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

Master Syllabus

CIS 2520 - Windows Server Advanced Services

Division: Business and Public Services

Department: Computer Information Systems

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

Prerequisite(s): CIS 2510

Date Revised: January 2016

Course Description:

Successfully plan, implement and troubleshoot a Microsoft Windows Active Directory® (AD) infrastructure. The course focuses on a Windows directory service environment including advanced services such as Federation Services, Certificate Services and Rights Management Services. Advanced network services using DHCPv6, Domain Name Service using DNSSEC and IP Address Management (IPAM) are included. High availability through Network Load Balancing, Clustering and Virtualization using Hyper-V is included.

General Education Outcomes:

- Critical Thinking/Problem Solving Competency
- Computer Literacy Competency

Course Outcomes:

Configure the Active Directory infrastructure
Manage multi-domain and multi-forest environment including external, forest, shortcut and realm trusts. Create and manage sites and site links for optimal Active Directory (AD) replication. Manage advanced AD services including Certificates, Digital Rights Management and Federation Services.

Assessment Method: Locally developed exams
Performance Criteria:

Students will perfrom at a 75% success rate on a locally developed exam.

Assessment Method: Simulations
Performance Criteria:

Students will perfrom at a 75% success rate on a locally developed rubric.

Assessment Method: Standardized national examinations
Performance Criteria:

Students will pass the related Microsoft Certification Exam (currently exam #70-412)

Configure and manage high availability in servers
Configure Network Load Balancing (NLB) including affinity, port rules and cluster operation modes. Configure fail over clustering roles including role specific settings and preferences. Implement business continuity and disaster recovery through backup strategies, site-level fault tolerance, and Hyper-V replicas.

Assessment Method: Locally developed exams
Performance Criteria:

Students will perfrom at a 75% success rate on a locally developed exam.

Assessment Method: Simulations
Performance Criteria:

Students will perfrom at a 75% success rate on a locally developed rubric.

Assessment Method: Standardized national examinations
Performance Criteria:

Students will pass the related Microsoft Certification Exam (currently exam #70-412)

Install and manage advanced network services
Implement an advanced DHCP and DHCPv6 solution using superscopes and multicast scopes; manage high availability and fail over for DHCP. Implement an advanced DNS solution using DNSSEC for security.

Assessment Method: Locally developed exams
Performance Criteria:

Students will perfrom at a 75% success rate on a locally developed exam.

Assessment Method: Simulations
Performance Criteria:

Students will perfrom at a 75% success rate on a locally developed rubric.

Assessment Method: Standardized national examinations
Performance Criteria:

Students will pass the related Microsoft Certification Exam (currently exam #70-412)

Configure file and storage solutions

Use advanced file services including Network File System data store, Branch Cache and File Classification Infrastructure using File Service Resource Manager (FSRM). Configure and optimize storage using iSCSI target and initiator, Internet Storage Name Server (iSNS) and thin provisioning.

Assessment Method: Locally developed exams
Performance Criteria:

Students will perfrom at a 75% success rate on a locally developed exam.

Assessment Method: Simulations
Performance Criteria:

Students will perfrom at a 75% success rate on a locally developed rubric.

Assessment Method: Standardized national examinations
Performance Criteria:

Students will pass the related Microsoft Certification Exam (currently exam #70-412)

Outline:

A. Configure and manage high availability

1. Configure Network Load Balancing (NLB). Install NLB nodes, configure NLB prerequisites, configure affinity, configure port rules, configure cluster operation mode, upgrade an NLB cluster

2. Configure failover clustering. Configure quorum, cluster networking, restore single node or cluster configuration, configure cluster storage, implement Cluster-Aware Updating, upgrade a cluster, configure and optimize clustered shared volumes, clusters without network names, storage spaces

3. Manage failover clustering roles. Configure role-specific settings, including continuously available shares; configure virtual machine (VM) monitoring; failover and preference settings; and, guest clustering

4. Manage VM movement. Perform live migration; perform quick migration; perform storage migration; import, export, and copy VMs; configure VM network health protection; configure drain on shutdown

B. Configure file and storage solutions.

1. Configure advanced file services. Configure Network File System (NFS) data store, configure BranchCache, configure File Classification Infrastructure (FCI) using File Server Resource Manager (FSRM), configure file access auditing

2. Implement Dynamic Access Control (DAC). Configure user and device claim types, implement policy changes and staging, perform access-denied remediation, configure file classification, create and configure Central Access rules and policies, create and configure resource properties and lists

3. Configure and optimize storage. Configure iSCSI target and initiator, configure Internet Storage Name server (iSNS), implement thin provisioning and trim, manage server free space using Features on Demand, configure tiered storage

C. Implement business continuity and disaster recovery.

1. Configure and manage backups. Configure Windows Server backups, configure Windows Azure backups, configure role-specific backups, manage VSS settings using VSSAdmin

2. Recover servers. Restore from backups, perform a Bare Metal Restore (BMR), recover servers using Windows Recovery Environment (Win RE) and safe mode, configure the Boot Configuration Data (BCD) store

3. Configure site-level fault tolerance. Configure Hyper-V Replica, including Hyper-V Replica Broker and VMs; configure multi-site clustering, including network settings, Quorum, and failover settings; configure Hyper-V Replica extended replication; configure Global Update Manager; recover a multi-site failover cluster

D. Configure Network Services.

1. Implement an advanced Dynamic Host Configuration Protocol (DHCP) solution. Create and configure superscopes and multicast scopes; implement DHCPv6; configure high availability for DHCP, including DHCP failover and split scopes; configure DHCP Name Protection; configure DNS registration

2. Implement an advanced DNS solution. Configure security for DNS, including Domain Name System Security Extensions (DNSSEC), DNS Socket Pool, and cache locking; configure DNS logging; configure delegated administration; configure recursion; configure netmask ordering; configure a GlobalNames zone; analyze zone level statistics

3. Deploy and manage IP Address Management (IPAM). Provision IPAM manually or by using Group Policy, configure server discovery, create and manage IP blocks and ranges, monitor utilization of IP address space, migrate to IPAM, delegate IPAM administration, manage IPAM collections, configure IPAM database storage

E. Configure the Active Directory infrastructure.

1. Configure a forest or a domain. Implement multi-domain and multi-forest Active Directory environments, including interoperability with previous versions of Active Directory; upgrade existing domains and forests, including environment preparation and functional levels; configure multiple user principal name (UPN) suffixes

2. Configure trusts. Configure external, forest, shortcut, and realm trusts; configure trust authentication; configure SID filtering; configure name suffix routing

3. Configure sites. Configure sites and subnets, create and configure site links, manage site coverage, manage registration of SRV records, move domain controllers between sites

4. Manage Active Directory and SYSVOL replication. Configure replication to Read-Only Domain Controllers (RODCs), configure Password Replication Policy (PRP) for RODC, monitor and manage replication, upgrade SYSVOL replication to Distributed File System Replication (DFSR)

F. Configure Identity and Access Solutions.

1. Implement Active Directory Federation Services (AD FS). Install AD FS; implement claims-based authentication, including Relying Party Trusts; configure authentication policies; configure Workplace Join; configure multi-factor authentication

2. Install and configure Active Directory Certificate Services (AD CS). Install an Enterprise Certificate Authority (CA), configure certificate revocation lists (CRL) distribution points, install and configure Online Responder, implement administrative role separation, configure CA backup and recovery

3. Manage certificates. Manage certificate templates; implement and manage certificate deployment, validation, and revocation; manage certificate renewal; manage certificate enrollment and renewal to computers and users using Group Policies; configure and manage key archival and recovery

4. Install and configure Active Directory Rights Management Services (AD RMS). Install a licensing or certificate AD RMS server, manage AD RMS Service Connection Point (SCP), manage RMS templates, configure Exclusion Policies, back up and restore AD RMS