**Managed Services Dependencies – Impact Assessment & Requirements**

**Migration Pod – Pod 1 – Scope Of Work**

The following shows the various apps are considered for migration pod 1. The table also highlights the various managed services dependencies for each of the apps considered for Pod 1 migration. Some of them have minor impact and some of them have significant impact.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| App ID | App Name | Cloud | Dependent Managed Services | | | | |
| Network | K8S | MS SQL | My SQL | Oracle |
| UHGWM110-005064 | Complex Medical Conditions Claims Portal | Azure | X | X | X |  |  |
| UHGWM110-005663 | Complex Medical Conditions Client | Azure | X | X | X |  |  |
| UHGWM110-000802 | Complex Medical Conditions Provider | Azure | X | X | X |  |  |
| UHGWM110-028731 | CCM PAC & RAD Data Mart | Azure | X | N/A | X |  |  |
| UHGWM110-017839 | PHS Digital transformation (Lobby) | Azure | X | X | X |  |  |
| UHGWM110-002705 | Agate | GCP | X | X |  | X |  |
| UHGWM110-000311 | CBMS - Customer Benefit Management System | GCP | X | X |  | X |  |
| AIDE\_0074661 | TraxCS Web Enabled | Azure | X | X | X |  |  |
| AIDE\_0075204 | Ubiquity - HPP | Azure | X | X | X |  |  |

Some of the apps are scheduled to go live in June and some are scheduled to go live by August.

**References -**

1. [Cloud Services Roadmap](https://docs.hcp.uhg.com/public-cloud/cloud-services-roadmap)
2. [Managed Networking – Guidelines](https://docs.hcp.uhg.com/cloud-networking/managed-networking-overview)
3. **Managed Network Dependency**

**Impact Assessment** – Optum Managed Networking was targeted for general availability in **April 2025**. However, it’s now **postponed with no target date** set. Managed Networking Impact is significant compared to all others highlighted in the impact table above.

Optum managed networking is designed for application teams to use Public Cloud Account Management (PCAM) and provides various network standardization inputs such as

* Network Name
* Region
* CIDR Range
* Number of subnets
* East-West traffic & firewalls rules
* Option to request on-premises connectivity.

Once launched application teams will no longer be able to create or modify networks on the native cloud services portal. They will need to use PCAM for any network management actions. For any new network, CIDR blocks will be assigned from the registered pool, effectively standardizing IP address management.

The **expected outcome of managed network** includes the following (**Once managed network services goes live**).

* **No Self-Managed Networks** - Once managed network solution becomes generally available, self-managed networks will not be allowed on any new accounts or existing accounts that do not have any networks in place within the public cloud account. **Application teams will no longer be able to create and manage networks outside of the new workflow in Public Cloud Account Management (PCAM)**.
* **Co-Existence** - Self-managed and managed networks cannot coexist within the same cloud account. Application teams must either create a new cloud account for managed networks or remove all self-managed networks before adding new managed networks.
* **On-Prem Connectivity Impact** - Accounts with existing (self-managed) networks can continue to operate if they comply with ingress and egress firewall requirements **and do not require on-premises connectivity**

The following value adds were expected out of the managed network services by the various LOBs.

* **Simplified Network Management -** PCAM abstracts the complexities of provisioning and managing networks, making these processes more straightforward.
* **Seamless Network Integration -** Networks are integrated with core components such as egress firewalls, optionally on-premises systems, and any other managed services attached to networks.
* **Built-in Security - Application** teams can focus on security at the application level while leveraging the platform's inherent network security features.
* **Easier Migration -** The infrastructure, including direct connectivity such as express route, enables the efficient transfer of large data needed for migration.
* **Adaptability**: The central management plane allows for quick adaptation to changing security landscapes and other business drivers.

**Workaround(s) & ETIPS Requirements**

Based on the above impact assessment and the dependency of managed network services across the board for all 9 applications targeted for migration pod 1, the following workarounds are suggested.

* **Self-Managed Networking** – Given the delay in launching managed networking, we (CmCoE migration pod team) assume that the applications getting migrated to Azure or GCP clouds are now going to be on Self-Managed Networking, until Optum Managed Networking is Generally available. CMCoE will also have to bake-in security management as per Optum standards for Self-Managed Networking infrastructure.
* **Rework - Migration from Self-Managed to Managed Networking** – This will require re-IP and deployment of various environments based on the CIDR blocks designed by Optum Managed Network Services Team. This will be a fair amount of rework deploying the infrastructure using IAC scripts but will also require the app teams to retest. There will also be customer impacts, firewall rules review/updates, DNS updates etc. The migration teams and line of business owners have to now bake in additional time and efforts for this rework.
* **On-Prem Connectivity** – API connectivity is available for a few apps which can be leveraged for on-prem connectivity. However, a good number of apps require direct DB connectivity due to legacy inter-application connectivity models. This will require a solution like express route VPN on Azure or Interconnect on GCP, which is currently not available due to managed network availability delays.

Lack of express route VPN or Interconnect will potentially cause network latencies depending on volume of data extracted/ingested. See Azure Reference architecture for Express Route Site to Site VPN options below. Azure ExpressRoute is a dedicated private connection between on-premises network and Azure public cloud, providing higher reliability, lower latency, and better security compared to internet-based VPNs.

Key components of Azure Express Route service include the following -

* ExpressRoute Circuit – A Dedicated connection between on-premises and Azure Edge
* ExpressRoute Gateway - Deployed in the Transit VNet (Hub) to route traffic.
* Peered VNets (Spokes) - Workloads in different VNets route traffic through the Hub.
* Azure Route Propagation - Ensures on-prem can communicate with peered VNets.

A diagram of a network

AI-generated content may be incorrect.  
For seamless migration, we need ETIPs team to provide express route site to site VPN (Azure) and interconnect for GCP. GCP Reference architecture below.

A diagram of a network connection

AI-generated content may be incorrect.

* **Network and Security Standards** – If there are no definitions of network standards made available and security standards, this will require significant rework in comparison to Optum standards.
* **On-Prem Connectivity (Data Migration) -** Data migration efforts could be a challenge if solutions like express route VPN or interconnect is not made available. CmCoE team can provide the volume of data that needs to be migrated for the initial cutover/migration. However, we don’t have any quantification of runtime data extraction/ingestion for apps that require direct DB connect, which would require Express Route VPN anyways.

1. **Managed Database(s) Dependency**

**Impact Assessment** – Optum Managed Database Dependency impacts applications teams to receive the same level of support as they are receiving today on-premises. While this can be mitigated by platform managed databases (SQL Server & My SQL), the businesses would still require support on the following.

* Proactive Managed Services
  + Planned Database Backup/Restore
  + Planned Maintenance activities (Indexing, Update Stats etc.)
  + Data Migration
  + New Environment Setup
  + Business Continuity/Disaster Recovery
  + Any data model help/support.
  + Data Retention Policy Management/Governance
  + Problem Management/Root Cause Analysis.
  + DB Fine Tuning – Cost & Performance Management
* Reactive Managed Services
  + Incident Management – Support for Unplanned Outages
  + Unplanned Business Continuity/Disaster Recovery
  + Performance Management & Troubleshooting

CmCoE would also require the DB Managed Services/network segmentation for databases, so it’s done as per Optum build standards, so the rework is minimal when the databases are moved over from self-service to managed services model.

1. **Managed K8S Dependency**

**Impact Assessment** – Optum Managed Kubernetes Services Dependency and Optum Managed Kubernetes Namespace as a Service impacts applications teams to receive the same level of support as they are receiving today on-premises. The workaround could be deploying the Kubernetes Cluster(s) and name space(s) in the Self-Service Cloud Accounts, leveraging the PaaS Kubernetes Services offered by the CSPs (AKS/GKE), but the application teams would still need support on the following,

* Proactive Managed Services
  + Kubernetes Cluster Sizing & Deployment
  + NodeGroup Configurations include resource allocations, autoscaling
  + Kubernetes Cluster monitoring and alerting
  + Ingress/LoadBalancer Configuration
  + Create/Manage Namespaces
  + Create/Manage Secrets
  + Containers build and deployments – Github Actions, Helm Chart
  + WAF/Web Security
  + Connectivity between services and databases
  + Observability – Install/Configure Prometheus/Grafana
  + Security Configurations – Splunk, IAM
* Reactive Managed Services
  + Kubernetes upgrade and maintenance
  + Kubernetes cluster scaling (upscaling and downscaling)
  + Troubleshooting any issues
  + Monitoring & Alerting
  + Incident Management – Support for Unplanned Outages
  + Unplanned Business Continuity/Disaster Recovery
  + Performance Management & Troubleshooting
  + CI/CD Updates including updates to Helm charts
  + Updates to Kubernetes clusters – Adding Nodes, change node types
  + Updates to Kubernetes namespaces
  + Security monitoring

1. **Other Recommendations**

Depending on the timelines of when managed services is going to be available, we need a team of operational support engineers to provide non-prod/prod support for the self-managed cloud infrastructure. This should include Network/Security, Databases (My-SQL, MS SQL), K8S and application observability. The number of resources required need to be quantified based on the number of Prod Vs Non-Prod environments.

Note – Managed Network availability issues might also potentially cause issues with ICE migration (currently worked under Microsoft cloud migration factory) and other apps which are in-flight for migration.