Cognizant CLOUD SERVICES

Blueprint – Azure Traffic Manager

Revision History

Date	Version	Author	Reviewer(s)	Comments
26-Feb-2018	1.0	Gurappa M	Tressa	Initial Draft

Contents

1. Scope

This document provides the blueprint for the <service name> offered by <Cloud provider>. This contains the below.

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

2. Overview

Azure Traffic Manager enables distribution of user traffic for service endpoints in different datacenters. Service endpoints supported by Traffic Manager include Azure VMs, Web Apps, cloud services and external non-Azure endpoints. Traffic Manager delivers high availability for your applications by monitoring your endpoints and providing automatic failover when an endpoint goes down. It improves application responsiveness by directing traffic to the endpoint with the lowest network latency for the client. With its external, non-Azure endpoints support, Azure Traffic Manager can be used with hybrid cloud and on-premises deployments.

For more details: https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

3. Service Usage

3.1 Technical Limitations

- When traffic manager directs traffic to newer endpoints, other endpoints might continue to receive traffic through existing connection till such time the sessions are terminated
- Only one web app endpoint from one region can be added to the same traffic manager profile
- Total wait time for the new endpoint to receive the traffic during a failover is DNS Time-to-Live (TTL) + 2 minutes
- Using endpoints from multiple subscriptions is not possible with Azure Web Apps

3.2 Best Practices

- Nested Traffic Manager profiles and traffic-routing methods to be combined to create sophisticated and flexible rules to support the needs of larger, more complex deployments
- Preferred end point monitoring configuration (https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring)

  Protocol: HTTPS

  Port: 443

  Path: /

  Probing interval: 30

Tolerated number of failures: 5
Probe timeout: 10

- Below are the supported routing methods (https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods)
    a. Priority: Select Priority when a primary service endpoint for all traffic is to be used and provide backups in case the primary or the backup endpoints are unavailable.
    b. Weighted: Select Weighted when traffic is to be distributed across a set of endpoints, either evenly or according to custom defined weights.
    c. Performance: Select Performance when there are endpoints in different geographic locations and end users need to use the "closest" endpoint in terms of the lowest network latency.
    d. Geographic: Select Geographic so that users are directed to specific endpoints (Azure, External, or Nested) based on which geographic location their DNS query originates from. This enables scenarios where knowing a user’s geographic region and routing them based on that is important. Examples include complying with data sovereignty mandates, localization of content & user experience and measuring traffic from different regions.
- Incoming connections from Traffic Manager IP Addresses should be allowed at the endpoints for health checks to work
- Create a CNAME DNS record to map Internet facing domain to Traffic Manager profile.

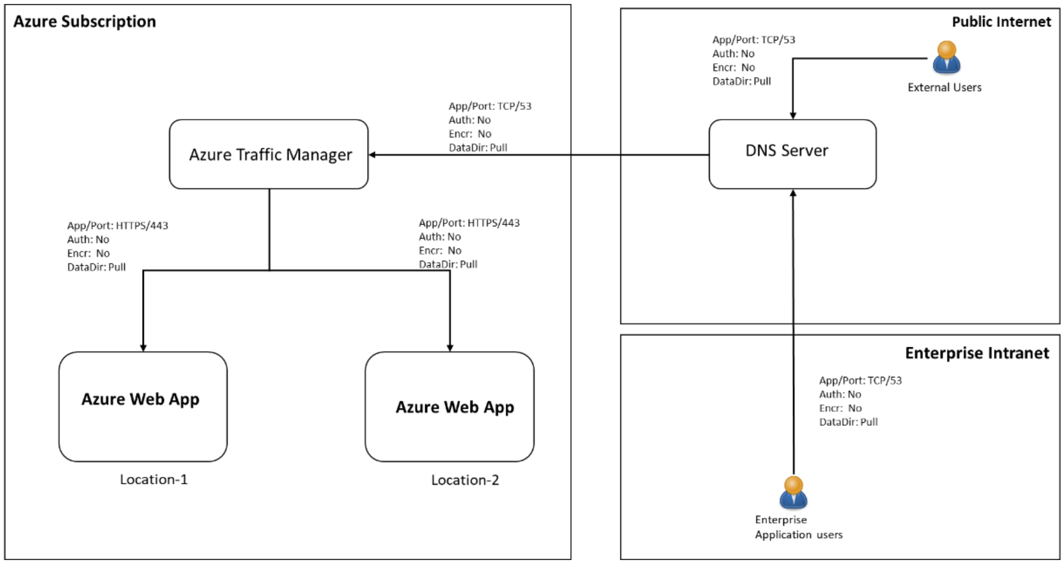
3.3 Microsoft SLA

- DNS queries will receive valid responses from at least one of the Azure Traffic Manager name server clusters at least 99.99% of the time.
https://azure.microsoft.com/en-us/support/legal/sla/traffic-manager/v1_0/

3.4 Additional Notes

- Sophisticated and flexible rules can be created to support the needs of larger, more complex deployments
- Only Web Apps at Standard SKU or above can be used with Traffic Manager
- Traffic Manager is not a proxy or a gateway. It does not see the traffic passing between the client and the service
- An endpoint which returns a HTTP 200 response back from the probe path is considered as online by Traffic Manager. Any other non-200 responses are a failure and is marked as degraded by traffic manager
- For TCP, if a response other than ACK or SYN-ACK is received to the SYNC request sent by Traffic Manager makes the endpoint to be marked as degraded
- For HTTPS probes, certificate errors are ignored
- Traffic Manager can be combined with Azure load balancer and Application Gateway and can be used to build an optimal solution. A scenario which uses all three services is specified at https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-load-balancing-azure

3.5 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
TrafficManagerName	Relative DNS name for the traffic manager profile, resulting FQDN will be <uniqueDnsName>.trafficmanager.net, must be globally unique
RoutingMethod	Enter the Routing Method for specific Traffic Manager profile
TagValues	Service Tags for the resource to categories
dnsTimetoLive	Enter the time window
endPointMonitoringPath	Enter the endpoint path

Template Script

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-
01/deploymentTemplate.json",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "TrafficManagerName": {
      "type": "string",
      "metadata": {
        "description": "Relative DNS name for the traffic manager profile,
resulting FQDN will be <uniqueDnsName>.trafficmanager.net, must be globally
unique."
      }
    },
    "RoutingMethod": {
      "type": "string",
      "defaultValue": "Performance",
      "allowedValues": [
        "Geographic",
        "Weighted",
        "Priority",
        "Performance"
      ],
      "metadata": {
        "description": "Enter the Routing Method for specific Traffic Manager
profile."
      }
    },
    "TagValues": {
      "defaultValue": {
        "Tag1Name": "Tag1Value",
        "Tag2Name": "Tag2Value"
      },
      "type": "object",
      "metadata": {
        "description": "Tags can be used for searching purpose."
      }
    },
    "dnsTimetoLive": {
      "type": "int",
      "defaultValue": 30
    },
    "endPointMonitoringPath": {
      "type": "string",
      "defaultValue": "/"
    }
  },
  "variables": {},
  "resources": [
    {
      "apiVersion": "2015-11-01",
      "type": "Microsoft.Network/trafficManagerProfiles",
      "name": "[parameters('TrafficManagerName')]",
      "location": "global",
      "tags": "[parameters('TagValues')]",
      "properties": {
        "profileStatus": "Enabled",
        "trafficRoutingMethod": "[parameters('RoutingMethod')]",
        "dnsConfig": {
          "relativeName": "[parameters('TrafficManagerName')]",
          "ttl": "[parameters('dnsTimetoLive')]"
        },
        "monitorConfig": {
          "protocol": "HTTPS",
          "port": 443,
          "path": "[parameters('endPointMonitoringPath')]"
        }
      }
    }
  ]
}
```

5. Support Objectives

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

1. Provision of Traffic Manager
2. De-Provision Traffic Manager
3. Onboarding Azure Traffic Manager
4. Configuring Traffic Manager Routing Method
5. Adding Endpoint
6. Endpoint Configurations
7. Deleting Endpoint
8. Toggle Traffic Manager Profile Status
9. Update Azure Traffic Manager Tags

6. Monitoring Metrics

Azure Traffic Manager doesn’t natively provide any metrics to be monitored.