|  |  |
| --- | --- |
| DR Failover & Failback Process Documentation | ALMP Platform Business Continuity and Disaster Recovery |
| This document describes the ALMP platform Business Continuity and Disaster Recovery failover and failback scenarios between the active-passive state of configuration and setup between UAE North and North European regions. | Document Status:  Author: **Saravanan Venkatarathnam (Cognizant), Eswaraiah Avvaru and Vinod Tiwari** |
| Last updated: 25-01-2024 |

**Table of Contents**

[1. DOCUMENT INFORMATION 3](#_Toc157510452)

[1.1 Version History 3](#_Toc157510453)

[1.2 Review and Approvals -AMericana 3](#_Toc157510454)

[2. ALMP deployment Architecture 4](#_Toc157510455)

[3. DR Swith over & fail back process flow 5](#_Toc157510456)

[4. DR failaover condtion 6](#_Toc157510457)

[5. ALMP Alerts applicable for DR switch over 7](#_Toc157510458)

[6. DR Failover steps 9](#_Toc157510459)

[7. DR Failback steps 10](#_Toc157510460)

[8. alerts 11](#_Toc157510461)

1. DOCUMENT INFORMATION
   1. Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Version* | *Date* | *Document Name* | *Role* | *Comments* |
| 0.1 | **25/1/2024** | **DR Failover & Failback Process Documentation** | **Architect** | **Initial document** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

***Table 1 - Version history***

* 1. Review and Approvals -AMericana

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Version* | *Date* | *Document Name* | *Role* | *Comments* |
| 0.1 |  | **DR Failover & Failback Process Documentation** | **client** | **Initial document** |
|  |  |  |  |  |
|  |  |  |  |  |

***Table 2 - Review and approvals***

* 1. DISCLAIMER

System and product names described in this document are not always accompanied by their Vendors or Owners trademark symbols (™, ®). It is hereby acknowledged that all trademarks are the property of their respective owners. Furthermore, any extracts from vendor documents implies that there is no intent not to acknowledge or violate any vendor’s copyrights.

1. Introduction

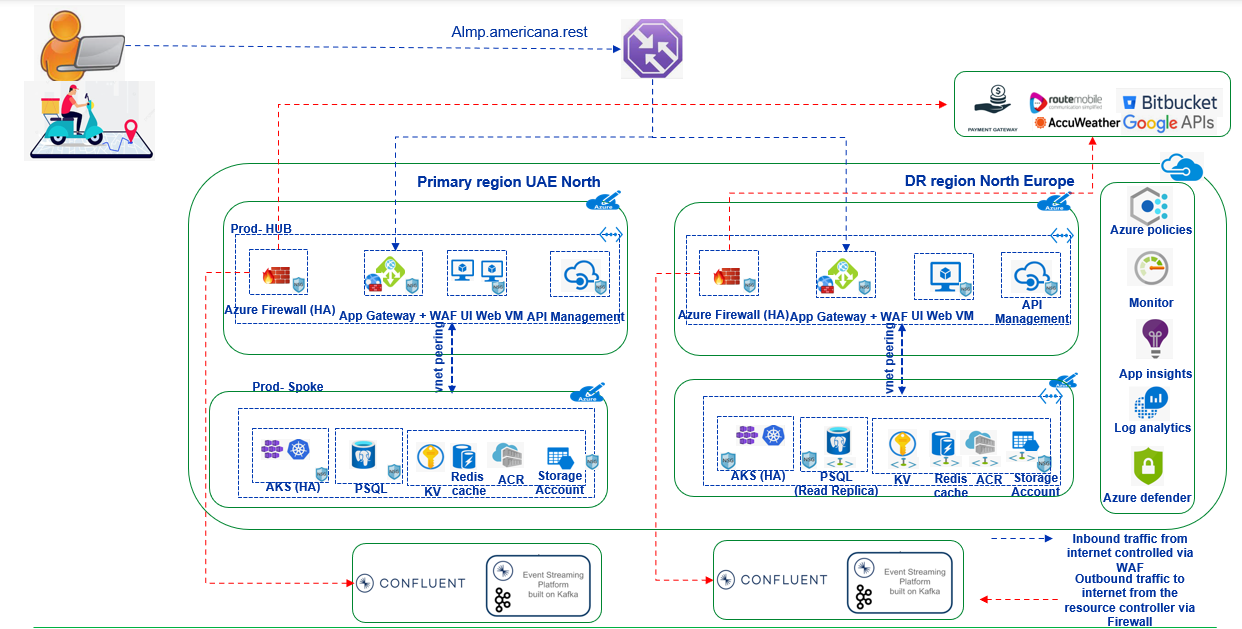
This document outlines the detailed process and technical specification of ALMP DR Failover and Failback operations. The technical design depicts key infrastructure, cloud services and outlines its configurations as required for deploying and operating for ALMP.

* 1. DISCLAIMER

System and product names described in this document are not always accompanied by their Vendors or Owners trademark symbols (™, ®). It is hereby acknowledged that all trademarks are the property of their respective owners. Furthermore, any extracts from vendor documents implies that there is no intent not to acknowledge or violate any vendor’s copyrights.

1. ALMP deployment Architecture

**Primary and DR architecture**



**DR End to End flow.**



**Availability SLAs of different components**

|  |  |  |  |
| --- | --- | --- | --- |
| **Azure Components** | **HA status** | **SLA** | **Reference** |
| Azure Firewall | Enabled | 99.99 | https://www.microsoft.com/licensing/docs?term=traffic%20manager |
| Traffic Manager | NA (Global Component) | 99.99 | https://www.microsoft.com/licensing/docs?term=traffic%20manager |
| Application Gateway | Enabled | 99.95 |  |
| API Management | Enabled | 99.99 | https://learn.microsoft.com/en-us/azure/api-management/high-availability |
| Virtual Machines | Enabled | 99.99 | Microsoft documentation |
| AKS | Enabled | 99.95 | Microsoft documentation |
| PSQL Flexi server | Enabled/Disabled | 99.99% /99.95% | Microsoft documentation  HA not enabled for “RIDER TRACKING” DB instance with 99% availability. |
| Keyvault | NA | 99.9 | Microsoft documentation |
| Container registry | NA | 99.9 | Microsoft documentation |
| Storage account | Enabled | 99.9 | Microsoft documentation |
| Redis cache | Enabled | 99 | Microsoft documentation |

1. DR failover Secnario (Systems)

Information updated based on the FMEA analysis.

**Conditions for DR failover required.**

|  |  |  |
| --- | --- | --- |
| **Resources** | **DR Failover required** | **Reason** |
| Application gateway failure | Failover required | Single or Multiple Failure in Microsoft Infrastructure. Microsoft needs to provide MTTR. For a prolonged outage it is inevitable to initiate the DR failover. |
| UI Both VM failure | Failover required |
| API Management failure | Failover required |
| AKS failure | Failover required |
| Firewall failure | Failover required |

**Conditions for DR failover can be deferred.**

|  |  |  |
| --- | --- | --- |
| **Resources** | DR Failover required | **Reason** |
| UI single VM failure | Not Required | Dashboard and other application can work from redundant server |
| Redis cache failure | Failover can be deferred. | Data can be loaded directly from the resource; application may respond with little latency |

1. ALMP Alerts applicable for DR switch over

**ALMP alerts Severity based on failure**

|  |  |  |
| --- | --- | --- |
| **Severity** | **Description** | **Impact** |
| Critical | One or more critical resource failure | Potential impact on Production |
| High | Specific Service failure | Potential/Partial impact on Production |
| Medium | High Utilization | No immediate impact, however fine tuning required on resource level |

**ALMP High/Critical alerts**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Resource name** | **Metric** | **Severity** | **Monitoring tools** | **Description** |
| Application gateway | UnhealthyHostCount | High | New relic/Azure alerts | Triggers alert when a backend service down on Appgw. |
| Service alert for availability | Critical | Azure alerts | Managed/Updated by Microsoft when there is a service failure. |
| Resource alert availability | Critical | Azure alerts | Based on the current resource state Azure monitor health probe this alert get triggered. |
| APIM | Service alert | Critical | Azure alerts | Managed/Updated by Microsoft when there is a service failure. |
| Resource alert | Critical | Azure alerts | Based on the current resource state Azure monitor health probe this alert get triggered. |
| AKS | Service alert | Critical | Azure alerts | Managed/Updated by Microsoft when there is a service failure. |
| Resource alert | Critical | Azure alerts | Based on the current resource state Azure monitor health probe this alert get triggered. |
| UI VM | Service alert | Critical | Azure alerts | Managed/Updated by Microsoft when there is a service failure. |
| Resource alert | Critical | Azure alerts | Based on the current resource state Azure monitor health probe this alert get triggered. |
| Redis cache | Service alert | Critical | Azure alerts | Managed/Updated by Microsoft when there is a service failure. |
| Resource alert | Critical | Azure alerts | Based on the current resource state Azure monitor health probe this alert get triggered. |
| PSQL | Service alert | Critical | Azure alerts | Managed/Updated by Microsoft when there is a service failure. |
| Resource alert | Critical | Azure alerts | Based on the current resource state Azure monitor health probe this alert get triggered. |

https://azure.status.microsoft/en-us/status

Note : Alerts will be refined further based on the individual failure simulation.

1. DR Swith over & fail back process flow

**Failover plan - MTTD**

QRT team receive an alert from Azure monitoring tool on the key component failure.

QRT team can validate the Azure resources status from the new-relic dashboard.

QRT team escalate the issue with the support team and based on the assessment the support team decides whether to proceed with the failover or not. Support team internally connect with respective Stakeholders and request a necessary approval to initiate DR failover.

Alert received.

Support team

Alert validation /Health check on new relic

Log it and update in Health check

Escalate to support team/Americana team

Failover required

Get an approval from Americana/Support team

Working on the fix and get a ETA from support team

1. DR Failover steps

**Prod- failover process to North Europe**

Support team block the incoming traffic from Primary resources to ALMP application.

Support team enable the DR region DB to read/write.

Support team enable the incoming traffic from “DR” resources and complete the sanity to release the system.

The detailed steps by step guide has been updated below.



**Teams to be involved.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Failover Steps** | **Tasks** | **Responsibility** | **Accountability** |
| Failover approval | Approval | ALMP governance team | ALMP governance team |
| Stops the inflow traffic from Primary region resources | Disable Traffic manager Primary endpoint | ALMP Support team | ALMP Support team |
| Enable DR to "Read/write | Promote replica DB | ALMP Support team | ALMP Support team |
| Enable the inflow traffic from DR region | Enable Traffic Manager DR endpoint | ALMP Support team | ALMP Support team |
| DB sanity check | Post failover activities | ALMP Support team | ALMP Support team |

|  |  |  |
| --- | --- | --- |
| **No.** | **Teams/Individual/Stockholders** | **Roles & Responsibilities** |
| 1 | ALMP L1/L2/L3 Support Team | L1 team will receive multiple automated failed alerts from Azure Monitor and New Relic will engage L2 and L3 support team to validate the DR criteria and DR region readiness. |
| 2 | ALMP Core Team | Disaster information will be received from ALMP support team and get on outage information in primary region to inform to the HD and stores teams via automated/manual communication channels. Engage with the ALMP engineering teams to perform the failover to DR region. |
| 3 | Americana HD Teams | The HD team will start coordinating the stores and drivers to continue the order deliveries with manual until DR region environment up and running. |
| 4 | Partner Management Team | ALMP Support team will also in parallel inform to the Partner’s core management responsible for this engagement to provide help and support during the disaster situation in primary region. |

**(Based on the input from Americana)**

1. Failback prepartion

**Prerequisites:**

Once the Primary region becomes operational.

* Core team restore the current production DB instances hosted in UAE region with different name for reference purpose. **(Optional)**
* Core team deletes the Primary DB instances (UAE North)
* Core team creates a new “replica” instance from “North Europe” to “UAE North”.

The detailed steps updated below.



1. DR Failback steps

**Prod- failback to UAE North**

**Prerequisites:**

Once the Primary region becomes operational.

* Core team restore the current production DB instances hosted in UAE region with different name for reference purpose.
* Core team deletes the Primary DB instances (UAE North)
* Core team creates a new “replica” instance from “North Europe” to “UAE North”

**Failback Process**

Inform to Americana and take a downtime during less business hours (Preferably morning hours)

Core team “Promote” the Primary “replica” to “read/write.”

Upon a completion “core” team disable the “Traffic manager” DR endpoint and enable “Primary endpoint” (UAE region), this ensure that the incoming traffic diverted from DR to Primary region.

Application and DB team validate the missing data during the “failback” time and take a necessary action.

Failback process updated here.



**Alert trigger metrics Template**

|  |  |
| --- | --- |
| **Event** | **Total Time** |
| Alert Triggering time vs Issue Start time |  |
| DR Switch over approval Time |  |
| Switch over validation time includes all validation and app sanity checks to release the environment |  |

1. alerts

Application Gateway

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Application gateway** |  |  |  |  |  |
| **Metirc** | **Condition** | **Alert Severity** | **Error message** | **Email recipeents** | **Period** |
| Backend Last Byte Response Time | > 500 Ms | Sev-2 | Error-Letency observed in Production application gatway | ALMP-Support team | 15 mins |
| Failed requests | >8000 | Sev 1 | Error-Letency observed in Production application gatway | ALMP-Support team | 15 mins |
| HealthyHostCount | < 2 | 0-Critical | Critical 1-One or more UI production frontend services down | ALMP-Support team | 15 mins |
| UnhealthyHostCount | > 0 | 0-Critical | Critical 1-One or more UI production frontend services down | ALMP-Support team | 15 mins |
| bad gateway errors | >6000 | warning | Production application gateway - bad gateway errors | Vinod | 15 mins |
| Client RTT | >500 | Sev-1 | Production Application gateway - Round trip time reached 500 milli seconds | ALMP-Support team | 15 mins |

API Manamgement

|  |  |  |  |
| --- | --- | --- | --- |
| **Metirc** | **Condition** | **Alert Severity** | **Error message** |
| Total requests | APIM- Backend error reached more than 10k | Sev -3 | APIM- Backend error reached more than 10k |
| APIM Utilization | Utilization <60 | Sev 3 | Prod API Management utlization reached 60 percentatge |