Hewlett Packard Enterprise

MOC On-Demand: Identity with Windows Server 2016 (20742) H6LB7S

This course teaches IT professionals how to deploy and configure Active Directory Domain Services (AD DS) in a distributed environment, how to implement Group Policy, how to perform backup and restore, and how to monitor and troubleshoot Active Directory-related issues with Windows Server 2016. Additionally, this course teaches how to deploy other Active Directory server roles such as Active Directory Federation Services (AD FS) and Active Directory Certificate Services (AD CS).

Order details
• MS Order-ID: Q4P-00313
• MOD Duration: 180 day
Digital MOC included

Audience
This course is primarily intended for existing IT professionals who have some AD DS knowledge and experience, and who aim to develop knowledge about identity and access technologies in Windows Server 2016. This would typically include:

• AD DS administrators who are looking to train in identity and access technologies with Windows Server 2012 or Windows Server 2016
• System or infrastructure administrators with general AD DS experience and knowledge who are looking to cross-train in core and advanced identity and access technologies in Windows Server 2012 or Windows Server 2016

Prerequisites
Before attending this course, students must have:
• Some exposure to and experience with AD DS concepts and technologies in Windows Server 2012 or Windows Server 2016
• Experience working with and configuring Windows Server 2012 or Windows Server 2016
• Experience and an understanding of core networking technologies such as IP addressing, name resolution, and Dynamic Host Configuration Protocol (DHCP)
• Experience working with and an understanding of Microsoft Hyper-V and basic server virtualization concepts
• An awareness of basic security best practices
• Hands-on working experience with Windows client operating systems such as Windows 7, Windows 8, Windows 8.1, or Windows 10
• Basic experience with the Windows PowerShell command-line interface

Why HPE Education Services?
• IDC MarketScape leader 5 years running for IT education and training*
• Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
• Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
• Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
• Simplified purchase option with HPE Training Credits

*Realize Technology Value with Training, IDC Infographic 2017, Sponsored by HPE, October 2017

Course data sheet

HPE course number  H6LB7S
Course length  180 Days
Delivery mode  Self-paced
View schedule, local pricing, and register  View now
View related courses  View now

Realize Technology Value with Training, IDC Infographic 2017, Sponsored by HPE, October 2017

MOC On-Demand: Identity with Windows Server 2016 (20742) H6LB7S

This course teaches IT professionals how to deploy and configure Active Directory Domain Services (AD DS) in a distributed environment, how to implement Group Policy, how to perform backup and restore, and how to monitor and troubleshoot Active Directory-related issues with Windows Server 2016. Additionally, this course teaches how to deploy other Active Directory server roles such as Active Directory Federation Services (AD FS) and Active Directory Certificate Services (AD CS).

Order details
• MS Order-ID: Q4P-00313
• MOD Duration: 180 day
Digital MOC included

Audience
This course is primarily intended for existing IT professionals who have some AD DS knowledge and experience, and who aim to develop knowledge about identity and access technologies in Windows Server 2016. This would typically include:

• AD DS administrators who are looking to train in identity and access technologies with Windows Server 2012 or Windows Server 2016
• System or infrastructure administrators with general AD DS experience and knowledge who are looking to cross-train in core and advanced identity and access technologies in Windows Server 2012 or Windows Server 2016

Prerequisites
Before attending this course, students must have:
• Some exposure to and experience with AD DS concepts and technologies in Windows Server 2012 or Windows Server 2016
• Experience working with and configuring Windows Server 2012 or Windows Server 2016
• Experience and an understanding of core networking technologies such as IP addressing, name resolution, and Dynamic Host Configuration Protocol (DHCP)
• Experience working with and an understanding of Microsoft Hyper-V and basic server virtualization concepts
• An awareness of basic security best practices
• Hands-on working experience with Windows client operating systems such as Windows 7, Windows 8, Windows 8.1, or Windows 10
• Basic experience with the Windows PowerShell command-line interface

Why HPE Education Services?
• IDC MarketScape leader 5 years running for IT education and training*
• Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
• Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
• Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
• Simplified purchase option with HPE Training Credits

*Realize Technology Value with Training, IDC Infographic 2017, Sponsored by HPE, October 2017
## Detailed course outline

| Module 1: Installing and configuring domain controllers | • Overview of AD DS  
• Overview of AD DS domain controllers | • Deploying a domain controller |
|--------------------------------------------------------|-------------------------------------------------|-------------------------------------------------|
| Module 2: Managing objects in AD DS | • Managing user accounts  
• Managing groups in AD DS  
• Managing computer objects in AD DS | • Using Windows PowerShell for AD DS administration  
• Implementing and managing OUs |
| Module 3: Advanced AD DS infrastructure management | • Overview of advanced AD DS deployments  
• Deploying a distributed AD DS environment | • Configuring AD DS trusts |
| Module 4: Implementing and administering AD DS sites and replication | • Overview of AD DS replication  
• Configuring AD DS sites | • Configuring and monitoring AD DS replication |
| Module 5: Implementing Group Policy | • Introducing Group Policy  
• Implementing and administering GPOs | • Group Policy scope and Group Policy processing  
• Troubleshooting the application of GPOs |
| Module 6: Managing user settings with Group Policy | • Implementing administrative templates  
• Configuring folder redirection, software installation, and scripts | • Configuring Group Policy preferences |
| Module 7: Securing Active Directory Domain Services | • Securing domain controllers  
• Implementing account security | • Implementing audit authentication  
• Configuring managed service accounts |
| Module 8: Deploying and managing AD CS | • Deploying CAs  
• Administering CAs | • Troubleshooting and maintaining CAs |
| Module 9: Deploying and managing certificates | • Deploying and managing certificate templates  
• Managing certificate deployment, revocation, and recovery | • Using certificates in a business environment  
• Implementing and managing smart cards |
| Module 10: Implementing and administering AD FS | • Overview of AD FS  
• AD FS requirements and planning | • Deploying and configuring AD FS  
• Overview of Web Application Proxy |
| Module 11: Implementing and administering AD RMS | • Overview of AD RMS  
• Deploying and managing an AD RMS infrastructure | • Configuring AD RMS content protection |
| Module 12: Implementing AD DS synchronization with Microsoft Azure AD | • Planning and preparing for directory synchronization  
• Implementing directory synchronization by using Azure AD Connect | • Managing identities with directory synchronization |
| Module 13: Monitoring, managing, and recovering AD DS | • Monitoring AD DS  
• Managing the Active Directory database | • Active Directory backup and recovery options for AD DS and other identity and access solutions |
## Detailed Lab outline

<table>
<thead>
<tr>
<th>Lab 1: Deploying and administering AD DS</th>
<th>• Deploying AD DS</th>
<th>• Administering AD DS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Deploying domain controllers by performing domain controller cloning</td>
<td></td>
</tr>
<tr>
<td>Lab 2-A: Managing AD DS objects</td>
<td>• Creating and managing groups in AD DS</td>
<td>• Managing computer objects in AD DS</td>
</tr>
<tr>
<td></td>
<td>• Creating and configuring user accounts in AD DS</td>
<td></td>
</tr>
<tr>
<td>Lab 2-B: Administering AD DS</td>
<td>• Delegate administration for OUs</td>
<td>• Creating and modifying AD DS objects with Windows PowerShell</td>
</tr>
<tr>
<td>Lab 3: Domain and trust management in AD DS</td>
<td>• Implementing forest trusts</td>
<td>• Implementing child domains in AD DS</td>
</tr>
<tr>
<td>Lab 4: Implementing AD DS sites and replication</td>
<td>• Modifying the default site</td>
<td>• Configuring AD DS replication</td>
</tr>
<tr>
<td></td>
<td>• Creating additional sites and subnets</td>
<td>• Monitoring and troubleshooting AD DS replication</td>
</tr>
<tr>
<td>Lab 5-A: Implementing a Group Policy infrastructure</td>
<td>• Creating and configuring GPOs</td>
<td>• Managing GPO scope</td>
</tr>
<tr>
<td>Lab 5-B: Troubleshooting Group Policy infrastructure</td>
<td>• Verify GPO application</td>
<td>• Troubleshooting GPOs</td>
</tr>
<tr>
<td>Lab 6: Managing user settings with GPOs</td>
<td>• Using administrative templates to manage user settings</td>
<td>• Configuring Folder Redirection</td>
</tr>
<tr>
<td></td>
<td>• Implement settings by using Group Policy preferences</td>
<td>• Planning Group Policy (optional)</td>
</tr>
<tr>
<td>Lab 7: Securing AD DS</td>
<td>• Implementing security policies for accounts, passwords, and administrative groups</td>
<td>• Creating and associating a group MSA</td>
</tr>
<tr>
<td></td>
<td>• Deploying and configuring an RODC</td>
<td></td>
</tr>
<tr>
<td>Lab 8: Deploying and configuring a two-tier CA hierarchy</td>
<td>• Deploying an offline root CA</td>
<td>• Deploying an enterprise subordinate CA</td>
</tr>
<tr>
<td>Lab 9: Deploying and using certificates</td>
<td>• Configuring certificate templates</td>
<td>• Configuring and implementing key recovery</td>
</tr>
<tr>
<td></td>
<td>• Enrolling and using certificates</td>
<td></td>
</tr>
<tr>
<td>Lab 10: Implementing AD FS</td>
<td>• Configuring AD FS prerequisites</td>
<td>• Configuring an internal application for AD</td>
</tr>
<tr>
<td></td>
<td>• Installing and configuring AD FS</td>
<td>• Configuring AD FS for federated business partners</td>
</tr>
<tr>
<td>Lab 11: Implementing an AD RMS infrastructure</td>
<td>• Installing and configuring AD RMS</td>
<td>• Using AD RMS on clients</td>
</tr>
<tr>
<td></td>
<td>• Configuring AD RMS templates</td>
<td></td>
</tr>
<tr>
<td>Lab 12: Configuring directory synchronization</td>
<td>• Preparing for directory synchronization</td>
<td>• Managing Active Directory users and groups</td>
</tr>
<tr>
<td></td>
<td>• Configuring directory synchronization</td>
<td></td>
</tr>
<tr>
<td>Lab 13: Recovering objects in AD DS</td>
<td>• Backing up and restoring AD DS</td>
<td>• Recovering objects in AD DS</td>
</tr>
</tbody>
</table>