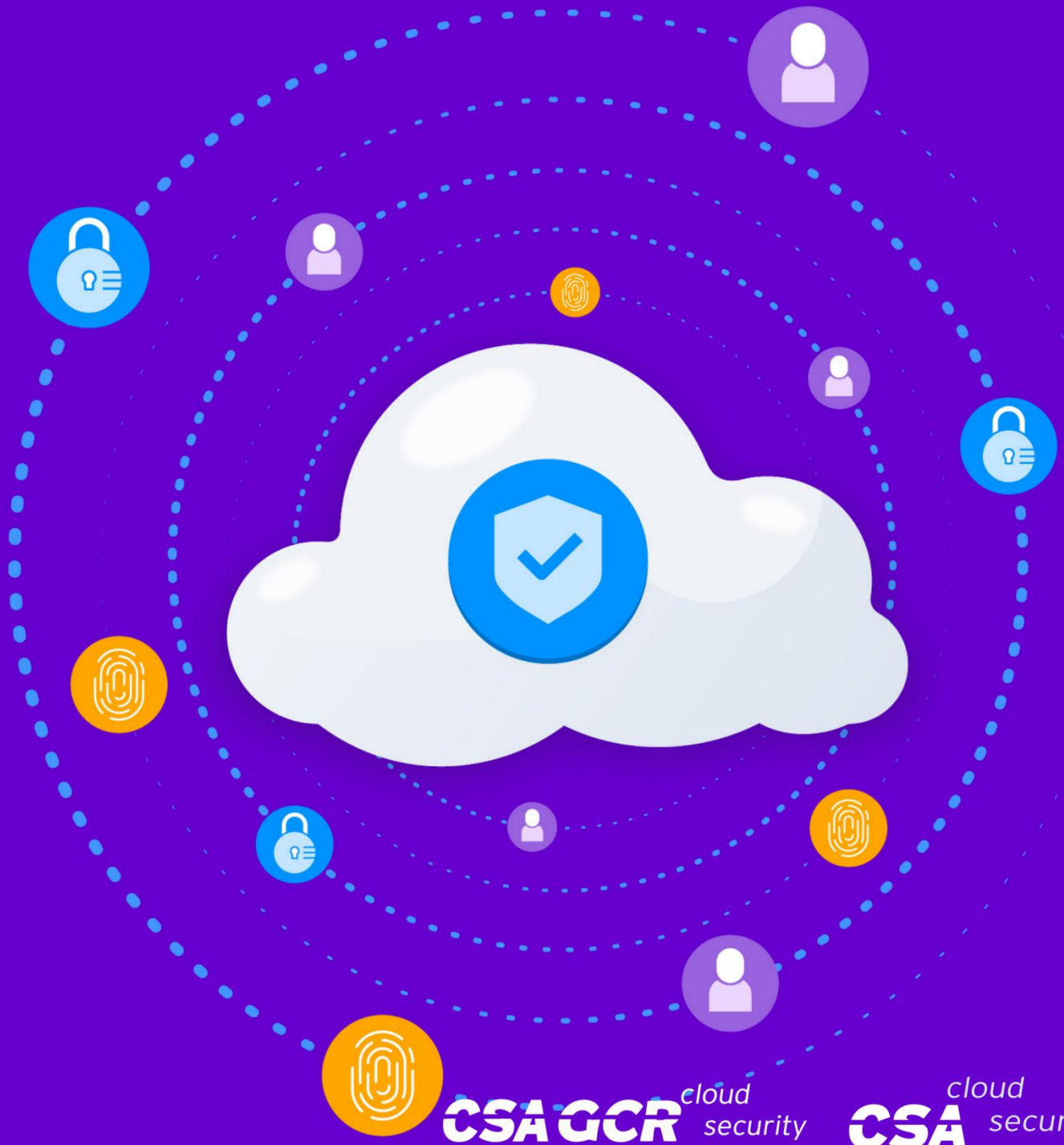
IAM在云环境下新的挑战



CSA GCR cloud security alliance GREATER CHINA REGION ®

CSA cloud security alliance ®

身份与访问管理工作组网址是：https://cloudsecurityalliance.org/research/working-groups/identity-and-access-management

@2023 云安全联盟大中华区-保留所有权利。你可以在你的电脑上下载、储存、展示、查看及打印，或者访问云安全联盟大中华区官网（https://www.c-csa.cn）。须遵守以下：(a)本文只可作个人、信息获取、非商业用途；(b) 本文内容不得篡改；(c)本文不得转发；(d)本文商标、版权或其他声明不得删除。请在遵循中华人民共和国著作权法相关条款情况下合理使用本文内容，使用时请注明引用于云安全联盟大中华区。

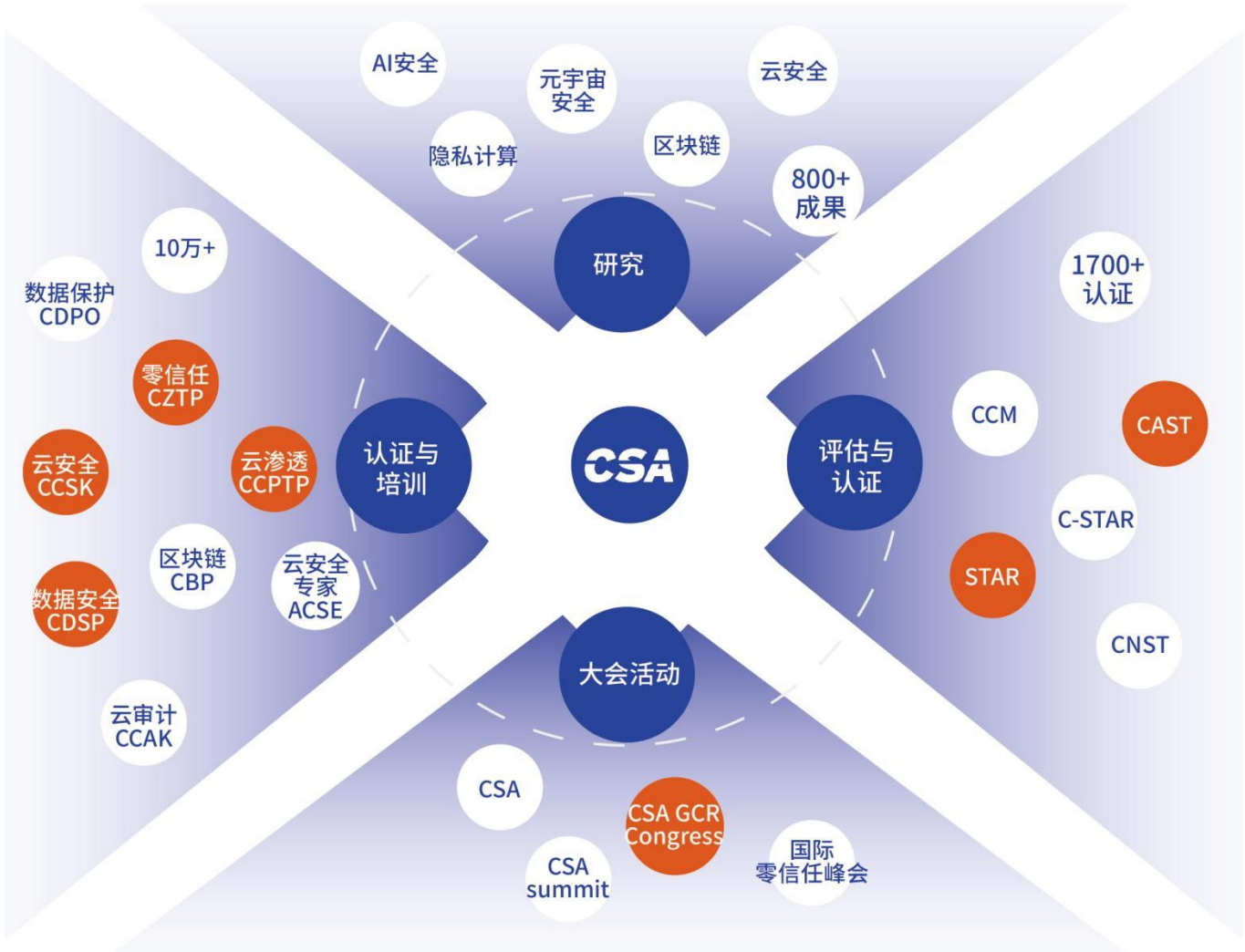
联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息



加入我们

CSA大中华区官网
（https://c-csa.cn）

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《IAM在云环境下新的挑战（What Is Identity & Access Management (IAM) For The Cloud? ）》由CSA工作组专家编写，CSA大中华区IAM工作组组织翻译并审校。

中文版翻译专家组（排名不分先后）：

组 长：

于继万

翻译组：

崔鉴　　王亮　　张彬　　鹿淑煜　　吕波

审校组：

戴立伟　　谢琴

研究协调员：

蒋好希

感谢以下单位的支持与贡献：

北京启明星辰信息安全技术有限公司　　奇安信网神信息技术（北京）股份有限公司

北京天融信网络安全技术有限公司　　深圳竹云科技有限公司

上海物盾信息科技有限公司　　安易科技（北京）有限公司

华为技术有限公司　　三未信安科技股份有限公司

阿里云计算有限公司

© 2023 云安全联盟大中华区版权所有

英文版本编写专家

主要作者：

Ravi Erukulla　　Ramesh Gupta　　Shruti Kulkarni　　Alon Nachmany

贡献者：

Faye Dixon　　Jonathan Flack　　Paul Mezzera　　Ansuman Mishra

Venkat Raghavan　　Heinrich Smit　　David Strommer

审校者：

Samuel Addington　　Radhika Bajpai　　Shannon Chisenga　　Ivan Djordjevic

Shamik Kacker　　Shamik Kacker　　Adnan Rafique　　Michael Roza

Nishanth Singarapu

CSA员工：

Ryan Gifford　　Stephen Lumpe

在此感谢以上专家。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给予雅正! 联系邮箱research@c-csa.cn； 国际云安全联盟CSA公众号。

© 2023 云安全联盟大中华区版权所有

目录

© 2023 云安全联盟大中华区版权所有

序言

在过去的几年里，全球事件加速了许多企业的数字化转型，陆续将业务迁移到云端成为了流行。目前大多数企业 IT 采用本地、云端或并行机制，在这样的状态下，提高可见性，安全性和保护数据的需求尤为重要，企业管理者发现在云中管理身份是一个首要问题，因为他们可能面临多个云服务提供商，业务跨多个节点，很容易形成身份孤岛从而增加风险暴露面。

身份管理与访问控制(IAM)是一个业务流程、策略和技术框架，使企业可以更轻松地管理数字身份。IAM 能够控制用户对其公司关键信息的访问，如今，组成 IAM 环境的许多组件（例如认证、授权、身份生命周期管理和特权访问）可以进行切片，以便企业可以选择在云中运行效率更高、更具成本效益的功能并保留必要的安全机制。基于云的 IAM 将成为企业上云进行网络防御、风险管理和数据保护能力的顶级安全安全实践。

本篇文献通过介绍影响 IAM 的云环境与本地环境之间的差异和过去解决方式的回顾，总结出目前 IAM 发展的趋势和在云环境中 IAM 面临的重要挑战，提出了针对云环境的有效的 IAM 最佳实践，用于帮助 IAM 在企业数字化转型中进行有效推动，从而加速数字经济，降低运营成本。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

© 2023 云安全联盟大中华区版权所有

摘要

身份管理与访问控制（Identity and Access Management，IAM）并非一种新的解决方案。IAM 工具和实践用于保护字（有时甚至是物理）资源，并满足法规/合规要求。

IAM 最初是一种通用的机制，通过对被授权的身份或身份组赋予权限来限制和控制对组织资源的访问。它最初的目标是验证权限，并且访问（控制）是完全基于对用户名和口令的判断，再加上直接在受访资源上分配的组成员身份或权限。这一模型后来演变为集中化的 IAM，而访问决策集中在一个权威机构上，如：服务、服务器或身份基础设施。多年来，威胁形势发生了重大变化，IAM 现今已成为任何数字访问模型的关键组成部分。随着用户、资源和系统这些（IAM 核心）性质发生变化，IAM 已经发展到使用不断增加的可见性、粒度和控制。例如：基于角色（RBAC）、属性（ABAC）或其他自适应（或启发式）的访问控制已经添加了分布式或基于事务的访问（控制能力）。随着多因素身份验证、通行密钥（passkeys）和数字证书的加入，身份验证工具和技术不断发展，并极大的增强了 IAM 的能力。

© 2023 云安全联盟大中华区版权所有

如今，IAM 已经远不仅是作为保护资源或者满足合规性的手段。随着全面云化、数字化以及由于 COVID 带来的远程和混合工作模式等发展趋势，IAM 已经成为一个业务的推动者，通常是网络安全的第一道防线。IAM 是组织零信任之旅的第一阶段，也往往是董事会级别的举措。随着云转型和云优先在组织的推动，

IAM的需求和实践也必须相应的发展，以保持与云环境新动态的同步。基于本地环境的传统IAM实践并不适用于云环境，因为云环境引入了更加短暂、敏捷、并且突破企业边界的访问。但是，并非所有的IAM团队或从业者都了解并且遵循IAM在云环境中的最佳实践，这使得IAM在云环境中的价值不佳，成本增高，并影响了满意度。

本文旨在提供以下内容的概述：

- 云环境与本地环境的差异对 IAM 的影响
- 影响 IAM 的因素，IAM 为解决这些问题而进行的改进，以及它将如何在未来进一步发展
- IAM 在云环境中与日俱增的重要性
- 组织在云环境中有效应用 IAM 时面临的挑战
- 在云环境下部署有成效的 IAM 项目时需要考虑的因素与最佳实践
- 为安全/IAM 领导者和从业者沟通 IAM 价值的提示

© 2023 云安全联盟大中华区版权所有

引言

对于任何组织的技术栈和安全基础设施而言，身份管理与访问控制（IAM）都是其关键的组成部分，特别是在云环境中。本文档的主要受众是 IAM 项目负责人和安全运营团队，然后是首席信息安全官（CISO）和高层领导。本文档的目的是介绍在云环境下管理 IAM 所涉及的挑战和注意事项，以及 IAM 对组织整体安全战略的重要性。

© 2023 云安全联盟大中华区版权所有

云环境与本地部署 IAM 的差异

所有权是企业使用云交付 IAM 解决方案与管理私有化部署的 IAM 解决方案之间的一个根本区别。当一个组织在内部环境部署 IAM 解决方案时，该组织拥有一切，包括软件许可证和用户管理；与 IAM 解决方案相关的持续资本支出的责任，例如硬件（例如，服务器购买）、功耗和物理空间；以及支持内部管理的 IAM 解决方案的基础设施所需的所有其他支出。客户利用云服务提供商(CSP)的 IAM 构建的应用程序，则使用订阅模式，并遵循共享责任模型。

使用基于云的 IAM 解决方案与部署 IAM 私有化解决方案之间的另一个基本区别是控制。在私有化部署中，组织管理 IAM 的各个方面，包括漏洞管理、修补、渗透测试等。当组织从云服务提供商（CSP）采购基础设施即服务（IaaS）等服务时，该组织则不需要考虑漏洞管理、补丁等因素，因为“云安全”的这些方面由 CSP 负责。

使用云 IAM 更大的挑战和复杂性是由组织采购的云环境的激增（译者注：比如多云环境）。当一个组织运行多个基础设施即服务（IaaS）环境、平台即服务（PaaS）采购和软件即服务（SaaS）时，IAM 变得复杂而富有挑战性。在每个环境中提供身份可能很简单，但访问控制审查和身份撤销可能并不简单，这可能导致离职者依然具有这些环境的访问权。

© 2023 云安全联盟大中华区版权所有

IAM 溯源分析

如前所述，IAM 不是一个新的解决方案。自大型机时代以来，它就一直存在，但在客户机/服务器时代，它变得更加重要，当时的应用程序变得更加分散，并包含了它们的身份烟囱。每个用户和权限都不得不在各个应用中管理，这导致了访问这些应用程序所需用户身份和口令数量的激增。

目录服务旨在通过提供集中的用户存储库以及一种称为轻量级目录访问协议（LDAP）的访问协议来解决这个问题。目录服务实现了跨多个平台（包括操作系统、数据库和 web 服务器）的相同登录。在此期间，Microsoft 的 Active Directory 成为管理计算机的公司标准，提供了管理用户、组和访问策略的体系结构。在互联网的早期，多个凭据和登录的问题比较严重，因此开发了单点登录（SSO）来促进跨组织应用程序的用户身份验证和授权，在大多数情况下利用 LDAP 目录作为身份存储。

此外，管理用户生命周期管理和访问策略的问题主要是通过定制的应用程序实现的，这些应用程序最终成为产品化的用户供应和管理解决方案。还需要治理功能来满足监管要求，并最终与身份管理和供应解决方案融合，成为现在所称的身份治理和管理（IGA）解决方案。在过去的十年里，这些解决方案作为云解决方案提供，利用了云的所有好处，包括维护 IAM 平台，在许多情况下，IAM 平台需要专门的资源来维护。为了进一步简化 IAM 的使用案例和部署，并减少与实施多种解决方案相关的成本和负担，解决方案正在融合，以提供 IAM 解决方案的组合，如身份治理和管理（IGA）、特权访问管理（PAM）以及客户身份管理与访问控制（CIAM）。

© 2023 云安全联盟大中华区版权所有

IAM 的发展趋势

数据经济时代，企业组织向混合办公和远程办公模式的转变，进一步加速了云解决方案的普及以及数字化转型的深入，许多组织在选择应用和安全解决方案时，积极采用 “云优先”的战略。此外，在云平台实施 IAM 解决方案以管理用户与权限，IAM 解决方案针对每个平台都是独特的。云上 IAM 引入了一整套云特有的原生身份参与者，例如机器身份、服务账号、工作负载身份和人员身份等。主要趋势包括:

> - 采用去中心化的身份模型：区块链和自主身份模型成为主流，用户能够掌控自己的身份数据，提供了一种替代传统身份供应商的解决方案。
> - 即时和基于风险的访问控制：越来越多的企业组织仅在需要时提供访问权限，并非授予广泛、长期有效的权限。此外，访问决策可能基于用户的风险级别和所请求访问的资源来进行判定。

许多组织努力争取对其用户和权限有正确的可见性和管理。这些服务通常分布在多个云平台，除了管理云服务之外，它还实现了一套通常由 DevOps 工具实例化的更短暂的工作负载。IAM 解决方案必须包括管理跨云服务的访问，如容器、无服务器基础设施、DevOps 和 CI/CD 工具，这些都需要访问策略才能运行。

云环境的IAM

与本地环境相比,在云中管理 IAM 存在独特的挑战,包括易变性和更快的增

© 2023 云安全联盟大中华区版权所有

长、对敏捷性的需求以及与合规性和其他问题相关的不同风险。一个关键的区别是云环境中 API 的使用量增加，而不是经常在本地环境中使用的基于组策略的方法。这些在技术和方法上的差异需要思维方式的转变和企业内部实践对云计算的适应。

多云/混合环境 IAM 解决方案的重要性与日俱增

云技术为企业带来了众多优势，例如按需付费、快速部署、短期运营以及长效投资、在几分钟内弹性伸缩资源等。由于这些优势，在过去几年中，我们看到了云在企业和个人应用的巨大增长。在迁移到云的过程中，企业仍然在采用混合模型（部分本地，部分上云），甚至采用多云策略来充分利用以实施最佳解决方案。

随着资源迁移到云上，无论是人还是非人实体，都需要在任何时间、任何地点，并具备适当的权限，经过身份认证和授权才能访问这些资源。与此同时，由于资源不再处于组织的网络边界内，它们也更容易受到攻击。因此，更需要确保实体对正确的资源具有适当的访问权限。

在多云环境中，用户需要访问各类分散的资源。如何确保用户对正确的资源具有适当的访问权限？如何管理他们的权限？服务账号和机器身份在多云环境中需要运行单独的自动化流程，并连接到不同的工作负载。如何管理这些身份及其权限？一个良好的云环境 IAM 策略是解决这些问题的答案。

IAM对企业高管的重要性

© 2023 云安全联盟大中华区版权所有

IAM 对于保护组织的资产和数据起着至关重要的作用。企业高管应该意识到 IAM 可以有效降低风险、促进合规性，并为企业组织整体安全战略方面创造价值。IAM 团队可以通过突出显示云迁移的好处来帮助展示这一价值，例如改进的多云可见性，以及保持对角色分配状态和更改警报的可见性的能力。

企业有效地采用云 IAM 所面对的挑战

身份管理十大挑战

1. 跨多个云环境的身份管理
2. 基于云的身份提供商面临的威胁
3. 确保符合法规和标准
4. 管理非人实体的身份
5. 与新兴趋势的整合
6. 跟上不断变化的威胁环境
7. 管理外部用户和合作伙伴的身份
8. 解决BYOD和身份的独特挑战
9. 管理IT/OT的身份，它们部署在本地，但与基于云的解决方案有接口
10. 保持对角色绑定和访问控制的可见性和控制

如需进一步了解，详情见我们的推文：“应对云身份管理与访问控制中的十大挑战”

© 2023 云安全联盟大中华区版权所有

云 IAM 带来更多商业机会

IAM 是绑定云服务的粘合剂。一个负责任的、经过深思熟虑的云 IAM 战略打开了巨大的业务机会，并促进了对新业务需求的更敏捷的响应。

> a. 加速企业数字化转型
>
> b. 推进新的商业模式创新
>
> c. 加速向数据经济转型
>
> d. 云IAM的自动化潜力为开发人员和构建者提供了巨大的生产力
>
> e. 缩减运营成本
>
> f. 简化合规与治理

© 2023 云安全联盟大中华区版权所有

在云环境中制定有效的 IAM 计划的注意事项和最佳实践

在云环境中制定有效的 IAM 计划的注意事项和最佳实践与传统本地部署环境有所不同，以下列举一些重要的考量因素：

- 多云与复合环境中集中管理身份、权限及授权。
- 自动化以及与现有系统集成。
- 安全可靠的认证方法。
- 基于用户角色和属性的授权与访问控制策略。
- 定期监控和审计相关访问行为和活动
- 遵守数据保护法规。
- 与加密、威胁保护等其他安全措施集成。
- 尽可能遵守“最小权限”、“按需最小了解范围”规则。
- 利用诸如及时检测（JIT）、特权访问管理（PAM）和特权身份管理（PIM）等高级功能。
- IAM 流程自动化。
- 全面监控与审计。

© 2023 云安全联盟大中华区版权所有

为了在云环境中有效实施 IAM 项目，推荐参考以下最佳实践：

- 实施多因子身份认证确保访问安全
- 创建并实施强口令策略
- 在适配场景下实现从高强度密码向无口令转变
- 针对用户和应用程序实施基于角色的访问控制（RBAC）
- 对传输中和静态的敏感数据（包括凭证）进行加密。
- 定期监控访问行为和活动日志，以及时发现异常和安全事件。
- 不断评估和更新安全策略，以应对最新威胁。
- 了解云环境中的 IAM 对云数据安全的直接影响。

© 2023 云安全联盟大中华区版权所有

给安全/IAM 领导和从业者关于沟通 IAM 价值的提示

- 明确阐述 IAM 的业务优势，例如改善最终用户体验、无缝单点登录、安全性与合规性提升，以及工作效率的提高。
- 介绍 IAM 项目如何帮助其他企业实现安全防护目标的实际案例。
- 利用数据和指标来证明 IAM 项目的投资回报率。
- 介绍 IAM 项目对企业整体安全策略的重要性。
- 对企业全体员工进行培训，确保他们了解 IAM 项目的重要性以及他们在企业安全防护方面的作用。
- 注重企业内部安全防护文化的培养，鼓励员工报告任何安全问题。
- 定期向所有利益相关者汇报 IAM 项目的最新进展。

© 2023 云安全联盟大中华区版权所有

结论

总之，与本地部署环境相比，在云环境中的进行 IAM 项目管理面临着独特挑战和一些特别注意事项。企业组织需要明确制定战略来应对这些挑战，确保企业资产和数据的安全。IAM 项目团队应与企业高管密切合作，探讨 IAM 项目的价值及其在组织整体安全战略角色中的作用。此外，企业应制定规范流程以监控和验证身份，并重视管理人类和非人类实体身份所面临的独特挑战。

© 2023 云安全联盟大中华区版权所有

CSA 企业会员案例

阿里云应用身份服务 IDaaS 在某游戏大厂实践案例

某游戏大厂与阿里云应用身份服务 IDaaS 携手共建身份认证平台，实现各大工作室人员身份的统一治理以及全球范围云服务器的权限管控，保障企业海内外业务高效安全发展。

方案背景

某游戏行业大厂发行的游戏覆盖全球市场，有多款 TOP 级游戏备受玩家青睐。

发展初期，企业人员不多，工作室数量也很少，业务集中在国内。但随着公司业务的高速扩展，产品不断丰富，以及业务出海，员工快速扩展到 2000 多人，建立了 10 余个工作室，在中国，以及美国、韩国、日本、泰国等国家都扩展了云服务资源。

公司对于工作室员工以及云服务资源管理的整体管理变得异常吃力：

1、沟通工具五花八门，用户多个账户，使用不便

每个工作室内部协同沟通工具五花八门，有企业微信、飞书、钉钉等，即便有工作室都在用企业微信，账号都是独立的，数据互不相通，员工访问业务应用时，需要再注册新的用户账号，相当于每个员工都有好几个账号。

2、权限开发管理各自为营，重复开发，造成资源浪费

© 2023 云安全联盟大中华区版权所有

公司每个云服务器都是由当地外包团队管理的，而每个游戏所在的地区的服务器权限都是由游戏开发团队开发，其中涉及到一些相对标准的用户角色，比如客服类，相同的开发工作和管理工作需要在不同的团队中重复进行，无法实现资源的合理利用和共享。

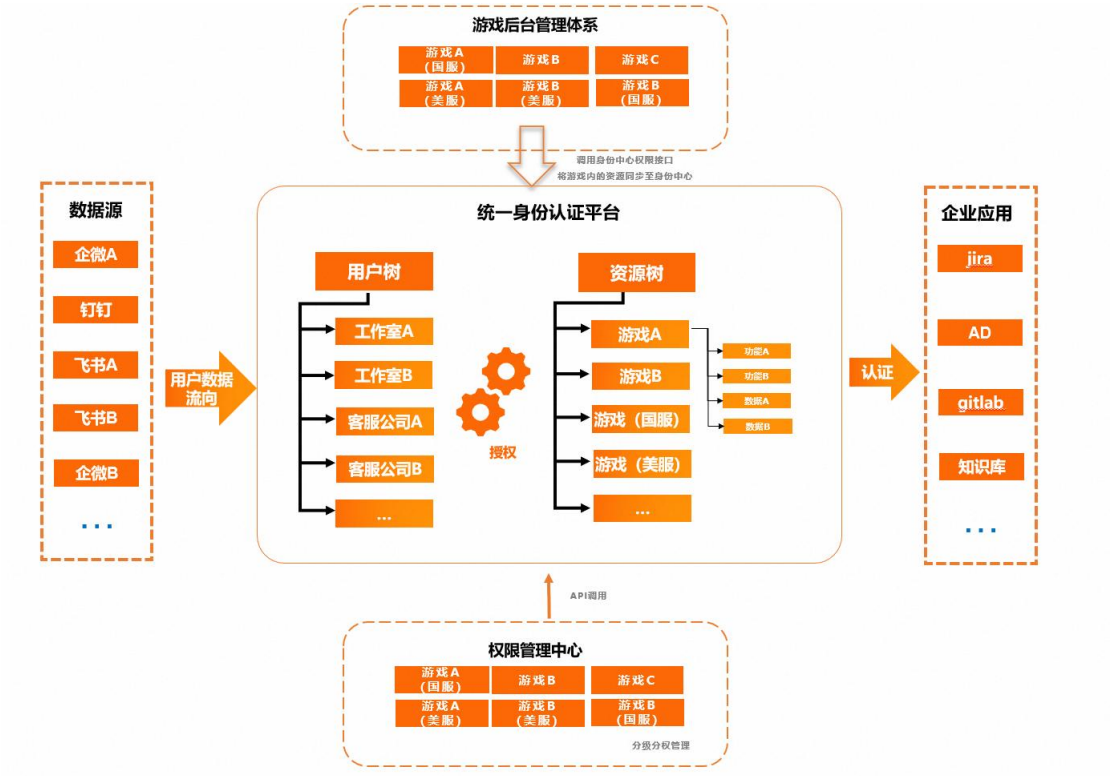
未来，这家游戏公司工作室还会持续扩增，人员只会越来越多，公司的游戏产品以及出海业务搭建的云服务器也只会更多。当下企业面临的用户身份数据、以及海外外包团队访问云服务器的权限管理问题若不解决，未来将会更棘手，被拖住的不仅是业务增长速度，还会引发安全问题。

建设方案

阿里云 IDaaS 以身份管理为核心，帮助某游戏大厂搭建统一身份认证平台，对多个沟通工具进行用户数据集成管理，打通该游戏公司所有工作室的员工身份数据，并进行统一管理，同时，建立统一的权限管理中心，所有海外云服务器的权限进行整合统一管控。从根源搬走阻挡企业发展的“绊脚石”，杜绝一切安全隐患发生。

© 2023 云安全联盟大中华区版权所有

具体实施方案如下：



1、建设身份中心，统管来源各异的身份数据

阿里云 IDaaS 通过搭建统一身份认证平台，上游对接游戏公司的各大工作室的各类沟通工具的身份数据，如企微、飞书、钉钉等，下游对接公司的各类应用工具。通过身份数据的打通，工作室的员工可以用原有的沟通平台账号直接登录公司的各类应用，如 jira、AD、gitlab、知识库等，极大地简化了员工的操作流程，以及提高了工作效率。

同时，阿里云 IDaaS 提供用户身份的自动同步更新，如各大工作室的钉钉中有员工账号信息发生变更（如入职、调岗、离岗等），无需管理员手动调整，都会自动同步到身份认证平台中，并同步到各业务应用中，确保各

© 2023 云安全联盟大中华区版权所有

个应用身份信息的一致性。

2、统管全域服务器账号权限，安全又高效

阿里云 IDaaS 通过为游戏企业搭建统一的权限管理中心，实现全域游戏服务的权限统一建设及管理。无需游戏工作室单独成立开发团队进行权限体系的建设，节省了开发的时间成本、人员成本以及后期权限的管理成本，真正实现管理上的降本增效。

基于阿里云 IDaaS 细粒度权限管理能力，实现所有游戏服务器管理员的分级分权控制，将用户划分为多个不同的级别或角色，每个级别或角色都被赋予相对应的权限，这些权限可以是对系统资源的访问、修改或执行特定操作的能力。权限管理细致程度能做到对每个用户访问某款游戏的某一项功能。用户只能执行其级别或角色所具有的权限，无法越权访问其他级别或角色的权限。

建设成果

阿里云 IDaaS 统一身份认证平台搭建之后，这家游戏大厂快速实现了旗下十余个工作室近 2000 名员工的统一管控，此前员工人均需要记住 4.8 个账号密码，日常使用的应用 17 个，每次都要重新输入账密进行登录，几乎每天都有员工出现忘记密码，需要重置密码的情况。现在人均只需要使用 1 套账密，经过一次认证即可登录所有应用，团队协作效率提升 51%，密码重置请求降低 74%。

同时，对于在多个国家部署的云服务器外包团队人员的权限进行了高效管理，以前需要十余个开发团队来完成的工作，现在仅需集中一个团队来完

© 2023 云安全联盟大中华区版权所有

成，除了减少重复开发工作，游戏公司可以更好地控制和管理公司内部的资源和权限，提高公司整体的运营效率。为公司每一个爆款游戏提供最高效的运营支撑，同时为公司未来的业务扩展提供了支持。

© 2023 云安全联盟大中华区版权所有

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