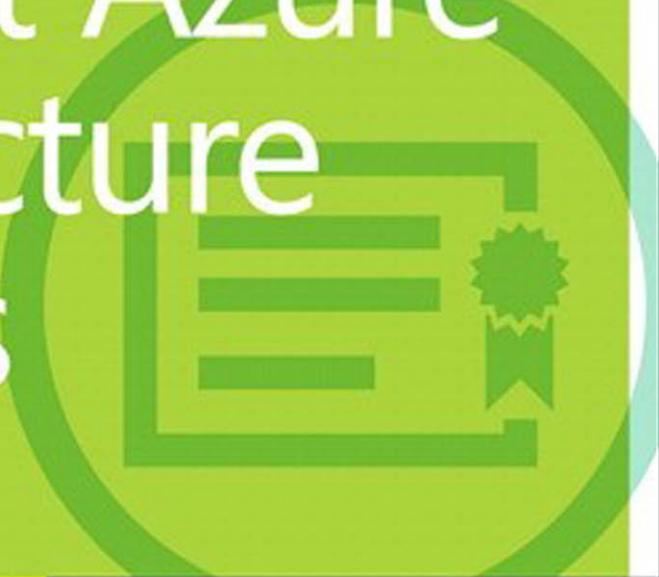




Microsoft

Implementing Microsoft Azure Infrastructure Solutions



Exam Ref 70-533

Michael Washam
Rick Rainey



Exam Ref 70-533

Implementing Microsoft

Azure Infrastructure

Solutions

Michael Washam

Rick Rainey

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2015 by Michael Washam and Rick Rainey

No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number: 2014951859
ISBN: 978-0-7356-9706-5

Printed and bound in the United States of America.

First Printing: February 2015

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at <http://aka.ms/tellpress>.

This book is provided "as-is" and expresses the author's views and opinions. The views, opinions and information expressed in this book, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

Microsoft and the trademarks listed at <http://www.microsoft.com> on the "Trademarks" Web page are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

Acquisitions Editor: Karen Szall

Developmental Editor: Karen Szall

Editorial Production: Troy Mott, Ellie Volckhausen

Technical Reviewers: Jeremy Johnson; Technical Review services
provided by Content Master, a member of CM Group, Ltd.

Copyeditor: Christina Rudloff

Indexer: Angela Howard

Cover: Twist Creative • Seattle

Contents at a glance

<i>Introduction</i>	xv
<i>Preparing for the exam</i>	xix
CHAPTER 1 Implement Websites	1
CHAPTER 2 Implement virtual machines	61
CHAPTER 3 Implement Cloud Services	151
CHAPTER 4 Implement storage	213
CHAPTER 5 Implement an Azure Active Directory	267
CHAPTER 6 Implement virtual networks	319
<i>Index</i>	355



Contents

Introduction xv

Microsoft certifications	xv
Acknowledgments	xvi
Free ebooks from Microsoft Press	xvi
Microsoft Virtual Academy	xvii
Errata, updates, & book support	xvii
We want to hear from you	xvii
Stay in touch	xvii
<i>Preparing for the exam</i>	xix

Chapter 1: Implement Websites 1

Objective 1.1: Deploy Websites	1
Creating an Azure website	2
Defining deployment slots	4
Swapping deployment slots	6
Publishing an Azure website	7
Deploying WebJobs	7
Objective summary	9
Objective review	9
Objective 1.2: Configure websites	10
Configuring site settings	11
Configuring a custom domain for a website	14
Configuring SSL certificates for an Azure website	16

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Configuring Azure Traffic Manager	18
Configuring handler mappings	22
Configuring handler mappings using Azure PowerShell	23
Configuring virtual applications and directories	23
Using the Azure Cross-Platform Command-Line Interface tools for configuration tasks	24
Objective summary	26
Objective review	27
Objective 1.3: Configure diagnostics, monitoring, and analytics.	28
Enabling application and site diagnostics	28
Retrieving diagnostic logs	30
Viewing streaming logs	32
Monitoring website resources	34
Configuring endpoint monitoring and alerts	36
Configuring alerts based on metrics and events	37
Monitoring Azure services	38
Configuring analytics	39
Configuring backup	40
Objective summary	42
Objective review	43
Objective 1.4: Configure scale and resilience.	44
Configuring Autoscale using schedules	44
Configuring Autoscale using metrics	46
Scaling up a website instance	47
Objective summary	48
Objective review	48
Objective 1.5: Manage hosting plans	48
Creating a new web hosting plan	49
Creating a website within an existing web hosting plan	50
Migrating websites between hosting plans	50
Objective summary	51
Objective review	52

Answers	53
Objective 1.1: Thought experiment	53
Objective 1.1: Review	53
Objective 1.2: Thought experiment	54
Objective 1.2: Review	55
Objective 1.3: Thought experiment	56
Objective 1.3: Review	56
Objective 1.4: Thought experiment	57
Objective 1.4: Review	58
Objective 1.5: Thought experiment	58
Objective 1.5: Review	58
Chapter 2: Implement virtual machines	61
Objective 2.1: Deploy workloads on Azure virtual machines (VMs)	61
Identifying supported workloads	62
Creating virtual machines	62
Managing the lifecycle of a virtual machine	80
Connecting to virtual machines	82
Objective summary	86
Objective review	86
Objective 2.2: Implement images and disks.	87
Uploading and downloading virtual hard disks	88
Copying virtual hard disks between storage accounts and subscriptions	89
Virtual machine images	89
Creating images and disks from a virtual hard disk	92
Managing data disks	96
Deleting images and disks	98
Objective summary	99
Objective review	100

Objective 2.3: Perform configuration management.....	100
Using the custom script extension	101
Implementing Windows PowerShell Desired State Configuration	103
Using the Virtual Machine Access Extension	109
Enabling the Puppet virtual machine extension	110
Enabling the Chef virtual machine extension	111
Extensions without cmdlets	111
Objective summary	112
Objective review	113
Objective 2.4: Configure VM networking.....	114
Understanding cloud services	114
Configuring endpoints	115
Configuring access control lists	119
Configuring reserved IP addresses	120
Configuring public IP addresses	121
Objective summary	122
Objective review	123
Objective 2.5: Configure VM for resiliency.....	124
Configuring availability sets	124
Scaling a virtual machine up and down	125
Implementing Autoscale	126
Objective summary	129
Objective review	129
Objective 2.6: Design and implement VM storage.....	130
Configuring virtual machine disk caching	130
Planning for storage capacity	131
Implementing disk redundancy for durability	131
Implementing disk redundancy for performance	132
Implementing Azure Files	133
Encrypting disks	134
Objective summary	134
Objective review	135

Objective 2.7: Monitor VMs.	136
Configuring metrics and alerts	136
Configuring endpoint monitoring	138
Configuring diagnostics	138
Objective summary	140
Objective review	140
Answers.	142
Objective 2.1: Thought experiment	142
Objective 2.1: Review	142
Objective 2.2: Thought experiment	143
Objective 2.2: Review	143
Objective 2.3: Thought experiment	144
Objective 2.3: Review	144
Objective 2.4: Thought experiment	145
Objective 2.4: Review	145
Objective 2.5: Thought experiment	146
Objective 2.5: Review	146
Objective 2.6: Thought experiment	147
Objective 2.6: Review	147
Objective 2.7: Thought experiment	148
Objective 2.7: Review	148
Chapter 3: Implement Cloud Services	151
Objective 3.1: Configure Cloud Services and roles	151
Configuring role instance count	152
Configuring role operating system settings	155
Configuring In-Role Cache for Microsoft Azure Cache	157
Configuring a custom domain	160
Configuring SSL	162
Configuring a reserved IP address	164
Configuring network traffic rules	166
Restricting web role access	168
Configuring local storage	170

Configuring role instance size	172
Configuring multiple websites on a web role	173
Configuring remote desktop	176
Objective summary	177
Objective review	178
Objective 3.2: Deploy and manage Cloud Services	180
Packaging a cloud service	180
Deploying a cloud service	182
Perform a virtual IP swap	187
Updating a cloud service deployment	187
Scaling a cloud service	189
Creating a Service Bus namespace	193
Objective summary	195
Objective review	195
Objective 3.3: Monitor Cloud Services	196
Monitoring a cloud service	196
Configuring endpoint monitoring	199
Monitoring a Service Bus queue	200
Monitoring a Service Bus topic	201
Monitoring a Service Bus relay	202
Monitoring a Notification Hub	202
Collecting diagnostics data	203
Objective summary	205
Objective review	205
Answers.....	206
Objective 3.1: Thought experiment	206
Objective 3.1: Review	206
Objective 3.2: Thought experiment	209
Objective 3.2: Review	209
Objective 3.3: Thought experiment	210
Objective 3.3: Review	210

Chapter 4: Implement storage	213
Objective 4.1: Implement blobs and Azure files	213
Managing blob storage	214
Understanding storage account replication options	216
Using the async blob copy service	218
Configuring, and using, Azure files	220
Using the Import and Export service	221
Implementing Content Delivery Network	223
Configuring custom domains	226
Objective summary	228
Objective review	228
Objective 4.2: Manage access.	229
Managing storage account keys	230
Creating, and using, shared access signatures	231
Using a stored access policy	232
Objective summary	233
Objective review	233
Objective 4.3: Configure diagnostics, monitoring, and analytics	234
Configuring Azure Storage Diagnostics	235
Analyzing diagnostic data	236
Enabling monitoring and alerts	238
Objective summary	240
Objective review	240
Objective 4.4: Implement SQL databases	241
Choosing a service tier	241
Implementing point-in-time recovery	243
Implementing geo-replication	245
Scalability strategies	249
Importing and exporting data	252
Objective summary	254
Objective review	255

Objective 4.5: Implement recovery services.	255
Protecting servers with Azure Backup	256
Objective summary	262
Objective review	262
Answers.	263
Objective 4.2: Thought experiment	263
Objective 4.2: Review	263
Objective 4.3: Thought experiment	264
Objective 4.3: Review	264
Objective 4.4: Thought experiment	265
Objective 4.4: Review	265
Objective 4.5: Thought experiment	266
Objective 4.5: Review	266
Chapter 5: Implement an Azure Active Directory	267
Objective 5.1: Integrate an Azure AD with existing directories	267
Implementing directory synchronization	268
Integrating Azure Active Directory with Office 365	274
Configuring a custom domain	278
Monitoring Azure Active Directory	280
Objective summary	286
Objective review	287
Objective 5.2: Configure the Application Access Panel	288
Adding SaaS applications to Azure Active Directory	289
Configuring access to SaaS applications	289
Customizing the Access Panel and sign-in page	293
Configuring Multi-Factor Authentication	294
Federating with Facebook and Google ID	298
Objective summary	299
Objective review	300

Objective 5.3: Integrate an app with Azure AD.....	301
Add a web application or web service	301
Adding a native application	307
Configuring graph API permissions for an application	309
Objective summary	311
Objective review	311
Answers.	313
Objective 5.1: Thought experiment	313
Objective 5.1: Review	313
Objective 5.2: Thought experiment	315
Objective 5.2: Review	315
Objective 5.3: Thought experiment	316
Objective 5.3: Review	317
Chapter 6: Implement virtual networks	319
Objective 6.1: Configure a virtual network.	319
Creating and configuring a virtual network	320
Deploying a virtual machine into a virtual network	324
Deploying a cloud service into a virtual network	326
Configuring internal load balancing	327
Objective summary	329
Objective review	329
Objective 6.2: Modify a network configuration	330
Importing and exporting network configuration settings	330
Changing an existing network configuration	332
Objective summary	334
Objective review	334
Objective 6.3: Design and implement a multi-site or hybrid network ..	335
Identifying the appropriate connectivity solution	335
Implementing a point-to-site VPN	337
Implementing a site-to-site VPN	340
Implementing a virtual network-to-virtual network VPN	342
Objective summary	350
Objective review	351

Answers.....	352
Objective 6.1: Thought experiment	352
Objective 6.1: Review	352
Objective 6.2: Thought experiment	353
Objective 6.2: Review	353
Objective 6.3: Thought experiment	354
Objective 6.3: Review	354

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Introduction

This book is written for IT professionals preparing for Exam 70-533 Implementing Microsoft Azure Infrastructure Solutions.

Microsoft Azure is the Microsoft cloud platform comprised of compute, data, application, and networking services. This book is written specifically for IT professionals who want to demonstrate their skills to implement and configure these services in Microsoft Azure.

At the time of this writing, two versions of the Web-based management portal for Azure are available. The current portal (the Azure management portal) is available at <https://manage.windowsazure.com>, and a preview portal (the Azure Preview Portal) is available at <https://portal.azure.com>. Throughout the book, as references to the portal are made, we use the Azure Preview Portal if the functionality is available in that portal. Otherwise, we use the Azure management portal. Chapters 3 and 5 reference only the Azure management portal because the topics discussed were not available in the Preview Portal at the time of this writing.

This book covers every exam objective, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions themselves and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the links you'll find in text to find more information and take the time to research and study the topic. Great information is available on MSDN, TechNet, and in blogs and forums.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO ALL MICROSOFT CERTIFICATIONS

For information about Microsoft certifications, including a full list of available certifications, go to <http://www.microsoft.com/learning>.

Acknowledgments

Bringing a book to print involves the work and dedication of many individuals beyond the author's names you see on the front cover. Without their attention to detail and coordination during technical and editorial reviews, this book would simply not be possible. Therefore, we would like to extend the sincerest thank you to the following people:

- Alison Hirsch
- Christina Rudloff
- Karen Szall
- Jeremy Johnson
- Trevor Sullivan

Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

<http://aka.ms/mspressfree>

And, if you're new to Microsoft Azure, download the free ebook "Microsoft Azure Essentials: Fundamentals of Azure". It provides both conceptual and how-to content for key areas, including:

- Azure Websites and Azure Cloud Services
- Azure Virtual Machines
- Azure Storage
- Azure Virtual Networks
- Databases
- Azure Active Directory

Microsoft Virtual Academy

Build your knowledge of Microsoft technologies with free expert-led online training from Microsoft Virtual Academy (MVA). MVA offers a comprehensive library of videos, live events, and more to help you learn the latest technologies and prepare for certification exams. You'll find what you need here:

<http://www.microsoftvirtualacademy.com>

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

<http://aka.ms/er533/errata>

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at
mspinput@microsoft.com.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to
<http://support.microsoft.com>.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

<http://aka.ms/tellpress>

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *<http://twitter.com/MicrosoftPress>*.

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam ref and another study guide for your “at home” preparation, and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

Note that this Exam Ref is based on publicly available information about the exam and the author’s experience. To safeguard the integrity of the exam, authors do not have access to the live exam.

CHAPTER 5

Implement an Azure Active Directory

Microsoft Azure Active Directory is the identity and access management solution for the Microsoft Azure platform. Organizations can use Azure Active Directory to configure access to applications used by the organization, manage users and groups, configure Multi-Factor Authentication (MFA) for users, identify irregular sign-in activity using advanced machine learning algorithms, extend existing on-premises Windows Server Active Directory implementations to Azure Active Directory, and empower users to manage their identity settings.

Objectives in this chapter:

- Objective 5.1: Integrate an Azure AD with existing directories
- Objective 5.2: Configure the Application Access Panel
- Objective 5.3: Integrate an app with Azure AD

Objective 5.1: Integrate an Azure AD with existing directories

Integrating Azure Active Directory with existing directories is one of the most common tasks for an IT professional because most organizations have an existing on-premises directory and/or online directory that the business depends on. Azure Active Directory is by no means intended to be a replacement for existing directories. It is a directory service that is specifically designed for the cloud, and, in particular, the Microsoft Azure platform. As such, it delivers services and features that can augment existing directory solutions to handle cloud-based identity and access needs for an organization.

Azure Active Directory is offered in either a Free, Basic, or Premium edition. The Basic and Premium editions offer advanced enterprise features, an unlimited number of directory objects, and SLAs. The content in this chapter discusses features and services of Azure Active Directory without regard for which edition the feature is offered in. Details about which features are available with each edition are available at <http://msdn.microsoft.com/en-us/library/azure/dn532272.aspx>.

This objective covers how to:

- Implement directory synchronization
- Integrate Azure Active Directory with Office 365
- Configure a custom domain
- Monitor Azure Active Directory

Implementing directory synchronization

Many organizations have a significant investment in their on-premises infrastructure that includes a Windows Server Active Directory used to manage users, groups, and other resources in the organization. This on-premises directory provides the identity and access capabilities needed by IT professionals to support their business operations on-premises.

As these organizations move workloads to Azure and leverage cloud applications to support their business, it is common for organizations to seek ways to leverage their on-premises investment in Windows Server Active Directory. Organizations do this to provide similar identity and access capabilities for their cloud environment in Azure.

Directory synchronization addresses the needs of IT professionals seeking to extend their on-premises Windows Server Active Directory to Azure Active Directory. It reduces the administration costs that would otherwise be associated with managing users and groups in different environments. It also promotes a more positive user sign-in experiences for users accessing applications in their on-premises environment and cloud applications running in Azure.

Azure Active Directory supports directory synchronization of users and groups under four scenarios. The scenario best suited for your environment will depend on your on-premises infrastructure and authentication requirements for your users. These scenarios and a description of each are shown in Table 5-1.

TABLE 5-1 Directory synchronization scenarios supported by Azure Active Directory

scenario	description
Directory synchronization	Synchronizes on-premises users and groups to Azure Active Directory. Synchronization occurs on scheduled intervals to synchronize changes made in the on-premises directory.
Directory synchronization with password sync	An extension to the directory synchronization scenario that synchronizes a hash of a user's on-premises password to Azure Active Directory. This enables users to authenticate to Azure Active Directory using the same credentials they use to authenticate to their on-premises directory.

MORE INFO CHOOSING THE RIGHT DIRECTORY SYNCHRONIZATION SCENARIO

Each directory synchronization scenario offers unique benefits. Additionally, the time and complexity involved in implementing a scenario can vary. A decision matrix is available for you to learn what you can accomplish with each scenario, and also the requirements for each scenario at <http://msdn.microsoft.com/en-us/library/azure/jj573649.aspx>.

Currently there are two tools used to implement directory synchronization, which are as follows:

- Azure Active Directory Synchronization tool (DirSync)
- Azure Active Directory Synchronization Services (AAD Sync)

Which tool you use also depends on the scenario you are implementing and the synchronization features that your scenario requires. AAD Sync should be the tool you look to first because this is the tool Microsoft is making investments in going forward. DirSync was the first directory integration tool released and is still required for some scenarios.

MORE INFO CHOOSING THE RIGHT DIRECTORY SYNCHRONIZATION TOOL

Microsoft is clear in their messaging that AAD Sync will eventually be the single synchronization tool for synchronizing your on-premises directory to Azure Active Directory. At the time of this writing, there are features in DirSync and Microsoft Forefront Identity Manager (FIM) 2010 R2 that have not yet been implemented in AAD Sync. A breakdown of which features are supported by which tool can be found at <http://msdn.microsoft.com/en-us/library/azure/dn757582.aspx>.

Enable directory integration

Regardless of the directory synchronization scenario you are implementing, the first task will be to enable directory synchronization for your Azure Active Directory. This can be accomplished in the Azure management portal by going to the Directory Integration page of your directory and setting the Directory Sync field to Activated, as shown in Figure 5-1.



FIGURE 5-1 Activating directory synchronization for an Azure Active Directory

After directory sync is activated for your directory, you can proceed with the implementation of one of the directory synchronization scenarios. As shown previously in 5-1, there are four directory synchronization scenarios supported by Azure Active Directory. The following scenarios are the most common, and therefore the focus for the next two sections:

- Directory synchronization with password sync
- Directory synchronization with single sign-on

Configure directory synchronization with password sync

Configuring directory synchronization with password sync is the simplest of the supported directory synchronization scenarios. It does not provide a true single sign-on experience for users, but it does enable users to sign-in using the same username and password that they use in their on-premises environment. For many organizations, this is sufficient to meet their authentication requirements for cloud applications if Active Directory Federation Services (AD FS) is not already configured on-premises.

NOTE DIRECTORY SYNCHRONIZATION WITH PASSWORD SYNC REQUIRES DIRSYNC

At the time of this writing, the new AAD Sync tool does not support directory synchronization with password sync. Therefore, DirSync is required for this scenario. The Azure management portal references it in the Directory Integration page after activating directory synchronization.

To get started with this scenario, the Azure management portal will open step three on the Directory Integration page where you activated directory synchronization. Click the download link for the directory sync tool and save it to either the on-premises domain controller, or a domain joined server that will be dedicated to running directory synchronization. The download is a single executable called DirSync.exe. After copying this to the target server in your on-premises environment, run DirSync.exe to start the installation.

NOTE DIRSYNC REQUIRES .NET FRAMEWORK 3.5 SP1

If the target server you download DirSync.exe to is running Windows Server 2012 or later, you may get an error when trying to run DirSync if it detects that .NET Framework 3.5 SP1 is not installed. On Windows Server 2012 and newer, this version of the .NET Framework is not installed by default. Therefore, it may be necessary for you to enable this feature before proceeding with the DirSync installation.

The DirSync installation is a wizard-driven experience that starts by prompting you for two sets of credentials that DirSync needs to configure directory synchronization. The credentials needed are as follows:

- The credentials for a *global administrator* in the Azure Active Directory
- The credentials for a *domain administrator* in the Windows Server Active Directory

The rest of the options are check boxes to enable or disable a feature of directory synchronization, such as Hybrid Deployment or Password Synchronization. The goal of this section of the objective is to configure password synchronization; therefore, this option must be checked in the wizard, as shown in Figure 5-2.



FIGURE 5-2 Enabling the Password Synchronization feature during DirSync installation

After exiting the DirSync Installation Wizard, DirSync will continue running in the background as a Windows Service and periodically synchronize objects from the on-premises Windows Server Active Directory to the Azure Active Directory. The name of the service is Windows Azure Directory Sync Service.



EXAM TIP

Directory synchronization can be invoked on-demand by using the Start-OnlineCoExistence-Sync Windows PowerShell cmdlet that is installed as part of the DirSync installation. Optionally, you can pass the **FullSync** switch to the command if you want to invoke a full directory synchronization. Otherwise, it will only synchronize the changes since the last synchronization occurred. The script to import the module containing the cmdlet is installed at `C:\Program Files\Windows Azure Active Directory Sync\DirSync\ImportModules.ps1`. You must execute this script first for the cmdlets to be available.

You can get a list of all of the configuration cmdlets installed by executing the command
`Get-Command -All -Module "Microsoft.Online.Coexistence.PS.Config" | Select Name`.

Invoking directory synchronization on demand is useful in scenarios where you need a change in the director to be synchronized immediately, such as removing a user from the on-premises directory.

Verifying that directory synchronization is working is a matter of simply checking the Users and/or Groups page of the directory in the management portal. Users that are synchronized from the on-premises Windows Server Active Directory will appear as sourced from the Local Active Directory, as shown in Figure 5-3. You can also check the event log on the server running DirSync to see logs recorded by DirSync. This will be covered in further detail in the Monitor Azure Active Directory section of this text.

The screenshot shows the 'Users' page in the Azure Active Directory management portal. At the top, there are navigation links for USERS, GROUPS, APPLICATIONS, DOMAINS, DIRECTORY INTEGRATION, CONFIGURE, and REPORTS. Below these, a section titled 'LICENSES' is visible. The main area is titled 'DISPLAY NAME' and shows two entries: '(Global Administrator)' which is 'Sourced from' Windows Azure Active Directory, and 'John Doe' which is 'Sourced from' Local Active Directory. There is also a small icon indicating a connection between the two sources.

FIGURE 5-3 Users page of a directory with directory synchronization configured

The default configuration for this scenario synchronizes user passwords *from* the Windows Server Active Directory *to* the Azure Active Directory. In the event that a user needs to reset his or her password, an administrator of the on-premises directory would have to reset the password for the user. Resetting user passwords is one of the most common IT tasks costing organizations time and money, and Azure Active Directory offers a feature to combat this through its self-service password reset (SSPR) feature. The SSPR feature enables you to define password reset policies for users in a way that gives the organization great control over how password resets are performed, while empowering users to complete the task on their own. This feature is available for Azure Active Directory Basic and Premium, and is enabled and configurable in the management portal, as shown in Figure 5-4.

The screenshot shows the 'user password reset policy' configuration page. It has several sections: 1. 'USERS ENABLED FOR PASSWORD RESET' with options 'NONE' and 'ALL' (selected). 2. A note: 'Before users can reset their passwords, they must first have at least one authentication method defined.' 3. 'AUTHENTICATION METHODS AVAILABLE TO USERS' with checkboxes for 'Office Phone' (unchecked), 'Mobile Phone' (checked), and 'Alternate Email Address' (unchecked). 4. 'NUMBER OF AUTHENTICATION METHODS REQUIRED' set to '1'. 5. A note: 'You can send users to a webpage where they can register their own authentication method information.' 6. 'REQUIRE USERS TO REGISTER WHEN SIGNING IN TO THE ACCESS PANEL?' with options 'YES' and 'NO' (selected).

FIGURE 5-4 Configuring password reset policies for users in the management portal

DirSync with password sync includes a feature called *password write-back* that can be enabled for an Azure Active Directory with SSPR enabled. With this feature, password resets performed in Azure Active Directory can be persisted back to the on-premises Windows Server Active Directory. The DirSync installation includes the following Windows PowerShell cmdlets to enable or disable this feature as shown here:

- Enable-OnlinePasswordWriteback
- Disable-OnlinePasswordWriteback

Before running these cmdlets, you must first run the Windows PowerShell script at %ProgramFiles%\Azure Active Directory Sync\DirSyncConfigShell.ps1 with elevated admin rights. Additional information, potential requirements, and troubleshooting steps for the password write-back feature are available at <http://msdn.microsoft.com/en-us/library/azure/dn688249.aspx>.

Configure directory synchronization with single sign-on

Configuring directory synchronization with single sign-on results in a better user experience for users than the password-sync scenario discussed in the previous section because it provides true single sign-on for the users. In this scenario, if a user is already authenticated in their on-premises environment, the user will not be prompted to re-authenticate when accessing cloud applications protected by Azure Active Directory. This is the most significant difference for users, as compared to the password sync scenario described earlier. In that scenario, the user would be prompted to sign-in when accessing cloud applications even if the user was already authenticated in their on-premises environment.

The single sign-on experience this configuration delivers is made possible by the fact that users *always* authenticate to their on-premises Windows Server Active Directory, whether they are accessing resources on-premises or in the cloud. In other words, there is no synchronization of hashed passwords to Azure Active Directory. Instead, users are prompted to authenticate at a security token service (STS) on-premises. Active Directory Federation Service (AD FS) is such a service and must be installed in the on-premises environment to implement this scenario.

MORE INFO AZURE ACTIVE DIRECTORY CONNECT (AAD CONNECT)

Microsoft has developed a tool called Azure Active Directory Connect that addresses the complexities of implementing directory synchronization. At the time of this writing, AAD Connect is in a Beta version and can be downloaded via the Microsoft Connect program at <https://connect.microsoft.com/site1164/program8612>.

AAD Connect is a wizard that takes care of configuring DirSync, installing the necessary perquisites, and configuring your environment for either directory synchronization with password sync or directory synchronization with single sign-on. The single sign-on scenarios are popular choices for many customers configuring directory synchronization because it provides the best user experience when signing in. However, installing and configuring AD FS to support the single sign-on scenarios is not a trivial task. The Azure Active Directory team developed this tool to simplify the implementation of directory synchronization. AAD Connect will even verify the configuration for you so that you have confidence that the implementation was done correctly.

To learn more about the initial Beta version features and how to use AAD Connect, read the post on the Active Directory Team Blog at <http://blogs.technet.com/b/ad/archive/2014/08/04/connecting-ad-and-azure-ad-only-4-clicks-with-azure-ad-connect.aspx>. The documentation for AAD Connect provides more details about the capabilities of the tool at <http://msdn.microsoft.com/en-us/library/azure/dn832695.aspx>.

Implementing this scenario requires the high-level tasks below. Each of these tasks are broken down further into several steps that must be completed.

- Have a custom domain configured for the Azure Active Directory that you are going to integrate with.
- Have an SSL certificate that can be used when communicating with the AD FS server in the on-premises domain.
- AD FS deployed.
- A trust setup between AD FS and Azure Active Directory.
- Directory synchronization (not password sync) installed and configured.

Assuming AD FS will be used for the on-premises STS, step-by-step instructions and guidance is available at <http://msdn.microsoft.com/en-us/library/azure/jj205462.aspx>.

If you have the required SSL certificates and servers available for the required federation servers and proxy servers, the AAD Connect tool will configure everything for you. This will be the recommended path for implementing this scenario for users who don't already have AD FS or another third-party STS implemented in their environment.

Integrating Azure Active Directory with Office 365

Although Microsoft Azure and Microsoft Office 365 are marketed and sold as separate subscriptions, there is one service that ties the two together, and that service is Azure Active Directory. If you are an Office 365 subscriber, you already have an Azure Active Directory, whether you have an Azure Subscription or not. That is because the directory you get with Office 365 is actually a tenant in Azure Active Directory. However, that does not mean you have the full set of services an Azure Subscription offers. To be able to provision services and resources in Microsoft Azure requires that you have an Azure subscription.

If you have an Office 365 subscription and an Azure subscription, the Azure Active Directory from your Office 365 can be integrated with your existing Azure subscription.

If you have an Azure subscription but don't have an Office 365 subscription, Office 365 can be added to your Azure subscription through the Application Gallery.

No matter which of these scenarios applies, integrating an Azure Active Directory from an Office 365 subscription with an Azure subscription offers your organization some important benefits, including the following:

- Authorized users in the Azure Active Directory can provision resources in the Azure subscription.
- Application access to software as a services (SaaS) applications that the organization depends on can be managed in the management portal for users in the directory.
- Applications an organization develops in-house can be protected such that only authenticated users in the directory can access them.

Sign up for Azure as an organization using Office 365 organization accounts

If you already have an Office 365 subscription but not an Azure subscription, the easiest way to add an Azure subscription for your organization is to go to <http://azure.com> and click the link to start a free trial subscription. When the sign in page appears, you should click the Sign In With Your Organizational Account link, as shown in Figure 5-5.

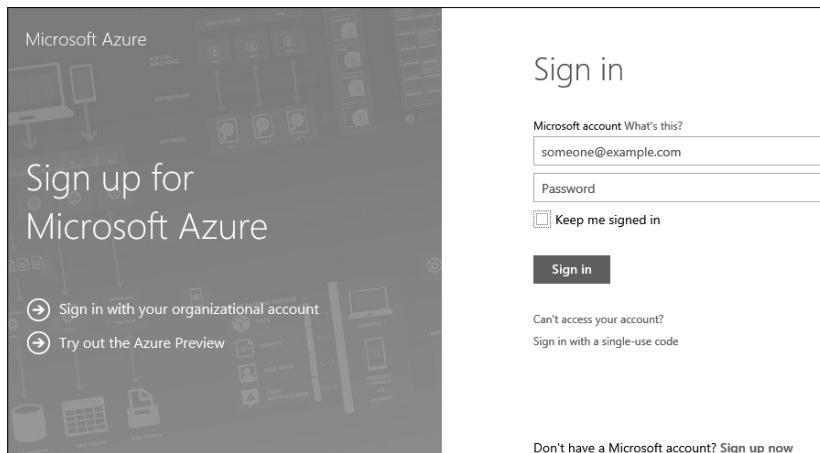


FIGURE 5-5 Sign up for Microsoft Azure using an existing organizational account

After clicking the link to sign in, using your organizational account, complete the process as follows:

1. Provide your contact information. Some of the fields will be pre-populated from your directory in Office 365 for you.
2. Provide mobile verification as a second authentication step.
3. Provide payment information.
4. Agree to the terms for an Azure subscription.

After completing these steps, the Azure subscription will be created, your directory from Office 365 will be accessible in the management portal, and you will be added as a service administrator on the Azure subscription. Optionally, you can add co-administrators to the Azure subscription so others in your organization can provision services in the Azure subscription. No further action is needed to integrate your Office 365 directory with your Azure subscription.

Integrate an Office 365 directory with an existing Azure subscription

If you already have an Office 365 subscription and an Azure subscription obtained from a Microsoft Account, you can integrate the Office 365 directory with the Azure subscription by adding an *existing directory* to your Azure subscription. To accomplish this, sign in to the management portal using your Microsoft account credentials associated with the Azure subscription. Next, click New, App Service, Active Directory, Directory, and Custom Create.

This opens a dialog box to add a directory. Change the drop-down box for the directory field to Use Existing Directory, as shown in Figure 5-6.

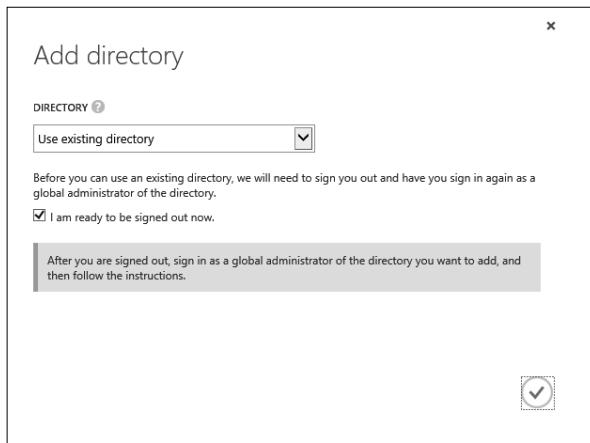


FIGURE 5-6 Add an existing directory to an Azure subscription

This approach requires you to sign out of the management portal and sign back in using the organizational account of a global administrator in the Office 365 directory. The reason you must sign back in as a global administrator of the directory is that Azure will add your Microsoft account to the directory as a global administrator and associate the directory with your Azure subscription, which requires the permissions of a global administrator to complete.

MORE INFO AZURE ACTIVE DIRECTORY USER ACCOUNTS

Azure Active Directory (and Office 365) offers several different administrator roles that can be assigned to users in the directory. This is useful in organizations where designating certain functions to other users is desired.

The following administrator roles can be assigned to users in the directory:

- **Billing administrator** This role can purchase Azure services, manage subscriptions and support tickets, and monitor service health.
- **Global administrator** This role has access to all administrative features in the directory and can assign other administrator roles.
- **Password administrator** This role can reset passwords for users and other password administrators. This role may not reset passwords for a global administrator. This role can also manage service requests and monitor service health.
- **Service administrator** This role can manage service requests and monitor service health.
- **User administrator** This role can reset password for users, manage user accounts, user groups, and service requests.

Complete details about these administrator roles, and any applicable constraints, can be found at <http://msdn.microsoft.com/library/azure/dn468213.aspx>.

After completing this step, your Office 365 directory will be the default directory associated with your Azure subscription. You will be able sign in to the management portal using your organizational account and provision services in the Azure subscription. No further action is needed to integrate your Office 365 directory with your Azure subscription.



EXAM TIP

An administrator role in Azure Active Directory, such as a global administrator, does not automatically have permission to provision services and resources in an Azure subscription. Only service administrators and co-administrators can provision services and resources in an Azure subscription. A global administrator has administrative permissions to the directory and all functions in the Office 365 Admin portal.

To add a user as a co-administrator for an Azure subscription, go to the settings section in the management portal, click the Administrators tab, and then click Add at the bottom of the page.

Adding Office 365 to an existing Azure subscription

If you have only an Azure subscription, you can add Office 365 for your organization by signing up for Office 365 using the organizational account credentials for a global administrator user in your Azure Active Directory. Unless you have created a different Azure Active Directory in your Azure subscription, the Default Directory that came with your Azure subscription will be used to purchase the Office 365 subscription.

Adding Office 365, using your existing Azure Active Directory, can be accomplished by going to <https://portal.office.com>. Sign in using the credentials for a global administrator in your directory. After signing in you will be in the Office 365 Admin portal. Because you don't have an Office 365 subscription associated with the Azure Active Directory you signed in with, you will be prompted to purchase services, as shown in Figure 5-7.

The screenshot shows the Microsoft Office 365 Admin center interface. At the top, there's a navigation bar with 'Office 365' on the left, 'Admin' and 'John Doe' dropdown menus, and a gear icon for settings. Below the navigation bar is a search bar labeled 'Search users, admin tasks an' with a magnifying glass icon. To the right of the search bar is a 'Default Directory' indicator. The main content area has a dark background with white text. On the left, a sidebar lists various admin tasks: 'DASHBOARD', 'SETUP', '▶ USERS', 'GROUPS', 'DOMAINS', '▶ BILLING', '▶ EXTERNAL SHARING', '▶ SERVICE SETTINGS', '▶ SERVICE HEALTH', '▶ SUPPORT', 'PURCHASE SERVICES', 'MESSAGE CENTER', and 'TOOLS'. A callout box in the center of the screen contains the following text:
Office 365 services are not available for one of these reasons:
• You aren't subscribed to any services. Purchase Services
• There is a network delay.
• A technical error has occurred.
If you believe that you have reached this page in error, please try again later. If the problem persists, please consult the Office 365 Community or contact Support.

FIGURE 5-7 Office 365 Admin portal with an option to purchase an Office 365 subscription

Proceeding through the options to purchase an Office 365 subscription will result in an Office 365 subscription that is backed by the Azure Active Directory in your Azure subscription. Just as in the previous scenarios, the Office 365 subscription will be integrated with the Azure Active Directory. Users and groups can be created using the management portal or the Office 365 Admin portal.

Configuring a custom domain

Each Azure subscription is assigned a default directory and DNS name on the shared domain *.onmicrosoft.com. For example, if you signed up for an Azure subscription using the name Contoso, the default directory and DNS name for your Azure subscription is *contoso.onmicrosoft.com*. Although this assigned domain is a fully functional domain, it isn't necessarily user friendly. Users would have to sign in using a sign in name, such as *john.doe@contoso.onmicrosoft.com*, which has the disadvantages of having to type in a rather long domain and also not being intuitive for a user in the Contoso directory.

By adding a custom domain to your directory, you can significantly improve the user sign-on experience for users in the directory. If you own the *contoso.com* domain, and associate it to your Azure directory, users would be able to sign in using a sign in name, such as *john.doe@contoso.com*.

Configuring a custom domain involves the following steps:

1. Obtain ownership of a domain if you don't already have one.
2. Add the domain to your Azure directory.
3. Update DNS records at the domain registrar.
4. Verify the domain in the management portal.
5. Change the primary domain for the directory.

Assuming the ownership of a domain has been established, the next step is to add the domain to the directory. In the management portal, go to the Domains page for the directory, and then click Add. This action opens a dialog box where you can specify the name of the domain and indicate whether you plan to configure the domain for single sign-on with a local Windows Server Active Directory, as shown in Figure 5-8.

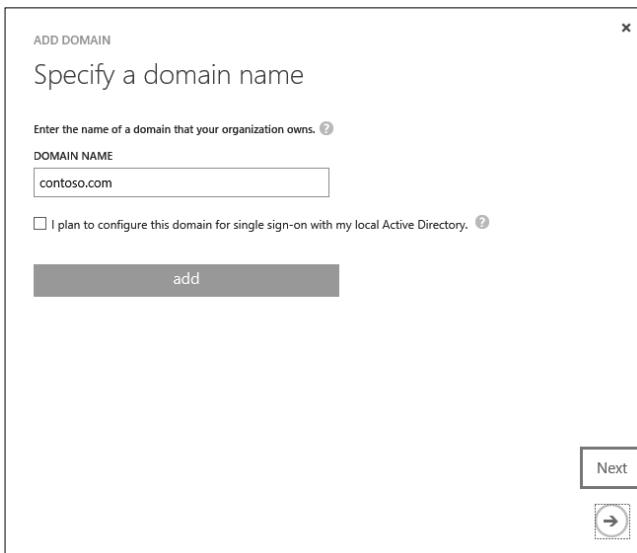


FIGURE 5-8 Adding a custom domain to a directory in the management portal

Clicking Add adds the domain to the directory and generates a unique DNS record value for the domain. The value of the DNS record is what you must enter at your domain name registrar because this record is what Azure uses in the final step to verify that you own the domain.

MORE INFO VERIFYING CUSTOM DOMAINS USING A TXT RECORD OR AN MX RECORD

A TXT record is the preferred record type used to verify a custom domain in Azure. However, not all domain registrars support adding TXT records. When Azure generates the unique values for the TXT record, it also generates unique values for an MX record that can be used as an alternate method for verifying the custom domain. More information about which type of record to choose can be found at <http://msdn.microsoft.com/en-US/library/azure/jj151776.aspx>.

After the domain has been successfully added to the directory, the management portal will present a second dialog box showing the unique value for the DNS record that must be added to the domain name registrar, as shown in Figure 5-9. The record type shown is a TXT record, which is preferred. However, if you need an MX record, you can get the value by selecting the MX record type in the dialog box.

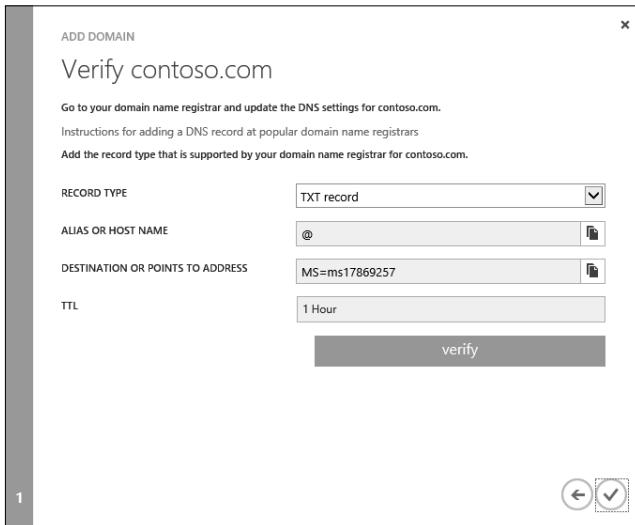


FIGURE 5-9 Verifying a custom domain in the management portal

After adding either the TXT record or the MX record to your domain name registrar, the next step is to verify the domain, which is accomplished by clicking Verify.

At this stage, you have two domain names associated with your directory: the one that was assigned to your directory on the *.onmicrosoft.com shared domain, and now your custom domain. The last step in this process is to make your custom domain the *primary* domain for your directory, which can be accomplished in the Domains page for the directory by clicking Change Primary, as shown in Figure 5-10.



FIGURE 5-10 Command buttons in management portal used to manage domain names for a directory

Monitoring Azure Active Directory

Azure Active Directory provides features that enable you to monitor activities of users in the directory. Using reporting, notifications, and services of Azure Active Directory, you can see the sign-in activity of users, identify suspicious activity, and identify application usage trends in the organization.

User and group activity sign-in reports

You can get user and group sign-in activity using the management portal. To see sign-in activity for a user, click the user you want to retrieve the report for in the Users page of the directory. In the individual user's page is an Activity tab where you can specify the criteria for the report, as shown in Figure 5-11.

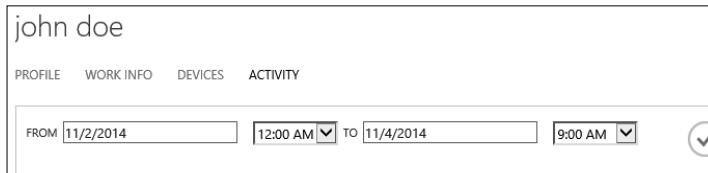


FIGURE 5-11 Specifying criteria for a user sign-in activity report in the management portal

You can also run a sign-in activity report for a group of users. To view sign-in activity for a group, click the group you want to retrieve the report for in the Groups page, and follow the same steps.

Whether your report is for a single user or a group, the information on the report will be comprised of the following:

- The date and time the sign in occurred.
- The application the user accessed. This could be an Office 365 application or an application registered in the directory for the organization, such as a SaaS application or a custom developed application.
- The user's IP address.
- The user's location, such as city and state.
- The type of client the user was running, such as Windows 8.

You can view the report in the management portal, or you can download it as a .csv file.

Azure reports

Azure Active Directory reports are an extremely useful monitoring tool that you can use to gain visibility into potential security risks for your organization, user activities such as sign in, password resets, and application usage.

The reports are available in the reports page of the directory in the management portal. They are organized into three groups of reports, which are *anomalous activity*, *activity logs*, and *integrated applications*. You can view the reports directly in the management portal or download them as .csv files.

MORE INFO AZURE ACTIVE DIRECTORY REPORTS AVAILABILITY

Some of the reports are only available in the Azure Active Directory Premium offering, such as advanced anomaly reports that use machine learning technology, and reports that provide advanced application usage.

Information about which reports are available in the Free, Basic, and Premium offerings is available at <http://msdn.microsoft.com/en-us/library/azure/dn283934.aspx>.

Anomalous activity reports are used to report sign in activity that Azure Active Directory found to be inconsistent with normal activity. Data in the report does not necessarily mean there is a security risk. Ultimately, that is for you decide. These reports are designed to bring

this information to your attention so you can make informed decisions about how to respond. Table 5-2 lists the anomalous activity reports available.

TABLE 5-2 Anomalous reports for Azure Active Directory

Report name	description
Sign ins from unknown sources	May indicate an attempt to sign in without being traced.
Sign ins after multiple failures	May indicate a successful brute force attack.
Sign ins from multiple geographies	May indicate that multiple users are signing in with the same account.
Sign ins from IP addresses with suspicious activity	May indicate a successful sign in after a sustained intrusion attempt.
Sign ins from possibly infected devices	May indicate an attempt to sign in from possibly infected devices.
Irregular sign in activity	May indicate events anomalous to users' sign in patterns.
Users with anomalous sign in activity	Indicates users whose accounts may have been compromised.

Activity log reports are used to report sign in activity, location of a user during sign in, the IP address of the user, and password reset activities. Table 5-3 lists the activity log reports available.

TABLE 5-3 Activity log reports for Azure Active Directory

Report name	description
Audit	Audited events in your directory.
Password reset activity	Provides a detailed view of password resets that occur in your organization.
Password reset registration activity	Provides a detailed view of password reset registrations that occur in your organization.
Groups activity	Provides an activity log to all group-related activity in your directory.

The integrated applications reports are where you can identify application usage trends and account provisioning events related to users being granted or denied access to SaaS applications. Table 5-4 lists the integrated applications reports.

TABLE 5-4 Integrated applications reports for Azure Active Directory

Report name	description
Application usage	Provides a usage summary for all SaaS applications integrated with your directory. This report is based on the number of times users have clicked the application in the Access Panel.
Account provisioning activity	Provides information pertaining to the provisioning of user or group access to a SaaS application.
Account provisioning errors	Use this to monitor errors that occur during the synchronization of accounts from SaaS applications to Azure AD.

Notifications

The notifications feature for Azure Active Directory Premium users enables administrators to be notified via email when anomalous sign in activity is detected. The email in the alert includes a link to a report identifying the situation and requires that the user viewing the report be both a co-administrator on the Azure subscription, and a global administrator for the directory. Additional notifications pertaining to password reset activity are also configurable in the Configure page of the directory in the management portal, as shown in Figure 5-12.

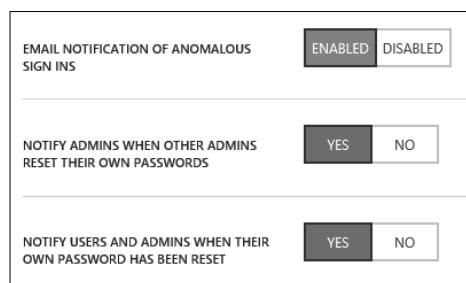


FIGURE 5-12 Configuring notifications in the management portal

Cloud App Discovery

Cloud App Discovery is a service you can use to discover cloud applications being used from within your organization. Unlike the application usage reports that report on application usage for applications you have provisioned in your Azure Active Directory, this service discovers applications that are being used that have not been provisioned in your directory. At the time of this writing, this service is in preview.

Cloud App Discovery is available at <https://appdiscovery.azure.com>. To get started using the service, you need to sign in using the organization credentials of a global administrator in the directory. The service works by collecting data from user's computers about which cloud applications they are accessing and using. This is accomplished through an agent that you must download and install on the users' machines you want to collect data for. The agent software runs on the user's computer as a service called the Microsoft Cloud App Discovery Endpoint Agent and captures application usage on the machine. The agent

periodically transfers the application usage data for the machine to the Cloud App Discovery service. You can download the agent from the Cloud App Discovery portal.

The Cloud App Discovery portal provides information about applications that have been discovered, the users that are accessing those applications, and application usage metrics such as the number of requests made to an application, the volume of data, and number of users. Using the management portal you can manage the applications discovered, proceed to add the application to your Azure Active Directory, and provision user and group access to it. Alternatively, you may decide the application is not suitable for the organization and take action to restrict access to it. Figure 5-13 shows a portion of the management portal where apps and users have been discovered.

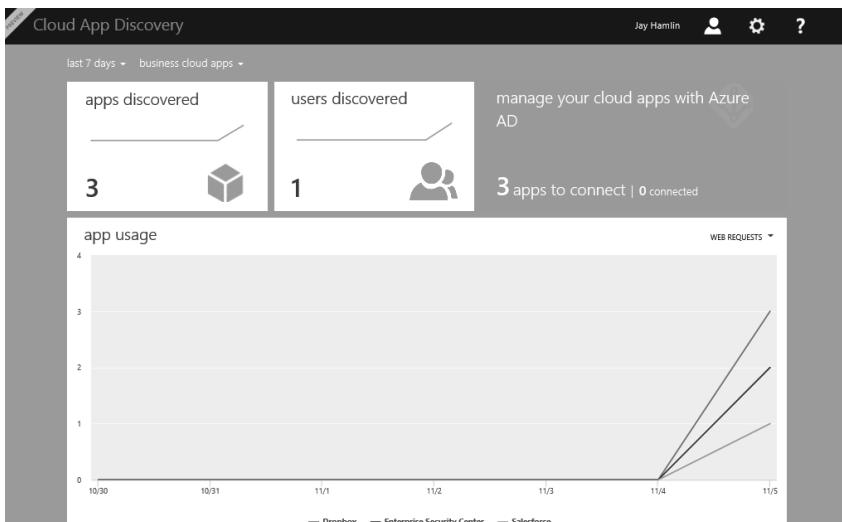


FIGURE 5-13 Cloud App Discovery portal

Monitoring directory synchronization

DirSync records events in the Windows Application Event Log. The source of the logs is Directory Synchronization. DirSync runs on an automatic schedule of every three hours, and the password sync extension runs on a schedule of every 30 minutes. Therefore, many of the logs will be a result of these scheduled synchronizations.

Part of the DirSync installation includes the Synchronization Service Manager from Microsoft Forefront Identity Manager (FIM) 2010 R2. It is located at C:\Program Files\Windows Azure Active Directory Sync\SYNCBUS\Synchronization Service\UIShell\msiiclient.exe.

NOTE SYNCHRONIZATION SERVICE MANAGER CLIENT INSTALLATION

The installation of this tool during the DirSync installation does not set up the required security groups to run it, as you would normally get in a full FIM installation. As a result, when you run the tool, you're likely to get an error indicating your account is not a member of a required security group. The security group missing is the MIISAdmins group. Therefore, you must create this group and add your user account to the group to use the tool. For more information about this issue and detailed steps to correct it, see <http://support.microsoft.com/kb/2791422>.

The advantage that Synchronization Service Manager provides is clickable links on directory synchronization events to see details of the object synchronized. As an example, when a user is updated, you will be able to see all the attributes for the user that were updated, such as the display name, surname, upn, and more. This level of detail does not exist in the event logs. Using this tool to monitor synchronization only works for adding, updating, or deleting directory objects. It does not display information for password sync events. Figure 5-14 shows the Synchronization Statistics window in the Synchronization Service Manager client for a single directory object that was added, and a directory object that was updated. Notice in the Staging section, the Adds and Updates are linkable and clicking either will display the details for that directory object.

Synchronization Statistics	
Staging	
Unchanged	0
Adds	1
Updates	1
Renames	0
Deletes	0
Discovery	
Filtered Objects	0
Inbound Synchronization	
Projections	1
Joins	0
Filtered Disconnectors	0
Disconnectors	0
Connectors with Flow Updates	2
Connectors without Flow Updates	0
Filtered Connectors	0
Deleted Connectors	0
Metaverse Object Deletes	0
Outbound Synchronization	Windows Azure Active Directory Connector
Export Attribute Flow	2
Provisioning Adds	1

FIGURE 5-14 Synchronization Statistics window in the Synchronization Service Manager client

In some cases it may be necessary to turn on additional logging that is not captured in the event log or discoverable through the Synchronization Service Manager. For example, if there are synchronization errors occurring, it may be necessary to see the result of each action occurring in the context of the synchronization. You can use the following Windows PowerShell cmdlets to enable or disable logs for directory synchronization and password synchronization.

- Enable-DirSyncLog
- Disable-DirSyncLog
- Enable-PasswordSyncLog
- Disable-PasswordSyncLog

When enabling logging, you can also indicate the desired *TraceLevel* for the logs, which can be Error, Info, Verbose, or Warning.



Thought experiment

Configure directory integration

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You are the IT administrator for Contoso. Contoso has an existing on-premises environment with Windows Server Active Directory and Active Directory Federation Services (AD FS) already configured. Contoso wants to extend their on-premises directory to Azure Active Directory. Users need to be able to sign in to on-premises applications and cloud applications running in Azure using the same username and password. Contoso also wants users to be able to change their password and reset their password without requiring the assistance of an administrator.

1. Which directory integration solution would you recommend and why?
2. What tools would you use to implement the solution?
3. Would Contoso need to change their Azure Active Directory tier?

Objective summary

- The default DNS name for an Azure Active Directory is assigned on the shared domain *.onmicrosoft.com.
- Verifying a custom domain can be done by adding either a TXT or an MX record to your domain name registrar. TXT records are the preferred method assuming that the domain registrar supports it. It is possible to have multiple domain names for a directory but only one domain can be the primary domain.
- Azure Active Directory Sync (AAD Sync) supports directory synchronization for multi-forest environments.
- Configuring directory synchronization with single sign-on requires an on-premises security token service (STS) be installed. In a Windows environment, this will generally be Active Directory Federation Services (AD FS), but other third-party products, such as Shibboleth, are also supported. The AAD Connect tool can be used to implement this scenario.

- A trust relationship between Azure Active Directory and the on-premises STS in the directory synchronization with single sign-on is required because Azure AD will externalize the authentication of users accessing the cloud application to the local STS. If a user is already authenticated in their on-premises environment, an authentication token will be issued by the STS without prompting the users again for credentials.
- The password write-back feature of directory synchronization with password sync requires the premium version for Azure AD.
- Azure Active Directory is offered in three tiers: Free, Basic, and Premium. The 99.9 percent SLA is only available in the Basic and Premium offerings.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the “Answers” section at the end of this chapter.

1. You need to give a user in your Azure Active Directory full administrative access. Which administrator role should you assign the user?
 - A. Global administrator
 - B. User administrator
 - C. Password administrator
 - D. Billing administrator
2. You have a user in your Azure Active Directory that needs permissions to create a virtual machine in the Azure subscription. What should you do to support this requirement?
 - A. Assign the global administrator role to the user.
 - B. Assign the user administrator role to the user.
 - C. Add the user as a co-administrator on the Azure subscription.
 - D. Add the user as a service administrator on the Azure subscription.
3. You need to verify a custom domain for an Azure Active Directory. Which type of DNS record can you add to your domain registrar to accomplish this? (Choose two.)
 - A. CNAME (Alias)
 - B. TXT (Text)
 - C. MX (Mail Exchanger)
 - D. A (Host)
4. You have configured directory synchronization with password sync between your on-premises Windows Server Active Directory and your Azure Active Directory. Which Windows PowerShell cmdlet should you use to allow password resets in Azure Active Directory to be persisted back to your on-premises directory?

- A. Enable-MSOnlinePasswordSync
 - B. Enable-PasswordSyncLog
 - C. Enable-DirSyncLog
 - D. Enable-OnlinePasswordWriteBack
- 5. You have removed a user from your on-premises directory that is configured for directory synchronization with your Azure Active Directory. You need for this change to be synchronized immediately. Which Windows PowerShell cmdlet will you use?
 - A. Start-OnlineCoexistenceSync
 - B. Set-DirSyncConfiguration
 - C. Enable-DirSyncLog
 - D. Set-FullPasswordSync
- 6. You need to implement directory synchronization with single sign-on for a multi-forest environment. Which tool should you use?
 - A. . DirSync
 - B. AAD Sync
 - C. AAD Connect
 - D. Synchronization Service Manager

Objective 5.2: Configure the Application Access Panel

The Azure Active Directory application access capabilities support integrating a directory with well-known software as a service (SaaS) applications that many organizations rely on for their day-to-day business needs. By integrating with these applications using Azure Active Directory, IT professionals are able to centrally manage access to the applications for users and groups in the organization. As applications are added to the directory, users are able to see and start the applications they have been assigned access to using the Access Panel.

MORE INFO AZURE ACTIVE DIRECTORY SAAS APPLICATIONS

The number of applications that can be integrated with Azure AD increases frequently. At the time of this writing, over 2,400 applications are available for organizations to use. Microsoft provides a gallery of all the applications available at <http://azure.microsoft.com/en-us/marketplace/active-directory/>. Using the gallery, you can search for applications by name, or browse through the applications by category.

This objective covers how to:

- Add SaaS applications to Azure Active Directory
- Configure access to SaaS applications
- Customize the Access Panel and sign-in page
- Configure Multi-Factor Authentication
- Federate with Facebook and Google ID

Adding SaaS applications to Azure Active Directory

The Applications page of an Azure Active Directory is where you can see and manage applications that have been added to your directory. At the bottom of this page is an Add button that will open an intuitive interface you can use to add a new SaaS application. Choose the option to Add An Application From The Gallery, and you will be able to select from the many applications available, as shown in Figure 5-15.

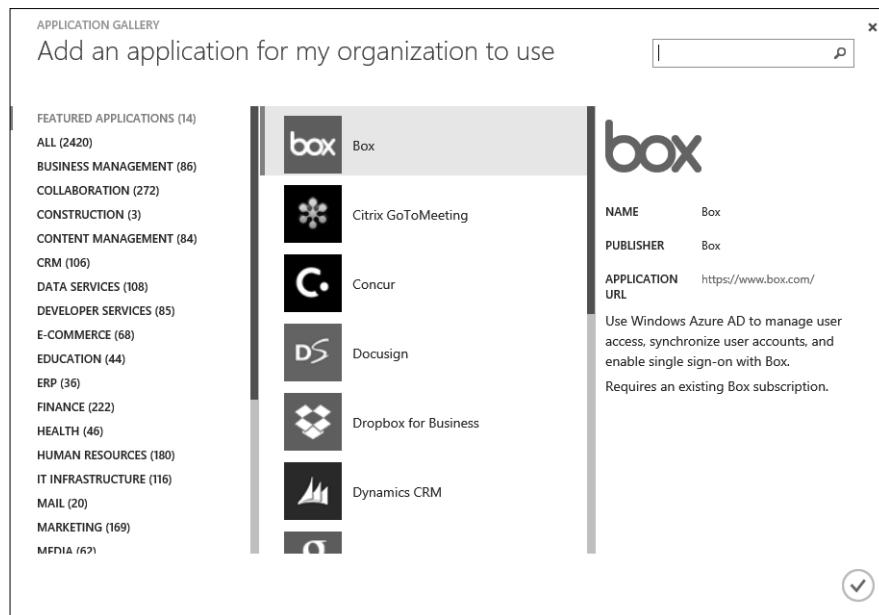


FIGURE 5-15 Application Gallery in the management portal

Configuring access to SaaS applications

Configuring user access to a SaaS application will vary depending on the sign in capabilities of the application. Azure Active Directory supports *single sign-on* and automatic *user provisioning* for third-party SaaS applications. Applications from the gallery will support one or both.

After an application has been added to the directory, the management portal provides a quick start guide on the steps needed to integrate it with your directory, as shown in Figure 5-16.

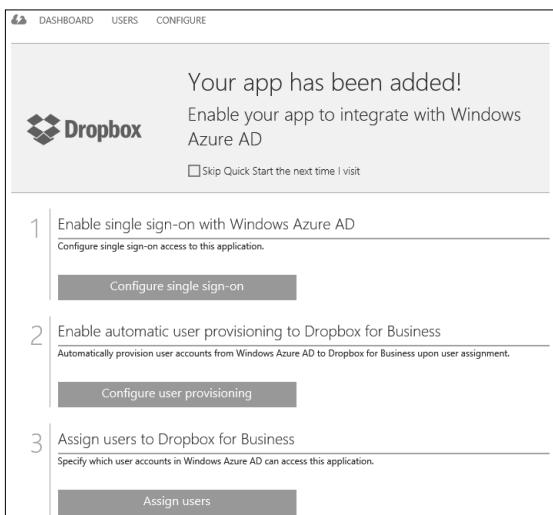


FIGURE 5-16 Quick start guide to adding Dropbox for Business to Azure AD

MORE INFO CONFIGURING USER ACCESS TO SAAS APPLICATIONS

Given the number of applications available in the application gallery, it's not feasible to provide step-by-step instructions for every application. The management portal does a nice job guiding you through the broader configuration tasks required for each application, such as configuring single sign-on, user provisioning, and assigning user access. There are also step-by-step tutorials for some common SaaS applications at http://msdn.microsoft.com/en-us/library/azure/dn308590.aspx#BMK_Tutorials.

Single sign-on

Azure Active Directory supports two modes for single sign-on, which are *federation-based* and *password-based*. Both modes provide a single sign-on experience for the user but differ on the credentials used to sign in to the SaaS application.

Federation-based single sign-on requires that users authenticate to Azure Active Directory using their organizational account credentials to access the application. In other words, a federated trust exists between Azure Active Directory and the SaaS application. In this mode, the SaaS application redirects users to sign in using an application (protocol) endpoint from your Azure Active Directory. The application endpoint used will depend on the protocol supported by the SaaS application. Azure Active Directory supports the WS-Federation, SAML-P, and OAuth protocols and therefore provides the expected sign-in and sign-out endpoints for each. This mode also requires that a certificate be uploaded to the third-party SaaS application that

it will use to validate authentication tokens issued by Azure Active Directory. The management portal provides the application endpoint URL and certificate during the configuration process, both of which will be needed when configuring the SaaS application for single sign-on.

NOTE EXISTING SINGLE SIGN-ON

Many applications that support the federation-based single sign-on mode will also have an option for existing single-sign-on. The difference with this option is that Active Directory Federation Services (AD FS) and other third-party on-premises STSs are used to configure single sign-on with the SaaS application. This option is ideal for organizations that already have a SSO solution implemented in their on-premises environment.

Password-based single sign-on uses the username and password from the third-party SaaS application to sign in the user. In this mode, the user authenticates to the SaaS application using his or her credentials for the application, not Azure Active Directory. The credentials for the user are encrypted and securely stored in Azure AD, such that an authenticated user is able to get a single sign-on experience through a browser extension that retrieves the credentials from Azure AD and presents them to the application for the user.

Automatic user provisioning

Some applications enable you to configure automatic user provisioning whereby user accounts for the application are automatically added or removed as users are added or removed from the Azure Active Directory. The setup experience for this feature varies by application, but it generally involves signing in to the third-party application using administrative credentials and granting permission to Azure AD to provision user accounts in the application.

MORE INFO MANAGING AZURE ACTIVE DIRECTORY USING WINDOWS POWERSHELL

The objectives discussed in this chapter are easily accomplished using the management portal and most are one-time configurations not worthy of being automated. Still, it is possible to achieve many of these administrative tasks using the Azure Active Directory Module for Windows PowerShell.

Before you can install the Azure Active Directory Module for Windows PowerShell, you must first install the Microsoft Online Sign-in Assistant for IT Professionals. Details about downloading, installing, and using the Azure Active Directory Module are available at <http://msdn.microsoft.com/en-us/library/azure/jj151815.aspx>.

Assigning user access to applications

After configuring the application for single sign-on or user provisioning, you can proceed to the final step, which is to assign user access to the application. Managing access to the application is done in the Users page for the application, as shown in Figure 5-17, where access can be assigned for a user, removed for a user, and the user's account settings can be edited, such as in the case of password-based single sign-on.

The screenshot shows the Azure Active Directory management portal interface. At the top, there's a header with the 'box' application name and navigation links for DASHBOARD, USERS, and CONFIGURE. Below this is a table titled 'ACCESS' with columns for DISPLAY NAME, USER NAME, JOB TITLE, DEPARTMENT, and ACCESS. Two users are listed: Jay Hamlin (jayhamlin@contoso...) with 'Yes' under ACCESS, and John Doe (johndoe@contoso...) with 'No'. At the bottom of the table are three buttons: ASSIGN, EDIT ACCOUNT, and REMOVE.

DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT	ACCESS
Jay Hamlin	jayhamlin@contoso...			Yes
John Doe	johndoe@contoso...			No

FIGURE 5-17 Managing access to the Box application using the management portal

MORE INFO ASSIGNING ACCESS FOR A GROUP TO A SAAS APPLICATION

One of the benefits of the Azure Active Directory Basic and Premium editions is the ability to assign or remove access to applications using groups. This can save you considerable time when you're managing application access for a large group of users. Information about how to assign application access for a group is available at <http://msdn.microsoft.com/en-US/library/azure/dn621141.aspx>.

Accessing applications from the Access Panel

SaaS applications added to Azure Active Directory are available to users in the directory through the Access Panel. The Access Panel is a portal, separate from the management portal, where users can see and launch the applications they have been assigned access to. Users can sign in to the Access Panel at <https://myapps.microsoft.com> using their organizational account credentials. They can launch applications that they have access to from the Applications page in the management portal, as shown in Figure 5-18.

The screenshot shows the Microsoft Access Panel. At the top, there's a browser-style header with back and forward buttons, a search bar containing 'https://account.activedirectory.windowsazure.com/applications', and a lock icon. Below this is a 'Microsoft Azure' header. The main area is titled 'applications' and shows three application tiles: 'Office 365 Exchange Online ...', 'Office 365 SharePoint Online ...', and 'Dropbox for Business ...'.

FIGURE 5-18 Access Panel showing SaaS applications available for a user

MORE INFO MY APPS SSO APP LAUNCHER FOR IOS 7

Users of iOS 7 devices can also access the applications they have been assigned access to using the My Apps application available in the Apple App store. The application provides the same features available in the Access Panel except it is optimized for iPhone and iPad devices. More information, including a link to the application in the Apple App Store, is available on the Active Directory Team Blog at <http://blogs.technet.com/b/ad/archive/2014/03/20/my-apps-sso-app-launcher-for-ios-now-available.aspx>.

Customizing the Access Panel and sign-in page

The Access Panel and the sign-in page users use to authenticate are generalized such that they can be used by all Azure Active Directory tenants. In the Premium edition of Azure Active Directory, you can apply customized branding to the sign-in page and Access Panel for your users to display your organization's logo, custom messaging, and colors. These customization features are available in the Configure page of the directory under the Directory Properties section. In Customize Branding, you can apply the desired customizations, as shown in Figure 5-19.

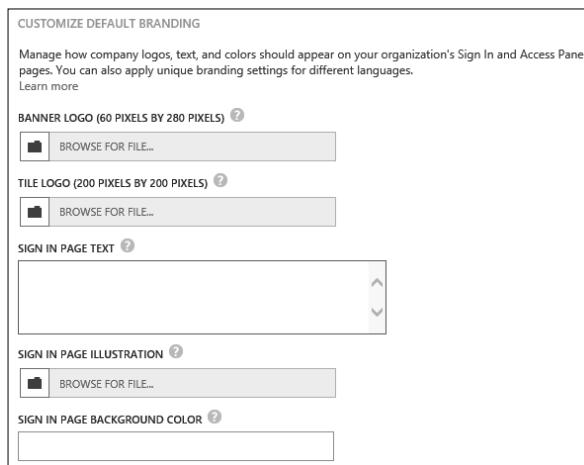


FIGURE 5-19 Customizing branding for the sign-in page and Access Panel

The customization options that are applicable to the Access Panel are limited to the banner logo. The banner logo and the other settings apply to the sign-in page.

MORE INFO CUSTOM BRANDING THE SIGN-IN AND ACCESS PANEL

Guidance about image constraints and illustrations depicting where customizations appear in the sign-in page and Access Panel is available at <http://msdn.microsoft.com/library/azure/dn532270.aspx>.

Configuring Multi-Factor Authentication

Multi-Factor Authentication (MFA) is an effective way to add additional security to applications and resources. Multi-Factor Authentication in Azure AD works by first challenging the user for a valid username and password during sign in. If successfully authenticated, the second leg of authentication begins by challenging the user to verify he or she using a *mobile app, phone call, or text message*. This layered approach to authentication increases security by challenging you during sign in for something known, such as a password, and something you have, such as a mobile device. Having one without the other is not sufficient to gain access to a system protected by MFA.

MORE INFO AZURE MULTI-FACTOR AUTHENTICATION SERVICE SOLUTIONS

Microsoft Azure Multi-Factor Authentication is a service that you can use to add additional security to resources in the cloud and in on-premises environments. This objective discusses adding MFA to Azure AD to secure access to Azure, Microsoft Online Services such as Office 365, and SaaS applications integrated with the directory. Details about the kinds of solutions that can be implemented for an on-premises environment using the Azure Multi-Factor Authentication service are available at <http://msdn.microsoft.com/en-us/library/azure/dn249466.aspx>.

MFA for administrators of an Azure subscription is available at no additional cost. However, to extend MFA to users of the directory and to be able to run reports from the MFA portal requires that you create a new MFA provider and configure it for your directory. You can choose from two billing options when creating a MFA provider, which are *per user* and *per authentication*.

The *per user* option is ideal in scenarios where you want MFA for a fixed number of users that authenticate regularly. The *per authentication* option is ideal for larger groups of users that authenticate less frequently. After a billing option is chosen and the MFA provider has been created, it cannot be changed. Therefore, it's a good idea to review the pricing details for each option at <http://azure.microsoft.com/en-us/pricing/details/multi-factor-authentication/>. If you do need to change the billing option, you must create a new MFA provider to replace the existing one.

Create a Multi-Factor Authentication provider

To create a new MFA provider using the management portal, select the Multi-Factor Auth Provider option under Application Services when creating a new resource, as shown in Figure 5-20.

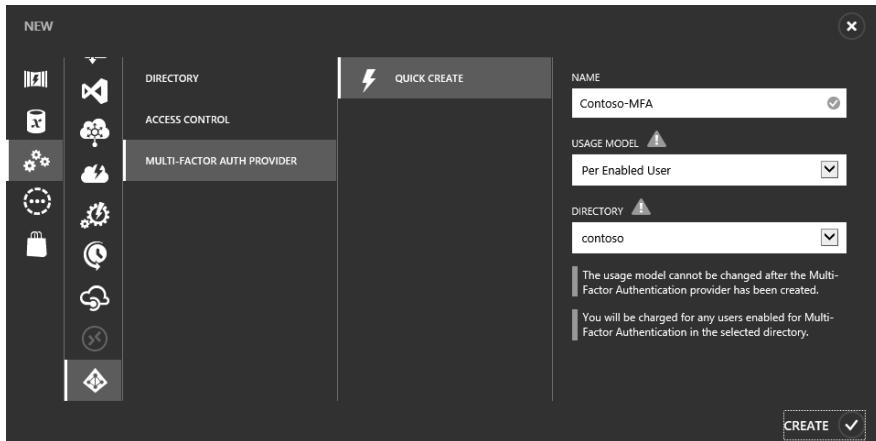


FIGURE 5-20 Creating a Multi-Factor Authentication provider

Configuring a Multi-Factor Authentication provider

The Azure Multi-Factor Authentication service is configurable through a separate portal that you can reach from the management portal. To access the Azure MFA portal, highlight the directory in the management portal and click the Multi-Factor Auth Providers tab at the top of the page. Select the MFA provider, and then click Manage .

The Azure MFA portal is where you can run MFA usage reports and configure settings for how the Azure MFA service will be used for your organization, as shown in Figure 5-21.

A screenshot of the Azure Multi-Factor Authentication service portal. The header features a mobile phone icon and the text 'Azure Multi-Factor Authentication'. On the left is a sidebar with links for User Administration (Block/Unblock Users, One-Time Bypass), View a Report (Usage, Server Status, Blocked User History, Bypassed User History, Fraud Alert, Queued), Configure (Settings, Caching, Voice Messages, Notifications), and Downloads (Server, SDK). The main content area is titled 'Welcome' and includes a message about tokenless MFA availability, the account ID 'Contoso-MFA', and 'Account ID: BOZI-FHG-DSUOR'. It also lists four options: 'VIEW A REPORT' (View usage of all users of Multi-Factor Authentication within an organization), 'CONFIGURE' (Configure Multi-Factor Authentication settings such as caching, voice messages and notifications received by users), 'DOWNLOADS' (Download the Multi-Factor Authentication Server), and a 'Contact Support' link.

FIGURE 5-21 Azure Multi-Factor Authentication service portal

In the Configure section, the following options are available:

- **Settings** Configure the number of attempts to allow during a MFA call, the phone number to be used for caller ID, the ability to empower users to submit fraud alerts, and whether to block a user's account after submitting a fraud report.
- **Caching** Set up a cache such that, after a user has successfully authenticated, subsequent authentication attempts within the time period specified for the cache will automatically succeed. A cache can be defined as one of three types as follows and multiple caches can be configured for a MFA provider:
 - **User** A user who has previously authenticated will be automatically authenticated on subsequent authentication attempts within the cache seconds specified.
 - **User, authentication type, application name** A user who has previously authenticated will be automatically authenticated on subsequent authentication attempts within the cache seconds specified if the user is using the same type of authentication and accessing the same application.
 - **User, authentication type, application name, IP address** A user who has previously authenticated will be automatically authenticated on subsequent authentication attempts within the cache seconds specified if the user is using the same type of authentication, accessing the same application, and is from the same IP address. This type of cache is only applicable for on-premises MFA servers and line of business applications developed using the MFA SDK.
- **Voice Messages** Replace the standard messages used during MFA calls with your own custom messages. The voice message can be used to replace message types such as greeting, retry, fraud greeting, and more. The voice message can also be applicable to a specific application.
- **Notifications** Specify email addresses that should receive notifications when a fraud alert is reported, a user account is locked, or a one-time bypass is used.

Enabling Multi-Factor Authentication for users

Multi-Factor Authentication can be enabled for users using a separate Multi-Factor Authentication portal. You can access this portal from the management portal by going to the Users page for your directory, and clicking Manage Multi-Factor Auth.

To enable Multi-Factor Authentication for a user, click the check mark button next to the user. Next, click the Enable link under the Quick Steps section, as shown in Figure 5-22.

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input checked="" type="checkbox"/> Jay Hamlin	jayhamlin@contosodir.onmicrosoft.com	Disabled
<input type="checkbox"/> john doe	johndoe@contosodir.onmicrosoft.com	Enforced

Jay Hamlin
jayhamlin@contosodir.onmicrosoft.com
quick steps
Enable
Manage user settings

FIGURE 5-22 Enabling Multi-Factor Authentication for a user

After enabling Multi-Factor Authentication for a user, the user's MFA status is updated to *Enabled*. It is a subtle but important distinction to note that MFA for the user is not being enforced yet. At this stage, the service has only been enabled for the user. To be enforced requires that user configuration for additional security verification be completed, which is the topic of the next section.

User configuration for additional security verification

A user that has been enabled for MFA will be prompted at the next sign in that an administrator has required the user to set up the account for additional security verification to be used during Multi-Factor Authentication. During this process, the user is able to select the contact method to be used during Multi-Factor Authentication, which can be one of the following:

- Mobile phone
- Office phone
- Mobile application

Depending on the method selected, the user will then be able to provide the additional information needed. For example, when choosing the mobile phone method, the user is then prompted to provide the phone number and whether to be contacted via text message or phone call from the Multi-Factor Authentication service, as shown in Figure 5-23.

You are required to sign in with your password as well as a registered device. This makes it harder for a hacker to sign in with just a stolen password. Follow these steps to get your account set up. [View video](#)

Step 1: Specify the contact method we should use by default

Mobile phone

United States (+1) 123-456-7890

Mode

Send me a code by text message

Call me

[next](#)

Standard telephone and SMS charges will apply.

FIGURE 5-23 Setting up additional security verification using the mobile phone contact method

After the user has verified the settings in step two, the Multi-Factor Authentication status for the account is updated to Enforced, and the user will start getting prompted for MFA during sign in.

MORE INFO APPLICATION PASSWORDS WITH AZURE MULTI-FACTOR AUTHENTICATION

For non-browser applications such as Microsoft Outlook and Lync, MFA is not supported. As a result, users who have MFA configured can't access such applications using just their organizational account credentials. Application passwords are created during additional security verification for users indicating they use non-browser applications. By updating an application to use the generated application password instead, a user is able to bypass Multi-Factor Authentication when signing in to use the application. More information about application passwords, applications that support using them, and how they are created is available at <http://msdn.microsoft.com/en-us/library/azure/dn270518.aspx#howapppassword>.

Federating with Facebook and Google ID

When adding users to Azure Active Directory, you typically add users to your organization. As an example, if the organization is Contoso, as a user is added you assign a username, such as jayhamlin@contoso.com.

It's also possible to add a user to the directory using their identity with a social identity provider such as Facebook, Google, and others. These are referred to as *federated identity providers* and are the authority for that user's identity. To add an external user to your directory, set the type of user to User With An Existing Microsoft Account, and then enter the email address associated with the user's Microsoft account.

MORE INFO MICROSOFT ACCOUNTS

Microsoft accounts are used by many popular Microsoft applications, online services, and devices such as Skype, OneDrive, Xbox Live, Windows Phone, Surface, and more. Therefore, users already using these apps, services, and devices already have a Microsoft account.

That account can be used to add them as external users to an Azure Active Directory. Users that don't already have a Microsoft account can get one at <http://microsoft.com/account> using any email address they already have, such as a Facebook, Google ID, or other email addresses. Users can then be added to an Azure Active Directory but use their existing email address when signing in.



EXAM TIP

When an external user of a directory signs in to access an application protected by Azure Active Directory, the user authenticates to the federated identity provider, not Azure Active Directory.

Adding a user to a directory using a Microsoft account is useful in situations where you want to grant access to applications for users who are not part of the organization but may be contracted to work on short-term project assignments. This has the benefit of these users being able to use existing credentials to access applications rather than being given new credentials to keep up with. When the user no longer needs access to the applications, you can remove the user's account from Azure Active Directory. The user's Microsoft account continues to work as it always has for other online applications and services.



Thought experiment

Configure a SaaS application for single sign-on

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You are the IT administrator for Contoso and responsible for installing and managing SaaS applications for the organization. Contoso has purchased a SaaS application subscription from an ISV and wants users in Contoso to be able to access and use the application using their Contoso credentials.

You have already confirmed that the SaaS application is in the Azure application gallery. You also have confirmed that the SaaS application supports federated single sign-on.

- 1. How will you add the SaaS application to the Contoso Azure Active Directory?**
- 2. How should you configure single sign-on for the application?**

Objective summary

- Azure Active Directory is the identity provider for users added to a directory as a new user in the organization. In this scenario, the organization owns and manages the user's identity. For users added to a directory using a Microsoft account, the user and the federated identity provider where the account was created own and manage the user's identity.
- A user added to a directory using a Microsoft account will not be able to use the Access Panel to see and launch applications assigned to him or her. Instead, the user must access the application URL and sign in using credentials associated with the account.
- A multi-factor authentication provider is available as either a per user or per authentication billing plan.
- SaaS applications added to a directory support single sign-on or automatic user provisioning configurations. For single sign-on, options may include password-based, federation-based, and existing single sign-on.

- The sign-in page and Access Panel can be custom branded for Azure Active Directory Premium users. You can apply localized branding settings for all or selected settings to support users in different locales.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the “Answers” section at the end of this chapter.

1. How can Azure Active Directory users see, and launch, the applications they have been granted access to? (Choose all that apply.)
 - A. management portal
 - B. Active Directory Portal
 - C. Access Panel
 - D. “My Apps” from the Apple App Store
2. Which of the following are valid contact methods for Multi-Factor Authentication users? (Choose all that apply.)
 - A. Mobile phone
 - B. Office phone
 - C. Email
 - D. Mobile application
3. Which two single sign-on modes does Azure Active Directory support for SaaS applications?
 - A. Automatic user provisioning
 - B. Password-based
 - C. Active Directory Federation Service (AD FS)
 - D. Federation-based
4. What is the URL where users can access the Access Panel?
 - A. <https://myapps.microsoft.com>
 - B. <https://portal.azure.com>
 - C. <http://azure.microsoft.com/en-us/marketplace/active-directory>
 - D. <http://account.windowsazure.com/organization>

Objective 5.3: Integrate an app with Azure AD

Organizations that develop their own line-of-business (LOB) applications can protect access to those applications using Azure Active Directory. The type of LOB application that can be integrated with Azure Active Directory can vary. It can be a web application that users access using their browser, or a desktop client application that is installed on the user's computer. It may be a web service lacking a user interface that other LOB applications depend on to provide a complete solution. It could also be an application that has capabilities to create, edit, or even delete objects in the directory.

The process for integrating an application developed in-house requires careful coordination between the IT professional managing the Azure Active Directory, and the application developer responsible for developing the application. The content in this objective draws attention to the skills and knowledge the IT professional needs to integrate these kinds of applications with Azure Active Directory and configure application permissions.

This objective covers how to:

- Add a web application or web service
- Add a native application
- Configure graph API permissions for an application

Add a web application or web service

The process of integrating either a web application or web service with Azure Active Directory using the management portal begins the same way. In the Applications page of your directory, click Add at the bottom of the page and choose the option to Add An Application My Organization Is Developing. This action launches a wizard where you can provide a name for the application and also indicate the type of application, as shown in Figure 5-24. The name can be anything you want it to be. Notice that for the application type, web application and web service (also known as web API) are considered one and the same.

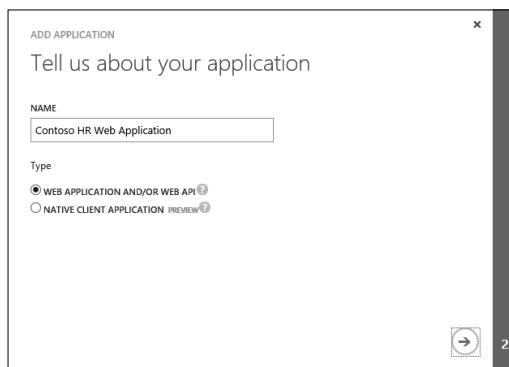


FIGURE 5-24 Adding a web application or web service to Azure Active Directory

After choosing the application type for Web Application And/Or Web API, the second and final page in the wizard prompts you for the application's sign-on URL and the application ID URI, as shown in Figure 5-25. The sign-on URL is the URL that clients will use to access the application. The application ID URI is a URI that uniquely identifies the application in your Azure Active Directory. The URI can be anything you want as long as it is unique to your directory and a valid URI.

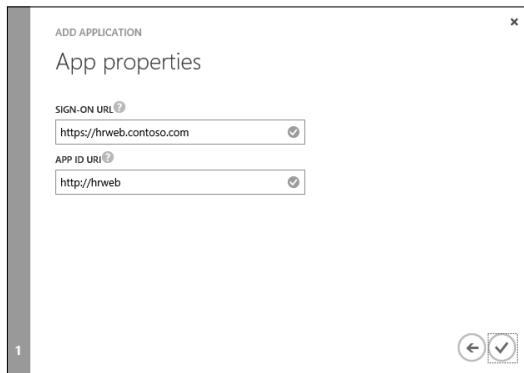


FIGURE 5-25 Specifying the sign-on URL and application ID URI

MORE INFO SIGN-ON URL AND APPLICATION ID URI

A subtle distinction between the sign-on URL and the application ID URI is the use of a URL for one and a URI for another. Many times these two terms, URL and URI, are used interchangeably. However, they are very different in their definition.

The uniform resource locator (URL) identifies a resource on the web and can be used to access that resource using, for example, your browser.

The uniform resource identifier (URI) identifies a resource. Usually the resource is a resource on the web, but it doesn't have to be.

A good blog discussing the relationship between URLs, URIs, and uniform resource names (URNs) is available at <http://www.cloudidentity.com/blog/2013/03/02/url-urn-uri-oh-my/>.

By completing the wizard to add the application you have created only the infrastructure that Azure Active Directory needs to support authenticating users of your application. Beyond the four settings you provided previously for this application, Azure Active Directory has also configured additional settings in your directory that application developers will need to build the application. This is where the careful coordination between the IT professional and application developer begins.

The application developer needs the following settings to develop and configure the application that will be protected by Azure Active Directory.

- **Application ID URI** The URI that you provided in the Add Application Wizard for the application. The application developer will use this in the code and/or configuration to associate the application with this entry in the directory.
- **Reply URL** By default, this is the sign-on URL you provided in the Add Application Wizard for the application. When Azure Active Directory issues a security token for a user of the application, it redirects the client back to the application URL so that the token can be presented to the application and validated.
- **Application endpoints** Endpoints that application developers can reference in the application code and/or configuration that are used to sign in and sign out users of the application.

The first two settings can be retrieved in the Single Sign-On section of the Configure page for the application, as shown in Figure 5-26. To get to the Configure page, click the application in the Applications page, and then click the Configure tab.

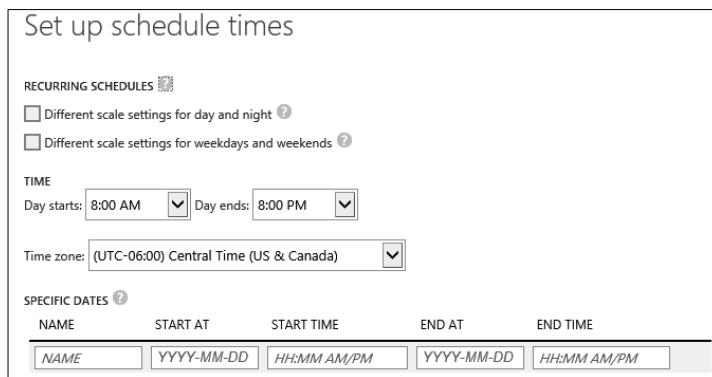


FIGURE 5-26 Single Sign-On section of the Configure page for an application in Azure Active Directory

The application endpoints can be accessed from the management portal by clicking View Endpoints. The application endpoints are the same for all applications in your Azure Active Directory. However, they are unique to each tenant (or organization) in Azure Active Directory. Azure Active Directory supports the following protocols and makes available application endpoints for each, as shown in Table 5-5.

TABLE 5-5 Protocols and application endpoints supported by Azure Active Directory

Protocol	application endpoints
WS-Federation	<a href="https://login.windows.net/<tenant>/wsfed">https://login.windows.net/<tenant>/wsfed
SAML-P	<a href="https://login.windows.net/<tenant>/saml2">https://login.windows.net/<tenant>/saml2
OAuth	<a href="https://login.windows.net/<tenant>/oauth2/token">https://login.windows.net/<tenant>/oauth2/token <a href="https://login.windows.net/<tenant>/oauth2/authorize">https://login.windows.net/<tenant>/oauth2/authorize

The <tenant> in the URL for the application endpoints above is a GUID/ID assigned to your tenant (or organization) in Azure Active Directory and therefore referred to as *tenant specific endpoints*. Application developers use these application endpoints in code and/or configuration to externalize the authentication of users to Azure Active Directory. Which endpoint is used depends largely on the type of application being developed and the authentication requirements for the application. Figure 5-27 shows all of the application endpoints available for a tenant in Azure Active Directory.

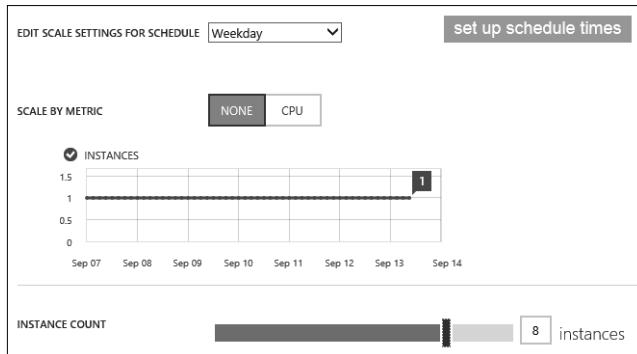


FIGURE 5-27 Application endpoints for an Azure Active Directory

In addition to the application protocol endpoints shown previously in Table 5-2, Azure Active Directory publishes additional tenant-specific endpoints that application developers may require when developing applications protected by Azure Active Directory. These are the federation metadata document and graph API endpoints.

The federation metadata document is an XML document that describes the security token service (STS) that is responsible for issuing SAML tokens to authenticated users. The URL for the STS is unique for each tenant in Azure Active Directory and is of the form <https://sts.windows.net/<tenant>>. This document also contains the certificate that Azure Active Directory will use to sign the tokens it issues and is one of the primary means by which applications validate tokens that are presented by clients accessing the application. If an application receives a token signed by an issuer other than the one it has externalized authentication to, then it can deny access to the application. The remainder of the federation metadata document describes the application endpoints for the WS-Federation and SAML-P protocols.

You can view the contents of the federation metadata document by opening the endpoint URL in a browser. However, it is more common that application development tools such as Visual Studio consume the metadata document because developers build applications using WS-Federation or SAML-P. The tools in Visual Studio, and other developer tools, take care of the extremely intricate configuration details required for the application to externalize authentication to Azure Active Directory by extracting the necessary information from the federation metadata document.

MORE INFO FEDERATION METADATA DOCUMENT

The federation metadata document is formatted using the Web Services Federation Language (WS-Federation) version 1.2. It isn't a proprietary Microsoft format. Therefore, any application development tool capable of interpreting this specification can be used by application developers to build applications protected by Azure Active Directory.

The protocol-specific application endpoints for WS-Federation and SAML-P that are described in the federation metadata document are also open standards maintained by OASIS. Therefore, any application that adheres to these specifications can be protected by Azure Active Directory using these protocols.

The specifications are available at <http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html>.

The graph API endpoint is used by applications to retrieve additional properties of directory objects such as users and security groups. It is also used by applications to create, edit, or even delete directory objects if the application has been configured with permissions to do so. This endpoint will be discussed further in the Configure Graph API permissions for an application section.

NOTE APPLICATIONS DEVELOPED INTERNALLY DON'T APPEAR IN THE ACCESS PANEL

Web applications and/or web services developed by an organization do not appear in the Access Panel for users. Therefore, it is expected that users will know the URL of line-of-business (LOB) applications they have been assigned access to. This is not suggesting that these applications are less secure. This is just a feature currently not supported by the Access Panel.

Enable access to a web application or web service from other applications

Many applications are architected in a way that allows certain features of the application to evolve and be versioned independently while collectively providing a complete solution for the business. For example, a web application that users interact with in a browser may have a dependency on a set of web services (or web APIs) that are used to send and receive data to a database, or perform business logic for the web application.

For a web service to be accessible from other applications registered in the directory, its application manifest must be updated to allow it. The application manifest is used to configure properties for an application that the management portal does not provide a user interface for. Enabling access to a web service from another application is one example where the application manifest has to be edited and can be done as follows:

1. Go to the Applications page in the management portal.
2. Click the name of the application whose manifest you want to edit.

3. At the bottom of the page, click Manage Manifest, and then select the Download Manifest option.
4. Save the manifest file to your local computer.
5. Edit the file using a text editor such as Notepad.
6. In the management portal, click Manage Manifest, and select the Upload Manifest option.
7. Click the check mark to upload the edited manifest file.

The application manifest is a JSON-formatted file. Listing 5-1 illustrates the default manifest for a web service added to Azure Active Directory.

LISTING 5-1 Application manifest for a web application/web service added to Azure Active Directory

```
{  
    "allowActAsForAllClients": null,  
    "appId": "7f12aa02-123f-4599-ad5d-f9851e36ce84",  
    "appMetadata": {  
        "version": 0,  
        "data": []  
    },  
    "appRoles": [],  
    "availableToOtherTenants": false,  
    "displayName": "Contoso Support Web Service",  
    "errorUrl": null,  
    "groupMembershipClaims": null,  
    "homepage": "https://contoso.com/support-api",  
    "identifierUris": [https://contoso-support-api  
                     https://contoso-support-api]  
],  
    "keyCredentials": [],  
    "knownClientApplications": [],  
    "logoutUrl": null,  
    "oauth2AllowImplicitFlow": false,  
    "oauth2AllowUrlPathMatching": false,  
    "oauth2Permissions": [],  
    "oauth2RequirePostResponse": false,  
    "passwordCredentials": [],  
    "publicClient": null,  
    "replyUrls": [https://contoso.com/support-api]  
],  
    "requiredResourceAccess": [  
        {  
            "resourceAppId": "00000002-0000-0000-000000000000",  
            "resourceAccess": [  
                {  
                    "id": "311a71cc-e848-46a1-bdf8-97ff7156d8e6",  
                    "type": "Scope"  
                }  
            ]  
        }  
    ],  
},
```

```

    "samlMetadataUrl": null,
    "defaultPolicy": [],
    "extensionProperties": [],
    "objectType": "Application",
    "objectId": "1688c779-e30b-4dea-9433-ea71bb44dced",
    "deletionTimestamp": null,
    "createdOnBehalfOf": null,
    "createdObjects": [],
    "manager": null,
    "directReports": [],
    "members": [],
    "memberOf": [],
    "owners": [],
    "ownedObjects": []
}

```

To allow this application to be accessible from other applications registered in Azure Active Directory requires that the *oauth2Permissions* node be updated with the property settings to allow access to it. Listing 5-2 illustrates the change to the *oauth2Permissions* node to allow full-delegated user access to the application.

LISTING 5-2 An abbreviated application manifest with *oauth2Permissions* added

```

... abbreviated ...
    "oauth2AllowImplicitFlow": false,
    "oauth2AllowUrlPathMatching": false,
    "oauth2Permissions": [
        {
            "adminConsentDescription": "Allow the app full access to the Contoso Support Web
API on behalf of the signed-in user",
            "adminConsentDisplayName": "Have full access to the Contoso Support Web API",
            "id": "C39B0282-F0F4-431D-941B-777DC456C962",
            "isEnabled": true,
            "origin": "Application",
            "type": "User",
            "userConsentDescription": "Allow the application full access to the Contoso
Support Web API on your behalf",
            "userConsentDisplayName": "Full access to Contoso Support Web API",
            "value": "user_impersonation"
        },
        "oauth2RequirePostResponse": false,
    ... abbreviated ...

```

With this edit in place, another application in Azure Active Directory will be able to see and configure access to this application if needed, which you see in the subsequent section where adding a native application to Azure Active Directory is discussed.

Adding a native application

Integrating a native application with Azure Active Directory using the management portal begins with a similar process to what you learned in the previous section for web applications and web services.

1. Go to the Applications page of your directory.
2. Click Add at the bottom of the page.
3. Choose the option to Add An Application My Organization Is Developing.
4. In the first page of the Add Application Wizard, provide a name for the application and select the option to indicate the application is a Native Client Application.
5. In the second page of the Add Application Wizard, provide a Redirect URI. This is a URL that uniquely identifies the application in your Azure Active Directory. It can be anything you want as long as it is unique to your directory and a valid URL.

As before, by completing the wizard to add a native application you have created the infrastructure that Azure Active Directory needs to authenticate users of your application. For native applications, an application developer needs the following settings to develop and configure the native application that will be protected by Azure Active Directory:

- **Redirect URI** The URI you provided in the second page of the Add Application Wizard.
- **Client ID** An identifier that Azure Active Directory generates and is used to identify the native application. Application developers use the Client ID in the application when accessing the graph API or other web APIs registered in Azure Active Directory.

You can get both of these values from the Properties section of the Configure page for the application, as shown in Figure 5-28.

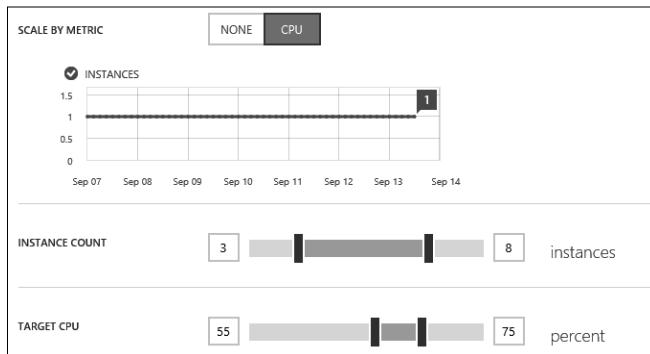


FIGURE 5-28 Properties of a native client application added to Azure Active Directory

Configure access to other applications

Native applications added to Azure Active Directory use the OAuth application endpoints to acquire an access token for a specified resource such as a web service application registered in the same directory. However, adding the native client application to Azure Active Directory does not mean the application has permissions to access the web service. Additional configuration must be added in Azure Active Directory to allow the native application to access the web service. This configuration is easily added using the management portal.

1. Go to the Applications page of your directory.
2. Click the name of the native application.
3. Click the Configure tab at the top of the page.
4. In the Permissions To Other Applications section, select the application you want to enable access to from the native application in addition to the appropriate permissions.

Figure 5-29 is an example of a native application being configured with permissions to a web service also registered in Azure Active Directory.

S1	STANDARD	S2	STANDARD	S3	STANDARD
1	Core	2	Core	4	Core
1.75	GB RAM	3.5	GB RAM	7	GB RAM
Storage	50 GB	Storage	50 GB	Storage	50 GB
Custom domains / SSL	5 SNI, 1 IP	Custom domains / SSL	5 SNI, 1 IP	Custom domains / SSL	5 SNI, 1 IP
Auto scale	Up to 10 instances	Auto scale	Up to 10 instances	Auto scale	Up to 10 instances
Backup	Daily	Backup	Daily	Backup	Daily
Website staging	5 slots	Website staging	5 slots	Website staging	5 slots
Geo availability	Traffic Manager	Geo availability	Traffic Manager	Geo availability	Traffic Manager
44.64		89.28		178.56	
USD/MONTH (ESTIMATED)		USD/MONTH (ESTIMATED)		USD/MONTH (ESTIMATED)	

FIGURE 5-29 Configuring permissions to other applications for a native application

MORE INFO OAUTH 2.0 IN AZURE ACTIVE DIRECTORY

When a native application accesses a web application or web service registered in Azure Active Directory, it does so using the Authorization Code Grant type. This is part of the OAuth 2.0 Authorization Framework specification available at <http://tools.ietf.org/html/rfc6749>.

The Authorization Code Grant flow makes use of the two OAuth application endpoints provided by Azure Active Directory by first obtaining an authorization code from the OAuth 2.0 authorization endpoint, and then later exchanging it for a token it obtains from the OAuth 2.0 token endpoint.

Additional information about how OAuth 2.0 is used in Azure Active Directory and best practices for application developers is available at <http://msdn.microsoft.com/en-us/library/azure/dn645545.aspx>.

Configuring graph API permissions for an application

The graph API is used by applications that need access to read directory objects in Azure Active Directory or to create, update, and delete objects. For example, an application may need to query the directory to determine a user's manager in the organization or add the user to a particular security group. Azure Active Directory supports these kinds of application requirements, but your application must be configured with the necessary permissions to allow it as this goes beyond the default settings that provide single sign-on support for users.

The graph API is available for both web applications/web services and native applications, and can be configured via application permissions or delegated permissions.

Application permissions may be assigned to access the directory without a user context and are only available for web applications/web services. Delegated permissions are used to access the directory as the user signed in to the application and are available for both web applications/web services and native applications.

Permissions to access the graph API can be added to the configuration for an application using the management portal by selecting either the Read Directory Data or Read And Write Directory Data permission for the Windows Azure Active Directory application. Figure 5-30 illustrates setting the Read And Write Directory Data permission for a web application added to the directory.

B1	BASIC	B2	BASIC	B3	BASIC
1	Core	2	Core	4	Core
1.75	GB RAM	3.5	GB RAM	7	GB RAM
	Storage	10 GB		Storage	10 GB
	Custom domains			Custom domains	
	Manual scale	Up to 3 instances		Manual scale	Up to 3 instances
	32.74		65.47		130.94
	USD/MONTH (ESTIMATED)		USD/MONTH (ESTIMATED)		USD/MONTH (ESTIMATED)

FIGURE 5-30 Setting Graph API permissions for an application in Azure Active Directory



Thought experiment

Configure a line-of-business application in Azure Active Directory

In this experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You are the IT administrator for Contoso and are responsible for managing the line-of-business applications developed by the development team at Contoso. A new web application has been developed for users to manage their benefit enrollment using their browsers. Per the application developers, the new benefits portal needs to be able to retrieve all properties for a sign-in user to pre-populate information for users on certain pages. The new benefits portal also includes a web service that the web application must be able to access.

1. What steps will you take to add the application to Azure Active Directory?
2. How will you configure the applications to meet the two requirements given to you by the development team?

Objective summary

- For SaaS applications configured using federation-based single sign-on, users are automatically signed in using their organizational account information in Azure Active Directory.
- For SaaS applications configured using password-based single sign-on, users are automatically signed in using their account information from the application. In this scenario, the user account information is securely stored in Azure Active Directory.
- Azure Active Directory provides application endpoints for WS-Federation, SAML-P, and OAuth 2.0 protocols. Azure Active Directory supports security token formats SAML and JWT.
- The oauth2Permissions array node in a web service application's manifest can be edited to allow the web service to be accessed from other applications registered in the directory, such as web applications or a native applications.
- The graph API is used by applications to create, read, update, or delete directory objects in Azure Active Directory. An application must be configured for either the Read Directory Data or Read And Write Directory Data permissions to use the graph API.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which protocols does Azure Active Directory provide application endpoints for? (Choose all that apply.)
 - A. WS-Federation
 - B. Federation metadata document
 - C. SAML-P
 - D. OAuth 2.0
2. Which application setting in Azure Active Directory is used to uniquely identify a web application that has been added to the directory?
 - A. Sign-on URL
 - B. Reply URL
 - C. Application ID URI
 - D. Name

3. What is the URL for the security token service (STS) endpoint that issues a SAML token for an authenticated user?

 - A. `https://sts.windows.net/<tenant>`
 - B. `https://login.windows.net/<tenant>/saml2`
 - C. `https://login.windows.net/<tenant>/wsfed`
 - D. `https://graph.windows.net/<tenant>`
4. A developer building a web application for your organization needs the certificate that your Azure Active Directory uses to sign SAML tokens. Which application endpoint should you provide the developer?

 - A. WS-Federation sign-on endpoint
 - B. SAML-P sign-on endpoint
 - C. Graph API endpoint
 - D. Federation metadata document endpoint

Answers

This section contains the solutions to the thought experiments and answers to the objective review questions in this chapter.

Objective 5.1: Thought experiment

1. You should recommend the Directory Sync with single sign-on solution for Contoso. Because they already have Active Directory Federation Services (AD FS) installed and configured in their on-premises environment, much of the heavy work to implement this solution is already done. This solution also delivers a true single sign-on solution because users will not be challenged for credentials when accessing cloud applications if they are already authenticated in their on-premises environment. Finally, Contoso may find comfort in knowing that this solution does not sync hashes of user passwords to Azure AD because users will always authenticate using the AD FS endpoints running on-premises.
2. The AAD Connect tool should be used to implement the solution. It provides an intuitive wizard that will download and install the prerequisites such as .NET Framework 3.5, Microsoft Online Services Sign-in Assistant, and the Azure Active Directory PowerShell module. This tool will also enable directory integration in your Azure Active Directory, install and configure the AAD Sync tool, and then verify that single sign-on is configured and working correctly between the on-premises directory and Azure Active Directory.
3. For users to change their password or reset their password and have the new password persisted back to their on-premises directory, Azure Active Directory Premium edition is required.

Objective 5.1: Review

1. **Correct answer:** A
 - A. **Correct:** A global administrator has full administrative access to the directory.
 - B. **Incorrect:** A user administrator can manage users, groups, and reset password for other users in the directory.
 - C. **Incorrect:** A password administrator can reset passwords for other users and other password administrators.
 - D. **Incorrect:** A billing administrator can purchase services, manage service requests, and monitor service health.
2. **Correct answer:** C
 - A. **Incorrect:** Assigning the global administrator role to the user would give the user full access to the directory, but would not allow the user to provision services in the Azure subscription.

- B. Incorrect:** Assigning the user administrator role to the user would enable the user to manage users and groups in the directory, but would not allow the user to provision services in the Azure subscription.
- C. Correct:** Adding the user as a co-administrator on the Azure subscription would allow the user to create a virtual machine in the Azure subscription and provision other resources as needed.
- D. Incorrect:** Adding the user as a service administrator on the Azure subscription would allow the user to create a virtual machine and other resources in the Azure subscription. However, this would also give the user access to billing and other features beyond what is required.
- 3. Correct answers:** B and C
- A. Incorrect:** A CNAME record is used to map a domain name to another domain name.
- B. Correct:** Azure supports custom domain verification for an Azure Active Directory using a TXT record entry in your domain name registrar.
- C. Correct:** Azure supports custom domain verification for an Azure Active Directory using a MX record entry in your domain name registrar.
- D. Incorrect:** An A (host) record is used to specify an IP address a domain name should resolve to.
- 4. Correct answer:** D
- A. Incorrect:** Enable-MSOnlinePasswordSync is the cmdlet used to enable the password synchronization feature for DirSync. It has the same effect as checking the option to enable password synchronization during installation of the DirSync tool.
- B. Incorrect:** Enable-PasswordSyncLog is the cmdlet used to enable logging for the password synchronization extension of DirSync.
- C. Incorrect:** Enable-DirSyncLog is the cmdlet used to enable logging for DirSync.
- D. Correct:** Enable-OnlinePasswordWriteBack is the cmdlet used to enable the password write-back feature.
- 5. Correct answer:** A
- A. Correct:** Start-OnlineCoexistenceSync is the cmdlet used to perform an on-demand synchronization.
- B. Incorrect:** Set-DirSyncConfiguration is used to apply configuration settings for directory synchronization.
- C. Incorrect:** Enable-DirSyncLog is the cmdlet used to enable logging for DirSync.
- D. Incorrect:** Set-FullPasswordSync is used to force a full sync the next time the synchronization service is started.

- 6. Correct answer:** B
- A. **Incorrect:** DirSync is used for single-forest directory synchronization.
 - B. **Correct:** AAD Sync is the tool that supports configuring directory synchronization in a multi-forest environment.
 - C. **Incorrect:** The AAD Connect tool currently does not support multi-forest environments. This feature is on the roadmap for the tool though.
 - D. **Incorrect:** The Synchronization Service Manager is a FIM client that can be used to monitor synchronization events.

Objective 5.2: Thought experiment

- 1. You should add the SaaS application to the Contoso Azure Active Directory using the management portal. In the applications page for the Contoso directory, you can add an application from the application gallery simply by selecting it in the application gallery. The management portal then guides you through the steps necessary to configure the application.
- 2. You should configure single sign-on using the Windows Azure AD Single Sign-On option in the wizard used to configure SSO. This establishes federation between Contoso's Azure Active Directory and the SaaS application. Another alternative would be to use the Existing Single Sign-On option. However, this would only be advisable if Contoso already had Active Directory Federation Services installed and configured in their on-premises environment.

Objective 5.2: Review

- 1. **Correct answers:** C and D
 - A. **Incorrect:** The management portal is where co-administrators of an Azure subscription can provision resources.
 - B. **Incorrect:** The Active Directory Portal is where global administrators can manage users and is often used by administrators of Office 365 subscriptions.
 - C. **Correct:** The Access Panel is where users can see and launch applications they have been assigned access to.
 - D. **Correct:** The My Apps application from the Apple App Store can be used for users of iOS 7 devices.
- 2. **Correct answers:** A,B, and D
 - A. **Correct:** Mobile phone is a valid contact method and can be configured to receive a text message or a phone call.
 - B. **Correct:** Office phone is a valid contact method.

- C. Incorrect:** Email is not a valid contact method when configuring Multi-Factor Authentication. It is used in the first leg of authentication though when authenticating using a username and password.
- D. Correct:** Mobile application is a valid contact method. When choosing this option, you are prompted to download the application to a device and activate it using a passcode provided. The supported device types are Windows Phone, Android, and iOS devices.
- 3. Correct answers:** B and D
- A. Incorrect:** Automatic user provisioning is used to provision user accounts in the SaaS application because users are provisioned in Azure Active Directory.
- B. Correct:** Password-based single sign-on uses the user's credentials with the SaaS application to authenticate.
- C. Incorrect:** Active Directory Federation Services can be a token provider in a single sign-on configuration, but it is not one of the single sign-on modes.
- D. Correct:** Federation-based single sign-on uses the user's credentials in Active Directory to authenticate when accessing the SaaS application.
- 4. Correct answer:** A
- A. Correct:** The URL <https://myapps.microsoft.com> is the URL for the Access Panel.
- B. Incorrect:** The URL <https://portal.azure.com> is the URL for the management portal.
- C. Incorrect:** The URL <http://azure.microsoft.com/en-us/marketplace/active-directory> is the URL for the Azure Active Directory applications gallery.
- D. Incorrect:** The URL <https://account.windowsazure.com/organization> is the URL to sign up for an Azure Subscription as an organization rather than as an individual.

Objective 5.3: Thought experiment

1. Use the management portal to add the application to Azure Active Directory. In the applications page of the management portal, click the Add button to start the Add Application Wizard. Add the web application using the type web application and/or web API. Repeat this for the web service so that you have two applications registered in Azure Active Directory. Provide the development team with the application endpoints for your Azure Active Directory and the application ID URI and reply URL for both applications.
2. The web service will need to be exposed such that the web application can be configured to access it on behalf of the signed-in user, which can be done by adding the oauth2Permissions configuration to the application manifest for the web service.

-
-
3. Using the management portal, configure the web application to access the graph API by assigning a delegated permission to read directory data for the existing Windows Azure Active Directory application. Add a second application permission setting for the web service and select the permission level that was added in the web service's application manifest file.

Objective 5.3: Review

1. **Correct answers:** A, C, and D
 - A. **Correct:** The WS-Federation endpoint is used often for browser-based web applications and provides user sign in and sign out support.
 - B. **Incorrect:** The federation metadata document endpoint contains metadata for the Azure Active Directory tenant, such as the certificate used to sign the security tokens it issues.
 - C. **Correct:** SAML-P provides support for the SAML 2.0 web browser single sign-on and sign-out profiles.
 - D. **Correct:** Azure Active Directory supports the OAuth 2.0 protocol via the OAuth 2.0 token endpoint and the OAuth 2.0 authorization endpoint.
2. **Correct answer:** C
 - A. **Incorrect:** The sign-on URL is the URL where clients can access the application using a browser or other web tool.
 - B. **Incorrect:** The reply URL is where Azure Active Directory will redirect the user to after a client has been authenticated and authorized to access the application.
 - C. **Correct:** The application ID URI is used to uniquely identify an application added to Azure Active Directory.
 - D. **Incorrect:** The name setting is only a friendly name chosen for the application and can be any value. The name is displayed in the applications page of Azure Active Directory for each application.
3. **Correct answer:** A
 - A. **Correct:** The URL `https://sts.windows.net/<tenant>` is a tenant-specific endpoint where SAML tokens are issued.
 - B. **Incorrect:** The URL `https://login.windows.net/<tenant>/saml2` is the application endpoint used to sign in and sign out users using the SAML-P protocol.
 - C. **Incorrect:** The URL `https://login.windows.net/<tenant>/wsfed` is the application endpoint used to sign in and sign out users using the WS-Federation protocol.
 - D. **Incorrect:** The URL `https://graph.windows.net/<tenant>` is the graph API application endpoint used by applications to perform CRUD operations on directory objects in Azure Active Directory.

4. Correct answer: D

- A. Incorrect:** The WS-Federation sign-on endpoint is where unauthenticated users of an application configured for WS-Federation are redirected to sign in.
- B. Incorrect:** The SAML-P sign-on endpoint is where unauthenticated users of an application configured for SAML-P are redirected at to sign in.
- C. Incorrect:** The Graph API endpoint is used by applications to read and/or write data in the Azure Active Directory.
- D. Correct:** The federation metadata document endpoint points to the metadata document for the Azure Active Directory, which contains the certificate used to sign SAML tokens.

Index

A

AAD. *See* Azure Active Directory (AAD)
AAD Sync tool 269
access control
 for Azure Storage account 229–234
 backing up and restoring ACLs 260–261
Access Panel, for SaaS applications 292–293
Active Directory Federation Service 273–274
active geo-replication 247–249
activity log reports 282
administrator roles, for Azure Active Directory 276, 277
affinity groups 320
alerts
 for Azure Storage accounts 238–239
 for cloud services 198–199
 for endpoint failures 36
 for events 38
 for performance counter metrics 37–38
Always On setting 11
analytics
 for Azure Storage accounts 236–238
 configuring 39–40
anomalous activity reports 281
application diagnostic logs
 enabling 28–30
 location of 30
 retrieving 30–32
 streaming 32–34
Applicationhost.config file 169–170
application settings
 configuring 11–13
 environment variables for 12
APPSETTING_ environment variables 12
A record, for DNS 14–15, 17
ASDB (Azure SQL Database Benchmark) 241
async copy service, for blob storage 218–219

authentication
 for Azure Active Directory 294–300
 for Azure Storage accounts 230–231
Autoscale
 configuring with metrics 46
 configuring with schedules 44–45
awverify CNAME record 15
Azure Active Directory (AAD) 267
 activity log reports 282
 administrator roles for 276, 277
 anomalous activity reports 281
 Cloud App Discovery 283–284
 custom domain for 278–280
 directory synchronization 268–274, 284–286
 domain join 325–326
 editions of 267
 federated identity providers for 298–299
 integrated application reports 282
 integrating with Office 365 274–278
 LOB applications, integrating 301–312
 monitoring 280–286
 Multi-Factor Authentication for 294–298
 notifications for 283
 SaaS applications, integrating 288–293
 user and group activity sign-in reports 280
Azure Active Directory Connect 273
Azure Backup 255–262
 Backup Agent for 256
 Backup Vault for 256
 Backup Wizard for 258
 Recovery Data Wizard 260–261
 Register Server Wizard 257
Azure cloud services
 configuration, updating 188
 custom domain, configuring 160–161
 deploying 182–186
 deployment, updating 187–189

- endpoint monitoring 199–200
- external endpoints 166
- fault domains 154–155
- In-Role Cache, configuring 157–160
- internal endpoints 166
- local storage, configuring 170–172
- monitoring 196–199
- network traffic rules, configuring 166–168
- packaging 180–182
- RDP (Remote Desktop) access, configuring 176–177
- reserved IP address, configuring 164–166
- scaling 189–192
- SSL, configuring 162–164
- startup tasks for 168–170
- upgrade domains 154–155
- virtual IP swap 187
- web role access, restricting 168–170
- web role instance count, configuring 152–155
- web role instance size, configuring 172–173
- web role operating system settings, configuring 155–157
- web roles, configuring multiple websites on 173–175
- Azure Cross-Platform Command-Line Interface (xplat-cli) tools 24–26
 - Azure ExpressRoute 336–337
 - Azure Files 220–221
 - Azure Gallery
 - templates 2–3
 - Azure management portal
 - analytics, configuring 39–40
 - Autoscale, configuring using schedules 44–45
 - Azure Active Directory reports, viewing 281
 - Azure Storage alerts, creating 239
 - Azure Storage Diagnostics, configuring 235
 - Azure Storage monitoring, enabling 238
 - Azure Traffic Manager profile, creating 19–20
 - Azure websites
 - creating 2–3
 - templates for 2–3
 - Backup Vault, creating 256
 - blades, customizing 34
 - CDN endpoints, creating 223–224
 - cloud service package, publishing 182–184
 - cloud services, monitoring 197–199
 - containers, creating 215
 - custom domain
 - adding 278–280
 - custom domain, associating with Azure website 15
 - custom domain, configuring 161
 - deployment slots
 - cloning 5
 - creating 4–5
 - swapping 6
 - diagnostic logs, enabling 29
 - directory synchronization, enabling 269–270
 - endpoint monitoring 36–37
 - export job, creating 223
 - fault domain for role instances, determining 155
 - file shares, creating 220
 - FTP settings 30
 - geo-replication of SQL Database 246
 - graph API permissions, adding 310
 - handler mappings, configuring 23
 - import job, creating 222
 - In-Role Cache, configuring 159
 - IP address, obtaining 14
 - logs, streaming 33
 - MFA portal, accessing 295
 - MFA provider, creating 294–295
 - native application, integrating 307–308
 - network configuration, exporting 330
 - Notification Hub, monitoring 202
 - notifications for Azure Active Directory, configuring 283
 - point-in-time recovery of database 243
 - RDP (Remote Desktop) access, configuring 176
 - replication options, setting 217
 - resources, monitoring 34–35
 - role instance count, configuring 153–154
 - role operating system settings, configuring 156–157
 - SaaS applications, integrating 290–291
 - scaling cloud services 189–192
 - Service Bus namespace, creating 193
 - Service Bus queue, monitoring 200–201
 - Service Bus relay, monitoring 202
 - Service Bus topic, monitoring 201
 - services, monitoring 38–39
 - site settings, configuring 12–13
 - SQL Database
 - exporting 252
 - importing 253
 - SSL bindings, configuring 17
 - SSL certificate, adding to cloud service 162–163
 - SSL certificate, uploading 16–17
 - storage account keys, accessing 230–231
 - upgrade domain for role instances, determining 155
 - user and group activity sign-in reports, viewing 280
 - user password reset, enabling 272

virtual applications or directories, configuring 24
 virtual networks, configuring 320–323
 web application or service, integrating 301, 305–306
 web hosting plans, creating 49–50
Azure PowerShell. *See also* specific cmdlets
 async blob copy service, running 218–219
Azure Storage Diagnostics, configuring 235
Azure Traffic Manager profile
 adding endpoints to 21
 creating 20
 disabling endpoints in 21
 removing endpoints from 21
Azure websites, creating 3–4
cmdlets. *See also* specific cmdlets
 online reference for 3
 containers, creating 215–216
 custom domain, associating with Azure website 15
 custom domain, configuring 161
 deployment slots
 creating 5
 swapping 6
 diagnostic logs
 enabling 30
 retrieving 32
 file shares, creating 220–221
 handler mappings, configuring 23
 IP address, removing 166
 IP address, reserving 164
 network configuration
 changing 333
 exporting 330
 importing 331
 point-in-time recovery of database 244
 publishing cloud service package 184
 RDP (Remote Desktop) access, configuring 176
 replication options, setting 217
 role instance count, configuring 153
 Service Bus namespace, creating 193
 Shared Access Signature (SAS), creating 231–232
 site settings, configuring 13
 SSL certificate, adding to cloud service 163
 streaming logs 34
 web deployment package, publishing 7
 WebJobs, deploying 8
 web role instance size, configuring 172–173
Azure Recovery Services 255
Azure services. *See* services; *See also* specific services
Azure Site Recovery 255
Azure SQL Database
 geo-replication for 245–249
 importing and exporting 252–254
 partitioning schemes 250–252
 performance levels for 241–243
 point-in-time recovery for 243–245
 scaling 249–252
 service tiers for 241–243
Azure SQL Database Benchmark (ASDB) 241
Azure Storage accounts 213
 access control for 229–234
 authentication for 230–231
 Azure Backup for 255–262
 Azure Files 220–221
 blob storage 214–216
 cache settings 157–158
 Content Delivery Network (CDN) 223–226
 custom domains for 226–228
 diagnostics data in 203–204
 diagnostics for 234–240
 Import and Export service 221–223
 monitoring 238–239
 monitoring logs in 197
 replication options 216–217
 types of storage 213–214
Azure Storage Diagnostics 234–240
Azure subscription
 adding Office 365 to 277–278
 adding to Office 365 subscription 275
 core capacity of 153
 integrating Office 365 directory with 275–277
 removing reserved IP address from 166
 website locations available 3
 websites in 25
Azure Traffic Manager 18
 DNS name 18, 22
 DNS time-to-live (TTL) 18
 load-balancing method 18–19
 monitoring settings 19
 profile for, creating 18–20
 website endpoints (deployments) 18
 adding to profile 20–21
 health of, determining 19
 selection method used for 22
Azure virtual machines (VMs)
 static IP address for 325
Azure virtual networks 319
 address spaces for 322–323
 Azure Active Directory domain join for 325–326
 changing configuration of 332–333
 connectivity for 321–322
 creating and configuring 319–323
 deploying cloud service to 185–186, 326–327

deploying virtual machine to 324–326
DNS server for 320–321
ExpressRoute for 336–337
hybrid connectivity options for 335–337
importing and exporting configuration of 330–332
internal load balancing 327–328
point-to-site connectivity for 335, 337–340
site-to-site connectivity for 336, 340–342
virtual network-to-virtual network VPN 342–350

Azure websites

- configuring 10–27
 - application settings 11–12
 - custom domain 14–15
 - database connection string 11–12
 - handler mappings 22–23
 - site settings 11–13
 - SSL certificates 16–17
 - virtual applications or directories 23–24
- creating 2–4
- deployment slots
 - creating 4–5
- diagnostic logs
 - enabling 28–30
 - location of 30
 - retrieving 30–32
 - streaming 32–34
- domain for
 - custom 14–15
 - default 4
- endpoints (deployments) 18
 - adding to profile 20–21
 - health of, determining 19
 - monitoring 36–37
 - selection method used for 22
- health check pages 19
- IP address 14, 17
- location
 - availability of 3
 - specifying 4
- multiple, configuring on a web role 173–175
- name
 - availability of 3
 - specifying 4
- publishing 7
- resources
 - monitoring 34–35
- scaling up 47
- templates 2–3
- web deployment package
 - publishing 7

Azurewebsites.net domain 4

B

Backup Agent 256
backups

- configuring 40–41
- restoring 41
- for servers. *See Azure Backup*

Backup Vault 256
Backup Wizard 258
BACPAC format 252–254
Basic tier plans 49
Billing administrator role 276
blob storage 214–216

- async copy service for 218–219
- containers for 214–215
- metadata for 216
- services in 214
- structure of 214
- time-to-live (TTL) period for 225
- types of 216

block blobs 216

C

caching

- capacity planning 159
- In-Role Cache, configuring 157–160
- Managed Cache 160
- options for 160
- Redis Cache 160

CDN (Content Delivery Network) 223–226

- content expiration for, setting 225
- custom domains for 226–228
- query strings for 226
- removing content from 226

Cloud App Discovery 283–284
cloud services. *See Azure cloud services; See Azure Cloud Services*
Cmdkey.exe utility 221
cmdlets. *See Azure PowerShell: cmdlets*
CNAME record, for DNS 14–15, 22
co-located cache 157
configuration files, application 12.

- See also site settings*

configuration files, cloud service 181–182

- diagnostics data 203
- network traffic rules 166–168

operating system settings 155–156

reserved IP address 165
 role instance count 152
 SSL settings 162
 configuration files, virtual networks
 importing and exporting 330–332
 for VPN 345–347
 connection string for database
 configuring 11–12
 environment variables for 12
 for SQL Database 247
 containers
 for blob storage 214–215
 Content Delivery Network (CDN) 223–226
 content expiration for, setting 225
 custom domains for 226–228
 query strings for 226
 removing content from 226
 Continuous jobs 8.
See also Continuously Running task WebJobs
 Continuously Running task WebJobs 7–8
 core capacity 153
 CPU usage
 configuring Autoscale using 46
 monitoring 35
 .cscfg file. *See* configuration files, cloud service
 .csdef file. *See* definition files, cloud service
 CSPack command-line tool 180–181
 .cspkg file 180, 181
 CUSTOMCONNSTR_environment variables 12
 custom domains 14–15
 for Azure Active Directory 278–280
 for Azure Storage account 226–228

D

databases
 as a service. *See* Azure SQL Database
 backups
 configuring 40–41
 restoring 41
 connection string for
 configuring 11–13
 data usage
 monitoring 35
 Debug Console, Site Control Manager 31–32
 dedicated cache 157
 definition files, cloud service
 local storage 171
 startup task in 169–170

web role instance size 173
 deploying
 cloud services 182–186, 187–189, 326–327
 virtual machines 324–326
 deployment slots
 cloning 5
 creating 4–5
 multiple, Standard mode required for 4
 production slot 5
 swapping 6
 deployments (website endpoints) 18
 adding to profile 20–21
 health of, determining 19
 monitoring 36–37
 selection method used for 22
 Detailed Error Messages, for site logs 29, 30
 diagnostics data
 for Azure Storage 234–240
 diagnostics data, for applications and sites
 enabling 28–30
 location of 30
 retrieving 30–32
 streaming 32–34
 diagnostics data, for cloud services 203–204
 Diagnostics.wadcfg file 203–204
 directory synchronization 268–274
 enabling 269
 monitoring 284–286
 with password sync 270–273
 scenarios for 268, 269
 with single sign-on 273–274
 tools for 269
 user passwords, resetting 272
 DirSync tool 269, 270
 Disable-OnlinePasswordWriteback cmdlet 272
 DNS name
 for Azure Traffic Manager 18, 22
 DNS records
 adding with domain registrar 14–15
 DNS time-to-live (TTL)
 for Azure Traffic Manager profile 18
 domain registrar
 custom domain values, adding 160–161
 DNS records, adding 14–15
 domains
 for Azure Active Directory, custom 278–280
 for Azure Storage account, custom 226–228
 for Content Delivery Network, custom 226–228

Enable-OnlinePasswordWriteback cmdlet

for Azure cloud service 160–161
for Azure Traffic Manager profile 18
for Azure website
 custom 14–15
 default 4

E

Enable-OnlinePasswordWriteback cmdlet 272
endpoints, for CDN 223–224
endpoints, for cloud services
 monitoring 199–200
 network traffic rules, configuring 166–168
endpoints, for websites. *See* deployments (website endpoints)
environment variables
 for application settings 12
 for connection strings 12
events
 alerts based on 38
 for directory synchronization 284–286
ExpressRoute 336–337

F

Facebook, as federated identity provider 298–299
Failed Request Tracing, for site logs 29, 30
Failover load balancing method 19
fault domains 154–155
federated identity providers 298–299
federation-based single sign-on 290
file shares (Azure Files) 220–221
file types
 for WebJobs 7
Freb.xlsx file 30
Free tier plans 50
FTP
 retrieving log files 30

G

Geographically redundant storage (GRS) option 216
geo-replication for database 245–249
Get-AzureDeployment cmdlet 161
Get-AzureReservedIP cmdlet 164
Get-AzureRoleSize cmdlet 172–173
Get-AzureSBLocation cmdlet 193
Get-AzureSqlDatabaseOperation cmdlet 245

Get-AzureSqlRecoverableDatabase cmdlet 244
Get-AzureStorageBlobCopyState cmdlet 219
Get-AzureStorageKey cmdlet 219
Get-AzureSubscription cmdlet 153
Get-AzureTrafficManagerProfile cmdlet 21
Get-AzureVM cmdlet 161, 333
Get-AzureVNETConfig cmdlet 330
Get-AzureWebsiteLocation cmdlet 3
Get-AzureWebsiteLog cmdlet 34
Get-Help cmdlet 3
Global administrator role 276
Google ID, as federated identity provider 298–299
graph API permissions, configuring 309–310
group activity sign-in reports 280
GRS (Geographically redundant storage) option 216

H

handlers (interpreters)
 mappings for, configuring 22–23
health check pages 19
horizontal partitioning for SQL Database 250
hosting plans. *See* web hosting plans (modes)
HTTP messages
 monitoring 35
HTTP requests
 monitoring 35
hybrid partitioning for SQL database 251

I

Import and Export service, for storage 221–223
In-Role Cache, configuring 157–160
integrated application reports 282
interpreters. *See* handlers
IP address
 for Azure website 14, 17
 for cloud service 164–166, 186
 removing from subscription 166
IP-based SSL 17

J

Java Version setting 11

K

Kudu. *See* Site Control Manager

L

load balancing
 for virtual networks 327–328
 load balancing method, Azure Traffic Manager 18–19
 LOB (line-of-business) applications
 enabling access from other applications 305–307
 graph API permissions for, configuring 309–310
 native applications, integrating with Azure Active Directory 307–309
 web applications or services, integrating with Azure Active Directory 301–307
 Locally-redundant storage (LRS) option 216
 local storage, for cloud services
 configuring 170–172
 location of Azure website
 availability of 3
 specifying 4
 logging. *See* diagnostics data
 LRS (Locally-redundant storage) option 216

M

Managed Cache 160
 Management Portal. *See* Azure Management Portal
 messaging services. *See* Microsoft Azure Service Bus;
 See also Azure Service Bus
 MFA (Multi-Factor Authentication) 294–298
 additional security verification with 297–298
 enabling 296–297
 provider for, configuring 295–296
 provider for, creating 294–295
 MFA portal 295, 296
 Microsoft accounts 298–299
 Microsoft Azure Active Directory (AAD). *See* Azure Active Directory (AAD)
 Microsoft Azure Cloud Services 151. *See* Azure Cloud Services
 cloud services created with. *See* Azure cloud services
 Microsoft Azure IaaS Deep Drive Jump Start 349
 Microsoft Azure Recovery Services 255
 Microsoft Azure Service Bus. *See* Service Bus
 Microsoft Azure SQL Database. *See* Azure SQL Database
 Microsoft Azure subscription
 adding Office 365 to 277–278
 adding to Office 365 subscription 275
 core capacity 153
 integrating Office 365 directory with 275–277

Microsoft Azure Virtual Networks. *See* Azure virtual networks
 Microsoft Azure Websites 1. *See also* Azure websites
 websites created with. *See* Azure websites
 Microsoft Office 365. *See* Office 365
 Microsoft Virtual Academy 40, 349
 monitoring. *See also* diagnostics data; *See also* alerts;
 diagnostics data
 alerts 198–199
 for endpoint failures 36
 for events 38
 for performance counter metrics 37–38
 analytics
 for Azure Storage accounts 236–238
 configuring 39–40
 Azure Active Directory 280–286
 Azure Storage 238–239
 cloud services 196–199
 deployments (website endpoints) 36–37
 endpoints 199–200
 Service Bus queue 200–201
 Service Bus relay 202
 Service Bus topic 201
 services 38–39
 website resources 34–35
 Multi-Factor Authentication. *See* MFA
 MX record, verifying custom domains using 279
 My Apps application 293
 MySQL
 connection string for 11–12
 MYSQLCONNSTR_environment variables 12

N

name of Azure website
 availability of 3
 specifying 4
 .NET Framework Version setting 11
 network traffic rules
 for cloud services, configuring 166–168
 New-AzureDeployment cmdlet 327
 New-AzureDNS cmdlet 323
 New-AzureQuickVM cmdlet 324
 New-AzureReservedIP cmdlet 164
 New-AzureSBNamespace cmdlet 193
 New-AzureService cmdlet 327
 New-AzureStorageAccount cmdlet 217
 New-AzureStorageBlobSASToken cmdlet 231–232
 New-AzureStorageContainer cmdlet 215

New-AzureStorageContext cmdlet

New-AzureStorageContext cmdlet 219, 221
New-AzureStorageShare cmdlet 221
New-AzureTrafficManagerProfile cmdlet 20
New-AzureVM cmdlet 323, 325, 328
New-AzureVNetGateway cmdlet 337
New-AzureWebsite cmdlet 4, 5
New-AzureWebsiteJob cmdlet 8
New Relic 199
Notification Hub
 monitoring 202
notifications
 for Azure Active Directory 283

O

Office 365, integrating with Azure Active Directory 274–278
On-Demand task WebJobs 7–8
One-time Scheduled task WebJobs 8
operating systems
 role settings for, configuring 155–157

P

PaaS (platform-as-a-service) 1, 151
packaging
 cloud services 180–182
page blobs 216
partitioning scheme for SQL Database 250–252
Password administrator role 276
password-based single sign-on 291
password sync, with directory synchronization 270–273
performance
 alerts based on 37–38
 for Azure SQL Database 241–243
Performance load balancing method 18
Php.ini file. *See* configuration files, application
PHP Version setting 11
platform-as-a-service. *See* PaaS
Platform setting 11
point-in-time recovery 243–245
point-to-site connectivity 321, 335, 337–340
PowerShell. *See* Azure PowerShell;
 See also Azure PowerShell; Windows PowerShell
production environment, cloud services
 swapping with staging environment 187
production slot 5
Publish-AzureServiceProject cmdlet 184

Publish-AzureWebsiteProject cmdlet 7
publishing. *See* deploying
Python Version setting 11

R

RAGRS (Read-access geographically redundant storage) option 216
RDP (Remote Desktop) access
 configuring 176–177
Recovery Data Wizard 260–261
recovery point objective (RPO) 242
Recovery Services 255
recovery time objective (RTO) 242
Recurring Scheduled task WebJob 8
Redis Cache 160
Register Server Wizard 257
Remote Debugging setting 11
Remote Desktop. *See* RDP (Remote Desktop) access
Remote Visual Studio Version setting 11
Remove-AzureReservedIP cmdlet 166
Remove-AzureServiceRemoteDesktopExtension cmdlet 177
Remove-AzureTrafficManagerEndpoint cmdlet 21
replication options, for storage 216–217
resources
 monitoring 34–35
roles, for cloud services. *See* web roles, for cloud services
Round Robin load balancing method 19
RPO (recovery point objective) 242
RRAS (Routing and Remote Access Service) 341–342
RSS feeds
 for service monitoring 39
RTO (recovery time objective) 242

S

SaaS (software as a service) applications
 Access Panel for 292–293
 automatic user provisioning for 291
 group access to, assigning 292
 integrating with Azure Active Directory 288–293
 single sign-on for 290–291
 user access to, configuring 289–293
SAS (Shared Access Signature) 231–232
Save-AzureWebsiteLog cmdlet 32
scalability 44
 Autoscale

configuring with metrics 46
 configuring with schedules 44–45
 scaling up a website 47
scaling
 Azure SQL Database 249–252
 cloud services 189–192
 Scheduled task WebJobs 7–8
schedules
 configuring Autoscale using 44–45
Select-AzureSubscription cmdlet 218
Server Name Indication (SNI) SSL 17
Service administrator role 276, 277
Service Bus
 namespace, creating 193–194
 queue, monitoring 200–201
 relay, monitoring 202
 topic, monitoring 201
service level agreement. *See SLA*
services
 announcements for, history of 39
 monitoring 38–39
Set-AzureRole cmdlet 153
Set-AzureServiceRemoteDesktopExtension cmdlet 176
Set-AzureStaticVNetIP cmdlet 325
Set-AzureStorageAccount cmdlet 217
Set-AzureStorageMetricsProperty cmdlet 235
Set-AzureStorageServiceLoggingProperty cmdlet 235
Set-AzureSubnet cmdlet 325, 333
Set-AzureTrafficManagerEndpoint cmdlet 21
Set-AzureTrafficManagerProfile cmdlet 21
Set-AzureVNETConfig cmdlet 331
Set-AzureWebsite cmdlet 13, 15, 23, 30
Shared Access Signature (SAS) 231–232
Shared tier plans 50
Site Control Manager (Kudu)
 Debug Console 31–32
 diagnostic logs, retrieving 31–32
 streaming logs 34
site diagnostic logs
 enabling 28–30
 location of 30
 retrieving 30–32
 streaming 32–34
Site Recovery 255
site settings 11–13
 precedence of 12
site-to-site connectivity 321–322, 336, 340–342
SNI (Server Name Indication) SSL 17
social identity providers 298–299
software as a service (SaaS) applications
 Access Panel for 292–293
 automatic user provisioning for 291
 group access to, assigning 292
 integrating with Azure Active Directory 288–293
 single sign-on for 290–291
 user access to, configuring 289–293
SQLAZURECONNSTR_environment variables 12
SQLCONNSTR_environment variables 12
SQL Database. *See Azure SQL Database*
 connection string for 11–12
SQL Server
 connection string for 11–12
SSL
 for CDN endpoints 224
 certificate for 162
 configuring for cloud services 162–164
 not supported for custom domains 227
SSL bindings, configuring 17
SSL certificates
 configuring 16–17
staging environment, cloud services
 swapping with production environment 187
standard geo-replication 245–247
Standard_GRS replication option 216
Standard_LRS replication option 216
Standard mode for Azure website
 for Azure Traffic Manager endpoints 21
 for multiple deployment sites 4
 for SSL certificates 16
Standard_RAGRS replication option 216
Standard tier plans 49
Standard_ZRS replication option 216, 217
Start-AzureSqlDatabaseCopy cmdlet 246, 248
Start-AzureSqlDatabaseRecovery cmdlet 244
Start-AzureSqlDatabaseRestore cmdlet 244–245
Start-AzureStorageBlobCopy cmdlet 218
Start-OnlineCoExistenceSync cmdlet 271
startup tasks
 for Azure cloud services 168–170
Stop-AzureSqlDatabaseCopy cmdlet 247, 249
Storage accounts. *See Azure Storage accounts*
stored access policy 232–233
streaming logs 32–34
subscription. *See Azure subscription*
subscription, Azure
 adding Office 365 to 277–278
 adding to Office 365 subscription 275

subscription, Azure

integrating Office 365 directory with 275–277
Switch-AzureWebsiteSlot cmdlet 6

T

templates for Azure website
 Azure Gallery 2–3
Test-AzureName-Website cmdlet 4
Tiers for SQL Database 241–243
Traffic Manager. *See* Azure Traffic Manager
Triggered jobs 8. *See also* On-Demand task WebJobs
TXT record, verifying custom domains using 279

U

Update-AzureVM cmdlet 333
upgrade domains 154–155
user activity sign-in reports 280
User administrator role 276
user analytics. *See* analytics

V

vertical partitioning for SQL Database 250
Virtual Academy 40
virtual applications
 configuring 23–24
virtual directories
 configuring 23–24
virtual IP swap, cloud services 187
virtual machines
 configuring in startup task for cloud service 168–170
virtual networks. *See* Azure virtual networks
VPN, virtual network-to-virtual network 342–350

W

WAImportExport.exe utility 221–222
web applications
 integrating with Azure Active Directory 301–307
 multiple, adding to website 175
Web.config file. *See also* configuration files, application
 web role access, restricting 169–170
web deployment package
 publishing 7
web hosting plans (modes) 48
 creating 49–50

creating websites within 50
for Azure Traffic Manager endpoints 21
for custom domains 15
for multiple deployment slots 4
for SSL certificates 16
migrating websites between 50
WebJobs 7
 deploying 7–9
 file types for 7
 types of 7
web roles, for cloud services
 fault domain for 155
 instance count for, configuring 152–155
 instance size, configuring 172–173
 multiple websites on, configuring 173–175
 operating system settings, configuring 155–157
 restricting access to 168–170
 scaling 189–192
 upgrade domain for 155
Web Server Logging, for site logs 28, 30
 streaming 33
website endpoints. *See* deployments (website endpoints)
websites. *See* Azure websites
Web Sockets setting 11
Windows Azure Directory Sync Service 271
Windows Server Active Directory, synchronizing with
 Azure Active Directory. *See* directory synchronization

X

xplat-cli (Azure Cross-Platform Command-Line Interface)
 tools 24–26

Z

ZRS (Zone redundant storage) option 216, 217

About the authors



MICHAEL WASHAM is a Microsoft MVP specializing in Microsoft Azure and is the founder and CEO of Opsgility (www.opsgility.com), a leader in instructor-led and on-demand training for Microsoft Azure and enterprise computing. Prior to starting Opsgility, Michael was a fifteen year Microsoft veteran, and while at Microsoft, Michael's roles included being a Senior Program Manager on the Microsoft Azure Runtime team and a Senior Technical Evangelist for Microsoft Azure Infrastructure Services. Michael was the original developer of the Microsoft Azure PowerShell cmdlets and is a globally recognized speaker for conferences such as TechEd and BUILD. When not focused on cloud computing Michael spends time with his wife and kids in the north Texas area.



RICK RAINY is a Microsoft Azure Insider and Advisor, Certified Trainer (MCT), blogger (<http://rickrainey.com>) and an Azure community enthusiast. At Microsoft, he worked closely with Microsoft Premier Enterprise customers, Independent Software Vendors, and Microsoft Engineering to design and develop applications for the Microsoft Azure platform. Today, he is the owner and CEO of CloudAlloc (<http://www.cloudalloc.com>), a provider of services and tools designed to achieve maximum business value from applications and infrastructure workloads running in the cloud.