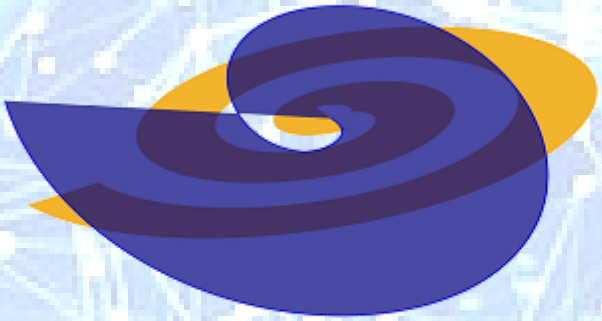

Cloud Migration Security Infrastructure Guide

Contents

Overview

Introduction

A Cloud Application Platform is defined as the set of browser, device, web, hosting and network infrastructure and services deployed to a hybrid deployment scenario (public and private clouds and on premises data centre services) required to support a business capability.

Cloud security services are more effective when they are deployed on a solid foundation of network, hosting infrastructure, platform and software deployment configuration.

The technical foundation for defence-in-depth security calls for:

1. Cloud Application Platform Security Management,
2. Application Monitoring,
3. Deployment Management and Monitoring
4. Service Operations Monitoring

A guided approach to ensuring that hosting, network and platform delivery is secure from the outset is essential for successful cloud migration

Intended Use

The purpose of this document is to provide technical security guidance on Cloud Application Platform Infrastructure Security.

The target audience for this document consists of all project stakeholders with an interest in security – including the steering committee, decision makers, business and technical subject matter experts, program and project managers. third-party partners and suppliers.

In Scope

The scope of this document includes the development of guidelines and selection criteria, automation of deployment and operations monitoring including

Cloud Application Platform IaaS, PaaS and SaaS services

1. Common platform services such as caching and content delivery, logging and monitoring 2. Network inter-connectivity between services and intra-connectivity between deployment domains e.g. cloud and enterprise

Out of scope

This guide excludes,

1. Application integration design

2. Service Management processes and tools
3. Application development -application Development Operations and Network teams artefacts
4. Development tools, source code, build, test and deployment management
5. Migration approach and code deployment
6. Secure DevOps

Pre-requisites

Functional, non-functional, technical and security requirements

1. IT Functional and Technical Specification Requirements
2. Security Regulation Compliance Requirements

Decisions and Assumptions

Key design decisions

Detail and document selection criteria for Cloud Application Platform security services to be developed. Key decisions to be documented.

Assumptions

1. CSP PaaS services to be utilised considering ease of operations, least complexity and rapid deployment
2. The principle of least privilege applies to access rights for all users, applications and services 3. On-premise configuration to be documented if relevant
4. Data privacy regulation compliance (e.g. PCI-DSS and GDPR and other PII information). An assessment of compliance will be applicable post deployment.
5. Secure access to application/DevOps team code repositories, pipeline scripts and infrastructure automation scripts
6. Disaster recovery design if required for production environment to be capable of handling production load at any point of time. (The DR setup should be active-active or active-passive with minimal effort to restore the services)

Reference Architecture

Cloud Application Platform

The Cloud Application Platform is defined as the software platform, hosting and network infrastructure to provide the development, testing/ QA, pre-prod and production environments and all supporting services to manage those environments. The following are general environment design guidelines

1. The application environments will have one or more types of environment as shown

below, a. Production – PROD and DR

b. Test – QA, Performance testing, UAT testing, etc.

c. System Test – Integration, Development and Security testing

d. Development.

2. The services deployed in an environment category cannot be shared with other environments to ensure that it meets isolation requirements. Exceptions may be made for example
3. Common services may be shared between application environments.

The various technologies/services that will be deployed in an environment (like production) are to be clearly documented.

Cloud Application Platform Accounts

Provide information about the account and subscription model

Cloud Application Platform Technical Reference Architecture

Provide links to technical architecture documents.

Security Principles

The following principles apply to the Cloud Application Platform

1. Applications that consist of multiple incoming traffic and outgoing traffic from desktop and mobile applications, internal and external users comprise multiple network segment and subnets to isolate the traffic.
2. Secure network connections established between network nodes and the Cloud Application Platform for internal and external users. Connectivity between cloud and enterprise domains and services to be secure.
3. The Cloud Application Platform must provide DDOS protection at the network layer for the incoming traffic and at the application layer for common exploits. DDoS attacks are most common at layers 3, 4, 6, and 7 of the Open Systems Interconnection (OSI) model, which is described in the table below. Layer 3 and 4 attacks correspond to the Network and Transport layers of the OSI model, referred to collectively as infrastructure layer attacks. Layer 6 and 7 attacks correspond to the Presentation and Application layers of the OSI model referred to collectively as application layer attacks. Filtering machine learning rules are deployed at the Application Gateway WAF for layer 7 protection before the connection terminates at web/app servers.
4. API protection using authentication and authorization to prevent exposing application functions directly to user web traffic.
5. Application security secrets and keys configured to use database and data services, and other PaaS services as required by the application security context risk.
6. Connections such as encrypted site to site connections from the enterprise to Cloud Application Platform secured by network layer security measures must be documented as part of the technical architecture

Anti DDoS Protection

DDoS Attack Vectors by OSI and TCP/IP Model Layer					
#	OSI Layer	TCP/IP Layer	Protocol Data Unit	Description	Common Attacks
7	Application	Application	Data	Network process to application	http floods, DNS query floods
6	Presentation		Data	Data representation & encryption	TLS/SSL Exploits
5	Session		Data	Interhost communication	N/A
4	Transport	Transport	Segments	End-to-end connections & reliability	SYN floods
3	Network	Internet	Packets	Path determination addressing	UDP reflection attacks
2	Datalinks	Network Access	Frames	Physical addressing	N/A
1	Physical		Bits	Media, signal & binary transmission	N/A

Source: https://aws.amazon.com/shield/ddos-attack-protection/

Identity Management

Policy based access to resources combined with Identity Management/Role Based Access Control is common for all cloud services across all Cloud Service Providers (CSPs). Separate groups can be

created & users added into groups with permission sets (often described by deployment identity policies). Group level access is provided in the first instance on an account basis, and subsequently mapped for access by particular privileges.

Identity Management roles generally are a set of access privileges for any user (can be a person, a device, an application or a service) granted short term credentials to any resources.

The following security configurations are recommended

Role Based Access Control

Every CSP uses roles to manage access to account resources. Assignment of these access rights is usually by defining a policy via the CSP platform web interface, command-line tools, and APIs. Users can be persons, devices, applications, services or resources.

Access is granted by assigning the appropriate RBAC role to users, groups, services and applications for a certain scope identified in the access policy. Each CSP has a different method of providing child access to resources using IAM policies and a rule set that applies logic to the order and superimposition of privileges across resources.

The RBAC role and its privileges governs what resource privileges the role, user, group, application or service can exercise within the scope of the access policy.

Multi Factor Authentication

Cloud Application Platform web interface access can be secured by enabling Multi-Factor Authentication (MFA). This ensures that there is an additional level of security mechanism for user validation as well as the default authentication method.
Options such as biometrics and additional code can be configured. MFA can be enabled for all web interface users. The users can select the second authentication option on their first login. In case of second factor change or loss, the users will have to re authenticate their login Cloud Application Platform web interface.

Privileged Identity Management

Cloud Application Platform privileged identities such as developers and administrators must be authenticated by the Cloud Application Platform Identity Management, with access monitored by platform logging and monitoring.

Privileged Identity Management can be configured to control and monitor privileged users for example

1. Monitor Identity Management/RBAC administrators
2. Report on administrator access history and changes in administrator assignments 3. Receive operational alerts about privileged role access
    a. Roles being assigned outside of privileges
    b. Roles being activated too frequently

c. Roles not required to have multi-factor authentication for activation

Identity Management/RBAC roles for privileged users must be carefully managed and reported on with access logging to ensure principles of 'least privilege' apply, and no unauthorised activity and no unnecessary escalation of privileges takes place. Identity Management/RBAC PIM can allow for temporary assignment of admin roles for existing users

CSP Identity Management/RBAC Privileged Identity Management monitoring dashboards can provide graphics privileged user accesses and even recommendations based on privilege usage.

Audit histories can be used to review the privileged roles usage. Periodic review of access validates whether the users continue to require privileged access and can be removed from the administrator group when required.

Anomaly notification can be configured to send emails to Administrators. For example, the anomaly report "Sign-ins from multiple geographies" includes successful sign-ins from a user where two sign-ins appeared to originate from different regions and the time between the sign-ins makes it impossible for the user to have travelled between those regions. It is important to aggregate identified security patterns across multiple logging sources to avoid false positives:

Possible causes include:

1. User is sharing their password with other users
2. User is using a remote desktop to launch a web browser for sign-in
3. A hacker has signed into the account of a user from a different country
4. User is using a VPN or proxy
5. User is signed in from multiple devices at the same time, such as a desktop and a mobile phone, and the IP address of the mobile phone is unusual.
6. The notification enabled in Identity Management/RBAC reports can trigger an email to all Admins who have been assigned to an account.

Network Setup

Document the design for secure networking

Network Segment Design

Cloud Application Platform Network Segment facilitates private IP address space for deployed Virtual Machines and other Cloud Application Platform services that support private IP addresses in the Cloud Application Platform. The IP Address range is allocated from new and existing Enterprise IP schema. The following diagram depicts a typical Network Segment design to be used in production, testing and development environments.

Network Segments can be created in each subscription/account. Design considerations are critical

for each deployment.

Subnet Design

Each network segment can have multiple subnets depending upon the security requirements, communications between each subnet can be restricted by defining Network Security Groups. Considerations for isolation of network subnets include data privacy, use of keys and secrets to secure functions and data, ownership of functional capability.

Network Security Groups

A network security group (NSG) contains access control list (ACL) rules that allow or deny network traffic to VM instances in a Virtual Network.

Site-to-Site Connectivity Requirements

Site-to-Site connectivity between the Cloud Application Platform and the enterprise on-premises data centre, public cloud platform and application services can be established. Care has to be given to ensure that the appropriate level of network security is enabled, particularly when sensitive/classified data, third parties, and internet connectivity are involved.

Consideration has to be given for active-active connections to provide high availability for networks that support dynamic routing.

The capability and limitations of networks has to be considered in view of the real level of security provided by the type of network connection, e.g. private network, IP-Sec VPN, SSL VPN, encryption, ZT SPA etc.

S2S connectivity for non-production environments can be treated differently in view of factors such

Private network connections can be used for Cloud Application Platform production environments and network segments at a throughput rate offered by the CSP (e.g. 200 Mbps capacity) with redundant connectivity to the Cloud Application Platform as required. The private connection can be established to connect for example the customer's data centre (primary and secondary) with the Cloud Application Platform CSP deployment regions.
In case of disaster scenario, the Cloud Application Platform DR region can access the backend services using the private connection with backend services in the customer's secondary data centre as required.

Applications Inbound Traffic Flow

Document and diagram all inbound traffic flows and their security protections
Applications will have multiple inbound connections coming from different sections of users, so it is useful to document the traffic to ensure that security is maintained.

Applications Outbound Traffic Flow

Document and diagram all outbound traffic security protections

Applications will have multiple outbound connections based on the inbound connection made, and the type of internal and external connectivity, e.g. https and encryption to database, private connection to third party data centre.

Test Environment

Document test environments networking arrangements, and any automated deployment scripts and pipelines

PaaS Components

Document the Cloud Application Platform CSP PaaS components/services configurations as a reference. The same configuration and standards can be followed for non-production environments with scaled down configuration.

Databases

Describe the databases that are created and used, the regions where the databases are deployed and connection string details or access services endpoints, including geographical replications

Describe the firewall rules to be set up to enable secure connection to the Cloud Application Platform databases, including the IP addresses can be whitelisted in the firewall rules for support activities if required. Otherwise list the access methods and the security used for accessing the deployed databases

Security Measures

Provide details for database and storage connectivity and platform security including configuration such as

1. Connection string to be secured using the Key vault and the resulting URL will be shared with the Application team for integration with the application.
2. Role Based secure access to the Cloud Application Platform databases including white listed IPs. 3. Cloud Application Platform database network firewalls from an internet gateway. 4. TCP port restrictions
5. Authentication and authorisation methods
6. Database events for monitoring and analysis.
7. Database encryption options
8. Data Masking to limit sensitive data exposure to non-privileged users.
9. SQL Threat Detection Policy configuration and security alerts upon detection of suspicious database activities.

Backup

Document backup requirements such as

1. Infrastructure-as-Code templates for each service with version details will be kept in a secure storage. In the case of disaster, can set up a new environment using templates.
2. Database backup includes both local database backups and geo-redundant backups.
3. These backups are created automatically.
4. For local database backups, full database backups happen weekly, differential database backups happen hourly, and transaction log backups happen every five minutes.
5. Transaction log backups happen every five minutes so we can do a point-in-time restore to the same server that hosts the database.
6. Retention period for the backup is 35 days or as per requirement, any data related to financial transactions to be configured for x years retention, configured to have backup for x years of production transactions.

In the case of disaster in a region, determine failover arrangements e.g. for a secondary database to be available in the appropriate region.

Common Services e.g. Logging, Cache, Search, Notifications, Secrets Vault etc

Provide details of common services security measures.

Follow best practice Cloud Security Provider (CSP) advice for securing common services such as Caching, Notifications, API Management, Blob/Bucket Storage, Content Edge services, etc.

General Security Measures

1. Database connection string to be secured using the key/secrets vault to be used for access/integration
2. Consider using different types of keys to access sensitive services.
3. Role Based Access Controls to be implemented.
4. Short term security credentials to be used for most services.
5. Key security to restrict access via the CSP CLI or provided APIs.
6. Protect private network segments.

High Availability

Part of the security of the Cloud Application Platform is high availability. A highly available application absorbs fluctuations in availability, load, and temporary failures in the dependent services and hardware. The application continues to operate at an acceptable user and systemic response level, as defined by business requirements or application service-level agreements (SLAs).

Cloud Application Platform Virtual Machines Availability

Cloud Application Platform continuity can be assured with high availability measures depending on the platform to ensure capacity and high availability even in case of partial VM outage occurring due to maintenance tasks.

High Availability for PaaS services

Document the measures taken to ensure high availability of all the PaaS services, e.g. a primary and a replica, automatic failover

Cloud Application Platform Database availability

1. Document the measures taken to ensure database availability
2. Premium tier database gives 99.99% availability Secondary Database in different regions will be available in read only mode until fail-over happens.
3. Application must be designed to connect to a secondary instance in case of failure in the primary instance.
4. For local database backups, full database backups happen weekly, differential database backups happen hourly, and transaction log backups happen every x minutes.
5. The transaction log backups happen every x minutes enabling a point-in-time restore to the same server that hosts the database.

Production Environment

Provide a detailed sizing document. An example of sizing for IaaS and Paas components in production environment are given below

DR Environment

Document the DR Environment. This will be similar to Production. All the components will be configured with similar sizing as per production.

TEST environments

Document the Test Environments

Storage Account Security

Cloud Application Platform VMs operating system disk space will be assigned as per the Cloud Application Platform instance selected. Security Principles to be followed for Storage Accounts.

Storage redundancy

1. Backup data across regions for business continuity
2. Access to the blob/bucket storage data secured by short term security credentials, whitelisted and restricted by https connections and time limits.
3. Storage account type private to restrict access in public.

Encryption in Transit

Transport-Level Encryption – Using httpS for Cloud Application Platform Files, Storage and Cloud Application Platform Apps.

Encryption at Rest

The Cloud Application Platform Storage encryption to be enabled for all the storage accounts

1. Cloud Application Platform storage automatically encrypts the data prior to persisting to storage and decrypts prior to retrieval.
2. The process of encryption, decryption and Key management is transparent
3. Encryption using 256-bit AES encryption.

Storage Account Replication

Cloud Service Providers offer various levels of data redundancy and replication features as part of storage account virtual machine disks, blob/bucket storage, storage for logs and storage for backup data.

1. Locally Redundant Storage (LRS): All data in the storage account is made durable by replicating transactions synchronously to several different storage nodes within the same region.

2. Geo Redundant Storage (GRS): This is the default option for redundancy when a storage account is created. Like LRS, transactions are replicated synchronously to several storage nodes within the primary region. Transactions may be queued for asynchronous replication to another secondary region.

Domain Services Availability

Deploying additional domain controllers increases the redundancy, which results in even greater resilience and higher availability. This also improves the performance of your directory by supporting a greater number of identity requests.

Monitoring

This section covers monitoring solutions for both infrastructure and application security & performance monitoring requirements. Document which monitoring tools will be used for a specific monitoring requirement.

The following table provides an example of requirements for internal and external regulatory monitoring.

Monitoring Requirement Response
Compliance Certifications ISO 27001, PCI-DSS Level 1, and SOC 1 / SSAE 16 Data Retention xGB depending on the deployment size for x years

Encryption	TLS 1.3 encryption for data in transit and transaction data encrypted at rest metrics
Infrastructure metrics collected	Host metrics (host details, RAM/CPU usage, hard disk IO usage, network activity, and database transactions) and various application metrics

Monitoring Deployment Architecture

Document and diagram the deployment architecture of monitoring tools. Explains the account permissions for monitoring tools.

Cloud Application Platform Infrastructure and Platform Monitoring

Cloud Application Platform monitoring must be enabled on the CSP platform for all CSP services such as

1. API Management
2. Load Balancers and Container Load Balancer
3. Virtual Machines and Containers
4. Key Vault Services
5. Cache Services
6. Databases
7. Search and Query Services
8. Storage services
9. Notification and email services

Backup Solution

Document the backup solution, and the arrangements to restore from backup

Logging and Log Management

Security for logging solutions for both infrastructure and application services is required. The following information provides an overview of typical logging services.

Identity Management/RBAC Logging

1. Sign-in activities – Information about the usage of managed applications and user sign-in activities 2. Audit logs - System activity information about users and group management, your managed applications and directory activities
3. Configuration Standards
4. Users can be created to perform various activities that include security analysis, application analysis and infrastructure operation management. The necessary roles will be defined with the appropriate permissions

5. TLS/SSL certificates to be configured on Cloud Application Platform
6. Separate indexes will be created for long-term (e.g., security logs) and short-term (e.g., app logs) with different retention periods
7. The necessary logical or role-base boundaries will be created for indexes to provide an isolation 8. The logs to have archival policy configuration

Web Application Firewalls

There are various security products for application layer endpoint monitoring, however they all have prevention and detection services for potential threats. This section refers to the generic capability of applying logic and pattern detection to potential threats. It also applies to operational analytics that either automatically or using analysis techniques detect risks, potential and actual attacks. The web application firewall (WAF) capability that protects the application against common vulnerabilities such as the following:

1. OWASP top 10 common web vulnerabilities
2. SQL injection protection
3. Cross site scripting protection
4. Common Web Attacks Protection such as command injection, http request smuggling, http response splitting, and remote file inclusion attacks.
5. Protection against http protocol violations
6. Protection against http protocol anomalies such as missing host user-agent and accept headers.
7. Prevention against bots, crawlers, and scanners
8. Detection of common application misconfigurations (i.e. Apache, IIS, etc)
9. Protects from common Application Layer 7 web attacks.

Key vault

Key Vaults can be to help safeguard cryptographic keys and secrets used by applications and services. Each environment may have a separate Key Vault. Administrator access to be audited.

Administrator capability

1. Create or import a key or secret
2. Revoke or delete a key or secret
3. Authorise users or applications to access the key vault, so they can then manage or use its keys and secrets
4. Configure key usage
5. Monitor key usage

Access to a key vault is controlled via two separate interfaces for both the management(administration) and data (access) planes. Access permissions are granted through CSP APIs, and access to be monitored and audited

Certificate Management

Decision and document public certificate providers for application URLs to be installed e.g. for

1. Web Server
2. Application Server
3. API Management
4. Content Delivery

Build Automation Templates

Infrastructure as Code automates the creation, deployment, monitoring, and maintenance of resources in the Cloud Application Platform environment using a template workflow execution engine.

Infrastructure as a Service Resources:-

An overview of IaaS provides a security view of the automation of infrastructure capabilities. Documentation of manual and automated management of resource planning is essential. This provides a record and a reference for how the infrastructure is designed and deployed for management and maintenance purposes.

Platform as a Service Resources:-

An overview of PaaS provides a security view of the CSP platform capabilities. Documentation of manual and automated management of resource planning is essential. This provides a record and a reference for how the platform is designed and deployed for management and maintenance purposes.

Business Continuity and Disaster Recovery

Cloud Application Platform Region Selection

Based on the business user's location, the primary Cloud Application Platform region is selected. The disaster region is chosen as the next nearest for the business users. Document both the primary and disaster regions and the rationale.

Active Passive Disaster Recovery

Provide a rationale for choosing active or passive DR configuration e.g. is primarily due to increased complexity or latency due to stateful services