Document:

ACURL Training Facility

Part:

High Level Design - Version 1.0

Dated:

05/05/2021

Company contact:

Daniel Wakely

daniel.wakely@downerdefence.com.au

Contents

1 Introduction 2

1.1 Scope 2

2 Solution Overview 3

2.1 Design Principles 3

2.2 Solution Requirements 3

2.3 Conceptual Design 4

2.4 Functional Specification 5

2.5 System Specification 5

2.6 Physical Specification 6

2.7 Interface Requirements 6

2.8 Security Architecture 6

2.9 Service Delivery 9

2.10 Users 9

3 Solution 10

3.1 End-user Application Services 10

3.2 End-user Devices 11

3.3 Platform Technical Services 12

3.4 Platform Security Services 16

3.5 Management Services 18

4 Transfer Device 18

5 Solution Sizing 18

6 Solution Deliverables 19

Figures

[Figure 1 - Conceptual Design 4](#_Toc71115976)

[Figure 2 - Functional Specification 5](#_Toc71115977)

[Figure 3 - Cyber Security Framework 7](#_Toc71115978)

[Figure 6 - Directory Services 14](#_Toc71115979)

[Figure 7 - Log Collection 15](#_Toc71115980)

[Figure 8 - Transfer Device 18](#_Toc71115981)

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Status | Description | Author | Reviewer |
| 0.1 | Draft | Initial draft | Bede Matthews, Solutions Architect, Downer | Robert Geraghty, Senior Project Manager, Communications Design and Management  Rick Bell, Senior Architect, Downer  Vishal Ohri, Solutions Architect, Downer |
| 0.2 | Draft | The document is updated to include the feedback. | Vishal Ohri, Solutions Architect, Downer | Robert Geraghty, Senior Project Manager, Communications Design and Management  Rick Bell, Senior Architect, Downer |
| 0.3 | Draft | Updated the document based on the meeting between CDM and Downer on 20/04/2021 to simplify the design by removing the Pre-Production environment, configuration management using Terraform, a non-Nutanix based infrastructure and removing the security zones by implementing a single Active Directory domain design. | Vishal Ohri, Solutions Architect, Downer | Robert Geraghty, Senior Project Manager, Communications Design and Management  Ian Jones, Network Architect, Communications Design & Management |
| 1.0 | Final | The document is updated to include the feedback and some minor changes to the wording in the document. | Vishal Ohri, Solutions Architect, Downer | Robert Geraghty, Senior Project Manager, Communications Design and Management |

# Introduction

In 2020, the Australian Department of Defence, through the Capability Acquisition & Sustainment Group (CASG) engaged Communications Design & Management (CDM) to develop a Project Definition Statement for a new overseas training facility.

This facility is intended to operate at the SECRET classification, with the ability to support up to 30 concurrent users. The facility must be capable of scaling up to support greater needs placed on it, such as an increase in data, greater display resolutions or more users.

The environment is classified and therefore the design must provide a high level of security, while remaining easy for the staff to manage and maintain. It must also deliver a common and consistent training environment for the students who will use it.

This High-Level Design (HLD) forms a part of the overall project documentation and provides sufficient information for CASG to understand what will be delivered, how it meets their needs. The HLD describes the physical and virtual ACURL Training Environment which will operate within the training facility.

## Scope

The scope of this high-level design is to provide a clear understanding of the technical architecture and build standards required to implement the ACURL Training Environment so that:

* The security of the environment is not compromised.
* It provides a common training environment for students.
* It is easy to support and maintain for staff.
* It can scale up to support additional users, more data or higher performance requirements.

### Inclusions

The High-Level Design document includes information on concepts, infrastructure, and software and how they meet the requirements for the Australian government’s SECRET classification.

### Exclusions

The HLD does not include configuration details or support plans. These will be covered in the Integrated Logistic Support (ILS) and Detailed Design.

The HLD does not include physical network or security designs. These will be transparent to the platform design and covered in the relevant detailed designs as well as at a high level in the PDS.

### Dependencies

* Network Design.
* Acceptance by Security Stakeholders.
* Acceptance by CDM.
* Acceptance by CASG.

### Assumptions

1. The following assumptions have been made:

* The environment will be completely stand-alone.
* Due to the disconnected state of the system and the requirement to apply updates and patches, there is a need for an offline data transfer mechanism to the system.
* The storage for the solution is to be designed to meet end-user, platform and development data requirements. It is expected that the application data storage will need to accommodate up to 100TB of information. The storage requirements will need to be expandable as the application data grows and will be detailed in the detailed design documentation after consultation with Defence.
* There is sufficient power and rack space available to host the infrastructure for this solution.
* There is no requirement to archive data, but the logs will be retained for management and security purposes to comply with the ISM controls.
* Software and hardware will be provided as GFX.
* The system is designed as a greenfield system with no requirements for data or application migration.
* The solution must be resilient and where possible, redundancy is provided to maintain business continuity.
* There is no separate Non-Production environment for testing purposes. If required, another instance of an application can be deployed within the production environment for testing purposes. This will require additional compute, storage and licensing.
* A Primary Domain Controller (PDC) Emulator will provide time services for the system, but it will use a reliable and the network core switch as its upstream time source provider. Some non-windows-based devices may also use the network device for their time service.

# Solution Overview

## Design Principles

1. The following principles have been used to prepare this design:

* Simple – The system is easy to implement and maintain whilst complying with the required security controls.
* Secure by Design – The system is designed to comply with the Australian Government controls required to operate at the SECRET classification.
* Separation of Concerns - each service performs its role and no more.
* Scalable- The system is designed and scaled appropriately, according to the functions provided and sized for the growth expected within the system’s life-of-type.
* Controlled Technical Diversity - ICT functions and subsystems should be reusable as much as practicable to simplify the support arrangements.

## Solution Requirements

1. Refer to the ‘Statement of Requirements’.

## Conceptual Design

1. The conceptual design is created to express the concepts of the ACURL Training Environment with stakeholders in a common format. The design builds on the principles of Simple, Secure by Design, Separation of Concerns and Scalable to meet the objectives outlined in the statement of requirements.
2. The design separates the systems based on their logical function into End-user services, Platform Services, and Infrastructure services with dedicated functions for Management and Transfer. A brief description of the services within the solution is:

* **End-user Services**– Provides the applications, devices and technical services required to provide a virtual desktop environment.
* **Platform Services** – Provides the security and support services required to secure and maintain the entire training environment.
* **Infrastructure Services** – Provides the underlying compute, network, and storage for the environment.
* **Management Services** – Provides a jump server and tools required to manage the systems in the environment.
* **Transfer** – Provides the ability to transfer material into the environment on secure media.

1. Figure 1 - Conceptual Design provides a high-level overview of the conceptual design. The following sections will detail the functions, systems, and information flows between each of these services.

Figure - Conceptual Design



## Functional Specification

1. The functional specification for the ACURL training environment has been developed under two main functions; Technology and Security. This specification forms a subset of the overall capability which will include Facilities Services, Support Services, Network Services, and some Security Services.
2. Figure 2 - Functional Specification provides a high-level view of the technology and security functions being provided by the solution.



Figure - Functional Specification

## System Specification

1. Unless otherwise stated, the latest versions of the software will be used within the solution.
2. The following software will be used:

Table : System Specification - Software

| 1. Functionality | 1. Software |
| --- | --- |
| Hypervisor / Virtualisation | 1. VMWare vSphere 7 / ESXi 7.0 |
| Database | 1. Microsoft SQL Server 2019 |
| Desktop Operating System | 1. Windows 10 Enterprise |
| Virtual Desktop Infrastructure (VDI) | 1. VMWare Horizon 8 |
| 1. Server Operating System | 1. Windows Server 2019 |
| 1. Naming | 1. Windows Server 2019 – Domain Name System (DNS) |
| 1. Addressing | 1. Windows Server 2019 – Dynamic Host Configuration Protocol (DHCP) |
| 1. Printing | 1. Windows Server 2019 - Print |
| 1. Windows Licensing | 1. Windows Server 2019 - Key Management Service (KMS) |
| 1. End-user Applications | 1. Microsoft Office 365 suite (Microsoft Word, Excel, and PowerPoint), 2. Microsoft Edge, 3. EWIRDB, 4. Matlab, 5. Jira (requires Tomcat), 6. MDFG, 7. SPECTRE, and 8. Ghosthawk |
| 1. Identity & Access Management | 1. Windows Server 2019 – Active Directory Domain Services (ADDS) |
| 1. Log Collection | 1. Elastic - Elasticsearch, Kibana, Logstash, Beats |
| 1. Vulnerability Scanning | 1. Tenable - Nessus |
| 1. Device Control | 1. Ivanti |
| 1. Antivirus and Application Whitelisting | 1. VMWare Carbon Black |
| 1. Secrets and Key Management | 1. KeePass |

## Physical Specification

1. The following hardware will be used:

Table : Hardware Specification

|  |  |
| --- | --- |
| 1. Function | 1. Hardware |
| Compute | Dell PowerEdge R740 |
| Storage | 1. Dell PowerVault ME4084 |
| 1. Virtual Desktop Device | 1. ClearCube – CD7922/24 Zero Client |
| 1. Printer | 1. Standard Konica MFD |
| 1. Monitors (Users and Instructor) | 1. HD resolution LCD displays |

NOTE: The hardware is provided as GFX. The compute nodes used to host the virtual desktops must contain GPUs to run the Matlab application.

## Interface Requirements

1. The system uses an approved device to download application updates from the Internet or system data from elsewhere. The device contains antivirus software to ensure the downloaded content is scanned for malicious software before it is transferred to the ACURL training environment through an approved USB device or optical media. More information regarding the transfer device can be found under section 4.

## Security Architecture

The Security Architecture is aligned with the common terminology of the National Institute of Standards & Technology (NIST) Cyber Security Framework. The framework outlines five functions; Identify, Protect, Detect, Respond and Recover. This is seen in Figure 3 - Cyber Security Framework.

Each function has several categories which can be further broken down into subcategories and controls. For the high level design, only the top-level categories will be listed.



Figure - Cyber Security Framework

### Identify

1. The ACURL training environment is primarily a virtual desktop environment. Virtual machines used for servers and desktops will be listed within vCenter with the remaining physical devices being listed in Active Directory.
2. Refer to https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
3. The system is designed to maintain services for 30 concurrent users but can be scaled up as required by adding compute and storage nodes, provided that there is sufficient rack space and power available to host these nodes.
4. It contains a number of commercial off-the-shelf (COTS) end-user applications that function based on a client-server application model. The client-side of end-user applications will be installed within a virtual desktop image which provides a common interface platform for users.
5. The environment is stand-alone and is not accessible through any remote network or the internet. Users access the system through zero client devices connected to its local area network (LAN). Administrators can also use the KVM console in the server cabinet.
6. The software selected for the ACURL environment aligns with the current Department of Defence (DoD) Common Operating Environment (COE) to ensure that the existing DoD artefacts can be reused to maintain a consistent approach to support.

### Protect

1. Identity Management for the system is provided by Microsoft Active Directory Domain Services (ADDS). A single Active Directory domain forest is used to provide role-based access to the system. Security roles and responsibilities will be covered in more detail in the detailed design.
2. End-user data is encrypted in transit through secure protocols.
3. The data-at-rest is not encrypted based on the advice from CASG security advisors. This risk is mitigated by the physical security in-depth mechanisms that include using an A-class cabinet to host the physical server and network infrastructure, cleared personnel, network isolation, stand-alone network, locked comms room, restricted building access and Defence base security protocols.
4. The system is not connected to any other network or the Internet. This prevents data leaks from the system. Device controls are implemented to ensure that only authorised devices are connected to the system. Only authorised users with approved and whitelisted storage devices and media are allowed to transfer data to and from the environment.
5. Application whitelisting is used to control the installation and execution of approved applications in the environment.
6. The standard operating environment is scanned for malicious content and configurations before being used.
7. All system changes will be performed by following the IT Service Management (ITSM) policies and procedures to provide governance and assurance to the system.
8. Being a training system, once it is built, it remains largely static. Backups are not performed regularly but on an ad-hoc basis, usually before and after a configuration change. Backups are created on the important information stores such as databases, home drives and application server virtual disks.
9. Data is destroyed in accordance with CASG policy for the appropriate classification.
10. Security incident response and the mechanisms used are outside the scope of the high level design but will be detailed in the Security Incident and Response plan component of the detailed design, which will be provided by Defence.
11. System maintenance is performed as specified in the operations manual. For virtual machines, updates are applied by updating the guest operating system of the gold image.
12. Security logs are collected and stored using Logstash and Elasticsearch. This allows for the indexing, searching, and alerting for both application and security logs within the environment. Administrators can access these logs through the dashboards provided by Kabana, by login into the jump host.
13. The environment is hardened in accordance with the controls required for a system to operate at SECRET classification.
14. The environment will be built and tested in Australia with an initial state which does not include classified software or data. The classified software and data will be installed after the system is delivered to site in the USA.

### Detect

1. The ACURL training environment will collect logs off all devices contained within it, including network, endpoint, hosting, and virtual servers. The logs will be collected centrally within an Elastic stack.
2. Visualisation of the logs will be provided by Kibana with Logstash providing the aggregation of logs. Elasticsearch provides the ability to query the logs and has an interface with Kibana.
3. Building physical security will be provided by the US Air Force.
4. Malicious code will be detected through VMware Carbon Black as well as regular vulnerability scans performed by Tenable Nessus.
5. Regular vulnerability scans are performed by Tenable Nessus to identify vulnerabilities within the system.

### Respond

Security incident response processes are outside the scope of the high level design but will be developed in the Security Incident and Response plan component of the detailed design, which will be provided by Defence. The tools implemented in the environment will allow for effective incident monitoring and response as required.

### Recover

Disaster recovery processes are outside the scope of the high level design but will be covered in the detailed design. The system supports backups of all data and virtual machines to allow for easy platform re-provisioning as required.

## Service Delivery

1. The system will be maintained in accordance with the established IT service management policies and procedures.

## Users

The Statement of Requirement has outlined five types of user:

* Students.
* Instructors.
* Staff.
* Administrators.
* Service Accounts.

Students, instructors and staff are issued with a unique standard (non-privileged) account to log in to their desktop. They have no access to the servers.

Staff are the users who support the environment. Similarly to the students and instructors, they log in to the system as a standard user but when performing privileged actions, they will use their separate ‘Administrator’ account.

Administrators are staff that have a unique account for systems administration purposes. Administrators have permissions to log in to the End-user, Platform and Management services, as well as administering the underlying infrastructure.

Service Accounts are non-person identities that are used to run system services. They do not have access to End-user information or the ability to perform anything other than their specified role.

# Solution

## End-user Application Services

1. The End-user Application Services contains the applications that are accessed by the users. It provides separation between the End-user devices and the data and applications they are accessing. All user types other than administrators are prevented from logging onto the application servers.

### Microsoft End-user Applications

1. The virtual desktop images will include the Microsoft Office suite including Microsoft Word, Excel, and PowerPoint. Microsoft Edge is included with the operating system which can be used to access web-based applications.

### EWIRDB

1. EWIRDB allows users to view source intelligence mission data. Using the statement of requirements, it will be deployed in the following manner:

* EWIRDB Toolkit installed on each workstation.
* EWIRDB Server file share deployed.

### Matlab

1. From the statement of requirements, Matlab will be deployed in the following configuration:

* MATLAB Runtime Components to be installed on each workstation. This will allow compiled MATLAB code to be executed without having to purchase additional licenses.
* MATLAB Compiler to be installed on the Instructor’s workstation to allow MATLAB code to be compiled and distributed to the student workstations.
* MATLAB to be installed on the Instructor’s workstation.

1. Matlab also has a requirement for OpenGL 3.3 with 1GB GPU memory. This will be provided by a virtual GPU (vGPU) assigned to the virtual desktop.

### Jira

1. Jira is a web application written in Java that is deployed to a servlet container. Within the solution Jira will use the following components:

* Windows Server running Tomcat.
* Microsoft SQL Server.
* File Share.
* Single Sign On (SSO) with Active directory.

1. The application server will be run as a single node instance with the ability to scale up or out as required. The application will be run using a dedicated service account and will be configured to use Transport Layer Security (TLS).

### MDFG

1. MDFG allows users to train on a Collateral Classified version of the mission data files. Based on the statement of requirements it will be deployed in the following manner:

* MDFG to be installed on each virtual desktop.
* MDFG SQL database deployed.

### SPECTRE

1. SPECTRE allows users to train on a Collateral Classified version of the mission data files. Based on the statement of requirements it will be deployed in the following manner:

* SPECTRE to be installed on each virtual desktop.
* SPECTRE SQL database deployed.

### Ghosthawk

Based on the statement of requirements, Ghosthawk will be deployed in the following manner:

* Ghosthawk tools installed on each virtual desktop.
* Ghosthawk SQL database deployed.

### Other

1. The statement of requirements has highlighted the need to add other application servers and services to the environment. These requirements are currently unknown, and therefore detail cannot be provided. The solution supports software deployments to the virtual desktops running Windows, Databases running SQL Server and file shares.

## End-user Devices

### Zero Client Devices

1. The solution will utilise ClearCube zero client devices to provide access to virtual desktops. The Zero Client devices have no removable parts and no built-in storage in order to prevent tampering. They support all standard peripherals such as mouse and keyboard as well as dual monitors and smart cards.

### Monitors

1. Students and Staff will be provided with dual monitors for every zero client devices. These monitors will be capable of providing High Definition 1920 x 1080 display.
2. There will be two large UHD displays for presenting content to students. These monitors will be connected to an Audio-Visual (AV) system which will allow mirroring of both of the instructor’s displays, or the primary display of any student terminal and the secondary display of the instructor’s terminal. The displayed resolution will be HD.

### Printer

1. A Multi-function Device (MFD) will be provided as a part of the site set-up to provide printing and scanning functionalities. Scanning through the MFD will be configured to store content to a user’s file share.

## Platform Technical Services

### Storage

1. The system will provide four types of storage:

* End-user file shares.
* Shared storage.
* Application storage.
* VM Storage.

1. The End-user file shares provide a restricted area for students, staff, and administrators to store documents and files for their own consumption. No other user will have access to the share.
2. The shared storage provides a common location for users to share, collaborate and store files that are required by more than one person. The shares can provide a mixture of team-based shares, open shares and read-only shares.
3. The statement of requirements lists a need for file shares to be provided for some applications. This will be in the form of a file share which is mapped to the virtual machine.

The VM storage will be the virtual disks of the machines running in the environment. It will contain the virtual disks required for the machines which will be thin provisioned. Applications requiring a shared drive will be provisioned as required.

The storage for the system is provided by using a single enterprise-grade storage node. A single storage node is cost-effective for a small deployment but at the same time provides resilience by using dual power supplies and RAID disk array. Disk redundancy within the storage node is provided by using storage volumes based on the RAID disk array.

If required, another storage node can be added to the system to increase the storage capacity.

### Compute

1. The compute for the system is provided by two Dell PowerEdge R740 servers each with GPU cards. A single Dell PowerEdge R740 server is sufficient to run the complete workload but an additional server is used to provide resilience to the environment. The GPUs are required to support the operation of Matlab which requires OpenGL 3.3.
2. There will be a ratio of four virtual cores to one physical core. Memory cannot be oversubscribed, and each virtual desktop will receive 1GB GPU memory allocation. Calculations show that all workloads can be run on a single node which allows for a single node to fail.

### Hypervisor

1. The hypervisor will be VMWare ESXi. This provides the functionality required to run a virtual desktop and server environment.

### Database

1. The database will be Microsoft SQL. There are currently four applications in the End-user application services that require the use of databases including JIRA, Ghosthawk, Spectre and MDFG. For the initial deployment, these will be deployed on a single virtual server.
2. A separate virtual database server will be provisioned to provide database services for the platform services applications. This aligns with the design architecture and reduces the technical complexity in the environment.
3. The latest version of SQL Server – being SQL Server 2019 – will be used.
4. As the demand changes on the system, these databases can be moved out to their own database server and enable the high availability features such as ‘Always-on availability groups’. This may result in additional compute, store and license requirements for the system.

### Virtual Desktop Infrastructure

1. The Virtual Desktop Infrastructure will be built on VMware Horizon 8. This aligns with the skills of the support staff as well as integrating with the hypervisor.
2. The zero client devices support PC over IP (PCoIP), so this protocol will be used to stream virtual desktops. PCoIP supports up to four monitors with 2560 x 1600 or three monitors at 3840 x 2160. This allows for a future upgrade of student monitors as well as supporting the UHD presentation screens. Note, however, that the currently selected zero client devices do not support UHD.
3. By default, only approved USB devices like smart card readers, keyboards and mice will be enabled.
4. Multimedia devices like webcams, speakers or microphones are not in scope for this design but could be supported by the platform.
5. For the initial deployment, the solution will support up to 30 desktops with the ability to scale to greater numbers as required.

### Virtual Image

1. Initially, there will be two images; one for the End-user desktops and one for the servers.
2. The virtual desktop image will be an ‘Instance clone’ based on the latest version of Windows 10 (20H2).
3. (refer to <https://techzone.vmware.com/resource/horizon-architecture#components>)
4. The images will be updated on at least a monthly basis or upon the release of critical security patches. They will be hardened in line with the Australian Cyber Security Centre (ACSC) guidance for Operating System Hardening using a combination of group policies, application control, device control and anti-virus.
5. Unused services and default accounts will be disabled or renamed. Users will be prevented from running PowerShell or adding or removing software.
6. Users will be able to support two displays running at a maximum of 2560x1600. If requirements change, the current architecture can support users running two screens at a maximum resolution of UHD.

### Identity & Access

1. Identity will be provided by Microsoft Active Directory Domain Services (ADDS). Access will be provided in the form of role groups that map through to specific permissions in applications or operating system.
2. The design includes two ADDS servers to provide resilience to the system. Certificates can be generated by the Certificate Authority, with Active Directory supporting the FIDO 2 standard.
3. Multi-Factor Authentication should be used by all privileged users as a minimum but the required tools will be identified during the detailed design phase.
4. A high-level view of the relationships for Directory Services is seen in Figure 6 - Directory Services.

This shows that End-users, applications and devices all authenticate against a common Active Directory Domain Services (ADDS) in the environment.



Figure - Directory Services

### Naming and Addressing

1. The ADDS servers will also host the Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHP).
2. All servers and virtual desktops will be joined to the Active Directory Domain, registering their DNS names.
3. Network addresses will be provided primarily by DHCP with virtual desktops and zero clients receiving their IP addresses dynamically. Application servers and Infrastructure will use static IP addresses.
4. DHCP will integrate with DNS to update endpoint address records. The logs of these actions will be kept for auditing purposes.
5. The network design will inform details like Subnets, VLANs and routes.

### Print Service

1. Printing will be provided by a windows server running the Print service. This will provide the print queues for the virtual desktops.

### Licensing

1. Licensing activation for Windows systems and Microsoft Office will be provided through a licensing server.

### Configuration Management

Configuration management will be performed in accordance with the IT service management processes and procedures.

The system will have as-built-as-configured documents along with build guides to ensure the baseline of the system is documented and maintained on an ongoing basis.

### Log Collection

1. Security logs from the application servers, infrastructure and End-user devices will be collected centrally and stored in ElasticSearch. ElasticSearch allows for the indexing of data which can then have search queries run across it.
2. An agent called ‘Filebeat’ will be installed on the servers which will ship the logs to the Logstash instance which will then aggregate and transform the logs before sending them to ElasticSearch.
3. An Event Logging Policy will be developed for the events to be logged, logging facilities to be used, event log retention periods and how event logs will be protected to comply with the ISM controls for a SECRET system.
4. Administrators will be able to access the logs through a web browser that provides the visualisation over the ElasticSearch instance.
5. Figure 7 - Log Collection shows a high-level view of the log collection architecture.



Figure - Log Collection

### Time

1. Time will be synchronised between the virtual infrastructure and the domain controller. The domain controller will sync its time from the core network switch.

### Backup and Recovery

1. Being a training system, once it is built, it remains largely static. Backups are not performed regularly but on an ad-hoc basis, usually before and after a configuration change.
2. Backups are created for the important information stores like databases, home drives and application server virtual disks.
3. Configuration within the as-built-as-configured document and the build guides along with the backups will provide a mechanism to recover the system during a disaster.

## Platform Security Services

1. Security services provide the identification, protection, detection, and recovery services for the solution. Agents are deployed on all servers and desktops to apply the controls.

### Device Control

1. The device control solution will use Ivanti device control. This product is used widely throughout Defence and allows for re-use of configuration from other environments.
2. The product provides the ability to whitelist devices based on a fingerprint. This fingerprint can then be assigned role-based access to allow different features such as read, write, execute. In emergencies, temporary access can be granted to allow users greater access.
3. A small list of approved USB devices will be created to support the peripherals in use in the solution.

### Application Whitelisting

1. Application whitelisting will be provided by VMware Carbon Black. Carbon Black provides a complete endpoint protection platform and is in use across Defence.
2. The application whitelists will include the various client applications installed on the virtual desktops and the management servers. Application whitelisting can be extended to other servers as required.

### Antivirus

1. Antivirus protection will be provided by VMware Carbon Black. Carbon Black provides a complete endpoint protection platform and is in use across Defence.

### Vulnerability Scanning

1. Tenable Nessus will be used within the environment to provide regular vulnerability scans. There will be agents deployed on all application servers, platform services and the transfer device. The virtual images used for the zero clients and the servers will be scanned on each update or once per month.

### Security Incident & Event Management

1. There will not be a complete Security Incident & Event Management (SIEM) solution deployed to the training environment. Security logs will be collected through Logstash and stored in ElasticSearch which can provide transforms, dashboards, and search capability. If there is a requirement to output the logs from the solution to a SIEM, the current design can do this inline or after the fact.

### Secrets and Key Management

1. Built-in privileged accounts, service accounts and keys will be stored in KeePass. KeePass is a free open-source password vault that allows for role-based access to secrets. KeePass will be installed on the management server and restricted to the administrator accounts.

## Management Services

1. Management services provide the interface to monitor, update or move resources. It contains the application servers required to run the services as well as the interface to them.

### Monitoring

1. Infrastructure monitoring will be provided through the VMWare vCentre portal. It is a web graphical interface to see the resource utilisation of the infrastructure and the virtual machines.

### System Management

1. To provide a management space with the tools that are required to administer the system, a virtual jump box running Windows Server will be provisioned. This management server allows for effective separation while also allowing administrators the ability to view and manage resources. The management server will have the required tools to troubleshoot and resolve issues as well as the ability to communicate with the End-user and platform services.
2. Out of band management will be performed through an Intelligent Platform Management Interface (IPMI) port using a rack-mounted KVM.

# Transfer Device

1. To import software updates, files, or additional content into the environment a laptop has been included in the design. This laptop also has the security software of the virtual machines like anti-virus and device controls.
2. The data from this machine can only be transferred via secure and approved removable media. This machine should be treated as a managed but untrusted device and never be connected directly to the Production environment due to its ability to connect to the Internet.
3. A high-level overview of the interactions that the transfer device is seen in Figure 8 - Transfer Device. It shows that a device can be used to download udpates or software from the internet and then the downloaded content can be transferred to approved media after a security scan. This device never connects directly to the system. The approved media can be used in the approved zero client devices for the administrators.



Figure - Transfer Device

# Solution Sizing

1. Refer to the separate ‘ACURL BoM’ document.

# Solution Deliverables

1. The following are the solution deliverables:

* Installation - Platform Technical Services
  + Compute and Storage (Dell PowerEdge R740 Servers and Dell ME4032 Storage Array)
  + Hypervisor (ESXi)
  + Database (SQL Servers)
  + Virtualisation (vSphere)
  + Virtual Gold Images – Desktop and Server
  + Identity & Access Management (ADDS), Naming and Addressing, Time
  + Print Service
  + Licensing (KMS)
  + Log Collection (ElasticSearch)
  + File Server
  + Backup and Recovery
* Installation - Platform Security Services
  + Device Control (Ivanti)
  + Application Whitelisting and Antivirus (Carbon Black)
  + Vulnerability Scanning (Nessus)
  + Secret and Key Management (KeePass)
* Installation - Management Services
  + Jump Host
* Installation - End-user devices
  + Zero Client Devices with monitors
  + Printer
* Installation - End-user Applications
  + Microsoft Office Suite
  + MATLAB
  + Jira
* Installation – Transfer Device
  + Laptop
* Documentation
  + Project Plan
  + Solution Detailed Design
  + As-built-as-configured
  + Build Instructions
  + Operations Manuals
  + System Test Plan and Report
* Project Management
  + Project Plan
  + Project Status Updates
* iRAP Documentation (To Be Provided by Defence)
  + System Overview Document (SOD)
  + System Security Plan (SSP)
  + Security Risk Management Plan (SRMP)
  + Statement of Applicability (SOA)
  + Security Incident and Response Plan (IRP)
  + Event Logging Plan