End-to-End Infrastructure and Endpoint Modernisation

Professional portfolio project summary

Amandio Pereira | UK Professional Standards Organisation | 2024/2025

Prepared as a concise technical narrative of the infrastructure stabilisation, storage and virtualisation improvements, identity and endpoint modernisation, monitoring, automation and operational handover delivered across the environment.

Project objective	Stabilise and modernise core on-premises infrastructure while moving endpoint management towards Entra ID and Intune without breaking access to existing network resources and business applications.
My role	Hands-on senior technical lead combining day-to-day infrastructure and user support with substantial modernisation across Hyper-V, storage, networking, Active Directory/DNS, backup, monitoring, Entra ID, Intune, Autopilot, MFA, Apple/Android integration and automation, alongside documentation and extensive technical training.
Business value	Improved resilience, storage and network performance, recoverability and monitoring while reducing reliance on legacy endpoint management and manual deployment processes.
Core technologies	Windows Server, Hyper-V, Dell PowerVault, iSCSI/MPIO, Veeam, Active Directory/DNS, Entra ID, Intune, Autopilot, Windows Hello for Business, Defender for Endpoint, LibreNMS, PowerShell, Apple Business Manager and Managed Google Play.

1. Executive Summary

As the senior technical lead, I identified the modernisation priorities, secured support for the proposed approach and led its implementation. The work combined improvements to the on-premises infrastructure with a move towards cloud-managed endpoints. Alongside designing and implementing the changes, I supported daily operations and trained the resident IT team to maintain the systems and processes introduced.

On the infrastructure side, I introduced a high-availability Dell storage area network (SAN), with redundant 10 Gbps iSCSI storage connections and Multipath I/O (MPIO) to maintain access if a connection failed. I also increased Hyper-V host capacity and consistency, improved network throughput, refreshed firmware and drivers, resolved live-migration stability issues, consolidated Veeam backup infrastructure and moved the onsite repository away from the previous NAS platform.

In parallel, I developed the path from hybrid domain-joined laptops towards Entra ID-managed devices using Windows Autopilot, Intune, Windows Hello for Business and Cloud Kerberos Trust. Dynamic groups, Company Portal delivery, Windows LAPS through Intune, automated OneDrive sign-in and user-folder backup, MFA migration, Apple Business Manager, macOS Platform SSO and Managed Google Play extended that model across the wider endpoint estate. Operational documentation and staff guidance were produced throughout so that the environment remained supportable after implementation.

2. Starting Point and Modernisation Priorities

The environment contained a mixture of established on-premises systems, ageing configuration and newer cloud-management capabilities. The aim was not to replace everything at once, but to remove avoidable weaknesses, make the existing infrastructure more dependable, and create a controlled transition path for devices and services that could benefit from modern management.

Area	Starting point	Engineering response
Storage and backup	Backup storage depended on an older NAS design with limited connection resilience.	Introduced a Dell PowerVault SAN, redundant 10Gb iSCSI connectivity with MPIO, and moved the onsite Veeam repository to the new storage.
Hyper-V platform	Cluster hardware and firmware had become inconsistent, and live migration showed stability problems.	Standardised RAM and disks, added 10Gb NICs, applied current HPE service packs and firmware, and resolved migration-related connectivity faults.
Directory services	DNS and AD contained stale records, incomplete reverse zones and configuration that no longer matched the live estate.	Cleaned DNS, enabled scavenging, aligned reverse zones and AD Sites and Services, reviewed GPOs and prepared standby Entra ID synchronisation.
Legacy workload	A business-critical database VM remained on an old Hyper-V platform.	Built an isolated test environment, validated the migration path and moved the workload to the supported HA cluster with documented access guidance.
Monitoring	Infrastructure visibility and alerting were fragmented.	Implemented LibreNMS on Ubuntu, added device monitoring, alerting, dependencies and maintenance windows, and documented administration.
Endpoint management	Laptops were primarily hybrid/domain managed and relied on more manual provisioning.	Built an Autopilot/Intune path with Entra ID join, Windows Hello, Company Portal, dynamic groups and Cloud Kerberos Trust for retained on-premises access.

3. Infrastructure, Storage and Hyper-V Stabilisation

The server-room work focused on making better use of available hardware while removing single-path and lifecycle risks. A new Dell PowerVault SAN replaced the previous NAS-based approach for key storage duties. Two 10Gb iSCSI paths were configured through separate controllers and switches, with MPIO providing host-side path resilience. CHAP was also documented as part of the storage authentication model.

Change	Implementation	Operational effect
SAN resilience	Dual 10Gb iSCSI paths through separate SAN controllers and switches, with Windows MPIO.	Continued storage access if one path, controller or associated switch path failed.
Hyper-V host consistency	RAM and disk configuration aligned across the cluster; additional 10Gb NICs installed.	Reduced configuration drift and improved host capability for clustered workloads.
Network capacity	Increased aggregate Ethernet link capacity per Hyper-V host to 12 Gbps.	More headroom for VM and host traffic than the previous layout.
Firmware lifecycle	HPE service-pack and firmware maintenance process established and documented.	Replaced older driver/firmware levels and provided a repeatable update method.

4. Reliability, Backup and Recovery Improvements

Hyper-V stability and legacy workload migration

Cluster issues were treated as engineering problems rather than isolated alerts. Firmware and driver consistency was brought up to date across the HPE Gen10 hosts, and Event Viewer evidence was used to work through faults affecting network continuity during live migration. The resulting maintenance approach was documented so future driver and firmware updates could be carried out consistently.

A separate migration addressed a business-critical legacy database VM. I built a fully segregated test environment to establish whether the workload could run correctly on the newer Hyper-V platform, used the findings to improve the migration documentation, then moved the production VM onto the supported high-availability cluster. This reduced dependence on the older host while preserving a tested, repeatable method for the team.

Veeam consolidation and storage

Backup infrastructure was simplified by consolidating Veeam onto a dedicated physical server and moving the onsite repository from the previous Synology platform to the new Dell SAN. The Veeam platform was upgraded, backup jobs were recreated on the newer configuration, and legacy backup sets, stale data and orphaned configuration records were removed.

I involved the IT team as each server backup was reintroduced, including assigning repository quotas, so they gained hands-on experience of the configuration rather than relying only on written guidance. The wider recovery design also included offsite cloud backup for local server workloads and Microsoft 365 data. Recovery procedures were documented alongside the practical training.

Area	Before / risk	Result
Onsite repository	Older NAS-backed repository with weaker path resilience.	Repository moved to Dell SAN with redundant iSCSI/MPIO connectivity.
Backup server	Backup roles distributed across older arrangements.	Veeam functions consolidated onto a dedicated physical server.
Configuration hygiene	Historic/orphaned backup entries consumed attention and space.	Obsolete configuration and old backup data cleaned up.
Operational continuity	Knowledge depended heavily on individuals.	Backup/recovery procedures documented and transferred to the IT team.

5. Directory Services and Hybrid Identity Hygiene

The on-premises AD and DNS environment contained stale and incomplete configuration that was worth addressing as part of the wider infrastructure modernisation. Stale DNS records were removed, scavenging was introduced, missing reverse lookup zones were added, and AD Sites and Services subnets were aligned with the live network.

Redundant Group Policy settings and stale device objects were also reviewed and removed or disabled. I involved a senior member of the IT team directly in the DNS cleanup and scavenging implementation work, providing that colleague with hands-on experience of the configuration so DNS could be maintained more effectively after my contract ended.

A secondary Entra ID synchronisation server was configured in staging mode and kept aligned with the primary configuration, ready for manual activation should the primary sync fail. This reduces recovery time by avoiding the need to rebuild the synchronisation service from scratch during an outage.

In parallel, server OUs containing domain controllers and other on-premises server workloads were excluded from Entra ID synchronisation where there was no requirement for those computer objects in the cloud environment. These systems remained under on-premises Active Directory and Group Policy management, keeping the boundary between on-premises server administration and cloud-managed endpoints deliberate rather than accidental.

6. Endpoint Cloud Transition and User Experience

Key staff worked mostly or fully from home, while laptops for the overseas branch were best purchased locally. I designed the Entra ID, Autopilot and Intune solution so that these devices could be prepared remotely. Once a laptop's hardware hash was registered and the required assignments were in place, it could enrol into company management and receive the settings and applications its user needed. Cloud Kerberos Trust enabled Windows Hello for Business authentication to the on-premises resources that staff still used, while access continued to require network connectivity to those resources and the domain controllers.

1. Register device	2. Autopilot enrolment	3. Entra ID + Intune	4. Windows Hello	5. Apps + on-prem access
Hardware identity prepared for corporate ownership.	Device provisions through the cloud rather than traditional imaging.	Policies, security settings and dynamic assignments apply automatically.	Passwordless sign-in configured with MFA-backed registration.	Company Portal/self-service delivery with Cloud Kerberos Trust retaining access to on-premises resources.

Key implementation areas

Capability	What changed	Why it mattered
Autopilot and Intune	Created the cloud onboarding path and coordinated staged migration from hybrid devices.	Enabled remote-friendly provisioning and reduced dependence on traditional imaging.
Windows build standardisation	Adapted and deployed an Intune PowerShell debloat script to remove unwanted Windows and OEM applications while retaining approved business and support tools.	Produced cleaner, more consistent Windows builds and reduced manual post-provisioning cleanup.
Windows Hello for Business	Configured passwordless sign-in for Autopilot-managed PCs.	Improved sign-in experience while keeping device-bound credentials.
Cloud Kerberos Trust	Configured Windows Hello for Business authentication from cloud-managed devices to on-premises resources.	Allowed modern endpoint management without immediately abandoning existing network services.
Dynamic groups	Automated user/device assignment to applications, policies and conditional access.	Reduced manual group maintenance and made targeting more scalable.
Company Portal / Win32 apps	Moved suitable applications towards managed Win32 and self-service delivery.	Reduced routine installation effort and enabled dependencies/supersedence.
Windows LAPS / OneDrive / MDE	Configured Windows LAPS password rotation through Intune, automatic OneDrive sign-in and backup of Desktop, Documents and Pictures, alongside endpoint-security lifecycle guidance.	Removed manual OneDrive setup, protected key user files automatically and improved local-admin credential security and endpoint supportability.
MFA transition	Coordinated migration from Cisco Duo to Microsoft Authenticator in staged phases.	Moved authentication onto the Microsoft identity stack while giving users clear preparation and support guidance.

7. Cross-Platform Management and Automation

Apple and Android management

The cloud-management model was extended beyond Windows. Apple Business Manager was connected to Intune to support corporate ownership and enrolment, macOS Platform SSO was implemented for work-account sign-in, and the certificate/token relationships needed to keep Apple MDM and application delivery operational were documented for annual renewal and support.

Managed Google Play was also integrated with Intune, allowing Android applications to be approved, synchronised and assigned through the management platform. Corporate-owned fully managed Android enrolment was documented using token/QR-based provisioning.

Platform	Management integration	Operational outcome
Windows	Entra ID, Intune, Autopilot, Windows Hello, Defender for Endpoint.	Cloud-based provisioning, policy and application delivery with retained access to required on-premises resources.
Apple	Apple Business Manager, Intune enrolment, Platform SSO, Apple MDM certificate and VPP token lifecycle.	Corporate ownership and managed onboarding for macOS/iOS with documented renewal dependencies.
Android	Managed Google Play and corporate-owned fully managed enrolment.	Corporate ownership, managed application catalogue and repeatable device provisioning through Intune.

PowerShell and self-service deployment

Operational automation supported the wider transition. PowerShell was used to improve device onboarding and to package difficult application workflows for Intune. I developed an Intune-deployed PowerShell solution to remove obsolete mandatory desktop shortcuts and replace them with a current set, reducing manual cleanup and keeping managed devices consistent.

I automated the installation of the FollowMe virtual printer and a critical legacy desktop client through Company Portal. The desktop client was the last application that still required manual installation by IT. Completing its automation meant that all required work applications could be deployed automatically or installed through self-service.

The legacy client was one of my final projects during the contract and extended my PowerShell work beyond routine scripting. Its deployment required a coordinated installation and removal process that continued after reboot, applied settings to user profiles and surfaced prompts from a SYSTEM deployment in the signed-in user's desktop session. Separate case studies explain the client and printer solutions in detail.

8. Monitoring, Documentation and Knowledge Transfer

LibreNMS was implemented as an Ubuntu VM on the Hyper-V platform to provide a single monitoring view across relevant infrastructure. Devices were added using SNMP where practical and ICMP where that was the appropriate fallback. Dependencies reduced redundant alerts when a host failure affected child VMs, while email alerting, threshold rules and maintenance windows improved operational use.

The monitoring platform itself was documented for validation, updates, device onboarding, alerting, health checks and maintenance. Similar handover material was produced for HPE service-pack updates, SAN/iSCSI configuration, Apple/Intune certificate dependencies, device enrolment, MFA changes and other operational tasks. This made troubleshooting and routine administration less dependent on undocumented knowledge.

Alongside the written handover material, I provided extensive practical training to the resident IT team across the systems and processes introduced or changed during the contract. This included infrastructure monitoring, Hyper-V and storage administration, backup and recovery, endpoint management, device enrolment and other day-to-day operational procedures, with the aim of leaving the team able to support the environment independently.

9. Outcome and Value Delivered

Taken together, the work left the environment with a stronger infrastructure base and a clearer endpoint-management direction. The on-premises platform became more resilient and supportable, while cloud onboarding and policy management were introduced without forcing an abrupt break from the network services and applications that still depended on the local domain.

Outcome	Delivered change	Practical value
Storage resilience	Dell SAN with redundant 10Gb iSCSI paths and MPIO.	Improved performance and path resilience for backup/storage workloads.
Virtualisation stability	Hyper-V host hardware aligned; drivers/firmware refreshed; live-migration issues resolved.	More predictable clustered operation and a repeatable maintenance process.
Recovery posture	Veeam consolidated, repository moved, legacy DB VM migrated to HA platform.	Reduced dependence on older systems and strengthened backup/recovery operations.
Operational visibility	LibreNMS deployed with alerting, dependencies and maintenance controls.	Faster awareness of infrastructure health and fewer avoidable alert cascades.
Modern endpoint management	Autopilot, Intune, Entra ID, Windows Hello, dynamic groups and Cloud Kerberos Trust.	Remote-friendly onboarding and automated policy/app delivery while retaining necessary on-premises access.
Cross-platform support	Apple Business Manager, Platform SSO and Managed Google Play integrated with Intune.	Extended corporate device-management practices beyond Windows.

Engineering approach

Understand → Think end-to-end → Control risk → Modernise carefully → Keep it maintainable → Leave it supportable

- Investigated the live environment before changing it, separating stale configuration from genuine dependencies.
- Worked across hardware, networking, Windows infrastructure and cloud endpoint management as one connected environment rather than as separate technical areas.
- Used isolated testing and staged migration where legacy workloads or hybrid dependencies created risk.
- Implemented Entra ID-joined device management alongside the existing hybrid estate, sequencing changes carefully to preserve established access, policies and user workflows.
- Favoured maintainable solutions and existing capabilities where they met the requirement, rather than adding complexity for its own sake.
- Produced practical documentation and explained changes clearly to IT colleagues and end users, helping the team support the environment independently.

End of case study