

# Peter Hinchley

SYSTEMS ENGINEER / SOLUTION ARCHITECT

---



I have over twenty years' experience working as a Systems Engineer and Solution Architect. I have designed and deployed desktop and server standard operating environments for several government departments. I have a deep technical knowledge of the Windows operating system and infrastructure services and considerable experience working with Azure and other cloud platforms. I have strong application development and packaging skills, and expertise in DevOps, automation, and security. I have also designed and deployed multiple large-scale projects, including a global privilege management service for BHP Billiton.

---

## CONTACT

**NISHI, ENINBURGH AVE,  
CANBERRA, ACT**

PHONE:  
0405 375 610

EMAIL:  
peter@hinchley.net

WEBSITE:  
<https://hinchley.net>

CLEARANCE:  
NV1 (Secret)

## EDUCATION

**BACHELOR OF COMPUTER  
ENGINEERING**

First Class Honours  
University of Canberra

**HIGH SCHOOL CERTIFICATE**

Dux of School  
Narrandera

## SKILLS

Desktop and Server Standard  
Operating Environments

Application Packaging

Systems Integration

Identity and Access Management

Programming / Web Development

Cyber Security / Cloud Transition

Solution Architecture

---

## CLOUD TRANSITION / SOLUTION ARCHITECTURE.

Comcare (2017 - Present).

### Overview

I have worked as a solution architect/engineer at Comcare since 2017. I am the lead technical resource responsible for supporting a vast number of essential services across the agency. This includes identity services (Microsoft Active Directory, Microsoft Entra ID, Microsoft Identity Manager, Okta, and greenID), integration platforms (both cloud-based and on-premise), and Microsoft Azure, AWS, and Oracle Cloud environments. I am also responsible for the desktop and server SOEs, including Comcare's remote access solutions (Cloud PC, Azure Virtual Desktop and Citrix). I am responsible for all application development and deployment tool chains (including Azure DevOps, TeamCity, and Octopus). I support our virtualisation platform (VMware), components of our network stack, including the corporate cloud proxy (iboss), and I am instrumental in supporting the Microsoft 365 suite of products (e.g. Power Platform, Teams, Exchange, SharePoint, etc). I have used custom code (often PowerShell) to automate repeatable processes, and developed a web-based administration portal and integration platform that is used by the Service Desk and other teams to perform a significant portion of all first and second level support tasks. I am the most experienced security engineer at Comcare and meet weekly with the IT Security Advisor to discuss approaches for improving Comcare's security posture and Essential Eight compliance. I also provide third level support, and am the technical escalation point, for almost the entirety of Comcare's technology stack. I work not just as an engineer, but also as a solution architect, regularly proposing and then implementing new products and services across the agency. I have an ongoing commitment to Comcare including provision of out of hours support and mentoring of junior staff.

### ***Identity and Access Management***

- Implemented Okta, a cloud-based identity and access management solution, for managing the identities and entitlements of staff and external users. The solution enables user self-service capabilities, multi-factor authentication, delegated administration, and single sign-on across corporate and cloud-based applications. Okta is currently used to mediate access to Microsoft 365 and over 80 additional applications and online services using standards that include OpenID Connect, OAuth 2.0, SAML, and WS-Federation. I personally completed every integration.
- Selected and deployed an identity proofing solution based on greenID (backed by the Home Affairs Document Verification System). The solution is used by public facing Comcare services that require registered users to verify their real-world identity using Government approved identity documents, such as a passport or driver's license.
- Designed and implemented an identity synchronisation and provisioning solution based on Microsoft Identity Manager. The system links Aurion (HR), Active Directory, and the building access system. It is used to provision new starters in Active Directory, automatically suspend and retire the accounts of staff that are on leave, or who have left the agency, and to flow identity and organisational changes between systems.

### ***DevOps and Cloud Services***

- Upgraded and then migrated the on-premise Microsoft TFS solution to Microsoft DevOps. This included migrating existing TFVC source code repositories to Git.
- Established automated build and deployment pipelines for several in-house developed applications. Systems that are hosted on-premise rely on TeamCity for builds, and Octopus for deployments, whilst all other pipelines are hosted in Azure DevOps.
- Provided best practice guidance and implementation support for colleagues seeking to adopt DevOps practices.
- Developed architectural guidance and implementation procedures enabling developers to leverage Docker containers as part of the software development lifecycle.
- With support from Microsoft Consulting Services, and a colleague, I co-developed an infrastructure as code model for managing the deployment and configuration of all resources in Azure. This approach uses a strict source control branching model with mandatory peer reviewed pull-requests. It uses pipelines to enable promotion of resources across landscapes, from development through to production, ensuring the consistent and reliable management of cloud artefacts.
- Implemented a web portal used by the IT Service desk for performing common administration tasks. The portal provides a streamlined graphical interface to a large collection of PowerShell scripts that perform complex backend administrative tasks in a consistent, secure, and repeatable manner. Nearly all first and second-level support tasks are performed via the Portal.
- Proposed, designed, and implemented an automated solution for managing the renewal of TLS certificates using Let's Encrypt. This included writing a PowerShell script for assigning and updating certificates on public-facing NetScaler infrastructure.
- Migrated the ORAMS (Occupational Rehabilitation and Medical Services) application from the DTA (Digital Transformation Authority) to Comcare. This including upgrading and refactoring both the frontend (React) and backend (Python) code and integrating it into Comcare's support toolchains. Also employed DevSecOps practices to perform static code analysis during the build process.
- Published several architectural and corporate standards documents, including an HTTP REST implementation policy, a comprehensive suite of identity and access management principles (covering technologies such as OAuth 2.0 and OpenID Connect), and defined the agency's register of officially supported web browsers.
- Implemented an automated system for retrieving scanned paper records from a third-party scanning service, auto-matching them against existing claim records, and uploading them into Content Manager (TRIM).
- Implemented AWS Simple Email Service (SES) for bulk email delivery.
- Implemented Comcare's SMS gateway (based on Telstra Rapid Alert). It is used for several purposes, including out-of-band incident notification to Comcare staff. The contact details of individuals are automatically maintained using custom code that leverages the product API.
- Implemented a cloud-hosted service monitoring tool (Sematext). The product monitors the availability and performance of both public facing and on-premise services. Multi-step verification workflows are defined using Puppeteer. I was responsible for product selection, solution design, and the implementation of all monitors.

### ***Desktop Standard Operating Environment (SOE)***

- In 2018, I was the sole technical resource on the design, build, and deployment of a Windows 10 SOE (1703 and 1709). The reference image was developed using Microsoft Deployment Toolkit and deployed via Configuration Manager. The project scope included the configuration of DirectAccess, BitLocker, Endpoint Protection, and the deployment of Office 365. Additional tasks included the configuration of group policy, application whitelisting, the design of the ongoing servicing model, and the packaging of over 180 applications.

Following the completion of this work, I developed a long-term strategy for the modernisation of the end-user computing environment. The blueprint outlined a roadmap for migrating from the on-premise device management product suite to a cloud-only toolchain (using technologies such as Okta, Microsoft Autopilot, and Intune).

In 2022, I delivered on this strategy, and migrated the agency to a cloud-enabled version of Windows 11. Devices are built using Autopilot, registered in Azure Entra ID (not domain joined), and entirely managed using cloud technologies including Intune and Defender for Cloud. I personally re-packaged all approved desktop software as part of this work, and implemented an automated process for generating application control policies that govern the use of the packaged software. As part of this work, Always on VPN was deployed to enable remote connectivity to on-premise resources, and user home drives were moved to OneDrive.

- Designed and delivered a remote access solution for Comcare staff based on Microsoft Azure Virtual Desktop (AVD) enabling access to corporate resources from personal devices. The session host servers are based on Windows 11 multi-session edition and are managed via Intune. A separate AVD host pool has also been established (and is currently in pilot) for providing access to Comcare's primary business application (as a replacement for the existing Citrix XenApp solution).
- Implemented desktop MFA (using Okta) for users logging onto the laptop SOE. Currently in pilot.
- Introduced ConnectWise ScreenConnect into the organisation to enable the Service Desk and End User Computing teams to perform remote client support.
- Deployed Microsoft Cloud PC as a remote access solution (laptop replacement) for external consultants and short-term contractors.

### ***Systems Integration and Security***

- Implemented a cloud proxy solution (based on iboss). All traffic from clients (including mobile devices) and servers passes through the cloud proxy. Was responsible for product selection and the solution design and implementation. Also responsible for all third level support and ongoing service enhancement. The solution provides content filtering, TLS inspection, malware defence, zero trust capabilities, and enforces conditional access policies.
- Introduced a new agency wide service for performing PDF conversion (including the conversion of inbound email to PDF/A format for long term retention). Involved market research, product evaluation and selection, solution design, implementation, and handover to support.
- Deployed a custom API proxy into the Comcare DMZ for providing REST-based access to on-premise systems. Also configured Azure API Management for mediating access to cloud-hosted services. This included developing several custom Azure function apps (primarily using Node.js) which are fronted by Azure API Management.
- Established an on-premise log aggregation service using both Windows event-forwarding and NxLog agents to forward key security events to a cloud-based SIEM based on FireEye Helix. Later migrated this capability to Microsoft Sentinel using Azure Monitor Agent.
- Enrolled all on-premise servers into Azure Arc and leveraged Azure Update Manger for the automated deployment of security updates.
- Implemented significant improvements to the security and data quality of the corporate Active Directory environment. This included the identification and removal of obsolete/redundant artefacts such as security groups, service accounts, and group policies. It also included the introduction of technical controls for the use of domain administrator accounts (based on Microsoft authentication silos). As part of this work, the use of multi-factor authentication was enforced for privileged activities performed via designated administration hosts.
- Formulated a role-based access control model for allocating resource privileges to IT support staff.
- Migrated Comcare's primary business application from on-premise Windows infrastructure to Linux hosts running in Oracle Gov Cloud (Comcare was the first customer). Tasks included configuring Linux and Oracle WebLogic Application Server instances and overcoming a range of integration challenges related to coexistence with legacy on-premise technologies.
- Participated in a range of tender evaluation panels for services including enterprise architecture, identity and access management, claims payment automation, network refresh, data centre refresh, and API management.

- Deployed and configured Citrix Netscaler appliances within the DMZ and the Comcare internal network. These appliances are used for load balancing web traffic, TLS offload, and for enabling multi-factor authentication for Citrix XenApp users against Comcare's cloud identity platform, Okta.
- Migrated DHCP and DNS services off Active Directory domain controllers running in remote state offices, allowing for the simplification of the environment and the decommission of on-premise hardware.
- Migrated Comcare to the Protective DNS service from the Australian Cyber Security Centre (ACSC).
- Implemented an IP Address Management (IPAM) solution based on Netbox (hosted on Linux in Azure). Migrated to Netbox from Gestio.
- Selected and deployed a cloud-hosted password management solution (Keeper) for storing personal and shared passwords, secrets, and other sensitive data.
- Wrote custom code to automate critical business processes. This included developing multiple add-ons to Microsoft Outlook. One was used to generate a consolidated PDF of emails (including nested attachments), and another was used to perform a bulk upload of emails to Content Manager. Also made extensive use of PowerShell DSC to facilitate the declarative configuration of server infrastructure.
- I am frequently engaged to perform security related activities at Comcare. This includes incident investigation, implementing new security controls, and evaluating the effective security posture of new and existing services. One example of this work involved using my low-level understanding of web technologies to identify several major vulnerabilities in two of Comcare's high profile public facing web sites.

## **SERVER STANDARD OPERATING ENVIRONMENT.**

Department of Border Protection (June 2017).

In this short-term contract, I designed and built a Windows Server 2016 SOE for the End User Computing Program. The reference image was built and deployed via Configuration Manager and the configuration of server roles was facilitated using PowerShell Desired State Configuration (DSC) policies. The pre-staging of servers in Configuration Manager was enabled through a purpose-built web user interface that invoked a custom PowerShell web service.

## **DESKTOP SPECIALIST.**

Department of Foreign Affairs and Trade (Jan 2013 - May 2017).

I was the technical lead on the development of a Windows 10 SOE that was deployed to 10,000 computers in over 100 countries. I also developed the Windows 2012 R2 SOE and a Microsoft SCCM 2012 R2 solution (with approximately 500 site system servers). Other achievements included designing a custom Linux thin-client image with support for both RDP and ICA connectivity. I also led the development of a briefcase solution for providing staff with mobile access to the Department's SECRET network.

## **DIRECTOR DESKTOP AND ACCESS SERVICES.**

Department of Finance (2010 - May 2012).

I was responsible for the strategic direction, implementation, and operational support of the following services: Desktop, Directory Services, Security and Mobility. I led the project to upgrade Active Directory 2003 to 2008 R2 and designed and built the authentication platform used by the Central Budget Management System and Online HR solution for Parliamentarians. I also took a lead role in delivering the Department's remote access solution, web proxy, and printer consolidation projects.

## **DESKTOP SOE / APPLICATIONS PACKAGING.**

Department of Finance (2008 - 2010).

I was the lead engineer responsible for delivering a Microsoft Windows Vista SOE for the Department of Finance. Key tasks included: configuring Microsoft MDT 2008 and SCCM 2007, packaging over 160 applications, defining group policy, and establishing a test framework to validate the implementation. After the deployment, I was responsible for third level support of the platform, and the delivery of ongoing performance and security improvements.

## **JOINT OPERATIONS PORTAL.**

CSC (2007 - 2008).

In the role of Portal Architect, I lead a small team tasked with the design and development of a national Portal for the Department of Defence. The Portal was designed to support the operational planning and execution activities undertaken by all three divisions of the Australian Defence Force. The solution was based on Microsoft Office SharePoint 2007.

## **ENTERPRISE META-DIRECTORY.**

CSC (2007).

Designed, developed, and deployed, an enterprise meta-directory for BHP Billiton that synchronised employee, contractor, and vendor identity data for over 120,000 objects between multiple SAP systems, Active Directory and AD LDS. The solution was built using Microsoft Identity Integration Server.

## **ENTERPRISE WEB ACCESS MANAGEMENT.**

CSC (2002 - 2007).

Designed, developed, and deployed, a global web access management service for BHP Billiton. The system was deployed in five continents and protected web sites hosted across over 80 servers. The solution was the "corporate standard" authentication and authorisation service for all new web applications in the enterprise. The service processed approximately 1 million authentication events each month, supported a range of multi-factor authentication options, and included deep integration into Documentum and Outlook Web Access.

## **SELF-SERVICE PASSWORD RESET.**

CSC (2006).

Designed, developed, and deployed, a global self-service password reset solution for BHP Billiton supporting approximately 60,000 users. The solution was based on CA Identity Manager.

## **EXTERNAL USER DIRECTORY.**

CSC (2005 - 2007).

Was responsible for the design and delivery of an authoritative user repository for managing identities external to the organisation (vendors, suppliers, selected contractors, etc). The user store was replicated across five continents. As part of this work, I developed a custom ASP application enabling delegated management of external users by authorised personnel.

## **DIRECTORY ARCHITECTURE.**

CSC (2004 - 2005).

Prepared an identity management framework for the Department of Immigration that addressed functional requirements including synchronisation, provisioning, password management, access control, single sign-on, and reporting. I also designed a directory service capable of supporting the eBusiness initiatives of the department.

## **WEB HOSTING.**

CSC (2002 - 2003).

Assisted in the design and deployment of a global web hosting service for BHP Billiton. The facility provided a three-tier architecture and was deployed on Solaris hardware. It supported high profile web sites including bhpbilliton.com and bmacoal.com. Key tasks included developing the logical technology model for the internet and intranet hosting zones, configuring all application software, and establishing the code deployment methodology and toolset.

## **ENTERPRISE META-DIRECTORY (SIEMENS).**

CSC (2001 - 2002).

Assisted Siemens in the development and deployment of an enterprise meta-directory that synchronised employee, contractor, and vendor identity data for over 60,000 objects between SAP HR, Windows NT, and Active Directory. The solution was built using Siemens DirX.

## **WEB HOSTING.**

Conde Nast (2000 - 2001).

Implemented significant improvements to the infrastructure hosting Conde Nast (UK) web sites including Vogue, Traveller, Brides, and GQ. This included the introduction of load balancing and clustering technology to remove existing single points of failure.

## **ASNET AND CABNET.**

CSC (1998 - 2000).

Worked my way up to be the lead architect in the design and implementation of the Australian Secure Network (ASNET) which serviced counter terrorist and dignitary protection activities, and CABNET, which enabled the secure electronic dissemination of Cabinet documents produced by Federal Parliament. Both solutions were based on Windows NT and Lotus Domino.

---

### **TECHNOLOGIES**

Microsoft 365 / Azure / Okta

Windows Server / 11 / Linux

Active Directory / Identity Manager

Intune / Configuration Manager

Azure DevOps / TeamCity / Octopus

iboss / NetScalers / Citrix

### **LANGUAGES**

PowerShell

JavaScript / TypeScript / Node.js

C# / VB.NET / VBScript

Python

HTML / CSS

C / C++

---