

TestOut[®]

TestOut Server Pro 2016: Identity – English 4.0.x

Objective Mappings:

TestOut Server Pro 2016: Identity
Microsoft 70-742

Contents

This document contains four objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to TestOut Server Pro 2016: Identity Objective	3
Objective Mapping: TestOut Server Pro 2016: Identity Objective to LabSim Section	6
Objective Mapping: LabSim Section to Microsoft 70-742 Objective	13
Objective Mapping: Microsoft 70-742 Objective to TestOut Section	19

Objective Mapping: LabSim Section to TestOut Server Pro 2016: Identity Objective

The TestOut Server Pro 2016: Identity course and certification exam cover the following TestOut Server Pro 2016: Identity objectives:

#	Domain	Section
1.0	Active Directory Domain Services	
1.1	Manage Active Directory 1.1.1 Backup and restore Active Directory 1.1.2 Manage a Read Only Domain Controller (RODC) 1.1.3 Raise functional levels 1.1.4 Raise the domain and/or forest levels	1.4 2.1 4.1, 4.3
1.2	Manage Active Directory sites 1.2.1 Configure sites 1.2.2 Manage sites, subnets, and site links	2.1
1.3	Manage Active Directory replication 1.3.1 Configure intrasite replication 1.3.2 Configure intersite replication	2.3
1.4	Manage Flexible Single-Master Operation (FSMO) roles and global catalog servers 1.4.1 Configure global catalog servers 1.4.2 Transfer RID and PDC masters 1.4.3 Transfer infrastructure masters 1.4.4 Troubleshoot operations masters 1.4.5 Enable Universal Group Membership Caching (UGMC)	2.2
1.5	Manage Active Directory trusts 1.5.1 Design trusts	2.4

	1.5.2 Create forest root, cross-forest, external, shortcut, and realm trusts	
2.0	Active Directory Objects	
2.1	Manage organizational units 2.1.1 Create organizational units (OUs) 2.1.2 Delete organizational units (OUs)	3.1
2.2	Manage computers 2.2.1 Create computer accounts	3.2
2.3	Manage Active Directory user accounts 2.3.1 Create user accounts 2.3.2 Manage user accounts	3.3, 3.5, 3.6, 3.7
2.4	Manage groups 2.4.1 Create global groups 2.4.2 Create a distribution group 2.4.3 Change the group scope 2.4.4 Implement a group strategy	3.4
3.0	Group Policy	
3.1	Manage Group Policy objects (GPOs) 3.1.1 Control GPO inheritance 3.1.2 Configure a password replication policy 3.1.3 Import a GPO 3.1.4 Backup a GPO 3.1.5 Restore a GPO	1.4 5.2, 5.7, 5.9

3.2	<p>Deploy software using group policy</p> <p>3.2.1 Assign software 3.2.2 Deploy software 3.2.3 Deploy desktop shortcuts</p>	5.3, 5.8
3.3	<p>Manage group policies</p> <p>3.3.1 Delegate administrative control 3.3.2 Configure browser settings in a GPO 3.3.3 Configure power options in a GPO</p>	3.7 5.2, 5.8
3.4	<p>Manage security policies</p> <p>3.4.1 Configure security settings with group policy 3.4.2 Configure password settings with group policy</p>	5.5, 5.6
4.0	Certificate Services and Rights Management Services	
4.1	<p>Install and configure certificates</p> <p>4.1.1 Manage certificates 4.1.2 Manage certificate revocation 4.1.3 Configure templates for autoenrollment 4.1.4 Enable autoenrollment for the domain 4.1.5 Create certificates for smart cards 4.1.6 Require smart cards for logon</p>	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7
4.2	<p>Manage AD RMS</p> <p>4.2.1 Configure AD RMS templates 4.2.2 Configure AD RMS exclusions</p>	6.2 8.2, 8.3

Objective Mapping: TestOut Server Pro 2016: Identity Objective to LabSim Section

The TestOut Server Pro 2016: Identity course covers the following TestOut Server Pro 2016: Identity exam objectives:

Section	Title	Objectives
0.0	Introduction	
0.1	Server Pro 2016: Identity Introduction	
0.2	The TestOut Lab Simulator	
1.0	Install Active Directory	
1.1	Active Directory Overview	
1.2	Install Active Directory	
1.3	Install Additional Domain Controllers	
1.4	Read-Only Domain Controllers (RODCs)	1.1 Manage Active Directory 1.1.2 Manage a Read Only Domain Controller (RODC) 3.1 Manage Group Policy objects (GPOs) 3.1.2 Configure a password replication policy
1.5	Domain Controller Cloning	
2.0	Plan Active Directory	
2.1	Active Directory Sites	1.1 Manage Active Directory

		<p>1.1.1 Backup and restore Active Directory</p> <p>1.2 Manage Active Directory sites</p> <p>1.2.1 Configure sites</p> <p>1.2.2 Manage sites, subnets, and site links</p>
2.2	FSMO Roles and Global Catalog Servers	<p>1.4 Manage Flexible Single-Master Operation (FSMO) roles and global catalog servers</p> <p>1.4.1 Configure global catalog servers</p> <p>1.4.2 Transfer RID and PDC masters</p> <p>1.4.3 Transfer infrastructure masters</p> <p>1.4.4 Troubleshoot operations masters</p> <p>1.4.5 Enable Universal Group Membership Caching (UGMC)</p>
2.3	Active Directory Replication	<p>1.3 Manage Active Directory replication</p> <p>1.3.1 Configure intrasite replication</p> <p>1.3.2 Configure intersite replication</p>
2.4	Active Directory Trusts	<p>1.5 Manage Active Directory trusts</p> <p>1.5.1 Design trusts</p> <p>1.5.2 Create forest root, cross-forest, external, shortcut, and realm trusts</p>
3.0	Manage Active Directory Objects	
3.1	Active Directory Organizational Units	<p>2.1 Manage organizational units</p> <p>2.1.1 Create organizational units (OUs)</p> <p>2.1.2 Delete organizational units (OUs)</p>
3.2	Active Directory Computers	2.2 Manage computers

		2.2.1 Create computer accounts
3.3	Active Directory Users	2.3 Manage Active Directory user accounts 2.3.1 Create user accounts 2.3.2 Manage user accounts
3.4	Active Directory Groups	2.4 Manage groups 2.4.1 Create global groups 2.4.2 Create a distribution group 2.4.3 Change the group scope 2.4.4 Implement a group strategy
3.5	Active Directory Service Accounts	2.3 Manage Active Directory user accounts 2.3.1 Create user accounts 2.3.2 Manage user accounts
3.6	Active Directory Bulk Operations	2.3 Manage Active Directory user accounts 2.3.2 Manage user accounts
3.7	Delegation of Control	2.3 Manage Active Directory user accounts 2.3.2 Manage user accounts 3.3 Manage group policies 3.3.1 Delegate administrative control
4.0	Managing the Active Directory Database	
4.1	Active Directory Backup and Restore	1.1 Manage Active Directory

		1.1.1 Backup and restore Active Directory
4.2	Manage the Active Directory Database	
4.3	Functional Levels	1.1 Manage Active Directory 1.1.3 Raise functional levels 1.1.4 Raise the domain and/or forest levels
5.0	Group Policy	
5.1	Group Policy Overview	
5.2	Group Policy Inheritance	3.1 Manage Group Policy objects (GPOs) 3.1.1 Control GPO inheritance 3.3 Manage group policies 3.3.1 Delegate administrative control
5.3	Deploy Software with Group Policy	3.2 Deploy software using group policy 3.2.1 Assign software 3.2.2 Deploy software 3.2.3 Deploy desktop shortcuts
5.4	Manage Windows Settings with Group Policy	
5.5	Manage Security Settings with Group Policy	3.4 Manage security policies 3.4.1 Configure security settings with group policy
5.6	Managing Passwords with Group Policy	3.4 Manage security policies

		3.4.2 Configure password settings with group policy
5.7	Group Policy Administrative Templates	3.1 Manage Group Policy objects (GPOs) 3.1.3 Import a GPO
5.8	Group Policy Preferences	3.2 Deploy software using group policy 3.2.3 Deploy desktop shortcuts 3.3 Manage group policies 3.3.2 Configure browser settings in a GPO 3.3.3 Configure power options in a GPO
5.9	Group Policy Backup	3.1 Manage Group Policy objects (GPOs) 3.1.3 Import a GPO 3.1.4 Backup a GPO 3.1.5 Restore a GPO
5.10	Troubleshooting Group Policy	
6.0	AD Certificate Services	
6.1	Install AD Certificate Services	4.1 Install and configure certificates 4.1.1 Manage certificates
6.2	Managing Certificates	4.1 Install and configure certificates 4.1.1 Manage certificates 4.1.2 Manage certificate revocation 4.2 Manage AD RMS

		<ul style="list-style-type: none"> 4.2.1 Configure AD RMS templates 4.2.2 Configure AD RMS exclusions
6.3	Certificate Enrollment	<ul style="list-style-type: none"> 4.1 Install and configure certificates <ul style="list-style-type: none"> 4.1.3 Configure templates for autoenrollment 4.1.4 Enable autoenrollment for the domain 4.1.5 Create certificates for smart cards 4.1.6 Require smart cards for logon
6.4	Certificate Revocation	<ul style="list-style-type: none"> 4.1 Install and configure certificates <ul style="list-style-type: none"> 4.1.2 Manage certificate revocation
6.5	Certificate Services Administration	<ul style="list-style-type: none"> 4.1 Install and configure certificates <ul style="list-style-type: none"> 4.1.1 Manage certificates
6.6	Key Archival and Recovery	<ul style="list-style-type: none"> 4.1 Install and configure certificates <ul style="list-style-type: none"> 4.1.1 Manage certificates
6.7	Back Up and Recover Certificate Services	<ul style="list-style-type: none"> 4.1 Install and configure certificates <ul style="list-style-type: none"> 4.1.1 Manage certificates
7.0	Active Directory Federation Services (AD FS)	
7.1	AD FS Installation	
7.2	AD FS Trusts	
7.3	Device Registration and Multi-Factor Authentication	

7.4	AD FS Integration	
7.5	Implement Web Application Proxy (WAP)	
8.0	Active Directory Rights Management Services (AD RMS)	
8.1	AD RMS Installation	
8.2	AD RMS Templates	4.2 Manage AD RMS 4.2.1 Configure AD RMS templates
8.3	AD RMS Exclusions	4.2 Manage AD RMS 4.2.2 Configure AD RMS exclusions
8.4	AD RMS Back Up and Restore	
A.0	TestOut Server Pro 2016: Identity - Practice Exams	
A.1	Prepare for Certification	
A.2	TestOut Server Pro 2016: Identity Question Review	
B.0	Microsoft 70-742 Practice Exams	
B.1	Preparing for Certification	
B.2	Microsoft 70-742 Question Review (20 Random Questions)	
B.3	Microsoft 70-742 Question Review (All Questions)	

Objective Mapping: LabSim Section to Microsoft 70-742 Objective

The TestOut Server Pro 2016: Identity course and certification exam cover the following Microsoft Identity with Windows Server 2016 objectives:

#	Domain	Section
1.0	Install and Configure Active Directory Domain Services (AD DS)	
1.1	Install and configure domain controllers <ul style="list-style-type: none"> 1.1.1 Install a new forest 1.1.2 Add or remove a domain controller from a domain 1.1.3 Upgrade a domain controller 1.1.4 Install AD DS on a Server Core installation 1.1.5 Install a domain controller from Install from Media (IFM) 1.1.6 Resolve DNS SRV record registration issues 1.1.7 Configure a global catalog server 1.1.8 Transfer and seize operations master roles 1.1.9 Install and configure a read-only domain controller (RODC) 1.1.10 Configure domain controller cloning 	1.1, 1.2, 1.3, 1.4, 1.5 2.2
1.2	Create and manage Active Directory users and computers <ul style="list-style-type: none"> 1.2.1 Automate the creation of Active Directory accounts 1.2.2 Create, copy, configure, and delete users and computers 1.2.3 Configure templates 1.2.4 Perform bulk Active Directory operations 1.2.5 Configure user rights 1.2.6 Implement offline domain join 1.2.7 Manage inactive and disabled accounts 1.2.8 Automate unlocking of disabled accounts 1.2.9 Automate password resets 	3.2, 3.3, 3.6, 3.7
1.3	Create and manage Active Directory groups and organizational units (OUs) <ul style="list-style-type: none"> 1.3.1 Configure group nesting 1.3.2 Convert groups <ul style="list-style-type: none"> o 1.3.2.1 Security 	3.1, 3.4

	<ul style="list-style-type: none"> ○ 1.3.2.2 Universal ○ 1.3.2.3 Domain local ○ 1.3.2.4 Global <p>1.3.3 Manage group membership using Group Policy</p> <p>1.3.4 Enumerate group membership</p> <p>1.3.5 Automate group membership management using Windows PowerShell</p> <p>1.3.6 Delegate the creation and management of Active Directory groups and OUs</p> <p>1.3.7 Manage default Active Directory containers</p> <p>1.3.8 Create, copy, configure, and delete groups and OUs</p>	
2.0	Manage and Maintain AD DS	
2.1	<p>Configure service authentication and account policies</p> <ul style="list-style-type: none"> 2.1.1 Create and configure Service Accounts 2.1.2 Create and configure Group Managed Service Accounts (gMSAs) 2.1.3 Configure Kerberos Constrained Delegation (KCD) 2.1.4 Manage Service Principal Names (SPNs) 2.1.5 Configure virtual accounts 2.1.6 Configure domain and local user password policy settings 2.1.7 Configure and apply Password Settings Objects (PSOs) 2.1.8 Delegate password settings management 2.1.9 Configure account lockout policy settings 2.1.10 Configure Kerberos policy settings within Group Policy 2.1.11 Configure Authentication Policies and Authentication Policy Silos 	<p>3.5, 3.7</p> <p>4.1</p>
2.2	<p>Maintain Active Directory</p> <ul style="list-style-type: none"> 2.2.1 Back up Active Directory and SYSVOL 2.2.2 Manage Active Directory offline 2.2.3 Perform offline defragmentation of an Active Directory database 2.2.4 Clean up metadata 2.2.5 Configure Active Directory snapshots 2.2.6 Perform object- and container-level recovery 2.2.7 Perform Active Directory restore 2.2.8 Configure and restore objects by using the Active Directory Recycle Bin 2.2.9 Configure replication to Read-Only Domain Controllers (RODCs) 2.2.10 Configure Password Replication Policy (PRP) for RODC 2.2.11 Monitor and manage replication 	<p>1.4</p> <p>2.3</p> <p>4.1, 4.2</p>

	2.2.12 Upgrade SYSVOL replication to Distributed File System Replication (DFSR)	
2.3	<p>Configure Active Directory in a complex enterprise environment</p> <p>2.3.1 Configure a multi-domain and multi-forest Active Directory infrastructure</p> <p>2.3.2 Deploy Windows Server 2016 domain controllers within a preexisting Active Directory environment</p> <p>2.3.3 Upgrade existing domains and forests</p> <p>2.3.4 Configure domain and forest functional levels</p> <p>2.3.5 Configure multiple user principal name (UPN) suffixes</p> <p>2.3.6 Configure external, forest, shortcut, and realm trusts</p> <p>2.3.7 Configure trust authentication</p> <p>2.3.8 Configure SID filtering</p> <p>2.3.9 Configure name suffix routing</p> <p>2.3.10 Configure sites and subnets</p> <p>2.3.11 Create and configure site links</p> <p>2.3.12 Manage site coverage</p> <p>2.3.13 Manage registration of SRV records</p> <p>2.3.14 Move domain controllers between sites</p>	2.1, 2.4 4.3
3.0	Create and Manage Group Policy	
3.1	<p>Create and manage Group Policy Objects (GPOs)</p> <p>3.1.1 Configure a central store</p> <p>3.1.2 Manage starter GPOs</p> <p>3.1.3 Configure GPO links</p> <p>3.1.4 Configure multiple local Group Policies</p> <p>3.1.5 Back up, import, copy, and restore GPOs</p> <p>3.1.6 Create and configure a migration table</p> <p>3.1.7 Reset default GPOs</p> <p>3.1.8 Delegate Group Policy management</p> <p>3.1.9 Detect health issues using the Group Policy Infrastructure Status page</p>	5.1, 5.9, 5.10
3.2	<p>Configure Group Policy processing</p> <p>3.2.1 Configure processing order and precedence</p> <p>3.2.2 Configure blocking of inheritance</p> <p>3.2.3 Configure enforced policies</p> <p>3.2.4 Configure security filtering and Windows Management Instrumentation (WMI) filtering</p>	5.2, 5.10

	<ul style="list-style-type: none"> 3.2.5 Configure loopback processing 3.2.6 Configure and manage slow-link processing and Group Policy caching 3.2.7 Configure client-side extension (CSE) behavior 3.2.8 Force a Group Policy update 	
3.3	<p>Configure Group Policy settings</p> <ul style="list-style-type: none"> 3.3.1 Configure software installation 3.3.2 Configure folder redirection 3.3.3 Configure scripts 3.3.4 Configure administrative templates 3.3.5 Import security templates 3.3.6 Import a custom administrative template file 3.3.7 Configure filtering for administrative template 	5.3, 5.4, 5.7
3.4	<p>Configure Group Policy preferences</p> <ul style="list-style-type: none"> 3.4.1 Configure printer preferences 3.4.2 Define network drive mappings 3.4.3 Configure power options 3.4.4 Configure custom registry settings 3.4.5 Configure Control Panel settings 3.4.6 Configure Internet Explorer settings 3.4.7 Configure file and folder deployment 3.4.8 Configure shortcut deployment 3.4.9 Configure item-level targeting 	5.8
4.0	Implement Active Directory Certificate Services (AD CS)	
4.1	<p>Install and configure AD CS</p> <ul style="list-style-type: none"> 4.1.1 Install Active Directory Integrated Enterprise Certificate Authority (CA) 4.1.2 Install offline root and subordinate CAs 4.1.3 Install standalone CAs 4.1.4 Configure Certificate Revocation List (CRL) distribution points 4.1.5 Install and configure Online Responder 4.1.6 Implement administrative role separation 4.1.7 Configure CA backup and recovery 	6.1, 6.4, 6.5, 6.7

4.2	<p>Manage certificates</p> <ul style="list-style-type: none"> 4.2.1 Manage certificate templates 4.2.2 Implement and manage certificate deployment, validation, and revocation 4.2.3 Manage certificate renewal 4.2.4 Manage certificate enrolment and renewal for computers and users using Group Policies 4.2.4 Configure and manage key archival and recovery 	6.2, 6.3, 6.4, 6.6
5.0	Implement Identity Federation and Access Solutions	
5.1	<p>Install and configure Active Directory Federation Services (AD FS)</p> <ul style="list-style-type: none"> 5.1.1 Upgrade and migrate previous AD FS workloads to Windows Server 2016 5.1.2 Implement claims-based authentication, including Relying Party Trusts 5.1.3 Configure authentication policies 5.1.4 Configure multi-factor authentication 5.1.5 Implement and configure device registration 5.1.6 Integrate AD FS with Microsoft Passport 5.1.7 Configure for use with Microsoft Azure and Office 365 5.1.8 Configure AD FS to enable authentication of users stored in LDAP directories 	7.1, 7.2, 7.3, 7.4
5.2	<p>Implement Web Application Proxy (WAP)</p> <ul style="list-style-type: none"> 5.2.1 Install and configure WAP 5.2.2 Implement WAP in pass-through mode 5.2.3 Implement WAP as AD FS proxy 5.2.4 Integrate WAP with AD FS 5.2.5 Configure AD FS requirements 5.2.6 Publish web apps via WAP 5.2.7 Publish Remote Desktop Gateway applications 5.2.8 Configure HTTP to HTTPS redirects 5.2.9 Configure internal and external Fully Qualified Domain Names (FQDNs) 	7.5
5.3	<p>Install and configure Active Directory Rights Management Services (AD RMS)</p> <ul style="list-style-type: none"> 5.3.1 Install a licensor certificate AD RMS server 5.3.2 Manage AD RMS Service Connection Point (SCP) 5.3.3 Manage AD RMS templates 5.3.4 Configure Exclusion Policies 	8.1, 8.2, 8.3, 8.4

	5.3.5 Back up and restore AD RMS	
--	----------------------------------	--

Objective Mapping: Microsoft 70-742 Objective to TestOut Section

The TestOut Server Pro 2016: Identity course covers the following Microsoft Identity with Windows Server 2016 exam objectives:

Section	Title	Objectives
0.0	Introduction	
0.1	Server Pro 2016: Identity Introduction	
0.2	The TestOut Lab Simulator	
1.0	Install Active Directory	
1.1	Active Directory Overview	1.1 Install and configure domain controllers 1.1.1 Install a new forest
1.2	Install Active Directory	1.1 Install and configure domain controllers 1.1.1 Install a new forest 1.1.3 Upgrade a domain controller
1.3	Install Additional Domain Controllers	1.1 Install and configure domain controllers 1.1.1 Install a new forest 1.1.2 Add or remove a domain controller from a domain 1.1.3 Upgrade a domain controller 1.1.4 Install AD DS on a Server Core installation 1.1.5 Install a domain controller from Install from Media (IFM)
1.4	Read-Only Domain Controllers (RODCs)	1.1 Install and configure domain controllers 1.1.9 Install and configure a read-only domain controller (RODC)

		<p>2.2 Maintain Active Directory</p> <p>2.2.9 Configure replication to Read-Only Domain Controllers (RODCs) 2.2.10 Configure Password Replication Policy (PRP) for RODC</p>
1.5	Domain Controller Cloning	<p>1.1 Install and configure domain controllers</p> <p>1.1.10 Configure domain controller cloning</p>
2.0	Plan Active Directory	
2.1	Active Directory Sites	<p>2.3 Configure Active Directory in a complex enterprise environment</p> <p>2.3.10 Configure sites and subnets</p>
2.2	FSMO Roles and Global Catalog Servers	<p>1.1 Install and configure domain controllers</p> <p>1.1.7 Configure a global catalog server 1.1.8 Transfer and seize operations master roles</p>
2.3	Active Directory Replication	<p>2.2 Maintain Active Directory</p> <p>2.2.11 Monitor and manage replication 2.2.12 Upgrade SYSVOL replication to Distributed File System Replication (DFSR)</p>
2.4	Active Directory Trusts	<p>2.3 Configure Active Directory in a complex enterprise environment</p> <p>2.3.6 Configure external, forest, shortcut, and realm trusts 2.3.7 Configure trust authentication 2.3.8 Configure SID filtering</p>
3.0	Manage Active Directory Objects	

3.1	Active Directory Organizational Units	<p>1.3 Create and manage Active Directory groups and organizational units (OUs)</p> <p>1.3.7 Manage default Active Directory containers 1.3.8 Create, copy, configure, and delete groups and OUs</p>
3.2	Active Directory Computers	<p>1.2 Create and manage Active Directory users and computers</p> <p>1.2.2 Create, copy, configure, and delete users and computers 1.2.6 Implement offline domain join</p>
3.3	Active Directory Users	<p>1.2 Create and manage Active Directory users and computers</p> <p>1.2.1 Automate the creation of Active Directory accounts 1.2.2 Create, copy, configure, and delete users and computers 1.2.3 Configure templates 1.2.6 Implement offline domain join 1.2.7 Manage inactive and disabled accounts 1.2.8 Automate unlocking of disabled accounts 1.2.9 Automate password resets</p>
3.4	Active Directory Groups	<p>1.3 Create and manage Active Directory groups and organizational units (OUs)</p> <p>1.3.1 Configure group nesting 1.3.2 Convert groups</p> <p>1.3.2.1 Security 1.3.2.2 Universal 1.3.2.3 Domain local 1.3.2.4 Global</p> <p>1.3.3 Manage group membership using Group Policy 1.3.4 Enumerate group membership 1.3.5 Automate group membership management using Windows PowerShell 1.3.8 Create, copy, configure, and delete groups and OUs</p>
3.5	Active Directory Service Accounts	<p>2.1 Configure service authentication and account policies</p>

		<ul style="list-style-type: none"> 2.1.1 Create and configure Service Accounts 2.1.2 Create and configure Group Managed Service Accounts (gMSAs) 2.1.3 Configure Kerberos Constrained Delegation (KCD) 2.1.4 Manage Service Principal Names (SPNs) 2.1.5 Configure virtual accounts
3.6	Active Directory Bulk Operations	<p>1.2 Create and manage Active Directory users and computers</p> <ul style="list-style-type: none"> 1.2.1 Automate the creation of Active Directory accounts 1.2.2 Create, copy, configure, and delete users and computers 1.2.4 Perform bulk Active Directory operations 1.2.9 Automate password resets
3.7	Delegation of Control	<p>1.2 Create and manage Active Directory users and computers</p> <ul style="list-style-type: none"> 1.2.5 Configure user rights <p>2.1 Configure service authentication and account policies</p> <ul style="list-style-type: none"> 2.1.8 Delegate password settings management
4.0	Managing the Active Directory Database	
4.1	Active Directory Backup and Restore	<p>2.1 Configure service authentication and account policies</p> <ul style="list-style-type: none"> 2.1.1 Create and configure Service Accounts <p>2.2 Maintain Active Directory</p> <ul style="list-style-type: none"> 2.2.1 Back up Active Directory and SYSVOL 2.2.2 Manage Active Directory offline 2.2.5 Configure Active Directory snapshots 2.2.6 Perform object- and container-level recovery 2.2.7 Perform Active Directory restore 2.2.8 Configure and restore objects by using the Active Directory Recycle Bin

4.2	Manage the Active Directory Database	<p>2.2 Maintain Active Directory</p> <p>2.2.3 Perform offline defragmentation of an Active Directory database</p> <p>2.2.4 Clean up metadata</p>
4.3	Functional Levels	<p>2.3 Configure Active Directory in a complex enterprise environment</p> <p>2.3.4 Configure domain and forest functional levels</p>
5.0	Group Policy	
5.1	Group Policy Overview	<p>3.1 Create and manage Group Policy Objects (GPOs)</p> <p>3.1.3 Configure GPO links</p> <p>3.1.4 Configure multiple local Group Policies</p>
5.2	Group Policy Inheritance	<p>3.2 Configure Group Policy processing</p> <p>3.2.1 Configure processing order and precedence</p> <p>3.2.2 Configure blocking of inheritance</p> <p>3.2.3 Configure enforced policies</p> <p>3.2.4 Configure security filtering and Windows Management Instrumentation (WMI) filtering</p> <p>3.2.5 Configure loopback processing</p> <p>3.2.6 Configure and manage slow-link processing and Group Policy caching</p>
5.3	Deploy Software with Group Policy	<p>3.3 Configure Group Policy settings</p> <p>3.3.1 Configure software installation</p>
5.4	Manage Windows Settings with Group Policy	<p>3.3 Configure Group Policy settings</p> <p>3.3.2 Configure folder redirection</p> <p>3.3.3 Configure scripts</p>

5.5	Manage Security Settings with Group Policy	
5.6	Managing Passwords with Group Policy	
5.7	Group Policy Administrative Templates	3.3 Configure Group Policy settings 3.3.4 Configure administrative templates 3.3.5 Import security templates 3.3.6 Import a custom administrative template file 3.3.7 Configure filtering for administrative template
5.8	Group Policy Preferences	3.4 Configure Group Policy preferences 3.4.1 Configure printer preferences 3.4.2 Define network drive mappings 3.4.3 Configure power options 3.4.4 Configure custom registry settings 3.4.5 Configure Control Panel settings 3.4.6 Configure Internet Explorer settings 3.4.7 Configure file and folder deployment 3.4.8 Configure shortcut deployment
5.9	Group Policy Backup	3.1 Create and manage Group Policy Objects (GPOs) 3.1.5 Back up, import, copy, and restore GPOs 3.1.6 Create and configure a migration table
5.10	Troubleshooting Group Policy	3.1 Create and manage Group Policy Objects (GPOs) 3.1.7 Reset default GPOs 3.1.9 Detect health issues using the Group Policy Infrastructure Status page 3.2 Configure Group Policy processing 3.2.8 Force a Group Policy update

6.0	AD Certificate Services	
6.1	Install AD Certificate Services	<p>4.1 Install and configure AD CS</p> <ul style="list-style-type: none"> 4.1.1 Install Active Directory Integrated Enterprise Certificate Authority (CA) 4.1.2 Install offline root and subordinate CAs 4.1.3 Install standalone CAs
6.2	Managing Certificates	<p>4.2 Manage certificates</p> <ul style="list-style-type: none"> 4.2.1 Manage certificate templates 4.2.2 Implement and manage certificate deployment, validation, and revocation 4.2.3 Manage certificate renewal 4.2.4 Manage certificate enrolment and renewal for computers and users using Group Policies
6.3	Certificate Enrollment	<p>4.2 Manage certificates</p> <ul style="list-style-type: none"> 4.2.3 Manage certificate renewal 4.2.4 Manage certificate enrolment and renewal for computers and users using Group Policies
6.4	Certificate Revocation	<p>4.1 Install and configure AD CS</p> <ul style="list-style-type: none"> 4.1.4 Configure Certificate Revocation List (CRL) distribution points 4.1.5 Install and configure Online Responder <p>4.2 Manage certificates</p> <ul style="list-style-type: none"> 4.2.2 Implement and manage certificate deployment, validation, and revocation
6.5	Certificate Services Administration	<p>4.1 Install and configure AD CS</p>

		4.1.6 Implement administrative role separation
6.6	Key Archival and Recovery	4.2 Manage certificates 4.2.4 Configure and manage key archival and recovery
6.7	Back Up and Recover Certificate Services	4.1 Install and configure AD CS 4.1.7 Configure CA backup and recovery
7.0	Active Directory Federation Services (AD FS)	
7.1	AD FS Installation	5.1 Install and configure Active Directory Federation Services (AD FS) 5.1.1 Upgrade and migrate previous AD FS workloads to Windows Server 2016
7.2	AD FS Trusts	5.1 Install and configure Active Directory Federation Services (AD FS) 5.1.2 Implement claims-based authentication, including Relying Party Trusts
7.3	Device Registration and Multi-Factor Authentication	5.1 Install and configure Active Directory Federation Services (AD FS) 5.1.3 Configure authentication policies 5.1.4 Configure multi-factor authentication 5.1.5 Implement and configure device registration
7.4	AD FS Integration	5.1 Install and configure Active Directory Federation Services (AD FS) 5.1.6 Integrate AD FS with Microsoft Passport 5.1.7 Configure for use with Microsoft Azure and Office 365 5.1.8 Configure AD FS to enable authentication of users stored in LDAP directories

7.5	Implement Web Application Proxy (WAP)	<p>5.2 Implement Web Application Proxy (WAP)</p> <ul style="list-style-type: none"> 5.2.1 Install and configure WAP 5.2.2 Implement WAP in pass-through mode 5.2.3 Implement WAP as AD FS proxy 5.2.4 Integrate WAP with AD FS 5.2.5 Configure AD FS requirements 5.2.6 Publish web apps via WAP 5.2.7 Publish Remote Desktop Gateway applications 5.2.8 Configure HTTP to HTTPS redirects 5.2.9 Configure internal and external Fully Qualified Domain Names (FQDNs)
8.0	Active Directory Rights Management Services (AD RMS)	
8.1	AD RMS Installation	<p>5.3 Install and configure Active Directory Rights Management Services (AD RMS)</p> <ul style="list-style-type: none"> 5.3.1 Install a licensor certificate AD RMS server 5.3.2 Manage AD RMS Service Connection Point (SCP)
8.2	AD RMS Templates	<p>5.3 Install and configure Active Directory Rights Management Services (AD RMS)</p> <ul style="list-style-type: none"> 5.3.3 Manage AD RMS templates
8.3	AD RMS Exclusions	<p>5.3 Install and configure Active Directory Rights Management Services (AD RMS)</p> <ul style="list-style-type: none"> 5.3.4 Configure Exclusion Policies
8.4	AD RMS Back Up and Restore	<p>5.3 Install and configure Active Directory Rights Management Services (AD RMS)</p> <ul style="list-style-type: none"> 5.3.5 Back up and restore AD RMS
A.0	TestOut Server Pro 2016: Identity - Practice Exams	

A.1	Prepare for Certification	
A.2	TestOut Server Pro 2016: Identity Question Review	
B.0	Microsoft 70-742 Practice Exams	
B.1	Preparing for Certification	
B.2	Microsoft 70-742 Question Review (20 Random Questions)	
B.3	Microsoft 70-742 Question Review (All Questions)	