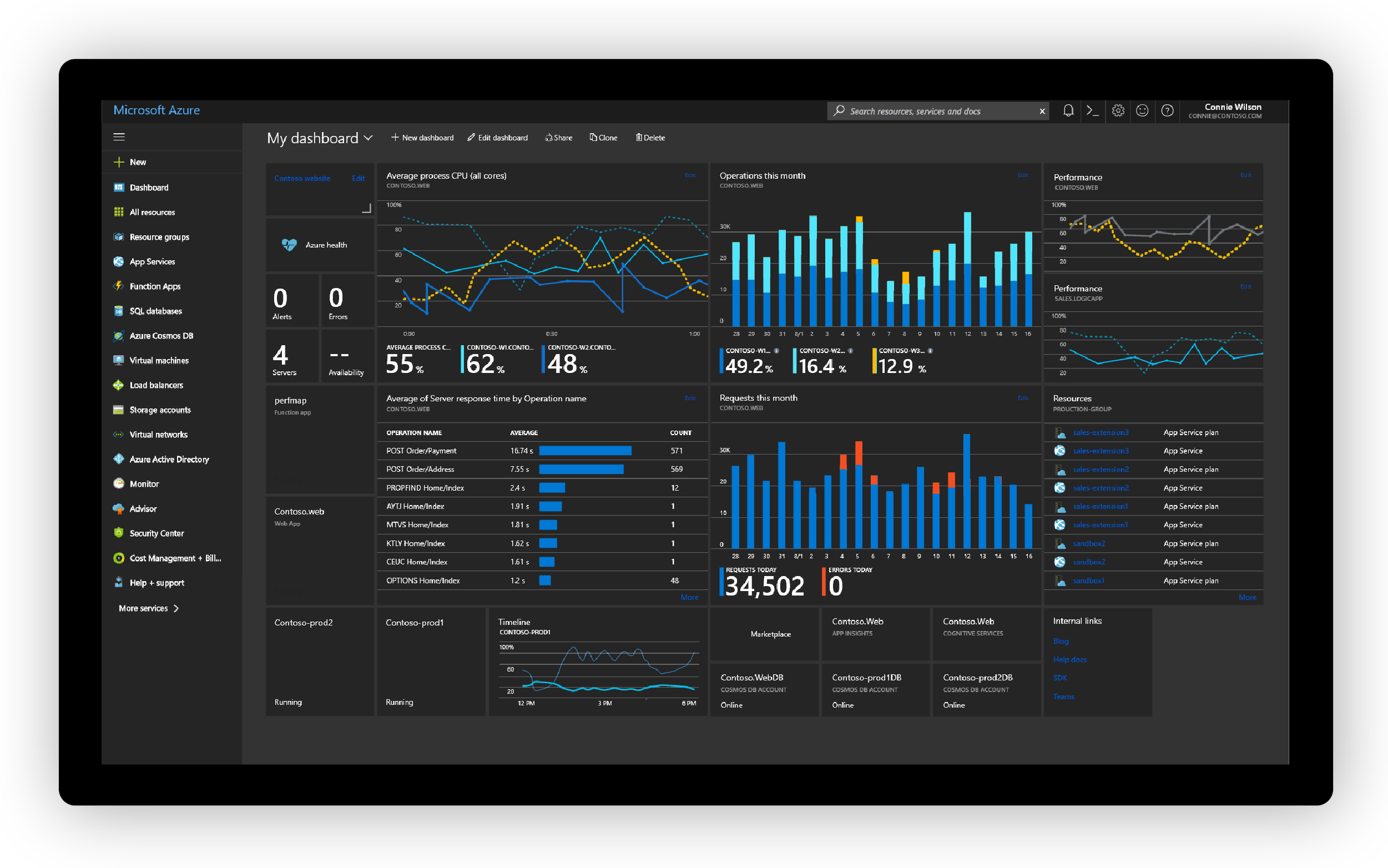
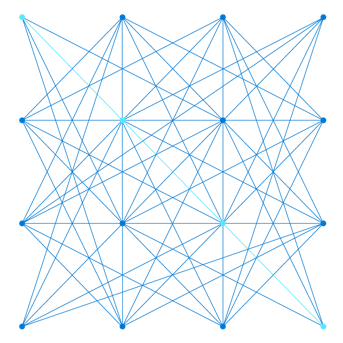
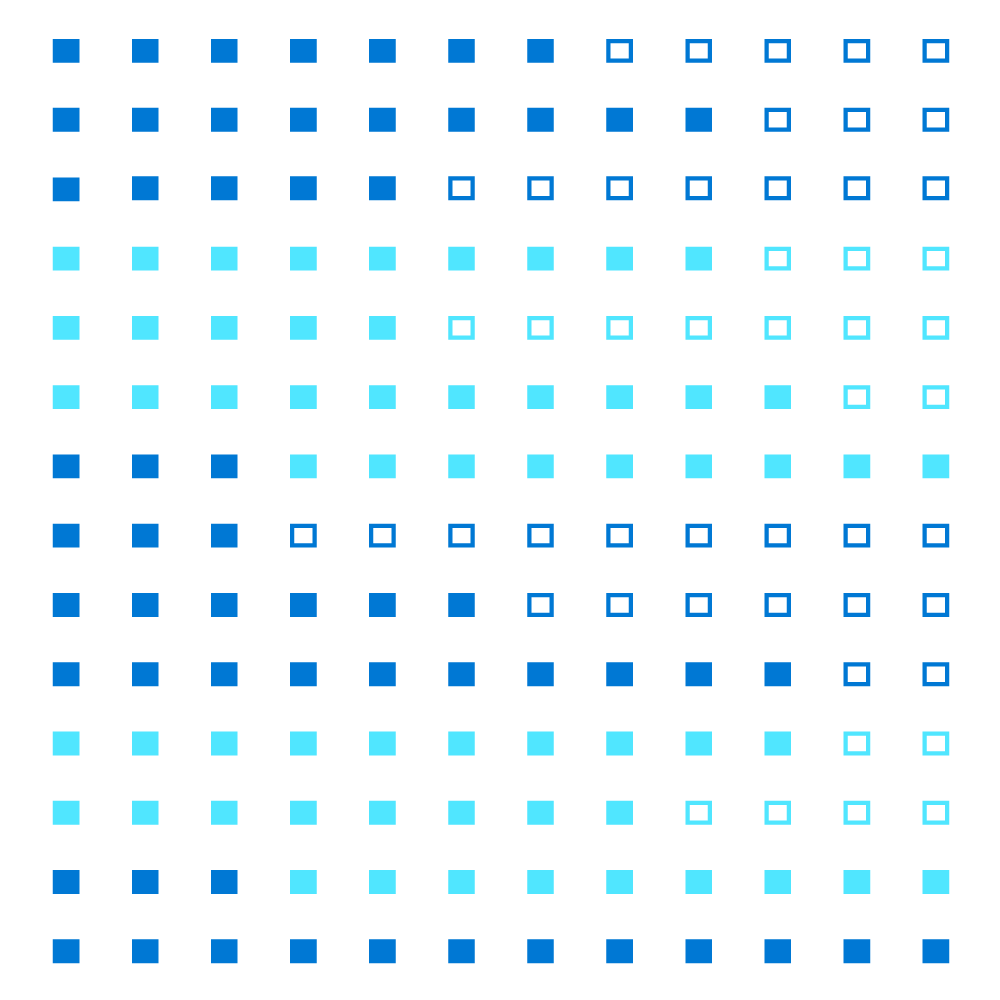
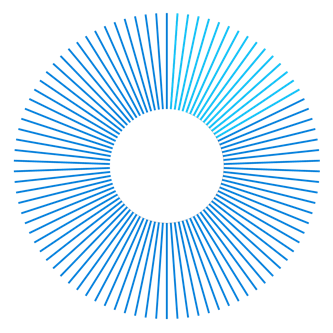
Hotel App

Well-Architected Reliability Assessment



Customer Success



Prepared for

Contoso Hotels

5/7/2024

Prepared by

**[Type Author Here]**

Cloud Solution Architect

email@microsoft.com

*Contributors*

[Type Contributors Here]

Table of Contents

[1 Introduction 5](#_Toc160097818)

[Workload information 5](#_Toc160097819)

[2 Executive Summary 6](#_Toc160097820)

[3.1 What is going well  6](#_Toc160097821)

[3.2 Baseline Resiliency Metrics & Insights Dashboard 7](#_Toc160097822)

[3.3 Health and Risk Dashboard 8](#_Toc160097823)

[**Dashboard** 8](#_Toc160097824)

[**Health Assessment Result (Azure Services)** – **Key High Impact issues** 8](#_Toc160097825)

[**Risk Assessment Result (Well-Architected Framework)** – **Key High Impact issues** 8](#_Toc160097826)

[**Health and Risk Charts** 9](#_Toc160097827)

[3 Baseline Resiliency Metrics & Insights details 11](#_Toc160097828)

[3.1 Zone and Region Resiliency 11](#_Toc160097829)

[3.2 ExpressRoute Resiliency 12](#_Toc160097830)

[3.3 Service Health Alerts for Resiliency 13](#_Toc160097831)

[4 Health and Risk Recommendations 14](#_Toc160097832)

[4.1 High Impact recommendations | Immediate fix needed 14](#_Toc160097833)

[4.2 Medium Impact recommendations | Fix within 3-6 months 14](#_Toc160097834)

[4.3 Low Impact recommendations | Needs to be reviewed 15](#_Toc160097835)

[5 Design, Platform and Support recommendations 16](#_Toc160097836)

[5.1 Architectural Recommendations 16](#_Toc160097837)

[5.2 Recent Microsoft Outages (past 3 or 6 months)  16](#_Toc160097838)

[5.3 Sev-A Support Requests (past 3-6 months) 17](#_Toc160097839)

[5.4 Azure Service Retirement Notifications 18](#_Toc160097840)

[6 Next Steps – Recommended Microsoft Services 19](#_Toc160097841)

[6.1 Key Customer Responsibilities 19](#_Toc160097842)

[6.2 Recommended Microsoft Services  19](#_Toc160097843)

[7 References 21](#_Toc160097844)

**VBD Updates (REMOVE THIS PAGE BEFORE DELIVERING TO CUSTOMER)**

|  |  |
| --- | --- |
| Date | Changelog |
| 2024-02-29 | Added Baseline Metrics & Insights and reordered sections. |
|  |  |
|  |  |
|  |  |
|  |  |
|  | For detailed updates, check the release notes in the Delivery Guide. |

1. Introduction

This document is delivered to **Contoso Hotels** to detail the Reliability recommendations and optimizations identified during the Well-Architected Reliability Assessment.

Resiliency, Availability, Reliability, Recoverability are very important aspects of any architecture. They provide availability assurances against application and hardware failures and faults. Losing these assurances can negatively impact on the business operations and revenue, as well as the organization’s reputation in the marketplace.

This document details recommendations and optimizations for the Workload architecture design, Azure Services, and management practices based on the Microsoft Well-Architected Framework.

All recommendations and findings in this report are based on the discussions and research that took place between Microsoft and Workload Admins from <MONTH> to <MONTH> <YEAR>.

The Microsoft team was granted read access to the relevant subscriptions through the Azure Lighthouse service and provided several architectural documents and diagrams. The findings include observations, relevant examples of the observations, and a set of recommendations to improve the reliability of the workloads.

## Workload information

[Explain in high level the target workload, how it works, how it is used by customers/users, its key integrations and/or dependencies with other systems, add the architecture diagram, subscription IDs, summary of resource group names (in case the subscription is hosting more workloads), user flows, etc – Add pictures, diagrams, etc.]

1. Executive Summary

Microsoft has completed the resiliency review of the **Hotel App** through a Discovery Workshop with the staff responsible for the workload and by running a suite of Azure tools to collect data from the target workload. The assessment provides findings and guidance based on analysis of your practices and Azure services being used against Microsoft proven best practices and recommendations provided by Azure documentation for each service, Well-Architected Framework documentation, and by the accredited Cloud Solution Architect(s) that delivered the engagement.

## 3.1 What is going well

* In place, active and tested Disaster Recovery and Backup solutions
* Internal load balancing within the application
* Current infrastructure sized to accommodate growth
* Azure resource monitoring connected to ITSM system to identify platform issues
* Redundant ExpressRoute paths to access the application exist
* Performance and fault testing process in place and operational

## 3.2 Baseline Resiliency Metrics & Insights Dashboard

This section shows the baseline metrics and insights critical for any workload. It highlights the adherence and adoption of Multi Zone, Multi Region, Multi ExpressRoute Peering Locations and configured Service Health Alerts.



Service Health Alerts are configured for all Services automatically triggering actions

ExpressRoute does not have multi peering location resiliency

Workload is not fully protected against zone and region failure

## 3.3 Health and Risk Dashboard

This section contains recommendations to improve the reliability and resiliency of your Workload, Azure services and practices. The recommendations are organized into two categories:

* **Health items:** cover areas such as configuration items and the proper function of the major components that make up your Azure Workload, such as Azure Resource configuration settings, dependencies on other services, and so on.
* **Risk items**: cover areas such as availability and recovery requirements, testing, monitoring, deployment, and other items that if left unresolved increase the chances of problems in the environment. Usually the Well-Architected Framework best practices.

The impact is categorized as follows:

* **High** - Immediate fix needed
* **Medium** - Fix within 3-6 months
* **Low** - Needs to be reviewed

**Dashboard**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Total recommendations** | | | **25** |  | | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Recommendations by impact** | | | | | | |  | |  | |  | | | **11** | High  impact | **7** | Medium impact | **7** | Low  impact | | |  |  | | --- | --- | | **Impacted resources** | | | **28** |  | |

**Azure Resources** – **Key High Impact issues**

* Ensure that storage accounts are zone or region redundant
* Run production workloads on two or more VMs using VMSS Flex
* Deploy VMs across Availability Zones
* Migrate VMs using availability sets to VMSS Flex
* Secure all incoming connections with SSL
* Use Standard Load Balancer SKU

**Well-Architected Framework** – **Key High Impact issues**

**Recommendations Charts**

The charts below show recommendations for Azure Resource and Resiliency Categories:

1. Baseline Resiliency Metrics & Insights details

This section shows the details of baseline metrics and insights critical for any workload. It highlights the adherence and adoption of Multi Zone, Multi Region, Multi ExpressRoute Peering Locations and configured Service Health Alerts.

## 3.1 Zone and Region Resiliency

This section shows a summary of the zonal and regional redundancy of the workload and key components. The purpose of this section is to highlight the workload resilience to key outage scenarios and whether existing mitigation plans are validated on a regular basis.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Workload Layer or Scenario**  **(Key Components Only)** | **Zone Failure Protection**  **(Yes/No/N.A.)** | **Region Failure Protection**  **(Yes/No/N.A.)** | **Zone Failure Testing**  **(Yes/No/N.A.)** | **Region Failure Testing**  **(Yes/No/N.A.)** |
| **Entire Workload** | No | No | No | No |
| AKS | Yes | Yes | Yes | Yes |
| App Services | No | No | Not Available | No |
| Azure SQL | Yes | No | Not Available | No |
| Virtual machines | No | No | Yes | No |
| Storage Accounts | Yes | Yes | Not Available | Yes |
| Virtual Network | Yes | Yes | Not Available | Yes |
| Azure Firewall | Yes | Yes | Not Available | Yes |

## 3.2 ExpressRoute Resiliency

This section shows a summary of the ExpressRoute Resiliency metrics and insight.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Service | Recommendations | | | | |
| ExpressRoute Gateways | **Is your ExpressRoute Gateway connected to two or more Circuits from different Peering Locations for higher resiliency?** | **Are you using Zone-redundant gateway SKUs?** | **Do you have monitoring and alerting configured for your ExpressRoute Gateway(s) for all gateway metrics and logs** | **Do you have diagnostic logs with all necessary logs, and alerts configured for your ExpressRoute Gateway(s)?** | **Do you have customer-controlled gateway maintenance (Preview) configured?** |
| GatewayName | **No** | Yes | **No** | Yes | **No** |
|  |  |  |  |  |  |
| ExpressRoute Circuits | **What is your current ExpressRoute Peering location?** | **Are the two physical links of your ExpressRoute circuit connected to two distinct edge devices (routers/firewalls) in your network?** | **Are both connections of the ExpressRoute circuit configured in active-active mode?** | **Is (BFD) Bidirectional Forwarding Detection enabled and configured on customer or provider edge routing devices?** |  |
| CircuitName | Ashburn | Yes | Yes | **No** |  |
|  |  |  |  |  |  |
| ExpressRoute Direct | **Is the “Admin State” of both Links of your ExpressRoute Direct in Enabled state?** | **Is your ExpressRoute Direct over-subscribed?** |  |  |  |
| ExpressRouteDirect Port Name | Yes | **No** |  |  |  |
|  |  |  |  |  |  |

## 3.3 Service Health Alerts for Resiliency

This section shows a summary of the Service Health Alerts configured.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Subscriptions | Alerts | Service Health Alerts configured to monitor: | | | | | | |
| Subscription Name | **Alert Name** | **All Azure Services?** | **All Regions?** | **Event Type:**  **Service Issues?** | **Event Type:**  **Planned Maintenance?** | **Event Type:**  **Service Advisories?** | **Event Type:**  **Security Advisory?** | **Automatically triggering Actions to your teams?** |
|  |  |  |  |  |  |  |  | Yes |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

1. Health and Risk Recommendations

This section outlines the recommendations organized by Azure services, Well-Architected Framework – Workload Lifecycle Stages, and Architecture Design. A number of risks have been identified through this assessment of solution. These risks are outlined below for review and remediation:

## 4.1 High Impact issues - Recommendations | Immediate fix needed

|  |  |  |  |
| --- | --- | --- | --- |
| # | Recommendation | Azure Service / WAF / Architecture Design | # of Impacted Resources |
| 1 | Ensure that storage accounts are zone or region redundant | storageAccounts | 6 |
| 2 | Run production workloads on two or more VMs using VMSS Flex | virtualMachines | 5 |
| 3 | Deploy VMs across Availability Zones | virtualMachines | 5 |
| 4 | Migrate VMs using availability sets to VMSS Flex | virtualMachines | 4 |
| 5 | Secure all incoming connections with SSL | applicationGateways | 2 |
| 6 | Use Standard Load Balancer SKU | loadBalancers | 2 |
| 7 | Deploy VMSS across availability zones with VMSS Flex | virtualMachineScaleSets | 1 |
| 8 | Set a minimum instance count of 2 | applicationGateways | 1 |
| 9 | Use Health Probes to detect backend availability | applicationGateways | 1 |
| 10 | Deploy Application Gateway in a zone-redundant configuration | applicationGateways | 1 |
| 11 | Use Standard or Premium tier | serverFarms | 1 |
|  |  |  |  |
|  |  |  |  |

## 4.2 Medium Impact issues - Recommendations | Fix within 3-6 months

|  |  |  |  |
| --- | --- | --- | --- |
| # | Recommendation | Azure Service / WAF / Architecture Design | # of Impacted Resources |
| 1 | Use ZRS Disks or Protect LRS Disks from Availability Zone Failure | virtualMachines | 7 |
| 2 | Enable Azure Private Link service for FSLogix storage account | storageAccounts | 6 |
| 3 | Enable Accelerated Networking (AccelNet) | virtualMachines | 5 |
| 4 | Replicate VMs using Azure Site Recovery | virtualMachines | 3 |
| 5 | Backup VMs with Azure Backup service | virtualMachines | 1 |
| 6 | Deploy VMSS with Flex orchestration mode instead of Uniform | virtualMachineScaleSets | 1 |
| 7 | Plan for backend maintenance by using connection draining | applicationGateways | 1 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 4.3 Low Impact issues - Recommendations | Needs to be reviewed

|  |  |  |  |
| --- | --- | --- | --- |
| # | Recommendation | Azure Service / WAF / Architecture Design | # of Impacted Resources |
| 1 | Ensure that your VMs are compliant with Azure Policies | virtualMachines | 84 |
| 2 | Enable VM Insights | virtualMachines | 10 |
| 3 | Network access to the VM disk should be set to Disable public access and enable private access | virtualMachines | 7 |
| 4 | Configure diagnostic settings for all Azure Virtual Machines | virtualMachines | 5 |
| 5 | Consider upgrading legacy storage accounts to v2 storage accounts | storageAccounts | 5 |
| 6 | Host database data on a data disk | virtualMachines | 3 |
| 7 | Enable Predictive autoscale and configure at least for Forecast Only | virtualMachineScaleSets | 1 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Design, Platform and Support recommendations

## 5.1 Architectural Recommendations

This section shows architectural recommendations that will help to mitigate some or all issues you faced in the past or will help to improve the overall resiliency and reliability of the workload.

[Add Diagrams if necessary]

|  |  |  |
| --- | --- | --- |
| **Component/Service** | **Observation** | **Recommendation/Change** |
|  |  |  |
|  |  |  |

## 5.2 Recent Microsoft Outages (past 3 months)

This section shows recent Microsoft outages (past 3 months) that may have impacted on the workload, as well as recommendations that will help to mitigate or minimize the impact of other possible similar outages. You can see this information via Azure Portal too.

|  |  |  |
| --- | --- | --- |
| **Tracking**  **ACM ID and**  **Outage Title** | **What Happened?** | **Recommendations** |
|  |  |  |
|  |  |  |

## 5.3 Sev-A Support Requests (past 3 months)

This section shows recent (past 3 months) critical Support Requests that Workload Admins opened with Microsoft Remote Support, as well as recommendations that will help to avoid, mitigate, or minimize the impact of other possible similar future incidents. You can see this information via Azure Portal too.

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident # and Title** | **Created Date** | **Cause and Resolution** | **Add your own recommendation. How they can avoid this happening again** |
|  |  |  |  |
|  |  |  |  |

## 5.4 Azure Service Retirement Notifications

This section shows Active Service Retirement Notifications that will likely affect the workload, as well as recommendations that will help to resolve the issue. You can see these notifications via Azure Portal too.

|  |  |  |
| --- | --- | --- |
| **Tracking**  **ACM ID and**  **Retirement Title** | **Subscriptions** | **Communication Update** |
| \_MYH-NTZ - Active : Transition to the ContainerLogV2 table by 30 September 2026 | 00000000-0000-0000-0000-000000000000 | 1. You’re receiving this notice because you use Azure Monitor container insights. 2. On 30 September 2026, we’ll retire the ContainerLog table in Azure Monitor and you’ll need to transition to the ContainerLogV2 table. The ContainerLogV2 table offers all the functionality of ContainerLog, plus: 3. Compatibility with the basic logs pricing tier. 4. Additional pod and container metadata for easier querying. 5. Support for multiline log entries. |
| \_MWK-DTZ - Active : Migrate to Azure Monitor VM insights by 30 September 2025 when Service Map will be retired | 00000000-0000-0000-0000-000000000000 | You're receiving this notice because you use Azure Service Map.  On 30 September 2025, Azure Service Map will be retired. To monitor connections between servers, processes, inbound and outbound connection latency, and ports across any TCP-connected architecture, you'll need to migrate to Azure Monitor VM insights.  The map experience of VM insights includes all the same functionality of Service Map, plus:  Improved scalability and support for more complex maps.  Deeper metrics capabilities for connections.  Support for grouping the machines you onboard to the map experience with subscriptions, resource groups, Azure Virtual Machine Scale Sets, and Azure Cloud Services. |
| XKB7-9TG - Active : Action required: Start using the Azure Monitor Agent before 31 August 2024 | 00000000-0000-0000-0000-000000000000 | You're receiving this notice because you use the Log Analytics Agent to monitor your Virtual Machines (VMs) or servers.  On 31 August 2024, we'll retire the Log Analytics Agent and it will no longer be supported by Microsoft. You'll need to start using the Azure Monitor Agent to monitor your VMs and servers in Azure. The Azure Monitor agent provides new features and capabilities, including:  Centralized configuration for multiple VMs.  Data limits and filters at the source.  Multiple destinations for data from a single agent. |
| WL54-58G - Active : Action required: Migrate classic application insights resources to workspace-based application insights | 00000000-0000-0000-0000-000000000000 | You're receiving this notice because you use classic application insights in Azure Monitor.  As of 29 February 2024, classic application insights in Azure Monitor has retired and you'll need to migrate your resources to workspace-based application insights. After 29 February 2024, your classic resources will continue to work and will not be deleted. If you have recently migrated to workspace-based application insights or are not currently using classic application insights, no further action is required.  Workspace-based application insights offers improved functionality such as:  Continuous export of app logs via diagnostic settings.  The ability to collect data from multiple resources in a single Azure Monitor log analytics workspace.  Enhanced encryption and optimization with a dedicated cluster.  New options to reduce costs.  Although most customers' pricing will remain the same, some may experience a change associated with this migration. Use the Azure pricing calculator to confirm your pricing. |
| VSQ2-DSG - Active : Retirement notice: Transition to using standard tests in Azure Monitor application insights | 00000000-0000-0000-0000-000000000000 | You’re receiving this notice because you use URL ping tests for single-step availability testing in application insights.  On 30 September 2026, the URL ping test capability of the application insights feature of Azure Monitor will be retired and ping tests will be removed from your resources. Before that date, you’ll need to transition to using standard tests, which also provide:  SSL certificate validity  Proactive lifetime check  HTTP request verb (such as GET, HEAD, POST)  Custom headers and custom data associated with HTTP requests  Recommended action  To ensure you can continue to run single-step availability tests in your application insights resources, review the pricing of standard tests and transition to using them before 30 September 2026. |
| RM64-FSZ - Active : Action required: Transition from Azure classic administrator roles to RBAC roles | 00000000-0000-0000-0000-000000000000 | You're receiving this notice because you use Azure classic administrator roles.  On 31 August 2024, Azure classic administrator roles will be retired. If your organization has active Co-Administrator or Service Admin roles, you'll need to transition to using Azure RBAC roles by then. (All Azure classic resources and Azure Service Manager will also be retired on that date.)  You may continue using these Azure classic admin roles until they're retired. However, starting 3 April 2024, you'll no longer be able to add new Co-Administrator roles through the Azure portal. |
| NNYV-38Z - Active : Action recommended: Update to using Grafana version 10 for Azure Managed Grafana | 00000000-0000-0000-0000-000000000000 | You’re receiving this notice because you’re using Grafana version 9 on Azure Managed Grafana.  Starting 31 August 2024, we will retire Grafana version 9. Before that date, you’ll need to update to Grafana version 10 as soon as possible. Grafana 10 provides all the functionality of Grafana 9 plus new ones, including:  New visualization panels  New or updated data source plugins  Tracing and correlations  Grafana version 9 will reach end-of-life support later this year and Grafana Labs will no longer provide security patches and other critical updates after that point. As a result, Azure Managed Grafana will stop offering Grafana version 9 as a supported software version on 31 August 2024. We strongly recommend that you upgrade your Managed Grafana workspace to Grafana 10 manually as soon as possible. If your workspace is still using Grafana version 9 after 31 August 2024, it will be migrated to Grafana version 10 in September 2024. You won’t be notified of the exact timing of this migration in advance.  You can still use Grafana 9 between 31 August 2024 and the date your workspace is automatically upgraded to Grafana version 10. However, during this period, Grafana version 9 will no longer receive updates from Microsoft.  Recommended Action  To avoid support disruptions, we strongly recommend that you manually upgrade to Grafana version 10 by 31 August 2024. |
| NKCZ-HZG - Active : Action required: Upgrade to Azure Standard Load Balancer by 30 September 2025 | 00000000-0000-0000-0000-000000000000 | You're receiving this notice because you've used Azure Basic Load Balancer within the last month.  This is a reminder that on 30 September 2025, Azure Basic Load Balancer will be retired. You can continue to use your existing Basic Load Balancers until then, but you'll no longer be able to deploy new ones after 31 March 2025.  To keep your workloads appropriately distributed, you'll need to upgrade to Standard Load Balancer, which provides significant improvements including:  High performance, ultra-low latency, and superior resilient load-balancing.  Security by default—closed to inbound flows unless allowed by a network security group.  Diagnostics such as multi-dimensional metrics and alerts, resource health, and monitoring.  SLA of 99.99 percent availability.  If you have any Basic Load Balancers deployed in Azure Cloud Services (extended support), those deployments will not be affected by this retirement and you don't need to take any action for them. |
| JNRV-3PZ - Active : Action recommended: Prepare for a version update in Azure OpenAI Service deployments | 00000000-0000-0000-0000-000000000000 | You're receiving this notice because you use Azure OpenAI Service.  On 8 March 2024, we'll begin updating Azure OpenAI deployments that use GPT-4 version 1106-preview to use version 0125-preview. The update will be completed within two weeks of that date.  GPT-4 version 0125-preview offers several improvements, including:  More complete code generation.  A higher rate of task completion.  Fixing a bug that affected non-English UTF-8 generations.  Because of these improved capabilities, you may notice some changes in the model behavior and compatibility after the update.  Recommended action  In a region where GPT-4 version 0125-preview is available, test your applications and workflows that use version 1106-preview before 8 March 2024 to ensure they'll continue working as expected. |
| FSQ7-B9G - Active : Retirement Notice: Support for the 1.x version of Azure Functions is ending on 14 September 2026 | 00000000-0000-0000-0000-000000000000 | You’re receiving this notice because you use version 1.x of the Azure Functions runtime.  On 14 September 2026, support for version 1.x of the Azure Functions runtime will end. You’ll still be able to use that version beyond that date, but it will no longer be supported or receive software or security updates.  To continue with a supported version, migrate to version 4.x of the Azure Functions runtime, which includes benefits such as:  Support for additional target framework versions, including .NET Framework 4.8, .NET 6, and .NET 7.  Ability to work with the latest Azure SDKs.  Enhanced monitoring options.  Improved reliability, throughput, and cold-start performance.  Recommended action  To ensure your function apps continue to run on a supported version, migrate to version 4.x of the Azure Functions runtime by 14 September 2026. |
| 7KFP-RTG - Active : Action required: Upgrade from Basic to Standard SKU public IP addresses in Azure by 30 September 2025 | 00000000-0000-0000-0000-000000000000 | You're receiving this notice because you've used Basic SKU public IP addresses within the last 30 days.  This is a reminder that on 30 September 2025, Basic SKU public IP addresses will be retired in Azure. You can continue to use your existing Basic SKU public IP addresses until then, however, you'll no longer be able to create new ones after 31 March 2025.  Standard SKU public IP addresses offer significant improvements, including:  Access to a variety of other Azure products, including Standard Load Balancer, Azure Firewall, and NAT Gateway.  Security by default—closed to inbound flows unless allowed by a network security group.  Zone-redundant and zonal front ends for inbound and outbound traffic.  If you have any Basic SKU public IP addresses deployed in Azure Cloud Services (extended support), those deployments will not be affected by this retirement and you don't need to take any action for them. |
| 3T\_R-3DZ - Active : Retirement notice: Windows Server 2022 will retire with k8s 1.34 on 15 March 2027 | 00000000-0000-0000-0000-000000000000 | You're receiving this notice because you currently use Windows Server 2022 node pools on AKS.  On 15 March 2027, Windows Server 2022 will be retired when Kubernetes 1.34 reaches the end of platform support. You won't be able to create new Windows Server 2022 node pools on Kubernetes 1.35 and above. We encourage you to make the switch before 15 March 2027 to gain the richer benefits of Windows Server 2025 or Windows Server Annual Channel. These new Windows OS versions will be supported on AKS before Windows Server 2022 is retired. For more updates, see our AKS public roadmap. |

1. Next Steps – Recommended Microsoft Services

Implementing the technical recommendations identified during this assessment will make your workload more resilient, lessen outage risk, and reduce downtime. Our approach is centered around customers taking the lead in optimizing their environments as a joint effort with Microsoft. The Service Recommendations in Section 4.2 detail how Microsoft can partner with you through your Unified Support Contract to build a reliable, well-architected environment following Microsoft Best Practices based on the Microsoft Well-Architected Framework.

## 6.1 Key Customer Responsibilities

We advocate for a customer-empowered approach to rectify the issues identified in this report. Our recommendations and follow-up services will equip you with the knowledge and tools needed to reinforce your system's reliability. While Azure provides reliable uptime, Customers are accountable for the proper configuration, management, and security of the applications, data, and services deployed on Azure. That includes tasks like setting up firewalls, configuring access controls, encrypting data, managing user access, and ensuring application-level security. All these practices will make significant and practical contributions to the stability and reliability of your important solutions.

## 6.2 Recommended Microsoft Services

Our recommended remediation services are collaborative in nature. Microsoft Cloud Solution Architects will work with your team, offering tailored guidance to address the pinpointed concerns. As we work side by side, you'll gain firsthand experience in configuring and fine-tuning critical components of your system. This collaborative effort ensures that your solution is not only well-architected but also well-understood by your team, enhancing your organization's overall technological acumen.

Your CSAM and other account team members will work with you to determine how we can best assist you to move forward on strengthening the resiliency of your Workload.

**Replace the content below with the VBDs that will be recommended to this customer according to your findings.**

|  |  |  |
| --- | --- | --- |
| **Priority** | **Recommended Microsoft Service** | **Customer Value (Outcomes)** |
| High | EXAMPLE - BCDR With Azure Backup And Azure Site Recovery | Explain how this Microsoft Service will help the customer to mitigate the discovered issues |
| High | EXAMPLE - Migrating and Modernizing Virtual Machines to Azure | Explain how this Microsoft Service will help the customer to mitigate the discovered issues |
| Low | EXAMPLE - Monitoring Workloads | Explain how this Microsoft Service will help the customer to mitigate the discovered issues |
| Medium | EXAMPLE - Security: Azure Networking Design & Implementation | Explain how this Microsoft Service will help the customer to mitigate the discovered issues |

1. References

Designing Reliable Applications

* + [Building Resilient and Reliable Azure Applications](https://docs.microsoft.com/en-us/azure/architecture/framework/resiliency/overview)
  + [Error Handling for Resilient Cloud Applications](https://docs.microsoft.com/en-us/azure/architecture/framework/resiliency/app-design-error-handling)
  + [Cloud Application Resiliency Patterns](https://docs.microsoft.com/en-us/azure/architecture/patterns/category/resiliency)
  + [Cloud Application Availability Patterns](https://docs.microsoft.com/en-us/azure/architecture/patterns/category/availability)

Mission-Critical Workloads

* + [What is a mission-critical workload?](https://learn.microsoft.com/en-us/azure/well-architected/mission-critical/mission-critical-overview#what-is-a-mission-critical-workload)

Operating Reliable Applications

* + [Site Reliability Engineering Resources](https://docs.microsoft.com/en-us/azure/site-reliability-engineering/)

Well Architected Framework Learning Path

* + <https://docs.microsoft.com/en-us/learn/paths/azure-well-architected-framework/>