AZURE OPTIMIZATION RSA

MONTHLY REVIEW REPORT

Customer

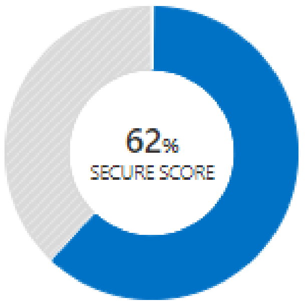
March, 2022

CLOUD SERVUS

Contents

1. Security Posture

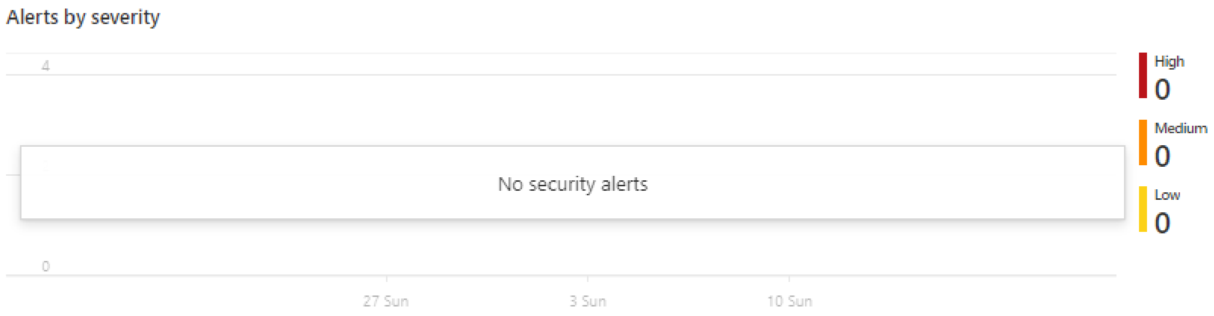
Secure Score and Alerts



As part of Security Center in Azure, Microsoft provides a high level “Secure Score” that takes into account the overal security posture of the environment.

This score will be the focal point of the Security Posture section and will be the main metric used to determine a positive **increasing** score or negative **decreasing** score.

Additionally, active security alerts will be created for any suspected or suspicious activity.



Alerts by severity

No security alerts

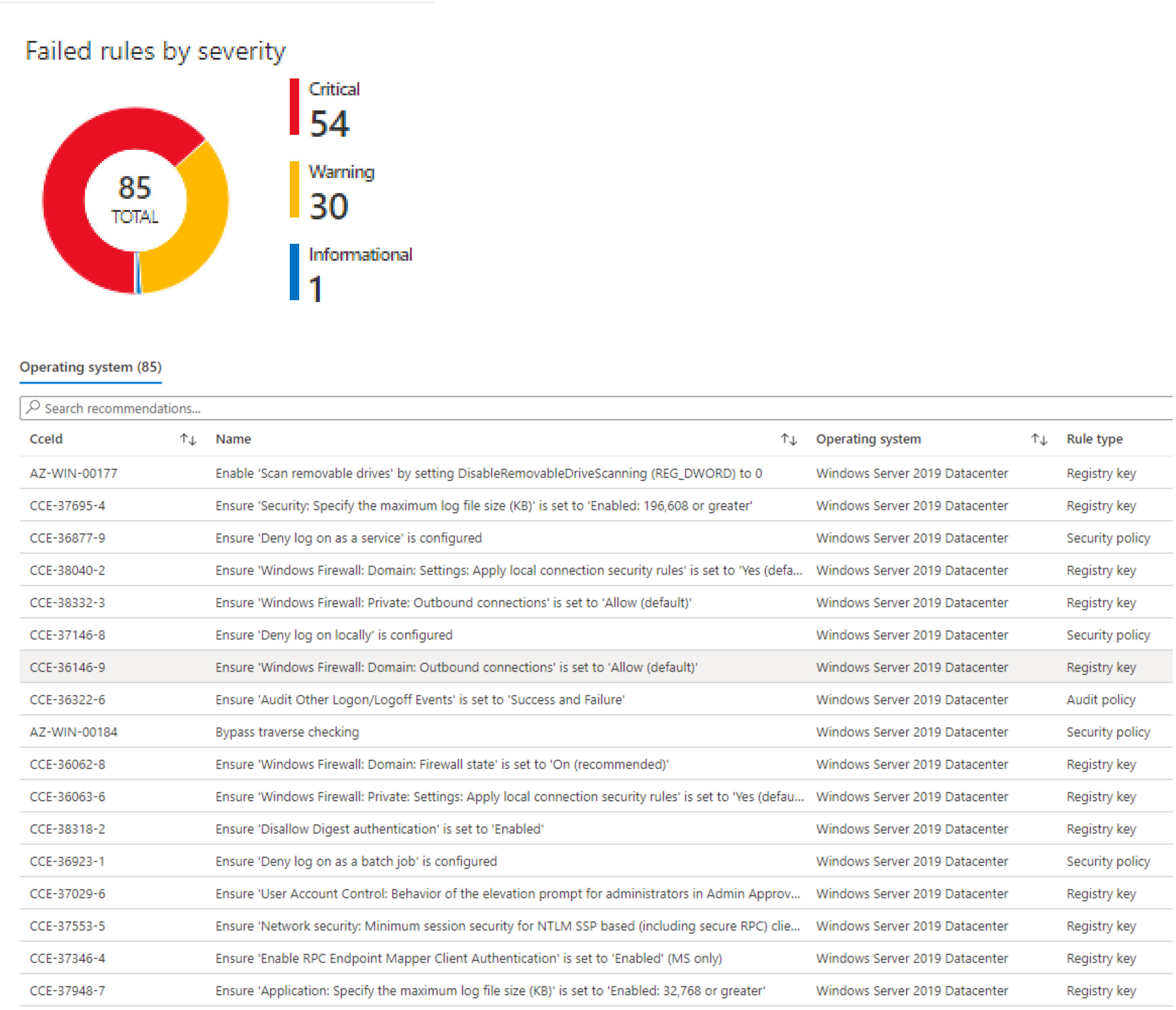
Secure Score is **Increasing** | **No Active Security Alerts**

Security Recommendations

The following is a backlog list of recommendations to improve the security posture of the Azure subscription:

Service	Task	Description
Auth	Multi-factor	Enable MFA on enabled accounts with owner/write permissions
VM	Encryption	Encrypt VM disks for VM1 and VM2
VM	Policy	Configure security policies for Windows Server 2019 to Microsoft Best Practice. *(See Screenshot)*
VM	Policy	Enable Adaptive Application Controls

App	Access	Disable FTP Access on WebAppProd and WebAppDev
App	Logging	Enable App/Diagnostic Logging on WebAppProd and WebAppDev
SQL	Access	Disable public network access WebAppProd, WebAppDev, and WebAppQA
Storage	Access	Remove public access to storageaccountprod and storageaccountdev
SQL	Access	Enable Azure AD access for WebAppQA
SQL	Logging	Enable Audit/Diagnostic logging on WebAppProd

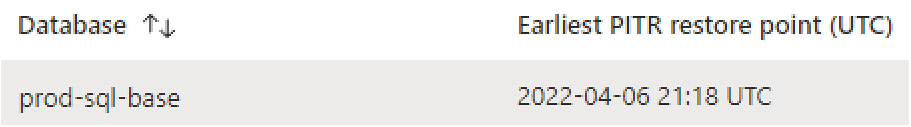


CceId	Name	Operating system	Rule type
AZ-WIN-00177	Enable 'Scan removable drives' by setting DisableRemovableDriveScanning (REG_DWORD) to 0	Windows Server 2019 Datacenter	Registry key
CCE-37695-4	Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	Windows Server 2019 Datacenter	Registry key
CCE-36877-9	Ensure 'Deny log on as a service' is configured	Windows Server 2019 Datacenter	Security policy
CCE-38040-2	Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (defa...	Windows Server 2019 Datacenter	Registry key
CCE-38332-3	Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	Windows Server 2019 Datacenter	Registry key
CCE-37146-8	Ensure 'Deny log on locally' is configured	Windows Server 2019 Datacenter	Security policy
CCE-36146-9	Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	Windows Server 2019 Datacenter	Registry key
CCE-36322-6	Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	Windows Server 2019 Datacenter	Audit policy
AZ-WIN-00184	Bypass traverse checking	Windows Server 2019 Datacenter	Security policy
CCE-36062-8	Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	Windows Server 2019 Datacenter	Registry key
CCE-36063-6	Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (defau...	Windows Server 2019 Datacenter	Registry key
CCE-38318-2	Ensure 'Disallow Digest authentication' is set to 'Enabled'	Windows Server 2019 Datacenter	Registry key
CCE-36923-1	Ensure 'Deny log on as a batch job' is configured	Windows Server 2019 Datacenter	Security policy
CCE-37029-6	Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approv...	Windows Server 2019 Datacenter	Registry key
CCE-37553-5	Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clie...	Windows Server 2019 Datacenter	Registry key
CCE-37346-4	Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only)	Windows Server 2019 Datacenter	Registry key
CCE-37948-7	Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Windows Server 2019 Datacenter	Registry key

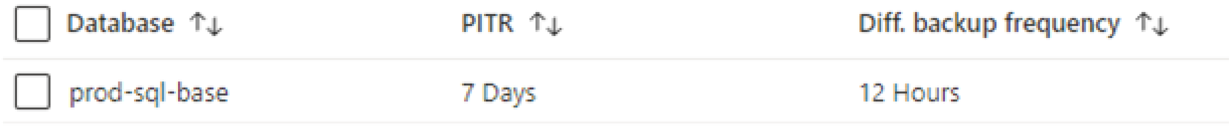
2. Resiliency

Backups

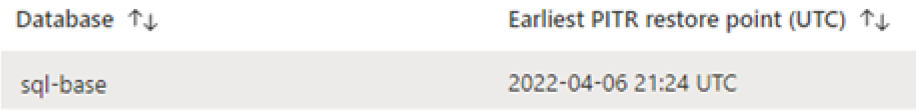
Azure SQL Backups are **Successful**



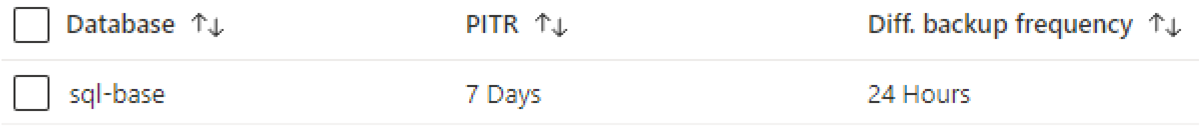
Database ↑↓	Earliest PITR restore point (UTC)
prod-sql-base	2022-04-06 21:18 UTC



□	Database ↑↓	PITR ↑↓	Diff. backup frequency ↑↓
□	prod-sql-base	7 Days	12 Hours

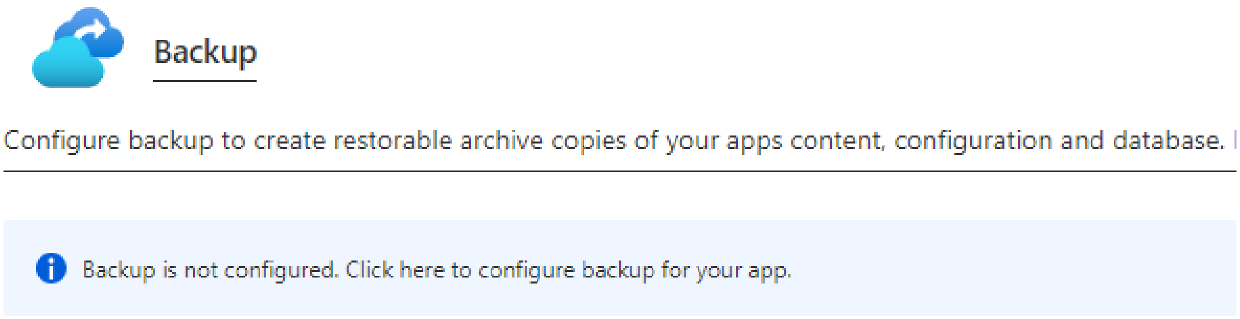


Database ↑↓	Earliest PITR restore point (UTC) ↑↓
sql-base	2022-04-06 21:24 UTC



□	Database ↑↓	PITR ↑↓	Diff. backup frequency ↑↓
□	sql-base	7 Days	24 Hours

Backups are not currently enabled for App Services, or Virtual Machines.

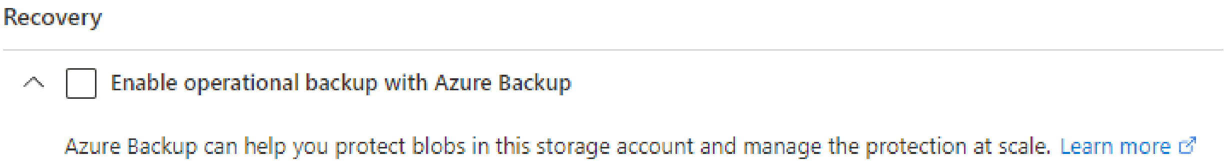


Backup

Configure backup to create restorable archive copies of your apps content, configuration and database.

Backup is not configured. Click here to configure backup for your app.

Backups are not currently enabled for Storage Accounts.



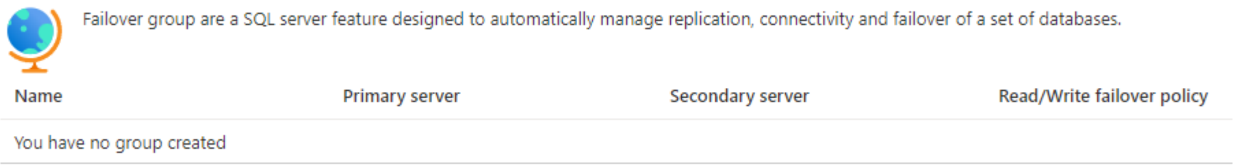
Recovery

□ Enable operational backup with Azure Backup

Azure Backup can help you protect blobs in this storage account and manage the protection at scale. Learn more

High Availability

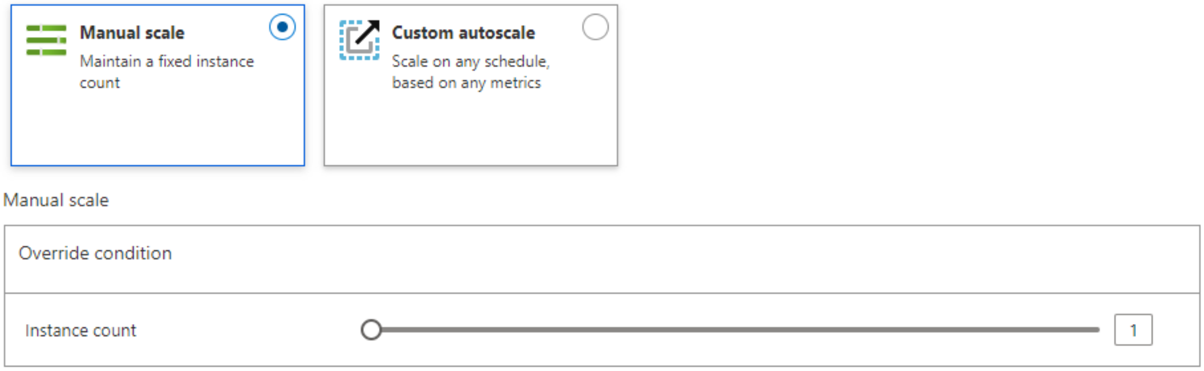
Azure SQL High Availability has not been configured.



Failover group are a SQL server feature designed to automatically manage replication, connectivity and failover of a set of databases.

Name	Primary server	Secondary server	Read/Write failover policy
You have no group created			

Azure App Service High Availability has not been configured.



● **Manual scale**
Maintain a fixed instance count

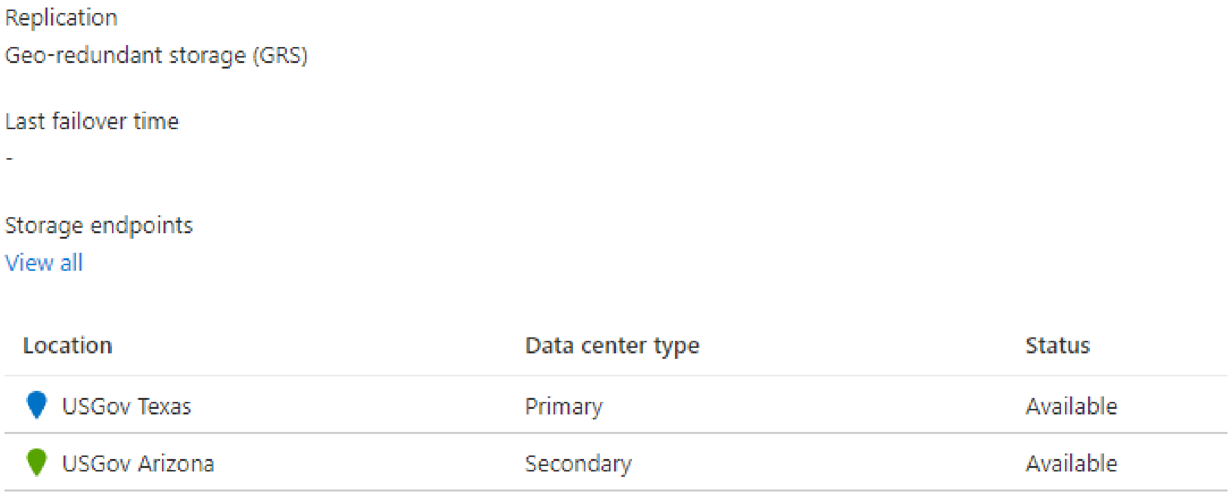
○ **Custom autoscale**
Scale on any schedule, based on any metrics

Manual scale

Override condition

Instance count 1

Azure Storage Account Geo-Replication is **Enabled.**



Replication
Geo-redundant storage (GRS)

Last failover time
-

Storage endpoints
View all

Location	Data center type	Status
USGov Texas	Primary	Available
USGov Arizona	Secondary	Available

Resiliency Recommendations

The following is a backlog list of recommendations to improve resiliency of the Azure subscription:

Service	Task	Description
VM	Backup	Enable VM backup and restore points.
App	Backup	Enable Azure Web App content backup
Storage	Backup	Enable Storage Account container backup
SQL	Availability	Enable secondary SQL Failover Group, replicate database copy
App	Availability	Configure Autoscale or Manual Instance increase to 2+ instances for high availability in the event of an app service outage or instance crash.

3. Optimization

Feature Enhancements

Azure DevOps Agents

As part of the deployment of the app two Virtual Machines were deployed as DevOps Agents. These machines execute code and infrastructure changes on the environment. Initially these machines were custom made Windows images and therefore need to be patched, secured, and maintained. Microsoft has recently released premade Linux build agents that have all the required build tools in a secured package.

Infrastructure as Code (IAC)

All the infrastructure in Azure can be captured and deployed as JSON templates. This allows for a repeatable deployment of resources and updates/changes. Leveraging the existing DevOps project resources can be configured in a build pipeline to deploy resources or be used as a backup deployment of the environment.

Bastion Host

With the current deployment, the agent virtual machines need to be accessed by public IP addresses and remote desktop. To further secure the environment the Bastion Host service can be enabled which would allow access to the VMs directly from the Azure Portal without needing to expose RDP ports to the internet.

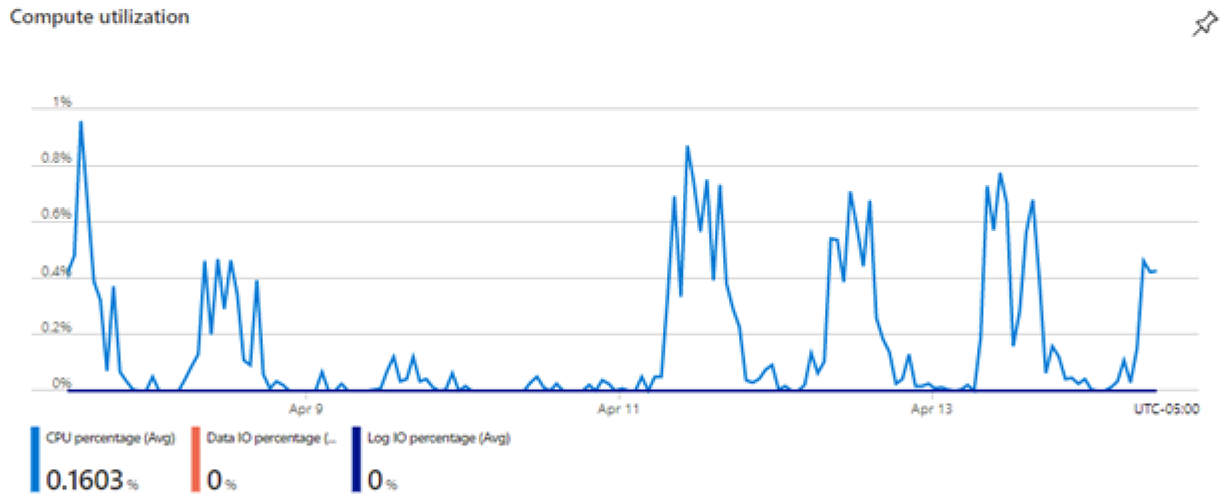
Update Management for Virtual Machines

Azure Automation has built in functionality to auto-update and reboot virtual machines with updates. Leveraging this service would allow the DevOps agents to be consistently updated without administrative interaction.

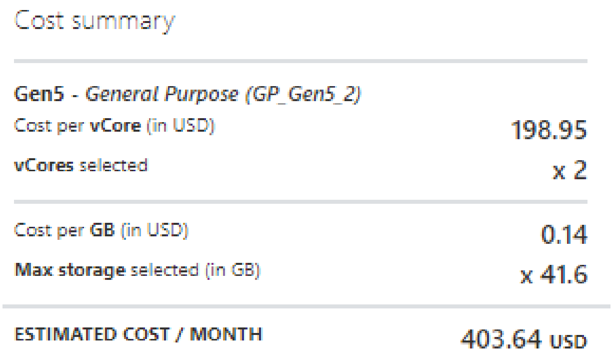
Cost Optimizations

Azure SQL Utilization

Current Azure SQL utilization is very low for the provisioned database resources. By changing the SKU for Azure SQL costs associated with production and pre-production databases can be reduced.



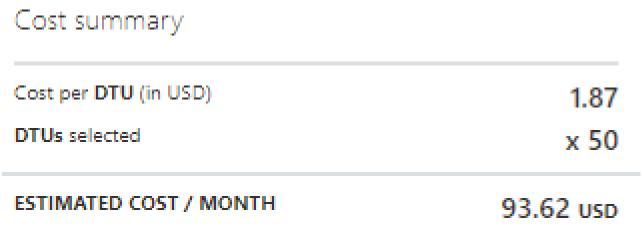
Existing SKU and Cost:



Cost summary

Gen5 - *General Purpose (GP_Gen5_2)*	
Cost per **vCore** (in USD)	198.95
vCores selected	x 2
Cost per **GB** (in USD)	0.14
Max storage selected (in GB)	x 41.6
ESTIMATED COST / MONTH	403.64 USD

Optimized SKU and Cost:



Cost summary

Cost per **DTU** (in USD)	1.87
DTUs selected	x 50
ESTIMATED COST / MONTH	93.62 USD

Azure Gov Feature Releases

Upcoming changes to Azure Front Door

Microsoft has recently released the V2 version of Azure Front Door in commercial tenants. This release includes significant changes including private link access from the Front Door to App Services. Upon its release to the Azure Gov subscription the networking configuration can be greatly enhanced. This will remove public access to the Web Apps from Front Door as well as streamline WAF functionality.

[Introducing the new Azure Front Door: Reimagined for modern apps and content | Azure Blog and Updates | Microsoft Azure]

Expected Release Date: Q3 2022

Optimization Recommendations

The following is a backlog list of recommendations to improve the Azure environment:

Service	Task	Description
VM	Deploy	Deploy new Prod and Dev Linux DevOps Agents
VM	Remove	Decommission and remove existing Windows DevOps Agents
DevOps	Create	Create Build Pipelines for Dev, QA, Prod
VM	Access	Enable Azure Bastion Host service for VM access
Automate	Deploy	Deploy Azure Automation for Update Management
SQL	Configure	Change Dev and Prod SQL SKUs