Security Architecture - DMP

Introduction

The objective of this document is to provide the program with a clear understanding of the security architecture for the DMP application. The Security Architecture defines the overall Security solution for DMP platform. The solution addresses the requirements as defined in the requirements section. The solution comprises of a number of elements or components, which are partitioned into subsets for implementation. The primary purpose of this section is to communicate the essential elements of the overall Security Architecture and Security solutions so that business implications can be assessed and understood, and so that the design and build activities can proceed. As such, it achieves the following:

· Provides references to security solutions for nonfunctional requirements

· Provides visibility and exposure to other architects (Infrastructure, Application, Security etc.) for peer review.

· Defines the overall security solution to the non-functional requirements.

· It provides a basis for assessment of the overall security solution once implemented.

· Provides the security controls, tools, processes and roadmap for their deployment.

· It describes how the development and deployment of the solution can be phased if this is required to meet business needs and or to meet technology constraints.

This document is relevant to all key stakeholders on the project:

· ADDA Director General

· ADDA Project Management Team

· Project consultants, architects and support personnel

· G42 Cloud Project Management Team

· G42 Cloud Architects and Development Teams

This section is not a supplement for the infrastructure or network architectures and therefore should not be considered as such. For infrastructure, data and network architectures, please refer to their appropriate sections within this document.

The structure of the document follows the G42 Cloud Tenant/Shared Responsibility Matrix structure. The Security Architecture follows the following structure:

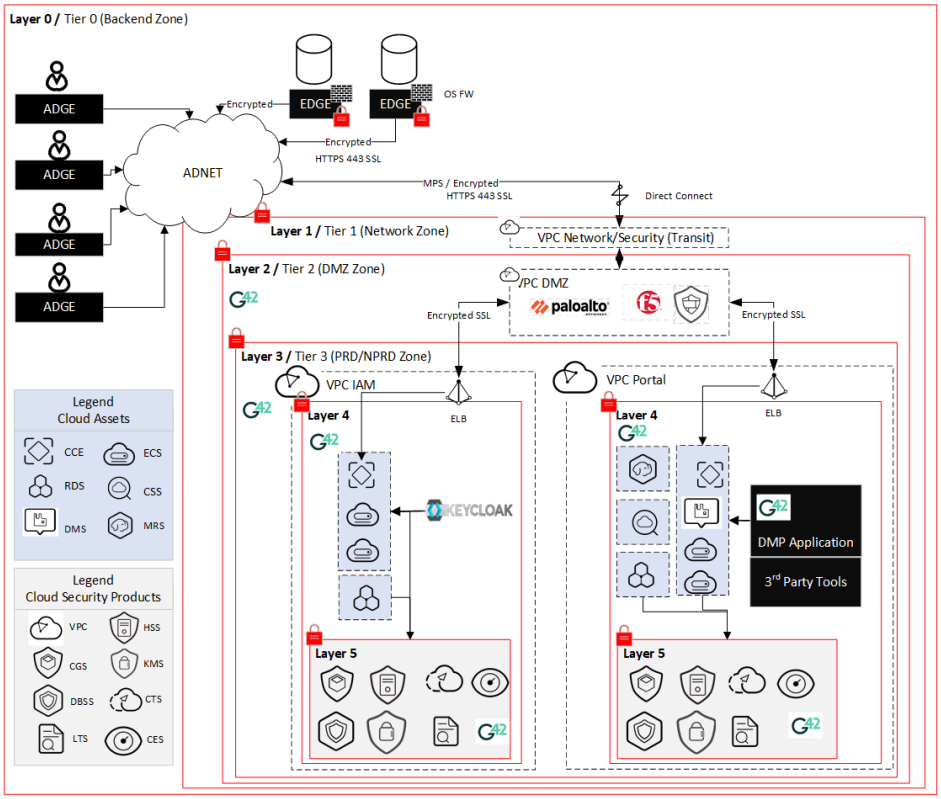
· Security Architecture Principles

- Security Architecture Requirements Design Mapping
- Security Overview
- Security Controls Mapping
- Compliance Security
- Tenant Security
- Infrastructure Security
- Application Security
  - DMP Application
  - EDGE Application
- Physical Security

Security Architecture Overview

Security Layers

The security architecture for the DMP program incorporates security layering and security zoning. The multiple security layers and zones are illustrated in the diagram below showing two VPC's inside the Production Enterprise Project (ie. PROD). NOTE: There are more VPC, below only two of the Production VPC are used for illustration purposes only.



· **Layer 0 -** External Layer: This layer is external to the G42 Cloud and is the security layer encompassing ADNET, ADGE's, the EDGE applications.

· **Layer 1** – Outer Layer: This is also known as the outer-perimeter layer, and references the connectivity between the ADNET and the G42 Cloud a MPLS/Direct Connect integration over an encrypted channel via the Cloud Gateways.

· **Layer 2** – Inner Perimeter Layer: This is the inner-perimeter of the cloud and is comprised of two VPC, the Transit VPC and the DMZ VPC.

· **Layer 3** – **Infrastructure -** Network Segmentation Layer: This layer concerns itself primarily with VPC segmentation, non security grouped cloud assets, such as DBSS, ELB, AS and etc. There are multiple VPCs and their connectivity is enforced by a secure channel via a VPC peering.

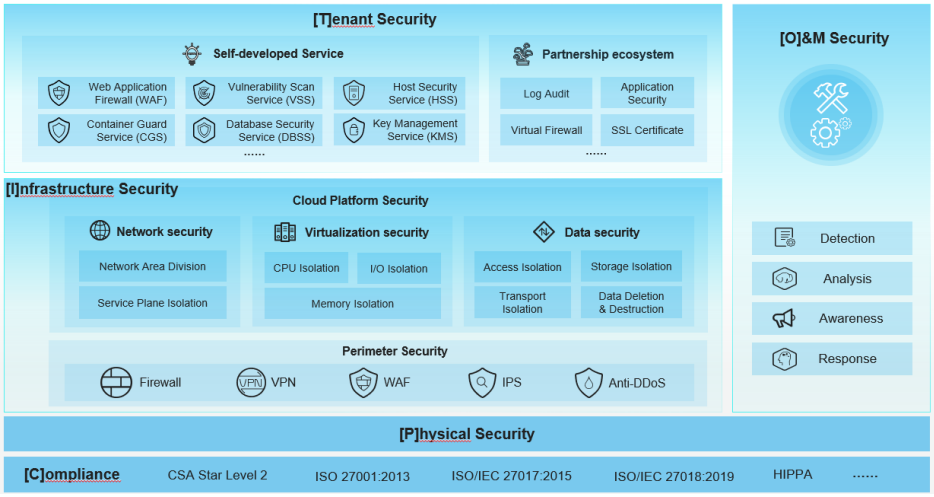
· **Layer 4** – **Infrastructure** Security Group Layer: This layer is a further sub-network segmentation layer. In this layer, logical components of the cloud assets are grouped for additional security segmentation.

· **Layer 5** – **Tenant** Security Layer: This layer concerns itself with applying security controls and products on the security assets, and inside the security groups.

The strength of this architecture approach is to identity security zones, from least trusted to highly trusted. The security layering provided different types of security controls in each layer, thereby increasing the security posture of the whole solution with every added layer of security.

Architecture Structure

In the Security Layers diagram above, there are references to infrastructure and tenant security domains. The diagram below shows the G42 Cloud shared responsibility matrix with emphasis on the five cloud security domains:

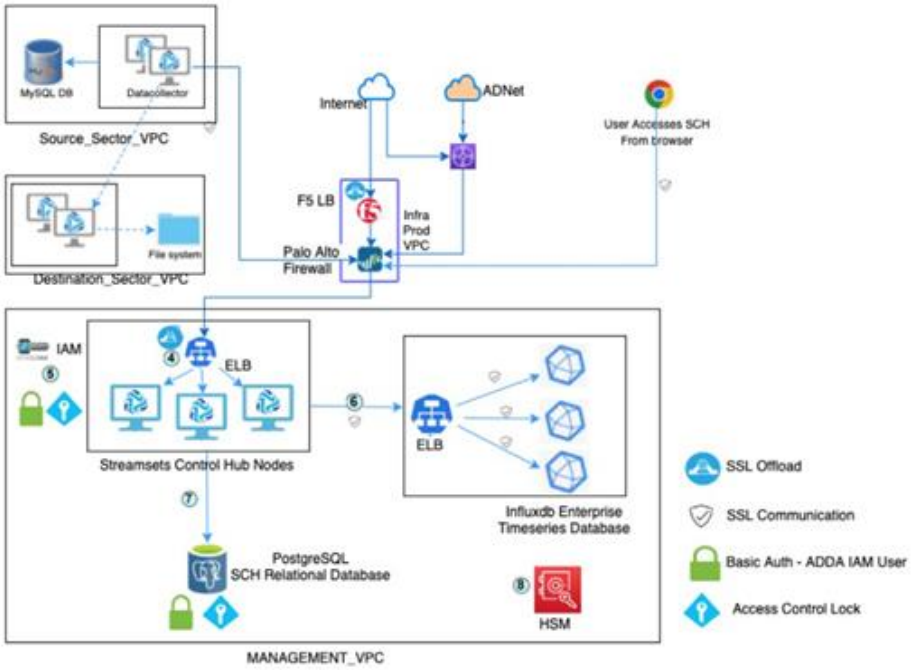


The above matrix will be used to described each of the core security domains as follows:

- Tenant Security – this is where all the security services provided by G42 Cloud exist. Any 3rd party tools will also be defined and descried here.
- Infrastructure Security – these are the Cloud Service Provider security controls of the platform itself. These services are configurable and will be provided to ensure security is adhered to at the platform level.
- Physical Security – this is the security of the physical devices that underpin the cloud platform and is purely within the domain of the Cloud Service Provider, i.e. G42 Cloud.
- O&M Security – this is a service provided by the G42 Cloud SOC team and is used to ensure that the cloud platform is secure, this does not include the customers SOC requirements.
- Compliance – this is the list of compliances that the G42 Cloud security adheres to. Additional compliances, such as ‘benchmarks’ will be explained and applied here.

2.3 Streamsets Security

Below sections depicts the various security controls considered in Data Integration solution



· ADDA User accesses the StreamSets Control Hub via Browser over SSL

· SSL Termination at F5 Load Balancer

· F5 Load Balancer Routes to an Internal Load Balancer

· Internal Load Balancer Routes to one of the SCH Nodes

· SCH Nodes work with KeyCloak IAM for Authentication and Authorization

· SCH Nodes communicate with Influx DB via an Internal Balancer over SSL using self-signed certificates

· SCH Nodes store/retrieve pipeline metadata in PostgreSQL DB

· All the certificates required for internal and external communication would be deployed from HSM

Security Design and Requirements Mapping

High Level Requirements Mapping

Below is a high-level listing of the core Security Domain requirements defined for the DMP project. The content in this table is high level and is used as a design guiding principle's in order to ensure that the core and fundamental requirements for the program are captured.

#	Security Domain	High Level Security Requirements
1	Identity and Access Management	Allow only trusted identities to access the DMP services. Consumers: DMP administrators, ADGE Applications, ADDA Applications Providers: Applications, Data Collectors, Provisioning Agents.
2	Host/Devices	Hosts must have intrusion detection, antivirus protection capabilities and security hardening Any additional controls (packet sniffers, EDRs, NDRs) that ADDA may require will be provided by ADDA and not the project. All host machines will be hardened and vulnerability analysis applied and any Critical, High severity issues remediated.
3	Infrastructure	External network access only to be allowed for Technical Support, via a VPN connection to the G42 Console. No public network access to the DMP consumers, all access with be via ADNet for all consumers. Use of network segmentation supported by G42 Cloud VPC technology. Network traffic from ADGE to G42 Cloud hosting DMP is to be encrypted Access points to DMP will be primarily via the ADNET MPLS network (with the exception of (1) above). All traffic to and from the ADNET for the services provided by DMP is to be via a Network Landing zone and DMZ zone.
4	Application	DMP Portal - Web based application.
5	Data Protection	Data at Rest: Must be encrypted Data in Motion: Must be encrypted Data is encrypted in-Transit using SSL/TLS
6	Incident Response and Monitoring	The data sources to be available for integration with ADDA's SOC requirements.

NFR-SE : Security Requirements

The following are the platform security requirements.

NFR	NFR Guideline	Security	Requirements	G42 Support Yes/No	Comments	Supporting Service
NFR-SE001	Security – Privacy	Security	Required security controls need to be in place between CCE clusters in DMZ zone and Internal zone	Yes	The CCE cluster is placed in a separate VPC and the inter VPC traffic is access control and monitored using Palo Alto firewall.	CCE, SG,NACL
NFR-SE002	Security – Privacy	Security	The Cloud platform's sector-facing API endpoints must be forcibly secured with SSL. The SSL certificate must be signed by a commonly trusted certificate authority (CA). It must not be a self-signed certificate.	Yes	ELB ingress supports configuring SSL certificates.	All G42 Cloud Platform resources APIs have SSL certificates. ELB, CCE

NFR-SE003	Security - Threat Management	Security	MVP environment must be protected with anti-virus / anti-malware/other service protection software on all underlying DMP/Other apps/systems.	Yes	The worker nodes are deployed with Host Security Service and supports the deployment if AV per the security polices of DMP.	HSS
NFR-SE004	Security – Privacy	Security	API gateway's or HTTP proxy servers should have dedicated SSL certificates	Yes	Certificates are provided by ADDA	ELB
NFR-SE005	Security - Threat Management	Security	Denial of Service Attacks and IP spoofing should be considered for Microservices and external networks	Yes	The Anti DDOS is part of security architecture. IP spoofing protected by G42 Platform.	ADDA provides Anti DDOS solution
NFR-SE006	Security – Privacy	Security	Secrets are stored in G42 approved key vault	Yes	KMS is used to store encryption keys.	KMS
NFR-SE007	Security – Compliance	Security	The environment meets UAE data protection laws.	Yes	Compliancy check by ADDA for Standards like NESA	G42 Cloud | The Leading Provider of Cloud & AI Solutions in UAE & The Middle East

NFR-SE008	Compatibility - Integration	Security	Weekly/Daily security updates to be applied without impacting overlaying microservices	Yes	Infrastructure design supports it.	DevSecOps to be implemented[GS1]
NFR-SE009	Security - Threat Management	Security	Monitoring to be in place for Kubernetes infrastructure for both active threats and potential security risks	Yes	Kubernetes environments are monitored using AOM service.	AOM, CES[GS2] R
NFR-SE010	Security – Privacy	Security	Limit the open ports between the cluster and external nodes (Example - Storage etc.) as per the requirements	Yes	Infrastructure design supports it.	SG, NACL, NG-Firewall
NFR-SE011	Security – Privacy	Security	Certificate Authority (CA) are on the private network for environment	Yes	CA is part of security architecture.	ADDA provides all the required Certificates
NFR-SE012	Security – Privacy	Security	Encrypted volumes should be used for data-at-rest	Yes	KMS keys are used to encrypt data at rest.	KMS[GS3]
NFR-SE013	Security - Access Control	Security	Firewalls and network access controls should be in place for data-in-motion	Yes	Palo Alto, F5 firewalls are used.	Palo Alto, F5

NFR-SE014	Security – Privacy	Security	API communication in the CCE cluster is encrypted with TLS	Yes		ELB, Certificates are provided by ADDA
NFR-SE015	Security - Access Control	Security	Environment will define and support a mechanism to manage identities	Yes	G42 cloud IAM provides the identities for infrastructure management roles.	IAM
NFR-SE016	Security – Privacy	Security	Scanning of container Images and code for any vulnerabilities should be in place	Yes	Harbor to be used as the private image repository of DMP platform.	CGS
NFR-SE017	Security - Access Control	Security	Platform will have the capability to grant, authenticate and revoke access across platform components, with a mechanism to identify and verify users	Yes		IAM

NFR-AP : Application Security Requirements

The following are the compliance requirements for Application Security

NFR	NFR Guideline	Platform Component	Requirements	G42 Support Yes/No	Comments	Supporting Service

NFR-AP001	Security – Privacy	Security	Store Database Credentials and API keys Secure in KMS	Yes	G42 Have the Native cloud Service supporting that	KMS[GS4]
NFR-AP002	Security – Privacy	Security	DevSecOps approach is used for DMP application development	Yes	G42 Cloud will 3rd party product and tools to cater for a DevSecOps solution. This solution will require a DVE bastion host implementation. The deisgn is yet to be confirmed.	3rdparty tools/application VPC, Bationhost ZeroTrust
NFR-AP003	Security – Privacy	Security	DMP portal is protected by ADDA approved CA certificate.	Yes	G42 cloud supports CA certificates provided by ADDA.	Yes, certificates provided by ADDA.
NFR-AP004	Security - Access Control	Security	For DMP application any authentication activities, whether successful or not, should be logged	Yes	G42 have the Native services to support Logging, but No SIEM service provided	LTS , CTS
NFR-AP005	Security – Privacy	Security	HTTPS must be applied to any authentication pages as well as to all pages after the user is authenticated.	Yes	G42 cloud will accomidate any 3rd party CA's. ADDA should provide the Certificates	ELB Ingress

NFR-AP006	Security – Privacy	Security	For all DMP pages requiring protection by HTTPS, the same URL should not be accessible via the insecure HTTP channel.	Yes	G42 cloud will accomidate any 3rd party CA's. ADDA should provide the Certificates	ELB Ingress and self-signed certifcates.
NFR-AP007	Security – Privacy	Security	Name on the HTTPS certificate should match the FQDN of the website. The certificate itself should be valid and not expired.	Yes	G42 cloud support 3rd party provided CA's. ADDA is to provide naming conventions of the certificates.	Yes
NFR-AP008	Security – Privacy	Security	No credentials to be stored directly within the application code	Yes	G42 cloud does not provide support for code review	Yes. Code scanning is applied using SonarQube. Manual verification is also applied to ensure no credentials are hard coded in code.

NFR-AP009	Security – Privacy	Security	User session tokens must be generated by secure random functions and must be of a sufficient length so as to withstand analysis and prediction	Yes	The tokens are provided for each session using Session IDs with a minimuam length of 16 characters. These tokens are managed by the codifed DMP application and provided in a JSON Sesison ID (encrypted).	Yes. DMP codified JSON session IDs.
NFR-AP010	Security – Privacy	Security	DMP application logs should be stored and maintained appropriately to avoid information loss or tampering by intruder. Log retention should also follow the retention policy set forth by the organization to meet regulatory requirements and provide enough information for forensic and incident response activities.	Yes	Logs from the DMP application are listed in the SOC integration section of this document.	Yes. Filebeat logs are provided by the DMP application using ELK.

NFR-AP011	Security – Privacy	Security	All access decisions for DMP will be based on the principle of least privilege	Yes	Least privilege Principle exist with G42 IAM	IAM

NFR-DC : Digital Certificates Requirements

Digital Certificates provide a means of proving identity. With a digital certificate, it can be assured the claiming identity is authentic. Digital certificates, bind an identity to a pair of electronic keys that can be used to encrypt and sign digital information. A Digital Certificate makes it possible to verify someone's claim that they have the right to use a given key, helping to prevent people from using phony keys to impersonate other users. Used in conjunction with encryption, digital certificates provide a more complete security solution, assuring the identity of all parties involved in a transaction

DMP platform when linked to other system should use digital certificates to identify the claimed component

NFR	NFR Guideline	Platform Component	Requirements	G42 Support Yes/No	Comments	Supporting Service
NFR-DC001	Security - Access Control	Security	DMP environment must use ADDA internal digital certificates for authentication and secure transmission on ADDA networks	Yes.	G42 Cloud supports all certificates provided by ADDA for external communications (i.e. external to cloud)	Yes. ADDA provided certifcates. Certificate Management needs to be introduced as a product.

NFR-NT : Network Security Requirements

NFR	NFR Guideline	Platform Component	Requirements	G42 Support Yes/No	Comments	Supporting Service

NFR-NT001	Security – Privacy	Network	DMP tenant are isolated from other tenants across network, storage, PaaS services etc. and allowed where needed.	Yes	G42 Cloud is a multi-tenant platform. Tenant resources such as compute, network, storage and PaaS services are isolated from other tenants and platform ensures that no other tenant can access/view the resources of other tenant. The platform offers shared infrastructure with logical isolation on hypervisor level.	VPC, ECS, RDS, MRS, IMS, CCE, ELB
NFR-NT002	Security - Access Control	Network	Kubernetes network policies are to be in place to control permissible types of traffic to, from and between pods.	Yes	CCE has Kubernetes-based network policy feature, allowing network isolation in a cluster by configuring network policies.	CCE
NFR-NT003	Security - Access Control	Network	Compute clusters is deployed with IP addresses that are independently routed.	Yes	The DMP is deployed on CCE cluster which is deployed in VPC, an isolated independent network segment. The routing of a VPC can be configured independently.	VPC

NFR-NT004	Security – Privacy	Network	Environment should support virtual networks that are fully isolated and not routable externally (Example Adnet)	Yes	The scope of Service and Container networks of CCE cluster is cluster based. These IP can only be accessed within the cluster unless exposed using the Nodeport/Load balancer.	CCE, VPC
NFR-NT005	Security – Privacy	Network	Environment configurations must exist that can reside only on isolated virtual networks and without having any public IP address or internet routing.	Yes	VPC network is used which is an isolated network segment by default. This is no public IP connection unless an Elastic IP EIP is bound to a resource.	VPC, ELB
NFR-NT006	Performance - Latency & Throughput	Network	Network latency between ADGE network and DMP clusters is below 5ms latency.	Yes	The network latency between ADNET and G42 cloud is less than 5ms over MPLS connection	Direct Connect
NFR-NT007	Security – Privacy	Network	Ingress traffic, Egress traffic, Pod-to-pod traffic and Management traffic (API server and user) are isolated from each other	Yes	Control plane and data plane traffic are isolated from each other in CCE cluster.	CCE

NFR-NT008	Performance - High availability	Network	CCE cluster is deployed with name resolution services in HA mode	Yes	CCE Clusters are deployed in HA which each cluster having 3 master nodes and more than 2 worker nodes. CCE provides a DNS add-on Service named coredns to automatically assign DNS domain names for other Services. CoreDNS is a DNS server that chains plugins and provides Kubernetes DNS Services	CCE
NFR-NT009	Security – Privacy	Network	Namespace components to be defined for components	Yes	DMP components such as portal, data-sharing are deployed in isolated namespaces	CCE
NFR-NT010	Compatibility - Data Exchange	Network	Platform should support standard kubernetes Container Network Interface (CNI) class	Yes	CCE supports CNI plug-ins	CCE
NFR-NT011	Compatibility - Data Exchange	Network	The Platform will always use open standards for data exchange	Yes	The DMP platform is built on top of G42 Cloud CCE platform which based on opensource kubernetes.	CCE

NFR-NT012	Performance - High availability	Network	Front end API Gateway for microservices is deployed with HA design	Yes	DMP API gateway uses dedicated ELB as ingress in HA mode.	ELB, CCE

NFR-CM : Compute Security Requirements

NFR	NFR Guideline	Platform Component	Requirements	G42 Support Yes/No	Comments	Supporting Service
NFR-CM001	Scalability & Elasticity - Scaling	Compute	Compute environment for DMP should automatically resize of the Cluster/node pools.	Yes	Horizontal Pod Auto scaling HPA and Cluster Auto scaling CA are supported on CCE.	CCE
NFR-CM002	Compatibility - Integration	Compute	All nodes in DMP clusters uses the same Container Runtime type and updated version	Yes	All CCE worker nodes use Docker 18.09.0 as runtime engine.	CCE
NFR-CM003	Compatibility - Integration	Compute	Underlying DMP CCE Virtual machines are up-to-date with latest patch and OS version	Yes	On delivery of the releases into production, all updates and patches are provided. In production, G42 Cloud Managed Services to ensure updates are applied and maintained.	CCE, ECS, MRS, RDS

NFR-CM004	Compatibility - Integration	Compute	DMP compute environment must have latest kubernetes version and OS patch	Yes	CCE releases only odd major Kubernetes versions, such as v1.19, v1.21, and v1.23. Kubernetes releases a major version in about three months. CCE follows the same frequency as Kubernetes to release major versions. To be specific, a new CCE version is released about three months after a new Kubernetes version is released in the community. The policy for fixing major OS vulnerabilities is consistent with the cluster patch upgrade policy.	CCE
NFR-CM005	Compatibility - Integration	Compute	DMP compute environment must have all required version of underlying databases types and storages	Yes	DMP platform consumes MySQL 8.0, Elasticsearch 7.9 and MRS 3.1.0. These databases are available as managed services in G42 Cloud.	RDS, MRS, CSS
NFR-CM006	Scalability & Elasticity - Elasticity	Compute	The DMP Kubernetes cluster must be appropriately sized to accommodate the number of services to be run.	Yes	DMP Kubernetes clusters can scale up to 200 nodes. Application team has confirmed the requirement to be 50 nodes cluster.	CCE

NFR-CM007	Performance - High availability	Compute	Infrastructure solutions (example server, storage etc.) should have a redundancy for sub-systems (N+1) designed to eliminate and manage for single point of failure.	Yes	1. More than 2 worker nodes are used in CCE cluster and anti-affinity policies are used to deploy then on different physical machines to avoid SPOF.	CCE, RDS, CSS, MRS
NFR-NT008	Performance - High availability	Network	CCE cluster is deployed with name resolution services in HA mode	Yes	1. Primary/Stand by version of RDS is used and deployed across two AZs to ensure HA.	CCE
NFR-NT009	Security – Privacy	Network	Namespace components to be defined for components	Yes	1. CCE control plane, CSS and MRS are also deployed in HA mode.	CCE
NFR-CM008	Security – Privacy	Compute	Data written to CCE etcd database should be encrypted	Yes	CCE has configured static encryption for secret resources. The secrets created by users will be encrypted and stored in etcd of the CCE cluster.	CCE

NFR-CM009	Compatibility - Integration	Compute	Underlying DMP Compute platform should have kubernetes version up to date with the supported N-2 versions.	Yes	latest kubernetes version is 1.25. CCE supports v1.21 as of now. Version v1.23 is currently available in Beta and will be commercially available within 3 months.	CCE
NFR-CM010	Performance - High availability	Compute	Microservices PODs should be distributed across 2 worker node or more as required by Microservices design	Yes	POD anti-affinity polices are configured to deploy pods on different work nodes.	CCE

NFR-ST : Storage Security Requirements

NFR	NFR Guideline	Platform Component	Requirements	G42 Support Yes/No	Comments	Supporting Service
NFR-ST001	Recoverability & Availability - Data recovery	Storage	DMP environment should be tested with data backup and restore services	Yes	Infrastructure design supports it.	CBR, RDS
NFR-ST002	Performance - Latency & Throughput	Storage	DMP backend storage should be capable of providing the following Latency and IOPS requirements - Latency (Min=5ms, recommended=1ms), IOPS (Min=5K, Recommended=20K)	No	Backup is stored on OBS which offers 10 ms. The parallel file system of OBS supports million level IOPS.	OBS

NFR-ST003	Compatibility - Data Exchange	Storage	Data sources and Data targets for DMP are defined and documented	Yes	Non infrastructure requirement and should be part of DMP application architecture document.	
NFR-ST004	Compatibility - Data Exchange	Storage	DMP platform should support dynamic volume provisioning without impacting existing volumes/application	Yes	CCE supports the dynamic provisioning of persistent volumes.	EVS, CCE
NFR-ST005	Compatibility - Data Exchange	Storage	DMP platform need to support standard kubernetes Container Storage Interface (CSI)	Yes	CCE supports CSI	CCE
NFR-ST006	Recoverability & Availability - Fault Tolerance	Storage	DMP platform should have ability to recover from various type of storage failures scenarios such as machine failure, single disk failure, storage array failure, storage controller failure and split-brain scenarios.	Yes	EVS disk is they underlying technology used which prevents single point of failure for storage media.	EVS, CCE
NFR-ST007	Compatibility - Integration	Storage	Compliance to GDPR regulations and ability to remove user data on-demand.	Yes	The requirement should be met by the DMP application. Infrastructure design supports it.	

NFR-ST008	Compatibility - Integration	Storage	DMP platform has the ability for data provider to have a unified data ingestion interface for multiple data sources	Yes	The requirement should be met by the DMP application. Infrastructure design supports it.	
NFR-ST009	Traceability & Auditability – Immutability	Storage	The DMP platform will ensure data stored in the system is tamper-proof	Yes	This is part of DMP security design document.	

NFR-MAO : Monitoring and Alarming Security Requirements

NFR	NFR Guideline	Platform Component	Requirements	G42 Support Yes/No	Comments	Supporting Service
NFR-MA001	Performance - Monitoring	Monitoring, alerting, logging, traceability	DMP CCE environment should be configured for monitoring with basic up and down notification of the platform	Yes	Cloud Eye Service is used to provide basic monitoring of cloud infrastructure services	AOM, CES
NFR-MA002	Performance - Monitoring	Monitoring, alerting, logging, traceability	DMP CCE environment should be configured for alerting with basic email notification	Yes	Cloud Eye Service supports the alarm configurations. AOM services allows to configure alarms for the container workloads	CES, AOM, SMN

NFR-MA003	Performance - Monitoring	Monitoring, alerting, logging, traceability	All data and network traffic should be traceable from source to destination and logging should be enabled for future investigation on identification of unauthorized data changes	Yes	The network traffic is access controlled on Palo Alto firewall. Service level logs can be configured on CCE service logs collected on AOM.	3rd party tool, AOM
NFR-MA004	Performance - Monitoring	Monitoring, alerting, logging, traceability	G42 monitoring platform should allow real time monitoring of infrastructure, process to enable informed decisions by analyzing patterns, logs, behavior etc.	Yes	Cloud Eye Service provide basic monitoring of cloud infrastructure services	CES
NFR-MA005	Traceability & Auditability - Auditability	Monitoring, alerting, logging, traceability	Distributed tracing of requests or transaction to be tested as it travels through the application that is being monitored	Yes	Infrastructure design supports the application to achieve it.	

NFR-MS : Application Security Requirements

NFR	NFR Guideline	Application	Requirements	G42 Support Yes/No	Comments

NFR-MS001	Performance - High availability	Application	In case of worker node down POD deployment request, control-plane and cluster communication are within satisfactory timelines	Yes	PODs are redeployed. The timeline needs to be tested by the application.
NFR-MS002	Resilience - Failures	Application	PODs in the DMP platform support self-healing mechanism for PODs which are unresponsive.	Yes	failed PODs replaced with fresh new pods.
NFR-MS003	Security – Privacy	Application	Container Image registry (retrieve and store images) should be on the private network for DMP platform	Yes	Harbor to be used as the private image repository of DMP platform.
NFR-MS004	Performance - Latency & Throughput	Application	End to End Latency and IOPS are must across Compute/Network/Storage/App/MRS/MySQL etc. and meets satisfactory write and read frequency	Yes	latency, IOPS requirements to be given and comparison to be made.
NFR-MS005	Compatibility - Federation	Application	The DMP platform allows all integration patterns interfaces and use an enterprise integration platform (except for tightly coupled components that are non-reusable elsewhere)	Yes	
NFR-MS006	Performance - Latency & Throughput	Application	Maximum satisfactory response time to be experienced for each distinct type of user-computer interaction (2 seconds)	Yes	Infrastructure design supports the application to achieve it.
NFR-MS007	Reusability – Modular Design	Application	DMP Components will be loosely coupled to allow for replacing them with least amount of effort and time	Yes	Infrastructure design uses CCE which supports the application to achieve it.

NFR-MS008	Reusability - Configurability	Application	All components and layers of the MVP architecture (such as frontend channels, integration, backend systems, etc.) will be configurable	Yes	

NFR-TST : Testing Security Requirements

NFR	NFR Guideline	Testing	Requirements	G42 Support Yes/No	Comments	Supporting Service
NFR-TE001	Testability - Scriptable	Testing	SIT and UAT for developers/operations is performed for DMP environment with scriptable test cases	Yes	To be performed by G42 delivery team	
NFR-TE002	Testability - Scriptable	Testing	DMP environment is tested with data requirements (object storage etc.) and data sources required connectivity	Yes	To be performed by G42 delivery team	
NFR-TE003	Testability - Scriptable	Testing	Storage IOPS read and write test results are documented as part of testing	Yes	To be performed by G42 delivery team	
NFR-TE004	Testability - Scriptable	Testing	Validate MVP product is not exposed to Internet as part of testing	Yes	To be performed by G42 delivery team	
NFR-TE005	Testability - Scriptable	Testing	DMP environment should be tested with end to end connectivity testing from one of the ADGE	Yes	To be performed by G42 delivery team	
NFR-TE006	Testability - Scriptable	Testing	CCE node's HA should be tested as part of MVP environment	Yes	To be performed by G42 delivery team	

NFR-TE007	Testability - Scriptable	Testing	Microservices are tested for isolated functionality	Yes	To be performed by G42 delivery team	
NFR-TE008	Testability - Scriptable	Testing	Deployed microservices are tested for scalability at the POD level.	Yes	To be performed by G42 delivery team	
NFR-TE009	Testability - Logging	Testing	DMP Platform must have logs implemented, that will provide what and where the error occurs	Yes	To be performed by G42 delivery team	
NFR-TE010	Testability - Logging	Testing	Reliability of the DMP platform is tested through forced failover testing with simulated outages	Yes	To be performed by G42 delivery team	

NFR-PL : Platform Security Requirements

NFR	NFR Guideline	Platform	Requirements	G42 Support Yes/No	Comments	Supporting Service
NFR-PL001	Performance - High availability	Platform	DMP environment should be tested with 100 concurrent end users performing operations	Yes	To be performed by G42 delivery team	
NFR-PL002	Operability – Supportability	Platform	The DMP platform will be easy to maintain and extend the features	Yes	To be performed by G42 delivery team	

[GS1]Do you have this in place today?

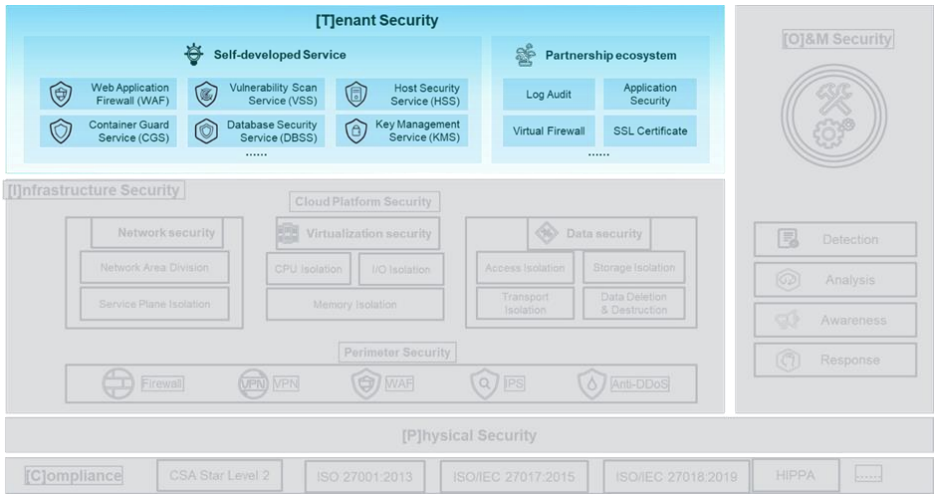
[GS2]Is G42 are doing threat management and threat modeling?

[GS3]Is solution available?

[GS4]Is the solution available in G42 for database encryption and API Keys?

Tenant Security

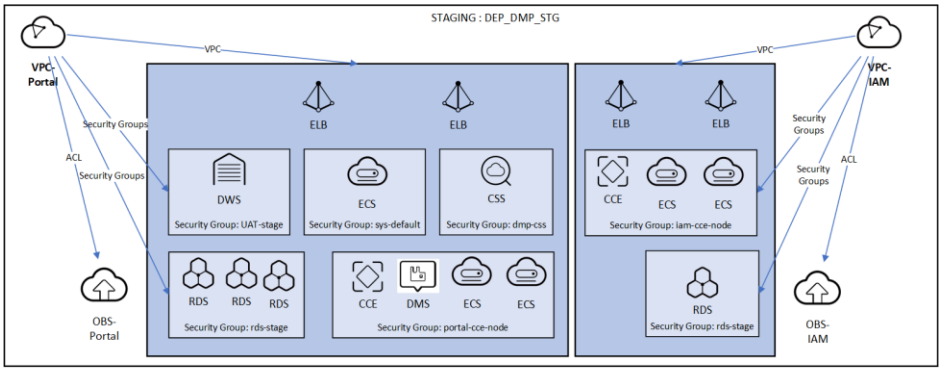
The tenant domain security is associated with tenant security functions and features based on the tenant services provided for DMP. The diagram below shows the broad set of tenants security services. The diagram below shows where Tenant Security is placed with reference to the Architecture Structure using the Share responsibility matrix.

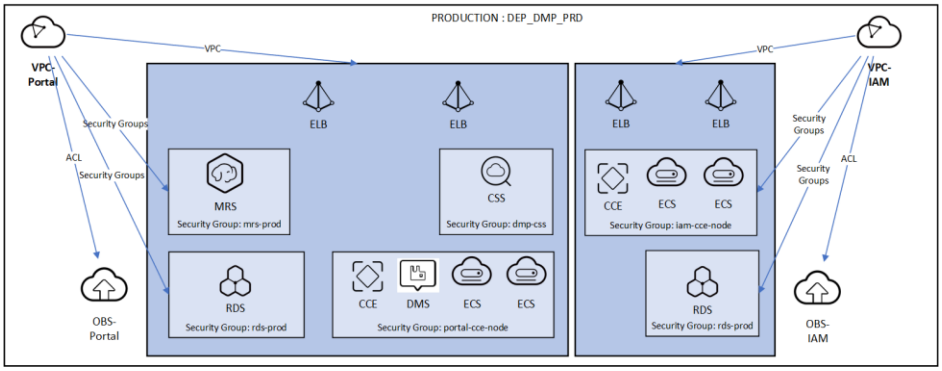


The tenant space utilizes a number of tenant assets allocated to the DMP infrastructure. These are listed below:

- ECS - Elastic Compute Service
- RDS - Relational Database Service
- CCE node - Cloud Container Engine
- OBS – Object Storage Service
- MRS - MapReduce Service
- DWS Cluster – Data Warehouse Service
- CSS – Cloud Search Service

The diagram below depicts all the main/core cloud assets deployed in the tenant space for DMP for staging and production.





Furthermore, the G42 Cloud native Tenant Security Services used for the DCD infrastructure deployment are as follows:

- HSS – Host Security Service
- IMS – Image Management Service
- DBSS – Database Security Service
- CGS – Container Guard Service
- CTS – Cloud Trace Service
- LTS – Log Tank Service
- KMS – Key Management Service

Asset: ECS - Elastic Compute Service – Security Controls

Elastic Compute Service (ECS) provides self-service virtual computing resources that tenants can subscribe on demand. Its cloud server instances, each of which is a VM, are virtual computing environments that include basic server components: CPUs, memory, an operating system, hard disks, and bandwidth. Tenants have administrator permissions for the instances that they create, and can mount hard disks, add NICs, create images, deploy environments, and perform other basic operations.

For DMP there are multiple deployments of ECS in both staging and production environments.

#	Env	Asset Name	Asset	VPC location	Security Group Settings (if inside a security group, please specify)	Security Controls
1	PRD	ecs-dmp-prod-proxy-server-01	ECS	vpc-adda-dep-dmp-iam-production	cce-dmp-prod-iam-cce-node	• **HSS** : Host Security Service • **IMS**: Image Hardening • **Network** Platform Hardening • **IP/MAC** Spoofing protection • **Security Groups** • **Remote Access** • **IAM/RBAC** access management
2	PRD	ecs-dmp-prod-proxy-server-02	ECS	vpc-adda-dep-dmp-iam-production	cce-dmp-prod-iam-cce-node	
3	PRD	ecs-dmp-prod-jump-server	ECS	vpc-adda-dep-dmp-portal-production	cce-dmp-prod-portal-cce-node	
4	PRD	ecs-dmp-prod-edge-registry	ECS	vpc-adda-dep-dmp-portal-production	cce-dmp-prod-portal-cce-node	
5	STG	ecs-dmp-stg-jump-server	ECS	vpc-adda-dep-dmp-portal-stage	cce-dmp-stg-portal-cce-node	
6	STG	ecs-dmp-stg-proxy-server-01	ECS	vpc-adda-dep-dmp-iam-stage	cce-dmp-stg-iam-cce-node	
7	STG	ecs-dmp-stg-proxy-server-02	ECS	vpc-adda-dep-dmp-iam-stage	cce-dmp-stg-iam-cce-node	
8	STG	Dynatrace-POC	ECS	vpc-adda-dep-dmp-portal-stage	Sys-default	
9	STG	ecs-dmp-stg-edge-registry	ECS	vpc-adda-dep-dmp-portal-stage	cce-dmp-stage-portal-cce-node	
10	UAT	ecs-dmp-uat-jump-server	ECS	vpc-adda-dep-dmp-portal-uat	cce-dmp-uat-portal-cce-node	
11	UAT	ecs-dmp-uat-sftp-01	ECS	vpc-adda-dep-dmp-portal-uat	sg-UAT-ecs	
12	UAT	ecs-dmp-uat-edge-02	ECS	vpc-adda-dep-dmp-portal-uat	sg-UAT-ecs	
13	UAT	ecs-dmp-uat-edge-03	ECS	vpc-adda-dep-dmp-portal-uat	sg-UAT-ecs	
14	UAT	ecs-dmp-uat-oracle-04	ECS	vpc-adda-dep-dmp-portal-uat	sg-UAT-ecs	

15	UAT	ecs-dmp-uat-erwin-05	ECS	vpc-adda-dep-dmp-portal-uat	sg-UAT-ecs	
16	UAT	ecs-dmp-uat-edge-registry	ECS	vpc-adda-dep-dmp-portal-uat	cce-dmp-uat-portal-cce-node	
17	QA	ecs-dmp-qa-jump-server	ECS	vpc-adda-dep-dmp-portal-qa		
18	QA	ecs-dmp-qa-edge-registry	ECS	vpc-adda-dep-dmp-portal-qa	cce-dmp-qa-portal-cce-node	

ECS provides multiple layers of protection and assurance, including host operating system security, VM isolation, and security groups. With its comprehensive security design covering virtual machines, hosts, and the networks that connect them, the service offers users a secure, reliable, user-friendly, and high-performing application environment.

ECS Security features and hardening:

- **HSS Host Security Service**:
  - Refer to information in Section on HSS – Host Security Service.
- **Image hardening**:
  - Refer to information in Section on IMS – Image Management Service.
- **Network and platform isolation:** On the network layer, a virtual switch provided by the hypervisor on each host is used to configure VLAN, VXLAN, and ACL settings to ensure that the VMs on that host are logically isolated. Conventional physical devices, mainly routers and switches, are still used to physically isolate different hosts.
- **IP/MAC address spoofing protection**: To avoid network issues that may occur if users change their IP or MAC addresses at will, IP and MAC addresses are bound together using DHCP snooping. Spoofing is further prevented by using IP Source Guard and dynamic ARP inspection (DAI) to filter out packets from unbound addresses.
- **Security groups:** Security groups containing multiple VMs to enable those VMs to access each other while maintaining isolation from other VMs. By default, VMs in the same security group can access each other but any two VMs in different security groups cannot access each other. That said, access and communication between any two VMs in different security groups can also be customized by the tenant. For a detailed description of security groups, see section on ACL and Security Groups.
- **Remote access control:** Tenants can log in to their VMs over SSH to perform system maintenance and using keys generates by KMS. However, leaving the SSH port open is a relatively high security risk. For security purposes, tenants can enable access authentication by username/password however on DMP, only crypto key (public and private key pair) are used.

NB**:** for DMP username/password SSH is disabled. Only key pairs are used for SSH.

- **Resource management**: Tenants can manage ECS computing resources through API. API access requests must be authenticated and authorized through IAM before resources can be managed.

Asset: RDS - Relational Database Service – Security Controls

Relational Database Service (RDS) allows tenants to rapidly provision different types of databases whose compute and storage resources can flexibly scale to meet tenants' service requirements. Automatic backup, database snapshot, and restoration functions are provided to prevent data loss. In addition, RDS parameter groups allow tenants to optimize their databases as needed by their business.

#	Env	Asset Name	Asset	VPC location	Security Group Settings (if inside a security group, please specify)	Security Controls
1	PRD	rds-dmp-iam-production	RDS	vpc-adda-dep-dmp-iam-production	sg-adda-dep-dmp-rds-production	• **DBSS**: Database Security Service • **DEW**: Data Encryption Workshop • Disks are **encrypted** • **Network** isolation • **Access** control
2	PRD	rds-dmp-portal-production	RDS	vpc-adda-dep-dmp-portal-production	sg-adda-dep-dmp-rds-production	
3	UAT	rds-dmp-iam-uat	RDS	vpc-adda-dep-dmp-iam-uat	sg-adda-dep-dmp-rds-uat	
4	UAT	rds-dmp-portal-uat	RDS	vpc-adda-dep-dmp-portal-uat	sg-adda-dep-dmp-rds-uat	
5	UAT	rds-dmp-portal-uat-datasource-01	RDS	vpc-adda-dep-dmp-portal-uat	sg-adda-dep-dmp-rds-uat	
6	UAT	rds-dmp-portal-uat-datasource-02	RDS	vpc-adda-dep-dmp-portal-uat	sg-adda-dep-dmp-rds-uat	
7	QA	rds-dmp-iam-qa	RDS	vpc-adda-dep-dmp-iam-qa	sg-adda-dep-dmp-rds-qa	
8	QA	rds-dmp-portal-qa	RDS	vpc-adda-dep-dmp-portal-qa	sg-adda-dep-dmp-rds-qa	

9	RnD	rds-sgs-rnd-postgre-sch-01	RDS	vpc-adda-dep-dmp-portal-RnD	sgs-dep-rnd-sg	• **Transmission Encryption** • Data **replication** • Data **deletion**
10	RnD	rds-dmp-iam-rnd	RDS	vpc-adda-dep-dmp-iam-RnD	sg-adda-dep-dmp-rds-rnd	
11	RnD	rds-dmp-portal-rnd	RDS	vpc-adda-dep-dmp-portal-RnD	sg-adda-dep-dmp-rds-rnd	

RDS Security features and hardening:

- **DBSS** – Database Security Service.

o Refer to information in section on DBSS.

- **DEW**: Data Encryption Workshop (DEW) is a full-stack data encryption service in the cloud. It covers Key Management Service (KMS), Key Pair Service (KPS), and Dedicated Hardware Security Module (Dedicated HSM). DEW uses HSMs to protect your keys, and can be integrated with other cloud services to meet even the most demanding scenarios. Additionally, DEW enables you to develop customized encryption applications. With CTS, you can record operations associated with DEW for later query, audit, and backtracking.
- **Network isolation**: RDS instances run in independent tenant VPCs and can also be deployed in subnet groups that span multiple AZs to provide high availability. After an RDS instance is created, the tenant is allocated an IP address in the subnet group for that instance to enable connection to the database. To control access to their databases, tenants can configure a range of IP addresses that are allowed to access their VPC(s) designated for database instance(s). After deploying an RDS instance on a VPC, tenants can configure a VPN to allow other VPCs to access it. Alternatively, tenants can deploy an Elastic Cloud Server in a VPC and connect to the database through a private IP address. Subnet groups and security groups can be configured in combination to isolate RDS instances and enhance instance security.
- **Access control**: Creating an RDS instance also creates a primary account for the instance that its creator can use to perform operations on it. The password of this account can be set by the creator. The primary account can be used to connect to the instance, create sub-accounts, and assign database objects to those sub-accounts based on service planning. This provides a certain degree of security isolation. Furthermore, during database instance creation, a security group can be selected in which to deploy the NICs for the instance. VPC can be used to set inbound and outbound rules for the RDS instance and thereby control the scope of access to it. Only the database listening port is allowed to

accept connections. Once configured, a security group immediately take effect without the need to restart an RDS instance.

- **Transmission encryption**: The connections between database clients and servers can be encrypted with TLS. A specified certificate authority generates a unique service certificate for each RDS instance upon provisioning. Database clients can download a root certificate from the management console and provide this certificate when connecting to the database to authenticate the server and enable encrypted transmissions.
- **Storage encryption**: RDS can encrypt data before storage. Encryption keys are managed by KMS.
- **Automatic backup and snapshot**: These features help recover RDS databases in the event of a fault. Automatic backup is enabled by default, and backups can be stored for a maximum of 35 days. Automatic backup allows tenants to perform point-in-time recovery (PITR) on their databases. Automatic backup performs a complete backup of all data and then incremental backups of transaction logs every 5 minutes so that a tenant can restore data to its status at any second before the previous incremental backup. Tenants can also manually create a complete backup, known as a snapshot. Database snapshots are stored in OBS buckets and removed upon deletion of the corresponding database instance. New instances can be created based on existing snapshots.
- **Data replication**: RDS instances can be deployed in a single AZ or across multiple AZs for high availability. When the latter option is chosen, RDS initiates and maintains data replication for database synchronization. High availability is achieved by having a secondary instance take over in the event that a failure occurs on the primary instance. It is also possible to create read-only MySQL database instances when operations are read-heavy. RDS maintains data synchronization between those read-only instances and primary instances, and tenants can connect to either type of instances as required by business to isolate read and write operations.
- **Data deletion**: Removing an RDS instance will delete all data stored in that instance. No one can view or restore data once deleted.

Asset: CCE - Cloud Container Engine – Security Controls

Cloud Container Engine (CCE) provides highly scalable, high-performance, enterprise-class Kubernetes clusters and supports Docker containers. With CCE, you can easily deploy, manage, and scale containerized applications in the cloud.

For DMP the only CCE’s are deployed in Staging environment as follows:

#	Env	Asset Name	Asset	VPC location	Security Group Settings (if inside a security group, please specify)	Security Controls
1	PRD	cce-dmp-prod-iam	CCE	vpc-adda-dep-dmp-iam-production	cce-dmp-prod-iam-cce-node	•

2	PRD	ad-dcd-stg-cce-edge-node-02	CCE	ad_dcd-dl_stg-vpc-landing	ad-dcd-stg-cce-edge-node	**CGS** : Container Guard Service • **IAM/RBAC** : Role-base Access Control • **CTS** : Cloud Trace Service • Cluster Security Configurations • **KMS** : Key Management Service
3	STG	cce-dmp-stg-iam	CCE	vpc-adda-dep-dmp-iam-stage	cce-dmp-stg-iam-cce-node	
4	STG	cce-dmp-stg-portal	CCE	vpc-adda-dep-dmp-portal-stage	cce-dmp-stg-portal-cce-node	
5	UAT	cce-dmp-uat-iam	CCE	vpc-adda-dep-dmp-iam-uat	cce-dmp-uat-iam-cce-node	
6	UAT	cce-dmp-uat-portal	CCE	vpc-adda-dep-dmp-portal-uat	cce-dmp-uat-portal-cce-node	
7	QA	cce-dmp-qa-iam	CCE	vpc-adda-dep-dmp-iam-qa	cce-dmp-qa-iam-cce-node	
8	QA	cce-dmp-qa-portal	CCE	vpc-adda-dep-dmp-portal-qa	cce-dmp-qa-portal-cce-node	
9	RnD	cce-dmp-rnd-iam	CCE	vpc-adda-dep-dmp-iam-RnD	cce-dmp-rnd-iam-cce-node	
10	RnD	cce-dmp-rnd-portal	CCE	vpc-adda-dep-dmp-portal-RnD	cce-dmp-rnd-portal-cce-node	

CCE Security features and hardening:

- **Container Guard Service (CGS)**:
  - Refer to more information in Section on CGS.
- **IAM/RBAC Access Management:** Permissions to the CCE are managed by the G42 Professional Services team for DMP. CCE permissions management allows you to assign permissions to IAM users and user groups under your tenant accounts. CCE combines the advantages of Identity and Access Management (IAM) and Kubernetes Role-based Access Control (RBAC) authorization to provide a variety of authorization methods, including IAM fine-grained authorization, IAM token authorization, cluster-scoped authorization, and namespace-wide authorization.
- **Cloud Trace Service (CTS):** Cloud Trace Service (CTS) records operations on cloud service resources, allowing users to query, audit, and backtrack the resource operation requests initiated from the management console or open APIs as well as responses to the requests. This is useful information when providing security-based analysis for incident forensics and passing information to the ADDA SOC team.
  - Refer to more information in Section on CTS.

The following events are gathered using CTS on the CCE clusters.

Operation	Resource Type	Event Name
Creating an agency	Cluster	createUserAgencies
Creating a cluster	Cluster	createCluster
Updating the description of a cluster	Cluster	updateCluster
Upgrading a cluster	Cluster	clusterUpgrade
Deleting a cluster	Cluster	claimCluster/deleteCluster
Downloading a cluster certificate	Cluster	getClusterCertByUID
Binding and unbinding an EIP	Cluster	operateMasterEIP
Waking up a cluster and resetting node management (V2)	Cluster	operateCluster
Hibernating a cluster (V3)	Cluster	hibernateCluster
Waking up a cluster (V3)	Cluster	awakeCluster
Changing the specifications of a cluster	Cluster	resizeCluster
Modifying configurations of a cluster	Cluster	updateConfiguration
Creating a node pool	Node pool	createNodePool
Updating a node pool	Node pool	updateNodePool
Deleting a node pool	Node pool	claimNodePool
Migrating a node pool	Node pool	migrateNodepool
Modifying node pool configurations	Node pool	updateConfiguration
Creating a node	Node	createNode
Deleting all the nodes from a specified cluster	Node	deleteAllHosts
Deleting a single node	Node	deleteOneHost/claimOneHost
Updating the description of a node	Node	updateNode
Creating an add-on instance	Add-on instance	createAddonInstance
Deleting an add-on instance	Add-on instance	deleteAddonInstance
Uploading a chart	Chart	uploadChart
Updating a chart	Chart	updateChart

Deleting a chart	Chart	deleteChart
Creating a release	Release	createRelease
Upgrading a release	Release	updateRelease
Deleting a release	Release	deleteRelease
Creating a ConfigMap	Kubernetes resource	createConfigmaps
Creating a DaemonSet	Kubernetes resource	createDaemonsets
Creating a Deployment	Kubernetes resource	createDeployments
Creating an event	Kubernetes resource	createEvents
Creating an Ingress	Kubernetes resource	createIngresses
Creating a job	Kubernetes resource	createJobs
Creating a namespace	Kubernetes resource	createNamespaces
Creating a node	Kubernetes resource	createNodes
Creating a PersistentVolumeClaim	Kubernetes resource	createPersistentvolumeclaims
Creating a pod	Kubernetes resource	createPods
Creating a replica set	Kubernetes resource	createReplicasets
Creating a resource quota	Kubernetes resource	createResourcequotas
Creating a secret	Kubernetes resource	createSecrets
Creating a service	Kubernetes resource	createServices
Creating a StatefulSet	Kubernetes resource	createStatefulsets

Creating a volume	Kubernetes resource	createVolumes
Deleting a ConfigMap	Kubernetes resource	deleteConfigmaps
Deleting a DaemonSet	Kubernetes resource	deleteDaemonsets
Deleting a Deployment	Kubernetes resource	deleteDeployments
Deleting an event	Kubernetes resource	deleteEvents
Deleting an Ingress	Kubernetes resource	deleteIngresses
Deleting a job	Kubernetes resource	deleteJobs
Deleting a namespace	Kubernetes resource	deleteNamespaces
Deleting a node	Kubernetes resource	deleteNodes
Deleting a Pod	Kubernetes resource	deletePods
Deleting a replica set	Kubernetes resource	deleteReplicasets
Deleting a resource quota	Kubernetes resource	deleteResourcequotas
Deleting a secret	Kubernetes resource	deleteSecrets
Deleting a service	Kubernetes resource	deleteServices
Deleting a StatefulSet	Kubernetes resource	deleteStatefulsets
Deleting volumes	Kubernetes resource	deleteVolumes
Replacing a specified ConfigMap	Kubernetes resource	updateConfigmaps
Replacing a specified DaemonSet	Kubernetes resource	updateDaemonsets

Replacing a specified Deployment	Kubernetes resource	updateDeployments
Replacing a specified event	Kubernetes resource	updateEvents
Replacing a specified ingress	Kubernetes resource	updateIngresses
Replacing a specified job	Kubernetes resource	updateJobs
Replacing a specified namespace	Kubernetes resource	updateNamespaces
Replacing a specified node	Kubernetes resource	updateNodes
Replacing a specified PersistentVolumeClaim	Kubernetes resource	updatePersistentvolumeclaims
Replacing a specified pod	Kubernetes resource	updatePods
Replacing a specified replica set	Kubernetes resource	updateReplicasets
Replacing a specified resource quota	Kubernetes resource	updateResourcequotas
Replacing a specified secret	Kubernetes resource	updateSecrets
Replacing a specified service	Kubernetes resource	updateServices
Replacing a specified StatefulSet	Kubernetes resource	updateStatefulsets
Replacing the specified status	Kubernetes resource	updateStatus
Uploading a chart	Kubernetes resource	uploadChart
Updating a component template	Kubernetes resource	updateChart
Deleting a chart	Kubernetes resource	deleteChart
Creating a template application	Kubernetes resource	createRelease

Updating a template application	Kubernetes resource	updateRelease
Deleting a template application	Kubernetes resource	deleteRelease

- **Cluster Security Configurations:** The following configurations are applied on the CCE to ensure security posture is maintained for DCD:
    - Using CCE Cluser of the latest version.
    - Disabling the automatic token mounting function of the default service account
    - Configuring Proper Cluster Access Permissions for the Users – managed by the G42 Cloud professional services team
    - Configuring Resource Quotas for Cluster Namespaces
    - Configuring LimitRange for Containers in a Namespace
    - Configuring Network Isolation in a Cluster
    - Enabling the Webhook Authentication Mode with kubelet
    - Prevent the container from obtaining host metadata.
    - Restrict the access of the container to the management plane

Asset: OBS – Object Storage Service – Security Controls

Object Storage Service (OBS) provides object-based mass storage that is secure, reliable, and economical. Tenants can perform a variety of operations (creating, modifying, deleting, uploading, and downloading) to control their objects and buckets. OBS can be used by any type of users – regular users, websites, enterprises, and developers – to store any type of files. As an Internet-facing service, OBS can be accessed over its HTTPS web interface from any computer anywhere as long as it is connected to the Internet. Users can access and manage their stored data at any time over the OBS management console or client.

For DMP there are multiple deployments of OBS in both staging and production environments.

#	Env	Asset Name	Asset	Enterprise Project	Security Configuration	Security Controls
1	PRD	obs-adda-sgs-dmp-prod-iam	OBS	DEP_DMP_PROD	Private - Encrypted	-**Access** controls -Access control list (**ACL**) -Bucket **policy**
2	PRD	obs-adda-sgs-dmp-prod-portal	OBS	DEP_DMP_PROD	Private - Encrypted	
3	STG	obs-adda-sgs-dmp-stage-iam	OBS	DEP_DMP_STG	Private - Encrypted	
4	STG	obs-adda-sgs-dmp-stage-portal	OBS	DEP_DMP_STG	Private - Encrypted	

5	UAT	obs-adda-sgs-dmp-uat-iam	OBS	DEP_DMP_UAT	Private - Encrypted	-Double Access **Keys** -Access **logs**
6	UAT	obs-adda-sgs-dmp-uat-portal	OBS	DEP_DMP_UAT	Private - Encrypted	
7	UAT	obs-adda-sgs-dmp-uat-datasource	OBS	DEP_DMP_UAT	Private - Encrypted	
	RnD	obs-adda-sgs-dmp-rnd-iam	OBS	DEP_DMP_RnD	Private - Encrypted	
	RnD	obs-adda-sgs-dmp-rnd-portal	OBS	DEP_DMP_RnD	Private - Encrypted	
	QA	obs-adda-sgs-dmp-qa-iam	OBS	DEP_DMP_QA	Private - Encrypted	
	QA	obs-adda-sgs-dmp-qa-portal	OBS	DEP_DMP_QA	Private - Encrypted	

OBS Security Hardening:

OBS offers a range of access controls, including ACLs and bucket policies, user authentication, and restrictions on tenant access requests. A series of mechanisms are also in place to protect tenant data: access log auditing, source and request type restrictions on access to resources shared across domains, URL anti-spoofing and validation, and server-side encryption. These ensure that data can be securely stored and accessed.

- **Access controls:** Requests to access OBS can be controlled through ACLs, bucket policies, and user signature verification.
    - Access control list (ACL): OBS access permissions can be assigned to accounts by using an ACL. The ACL can grant all or certain accounts read, write, or full permissions on a per-bucket or per-object basis. Other access policies can also be configured, such as public access to a specified object (allowing all users read permissions only). By default, a bucket and the object(s) in the bucket can be accessed only by the creator of the bucket.
    - Bucket policy: The owner of a bucket can create a bucket policy to restrict access to the bucket. Bucket policies restrict access in a centralized fashion based on many conditions: OBS operation, applicant, resource, and other request information (such as IP address). Permissions can be assigned for specific buckets and specific accounts.
    - Unlike ACLs, which only control permissions for single objects, bucket policies can affect multiple or all objects within buckets. Permissions for any number of objects in a bucket can be configured with a single request. Multiple objects can be specified by using wildcard characters in resource names and other fields,

similar to regular expression operators, which allows the configuration of permissions for groups of objects.
    - OBS determines whether to accept or deny requests to access a bucket based on the policy configured for that bucket.
    - User signature verification: To access OBS, users must provide an access key ID (AK) and secret access key (SK), which are authenticated by IAM. Therefore, OBS authenticates and authorizes user accounts with the AK and SK to ensure that OBS resources cannot be accessed without proper authorization. The headers of access requests sent to OBS contain authentication information generated based on the SK, request timestamp, and request type. OBS also independently performs URL encoding on bucket and object names before generating authorization information. Only accounts that pass crypto-based authentication and authorization can access OBS resources.
- **Data reliability and durability**: OBS provides highly reliable storage. With redundant node design and highly reliable networks connecting service nodes, it offers 99.99% availability. In addition, by using automated recovery technology that provides data redundancy and ensures consistency, OBS offers data durability of 99.999999999% (11 nines). OBS can retain multiple versions of an object so that users can conveniently retrieve or restore previous versions and quickly recover data in the event of an accidental operation or application failure. Version control provides users with a way to recover objects that were unintentionally deleted or overwritten. Note that version control is not enabled by default for new OBS objects. Unless version control is enabled, an object uploaded to a bucket that contains another object with the same name will replace the original object.
- **Access logs:** OBS can log bucket access requests for use in analysis or auditing. These access logs allow the owner of a bucket to comprehensively analyze the nature and type of requests to access the bucket and identify trends. Once logging is enabled for a bucket, OBS automatically records all access requests into a log file that is written to a user-specified bucket. Note that because these logs occupy tenants' OBS space and may cause additional storage fees to be incurred, logging is disabled by default. Tenants can enable it manually if required for analysis or auditing purposes.
- **Cross-Origin Resource Sharing (CORS)**: OBS supports standard CORS, allowing access to OBS resources across domain boundaries. CORS is a World Wide Web Consortium (W3C) standard for web browsers that defines interactions between web applications in one domain and resources in another. This enables static websites hosted on OBS to respond to requests from websites in other domains, provided that CORS is configured properly on the corresponding bucket. Website scripts and content can then interact across domains even when a same-origin policy (SOP) is in place.
- **URL anti-spoofing and validation**: To prevent URL spoofing for OBS tenants, URL validation based on HTTP header and referer as well as access whitelists and blacklists are supported. The source website from which a user is linked to a destination website can be determined based on the header of the HTTP request. Requests that originate from an external website can then be denied or redirected to a specified web page. URL anti-spoofing and validation mechanism can also check requests against a blacklist or whitelist; access is granted when a match with a whitelist entry, otherwise denied or redirected to a specified web page.

- **Server-side encryption (SSE)**: Objects uploaded by users are encrypted on the server side into cipher text before being stored. When an encrypted object is downloaded, the cipher text is decrypted on the server side and then transmitted as plaintext. Keys managed by KMS (SSE-KMS) or provided by the client (SSE-C) can both be used for SSE:
    - In SSE-KMS, OBS uses keys provided by KMS to perform encryption. Users must create a key on KMS (or use the default KMS key) and then select that key for SSE when uploading objects.
    - In SSE-C, OBS uses keys provided by the user and the corresponding hash values to perform encryption. The interface used to upload objects can transmit keys, which OBS can use for server-side encryption. Note that OBS does not store user-provided key information, therefore users will be unable to decrypt their objects without the proper keys.

Asset: MRS – MapReduce Service – Security Controls

MapReduce Service (MRS) provides high-performing hosted Big Data clusters that are reliable, scalable, fault-tolerant, and easy to operate and maintain. MRS **clusters** provides a Big Data management and analytics platform hosted in the cloud. All cluster nodes are deployed on the same tenant VLAN, and mutual trust relationships are established between the active/standby Operations and Maintenance Service (OMS) nodes and other nodes in the cluster.

Users can log in to MRS using its client or a web browser. The MRS supports single sign-on (SSO) based on central authentication service (CAS) so that users can conveniently access the web pages of other Big Data platform components without being prompted for authentication again.

On DMP MRS's are located in the Production, Staging, UAT, QA and RnD VPC as shown in the table below:

#	Env	Asset Name	Asset	VPC	Security Group	Security Controls
1	PRD	mrs-dmp-prod-portal	MRS	vpc-adda-dep-dmp-portal-production	mrs_mrs-dmp-prod-port	-User **password** management -**Permissions** control -Data **encryption** -Data **integrity** -Disaster **Recovery**
2	STG	mrs-dmp-stg-portal	MRS	vpc-adda-dep-dmp-portal-stage	mrs_mrs-dmp-stg-port	
3	UAT	mrs-dmp-uat-portal	MRS	vpc-adda-dep-dmp-portal-uat	mrs_mrs-dmp-uat-port	
4	QA	mrs-dmp-qa-portal	MRS	vpc-adda-dep-dmp-portal-qa	mrs_mrs-dmp-qa	
5	RnD	mrs-dmp-rnd-portal	MRS	vpc-adda-dep-dmp-portal-RnD	mrs_mrs-dmp-rnd	

MRS Security Hardening:

- **User password management**: MRS uses IAM (Kerberos and LDAP) to manage user passwords. Kerberos encrypts user passwords and saves them to the LDAP database.
- **Permissions control**: MRS uses RBAC. Assigning a role to a user grants that user the permissions associated with the role. The permissions of each role can be configured based on the component resources that the role is required to access.
- **Data encryption**: The HBase and Hive functions of MRS support column-based storage encryption. When importing data, users can choose which data to store under encryption.
- **Data integrity**: MRS user data is stored in Hadoop Distributed File System (HDFS), which uses CRC32C to verify data integrity. Note that the default setting of CRC32C can be changed to the slower CRC32 if desired. Verification data is stored on the HDFS DataNode (DN). If the DN detects that data transmitted from a client is abnormal (i.e. incomplete), the DN reports an exception to the client and asks it to write the data again. Data integrity is also verified by the client when reading data from the DN. If the client detects that the data is incomplete, it attempts to read the data from another DN.
- **Disaster recovery**: MRS provides geographically redundant disaster recovery for user data stored in its cluster along with a basic O&M tool for external systems that can set active and standby nodes, rebuild and verify data, and check the progress of data synchronization. To implement disaster recovery, MRS backs up data from the HBase cluster to another cluster, and clusters and data tables requiring synchronization are configured to trust each other. Note that HBase, HDFS, ZooKeeper, Kerberos, and LDAP Server must be installed on the cluster for this process to succeed. Once disaster recovery is configured, a standby cluster can immediately take over services in the event that data on the active cluster is damaged.

Asset: DWS - Data Warehouse Service – Security Controls

GaussDB(DWS) is an online data processing database that runs on the cloud infrastructure to provide scalable, fully-managed, and out-of-the-box analytic database service, freeing you from complex database management and monitoring. It is a native cloud service based on the converged data warehouse GaussDB, and is fully compatible with the standard ANSI SQL 99 and SQL 2003, as well as the PostgreSQL and Oracle ecosystems. GaussDB(DWS) provides competitive solutions for PB-level big data analysis in various industries.

For DMP the DWS is only deployed in the UAT environment.

#	Env	Asset Name	Asset Description	VPC location	Security Group Settings	Security Controls
1	UAT	dws-dmp-uat-01	DWS Cluster	vpc-adda-dep-dmp-portal-uat	sg-dws-dmp-uat-01	• Security Permissions • Encryption DWS • Rotating Keys • KMS

DWS Security Hardening:

- **Security Permissions**: By default, the administrator specified when you create a GaussDB(DWS) cluster is the database system administrator. The administrator can create other users and view the audit logs of the database. That is, separation of permissions is disabled.

GaussDB(DWS) supports role-based separation of permissions. In this way, different roles have different permissions and cluster data can be better protected.

For details about the default permissions mode and the separation of permissions mode, see "Database Security Management > Managing Users and Their Permissions > Separation of Permissions" in the Data Warehouse Service (DWS) Developer Guide.

- **Encrypting (DWS) Database**: In GaussDB(DWS), database encryption for a cluster is enabled and therefore all static data in protected. When encryption is enabled, data of the cluster and its snapshots is encrypted.

NB: To encrypt an unencrypted cluster (or in reverse), you need to export all data from the unencrypted cluster and import it to a new cluster that has enabled database encryption.

Database encryption is performed when data is written to GaussDB(DWS). That is, GaussDB(DWS) encrypts data when the data is written to GaussDB(DWS). If you want to query the data, GaussDB(DWS) automatically decrypts it and returns the result to you.

A three-layer key management structure is adopted, including the cluster master key (CMK), cluster encryption key (CEK), and database encryption key (DEK).

o The CMK is used to encrypt the CEK and is stored in KMS.

o The CEK is used to encrypt the DEK. The CEK plaintext is stored in the data warehouse cluster's memory, and the ciphertext is stored in GaussDB(DWS).

o The DEK is used to encrypt database data. The DEK plaintext is stored in the data warehouse cluster's memory, and the ciphertext is stored in GaussDB(DWS).

When the cluster is restarted, it automatically requests the DEK plaintext from GaussDB(DWS) through an API. GaussDB(DWS) loads the CEK and DEK ciphertext to the cluster's memory, invokes KMS to decrypt the CEK using the CMK, loads the CEK to the memory, decrypts the DEK using the CEK plaintext, loads the DEK to the memory, and returns it to the cluster.

- **Rotating Encryption Keys**: Encryption key rotation is used to update the ciphertext stored on GaussDB(DWS). On GaussDB(DWS), you can rotate the encrypted CEK of an encrypted cluster.

You can plan the key rotation interval based on service requirements and data types. To improve data security, you are advised to periodically rotate the keys to prevent the keys from being cracked. Once you find that your keys may have been disclosed, rotate the keys in time.

- **KMS – Key Management Service:**

  - Refer to more information in Section on KMS.

Asset: CSS – Cloud Search Service – Security Controls

Cloud Search Service (CSS) is a fully managed, distributed cloud service powered by Elasticsearch and is part of the ELK Stack. It is compatible with open-source Elasticsearch, Kibana, and Cerebro.

For DMP CSS is deployed across all the environments.

#	Env	Asset Name	Asset	VPC	Security Group	Security Controls
1	PRD	css-dmp-portal-production	CSS	vpc-adda-dep-dmp-portal-production	sg-adda-dep-dmp-css	-Network isolation -Access controls -Data security -Operation Audit
2	STG	css-dmp-portal-stage	CSS	vpc-adda-dep-dmp-portal-stage	sg-adda-dep-dmp-css	
3	UAT	css-dmp-portal-uat	CSS	vpc-adda-dep-dmp-portal-uat	sg-adda-dep-dmp-css-uat	
4	QA	css-dmp-portal-qa	CSS	vpc-adda-dep-dmp-portal-qa	sg-adda-dep-dmp-css-qa	
5	RnD	css-dmp-portal-rnd	CSS	vpc-adda-dep-dmp-portal-RnD	sg-adda-dep-dmp-css-rnd	

CSS Security Hardening:

CSS ensures secure running of data and services from the following aspects:

- Network Isolation: CSS ensures secure running of data and services from the following aspects.
  - Service plane: refers to the network plane of the cluster. It provides service channels for users and delivers data definition, index, and search capabilities.
  - Management plane: refers to the management console. It is used to manage CSS.
  - VPC security groups or isolated networks ensure the security of hosts.
- **Access controls:** Requests to access OBS can be controlled through ACLs, bucket policies, and user signature verification.

    - Using the network access control list (ACL), you can permit or deny the network traffic entering and exiting the subnets.
    - Internal security infrastructure (including the network firewall, intrusion detection system, and protection system) can monitor all network traffic that enters or exits the VPC through the IPsec VPN.
    - User authentication and index-level authentication are supported. CSS also supports interconnection with third-party user management systems.
- **Data security**:
    - In CSS, the multi-replica mechanism is used to ensure user data security.
    - Communication between the client and server can be encrypted using SSL
- **Operation Audit:**
    - Cloud Trace Service (CTS) can be used to perform auditing on key logs and operations.

Security Service: HSS – Host Security Service (HSS)

Host Security Service (HSS) helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats. G42 Cloud HSS provides the following functions:

· Asset management: manages and analyzes security asset information, such as accounts, ports, processes, web directories, and software.

· Vulnerability management: detects vulnerabilities in the Windows and Linux operating systems and software such as SSH, OpenSSL, Apache, and MySQL, and provides fixing suggestions.

· Baseline check: checks system password complexity policies, typical weak passwords, risky accounts, and common system and middleware configurations to identify insecure items and prevent security risks.

· Account cracking prevention: detects password cracking attacks on accounts such as SSH, RDP, FTP, SQL Server, and MySQL, blocks the identified attack source IP addresses for 24 hours, and forbids them to log in again to prevent hosts from being intruded due to account cracking.

· Two-factor authentication: HSS authenticates login attempts to Elastic Cloud Servers twice by SMS messages and emails. This significantly improves account security.

· Key file tampering detection: HSS monitors key files (such as ls, ps, login, and top files) and prompts users about possibility of tampering once the files are modified.

· Detection of malicious programs: By detecting program features and behaviors and using the AI image fingerprint algorithm and cloud-based virus scanning and removal, the system can

effectively identify malicious programs, such as viruses, Trojan horses, backdoors, worms, and mining software, and provide one-click isolation and virus removal capabilities.

· Website backdoor detection: HSS checks files in web directories to help identify webshells (such as php and jsp) in Elastic Cloud Servers.

· Web page anti-tamper: HSS protects web pages, electronic documents, images, and other files of websites from tampering or sabotage by hackers.

· Effective host risk prevention: The asset management, vulnerability management, and baseline check functions can detect and prevent host vulnerabilities, weak passwords, and insecure configurations, reducing the attack surface by 90%.

· Strong account cracking defense capability: Two-factor authentication upon host login and advanced protection algorithms can effectively prevent brute-force cracking attacks.

· High detection rate of malicious programs: The behaviour analysis and AI-based image fingerprint algorithm can effectively detect and remove unknown and variant malicious programs, providing an industry-leading detection rate.

· Effective web page anti-tamper: The web page anti-tamper function provides three protection capabilities: web file directory locking, automatic restoration upon tampering detection, and web page restoration based on remote backup. This prevents web page tampering and has become a mandatory security service for government, education, and large enterprise websites.

Mandatory services for graded security protection assessment: The intrusion detection function meets host intrusion prevention and malicious code prevention requirements. The vulnerability management function meets host vulnerability scanning requirements. The web page anti-tamper function meets data integrity requirements.

Security Service: IMS – Image Management Service

An image is a template containing software and configurations for a cloud virtual server or bare metal server. Each image must contain an operating system and may additionally contain preinstalled applications such as database software. G42 Cloud classifies images into public, private, and shared:

· Public images are standard operating system images provided by G42 Cloud.

· Private images are created by users for their own use.

· Shared images are custom images created by any user, maintained on a voluntary basis by the user community and provided for all users to use.

Image Management Service (IMS) provides simple and convenient self-service management functions for images. Tenants can manage their images through the IMS API or the management console. G42 Cloud staff update and maintain public images, which includes performing security hardening and applying security patches on them as required. The staff also provide security-related information for users to reference in deployment testing, troubleshooting, and other O&M activities. Users can deploy their ECS servers by selecting one of the public images provided, creating a private image from an existing cloud server deployment or an external image file, or using a shared image and participating in its development and maintenance.

Considering that attacks on the IMS API could have severe consequences, such as the disclosure of many tenants' data or the interruption of management services, IMS offers a wide range of security measures to protect the IMS management system from such attacks. Tenants must be authenticated with IAM and receive a token before they can use IMS. The service uses a multi-tenancy-based permissions management model and secure communications protocols, strictly verifies parameters, and provides measures for protecting sensitive information and auditing logs.

IMS supports encryption and integrity verification for the transmission and storage of images. All data is stored in an image database on a trusted subnet, and public and private images are stored in different buckets using Object-based Storage (OBS). IMS comes with secure cryptographic algorithms and functions that enable users to encrypt their image files and sensitive data in both transmission and storage.

IMS requires tenants to have sufficient permissions to perform any operation, and keeps audit logs of major operations. Audit logs are retained indefinitely so that tenants can accurately trace operations performed over a long period of time.

Security Service: DBSS – Database Security Service

Database Security Service (DBSS) provides the database audit service in out-of-path mode. It records user access to the database in real time, generates fine-grained audit reports, sends real-time alarms for high-risk operations and attacks. In addition, database audit generates compliance reports that meet data security standards (such as Sarbanes-Oxley) to locate internal violations and improper operations, thus ensuring data asset security.

DBSS protects self-built databases on Elastic Cloud Server (ECS) and Bare Metal Server (BMS), and RDS instances within the same VPC and its subnets. Due to network restrictions, DBSS cannot protect self-built databases and RDS instances on ECSs and BMSs if they are not in the same VPC and its subnets.

DBSS provides the following security functions:

- User Behaviour Detection and Audit
    - Associates access operations in the application layer with those in the database layer.

    - Uses built-in or user-defined privacy data protection rules to mask private data (such as accounts and passwords) in audit logs displayed on the console.
- Multi-dimensional Lead Analysis
    - Behaviour analysis[GS1]
    - Supports analysis in multiple dimensions, such as audit duration, statement quantity, risk quantity, risk distribution, session statistics, and SQL distribution.
    - Session analysis
    - Conducts analysis based on time, user, IP address, and client.
    - Statement analysis
    - Provides multiple search criteria, such as time, risk severity, user, client IP address, database IP address, operation type, and rule.
- Real-time Alarms for Risky Operations and SQL Injection
    - Risky operation
    - Defines a risky operation in fine-grained dimensions such as operation type, operation object, and risk severity.
    - SQL injection
    - Provides an SQL injection library, which facilitates alarm reporting for database exceptions based on the SQL command feature or risk severity.
    - System resource
    - Reports alarms when the usage of system resources (CPU, memory, and disk) reaches configured threshold.
- Fine-grained Reports for Various Abnormal Behaviours
    - Session behaviour
    - Provides session analysis report of the client and database users.
    - Risky operation
    - Provides the risk distribution and analysis report.
    - Compliance report
    - Provides compliance reports that meet data security standards (for example, Sarbanes-Oxley).
- DBSS has the following advantages:
    - Simple to set up: Database audit is deployed in bypass pattern. It is simple to set up and operate.
    - Comprehensive audit: Supports audit of RDS databases and self-built databases on ECS/BMS on the management console.
    - Quick identification: Implements 99%+ application association audit, complete SQL parsing, and accurate protocol analysis.
    - Efficient analysis: Responds quickly for data query with 10,000 requests per second from massive volumes of data saved.
    - Compliance with various regulations: Complies with laws and regulations, such as the cybersecurity law and SOX.
    - Clear permission division: Clearly divides permissions among the system administrator, security administrator, and audit administrator, meeting audit security requirements.

Security Service: CGS – Container Guard Service

Container Guard Service (CGS) can scan vulnerabilities and configuration information in images, helping enterprises resolve container environment problems that cannot be detected by traditional security software. In addition, CGS provides the container process whitelist, read-only file protection, and container escape detection functions to prevent security risks during container running.

G42 Cloud CGS mainly provides the following functions:

- Image vulnerability management: CGS can scan private, official, and all running images in G42 Cloud to detect vulnerabilities in the images and provide fixing suggestions, helping users obtain secure images.
- Container security policy management: CGS supports the configuration of security policies to help enterprises define the container process whitelist and file protection list, improving system and application security during container running.
- Container process whitelist: Defining such a whitelist can effectively prevent security risks such as abnormal processes, privilege escalation attacks, and noncompliant operations.
- File protection: Read-only protection must be configured for key application directories (such as bin, lib, and user system directories) in containers to prevent tampering and hacker attacks. This function can restrict the access (set to read-only) to these directories to prevent security risks such as file tampering.
- Container escape detection: This function scans all running containers, detects exceptions (including escape vulnerability attacks and escape file access) in the containers, and provides solutions.

Security Service: CTS – Cloud Trace Service

Cloud Trace Service (CTS) records operations on cloud service resources so that they can be queried, audited, and traced. It records operations performed on the management console, executed through an API, and internally triggered on the G42 Cloud system. CTS is an essential support system for tenant-specific industry certification and IT compliance certification. It provides the following functions:

- Resource change auditability: Changes to G42 Cloud resource and system configurations performed by all users are recorded systematically and in real time. This is superior to the traditional method in enterprise IT environments of manually auditing each change.
- Access security monitoring and auditability: All management console operations and API calls are recorded systematically and in real time to help query, analyze, and locate issues closer to real time or after fact.
- Data auditability: Users can verify whether data has been disclosed by collecting activity data about OBS objects and object-level API events recorded by CTS for audit purposes.
- Low cost: CTS can merge records into event files on a regular basis and move these to an OBS bucket for storage, making logs highly available over a long period of time and at a low cost.
- The security design for CTS is based on the G42 Cloud security framework. The security of the cloud computing services provided to tenants is ensured through secure network

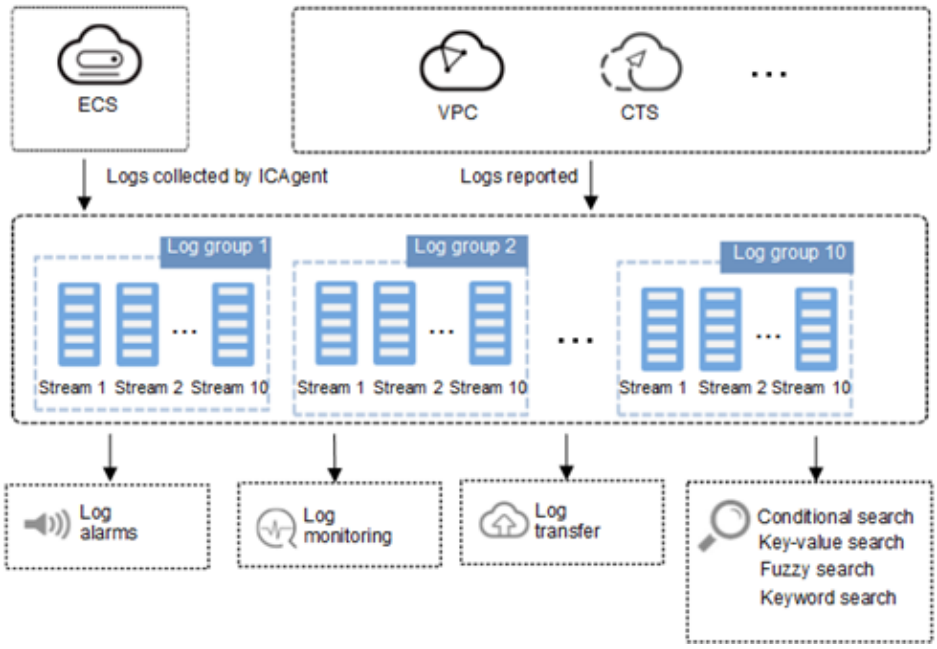
architecture and through the implementation of network perimeter, application, and data protection. Application and data security are described as follows.

- Application security: Valid requests for compliance event queries and tracker operations sent by legitimate users and also valid compliance events from interconnected services are accepted and processed by CTS. All requests must be transmitted over HTTPS. Sensitive data is encrypted, and a number of measures are taken to ensure security when interacting with external services: interface control, whitelist control, requestor authentication, and multiple rounds of verification. Furthermore, the web security of CTS control nodes has been hardened to defend against a wide range of attacks.
- Data security: The security requirements for user log data processed by CTS differ as the data is generated, transmitted, and stored. When generated, log data must be desensitized within each service and verified to contain no sensitive data. When transmitted, the accuracy and completeness of log data transmission and storage must be ensured through identity authentication, format validation, whitelist inspection, and unidirectional reception. When stored, log data must have multiple backup copies stored in a distributed manner, and databases must be hardened in accordance with G42 security requirements to prevent data security threats such as spoofing, repudiation, tampering, and leakage. For additional security, CTS can be configured for encryption of log data when saved in an OBS bucket.

Security Service: LTS – Log Tank Service

Log Tank Service (LTS) supports the security function to ensure that specific logs are collected from CTS and other assets for analysis and further parsing to syslogs/ICagents for SOC management. LTS enables you to collect logs from hosts and cloud services for centralized management, and analyze large volumes of logs efficiently, securely, and in real time. LTS provides you with the insights for optimizing the availability and performance of cloud services and applications. It allows you to make faster data-driven decisions, perform device O&M with ease, and analyze service trends.

The diagram below shows how LTS works:



LTS collects logs from hosts and cloud services, and displays them on the LTS console in an intuitive and orderly manner. You can transfer logs for long-term storage. Collected logs can be quickly queried by keyword or fuzzy match. You can analyse real-time logs for security diagnosis and analysis, or obtain operations statistics, such as cloud service visits and clicks.

Security Service: KMS – Key Management Service

KMS service will be used to encrypt RDS and OBS services for data at rest encryption. KMS service will provide KEYS or own key will be brought by ADDA(BYOK).

For DMP, KMS distributions is as follows:

IAM Project	Enterprise Project	KMS Key Groupings	Description
default	DEP_DMP_PROD	KMS-adda-dep-dmp	Be used for PRD and STG
	DEP_DMP_QA	KMS-adda-sgs-dmp-qa	Be used for QA
	DEP_DMP_UAT	KMS-adda-sgs-dmp-uat	Be used for UAT
	DEP_DMP_UAT	KMS-adda-sgs-dmp-rnd	Be used for RnD
datalake_dev	DEP_DL_DEV	KMS-adda-dep-datalake-dev	Be used for all encrpytion in datalake_dev
datalake_rnd	DEP_DL_RnD	KMS-adda-dep-datalake-RnD	Be used for all encrpytion in datalake_rnd

datalake_stg	DEP_DL_STG	KMS-adda-dep-datalake-stg	Be used for all encrpytion in datalake_stg
datalake_prod	DEP_DL_PROD	KMS-adda-dep-datalake-prod	Be used for all encrpytion in datalake_prod

Key Management Service (KMS) is a secure, reliable, and easy-to-use service that helps users centrally manage and safeguard their Customer Master Keys (CMKs).

This service uses hardware security modules (HSMs) to protect CMKs. HSMs help you create and control CMKs with ease. All CMKs are protected by root keys in HSMs to avoid leakage caused by human error. KMS implements access control and log-based tracking on all operations involving CMKs. Additionally, it provides use records of all CMKs, meeting your audit and regulatory compliance requirements.

IMPORTANT NOTE: HSM is not a separate service offered to tenants by G42 Cloud, instead it is a service used to support KMS and is a backend service only.

KMS provides the following functions:

- Manages CMKs.

Using the KMS console or APIs, you can perform the following operations on CMKs:

- Creating, querying, enabling, disabling, scheduling the deletion of, and cancelling the deletion of CMKs
- Importing CMKs and deleting CMK material
- Modifying the aliases and description of CMKs

Creates, encrypts, and decrypts DEKs:

You can create, encrypt, and decrypt a DEK by calling KMS APIs. For details, see the Key Management Service API Reference.

Generates hardware true random numbers:

You can generate 512-bit hardware true random numbers using a KMS API. The 512-bit hardware true random numbers can be used as or serve as basis for keys and encryption parameters. For details, see the Key Management Service API Reference.

IAM – identity and access management

User Access Management (UAM) is the administration of the DMP platform. IAM supports the UAM capability across DMP, cloud resources and individual application access.

There are three means by which UAM is applied as shown below:

- IAM G42 Console
- IAM DMP Portal (Refer to Application > DMP Applilcation Security > Access Control)

IAM G24 Console

This IAM is used solely for administering of the G42 Cloud assets inside the DMP tenant and is administered by G42 Managed Services. G42 IAM uses policies to add the users into groups and assign the rights for each group within the enterprise projects the detailed enterprise projects and groups. G42 Cloud Managed Services can provide details on the G42 IAM Console roles.

IAM is a user account management service designed for enterprises that allocates resources and operation permissions to enterprise users in a differentiated manner. Once IAM has authenticated and authorized these users, they can use an access key to access G42 Cloud resources through APIs.

IAM supports hierarchical fine-grained authorization to ensure that the various users who are part of an enterprise tenant use cloud resources as authorized. This authorization scheme prevents users from exceeding the scope of their permissions and ensures the continuity of tenant services.

Password-based authentication: A password is specified when a user account is registered or created. The password is required to log in to the G42 Cloud console and can also be used to access G42 Cloud resources using APIs.

Password policy: IAM allows the security administrator for each tenant to set a policy for user passwords to reduce the likelihood that user accounts can be exploited. Password policies include rules such as password length, complexity and expiration interval.

Login policy: IAM also allows security administrators to create account lockout policy for user login to prevent user passwords from brute force and phishing attacks.

ACL: Tenants can configure an IP address-based ACL to ensure that enterprise users can access G42 Cloud resources only from a secure network environment, greatly mitigating the risk of data leakage that would be rampant otherwise.

Multi-factor authentication (MFA): MFA is an optional security measure that enhances account security. If MFA is enabled, users who have completed password authentication will receive a one-time SMS authentication code that they must use for secondary authentication. MFA is used by default for changing important or sensitive account information such as passwords or mobile phone numbers.

Access key: API requests must be signed with an access key to manage G42 Cloud resources using O&M tools or API commands. Signature information is verified by the API gateway. Digital signatures and timestamps prevent requests from being tampered with and protect against replay attacks.

Enterprise administrators can create and download an access key on the My Credentials page at any time and view the status of the key. However, for security purposes, the access key cannot be recovered or re-downloaded in the event that the access key is lost or forgotten. The administrator must create a new access key and then disable or delete the old one. The access key must be stored in a safe location and changed regularly. Under no circumstances should it be hardcoded.

Identity Federation: Secure and reliable external services for identity authentication that support Security Assertion Markup Language (SAML) 2.0, such as LDAP and Kerberos, can be used for user authentication. To enable authentication by an external service, tenants must configure the service as an identity provider (IdP) and G42 Cloud as the service provider (SP). Enterprise tenants can then log in to the G42 Cloud console over SAML or use APIs to access cloud resources without synchronizing user information to G42 Cloud.

Tenants can use federated identity authentication to map external users to temporary G42 Cloud users and allow those users to access G42 Cloud resources for a specified time period. An appropriate user group (i.e. set of permissions) must be created for these temporary users to restrict their permissions.

Long-term security credentials should not be hardcoded into mobile or web applications that access G42 Cloud resources. Instead, such applications should prompt users to first log in, then use already authenticated identity information to obtain temporary credentials through identity federation.

Permissions management: IAM includes user administration permissions and cloud resource permissions. User administration permissions deal with creating, deleting, modifying, and assigning permissions to users and user groups, while cloud resource permissions have to do with creating, deleting, modifying, and configuring cloud resources. Users inherit the cloud resource permissions assigned to their user group. Managing user permissions by user groups therefore makes the process more organized. IAM can also work with PAM to implement fine-grained management of privileged accounts.

Application > DMP Applilcation Security > Access Control) [GS1]

Infrastructure Security

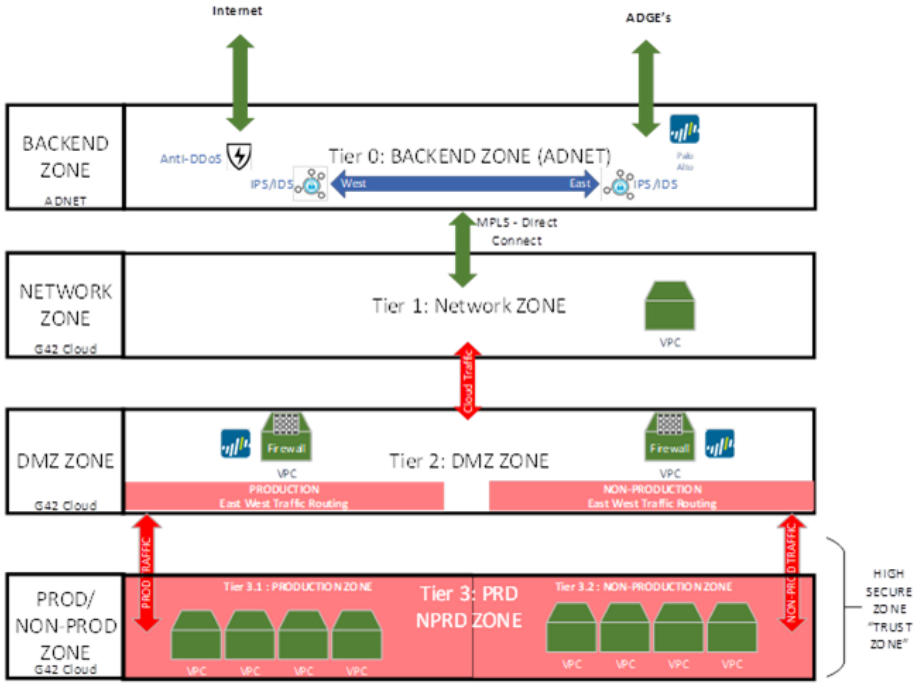
The infrastructure security is based on the security controls and methods applied across the infrastructure assets. Based on the Infrastructure design, the key assets are as follows:

- Subnetting
- Port allocations
- VPC peering and routing
- IP whitelisting
- ACL management
- Security Group management

The above G42 Cloud services will be described in subsequent sections below.

Zoning – Three Tier Security Zoning

The network zoning is applied as a security best practice measure and supported by the above G42 Cloud services. The zones are depicted in the diagram below.



The description of each of the zones defined above is as follows:

- **Tier 0 – Backend Zone:** This is the existing ADDA network zone commonly referred to ADNET. The physical connections between ADnet and G42 Cloud is dedicated MPLS encrypted connections. This zone will provide the connectivity between the ADGE's and the G42 Cloud via the Cloud Gateways. Virtual Gateway is Cloud Native Service to terminate the Direct Connect with ADnet , and it works in redundancy mode.
    - Traffic from ADGEs forward to G42 Cloud Tenant via ADnet Connections.
    - G42 Cloud Tenant connected to DCD Tenant via Cross Tenant VPC Peering over the DMZ VPC
    - Virtual Gateway is Cloud Native Service to terminate the Direct Connect with ADnet , and it works in redundancy mode.
    - Traffic from ADGEs forward to G42 Cloud Tenant via ADnet Connections.
    - SGS Tenant connected to HC Tenant via Cross Tenant VPC Peering over the Infra VPC.
    - This zone provides the connectivity to the security functions and features provided by ADNET, this includes:
    - Anti-DDoS – Provided by Etisalat/Arbor subscription which protects ADNET and by sub-set G42 Cloud from internet originating DDoS Attacks.

    - East-West Traffic is protected using ADNET's (TrendMicro, PaloAlto and MacAfee) solutions to provide Intrusion Protections and Intrusion Detection solutions.
- **Tier 1 - Network Zone:** This is the perimeter security zone specifically applied to provide separation between the DCD datalake cloud assets and the external interfaces that are integrated with ADNet. This zone contains the Transit VPC and is a security zone to ensure that all traffic lands in this zone prior to accessing the DMZ zone. Additional security controls can be applied on this zone in the future and allows for security scalability.
- **Tier 2 - DMZ Zone:** This is the primary DMZ security zone which is used route East/West traffic across all the production and non-production VPCs. This zone contains the Firewalls for production and non-production.
    - Namely the cloud firewall: PaloAlto
- **Tier 3.1 - Production Zone**: The production zone is a critical and security hardened environment. This zone is the primary DCD production zone and contains all vital and important production data and information.
    - NOTE: A specific PaloAlto FW is provided for the Production Zone via the DMZ.
    - NOTE: Production traffic is routed via the Transit VPC, to the DMZ Zone where it is filtered using a dedicate Palo Alto firewall and from where it is routed using PA's zoning and VPC Peering to the Production Zone and the VPC's inside the Production Zone.
- **Tier 3.2 - Non-Production Zone**: This zone contains all the non-production assets and is used for development and testing.
    - NOTE: A specific PaloAlto FW is provided for the Non-Production Zone via the DMZ.
    - NOTE: Non-Production traffic is routed via the Transit VPC, to the DMZ Zone where it is filtered using a dedicated Palo Alto firewall and from where it is routed using PA's zoning and VPC Peering to the Production Zone and the VPC's inside the Production Zone.

The above zones are layered with security controls supported by:

- G42 Cloud VPC peering,
- G42 Cloud Network ACL and,
- G42 Cloud Security Groups,
- PaloAlto firewall filtering
- PaloAlto zoning network segregation.

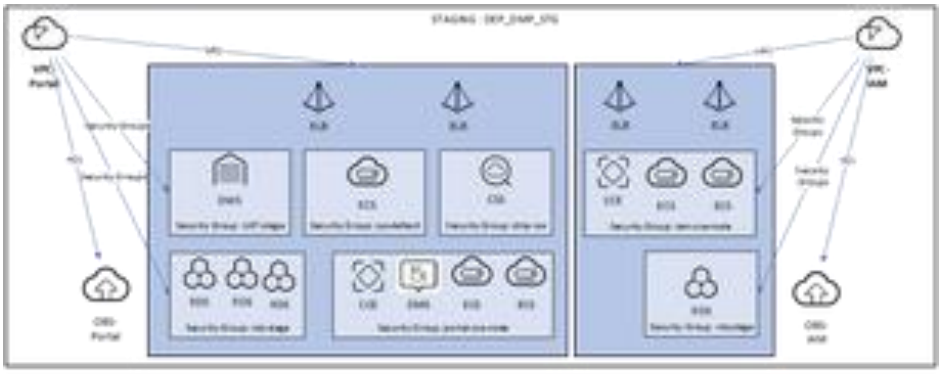
These infrastructure security components are described in the subsequent sections.

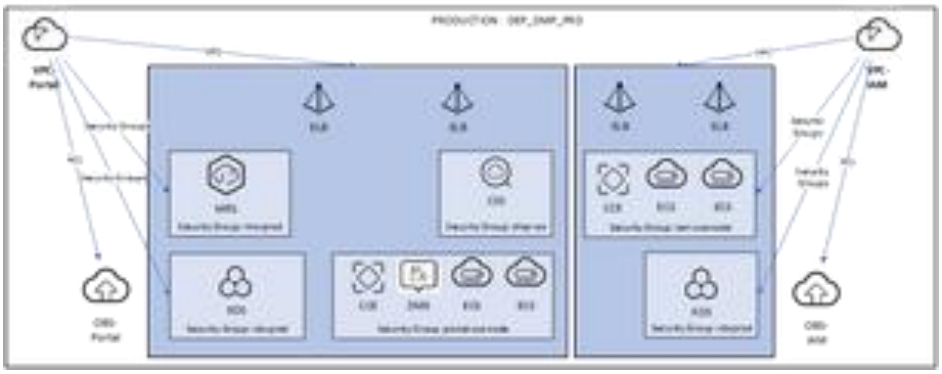
VPC - Network Segmentation

Network segmentation on the G42 Cloud is supported by Virtual Private Cloud (VPC) services. VPC enables ADDA to provision logically isolated, configurable, and manageable virtual networks for Elastic Cloud Servers (ECSs) and CCE's, improving cloud resource security and simplifying network deployment. VPCs support the following permission and security features:

- Subnetting
- Port allocations
- VPC peering and routing
- IP whitelisting
- ACL management
- Security Group management

The diagram below shows the VPC network segmentation and the Security Groups allocations for Staging and Production environments.





VPC provides the following network security features:

- VLAN isolation: VLAN, which works on Layer 2, uses virtual bridging to support VLAN tagging and implement virtual switching to ensure secure isolation between VMs.
- IP and MAC address binding: This measure enhances the security of virtual networks by preventing VM users from spoofing IP or MAC addresses. DHCP snooping is used to bind IP addresses with corresponding MAC addresses. IP Source Guard and dynamic ARP inspection are also used to filter out packets from non-bound sources.
- DHCP server isolation: To ensure that IP addresses are allocated properly, users are not allowed to run DHCP servers.

- DoS and DDoS mitigation: The number of tracked connections to virtual ports is restricted so as to prevent traffic flooding attacks

[1] from inside or outside the cloud platform.

NOTE: VPC's provides security functions at the lower-stack of the OSI model.

For DMP, There are a total of 10 unique VPC's for DMP as listed below:

1. vpc-adda-dep-dmp-iam-stage
1. vpc-adda-dep-dmp-portal-stage
1. vpc-adda-dep-dmp-iam-production
1. vpc-adda-dep-dmp-portal-production
1. vpc-adda-dep-dmp-iam-uat
1. vpc-adda-dep-dmp-portal-uat
1. vpc-adda-dep-dmp-iam-qa
1. vpc-adda-dep-dmp-portal-qa
1. vpc-adda-dep-dmp-iam-RnD
10. vpc-adda-dep-dmp-portal-RnD

---

[1] Traffic flooding attacks interrupt service and management traffic by generating a large number of connection tracking entries, which exhausts connection tracking table resources and prevents legitimate connection requests from being received.

The table below defines shows the distribution of the above ten VPC's across all the assets and environments.

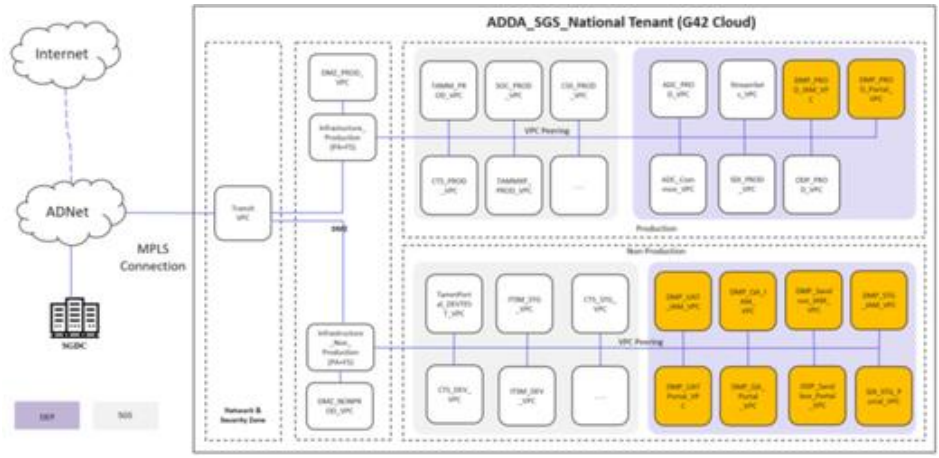
Asset Name	**Asset**	**VPC List**	**Environment**

cce-dmp-stg-iam	CCE	vpc-adda-dep-dmp-iam-stage	STG
cce-dmp-stg-portal	CCE	vpc-adda-dep-dmp-portal-stage	STG
ecs-dmp-stg-jump-server	ECS	vpc-adda-dep-dmp-portal-stage	STG
ecs-dmp-stg-proxy-server-01	ECS	vpc-adda-dep-dmp-iam-stage	STG
ecs-dmp-stg-proxy-server-02	ECS	vpc-adda-dep-dmp-iam-stage	STG
Dynatrace-POC	ECS	vpc-adda-dep-dmp-portal-stage	STG
ecs-dmp-stg-edge-registry	ECS	vpc-adda-dep-dmp-portal-stage	STG
elb-adda-dep-dmp-nginx-stage	ELB	vpc-adda-dep-dmp-iam-stage	STG
elb-adda-dep-dmp-console-stage	ELB	vpc-adda-dep-dmp-portal-stage	STG
elb-adda-dep-dmp-api-stage	ELB	vpc-adda-dep-dmp-portal-stage	STG
elb-adda-dep-dmp-iam-stage	ELB	vpc-adda-dep-dmp-iam-stage	STG
css-dmp-portal-stage	CSS	vpc-adda-dep-dmp-portal-stage	STG
rds-dmp-iam-stage	RDS	vpc-adda-dep-dmp-iam-stage	STG
rds-dmp-portal-stage	RDS	vpc-adda-dep-dmp-portal-stage	STG
mrs-dmp-stg-portal	MRS	vpc-adda-dep-dmp-portal-stage	STG
mrs-dmp-stg-portal-v1	MRS	vpc-adda-dep-dmp-portal-stage	STG
rabbitmq-dmp-stg	DMS	vpc-adda-dep-dmp-portal-stage	STG
dbss-dmp-stg-iam	DBSS	vpc-adda-dep-dmp-iam-stage	STG
dbss-dmp-stg-portal	DBSS	vpc-adda-dep-dmp-portal-stage	STG
cce-dmp-prod-iam	CCE	vpc-adda-dep-dmp-iam-production	PRD
cce-dmp-prod-portal	CCE	vpc-adda-dep-dmp-portal-production	PRD
ecs-dmp-prod-proxy-server-01	ECS	vpc-adda-dep-dmp-iam-production	PRD
ecs-dmp-prod-proxy-server-02	ECS	vpc-adda-dep-dmp-iam-production	PRD
ecs-dmp-prod-jump-server	ECS	vpc-adda-dep-dmp-portal-production	PRD
ecs-dmp-prod-edge-registry	ECS	vpc-adda-dep-dmp-portal-production	PRD

elb-adda-dep-dmp-nginx-production	ELB	vpc-adda-dep-dmp-iam-production	PRD
elb-adda-dep-dmp-console-production	ELB	vpc-adda-dep-dmp-portal-production	PRD
elb-adda-dep-dmp-api-production	ELB	vpc-adda-dep-dmp-portal-production	PRD
elb-adda-dep-dmp-iam-production	ELB	vpc-adda-dep-dmp-iam-production	PRD
css-dmp-portal-production	CSS	vpc-adda-dep-dmp-portal-production	PRD
rds-dmp-iam-production	RDS	vpc-adda-dep-dmp-iam-production	PRD
rds-dmp-portal-production	RDS	vpc-adda-dep-dmp-portal-production	PRD
mrs-dmp-prod-portal	MRS	vpc-adda-dep-dmp-portal-production	PRD
mrs-dmp-prod-portal-v1	MRS	vpc-adda-dep-dmp-portal-production	PRD
rabbitmq-dmp-prod	DMS	vpc-adda-dep-dmp-portal-production	PRD
dbss-dmp-prod-iam	DBSS	vpc-adda-dep-dmp-iam-production	PRD
dbss-dmp-prod-portal	DBSS	vpc-adda-dep-dmp-portal-production	PRD
cce-dmp-uat-iam	CCE	vpc-adda-dep-dmp-iam-uat	UAT
cce-dmp-uat-portal	CCE	vpc-adda-dep-dmp-portal-uat	UAT
ecs-dmp-uat-jump-server	ECS	vpc-adda-dep-dmp-portal-uat	UAT
ecs-dmp-uat-sftp-01	ECS	vpc-adda-dep-dmp-portal-uat	UAT
ecs-dmp-uat-edge-02	ECS	vpc-adda-dep-dmp-portal-uat	UAT
ecs-dmp-uat-edge-03	ECS	vpc-adda-dep-dmp-portal-uat	UAT
ecs-dmp-uat-oracle-04	ECS	vpc-adda-dep-dmp-portal-uat	UAT
ecs-dmp-uat-erwin-05	ECS	vpc-adda-dep-dmp-portal-uat	UAT
ecs-dmp-uat-edge-registry	ECS	vpc-adda-dep-dmp-portal-uat	UAT

elb-adda-dep-dmp-console-uat	ELB	vpc-adda-dep-dmp-portal-uat	UAT
elb-adda-dep-dmp-api-uat	ELB	vpc-adda-dep-dmp-portal-uat	UAT
elb-adda-dep-dmp-iam-uat	ELB	vpc-adda-dep-dmp-iam-uat	UAT
css-dmp-portal-uat	CSS	vpc-adda-dep-dmp-portal-uat	UAT
rds-dmp-iam-uat	RDS	vpc-adda-dep-dmp-iam-uat	UAT
rds-dmp-portal-uat	RDS	vpc-adda-dep-dmp-portal-uat	UAT
rds-dmp-portal-uat-datasource-01	RDS	vpc-adda-dep-dmp-portal-uat	UAT
rds-dmp-portal-uat-datasource-02	RDS	vpc-adda-dep-dmp-portal-uat	UAT
dws-dmp-uat-01	DWS	vpc-adda-dep-dmp-portal-uat	UAT
mrs-dmp-uat-portal	MRS	vpc-adda-dep-dmp-portal-uat	UAT
mrs-dmp-uat-portal-v1	MRS	vpc-adda-dep-dmp-portal-uat	UAT
rabbitmq-dmp-uat	DMS	vpc-adda-dep-dmp-portal-uat	UAT
dbss-dmp-uat-iam	DBSS	vpc-adda-dep-dmp-iam-uat	UAT
dbss-dmp-uat-portal	DBSS	vpc-adda-dep-dmp-portal-uat	UAT
cce-dmp-qa-iam	CCE	vpc-adda-dep-dmp-iam-qa	QA
cce-dmp-qa-portal	CCE	vpc-adda-dep-dmp-portal-qa	QA
ecs-dmp-qa-jump-server	ECS	vpc-adda-dep-dmp-portal-qa	QA
ecs-dmp-qa-edge-registry	ECS	vpc-adda-dep-dmp-portal-qa	QA
elb-adda-dep-dmp-console-qa	ELB	vpc-adda-dep-dmp-portal-qa	QA
elb-adda-dep-dmp-api-qa	ELB	vpc-adda-dep-dmp-portal-qa	QA
elb-adda-dep-dmp-iam-qa	ELB	vpc-adda-dep-dmp-iam-qa	QA
css-dmp-portal-qa	CSS	vpc-adda-dep-dmp-portal-qa	QA
rds-dmp-iam-qa	RDS	vpc-adda-dep-dmp-iam-qa	QA
rds-dmp-portal-qa	RDS	vpc-adda-dep-dmp-portal-qa	QA
mrs-dmp-qa-portal	MRS	vpc-adda-dep-dmp-portal-qa	QA
mrs-dmp-qa-portal-v1	MRS	vpc-adda-dep-dmp-portal-qa	QA
rabbitmq-dmp-qa	DMS	vpc-adda-dep-dmp-portal-qa	QA
dbss-dmp-qa-iam	DBSS	vpc-adda-dep-dmp-iam-qa	QA
dbss-dmp-qa-portal	DBSS	vpc-adda-dep-dmp-portal-qa	QA

cce-dmp-rnd-iam	CCE	vpc-adda-dep-dmp-iam-RnD	RnD
cce-dmp-rnd-portal	CCE	vpc-adda-dep-dmp-portal-RnD	RnD
ecs-dmp-rnd-jump-server	ECS	vpc-adda-dep-dmp-portal-RnD	RnD
sgs-rnd-str-sch-01	ECS	vpc-adda-dep-dmp-portal-RnD	RnD
sgs-rnd-str-sdc01	ECS	vpc-adda-dep-dmp-portal-RnD	RnD
sgs-rnd-str-sdc02	ECS	vpc-adda-dep-dmp-portal-RnD	RnD
sgs-rnd-adda-ecs01	ECS	vpc-adda-dep-dmp-portal-RnD	RnD
sgs-rnd-adda-ecs02	ECS	vpc-adda-dep-dmp-portal-RnD	RnD
sgs-rnd-adda-ecs03	ECS	vpc-adda-dep-dmp-portal-RnD	RnD
sgs-rnd-adda-ecs04	ECS	vpc-adda-dep-dmp-portal-RnD	RnD
sgs-rnd-adda-ecs05	ECS	vpc-adda-dep-dmp-portal-RnD	RnD
ecs-dmp-rnd-edge-registry	ECS	vpc-adda-dep-dmp-portal-rnd	RnD
elb-adda-dep-dmp-console-rnd	ELB	vpc-adda-dep-dmp-portal-RnD	RnD
elb-adda-dep-dmp-api-rnd	ELB	vpc-adda-dep-dmp-portal-RnD	RnD
elb-adda-dep-dmp-iam-rnd	ELB	vpc-adda-dep-dmp-iam-RnD	RnD
css-dmp-portal-rnd	CSS	vpc-adda-dep-dmp-portal-RnD	RnD
rds-sgs-rnd-postgre-sch-01	RDS	vpc-adda-dep-dmp-portal-RnD	RnD
rds-dmp-iam-rnd	RDS	vpc-adda-dep-dmp-iam-RnD	RnD
rds-dmp-portal-rnd	RDS	vpc-adda-dep-dmp-portal-RnD	RnD
mrs-dmp-rnd-portal	MRS	vpc-adda-dep-dmp-portal-RnD	RnD
mrs-dmp-rnd-portal-v1	MRS	vpc-adda-dep-dmp-portal-RnD	RnD
rabbitmq-dmp-rnd	DMS	vpc-adda-dep-dmp-portal-RnD	RnD
dbss-dmp-rnd-iam	DBSS	vpc-adda-dep-dmp-iam-RnD	RnD
dbss-dmp-rnd-portal	DBSS	vpc-adda-dep-dmp-portal-RnD	RnD



Then the traffic will flow through the VPC peering to the Destination VPC, shown in the Architecture in the above diagram. A VPC peering connection is a network connection between two VPCs in one region that enables you to route traffic between them using private IP addresses. ECSs in either VPC can communicate with each other just as if they were in the same region. You can create a VPC peering connection between your own VPCs, or between your VPC and another account's VPC within the same region. However, you cannot create a VPC peering connection between VPCs in different regions.

The tenant infrastructure is divided into three logical zones. Production, non-production and demilitarized (DMZ) zone in order to isolate production and non-production traffic.

Production zone hosts the infrastructure resources required for the production environments of different shared services. DMP production environment consumes the shared resources such as firewall and load balancer. DMP staging environment is part of this group, i.e. all traffic between the VPC flows through the PaloAlto, therefore allowing for East/West traffic security adherance.

Transit VPC: All inbound connections (VPN and DC) will be terminated in transit VPC. This VPC acts as the transit for the communication between ADGEs and G42 Cloud tenant. This alklows for network segmentation and an isolation of the traffic from production and non-production VPC’s

DMZ Prod VPC: A centralized production VPC where firewall virtual appliance instances are deployed. This VPC peers with DMP production environment VPCs to provide secure connectivity.

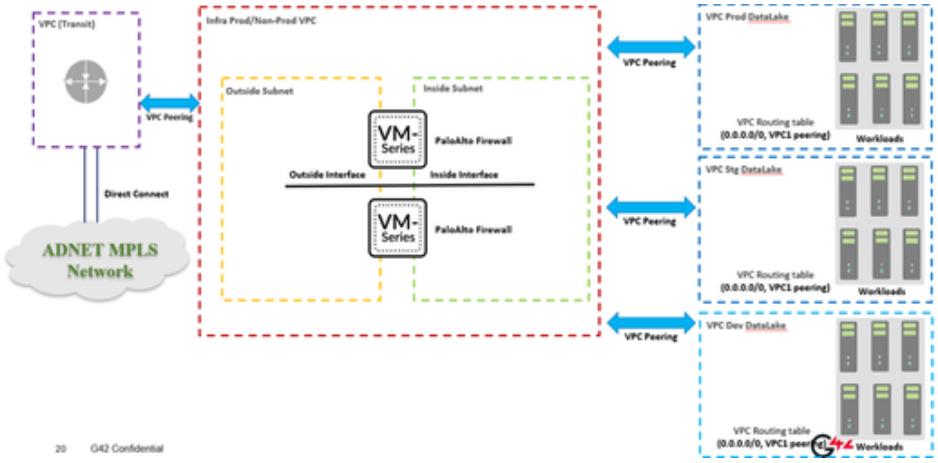
DMZ Non-Prod VPC: A centralized production VPC where firewall virtual appliance instances are deployed. This VPC peers with DMP non-production environment VPCs to provide secure connectivity.

Landing VPC : Contains the resources for ingestion such as CDM, DIS and SFTP server deployed on top of ECS.

Datalake VPC: Datalake VPC hosts the DWS and DLI services.

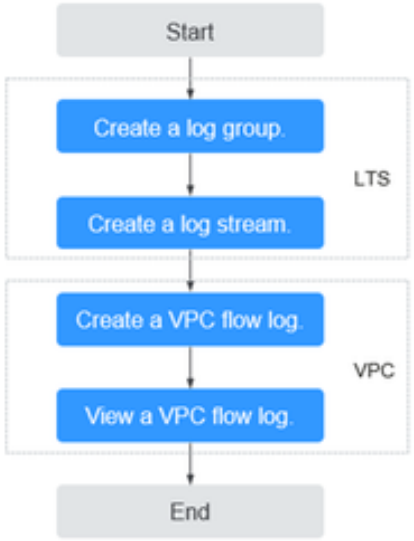
Datalake Application VPC: Datalake application VPC hosts analytics services for KPI publishing, CCE cluster and CSS cluster.

The diagram below shows how security is applied using PA for each of the network segmentations as defined below for Staging and Production.



A VPC flow log records information about the traffic going to and from a VPC. VPC flow logs help you monitor network traffic, analyze network attacks, and determine whether security group and network ACL rules require modification.

VPC flow logs must be used together with the Log Tank Service (LTS). Before you create a VPC flow log, you need to create a log group and a log stream in LTS.



ACL - Network ACL and SG -Security Groups

Network ACLs and security groups are both major factors in enhancing the cybersecurity of G42 Cloud VPCs, understanding the differences between them is important for creating effective network security policies for VPCs. These differences are summarized in the table below.

After the network segmentation provided by VPC, further security zoning is enforced by apply Security Group's on ECS assets. Security Groups protect the traffic flow inside the VPC's to ensure that only the IPs allocated specific traffic rule (using security group rules) are applied between assets inside the VPC.

Security Groups support:

- Work on the a wide range of cloud asset at the instance level (first layer of protection).
- Support permit policies.
- If rules conflict with each other, only the parts in agreement take effect.
- Must be selected when an Elastic Cloud Server instance is created; take effect automatically on Elastic Cloud Server instances.
- Support packet filtering by 3-tuple (protocol, port, and destination IP address).

Security Groups are a collection of access control rules for cloud resources, such as cloud servers, containers, and databases, that have the same security protection requirements and that are mutually trusted within a VPC. For DMP, security groups are created for EDGE traffic, such that various access rules are applied to direct the traffic to the CCE clusters where the SSL is terminated. These rules are applied by the Console Administrators are not changed without strict administration protocols.

For DMP there are a total of 33 Security Groups as follows:

1. cce-dmp-stg-iam-cce-node
1. cce-dmp-stg-portal-cce-node
1. Sys-default
1. cce-dmp-stage-portal-cce-node
1. sg-adda-dep-dmp-css
1. sg-adda-dep-dmp-rds-stage
1. mrs_mrs-dmp-stg-port

1. cce-dmp-prod-iam-cce-node
1. cce-dmp-prod-portal-cce-node
10. sg-adda-dep-dmp-rds-production
11. mrs_mrs-dmp-prod-port
12. cce-dmp-uat-iam-cce-node
13. cce-dmp-uat-portal-cce-node
14. sg-UAT-ecs
15. sg-adda-dep-dmp-css-uat
16. sg-adda-dep-dmp-rds-uat
17. sg-dws-dmp-uat-00
18. sg-dws-dmp-uat-01
19. mrs_mrs-dmp-uat-port
20. sg-adda-dep-dmp-MQ-uat
21. cce-dmp-qa-iam-cce-node
22. cce-dmp-qa-portal-cce-node
23. sg-adda-dep-dmp-css-qa
24. sg-adda-dep-dmp-rds-qa
25. mrs_mrs-dmp-qa
26. sg-adda-dep-dmp-MQ-qa
27. cce-dmp-rnd-iam-cce-node
28. cce-dmp-rnd-portal-cce-node
29. sg-adda-dep-dmp-css-rnd
30. sgs-dep-rnd-sg
31. sg-adda-dep-dmp-rds-rnd
32. mrs_mrs-dmp-rnd
33. sg-adda-dep-dmp-MQ-rnd

The above Security Groups are distributed across the cloud assets and environments as shown in the below table:

Asset Name	Asset	Security Enhancement	Environment
cce-dmp-stg-iam	CCE	cce-dmp-stg-iam-cce-node	STG
cce-dmp-stg-portal	CCE	cce-dmp-stg-portal-cce-node	STG
ecs-dmp-stg-jump-server	ECS	cce-dmp-stg-portal-cce-node	STG
ecs-dmp-stg-proxy-server-01	ECS	cce-dmp-stg-iam-cce-node	STG
ecs-dmp-stg-proxy-server-02	ECS	cce-dmp-stg-iam-cce-node	STG
Dynatrace-POC	ECS	Sys-default	STG
ecs-dmp-stg-edge-registry	ECS	cce-dmp-stage-portal-cce-node	STG
css-dmp-portal-stage	CSS	sg-adda-dep-dmp-css	STG
rds-dmp-iam-stage	RDS	sg-adda-dep-dmp-rds-stage	STG
rds-dmp-portal-stage	RDS	sg-adda-dep-dmp-rds-stage	STG
mrs-dmp-stg-portal	MRS	mrs_mrs-dmp-stg-port	STG
mrs-dmp-stg-portal-v1	MRS	mrs_mrs-dmp-stg-port	STG
rabbitmq-dmp-stg	DMS for RabbitMQ	cce-dmp-stg-portal-cce-node	STG
cce-dmp-prod-iam	CCE	cce-dmp-prod-iam-cce-node	PRD
cce-dmp-prod-portal	CCE	cce-dmp-prod-portal-cce-node	PRD
ecs-dmp-prod-proxy-server-01	ECS	cce-dmp-prod-iam-cce-node	PRD
ecs-dmp-prod-proxy-server-02	ECS	cce-dmp-prod-iam-cce-node	PRD
ecs-dmp-prod-jump-server	ECS	cce-dmp-prod-portal-cce-node	PRD
ecs-dmp-prod-edge-registry	ECS	cce-dmp-prod-portal-cce-node	PRD
css-dmp-portal-production	CSS	sg-adda-dep-dmp-css	PRD
rds-dmp-iam-production	RDS	sg-adda-dep-dmp-rds-production	PRD

rds-dmp-portal-production	RDS	sg-adda-dep-dmp-rds-production	PRD
mrs-dmp-prod-portal	MRS	mrs_mrs-dmp-prod-port	PRD
mrs-dmp-prod-portal-v1	MRS	mrs_mrs-dmp-prod-port	PRD
rabbitmq-dmp-prod	DMS for RabbitMQ	cce-dmp-prod-portal-cce-node	PRD
cce-dmp-uat-iam	CCE	cce-dmp-uat-iam-cce-node	UAT
cce-dmp-uat-portal	CCE	cce-dmp-uat-portal-cce-node	UAT
ecs-dmp-uat-jump-server	ECS	cce-dmp-uat-portal-cce-node	UAT
ecs-dmp-uat-sftp-01	ECS	sg-UAT-ecs	UAT
ecs-dmp-uat-edge-02	ECS	sg-UAT-ecs	UAT
ecs-dmp-uat-edge-03	ECS	sg-UAT-ecs	UAT
ecs-dmp-uat-oracle-04	ECS	sg-UAT-ecs	UAT
ecs-dmp-uat-erwin-05	ECS	sg-UAT-ecs	UAT
ecs-dmp-uat-edge-registry	ECS	cce-dmp-uat-portal-cce-node	UAT
css-dmp-portal-uat	CSS	sg-adda-dep-dmp-css-uat	UAT
rds-dmp-iam-uat	RDS	sg-adda-dep-dmp-rds-uat	UAT
rds-dmp-portal-uat	RDS	sg-adda-dep-dmp-rds-uat	UAT
rds-dmp-portal-uat-datasource-01	RDS	sg-adda-dep-dmp-rds-uat	UAT
rds-dmp-portal-uat-datasource-02	RDS	sg-adda-dep-dmp-rds-uat	UAT
dli_dmp_uat_sql_01	DWS	sg-dws-dmp-uat-00	UAT
dws-dmp-uat-01	DWS	sg-dws-dmp-uat-01	UAT
mrs-dmp-uat-portal	MRS	mrs_mrs-dmp-uat-port	UAT
mrs-dmp-uat-portal-v1	MRS	mrs_mrs-dmp-uat-port	UAT
rabbitmq-dmp-uat	DMS for RabbitMQ	sg-adda-dep-dmp-MQ-uat	UAT
dbss-dmp-uat-iam	DBSS	sg-adda-dep-dmp-rds-uat	UAT

dbss-dmp-uat-portal	DBSS	sg-adda-dep-dmp-rds-uat	UAT
cce-dmp-qa-iam	CCE	cce-dmp-qa-iam-cce-node	QA
cce-dmp-qa-portal	CCE	cce-dmp-qa-portal-cce-node	QA
ecs-dmp-qa-jump-server	ECS	cce-dmp-qa-portal-cce-node	QA
ecs-dmp-qa-edge-registry	ECS	cce-dmp-qa-portal-cce-node	QA
css-dmp-portal-qa	CSS	sg-adda-dep-dmp-css-qa	QA
rds-dmp-iam-qa	RDS	sg-adda-dep-dmp-rds-qa	QA
rds-dmp-portal-qa	RDS	sg-adda-dep-dmp-rds-qa	QA
mrs-dmp-qa-portal	MRS	mrs_mrs-dmp-qa	QA
mrs-dmp-qa-portal-v1	MRS	mrs_mrs-dmp-qa	QA
rabbitmq-dmp-qa	DMS for RabbitMQ	sg-adda-dep-dmp-MQ-qa	QA
dbss-dmp-qa-iam	DBSS	sg-adda-dep-dmp-rds-qa	QA
dbss-dmp-qa-portal	DBSS	sg-adda-dep-dmp-rds-qa	QA
cce-dmp-rnd-iam	CCE	cce-dmp-rnd-iam-cce-node	RnD
cce-dmp-rnd-portal	ECS	cce-dmp-rnd-portal-cce-node	RnD
ecs-dmp-rnd-jump-server	ECS	cce-dmp-rnd-portal-cce-node	RnD
sgs-rnd-str-sch-01	ECS	cce-dmp-rnd-portal-cce-node	RnD
sgs-rnd-str-sdc01	ECS	cce-dmp-rnd-portal-cce-node	RnD
sgs-rnd-str-sdc02	ECS	cce-dmp-rnd-portal-cce-node	RnD
sgs-rnd-adda-ecs01	ECS	cce-dmp-rnd-portal-cce-node	RnD
sgs-rnd-adda-ecs02	ECS	cce-dmp-rnd-portal-cce-node	RnD
sgs-rnd-adda-ecs03	ECS	cce-dmp-rnd-portal-cce-node	RnD
sgs-rnd-adda-ecs04	ECS	cce-dmp-rnd-portal-cce-node	RnD

sgs-rnd-adda-ecs05	ECS	cce-dmp-rnd-portal-cce-node	RnD
ecs-dmp-rnd-edge-registry	ECS	cce-dmp-rnd-portal-cce-node	RnD
css-dmp-portal-rnd	CSS	sg-adda-dep-dmp-css-rnd	RnD
rds-sgs-rnd-postgre-sch-01	RDS	sgs-dep-rnd-sg	RnD
rds-dmp-iam-rnd	RDS	sg-adda-dep-dmp-rds-rnd	RnD
rds-dmp-portal-rnd	RDS	sg-adda-dep-dmp-rds-rnd	RnD
mrs-dmp-rnd-portal	MRS	mrs_mrs-dmp-rnd	RnD
mrs-dmp-rnd-portal-v1	MRS	mrs_mrs-dmp-rnd	RnD
rabbitmq-dmp-rnd	DMS for RabbitMQ	sg-adda-dep-dmp-MQ-rnd	RnD
dbss-dmp-rnd-iam	DBSS	sg-adda-dep-dmp-rds-RnD	RnD
dbss-dmp-rnd-portal	DBSS	sg-adda-dep-dmp-rds-RnD	RnD

For DMP: there are 33 unique Security Groups applied across a range of assets. Therefore, prior to traffic landing in CCE's (cluster), the traffic will be channelled through specific security group rules to ensure that the traffic is provided the specific controls to avoid broadcasting across the VPC, instead it is routed to the correct CCE via VPC peering's and Security Groups rules.

NOTE: Default Security Groups are disabled in DMP and only configurable and customised security groups are applied.

Network ACLs are systems that specify, maintain, and enforce access control policies for one or more subnets. They determine whether to permit packets to enter or leave a subnet based on the inbound or outbound rules associated with that subnet. This service functions on the network traffic level and is consider the 2nd layer of protection after security group allocation. This supports permission and denial of polices.

1.1.1 ELB - Elastic Load Balancer

Elastic Load Balance (ELB) automatically distributes access traffic among multiple Elastic Cloud Servers, improving the ability of application systems to provide service and enhancing the fault tolerance of application programs.

For the DMP deployment the following ELBs are provisioned:

#	Env	Asset Name	Asset	VPC location	Security Group Settings (if inside a security group, please specify)	Security Controls
1	PRD	elb-adda-dep-dmp-nginx-production	ELB	vpc-adda-dep-dmp-iam-production	N/A	• IP address and port **masking** • Automatic **scaling** based on traffic status • ELB Intranet **security groups** • Source IP address **transparency** • **SSL/TLS offloading** and certificate management • Support for **encryption** protocols and cipher suites
2	PRD	elb-adda-dep-dmp-console-production	ELB	vpc-adda-dep-dmp-portal-production	N/A	
3	PRD	elb-adda-dep-dmp-api-production	ELB	vpc-adda-dep-dmp-portal-production	N/A	
4	PRD	elb-adda-dep-dmp-iam-production	ELB	vpc-adda-dep-dmp-iam-production	N/A	
5	STG	elb-adda-dep-dmp-nginx-stage	ELB	vpc-adda-dep-dmp-iam-stage	N/A	
6	STG	elb-adda-dep-dmp-console-stage	ELB	vpc-adda-dep-dmp-portal-stage	N/A	
7	STG	elb-adda-dep-dmp-api-stage	ELB	vpc-adda-dep-dmp-portal-stage	N/A	
8	STG	elb-adda-dep-dmp-iam-stage	ELB	vpc-adda-dep-dmp-iam-stage	N/A	
9	UAT	elb-adda-dep-dmp-console-uat	ELB	vpc-adda-dep-dmp-portal-uat	N/A	
10	UAT	elb-adda-dep-dmp-api-uat	ELB	vpc-adda-dep-dmp-portal-uat	N/A	
11	UAT	elb-adda-dep-dmp-iam-uat	ELB	vpc-adda-dep-dmp-iam-uat	N/A	
12	QA	elb-adda-dep-dmp-console-qa	ELB	vpc-adda-dep-dmp-portal-qa	N/A	

13	QA	elb-adda-dep-dmp-api-qa	ELB	vpc-adda-dep-dmp-portal-qa	N/A	
14	QA	elb-adda-dep-dmp-iam-qa	ELB	vpc-adda-dep-dmp-iam-qa	N/A	
15	RnD	elb-adda-dep-dmp-console-rnd	ELB	vpc-adda-dep-dmp-portal-RnD	N/A	
16	RnD	elb-adda-dep-dmp-api-rnd	ELB	vpc-adda-dep-dmp-portal-RnD	N/A	
17	RnD	elb-adda-dep-dmp-iam-rnd	ELB	vpc-adda-dep-dmp-iam-RnD	N/A	

Note: Certificates are stored on OBS and currently managed manually.

ELB provides the following security functions:

- IP address and port masking: ELB allows external networks to see only a single IP address and service port(s); the actual IP address(es) and port(s) used by the backend are not exposed. This prevents the disclosure of network information and minimizes the attack surface.
- Automatic scaling based on traffic status: ELB can work with AS to provide more flexible scaling and better DDoS mitigation than the traditional method of directly connecting to single backend server(s) and service(s).
- ELB Intranet security groups: ELB security groups can be created on a tenant's intranet to ensure that tenant instances only receive traffic from the load balancer. Tenants can define allowed ports and protocols to ensure that traffic in both directions is sent through ELB. For a detailed description of security groups, see section on VPC.
- Source IP address transparency: ELB can transparently transmit source IP addresses when listening for HTTP and HTTPS services. This enables tenants to perform source tracing, collect connection or traffic statistics, enforce blacklisting or whitelisting for source IP addresses, and perform other tasks needed to meet enhanced security requirements. By implementing these through their applications, tenants can more quickly detect and respond to attacks.
- SSL/TLS offloading and certificate management: With SSL/TLS offloading, the SSL/TLS encryption and decryption of packets is performed on ELB, reducing the processing burden that these tasks place on the tenant's backend server. In this process, encrypted traffic is sent to ELB for decryption and then delivered to the tenant's backend server; likewise, outbound traffic is sent to ELB for encryption and then on to its destination. To use SSL/TLS offloading, tenants must upload any SSL/TLS certificates and private keys required to ELB for management.
- Support for encryption protocols and cipher suites: Tenants communicating with ELB over HTTPS can select an encryption protocol and configuration as required. TLS 1.2 is

used by default. Tenants requiring higher security and more robust encryption algorithms can select them from ELB's extended list of cipher suites.

SOC Integration

SOC integration will be between the Production VPC cloud assets to the ADDA SOC applications. This section details the logs that the system will make available to support the SOC. Multiple logs will be captured as part of the infrastructure and application.

The system will use ICAgent, filebeats and syslogs and based on the SOC team's request, these logs will be available to the SOC team. The SOC team logs will provide the following minimal set of logs to the ADDA SOC team:

1. DMP Portal Logs.
2. CCE, MRS logs and will be concentrating only on the application/security related logs.
3. Differentiation of the useful logs from the LTS can be performed and forwarded to the SIEM
4. Below are different log sources that was decided to be send as part of the initial phase

a) IAM authentication logs

b) Application logs

c) Audit Logs

d) EDGE component logs

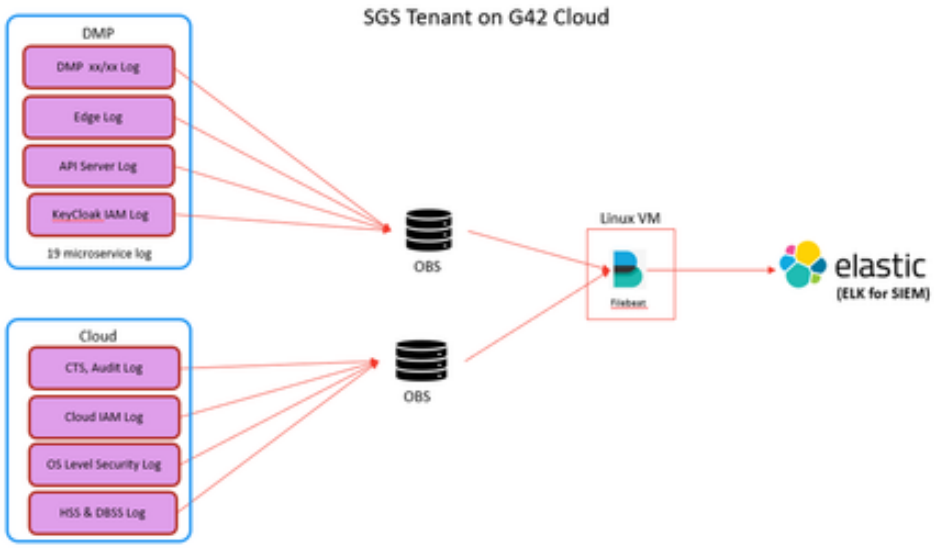
e) API server logs

f) OS level Security logs for all servers

g) HSS and DBSS logs

1. With reference to the IAM solutions, only the application logs will be sent to the OBS bucket using the filebeat and it will be further pushed to the ADDA SOC SIEM.
2. If a new instance of an OBS bucket (with filebeats) is needed to support additional logs, this will need to be provided and the Firewall rules will need to be updated to parse the logs to the SOC SIEM.
3. VDI access logging will also need to be considered by the SOC team and will be mostly based on authentication via VDI.
4. ICAgent server logs will be considered based on a deep dive discussion with the SOC team. NB: Additional logs captured by the SOC team will require adequate licencing be provided by the ADGE SOC Team.

The diagram below depicts the SOC integration high-level design using file-beats integrtaio nto the ADDA SOC SIEM.



In the above diagram, the DMP and Cloud native logs originating from the Production VPC in the DMP Enterprise project are transferred to intermediate OBS, one for DMP and the other for Cloud Native, as depicted in the diagram above. Filebeat is implemented in a ECS which is configured to pull data from the two buckets and is primarily used to curate the logs in readiness for the Elastic SIEM.

Given Filebeat and eslastic are based on the same technical upderpinning, i.e elastric search, the inetrgation between the Cloud native logs and DMP logs from the OBS will be using a direct elastic search listener from where the SIEM elastic will ‘pull’ logs to ADDA SOC.

The PaloAlto Firwall rules must be changed to the production VPC to ensure dataflow is allowed uni-dorectional from the Filebeat in the Cloud Productio VPC (G42 Cloud) to the Elastic SIEM (ADDA SOC).

For the DMP log, the list of log files that will be used for the OBS bucket polling done by Filebeat is listed below:

In the above diagram, the DMP and Cloud native logs originating from the Production VPC in the DMP Enterprise project are transferred to intermediate OBS, one for DMP and the other for Cloud Native, as depicted in the diagram above. Filebeat is implemented in a ECS which is configured to pull data from the two buckets and is primarily used to curate the logs in readiness for the Elastic SIEM.

Given Filebeat and eslastic are based on the same technical upderpinning, i.e elastric search, the inetrgation between the Cloud native logs and DMP logs from the OBS will be using a direct elastic search listener from where the SIEM elastic will ‘pull’ logs to ADDA SOC.

The PaloAlto Firwall rules must be changed to the production VPC to ensure dataflow is allowed uni-dorectional from the Filebeat in the Cloud Productio VPC (G42 Cloud) to the Elastic SIEM (ADDA SOC).

For the DMP log, the list of log files that will be used for the OBS bucket polling done by Filebeat is listed below:

DMP Service Log Name	Enterpirse Proj.	VPC Name	Source Bucket Name	subPath
keycloak	dmp-iam	cce-obs-dmp-iam	pvc-8db6ca11-a371-48e5-8260-2fc3a5a3636d	/opt/keycloak/logs
registry	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/registry/logs
metric	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/edge-admin/logs
ad-console	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/edge-admin/logs
edge-admin	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/edge-admin/logs
docs-console	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/edge-admin/logs
edge-console	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/edge-admin/logs
catalog	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/catalog/logs
console	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/console/logs
apache-atlas	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/apache-atlas/logs
metadata	dmp-sharing	cce-obs-data-sharing	pvc-e66efebc-081c-4710-a905-400fa0d2e739	/opt/metadata/logs
ad-server	dmp-sharing	cce-obs-data-sharing	pvc-e66efebc-081c-4710-a905-400fa0d2e739	/opt/ad-server/logs
gateway	dmp-sharing	cce-obs-data-sharing	pvc-e66efebc-081c-4710-a905-400fa0d2e739	/opt/gateway/logs
edge	dmp-sharing	cce-obs-data-sharing	pvc-e66efebc-081c-4710-a905-400fa0d2e739	/opt/edge/logs

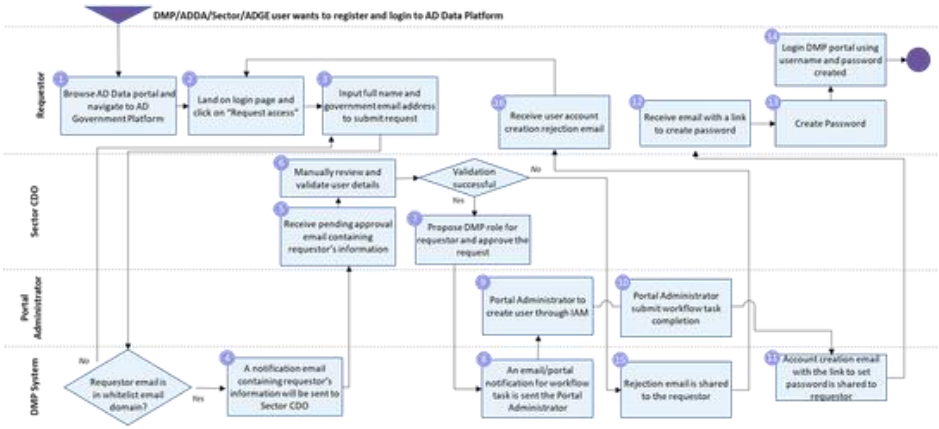
filebeat	dmp-sharing	cce-obs-data-sharing	pvc-e66efebc-081c-4710-a905-400fa0d2e739	/opt/filebeat/logs
connection	dmp-sharing	cce-obs-data-sharing	pvc-e66efebc-081c-4710-a905-400fa0d2e739	/opt/connection/logs
api-controller	dmp-sharing	cce-obs-data-sharing	pvc-e66efebc-081c-4710-a905-400fa0d2e739	/opt/api-controller/logs
api-server	dmp-sharing	cce-obs-data-sharing	pvc-e66efebc-081c-4710-a905-400fa0d2e739	/opt/api-server/logs
batch-copy	dmp-sharing	cce-obs-data-sharing	pvc-e66efebc-081c-4710-a905-400fa0d2e739	/opt/batch-copy/logs
schedule	dmp-sharing	cce-obs-data-sharing	pvc-e66efebc-081c-4710-a905-400fa0d2e739	/opt/schedule/logs
keycloak	dmp-iam	cce-obs-dmp-iam	pvc-8db6ca11-a371-48e5-8260-2fc3a5a3636d	/opt/keycloak/logs
registry	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/registry/logs
metric	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/edge-admin/logs
ad-console	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/edge-admin/logs
edge-admin	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/edge-admin/logs
docs-console	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/edge-admin/logs
edge-console	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/edge-admin/logs
catalog	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/catalog/logs
console	dmp-portal	cce-obs-dmp-portal	pvc-e35d435c-9893-457e-998c-7d0fb441efc0	/opt/console/logs

DMP Application Security

DMP is a unified data management solution that helps users classify, organize, discover, share and consume data across organizations to maximize data value. This article outlines the application architecture of DMP

Access control

User Access Management (UAM) is the administration of individual AD government users willing to browse, subscribe and publish data assets in Abu Dhabi Data platform. UAM follows below guiding principles in alignment with security and architecture requirements. The diagram below shows the business process flow for UAM for DMP:



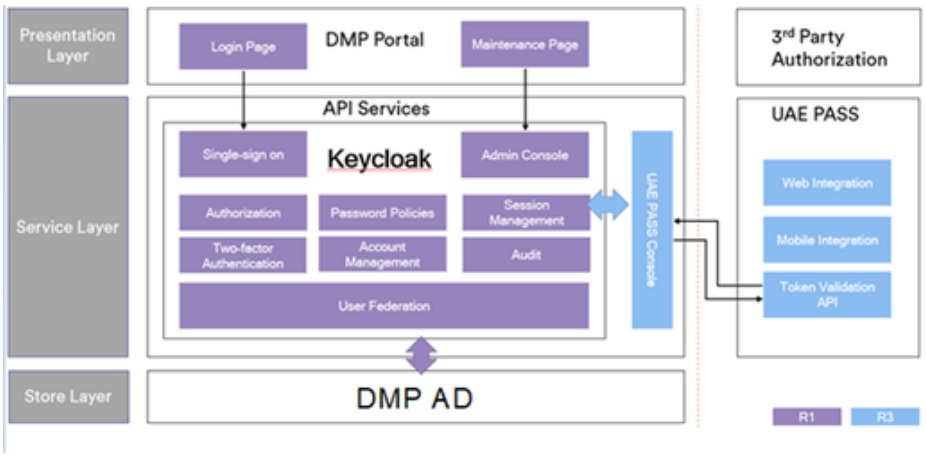
Principle of least privilege: every user in the platform can only access the information and resources necessary to perform their job functions.

An IAM solution is deployed on Data Management Platform – DMP. Datalake access for DMP will be the same as for the core DMP access using Keycloack Solution. The access and privilege control is the same as for G42 Console, i.e. by the G42 Cloud Managed Service Team. Refer to the DMP Security Architecture document for more detail.

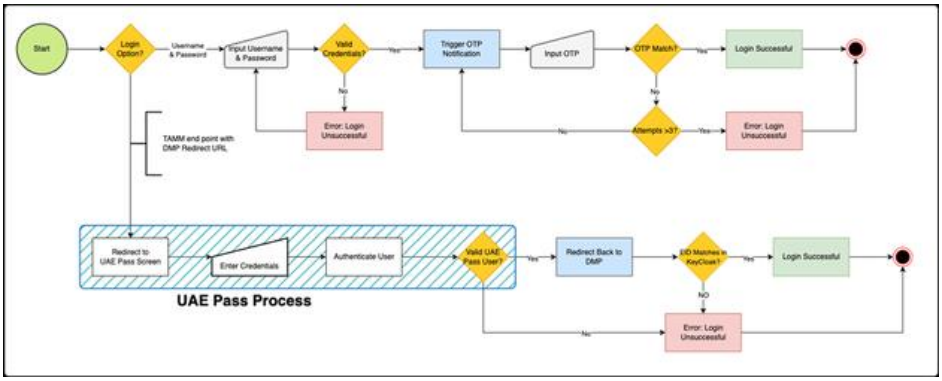
DMP access management using Keycloak

Keycloak is a 3rd party IAM solution and is used for acing the DMP portal by registered DMP Portal users, including approved ADGE users. Details about this product can be found here: https://www.keycloak.org/

The Keycloak implementation is as follows:



The diagram below is a logical view for DMP access management.



For Access Control Service, Keycloak is integrated with UAE PASS. Keycloak is an open-source Identity and Access Management solution targeted towards modern applications and services. Keycloak offers features such as Single-Sign-On (SSO), Identity Brokering and Social Login, User Federation, Client Adapters, an Admin Console, and an Account Management Console. As a requirement for DMP Portal access, Multi-Factor authentication (MFA) or Two Factor Authentication (2FA) must be enabled so that a user is required to present more than one type of evidence to authenticate on the system. MFA enhances the organization's security by requiring the users to identify themselves with more than a username and password. Even if usernames and passwords are leaked or stolen by other third parties due to vulnerabilities in the system, MFA protects user accounts from being hijacked. OTP generation and UAE PASS MFA is integrated into the IAM solution as part of the MFA requirements. This will add another layer of security when users log in to the DMP product.

Keycloak, is utilized for internal user registration, authentication and access control for DMP Portal. The overall objective of using Keycloak is to have a centralized solution for access and roles management. The scope of Access Control is as follows:

· Centralized solution – Through the admin console administrator can centrally manage all aspects of the access control:

o Create and manage applications and services and define fine-grained authorization policies.

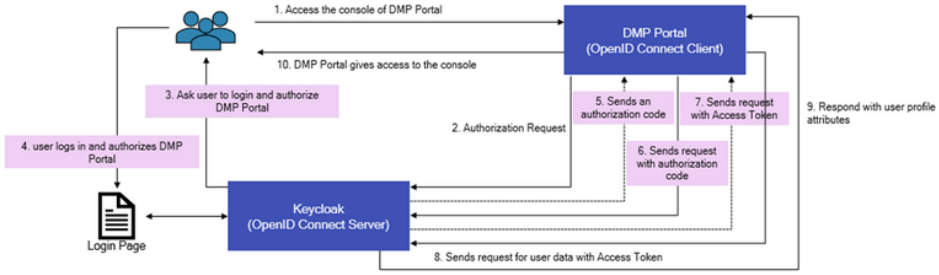
o Manage users, including permissions and sessions.

· Single Sign-On (SSO) – is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials. Keycloak has full support for Single Sign-On and Single Sign-Out.

· UAE PASS Integration – While Keycloak supports OAuth 2.0 and OpenID Connect (OIDC), it will integrate with UAE PASS to make external users able to access DMP Platform.

· The Single-Sign On (SSO) capability and flow from (1) to (7) is defined below.

The diagram below shows a high level view of Access Management using KeyCloak.



· Limit or eliminate super-user access privilege: follow zero-trust for all users and enforce an auditable process to grant any privilege.

Access control using Keycloak Administration Console provides the following:

· Manage Clients:

Clients that can request Keycloak to authenticate a user. Most often, clients are applications and services that want to use Keycloak to secure themselves and provide a single sign-on solution.

· Manage Users:

Users that can log into DMP Platform and other integrated applications. They can have attributes associated with themselves like email, username, address, phone number, and birthday. They can be assigned group membership and have specific roles assigned to them.

· Manage Roles:

Identify a type or category of user. Applications often assign access and permissions to specific roles rather than individual users as dealing with users can be hard to manage.

· Manage Session:

When a user logs in, a session is created to manage the login session. A session contains information like when the user logged in and what applications have participated within single sign-on during that session.The scope for UAEPass is as follows:

· UAE PASS as identity provider (IDP):

Keycloak will act as an Identity Broker is an intermediary service connecting service providers with identity providers. The identity broker creates a relationship with an external identity provider to use the provider's identities to access the internal services the service provider exposes.

· UAE PASS will be considered as default identity provider for Keycloak:

Keycloak will redirect the user by default to UAE PASS instead of asking the user to select UAE PASS login button inside Keycloak login form. User will be able to login or log out using UAE PASS through Keycloak.

· Events logging:

Keycloak will send logs to a centralized log management system like Elasticsearch. There are two kinds of events as following:

o Login Events: Are emitted every time a user-related action around authentication is executed, such as (login, logout, or code-to-token exchanges, …etc.).

o Admin Events: Are emitted on every change of a resource via Keycloak Admin API. Admin events will be stored internally in Keycloak for review

Out of scope is:

· New User registration with UAE Pass, i.e. UAEPass is not used for new user registration.

The Pre-requisite is:

· The user is registered in DMP via KeyCloak

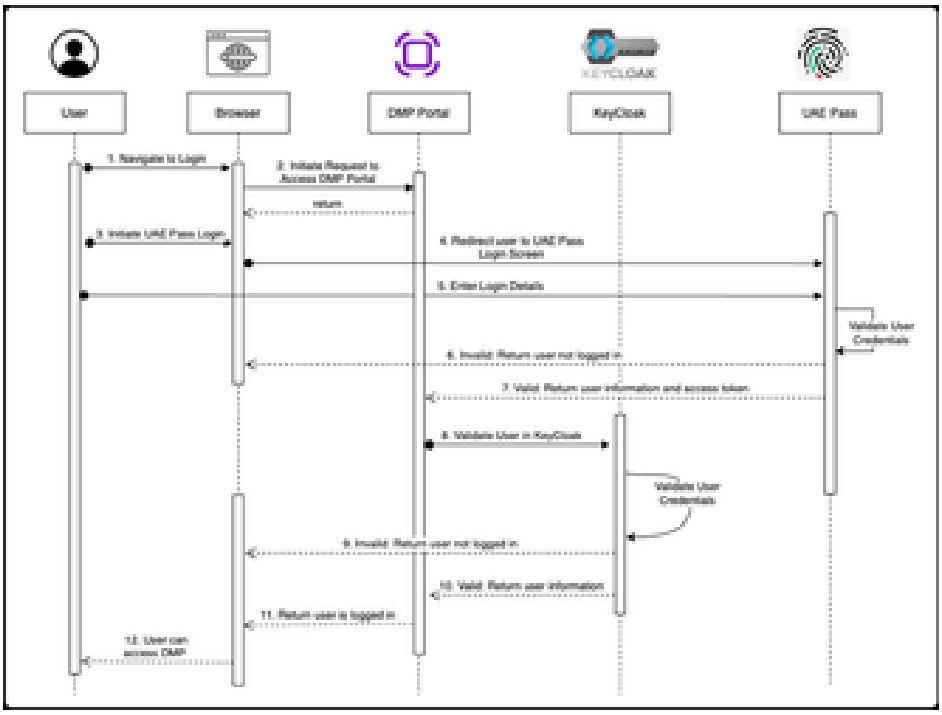
· The user has EID added to the user profile as an attribute in KeyCloak

Firewall updates to TAMM's UAEPass end points.

UAE Pass design

Keycloak, as defined above, provides a means by which integration to 3rd party IdP's is possible. This section defined elements of the integration between Keycloak and UAEPass. The objective is to integrate Keycloak with UAE PASS as a default identity provider, to make sure that the user experience will not be affected when trying to login or log out.

Login Flow Diagram for UAE Pass is shown below defined in blue below.



To integrate Keycloak with UAE PASS, the following should be provided:

- UAE PASS Client ID and Secret
- Authorization URL
- Token URL
- Logout URL
- User Info URL

Below is the UAE pass typical endpoints that are need to ensure UAEPass integration operates according to the sequence diagram shown above.

Authorization	https://stg-id.uaepass.ae/idshub/authorize	https://id.uaepass.ae/idshub/authorize
Token	https://stg-id.uaepass.ae/idshub/token	https://id.uaepass.ae/idshub/token
User Info	https://stg-id.uaepass.ae/idshub/userinfo	https://id.uaepass.ae/idshub/userinfo
Logout	https://stg-id.uaepass.ae/idshub/logout	https://id.uaepass.ae/idshub/logout

To have an identity provider we should select the proper type for that provider, in our case we will select OpenID Connect while is the same identity layer in UAE PASS. OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

In OpenID Connect protocol we will follow Authorization Code Flow which is required by UAE PASS. The Authorization Code Flow goes through the following steps.

1. Client prepares an Authentication Request containing the desired request parameters.
2. Client sends the request to the Authorization Server (UAE PASS).
3. Authorization Server Authenticates the End-User.
4. Authorization Server sends the End-User back to the Client with an Authorization Code.
5. Client requests an Access Token by sending the Authorization Code at the Token Endpoint.
6. Client receives a response that contains an ID Token and Access Token in the response body.
7. Client validates the ID token and retrieves the End-User's Subject Identifier (A unique, one-time identifier for the End-User and is intended to be consumed by the client).

To integrate Keycloak with UAE PASS, there are mandatory fields that should be filled to configure Keycloak properly as described below:

Authorization Endpoint

The Authorization Endpoint performs Authentication of the End-User. This is done by sending the User Agent to UAE PASS Authorization Endpoint for Authentication and Authorization, using request parameters defined by OAuth 2.0 and additional parameters and parameter values defined by OpenID Connect.

Token Endpoint

To obtain an Access Token, the client sends a token request to the token endpoint to obtain a token response using an authorization code obtained through the Authorization Endpoint. Refer to UAE PASS Endpoints.

User Info Endpoint

The User Info Endpoint is an OAuth 2.0 Protected Resource that returns Claims about the authenticated End-User. To obtain the requested Claims about the End-User, the Client makes a request to the User Info Endpoint using an Access Token obtained through the Token Endpoint. These Claims are normally represented by a JSON object that contains a collection of name and value pairs for the Claims.

Logout Endpoint

Logout Endpoint sends a logout request to UAE PASS to logout from the provider while logging out the user from the DMP Platform.

UAE PASS Client Authentication

Client authentication is a process allowing an authorization server (in this case, UAE PASS) identify a client and either grant them a token (which can be used to access the resource server) or prevent from getting a token.

- Client ID (*client_id*). OAuth 2.0 Client Identifier valid at the authorization server (UAE PASS).
- Client Secret (client_secret). Used by OAuth Client to authenticate to the authorization server (UAE PASS). The Client Secret is a secret known only to the OAuth client and the authorization server (UAE PASS). Client Secret must be sufficiently random to not be guessable.

UAE PASS Roles Mapping

While Keycloak supports Role-based access control (RBAC), Keycloak will assign a role based on UAE PASS User Type (SOP1, SOP2, SOP3, or other user type) on first succeeded UAE PASS login for the user. Based on the assigned role, user will be able to access the eligible services for that role only as defined by the DMP application.

UAE end points Environment		
Authorization	https://stg-id.uaepass.ae/idshub/authorize	https://id.uaepass.ae/idshub/authorize
Token	https://stg-id.uaepass.ae/idshub/token	https://id.uaepass.ae/idshub/token
User Info	https://stg-id.uaepass.ae/idshub/userinfo	https://id.uaepass.ae/idshub/userinfo
Logout	https://stg-id.uaepass.ae/idshub/logout	https://id.uaepass.ae/idshub/logout

The following tables show the UAM requirements as part of the the DMP access management.

USER REGISTRATION REQUIREMENTS	
Requirements	**Description**
Initiate manual registration on DMP	As a DMP End User, I would like to initiate registration by filling and submitting registration information form present on portal. I expect to receive username and password from DMP through email
Manual user registration process using government email-id	As a Portal Administrator, I should manually register DMP End Users on DMP portal and provide them their login credentials

Account activation email notification to new user	As a DMP user, system shall provide activation email to newly registered users manually or through DMP portal with timeout so that new user can activation can be confirmed.
Activate / De-activate User Account	As a DMP Administrator, I shall be able to activate or deactivate user accounts
Automatic Activation of User Account	As a DMP user, system shall activate user once activation link accessed by user so that new user can be activated automatically.
Manual bulk user registration process using government email-ids	As a Portal Administrator, I would like to manually register bulk users in to DMP portal through IAM
Manual entity/organization registration	As a Portal Administrator, I should manually register/onboard entity on DMP portal
Entity registration flow through DMP portal	As ADGE, we would like to register our entity using DMP portal through authorized personnel
Entity organization management	As CDO of entity, I shall be able to perform organization management

AUTHENTICATION REQUIREMENTS	
Requirements	**Description**
Password Rules	The following requirements meet the best practices for password management approved by the ADDA management. • Password must have at least 1 Uppercase Character • Password must have at least 1 Lowercase Character • The minimum password length must be 8 digits • Password must have at least 1 Special Character • Maximum Length of password must be 20 digits • Password must be changed every 90 days • Password must not contain your username or dictionary words • Password must be different from previously used 30 days passwords • Lockout threshold: 3 • Lockout duration: 30 or 60 minutes
Change default password	As a DMP End User, System should notify me to change my password when I login for the first time with the default password received by DMP

Login using MFA - multifactor authentication	As a DMP user, I shall be able to login into DMP portal with a combination of password ANDSMS code/Email Code OR UAEPass authentication. 1st Authentication: user id and password 2nd authentication: OTP sms or email OR, 3rd Authentication: UAE Pass identity verification and MFA
Login using two factor authentication - Email	As a DMP user, I shall be able to login into DMP portal with a combination of password and email code
Login using UAE Pass	As a DMP user, I shall be able to login into DMP portal through UAE Pass MFA.
Login using password based on password policy	As a DMP End User, I shall be able to use password based on pre-defined password policy
Forgot password through email address	As a DMP End User, I shall be able to reset my password using registered email address
Reset password through DMP portal	As a DMP End User, I would like to change the existing login credentials through DMP portal
Password lockouts	System shall be able to block login credentials in case of unauthorized or unsuccessful login attempts
User inactivity timeout	As a DMP user, I shall be able to change active session time from default 60 mins
Remember user login credentials	As a DMP user, I would like system to remember my login credentials so that I can avoid rewriting my login details every time I want to access the DMP portal
Password expiry reminder	It is suggested that the system should notify user 3 or 7 days before the password expires. Each time you log in, you will be prompted that the password is about to expire. Please change the password.
User Logout	As a DMP End User, I shall be able to logout from DMP portal
Password Expiry / Renewal	As a DMP Consumer/Steward/Data Owner/Administrator, System shall be able to force users to change password for defined period of time.
Create Password Policy	As a Portal Administrator and Cloud Resource Administrator, I shall have capability to create a password policy by configuring max. length, min. length, special characters, etc through IAM

Integration with Active Directory for identity federation	Portal should provide functionality for Integration with Active Directory for identity federation
AUTHORIZATION REQUIREMENTS	
Roles and Authorization	**Description**
Entity users management	As CDO of entity, I shall be able to update and approve requests for user profile changes, assign and approve roles/permissions for individual users
Data asset consumption access control	As a Sector/ADGE steward, I shall be able to perform access control at entity level to manage consumption
Data Asset maintenance - manage approvers	As a Sector/ADGE steward, I shall be able to manage approvers for data assets from my ADGE/sector
Grant, Reject or Revoke Access	System shall provide DMP Steward/Data Owner ability to grant/reject or revoke access permission for data assets they are owning
Request change of approvers	As a CDO for entity, I shall be able to provide update/make request for change of approvers
Create user roles	As a Portal Administrator, I should assign create following user roles: 1. DMP End User 2. Data Steward 3. CDO 4. Governance - Data Quality 5. Governance - Data Security 6. Data scientist
Assign permissions to user roles	As a Portal Administrator, I should assign permissions to created user roles
Assign security classification to the users. (Open, Restricted, Confidential, Secret)	As a Portal administrator, There should be a approval workflow based on users classification. For example, If user has open classification he can access data assets with open classification without need of any approval but to access data asset with Restricted, Confidential, Secret classification, the user needs to get approval. Similarly, User with Restricted classification can access data assets with open, restricted classification but can't access data assets with confidential and secret classification without approval

Create users & assign permissions through portal	As a Portal Administrator, I should be able to create users & assign permissions through portal
User roles specific access to data asset	As a Portal Administrator, I should be able to assign user roles specific access to data asset

Other requirements	
Requirement	**Description**
Masking as per user privileges and corresponding access to data	As a steward, I shall be able to mask attributes as per user privileges and access to data asset
Explore Product Marketplace pages - Advanced	As an ADGE/Sector Data steward, I shall be able to apply permissions at entity/organization level to browse and view list of published data assets
Notifications about passwords	As a DMP End User, I shall get notifications regarding: Password expiry reminder, Change password reminder on both portal and email

User Roles[GS1]

Sr. No	**Role**	**Description**	**Source**
1	Data Owners	The Entity shall identify and appoint Data Owners (within their department or section) to support, monitor, and guide the Data Stewards. Data Owners will be drawn from existing department managers (or section heads if needed) from both the business and technical areas of the organization. Data Owners shall be responsible to: · Take accountability for their department (or section) data throughout the lifecycle across systems and ownership boundaries. · Take responsibility to support, guide, review, correct and/or approve their data stewards' work to ensure that their dataset is maintained to the highest standards of quality possible.	AD DM Standards Document

2	Analytics Champion	The Entity shall assign an Analytics Champion entrusted to empower data value realization from the Entity's business-driven use cases, particularly from an analytics perspective. The Analytics Champion is responsible to: · Own the Entity's Use Cases identification process, use cases portfolio management, and assist the chief data officer in establishing a data-driven culture · Define the end-to-end use cases implementation roadmap, including data, people, processes and technology components · Collect business requirements and proactively propose enhancements or new use cases · Lead use cases prioritization efforts · Act as innovation promoter and define proofs of concepts to test usage models, architectures and associated technologies · Assist in the implementation of analytics use cases and monitor their performance	AD DM Standards Document
3	Data Products Officer	The Entity shall appoint a Data Products Officer responsible to ensure all data products including open data, data sharing, data monetization and others are provisioned to end customers according to Abu Dhabi defined processes, through the adequate channels and in a timely and accurate manner	AD DM Standards Document
	Data Steward	The Entity shall identify and appoint Data Stewards to support the Chief Data Officer in both the business and technical areas of the organization, responsible to: · Take responsibility for the lifecycle of the data as it passes through information systems and ownership boundaries · Take responsibility for the quality of the data under their stewardship and cleanse the data as necessary · Review and ensure the supply of business, process, and technical metadata	AD DM Standards Document

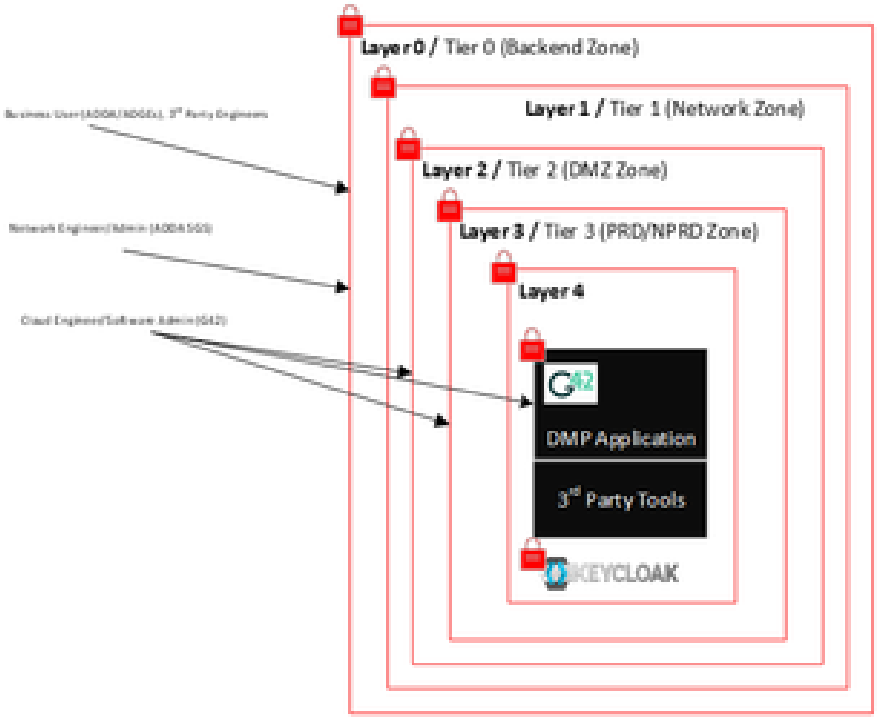
	Chief Data Officer	The Entity shall appoint a Chief Data Officer (CDO) or equivalent role responsible to: · Maintain delegated authority and responsibility for the execution of directives from the Data Committee · Ensure compliance with governance, policy, and standards · Ensure data privacy and data protection throughout the implementation of the data management program · Ensure compliance with all relevant regulations (national and international as per their applicability) · Ensure coordination and execution of Entity'sdata awareness and capability building programs · Collaborate with other Entities on knowledge transfer and best practices sharing	AD DM Standards Document
	Compliance Officer	The Entity shall appoint a Compliance Officer responsible to: · Ensure data management practices comply with Abu Dhabi Data Management Policy, Data Management Standards and relevant federal and international standards · Oversee the implementation of the Entity's data management program and compliance with Policies and Laws · Monitor the ethical handling of data within the entity and ensure the Entity adheres to data management ethics principles · Develop risk-assessment and mitigation plans for data management breaches	AD DM Standards Document
	Data Quality Lead	Collaborates with Data Quality & Metadata Lead to maintain alignment on critical data elements (CDEs) and the quality of all types of data e.g., metadata, transaction, master, reference.	ADDBOK DCMM Document

[GS1]Are these roles aligned with ADDA?

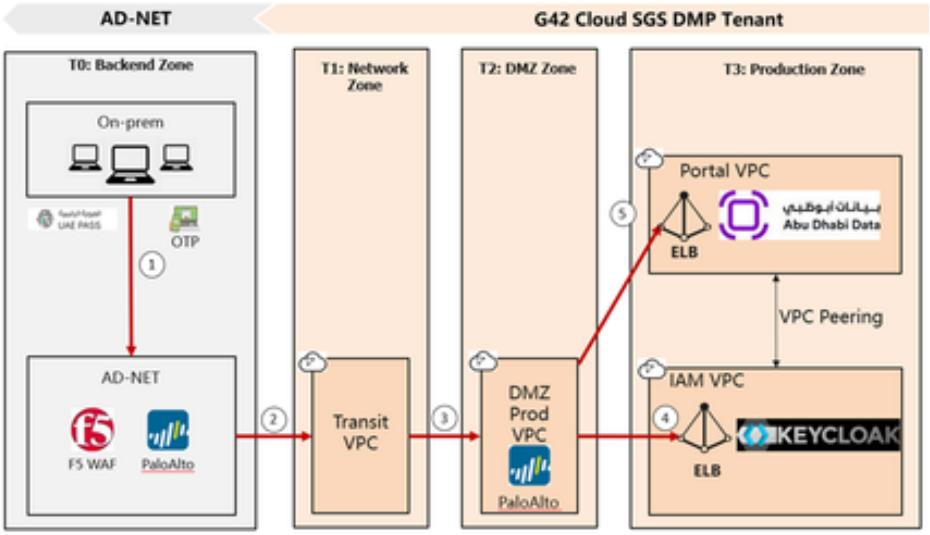
Resiliance

Layered Architecture

As per the Security Overview diagram, there are a number of security layers and security zones that provide a layered security design thereby underpinning security resilience from a security design/controls perspective. The diagram below is a simplified view of the diagram in the Security Overview section showing the layers of security and the security zones applied.



The diagram below shows the high-level flow of the DMP access management, showing resilience through out the security zones.



The above diagram shows that the DMP application and IAM are located in the Production Zone, i.e. in Teir 3 of the solution. This zone is behind multiple layers of security

· ADNET is the ADDA's secured network environment. All users on ADNET must be using endorsed terminals as defined and administered by ADDA. The network is monitored and controlled by ADDA this includes, network VPN and WAN network access. All IPs using ADNET are whitelisted allowing only select traffic frim AD-NET firewalls and WAF to the G42 Cloud DMP Tenant space and onwards to the Transit VPC located in the Network Zone.

User Request is sent through ADNET MPLS Network to the Production VPC's running the IAM Keycloak. Tableau Server Install the Certificate file provided by the certificate authority to ensure the request authenticity. The user access request using https protocol to ensure the security and data encryption.

Once the network connection is established, the channel is encrypted. The encrypted channel is established across (1), (2), (3) and (4) using the Certificated provided by ADDA (DigiCert) for the DNS to the DMP portal. The certificate is offloaded at the Application VPC on ingress to ELB at (4).

The two modes of connection are management by Keycloak (Refer to previous section) as an OTP or via a UAEPass anthentication. Once the authentication is established, the URL is redirected to the DMP application using a full end to end encryption using the certificate provided by ADDA to the DMP Portal. The Encryption is over a 445 port HTTPS using TLS 1.2 (and above).

Below is the UAEPass Screen Mockups showing the access process shown in the above sequence diagram.

For further information on the Design for UAEPass, please refer to the previous section.

· The connection between ADNET and G42 Cloud is via an MPLS Connection which is encrypted and over a leased lined. This connection is a dedicated encrypted physical connection. The endpoint of this connection on the cloud side is to the ‘Cloud Virtual Gateway’ where it is routed onwards to the DMZ zone.

· As the DMZ Zone the traffic is received by the firewall PaloAlto and is filtered and routed to the correct Production Zone based on the Layer 7 DNS provided at (1). Palo Alto performs an analysis and filtering on all packets from the Network Zone to the Production Zones. This is provided using the virtually hosted Palo Alto on the DMZ provided by ADDA as part of the SGS Tenant. From there it is routed to the designated DNS. At this point, the data is encrypted as the connection between the Application Tenants and the user is established based on the ADDA CA certificates provided.

The traffic is VPC Peered between the Transit VPC and the DMZ Prod VPC. The routing is managed and dedicated using the VPC consoles and the subsequent routing tables enforced to ensure that the correct IPs are forwarded between T1 and T2 zones. Refer to Section on VPC peering and on ACL and SG subnetting.

· The SSL certificates are offloaded on the ELB ingress at the ‘IAM and Portal VPC’. The traffic is then forwarded to the DMP Portal on the Cluster nodes inside the DMP Portal. This traffic is encrypted using CA provided certificates up to this point where the SSL is offloaded.

On first integration, Keycloak is used to integrate with UAEPass to authentication and authorize a registered user.

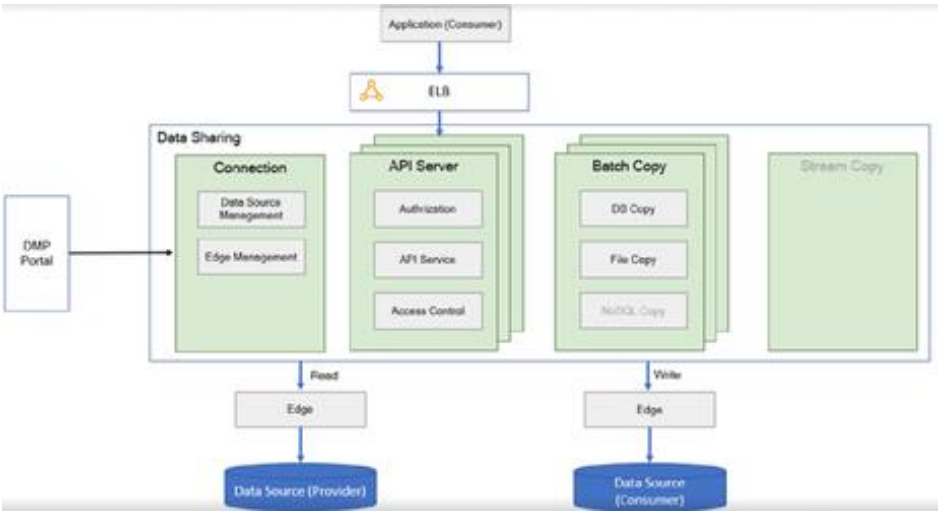
The traffic is then forwarded to the Application VPC via a VPC peering between the IAM VPC and the Portal VPC. NB: The traffic is VPC Peered between the DMZ VPC and the Landing VPC. The routing is managed and dedicated using the VPC consoles and the subsequent routing tables enforced to ensure that the correct IPs are forwarded between T2 and T3 zones.

IMPORTANT: The IAM VPC is used to house the IAM tools and capabiltyies separate from the Portal. All authentication is conducted initially in the IAM VPC and via VPC Peering to Portal VPC. Once authentication is established on IAM, the user is redirected to the DNS to the Portal using the authentication tokens provided by the IAM VPC.

· The traffic is routed using VPC peering, ACL and Security Group to the DMP portal VPC assets Cluster, VMs, RBS, MRS and etc is located on the Portal VPC. The users will only have access to the DMP Portal authenticated features. This is controlled by the DMP RBAC configuration for the specific user roles provided by the DMP application as defined im the IAM Section of this document.

Data Sharing

Data Sharing enables the safe and efficient transfer of data from data providers to data consumers. Currently data sharing provides two data sharing methods: API Server and Batch Copy.



Connection:

Connection is responsible for the management of Edge and Data Source, including the registration of Edge and the management of communication channels between DMP and Edge. Connection enables a CDO to manage his own organization's data sources.

API Server:

API Server is a lightweight, stateless, high-performance service with provides the data consumer with REST APIs for downloading the data he has subscribed to.

API Server security features:

· Authentication and authentication

· Data sorting

· Data filtering

- Download all data for a dataset with one API call
- Download data page by page

The customer uses his credentials with the Two factor Authentication code and send them over SSL/TLS to the API Gateway to be validated and if successful a Token is returned with all the roles and rights for the user and valid for some time defined by the IAM server.

Below is the Best Practice for API security followed for the DMP and EDGE platforms:

Encryption: All API calls are encrypted using SSL/TLS with the strongest ciphers

Authentication: A token that is generated by an Identity Provider (IdP) server. OAuth2 protocol is the one used for a robust security of API Authentication.

OAuth & OpenID Connect: OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

Two Factor Authentication: The implementation of two factor Authentication makes it hard to guess the credentials.

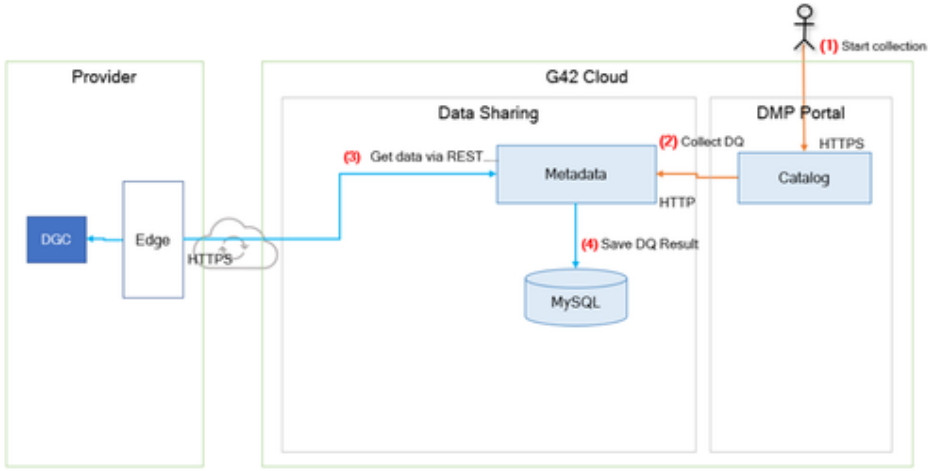
Monitoring: audit, log, and version: API logs is always being Monitored for the failed logins and other monitoring metrics also Audited to have reports and statistics for both success and failed logins

API firewalling: WAF is implemented in-front of the API Gateway to filter all the security parameters for block and pass

Batch Copy:

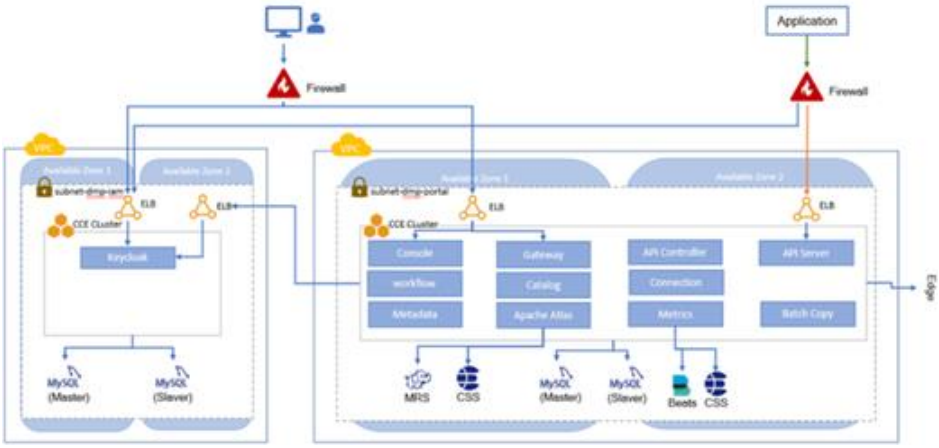
The provider and consumer can be located in the on-premise environment or the tenant in the G42 cloud, and both networks can not directly communicate with each other. In the DMP solution, two edges as agents are deployed on both sides. Edge exposes the REST API for reading and writing data from data source to Batch Copy.

Only HTTPS are allowed for the communication to keep data Encrypted on Transit.



DMP integration to MRS

MapReduce Service (MRS) provides enterprise-level big data clusters on the cloud, which are fully controlled by tenants and support the Hadoop, Spark, HBase, Kafka, and Storm components. The below architecture is explaining the MRS integration with DMP application.



From the above diagram:

· Atlas supports integration with a large number of sources of metadata. For the DMP application, we are using HBASE for ingesting and managing metadata (which is provided by MRS) and Elasticsearch (which is provided by CSS).

· MRS support Kerberos authentication, however for security recialiance this is disabled.

· SSL connection between Atlas and MRS is not required since Atlas and MRS are coolocated in the same security subnet in the same VPC.

· Application portals are published behind a Firewall.

· DMP application supports Authentication supported with MFA provided by KeyClock and UAE Pass.

· ELB Ingress for the CCE clusters have a configured SG to only allow required connections.

Data Security

Data security refers to the comprehensive protection of users' data and information assets through security measures spanning many aspects such as confidentiality, integrity, availability, durability, and traceability. G42 Cloud attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. G42 Cloud will continue to embrace industry-leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, G42 Cloud will always strive toward the most practical and effective data protection possible in order to best safeguard the privacy, ownership, and control of our tenants' data against data breaches and impacts on their business.

Access Isolation

- Identity Authentication and Access Control: The access control capabilities of G42 Cloud are facilitated through its Identity and Access Management (IAM) service. The IAM service is a security management service optimized for enterprise tenants. Through the IAM service, tenants can manage users and security credentials (such as access keys) in a centralized manner and control users' administrative privileges and cloud resource access permissions.

The IAM service allows tenant administrators to manage user accounts (such as employee, system, and application accounts) and privileges to access resources within the corresponding tenant space. If an enterprise tenant requires resource access by multiple users for collaborative purposes, the IAM service can be used to prevent users from sharing account and password information, as well as assign permissions to users based on the least privilege principle. In addition, the IAM service supports security policy configuration for login authentication, passwords, and access control lists (ACL) to ensure user account and access security. In summary, the IAM service helps mitigate the security risks associated with enterprise tenant information.

- Data Isolation: G42 Cloud facilitates data isolation in the cloud through the Virtual Private Cloud (VPC) service, the VPC uses the network isolation technology to isolate tenants at Layer 3. Tenants can control their own virtual network construction and configuration. On the one hand, a tenant's VPC can be connected to the tenant's enterprise network traditional data center using VPN or Direct Connect service such that tenant's applications and data residing in its internal network can be seamlessly migrated to the tenant's VPC. On the other hand, the ACL and security group function of the VPC can be used to configure network security and access rules as per the tenant's specific requirements for finer-grained network segregation.

-

Transport Security

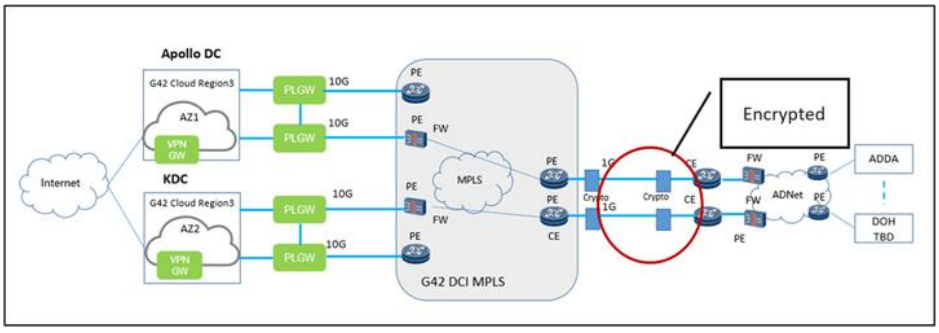
Data is transmitted between clients and servers, between servers of the G42 Cloud as well as between G42 Cloud and tenant internal networks via common information channels. Therefore, it is particularly important to protect data in transit.

- VPN: The Virtual Private Network (VPN) service is used to establish a secure encrypted communication channel that complies with industry standards between a remote user and a tenant VPC such that a tenant's existing traditional data center seamlessly extends to G42 Cloud while ensuring end-to-end data confidentiality. With a VPN-based communication channel established between the traditional data center and the VPC, a tenant can utilize G42 Cloud resources such as cloud servers and block storage at one's convenience. Applications can be migrated to the cloud, additional web servers can be launched, and the compute capacity within a tenant space can be expanded so as to establish enterprise hybrid cloud architecture and also lower risks of unauthorized dissemination of a tenant's core business data.

Currently, G42 Cloud uses IPSec VPN together with Internet Key Exchange (IKE) to encrypt data in transit and ensure transport security. Specifically, for DCD, VPN is used to support connectivity between clients and the Tableau application located in the G42 Cloud Sector Lake as shown in the diagram below.

- Application-Layer TLS: G42 Cloud supports data transmission in REST and Highway modes. In REST mode, a service is published to the public as a RESTful service and the initiating party directly uses an HTTP client to initiate the RESTful API for data transmission. In Highway mode, a communication channel is established using a high-performing G42-proprietary protocol, which is best suited for scenarios requiring especially high performance. Both REST and Highway modes support TLS 1.2 for data in transit encryption and X.509 certificate-based identity authentication of destination websites.

Furthermore, encryption in motion is a core aspect of data security of the overall design. At the network level, all traffic that is passed through non-G42 internal network is encrypted at the Application Level using certificates that are provided by ADDA. All internal traffic is self-signed and encrypted. The diagram below shows a typical end to end data flow and encryption.



Storage Security

Key Protection and Management: The Key Management Service (KMS) is a secure, reliable, and easy-to-use key escrow service that facilitates centralized key management in order for users to achieve better key security to support their database encryption. The KMS employs Hardware Security Module (HSM) technology for key generation and management, preventing the disclosure of plaintext keys outside the HSM and ensuring key security. The KMS enforces access control of all crypto key-related operations with logging enabled for audit trail of all crypto key usage records, which meets audit and compliance requirements. G42 Cloud's in-house-developed KMS already supports integration with the following G42 Cloud services:

- Elastic Volume Service (EVS)
- Object Storage Service (OBS)
- Scalable File Service (SFS)
- Image Management Service (IMS)

Data Confidentiality and Reliability Assurance: G42 Cloud offers data protection functions and recommendations for each cloud storage service. See table below:

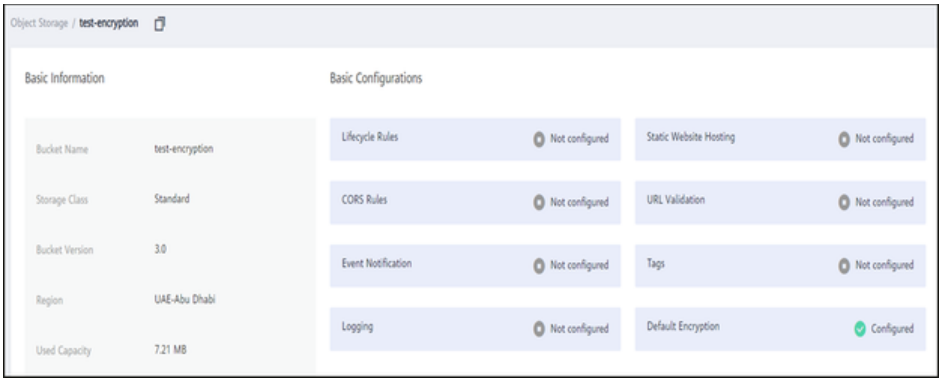
Storage Service	**Description**	**Confidentiality**	**Reliability**
EVS	The EVS is a virtual block storage service that is based on a distributed architecture and can scale flexibly.	KMS provides crypto keys as needed. It supports the management of Customer Master Keys (CMKs) from generation to erasure. CMKs are used to encrypt and decrypt data encryption keys. The volume encryption function is also supported.	Three-copy data backup with data durability up to 99.99995%. The CBR can be used to implement volume backup and restore and supports volume creation based on a volume backup.

OBS	The OBS is an object-based mass storage service, which provides users with massive, low-cost, highly reliable, and secure data storage capabilities.	The following encryption key management modes are supported: SSE-C mode[1]: A user provides an encryption key, the hash value of the key, and the encryption algorithm AES256. In this mode, requests must be sent through HTTPS. SSE-KMS mode: The KMS provides and manages keys. When a user uploads an object to be encrypted in SSE-KMS mode to the bucket in the zone, the OBS automatically creates the CMK for data encryption and decryption.	Data durability up to 99.999999999% and service availability up to 99.99%. Data integrity is checked right before data storage, ensuring that the data to be stored matches the uploaded data. Slice redundancy is achieved by storing multiple slice copies on different disks after data slicing. The service backend automatically checks the slice integrity and promptly repairs damaged data
RDS	The Relational Database Service (RDS) is an online relational database service that is based on the cloud computing platform. It is turnkey upon subscription and is stable, reliable, readily scalable, and easy to manage.	The database management system is used to encrypt database files such that data cannot be decrypted in the event of data leakage or loss. Tenants are advised to encrypt data to be uploaded before saving the data to the database.	Three-copy data backup with data durability up to 99.99995%. The active and standby database instances can be quickly switched over between them upon a fault or failure. Service availability up to 99.95%. Automatic data backup and snapshot creation are supported. Data can be restored to the time when a specific backup file was created.

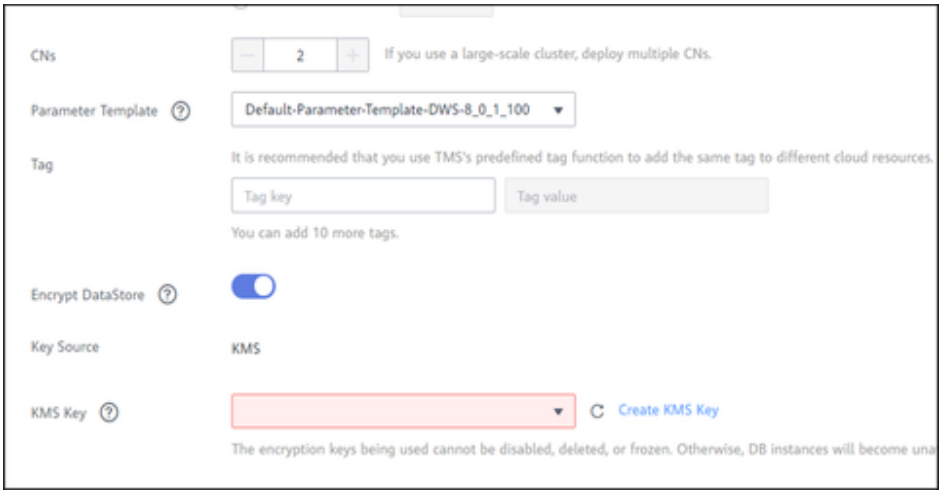
IMS	The IMS provides user-friendly self-service and complete image management capabilities. Users can select images from the rich public image library and create private images in order to quickly create or bulk copy of Elastic Cloud servers.	Same as EVS above. In addition, G42 Cloud supports two ways for encrypted image creation: setting up encrypted Elastic Cloud Servers and creating external image files.	Ensures private image redundancy by storing multiple copies. Data durability up to 99.999999999%.

[1] SSE-C refers to server side encryption with customer-provided key.

For DMP, all object storage and DWS services support encryption as depicted below. OBS encryption 'Default Encryption' is 'Configured':



For DWS, the 'Encrypt DataStore' is enabled as shown below:

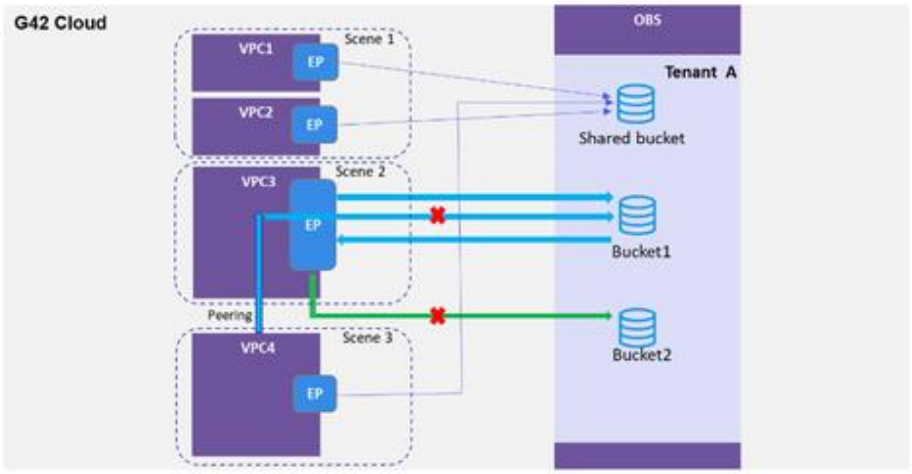


IMPORTANT NOTE: For DGC Data Masking will be enabled to allow for dev environment work. This is conducted using separate ETL jobs such that the following information shall be masked.

No.	Attribute / Field Name	Masking Method
1	Date_of_Birth (all Date column that is considered for masking)	turn the day to the first day of the month
2	Emirate_id	784+ the following numbers are arranged in asc order. For example: 784199308062334->784001233346899
3	Email_ID	hash
4	First_Name	hash
5	First_Name_Ar	hash
6	Second_Name	hash
7	Second_Name_Ar	hash
8	Third_Name	hash
9	Third_Name-Ar	hash
10	Full_Name	Hash
....		

OBS or Object Storage are being used with Encryption based on DEW and KMS encryption. OBS is protected by Encryption and by Access policy as shown below for the scenarios used to protect the Buckets and Objects stored inside it

- In VPC side, VPCEP policy is used to generate VPC egress whitelist .
- In OBS side, Bucket policy is used to generate bucket ingress whitelist



Scene1 :
For the VPC there is no requirement to access to bucket, fixing all the VPC with same black hole bucket ensures that data is not transferred to other tenant spaces.
Scene2 :
For the VPC that has to access to OBS, double fixed is configured for each pair specific VPC and bucket, which ensures the mapping between application and storage.
Scene3 :

For the VPC4 that has peering with VPC3, the VPC4 can not access to VPC3's bucket by peering

Data Deletion & Destruction

G42 Cloud protects tenant data against unauthorized disclosure during and after data deletion.

- **Memory erasure:** Before the cloud operating system reallocates memory space to new users, G42 Cloud performs a zero-fill data wipe procedure in the memory space to be reallocated. This procedure ensures that malware detection software cannot detect valuable information in the memory on a newly-initiated VM and prevents data leakage that would otherwise result from the restoration of deleted data from the physical memory.
- **Secure (logical) data deletion:** G42 Cloud offers a one-click feature for the logical deletion of discarded data, which gives tenants the flexibility to delete data (for example, data stored in cloud storage services such as RDS) from the management console with a single click whenever needed.
- **Hard disk data deletion:** G42 Cloud performs a zero-fill data wipe procedure on virtual volumes of both deleted accounts and disabled accounts, ensuring that deleted data cannot be restored and preventing data leakage that would otherwise result from malicious tenants retrieving valuable data on the hard disk using data restoration software.
- **Encryption-based data leakage prevention:** G42 Cloud advises tenants to encrypt their high value data prior to uploading to G42 Cloud as well as configure encryption for data in transit and data in storage. When data in the cloud needs to be discarded, the tenant may simply perform the "secure delete" operation on the data-encrypting key(s) in order to prevent data leakage. Moreover, before physical disks and memories are reassigned, G42 Cloud performs a routine zero-fill data wipe operation.
- **Physical disk destruction:** When a physical disk needs to be decommissioned, G42 Cloud permanently deletes the data present on the disk by means of physical disk degaussing and/or shredding as needed to ensure user privacy and avoid unauthorized data access. In addition, G42 Cloud adheres industry standard practices and keeps a complete data deletion activity log for chain of custody and audit purposes.

Data Applied Security Controls

For Data Protection we are using many Services to secure it like we showed for the DEW service and below is for Data Base Security Service DBSS used for Data base protection.

Each DB service which is RDS is protected by DBSS which provides the below functions to secure the DB

· Database audit provides you with the database audit function in out-of-path pattern, enabling the system to generate real-time alarms for risky operations. In addition, database audit generates compliance reports that meet data security standards. In this way, it locates internal violations and improper operations, protecting your data assets.

- Simple to set up

- Database audit is deployed in out-of-path pattern. It is simple to set up and operate.

- Comprehensive audit

Supports audit of databases built on RDS and ECS.

- Quick identification

Implements 99%+ application association audit, complete SQL parsing, and accurate protocol analysis.

- Efficient analysis

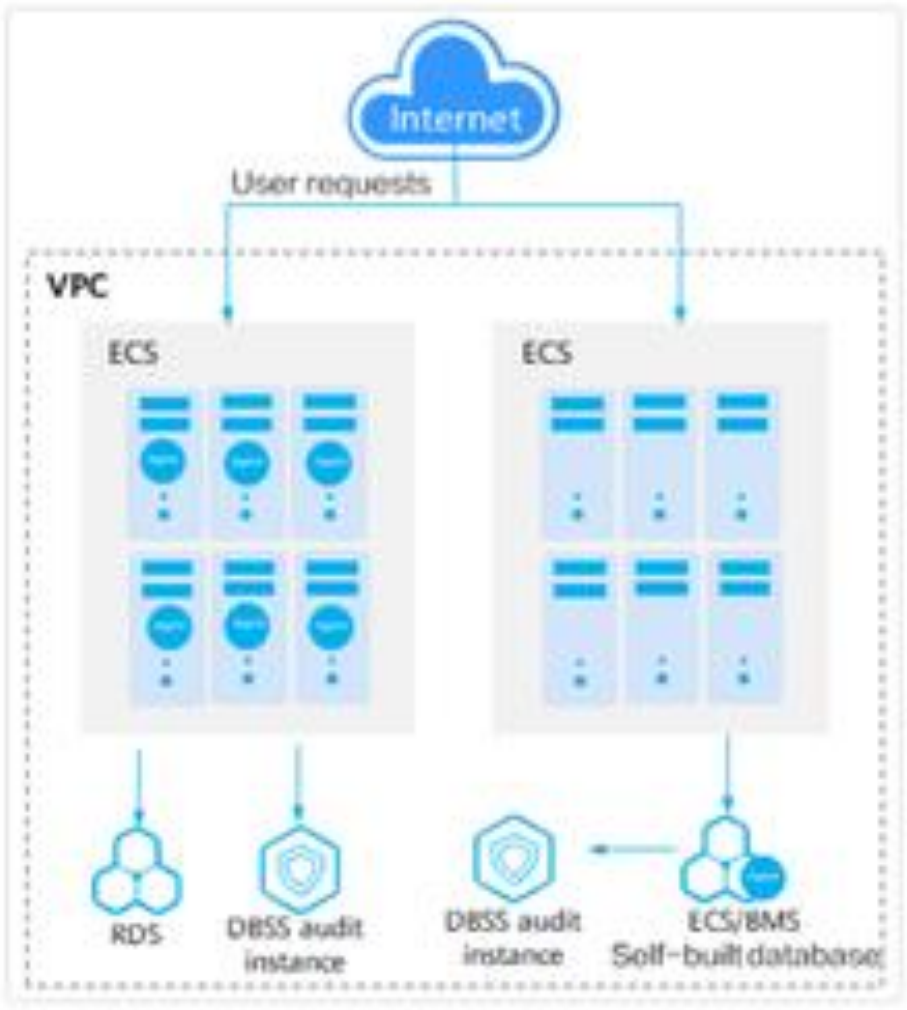
Responds quickly for data query with 10,000 requests per second from massive volumes of data saved.

- Clear permission division

Clearly divides permissions among the system administrator, security administrator, and audit administrator, meeting audit security requirements.

· Deployment Architecture

below diagram shows that Database audit is deployed in out-of-path pattern. It can audit databases built on ECS, BMS and RDS on the management console.



· The agent deployment for database audit is as follows:

- Self-built database on ECS/BMS
  - Deploy the agent on the database side.
- RDS database
  - Deploy the agent on the application or proxy side.

· Permissions Management for DBSS

With Tenant IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use DBSS but must not delete DBSS resources or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using DBSS resources.

- Below table shows System roles supported by DBSS
-

Role Name	Description	Dependency
DBSS System Administrator (DBSS system administrator, who has the permissions to perform operations on DBSS system resources)	Users with this set of permissions can perform the following operations on database audit: o Purchasing an instance o Starting, disabling, and restarting an instance o Obtaining the instance list o Obtaining the basic information of an instance o Obtaining the audit statistics o Obtaining the monitoring information o Obtaining the operation logs o Managing databases o Managing agents o Configuring email notifications o Backup and restoration	To perform payment operations (for example, purchasing or renewing a DBSS instance), you must have the **BSS Administrator**, **VPC Administrator**, and **ECS Administrator** roles. · **VPC Administrator**: Users with this set of permissions can perform all execution permission for Virtual Private Cloud (VPC). It is a project-level role, which must be assigned in the same project. · **BSS Administrator**: Users with this set of permissions can perform any operation on menu items on pages **My Account**, **Billing Center**, and **Resource Center**. It is a project-level role, which must be assigned in the same project. · **ECS Administrator**: Users with this set of permissions can perform any operations on an ECS. It is a project-level role, which must be assigned in the same project.

DBSS Audit Administrator (DBSS audit administrator, who has the permissions to check DBSS security logs)	Users with this set of permission can perform the following operations on database audit: o Obtaining the instance list o Obtaining the basic information of an instance o Obtaining the audit statistics o Obtaining the report results o Obtaining the rule information o Obtaining the statement information o Obtaining the session information o Obtaining the monitoring information o Obtaining the operation logs o Obtaining the database list o Managing reports	None

DBSS Security Administrator (DBSS security administrator, who has the permissions to set DBSS security policies)	Users with this set of permission can perform the following operations on database audit: o Obtaining the instance list o Obtaining the basic information of an instance o Obtaining the audit statistics o Obtaining the report results o Obtaining the rule information o Obtaining the statement information o Obtaining the session information o Obtaining the monitoring information o Obtaining the operation logs o Obtaining the database list o Configuring audit rules o Configuring alarm notifications o Managing reports	None

For Data logs we are using Cloud Trace Service (CTS) which is a log audit service designed to strengthen cloud security. It allows you to collect, store, and query resource operation records.

You can use these records to perform security analysis, track resource changes, audit compliance, and locate faults.

CTS is built based on concepts to collect all Trace logs for further processing and Audits

· Tracker

Before using CTS, you need to enable it. A tracker is automatically created when CTS is enabled. The tracker identifies and associates with all cloud services you are using, and records all operations on the services.

A management tracker and 100 data trackers can be created for a tenant.

· Trace

Traces are cloud resource operation logs captured and stored by CTS. You can view traces to identify when operations were performed by which users for tracking.

There are two types of traces. Management traces are operation records reported by cloud services, whereas data traces are read/write operation records reported by Object Storage Service (OBS).

· Account

An account is created upon successful registration. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used directly to perform routine management. For security purposes, create Identity and Access Management (IAM) users and grant them permissions for routine management.

· User

An IAM user is created by an account in IAM to use cloud services. Each IAM user has its own identity credentials (password and access keys)

· Region

A region is a geographic area in which cloud resources are deployed. Availability zones (AZs) in the same region can communicate with each other over an intranet, while AZs in different regions are isolated from each other. Deploying cloud resources in different regions can better suit certain user requirements or comply with local laws or regulations.

Filescanning

Files will be imported into DMP from two main sources:

- DMP Portal: User Driven

The end user has the option of downloading files and modifying them, after which they may upload them. The main file types for upload are; .XML and .XLS, files.

- EDGE:

Automatic: The remote EDGE has the ability to transfer (vis SFTP) a number of different file types. This is an inline and automatic process. The types of files from the remote EDGE are .pdf, .xls, .doc, .xml and etc.

The file/data flow from the above two methods is sourced from a trusted zone, i.e. 'Layer 0 : Tier 0 : Backend Zone'. The risk of malware in the files is low, given the trusted zone file uploads are conducted from ADGE's which are on ADNET and have security capabiliyties inherit as part of the 'Backend Zone'. Given the DMP policy of zero-trust, file scanning in required to ensure that files uploaded to DMP or passingthrough DMP are scanned.

The diagram below shows the incorporation of a filescanning toolm OPSWAT. The key decisions are as follows:

- Uploaded or imported files are directed to the OPSWAT Metadefender Server.
- File scanning is conducted outside of the core security layers (i.e. before the FW/DMZ zones). This will allow for network segmetayion protection from any infected files.
- The files uploaded are treated as potential risks, therefore, all file uploads must pass through the OPSWAT Metadefender application.
- Once the file is successfully scanned, it is passed back (redirected) to its destination.
- Files identified as hazadaous, are moved to a quantine folder from where they are quied for 'file distruction' inside the Networ/Security Zone (i.e. outside of the core Cloud zone).

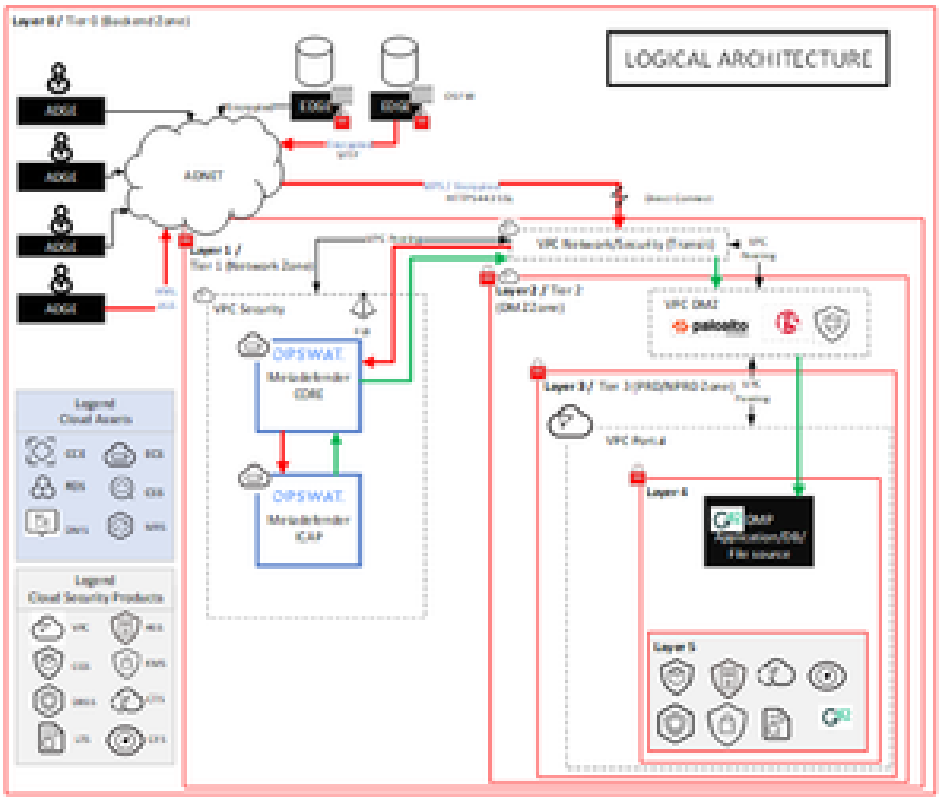
o API's will be used to communicate to the OPSWAT Server loading the status, destination, source and re-routing address.

- The EDGE application is to point all SFTP loaded files to the OPSWAT Server for scanning.

o Any files identified as 'failed scan' are to be alerted to the DMP Data Stweard and information is to be sent to the DMP Dashboard.

- The DMP application is to be adjusted to ensure all uploads are sent to the OPSDWAT Server for scanning.

o Files that fail the scan will need a User Interface alert and indication



Hardening

For the DMP application the following hardening capabilities are applied:

Security Domains	Security Controls and Products:

VPC Location	Refer to section on network segementation using VPC's. vpc-adda-dep-dmp-iam-stage vpc-adda-dep-dmp-portal-stage vpc-adda-dep-dmp-iam-production vpc-adda-dep-dmp-portal-production vpc-adda-dep-dmp-iam-uat vpc-adda-dep-dmp-portal-uat vpc-adda-dep-dmp-iam-qa vpc-adda-dep-dmp-portal-qa vpc-adda-dep-dmp-iam-RnD vpc-adda-dep-dmp-portal-RnD

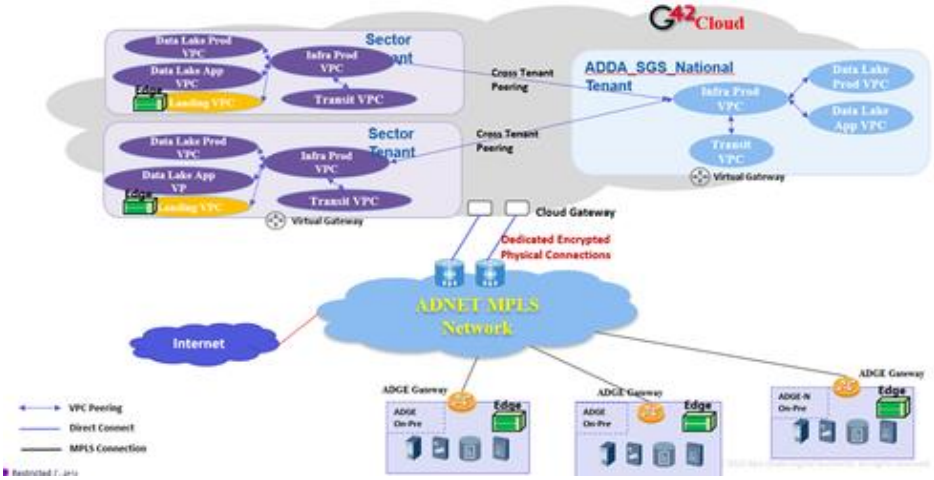
Security Group	Refer to section on ACL and Security Groups. cce-dmp-stg-iam-cce-node cce-dmp-stg-portal-cce-node Sys-default cce-dmp-stage-portal-cce-node sg-adda-dep-dmp-css sg-adda-dep-dmp-rds-stage mrs_mrs-dmp-stg-port cce-dmp-prod-iam-cce-node cce-dmp-prod-portal-cce-node sg-adda-dep-dmp-rds-production mrs_mrs-dmp-prod-port cce-dmp-uat-iam-cce-node cce-dmp-uat-portal-cce-node sg-UAT-ecs sg-adda-dep-dmp-css-uat sg-adda-dep-dmp-rds-uat sg-dws-dmp-uat-01 mrs_mrs-dmp-uat-port sg-adda-dep-dmp-MQ-uat cce-dmp-qa-iam-cce-node cce-dmp-qa-portal-cce-node

	sg-adda-dep-dmp-css-qa sg-adda-dep-dmp-rds-qa mrs_mrs-dmp-qa sg-adda-dep-dmp-MQ-qa cce-dmp-rnd-iam-cce-node cce-dmp-rnd-portal-cce-node sg-adda-dep-dmp-css-rnd sgs-dep-rnd-sg sg-adda-dep-dmp-rds-rnd mrs_mrs-dmp-rnd sg-adda-dep-dmp-MQ-rnd
Data Security	• ECS • DBSS • Data Security Section • Network segementation Refer to Secytion on Data Security.
Application Security (WAF), (VSS), (etc)	Refer to the Access Control and Resiliance Sections above.
Compute Security (HSS), (CGS)(etc)	• ECS – Section 12.2.1 • HSS – Section 12.2.8
Cyber Security (AV - type),(Anti-DDoS),(Adv Anti-DDoS),(EDR), (IPS), (IDS) etc	• Anti-DDoS by Etisalat Anti DDoS – Arbor • ADNET East West IPS/IDS – Tier 0 – Backend Zone security • IDS/IDPS by HSS –for host security services • KMS – for ECS access management • VLAN security by using VPC

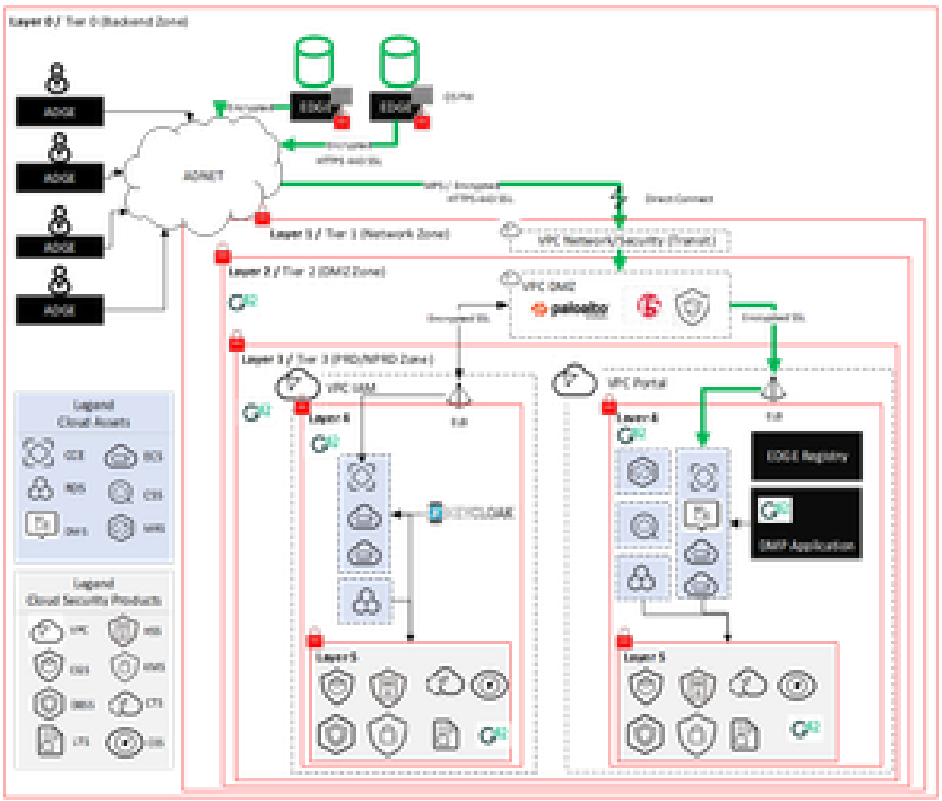
User Access Management	• ADNET connectivity • G42 Cloud IAM • Keycloak • MFA/ UAEPass • RBAC allocation – G42 Managed Services
Protocols	• HTTPS, IPSec, TLS 1.2 • DISABLE OLDER VERSIONS OF TLS: -ENABLE HTTP Strict Transport Security for web browser clients.
Compliance	• OS Hardening CIS Benchmark Windows Server • Nessus OS Scan
Update to Current Version	We recommend that you always run the latest version of Tableau Server. Additionally, Tableau periodically publishes maintenance releases of Tableau Server that include fixes for known security vulnerabilities. To get the latest version or maintenance release of Tableau Server, visit the Customer Portal(Link opens in a new window)
Enable SSL encryption between Tableau and Porstgres	Configure Tableau Server to use SSL to encrypt all traffic between the Postgres repository and other server components. By default, SSL is disabled for communications between server components and the repository.
Disable services not used	All

EDGE Application Security

The diagram below depicts the overview of the communication and data flow between EDGE and the DMP. Security is concerned with the end to end security of the data and the EDGE appliance security at the ADGE's.



All the communication between the Customer side at ADGE's and EDGE is via the MPLS and Direct connect VPN which is encrypted tunnel and the data will be encrypted using SSL/TLS, then the traffic goes to the transit VPC and to the peering VPC to the Final destination Landing VPC. The diagram below shows the communication between the ADGE's and the G42 Cloud via ADNet and in reference to the security layers as depicted for DMP in the previous sections of this document.



The Edge collector platform from a Sector perspective is located inside the Landing VPC, where the data from EDGE is collected by the DMP portal.

Access Control

The EDGE data lands on the allocated cluster nodes which are located behind Layers 2 and 4 as defined in the above sections. Access to the cluster nodes and cluster base nodes is highly restricted.

- Cluster nodes : Restricted Access using Permissions allocated by the G42 Cloud Managed Service Team. Business Users do not have access to these nodes.
- Base nodes : Restricted access, this access is not granted to Business Users and is not available to G42 Cloud Managed Resources. This is managed by the G42 Cloud R&D team and no access is available to these nodes as it is part of the G42 Cloud platform.

CCE node permissions management allows permissions to G42 Cloud IAM users and user groups under tenant accounts. CCE combines the G42 Cloud Identity and Access Management (IAM) and Kubernetes Role-based Access Control (RBAC) authorization to provide a variety of authorization methods, including IAM fine-grained authorization, IAM token authorization, cluster-scoped authorization, and namespace-wide authorization.

RESTRICTED USERS	**Clusters of v1.11.7-r2**
User with the Tenant Administrator permissions	· Has all namespace permissions when using CCE on the console. · Requires Kubernetes RBAC authorization when using CCE via kubectl. **NOTE:** When such a user accesses the CCE console, an administrator group is added. Therefore, the user has all namespace permissions.
IAM user with the CCE Administrator role	· Has all namespace permissions when using CCE on the console. · Requires Kubernetes RBAC authorization when using CCE via kubectl. **NOTE:** When such a user accesses the CCE console, an administrator group is added. Therefore, the user has all namespace permissions.
IAM user with the CCE FullAccess or CCE ReadOnlyAccess role	Requires Kubernetes RBAC authorization.
IAM user with the Tenant Guest role	Requires Kubernetes RBAC authorization.

IMPORTANT NOTE: The above access is highly restricted and not within the business user domain.

The CCE Cluster offers Kubernetes version 1.19.10 and consists of 3 master and multiple worker nodes. Following Namespaces are created：

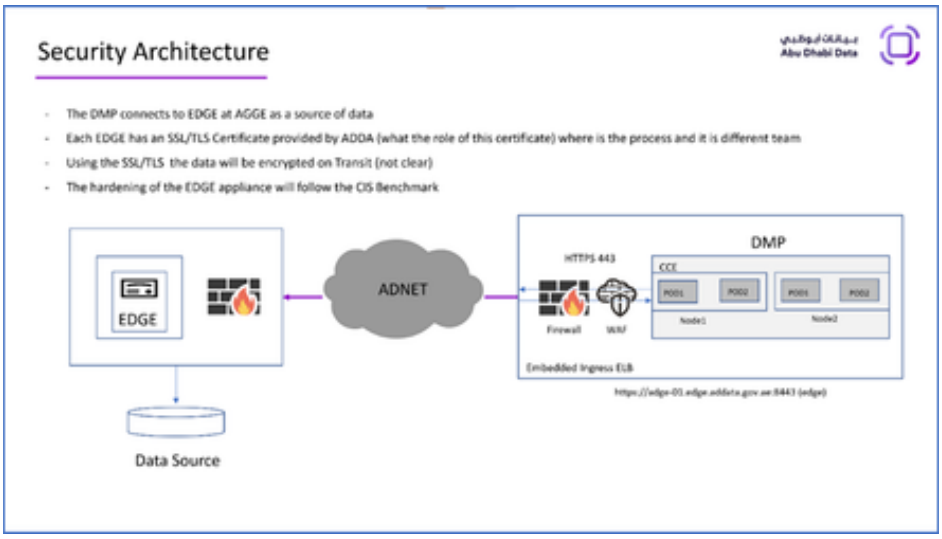
- kube-public: used for deploying public add-ons and container templates.
- kube-system: used for deploying Kubernetes system components.
- default: Used for deployment of Edge deployment.
- velero: Used for deployment of Velero server for the cluster objects and workload backup and restore functions.

All access to the CCE's is monitored by Cloud Trace Service (CTS) which records operations on cloud service resources, allowing users to query, audit, and backtrack the resource operation requests initiated from the management console or open APIs as well as responses to the requests.

Resiliance

Remote Access and Integration – Layer 2 Security

Network traffic from the remote EDGE is transferred encrypted using SSL certificates which are terminated on ingress to the CCE clusters and ingested in the EDGE appliance itself. The ADGE(x) traffic to the G42 Cloud uses TLS/SSL encryption v1.2 or higher and is contained within a trusted network, i.e. ADNET. The diagram below depicts the core transmission security functions.



The traffic is passes onto the Network and Security Zone through the implemented Palo Alto Firewall and F5 Load Balancer. The traffic is offloaded to HTTP as part of the solution to reduce resource usage on the ELB's and ingress into CCE's (i.e. clusters inside the DMP VPC). The F5 has WAF capabilities are used to block web-based attacks targeting layer 7 of the OSI model.

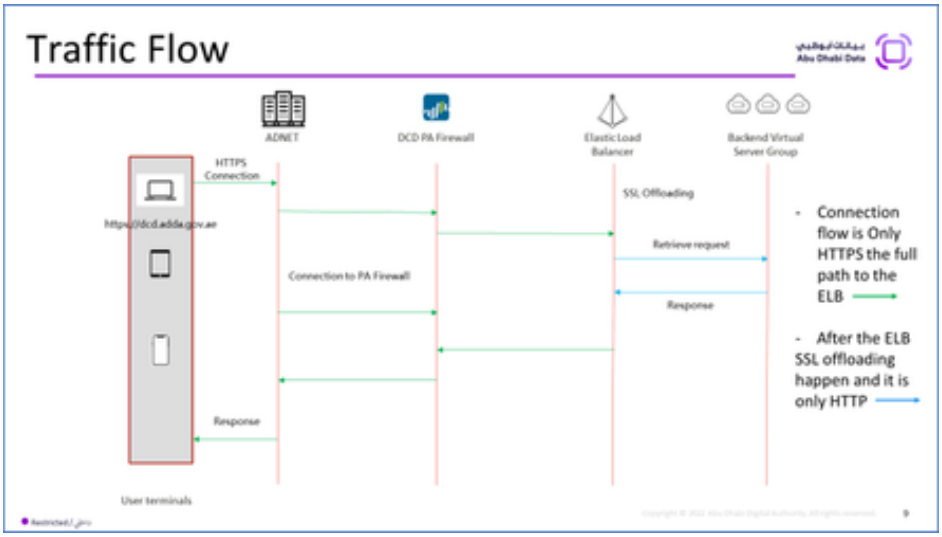
Using the OSI Model, the following security controls are in place:

- OS Layer 4 we have the Palo Alto Firewalls and F5 working as Master Slave for high availability
- OS Layer 7 we have the F5 WAF implemented to protect the Application.

The core transmission protocols used to ensure security between the Datasource, EDGE applicance and G42 Cloud are :

- TLS/SSL 1.3 encryption.
- X509TrustManager certificate management codified.
- HTTPS between all customer facing communications, i.e. between the ADGE data source and EDGE.
- Certificate Authority and Self Signed Certificates to be applied
- Certificate expiry and management to be applied
- ELB's are used as the source and the offloading locations for all certificates.

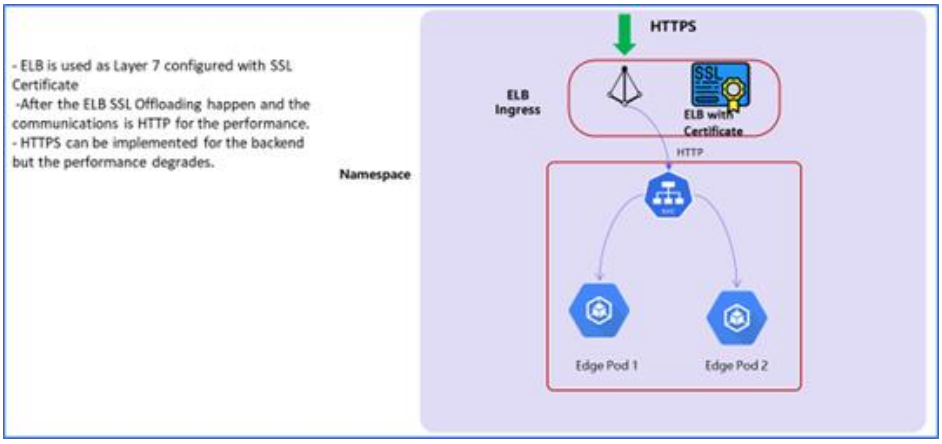
The diagram below shows the traffic flow between the EDGE and the backend DMP services.



Certificates are managed and provided by ADDA.

- ELB is used as Layer 7 configured with SSL Certificate. The certificates obtained are from a Certificate Authority and provided by ADDA.
- Policy: All out-gross and ingress communications from the G42 Cloud VPC and EIPs must utilize SSL certificates from a reputable Certificate Authority. Example, between

VPC, between environments and external facing communication (e.g. DMP portals and EDGE communications).

- Policy: All internal communication inside the VPC should be at least self-signed certificates, such that encryption is mandatory at all times. NOTE: No plane text communications is to occur between servers and services inside VPCs.
- After the ELB SSL Offloading occurs from external traffic, communication remains HTTPS inside the VPC and between software components and cluster nodes using either self-signed certificates or authorized CA certificates (i.e. JAVA codified certificates using X509TrustManager methods), applying encryption to ensure minimal attack surface exists.
- On landing, the certificates are terminated on ELB ingress as shown in the diagram below:
- 

Network Segmentation in Cloud – Layer 3 Security

Network segmentation on the G42 Cloud is supported by Virtual Private Cloud (VPC) services. VPC enables ADDA to provision logically isolated, configurable, and manageable virtual networks for Elastic Cloud Servers (ECSs) and CCE's, improving cloud resource security and simplifying network deployment. VPCs support the folowing permission and security features:

- Subnetting
- Port allocations
- VPC peering and routing
- IP whitelisting
- ACL management
- Security Group management

VPC also provides the following network security features:

- VLAN isolation: VLAN, which works on Layer 2, uses virtual bridging to support VLAN tagging and implement virtual switching to ensure secure isolation between VMs.
- IP and MAC address binding: This measure enhances the security of virtual networks by preventing VM users from spoofing IP or MAC addresses. DHCP snooping is used to

bind IP addresses with corresponding MAC addresses. IP Source Guard and dynamic ARP inspection are also used to filter out packets from non-bound sources.

- DHCP server isolation: To ensure that IP addresses are allocated properly, users are not allowed to run DHCP servers.
- DoS and DDoS mitigation: The number of tracked connections to virtual ports is restricted so as to prevent traffic flooding attacks

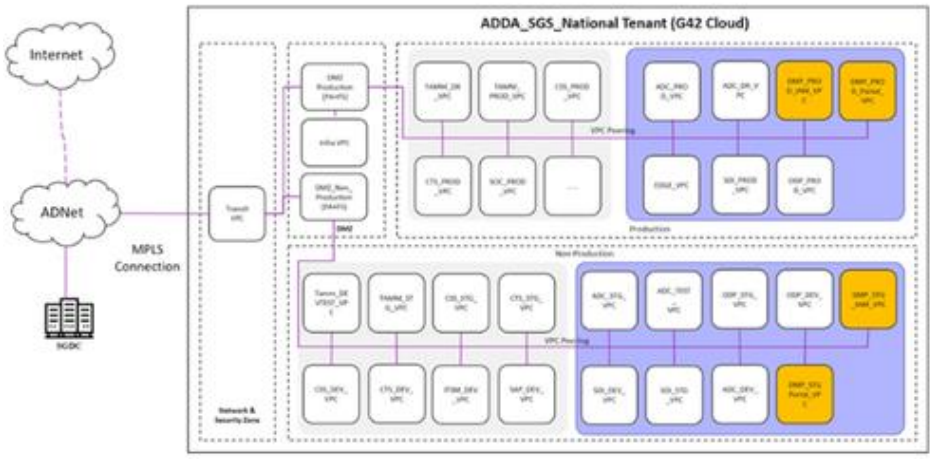
[1] from inside or outside the cloud platform.

NOTE: VPC's provides security fucntions at the lower-stack of the OSI model.

The network segmentation is provided by the use and configuration of multiple VPC's as shown in the diagram below:

---

[1] Traffic flooding attacks interrupt service and management traffic by generating a large number of connection tracking entries, which exhausts connection tracking table resources and prevents legitimate connection requests from being received.



Then the traffic will flow through the VPC peering to the Destination VPC, shown in the Architecture in the above diagram. The tenant infrastructure is divided into three logical zones. Production, non-production and demilitarized (DMZ) zone in order to isolate production and non-production traffic.

Production zone hosts the infrastructure resources required for the production environments of different shared services. DMP production environment consumes the shared resources such as firewall and F5 load balancer. Similarly, for non-production zone hosts other environments

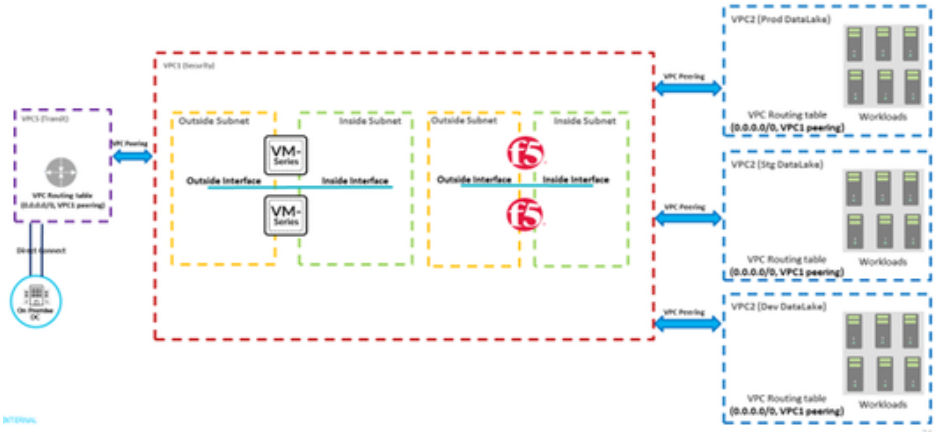
infrastructure such as staging, development, QA and UAT of shared government services. DMP staging environment is part of this group, i.e. all tarffic between the VPC flows through the PaloAlto and F5, therefore allowing for East/West traffic security adherance.

Transit VPC: All inbound connections (VPN and DC) will be terminated in transit VPC. This VPC acts as the transit for the communication between ADGEs and G42 Cloud tenant. This alklows for network segmentation and an isolation of the traffic from production and non-production VPC's

Infrastructure Prod VPC: A centralized production VPC where firewall virtual appliances and F5 instances are deployed. This VPC peers with DMP production environment VPCs to provide secure connectivity.

Infrastructure Non-Prod VPC: A centralized non-production VPC where non-production firewall virtual appliances] and F5 instances are deployed. This VPC peers with the DMP staging environment VPCs to provide secure connectivity.

The diagram below shows how security is applied using PA and F5 for each of the network segmentations as defined below for Staging and Production.



Security Grops and ACLs - - Layer 4 Security

Network ACLs and security groups are both major factors in enhancing the cybersecurity of G42 Cloud VPCs, understanding the differences between them is important for creating effective network security policies for VPCs. These differences are summarized in the table below.

After the network segmentation provided by VPC, further security zoning is enforced by apply Security Group's on ECS assets. Security Groups protect the traffic flow inside the VPC's to ensure that only the IPs allocated specific traffic rule (using security gropup rules) are applied between assets inside the VPC.

Security Groups support:

- Work on the a wide range of cloud asset at the instance level (first layer of protection).
- Support permit policies.
- If rules conflict with each other, only the parts in agreement take effect.
- Must be selected when an Elastic Cloud Server instance is created; take effect automatically on Elastic Cloud Server instances.
- Support packet filtering by 3-tuple (protocol, port, and destination IP address).

Security Groups are a collection of access control rules for cloud resources, such as cloud servers, containers, and databases, that have the same security protection requirements and that are mutually trusted within a VPC. For DMP, security groups are created for EDGE traffic, such that various access rules aer applied to direct the tarffic to the CCE clusters where the SSL is terminated. These rules are applied by the Console Administrators are are not changed without strict administartion protocols.

On the DMP VPC, there are 22 Security Groups applied across a range of assets. Therefore, prior to the EDGE traffic landing in any of the CCE's (cluster), the traffic will be channled through specific security group rules to ensure that the traffic is provided the specific controls to avoid bradcasting across the VPC, instead it is routed to the correct CCE via VPC peerings and Security Groups rules.

NOTE: Default Security Groups are diabled in DMP and only configurable and customised security groups are applied.

Network ACLs are systems that specify, maintain, and enforce access control policies for one or more subnets. They determine whether to permit packets to enter or leave a subnet based on the inbound or outbound rules associated with that subnet. This service functions on the network traffic level and is consider the 2nd layer of protection after security group allocation. This supports permition and denial ofl polcies.

EDGE Application Host Security – Layer 5 Security

Container Guard Service (CGS) can scan vulnerabilities and configuration information in images, helping enterprises resolve container environment problems that cannot be detected by traditional security software. In addition, CGS provides the container process whitelist, read-only file protection, and container escape detection functions to prevent security risks during container running.

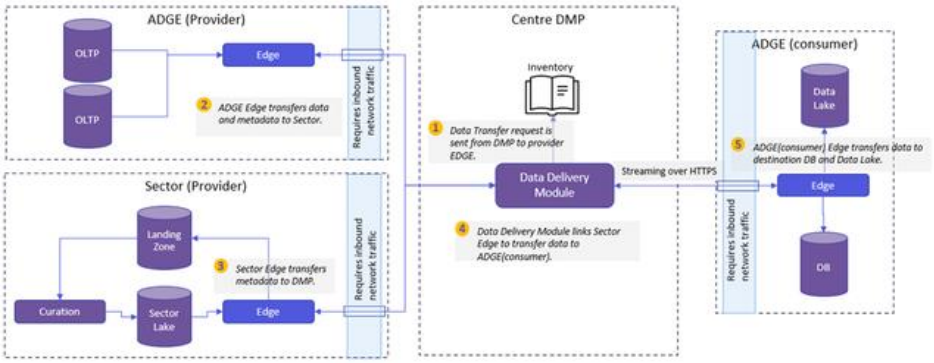
- G42 Cloud CGS mainly provides the following functions:
- Image vulnerability management: CGS can scan private, official, and all running images in G42 Cloud to detect vulnerabilities in the images and provide fixing suggestions, helping users obtain secure images.
- Container security policy management: CGS supports the configuration of security policies to help enterprises define the container process whitelist and file protection list, improving system and application security during container running.

- Container process whitelist: Defining such a whitelist can effectively prevent security risks such as abnormal processes, privilege escalation attacks, and noncompliant operations.
- File protection: Read-only protection must be configured for key application directories (such as bin, lib, and user system directories) in containers to prevent tampering and hacker attacks. This function can restrict the access (set to read-only) to these directories to prevent security risks such as file tampering.

Container escape detection: This function scans all running containers, detects exceptions (including escape vulnerability attacks and escape file access) in the containers, and provides solutions.

Hardening

There are two core applications associated with EDGE, i.e. the EGDE Virtual Appliance and the DMP Portal Application. The layout of the EDGE application as it relates to DMP is shown in the below diagram:



The focus of this paper is not the security of DMP application, but rather the EDGE application herein. The Edge Application is deployed as an OVA image, virtual appliance. Its is installed on remote sites and configured for the remote data sources from where it will transfer data. The EDGE application is a headless service that executes using a High Availability deployment based on a CentOS 7.9 and Docker. Two edges are running in Active-Active mode.

The security measure applied to the EDGE are as follows:

· Encryption: All disks are LUKS encrypted, passphrase OS kernel based encryption requiring a 16 character based password.

· Accessibility: The appliance is a headless service and it is not design for a multi-user capability, therefore access to the operating system is restricted and not available to the business end-user.

- Privilege Access Management PAM.D is installed and configured to lock an account after 5 failed attempts with 900 sec delay.

- Limited accounts available: Root, Bootuser, dmp.
- All access is managed and controlled by G42 Cloud, 16-character minimal length

· Communication: SSL certificate: The certificate crt file is applied to the OS, and all traffic is diverted to the SSL.

· OS hardening:

- The Operating systems is validated using CIS CentOS benchmark CIS CentOS 7 Benchmark L1 and L2.
- Disabling unused network ports (Port 22 and Port 443 are open).
- SSH access hardened using; 22 CIS benchmark recommendation, e.g. root access disabled, maximum authentication tries set to 4, remote host disabled, strong ciphers enabled and etc.
- Disk partitioning to avoid hard drive overflowing by logs, partition encryption.
- Below is the depiction of the CIS benchmark ecosystem of security controls.

Security Architecture Principles

The continuous integration, delivery, and deployment practices, which are characteristic of online and cloud services development and operations, require entirely new mindset, methodologies, and processes, as well as an all-new tool chain. G42 Cloud security process, including security design, secure coding and security testing, third-party software security management, configuration and change management, and pre-release security approval.

Security Design

G42 believes that security fundamentally stems from excellence in design. G42 Cloud and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements.

G42 Cloud runs threat analysis based on the service scenario, data flow diagram, and networking model during the security requirement analysis and design phases.

The threat analysis library, threat mitigation library, and security design solution library used to guide G42 Cloud threat analysis draws from security accumulation and industry best practices in traditional products and new cloud domain products.

After identifying the threat, design engineers develop mitigation measures by utilizing the threat mitigation library and security design solution library, and then implement the corresponding security solution design.

All threat mitigation measures will eventually become security requirements and functions. Additionally, security test case design is completed in accordance with the company's security test case library, and these designs are then implemented to ensure the ultimate security of products and services.

Secure coding and Security Test

G42 Cloud strictly complies with the secure coding specifications released by G42. Before they are on boarded, G42 Cloud service development and test personnel are all required to learn corresponding specifications and prove they have learned these by-passing examinations on them.

G42 adheres to daily checks of the static code using scanning tool, with the resulting data is fed into the cloud service Continuous Integration/Continuous Deployment (CI/CD) tool chain for control and cloud service product quality assessment through the use of quality thresholds. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code-related issues that can extend rollout time coding.

All cloud services pass multiple security tests before release, including but not limited to micro service-level functions and interface security tests such as authentication, authorization, and session security in the alpha phase; API and protocol fuzzing type of testing incorporated in the beta phase; and database security validation testing in the gamma phase.

The test cases cover the security requirements identified in the security design phase and include test cases from an attacker's perspective.

Third-Party Software Security Management

G42 Cloud ensures the secure introduction and use of open source and third-party software based on the principle of strict entry and wide use. G42 Cloud has formulated clear security requirements and complete process control solutions for introduced open source and third-party software, and strictly controls the selection analysis, security test, code security, risk scanning, legal review, software application, and software exit. For example, cybersecurity assessment requirements are added to open-source software selection in the selection analysis phase to strictly control the selection. During the use of third-party software, carry out related activities by taking the third-party software as part of services or solutions, and focus on the assessment of the integration of open source, third-party, and self-developed software, or whether new security issues are introduced when independent third-party software is used in solutions.

Configuration and Change Management

Configuration and change management plays a key role in assuring G42 Cloud security. In G42 Cloud, configuration managers are assigned to manage the configuration of every cloud service, including extracting configuration models (configuration item types, attributes, and relationships) and recording configurations. Additionally, an industry-grade Configuration Management Database (CMDB) tool is utilized to manage configuration items and their relationships with configuration item attributes.

Changes to environments include but are not limited to data center equipment, networks, system hardware and software, and applications, whether those are changes in the equipment used, architectural changes, system software updates (including network device software, OS image, and application container software), or changes in configuration. All changes performed in an organized and priority-driven fashion. After all change requests are generated, they are submitted to the G42 Cloud change and incident management system with change classification assigned. G42 Cloud has established change and incident management processes, followed the industry leading best practices. After the assigned team has reviewed and dedicated change manager approved the requests, the planned changes can be implemented on the production network. Before submitting a change request, the change must undergo an evaluation process. This ensures that the change initiator clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts. All changes and incident activity are subject of tracking and logging for a process quality improvement. G42Cloud perform regular change management process reviews.

Pre-Release Security Approval

To ensure that G42 Cloud infrastructure and cloud services comply with the laws and regulations and customer security requirements G42 Cloud security team and G42 legal and compliance personnel both participate in the decision making of the process of deployment or major update functionality of cloud services. Before releasing new cloud platform versions and key cloud

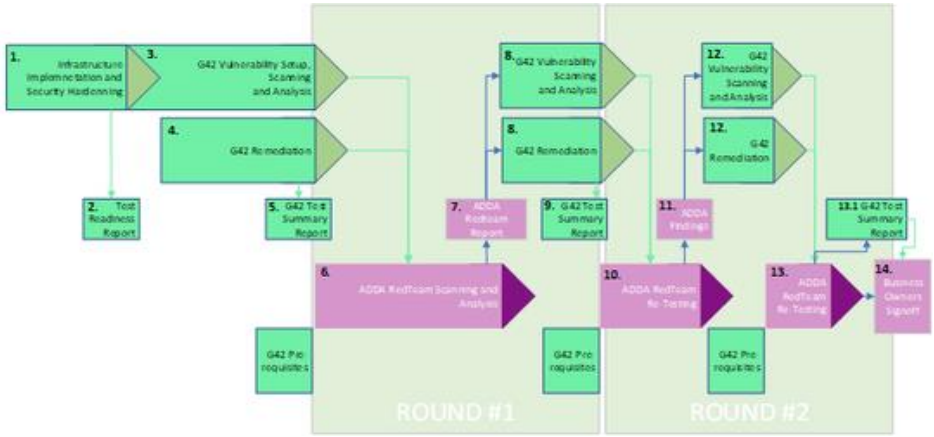
services, teams work together to analyze and determine whether the versions and services to be released meet the security and privacy requirements of the customer and region-specific compliances and regulations.

Security Assurance

Security Testing and Configuration Review is applied across the DEP program. The core aspects of the security assurance activities are based on four key attributes:

- Participants: Who participants and to what extent is their participation.
- Scope: What the targets for security testing (not limited to)/
- Tools: What are the tools/apps used to support security testing.
- Deliverables: What are the outcomes/document of the security testing effort

The diagram below supports the high-level work flow of the security assurance process.



The key tack aways of the process defined above are as follows:

- This procress is to be applied prior to ‘go-live’ for each major release on the DEP program.
- G42 Cloud Program Security Team is to conduct security testing prior to ADDA RedTeam’s security assessment
- G42 Cloud along side 3

rd party vendors will provide the remediations and fixes

- ADDA RedTeam will be engaged 3 times; initial scan, re-test and final re-test (if needed).

- Two rounds of testing are to be planned with 3 round of enaggements with ADDA RedTeam

- The outcome of the security assurance process is a signed-off TSR (aka Secuirty Assessment Report).

The table below lists all the activities shown in the above process diagram.

1. (1) G42 will implement the infrastructure according to the Infrastructure and Network Design and the Security Design documents. Security products and tools will be applied. All security hardening is to be conducted during this period.	1. (2) Prior to the commencement of the G42 Security Testing, a TRR, Test Readiness Review report is to be published, detailing the checklist and prerequisites for the commencement of Security Testing.	1. (3) G42 is to commence with setup of scanning tools and environment and commence the testing activities. All results are to be published in JIRA and/or Excel. The repository must be secure, else, the results are only to be shared using password protections.
1. (4) G42 is to commence remediation as soon as findings are reported.	1. (5) G42 is to prepare a TSR, Test Summary Report (aka SAR) indicating readiness for ADDA RedTeam to commence testing.	1. (6) ADDA Red Team is to commence testing. NB: G42 will apply any prerequisites defined by ADDA RedTeam.
1. (7) ADDA Red Team publish a report and all their findings.	1. (8) G42 is to commence remediation and rescanning in parallel.	1. (9) G42 is to prepare an update TSR (aka SAR) in readiness for the second round of testing with ADDA RedTeam

10. (10) Repeat 6. Reduced scope given initial findings see (7).	(11) Repeat 7. New findings and confirmation of the initial findings.	(12) Remediation and rescanning by G42. (i.e. Repeat 8, new and initial findings to be applied. Reduce scope as compared to (8) is expected).
11. (13) ADDA Red Team commence a retest. This is the final retest to confirm the findings in the 1st and 2nd tests are resolved.	12. (13.1) Final report to be published by G42 showcasing the outcome s of all ADDA redteam tests and any quaifciations that are needed. All outstanding issues are to have a RISK ASSESSMENT and ETA for any future remeduations. The Report is to be published and reviewed prior to the final signoff.	(14) The final SAR (TSR), as prepared by G42 is to be signed off by: • ADDA Security Track lead • G42 Delivery Directory • ADDA Business Track Lead • ADDA Program Director • G42 Program Director • G42 Security Director

Participants

- · G42 Cloud:
  - Responsible: Conduct the security assessment prior to ADDA RedTeam.
  - Responsible: Recursively test the security of the infrastructure and the application.
  - Responsible: Conduct the remediation of the software, infrastructure and data in G42 Cloud.
  - Responsible: Participant in security outcomes, walkthroughs and discussions on the overall security risk of the solution.
  - Accountable: All G42 Cloud native security assets inside the cloud are the security responsibility of G42 Cloud.
  - Responsible: Provide the Security Assessment Report (TSR) for signoff.
- ADDA RedTeam:
  - Responsible: Conduct the initial security assessment and participate in scoping and planning activities.

- o Responsible: Provide a security report on the initial and subsequent security assessments
    - Responsible: Participant in security outcomes, walkthroughs and discussions on the overall security risk of the solution.
    - Responsible: Conduct retests on their findings.
- ADDA Security and Business Track leads:
    - Responsible: To participate, plan and coordinate security assessment meetings prior to go-live for each of the DMP releases.
    - Accountable: For the overall security outcome and the acceptable of the Security Assessment Report.
    - Accountable: Provide signoff on the SAR (Security Assessment Report).

Scope

Scope of each assessment encompasses (not limited to) the following categories:

1. Code scanning
2. Infrastructure security
3. Application Security
4. Security Configuration Review

Code scanning:

- This is performed by G42 Cloud development team and assessed and reported on by the G42 Program Security Team.

Infrastructure:

- This is a vulnerability scan on all the security assets inside G42 Cloud.
- All the IPs are scanned and the outcome of these scanned reports are remediated by the G42/3

rd part vendors.

- Standards are applied, such as CIS benchmarks and API security standards.

Application Security:

- This test targets the G42 web portals DMP and applications EDGE.
- Security hardening features
- Functional security tests using core roles

Security Configuration Review:

- This test reviews the configuration of each of the cloud assets and 3rd party applications.
- The list of the configuration review is assessed against the design and configirmation is made in the SAR as to the configuration outcome of the review
- Security Controls in place are reviewed as to their configuration and status.

IMPORTANT NOTE: In addition to G42 Cloud Program Security Team, the above scope is performed by ADDA RedTeam, based on agreed scope.

Security Testing Tools

Below is the list of tools used for security testing (but not limited to):

Tool	**Reason**	**Who**
Kali Distro	Penetration Testing, Tool rich to conduct many types of security testing	G42 Program Security Team and ADDA RedTeam
Burpsuite	Web Application testing and Traffic sniffing.	G42 Program Security Team and ADDA RedTeam
Tenable, NESSUS	Infrastructure, network and OS scanners. Benchmark scanner.	G42 Program Security Team and ADDA RedTeam
SonarQube	Code security scanning.	G42 Development team
JetBrains, IntelliJ	Java code development. Realtime security scanning and testing	G42 Development team
42Crunch	API standards assessments	G42 Development team
JIRA	Security Issues Tracking.	G42 Security Program Team, Project Managers, G42 Development Team, G42 Infrastructure Team, G42 Managed Services Team.

What are the deliverables

Document/Administration	**Responsible**	**Accountable**
Security Assessment Report (aka TSR)	G42 Cloud Program Security Team	G42 Security Program Director
Risk Acceptance Form	G42 Cloud Program Security Team	ADDA Security Track Owner

Risk Assessment Table	G42 Cloud Program Security Team	G42 Security Program Director
JIRA Tickets	G42 Cloud Program Security Team	Project Manager(s)

JIRA Tickets	G42 Cloud Program Security Team	Project Manager(s)

Compliance Security

Compliance with security standards and regulations is an absolute necessity for gaining and maintaining baseline customer trust. It is also an important measure to defend against insider attacks. Certifications for compliance with security standards and regulations not only improve G42 Cloud's overall security capabilities and service level, but also help mitigate customers' concerns regarding compliance and data security. G42 has information security management system based on applicable UAE laws, industry regulations and international standard.

G42 Cloud ensures that its infrastructure and major cloud services pass evaluations conducted by independent, authoritative, and industry-reputable third-party security organizations as well as reviews by security certification agencies. G42 Cloud provides on its infrastructure only those cloud services that comply with mandatory security standards and regulations. Industry security evaluations and certifications demonstrate G42 Cloud's security strategies, policies, and risk management mechanisms in the people/organization, process, and technology aspects throughout the R&D and O&M lifecycle of its infrastructure and cloud services. Customers can also gain an unbiased and in-depth understanding of G42 Cloud's capabilities and effectiveness in user data protection and cloud service security.

G42 Cloud has established information security management system based on ISO 27001, NESA, ISO 27017, ISO 27018, NIST, CSA CCM, PCI DSS and related standards. The policies and procedures are aligned with P1, P2, P3 and P4 requirements of NESA. Customers can query a formal statement of compliance which will confirm the level of implementation.

G42 Cloud has established more than 30 individual policies for each of the practice areas for Security and Privacy. In alignment with the Information Security Management System, these policies are based on international standards like ISO 27001, NIST, ISO 27017, ISO 27018 etc. and regulations like NESA UAE NIA. In order to maintain an updated status and validity on the certifications, G42 Cloud regular undertakes independent audits and assessments from reputable firms and certification bodies. It is certified on the following standards .

- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- ISO 9001:2015
- ISO 14001:2015
- ISO 45001:2018
- NEAS UAE NIA
- Health Insurance Portability and Accountability Act (HIPAA)
- CSA Star Level 2
- Uptime Tier 3
- DESC – Cloud Service Provider Security Standard by Dubai Electronic Security Center (DESC)
- CSA Trusted Cloud Service Provider
- Payment Card Industry Data Security Standards (PCI DSS) v3.2.1
- ISO 31000:2018
- SOC 1, SOC 2 – Type 1 attestation

Finally, G42 Cloud has established a formal and regular audit plan, including continuous and independent internal and external evaluation. Internal evaluation continuously tracks the effectiveness of security control measures, and external evaluation is audited as an independent auditor for reviewing the efficiency and effectiveness of security controls. Aside from this evaluations, G42 Cloud conducts penetration tests on a regular basis, and has a dedicated team to follow up the test results. The penetration test report and follow-up would be verified by internal audits and external certification agencies, but the report is not provided to tenants as it may violate privacy rights of other tenants.

G42 Cloud has set up professional positions to maintain contact with external parties to monitor relevant laws and regulations. When new laws and regulations related to G42 Cloud services are released, G42 Cloud would promptly adjust internal security requirements, security controls and follow up the compliance of laws and regulations

G42 Cloud security is following NESA policies and Standards. This section will explains the security controls sets from NESA that fit our DCD implementation as below:

#	**Security Control Sets**	**Description Referenced to DMP**
1	Information security policies	The IAM service and the details about the enterprise projects, groups and users are covered in the IAM and DMP Access sections of this document. IAM Service covers all the security controls like Authentication, Identity Federation and Account management.
2	Access control	G42 Cloud services access is defined based on the platform function and the exposed services can be accessed through ADNET MPLS. The traffic passes the PA firewall to make sure the applied policies by the firewalls. Refer to the IAM, UAM, VPC, Security Gates, Security Layers and Zoning defined in this document.
3	Physical and environmental security	Physical security of G42 Cloud is based on the Risk and Compliance standards of the Cloud Service Provider and is part of the Terms and Conditions based on the Shared Responsibility Matrix. Environmental security includes the security controls for the infrastructure security, application security and data security.
4	Cryptography	Encryption controls are applied for data at rest by using KMS service. AES256 is used for all encryption for data-at-rest and using RSA tokens greater than 16 characters. Data in transit is using encryption controls applied for data at transit by using SSL/TLS 1.2 and above. Refer to the previous section for all encryption references.

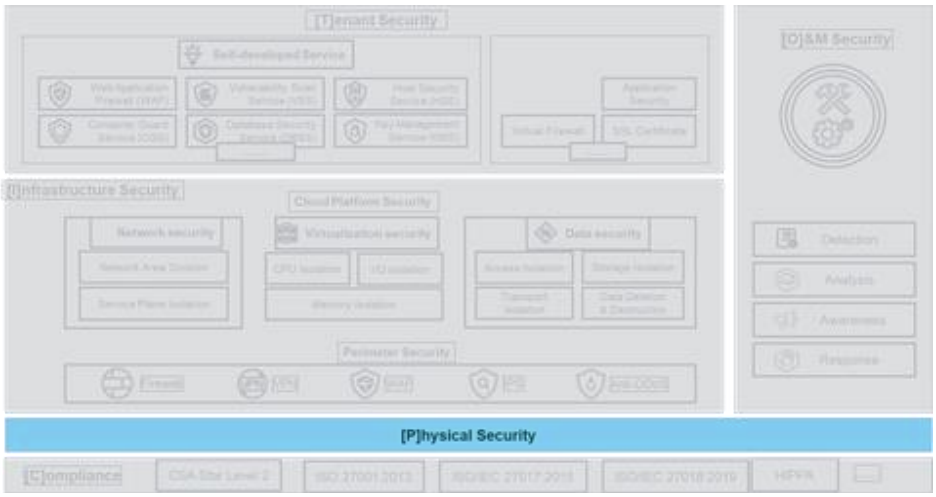
The G42 Security Assurance reports and due diligence shall comply with benchmark standards across the Tenant assets including APIs.

#	**Assets and Configurations**	**Standards and Tools**

1	OS Hardening – CentOS, Windows	CIS CentOS benchmark – supported by Tenable Nessus CIS Policy (CIS WorkBench / Benchmarks (cisecurity.org)) CIS Windows version X benchmark – supported by Tenable Nessus CIS Policy (CIS WorkBench / Benchmarks (cisecurity.org))
2	Apache Tomcat	CIS Apache Tomcat * Benchmark - – supported by Tenable Nessus CIS Policy (CIS WorkBench / Benchmarks (cisecurity.org))
3	MySQL (stand alone)	CSI MySQL Benchmark - – supported by Tenable Nessus CIS Policy (CIS WorkBench / Benchmarks (cisecurity.org))
4	Postgre (stand alone)	CSI PostgreSQL Benchmark - – supported by Tenable Nessus CIS Policy (CIS WorkBench / Benchmarks (cisecurity.org))
5	MySQL, PostgrSQL	Partial CIS MySQL / PostgrSQL Benchmark (i.e. 34 items not applicable since RDS is a database as a service and not MySQL) - – supported by Tenable Nessus CIS Policy (CIS WorkBench / Benchmarks (cisecurity.org))
6	Docker	CSI Docker Benchmark - supported by Tenable Nessus CIS Policy (CIS WorkBench / Benchmarks (cisecurity.org)
7	API Security	OWASP API Security Top 10 – supported by 42Crunch and APIsecuirty.io (OWASP API Security Top 10 cheat sheet)

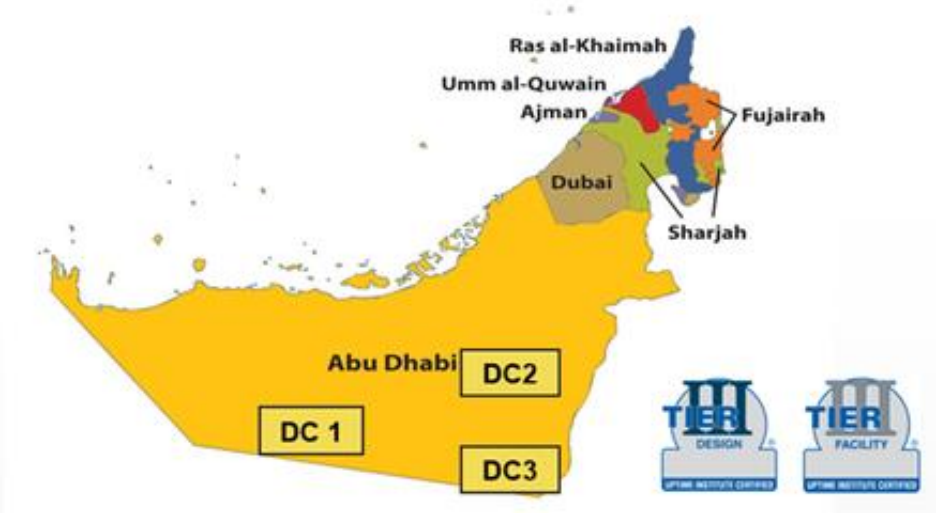
By default, all tenant assets that are applied and that need to be assessed against a security standard benchmark, CIS (Center for Internet Security) and OWASP will be applied by default where it has not be explicitly defined by ADDA.

Physical Security

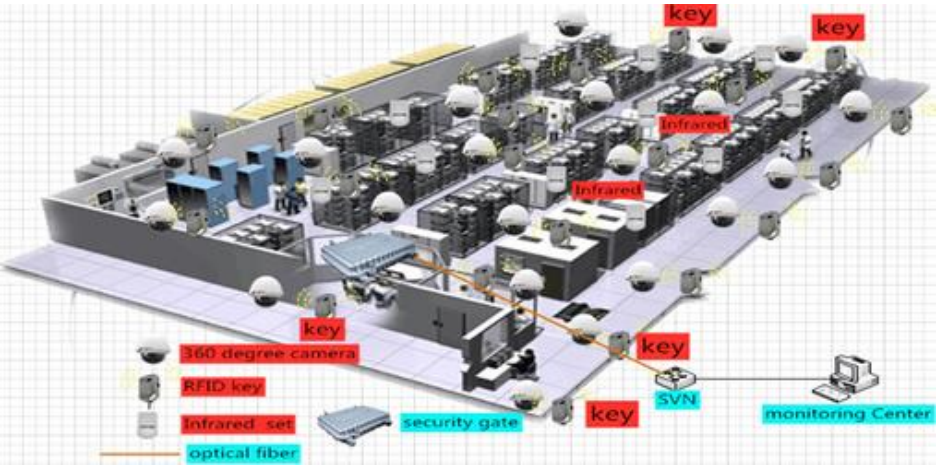


G42 Cloud has established comprehensive physical security and environmental safety protection measures, strategies, and procedures that comply with T3+ standard of TIA-942 Telecommunications Infrastructure Standard for Data Centers. G42 Cloud data centers are located on suitable physical sites within UAE, as determined from solid site surveys. During the design, construction, and operation stages, the data centers have proper physical zoning and well-organized placement of information systems and components, which helps prevent potential physical and environmental risk scenarios (for example, fire or electro-magnetic leakage) as well as unauthorized access. Furthermore, sufficient data center space and adequate electrical, networking, and cooling capacities are reserved in order to meet not only today's infrastructure requirements but also the demands of tomorrow's rapid infrastructure expansion. The G42 Cloud O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental safety of G42 Cloud data centers.

Data Center Site Selection: When choosing a location for a G42 Cloud data center, G42 Cloud factors in the risks of potential natural disasters and environmental threats, making sure to always avoid hazardous and disaster-prone regions and minimize the potential operational interruption by the surrounding environment of a G42 Cloud data center. For example, G42 Cloud data centers are always located in areas where there are no potentially hazard-causing laboratories, chemical plants, or other hazardous zones within 400 meters. Site selection also ensures the availability and redundancy of supporting utilities for data center operations, such as power, water, and telecommunication circuits.



Physical access control: G42 Cloud enforces stringent data center access control for both personnel and equipment. Security guards, stationed 24/7 at every entrance to each G42 Cloud data center site as well as at the entrance of each building on site, are responsible for registering and monitoring visitors and staff, managing their access scope on an as-needed basis. Different security strategies are applied to the physical access control systems at different zones of the data center site for optimal physical security. Security guards strictly review and regularly audit user access privileges. Important physical components of a data center are stored in designated safes with crypto-based electronic access code protection in the data center storage warehouses. Only authorized personnel can access and operate the safes. Work orders must be filled out before any physical components within the data center can be carried out of the data center. Personnel removing any data center components must be registered in the warehouse management system (WMS). Designated personnel perform periodic inventories on all physical equipment and warehouse materials. Data center administrators not only perform routine safety checks but also audit data center visitor logs on an as-needed basis to ensure that unauthorized personnel have no access to data centers.



Safety measures: G42 Cloud data centers employ industry standard data center physical security technologies to monitor and eliminate physical hazards and physical security concerns. CCTV monitoring is enabled 24/7 for data centers' physical perimeters, entrances, exits, hallways, elevators, and computer cage areas. CCTV is also integrated with infrared sensors and physical access control systems. Security guards routinely patrol data centers and set up online electronic patrol systems such that unauthorized access and other physical security incidents promptly trigger sound and light alarms.

Electrical safety: G42 Cloud data centers employ a multi-level safety assurance solution to ensure 24/7 service availability and continuity. Daily electricity consumption at data centers relies on dual power supply from different power substations. Data centers are equipped with diesel generators, which are run in the event of power outage, and also Uninterruptible Power Supply (UPS), which provides temporary power as a backup. Data center power lines have voltage regulator and overvoltage protection. Power supply equipment is configured with redundancy and power lines run in parallel to ensure power supply to data center computer systems.

Temperature and humidity control: G42 Cloud data centers are fitted with high precision air conditioning and automatic adjustment of centralized humidifiers to ensure that computer systems operate optimally within their specified ranges of temperature and humidity. Hot and cold air channels for computer cabinets are properly designed and positioned. Cold air channels are sealed to prevent isolated hot spots. The space beneath the raised floor is used as a static pressure box to supply air to computer cabinets.

Fire control: G42 Cloud data centers comply with Level-1 design and use Class-A fireproof materials for their construction in compliance with country-specific fire control regulations. Flame retardant and fire-resistant cables are used in pipelines and troughs, alongside power leakage detection devices. Automatic fire alarm and fire extinguishing system is deployed to quickly and accurately detect and report fires. Automatic alarm system links with power supply, monitoring, and ventilation systems such that the fire extinguishing system can activate itself even when unattended, autonomously keeping fires under control.

Routine monitoring: G42 Cloud personnel conduct daily patrols and routine inspections of power, temperature, humidity, and fire controls in all data centers, which allows for the timely discovery of safety hazards and ensures smooth operation of all data center equipment.

Water supply and drainage: The water supply and drainage system at each G42 Cloud data center is designed, implemented, and operated to an exacting standard, ensuring that main valves function as per specification and key personnel are aware of valve locations. This prevents water damage to the data center equipment, especially computer information systems. Data center buildings reside on elevated ground with peripheral green drains and each floor is raised, which speeds up water drainage and reduces the risk of flooding. Data center buildings all meet Level-1 water resistance requirements, ensuring that rainwater does not seep through roofs and walls into the data center, and that there is proper drainage in case of a flood.

Anti-static control: G42 Cloud data centers are paved with anti-static flooring materials and have wires connect raised floor brackets to grounding networks, discharging static electricity from computer equipment. Data center roofs are fitted with lightning belts, and power lines are fitted with multiple-level lighting arresters, diverting the current safely to grounding.