**M365 and Azure Enterprise Cloud expert**

**Adrian’s experience - When I have carried out a global deployment of Intune**

During my experience with a global deployment of Microsoft Intune, I led the initiative to implement comprehensive device management across multiple regions. I was responsible for configuring policies, deploying security measures, and ensuring seamless integration with other Microsoft services like Azure AD. My role involved coordinating with international teams to ensure smooth rollout and compliance with local regulatory requirements. I also provided training and ongoing support to ensure users could effectively manage their devices, improving the organization's overall security posture and mobile device management capabilities.

**Adrian’s involvement with app packing**

In my involvement with application packaging through Microsoft Intune, I worked on streamlining the deployment of applications across a global network of devices. This involved creating and customising app packages that could be distributed via Intune’s endpoint management solution. I ensured that the applications were properly configured for deployment, with considerations for device compatibility, security policies, and corporate compliance standards. I was also responsible for troubleshooting packaging issues and ensuring seamless integration with Intune’s app deployment features, facilitating efficient software distribution across various platforms and ensuring consistency in user experiences globally.

**Adrian’s experience with device enrolment and management in Intune**

In my experience with device enrolment and management using Microsoft Intune, I was responsible for overseeing the seamless integration of a diverse range of devices into the enterprise ecosystem. This included automating the enrolment process for Windows, iOS, and Android devices through bulk enrolment methods such as Autopilot and Apple Business Manager. I implemented policies for compliance, security, and conditional access, ensuring that each device met corporate governance standards. Additionally, I managed device lifecycles by enforcing security updates, remotely monitoring devices, and providing troubleshooting support to resolve issues promptly. This ensured a secure and efficient device management environment across the organisation.

**My experience building validating an Autopilot deployment**

In my experience building and validating an Autopilot deployment, I was responsible for configuring and streamlining the Windows Autopilot process to enable zero-touch provisioning of devices. I set up and customised deployment profiles to automate the setup and configuration of new devices, ensuring that they met organisational requirements for security, compliance, and user experience. Throughout the deployment, I performed extensive testing and validation to ensure that devices enrolled smoothly, policies were correctly applied, and users could sign in and start working without manual intervention. My role also involved troubleshooting any deployment issues and refining configurations to optimise performance and efficiency, ultimately improving the overall device provisioning process.

**Adrian’s experience with device patching and updates**

In my experience with device patching and updates, I was responsible for implementing and managing update policies across a wide range of devices using tools like Microsoft Intune and Windows Update for Business. I ensured that critical security patches, feature updates, and firmware upgrades were deployed systematically to minimise vulnerabilities and maintain device performance. I configured automated update schedules and used compliance policies to enforce timely patching, while also managing exceptions for devices requiring extended testing or manual intervention. My role involved closely monitoring update statuses, troubleshooting failed deployments, and coordinating with IT teams to ensure minimal disruption to users during patch rollouts. This approach helped enhance the security and reliability of the organisation's device fleet.

**Adrian’s experience converting GPO to Intune Policies**

In my experience converting Group Policy Objects (GPO) to Intune policies, I managed the migration of traditional on-premises configurations to cloud-based modern management. I assessed existing GPO settings to identify those that could be replicated within Microsoft Intune’s policy framework, ensuring that security, compliance, and configuration settings were maintained. This involved mapping GPOs to equivalent configuration profiles in Intune, such as device restrictions, security baselines, and compliance policies. I also handled testing to ensure that Intune-based policies were applied correctly across diverse device types. By automating and streamlining these processes, I successfully transitioned the organization to a cloud-first approach, reducing dependency on legacy infrastructure and enhancing flexibility for remote device management.

**Adrian’s additional skills or experience M365 Administrator and Azure**

**1. Advanced M365 Administration**:

Microsoft 365 Security & Compliance: Experience configuring and managing advanced security features like Microsoft Defender, Conditional Access, Data Loss Prevention (DLP), and multi-factor authentication (MFA) to safeguard data and identities.

Microsoft Exchange Online: Proficiency in managing mailboxes, configuring hybrid environments, and implementing Exchange Online Protection (EOP) to ensure seamless email communication and security.

SharePoint Online & OneDrive: Expertise in administering SharePoint Online and OneDrive for Business, managing site collections, permissions, and collaboration features for effective document management.

PowerShell Automation: Advanced PowerShell scripting for automating administrative tasks, such as bulk user provisioning, configuration changes, and reporting within M365 and Azure environments.

**2. Azure Administration:**

Azure Active Directory (AAD): Deep understanding of managing identities, users, groups, and access controls within Azure AD. Experience configuring role-based access control (RBAC) and managing enterprise-wide identity services.

Azure Monitor & Security Centre: Knowledge of setting up monitoring and alerting through Azure Monitor and using Azure Security Center for proactive security management and compliance tracking.

Virtual Machines & Networking: Proficiency in deploying, configuring, and managing Azure virtual machines, along with setting up Azure networking services like virtual networks, firewalls, and VPNs.

Azure Cost Management & Governance: Experience in optimizing Azure spend and implementing governance policies through Azure Blueprints and cost management tools, ensuring resource efficiency and budget compliance.

**3. Cloud Migration & Hybrid Environments:**

Extensive experience leading or contributing to cloud migrations, including email migrations (e.g., Exchange to Exchange Online), SharePoint migrations, and moving on-premises services to Azure.

Proficiency in managing hybrid environments, ensuring seamless integration between on-premises systems and cloud platforms, particularly using Azure AD Connect and hybrid configurations for Exchange and SharePoint.

**Why am I currently looking for a new opportunity**

I'm looking for a role that offers new challenges and opportunities for professional development, particularly in advanced areas of Microsoft 365 and Azure, where I can further develop my skills and leadership abilities. I'm seeking a position where I can make a more significant contribution to strategic decisions and help shape the direction of IT infrastructure, particularly in cloud-based solutions. I'm looking for a role that aligns more closely with your passion for modern cloud technologies like M365 and Azure, providing opportunities to focus on cutting-edge solutions.