aws

保护半导体开发环境的策略 AWS

AWS 规范性指导

AWS 规范性指导: 保护半导体开发环境的策略 AWS

Table of Contents

简介 1
半导体行业概述 1
半导体公司需要最新的技术能力 1
利用规模经济、弹性和自动化 1
安全与合规 3
减少合规工作 3
使用参考架构 3
保护半导体数据 4
防止未经授权的访问和数据外泄 4
配置权限 4
验证用户身份 5
传输数据 5
加密数据 6
管理出站网络流量 6
满足数据驻留要求 6
保护远程体验 8
优化远程桌面体验 8
保护与第三方的协作 9
AWS 保安服务 11
防范勒索软件 12
AWS 云 差异化优势 13
结论 14
文档历史记录 15
..... xvi

保护半导体开发环境的策略 AWS

Mike Virgilio、Allan Carter 和 Nikhil Marrapu，Amazon Web Services（AWS）

2023 年 6 月（文档历史记录）

本文档提供了战略性指导，帮助您保护在 AWS 云中运行的半导体工作负载并满足其合规性要求。它包括示例架构以及 AWS 服务 和功能概述，可用于实施该指导并帮助保护敏感数据免受安全风险。

半导体行业概述

根据半导体行业协会的数据，半导体业务是一个价值 USD573 44亿美元的全球产业。为了保护知识产权（IP），安全是该行业的重中之重。半导体公司需要开发环境，以使他们的工程师能够设计芯片、电子系统、电路板和其他产品。安全的开发环境必须严格控制可以访问其中 IP 的人员。

公司开发自己的知识产权，但他们通常也使用来自第三方供应商的知识产权，例如处理器内核、标准接口、半导体代工厂的工艺设计套件 (PDKs) 以及电子设计自动化 (EDA) 公司的许可工具。高度协作性质的开发过程意味着内部工程师以及来自第三方公司的工程师都需要访问开发环境。一项关键的安全要求是防止未经授权的数据从安全的开发环境中泄露。

半导体公司需要最新的技术能力

半导体公司在竞争激烈的行业中运营 speed-to-market，在这个行业中，创新是成功的关键。随着芯片设计和制造要求日益复杂，半导体公司需要掌握最新技术，才能满足甚至超越行业需求。 AWS 云的可扩展性和容量能够满足指数级增长的计算和存储需求。凭借全面的基础设施和一系列强大的计算、网络和存储解决方案， AWS 助力半导体公司，使其能够利用机器学习、高性能计算和自动化等尖端技术。使用这些技术可以加快研发工作的速度，优化制造流程，并提供获得最新技术的途径。宝贵的 IP 很容易成为复杂攻击的目标，因此安全性成为安全开发环境的重中之重。

利用规模经济、弹性和自动化

AWS 为公司提供成功所必需的规模经济、资源弹性和自动化能力。由于 AWS 已经与成千上万家公司合作，因此可以实现大规模的规模经济，从而降低所有人的成本。 AWS 基础设施弹性使公司能够轻松地向上扩展以满足最苛刻的工作负载，然后向下扩展以优化成本。此外， AWS 自动化功能可帮助公司创建可重复的流程，从而最大限度地减少无差别的手动任务。 AWS 提供广泛的安全服务和功能，帮助半导体公司通过强大的安全控制来保护其工作负载，包括网络分段、数据加密和监管合规性。通过构

建 AWS 云，半导体公司可以专注于创新和增长，同时还可以确保其数据和运营能够抵御潜在的安全风险。

实现半导体开发环境的安全性和合规性 AWS

AWS 已制定实施安全控制的最佳实践指南，并发布了满足半导体行业需求的参考架构。本节讨论如何使用 AWS 推荐的设计和参考架构来帮助实现任务关键型工作负载的安全性和合规性。 AWS

减少合规工作 AWS

分AWS 担责任模型描述了客户和客户之间 AWS 如何分担安全和合规责任。 AWS 负责云的安全，客户负责云端的安全。通过让 AWS承担云基础设施的责任，这可以帮助公司减少实现符合企业与监管要求所需的工作。

以下内容 AWS 服务 可以帮助半导体公司证明其符合公司和监管要求：

- AWS Artifact 提供各种合规性框架的可下载合规性报告，包括国际标准化组织（ISO）、美国国家标准与技术研究所（NIST）和联邦风险与授权管理计划（FedRAMP）。您可以将 AWS Artifact 报告与企业对云资源的评估相结合，向审计员证明合规性，并帮助减少遵守美国国际武器贸易条例 (ITAR) 等法规所需的时间和精力。
- AWS Audit Manager可以使用预建和自定义框架以及自动证据收集将您的合规要求与 AWS 使用数据对应起来。

通过使用这些服务和功能，公司可以更高效、更有效地符合企业和监管要求。有关是否在 AWS 保障计划范围内的更多信息，请参阅AWS 服务 按合规计划划分的范围。 AWS 服务

使用提供的参考架构

AWS 根据各行各业的数千次部署制定规范性指导和最佳实践。这些建议包含在 Well-Ar AWS chitected 框架AWS 、云采用框架AWS (CAF) AWS 和安全参考架构 (SRA) 中。AWS

在设计和设计安全开发环境时， AWS 提供基于上述框架的半导体和电子参考架构。这些参考架构旨在保护数据和工作负载。

您可以使用 AWS 安全成熟度模型来指导您分阶段完成待办安全控制措施。

通过利用这些框架、模型和参考架构，您可以在云建立强大的安全状况并帮助保护关键资产。

保护半导体数据 AWS

使用 AWS，您可以管理数据的隐私控制，并控制数据的使用方式、谁有权访问数据以及如何对其进行加密。这些能力以灵活安全的云计算环境为基础。本节回顾了帮助半导体公司实施数据访问控制和满足数据驻留要求 AWS 的能力。

本节包含以下主题：

- 防止未经授权的访问和数据外泄
- 满足以下方面的数据驻留要求 AWS

防止未经授权的访问和数据外泄

根据 2022年数据泄露成本报告（Ponemon Institute报告），2022年数据泄露的平均成本为百万美元。USD4.3 对于半导体公司而言，保护知识产权（IP）至关重要。由于未经授权访问而导致的 IP 丢失可能造成经济损失、声誉受损，甚至是监管后果。这些潜在的后果使得控制数据访问和数据流成为架构完善设计中的关键环节。

保护数据安全的关键考虑因素包括：

- 访问安全开发环境的用户身份验证
- 访问安全开发环境内数据的用户授权
- 记录进出安全开发环境的所有传输
- 架构环境之间的安全数据流动
- 传输中数据和静态数据加密
- 限制和记录出站网络流量

配置权限

AWS Identity and Access Management (IAM) 通过控制谁经过身份验证并有权使用 AWS 资源，从而帮助您安全地管理对资源的访问权限。默认情况下，除非明确允许 AWS ，否则中的任何操作都会被隐式拒绝。您可以通过创建策略来管理 AWS 中的访问权限。您可以使用策略来精细定义哪些用户可以访问哪些资源，以及他们可以对这些资源执行哪些操作。 AWS 最佳做法是应用最低权限权限，这意味着您只向用户授予他们执行任务所需的权限。有关更多信息，请参阅 IAM 文档中的以下内容：

- IAM 中的策略和权限

- 策略评估逻辑
- IAM 安全最佳实操

验证用户身份

AWS 最佳做法是要求人类用户使用与身份提供商的联合身份验证才能使用临时证书 AWS 进行访问。集中处理用户员工访问权限的推荐服务是 AWS IAM Identity Center。此服务可帮助您安全地创建或连接员工身份，并集中管理他们对 AWS 账户 和应用程序的访问权限。IAM Identity Center 可以使用 SAML 2.0、Open ID Connect (OIDC) 或 OAuth 2.0 与外部身份提供商 () 联合，以提供无缝集成和用户管理。IdPs有关更多信息，请参阅 AWS（AWS 营销）中的身份联合和身份提供商和联合（IAM 文档）。

您还可以使用 AWS Directory Service 管理在 Active Directory 等目录中定义的用户和组，对用户进行身份验证和授权。在安全的开发环境中，您可以使用 Linux 文件权限来授权和限制虚拟私有云（VPC）内的数据访问。使用 VPC 终端节点提供访问权限， AWS 服务 无需通过公共互联网。使用终端节点策略限制哪些 AWS 委托人可以使用终端节点，并使用基于身份的策略来限制对终端节点的访问。 AWS 服务

传输数据

AWS 提供了多种将本地数据迁移到云端的方法。通常将数据最初存储在 Amazon Simple Storage Service（Amazon S3）中。Amazon S3 是一项基于云的对象存储服务，可帮助您存储、保护和检索任意数量的数据。传输数据出入 Amazon Elastic Compute Cloud（Amazon EC2）实例时，它可提供高达 25 Gbps 的带宽。该服务还提供跨区域数据复制和数据分层。存储在 Amazon S3 中的数据可以用作复制源。您可以使用它来创建新的文件系统或将数据传输到 EC2 实例。您可以将 Amazon S3 用作半导体工具和流程的 AWS 托管、符合便携式操作系统接口 (POSIX) 标准的文件系统的后端。

另一项 AWS 存储服务是 Amazon FSx，它提供的文件系统支持行业标准的连接协议，并提供高可用性和跨复制功能。 AWS 区域半导体行业的常见选择包括适用于 NetApp ONTAP 的亚马逊 FSx、适用于 Lu stre 的亚马逊 FSx 和 OpenZFS 的亚马逊 FS x。Amazon FSx 中的可扩展、高性能文件系统非常适合在安全的开发环境中本地存储数据。

AWS 建议您 AWS 先定义半导体工作负载的存储要求，然后确定适当的数据传输机制。 AWS 建议使用AWS DataSync将数据从本地传输到 AWS。 DataSync 是一项在线数据传输和发现服务，可帮助您在 AWS 存储服务之间移动文件或对象数据。根据您使用的是自我管理的存储系统还是存储提供商（例如） NetApp，您可以进行配置 DataSync 以加快通过 Internet 或通过互联网向安全开发环境移动和复制数据的速度。 AWS Direct Connect DataSync 可以传输您的文件系统数据和元数据，例如所有权、时间戳和访问权限。如果您要在适用于 ONTAP 的 FSx 和 ONTAP 之间传输文件， NetApp 建议

使用。 AWS NetApp SnapMirrorAmazon FSx 支持静态加密和传输中加密。使用 AWS CloudTrail 和其他服务特定的日志记录功能，记录所有 API 调用和相关数据传输。将日志集中在专用账户中，并对不可变的历史记录应用精细的访问策略。

AWS 提供其他服务来帮助控制数据流，包括具有应用程序感知能力的网络防火墙 AWS Network Firewall，例如 Amazon Route 53 Resolver DNS 防火墙和 Web AWS WAF代理。通过在 Amazon Virtual Private Cloud（Amazon VPC）中使用安全组、网络访问控制列表和 VPC 端点，以及在 AWS Organizations中使用网络防火墙、中转网关路由表和服务控制策略（SCP）来强制执行网络分段，从而控制环境中的数据流。使用 VPC 流日志和 VPC 流日志版本 2-5 中的可用字段集中记录所有网络流量。

加密数据

使用 AWS Key Management Service （AWS KMS）客户自主管理型密钥或 AWS CloudHSM 加密所有静态数据。创建和维护精细的密钥资源策略。有关详细信息，请参阅 Creating an enterprise encryption strategy for data at rest。

使用行业标准的 256 位高级加密标准 () AES-256 密码强制执行至少 TLS 1.2，对传输中的数据进行加密。

管理出站网络流量

如果安全开发环境需要访问互联网，则应通过网络级执行点（例如通过 Network Firewall 或开源代理 Squid）记录和限制所有出站互联网流量。VPC 端点和互联网代理可帮助防止用户未经授权的数据外泄。这对于允许在安全开发环境中且仅在 VPC 内访问数据至关重要。

最后，您可以使用网络访问分析器（Amazon VPC 的一项功能）执行网络分段验证，并识别不满足指定要求的潜在网络路径。

通过分层安全控制措施，您可以建立和强制执行强大的数据边界。有关更多信息，请参阅在上构建数据边界。 AWS

满足以下方面的数据驻留要求 AWS

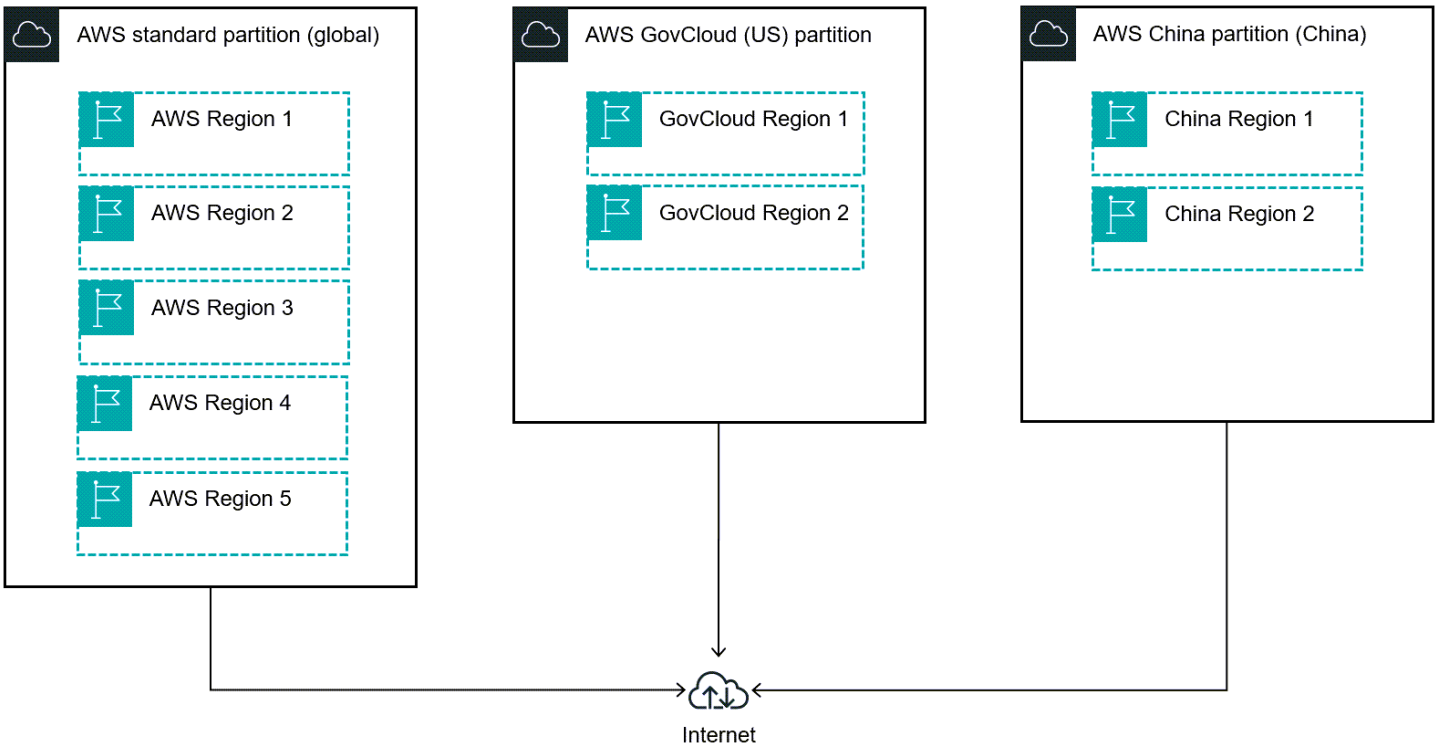
可用分区 AWS 区域、可用区域和 Local Zones 允许公司根据其独特要求为其数据和工作负载选择最佳位置：

- 分区是一个逻辑组 AWS 区域。 AWS 商业区域位于aws分区中，中国的区域位于分区aws-cn中，AWS GovCloud (US) Regions 并且在分区aws-us-gov中。

- AWS 区域是 AWS 集群数据中心的独立地理区域。
- 每个 AWS 区域 都有多个被称为可用区的隔离位置。
- 本地区域是在地理位置上靠近用户的区域的扩展。

有关当前可用区域、可用区和本地区域的更多信息，请参阅 AWS 全球基础设施。

分区可将数据、网络和计算机与其他分区中的区域隔离。 AWS 分区创建逻辑网络隔离，在不同分区中的区域之间使用单独的凭证访问权限。分区包括一个或多个区域，但一个仅 AWS 区域 存在于一个分区中； AWS 区域 不能是两个分区的一部分。



您可以根据是否需要美国政府安全分类在分区之间进行选择。处理未分类数据或官方数据的工作负载可以同时使用标准分区 AWS GovCloud (US) 或标准分区。 AWS 还提供了其他经过认证可以在 Secret 和 Top-Secret US 安全分类级别上运行工作负载的分区，但这些分区不在本指南的讨论范围之内。有关在这些分类级别运行工作负载的更多信息，请参阅 Cloud Computing for US Defense 和 Cloud Computing for the US Intelligence Community。

我们建议在单个分区内部署多区域工作负载，以减少任何合规性、运营和技术难题。但是，在有限的用例中，例如 with AWS Direct Connect或 Amazon CloudFront，您可以跨多个使用场景集成服务以实现特定目标。有关更多信息，请联系您的 AWS 解决方案架构师。

为工程师提供安全的远程体验

远程可视化是半导体设计的重要组成部分。工具工程师使用远程验证，而芯片设计人员使用远程验证来提交作业并查看其状态。本节介绍一种强大的解决方案，它可以在不同的网络条件下均表现良好。它采用云原生设计，因此可以与 AWS 安全服务无缝集成。

本节包含以下主题：

- 优化远程桌面体验
- 保护与第三方的工程协作

优化远程桌面体验

设计人员通常使用基于终端的 SSH 会话或图形远程桌面来提交和可视化工作流程。远程桌面提供 GUI-driven 交互式工具（例如布局、位置和路线），供刀具工程师和芯片设计师提交作业。 AWS 提供 Amazon DCV，这是一种高性能的远程显示协议，可为工程和物理设计团队提供强大的用户界面。Amazon DCV 在不同的网络条件下均表现良好。

为帮助保护数据隐私，Amazon DCV 流式传输的是像素而不是几何图形。此外，Amazon DCV 使用 TLS 来保护像素和最终用户输入。

使用连接文件，用户可以立即连接到 Amazon DCV 会话。但是，请注意，连接文件参数使用 `password` 和 `proxypassword` 字段而不加密。有关更多信息，请参阅 Using a connection file。Amazon DCV 在服务器与客户端之间建立 TLS 连接。连接文件中的验证策略确定在无法验证证书是否可信时客户端如何响应。有关更多信息，请参阅 Set certificate validation policy。

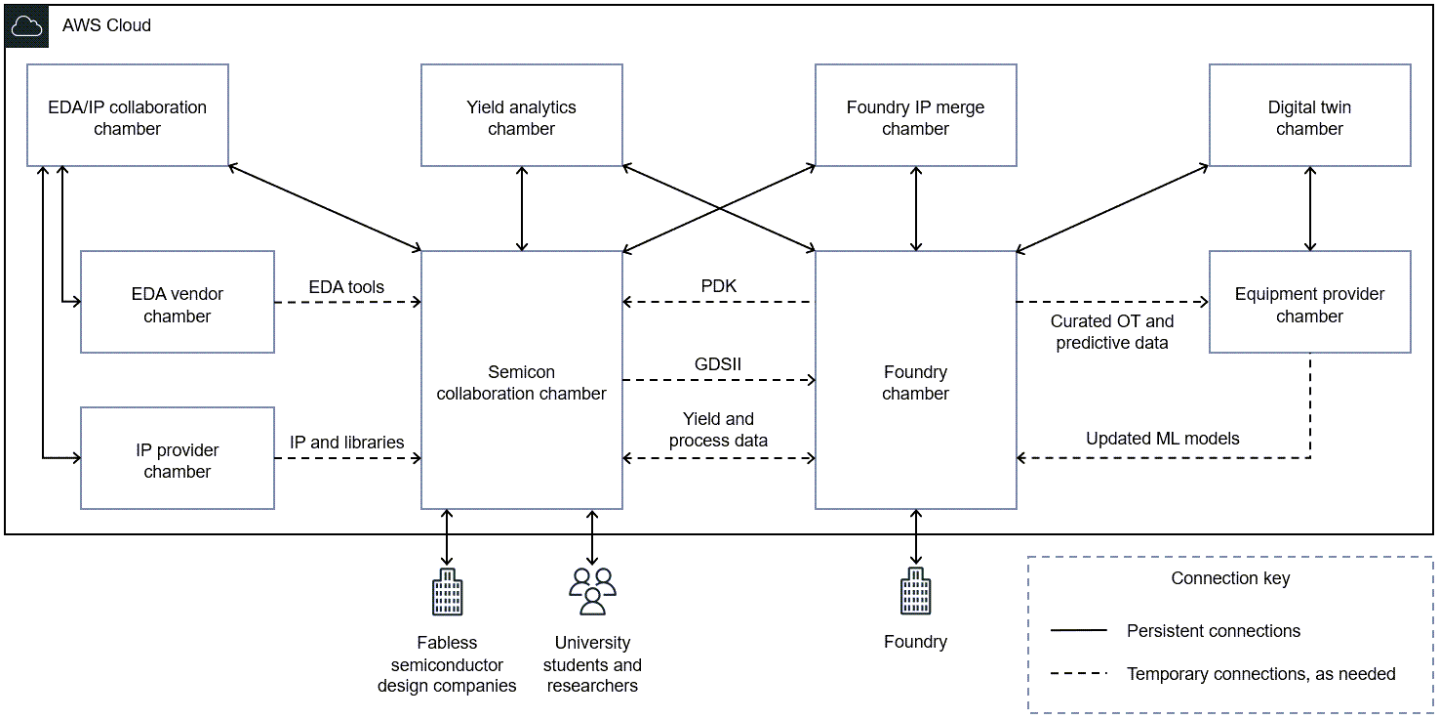
其他提供远程桌面功能的本地商业解决方案包括NoMachine或 Exceed Tur OpenText Box。

对于任何远程桌面解决方案，底层基础设施均由 Amazon Elastic Compute Cloud（Amazon EC2）提供支持。根据责任共担模式，您的责任包括以下几个方面，以帮助保护远程桌面实例：

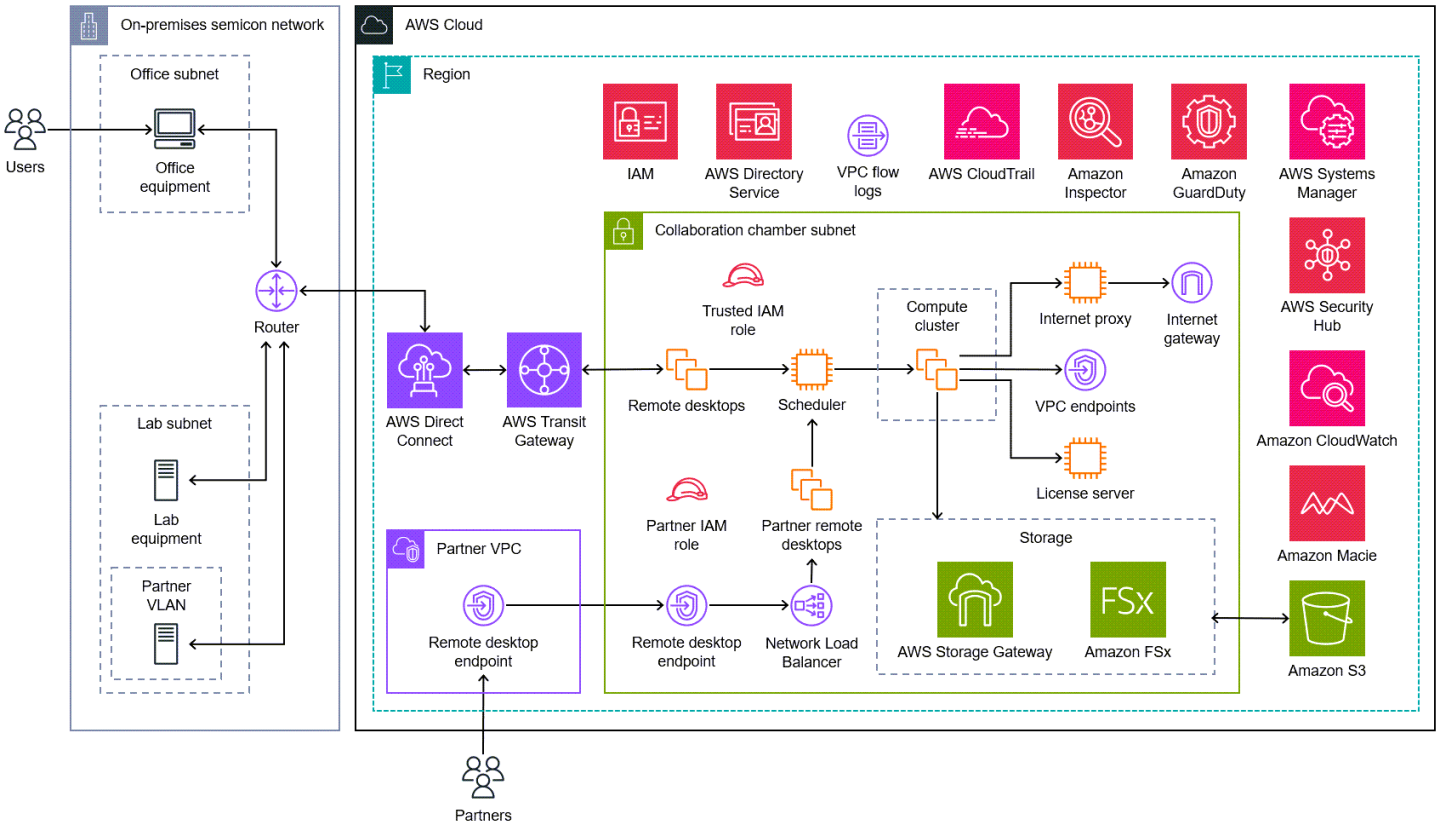
- 例如，通过配置 VPC 和安全组来控制对实例的网络访问。有关更多信息，请参阅控制网络流量。
- 管理用于连接到您的实例的凭证。
- 管理访客操作系统和部署到访客操作系统的软件，包括更新和安全补丁。有关更多信息，请参阅 Amazon EC2 中的更新管理。
- 配置附加到实例的 IAM 角色以及与这些角色关联的权限。有关更多信息，请参阅 Amazon EC2 的 IAM 角色。

保护与第三方的工程协作

为调试工具问题、获得设计 IP 集成方面的帮助，以及引进具有专业技能的外部承包商，在开发过程中与第三方合作至关重要。从本地基础设施向第三方提供安全访问可能非常困难。通过使用 AWS 基础设施即代码 (IaC)，您可以创建主安全开发环境的副本，称为协作室。为了防止数据外泄，请通过不允许访问互联网来加强协作空间的安全状况。协作空间有协作者的账户，您可以整理该空间中的数据、工具和基础设施，使其仅包含协作所需的内容。协作完成后，删除协作空间以降低成本，并消除对数据的任何潜在访问权限。下图显示设计和制造过程中的不同参与者可能如何使用各种类型的协作空间。



下图是协作空间的参考架构。在 AWS上设计和构建协作空间时，可以将此架构用作参考。图中的 AWS 安全、治理和监控服务有助于保护商会的安全，从而保护知识产权。有关这些服务的更多信息，请参阅本指南中的AWS 半导体开发环境的安全服务。


On-premises semicon network
Office subnet
Users
Office equipment
Router
Lab subnet
Lab equipment
Partner VLAN
AWS Cloud
Region
IAM
AWS Directory Service
VPC flow logs
AWS CloudTrail
Amazon Inspector
Amazon GuardDuty
AWS Systems Manager
Collaboration chamber subnet
Trusted IAM role
Compute cluster
Internet proxy
Internet gateway
AWS Security Hub
AWS Direct Connect
AWS Transit Gateway
Remote desktops
Scheduler
VPC endpoints
Amazon CloudWatch
License server
Partner IAM role
Partner remote desktops
Storage
Amazon Macie
Partner VPC
Remote desktop endpoint
Remote desktop endpoint
Network Load Balancer
AWS Storage Gateway
Amazon FSx
Amazon S3
Partners

AWS 半导体开发环境的安全服务

AWS 开发了安全服务，旨在保护您的工作负载和应用程序 AWS 云。这些服务可以帮助保护在云运行的任何类型的工作负载，而不仅仅是半导体工作负载。通过使用这些工具 AWS 服务，公司可以建立强大的预防和侦查控制措施，近乎实时地监控其安全态势，并在出现安全风险和事件时快速对其进行补救。这些服务能够随着环境的增长而自动扩展，以保持覆盖范围并维持既定的安全状况。此外，虽然这些服务可能侧重于特定功能，但它们支持名为 Amazon 的通用消息总线， EventBridge因此您可以集成服务并自动响应安全风险。

以下 AWS 服务 和功能可以帮助您管理访问权限和策略、检测和响应安全风险和事件，以及在您的 AWS 环境中实施监控和日志记录：

- AWS CloudTrail 可帮助您审计 AWS 账户的治理、合规性和运营风险。
- Amazon GuardDuty 是一项持续的安全监控服务，可分析和处理日志，以识别您的 AWS 环境中意外和可能未经授权的活动。
- Amazon Inspector 是一项漏洞管理服务，可持续扫描您的 AWS 工作负载，以查找软件漏洞和意外网络泄露。
- AWS Security Hub CSPM提供了您的安全状态的全面视图 AWS。它还可以帮助您根据安全行业标准和最佳实践检查您的 AWS 环境。
- Amazon Security L ake 会自动将来自云端、本地和自定义来源的安全数据集中到存储在您的专用的数据湖中。 AWS 账户您可以查询和分析这些安全数据，以发现趋势和异常情况。
- 服务控制策略 (SCPs) 是一种策略 AWS Organizations ，可帮助您集中管理 AWS 服务 多个账户的使用。
- VPC Flow Logs 是 Amazon Virtual Private Cloud（ Amazon VPC ）的一项功能，可捕获进出 VPC 网络接口的 IP 流量信息。您可以使用这些数据进行排查，并对事件进行响应。

保护半导体工作负载和数据免受勒索软件攻击

勒索软件是一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。不幸的是，这种攻击在互联网上非常普遍，可能影响任何规模的企业。除了经济损失和声誉受损外，半导体公司还必须防止运营中断，因为中断可能会对整个业务生态系统造成大规模的连锁供应链影响。它还可能导致宝贵的知识产权损失。

为了帮助防范勒索软件，半导体公司必须保持警惕，保护其本地和云环境的各个方面，尤其是存储、处理或传输数据的系统。 AWS 提供了许多架构设计和控件，可以帮助防范此类事件。除了本指南中提到的控件外，请参阅以下有关保护云工作负载免受勒索软件侵害的 AWS 资源：

- AWS 云 安全-防范勒索软件（AWS 云 安全）
- AWS 勒索软件防御蓝图（AWS 安全博客文章）
- 保护您的 AWS 环境免受勒索软件的侵害（AWS 网络研讨会）
- 电子书：保护您的 AWS 环境免受勒索软件的侵害（AWS 电子书）
- The anatomy of ransomware event targeting data residing in Amazon S3（AWS 安全博客文章）
- 关于 AWS 使用 NIST 网络安全框架 (CSF) 的勒索软件风险管理（白皮书）AWS

半导体 AWS 云 行业的差异化因素

对于半导体公司来说，从本地环境迁移到本地环境的商业案例 AWS 可能极具吸引力。本地基础设施的管理成本可能较高，且需要大量的前期投资，同时需要大量的工作来维护和保持最新技术，还需要从众多独立供应商采购安全工具。使用 AWS，您只需为使用的资源付费，这可以帮助您优化工作负载的成本。 AWS 还提供对最新高性能计算 (HPC) 和云存储服务和功能的即时访问。例如， FSx 适用于 NetApp ONTAP 的 Amazon 是一种常用的存储服务。您可以使用它将数据从本地 NetApp 存储无缝迁移到，它还提供网络隔离 AWS 云、资源级权限、基于身份的身份验证、加密、日志记录和审计。

AWS 还可以提高为半导体公司提供和管理安全解决方案的效率。使用中的高级安全功能和服务 AWS，您可以实施强大的安全态势，帮助保护您的数据和工作负载免受安全风险的侵害。通过使用 AWS Organizations 和集成式安全服务，您可以在组织内的所有 AWS 账户 自动部署安全控制措施。自动化功能可帮助您自动应对风险并简化安全运营，从而减少管理全面安全架构所需的时间和资源。例如， AWS 提供工具和服务，用于在整个环境中进行自动化安全管理、持续合规监控以及风险检测和响应。通过使用这些解决方案，半导体公司可以改善其安全状况，同时还可以降低成本和提高效率。总体而言，迁移到 AWS 可以帮助半导体公司在可扩展性、灵活性和安全性方面实现显著优势。

结论

AWS 提供了一个广泛而安全的平台，该平台支持半导体公司的需求。通过使用最新技术，并利用规模经济、弹性扩展能力和广泛的安全服务，半导体公司可以在 AWS 云中实现业务转型。这些 AWS 云优势可以解决复杂的挑战，同时优化创新和持续增长。AWS 全球基础设施已准备好支持最复杂的要求，例如数据驻留和安全分类要求。AWS 可以帮助您降低成本、提高敏捷性、加快创新速度并保护云知识产权。如需在 AWS 云中配置半导体开发环境的帮助，请联系您的 AWS 账户团队或使用联系 AWS 表。有关半导体行业的其他 AWS 信息和资源，请参阅 Semiconductor & Hi-Tech Electronics。

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

变更	说明	日期
初次发布	—	2023 年 6 月 20 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。