Designing a Highly Secured, Hybrid, Multi-Cloud Infrastructure for an Enterprise

A Precise Software Solutions Presentation:

Ben Duan, Chief Technology Officer

Steven Kahn, Engineering Lead

June 26, 2019

PRECISE
Agility. Performance. Innovation.

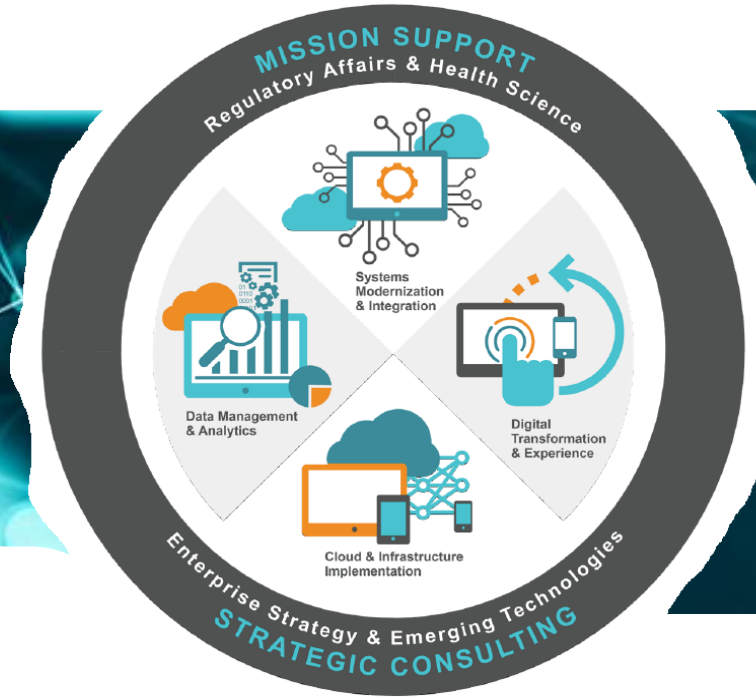
Please visit us at www.precise-soft.com

CLOUD EXPO

About Precise Software Solutions – Rockville, MD

ABOUT PRECISE

Precise Software Solutions, Inc. (Precise) is a nimble and fast-growing SBA 8(a) certified small business focusing on strategy and IT consulting services to public sector customers. We are proud of our strong reputation for overcoming obstacles and delivering innovative, quality work with measurable results. For detail information, please visit us at www.precise-soft.com



CMMI DEV/3 SM
Exp. 2021-05-23 / Appraisal #31079

Washington Technology FAST50

CEO report 2018 WINNER Velocity Growth AWARDS

Washington Business Journal 2018 TOP 30 SMALL TECHNOLOGY COMPANIES Precise Software Solutions, Inc. #28

Inc. 5000 #938 2018

Senate Small Business of the Week
2019. 05

aws partner network
Standard Consulting Partner

ORACLE Gold Partner

PRECISE
Agility. Performance. Innovation.

CLOUD EXPO

Agenda

Multi-Cloud, Hybrid Cloud Adoption

Why Multi-Cloud

- ✓ Leverage best of breed vendor solutions
- ✓ Benefit from competing vendor pricing
- ✓ Avoid vendor lock-in
- ✓ Mitigate risks

Why Hybrid Cloud

- ✓ Integration with on-premises systems
- ✓ Cloud as disaster recovery site
- ✓ Data Center extension to the cloud
- ✓ Centralized on-premises Data Center and cloud management
- ✓ Centralized security management
- ✓ ATO requirements

PRECISE
Agility. Performance. Innovation.

A Hybrid, Multi Cloud Case Study

Customer to implement IaaS in both AWS and Azure to:

- ✓ Give business options to choose cloud service providers (CSPs)
- ✓ ATO AWS to high to host mission critical systems
- ✓ Utilize enterprise license agreement with Microsoft to simplify cloud acquisition process
- ✓ Leverage enterprise license discount with Microsoft to reduce windows VM cost

Customer to implement hybrid cloud to:

- ✓ Meet cloud-first, Cloud-smart mandate
- ✓ Meet FITARA requirement to improve enterprise virtualization ratio
- ✓ Extend on-premises data centers to the cloud
- ✓ Implement next-generate cloud native applications
- ✓ Migrate on-premises systems to the cloud
- ✓ Leverage cloud as DR options
- ✓ Maintain consolidated data center and cloud security and operation management on premises

OUR TASK

- ✓ To design and implement enterprise IaaS in AWS and Azure
- ✓ To achieve AWS to high, Azure to moderate ATO
- ✓ Single pane of glass cloud management on both AWS and Azure

Please visit us at www.precise-soft.com

Design Considerations

Design for Security Compliance

Design for HA, Reliability and Performance

Design for Consistent Cloud Architecture

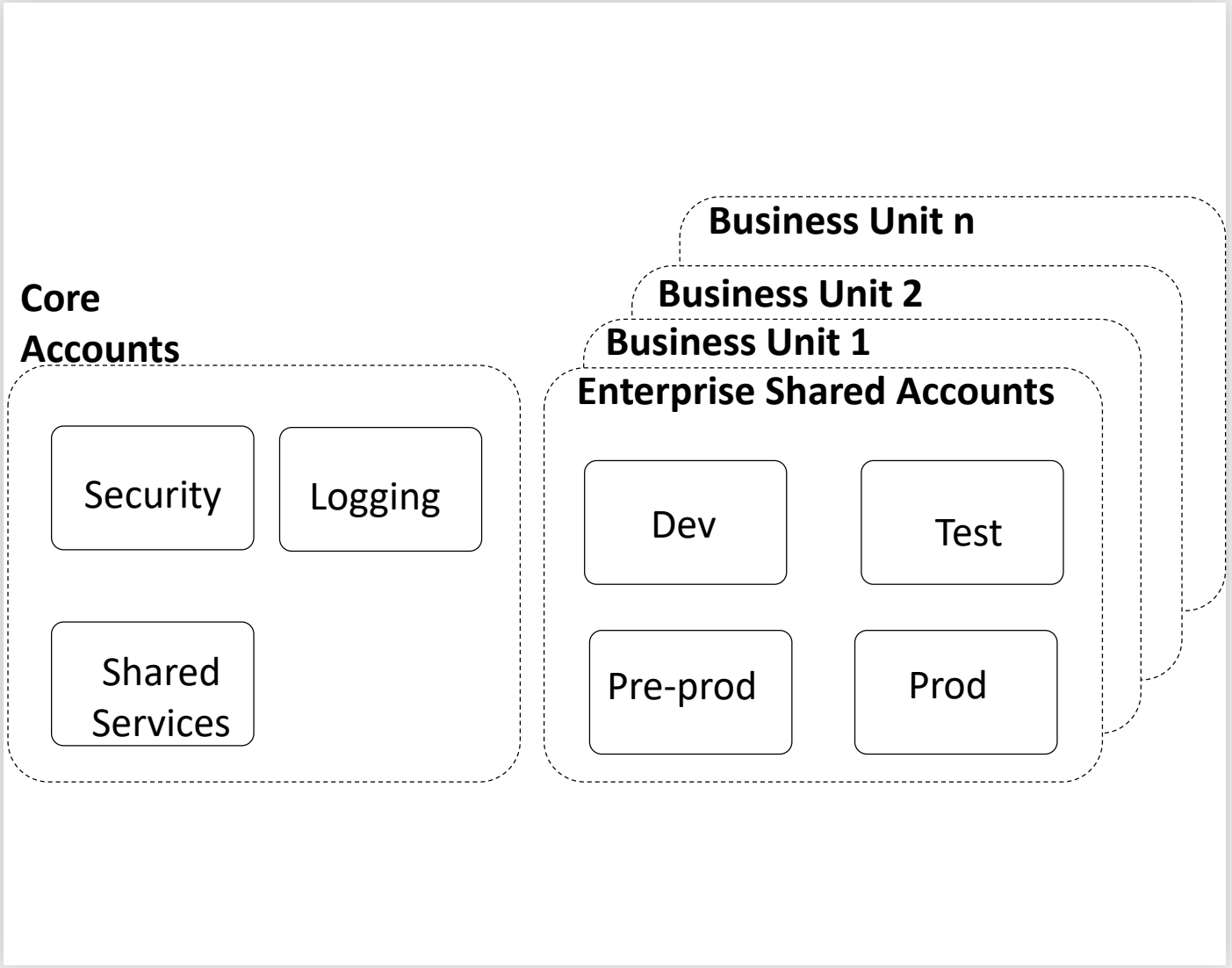
Cloud as Extension of On-premises Data Center

Leverage Existing Customer Best Practices and Tools

Leverage CSP Reference Architectures

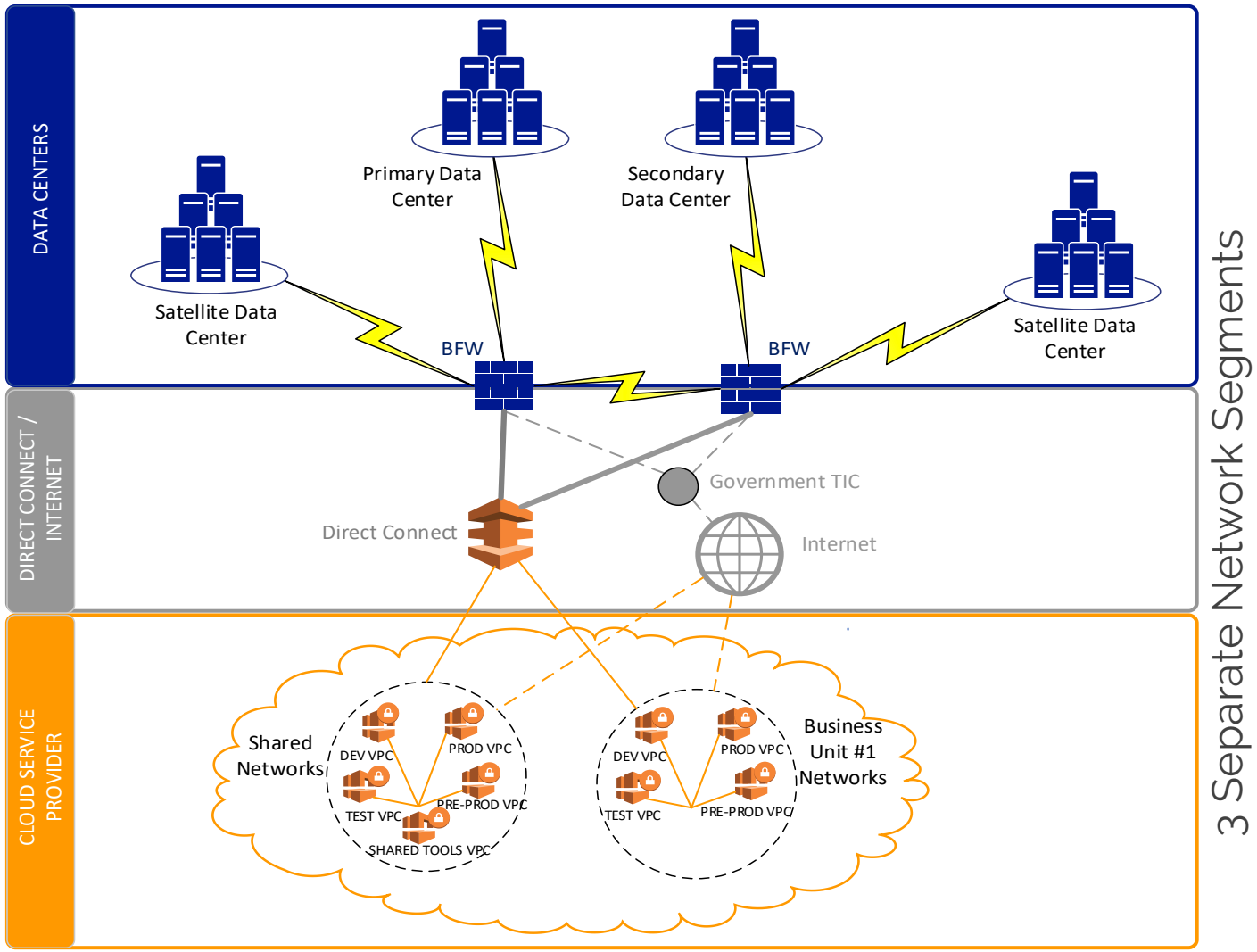
Consistent Management for Multi-cloud

Multi-Account Structure



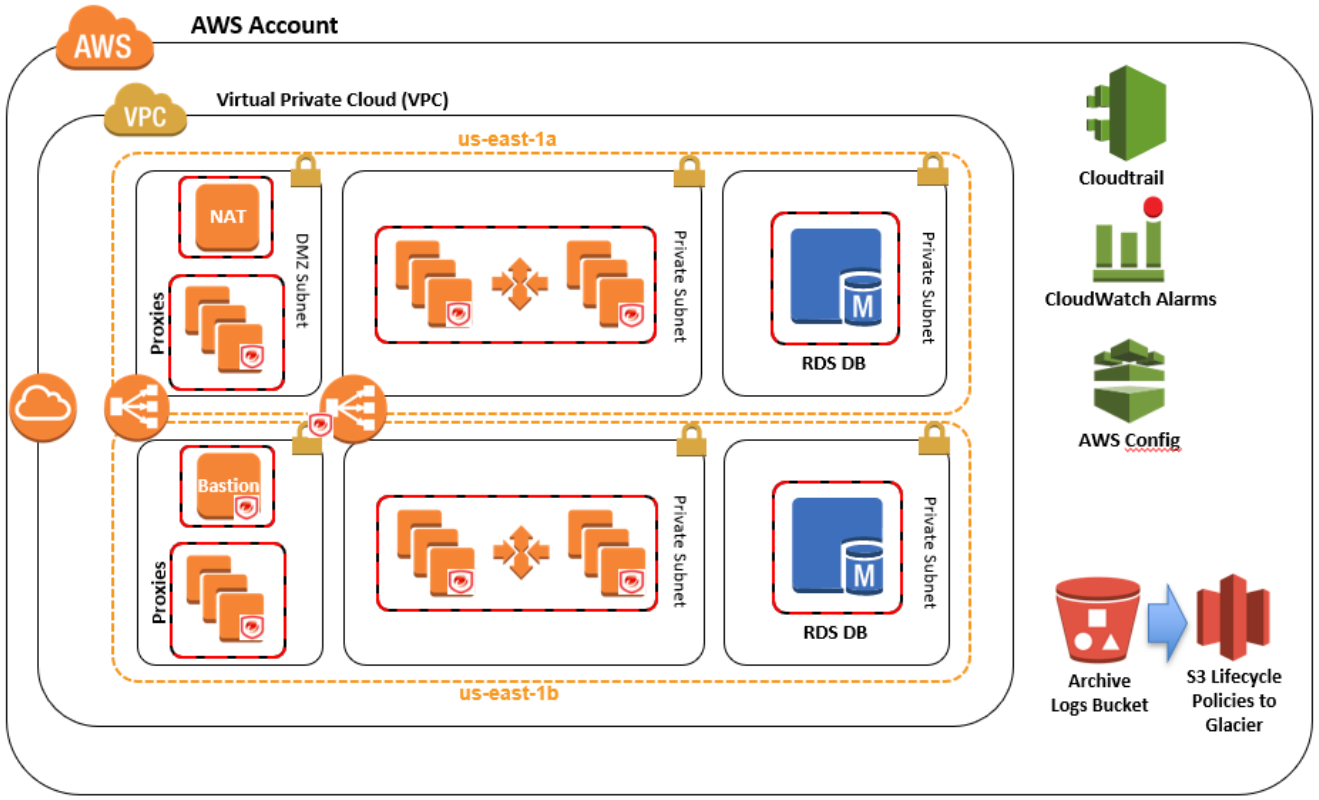
- Core Accounts
  - Logging: Centralized logs
  - Security: Config rules, security tools
  - Shared services: AD, deployment tools, patching, monitoring, anti-virus.
- Business Unit Accounts
  - Enterprise Shared Accounts: For business units that wish to share account and environments. Include Dev, Test, Pre-prod, Prod.
  - Business Unit Accounts: For business wish to have separated accounts and environments

Hybrid Cloud High Level Architecture



- Shared Cloud Networks for Shared Tools and other Shared Environments
- Optional Business Unit Networks for Optimal Use of Resources
- Flexible Hybrid Architecture
  - Improved Bandwidth
  - Better Traffic Isolation
  - Increased Stability
  - Cost Separation
  - Direct Connect or Internet (TIC)
- Local Shared Tools to Reduce Network Latency and Egress Charges

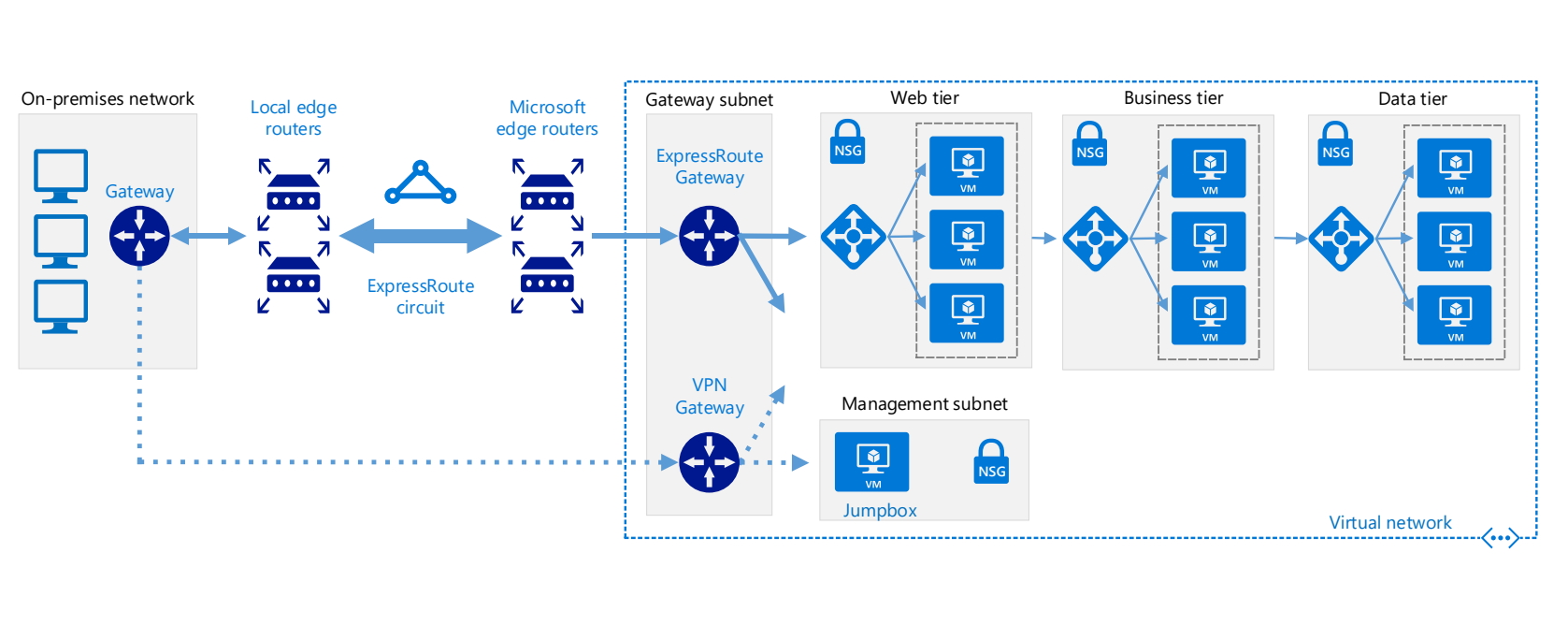
VPC Network Reference Architecture



Source: AWS - Standardized Architecture for NIST-based Assurance Frameworks on AWS

- Adopting AWS Best Practices for Hybrid Cloud
- Separate subnets for Web, App and DB tiers
- Inter-subnet traffic managed and inspected by Gateway devices
- High Availability Across Multiple Availability Zones
- Full deployment of AWS CloudTrail, CloudWatch, and AWS Config
- Audit logs captured in centralized S3 logs bucket
- Database HA?

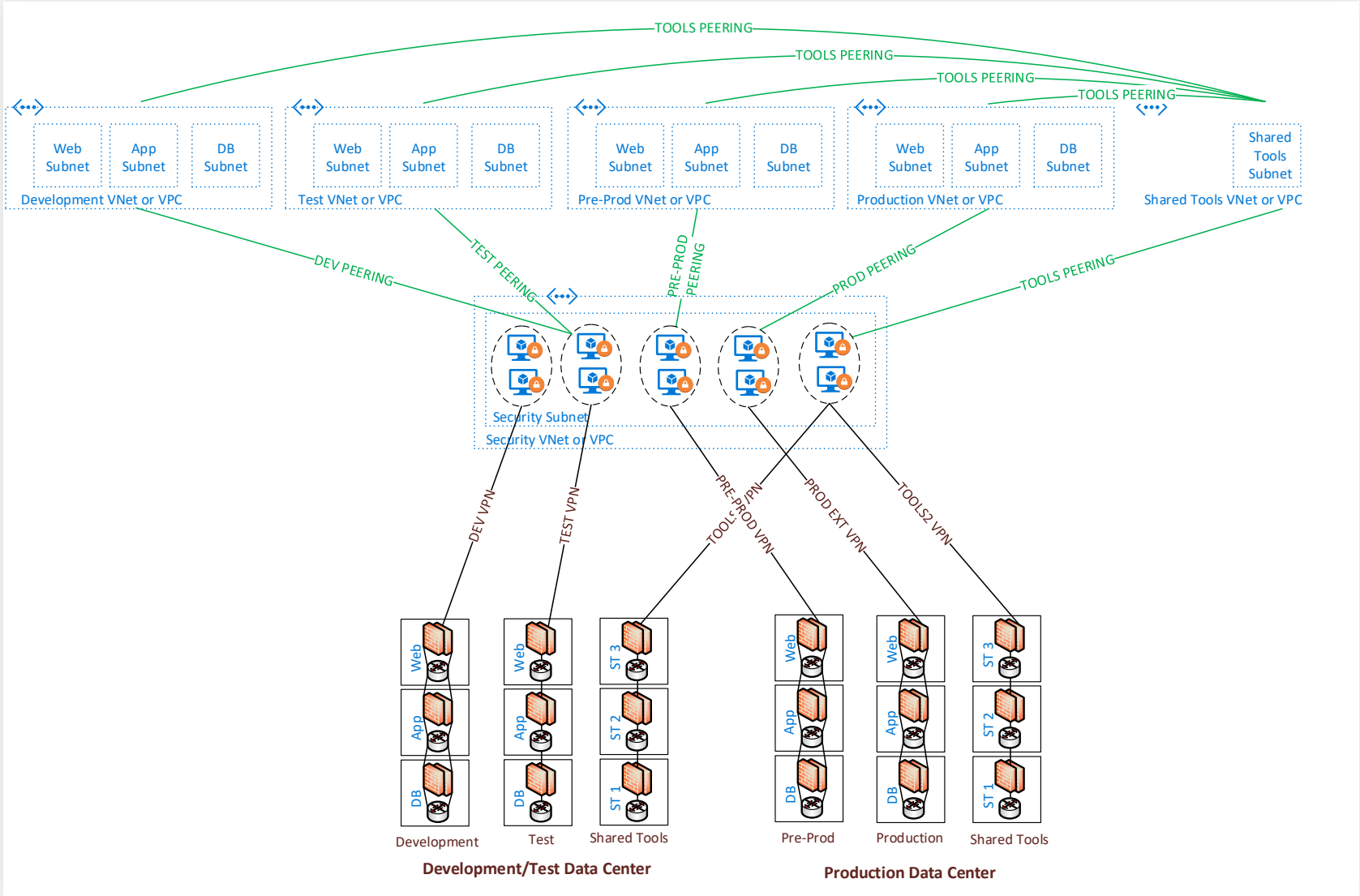
VNet Network Reference Architecture



- Best Practices for Hybrid Cloud Implementation
- Separate subnets for Web, App and DB tiers
- Implement Cross-zone Load Balancing to Create Multi-tier highly available applications
- ExpressRoute is Primary Communication to On-Premises; VPN is Secondary

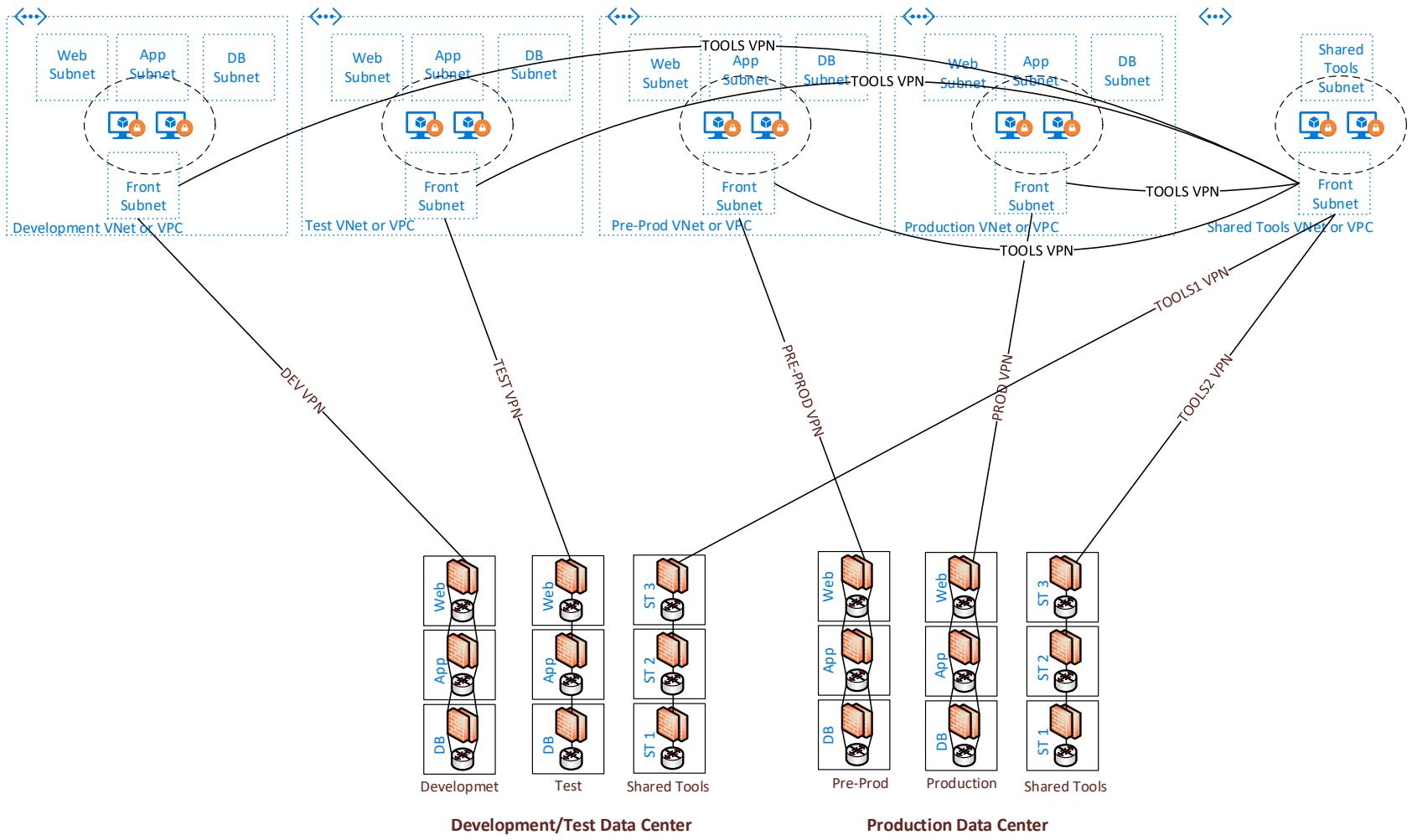
Source: Microsoft – Azure Reference Architecture: Connect an on-premises network to Azure using ExpressRoute with VPN failover

Hybrid Cloud Design Option 1



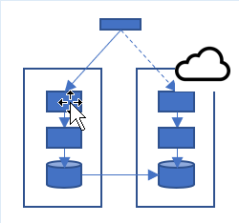
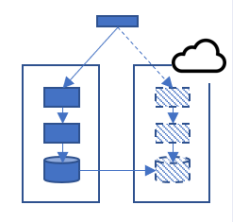
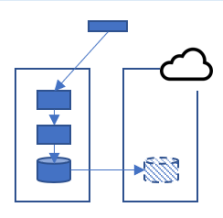
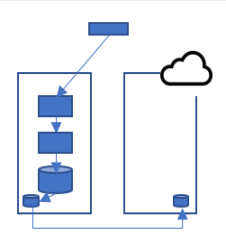
- 3rd Party Virtual Gateways
- Improved Cloud Traffic Management and IDS/IPS capability
- Consistent Security Policy Across Enterprise
- Dedicated Gateways Per Environment
- Cloud Environments extend On-Premises Environments
- Security VPC for North-South Communication

Hybrid Cloud Design Option 2



- More Consistent with On-premises Environment
- Control by On-Premises Security Team
- Routing Controlled by Virtual Gateways
- VPN Communication to Management

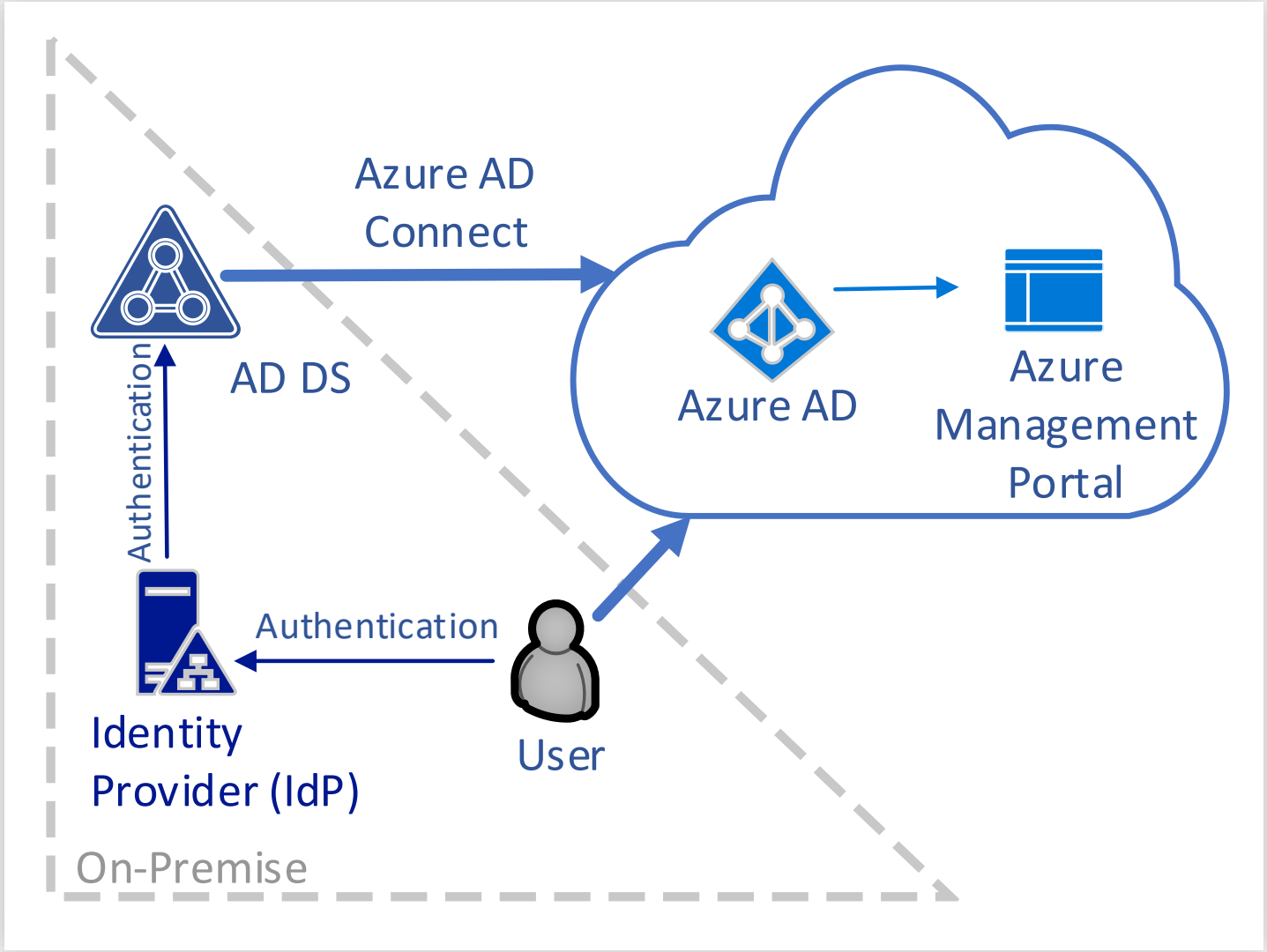
Cloud DR Options

Solution	Description		RTO, RPO	Cost
Hot Standby	Servers at DR site are running 24x7. Data are replicated from primary site to DR site in real time. When disaster happens at primary site, switching global DNS or global load balancer will effectively switch the system to DR site		Low RTO ~ minutes - hours RPO ~ minutes	Very high
Cold Standby	Servers at DR site are shutdown. Data are replicated from primary site to DR site in real time. When disaster happens at primary site, servers at DR site will be brought up, and global DNS or load balancer will switch to point to DR site		Moderate RTO ~ hours - days RPO ~ minutes	High
Replication	No servers at DR site for the system, but data are replicated real time from primary site to DR site. When disaster happens at primary site, servers need to be built at DR site, and connect/mount to the data. Global DNS or load balancer will switch to point to DR site		High RTO ~ days - weeks, RPO ~ minutes - hours	Moderate
Backup	No servers at DR site for the system. No real time data replication. Primary site data are periodically backed up to DR site. When disaster happens at primary site, servers need to be built at DR site, data need to be restored at DR site. Global DNS or load balancer will switch to point to DR site		Very high RTO ~ weeks –months RPO ~ hours-days	Low

Security in Depth

Layers	AWS	Azure
OS Security	Customer approved RHEL and Windows AMIs with timely security patching	
Network security	• 3rd Party Virtual firewall monitor and inspect all inter-subnet traffic • Security groups • Access control lists • Elastic Load Balancers	
Authentication and Access Management	• PIV authentication • Identity Provider identity federation for AWS and Azure Management Portal access • Identity Provider solution for individual VM console access • VDI jump-box	
	• AWS IAM • AWS KMS	• Azure IAM • Azure Key Vault
Centralized Account Management	• Active Directory	
Intrusion Detection and Prevention	• 3rd Party IDS Vendor	
Configuration Management	• 3rd party configuration tools, Ansible, Chef etc.	
	• AWS Config Rules • Lambda scripts • CloudFormation	• Azure Configuration manager • Azure Powershell
Logging and Auditing	• CloudTrail • CloudWatch • AWS Config • Centralized S3 log bucket • SIEM	• Azure Activity Log • SIEM
Data security	• EBS, S3, RDS encryption enforcement by Config Rules	• Azure disk encryption, Azure SQL database encryption
Anti Virus	• End Point Protection Vendor	

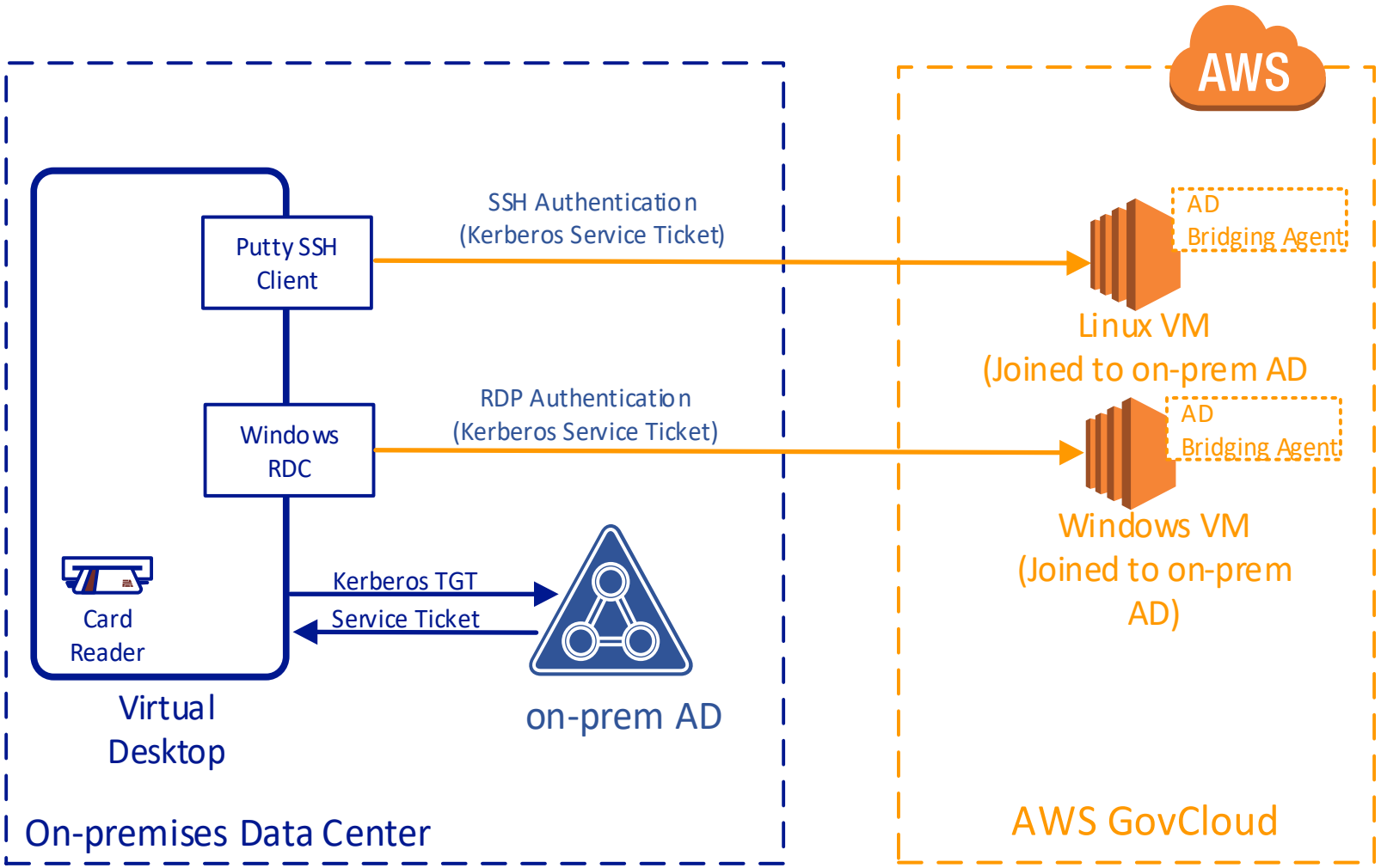
Cloud Resource Authentication



Federation Access Control for Console and Resources

- Implement PIV card for multi-factor authentication
- One unique Account for both on-premises and public clouds
  - One consistent process for add, update, and delete
- Authentication occurs on-premises
- Keep some local accounts as backup

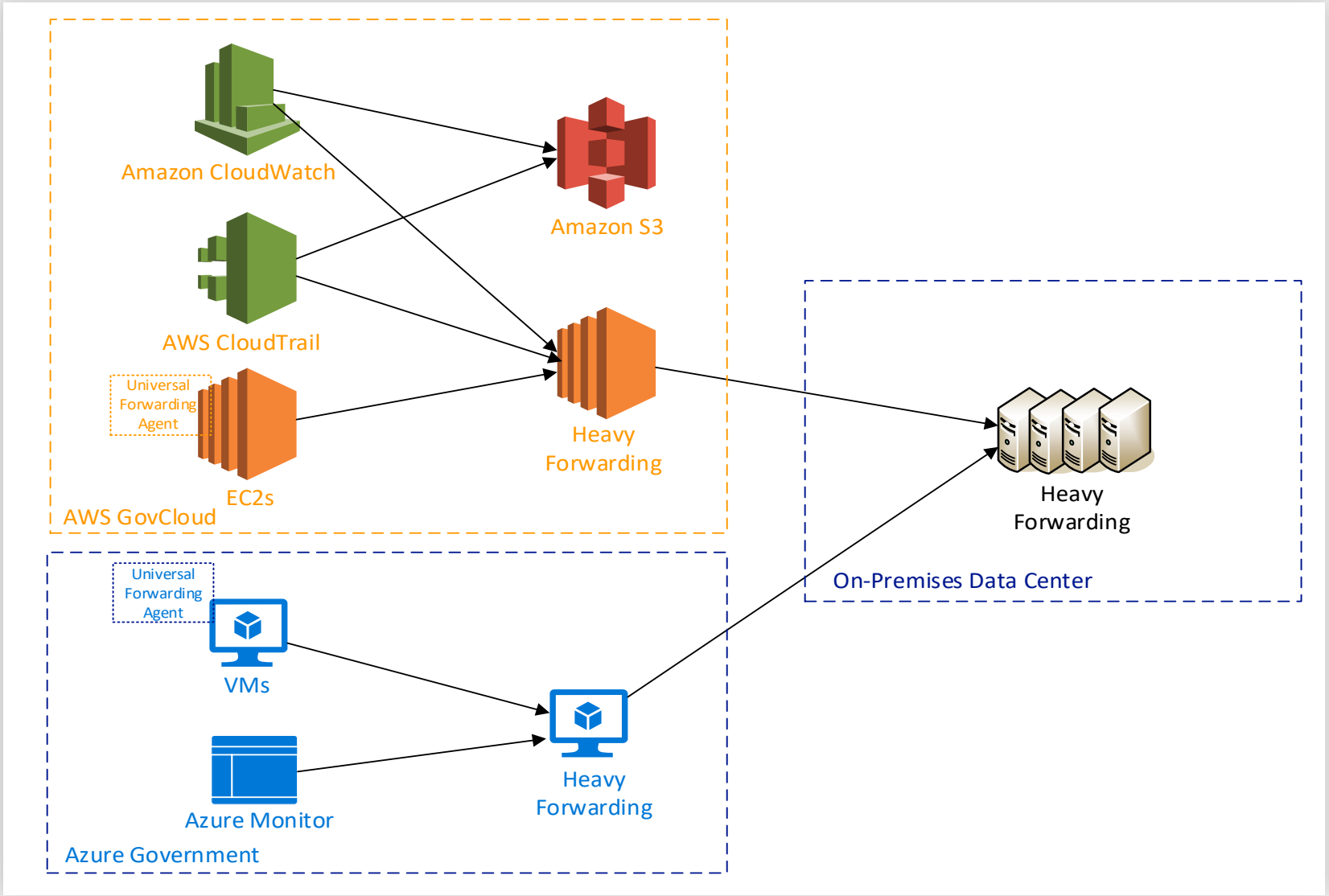
Virtual Machine Authentication



Access Control for Virtual Machines

- Implement PIV card for multi-factor authentication
- Linux domain join to Windows
- One unique Account for both on-premises and public clouds
- One consistent process for add, update and delete
- Consistent with on-premises access to Servers

Central Audit Logging



- Cloud Audit Logs Integrated with on-premises Security Information and Even Management (SIEM)
- Enable your organization to perform log analysis across the enterprise
- Consider the scope of logs sent to on-premises

Miscellaneous Security Processes

Cloud Services vs. On-premises tools

Recommendation: On-premises works for hybrid cloud solution

- Vulnerability Scanning – Golden Images
  - Establish Golden Images Early
  - Scanning locally
  - Integrate Vulnerability Tracking with Existing Process
- Patch Management – Windows, Linux
  - Local Patch Repositories
  - Proxies
- Anti-Virus Protection
  - Local Virus Update Repositories

Compliance – Assess, Authorize (ATO), Monitor

- Federal Risk Authorization Management Program (FedRAMP) - 2011
  - Completed by Cloud Service Providers
  - FedRAMP Marketplace Listing
  - Based on NIST SP 800-53 controls (low, medium, high categories)
- Federal Information Security Management Act (FISMA) – 2002, 2014
  - Completed by Government Agencies
  - Coordinate w/ Security early in the Design Process
  - Based on NIST SP 800-53 controls (low, medium, high categories)
    - Authorize Infrastructure, Services, & Custom Applications
    - **Recommendations**
      - Assess Controls early in the Design Process
      - Divide Controls into Policy and Technical Categories
      - Assess Risk for Controls not met

Design for Compliance – AWS NIST Quick Start

NIST SP 800-53 rev4 Controls									AWS Quick Start Architecture Comments for NIST SP 800-53 Controls			
Family	Control (Major)	Control (Sub-parts)	Title	Description	Priority	Control Baseline: Low	Moderate	High	Addressed By This Quick Start	Category: Influence	Category: Responsibility	AWS Quick Start Security Control Implementation Description
AUDIT AND ACCOUNTABILITY	AU-8	AU-8b	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement]			X	X	Yes	Information Systems	Shared	In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are employed. AWS built-in features of native logging provide time stamps as specified in the ISO 8601 standard. ISO 8601 represents local time (with the location unspecified), as UTC, or as an offset from UTC.
AUDIT AND ACCOUNTABILITY	AU-8 (1)	AU-8 (1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	The information system:			X	X	Yes	Information Systems (Header)	Shared (Header)	See control subpart details below.
AUDIT AND ACCOUNTABILITY	AU-8 (1)	AU-8 (1)(a)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	Compares the internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and			X	X	Yes	Information Systems	Shared	In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are employed, and the initial EC2 instances launched (bastion host, application servers, proxy servers, and EC2-based NAT instances in AWS Regions where Managed NAT Gateways are not yet available) use Amazon Linux AMIs, which have NTP configured by default to sync time with pool.ntp.org servers (these NTP servers are not owned, managed, or guaranteed by AWS. For more information, see http://www.pool.ntp.org/en/) AWS built-in features of native logging use time stamps provided by AWS region internal system clocks that are continuously synchronized
AUDIT AND ACCOUNTABILITY	AU-8 (1)	AU-8 (1)(b)	SYNCHRONIZATION WITH AUTHORITATIVE	Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment:			X	X	Yes	Information Systems	Shared	In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are employed, and the initial EC2 instances launched (bastion host, application servers,

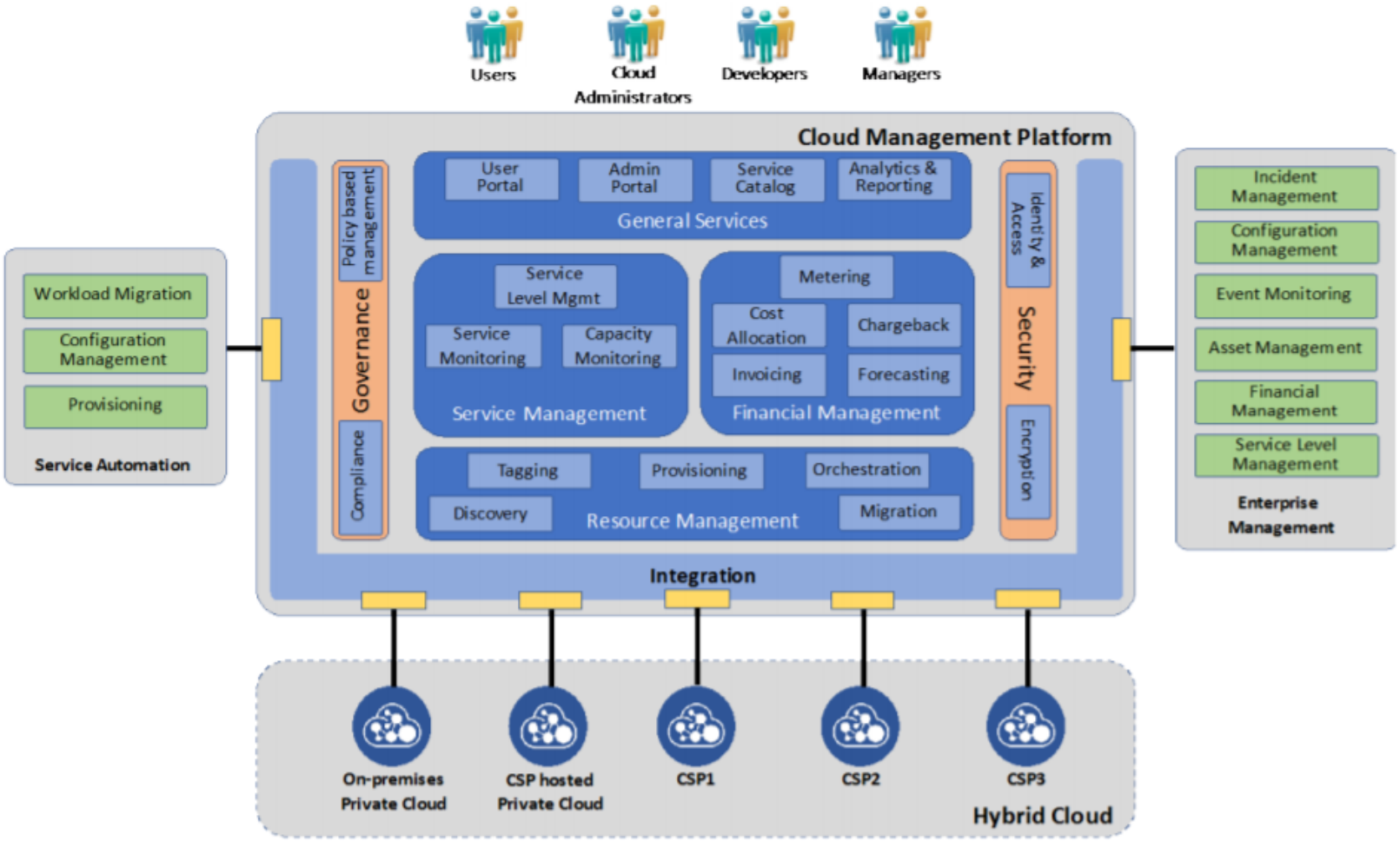
Quick Start provides guidance to meeting NIST SP 800-53 controls!

PRECISE
Agility. Performance. Innovation.

Please visit us at www.precise-soft.com

CLOUD EXPO

Multi-Cloud Management



[Hybrid Cloud Management reference architecture (Cloud Standard Customer Council)]

Cloud Center of Excellence

Innovation

Brings innovative solutions to leverage technology innovations in the Cloud marketplace

Predictability & Decision Making

Provides on demand Cloud analytics covering impact, service levels, monitoring, utilization, costs comparison, compliance and demand forecasting for strategic decision making

Leadership & Capability Development

Provides leadership, management and strategic workforce planning, and critical acquisition, ongoing capability development to meet future demands and innovation

Multi Vendor Management

Concentrates on key vendors for optimal efficiency and cost effectiveness, ROI/ROV management and governance

People: Digital Workforce

Governance

Promotes Cloud rationalization, reference architecture and implementation, standardization across the enterprise.

Operational Efficiency & Agility

Improves Cloud operation efficiency and agility via automation leveraging Infrastructure as Code, DevOps technologies

Solution Delivery Life Cycle Support

Ensures cloud aspects of requirements definition, solution design, architectures, development, testing and implementation and migration are supported

Cloud Center of Excellence Key Focus Areas

Ensuring cloud workload is well-architected to enhance mission effectiveness and reduce mission risks

Cost and operational efficiency

- ✓ Infrastructure as Code, CI/CD pipelines for end-to-end cloud infrastructure provisioning and application deployment

AUTOMATION

Architectures Standards

- ✓ Reference architectures and implementations for typical solutions
- ✓ Standard cloud service catalogs
- ✓ Templates for design, test, infrastructure provisioning, O&M

REFERENCE ARCHITECTURE & IMPLEMENTATION

Cloud adoption

- ✓ Advocate cloud value proposition
- ✓ Assist in the entire EPLC lifecycle of cloud projects
- ✓ Cross functional seminars and knowledge sharing

ACTIVE BUSINESS ENGAGEMENT

Thank You!

www.precise-soft.com

ben.duan@precise-soft.com
steven.kahn@precise-soft.com

1445 Research Blvd. Suite #500
Rockville, MD 20850