Portfolio of Work: Design and Build Document

Note: Contents have been deleted. This is not a full version of the document.

Prepared for

TechT NZ

Date: December 2024

_____

Prepared by

Zero-Trust Interface

Author: Jean-Philippe LO SIOU

Version: 1.0

CONTENTS

Table Contents 4
Figure Contents 7
Document Control 10
Stakeholders & Audience 10
Introduction 12
Executive Summary 12
Key analysis 12
Company Background 13
Business Analysis 14
Current State – Discovery 14
Network Infrastructure 14
Existing Server Environment 15
Existing End User and Other Devices 15
Stakeholder Feedback – Analysis 16
Identified Requirements 20
Moscow Analysis 22
Project Requirements 24
Problem/Solution Overview 24
Technical Solutions Pratical 28
Identity and Access 28
1. Microsoft Tenant 28
2. Microsoft Entra ID / Licenses 31
3. Implementing Identity Synchronization : Microsoft Entra Connect Sync 38
4. Manage Secure User Access 42
6.1. Identity Access Management (IAM) 42
6.2. Azure Role Based Access Control (RBAC) 45
6.3. Multi-Factor Authentication (MFA) Policy (Azure | Microsoft 365) 47
6.4 Conditional Access Policy (Azure | Microsoft 365) 50
6.5 Privileged Identity Management (PIM) Administrator Approval (Microsoft 365) 53
6.6 Identity Secure Score and Manage Identity Security Posture 54
6.7 User Risk Policy 54

6.8 Smart Lockout 55
Scalabilities Challenges ..... **Error! Bookmark not defined.**
1. Azure Public & Private DNS ..... **Error! Bookmark not defined.**
2. Azure Regions & Azure Availabilities zone ..... **Error! Bookmark not defined.**
3. Azure Private Virtual Network & Azure Private Network Local Peering ..... **Error! Bookmark not defined.**
4. Azure Resources group ..... **Error! Bookmark not defined.**
4.1. Web Application ..... **Error! Bookmark not defined.**
4.1.1. Azure Storage Account ..... **Error! Bookmark not defined.**
4.1.2. Azure Service APP Plan & Azure Web Apps ..... **Error! Bookmark not defined.**
4.1.3. Azure Web App Service ..... **Error! Bookmark not defined.**
4.2. Database ..... **Error! Bookmark not defined.**
4.2.1 Microsoft Azure SQL Database ..... **Error! Bookmark not defined.**
5.3. Microsoft Exchange to Microsoft 365 ..... **Error! Bookmark not defined.**
5.3.1. Microsoft Outlook Online ..... **Error! Bookmark not defined.**
Security Vulnerabilities ..... **Error! Bookmark not defined.**
1. Network Security Group & Application Security Groups ..... **Error! Bookmark not defined.**
2. Azure Firewall ..... **Error! Bookmark not defined.**
3. Azure Resources Lock ..... **Error! Bookmark not defined.**
4. Azure Key Vault ..... **Error! Bookmark not defined.**
5. Microsoft Sentinel ..... **Error! Bookmark not defined.**
6. Microsoft Defender for Office 365 ..... **Error! Bookmark not defined.**
7. Microsoft Defender for Cloud ..... **Error! Bookmark not defined.**
Device and Application Management ..... **Error! Bookmark not defined.**
1. Microsoft Intune ..... **Error! Bookmark not defined.**
2. Microsoft Autopilot ..... **Error! Bookmark not defined.**
Data Governance and Compliance ..... **Error! Bookmark not defined.**
1. Microsoft Intune ..... **Error! Bookmark not defined.**
2. Microsoft Purview ..... **Error! Bookmark not defined.**
3. Microsoft Teams ..... **Error! Bookmark not defined.**
Collaboration and Productivity Tools ..... **Error! Bookmark not defined.**
1. Microsoft Teams ..... **Error! Bookmark not defined.**
2. Microsoft SharePoint ..... **Error! Bookmark not defined.**
3. Microsoft OneDrive for Business ..... **Error! Bookmark not defined.**

Value Added-Proposition(s) ..... **Error! Bookmark not defined.**

1. A.I Products and Services ..... **Error! Bookmark not defined.**

1.1 Microsoft Copilot ..... **Error! Bookmark not defined.**

2. Business Continuity and Disaster Recovery ..... **Error! Bookmark not defined.**

2.1. Microsoft Azure SQL Database ..... **Error! Bookmark not defined.**

2.2. Azure Backup and Recovery Vault ..... **Error! Bookmark not defined.**

3. Monitoring ..... **Error! Bookmark not defined.**

3.1. Azure Monitor Log ..... **Error! Bookmark not defined.**

3.2. Azure Alert monitor Action and Group ..... **Error! Bookmark not defined.**

Conclusion 56

Project Outcomes 56

Recommendations 56

Reference List 57

Appendix 57

Microsoft 365 Licenses 57

Execution Phase 3 : Migrate Applications to fix scalabilities issues (SupportDesk and XYZ Payroll Manager) to Azure Service Plan 58

TABLE CONTENTS

Table 1 Current State | Network Infrastructure 15

Table 2 Current State | Server Environment 15

Table 3 Current State | End User And Other Devices 16

Table 4 MoSCoW Analysis 23

Table 5 Microsoft Tenant | Example 30

Table 6 Entra ID - Users and Groups | Example 33

Table 7 Microsoft Entra - Licenses | Example 35

Table 8 Microsoft 365 - Licenses | Example 36

Table 9 Microsoft 365 - Roles Assignment | Example 37

Table 10 Implementing Identity synchronization | Example 42

Table 11 Resource Group - IAM | Example 43

Table 12 Azure Management Groups | Example 44

Table 13 Azure Role Based Administration Control | Example 46

Table 14 MFA policy | Example 49

Table 15 *Condition Access Policy | Example* 52

Table 16 Privileged Identity Management (PIM) Administrator Approval | Example.... **Error! Bookmark not defined.**

Table 17 Monitor Identity Secure Score and Manage Identity Security Posture| Example .....**Error! Bookmark not defined.**

Table 18 User Risk Policy ..... **Error! Bookmark not defined.**

Table 19 User Risk Policy ..... **Error! Bookmark not defined.**

Table 20 Azure DNS for External Name Resolution (Public DNS) | Example ..... **Error! Bookmark not defined.**

Table 21 Azure DNS for Internal Name Resolution (Private DNS) | Example ..... **Error! Bookmark not defined.**

Table 22 Azure Public IP Addresses | Configuring | Example..... **Error! Bookmark not defined.**

Table 23 Azure Regions & Azure Availabilities Zones | Example..... **Error! Bookmark not defined.**

Table 24 Private Virtual Network and Azure Private Network Local Peering | Example **Error! Bookmark not defined.**

Table 25 Resources Group | Example..... **Error! Bookmark not defined.**

Table 26 Azure Storage account | Example..... **Error! Bookmark not defined.**

Table 27 Azure Service Plan | Example ..... **Error! Bookmark not defined.**

Table 28 Azure Web App | Example ..... **Error! Bookmark not defined.**

Table 29 AutoScalling feature | Example ..... **Error! Bookmark not defined.**

Table 30 *Microsoft Azure SQL Database | Example* ..... **Error! Bookmark not defined.**

Table 31 Microsoft Outlook Web | Example ..... **Error! Bookmark not defined.**

Table 32 Network Security Group and Application Security Group | Example ..... **Error! Bookmark not defined.**

Table 33 Firewall | Example ..... **Error! Bookmark not defined.**

Table 34 Azure Resource Lock ..... **Error! Bookmark not defined.**

Table 35 Azure Key Vault | Example..... **Error! Bookmark not defined.**

Table 36 Microsoft Sentinel | Example ..... **Error! Bookmark not defined.**

Table 37 Microsoft Defender | Example ..... **Error! Bookmark not defined.**

Table 38 Microsoft Defender for Cloud | Example..... **Error! Bookmark not defined.**

Table 39 Microsoft Intune | Enrollment | Example ..... **Error! Bookmark not defined.**

Table 40 Microsoft Intune | Configuration Profile for End-User device | Example ..... **Error! Bookmark not defined.**

Table 41 Microsoft Intune | Configuration Profile for handheld device | Example ..... **Error! Bookmark not defined.**

Table 42 Microsoft Intune | Monitor Device and User Activity | Example ..... **Error! Bookmark not defined.**

Table 43 Microsoft Intune | Security Endpoint | Example..... **Error! Bookmark not defined.**

Table 44 Microsoft Autopilot | Deploy Windows | Example ..... **Error! Bookmark not defined.**

Table 45 Microsoft Intune | Compliance Policy | Example ..... **Error! Bookmark not defined.**

Table 46 Microsoft Intune | Security Endpoint | Disk Encryption | Example ..... **Error! Bookmark not defined.**

Table 47 Microsoft Purview – Data Governance and Compliance | Example ..... **Error! Bookmark not defined.**

Table 48 Microsoft Purview | Teams | Retention Policy | Lifecycle Management and Governance| Example ... **Error! Bookmark not defined.**

Table 49 Microsoft Teams | Teams Management tools | Example ..... **Error! Bookmark not defined.**

Table 50 Microsoft SharePoint | Example ..... **Error! Bookmark not defined.**

Table 51 Microsoft Copilot | Example ..... **Error! Bookmark not defined.**

Table 52 Azure Backup | Example ..... **Error! Bookmark not defined.**

Table 53 Recovery | Example ..... **Error! Bookmark not defined.**

Table 54 Monitor Log | Example ..... **Error! Bookmark not defined.**

Table 55 Tag on a Storage Account to monitor | Example ..... **Error! Bookmark not defined.**

Table 56 Alert Monitor Action and Group | Example ..... **Error! Bookmark not defined.**

FIGURE CONTENTS

Figure 1 Initializing a Microsoft Tenant | Example of a new Microsoft Tenant created 28

Figure 2 Initializing a Microsoft Tenant | Example of setting up an Organization Profile 28

Figure 3 Initializing a Microsoft Tenant | Example of Changing Tenant Name and Technical Contact 29

Figure 4 Initializing a Microsoft Tenant | Example of reviewing the country and data location the tenant is located 29

Figure 5 Initializing a Microsoft Tenant | *P*rivacy info like Global privacy contact and Privacy statement URL can be added 30

Figure 6 Microsoft Entra Admin Center - Licenses 34

Figure 7 Microsoft Entra Admin Center – Licensed Users 34

Figure 8 Microsoft Entra Connect Sync - Configuration Synchronization 38

Figure 9 Microsoft Entra Connect Sync - Complete Synchronization 38

Figure 10 Microsoft Entra ID - All Users has been synced with the value "Yes" for the attribute "on-premises sync enabled " 39

Figure 11 Microsoft Entra ID - All Groups has been synced with the value of "Windows Server AD" for the attribute "source" 39

Figure 12 Resource Group | Role Assign to ServiceDesk Group 43

Figure 13 Resource Group | Role Assignment IAM 43

Figure 14 Example of Management Groups created 44

Figure 15 RBAC Assignment 45

Figure 16 RBAC – View Assignment – Management Group 45

Figure 17 New Support Request possible 46

Figure 18 Multifactor Authentication | Configure 47

Figure 19 Multifactor Authentication | Configure| On 47

Figure 20 Multifactor Authentication Registration Policy | Enforce Enabled 48

Figure 21 Multifactor Authentication Validation with a user sign-in 48

Figure 22 Multifactor Authentication Validation with a user sign-in | Phone Complete 49

Figure 23 Conditional Access Policy | MFA for all Microsoft 365 Users | 1 50

Figure 24 Conditional Access Policy | MFA for all Microsoft 365 Users | 2 50

Figure 25 Conditional Access Policy | MFA for all Microsoft 365 Users| Test Sign-in 51

Figure 26 Conditional Access Policy | MFA for all Microsoft 365 Users| Test Sign-in Success 51

Figure 27 Conditional Access Policy | MFA for all Microsoft 365 Users| Test Sign-in | Access Word 52

Figure 28 Azure Resource Group | Different Regions ..... **Error! Bookmark not defined.**

Figure 29 Azure Regions & Availabilities zones | VM Zone 1 ..... **Error! Bookmark not defined.**
Figure 30 Azure Regions & Availabilities zones | VM Zone 2 ..... **Error! Bookmark not defined.**
Figure 31 Azure Private Virtual Network | Peering ..... **Error! Bookmark not defined.**
Figure 32 Azure Private Virtual Network | Global Peering - Local Peering..... **Error! Bookmark not defined.**
Figure 33 Azure Private Virtual Network| Global Peering..... **Error! Bookmark not defined.**
Figure 34 Creation of Web Apps..... **Error! Bookmark not defined.**
Figure 35 Overview Web Apps ..... **Error! Bookmark not defined.**
Figure 36 Azure Web App | Homepage from url..... **Error! Bookmark not defined.**
Figure 37 Azure Web App | AutoScale settings | Rules ..... **Error! Bookmark not defined.**
Figure 38 Azure Web App | AutoScale settings| Instance ..... **Error! Bookmark not defined.**
Figure 39 Azure Web App | Instance Count Updated ..... **Error! Bookmark not defined.**
Figure 40 Microsoft SQL Database Overview ..... **Error! Bookmark not defined.**
Figure 41 Microsoft Outlook Web | Mailbox ..... **Error! Bookmark not defined.**
Figure 42 Azure Key vault created..... **Error! Bookmark not defined.**
Figure 43 Microsoft Defender – Threats Policies - Safe Attachment Policy ..... **Error! Bookmark not defined.**
Figure 44 Microsoft Defender – Threat Policies - Safe Links Policy..... **Error! Bookmark not defined.**
Figure 45 Microsoft Defender -Threat Policies - Blocking Urls..... **Error! Bookmark not defined.**
Figure 46 Microsoft Defender - Safe Links - Validation ..... **Error! Bookmark not defined.**
Figure 47 Microsoft Defender - Blocking Urls - Validation ..... **Error! Bookmark not defined.**
Figure 48 Microsoft Defender - Alert Policy - Mailbox Permission Change..... **Error! Bookmark not defined.**
Figure 49 Microsoft Defender - Alert Policy - Mailbox Permission Change - Triggered . **Error! Bookmark not defined.**
Figure 50 Microsoft Defender – Alert Policy - SharePoint Permission Alert ..... **Error! Bookmark not defined.**
Figure 51 SharePoint Permission Alert – Triggered..... **Error! Bookmark not defined.**
Figure 52 SharePoint Permission Alert – Email Notification - Validation ..... **Error! Bookmark not defined.**
Figure 53 Microsoft Defender – Alerts - SharePoint Permission – Validation..... **Error! Bookmark not defined.**
Figure 54 Microsoft Defender – Simulation - Drive by URL Attack – Configuration..... **Error! Bookmark not defined.**
Figure 55 Microsoft Defender – Simulation – Drive by URL Attack – Triggered 1..... **Error! Bookmark not defined.**
Figure 56 Microsoft Defender – Simulation – Drive by URL Attack – Validation..... **Error! Bookmark not defined.**
Figure 57 Microsoft Defender – Simulation – Drive by URL Attack – Validation 2..... **Error! Bookmark not defined.**
Figure 58 Microsoft Defender – Simulation – Drive by URL Attack – Report ..... **Error! Bookmark not defined.**
Figure 59 Microsoft Defender – Simulation - A Spear Phishing Attack - Configuration . **Error! Bookmark not defined.**
Figure 60 Microsoft Defender – Simulation - A Spear Phishing Attack – Scheduled..... **Error! Bookmark not defined.**
Figure 61 Microsoft Defender – Simulation – Spear Phishing Attack – Validation 1..... **Error! Bookmark not defined.**

Figure 62 Microsoft Defender – Simulation – Spear Phishing Attack – Validation 2..... **Error! Bookmark not defined.**

Figure 63 Microsoft Defender – Simulation – Spear Phishing Attack – Validation 3..... **Error! Bookmark not defined.**

Figure 64 Microsoft Defender – Simulation – Spear Phishing Attack – Validation 4..... **Error! Bookmark not defined.**

Figure 65 Microsoft Defender – Simulation – Spear Phishing Attack –Report..... **Error! Bookmark not defined.**

Figure 66 Microsoft Intune | Compliance Policy ..... **Error! Bookmark not defined.**

Figure 67 Microsoft Intune | Compliance Policy | Settings | No Compliance..... **Error! Bookmark not defined.**

Figure 68 Microsoft Purview | DLP Policy ..... **Error! Bookmark not defined.**

Figure 69 Microsoft Purview | DLP Policy 2..... **Error! Bookmark not defined.**

Figure 70 Microsoft Pureview | DLP Apply Where ..... **Error! Bookmark not defined.**

Figure 71 Microsoft Purview | DLP Policy recognized an IP Address ..... **Error! Bookmark not defined.**

Figure 72 Microsoft Purview | DLP Policy recognized an IP Address | Notification..... **Error! Bookmark not defined.**

Figure 73 Microsoft Purview | DLP Policy recognized 2 IP Address ..... **Error! Bookmark not defined.**

Figure 74 Microsoft Purview | DLP Policy recognized 2 IP Address| Send Blocked ..... **Error! Bookmark not defined.**

Figure 75 Microsoft Purview | DLP Policy recognized 2 IP Address| Business Justification Override **Error! Bookmark not defined.**

Figure 76 Microsoft Purview | DLP Policy recognized 2 IP Address| Business Justification Override Confirmation ..... **Error! Bookmark not defined.**

Figure 77 Microsoft Purview | Sensitivity labels Where applying..... **Error! Bookmark not defined.**

Figure 78 Microsoft Teams | Groups Expiration Policy ..... **Error! Bookmark not defined.**

Figure 79 Microsoft Teams | Group Naming Policy..... **Error! Bookmark not defined.**

Figure 80 Microsoft Team | Naming policies Applied to a Team ..... **Error! Bookmark not defined.**

Figure 81 Microsoft teams | Manage Teams ..... **Error! Bookmark not defined.**

Figure 82 Microsoft teams | Teams Policies ..... **Error! Bookmark not defined.**

Figure 83 Microsoft Teams | Add members to the Public Teams created..... **Error! Bookmark not defined.**

Figure 84 Microsoft Teams | Teams Members ..... **Error! Bookmark not defined.**

Figure 85 Microsoft Teams | Private Team Created..... **Error! Bookmark not defined.**

Figure 86 Microsoft Teams | Webinars Published ..... **Error! Bookmark not defined.**

Figure 87 Microsoft Teams | Webinars | HomePage..... **Error! Bookmark not defined.**

Figure 88 Microsoft Teams | Request Apps for Approval ..... **Error! Bookmark not defined.**

Figure 89 Microsoft Teams | Collaboration through Planner ..... **Error! Bookmark not defined.**

Figure 90 Microsoft Teams | Messaging ..... **Error! Bookmark not defined.**

Figure 91 Microsoft Teams | Tabs | Files to quickly have access..... **Error! Bookmark not defined.**

Figure 92 Microsoft SharePoint | Share Documents..... **Error! Bookmark not defined.**

Figure 93 Microsoft OneDrive | Sharing Links ..... **Error! Bookmark not defined.**

Figure 94 Microsoft Copilot | Use Case ..... **Error! Bookmark not defined.**

Figure 95 Premium and Business Critical Microsoft Azure SQL Database (WilliamDAssafMSFT, 2024) ..... **Error! Bookmark not defined.**

Figure 96 Microsoft SQL Server | Backups ..... **Error! Bookmark not defined.**

Figure 97 Microsoft 365, Office 365, Enterprise Mobility + Security, and Windows 11 subscription (Microsoft, 2024) ..... **Error! Bookmark not defined.**

Figure 98 Migrate Applications to fix scalabilities issues (SupportDesk and XYZ Payroll Manager) to Azure Service Plan ..... **Error! Bookmark not defined.**

DOCUMENT CONTROL

Date	Author	Ver	Comments
01/11/2024	Jean-Philippe LO SIOU	0.1	First Drafts of Design and Build
11/11/2024	Jean-Philippe LO SIOU	0.2	First Release
12/11/2024	Jean-Philippe LO SIOU	0.3	Various Minor Updates (Formatting)
14/11/2024	Jean-Philippe LO SIOU	0.4	Various Minor Updates with added Detail Design
02/12/2024	Jean-Philippe LO SIOU	1.0	Final Release

STAKEHOLDERS & AUDIENCE

The Audience for this document is:

- Operation Manager
- CIO
- IT Teams:
  - IT Team Lead
  - IT Director
  - Solution Architects
  - SME
- Stakeholders
- Other interested parties

List of Stakeholders involved:

Name	Title	Project Role	Detail
Jean-Philippe Lo Siou	Project Lead	Project Lead	Ownership of Project Delivery
Mike Spencer	C.E.O		Steering and Oversight
Joseph Jeong	IT Coordinator	Project Coordinator	
Abigail Mars	Network Administrator	Project Team Member	
Leah Bucknell	Business Analyst	Steering Committee	

INTRODUCTION

EXECUTIVE SUMMARY

This Design and Build Document (DBD) with any appendices and attachments to it outlines the business analysis, project requirements, and technical design and build of the solutions for the Delta Cloud project, the terms of which are incorporated herein by reference, by and between TechT New Zealand (“TTNZ”) (“Customer”, “you”, “your”) and Zero-Trust Interface (“ZTI”, “us”, “we”, “our), and sets forth the services to be performed by us related to Delta Cloud Deployment (“project”).

This DBD represents the complete baseline for services and acceptance applicable to this project. It outlines the framework for migrating TTNZ’s on-premises infrastructure to a Cloud environment (Microsoft Azure and Microsoft 365)

The objective of this project is to propose a comprehensive example of the design and the implementation of our Delta Cloud Deployment strategy as listed with the solutions in the Statement of Work. The necessary configurations to ensure a complete transition to the solution aim to address issues regarding the business requirement.

KEY ANALYSIS

TTNZ is a medium sized business with approximately 500 end users and workstations. Their head office is based in Auckland with approximately 250 end-user devices (100 Workstations, 150 laptops) and they have a Wellington Branch with approximately 120 end-user devices (50 Workstations, 70 laptops) and a Christchurch branch with approximately 50 end-user devices (20 Workstations, 30 laptops)

TechT NZ is a retail and wholesale group within NZ” All things Tech”. They are supplying several retailers.

COMPANY BACKGROUND

ZTI was founded in 2005 helping New Zealand businesses to get the support, technology and expertise they need to tackle the digital transformation.

Our area of expertise are:

- Defining a clear Technology Strategy
- Manage Cyber security Risk
- Implement Disaster Recovery Plan
- Control their tech project costs
- Help on the IT Support
- Meet the Modern Workplace
- Transform your environment into the Cloud

Our expertise is Cloud Management, we successfully completed a migration over on-premises to the cloud for the "Cinema NZ". Our team is trained with different cloud provider, project management and implementation of a good Disaster Recovery solution to ensure we meet the highest technical and regulatory standards.

Our testimonials from our clients: https://www.zero-trust-int.co.nz/testimonials

BUSINESS ANALYSIS

CURRENT STATE – DISCOVERY

The on-premises infrastructure is provided as follows:

NETWORK INFRASTRUCTURE

Office Location	WAN Connection Type - Fibre Link Speed	Routers/Firewall	Managed Switches	Unmanaged Switches	Wi-Fi 6 - Access Points	Cabling	Network(s)	Comments
Auckland	SD WAN 2x 5gbps Connection High Availability - Failover Enabled	2x FortiGates HA Active-Active	8x 48 Port Switches - 4x VLANs (Stacked on Main Office Floors)	16x 24 Port Switches	16x Total - Across Floors	CAT6a	172.16.0.0/19 10.0.0.0/20	VLANs & DHCP Config; Servers, Wired, Wireless APs & Critical Workloads
Wellington	WAN Connection 1x 5gbps Connection	1x FortiGate	4x 48 Port Switches - 3x VLANs	10x 24 Port Switches	10x Total - Across Floors	CAT6a	172.15.0.0/19	VLANs & DHCP Config; Servers, Wired, Wireless

Christchurch	Starlink WAN Connection 1x 5gbps Connection	1x FortiGate	2x 48 Port Switches - 3x VLANs	6x 24 Port Switches	6x Total - Across Floors	CAT6a	172.14.0.0/19	VLANs & DHCP Config; Servers, Wired, Wireless

Table 1 Current State | Network Infrastructure

- They use Fortinet Devices on their networking infrastructure
- The above inventory is available but some of them are not used because on floor configuration and number of employees.

EXISTING SERVER ENVIRONMENT

Office Location	Domain Controllers	SQL Servers	Exchange Servers	SharePoint Servers	WDS Servers	File Servers	IIS Servers	Backup Servers	Monitoring and Logging Servers	Total
Auckland	2x	4x	1x	1x	1x	2x	2x	2x	2x	17
Wellington	2x	1x	1x	1x	1x	1x	1x	1x	1x	10
Christchurch	2x	1x	1x	0x	1x	1x	0x	1x	1x	8
Total	**6**	**6**	**3**	**2**	**3**	**4**	**3**	**4**	**4**	**35**

Table 2 Current State | Server Environment

EXISTING END USER AND OTHER DEVICES

Office Location	Desktop Workstations	Staff Laptops	Total Est End-User Devices	Smartphones Android	Smartphone IOS	Total Est Handheld devices	Other IoT Devices

Auckland	100x	150x	**250 Est**	150x Est	100x Est	**250 Est**	20x Est
Wellington	50x	70x	**120 Est**	35x Est	25x Est	**60 Est**	10x Est
Christchurch	20x	30x	**50 Est**	25x Est	15x Est	**40 Est**	10x Est
		Total Est	**420 Est**			**350 Est**	

Table 3 Current State | End User And Other Devices

- They provide a $1200 grant to new employees to enable them to purchase a Mobile Device
- Other IoT Devices are: Tablets, Kiosk(s), TVs, Touch Screens, Projectors, Fridges and more.

STAKEHOLDER FEEDBACK – ANALYSIS

#	Question	Answer
Q01	*"Which Apps and licenses are TTNZ currently using ?"*	• *"*TTNZ currently has multiple legacy applications: • XYZ *Payroll Manager* • *Skype for business* • *Office 2013 "* *"Additionally, the legacy services and apps hosted through their on-premises infra"*
Q02	1- *"What does TechTNZ do ? "* 2- *"In which field TechTNZ are specialized ? "* 3- *"What is TechTNZ budget for the project ? "* 4- *"Are they any other requirements from other stakeholder / department ? "*	1-*"*TechT a retail and wholesale Group within New Zealand's "all things Tech" sourcing and supplying for several retailers within the country, under the brand "TechT New Zealand", Additionally they manage much of the "Groups" Tier 1-2 IT Support, in house! *"* 2-"Everything Tech", and In-house/group Tier 1-2 Support, relevant information is above in #1 3- *"*The budget is not defined, the governance team are seeking advice and recommendations for "high-end solutions" to bring the business and output into the modern era, and based on expert advice and recommendation they can be swayed to "approve" the project teams proposed budget*"* *"*I hope this provides some clarity, and direction going forward! *"*

Q03	1-”What kind of local security measures are in place ? ” 2-”What are the demands for legislative compliance ? ” 3-”Which apps are experiencing latency ? ”	”I will enquire with our wider team as more pertinent information if you may require For now, I can tell you that... TechT security related details and objectives to follow coming weeks... We aim to meet... 2- Legislation surrounding Privacy Act 2020 Compliance surrounding handling of Data and Information 3- From my understanding latency has been stable for the most part... There have occasional distributions with some of our legacy on prem file and email services, mostly around unscheduled restarts, updates and server down time”
	1. Are there any concerns moving from onsite to cloud? 2. How does the current infrastructure impact the workload? 3. How would TechT prioritize scalability versus cost-efficiency in cloud solutions? 4. What features in cloud security are most critical to TechT? 5. Does TechT have any concerns with the subscription-based pricing?	1. "that require further analysis and cloud-based solution(s)" 2. ”Several mentions within case study” 3. ”You tell us? determine critical workloads? define peak times? assume aspects to drive your ideas and solutions! ” 4. ”End-to-End protection, Data of any form is CRITICAL” 5. ” Balance cost and benefits, these must be discussed, considered analyzed” ”i.e. Solutions! Please! Collaborate and in combination, the team should be resolving/evolving the current state”
	1. ”Current "Secure access across devices" solution? ” 2. ” How old are the current desktop workstations ? ”	1. ” Secure L2TP VPN for off-site Staff Access to the Domain, Workloads, e.g. Storage Spaces, Distributed Filesystem and more, with Shares, Security and Roles applying somewhat, access controls to groups/users as highlighted in scenario” 2. ”This varies, not more than 4-5 years old, yet some devices for some staff, at each office location are more modern than others”
	What is the average yearly revenue after tax for TechT and what are their current operational expenditure costs?	Please consider the following to help support your costing analysis I. Salaries for all staff = ? II. Utilities for each office, electricity, water, internet = ? III. Office lease = ?

		IV. IT Infrastructure e.g. Hardware, Licensing, Subscriptions and more = ? V. Upkeep and maintenance i.e. of everything = ? VI. Total Monthly OPex = $500,000-700,000 Est VII. On average based on Q1 Q2 Q3 2024 (so far this year) Additionally, I can say that the company consistently has been in profit ranging from 10%-15% annually over the past 6 years
QEXTRA01	What is the network I.P addressing of the on-premises architecture for the database, application and the access?	Address IP Range : 172.16.0.0/19 Auckland – Access: 172.16.20.0 /24 Auckland – Database Access: 172.16.21.0 /24 Auckland – Applications: 172.16.22.0 /24 HA Active-Active : 10.0.0.0/20 Address IP Range : 172.15.0.0/19 Wellington – Access: 172.15.20.0 /24 Wellington – Database Access: 172.15.21.0 /24 Wellington – Applications: 172.15.22.0 /24 Address IP Range : 172.14.0.0/19 Christchurch – Access: 172.14.20.0 /24 Christchurch – Database Access: 172.14.21.0 /24 Christchurch – Applications: 172.14.22.0 /24
QEXTRA02	What would be the application that would need to migrate from low to high priority and their infrastructure they are used?	Applications | Priority | Impact | Servers used

<table>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>Support Desk</td><td>Low</td><td>Low</td><td>SQL Server + IIS Servers</td></tr>
<tr><td>XYR Payroll Manager</td><td>Low</td><td>Low</td><td>SQL Server + IIS Servers</td></tr>
<tr><td>SharePoint</td><td>Medium</td><td>Medium</td><td>SharePoint Servers</td></tr>
<tr><td>File Sharing</td><td>Medium</td><td>Medium</td><td>File Servers</td></tr>
<tr><td>Windows Deployment Services</td><td>Medium</td><td>Medium</td><td>WDS Servers</td></tr>
<tr><td>Microsoft Exchange</td><td>High</td><td>Very High</td><td>Exchange Server</td></tr>
</table>
</td></tr>
<tr><td>QEXTRA03</td><td>What is the current Backup and Restore plan?</td><td>- ”Backup Servers with Veeam Data Backup platform”
- ”Network Area Storage ”
- ”Veeam Backup replication: twice a day of VMs in off-site1 through”
- ”Veeam Backup: backup every day at 10:00PM”
- ”Data Retention is 30 days of backup”</td></tr>
<tr><td>QEXTRA04</td><td>What is the current security policy in all windows workstation?</td><td>”All Windows workstation are built with security policy:
• Users cannot install any software that is already provided
• Users can only connect to the internet via VPN connection through on-premises internet. ”</td></tr>
</table>

IDENTIFIED REQUIREMENTS

"The Operations Manager, and CIO of has raised various issues that affect the current End User environment that require further analysis and need resolution including the following" :

- **« Identity and Access Management »**
    - « Difficulty managing secure access across devices, especially for remote users»
    - « User Groups and Accounts, are provisioned on AD-HOC basis, roles and accounts are cluttered and unorganized»
    - « Need for centralized identity management and access controls is essential»
- **« Scalability Challenges »**
    - « On-prem infrastructure struggles to keep up with growing demands»
    - « Need for scalable, cost-effective cloud-based solutions throughout current state on-prem workloads»
- **« Security Vulnerabilities »**
    - « Local security measures leave gaps in threat detection and response»
    - « Need for advanced protection and cyber defense capabilities»
- **« Device and Application Management »**
    - « Increasing number of devices (desktops, laptops, smartphones) needs centralized management. »
    - « Need for modernized secure device and application management»
- **« Data Governance and Compliance »**
    - «Increasing regulatory demands for security, data privacy, and legislative compliance»
    - «Need for effective solutions to manage sensitive data and ensure compliance more efficiently»
- **« Collaboration and Productivity Tools »**
    - «Inefficiencies in current collaboration between offices»
    - «Need for better integration of software services and streamline day-to-day staff productivity»

- **« Value Added-Proposition(s) »**
    - «Interest in using AI products and Services to automate tasks and improve employee productivity»
    - «Any other proposed adoption or migration of current workloads to enhance and streamline business operations»

«ZTI proposes a migration to certain aspect of the infrastructure from on-premises to the cloud that allowing to increase the productivity, availability, resiliency».

«As per the in-person meeting with TTNZ before starting the project we have received an in-detail list of what the issues are at TTNZ. This list will require ZTI to work for the customer for 2 months. »

MOSCOW ANALYSIS

#	Requirement	Comment/Solutions	MoSCoW
BR1	Identity and Access Management	• For remote users, the managing secure access across devices has been a difficulty. • The users and groups are not stored properly in the Active Directory. • A centralized identity and access management is needed with Azure Active Directory in order to make it standard for controlling the access across devices. • Provision and de-provision users and groups with roles that will reduce manual account creation or on AD-HOC basic and clutter. • Enhanced security with Multi-Factor Authentication (MFA).	**Must-Have**
BR2	Scalability Challengers	• Implementation to a scalable cost-effective cloud-based solution to handle growing traffic. • Migrate the essential on-prem applications to Azure cloud to scale automatically based on the workload to meet demands. • Azure hybrid solution with using the existing on-prem licenses in order to be cost-effective.	**Must-Have**
BR3	Security Vulnerabilities	• Implementation for an advanced protection, cyber defense capabilities and a centralized monitoring in order to resolve the weak local security in place. • Multi-Factor Authentication in place alongside with Condition Access Policies.	**Must-Have**
BR4	Device and Application Management	• Due to the increase of devices (Desktops, laptops, smartphones), a centralized device management solution is required to secure and manage devices and applications (Microsoft Intune)	**Must-Have**
BR5	Data Governance and Compliance	• Due to the increase of the regulatory compliance for security, data privacy and legislative compliance, it is required to implement a solution to maintain data privacy and meet regulatory compliance with Microsoft PurView and Compliance Manager. • An effective solution to manage sensitive data and ensure efficient compliance with ongoing regulatory. • Conduct a compliance assessment and audits.	**Must-Have**
BR7	Value-Added Propositions	• A Business Continuity and a Disaster Plan recovery need to be in place.	**Must-Have**
BR6	Collaboration and Productivity Tools	• Collaboration between Auckland, Wellington and Christchurch offices is not efficient • A better integration with communication tools to deliver a workflow to increase day-to-day productivity. • In order to improve collaboration: Microsoft Teams, SharePoint and OneDrive can be leveraged to increase collaboration and productivity across the three offices.	**Should-Have**
BR2	Scalability Challenges	• To have a gradual migration, a hybrid-cloud configuration can be implementing in order to slowly migrate applications from on-premises to Azure.	**Should-Have**
BR3	Security Vulnerabilities	• For an enhanced incident management, the implementation of Microsoft Sentinel can be a proactive solution in order to have a threat and responses strategy.	**Should-Have**

BR1	Identity and Access Management	• Report and Analytic on user access pattern to get better understanding how they use and be able to secure more.	**Could-Have**
BR7	Value-Added Proposition	• Automation tasks with AI in order to enhance productivity and reduce manual repetition tasks.	**Could-Have**
BR6	Identity and Access Management	• Additional AI tools in order to improve employee experience. • Help optimize work process across teams with analyzing collaboration pattern by implementing Microsoft Viva Insights.	**Could-Have**
BR8	Upgrades investment on legacy on-prem infrastructure	• Large upgrading on-prem Investment in profit for the cloud solutions.	Won't-Have
BR9	Applications non-compliance with regulatory standard	• Solutions that are not in compliance with regulatory requirements won't be in the migration to the cloud.	Won't-Have

Table 4 MoSCoW Analysis

PROJECT REQUIREMENTS

PROBLEM/SOLUTION OVERVIEW

Business Requirements	**Business Solutions**
Identity and user management *TTNZ user groups and account's (on-premise active directory) are cluttered and unorganized, their users need to be synchronized to the Azure Cloud with their respective permissions.* *The customer has difficulty managing secure access across devices for remote users, a centralized identity management access control is important.*	**Microsoft Entra ID** It is the Active Directory in the cloud. It is the identity and access management service attached to an Azure tenant that contains the user accounts and password. It allows user to have access external resources or on-premises resources. We will be synchronizing TTNZ on-premises Active Directory with Entra ID. **Microsoft Azure tenant** It is an instance of Microsoft Entra ID service and represent a single organization. It provides a sole place to manage users, groups and their permissions to access resources. We will be using "TechTNZCloud.co.nz" as TTNZ unique name. In one single instance, a tenant can hold one or more subscriptions. **Microsoft Azure Subscription** It is an agreement with Microsoft and our customer to have access to Azure services. Each subscription relies on one and single Azure Tenant to authorize and authenticate users. We will use for each department in order to put resources into logical container. **Azure Identity Access Management (IAM)** It is a service in Azure that allow user and permissions management. We will setup permissions to secure the access of azure cloud. **Microsoft Entra Cloud Sync** It is a directory provisioning that involves a synchronization with on-premises Active Directory to the Microsoft Entra ID. We will be installing the provisioning agent to customer's Domain Controllers (Auckland, Wellington, Christchurch)
Scalability Challenges *TTNZ on-premises' architecture cannot keep up with the growing demands because it required scalable*	

cloud solutions at a considered cost to accommodate the IT workloads. **Increase stability, reliability, and support** *TTNZ on-premises architecture required resilient capabilities because they have 3 remote sites where employees work remotely.*	
Security Vulnerabilities *TTNZ need to enhanced security and monitoring their on-premises and cloud architecture.* *Customer's local security measure are weak and have some gaps in threat detection and response.* *It is the first barrier to protect security environment to TTNZ's azure cloud with a real-time response threat capability.*	

Device and Application Management *Due to increase number of devices TTNZ need a centralize management device solution allowing to secure modern device and manage application*	
Data Governance and Compliance *Regulatory demand for security, data privacy and legislative compliance that TTNZ need to address to. They need effective solutions for managing sensitive data and ensure that they are compliant.*	
Collaboration and Productivity Tools *TTNZ wants to improve the collaboration between offices due to its poor efficacity with a better software services integrations that will allow to streamline staff productivity daily*	

Value Added-Proposition(s)	
Automation with AI *TTNZ is interested to leverage automation with AI products and service in order to improve employee productivity.*	
Improve business continuity, backup and disaster recovery *TTNZ key is to be 100% to accompany retailer New Zealand business in order to achieve it, they need a good Disaster Recovery Solution*	
Optimise costings	

TECHNICAL SOLUTIONS PRATICAL

IDENTITY AND ACCESS

1. MICROSOFT TENANT

Initializing a Microsoft Tenant | Example

We would initialize a Microsoft tenant as below

Figure 1 Initializing a Microsoft Tenant | Example of a new Microsoft Tenant created

Figure 2 Initializing a Microsoft Tenant | Example of setting up an Organization Profile

Figure 3 Initializing a Microsoft Tenant | Example of Changing Tenant Name and Technical Contact

Figure 4 Initializing a Microsoft Tenant | Example of reviewing the country and data location the tenant is located

Figure 5 Initializing a Microsoft Tenant | *Privacy info like Global privacy contact and Privacy statement URL can be added*

Table 5 Microsoft Tenant | Example

2. MICROSOFT ENTRA ID / LICENSES

Entra ID – Users and Groups

Entra ID

- ***Bulk import of users***
- ***Create Manually new user***
- ***Create Manually new group***

- ***Bulk import of users***

- ***Create Manually new user***

- ***Create Manually new group***

Table 6 Entra ID - Users and Groups | Example

Microsoft Entra - Licenses | Example

Licenses can be located in Microsoft Entra Admin Center
Licensed user can be listed

Figure 6 Microsoft Entra Admin Center - Licenses

Figure 7 Microsoft Entra Admin Center – Licensed Users

License Assignment to a User

Table 7 Microsoft Entra - Licenses | Example

Microsoft 365 - Licenses | Example

Licenses can be found In Microsoft 365 Admin Center.
Subscriptions/License are listed as below can be assigned on users or Groups as shown below

Table 8 Microsoft 365 - Licenses | Example

Microsoft 365 - Roles Assignment | Example

User has been assigned administrator roles

Table 9 Microsoft 365 - Roles Assignment | Example

3. IMPLEMENTING IDENTITY SYNCHRONIZATION : MICROSOFT ENTRA CONNECT SYNC

Implementing Identity synchronization | Example

We would install Microsoft Entra Connect Sync on-premise Windows Server and initiate synchronization with some created user and group accounts in the on-premise Windows Server Active Directory in order to test the synchronization on-premises.

- ***After configuration is done, the synchronization process would start***

Figure 8 Microsoft Entra Connect Sync - Configuration Synchronization

Figure 9 Microsoft Entra Connect Sync - Complete Synchronization

- ***After completion of the sync, the Users and Group Accounts created on-premise Windows Server Active Directory have been synced with Microsoft Entra ID :***

Figure 10 Microsoft Entra ID - All Users has been synced with the value "Yes" for the attribute "on-premises sync enabled "

Figure 11 Microsoft Entra ID - All Groups has been synced with the value of "Windows Server AD" for the attribute "source"

Settings
About
Device specifications
Device name jeanphilippels
Processor 11th Gen Intel(R) Core(TM) i7-1180
2.30 GHz
Installed RA
Device ID
Product ID
C:\windows\system32\c...
(c) Microsoft Corporation. All
s reserved.
C:\Users\WpcmD2>whoami
jeanphilippels\wpcmd2
C:\Users\WpcmD2>
jeanphilippelsDC01 on JEANPHILIPPELS - Virtual Machine Connection
File Action Media View Help
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
jeanphilippe.local
Builtin
CloudUsers
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Type
Schema Admins
Security Group - Universal
Sales
Security Group - Global
Marketing
Key Admins
jpls3
jpls2
jpls1
Guest
Marketing Properties
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
Cai Chu
jeanphilippe.local/CloudUsers
jplscloud1
jeanphilippe.local/CloudUsers
jplscloud2
jeanphilippe.local/CloudUsers
Shannon Booth
jeanphilippe.local/CloudUsers
Active Directory Domain Services
Do you want to remove the selected member(s) from the group?
Yes
No
Add...
Remove
OK
Cancel
Apply

- ***Force a manual synchronization with Powershell :***

- ***Validate the Results of Directory Synchronization:***

Table 10 Implementing Identity synchronization | Example

4. MANAGE SECURE USER ACCESS

6.1. IDENTITY ACCESS MANAGEMENT (IAM)

Resource Group – IAM | Example
Role assignment to a Resource Group

Figure 12 Resource Group | Role Assign to ServiceDesk Group

Figure 13 Resource Group | Role Assignment IAM

Table 11 Resource Group - IAM | Example

Azure Management Groups | Example

Example of two Management groups created

Management group sit at the top of the Azure hierarchy (Root Management Group) and provide a way to manage access, policies, and compliance across multiple Azure subscriptions.

Figure 14 Example of Management Groups created

Table 12 Azure Management Groups | Example

6.2. AZURE ROLE BASED ACCESS CONTROL (RBAC)

Azure Role Based Administration Control | Example

We showing an example of a custom Role-Based Access control (RBAC) role to a user to create support requests.
In order to do that, we created an Entra ID user and assigned the RBAC role to user and we checked if the user can perform the task.

Figure 15 RBAC Assignment

Figure 16 RBAC – View Assignment – Management Group

Figure 17 New Support Request possible

Table 13 Azure Role Based Administration Control | Example

6.3. MULTI-FACTOR AUTHENTICATION (MFA) POLICY (AZURE | MICROSOFT 365)

MFA Policy | Example

- **Azure Multi-Factor Authentication options**
- **Ensure by sign-in with a user**

- **Azure Multi-Factor Authentication options**

Figure 18 Multifactor Authentication | Configure

Figure 19 Multifactor Authentication | Configure| On

Figure 20 Multifactor Authentication Registration Policy | Enforce Enabled

- **Ensure by sign-in with a user**

Figure 21 Multifactor Authentication Validation with a user sign-in

Figure 22 Multifactor Authentication Validation with a user sign-in | Phone Complete

Table 14 MFA policy | Example

6.4 CONDITIONAL ACCESS POLICY (AZURE | MICROSOFT 365)

Condition Access Policy | Example

A conditional policy has been created to implement MFA to some users in order to access Microsoft 365 apps

Figure 23 Conditional Access Policy | MFA for all Microsoft 365 Users | 1

Figure 24 Conditional Access Policy | MFA for all Microsoft 365 Users | 2

- ***Test MFA for included user***

Figure 25 Conditional Access Policy | MFA for all Microsoft 365 Users| Test Sign-in

Figure 26 Conditional Access Policy | MFA for all Microsoft 365 Users| Test Sign-in Success

Figure 27 Conditional Access Policy | MFA for all Microsoft 365 Users| Test Sign-in | Access Word

Table 15 ***Condition Access Policy | Example***

6.5 PRIVILEGED IDENTITY MANAGEMENT (PIM) ADMINISTRATOR APPROVAL (MICROSOFT 365)

6.6 IDENTITY SECURE SCORE AND MANAGE IDENTITY SECURITY POSTURE

6.7 USER RISK POLICY

6.8 SMART LOCKOUT

CONCLUSION

PROJECT OUTCOMES

As mentioned throughout the Statement of Work and this design and build document with the technical solutions detail and design. Those components can meet and resolve TTNZ's issues in term of identity and access management by providing a structured and organized identity management, with Azure resources that can scale vertically or horizontally to accommodate the growing demands, by implementing security tools that can monitor and response automatically to threats on end-users' devices , having compliance build-in capabilities allowing to be in compliant with regulation standard. In order to enhance collaboration and productivity, users can use multiple tools at their disposal to focus more on more added-value activities.

RECOMMENDATIONS

We recommend a hybrid-cloud solution by leveraging Microsoft Azure and Microsoft 365 and on-premises in order to have scalabilities and productivity. Training and hiring more resources can be beneficial to manage efficiently this modern workplace infrastructure.

REFERENCE LIST

Referencing APA 7 List

1. *OwenRichards. (2024, January 11). Quickstart: Create a Microsoft Entra tenant - Microsoft identity platform. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-create-new-tenant*
2. *Barclayn. (2024, May 22). What is Microsoft Entra ID? - Microsoft Entra. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/fundamentals/whatis*
3. *Rwike. (2024, May 31). What is identity and access management (IAM)? - Microsoft Entra. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/fundamentals/introduction-identity-access-management*
4. *Barclayn. (2024a, March 22). Add an existing Azure subscription to your tenant - Microsoft Entra. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/fundamentals/how-subscriptions-associated-directory*
5. *Justinha. (2023, October 6). Common deployment scenarios for Microsoft Entra Domain Services - Microsoft Entra ID. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/identity/domain-services/scenarios#azure-ad-ds-for-hybrid-organizations*

APPENDIX

MICROSOFT 365 LICENSES

EXECUTION PHASE 3 : MIGRATE APPLICATIONS TO FIX SCALABILITIES ISSUES (SUPPORTDESK AND XYZ PAYROLL MANAGER) TO AZURE SERVICE PLAN