Microsoft

Microsoft Online Tech Forum

微软在线技术峰会

如何提升Azure云平台的隐私与环境治理

赵健　微软云架构师

Agenda

- 云端治理的意义 & 持续云端治理的过程
- Azure云端治理的框架
- 云端治理之安全&身份管理
- 云端治理之部署加速
- 云端治理之资源一致性
- 云端治理之花费管理

Microsoft

云端治理的意义 & 持续云端治理的过程

治理的定义

Governance is all of the processes of governing, whether undertaken by a government, market or network, whether over a family, tribe, formal or informal organization or territory and whether through the laws, norms, power or language of an organized society.

It relates to "the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions."

In lay terms, it could be described as the political processes that exist in between formal institutions.

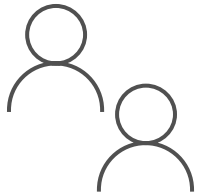
https://en.wikipedia.org/wiki/Governance

云端治理需求

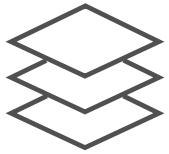
公司的多个部门正在云环境中部署资源，进行数字化转型，如果云中资源没有很好的被管理，企业在云端将会面临严重的业务风险及危害

企业需要规范化云端资源的使用，通过合理的资源配置及要求，满足企业上云的合规性、成本管理、安全性、架构等多方面需求

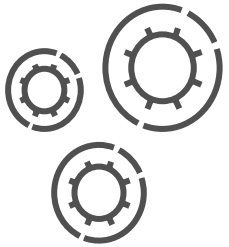
尽早实现云端资源的规范化管理，助力企业的数字化转型成功



优秀的人才



恰当的资源



合理的配置

持续化治理

治理的三要素

1. **规划**
   - 不同的系统迁移上云，都会面临各种**业务风险**，以及所能够**承受的风险损失**，及早**发现问题**，及时**规避风险**，能够加速企业云端转型
   - 各类云端系统，需要满足不同的**数据保护**以及相应的**合规性要求**

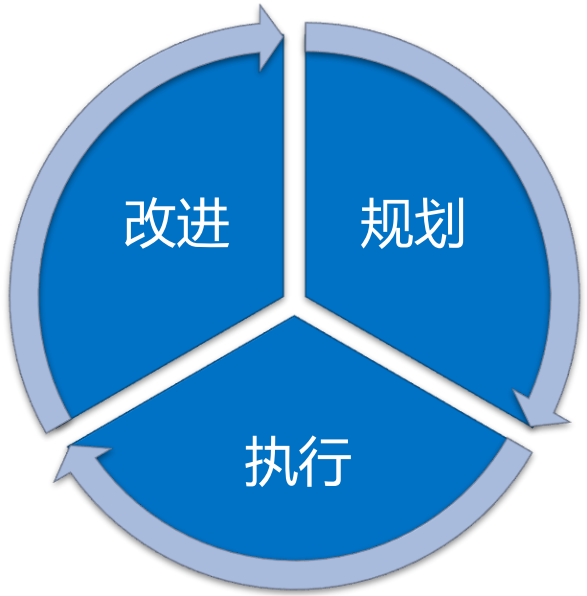
   将**风险管理**转化成为**云端管理规范**，是开启云端治理的第一步

2. **执行**

   明确所采取的**方法及工具**，来满足云端管理规范，如：报告，加密，审核等，通过**合理化的实施及量化的指标**，确保云端资源符合公司的管理要求

3. **改进**

   确保治理实施**符合预期**；定期**审核环境**中的资源，对不合规范资源进行**整治**，对治理流程进行**优化**，来最大限度的**减少业务风险**



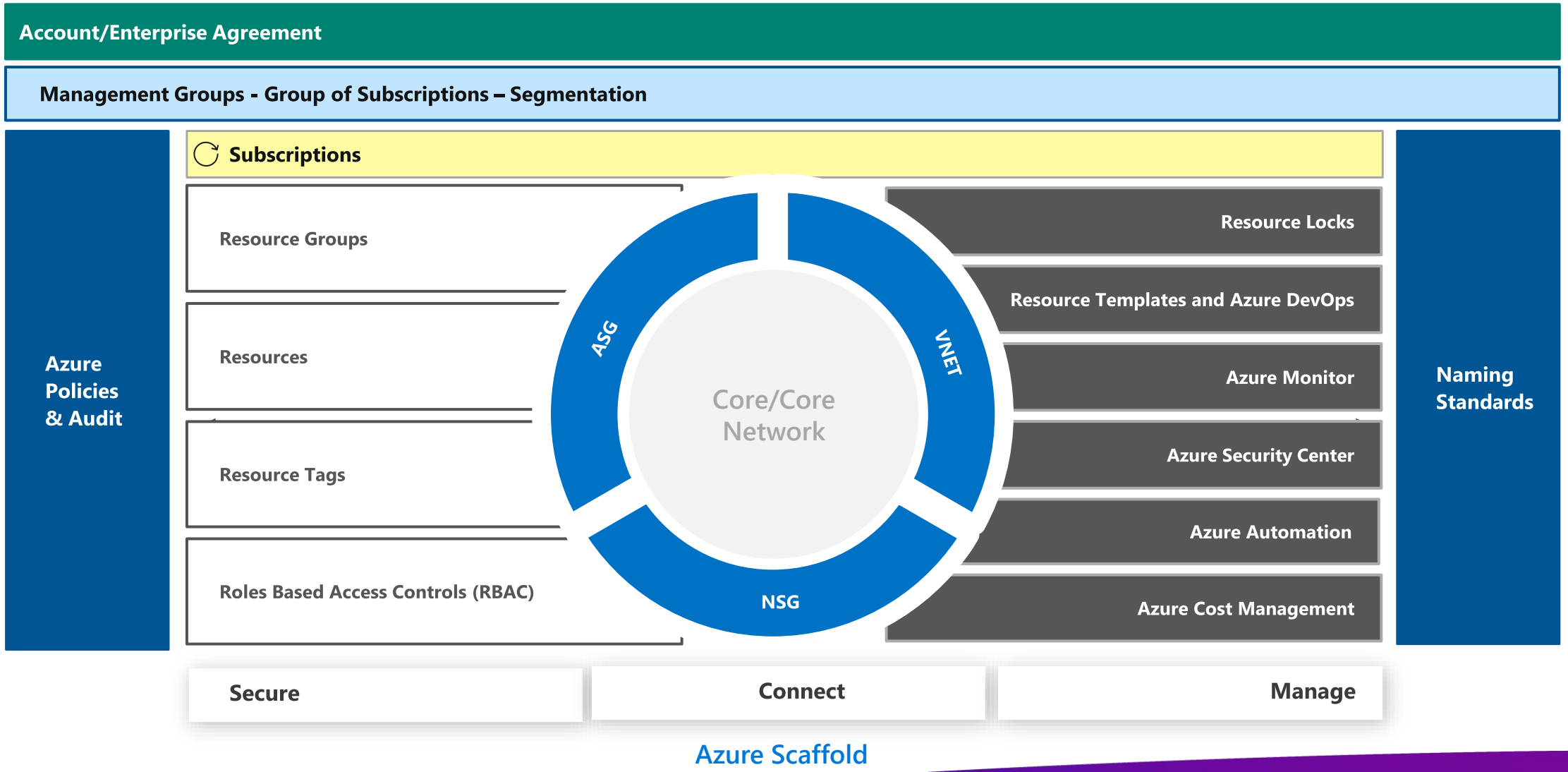
- 安全标准 & 企业规范
- 合理的权限划分
- 合理的资源划分管理
- Azure的管理分配
- 命名规范
- 费用管理
- 运维模式
- …

规划-实施-检查-改进（Plan-Do-Check-Adapt）

Microsoft

Azure云端治理的框架

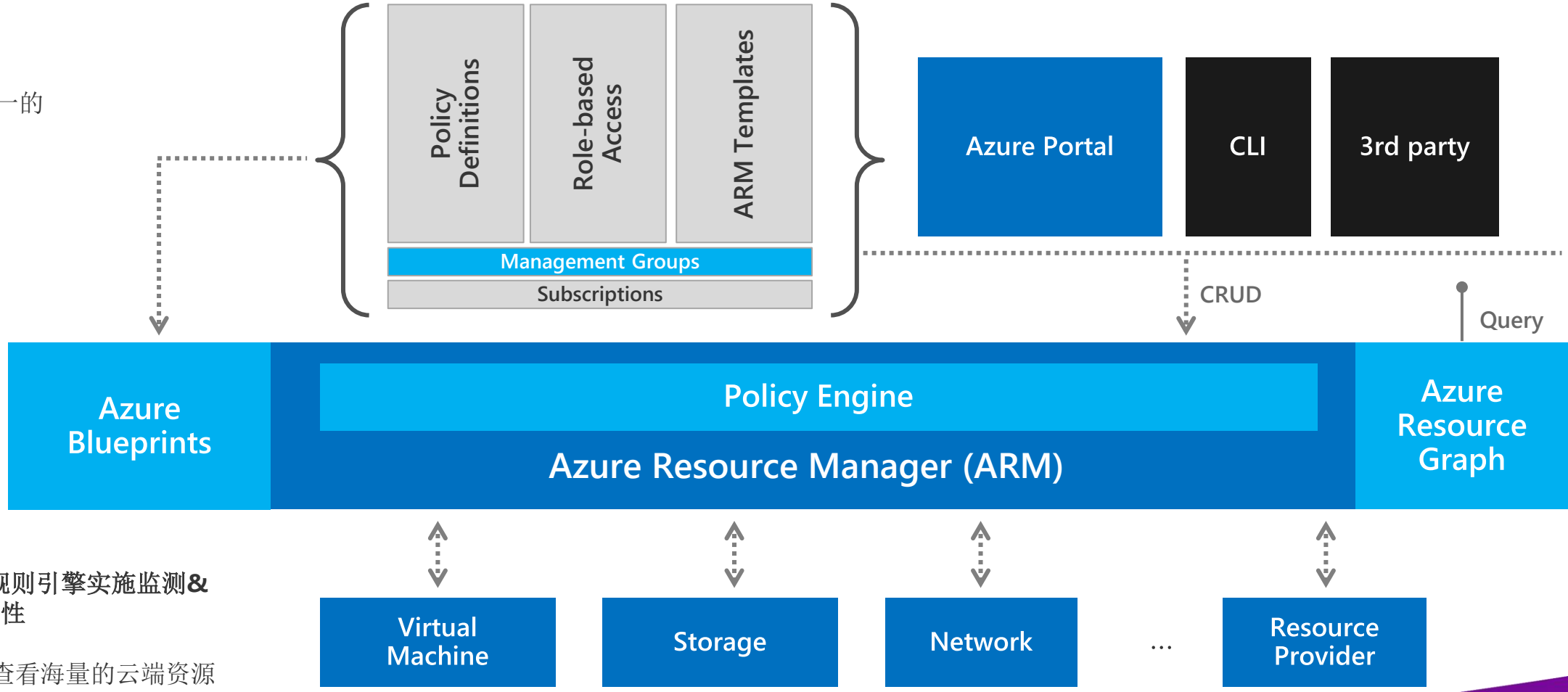
Azure 资源组织框架



Azure Scaffold

Azure 资源管理框架

1. **环境标准化：**通过统一的部署&更新云端资源



2. **规范化控制：**通过规则引擎实施监测&审核环境中资源的规范性

3. **资源可见性**: 清晰的查看海量的云端资源

规则引擎 – Azure Policy

Security	Regulatory Compliance	Tags	Resource standardization	Cost
Azure Security Center	NIST SP 800-53 R4	Require specified tag	Allowed/ not allowed RP	Allowed VM SKUs
Guest Config baselines	ISO 27001:2013	Add or replace a tag	Allowed locations	Allowed Storage SKUs
Key Vault certificate	CIS	Inherit a tag from the RG	Naming convention	
NSG rules	PCI v3.2.1:2018	Append a tag	Back up VMs	
AKS & AKS Engine	FedRAMP Moderate		Allowed images for AKS	
RBAC role assignment	Canada Federal PBMM			
	SWIFT CSP-CSCF v2020			
	UK Official and UK NHS			
	IRS 1075			

规范化的命名 & 适当的标签分类

规范化的命名能够帮助您快速的定位云端资源，并能够更好的结合工具，如：日志查询工具，脚本工具等，进行管理

适当的标签分类，是与规范化的命名紧密联系在一起的。通过标签，资源可以更好的被定制化的区分

General

Entity	Scope	Length	Casing	Valid Characters	Suggested Pattern	Example
Resource Group	Subscription	1-90	Case insensitive	Alphanumeric, underscore, parentheses, hyphen, period (except at end), and Unicode characters that match the regex documented here.	`<service short name>-<environment>-rg`	`profx-prod-rg`

Compute

Entity	Scope	Length	Casing	Valid Characters	Suggested Pattern	Example
Virtual Machine	Resource Group	1-15 (Windows), 1-64 (Linux)	Case insensitive	Alphanumeric and hyphen	`<name>-<role>-vm<number>`	`profx-sql-vm1`
Function App	Global	1-60	Case insensitive	Alphanumeric and hyphen	`<name>-func`	`calcprofit-func`

Microsoft

云端治理之安全&身份管理

安全是云端管理的第一要务

Identity & access management

- Azure Active Directory
- Multi-Factor Authentication
- Role Based Access Control
- Azure Active Directory (Identity Protection)

Data protection

- Encryption (Disks, Storage, SQL)
- Azure Key Vault
- Confidential Computing

Network security

- VNET, VPN, NSG
- Application Gateway (WAF), Azure Firewall
- DDoS Protection Standard
- ExpressRoute

Threat protection

- Azure Security Center
- Microsoft Antimalware for Azure

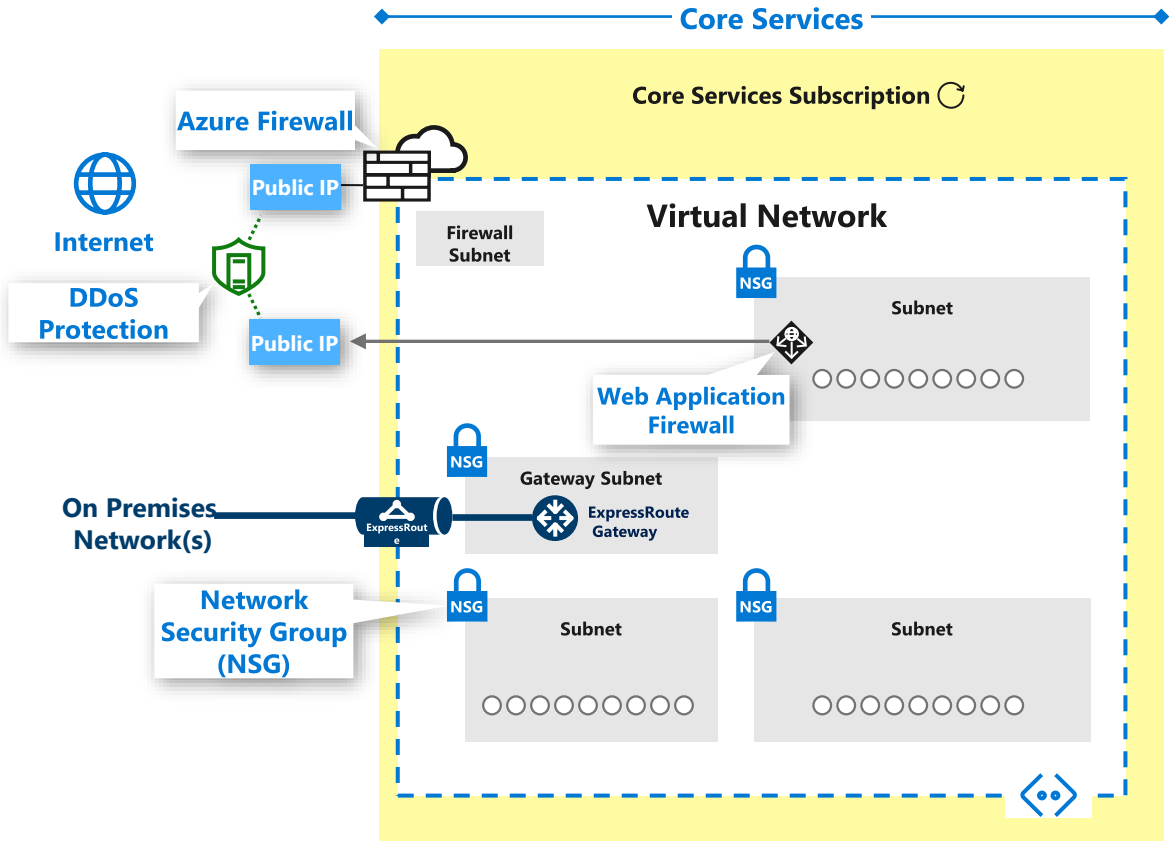
Security management

- Azure Security Center
- Azure Log Analytics

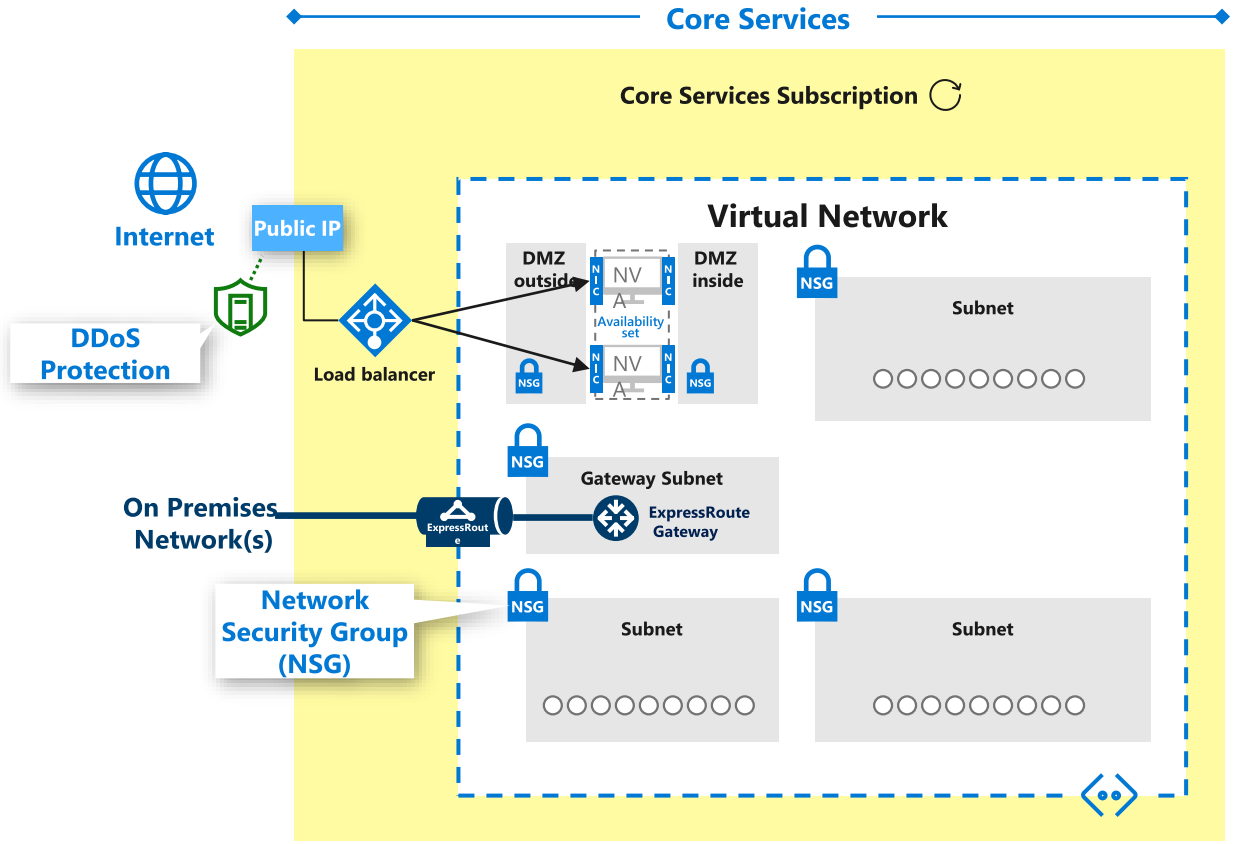
+ Partner Solutions

网络架构的设计

With native controls



With network virtual appliance(s)



https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/shared-services

数据保护

VIRTUAL MACHINES – WINDOWS & LINUX

AZURE DISK ENCRYPTION - <BitLocker [Windows], DM-Crypt [Linux]>
PARTNER VOLUME ENCRYPTION - <CloudLink SecureVM, SafeNet ProtectV, etc.>

SQL SERVER (VM), AZURE SQL DATABASE & AZURE SQL DATA WAREHOUSE

TDE (TRANSPARENT DATA ENCRYPTION) - <SQL Server, Azure SQL Database or Azure SQL Dara Warehouse>
CLE (CELL LEVEL ENCRYPTION) - <SQL Server or Azure SQL Database>
SQL SERVER ENCRYPTED BACKUPS
ALWAYS ENCRYPTED - <SQL Server or Azure SQL Database>

AZURE COSMOS DB

AZURE COSMOS DB

AZURE DATA LAKE

AZURE DATA LAKE – Always enabled if selected (key management scheme choice)

STOCKAGE AZURE

APPLICATION LEVEL ENCRYPTION - <Client-side encryption>
AZURE STORAGE SERVICE ENCRYPTION (Blobs, Files, Managed Disks)

AZURE HDINSIGHT

AZURE HDINSIGHT - <Leverage Azure Storage Service Encryption>

AZURE BACKUP SERVICE

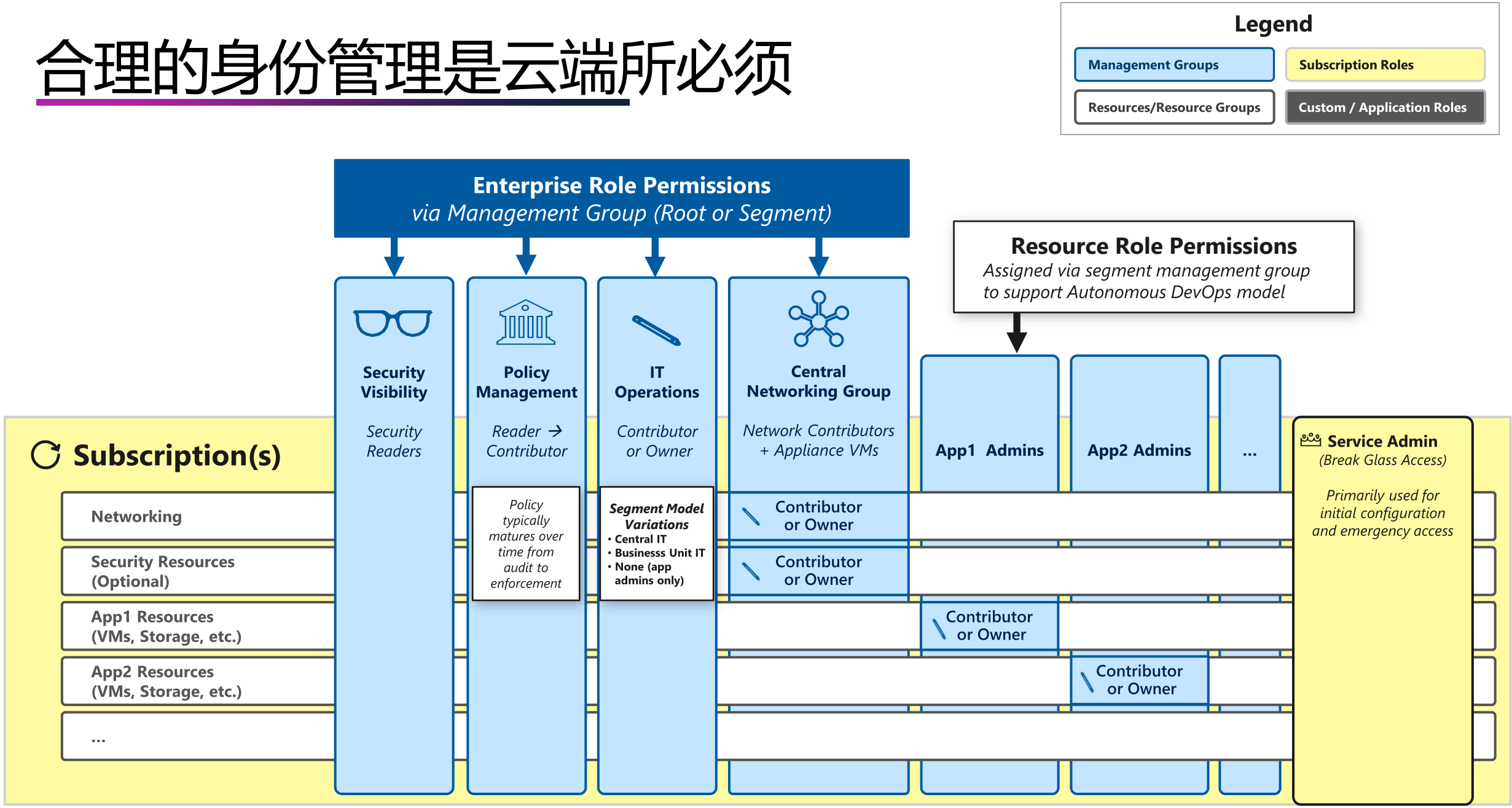
AZURE BACKUP SERVICE - <Leverage Azure Disk Encryption>

KEY MANAGEMENT INTERFACES

AZURE KEY VAULT
<Keys and Secrets controlled by customers in their key vault>

AUTHENTICATION TO KEY VAULT
<Authentication to Key Vault is using Azure AD>

合理的身份管理是云端所必须



Microsoft

云端治理之部署加速

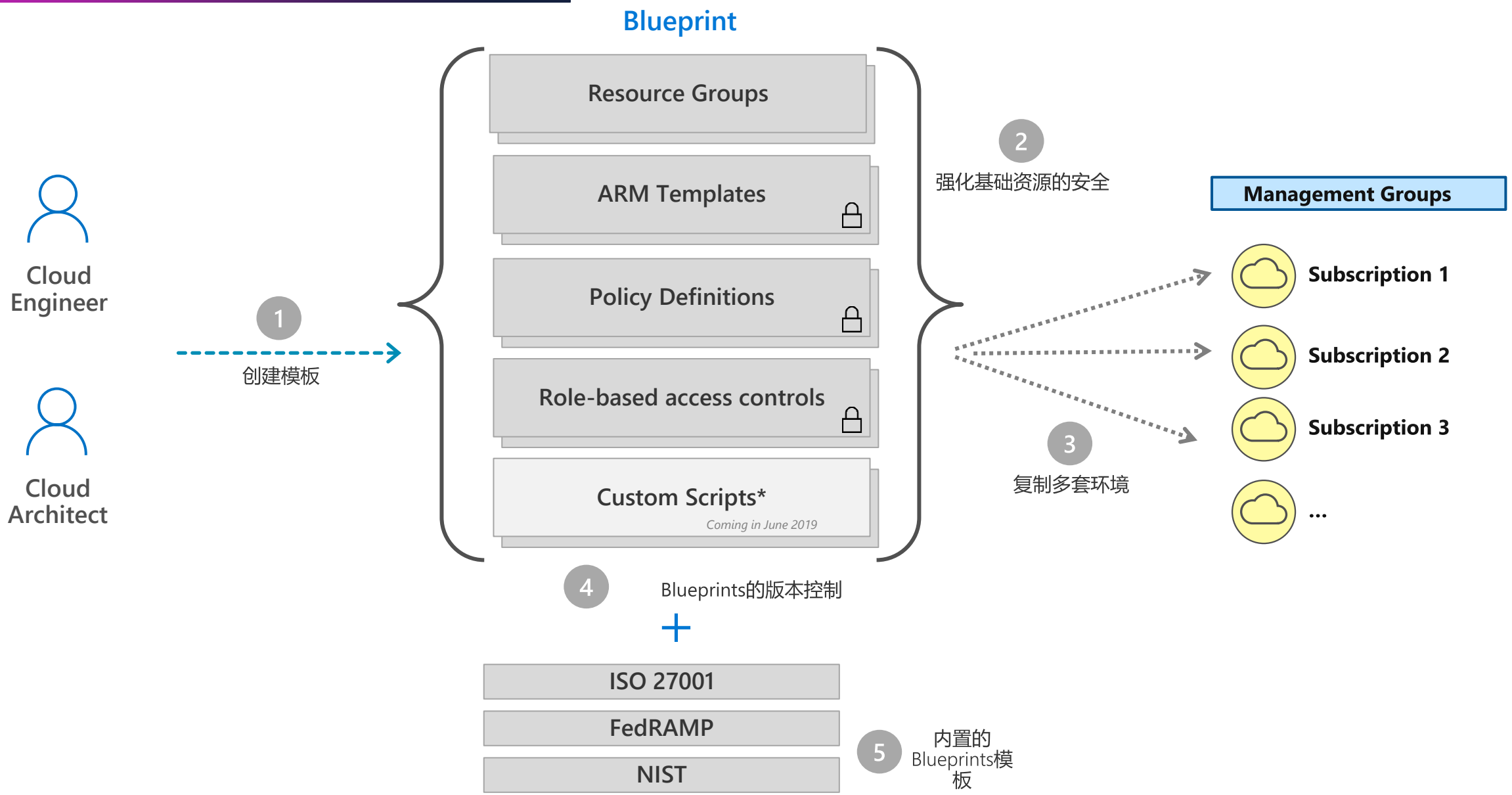
资源部署管理

选择合适的工具，规范合适的流程，来部署、管理云端资源

云端资源的部署管理，包含了资源的创建、更新以及相关配置的变更等. 在标准化流程约束下，既可以手动完成相关操作，也可以采用现代化、自动化的方式，如：DevOps 来完成

云端环境管理自动化的能力，是衡量云服务提供商成熟度的一个重要标准

Azure Blueprints

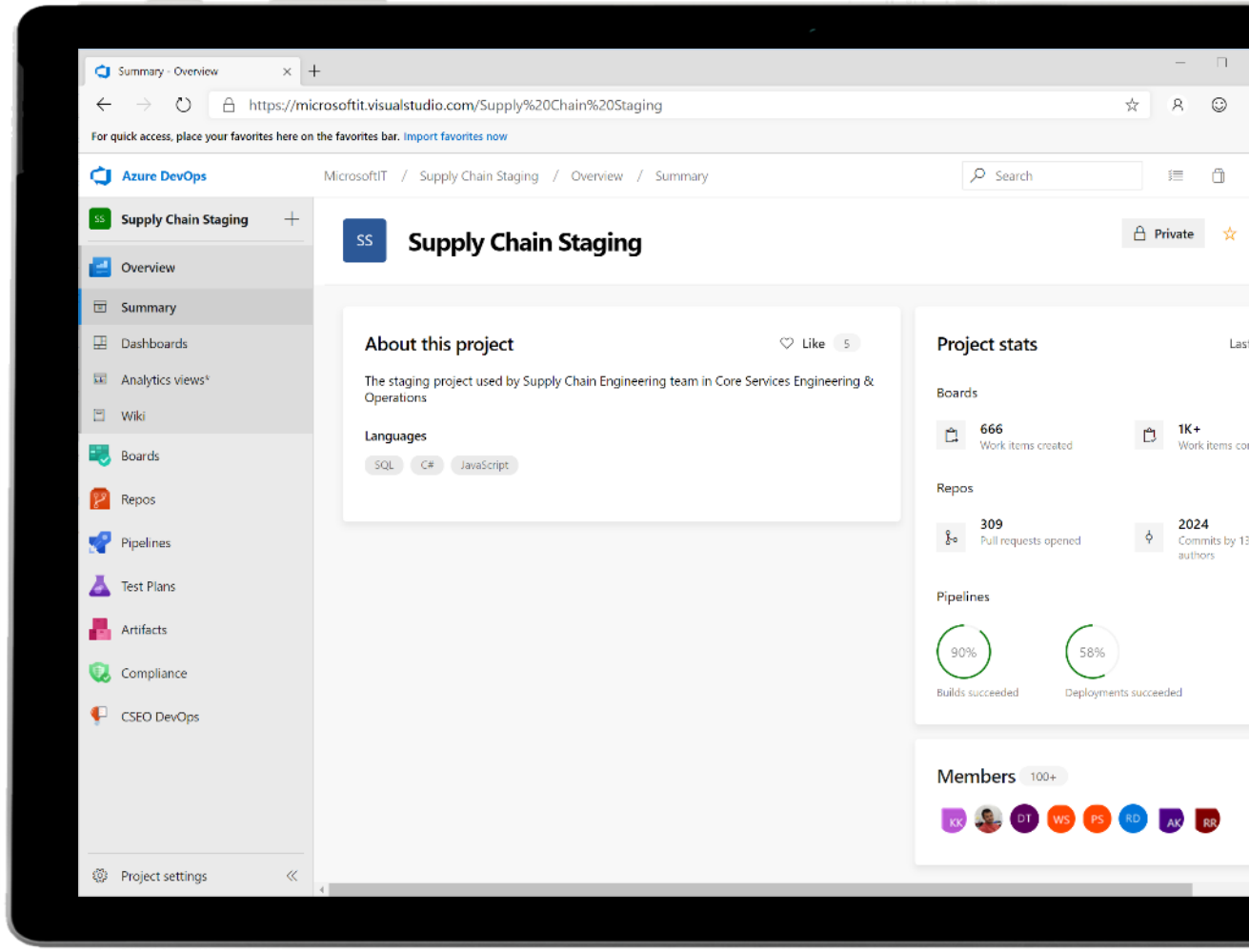


Azure DevOps

选择Azure DevOps中的一个或多个组件，开始构建规范化&自动化的部署流程

核心组件

- **Azure Boards**
- **Azure Pipelines**
- **Azure Repos**
- **Azure Test Plans**
- **Azure Artifacts**
- **Extensions marketplace**



https://docs.microsoft.com/en-us/azure/devops/index?view=azure-devops

Microsoft

云端治理之资源一致性

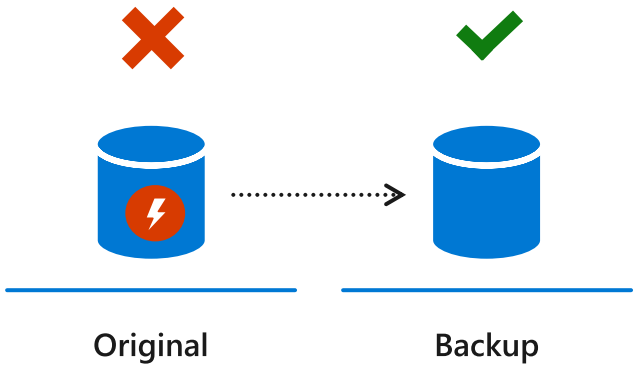
资源一致性的三个方面

资源一致性涉及了包括资源监控在内的多个方面，确保云端资源的管理团队能够及时了解云端资源的

- 可用性 – 系统预期的可用性，SLA
- 可见性 – 云端资源的数字化清单
- 可优化性 – 确保云端资源合理的利用率

https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/resource-consistency/

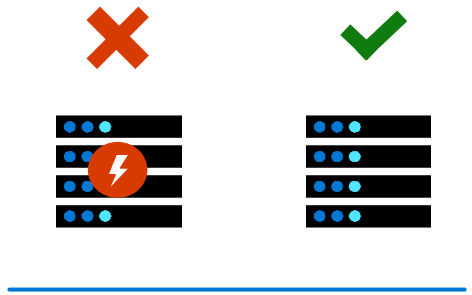
采取合适的架构设计 – 确保应用的稳定



Backup

当资源遭到破坏，备份可以快速帮助你恢复

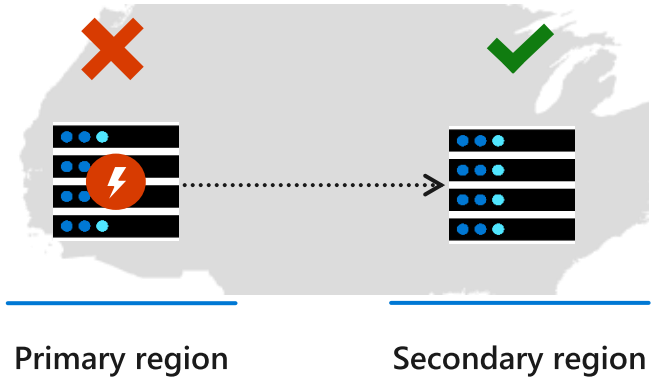
Azure Backup



High availability

当应用或基础架构损坏，高可用设计能够帮助你快速切换，最大限度减少对前端业务的影响

Availability Sets, Zones and Region Pairs

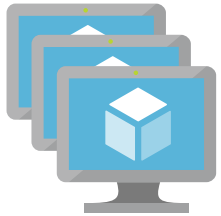
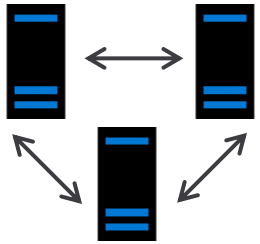
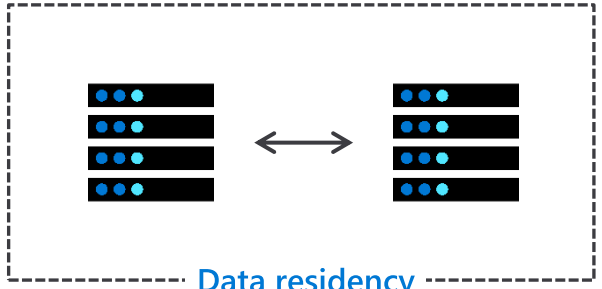


Disaster recovery

当主站出现灾难性损坏，备用站点可以尽快上线，确保业务连续性

Azure Site Recovery

Azure中的高可用选择

Industry-only	High availability SLA		Disaster recovery
VM SLA 99.9%	**VM SLA** 99.95%	**VM SLA** 99.99%	**Regions** 54
			
Single VM Protection with Premium Storage	**Availability sets** Protection against failures within datacenters	**Availability zones** Protection from entire datacenter failures	**Site Recovery & Region pairs** Protection from disaster with Data Residency compliance

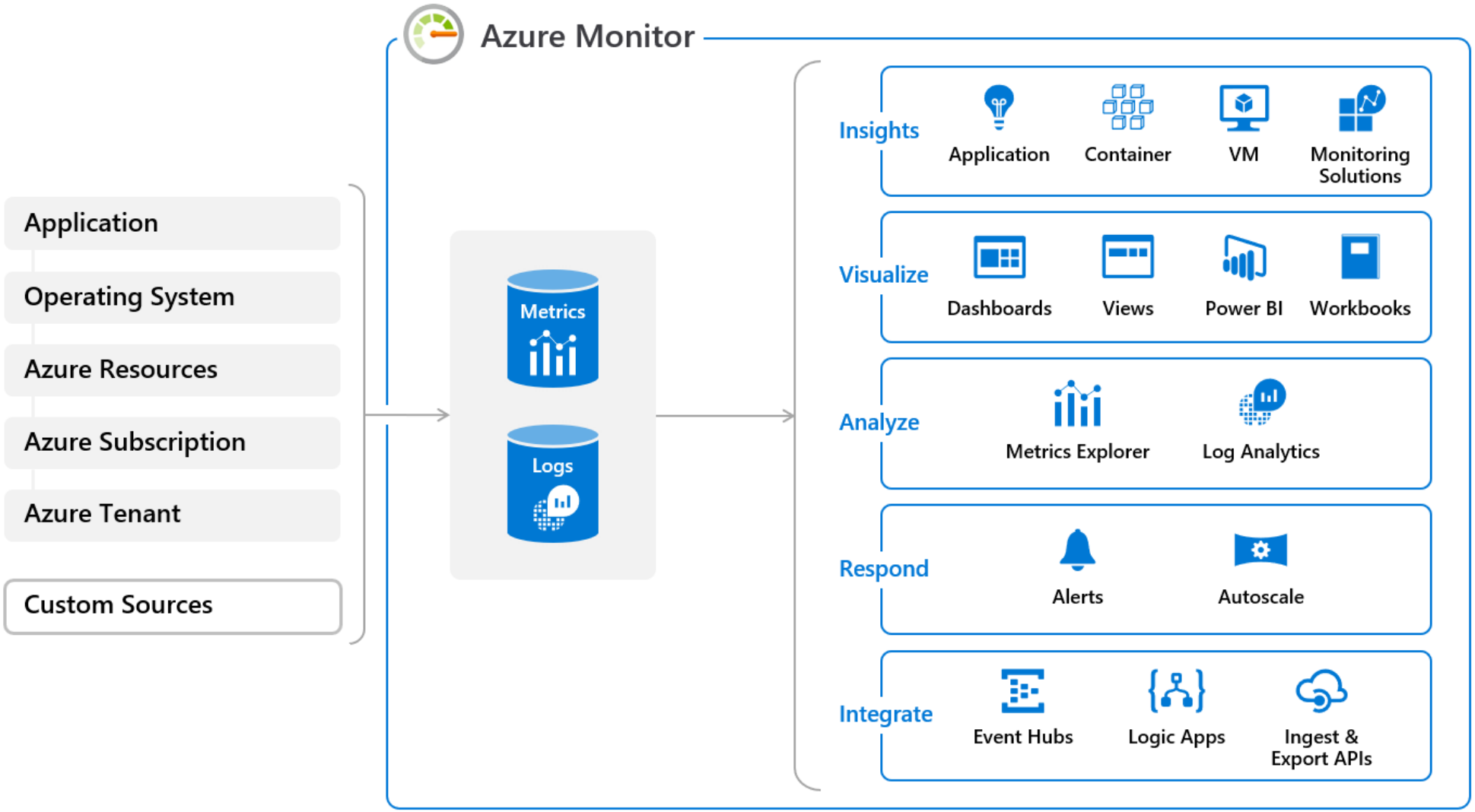
AZs available across US, Europe and Asia… more regions coming soon

Azure 监控中心

提供统一的监控体验，多维度、智能化的监控云端环境&资源

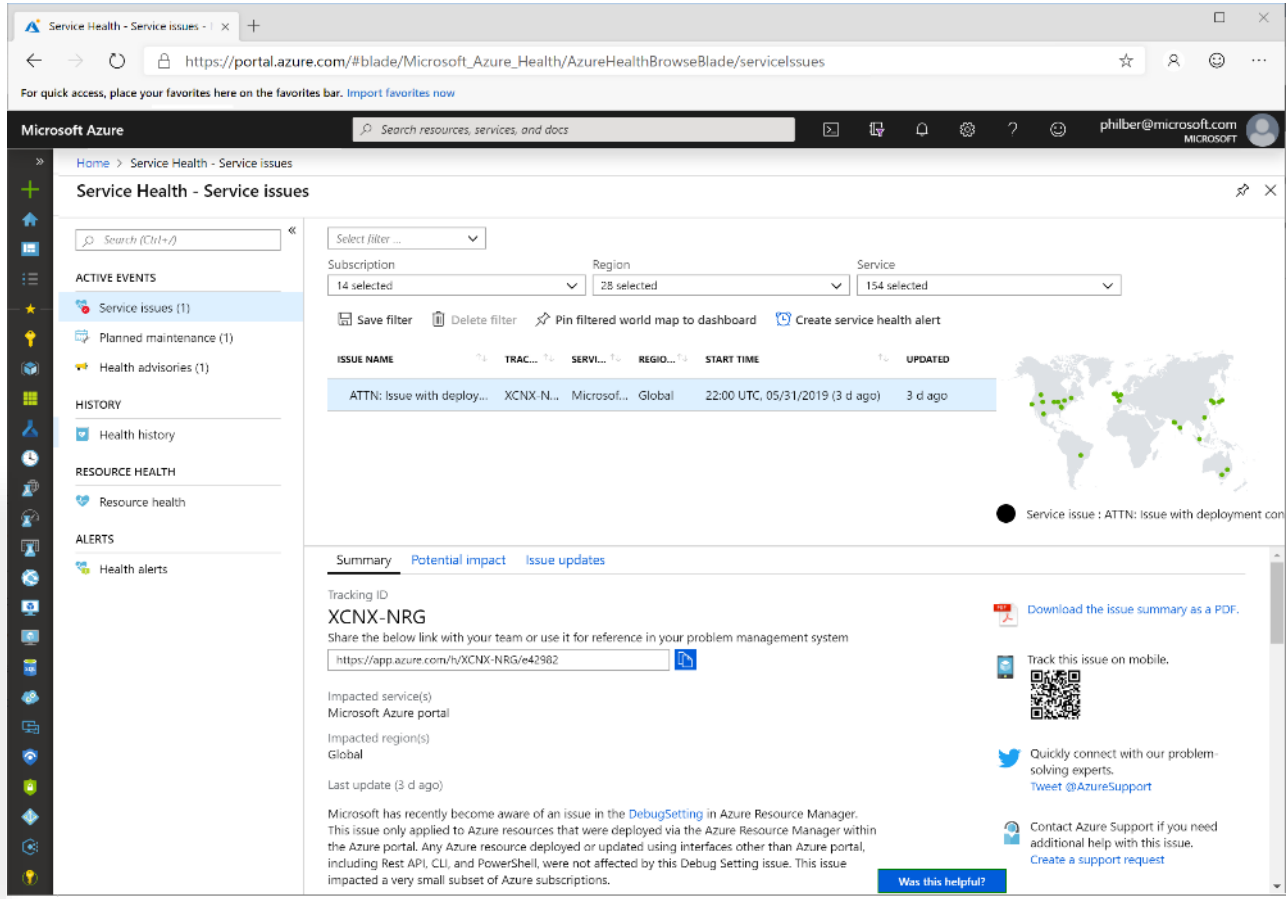
Key capabilities

- **Unified**
- **Integrated**
- **Intelligent**
- **Interoperable**



平台健康中心 – Azure Service Health

及时了解平台服务的健康状况，出现平台问题第一时间收到通知，并及时跟进处理状态



Types of health events

- **Service issues**
- **Planned maintenance**
- **Health advisories**
- **Health history**

云端资源的可见性 – Azure Resource Graph

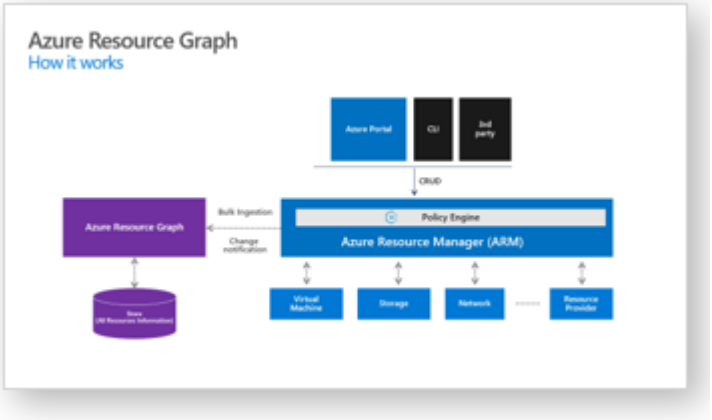
Resource Graph 能够针对云端海量资源实现快速的查询，并提供可视化见解；利用 KUSTO 查询语言，云管理团队可以很方便的上手使用

Key features

- **Explore**
- **Query & analyze**
- **Assess impact**
- **Change History**

Examples

- ✓ 计算不同种类资源数量
- ✓ 根据OS&区域统计虚拟机的数量
- ✓ 列出所有公共IP地址
- ✓ 根据标签列出相应的资源清单
- ✓ 查看所有涉及数据的资源

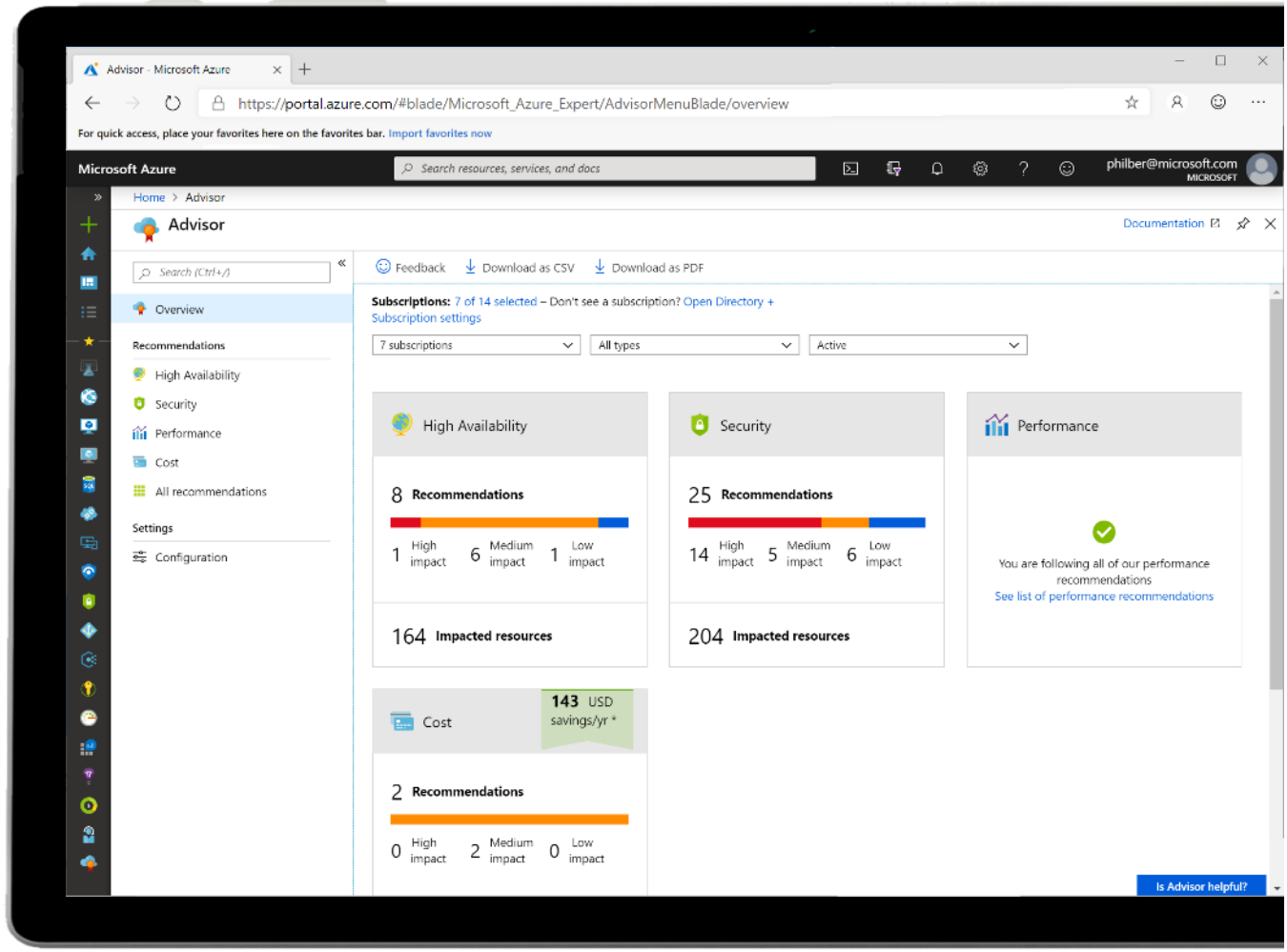


云端资源可优化性 – Azure Advisor

针对云端资源提供持续的优化建议，例如：虚拟机的CPU利用率，建议购买RI，或建议更改的型号等

可提供优化建议的四个方面

- **high availability**
- **Performance**
- **Security**
- **Cost**



Microsoft

云端治理之花费管理

持续的云端费用优化

明确云端花费管理的职责，包括费用明细、权限管理及资源的合理标记

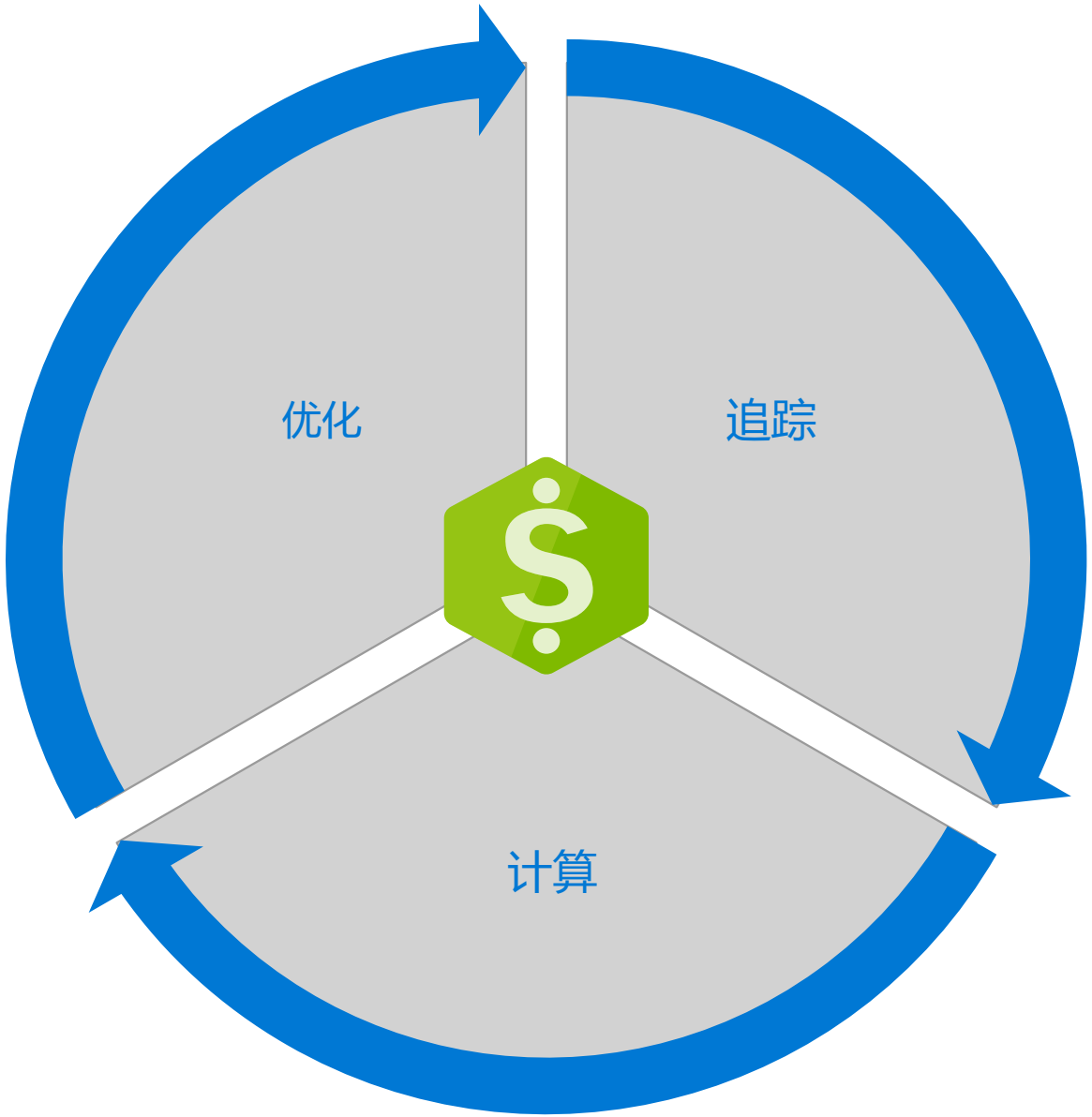
Management teams

明确目标： 预算 & 超支告警

Finance teams

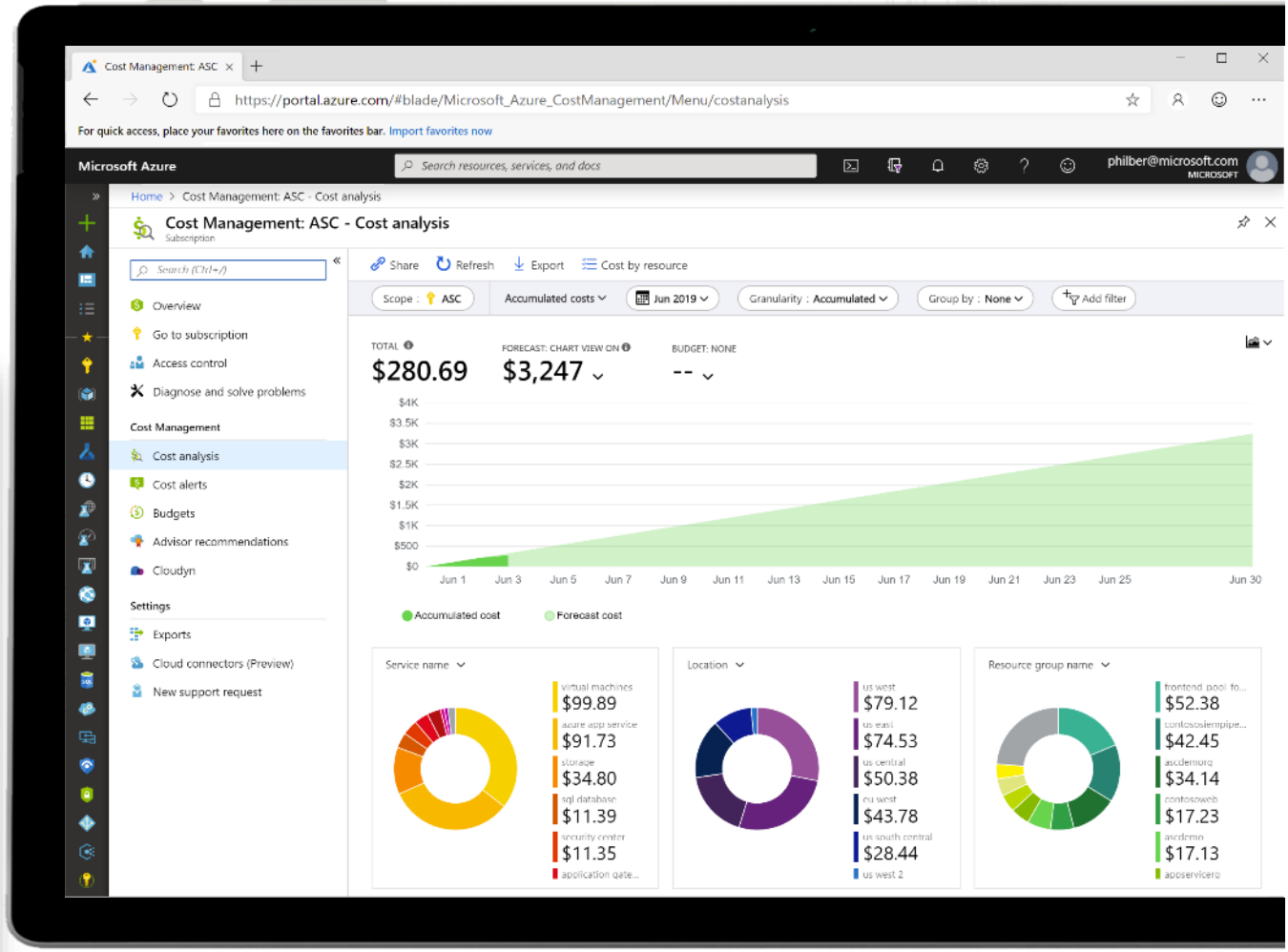
清晰的查看各Team的花费，并定期进行审核优化

App teams



费用管理利器 – Azure Cost Management

实时查看云端花费，未来30天花费预期，花费的区域分布，资源分布等，清晰的管控云端费用



Key features

- **Monitor Cloud spend**
- **Drive organizational accountability**
- **Optimize cloud efficiency**
- **Cross-cloud support (in preview)**

Microsoft

The End & 开启云端治理

云端治理 & 云端采用的相关资料

Microsoft Cloud Adoption Framework for Azure

https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/journeys/overview

Governance in the Microsoft Cloud Adoption Framework for Azure

https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/

Decision guide in the Microsoft Cloud Adoption Framework for Azure

https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/decision-guides/

Azure Governance Docs (Policy, Resource Graph, Blueprints)

http://aka.ms/governancedocs

Azure enterprise scaffold: Prescriptive subscription governance

https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/appendix/azure-scaffold

Azure Virtual Datacenter and the Enterprise Control Plane

https://docs.microsoft.com/en-us/azure/architecture/vdc/

Microsoft

扫码下载讲师PPT

更多精彩尽在【微软市场活动】