POC Document

Managed Network Grid Validation for Complex Medical Conditions

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Description | Author | Reviewer | Date |
| 1 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Introduction

## Purpose

The purpose of this document is to outline the Proof of Concept (POC) conducted to validate network connectivity between On-Premises systems and CMC Cloud Systems. It includes detailed implementation steps, validation procedures, and the results obtained to confirm successful connectivity and identify any potential issues.

## Background

CMC portals and their associated databases are being migrated to the Azure cloud, while batch jobs and the Facets database will remain in the on-premises datacenter for the time being. These on-premises components are planned to be migrated to the cloud in future phases. There are business requirements to have cloud file share and databases to be accessible from on-premises. Ensuring robust connectivity between on-premises and cloud-based services is critical to support seamless operations during and after migration.

Managed Network provides a network mesh and service discovery that integrates with cloud infrastructure and on-premises networks. Managed network bootstraps all necessary controls and connectivity for each cloud account, ensuring a seamless and secure experience.

Azure Network Management provides comprehensive managed networking - creation of virtual networks, creation and management of subnets, NSGs, route table, and routes. It integrates with IP address management (IPAM) for CIDR block allocation and offers an option to enable on-premises connectivity.

UHG Grid is a service mesh enabling service to service communication between on-perm and cloud as well as between cloud and cloud.

## Goal

The goal of the PoC is to complete the configuration of the GRID Network, onboard on-premises, and cloud resources that should be accessed across, and validate the access.

Implementation Steps

## Azure Cloud Setup

The following are standard steps that are required to provision nonproduction environment for CMC. The following steps are carried out to provision infrastructure that is required for PoC and validation.

1. Create Account in HCP with help of Optum App Owner
   1. An account for CMC is created in HCP.
   2. Ref: https://docs.hcp.uhg.com/account-manager/overview
2. Create HCP Account Resource Group and HCP Standard Resource Group with App Owner
   1. An HCP account resource group with name “cmc-main-cloud-resource-group-fdc45d0” is created.
   2. Ref: https://docs.hcp.uhg.com/account-manager/create-resource-group
3. Create NonProd Azure subscription from a non Contractor User
   1. A nonproduction subscription for CMC is created in HCP with name “azu-complex-medical-conditions-nonprod”
   2. The subscription is boot strapped with a VNet in the subscription that hosts VM instances that runs HA Proxy cluster as Mesh Gateway. Necessary event and routing are added for passing the ingress and egress traffic via the Grid Network.
   3. Ref: https://docs.hcp.uhg.com/public-cloud-account-management/non-production-public-cloud-account-creation
4. Create Immerse Teams for admin group and contributor group
   1. Ref: <https://immerse.uhg.com/teams>
5. Request for CIDR from IPAM
   1. A request for CIDR is made from HCP and obtained the CIDR as “10.88.176.0/22”
6. Create VNet
   1. A VNet for the POC purpose is created in Azure with name “vnet-grid-poc”.
   2. Ref: [Azure Virtual Network Management - PCAM UI - Cloud Networking | HCP Docs](https://docs.hcp.uhg.com/cloud-networking/azure-network-management-pcam-ui#vnet-creation)
7. Create NSG and Firewall Creation
   1. A Network Security Group is created with name “nsg-grid-poc”
   2. Ref: [Azure Virtual Network Management - PCAM UI - Cloud Networking | HCP Docs](https://docs.hcp.uhg.com/cloud-networking/azure-network-management-pcam-ui#nsg-and-rule-creation)
8. Route Table Creation
   1. A Route Table is created with name “rt-grid-poc-core”
   2. Ref: [Azure Virtual Network Management - PCAM UI - Cloud Networking | HCP Docs](https://docs.hcp.uhg.com/cloud-networking/azure-network-management-pcam-ui#route-table-creation)
9. Subnet Creation
   1. A subnet is created with name “sent-grid-poc-core”
   2. Ref: [Azure Virtual Network Management - PCAM UI - Cloud Networking | HCP Docs](https://docs.hcp.uhg.com/cloud-networking/azure-network-management-pcam-ui#subnet-creation)

# Service Onboarding

The intention is to establish connectivity of on-premises Facets database from workload in Cloud. The on-premises Facets database is “”

1. Service Registration
   1. The facets database endpoint is registered in the Service Discovery (Consul)
      1. Host: facets-oc-cmc-db-server.service.aide-0090093.ap.east.azu.stage.mesh.uhg.com
      2. Port: 1433
      3. Endpoint to access from cloud:
         1. facets-oc-cmc-db-server.service.aide-0090093.ap.central.azu.stage.mesh.uhg.com
         2. grid-gateway.service.aide-0090093.ap.central.azu.stage.mesh.uhg.com
   2. Tags added for this registration are
      1. "external"
      2. "tcp"
      3. "haproxy\_ports:1433"
      4. "haproxy\_mode:tcp"
   3. Ref: <https://github.com/uhg-arc/grid-onboarding/wiki/Service-Registration>
2. Application to Application communication
   1. Ref: [Application to Application Communication · uhg-arc/grid-onboarding Wiki](https://github.com/uhg-arc/grid-onboarding/wiki/Application-to-Application-Communication)

# Validation Steps & Results

1. Create an AppService
2. Deploy Powershell Script to AppService
3. Trigger the AppService and Validate connectivity in logs

# Reference Documents

Azure Managed Network: [Azure Virtual Network Overview - Cloud Networking | HCP Docs](https://docs.hcp.uhg.com/cloud-networking/azure-virtual-network-overview)

Architecture Diagram: [s3api-core.optum.com/mesh/meshv5.svg](https://s3api-core.optum.com/mesh/meshv5.svg)

Grid Onboarding: [Home · uhg-arc/grid-onboarding Wiki](https://github.com/uhg-arc/grid-onboarding/wiki)