Voyager Infinity - Security, Resilience & Disaster Recovery

Deployment Types

Infinity is a client-server application that can be deployed entirely on-premise or in a SaaS environment with Voyager Software hosting the service and data on the Azure platform. Server Azure regions are used based on the customer's location - for example UK clients are deployed using the Western Europe region[1]. This document is primarily focused at the Infinity SaaS platform but does include on-premise information where relevant.

Infinity Client to Server (Middle Tier) Communication

The Infinity client communicates with the middle tier, be it on-premise or SaaS, over TCP using the Microsoft WCF framework. WCF over TCP uses Transport Level Security (TLS) provided by the underlying OS[2] with an x509 certificate used to verify client server authentication[3]. Infinity SaaS uses a third-party publicly trusted certificate and Infinity on-premise ships with an Ikiru People generated SSL certificate.

Infinity Middle Tier to SQL Server

The Infinity SaaS middle tier connects to the SQL Server using a connection string with Encrypt=true and TrustServerCertificate=False. This ensures that the communication between the Infinity SaaS middle tier and Azure SQL Server is encrypted by the underlying OS using Transport Layer Security and a certificate supplied by the Azure platform. Infinity on-premise defaults to Encrypt=True and TrustServerCertificate=True. Whilst this ensures that the data is secured using Transport Layer Security, it does not prevent man-in-the-middle attacks and organisations wishing to secure against this must configure their on-premise SQL Server with the necessary certificates.

Infinity User Authentication

Each Infinity user, whether on SaaS or on-premise, will be given a unique username and password. These are managed from within the Infinity product by users with the necessary permissions. The Infinity system can be configured to ensure that user passwords have a minimum length, at least one alpha and numeric, an expiry window and a history to prevent password re-use.

2-Factor Authentication (MFA)

MFA, or specifically 2-Factor Authentication, can be enabled by a customer's Infinity Administrator which will then require a code to be generated using an authenticator app and entered on the screen each time the user logs into the Infinity application. Supported smartphone authenticator apps include Google Authenticator and Microsoft Authenticator.

Infinity App Server

The Infinity App Server VM is deployed as part of the Infinity SaaS infrastructure and is used to host the various Infinity integration services. These integration services connect to third party services such as Broadbean, Logic Melon, TimesheetPortal and Office365 Exchange. Access to the read-only VM is required by Voyager support staff to diagnose customer reported issues and is done via a non-admin read-only account. Admin access is available to a subset of the development team for more advanced support and deployment purposes. The Infinity App Server VM OS and data disks are encrypted using Bitlocker with keys and secrets secured in Azure KeyVault. Plus, the Infinity App Server VM is configured on a virtual network with network security groups to limit access to Infinity SaaS services and IPs only.

Infinity SaaS Penetration Testing

A third-party security company conducts regular penetration of the Infinity SaaS product.

Configuration Management & Version Control

Infinity is developed using automated continuous deployment. This means that each version is compiled, unit tested and deployed automatically to the development SaaS environment, usually daily during a sprint. When the release has passed formal testing, it can then be deployed automatically to a staging environment and subsequently to the live environment. Each build in a sprint increments the release version, and the installers for each version are automatically signed with a code signing certificate which can be checked to ensure that the installer is valid.

Azure Platform Security

SQL Azure is configured with Transparent Data Encryption[4] enabled. This ensures that each database is encrypted at rest.

SQL Azure Firewall with virtual network rules are configured to limit access to Infinity SaaS services and IPs only.

Items stored in the Azure Redis cache are encrypted, expire after six hours and are not persisted when the Redis service restarts.

SQL Server Azure Auditing[5] and Threat Detection[6] is active with alerts. Customer auditing information/report requests relating to Infinity activity are chargeable on a per case basis and can be logged with the Support Team.

SQL Azure Firewall is configured to limit access to Azure services and Voyager IPs only.

Azure Security Centre[7] is monitored and used to ensure that security risks are actioned and resolved.

Sensitive application configuration settings are encrypted with a certificate and private key during the deployment process, so this is never exposed in the live environment.

Access to the Azure platform is limited to a subset of the development team who use their Azure Active Directory account for authentication. Multifactor authentication is enabled on all Ikiru People Azure Active Directory user accounts.

Passwords for special functions, such as the deployment account, are stored in a secure encrypted system with access which is limited to the subset of the development team.

The development team monitors enhancements of the general Azure platform and schedules work into the development roadmap to take advantage of new security features.

Azure Platform Scalability

The Infinity SaaS SQL Azure databases are deployed into an Elastic Pool. This enables any individual database to increase its consumption of resources such as CPU and memory by using the pool of shared resources. The elastic pool is significantly oversized and at the time of writing average weekly eDTU (a measure of resource consumption on the SQL Azure Elastic pool) is at 11.6%.

The Infinity SaaS middle tier is based on Azure Cloud Services. These cloud services are configured to autoscale based on demand. At the time of writing, the most heavily used cloud services are running with twenty-four instances during peak demand. If needed, additional services can be added in minutes by simply increasing a number in the Azure portal.

Backup

Infinity SaaS uses the Standard tier of SQL Azure. This provides automatic georedundant full, differential, and transactional backups[8]. This means that Infinity SaaS databases can be restored to the transactional log period, which according to Microsoft is approximately 5 to 10 minutes. Backups are retained for 35 days.

Disaster Recovery

Should a disaster recovery process be required, the automated deployment process allows the Infinity team to recreate a mirror Infinity SaaS environment in a different Azure region. This mirror environment would usually be created in the partner region for the SQL Azure georedundant backups.

The SQL Azure standard tier provides an Estimated Time to Recovery of less than 12 hours and a Recovery Point Objective of an hour[9]. This means that in a full DR the database restore is expected to take less than twelve hours and less than one hour’s worth of data would be expected to be lost.

This DR process is tested on a regular basis to ensure that there has been no “drift” between the live environment and the deployment scripts.

Staff & Compliance Enforcement

a) Staff Onboarding

All staff who have access to client data are reference checked and background checked prior to commencing employment with Ikiru People. Staff are trained on data protection legislation and cyber security as part of their induction process using both internal and third party learning methods.

b) Staff Leaving

There is a defined procedure for staff departing the company. This sets out amongst other things the removal of physical access to premises, the withdrawal of networking accounts and the removal of any company related equipment.

c) Confidentiality Agreements

All staff sign a confidentiality agreement upon commencement of employment with Ikiru People.

d) Ongoing Training & Meetings

Regular meetings occur across all departments including development, project management, cloud delivery and deployment, network and security, support and account management to ensure compliance and on-going training.

e) Support

On occasions where our support teams might need access to front end client systems, this is typically undertaken via specialised tool which does not expose the logon credentials to the end user. Hence the support team never have sight of these credentials.

f) Risk Assessment

There is a formal risk register which all departments provide input into which is reviewed at board level as well as at management level. It is a permanent item on the board agenda.

References

[1] https://azure.microsoft.com/en-gb/regions/

[2] https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/transport-security-overview

[3] https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/transport-security-with-certificate- authentication

[4] https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-azure- sql

[5] https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing

[6] https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection

[7] https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

[8] https://docs.microsoft.com/en-us/azure/sql-database/sql-database-automated-backups

[9] https://docs.microsoft.com/en-us/azure/sql-database/sql-database-business-continuity#sql-database-features-that- you-can-use-to-provide-business-continuity