Data Center Technician Foundations 1 Course Description

Overview

Data Center Technician Foundations 1 is an introductory course designed to provide learners with practical knowledge and skills required for entry-level roles in data center operations and infrastructure support. By the end of this course, learners will be able to explain core data center concepts and architectures; understand cloud fundamentals and Oracle Cloud Infrastructure (OCI); apply structured troubleshooting methodologies; demonstrate effective ticketing and communication practices; and recognize key hardware, cabling, and asset management principles used in modern data centers.

Available Curriculum Languages:

- English

Duration

- Recommended total course time: 60 hours*
- Suggested schedule: 20 weeks; 2 sessions/week; 90 minutes/session (≈ 3 instructional hours/week)

*Course time may include instruction, guided practice, labs, simulations, projects, self-study/homework, and assessments.

Target Audiences

Educators

- Technical, vocational, and community college instructors teaching IT infrastructure, networking, cloud computing, or data center operations.
- Secondary and vocational school educators supporting pathways in ICT, networking, or infrastructure careers.

Students

- Students seeking foundational knowledge for entry-level data center technician roles.
- Students interested in cloud computing, infrastructure, or IT operations careers.
- Students with basic logical thinking, problem-solving, and technical curiosity.
- This course is suitable for both technical and non-technical learners beginning their data center journey.

Prerequisites

Suggested

- Basic computer literacy and familiarity with operating systems
- Ability to follow structured procedures and interpret basic technical concepts
- Fundamental understanding of networking concepts is helpful but not required

Suggested Next Courses

- Data Center Technician Foundations 2
- Linux Web Services
- OCI Compute Virtual Machine

Lesson-by-Lesson Topics and Objectives

Module 1: Data Centers & Cloud Foundations

1-1 Data Center Overview & Design Principles:

- Define what a data center is
- Introduce core subsystems (power, cooling, network, physical security)
- Compare data center models (enterprise, colocation, hyperscale, edge)
- Cover when to use traditional infrastructure vs. cloud, plus basics of distributed cloud hosting.

1-2 Redundancy, Cooling, and Uptime:

- Teach redundancy concepts and configurations (N, N+1, 2N, 2(N+1)), availability thinking, and failover patterns (active/active vs. active/passive)
- Introduce cooling fundamentals (CRAC/CRAH, hot-aisle/cold-aisle containment, liquid cooling concepts) and efficiency monitoring (PUE)
- Reinforce access control and handling of data-bearing devices.

1-3 Oracle Data Centers & OCI Architecture:

- Explain OCI's physical/logical layout (Regions, Availability Domains, Fault Domains) and how this supports resilience.
- Cover OCI approaches to redundancy, load balancing/failover, replication/DR, and uptime SLAs, plus data sovereignty and compliance considerations.
- Introduce cloud service models (IaaS/PaaS/SaaS).

Module 2: Troubleshooting & Incident Response Fundamentals

2-1 Troubleshooting Framework and Mindset:

- Provide a structured troubleshooting lifecycle (isolate → diagnose → resolve → document), emphasizing hypothesis testing, elimination, and verification.
- Introduce common network and Linux diagnostic tools (ping/traceroute/nslookup; dmesg, SMART, iostat, netstat, top) and log review fundamentals (e.g., key paths under /var/log).
- Stress documentation quality for audit/compliance and knowledge sharing.

Module 3: Ticketing, Communication, and Operational Quality

3-1 Introduction to Ticketing Systems:

- Understand the purpose and structure of ticketing workflows
- Explore ticketing tools: ServiceNow and Jira
- Recognize the role of ticketing in traceability, accountability, and SLA management

- Follow a ticket through its lifecycle, from creation to closure
- Identify best practices and avoid common pitfalls in ticket management

3-2 ServiceNow/Jira Walkthrough:

- Train on writing and managing tickets end-to-end (create, assign, escalate, close), with attention to required fields (description, priority, category, impact) and workflow differences between tools.
- Practice through sandbox labs and scenario simulations (minor issue, major incident, cross-team coordination).
- Add a communications workshop: professional tone, concise escalations, and effective hand-offs.
- Close with QA metrics (MTTR, backlog, SLA breaches) and using data for continuous improvement.

Module 4: Structured Cabling (Concepts to Implementation)

4-1 Introduction to Structured Cabling Concepts:

- Establish copper vs. fiber positioning, cabling standards (TIA/EIA-568, ISO/IEC 11801, ANSI/TIA-942), and structured cabling hierarchy (MDF/IDF/patch panels).
- Introduce basic network component context (switch/MAC learning, router role) to support cabling rationale.

4-2 Copper Cabling Fundamentals:

- Explore copper cabling in depth: twisted pair rationale, shielding (UTP/STP), crosstalk, and termination standards (T568B), plus correct crimping and common termination errors.
- Teach testing (continuity + performance measures) and documentation of test results.

4-3 Fiber Optic Cabling Fundamentals:

- Analyze the fundamentals of fiber optic cabling
- Explain the differences between single-mode and multi-mode fibers
- Identify key terminology related to fiber optic cabling
- Describe the importance of safety protocols in fiber optic systems

4-4 Cross-Connects and Rack Implementation:

- Apply SOP-driven cabling operations—cross-connect procedures, horizontal vs. vertical cabling, executing MACs during maintenance windows, labeling/traceability, and change management/documentation for compliance.
- Include rack planning concepts (rack diagrams, rack units) and power-to-rack basics (A/B feeds, PDUs).

4-5 Cable Runs and Documentation:

- Reinforce routing best practices (tray/raceway use, bend management, separating power/data), neat cable management, durable labeling systems, and the operational rule to confirm a link is down before disconnecting cables.

Module 5: Hardware Fundamentals, Storage, and Safe Maintenance

5-1 Introduction to Data Center Hardware:

- Survey server form factors (rack/blade/tower/hyperconverged), storage types (SAN/NAS/DAS), and core networking devices (switches/routers) in a data center context.

5-2 Server Architecture Deep Dive:

- Break down core server components and roles (motherboard/CPU/RAM/ECC, power supplies, NICs), plus boot fundamentals (BIOS/UEFI, POST) for troubleshooting.
- Emphasize documentation and inventory practices (serials/FRUs) and typical tooling approaches (DCIM/ITAM examples).

5-3 Storage Concepts and RAID:

- Explain storage arrays/controllers and core RAID levels (0/1/5/10), focusing on trade-offs between redundancy, capacity, and performance, with scenario-based selection and a RAID build/failure/rebuild monitoring exercise concept.

5-4 FRUs and Hot-Swap Practices:

- Teach FRU identification and replacement approaches (hot-swap vs. cold-swap), with pre/post checklists (status lights, CMDB updates, error checks).
- Includes strict production safety guidance (e.g., do not use production rack PDUs to power non-production devices).

5-5 Safety, ESD Handling and Hardware Troubleshooting:

- Establish ESD fundamentals and safe handling (lifting, unpacking, installation), then introduce hardware fault indicators (LEDs, beep codes) and out-of-band diagnostics (IPMI/iDRAC/iLO).
- Also frames maintenance strategy options (PM, predictive, condition-based, reliability-centered) and what "good maintenance" includes for power, cooling, and connectivity domains.

Module 6: Inventory and Asset Management (CMDB)

6-1 Introduction to Asset Management and CMDB:

- Define what an IT "asset" is in a data center context (servers, network devices, racks, cables, etc.) and introduce CMDB fundamentals as a centralized system that stores configuration items and their relationships (not just inventory).
- Cover DCIM at a high level and why accurate inventory matters for operations, lifecycle management, proactive issue detection, and cross-team trust (IT/finance/compliance).
- Operational hygiene / best practices: Regularly update and verify asset records; use automation where possible; define ownership and maintenance responsibilities; integrate asset updates into daily workflows; and schedule periodic data-quality reviews.
- Audit, compliance, and risk: Explain how accurate inventory supports audits and regulatory compliance (examples referenced include SOX, GDPR, ISO) and the operational consequences of inaccurate records (slower troubleshooting, higher downtime, audit risk, higher costs/security exposure).
- Tagging and identification standards: Standardized tagging practices (durable, machine-readable, consistently applied) and asset ID conventions (structured unique IDs, avoid reuse, consistency, documented conventions). Compare barcodes vs. RFID and how tags link back to CMDB records, including handling tag replacements and discrepancy resolution with documented traceability.
- Lifecycle management and secure retirement: Walk through the asset lifecycle (procurement → deployment → maintenance → decommissioning) and its impact on planning/support. Emphasize secure decommissioning practices, including the need for destruction records for "must destroy" (typically data-bearing) parts and careful handling of defective parts for return/reuse.