Australian Government

Department of Education, Employment and Workplace Relations

ICANWK505A Design, build and test a network server

Release: 1

ICANWK505A Design, build and test a network server

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to design, install and test a server in a complex network environment.

Application of the Unit

This unit applies to those employed in network or systems engineering roles, such as network engineers who are required to design and build network servers in a complex computing environment of medium to large organisations.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
Elements describe the essential outcomes of a unit of competency.	*Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.*

Elements and Performance Criteria

1. Plan and design network servers to meet business requirements	1.1 Consult with **client** and key **stakeholders** to identify requirements
	1.2 Assess business problems, opportunities, scope, objectives and budget, confirming details with appropriate person
	1.3 Analyse and document data migration requirements
	1.4 Review requirements to identify **network server specifications**
	1.5 Produce detailed documentation for the design and configuration of the network services, **server applications**, **security** and **redundancy**
	1.6 Prototype design and update documentation as necessary
	1.7 Produce installation checklists as part of the quality assurance process
	1.8 Develop the test plan to ensure that the system meets client requirements, performance standards and quality expectations
	1.9 Obtain client sign-off for the design report
2. Prepare for network server installation	2.1 Prepare for work, according to site-specific safety requirements and enterprise OHS processes and procedures
	2.2 Identify safety hazards and implement risk control measures in consultation with appropriate personnel
	2.3 Consult appropriate personnel to ensure the task is coordinated effectively with others involved at the worksite
	2.4 Back up local data in preparation for installation
3. Build and configure the servers according to design	3.1 Install **network operating system** to design specifications using installation checklists
	3.2 Install additional tools or third-party software applications as required by the design
	3.3 Patch the operating system and applications to ensure maximum security and reliability
	3.4 Configure **network services** and applications
	3.5 Implement security design to prevent unauthorised access to **system**
	3.6 Reconnect and reconfigure connectivity devices
	3.7 Configure **update services** to provide automatic updates for operating system and applications
	3.8 Restore local data to new server

     Innovation and Business Skills Australia

	3.9 Implement backup and recovery methods to enable restoration capability in the event of a disaster
4. Test and reconfigure network servers	4.1 Test server for benchmarking against client specification and requirements according to test plan, and record outcomes
	4.2 Analyse the error report and make changes as required
	4.3 Use troubleshooting tools and techniques to diagnose and correct *server problems*
	4.4 Test required changes or additions
	4.5 Validate changes or additions against specifications
5. Complete and document network design and installation	5.1 Make and document server configuration and operational changes
	5.2 Complete client report and notify of server status
	5.3 Clean up and restore worksite to client's satisfaction
	5.4 Secure sign-off from appropriate person

Innovation and Business Skills Australia

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- communication skills to liaise with internal and external personnel on technical, operational and business-related matters
- literacy skills to:
    - read and interpret enterprise procedures, manuals and specifications
    - interpret technical documentation
    - write reports in required formats
- numeracy skills to:
    - take test measurements
    - interpret results
    - evaluate performance and interoperability of network
- planning and organisational skills to plan, prioritise and monitor own work
- problem-solving and contingency-management skills to:
    - deal with unexpected situations on the basis of safety and specified work outcomes
    - adapt configuration procedures to requirements of network and reconfigure depending on differing operational contingencies, risk situations and environments
- safety awareness skills to:
    - apply precautions and required action to minimise, control or eliminate hazards that may exist during work activities
    - follow enterprise OHS procedures
    - work systematically with required attention to detail without injury to self or others, or damage to goods or equipment
- research skills to interrogate vendor databases and websites to implement different configuration requirements to meet security levels
- technical skills to:
    - identify the technical requirements, constraints and manageability issues for given customer server requirements
    - design a server and associated network services
    - install a server design
    - select and use server and network diagnostics, test application software and hardware to suit different network applications.

Required knowledge

- features of:
    - current network operating systems (NOS)
    - current server applications compatibility issues and resolution procedures
- detailed knowledge of:
    - network service configuration, including:

- domain name system (DNS)
- dynamic host configuration protocol (DHCP)
- file transfer protocol (FTP)
- mail
- network time protocol (NTP)
- proxy
- server messages block (SMB)
- web

- network service management, including start, stop, restart and start on boot
- network service security
- server firewall configuration
- troubleshooting tools and techniques, including network diagnostic utilities
- operating system installation methods, including installation from: CD, DVD, universal serial bus (USB) boot disk, network and script (automated install), deployment services
- user authentication and directory services
- best practice procedures for implementing backup and recovery
- error and event logging and reporting
- documentation skills for networks
- boot process and diagnosing boot failures
- operating system rescue environment
- operating system help and support utilities
- storage options, including file systems and disk partitioning schemes
- performance monitoring tools and tuning options
- compatibility issues and resolution procedures
- high availability options for servers
- file and print management
- process or task management
- task scheduling utilities.

Evidence Guide

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • produce design report for a server (or servers) with complex user and network service requirements • install and configure the server according to the produced design • monitor and test the server • troubleshoot server and network failures • configure a wide range of server network and security services, including DNS, DHCP, web and proxy, mail, FTP and firewall.

Context of and specific resources for assessment	Assessment must ensure access to:
	
	• site where server installation may be conducted
	• relevant server specifications:
	   • cabling
	   • networked (LAN) computers
	   • server diagnostic software
	   • switch
	   • client requirements
	   • wide area network (WAN) service point of presence
	   • workstations
	• relevant regulatory documentation that affects installation activities
	• appropriate learning and assessment support when required.
	
	Where applicable, physical resources should include equipment modified for people with special needs.

Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • evaluation of design report for a server in a complex network environment • direct observation of the candidate installing or updating a server in a complex network environment • verbal or written questioning of required skills and knowledge • evaluation of report that outlines testing procedures, test

	results and recommendation to server changes
	• evaluation of design and implementation of the system in terms of performance and suitability for business needs.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate. Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.

Innovation and Business Skills Australia

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Client may include:	- external organisations - information and communications technology (ICT) company - individuals - internal departments - internal employees - service industry.
Stakeholders may include:	- development team - information technology (IT) manager or representative - project team - sponsor - user.
Requirements may refer to:	- application - business - database - network - people in the organisation - performance - platform - system - technical needs.
Network server may include:	- multiple - physical - virtual.
Specifications may include:	- IP addressing, such as: - IPsec - IPv4 and IPv6 - subnetting - supernetting - DHCP, including: - options - relay agents - exclusions - fixed addresses and address ranges

     Innovation and Business Skills Australia

| | pre-boot eXecution environment (PXE) boot scopes routing, including: default gateway open shortest path first (OSPF) persistent routing routing internet protocol (RIP) static routing authentication services, including: biometrics enterprise single sign-on Hesiod Kerberos lightweight directory access protocol (LDAP) network information system (NIS) Novell Directory Services (NDS) pluggable authentication modules (PAM) public key infrastructure (PKI) and digital certificates public key authentication Red Hat Directory Services security tokens and smart cards SMB or Samba two-factor and multifactor authentication Windows Active Directory Services file services, including: disk partitioning schemes, such as partitions, extended partitions, logical partitions, RAID, logical volumes, swap space disk quotas distributed file systems encrypted file systems files, directories, shares and their permissions file systems, such as NTF-based data.gb (NTFD), file allocation table (FAT), EXT, hierarchical file system (HFS) network file systems (NFS) RAID shadow copy services SMB or Samba print services, including: |

- print drivers
- print queues
- print server
- print spool location
- printer pools
- name resolution services may include detailed DNS configuration, such as:
    - cache-only name server
    - client configuration
    - conditional forwarding
    - DNS record types, such as A, PTR, MX, NS
    - DNS zones
    - dynamic updates
    - external forwarders
    - master and slave name servers
    - replication
    - root hints
    - Time to Live (TTL)
    - WINS and DNS integration
- web and proxy services, including:
    - Apache
    - extranet
    - HTTP or HTTPS
    - internet information server (IIS)
    - intranet
    - internet security and acceleration (ISA) server
    - squid
    - secure socket later (SSL) certificates
    - virtual hosts
    - website security, access control and authentication
- mail services, including:
    - dovecot
    - IMAP or IMAPS
    - mail filtering and virus scanning
    - Microsoft exchange
    - POP3
    - procmail
    - sendmail
    - simple mail transfer protocol (SMTP)
- FTP services, including:

Innovation and Business Skills Australia

<table>
<tr><td></td><td>

- access to home directories
- anonymous FTP
- FTP authentication
- FTP server
- securing FTP
- very secure FTP (VSFTP)

- firewall, including:
  - incoming and outgoing traffic filtering
  - IP tables
  - ISA server
  - kernel level firewalls
  - Microsoft Windows Firewall
  - SmoothWall
  - third-party firewalls
  - traffic filtering by ports and protocols
- remote access, including:
  - dial-up
  - inbound or outbound filters
  - internet connection sharing (ICS)
  - network address translation (NAT)
  - remote authentication dial-in user service (RADIUS)
  - RADIUS proxy
  - remote access policy
  - remote access protocols
  - routing and remote access services (RRAS)
  - secure shell (SSH)
  - terminal services
  - VPN
  - wireless
- hardware
- NOS
- network services
- server applications
- security
- redundancy.

</td></tr>
<tr><td>

Server applications may include:

</td><td>

- database and data warehousing
- directory services
- file sharing
- line of business applications
- management

</td></tr>
</table>

	• messaging • name services • network and remote access • terminal services • web applications • Windows media server • Microsoft SharePoint.
Security may include:	• access control lists • authentication • encryption • file and directory permissions • firewalls • network service security • network share permissions • password security • physical security • SE Linux • security for system resources, such as printers, databases, SharePoint sites, applications and websites • transmission control protocol (TCP) wrappers • Windows group policy.
Redundancy may include:	• dual boot read-only memory (ROMs) • error correcting random access memory (RAM) • failover clustering • multiple fans • multiple power supplies • redundant array of inexpensive or independent disks (RAID) • replication • uninterruptible power supply (UPS).
Network operating system may include:	• Linux OS • Unix OS • Windows Server OS.
Network services may include:	• DHCP • DNS • FTP • firewall • hypertext transfer protocol (HTTP or HTTPS) • internet message access protocol (IMAP) • network file system (NFS) • NTP • post office protocol (POP)

	• print services • proxy • SMB • simple mail transfer protocol (SMTP) • simple network management protocol (SNMP) • structured query language server (SQL) • transmission control protocol or internet protocol (TCP/IP).
System may include:	• application • business • computers • database system • financial system • information system • management system • network • software • website.
Update services may include:	• Potentially Unwanted Program Remover (PUP) • Red Hat Network • Windows Server Update Services • Yellow Dog Update Manager (YUM).
Backup and recovery may include:	• automated backups using operating system backup and job scheduling tools • backup and recovery of mail systems • backup and recovery of network directory service objects • backups using third-party software • database backup and recovery • volume shadow copies.
Server problems may include:	• disk failure • email problems • file system problems • hostname resolution problems • internet connectivity problems • logged system errors • misconfigured networking • security breaches • web server problems.

Unit Sector(s)

Networking