Definition of Done - MVP

MVP Services

Clarify Connectivity Requirements

On-prem to GCP as well as GCP to On-prem services

Connectivity requirements are being captured and documented [here](#)

Resource hierarchy needs to be documented

Shared VPC

Host Projects

Service Projects

Personas

Two main personas

1. Admin to be used by Platform engineering team
2. User to be used by users; developers, analytical users

Above categorization hopefully results in 2 sets of permissions being identified

We should be able to apply each of these sets to many service accounts

Admin Role should have the ability to perform all the following activities

- Managing Quotas
- implementing guard rails
- Service project creation
- Admin Role should have the ability to perform IAC, Manage ephemeral cluster , Project level administration

	Google Services	Owner	Platform Engineering Role (Admin)	Consumer Role (Developer)
1	**Google Cloud Storage (GCS)**	Kasi Viswanadham Vallabhaneni Karthikeyan Chelliah	- Ability to Create buckets (Single / /Dual Region/Multi Region) - Create "fine-grained" ACLS on bucket level - Ability to create folders , Place Data, Retrieve data - Data transfer <> GCS & DataMovers <> GCS	- Ability to create folders , Place Data, Retrieve data - Data transfer - GCS & DataMovers <> GCS
2	**Cloud Dataproc**	Kasi Viswanadham Vallabhaneni Karthikeyan Chelliah	- Ability to create, edit, start/stop and delete cluster - Ability to submit Spark, MR jobs to the cluster - Ability to create and execute work flows. - Ability to use shared subnets in respective regions allocated to respective environments - Should be able to SSH to cluster hosts from jump host - Should be able to connect to enterprise nexus repo (non-default os packages, python modules) VIA PSC - Should be able to create custom image - Validate connectivity to other Google services BQ,GCS,~~Cloud SQL~~, PubSub, cloud KMS (read & write), Bigtable	- Ability to create, edit, start/stop and delete cluster - Ability to submit Spark, MR jobs to the cluster - Ability to create and execute work flows. - Ability to use shared subnets in respective regions allocated to respective environments - Should be able to SSH to cluster hosts from jump host - Validate connectivity to other Google services BQ,GCS,~~Cloud SQL~~, PubSub, cloud KMS (read & write)
3	**Cloud SQL**	Karthik Kuppuraj	- Ability to create CloudSQL instances - Ability to create database structures (instance, databases, accounts) and submit jobs - Ability to administer jobs and queries - Ability to grant object level permissions - Ability to do DB admin tasks	- Ability to connect and use CloudSQL instances, submit jobs - Ability to do SUID operations on database objects - Access job execution logs - Ability to use CloudSQL API's

#	Service	Owner	Admin Access Requirements	User Access Requirements
4	**Google Compute Engine (GCE)**	Kasi Viswanadham Vallabhaneni	• Ability to create compute instance with default images along with GPU • Ability to start/stop/edit/delete instance • Should be able to use shared subnets in respective regions (e.g. US east 4 / US Central) allocated to respective environments (e.g.E1,E2,E3) • Should be able to SSH to GCE instance from jumphost • Should be able to connect to nexus-repo as well as Docker proxy VIA PSC. • Validate the connectivity to other Google services BQ, GCS,Cloud SQL, PubSub (read & write)	• Should be able to SSH to GCE instance from jumphost • Validate the connectivity to other Google services BQ,GCS,Cloud SQL, PubSub (read & write)
5	Cloud VPN			
6	Cloud IAM			
7	Persistent Disk			
8	VM Manager			
9	OS Login			
10	**Cloud Console**			
11	VPC			
12	Cloud DNS			
13	**Cloud Monitoring**			
14	**Cloud Logging**			
15	Resource Manager			
16	Cloud Identity /Workspaces			
17	VPC Service Controls			
18	**Cloud Key Management**	Manisha Gureja Sulabh Shukla Karthik Kuppuraj	• GCP KMS keyring create and maintain • GCP KMS key create and Maintain • Import Onpem KMS keys to GCP KMS (from respective Onprem environment edgenode) • Perform Decrypt functions in GCP	• KMS keyring List and Get • KMS crypto keys List and Get • Ability to list the import jobs • Ability to perform Encrypt / Decrypt functions
19	**Cloud Bigtable**	Kasi Viswanadham Vallabhaneni Karthikeyan Chelliah	• Ability to create instance/cluster and setup replication • Create/read/load/delete table • Validate the connectivity to other Google services GCE, DP,BT and Dataflow	• Create/read/load/delete table • Validate the connectivity to other Google services GCE,DP,BT and Dataflow
20	**Cloud Composer**	Kunal Jain	• Ability to create Environment • Run Dags and Trigger jobs • Admin access to Airflow Web UI. • RBAC enabled • Need connectivity to DP / DF, BQ, GCS, Cloud KMS	• Run Dags and Trigger jobs • Need connectivity to DP, DF, BQ, GCS, Cloud KMS
21	**Cloud Dataflow**	Kunal Jain	• Ability to view and submit dataflow job • Validate connectivity to other Google services BQ,GCS,~~Cloud SQL~~, PubSub, cloud KMS (read & write), Bigtable	• Ability to view and submit dataflow job • Validate connectivity to other Google services BQ,GCS,~~Cloud SQL~~, PubSub, cloud KMS (read & write), Bigtable
22	**Big Query**	Karthik Kuppuraj	• Ability to create high level structures(Datasets & Below) and submit jobs • Ability to administer jobs and queries • Import/Export data from GCS • Connect from data processing frameworks (dataflow, dataproc etc) • Ability to grant object level permissions • Create and maintain row and column level policies • Ability to perform encryption and decryptions on data • Create and maintain WLM configurations • Ability to use API's (cloud asset, data transfer, storage read/write) • Workload monitoring via admin panels and cloud monitoring	• Ability to create database objects (Tables,Views,SPs) and submit jobs • Import/Export data from GCS • Submit jobs to read/write data from processing frameworks (dataflow, dataproc etc) • Ability to use API's (Storage read/write, BigQuery API) for data access • Access job execution logs • Ability to perform data encryption/decryption
23	**Pub/Sub**	Kunal Jain	Ability to create topics, subscriptions, schemas and snapshots Ability to publish to topics and consume from topics	Ability to publish to topics and consume from topics

24	**Data Catalog**	Umesh Singh Chauhan Satish Anupindi	• Add/Remove/Edit/Search Tag Templates • Add/Remove/Edit/Search existing Tags for their specific dataset	• Not expecting direct permissions on GDC. Users will request to add /remove/udpdate/search tag changes through Lumi Portal, which would call necessary GDC APIs.
25	**Cloud DLP**	Umesh Singh Chauhan Akshay Pore	• create/remove/start/stop DLP jobs • create/edit dashboards • create/edit/remove DLP job triggers • inspection template/ data profile/ estimate/ de-identification / infoType permissions for administrative functions	• create/edit dashboards
26	**Cloud Asset Inventory**	Karthik Kuppuraj	• Ability to use Cloud Asset API's • Export asset inventory metadata and take asset snapshot • create, delete, and update events for assets • Monitor resource and policy changes • view insights generated from assets and manage insights in Recommender	• Ability to use Cloud Asset API's • Export asset inventory metadata • create, delete, and update events for assets • Monitor resource and policy changes • View insights generated from assets and view insights in Recommender
27	**Google Kubernetes Engine (GKE)**	Kasi Viswanadham Vallabhaneni Karthikeyan Chelliah Kunal Jain	• Ability to manage clusters and their Kubernetes API objects	• Ability to access clusters and their Kubernetes API objects

Post MVP Services