Washtenaw Community College Comprehensive Report

CNT 224 Identity with Windows Server
Effective Term: Spring/Summer 2022

Course Cover

College: Business and Computer Technologies
Division: Business and Computer Technologies
Department: Computer Science & Information Technology
Discipline: Computer Networking Technology
Course Number: 224
Org Number: 13400
Full Course Title: Identity with Windows Server
Transcript Title: Identity with Windows Server
Is Consultation with other department(s) required: No
Publish in the Following: College Catalog , Time Schedule , Web Page
Reason for Submission: Course Change
Change Information:
Course title
Course description
Objectives/Evaluation
Rationale: Remove all instances of 2016 from the title and description.
Proposed Start Semester: Winter 2022
Course Description: In this course, students will learn the skills and knowledge necessary to manage and maintain the core infrastructure required for a Windows Server environment. Topics include all aspects of active directory and includes initial A.D. and DNS installations, as well as creating and managing users, groups, and computers. Group policies are emphasized which include security policies, auditing, inheritance, software installations, folder redirection, logon scripts, and printer installations. Also covered are dynamic access control, trusts, sites, certificate server, and delegation. The title of this course was previously Identity with Windows Server 2016.

Course Credit Hours

Variable hours: No
Credits: 4
Lecture Hours: Instructor: 60 **Student:** 60
Lab: Instructor: 0 **Student:** 0
Clinical: Instructor: 0 **Student:** 0

Total Contact Hours: Instructor: 60 **Student:** 60
Repeatable for Credit: NO
Grading Methods: Letter Grades
Audit
Are lectures, labs, or clinicals offered as separate sections?: NO (same sections)

College-Level Reading and Writing

College-level Reading & Writing

College-Level Math

No Level Required

Requisites

General Education

General Education Area 7 - Computer and Information Literacy

Assoc in Arts - Comp Lit
Assoc in Applied Sci - Comp Lit
Assoc in Science - Comp Lit

Request Course Transfer

Proposed For:

Student Learning Outcomes

1. Identify the concepts behind Windows Certificate Server including Server installation and configuration, issuance of both Web Server and client certificates, revocation of certificates, and the process for importing and exporting certificates.
   Assessment 1
   Assessment Tool: Outcome-related test questions
   Assessment Date: Winter 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer key and departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of the students will correctly answer 70% of the outcome-related questions
   Who will score and analyze the data: Departmental faculty

2. Identify the principles related to installing and configuring Active Directory Services, including identifying the various objects, the creation and management of domains and organizational units, user and computer accounts, user profiles, and the use of Windows groups as part of A.D. administration.
   Assessment 1
   Assessment Tool: Outcome-related test questions
   Assessment Date: Winter 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer key and departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of the students will correctly answer 70% of the outcome-related questions
   Who will score and analyze the data: Departmental faculty

3. Identify and define Active Directory Group Policy concepts which consist of security settings (including account and password policies, user rights and security options), Desktop Management, inheritance, Folder Redirection, Logon Scripts, software deployment, loopback policies and printer installations.
   Assessment 1
   Assessment Tool: Outcome-related test questions
   Assessment Date: Winter 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer key and departmentally-developed rubric

Standard of success to be used for this assessment: 70% of the students will correctly answer 70% of the outcome-related questions
Who will score and analyze the data: Departmental faculty

4. Identify the implementation of Advanced Active Directory concepts including sites, site links, inter-site domain replication, FSMO roles, functional levels, and distinguish the different types of A.D. trusts including cross-forest and external trusts.
   Assessment 1
   Assessment Tool: Outcome-related test questions
   Assessment Date: Winter 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer key and departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of the students will correctly answer 70% of the outcome-related questions
   Who will score and analyze the data: Departmental faculty

5. Define the different types of Advanced Access Control including Federation Server, Rights Management Server, access-based enumeration, file screening, quotas, encryption, software restriction, AppLocker, and Dynamic Access Control.
   Assessment 1
   Assessment Tool: Outcome-related test questions
   Assessment Date: Winter 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer key and departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of the students will correctly answer 70% of the outcome-related questions
   Who will score and analyze the data: Departmental faculty

Course Objectives

1. Define the installation procedures associated with the installation of Windows Certificate Server Authorities for both Standalone and Enterprise Types including the proper naming and generation of the self-signed root certificates.
2. Identify the methods for issuing both Server and Client certificates, including the various alternatives for requesting, approving, and retrieving them; distinguish between the differences between the two types.
3. Define the methods for exporting and importing certificates/public keys with/without the private key, including identifying the various types, the locations where they can be placed, and the use of both a Web Server and a regular LAN connection for moving them between devices.
4. Define the methods for Certificate Revocation including the different types as well as identifying the Certificate Revocation Lists (CRLs), their storage locations on Certificate Server, and CDPs (Certificate Distribution Points) for access from the Internet.
5. Define the basic concepts associated with the Digital Security including the Public Key Infrastructure, Symmetrical Encryption, Digital Signatures, and the use of Hashes.
6. Identify the different types of Servers which are part of a Certificate Server Hierarchical Structure including the Root Server, Intermediate Servers, and Issuing Servers; define their location and function in the Server chain.
7. Identify the basic Active Directory structure, including the different components, Forest, Trees, Schema, Global catalog, and Domains, including the creation and configuration of a Domain Controller.
8. Identify the different methods for the creation of user accounts in an Active Directory Environment, defining the different user name configurations and differentiating the methods of joining computers

to the Active Directory forest/domain as workstations or member services, as well as the alternative methods for placement of these computer accounts.

9. Distinguish the three main types of Windows Groups including their characteristics and their uses, define the types and uses for the Delegation of Authority Tool, and identify the steps in the Organization Unit design and creation process.
10. Identify the methods for the implementation of Shadow Copies within the Active Directory structure, and then define the use and configuration of DNS for communication throughout the Active Directory Forest and Domains.
11. Identify the steps in setting up Publishing in Active Directory for printers, folders, and files, including the use of both local/network printers in the configurations and the use of the FIND tool for locating them at the client end.
12. Identify the steps required to implement a Group Policy, using various tools, and demonstrate an understanding of the structure of these policies, such as Computer Configuration, User Configuration, with emphasis on differences between the two Default Policies: Domain Policy and Domain Controller Policy.
13. Identify the various types of Group Policy security settings and the auditing of them with both Basic Auditing and Advanced Auditing, using Authentication as well as Object Access for their configuration and implementation.
14. Identify the uses of the RSOP (Resultant Set of Policy) tool in the testing of Group Policy application and the importance of using it at the client, both to see that the policy got there, and that it was configured correctly.
15. Define the group policies used to manage user desktop settings and other user configurations including the use of loopback policies to provide a standard desktop; identify the means of testing inheritance of the policies with various implementations.
16. Distinguish the use of group policies for implementing folder redirection to provide central storage of user document, for using logon/logoff scripts to set up a User Environment, and for software deployment using either assigned or published MSI files.
17. Define the procedure for creating a Child Domain and identify the five FSMO roles performed by Domain Controllers within a domain or within the forest, plus configure a transfer of one of the domain roles from the forest root domain controller to a child domain controller.
18. Identify and configure the functional levels within an Active Directory forest through the use of promotion techniques on both the forest root and child domain controllers.
19. Distinguish between the logical and physical representations of Active Directory, defining Sites, Site Links, Subnets, Replication Times, Dates, and Costs as well as describing the function of the Bridgehead Server.
20. Define the steps required to implement a second site within a multiple Domain Active Directory Forest, including the use of separate subnets, the implementation of a simulated routed connection and the configuration of a replication schedule.
21. Define the various forms of trust relationships within and between Active Directory forests including Cross-Forest, External, Shortcut, etc. as well as the implementation and configuration of an external trust between two domains.
22. Define the characteristics of the following advanced security concepts, including access-based enumeration, file screening, and encryption as well as software restrictions and AppLocker to prevent the install or executing of unwanted applications.
23. Identify the key components of Dynamic Access Control, including identifying data by using automatic and manual classification of files, controlling access to files by applying safety-net policies controlled centrally, and auditing access to files by using central audit policies for compliance reporting and forensic analysis.
24. Define Rights Management characteristics, including the use of encryption with a form of selective functionality denial for limiting access to documents such as corporate e-mail, Word documents, and web pages, as well as limiting the operations authorized users can perform on them.
25. Describe the characteristics of federation services, including browser cookies which can provide a user with a single sign on (SSO) to multiple separate LDAP services through secure sharing of identity information between trusted business partners across an extranet.

New Resources for Course

Course Textbooks/Resources

Textbooks

Warren, Andrew. *Identity with Windows Server 2016*, 1st ed. Microsoft, 2017, ISBN: 0735698813.

Manuals

Periodicals

Software

Equipment/Facilities

Level III classroom

Reviewer	Action	Date
Faculty Preparer:		
Michael Kidd	*Faculty Preparer*	*Oct 15, 2021*
Department Chair/Area Director:		
Cyndi Millns	*Recommend Approval*	*Nov 10, 2021*
Dean:		
Eva Samulski	*Recommend Approval*	*Nov 10, 2021*
Curriculum Committee Chair:		
Randy Van Wagnen	*Recommend Approval*	*Dec 14, 2021*
Assessment Committee Chair:		
Shawn Deron	*Recommend Approval*	*Jan 30, 2022*
Vice President for Instruction:		
Kimberly Hurns	*Approve*	*Jan 30, 2022*

Washtenaw Community College Comprehensive Report

CNT 224 Identity with Windows Server 2016
Effective Term: Spring/Summer 2018

Course Cover

Division: Business and Computer Technologies
Department: Computer Instruction
Discipline: Computer Networking Technology
Course Number: 224
Org Number: 13400
Full Course Title: Identity with Windows Server 2016
Transcript Title: Identity with Win Server 2016
Is Consultation with other department(s) required: No
Publish in the Following: College Catalog , Time Schedule , Web Page
Reason for Submission: Course Change
Change Information:
Course title
Course description
Outcomes/Assessment
Objectives/Evaluation
Other:
Rationale: The three Microsoft MCSA Certifications have totally changed for the 2016 version of Windows Server. The emphasis with the 3rd certification (which CNT224 aligns to) is now "Identity with Server 2016" (Basically all aspects of Active Directory) in contrast to the Windows Server 2012 version which covered topics that have now been moved to the other two certifications. Also, a considerable number of new features have been added, resulting in additional material to incorporate into this version of the course.
Proposed Start Semester: Spring/Summer 2018
Course Description: This course is part of a series of courses that provide the skills and knowledge necessary to manage and maintain the core infrastructure required for a Windows Server 2016 environment, and lays a foundation in the preparation for the Windows Server 2016 MCSA certification. Topics include all aspects of active directory and includes initial A.D. and DNS installations, as well as creating and managing users, groups, and computers. Group policies are emphasized which include security policies, auditing, inheritance, software installations, folder redirection, logon scripts, and printer installations. Also covered are dynamic access control, trusts, sites, certificate server, and delegation. The title of this course was previously Configuring Advanced Windows Server 2012 Services.

Course Credit Hours

Variable hours: No
Credits: 4
Lecture Hours: Instructor: 60 **Student:** 60
Lab: Instructor: 0 **Student:** 0
Clinical: Instructor: 0 **Student:** 0

Total Contact Hours: Instructor: 60 **Student:** 60
Repeatable for Credit: NO
Grading Methods: Letter Grades
Audit
Are lectures, labs, or clinicals offered as separate sections?: NO (same sections)

College-Level Reading and Writing

College-level Reading & Writing

College-Level Math

No Level Required

Requisites

General Education

General Education Area 7 - Computer and Information Literacy

Assoc in Arts - Comp Lit
Assoc in Applied Sci - Comp Lit
Assoc in Science - Comp Lit

Request Course Transfer

Proposed For:

Student Learning Outcomes

1. Identify the concepts behind Windows Certificate Server including Server installation and configuration, issuance of both Web Server and client certificates, revocation of certificates, and the process for importing and exporting certificates.

   Assessment 1

   Assessment Tool: Written exam specifically created for the assessment
   Assessment Date: Fall 2020
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All course sections
   Number students to be assessed: All students
   How the assessment will be scored: A written test will be given that addresses both the outcomes and objectives listed in the syllabus. This test will be divided into sections, each identified with an outcome, and the questions in each section will address the respective objectives.
   Standard of success to be used for this assessment: Average of all students taking the test should equal or exceed 70% correct answers for all questions used in the assessment test. 70% or greater of the number of students taking the assessment test should equal to or exceed that 70% mark for all the questions in the assessment test. Outcome success: average of all student scores for each particular outcome's part of the test equal to or exceed 70%.
   Who will score and analyze the data: All departmental instructors who teach sections of this course

2. Identify the principles related to installing and configuring Active Directory Services, including identifying the various objects, the creation and management of domains and organizational units, user and computer accounts, user profiles, and the use of Windows groups as part of A.D. administration.

   Assessment 1

   Assessment Tool: Written exam specifically created for the assessment
   Assessment Date: Fall 2020
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All course sections
   Number students to be assessed: All students
   How the assessment will be scored: A written test will be given that addresses both the

outcomes and objectives listed in the syllabus. This test will be divided into sections, each identified with an outcome, and the questions in each section will address the respective objectives.
Standard of success to be used for this assessment: Average of all students taking the test should equal or exceed 70% correct answers for all questions used in the assessment test. 70% or greater of the number of students taking the assessment test should equal or exceed that 70% mark for all the questions in the assessment test. Outcome success: average of all student scores for each particular outcome's part of the test equal to or exceed 70%.
Who will score and analyze the data: All departmental instructors who teach sections of this course

3. Identify and define Active Directory Group Policy concepts which consist of security settings (including account and password policies, user rights and security options), Desktop Management, inheritance, Folder Redirection, Logon Scripts, software deployment, loopback policies and printer installations.

Assessment 1

Assessment Tool: Written Exam specifically created for the assessment
Assessment Date: Fall 2020
Assessment Cycle: Every Three Years
Course section(s)/other population: All course sections
Number students to be assessed: All students
How the assessment will be scored: A written test will be given that addresses both the outcomes and objectives listed in the syllabus. This test will be divided into sections, each identified with an outcome, and the questions in each section will address the respective objectives.
Standard of success to be used for this assessment: Average of all students taking the test should equal or exceed 70% correct answers for all questions used in the assessment test. 70% or greater of the number of students taking the assessment test should equal or exceed that 70% mark for all the questions in the assessment test. Outcome success: average of all student scores for each particular outcome's part of the test should equal to or exceed 70%.
Who will score and analyze the data: All departmental instructors who teach sections of this course

4. Identify the implementation of Advanced Active Directory concepts including sites, site links, inter-site domain replication, FSMO roles, functional levels, and distinguish the different types of A.D. trusts including cross-forest and external trusts.

Assessment 1

Assessment Tool: Written exam specifically created for the assessment
Assessment Date: Fall 2020
Assessment Cycle: Every Three Years
Course section(s)/other population: All course sections
Number students to be assessed: All students
How the assessment will be scored: A written test will be given that addresses both the outcomes and objectives listed in the syllabus. This test will be divided into sections, each identified with an outcome, and the questions in each section will address the respective objectives.
Standard of success to be used for this assessment: Average of all students taking the test should equal or exceed 70% correct answers for all questions used in the assessment test. 70% or greater of the number of students taking the assessment test should equal or exceed that 70% mark for all the questions in the assessment test. Outcome success: average of all student scores for each particular outcome's part of the test should equal to or exceed 70%.
Who will score and analyze the data: All departmental instructors who teach sections of this

course

5. Define the different types of Advanced Access Control including Federation Server, Rights Management Server, access-based enumeration, file screening, quotas, encryption, software restriction, AppLocker, and Dynamic Access Control.

Assessment 1

Assessment Tool: Written exam specifically created for the assessment
Assessment Date: Fall 2020
Assessment Cycle: Every Three Years
Course section(s)/other population: All course sections
Number students to be assessed: All students
How the assessment will be scored: A written test will be given that addresses both the outcomes and objectives listed in the syllabus. This test will be divided into sections, each identified with an outcome, and the questions in each section will address the respective objectives.
Standard of success to be used for this assessment: Average of all students taking the test should equal or exceed 70% correct answers for all questions used in the assessment test. 70% or greater of the number of students taking the assessment test should equal or exceed that 70% mark for all the questions in the assessment test. Outcome success: average of all student scores for each particular outcome's part of the test should equal to or exceed 70%.
Who will score and analyze the data: All departmental instructors who teach sections of this course

Course Objectives

1. Define the installation procedures associated with the installation of Windows Certificate Server Authorities for both Standalone and Enterprise Types including the proper naming and generation of the self-signed root certificates.
2. Identify the methods for issuing both Server and Client certificates include the various alternatives for requesting, approving, and retrieving them and distinguish between the differences between the two types.
3. Define the methods for Exporting and Importing Certificates/Public Keys with/without the Private Key, including identifying the various types, the locations where they can be placed, and the use of both a Web Server and a regular LAN connection for moving them between devices.
4. Define the methods for Certificate Revocation including the different types as well as identifying the Certificate Revocation Lists (CRL's), their Storage locations on Certificate Server, and CDP's (Certificate Distribution Points)for access from the Internet.
5. Define the basic concepts associated with the Digital Security including the Public Key Infrastructure, Symmetrical Encryption, Digital Signatures, and the use of Hashes.
6. Identify the different types of Servers which are part of a Certificate Server Hierarchical Structure including the Root Server, Intermediate Servers, and Issuing Servers plus define their location and function in the Server chain.
7. Identify the basic Active Directory structure, including the different components, Forest, Trees, Schema, Global catalog,and Domains including the creation and configuration of a Domain Controller.
8. Identify the different methods for creation of user accounts in an Active Directory Environment, defining the different user name configurations and differentiate the methods of joining computers to the Active Directory forest/domain as workstations or member services,as well as the alternative methods for placement of these computer accounts.
9. Distinguish the three main types of Windows Groups including their characteristics and their uses, define the types and uses for the Delegation of Authority Tool, and identify the steps in the Organization Unit design and creation process.
10. Identify the methods for the implementation of Shadow Copies within the Active Directory structure, and then define the use and configuration of DNS for communication throughout the Active Directory

Forest and Domains.

11. Identify the steps in setting up Publishing in Active Directory for printers, folders, and files, including the use of both local/network printers in the configurations and the use of the FIND tool for locating them at the client end.
12. Identify the steps required to implement a Group Policy, using various tools, and demonstrate an understanding of the structure of these policies, such as Computer Configuration, User Configuration, with emphasis on differences between the two Default Policies: Domain Policy and Domain Controller Policy.
13. Identify the various types of Group Policy security settings and the auditing of them with both Basic Auditing and Advanced Auditing,using Authentication as well as Object Access for their configuration and implementation.
14. Identify the uses of the RSOP (Resultant Set of Policy) tool in the testing of Group Policy application and the importance of using it at the client, both to see that the policy got there, and that it was configured correctly.
15. Define the group policies used to manage user desktop settings and other user configurations including the use of loopback policies to provide a standard desktop and identify the means of testing inheritance of the policies with various implementations.
16. Distinguish the use of group policies for implementing folder redirection to provide central storage of user document, for using logon/logoff scripts to set up a User Environment, and for software deployment using either assigned or published MSI files.
17. Define the procedure for creating a Child Domain and identify the five FSMO roles performed by Domain Controllers within a domain or within the forest, plus configure a transfer of one of the domain roles from the forest root domain controller to a child domain controller.
18. Identify and configure the functional levels within an Active Directory forest through the use of promotion techniques on both the forest root and child domain controllers, with the goal of raising the forest and domain levels from the 2000 mode up to the 2016 mode.
19. Distinguish between the logical and physical representations of Active Directory, defining Sites, Site Links, Subnets, Replication Times, Dates, and Costs as well as describing the function of the Bridgehead Server.
20. Define the steps required to implement a second site within a multiple Domain Active Directory Forest, including the use of separate subnets, the implementation of a simulated routed connection and the configuration of a replication schedule.
21. Define the various forms of trust relationships within and between Active Directory forests including Cross-Forest, External, Shortcut, etc. as well as the implementation and configuration of an external trust between two domains.
22. Define the characteristics of the following advanced security concepts, including access-based enumeration, file screening, and encryption as well as software restrictions and AppLocker to prevent the install or executing of unwanted applications.
23. Identify the key components of Dynamic Access Control, including identifying data by using automatic and manual classification of files, controlling access to files by applying safety-net policies controlled centrally, and auditing access to files by using central audit policies for compliance reporting and forensic analysis.
24. Define Rights Management characteristics, including the use of encryption with a form of selective functionality denial for limiting access to documents such as corporate e-mail, Word documents, and web pages, as well as limiting the operations authorized users can perform on them.
25. Describe the characteristics of federation services, including browser cookies which can provide a user with a single sign on (SSO) to multiple separate LDAP services through secure sharing of identity information between trusted business partners across an extranet.

New Resources for Course

Course Textbooks/Resources

Textbooks

Warren, Andrew. *Identity with Windows Server 2016*, 1st ed. Microsoft, 2017, ISBN: 0735698813.

Manuals

Reichert, W.. CNT 224 Lab Projects & Lab Questions, Huron Valley Publishers, 04-30-2010

Periodicals

Software

Equipment/Facilities

Level III classroom

Reviewer	Action	Date
Faculty Preparer:		
William Reichert	*Faculty Preparer*	*Aug 25, 2017*
Department Chair/Area Director:		
Philip Geyer	*Recommend Approval*	*Sep 18, 2017*
Dean:		
Eva Samulski	*Recommend Approval*	*Sep 19, 2017*
Curriculum Committee Chair:		
Lisa Veasey	*Recommend Approval*	*Dec 11, 2017*
Assessment Committee Chair:		
Michelle Garey	*Recommend Approval*	*Dec 20, 2017*
Vice President for Instruction:		
Kimberly Hurns	*Approve*	*Dec 20, 2017*