COURSE SYLLABUS

LAST REVIEW	Fall 2022
COURSE TITLE	Server Administration
COURSE NUMBER	CRTE 0201
DIVISION	Career and Technical Education
DEPARTMENT	CRTE
CIP CODE	11.1006
CREDIT HOURS	3
CONTACT HOURS/WEEK	Class: 2 Lab: 2
PREREQUISITES	None

COURSE DESCRIPTION

This class will introduce the student to the knowledge and skills required to build, maintain, troubleshoot and support server hardware and software technologies. The successful candidate will be able to identify environmental issues; understand and comply with disaster recovery and physical / software security procedures; be familiar with industry terminology and concepts; understand server roles / specializations and interaction within the overall computing environment.

PROGRAM ALIGNMENT

This course is part of a program aligned through the Kansas Board of Regents and Technical Education Authority. For more information, please visit: https://kansasregents.org/workforce_development/program-alignment

PROGRAM LEARNING OUTCOMES

1. Students will be able to configure a router and a switch for basic functionality
2. Students will be able to configure, monitor and troubleshoot access controls lists for various addressing methods
3. Students will be able to build, maintain and troubleshoot server hardware and software technologies
4. Students will be able to explain and enforce basic concepts of computer network security

TEXTBOOKS

http://kckccbookstore.com/

METHODS OF INSTRUCTION

A variety of instructional methods may be used depending on content area. These include but are not limited to: lecture, multimedia, cooperative/collaborative learning, labs and demonstrations, projects and presentations, speeches, debates, panels, conferencing, performances, and learning experiences outside the classroom. Methodology will be selected to best meet student needs.

COURSE OUTLINE

I. IT Environment

A. Write, utilize and maintain documentation, diagrams and procedures

1. Follow pre-installation plan when building or upgrading servers

2. Labeling

3. Diagram server racks and environment topologies

4. Hardware and software upgrade, installation, configuration, server role and repair logs

5. Document server baseline (before and after service)

5. Original hardware configuration, service tags, asset management and warranty

6. Vendor specific documentation

a. Reference proper manuals

b. Websites

c. Support channels (list of vendors)

B. Given a scenario, explain the purpose of the following industry best practices

1. Follow vendor specific server best practices

a. Documentation

b. Tools

c. Websites

2. Explore ramifications before implementing change – determine organizational impact

3. Communicate with stakeholders before taking action and upon completion of action

4. Comply with all local laws / regulations, industry and corporate regulations

5. Purpose of Service Level Agreement (SLAs)

6. Follow change control procedures

7. Equipment disposal

C. Determine an appropriate physical environment for the server location

1. Check for adequate and dedicated power, proper amperage and voltage

a. UPS systems (check load, document service, periodic testing)

b. UPS specifications (run time, max load, bypass procedures, server

2. Server cooling considerations – HVAC

a. Adequate cooling in room

b. Adequate cooling in server rack

c. Temperature and humidity monitors

D. Implement and configure different methods of server access

1. KVM (local and IP based)

2. Direct connect

3. Remote management communication and shut down, proper monitoring)

a. Remote control

b. Administration

c. Software deployment

e. Dedicated management port

E. Given a scenario, classify physical security measures for a server location

1. Physical server security

a. Locked doors

b. Rack doors

        - c. CCTV
        - d. Mantraps
        - e. Security personnel
    - 2. Access control devices (RFID, keypads, pinpads)
        - a. Biometric devices (fingerprint scanner, retina)
    - 3. Security procedures
    - 4. Defense in-depth – multiple layers of defense
    - 5. Reasons for physical security
    - 6. Secure documentation related to servers
        - a. Limited access
        - b. Access logs
        - c. Limited hours
        - d. Theft
        - e. Data loss
        - f. Hacking
        - g. Passwords
        - h. System configurations
        - i. Logs

- II. Disaster Recovery
  - A. Compare and contrast backup and restoration methodologies, media types and concepts
    - 1. Methodologies (full, incremental, differential, selective)
      - a. Snapshot
      - b. Copy
      - c. Bare metal
      - d. Open file
      - e. Databases
      - f. Data vs. OS restore
      - g. Rotation and retention (grandfather, father and son)
    - 2. Media types
      - a. Tape
      - b. Disk
      - c. WORM
      - d. Optical
      - e. Flash
    - 3. Backup security and off-site storage
    - 4. Importance of testing the backup and restoration process
  - B. Given a scenario, compare and contrast the different types of replication methods
    - 1. Disk to disk
    - 2. Server to server
      - a. Clustering
      - b. Active/active
      - c. Active/passive
    - 3. Site to site
    - 4. Site types
      - a. Cold site
      - b. Hot site
      - c. Warm site

d. Distance requirements

C. Explain data retention and destruction concepts

1. Awareness of potential legal requirements
2. Awareness of potential company policy requirements
3. Differentiate between archiving and backup plan

D. Given a scenario, carry out the following basic steps of a disaster recovery

1. Disaster recovery testing process

Follow emergency procedures (people first)

3. Use appropriate fire suppressants
4. Follow escalation procedures for emergencies
5. Classification of systems (prioritization during recovery)

III. Troubleshooting

A. Explain troubleshooting theory and methodologies

1. Identify the problem and determine the scope

a. Question users/stakeholders and identify changes to the server/environment

b. Collect additional documentation/logs

c. If possible, replicate the problem as appropriate

d. If possible, perform backups before making changes

2. Establish a theory of probable cause (question the obvious)

a. Determine whether there is a common element of symptom causing multiple problems

3. Test the theory to determine cause

a. Once theory is confirmed determine next steps to resolve problem

b. If theory is not confirmed re-establish new theory or escalate

4. Establish a plan of action to resolve the problem and notify impacted users
5. Implement the solution or escalate as appropriate

a. Make one change at a time and test/confirm the change has resolved the problem

b. If the problem is not resolved, reverse the change if appropriate and implement new change

6. Verify full system functionality and if applicable implement preventative measures
7. Perform a root cause analysis
8. Document findings, actions and outcomes throughout the

B. Given a scenario, effectively troubleshoot hardware problems, selecting the appropriate tools and methods

1. Common problems

a. Failed POST

b. Overheating

c. Memory failure

d. Onboard component failure

e. Processor failure

f. Incorrect boot sequence

g. Expansion card failure

h. Operating system not found

i. Drive failure

j. Power supply failure

        k. I/O failure
    2. Causes of common problems
        a. Third party components or incompatible components
        b. Incompatible or incorrect BIOS
        c. Cooling failure
        d. Mismatched components
        e. Backplane failure
    3. Environmental issues
        a. Dust
        b. Humidity
        c. Temperature
        d. Power surge / failure
    4. Hardware tools
        a. Power supply tester (multimeter)
        b. System board tester
        c. Compressed air
        d. ESD equipment

C. Given a scenario, effectively troubleshoot software problems, selecting the appropriate tools and methods

    1. Common problems
        a. User unable to logon
        b. User cannot access resources
        c. Memory leak
        d. BSOD / stop
        e. OS boot failure
        f. Driver issues
        g. Runaway process
        h. Cannot mount drive
        i. Cannot write to system log
        j. Slow OS performance
        k. Patch update failure
        l. Service failure
        m. Hangs no shut down
        n. Users cannot print
    2. Cause of common problems
        a. Malware
        b. Unauthorized software
        c. Software firewall
        d. User Account Control (UAC/SUDO)
        e. Improper permissions
        f. Corrupted files
        g. Lack of hard drive space
        h. Lack of system resources
        i. Virtual memory (misconfigured, corrupt)
        j. Fragmentation
        k. Encryption
        l. Print server drivers/services
        m. Print spooler

3. Software tools
a. System logs
b. Monitoring tools (resource monitor, performance monitor)
c. Defragmentation tools

D. Given a scenario, effectively diagnose network problems, selecting the appropriate tools and methods

1. Common problems
a. Internet connectivity failure
b. Email failure
c. Resource unavailable
d. DHCP server mis-configured
e. Non-functional or unreachable
f. Destination host unreachable
g. Unknown host
h. Default gateway mis-configured
i. Failure of service provider
j. Can reach by IP not by host name

2. Causes of common problems
a. Improper IP configuration
b. VLAN configuration
c. Port security
d. Improper subnetting
e. Component failure
f. Incorrect OS route tables
g. Bad cables
h. Firewall (mis-configuration, hardware failure, software failure)
i. Mis-configured NIC, routing / switch issues
j. DNS and/or DHCP failure
k. Mis-configured hosts file

3. Networking tools
a. Ping
b. Tracert/traceroute
c. Ipconfig/ifconfig
d. Nslookup
e. Net use/mount
f. Route
g. Nbtstat
h. Netstat

E. Given a scenario, effectively troubleshoot storage problems, selecting the appropriate tools and methods

1. Common problems
a. Slow file access
b. OS not found
c. Data not available
d. Unsuccessful backup
e. Error lights
f. Unable to mount the device
g. Drive not available

h. Cannot access logical drive
i. Data corruption
j. Slow I/O performance
k. Restore failure
l. Cache failure
m. Multiple drive failure

2. Causes of common problems

a. Media failure
b. Drive failure
c. Controller failure
d. HBA failure
e. Loose connectors
f. Cable problems
g. Mis-configuration
h. Improper termination
i. Corrupt boot sector
j. Corrupt file system table
k. Array rebuild
l. Improper disk partition
m. Bad sectors
n. Cache battery failure
o. Cache turned off
p. Insufficient space
q. Improper RAID configuration
r. Mis-matched drives
s. Backplane failure

3. Storage tools

a. Partitioning tools
b. Disk management
c. RAID array management
d. Array management
e. System logs
f. Net use / mount command
g. Monitoring tools

COURSE LEARNING OUTCOMES AND COMPETENCIES
Upon successful completion of this course, the student will:

A. Write, utilize and maintain documentation, diagrams and procedures.
1. Follow a pre-installation plan before upgrading a server.
2. Diagram a basic network.

B. Explain industry best practices.
3. Describe industry best practices.
4. Analyze service level agreements.

C. Determine an appropriate physical location for a server room.
5. Analyze the requirements for a server room.

D. Implement and configure different methods of server access.
   6. Utilize a KVM.
   7. Perform a remote access to a server.

E. Discuss physical security methods.
   8. Discuss physical server security methods.
   9. Configure physical control devices.

F. Compare and contrast backup and restoration methodologies.
   10. Describe backup methods.
   11. Describe restoration methods.
   12. Compare and contrast backup media types.

G. Compare and contrast different types of server replication methods.
   13. Describe disk to disk replication.
   14. Describe server clustering.

H. Explain data retention and destruction methods.
   15. Describe data retention and destruction methods.

I. Describe basic steps of disaster recovery.
   16. Describe the steps for disaster recovery.

J. Explain troubleshooting theory and methodologies.
   17. Identify a problem and determine the scope.
   18. Establish a theory of probable cause.
   19. Test a theory.

K. Utilize appropriate tools to troubleshoot software problems.
   20. Troubleshoot a post failure.
   21. Troubleshoot a overheating problem.

L. Diagnose network problems.
   22. Diagnose a network problem.

M. Diagnose storage problems.
   23. Explain common storage problems.

ASSESSMENT OF COURSE LEARNING OUTCOMES AND COMPETENCIES

Student progress is evaluated through both formative and summative assessment methods. Specific details may be found in the instructor’s course information document.

COLLEGE POLICIES AND PROCEDURES

Student Handbook
https://www.kckcc.edu/files/docs/student-resources/student-handbook-and-code-of-conduct.pdf

College Catalog

https://www.kckcc.edu/academics/catalog/index.html

College Policies and Statements
https://www.kckcc.edu/about/policies-statements/index.html

Accessibility and Accommodations
https://www.kckcc.edu/academics/resources/student-accessibility-support-services/index.html.