Connectivity Requirements Overview

On-prem to GCP

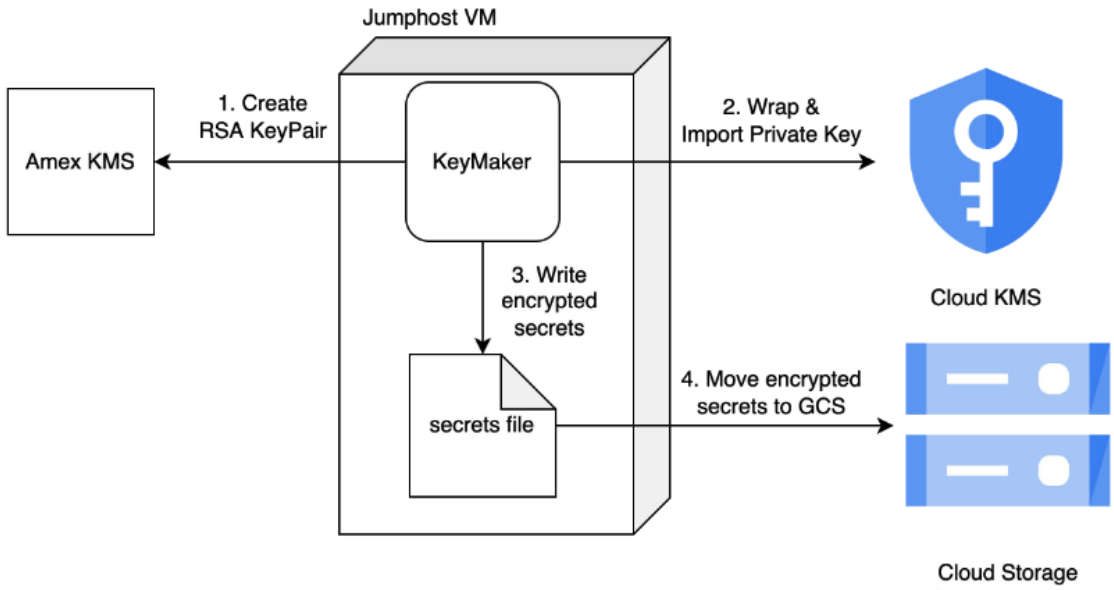
	Capability	Requestor	On Prem System	Source IP / Subnet	GCP Environment	GCP Service / Endpoint	Remarks
1	Data Movement	Tien Q Vo	Silver Big Data Batch Cluster	Silver Batch cluster Data nodes + Dedicated Edge node(lppbd4801agk03.phx.aexp.com)	**E1**	**From Data nodes:** storage.googleapis.com www.googleapis.com **From Edge node:** storage.googleapis.com cloudresourcemanager.googleapis.com www.googleapis.com dl.google.com accounts.google.com	Temporary solution is to use WebProxy. ITSC request **REQ6749595** POA solution is to use Private Service Connect (PSC). Reference Link: https://enterprise-confluence.aexp.com/confluence/x/dJjFJ
2	Data Movement	Tien Q Vo	Gold Big Data Batch Cluster	Big Data Batch cluster subnets + Dedicated Edge nodes	E2	**From Data nodes:** storage.googleapis.com www.googleapis.com **From Edge node:** storage.googleapis.com cloudresourcemanager.googleapis.com www.googleapis.com dl.google.com accounts.google.com	
3	Data Movement	Tien Q Vo	Platinum Big Data Batch Cluster	Big Data Batch cluster subnets + Dedicated Edge nodes	E3	**From Data nodes:** storage.googleapis.com www.googleapis.com **From Edge node:** storage.googleapis.com cloudresourcemanager.googleapis.com www.googleapis.com dl.google.com accounts.google.com	
4	Data Movement	Tien Q Vo	Palladium Big Data Batch Cluster	Big Data Batch cluster subnets + Dedicated Edge nodes	??	From Data nodes: storage.googleapis.com www.googleapis.com From Edge node: storage.googleapis.com cloudresourcemanager.googleapis.com www.googleapis.com dl.google.com accounts.google.com	
5	Data Movement	Tien Q Vo	Silver (Dedicated) Edge Nodes	lppbd4801agk03.phx.aexp.com lppbdsv075.gso.aexp.com lppbdsv575.gso.aexp.com	E1	pubsub.googleapis.com	When data movement jobs complete successfully to move on-premise to data to GCS, we need to publish an event in pub/sub so that data ingestion can be triggered to ingest the data into BQ.
6	Data Movement	Tien Q Vo	Gold (Dedicated) Edge Nodes	need IPs	E2	pubsub.googleapis.com	
7	Data Movement	Tien Q Vo	Platinum (Dedicated) Edge Nodes	need IPs	E3	pubsub.googleapis.com	
8	Data Movement	Tien Q Vo	Palladium (Dedicated) Edge Nodes	need IPs	??	pubsub.googleapis.com	

9	CI/CD E1	Harinadha Naidu Vadlamudi	CI/CD Pipeline		E1	Google Cloud Storage	Hari confirmed he was able transfer artifacts to E1 ingestion Project.
10	CI/CD E2	Harinadha Naidu Vadlamudi	CI/CD Pipeline		E2	Google Cloud Storage	
11	CI/CD E3	Harinadha Naidu Vadlamudi	CI/CD Pipeline		E3	Google Cloud Storage	
12	Portal / Metadata Management	Amit Sharma	E1 Portal (eCP Hosts)	10.9.157.38/23, 10.9.157.37/23	E1	• MDM services hosted in GKE. - will need endpoints (hosted in GCP / Cloud Run or GKE) • Other services on GKE / GCE • Google Catalog APIs https://datacatalog.googleapis.com/	
13	Portal / Metadata Management	Amit Sharma	E2 Portal (eCP Hosts)	10.9.27.108,10.9.27.107	E2	• MDM services hosted in GKE. - will need endpoints (hosted in GCP / Cloud Run or GKE) • Other services on GKE / GCE • • Google Catalog APIs https://datacatalog.googleapis.com/	Do we need one here for Palladium eventually?
14	Portal / Metadata Management	Amit Sharma	E2 Portal (eCP Hosts)	10.13.19.166,10.13.19.165 10.37.35.202,10.37.35.201 10.45.55.194,10.45.55.193	E3	• MDM services hosted in GKE. - will need endpoints (hosted in GCP / Cloud Run or GKE) • Other services on GKE / GCE • Google Catalog APIs https://datacatalog.googleapis.com/	

15	Data Governance	Kyle Dillon McKissack	Collibra / Governance -	need IPs	??	Lumi Portal (eCP) to Collibra (SaaS GCP) Connectivity GCP Google Data Catalog to Metadata Reconciliator (Springboot App) in eCP Connectivity Metadata Reconciliator (Springboot App) in eCP to Collibra (SaaS GCP) Connectivity Details such as endpoint/IPs TDB	Kyle Dillon McKissack& Donovan Hsiehto provide more info.
16	Data Protection	Manisha Gureja	Silver (Dedicated) Edge Nodes	lppbd4801agk03.phx.aexp.com	E1	**OnPrem** • KMS CBIS endpoint: https://securityapi-dev.aexp.com/kms/v2 • KMS CBIS TOKEN endpoint: https://mycaservicese1qonline.webqa.ipc.us.aexp.com/security/digital/v1/application/token **GCP** • cloudkms.googleapis.com • storage.googleapis.com	need to align with NetSec team. Requirement: Onprem edge node to ▪ Generate KEKs from Onprem KMS APIs ▪ Import KEKs (generated Onprem) to GCP KMS. ▪ Import encrypted DEKs to Google Cloud Storage ▪ Reference Link: Data Protection Architecture
17	Data Protection	Manisha Gureja	Gold (Dedicated) Edge Nodes	need IPs	E2	• cloudkms.googleapis.com • storage.googleapis.com	ITSC request #**REQ6764076**
18	Data Protection	Manisha Gureja	Platinum (Dedicated) Edge Nodes	need IPs	E3	• cloudkms.googleapis.com • storage.googleapis.com	
19	Data Protection	Manisha Gureja	Palladium (Dedicated) Edge Nodes	need IPs	??	• cloudkms.googleapis.com • storage.googleapis.com	
20	MDM Integration	Satish Anupindi	ECP containers	10.9.156.88,10.9.156.87	E1	pubsub.googleapis.com	The connectivity from eCP hosted mdm_adapter application to pubsub is required because the non-PII metadata that is gathered from mdm_adapter needs to be transferred to the GCP hosted MDM Cloud SQL as part of the Lumi (next Gen Big Data) project. Satish Anupindi opened an ITSC request RITM2868198
21	MDM Integration	Satish Anupindi	ECP containers	10.9.26.206,10.9.26.205	E2	pubsub.googleapis.com	
22	MDM Integration	Satish Anupindi	ECP containers		E3	pubsub.googleapis.com	

23	BI Work stream	Raunak Rudra	Remote Desktop server access to Tableau servers in GCP In POA environment, required connectivity from AMEX_ALL to Bigquery, GCS and GCP Tableau servers so that developers can create and publish dashboards on Tableaus servers so that users can access them.	Citrix Server	E1	E1 subnet	Citrix Server setup in Progress - TIMS IRD - 9803 (GCT) In POA environment, required connectivity from AMEX_ALL to Bigquery, GCS and GCP Tableau servers so that developers can create and publish dashboards on Tableaus servers so that users can access them.
24			HyperDrive			Pub / Sub	Later
25			PostgreSQL (Hyperdrive) replication for runtime configurations			CloudSQL (PostgreSQL Hyperdrive)	Later
26	DQaaS	Achut Perumbala	eCP containers	10.9.4.82, 10.9.4.83	E1	pubsub.googleapis.com bigquery.googleapis.com MDM (Cloud SQL?)	
27	DQaaS	Achut Perumbala	eCP containers	10.0.90.160, 10.0.90.161	E2	pubsub.googleapis.com bugquery.googleapis.com MDM (Cloud SQL?)	
28	DQaaS	Achut Perumbala	eCP containers	10.13.77.13, 10.13.77.14, 10.37.78.166, 10.37.78.167, 10.45.94.172, 10.45.94.173	E3	pubsub.googleapis.com bigquery.googleapis.com MDM (Cloud SQL?)	
29	DQaaS	Achut Perumbala	Silver dedicated edge nodes	lppbd4801agk03.phx.aexp.com	E1	pubsub.googleapis.com	Opened already #17
30	DQaaS	Achut Perumbala	Gold dedicated edge nodes	?	E2	pubsub.googleapis.com	
31	DQaaS	Achut Perumbala	Platinum dedicated edge nodes	?	E3	pubsub.googleapis.com	
32							

KeyMaker : Key generation and Import architecture flow for Pilot and MVP



GCP to on-prem

Capability	Requestor	GCP Service	On Prem System / Service / Endpoint	On-Prem FQDN's	Questions from PD
Infrastructure	Kasi Viswanadham Vallabhaneni	DataProc / GCE	Nexus Repository Docker Repository	https://ci-repo.aexp.com https://dockerproxy.aexp.com gcprepo.aexp.com	Required for Pilot use cases implementation.
Data Security	Manisha Gureja	Dataproc/Dataflow (for data ingestion jobs that will use hiped library to decrypt data)	On-Prem KMS	**CBIS endpoints:** E1 - KMS CBIS endpoint: https://securityapi-dev.aexp.com/kms/v2 KMS CBIS TOKEN endpoint: https://mycaservicese1qonline.webqa.ipc.us.aexp.com/security/digital/v1/application/token E2 - KMS CBIS endpoint: https://securityapi-qa.aexp.com/kms/v2 KMS CBIS TOKEN endpoint: https://mycaservicese2qonline.webqa.ipc.us.aexp.com/security/digital/v1/application/token E3 - KMS CBIS endpoint: https://securityapi.aexp.com/kms/v2 KMS CBIS TOKEN endpoint: https://mycaservicesonline.web.ipc.us.aexp.com/security/digital/v1/application/token **KMS V2 Service is protected by CBIS** below URI and HTTP methods are submitted through IDaaS potal for CBIS onboarding request (Application ID: 500000272) E1 - https://kms-dev.aexp.com/ E2 - https://kms-qa.aexp.com/ E3 - https://kms2.aexp.com/ • /kms/v2/keys/* GET method • /kms/v2/keysets/*, /kms/v2/keysets GET method • /kms/v?/keys::POST	Is this design for pilot only or MVP? Seems to be different from about diagram from Sulabh Shukla more design aspects coming here. It is not required for MVP1.
		Pub / Sub	Data Transfer Utility		will we be using pub / sub to call back to onPrem? (Satish Anupindi thinks no for MDM). this will be the subscribe this will be bi-directional from above.
		Google Cloud Storage	Data Transfer Utility. ??		may not need this as perhaps GKE or other services will be used. (Patrick S Dillon will talk to leadership) Read from GCS and bring to onPrem for Chatbot
		Big Query			
		Bigtable			
			OneAmex ?? Talk to Ashok K Nair		
		GKE for MDM	eCP - Portal		
		GKE for Data Catalog	eCP - Portal		
		API authentication?	AuthBlue or OKTA		Abhinav Gyan input.
		Pub / Sub	Hyperdrive		Is this needed for MVP
		Cloud Run (Hyperdrive)	Kafka (Hyperdrive)		Cloud Run not in the list for MVP release
					Are there other on-prem endpoints we will need to consider relative to the data movement coming from each of the big data environments?
DQaaS	Achut Perumbala	Cloud Composer	eCP containers	E1: 10.9.4.82, 10.9.4.83 E2: 10.0.90.160, 10.0.90.161 E3: 10.13.77.13, 10.13.77.14, 10.37.78.166, 10.37.78.167, 10.45.94.172, 10.45.94.173	
DQaaS	Achut Perumbala	Cloud Composer	Kafka On-prem		
DQaaS	Achut Perumbala	Cloud DataProc	Kafka On-prem		