MODULE 15 · STUDY NOTES

Managing Data Centers

The tools that keep a data center visible and healthy, the change-management discipline behind every modification, and how to retire a data center safely

Running a data center is less about any single machine than about keeping thousands of interdependent components visible, healthy, and changing safely. Data center management monitors and tracks the convergence of a facility's active and passive components to give an administrator a holistic view — which also drives efficient use of energy, equipment, and floor space. This module works through that discipline from three angles. First, the tools: the monitoring and management software that lets a manager see everything from a whole floor to a single outlet on a power distribution unit, and the software-defined data center that virtualizes the entire facility and manages it proactively. Second, change management: because technology and processes never stop evolving, every modification — a cable swap, a patch, an expansion, a merger — must be planned so it happens without downtime, framed by the 7 Rs and carried out through a disciplined process and set of best practices. Third, decommissioning: retiring or replacing old servers is routine IT work, yet it is more complex than building a data center because of the business-disruption and data-security risks involved, so it follows a deliberate sequence of planning and operational steps.

LEARNING OBJECTIVES

- Identify the responsibilities of data center managers
- Identify the various tools used to manage a data center
- Describe a software-defined data center (SDDC) and its benefits
- Describe change management and how it is used in data centers
- Identify the 7 Rs of change management
- Identify the need to decommission a data center
- Identify the steps to decommission a data center

15.1 Overview of data center management

Data center management effectively monitors and tracks the convergence of active and passive components to provide the administrator with a holistic view of the data center. That single, complete view is what makes it possible to use energy, equipment, and floor space in an efficient manner. Every piece of a data center infrastructure sorts into one of two categories, defined by the role the component plays: **active components take part *directly* in the operations** of the data center, while **passive components *support* the active components** in carrying out those operations. The divider is role, not whether a device happens to be powered on.

ACTIVE COMPONENTS	PASSIVE COMPONENTS
take part directly in operations	*support the active components*
▪ Network equipment — routers, switches ▪ Servers and computers ▪ Storage — SAN, backups, tape storage ▪ Security components such as firewalls ▪ Data center management software and applications ▪ The network operations center (NOC) — first line of support, with the service desk, incident management, and problem management	▪ Facility, site, power, cooling ▪ Cabling system ▪ Physical security — biometric security, access card, iris scanner, palm reader ▪ Racks and computing hardware ▪ Uninterruptible power supply (UPS) and fire protection ▪ Energy production systems (such as a generator) and environment control

Because these components must never go dark, **maintaining continuous uptime has become one of the highest priorities** in a data center: even a single minute of downtime can incur losses of millions of dollars, and even at small and medium enterprises the lost productivity from an outage can do serious damage. Monitoring helps you *anticipate* potential outages and address problems proactively — as, or before, they arise — and that is the job of **monitoring software**.

WHAT MONITORING SOFTWARE DOES

- Monitors and observes the performance of **IP-based devices**
- Monitors network services, switches, bandwidth utilization, routers, and traffic flow
- Monitors storage systems, servers, access control, security, power, and cooling
- Remotely assesses system performance
- Tracks and monitors IT-based devices such as **CCTV cameras** and **biometric devices**

15.2 Data center managers and their activities

A data center manager can monitor everything from the entire data center floor down to a **single outlet on an intelligent power distribution unit (PDU)**. In modern data centers, managers can even monitor the specific cabinets their company owns in a **colocation** data center situated elsewhere. Their work centers on keeping the facility running with as little downtime as possible.

RESPONSIBILITIES OF A DATA CENTER MANAGER

- **Perform maintenance on all the infrastructure** — replacing cables, upgrading hardware and software based on customer needs, and managing and maintaining devices and accessories
- **Prepare data center floor plans and schematic diagrams** with details of all installed equipment, including devices mounted on racks
- **Use data center management tools to minimize downtime**
- **Act immediately** based on the alerts and data received from the management tools

To do this, managers use a **variety of management tools** to measure, manage, and control the data center's energy consumption and achieve little to no downtime. The tools monitor all IT-related equipment — servers, storage, and network devices — along with facilities, power, climate control, and access control. They **provide visibility** into the

infrastructure, **track devices**, report the **health status** of components, and **send real-time alerts and notifications when a threshold limit is breached**. Finally, they **analyze the data** collected from every device and display it on a **dashboard** so the manager can act right away.

15.3 Data center management tools

Several management tools are available to monitor and manage everything from electrical systems to IT services. It is important to **select and deploy the right tools according to purpose and use**, so that managers can run the entire data center efficiently.

TABLE 15.1 The core data center management tools

TOOL	WHAT IT MONITORS OR MANAGES
Electrical power management system (EPMS)	Monitors and manages electrical systems for uninterrupted operations; provides intelligent, detailed power-quality data on the electrical distribution so you can analyze, optimize energy use, and decrease power consumption
Building management system (BMS)	Monitors heating and ventilation systems, as well as lighting, security, fire safety, plumbing, and water systems; can also detect electrical system issues through basic alarm and control notification
Server monitoring system	Monitors and tracks servers' performance — CPU usage, memory allocation, and more — so managers can identify and solve server-related issues and prevent downtime
Network monitoring system	Monitors all networking components (routers, switches, firewalls) for faults and performance to maintain and optimize availability; collects network uptime and bandwidth data
Storage monitoring system	Monitors storage performance to analyze and solve issues quickly — storage is a critical component for virtualization and big data, where performance issues hurt end users
IT service management (ITSM)	A ticketing system with workflows that supports managing activities and processes such as tracking IT assets, configuration management, and management of incidents, problems, and changes

15.4 The software-defined data center (SDDC)

A data center that is **fully automated by software** is called a **software-defined data center (SDDC)**, also known as a **virtual data center**. In an SDDC, all the infrastructure is virtualized and offered as a service: it consists of a storage facility in which **all hardware devices, networking, storage, CPU, and memory are delivered as a service through virtualization**. The hardware controls and configurations are held in a storage system; deployment, operation, and configuration are fully automated, and all configurations are already created and stored so they can be provisioned and customized whenever an organization requests virtual service from the data center.

TABLE 15.2 Benefits of an SDDC

BENEFIT	WHAT IT DELIVERS
Eliminates hardware dependency	Removes hardware and manual-interface dependency — all functions can be automated. Through artificial intelligence the SDDC learns commands and interfaces as changes are made and self-adjusts on any deviation, freeing IT staff from monitoring specific network segments so they can focus on innovation
Simplifies data management	Eliminates the use of multiple monitoring and configuration tools; integrates the entire infrastructure as a single unit managed with the click of a button. Device and data monitoring, storage allocation, and reconfiguring allocations happen from a single window
Automation and artificial intelligence	Improves the workflow of any repeatable, complex IT service as it continuously learns and improves itself; its main characteristics are specialized automation, direction, and abstraction of resources into software code — more accurate and reliable than human interaction
Proactive monitoring	Converts the reactive monitoring approach of legacy management tools into a proactive one

PROACTIVE MONITORING HELPS ADMINISTRATORS TO

- Identify slow application performance
- Detect and resolve issues
- Understand network bandwidth and allocate resources accordingly
- Identify security threats and chokes in network traffic
- Monitor IP assets and equipment upgrades

COMMON PITFALL

An SDDC is not simply a well-monitored data center. Its defining trait is that the whole facility — hardware, networking, storage, CPU, and memory — is delivered **as a service through virtualization** and is **fully automated by software**, which is why software (more accurate and reliable than human interaction) can handle changing requirements better than a legacy data center managed by personnel.

15.5 Change management and the need for it

Change management is a systematic approach for transition, transformation, and resulting safety precautions that includes implementing strategies for managing changes involving **people, processes, and technologies**. Changes in a data center are **inevitable** because technology and process improvements are always changing; they can be required in **systems, equipment, process, or personnel**; and every one **must be managed to ensure smooth functioning without downtime**. For example, a rise in customers might drive an expansion to fit more equipment, or you may need to redo cabling to replace old, worn-out cables. Because of this, the change management process must be clearly laid out, and you must plan and implement strategies so the changes are adopted and implemented effectively.

SITUATIONS THAT CALL FOR A CHANGE MANAGEMENT PLAN

- **Replacing network, fiber-optic, and power cables** — often done in phases; a plan keeps work smooth without affecting current operations and with minimal downtime
- **Decommissioning legacy hardware and software** — ensure remaining equipment can handle the added workload and that replacement software is already in place
- **Updating configuration, process, and security** — must both implement the change smoothly and mitigate any system vulnerability risk
- **Applying patches** and **changing or updating monitoring tools** — either can create unexpected situations; a plan rolls them out smoothly
- **Introducing new technologies** — requires training personnel and planning so existing operations are not affected
- **Conducting a merger or acquisition** of a new data center — must not disrupt existing operations
- **Expanding a data center** — by adding a new location and systems, or more equipment to an existing site — while keeping existing equipment in service
- **Implementing or expanding power, cooling, or security systems** — the three components of the network-critical physical infrastructure (`NCPI`) framework

Power, cooling, and security are the three important components of the `NCPI` framework in a data center. To prevent disruption in service, any change to these components should be supported by a change management plan *in addition to* the implementation plans for the systems themselves.

15.6 The 7 Rs of change management

When a change is proposed, you must create a **change management plan** that details **who, when, what, where, and how** the change will be implemented. To build an effective plan, answer the **7 Rs of change management** — seven questions that pin down every dimension of the proposed change.

TABLE 15.3 The 7 Rs and what each identifies

R	QUESTION TO ANSWER	WHAT THE RESPONSE IDENTIFIES
Raised by	Who has raised the change?	The change initiator
Reason for	What is the reason for the change?	The purpose of the change
Returns	What return or improvement is expected from the change?	The key benefit
Risks	What are the risks involved, and the mitigation plan?	Risks and mitigation plans
Resources	What resources or skill sets are required to deliver it?	Team, skill sets, and training needs
Responsibility	Who is responsible for creating, testing, and implementing it?	The team and change ambassadors
Relationships	What is the relationship between this change and other changes?	Interdependencies

COMMON PITFALL

Do not confuse the mnemonic. The 7 Rs are **Raised by, Reason for, Returns, Risks, Resources, Responsibility, and Relationships** — *not* Reply, Restore, or Recovery, which are common distractors on the knowledge check.

15.7 The change management process

Every data center must have a **detailed change management plan** that specifies the processes used to manage a change. Using a basic generic process together with the answers obtained from the 7 Rs, you can create an **implementation plan** for the proposed change.

GENERIC STEPS IN THE CHANGE MANAGEMENT PROCESS

- **Identify the components** that must be added or changed — products, services, or processes
- **Create a strong business case** outlining the need and benefits, then **get approval** from leadership or management
- Once approved, **assess the downtime** that could occur during implementation
- **Identify the team members** who will implement the change, and **train** them if necessary
- **Communicate to stakeholders** about the change and the potential downtime
- **Carry out the change** per the plan, monitoring and managing dependencies, risks, and budgets
- **Evaluate whether the change succeeded or failed** — if it failed, consider **returning to the previous state**
- If it succeeded, **review the change and implement a continuous improvement plan (`CIP`)** to maintain its effect

15.8 Best practices for change management

Certain best practices help ensure the successful implementation of changes in a data center. They span the *people* who carry out the change, the *case* made for it, and the *care* taken during and after the rollout.

TABLE 15.4 Change management best practices

BEST PRACTICE	WHAT IT INVOLVES
Choose the right change representation	Select a team with commitment, strong communication skills, good collaboration skills, and proficiency in problem solving and prioritizing jobs
Be sure the change fits the purpose	Align the objectives of the change with the objectives of the organization, and highlight benefits that apply directly to the end user
Sell the change	Prepare a solid business case so stakeholders understand the nature of the change, why it is applied, what will be different, and its benefits
Communicate the change	Use a positive top-down approach — employees respond better hearing about change from top leaders than from the change manager
Time the change	Carry out certain changes at specific times (for example a server switch on a Saturday evening) and implement incrementally to reduce resistance
Iron out all the issues before the release	Thoroughly try and test any data-center software change to detect and resolve bugs before release
Nominate the bar raisers	Use internal resources with the experience, expertise, and time to review the change and plan and provide guidance and verification
Integrate the change	Keep all change-management materials up to date so employees can review guidelines and see how the change meets organizational objectives
Check in with the employees	Monitor the change at the system and personnel levels; meet employees regularly and ask for feedback
Be flexible	Accept questions, concerns, and suggestions, and implement feedback when necessary to help employees adopt the change

COMMON PITFALL

When choosing the change representation team, **accuracy outweighs speed**. Completing the job faster while being inaccurate is *not* a desired trait — the change must seamlessly integrate with the existing system — so look for communication, collaboration, and problem-solving and prioritization skills, plus the flexibility to take employee feedback.

15.9 Decommissioning a data center

Decommissioning a data center involves replacing old servers with new ones or removing them from service. It is an activity performed **regularly** within IT organizations, but it is a **complex process — more complicated than building a data center** — because of the risk of **business disruption** across the whole process. Data centers hold an organization's data, including sensitive and confidential information, so any potential breach can put the company's future at risk. For all these reasons, a **decommission plan** is essential and should be completed by professionals, with professional handling and supervision throughout.

COMMON REASONS TO DECOMMISSION A DATA CENTER

- **Move to cloud-based servers** — replace physical data servers for improved efficiency and speed
- **Upgrade to newer hardware** — to enhance security and provide updates
- **Adopt colocation services** — lease rack space from a third-party provider, usually more flexible, secure, reliable, and cost-effective than owning a data center
- **Centralize data centers** — move them to one location to simplify administration and maintenance
- **Replace and upgrade old equipment** — to better manage workload requirements

COMMON PITFALL

"Decommissioning just means turning off the data center switch" is wrong. Decommissioning means **replacing old servers with new ones or removing them from service** — a routine but complex activity that preserves data and application logic and requires professional handling, not a simple power-down.

15.10 Steps to decommission a data center

Because decommissioning is complex, **specific protocols must be followed** and a decommission plan ensures a smooth transition. Although each organization may set its own protocols, the process is usefully viewed at two levels: the **major planning steps** of the overall process, and the **operational steps** performed on the equipment itself.

TABLE 15.5 The five major steps of the decommissioning process

MAJOR STEP	RELATED ACTIVITY
Establish a migration plan	Create a plan to migrate data from the servers that will be decommissioned to the target system
Perform migration activities	Migrate the data and create the certificate of migration
Establish a decommission plan	Create a plan to decommission the old system while preserving the data and application logic
Decommission the old system	Once the decommission plan is approved, decommission the old system
Perform a post-decommissioning review	Review the timelines for each step and document lessons learned for the future

SET UP A PROJECT MANAGEMENT OFFICE (PMO) FIRST

- **Define the scope and budget** and finalize an estimated timeline for the work
- **Establish a timeline and cutover date** — by which all data should be backed up and restored to another data center
- **Manage risk** — along with quality, resources, communication, and procurement, from planning through completion
- **Inform stakeholders** so they can take precautions for their data and applications before decommissioning
- **Conduct a physical audit** of the equipment and create an **asset map**

OPERATIONAL STEPS TO DECOMMISSION

- Finalize an **updated asset map**
- Run **tests and simulations**
- Create a **comprehensive backup**
- **Disconnect** all the equipment
- **Verify** the documentation
- Carry out **disposal**

Module summary

- A data center's infrastructure divides into active components (which take part directly in operations — network equipment, servers, computers, storage, security, management software, the NOC) and passive components (which support them — facility, power, cooling, cabling, physical security, racks, UPS, fire protection, energy production, environment control).
- Because a minute of downtime can cost millions, monitoring software remotely observes IP-based devices, network services, storage, servers, power, cooling, and IT devices such as CCTV and biometrics so managers can act proactively.
- Data center managers perform maintenance on all infrastructure, prepare floor plans and schematic diagrams, use management tools to minimize downtime, and act immediately on the alerts and dashboards those tools provide.
- The core management tools are EPMS (electrical), BMS (building systems), server monitoring, network monitoring, storage monitoring, and ITSM (a ticketing system for assets, configuration, and incident/problem/change management).
- A software-defined data center is fully automated by software — a virtual data center delivering hardware, networking, storage, CPU, and memory as a service through virtualization — eliminating hardware dependency, simplifying management, adding automation and AI, and enabling proactive monitoring.
- Change management is a systematic approach to transition and transformation involving people, processes, and technologies; changes are inevitable, can affect systems, equipment, process, or personnel, and must be managed without downtime — including changes to power, cooling, and security, the three components of NCPI.
- Every change is planned by answering the 7 Rs — Raised by, Reason for, Returns, Risks, Resources, Responsibility, Relationships — then implemented through a generic process (identify, business case and approval, assess downtime, staff and train, communicate, execute, evaluate, and run a continuous improvement plan) and guided by best practices for the people, the case, and the care taken.
- Decommissioning — replacing or retiring old servers — is routine but more complex than building a data center because of business-disruption and data-security risk; it follows five major steps (migration plan, migration activities, decommission plan, decommission, post-decommissioning review), begins with a project management office, and runs the operational sequence of asset map, tests and simulations, backup, disconnect, verify documentation, and disposal.

Review questions

1. **Distinguish active from passive components, with examples of each.**

   Answer: Active components take part directly in operations: network and networking equipment (routers, switches), servers, computers, storage (SAN, backups, tape), security (firewalls), management software and applications, and the NOC. Passive components support the active ones: facility, site, power, cooling, cabling, physical security (biometric, access card, iris, palm), racks, computing hardware, UPS, fire protection, energy production (generator), and environment control.

2. **Why is monitoring software so important, and what does it monitor?**

   Answer: Even a single minute of downtime can cost millions and hurt productivity, so monitoring lets managers anticipate and proactively address outages. It observes the performance of IP-based devices; monitors network services, switches, bandwidth, routers, traffic flow, storage, servers, access control, security, power, and cooling; and tracks IT devices such as CCTV cameras and biometric devices.

3. **What is an SDDC, and what are its four benefits?**

   Answer: A software-defined data center is a data center fully automated by software — a virtual data center where all hardware, networking, storage, CPU, and memory are delivered as a service through virtualization. Its benefits are eliminating hardware dependency, simplifying data management, providing automation and artificial intelligence, and enabling proactive monitoring.

4. **What is change management, and why are changes inevitable in a data center?**

   Answer: It is a systematic approach for transition, transformation, and safety precautions that implements strategies to manage changes involving people, processes, and technologies. Changes are inevitable because technology and process improvements are always changing; they can be required in systems, equipment, process, or personnel and must be managed to avoid downtime.

5. **List the 7 Rs of change management and what each identifies.**

   Answer: Raised by (the initiator), Reason for (the purpose), Returns (the benefit), Risks (risks and mitigation plans), Resources (team, skill sets, and training needs), Responsibility (the team and change ambassadors), and Relationships (interdependencies with other changes).

6. **Outline the generic steps of the change management process.**

   Answer: Identify the components to add or change; build a business case and get leadership approval; assess potential downtime; identify and train the implementation team; communicate to stakeholders; carry out the change while managing dependencies, risks, and budgets; evaluate success or failure (roll back if it failed); and if it succeeded, review it and implement a continuous improvement plan (CIP).

7. **Why is decommissioning considered more complex than building a data center, and what precautions are taken?**

   Answer: It carries a high risk of business disruption and involves sensitive, confidential data whose breach can risk the company's future. Precautions include professional handling and a formal decommission plan, plus a project management office that defines scope, budget, and timeline (with a cutover date), manages risk, informs stakeholders, and conducts a physical audit to create an asset map.

8. **List the operational steps to decommission a data center, in order.**

   Answer: Finalize an updated asset map, run tests and simulations, create a comprehensive backup, disconnect all equipment, verify the documentation, and perform disposal.