BUILDING A STRATEGY FOR PERIODIC OPTIMIZATION OF AZURE ENVIRONMENTS

SECURITY, COST, PERFORMANCE, AND SUPPORT

Aman Sharma
Principal Consultant

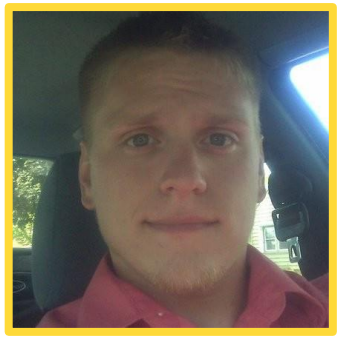
Eric Bogenschuetz
Azure Architect

ABOUT THE PRESENTERS

Aman Sharma
Principal Architect
Lunavi

Aman Sharma is a five-time Microsoft MVP in Azure and has presented at various events including Microsoft TechReady, Virtual Tech Day, TechEd, User Groups, etc. He is a Principal Consultant at Lunavi and a former employee of Microsoft. He has designed and built enterprise cloud solutions. In his day-to-day work, he focuses on building solutions around different services within Microsoft Azure.

Blog: www.HarvestingClouds.com
YouTube Channel: HarvestingClouds
Twitter: @20aman



Eric Bogenschuetz
Azure Architect
Eversource Energy

Eric Bogenschuetz is the lead Azure Cloud Domain Architect at Eversource Energy, the largest energy provider in New England. With over 10 years of IT experience, Eric designs and operates enterprise-scale Azure environments including architecture, dev/test, automation, monitoring, and daily management.

Blog: https://NavigatingClouds.wordpress.com/

Agenda

1. INTRODUCTION
2. BUILDING A STRATEGY
3. SECURITY OPTIMIZATIONS
4. COST & PERFORMANCE OPTIMIZATIONS
5. SUPPORT & MANAGEMENT OPTIMIZATIONS
6. NEXT STEPS

INTRODUCTION

OPTIMIZATIONS ARE KEY

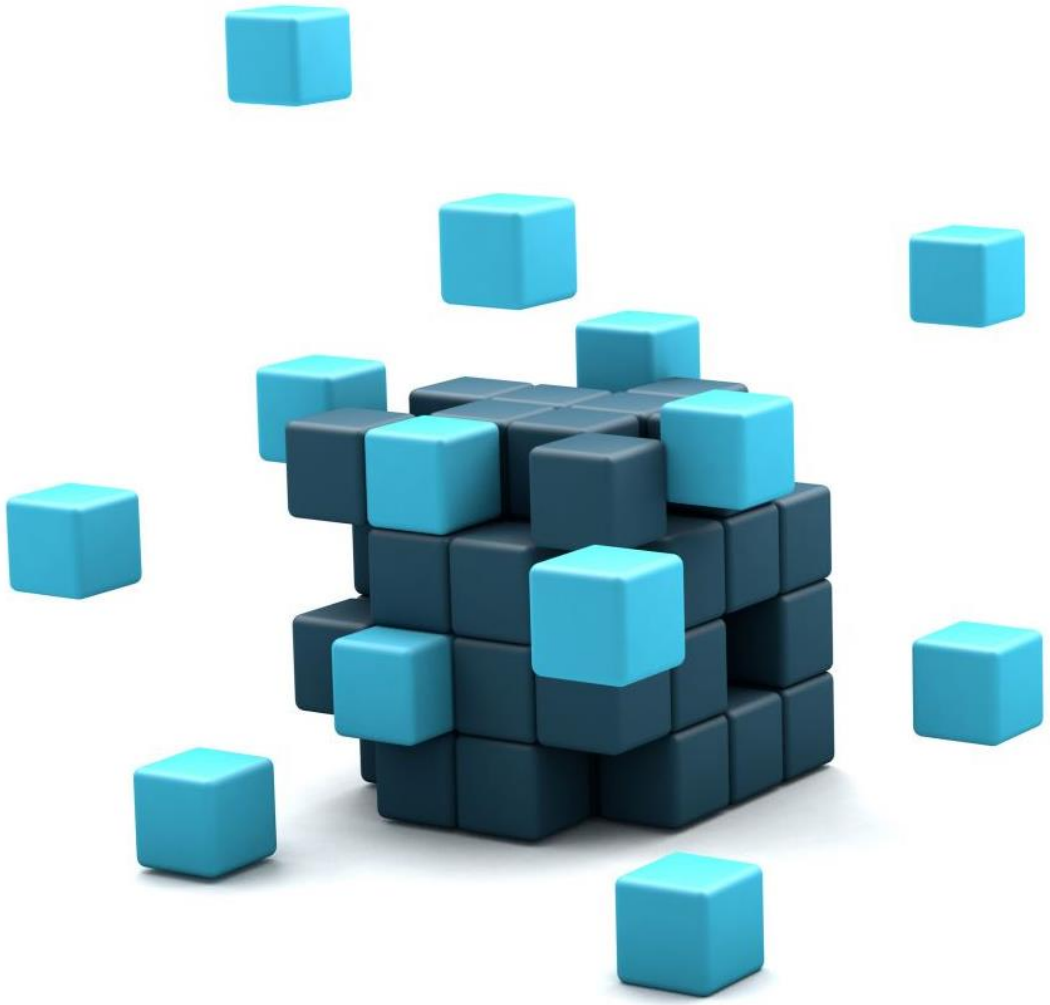
- Cost creep
- Smallest security vulnerability can compromise the whole environment
- Unmanaged systems or standards can become support nightmares in the long run
  - Measure twice, cut once

CONTINUOUS CLOUD EVOLUTION

FRAMEWORK IS CRITICAL TO SUCCESS

Foundation for Cloud Adoption Framework	
Ensuring the cloud migration pays off	
Support plans drive cloud utilization	
Regular reviews	Quarterly and annual reviews
Well-defined support structure	RACI matrix in place

BUILDING BLOCKS FOR A STRATEGY



BUILDING BLOCKS

- **Automation and Scripts**
- **Periodic Reports and Email Digests**
- **Automated Alerts and Action Groups**
- **Solidified RACI Matrix**
- **Identifying what to optimize**
  - Security
  - Cost
  - Performance
  - Support/Maintenance

DECIDING ON FREQUENCY

- Annual
- Bi-annual
- Quarterly
- Monthly

SETUP REVIEW PROCESS

1. The Report and Email Digest get’s generated.
2. Review
3. Remediate
4. Add policies/automation to avoid deviations in future

SECURITY OPTIMIZATIONS

SECURITY AT THE IDENTITY LEVEL

PIM – Privileged Identity Management

MFA – Multi-Factor Authentication

Conditional Access

Azure AD access reviews

RBAC - Role-Based Access Control reviews

- Memberships/Access
- Managed Identities
- App Registrations

Custom Role usage

- Principle of least privilege

STRENGTHEN SECURITY

Microsoft Defender for Cloud

- JIT – Just-in-time VM Access
- Adaptive controls
- Network Map and Dependency

Microsoft Sentinel

Any public IP should be justified via business requirements

Review NSG configurations

Enable soft delete

OTHER SECURITY OPTIMIZATIONS

Key Vault	Policies	Expirations	Disable
Key Vault Usage • No credentials stored anywhere else	Leverage Azure Policies • Policy exemption should always have expirations	Leverage Cert and Secret Expirations	Disable Anonymous Access • Storage accounts • Restricting via policy

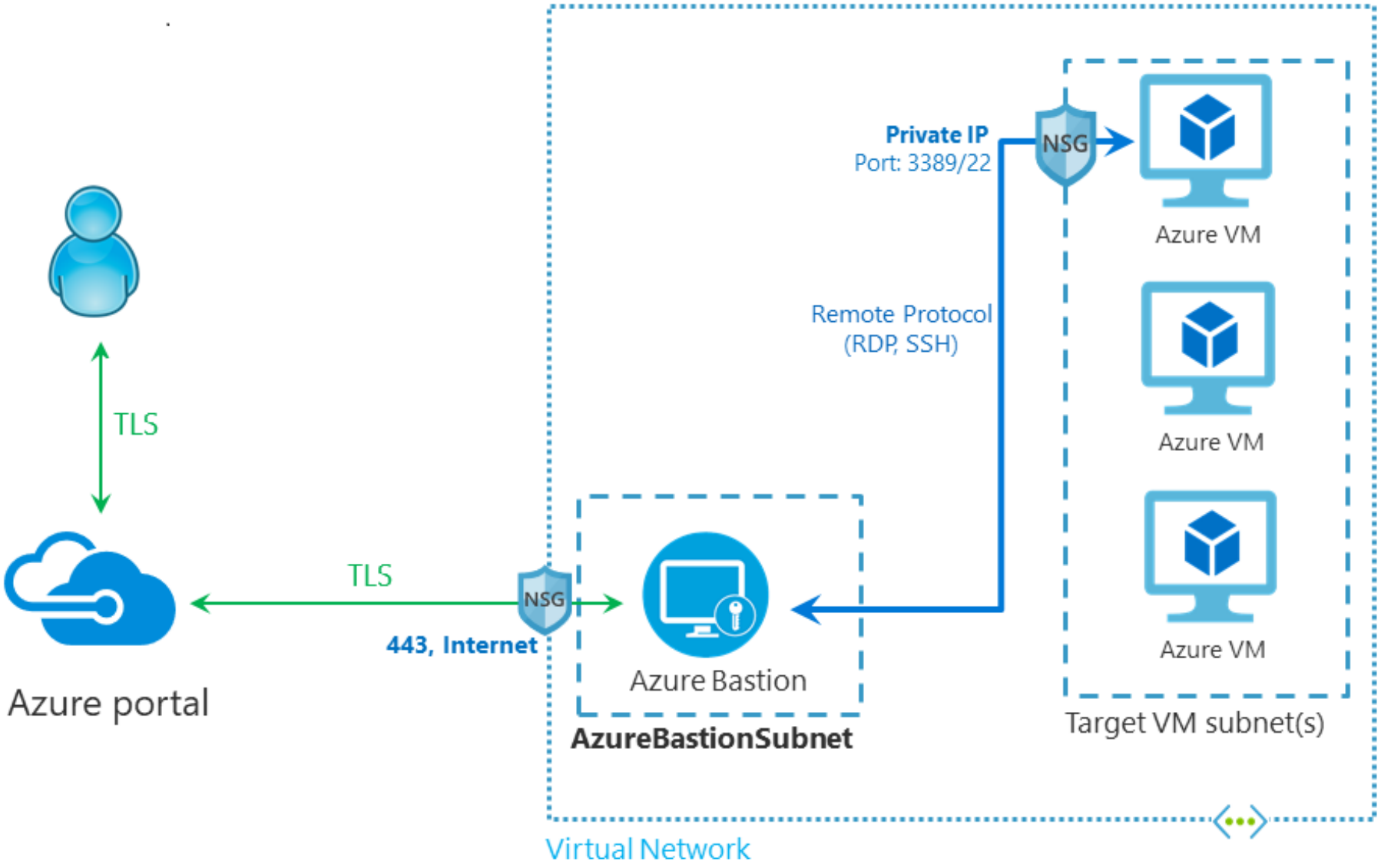
AZURE BASTION

Fully managed
PaaS

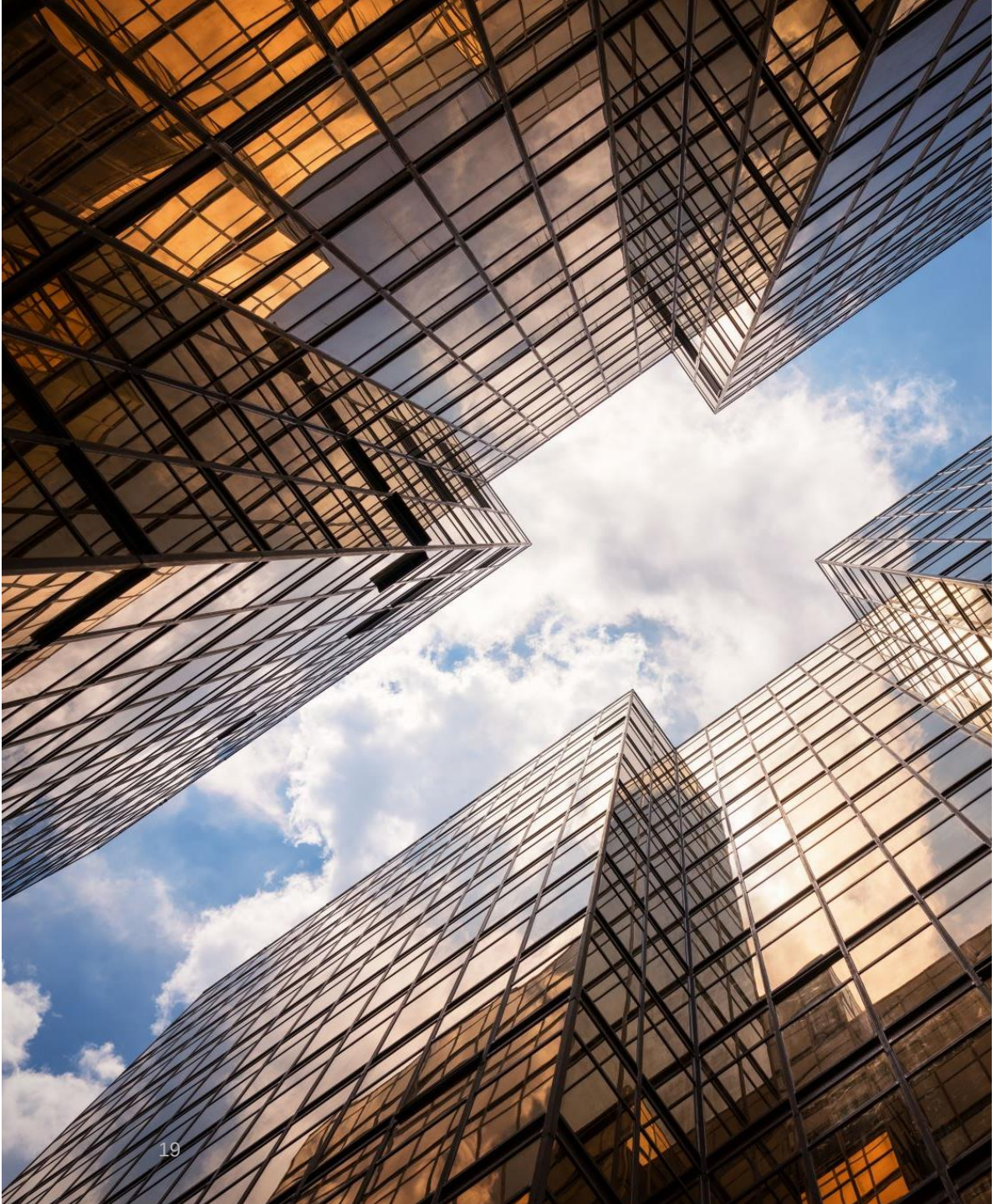
Restricts
RDP access

Allows RDP
via portal

AZURE BASTION – HOW IT WORKS



COST & PERFORMANCE OPTIMIZATIONS



CLOUD STICKER SHOCK!

- Workloads bursting above agreed capacity
- Overprovisioning of compute or storage resources
- Storage blocks that are no longer attached to a compute instance
- Poor job scheduling
- Over-buying or having unused reserved instances

DESIGN CHOICES AND TRADE-OFFS

1. **Ideal environment**
   - Most secure, high-performance, highly available, scalable, recoverable, and efficient environment
2. **Downsides**
   - Cost
   - Time to deliver
   - Operational agility

COST MANAGEMENT

- Cost Analysis
- Cost Alerts
- Budgets
- Cost Allocations

OPTIMIZATIONS – COST AND PERFORMANCE

Reservations & Azure Dedicated Host

Right-sizing

- VMs - Monitor CPU, Memory and IOPS
- Disks
- Storage
- SQL Databases
- App Service Tiers

Hybrid Use Benefit (HUB)

- Operating Systems (VMs), SQL, etc.

Orphaned items (i.e. Unattached)

- Managed Disks, Public Ips, NICs, Backups, Snapshots etc.

Decommissioning unused items

- VMs, Storage Accounts, SQL Databases, App Services, etc.

Scheduling auto-shutdowns

Autoscaling

22 | © 2022 | Confidential

AZURE ADVISOR

AZURE ADVISOR

- Recommendations
  - Cost
  - Security
  - Reliability
  - Operational Excellence
  - Performance
- Ties into Well-Architected Framework

SUPPORT & MANAGEMENT OPTIMIZATIONS

OPTIMIZATIONS – MANAGEMENT

Monitoring	Alerting	Locks	Backup Policies	Disaster Recovery
• All resources monitored • Diagnostics set up • Cert and App Registration secret expirations • Activity and Audit logs	• Based on resource criticality (CPU, Memory, IOPS, etc.) • Failing jobs (backup, replication, automation runbooks, etc.) • Security events (bulk deletion/additions, PIM elevations, etc.)	• Lock your high-priority resources • Prevent accidental deletion or changes • Resource Guard	• Azure Backup	• ASR

OPTIMIZATIONS – MANAGEMENT (CONTD.)

Quotas

- Service limits
  - Soft vs Hard limits
- Monitor network address space

Tagging

Regular Cleanup

- Unattached resources (NSGs, NICs, etc.)
- Configurations cleanup
  - E.g., Availability Sets with less than two members
  - Boot diagnostic files without VMs
- Empty Resource Groups

Configuration Drifts

- Ansible, Chef, Puppet, DSC, etc.

Azure DevOps

- Streamline deployments

OPTIMIZATIONS – MANAGEMENT (NEW FEATURES)

- Windows Admin Center (preview)
- Template Specs

NEXT STEPS

NEXT STEPS

CREATE AN AZURE OPTIMIZATION PLAN

SET UP PERIODIC REVIEWS

TAKE RELEVANT AZURE CERTIFICATIONS

HIRE CONSULTANTS TO REVIEW YOUR ENVIRONMENT

REFERENCES

Reference	Link
General	
Gartner Report	https://www.gartner.com/doc/reprints?id=1-28R38PF9&ct=220114&st=sb&submissionGuid=c5a828a0-e4d7-4318-9b7a-3a83a4113c70
Cloud Sticker Shock and related survey information	https://www.zdnet.com/article/cloud-sticker-shock-all-too-common-but-somewhat-avoidable/
Align responsibilities across teams (RACI)	https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/organize/raci-alignment
Cloud Adoption Framework	https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/
Microsoft Azure Well-Architected Framework	https://docs.microsoft.com/en-us/azure/architecture/framework/

REFERENCES

Reference	Link
Security	
Azure AD Privileged Identity Management (PIM)	https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
Enable Azure AD Multi-Factor Authentication	https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa
Conditional Access	https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview
Azure AD access reviews	https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview
Azure Policy exemptions	https://docs.microsoft.com/en-us/azure/governance/policy/concepts/exemption-structure
Microsoft Defender for Cloud	https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction
Azure Bastion	https://harvestingclouds.com/post/azure-bastion-series-index/
Azure Policy Sample - Block all public access to Azure Storage Accounts	https://harvestingclouds.com/post/block-all-public-access-to-azure-storage-accounts-via-azure-policy-with-complete-sample/

REFERENCES

Reference	Link
Cost and Performance	
Azure Advisor	https://docs.microsoft.com/en-us/azure/advisor/advisor-overview
Cost analysis	https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/quick-acm-cost-analysis
Cost Management best practices	https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/cost-mgt-best-practices
Cost alerts	https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/cost-mgt-alerts-monitor-usage-spending
Create and manage Azure budgets	https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/tutorial-acm-create-budgets
Hybrid Benefit	https://azure.microsoft.com/en-us/pricing/hybrid-benefit/
Reserved Instances	https://azure.microsoft.com/en-ca/pricing/reserved-vm-instances/

REFERENCES

Reference	Link
Support and Management	
Azure Monitor overview	https://docs.microsoft.com/en-us/azure/azure-monitor/overview
Alerts in Microsoft Azure	https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview
Alerts and automated actions	https://docs.microsoft.com/en-us/azure/azure-monitor/best-practices-alerts
Lock resources to prevent unexpected changes	https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json
Azure Desired State Configuration	https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview
Azure subscription and service limits, quotas, and constraints	https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits
Windows Admin Center	https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/manage-vm

Q&A

Thank you.