Sinclair Community College
444 E. Third St.
Dayton, OH 45402

Master Syllabus

CIS 2515 - Windows Network Infrastructure

Division: Business and Public Services

Department: Computer Information Systems

Credit Hour Total: 3.0 **Lecture Hrs:** 3.0

Prerequisite(s): CIS 2510

Date Revised: June 2014

Course Description:

Intermediate administration and support functions of the current Windows Server operating system. Focus is on more detailed functions of common roles and features such as core networking, security, and Windows Updating. Also more advanced use of Active Directory and Group Policy.

General Education Outcomes:

- Critical Thinking/Problem Solving Competency
- Computer Literacy Competency

Course Outcomes:

Configure and manage Active Directory.
Configure Domain Controllers (DCs) including operations masters, read only DCs and backup of DCs. Configure and manage group policies including ordering, blocking inheritance, logon/logoff scripts, folder redirection, security template settings and more.

Assessment Method: Locally developed exams
Performance Criteria:

Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations
Performance Criteria:

Students will perform at a 75% or higher level on a locally developed lab simulation.

Configure network services and access.
Configure and manage access to the network via Remote Access, Virtual Private Networks (VPNs), Remote Desktop, RADIUS, wireless access and other methods and to configure Network Access Protection.

Assessment Method: Locally developed exams
Performance Criteria:

Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations
Performance Criteria:

Students will perform at a 75% or higher level on a locally developed lab simulation.

Deploy, manage and maintain servers.
Install servers via Windows Deployment Services (WDS) including image creation and management. Manage Windows Update Services (WSUS) for patch management.

Assessment Method: Locally developed exams
Performance Criteria:

Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations
Performance Criteria:

Students will perform at a 75% or higher level on a locally developed lab simulation.

Manage and configure file and print services.
Configure file servers to manage backup and restore services, to assign disk quotas, file and disk encryption, shadow copies and the distributed file system (DFS).

Assessment Method: Locally developed exams
Performance Criteria:

Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations
Performance Criteria:

Students will perform at a 75% or higher level on a locally developed lab simulation.

Outline:

A. Deploy, manage and maintain servers
1. Deploy and manage server images. Install the Windows Deployment Services (WDS) role; configure and manage boot, install,

and discover images; update images with patches, hotfixes, and drivers; install features for offline images; configure driver groups and packages
2. Implement patch management. Install and configure the Windows Server Update Services (WSUS) role, configure group policies for updates, client-side targeting, WSUS synchronization, WSUS groups, manage patch management in mixed environments
3. Monitor servers. Configure Data Collector Sets (DCS), configure alerts, monitor real-time performance, monitor virtual machines (VMs), monitor events, configure event subscriptions, network monitoring, and schedule performance monitoring

B. Configure File and Print Services.
1. Configure the Distributed File System (DFS). Install and configure DFS namespaces, configure DFS Replication Targets, configure Replication Scheduling, configure Remote Differential Compression settings, configure staging, fault tolerance, clone a DFS database, recover DFS databases, optimize DFS replication
2. Configure File Server Resource Manager (FSRM). Install the FSRM role service, configure quotas, configure file screens, configure reports, configure file management tasks
3. Configure file and disk encryption. Configure BitLocker encryption; configure the Network Unlock feature; configure BitLocker policies; configure the EFS recovery agent; manage EFS and BitLocker certificates, including backup and restore
4. Configure advanced audit policies. Implement auditing using Group Policy and AuditPol.exe, create expression-based audit policies, create removable device audit policies

C. Configure network services and access.
1. Configure DNS zones. Configure primary and secondary zones, stub zones, conditional forwards, zone and conditional forward storage in Active Directory, zone delegation, zone transfer settings, notify settings.
2. Configure DNS records. Create and configure DNS Resource Records (RR), including A, AAAA, PTR, SOA, NS, SRV, CNAME, and MX records; configure zone scavenging; configure record options, including Time To Live (TTL) and weight; configure round robin; configure secure dynamic updates.
3. Configure virtual private network (VPN) and routing. Install and configure the Remote Access role, implement Network Address Translation (NAT), configure VPN settings, configure remote dial-in settings for users, configure routing, configure Web Application proxy in pass through mode.
4. Configure Direct Access. Implement server requirements, implement client configuration, configure DNS for Direct Access, configure certificates for Direct Access.

D. Configure a Network Policy Server (NPS) infrastructure.
1. Configure Network Policy Server. Configure a RADIUS server, including RADIUS proxy; configure RADIUS clients; configure NPS templates; configure RADIUS accounting; configure certificates.
2. Configure NPS policies. Configure connection request policies, configure network policies for VPN clients (multilink and bandwidth allocation, IP filters, encryption, IP addressing), import and export NPS policies.
3. Configure Network Access Protection (NAP). Configure System Health Validators (SHVs), configure health policies, configure NAP enforcement using DHCP and VPN, configure isolation and remediation of non-compliant computers using DHCP and VPN, configure NAP client settings.

E. Configure and manage Active Directory.
1. Configure service authentication. Create and configure Service Accounts, create and configure Group Managed Service Accounts, configure Kerberos delegation, manage Service Principal Names (SPNs), configure virtual accounts.
2. Configure domain controllers. Transfer and seize operations master roles, install and configure a read-only domain controller (RODC), configure domain controller cloning.
3. Maintain Active Directory
Back up Active Directory and SYSVOL, manage Active Directory offline, optimize an Active Directory database, clean up metadata, configure Active Directory snapshots, perform object- and container-level recovery, perform Active Directory restore, configure and restore objects by using the Active Directory Recycle Bin.
4. Configure account policies. Configure domain and local user password policy settings, configure and apply Password Settings Objects (PSOs), delegate password settings management, configure account lockout policy settings, configure Kerberos policy settings.

F. Configure and manage Group Policy.
1. Configure Group Policy processing. Configure processing order and precedence, configure blocking of inheritance, configure enforced policies, configure security filtering and Windows Management Instrumentation (WMI) filtering, configure loopback processing, configure and manage slow-link processing and Group Policy caching, configure client-side extension (CSE) behavior, force Group Policy Update.
2. Configure Group Policy settings. Configure settings, including software installation, folder redirection, scripts, and administrative template settings; import security templates; import custom administrative template file; configure property filters for administrative templates.
3. Manage Group Policy objects (GPOs). Back up, import, copy, and restore GPOs; create and configure Migration Table; reset default GPOs; delegate Group Policy management.
4. Configure Group Policy preferences (GPP). Configure GPP settings, including printers, network drive mappings, power options, custom registry settings, Control Panel settings, Internet Explorer settings, file and folder deployment, and shortcut deployment; configure item-level targeting.