Cognizant CLOUD SERVICES

Blueprint – Azure Storage

Revision History

Date	Version	Author	Reviewer(s)	Comments
2-Aug-2018	1.0	Sudarson	Tressa	Initial Draft

Contents

1. Scope

This document provides the blueprint for the Azure Storage offered by Azure. This contains the below.

1. Service Usage
2. Provisioning Scripts
3. Support Objectives
4. Monitoring metrics
5. Monitoring Setup Scripts

2. Overview

Azure Storage is one of several storage types offered in Azure Storage. Azure Storage provides the below options

1. Blob Storage – This is used to store unstructured data as blobs (objects) in Azure Storage. This is typically used to serve images / documents directly to a browser, store files for distributed access, streaming media (video & audio) and data backup.
2. Table Storage – This is used as a NoSQL data store, where data can be stored as table entities.
3. Queue Storage – This is used to queue messages for processing
4. File – This is used to store files and used as a file share from VM instances / azure services using SMB protocol.

3. Service Usage

3.1 Technical Limitations

- When firewall rules are enabled on the storage account and even if the access is enabled to Azure services, it is possible that quite a few services will not be able to access the storage account (E.g.: Azure functions).
- Table storage has High availability in single region with one optional readable secondary read region and can't initiate failover.
- Table storage has only primary index on PartitionKey and RowKey. No secondary indexes are supported.
- A table entity can have up to 255 properties, including 3 system properties: PartitionKey, RowKey, and Timestamp. So up to 252 custom properties can be defined for an entity
- A single queue message can be up to 64 KB in size
- The maximum time that a message can remain in the queue is seven days

3.2 Best Practices

- Blob storage to be preferably used for backup, data archive, analysis. It is not recommended to use this for VM disks vis-à-vis Managed Disks.
- Shared Access Signature to be used to access the blobs instead of account key.

- Blob storage provides multiple tiers. Below is the list with the recommended use cases
    a. Hot Access default access tier - Use when objects in the storage account will be more frequently accessed
    b. Cold Access tier - Use when the data stored is infrequently accessed and stored for at least a month with no access. Data in the cool storage tier can have slightly lower availability, but still high durability and similar time-to-access and throughput characteristics as hot data tier.
    c. Archive Access tier - Use when stored data is not accessed but only stored (Archived) for long periods of time. Durability remains high but access may require hours to enable. This is the lowest cost tier.
- All data in a storage account is to be encrypted using SSE (Storage Service Encryption)
- Anonymous and public read access to a container and its blobs in Azure Blob Storage must be disabled, unless there is a very specific business need which can't be achieved using Shared Access Signature
- Access to be restricted to specific IP addresses using Firewall configuration
- Rotate the storage account keys periodically
- It is recommended to enable Threat Detection.
- To effectively query the data in table storage, please follow the guidelines at https://docs.microsoft.com/en-us/azure/storage/tables/table-storage-design-for-query
- Table storage can be used over the one offered in Cosmos DB, if the data is less as the table storage is charged based on the amount of data.
- DR approach for storage to be followed as per https://docs.microsoft.com/en-us/azure/storage/common/storage-disaster-recovery-guidance?toc=/azure/storage/blobs/toc.json
- Best practices on managing concurrency to be followed as per https://docs.microsoft.com/en-us/azure/storage/common/storage-concurrency?toc=/azure/storage/queues/toc.json#managing-concurrency-in-the-queue-service

3.3 Microsoft SLA

99.9% of the time.

Refer https://azure.microsoft.com/en-in/support/legal/sla/storage/v1_0/

3.4 Additional Notes

1. Blob Rehydration - To read data in archive storage, the tier of the blob has to be first changed from archive to hot or cool. This process is known as rehydration and can take up to 15 hours to complete.
2. Large blob sizes are strongly recommended for optimal performance. Rehydrating several small blobs concurrently may add additional time.
3. A queue can contain millions of messages, up to the total capacity limit of a storage account

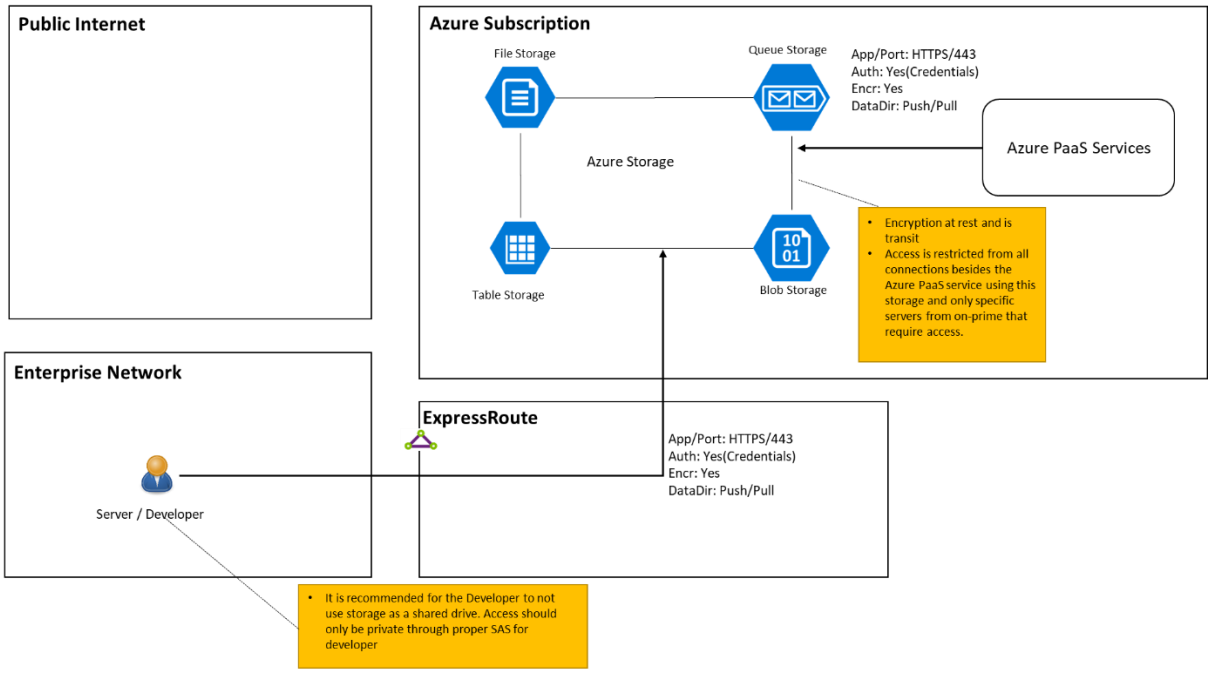
3.5 Recommended tiers for enterprise usage

LRS, GRS, RA-GRS, ZRS - based on replication requirements

3.6 Service Connectivity

Can be connected to from Express Route over https. Recommended to not make the content public.

3.7 Service Usage Diagram



4. Provisioning Script

The below ARM template is to be used to provision an instance of the service.

This consists of the below parameters

Parameter Name	Description
StorageName	The name of the storage account that you wish to create.Name must be in lowercase without special characters
Performance	Type of new Storage Accounts (Standard_LRS, Standard_GRS, Standard_ZRS or Premium_LRS) will be create.
Location	Location of the Stroage Account

EncryptionEnabled	Enable or disable Blob encryption at Rest.
httpsTrafficOnlyEnabled	The secure transfer option enhances the security of your storage account by only allowing requests to the storage account by secure connection
TagValues	Service Tags for the resource to categories

Template Script

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-
01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "StorageName": {
      "type": "string",
      "metadata": {
        "description": "The name of the storage account that you wish to
create.Name must be in lowercase without special characters."
      }
    },
    "Performance": {
      "type": "string",
      "defaultValue": "Standard_LRS",
      "allowedValues": [
        "Standard_LRS",
        "Standard_GRS",
        "Standard_ZRS",
        "Standard_RAGRS",
        "Premium_LRS"
      ],
      "metadata": {
        "description": "Type of new Storage Accounts (Standard_LRS, Standard_GRS,
Standard_ZRS or Premium_LRS) will be create."
      }
    },
    "Location": {
      "type": "string",
      "defaultValue": "South Central US",
      "allowedValues": [
        "South Central US",
        "North Central US"
      ],
      "metadata": {
        "description": "Location of the Storage Account"
      }
    },
    "EncryptionEnabled": {
      "type": "bool",
      "defaultValue": true,
      "metadata": {
        "description": "Enable or disable Blob encryption at Rest."
```

```
      }
    },
    "httpsTrafficOnlyEnabled": {
      "type": "bool",
      "defaultValue": true,
      "metadata": {
        "description": "The secure transfer option enhances the security of your
storage account by only allowing requests to the storage account by secure
connection."
      }
    },
    "TagValues": {
      "defaultValue": {
        "Tag1Name": "Tag1Value",
        "Tag2Name": "Tag2Value"
      },
      "type": "object",
      "metadata": {
        "description": "Tagsvalue can be used for searching purpose."
      }
    }
  },
  "resources": [
    {
      "apiVersion": "2017-06-01",
      "name": "[parameters('StorageName')]",
      "location": "[parameters('Location')]",
      "tags": "[parameters('TagValues')]",
      "type": "Microsoft.Storage/storageAccounts",
      "sku": {
        "name": "[parameters('Performance')]"
      },
      "kind": "Storage",
      "properties": {
        "supportsHttpsTrafficOnly": "[parameters('httpsTrafficOnlyEnabled')]",
        "encryption": {
          "services": {
            "blob": {
              "enabled": "[parameters('EncryptionEnabled')]"
            },
            "file": {
              "enabled": "[parameters('EncryptionEnabled')]"
            }
          },
          "keySource": "Microsoft.Storage"
        }
      },
      "dependsOn": []
    }
  ],
  "outputs": {
    "StorageName": {
      "type": "string",
      "value": "[parameters('StorageName')]"
    }
  }
```

}

5. Support Objectives

Below are the objectives to be fulfilled while providing support for instances of Azure Storage.

1. Request for Provision Azure Storage Account
2. Request for De-Provision Azure Storage Account
3. Onboarding Existing Azure Storage Account
    a. Setting up tags as defined by the enterprise
    b. Configuring monitoring metrics
4. Request for Configure Azure Storage Account
    a. Storage Performance Configuration
    b. On Request Access Key Rotation
    c. Request for Updating Storage Account Tags
5. On Schedule Access Key Rotation

6. Monitoring Metrics

This section details the metrics which are to be monitored for instances of Azure Storage Blob.

6.1 Recommended Metrics

Note: Performance and Latency monitoring options will not be available for the Archive access tier.

It is recommended to enable the following metrics by default.

Metrics	Category	Operator Type	Threshold	Unit	Frequency in Mins/Hrs
Availability	Information	<	100	percent	5M
AverageE2Latency	Performance	>	**Production:** 50 **Development:** 60	millisecond	5M
AverageServerLatency	Performance	>	**Production:** 3 **Development:** 5	millisecond	5M
Capacity	Information	>=	**Production:** 65% threshold: **Development:** 80% threshold: - Extra Small (1 GB) - Small (10 GB) - Medium (50 GB) - Large (100 GB) - X Large (500 GB) 100 GB left threshold: - 2X Large (1 TB) - 3X Large (5 TB) - 4X Large (10 TB)	bytes	24H
PercentAuthorizationError	Information	>	**Production:** 7 **Development:** 10	percent	3H

6.2 Optional Metrics

The following monitoring metrics are optional and can be enabled on a need basis.

Metrics	Category	Operator Type	Threshold	Unit	Frequency in Mins/Hrs
AnonymousAuthorizationError	Information	>	1	count	5M
AnonymousClientOtherError	Performance	>	1	count	5M
AnonymousClientTimeoutError	Information	>	1	count	5M
AnonymousNetworkError	Information	>	1	count	5M
AnonymousServerOtherError	Information	>	1	count	5M

AnonymousServerTimeoutError	Information	>	1	count	5M
AnonymousThrottlingError	Performance	>	1	count	5M
AuthorizationError	Performance	>	1	count	5M
PercentNetworkError	Performance	>	**Production:** 7 **Development:** 10	percent	5M
PercentServerOtherError	Performance	>	**Production:** 7 **Development:** 10	percent	5M

7. Monitoring Metrics Setup Script

This section provides a single script which can setup all the recommended metrics for monitoring.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-
01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "Alertname-Availability": {
      "type": "string",
      "metadata": {
        "description": "Name of alert"
      }
    },
    "Alertname-AverageE2ELatency": {
      "type": "string",
      "metadata": {
        "description": "Name of alert"
      }
    },
    "Alertname-AverageServerLatency": {
      "type": "string",
      "metadata": {
        "description": "Name of alert"
      }
    },
    "Alertname-Capacity": {
      "type": "string",
      "metadata": {
        "description": "Name of alert"
      }
    },
    "Alertname-PercentAuthorizationError": {
      "type": "string",
      "metadata": {
        "description": "Name of alert"
      }
    },
```

```
    "Alertname-Description": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "Description of alert"
      }
    },
    "SubscriptionName": {
      "type": "string",
      "metadata": {
        "description": "Name of the subscription"
      }
    },
    "Alert-NofificationEnable": {
      "type": "Bool",
      "defaultValue": true,
      "metadata": {
        "description": "Specifies whether alerts are enabled"
      }
    },
    "Storage-ResourceID": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "Resource ID of the resource emitting the metric that will
be used for the comparison."
      }
    },
    "SendEmailToBusinessOwners": {
      "type": "bool",
      "defaultValue": false,
      "metadata": {
        "description": "Specifies whether alerts are sent to service owners"
      }
    }
  },
  "resources": [
    {
      "type": "Microsoft.Insights/alertRules",
      "name": "[parameters('Alertname-Availability')]",
      "location": "[resourceGroup().location]",
      "apiVersion": "2016-03-01",
      "properties": {
        "name": "[parameters('Alertname-Availability')]",
        "description": "[parameters('Alertname-Description')]",
        "isEnabled": "[parameters('Alert-NofificationEnable')]",
        "condition": {
          "odata.type":
"Microsoft.Azure.Management.Insights.Models.ThresholdRuleCondition",
          "dataSource": {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleMetricDataSource",
            "resourceUri": "[parameters('Storage-ResourceID')]",
            "metricName": "Availability"
          },
          "operator": "LessThan",
```

```
          "threshold": "100",
          "windowSize": "PT5M",
          "timeAggregation": "Average"
        },
        "actions": [
          {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleEmailAction",
            "sendToServiceOwners": "[parameters('SendEmailToBusinessOwners')]"
          },
          {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleWebhookAction",
            "serviceUri": "https://replacewithmonitoringsolutionwebhookurl",
            "properties": {

              "severity": "Warning",
              "subscriptionname": "[parameters('SubscriptionName')]"
            }
          }
        ]
      }
    },
    {
      "type": "Microsoft.Insights/alertRules",
      "name": "[parameters('Alertname-AverageE2ELatency')]",
      "location": "[resourceGroup().location]",
      "apiVersion": "2016-03-01",
      "properties": {
        "name": "[parameters('Alertname-AverageE2ELatency')]",
        "description": "[parameters('Alertname-Description')]",
        "isEnabled": "[parameters('Alert-NofificationEnable')]",
        "condition": {
          "odata.type":
"Microsoft.Azure.Management.Insights.Models.ThresholdRuleCondition",
          "dataSource": {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleMetricDataSource",
            "resourceUri": "[parameters('Storage-ResourceID')]",
            "metricName": "AverageE2ELatency"
          },
          "operator": "GreaterThan",
          "threshold": "60",
          "windowSize": "PT5M",
          "timeAggregation": "Average"
        },
        "actions": [
          {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleEmailAction",
            "sendToServiceOwners": "[parameters('SendEmailToBusinessOwners')]"
          },
          {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleWebhookAction",
            "serviceUri": "https://replacewithmonitoringsolutionwebhookurl",
```

```
            "properties": {

              "severity": "Warning",
              "subscriptionname": "[parameters('SubscriptionName')]"
            }
          }
        ]
      }
    },
    {
      "type": "Microsoft.Insights/alertRules",
      "name": "[parameters('Alertname-AverageServerLatency')]",
      "location": "[resourceGroup().location]",
      "apiVersion": "2016-03-01",
      "properties": {
        "name": "[parameters('Alertname-AverageServerLatency')]",
        "description": "[parameters('Alertname-Description')]",
        "isEnabled": "[parameters('Alert-NofificationEnable')]",
        "condition": {
          "odata.type":
"Microsoft.Azure.Management.Insights.Models.ThresholdRuleCondition",
          "dataSource": {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleMetricDataSource",
            "resourceUri": "[parameters('Storage-ResourceID')]",
            "metricName": "AverageServerLatency"
          },
          "operator": "GreaterThan",
          "threshold": "60",
          "windowSize": "PT5M",
          "timeAggregation": "Average"
        },
        "actions": [
          {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleEmailAction",
            "sendToServiceOwners": "[parameters('SendEmailToBusinessOwners')]"
          },
          {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleWebhookAction",
            "serviceUri": "https://replacewithmonitoringsolutionwebhookurl",
            "properties": {

              "severity": "Warning",
              "subscriptionname": "[parameters('SubscriptionName')]"
            }
          }
        ]
      }
    },
    {
      "type": "Microsoft.Insights/alertRules",
      "name": "[parameters('Alertname-Capacity')]",
      "location": "[resourceGroup().location]",
      "apiVersion": "2016-03-01",
```

```
      "properties": {
        "name": "[parameters('Alertname-Capacity')]",
        "description": "[parameters('Alertname-Description')]",
        "isEnabled": "[parameters('Alert-NofificationEnable')]",
        "condition": {
          "odata.type":
"Microsoft.Azure.Management.Insights.Models.ThresholdRuleCondition",
          "dataSource": {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleMetricDataSource",
            "resourceUri": "[parameters('Storage-ResourceID')]",
            "metricName": "Capacity"
          },
          "operator": "GreaterThanOrEqual",
          "threshold": "80",
          "windowSize": "PT5M",
          "timeAggregation": "Maximum"
        },
        "actions": [
          {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleEmailAction",
            "sendToServiceOwners": "[parameters('SendEmailToBusinessOwners')]"
          },
          {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleWebhookAction",
            "serviceUri": "https://replacewithmonitoringsolutionwebhookurl",
            "properties": {

              "severity": "Info",
              "subscriptionname": "[parameters('SubscriptionName')]"
            }
          }
        ]
      }
    },
    {
      "type": "Microsoft.Insights/alertRules",
      "name": "[parameters('Alertname-PercentAuthorizationError')]",
      "location": "[resourceGroup().location]",
      "apiVersion": "2016-03-01",
      "properties": {
        "name": "[parameters('Alertname-PercentAuthorizationError')]",
        "description": "[parameters('Alertname-Description')]",
        "isEnabled": "[parameters('Alert-NofificationEnable')]",
        "condition": {
          "odata.type":
"Microsoft.Azure.Management.Insights.Models.ThresholdRuleCondition",
          "dataSource": {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleMetricDataSource",
            "resourceUri": "[parameters('Storage-ResourceID')]",
            "metricName": "PercentAuthorizationError"
          },
          "operator": "GreaterThan",
```

```
          "threshold": "7",
          "windowSize": "PT5M",
          "timeAggregation": "Average"
        },
        "actions": [
          {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleEmailAction",
            "sendToServiceOwners": "[parameters('SendEmailToBusinessOwners')]"
          },
          {
            "odata.type":
"Microsoft.Azure.Management.Insights.Models.RuleWebhookAction",
            "serviceUri": "https://replacewithmonitoringsolutionwebhookurl",
            "properties": {

              "severity": "Error",
              "subscriptionname": "[parameters('SubscriptionName')]"
            }
          }
        ]
      }
    }
  ]
}
```