”方法，识别系统性失败，而不归咎于个人。

韧性规划

- 从单区域韧性开始，使用自动扩展、负载均衡和备份策略。
- 考虑多区域韧性，以提高容错能力和地理多样性。
- 对于需要最高可用性的关键应用，评估多提供商韧性。
- 利用 IaaS 和 PaaS 工具，如自动扩展、无服务器计算和基础设施即代码（IaC），以提高韧性。
- 使用 CI/CD 流水线自动化修复和新堆栈的部署。
- 实施混沌工程原理，通过故障注入验证韧性。

补充指南

- 云事件响应框架 | CSA
- 云事件响应框架 – 快速指南 | CSA
- CSA 医疗设备事故响应操作手册 | CSA
- 云渗透测试操作手册 | CSA
- 云渗透测试指南 | CSA

领域 12：相关技术与策略

在云安全领域，我们需要从多个维度进行深入分析，以便全面理解其所面临的挑战。所谓的“视角”，本质上是我们分析问题的不同立足点，它们可以帮助我们能够从多角度审视问题，从而在战略层面做出考量。“流程”则为我们提供了一套方法论和框架，帮助我们在决策过程中做出明智的选择，并以一种可复制的方式采取必要的措施。通过将“视角和“流程”这两者结合起来，我们就形成了一套全面的策略来确保云应用程序、系统和数据的安全性和合规性。

我们深入研究了涉及各种关键安全领域的一系列视角和流程，例如组织管理、身份和访问管理 (IAM)、安全监控、网络、工作负载、应用程序以及数据安全。这些视角和流程构成了多个安全领域中不可或缺的重要环节。

学习目标

本领域的学习目标旨在为读者提供如下内容知识：

- 探讨将人工智能整合到云安全威胁与漏洞管理中的优势。
- 阐述人工智能在云安全中的角色作用。
- 识别零信任网络安全策略的关键组成部分。

12.1 零信任

零信任 (ZT) 是一种网络安全方法，旨在保护超出传统网络边界之外的资源（用户、资产和数据）。零信任（ZT）超越了传统的受信任或不受信任用户和网络概念，而是依赖于持续多因素身份认证(CMFA)、微隔离、加密、终端安全、自动化和分析等手段。此外，零信任（ZT）还包括对数据、应用程序、资产和各项服务 (Data, Applications, Assets, and Services,DAAS) 的增强审计。零信任架构 (Zero Trust Architecture, ZTA) 的核心宗旨在于减少基于信任假设或访问控制不足所带

来的固有安全风险。为了缓解这些风险，常见的策略包括最小化（收敛）攻击面以及提高安全措施的有效性和细粒度。在云环境中，这些策略尤其关键，因为需要应对多租户、高度分布式的访问以及面向互联网的广泛攻击面。

零信任架构（ZTA）为组织提供了一种整体性的安全防护策略，以防御那些可能针对传统安全措施和多层防御体系中的漏洞进行利用的内外威胁及攻击。

零信任架构（ZTA）的显著特征是授予请求方对资源、数据和计算工作负载的访问权具有临时性。这种特性，辅以动态策略实施和决策的能力，强化了包含云和本地（混合云架构）基础设施的组织安全环境。这对于防范那些可能利用暴露访问机制的内外部威胁而言，同样有效。

零信任（ZT）策略在技术层面为资源保护提供了一套框架，不仅优化了用户的操作体验，收敛了潜在的攻击面和复杂性，强化了最小权限原则，还提升了控制力和系统的弹性能力，并缩小了安全事件的影响范围。从业务角度上来看，零信任有助于组织降低风险、增强合规性，并确保组织文化与领导层的风险承受能力和治理框架相契合。

12.1.1 零信任的技术目标

零信任（ZT）的技术目标均致力于提高云平台的安全性。如下是一些技术目标及其如何与零信任之间相结合的示例。

- **保护框架**

零信任（ZT）构建了一个防御性框架，并引入了一种创新的网络安全策略。其核心理念在于，组织不应自动信任其边界内外的任何实体。这一新的防护框架使得重点可以转移到更注重业务目标的方向，系统围绕数据的价值和特定的保护需求而设计。许多过去有效的安全流程和策略现在已不足以应对当前的安全挑战。因此，组织在传统网络安全技术和方法上的投资正在逐渐显示出效果有限和保护不足的问题。

传统的安全防护措施，依赖于物理对象或代码签名，目前已无法满足当前的安全需求。鉴于攻击事件的日益频繁和规模化，以及现代社会的高度互联特性，组织必须对网络安全配置、监测机制以及预防策略进行彻底的重新评估。

- **简化用户体验**

零信任架构（ZTA）通过在整个环境（包括网络及其他组成部分）中执行统一的访问模型来简化用户体验。每个访问请求（无论是显式的还是隐式的）均遵循统一的逻辑流程，并进行诸如如下问题的判断：你是谁？你需要访问哪些具体数据？你现在就需要这些访问权限吗？一旦审批通过，用户将被授予在指定时间段内访问特定资源的权限。

在零信任架构（ZTA）模式下，不存在以下情况：

- 错综复杂的嵌套组图表，可能内嵌有遗留的访问控制列表（ACL），这些列表规定了访问权限，既可授权也可拒绝，有时却可能引发非预期的后果。
- 错综复杂的组织架构，其中一些层级可能由已不再承担相关职责的决策者所管理。
- 由于所有者离职而导致的孤立组，或类似本地与全局授权等不可预测的机制。
- 在访问权限的配置、解除配置或撤销过程中的延迟。所有访问请求都由策略决策点（PDPs）以一致且及时的方式处理。

- **减少攻击面**

零信任架构（ZTA）在整个网络和基础设施中实施严格的访问控制、持续身份验证和最小特权原则。这意味着假设威胁可能已经存在于网络内部，并采用“永不信任，始终验证”的访问和权限方法。通过持续验证用户、设备和应用程序的身份和安全状况，零信任旨在防止攻击者的横向移动并限制安全漏洞的潜在影响。

- **降低复杂性**

正如本文档开头所述，组织在数字化领域的不断转型可能使其信息技术环境变得日益复杂。尤其是一些访问权限的决策可能是在实际需要之前的几个月甚至几年前就已做出。但随着时间的推移，这些决策者可能因职位变动或其他原因而离开，留下一些无人监管的资源，这些资源的访问权限变得难以管理。这种复杂性是组织面临的一个主要安全难题。它常常导致监控盲点、配置复杂化、安全弱点和漏洞的增加，为攻击者提供了可乘之机。零信任策略通过简化这些复杂性，帮助组织减轻这一难题。

组织在数字化转型过程中可能遇到的一些复杂性情形包括：

- 混合云：云服务与本地基础设施的融合部署
- 多云架构：采用多个云服务提供商构建的多云架构

- 边缘计算：在网络边缘执行数据处理和分析的边缘计算技术

从访问控制策略的角度来看，上面所述的每个情形都带来了极大的复杂性。在零信任（ ZT）环境中，在零信任（ZT）环境中，所有应用程序访问均被假定为可能具有恶意或不受欢迎的性质。因此，无需尝试监管组织网络中的所有边界和路径，而是应构建应用程序和数据孤岛。这些孤岛能够获得更为精准的保护。这是因为构建 ZT 策略所需的属性远超过传统安全机制。随着组织简化网络并整合数据中心以增强灵活性，ZT 提供了一种强化的安全机制，通过在应用程序和身份周围构建边界来降低任何安全架构的复杂性。这也意味着对每个用户身份可进行的活动实施更为严格的控制，以及对个人访问权限和特权的更严密的可见性，特别是针对第三方和供应商的访问权限和特权。

- **执行最小特权原则**

执行最小特权原则是用户和程序只应拥有完成任务所必需的权限。简而言之，用户只能在需要的时候获得完成其业务所需的确切访问权限。简化的访问授权流程极大地方便了安全运营和治理团队能够更轻松地管理应对持续变化的安全环境。它还通过在适当的时间提供适当的服务来提升最终用户地体验。

为了进一步提升安全防护能力，组织应需考虑采纳更多的防护措施，例如：用户和实体行为分析（UEBA）特权访问管理（PAM）以及身份访问治理等，这些防护措施有助于深入理解用户行为模式，严格控制特权访问权限，并确保对身份认证相关的访问控制实施有效管理，进而在零信任架构框架下巩固最小权限原则。

- **提高安全态势和恢复能力**

从组织外部的角度来看，零信任架构（ZTA）能够有效降低 IT 基础设施系统及个人资产对黑客的可见性，从而缩小潜在的攻击面。

从组织内部来看，零信任架构（ZTA）着重于：

- 最小化横向移动
- 限制跨网络与跨系统的攻击可能性
- 降低任何恶意行为者一旦渗透到任何区域所带来的风险。

外部用户被限定在网络的一个小范围内，以保整个 IT 基础设施的弹性。因此，一旦发生攻击，可以迅速在小范围内控制并处理，使系统能够快速恢复到先前的状态。缩小的攻击面意味着，除非用户在零信任架构中获得授权，否则他们发起的所有源代码扫描和映射尝试都将失败。采用控制平面和数据平面分离的双层架构，确保了只有经过正确身份验证和授权的用户及其设备才能进入组织的网络。

- **提升事件控制和管理效率**

提高组织事件管理过程的有效性和效率是零信任架构（ZTA）的核心目标。这一目标的实现依赖于 ZTA 的基本原则和设计理念。首先，我们假设所有实体在未经证实之前都是不可信的。其次，我们认为系统可能正遭受入侵，因此必须持续监控系统中每个实体的行为。

通过微分割和对网络访问权限的持续授权，可以缩小潜在安全漏洞的影响范围，因为这样可以更有效地控制攻击者的横向移动。一旦发生安全事件，组织能够通过更有效的控制措施限制事件的影响，并在事件影响有限的情况下，更容易地进行消除和修复。

此外，零信任架构（ZTA）所包含的持续监控功能可以更有效地识别异常和事件。事件相关数据还被用于更新策略决策点（PDP），这使得策略定义能够动态调整并得到执行。这些措施进一步防止了事件在组织网络中的扩散。

12.1.2 零信任业务目标

如同技术目标，零信任的业务目标同样能够提升组织的安全防护水平，确保敏感数据的安全，并体现零信任（ZT）的实际商业价值。以下是一些业务目标以及其与零信任关系的示例。

降低风险

- 零信任有助于降低组织面临的网络安全风险。组织通过采用这种方法，建立起一种主动防御的安全模型，该安全模型不再默认网络边界内的所有元素都是安全的，而是认为威胁可能来自网络的任何地方。

- 传统安全模型依赖于基于边界的防御，认为边界内的所有内容都是可信的。但随着网络攻击手段的不断进步，以及远程办公和云计算的普及，这种依赖边界的防御策略已经不能满足当前的安全需求。

● 零信任通过执行严格的访问权限控制、持续的身份验证和最小特权原则来降低风险。这意味着即使攻击者获取了网络访问权限，他们的行动范围和对敏感资源的访问也会受到限制，从而减少了安全事件可能带来的损害。

提高合规性

● 对于组织尤其是那些在金融、医疗和政府等高度规范的行业中运营的组织来说，遵循法规要求和行业标准是至关重要的。

● 零信任（ZT）通过提供对敏感数据和资源的精细控制，帮助组织提高合规性。组织通过实施零信任原则，能够向监管机构和审计人员证明他们已采取了积极的措施来保护其数据和系统。

● 诸如 GDPR 和 HIPAA 等法规要求组织执行强有力的访问控制和数据保护措施。零信任通过实施严格的身份认证、加密和访问策略来满足这些要求。

与组织文化及领导层的风险承受能力相契合

● 采用零信任需要组织各个层面（从一线员工到高层管理人员）的致持。它促进了一种安全意识、责任感和持续改进的文化氛围。

● ZT 提供主动且灵活的安全策略，优先考虑降低风险和提高恢复能力，与领导层的风险偏好保持一致。它强调持续评估和降低风险的重要性，而不是仅仅依赖被动的安全措施。

● 零信任架构与管理层的风险容忍度相匹配，通过实施积极且灵活的安全策略，优先考虑降低风险并提升系统弹性。该架构突出了持续评估与降低风险的必要性，而非仅仅依靠被动的安全防护措施。

● 组织通过采用零信任原则，展现了他们对网络安全和弹性的承诺，这可以增强客户、合作伙伴和利益相关者之间的信任和信心。

12.1.3 零信任支柱与成熟度评估模型

零信任的安全原则被归纳为几个核心支柱，这些支柱与我们在下图中展示的控制领域紧密对应。它们旨在协同工作，为关键资产和资源提供更强大的保护。这些支柱及其各自的能力和功能在美国网络安全和基础设施安全局 (CISA)的零信任成熟度模型（ZTMM）和国防部（DoD）的零

信任参考架构中有所描述。虽然这些文件对支柱的具体描述有所不同，但它们的模型在本质上是等效且一致的。

零信任安全策略和框架的能力可与云安全责任共担 (SSRM) 结合使用，确保云部署的安全，同时利用云服务提供商（CSP）所提供的基础设施安全和相关服务。来作为组织级的安全策略，同时零信任同样适用于保障多云和混合云环境的安全。

下图为“CISA 零信任成熟度模型（ZTMM）中的支柱和跨领域能力”

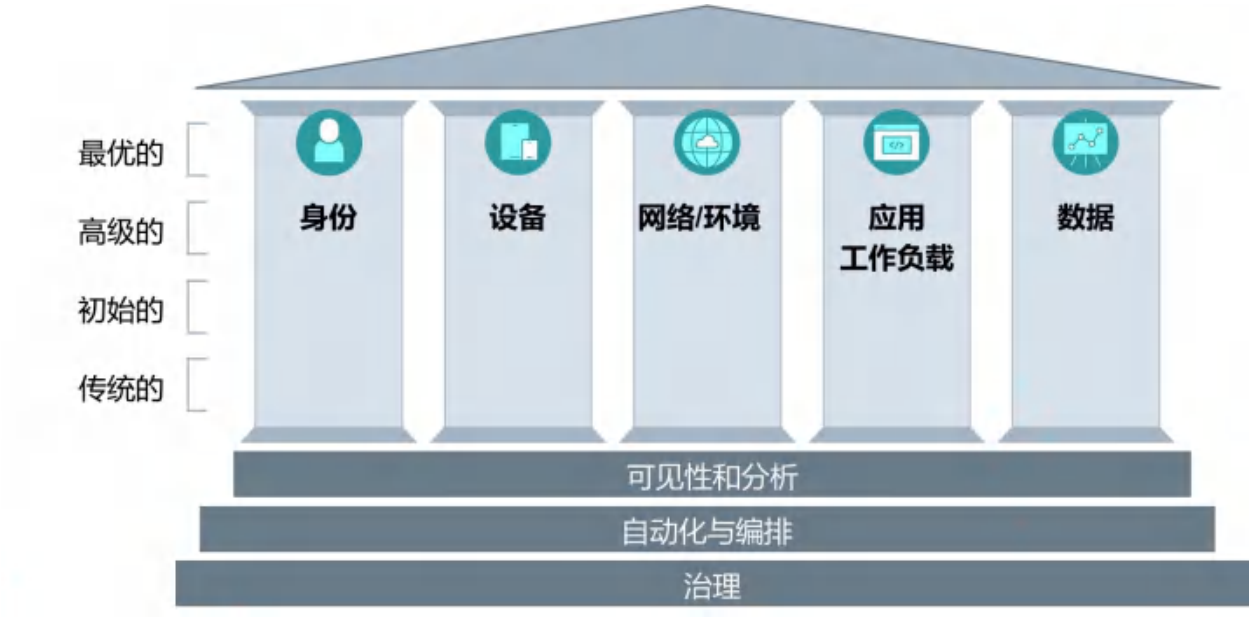


图 67: CISA 零信任成熟度模型图解

以下是 CISA ZTMM 中的支柱和跨领域能力

● **身份**（在某些模型中也被称为用户）：确保个人、非个人实体以及联合身份实体对数据、应用程序、资产和服务的访问安全、受限且受控，这涉及到身份验证、凭证和访问管理等能力，例如多因素认证（MFA）和基于上下文的多因素认证（CMFA）。组织必须能够持续进行身份验证、授权和监控活动模式，以管理用户的访问权限，同时保护所有交互的安全。在这个支柱中，基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）将应用于策略，以便根据动态的、基于上下文的访问策略来授权用户访问应用程序和数据。

● **设备:**在零信任（ZT）框架下，拥有识别、认证、授权、清点、隔离、保护、修复和控制所有设备的能力至关重要。对组织设备进行实时的安全验证和补丁更新是确保安全的关键环节。

诸如移动设备管理器或合规连接方案等工具，为评估设备的安全状况提供了重要数据。对于每一次访问请求，都应进行适当的验证，包括检查设备是否被侵入、异常行为检测、软件版本和补丁更新情况、保护状态、加密功能的启用等。。

● **网络：**在零信任架构下，组织需要在逻辑上（通过虚拟化手段）和物理上对网络环境（无论是本地还是云端/异地）进行分离、隔离和控制。这包括实施细致的访问控制和策略限制。随着通过宏观分离技术使网络边界变得更加精细，进一步启用微分割可以增强对数据、应用程序、资产和服务（DAAS）元素的保护和控制。重要的是：

● 限制和管理特权访问

● 监控并控制内外数据传输

● 防止攻击者在网络内的横向移动

● 应用程序和工作负载：无论是本地部署的系统或服务上的任务，还是在云环境中运行的应用程序或服务，都应纳入零信任的考量范围。零信任的工作负载应覆盖从应用层到虚拟机监视器的整个应用堆栈。确保应用层、计算容器和虚拟机的安全与适当管理是采纳零信任架构的关键。在整个软件开发生命周期中，实施严格的代码审查、漏洞扫描和安全测试流程对于降低风险和预防安全漏洞至关重要。内部源代码和常用库应通过 DevSecOps 的开发实践进行审查，以确保应用程序从设计之初就具备安全性。

● **数据：**零信任架构（ZTA）致力于保护组织的核心数据、应用程序、资产和服务（DAAS）。深入理解组织的 DAAS 对于有效实施零信任架构是至关重要的。组织应根据数据对业务的关键程度进行分类，构建数据架构以及对静态数据和传输中的数据实施加密来实现。像数据权限管理（DRM）、数据丢失预防（DLP）、软件定义网络（SDN）以及细粒度数据标记等技术解决方案，在确保关键数据安全方面发挥着关键作用。

● **可视性和分析**（CISA 模型中的跨领域能力）：必须包含关键的上下文信息，以便更全面地理解性能行为和各个零信任支柱的活动基准。这种可见性提升了异常检测的能力，并使得能够根据实时上下文动态调整安全策略和访问决策。此外，利用传感器数据和遥测等其他监控系统，有助于更全面地了解环境的当前状况。这将有助于触发警报并做出响应。在零信任组织中，将捕获并检查网络流量，不仅分析网络遥测数据，还要深入到数据包层面，以观察威胁并相应地调整防御措施。

● **自动化和编排**（CISA 模型中的跨领域能力）：将手动安全流程自动化，以便能够快速且大规模地在组织范围内执行基于策略的操作。通过安全编排、自动化和响应（SOAR）技术，可以提升安全性能并缩短响应时间。安全编排将安全信息和事件管理（SIEM）系统与其他自动化安全工具相结合，以协助管理不同的安全系统。为了实现主动的指挥和控制，自动化安全响应需要在所有零信任组织中定义清晰的流程，并持续执行一致的安全策略。

● **治理**（CISA 模型中的跨领域能力）：治理是一项重要功能，因为它确保了业务战略、风险管理和 IT 信息技术视角之间的一致性。 治理有助于明确定义零信任架构（ZTA）策略，例如访问控制和数据处理等方面。从非技术角度上来看，治理还应致力于管理和简化复杂性。为了成功减少复杂性，应重点关注受保护的范围，从技术角度来看，治理策略应通过策略执行点（PEP）来实施，确保策略得到有效执行。

CISA 零信任成熟度模型（ZTMM ）协助组织提升其零信任（ZT）策略，通过明确传统、初始、高级和最优等成熟阶段来覆盖增强零信任（ZT）的各个支柱和能力。这些阶段覆盖了零信任的各个支柱（身份、设备、网络、应用程序和工作负载以及数据）和能力（可见性、自动化、治理）。这些成熟度阶段指导组织如何评估现状、规划未来并采取必要措施，以向更安全的零信任架构迈进。如下图所示的 CISA 零信任成熟度模型发展阶段，其描绘了一条通往实现最优零信任成熟度的路径。这种直观的可视化展示说明了组织如何逐步通过零信任的不同成熟度层次，实现安全策略的持续提升。

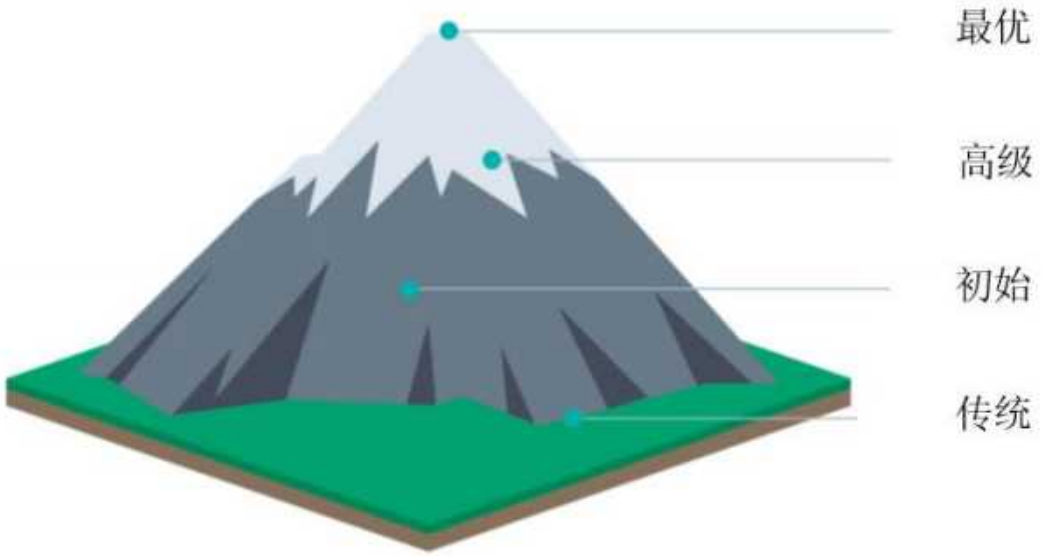


图 68: 零信任（ZT）安全模型成熟度发展阶段

要有效利用 CISA ZTMM，您需要掌握框架、完善职能并评估当前的 ZT 成熟度。最后，规划成熟度提升步骤， 并将它们与组织项目和优先事项保持一致，并使用优先级模型作为指导。

为了有效运用 CISA 零信任成熟度模型（ZTMM），您首先需要深入理解掌握这一成熟度框架，优化您的功能并评估当前的零信任成熟度水平。然后，制定提升成熟度的步骤计划，并将其与组织的项目和优先级相结合，同时运用一个优先级模型来引导您的步骤。

通过深入了解每个成熟度阶段的特点和目标，组织可以评估自身现状，找出需要改进的地方，并制定出一条通过零信任成熟度发展路径的路线图。下表展示了零信任成熟度模型中每个成熟度阶段的特点。

表 10：零信任成熟度阶段

成熟度阶段	描述	特征
传统阶段	传统成熟阶段标志着组织开始其零信任旅程的起点。在这一阶段，安全措施主要侧重于网络边界，并默认信任内部网络流量。	• 安全控制措施主要依赖于边界防护，例如防火墙和入侵检测系统（IDS）。 • 通常根据网络位置而非用户身份或设备状态授予对资源的访问权限。 • 安全策略往往是静态和被动的，对用户活动和网络流量的可见性有限。
初始阶段	在初始成熟度阶段，组织开始采用零信任的基本原则和技术，以提升其安全防护水平。	• 组织开始集中身份管理流程并实施基础的身份验证控制，例如对关键系统设置密码策略和多因素认证（MFA）。 • 引入设备安全措施，如终端保护软件和设备加密，以提升终端的安全性。 • 开始进行网络分段工作，以缩小攻击面并限制网络环境中的横向移动。
高级阶段	在高级成熟度阶段，组织在多个关键领域内实施零信任的实	• 在高级成熟度阶段，身份访问管理变得更加集中化和自动化，引入了自适应

	践和技术方面取得了显著进展。	和持续认证等先进的认证机制。 • 设备安全措施得到加强，包括对设备健康状况和合规性的持续监控，以及对安全漏洞的自动修复。 • 网络分段工作进一步扩展，实施了基于用户上下文环境和应用程序敏感度的动态访问控制，并广泛采用了加密通信渠道。
最优阶段	最优成熟阶段标志着零信任成熟度的最高水平，在此阶段，组织已将其安全策略和运营完全整合进零信任原则中。	• 身份治理流程实现了全面自动化，并具备用户入职、离职、访问请求的自助服务功能，以及用于检测和减轻身份相关威胁的高级分析能力。 • 设备安全措施与零信任架构紧密结合，包括端到端的检测和响应（EDR）功能，以及用于主动搜寻威胁的高级威胁情报。 • 网络分段做到了细致且具有自适应性，网络中集成了自动化的威胁检测与响应机制，并在应用层实施了零信任访问控制。

12.1.4 零信任设计和实施步骤

当我们考虑如何策略性地采用零信任（ZT）时，我们需要遵循四个核心设计原则来构建一个具有弹性的架构，并且有一个可重复的五步实施步骤过程，这个过程支持交互式和逐步执行，确保能够基于风险优先级来保护组织的资产。

除此之外，CISA 的零信任成熟度模型（ZTMM）也是一个重要的参考，虽然它不属于五个步骤之一，但它对于理解组织在零信任实施过程中的逐步发展至关重要。

零信任的设计原则包括：

- 关注业务成果：明确零信任如何与组织的首要业务目标保持一致并为其提供支持。
- 由内而外构建设计：在将安全策略扩展到组织外部之前，首先从内部着手进行构建。
- 明确访问需求：确定哪些用户和设备需要访问特定的资源。
- 检查并记录关键流量：致力于监控并记录关键活动，以便更有针对性地发现潜在的安全威胁。

一个可重复的零信任实施过程包括五个步骤：

- 第一步：定义保护范围：识别并评估关键的业务信息系统，包括其组成的数据和资源（DAAS 元素），确定这些系统的业务风险等级，并评估其当前的安全成熟度，以此来帮助确定实施的优先顺序。
- 第二步：梳理信息流动（绘制信息流图）：深入理解信息在系统和组织内部以及与外部的流动路径，以及每个流动路径上信息的潜在分类。这一步骤的目的是识别出最敏感的信息和资产的所在，并确定在控制访问权限方面能够发挥最大效用的关键点，这些信息将作为零信任架构设计和开发的重要参考。
- 第三步：构建零信任架构（ZTA）：设计并开发所需的基础设施、功能和控制措施，确保能够为关键业务系统和资产提供零信任的安全防护。
- 第四步：制定零信任策略：确立并执行策略控制，为关键业务系统和资产的网络访问、系统操作和数据管理制定相应的指导方针与规则，确保安全性得到保障。
- 第五步：监控和维护网络（环境）：对零信任环境进行不间断的监控，确保安全措施的持续性，并针对新出现的威胁进行适应性调整。

12.1.5 零信任与云安全

下述的表格归纳了零信任（ZT）的核心原则，并将其与安全领域相对应，详细阐述了这些原则如何被应用来降低风险，并提升组织整体的网络安全防护能力。

表 11:云安全知识认证（CCSK）安全领域与对应的零信任原则

安全域	零信任原则
组织管理	零信任（ZT）作为一种组织级的安全与连接策略，最好是在具备零信任（ZT）文化的背景下实施。
身份与访问管理	采用持续且抗网络钓鱼能力的多因素认证（MFA），并根据用户、设备和访问请求的具体情况进行授权，以实现更精细的安全管理。
安全监控	全面监控所有活动，基于假设违规行为的前提，及时捕捉可疑行为，并根据情况的变化灵活调整访问控制。
网络	采用微隔离技术，构建零信任网络架构，并实施软件定义边界策略，以增强网络安全性。
工作负载	实施零信任原则对设备和工作负载进行安全和完整性的检查，监控恶意软件活动和数据泄漏情况，并应用零信任模型对工作负载的访问进行严格控制。
应用程序	实施细粒度控制，确保访问授权遵循最小权限访问原则并与职责分离相结合；将用户的权限严格限制到完成任务所需的最低限度的数据和功能上。
数据	对静态数据、传输中数据和使用中的数据进行分级分类，保护和持续监控，并实施严格的零信任数据访问控制。

如下是零信任安全的核心理念对主要云安全领域的具体影响：

● 身份和访问管理（IAM）：是零信任实施的核心，其重点在于强化持续的身份认证和精细的授权管理，确保资源的访问既安全又具有上下文感知能力。

● 安全监控：通过融入零信任原则，预设可能存在的安全漏洞，并通过策略性网络访问控制和严格的事件响应流程来降低潜在影响，以此提升操作安全监控和警报的有效性。

● 网络：强制实施零信任访问控制，利用微隔离技术降低潜在的攻击面，采用虚拟防火墙和加密措施来保障安全，并遵循如最小权限和持续认证等零信任原则，以有效控制网络访问。

● 终端安全：强制实施零信任原则，防范诸如恶意软件和勒索软件等威胁，并确保对访问云资源的设备实行严格的认证、授权和访问控制。

若要深入研究这些内容，我们建议参考由经验丰富的网络安全专家提供的零信任用例。您可以考虑学习云安全联盟（CSA）在零信任能力认证培训中的用例集合。

12.2 人工智能

人工智能 (AI) 既可用作云托管服务，也是一类增强云安全性的新兴工具。虽然 AI 服务通常部署在云端，但对于某些特定的应用场景，也可以选择使用本地托管解决方案。此外，AI 在云安全中扮演着双重角色：一方面，它可以用来增强云安全措施，但另一方面，它又作为一种新的攻击工具带来了风险。由 AI 驱动的算法能够发现漏洞、设计并执行复杂的攻击行动，这凸显了保护 AI 服务以及采取强大安全措施以抵御 AI 驱动威胁的重要性。

12.2.1 AI 与云安全

与本章 12.1 节所讨论的零信任一样，AI 与多个关键云安全领域紧密相关。此外，当今的零信任架构通常依赖 AI 技术来执行多种任务，例如：执行严格的访问控制策略，做出情境感知访问决策等。这种领域的交叉融合凸显了 AI 在整个云环境的安全实践不断演变增强中所起到的关键作用。

表 12：安全领域与人工智能的交集

安全域	人工智能方面
组织管理	AI 的部署位置及方式

身份与访问管理 (IAM)	“AuthN/Z”
安全监控	人工智能监控及记录；人工智能用于检测和分析
网络	自行或云托管 AI 时的网络安全
工作负载	安全 AI 工作负载托管
应用	AI 集成、API 安全
数据	训练数据、数据存储、数据泄露

- 对于组织管理而言，组织必须确定 AI 策略、提供商及其期望。根据服务的具体情况，设立相应的账户和服务，并启用必要的安全控制。
- 与任何云服务一样，IAM 是最重要的安全控制手段。对于 AI 它将影响用户、管理员、AI 模型/工作负载本身以及所有对底层训练或分析数据的访问。
- 安全监控应包括提示、输出和数据访问。
- 托管 AI 服务时必须确保底层网络的安全。为了限制对 AI 即服务（AIaaS）平台的访问，还需要采取额外的网络安全性措施。
- 任何运行 AI 或访问 AI 的工作负载都需要遵循基本的安全实践。
- 大部分的 AI 安全是在应用层实现的，包括应用逻辑和 API 安全。
- 所有训练、分析及其他数据存储库都必须得到保护。这些存储库通常都会包含大量数据。

12.2.1.1 AI 与云安全的结合

人工智能正在重塑组织在数字环境中处理安全的方式，AI 与云安全的交汇代表了一种范式的转变，旨在应对不断发展的网络安全挑战。

随着组织越来越依赖云服务来托管关键工作负载和敏感数据，集成 AI 技术为增强安全措施和降低风险带来了新的机会。从 AIaaS 产品到利用云基础设施部署 AI 模型，有多种选择可以利用 AI 的强大功能来保护云环境。

AI 增强型安全工具在威胁检测、访问控制和策略实施等方面发挥了重要作用。对于寻求加强自身防御并应对现代网络安全环境复杂挑战的组织来说，了解不同 AI 模型的消费模式及其与云安全工具的集成方式至关重要。AI 与云安全的交叉应用模式多种多样，主要分为四类：

1.人工智能即服务（SaaS 模式）：在此模型中，云提供商将 AI 作为一项完整的、随时可用的服务提供。例如 Claude 这样的产品可以直接利用 AI 功能，而无需构建或训练组织自己的模型。完整的软件即服务 (SaaS)非常适合那些希望快速采用 AI 但不具备深厚技术专业知识的组织，因为您可以轻松地仅选择已获得组织批准的服务。此类产品大多数都包括数据隐私升级、仅允许使用批准数据以及轻松跟踪提示和结果的功能。

2.人工智能服务（PaaS 或基础模型托管）：云提供商提供底层基础设施和工具来托管和运行 AI 模型，但将模型开发和应用构建留给客户。AWS Bedrock 就是一个例子：它提供了基础模型和托管环境，但客户需要在此基础上创建自己的解决方案。这种模式赋予了组织更多的控制权和定制空间，并能有效防御对抗性攻击如注入攻击或越狱攻击。此类产品的其他特性还包括安全的训练数据、安全的应用集成和部署环境以及安全的用户和访问管理。

3.云作为 AI 工作负载的托管平台（自带模型）：在这种情况下，组织组织从头开始开发 AI 模型或部署现成的模型（代码），而仅使用云作为托管环境。组织需负责整个 AI 生命周期，即从数据准备到模型训练再到部署。云只提供基础计算资源。这种方式提供了最大的灵活性，但也要求组织具有较强的内部 AI 技能，并承担起构建内部应用程序的责任。

4.AI 增强的安全工具：除了提供上述的托管服务之外，AI 还被嵌入到各种云安全产品中，使其更加智能和高效。比如人工智能驱动的威胁检测、智能访问控制、自动策略执行等。随着 AI 技术的日益成熟，我们预计将看到更多的 AI 增强的传统安全解决方案。

12.2.2 AI 赋能安全

人工智能和机器学习 (ML) 已广泛应用于安全领域，例如恶意软件检测和用户行为分析。随着大语言模型(LLMs)的出现，新的 AI 增强型安全工具正在迅速涌现，尤其是在数据分析和数据集优先级排序方面。

图 69：人工智能提升安全工具与流程的应用实例

人工智能和大语言模型在安全领域的重要应用领域包括：

● **威胁检测：**利用 AI 和 ML 模型来分析网络流量和系统行为，增强对新兴威胁的识别能力，同时利用 LLMs 模型生成富有洞察力的威胁情报报告。与传统基于规则的系统相比，AI 算法能够快速准确地从海量数据中识别出可疑模式和潜在威胁。这有助于安全团队在不断变化的威胁形势中保持领先地位。

● **日志分析：**用 AI 和 ML（包括自然语言处理）模型来分析非结构化日志数据、检测安全模式和异常，并提供实际可操作的分析。现代云环境会生成海量日志数据，以至于无法人工审查。AI 可以自动解析这些日志数据、关联不同系统中的事件，并标记可能预示安全事件的异常。

● **事件响应：**AI 通过使用自动化工作流程、使用 ML 模型按风险对警报进行优先级排序以及使用 LLMs 模型生成详细的事件报告并提出操作建议，来增强事件响应能力。当检测到威胁时，AI 可以协助调查损害范围、确定根本原因，甚至可以隔离受影响的系统或撤销被盗用的凭证，以此来自动控制损害。这大大加快了事件响应时间。

● **态势评估：**利用 AI 持续监控并评估组织在所有领域的安全状况，运用 ML 模型来查明错误配置和安全漏洞，而 LLMs 模型则提供详细的摘要和可行的建议，以增强安全措施。

● **安全代码分析：**利用 AI 来仔细检查源代码中的漏洞，通过 ML 模型完善建议，并利用 LLMs 模型解释安全编码实践并提出建议。这种“左移”方法包括架构风险分析、动态分析和其他主动技术，可以在问题进入生产环境之前发现它们，从而降低风险。

● **恶意软件分析：**AI 通过自动执行代码反混淆和行为分析等任务来增强恶意软件逆向工程的能力，ML 模型用于对恶意软件族进行分类并识别其模式，LLMs 模型生成详细的分析报告以促进研究人员间的协作。

● **风险优先级：**利用 AI 和 ML 模型分析来自安全工具和外部来源的数据，根据多种因素量化风险，并清晰地向利益相关者传达风险评估结果。通过量化风险，组织可以做出数据驱动的决策，合理分配有限的安全资源以获得最大效果。

● **权限管理：**通过运用 AI 和 ML 技术来分析角色和活动模式，从而增强访问控制，简化权限，并根据最小权限原则优化策略和自动生成访问审查报告。

随着人工智能和大语言模型的不断发展，我们期望在网络安全领域看到更多创新应用。然而，组织还必须注意人工智能的潜在风险和局限性，例如生成结果的偏差、模型可解释性和对抗性攻击。通过将人工智能的力量与人类的专业知识相结合和监督，安全团队可以增强其能力，并在日益复杂的数字环境中领先于不断演变的威胁。

12.3 威胁与漏洞管理

威胁和漏洞管理(TVM)使组织能够更好地预测、检测和应对动态云环境中的威胁，从而降低其遭受网络攻击时的脆弱性并确保持续的安全合规性。此外，将 AI 集成到 TVM 中有望成为保护云环境的标准做法。本节为讨论云服务威胁管理的进一步创新和挑战奠定了基础。

下表列出了与安全域相交叉的 TVM 方向。

表 13：TVM 中的安全领域

安全域	人工智能方面
组织管理	组织策略、影响范围控制、CSPM/CNAPP
IAM	凭证保护、PIM/PAM

安全监控	检测与分析
网络	影响范围控制、流量、DNS 监控
工作负载	端点保护、检测、响应
应用	应用程序和 API 安全
数据	资源策略、数据日志

以下是对应于 TVM 中的每个安全领域的简要分析：

● 组织管理：建立组织范围的安全策略，例如在云环境中配置 blast radius 控制和安全态势管理 (CSPM/ CNAPP) 活动。

● IAM：处理凭证保护并实施特权身份管理(PIM)和特权访问管理(PAM)。

● 安全监控：作为主动威胁监测的核心领域，负责分析安全事件和发出警报。

● 网络：通过网络分段和网络流量监控（例如流日志、DNS 查询）提供 blast radius 控制，控制网络访问和流量流向。

● 工作负载：专注于保护端点、检测威胁和协调事件响应行动，以确保运行应用程序的计算实例、容器和无服务器函数的安全。

● 应用：通过安全设计、严格的访问控制和主动保护来确保应用层安全，并利用工具来防范应用程序和 API 的特定漏洞。

● 数据：定义数据处理策略，记录数据事件，扫描异常访问模式，并调查数据泄露事件。

12.3.1 云威胁管理更新

在维护和更新云服务的威胁管理策略时，保护这些云服务的责任会根据不同情况和涉及的组织而有所不同。例如，CSP 负责确保其服务的安全，而组织组织或消费者负责配置和使用这些服务。

在云环境中，管理平面（例如 CSP 控制台、APIs）成为攻击者的主要目标。因此，除了轮换访问密钥和凭据以及监控异常行为或可疑操作外，还必须重点关注对云管理平台的访问和活动的保护。

当将管理平面视为新的攻击面时，请考虑以下几点。

● 管理平面成为新的攻击面：重点在于防御、监控云管理平面的访问和活动，因为管理平面成为了攻击者的主要目标。

● 漏洞扫描：漏洞扫描使用 CSPM、SSPM 和 CASB 等工具来识别和修复 IaaS 和 SaaS 设置中的安全问题，并使用基础设施即代码 (IaC) 扫描程序在开发早期纠正错误配置。

● 保护容器和虚拟机：利用适用于动态云环境的 CWPP/CNAPP 等现代漏洞管理工具，并将扫描集成到持续集成/持续交付 (CI/CD) 流水线中以主动检测问题，因为传统方法在处理容器等短暂资产时容易失效。

● 凭证盗窃和权限提升：为了降低凭证盗窃和权限提升的风险，实施强大的 IAM 控制、执行最小权限访问策略、定期调整和审查权限以及监控任何可疑凭证使用情况至关重要。

● 云原生威胁检测：利用云平台功能（例如 VPC 流日志、DNS 日志以及基于代理和无代理的解决方案） 来监控和识别跨网络和云工作负载（CWPP/CNAPP）中的威胁。

● 软件供应链安全：实施代码或图像签名、自动漏洞扫描和安全工件管理等措施，以保护软件依赖关系并增强对代码漏洞的响应。

● 威胁情报：使用来自 CSP 和第三方源的威胁情报来随时了解情况，并利用威胁情报主动寻找失陷指标。

组织内的团队可以参考下表中的建议和策略，共同识别、减轻并应对云环境

表 14：云安全实践和实施建议

安全实践或策略	实施建议
管理平面成为新的攻击面	在云中，管理平面（例如，CSP 控制台、APIs）成为攻击者的主要目标 ● 重点防御和监控云管理平面的访问和活动。 ● 保护并轮换访问密钥和凭证

	● 在管理平面日志中查找异常行为或可疑动作
漏洞扫描	● 云安全态势管理 (CSPM) 工具可扫描组织的 IaaS 环境，以识别错误配置和安全漏洞 ● SaaS 安全态势管理 (SSPM) 和云访问安全代理(CASB) 对组织的 SaaS 安全设置和使用情况进行评估 ● 定期使用这些工具来查找并修复漏洞和错误配置，以免被攻击者利用。这些错误配置通常可以在互联网上直接访问，因为组织没有网络边界来控制它们 ● 基础设施即代码（IaaC）扫描器可在将变更部署到生产环境之前检测安全配置错误。换句话说，采用左移策略以尽可能早地在软件开发生命周期中减少漏洞
保护容器和虚拟机	● 使用专为动态云环境设计的现代漏洞管理工具和流程（例如 CWPP/CNAPP） ● 传统的扫描方法不适用于容器等短期资产 ● 将漏洞扫描集成到 CI/CD 流水线中，以尽早发现问题
凭证盗窃和权限提升	● 攻击者越来越多地瞄准云凭证和权限，以获取未经授权的访问和枢轴攻击 实施强大的 IAM 控制: ● 使用最低权限访问策略 ● 定期审查并适当调整权限 ● 监控可疑凭证的使用情况
云原生威胁检测	● 云平台提供基于网络和主机的威胁检测的原生功能

	● 利用 VPC 流日志和 DNS 日志等功能进行网络安全监控 ● 使用基于代理或无代理的解决方案对云作负载进行威胁检测（CWPP/CNAPP）
软件供应链安全	● 保护组织的软件依赖项并了解其软件物料清单将有助于更有效地应对其代码和图像库中的漏洞。 实施如下控制措施： ● 代码或图像签名和完整性验证 ● 自动化漏洞扫描和修补 ● 安全工件存储库和发布管理流程
威胁情报	● 利用组织的云服务提供商（CSP）的威胁情报源来随时了解特定于云的威胁和趋势 ● 补充第三方威胁情报以获得更全面的视角 ● 使用威胁情报主动寻找危害指标并改进检测

12.3.2 云威胁情报来源

许多威胁情报源侧重于与云无关或非特指云的威胁行为者和指标。以下来源可以增强组织对云的威胁情报。

● 云安全联盟（CSA）的顶级威胁报告包含了针对公共事件中最常见的主动违规行为的威胁建模。该项目还包括对重大事件的深入研究。这对于了解实际违规行为的发生方式非常有用。

● MITRE ATT&CK 包含一个云矩阵，描述了攻击者用来攻击组织云部署的策略和技术（以及子技术）。

● 许多供应商都会发布威胁研究和报告。这些报告越来越多地包含了他们的研究和响应团队发现的云攻击信息。然而，有必要仔细评估这些报告，因为供应商可能会因其业务、产品和以往经验产生选择偏差。

● 开源项目独立运行并且收集和共享公开的威胁数据。Breaches.cloud 就是一个例子，它追踪已知的公共违规行为并正在积极维护。

总结

我们已经开始通过相关技术和策略的角度来分析云安全挑战。借助零信任（ZT）策略，您可以持续验证所有用户和设备，最小化信任，并应用最小特权原则，使用多因素身份验证、微隔离和加密等技术来保护资源，缩小攻击面并增强安全弹性。借助 AI，您可以通过威胁检测、访问控制和策略实施来增强云安全性。AI 还可以利用机器学习来改进异常检测和风险管理。借助 TVM，您可以使用 CSPM 和持续监控等工具来识别、评估和缓解安全威胁。TVM 还可以帮助您保护云环境并确保合规。将 AI 集成到您的 TVM 中可以增强威胁检测和响应策略，帮助维持稳健的安全态势。

建议

有效的云安全总是始于建立一个完善的治理模型，该模型为组织职责、识别风险和管理策略控制提供了框架。

治理与框架：这涉及到明确界定整个组织的角色和职责，识别与云使用相关的主要风险，并实施一个框架来一致地管理安全控制。治理结构应与总体业务目标保持一致，同时提供充分的监督和问责。

IANS云安全成熟度模型可以指导和支持安全计划。

从IaaS到SaaS，IAM都是安全管控的首要发力点。

● 使用组织管理来控制组织的影响半径和云安全态势。

● 建立一致的安全遥测收集，以实现有效监控。

● 网络、工作负载、应用程序和数据安全通常会有一组共享服务，但安全性需要根据不同部署的需求进行定制。

● 组织的云安全控制规范将定义基本要求，但需要在安全设计和架构上与 DevOps和云团队进行合作。

● 使用持续评估来识别导致公共暴露或创建 IAM 漏洞的错误配置，并使用事件响应（包括威

胁检测）来快速识别和补救攻击和暴露。

云安全成熟度模型还有助于构建和指导云安全程序开发。以下列出了一些具体的建议。

IAM 是优先事项

无论服务模式如何（IaaS、PaaS 或 SaaS），IAM 都应该是任何云安全计划的首要优先事项。IAM 控制着谁可以访问哪些资源以及他们可以执行哪些操作。配置错误或管理不善的IAM可能导致未经授权的访问、数据泄露和其他安全事件。重点是实施强大的身份验证机制、应用最小特权原则、定期审查、定期轮换访问密钥以及监控异常活动。

影响范围控制与监测的组织管理

使用云平台提供的组织管理功能来控制影响半径（安全事件的潜在影响）。这可以通过适当的账户结构、为不同环境（例如生产、准备、开发）使用单独的账户以及实施网络分段来实现。建立一致的安全遥测收集流程，以集中来自各种来源的日志和事件，从而实现有效的监控和事件响应。

为不同的部署定制安全措施

虽然整个组织可能存在一组共享的安全服务，但根据不同部署的具体需求定制安全控制非常重要。面向公众的Web应用程序的网络安全要求与内部数据库的网络安全要求不同。同样，容器工作负载安全措施也与无服务器函数的安全措施不同。与应用程序团队密切合作以了解他们独特的安全要求，并实施适当的控制措施。

与 DevOps 和云团队的合作

云安全不应孤立运作。与DevOps和云团队合作，将安全措施纳入项目的设计和架构阶段。定义团队可以参考的基线安全控制规范，但也要根据具体用例进行调整。培养一种共享责任的文化，让每个人都在维护安全态势中发挥作用。

持续评估和事件响应

实施持续评估流程以主动识别可能导致安全风险的错误配置，例如资源的公开暴露或 IAM 漏洞。定期扫描并修复这些问题。制定强大的事件响应计划，以快速检测、调查和缓解安全事件。利用威胁检测工具并自动化响应工作流程，以最大限度地减少潜在违规行为的影响。

重要的是要记住，云安全是一个持续的过程，需要持续监控、评估和改进。建议定期审查和更新组织的安全策略、程序和控制措施，以跟上不断变化的威胁形势和云环境。

补充指南

- 生成式人工智能与快速工程简介 | CSA
- 实践原则：动态监管环境中负责任的人工智能 | CSA
- 人工智能韧性：人工智能安全的革命性基准测试模型 | CSA
- AI 组织责任 - 核心安全责任 | CSA
- 零信任能力证书 (CCZT) | CSA
- DoD 零信任参考架构 | DoD
- 零信任成熟度模型 | CISA
- 网络安全框架 | NIST
- SP 800-207A，零信任架构模型 | NIST
- CIS 关键安全控制

CSA GCR cloud security alliance
GREATER CHINA REGION

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905