Microsoft Azure Architect Technologies

Exam Ref AZ-303

Mike Pfeiffer • Derek Schauland
Nicole Stevens • Gurvinder Singh

Microsoft

Exam Ref AZ-303 Microsoft Azure Architect Technologies

Mike Pfeiffer
Derek Schauland
Gurvinder Singh
Nicole Stevens

Exam Ref AZ-303 Microsoft Azure Architect Technologies

Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.
Hoboken, NJ

ISBN-13: 978-013-680509-0
ISBN-10: 0-136-80509-4

Library of Congress Control Number: 2020947522

ScoutAutomatedPrintCode

CREDITS

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

ASSISTANT SPONSORING EDITOR
Charvi Arora

DEVELOPMENT EDITOR
Rick Kughen

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Rick Kughen

INDEXER
Timothy Wright

PROOFREADER
Abigail Bass

TECHNICAL EDITOR
Thomas Palathra

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

Contents at a glance

	Acknowledgments	*xi*
	About the Authors	*xiii*
	Introduction	*xv*
CHAPTER 1	**Implement and monitor an Azure Infrastructure**	**1**
CHAPTER 2	**Implement management and security solutions**	**131**
CHAPTER 3	**Implement Solutions for Apps**	**249**
CHAPTER 4	**Implement and manage data platforms**	**269**
	Index	*325*

Contents

Introduction **xv**

Organization of this book *xv*
Preparing for the exam *xvi*
Microsoft certifications *xvi*
Quick access to online references *xvii*
Errata, updates, & book support *xvii*
Stay in touch *xvii*

Chapter 1 Implement and monitor an Azure Infrastructure **1**

Skill 1.1: Implement cloud infrastructure monitoring 2
Monitor security 2
Monitor performance 4
Monitor health and availability 13
Monitor cost 15
Configure advanced logging 18
Configure logging for workloads 24
Initiate automated responses by using Action Groups 26
Configure and manage advanced alerts 27

Skill 1.2: Implement storage accounts 30
Select storage account options based on a use case 30
Configure Azure Files and Blob Storage 32
Manage access keys 35
Configure network access to the storage account 36
Implement Shared Access Signatures and access policies 39
Implement Azure AD authentication for storage 42
Implement Azure Storage replication 46
Implement Azure Storage account failover 48

Skill 1.3: Implement VMs for Windows and Linux 48
Select virtual machine size 49
Configure storage for VMs 50

Configure Azure Disk Encryption 53
Configure High Availability 56
Deploy and Configure Scale Sets 60
Implement Azure Dedicated Hosts 63
Skill 1.4: Automate deployment and configuration of resources 63
Save a deployment as an Azure Resource Manager template 64
Modify Azure Resource Manager template 66
Evaluate location of new resources 69
Deploy from a template 70
Configure a virtual disk template 73
Manage a template library 74
Create and execute an automation runbook 75
Skill 1.5: Implement virtual networking. 80
Implement VNet-to-VNet connections 80
Implement VNet peering 83
Skill 1.6: Implement Azure Active Directory. 86
Add custom domains 87
Manage multiple directories 88
Implement self-service password reset 89
Configure user accounts for MFA 93
Configure fraud alerts 96
Configure bypass options 97
Configure trusted IPs 98
Configure verification methods 100
Implement and manage guest accounts 101
Configure Azure AD Identity Protection 106
Implement Conditional Access including MFA 108
Skill 1.7: Implement and manage hybrid identities 111
Install and configure Azure AD Connect 112
Identity synchronization options 118
Configure and manage password sync and password writeback 119
Configure Single Sign-On 123
Use Azure AD Connect Health 125

Chapter summary 127
Thought experiment 128
Thought experiment answers 129

Chapter 2 Implement management and security solutions 131

Skill 2.1: Manage workloads in Azure 131
Configure the components of Azure Migrate 132
Skill 2.2: Implement disaster recovery using Azure Site Recovery 153
Configure Azure components of Site Recovery 153
Configure on-premises components of Site Recovery 155
Replicate data to Azure 160
Migrate by using Azure Site Recovery 163
Skill 2.3: Implement application infrastructure 163
Create a simple logic app 164
Manage Azure Functions 168
Manage Azure Event Grid 172
Manage Azure Service Bus 174
Skill 2.4: Manage security for applications 176
Using Azure Key Vault to store and manage application secrets 176
Using Azure Active Directory Managed Identity 181
Azure Active Directory application registration 183
Creating application secrets for registered applications 186
Skill 2.5: Implement load balancing and network security 187
Configure Application Gateway and load balancing rules 188
Implement front-end IP configurations 190
Manage application load balancing 191
Implement Azure Load Balancer 195
Configure and manage Azure Firewall 199
Configure and Manage Azure Front Door 204
Implement Azure Traffic Manager 208
Manage and configure Network and Application Security Groups 211

Network Security Groups 211
Application Security Groups 214
Implement Azure Bastion 215

Skill 2.6: Integrate an Azure virtual network and an on-premises network. . . . 218
Create and configure Azure VPN Gateway 219
Create and configure site-to-site VPN 221
Verify on-premises connectivity 222
Manage on-premises connectivity with Azure 224
Configure ExpressRoute 225

Skill 2.7: Implement and manage Azure governance solutions. . . . 228
Implement Azure Policy 228
Implementing Azure Blueprint 232
Implementing and leveraging management groups 235

Skill 2.8: Manage Role-Based Access Control (RBAC). . . . 237
Create a custom role 237
Configure access to resources by assigning roles 240
Configure Management Access to Azure 241
Troubleshoot RBAC 243

Chapter summary 246

Thought experiment. . . . 247

Thought experiment answers 247

Chapter 3 Implement Solutions for Apps 249

Skill 3.1: Implement an Application Infrastructure. . . . 249
Create and configure Azure App Service 250
Create an App Service web app for containers 251
Configure networking for an App Service 253
Create and manage deployment slots 254
Implement Logic Apps 255
Implement Azure Functions 257

Skill 3.2: Implement Container-based Applications 261
Create a container image 261
Publish and automate image deployment to the Azure Container Registry 262

Implement an application that runs on an Azure Container Instance 264
Manage container settings by using code 265
Configure Azure Kubernetes Service 266
Chapter summary 267
Thought experiment 268
Thought experiment answers 268

Chapter 4 Implement and manage data platforms 269

Skill 4.1: Implement NoSQL Databases 269
Configure storage account tables 270
Azure Table storage service underlying data model 271
Create an Azure Table storage service 273
Configure Table Storage Data Access 274
Choose between Azure Table storage service and CosmosDB Table API 276
Azure Cosmos DB 276
Select appropriate Cosmos DB APIs 281
Set up replicas in Cosmos DB 287
Skill 4.2: Implement Azure SQL Databases 288
Provision and configure relational databases 289
Configuring Azure SQL Database settings 291
Implement Azure SQL Database Managed Instance 305
Configure HA for an Azure SQL Database 309
Publish an Azure SQL Database 314
Chapter summary 321
Thought experiment 322
Thought experiment answers 322

Index *325*

Acknowledgments

I am indebted to Microsoft Press for the opportunity to co-author this book, in association with Mike Pfeiffer, Derek Schauland, and Nicole Stevens. The co-authors hardly need any introduction, as they are well known for their professional prowess and their in-depth knowledge of the Microsoft Azure Platform.

A big thank you goes to reviewers Thomas Palathra and Rick Kughen for their well-coordinated efforts and due diligence, from conceptualization to publication of this book. I am indeed grateful to the entire Pearson Team, especially Ms. Loretta Yates and Ms. Charvi Arora, for their cooperation, support, and patience throughout this journey.

I am indeed grateful to my wife, Jaspreet Kaur, and, daughter Amritleen Kaur, for the tremendous encouragement that helped me walk the tightrope of schedules and deadlines.

Last but not least, I submit myself in reverence to Guru Nanak, the great spiritual Guru, whose blessings enabled an incredibly small and a nondescript individual like me with wisdom and opportunity.

—Gurvinder Singh

About the Authors

MIKE PFEIFFER Mike Pfeiffer is a 20-year tech industry veteran who's worked for some of the largest technology companies in the world, including Microsoft and Amazon Web Services (AWS). He's the founder and chief technologist at CloudSkills.io, a cloud consulting and training firm. Mike is an author for Pluralsight, international conference speaker, Microsoft Azure MVP, and host of the CloudSkills.fm podcast.

DEREK SCHAULAND Derek Schauland is an IT professional with 20 years' experience. He currently specializes in cloud technologies. He spent 10 years of his career as a Microsoft MVP, first in file system storage and then in cloud and datacenter management. In addition to writing about cloud technologies, he has co-authored three other books and countless articles and blogs. Outside of the technology space, he enjoys barbecuing with family and friends.

GURVINDER SINGH Gurvinder Singh is a Microsoft Certified Azure Solutions Architect with 13 years of diversified software development experience. He has a strong programming background and hands-on experience on .NET and C#. Since the past few years, Gurvinder has been guiding large enterprises in the transformation of legacy applications into cloud-native architecture with a focus on migration to Microsoft Azure. He is extremely passionate about technology, especially with the Microsoft Azure platform (PaaS, IaaS, and Serverless).

NICOLE STEVENS Nicole Stevens is technical director of an independent software vendor (ISV) in the United Kingdom. Nicole has 20 years' experience in software development, starting out as an Oracle DBA troubleshooting performance, design, and integration issues for large enterprises across EMEA (Europe, Middle East, and Africa). Switching to an ISV start-up brought fresh challenges, with a role spanning IT pro, technical consultancy, and DevOps engineer. Nicole's current focus is architecting cloud native solutions whilst assisting in the refactor of legacy software solutions for customers in Azure.

Introduction

The purpose of the AZ-303 certification exam is to test your understanding of the Microsoft Azure solutions architecture. The exam validates your ability to recognize which Azure services comprise a particular solution, and it validates your knowledge of real-world design scenarios and architecting Microsoft Azure solutions. This book provides a broad understanding of Microsoft Azure that empowers small, medium, and large-scale enterprises who want to adopt comprehensive app innovation and modernization strategies using the tools and services of their choice.

While we've made every effort possible to make the information in this book accurate, Azure is rapidly evolving, and there's a chance that some of the screens in the Azure portal are slightly different now than they were when this book was written. It's also possible that other minor changes have taken place, such as name changes and so on.

Azure supports a wide range of programming languages, frameworks, databases, and services. Consequently, IT professionals must quickly learn a wide range of technical topics. An overabundance of instructional content is available, which makes finding the right material difficult. This book cuts through the extraneous content and provides the information you need to prepare for the exam.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. We encourage you to 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 "Need more review?" links in the text to find more information and take the time to research and study the topic. Great information is available in the Microsoft Azure documentation (*https://docs.microsoft.com/azure*) and Microsoft Learn (*https://microsoft.com/learn*).

Organization of this book

This book is organized by the "Skills measured" list published for the exam. The "Skills measured" list is available for each exam on the Microsoft Learn website: *http://aka.ms/examlist*. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter's organization. If an exam covers six major topic areas, for example, the book will contain six chapters.

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. This book is *not* designed to teach you new skills.

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. Learn more about available classroom training and find free online courses and live events at *http://microsoft.com/learn*. Microsoft Official Practice Tests are available for many exams at *http://aka.ms/practicetests*.

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.

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/learn*.

Quick access to online references

Throughout this book are addresses to webpages that the author has recommended you visit for more information. Some of these links can be very long and painstaking to type, so we've shortened them for you to make them easier to visit. We've also compiled them into a single list that readers of the print edition can refer to while they read.

Download the list at *MicrosoftPressStore.com/ExamRefAZ303/downloads*

The URLs are organized by chapter and heading. Every time you come across a URL in the book, find the hyperlink in the list to go directly to the webpage.

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:

MicrosoftPressStore.com/ExamRefAZ303/errata

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

For additional book support and information, please visit *http://www.MicrosoftPressStore.com/Support*.

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*.

Stay in touch

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

CHAPTER 2

Implement management and security solutions

Organizations are still working out the details of getting to the cloud. With all the hardware and servers running in datacenters and co-location spaces, moving to the cloud still takes a bit of effort.

Architecting solutions in Azure is not just development or infrastructure management in the cloud. It's much more than that, and you need to understand how the Azure resources an organization needs to operate will sometimes be centered in development and sometimes in infrastructure. It's up to you to know enough about these topics.

This chapter helps you understand how you can bring your existing workloads to Azure by allowing the use of some familiar resources (IaaS Virtual Machines) and others that may be new (such as serverless computing) to your environment. In addition, the use of multifactor authentication (MFA) is covered here to ensure your cloud environment is as secure as possible. An Azure Solutions Architect might face all these situations in day-to-day work life and needs to be ready for each of them.

Skills covered in this chapter:

- Skill 2.1: Manage workloads in Azure
- Skill 2.2: Implement disaster recovery using Azure Site Recovery
- Skill 2.3: Implement application infrastructure
- Skill 2.4: Manage security for applications
- Skill 2.5: Implement application load balancing and network security
- Skill 2.6: Integrate an Azure virtual network and an on-premises network
- Skill 2.7: Implement and manage Azure governance solutions
- Skill 2.8: Implement multifactor authentication (MFA)

Skill 2.1: Manage workloads in Azure

Because most organizations have been operating on infrastructure running in house, there is a significant opportunity to help them migrate these workloads to Azure, which might save some costs and provide efficiencies for these servers that their datacenters might not. Also,

some organizations might want to explore getting out of the datacenter business. How can you help your organization or customer move out of a datacenter into the Azure cloud?

The recommended tool for this is Azure Migrate, which offers different options depending on the type of workload you're migrating (physical or virtual). Azure Site Recovery has not gone away, though it is used primarily for disaster-recovery scenarios where Azure is the target for disaster recovery. See Skill 2-2, "Implement disaster recovery using Azure Site Recovery," for more info.

This skill covers:

- Configure the components of Azure Migrate
- Migrate Virtual Machines to Azure
- Migrate data to Azure
- Migrate web applications
- Configure the components needed to migrate databases to Azure SQL or an Azure SQL–managed instance

Configure the components of Azure Migrate

Azure Migrate uses migration projects to assess and manage any inbound migration of workloads to Azure. To create a migration project and get started, follow these steps:

1. Determine the workload type to migrate:
   - **Servers.** Virtual or physical servers
   - **Databases.** On-premises databases
   - **VDI.** Virtual Desktop Infrastructure
   - **Web Apps.** Web-based applications
   - **Data Box.** Offline data migration to Azure
2. Add the tools for the selected migration to create a Migrate Project
3. Perform a migration of the selected workloads to Azure

Azure Migrate Assessment Tools

Before executing the migration of any workload to Azure, with the exception of a Data Box migration, the assessment of the current status of on-premises resources will help determine the type of Azure resources needed, as well as the cost to migrate them to Azure.

There are two assessment tools for migrating servers to Azure:

- **Azure Migrate Server Assessment.** This service has been the built-in assessment tool for some time and has roots in Site Recovery. It will discover and review VMware, Hyper-V, and physical servers to determine if they are ready and able to make the transition to Azure.

- **Movere.** This assessment tool was a third-party company until late 2019, which was acquired by Microsoft to broaden the tools available for getting resources into Azure. With the assessments performed by Movere, an agent is loaded within the on-premises environment and scans are performed to determine the volume of servers in the environment. Additional information, including SQL Server instances, SharePoint instances, and other applications, are also reported by Movere.

In addition to server assessments, Azure Migrate has tools to review existing web applications with the Web App Migration Assistant and on-premises SQL Server databases with the Database Migration Service. The assessment for SQL Server will also review the fit of the databases discovered within the three Azure offerings for SQL Server: Azure SQL Database, Managed Instance SQL, and SQL Server running on VMs in Azure.

> ***NOTE*** **AZURE SQL ADDITIONAL FIXES MAY BE REQUIRED**
>
> **When migrating SQL databases, there might be additional steps identified by the assessment that need to be remedied based on the destination implementation of the chosen SQL. In our experience, Azure SQL Database will have the most items for review because it is the most different (and potentially feature-restricted) option.**

Azure Migrate Server Assessment Tool

The Server Assessment Tool provides the following information to help your organization make the best decisions when preparing to move resources to Azure:

- **Azure Readiness.** This tool determines if the servers discovered on-premises are good candidates for moving to Azure.
- **Azure Sizing.** This tool estimates the size of a virtual machine once it has migrated to Azure, based on the existing specifications of the on-premises server.
- **Azure Cost Estimation.** This server assessment tool will help to estimate the run rate for machines that are migrated to Azure.

No agents are required by the Server Assessment tool. Server assessment is configured as an appliance and runs on a dedicated VM or physical server in the environment being evaluated.

Once an environment has been scanned for assessment, administrators can review the findings of the tool and group servers for specific projects or lifecycles. (The grouping of servers is done after assessment.) Then, groups of servers can be evaluated for migration to Azure.

When reviewing server groups for migration, be sure to consider things like connectivity to Azure and any dependencies that applications or servers being moved may have.

To complete a server environment assessment, perform the following steps:

1. Locate Azure Migrate within the Azure Portal.
2. Create an Azure Migrate resource from the Azure portal by selecting **Assess and Migrate Servers** on the **Overview** blade, as shown in Figure 2-1.

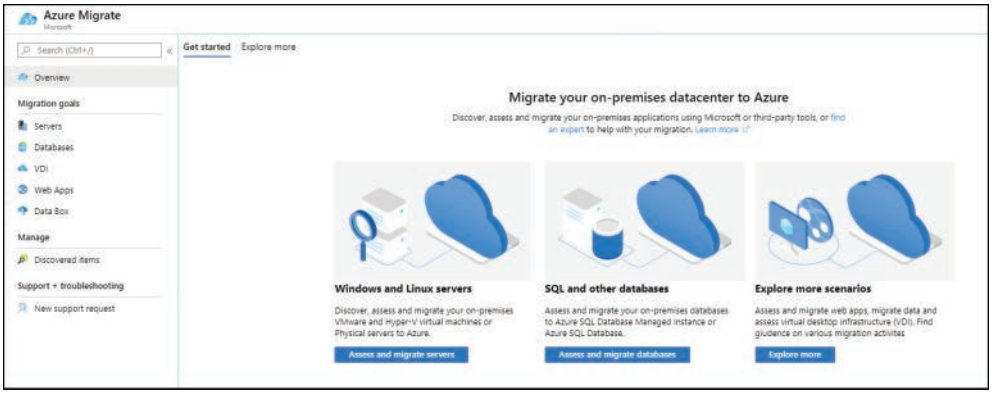

FIGURE 2-1 Choosing Assess And Migrate Servers

3. Select **Add Tool(s)** to create a project and select assessment and migration tools, as shown in Figure 2-2.

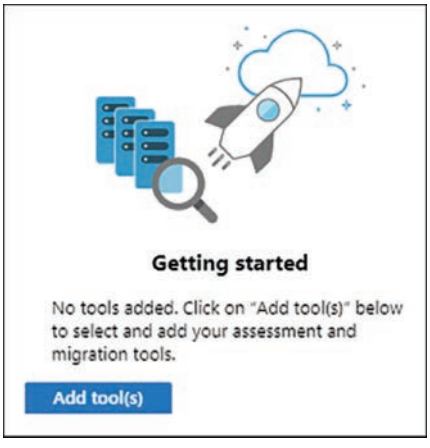

FIGURE 2-2 Assessment and migration tool selection

4. Enter the details required for the migration project for servers, as shown in Figure 2-3.
5. Select a **Subscription**.
6. Select a **Resource Group**.
7. Enter a name for the Azure Migrate project.

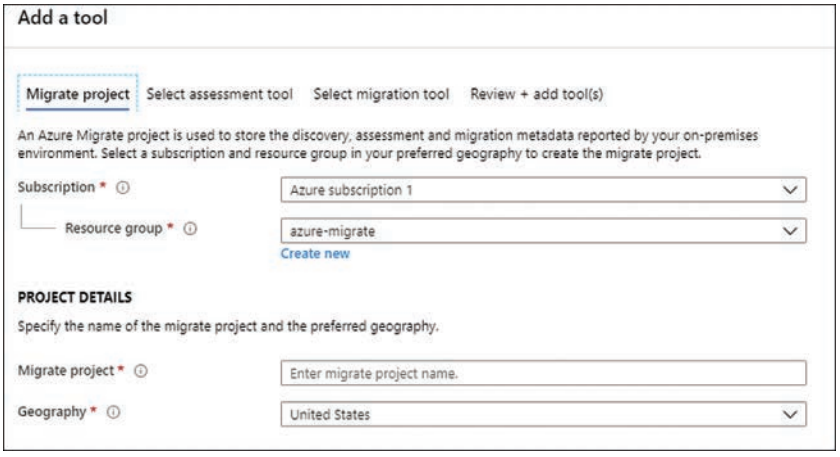

FIGURE 2-3 Details for configuration of server migration project

8. Select the **Azure Migrate: Server Assessment** tool and click **Next**, as shown in Figure 2-4.

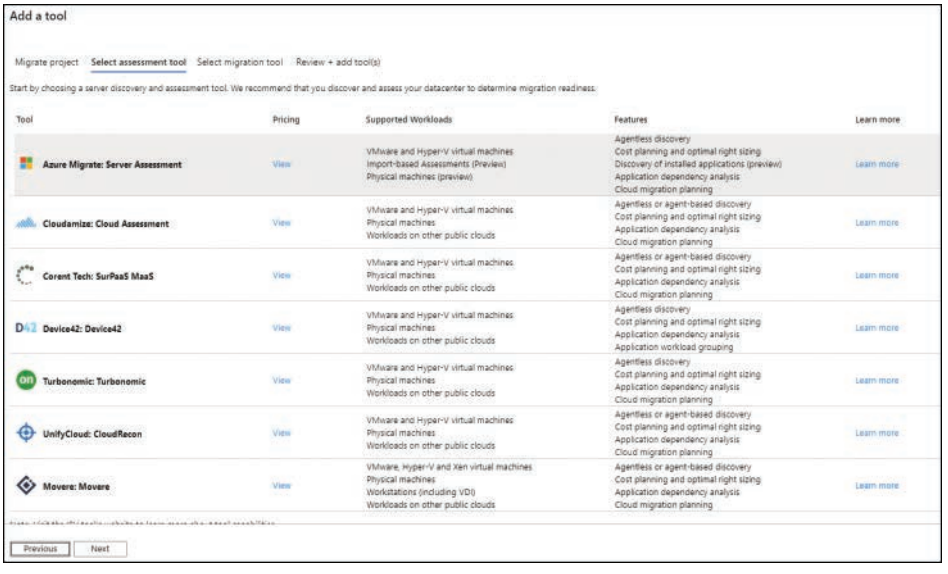

FIGURE 2-4 Tools for server assessment to Azure

9. Select the **Skip Adding A Migration Tool For Now** check box and click **Next**, as shown in Figure 2-5.

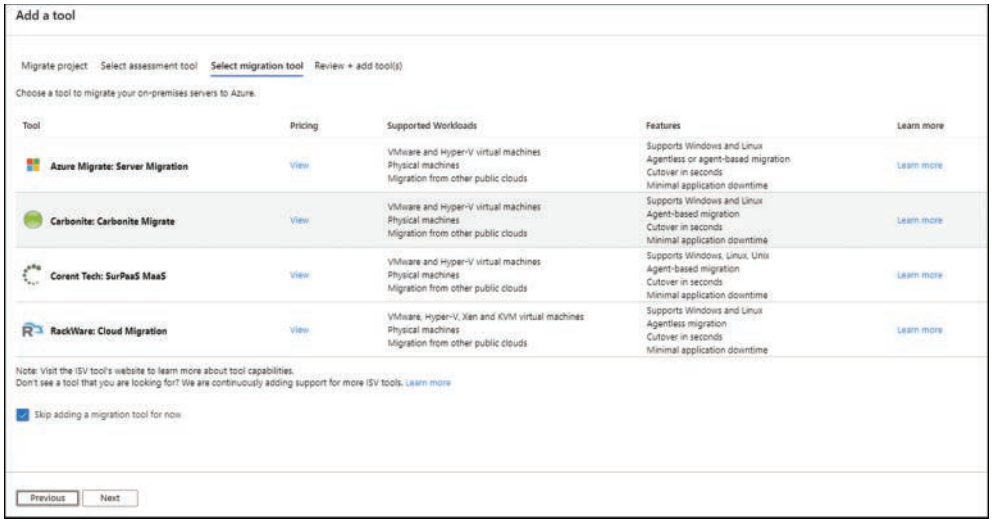

FIGURE 2-5 Server migration tools

10. Review the assessment selections made and click **Add Tool(s)**, as shown in Figure 2-6.

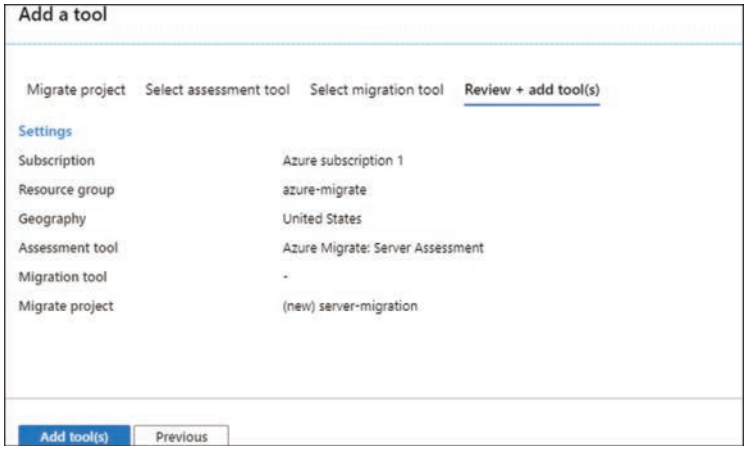

FIGURE 2-6 Review choices and continue

11. Once the assessment tool has been chosen in Azure, additional setup of the appliance is necessary.

12. Click **Discover** under **Assessment Tools**. The **Azure Migrate: Server Assessment** dialog box shown in Figure 2-7 below.

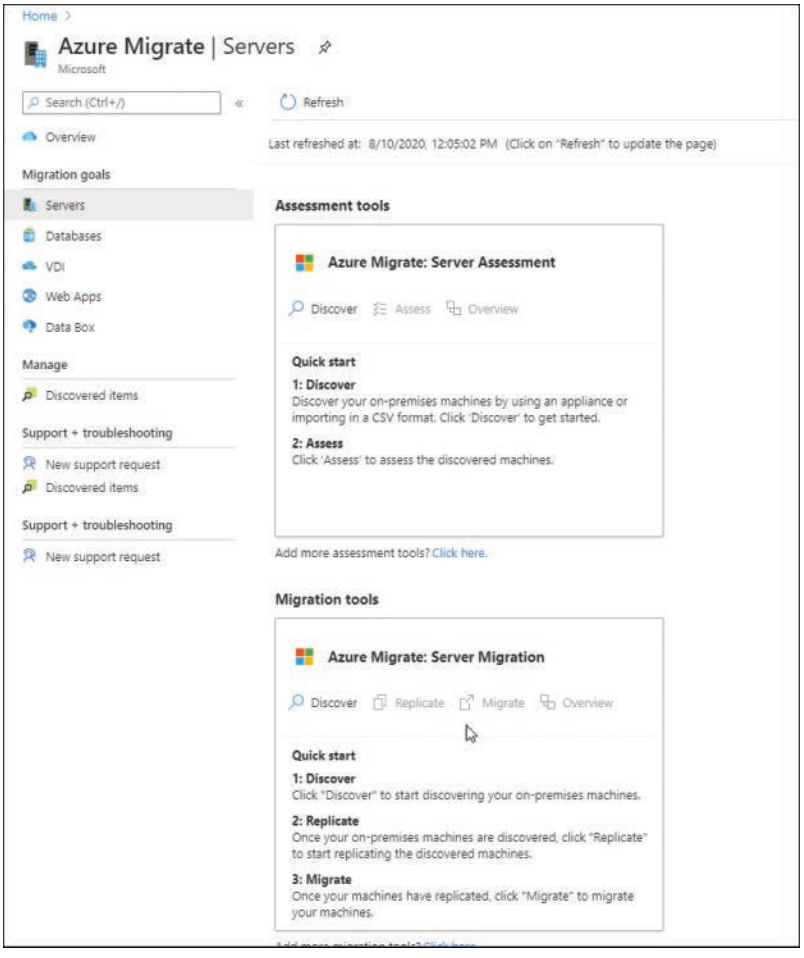

FIGURE 2-7 Discovering servers for migration to Azure

13. To use an appliance, select **Discover Using Appliance**, as shown in Figure 2-8.

FIGURE 2-8 Discovering servers using a self-hosted appliance

14. Choose the hypervisor type used in the environment: **Hyper-V**, **VMware**, or **Physical Servers**.
15. Download the appliance and install it in the environment.
16. Using a browser, visit the IP address of the appliance, configure it to reach the Azure Migrate project, and then start discovery.

After about 15 minutes, machines that are discovered will begin to appear in the Azure Migrate Discovery Dashboard.

You can also complete a CSV template, which supplies the details of your environment, and then upload it to the Azure Migrate project if you would rather not use the discovery appliance. This is shown in Figure 2-9.

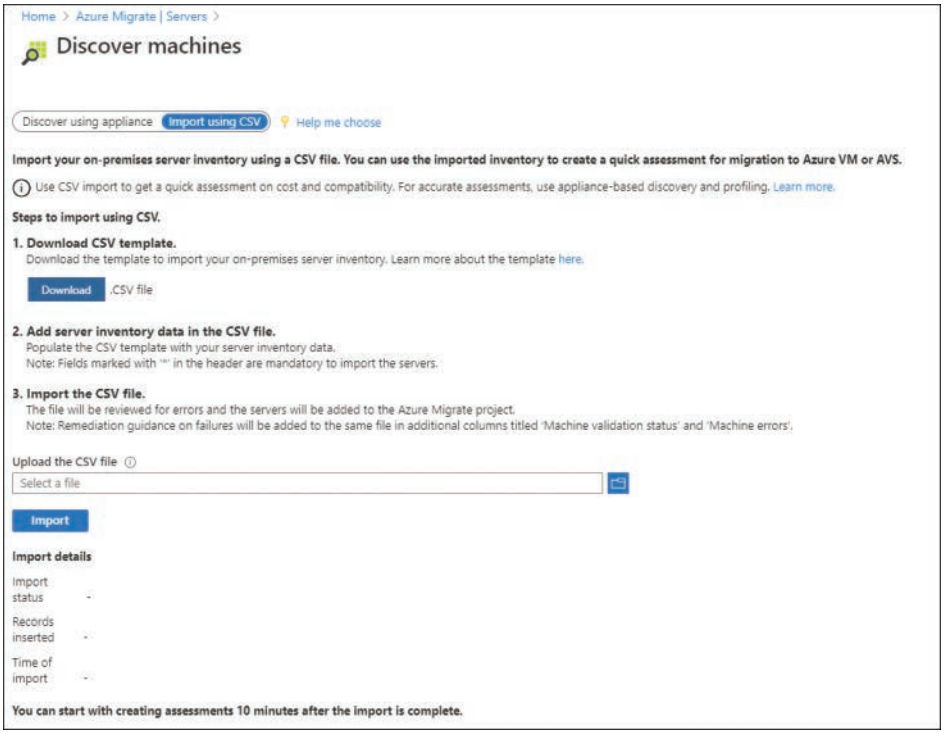

FIGURE 2-9 CSV template download to provide information about environment

NOTE **ASSESSMENT AND MIGRATION – BETTER TOGETHER**

Assessment and migration are discussed together here because the same tool is used for both operations.

To complete a web app assessment and migration, complete the following steps:

1. Inside the existing Azure Migrate project, select **Web Apps** from the **Migration Goals** section of the navigation bar.
2. Select **Add Tool(s)** and choose the **Azure Migrate: Web App Assessment** tool, as shown in Figure 2-10.

FIGURE 2-10 Adding Azure Migrate: Web App Assessment tool

3. Click **Next**.
4. Select the **Skip Adding A Migration Tool** check box and click **Next**.
5. After reviewing the configuration, click **Add Tool(s)**.
6. Once the web app assessment tool has been added, download the Azure App Service Migration Assistant to assess internal web applications. If the application has a public URL, it can be scanned via the public Internet.
7. Install the assessment tool on any web servers containing applications for migration. IIS 7.5 and administrator access on the server(s) are the minimum requirements to complete an assessment. Currently, PHP and .NET apps are supported for migration, with more application types coming soon.
8. The migration tool will determine whether the selected websites are ready to migrate to Azure, as shown in Figure 2-11.

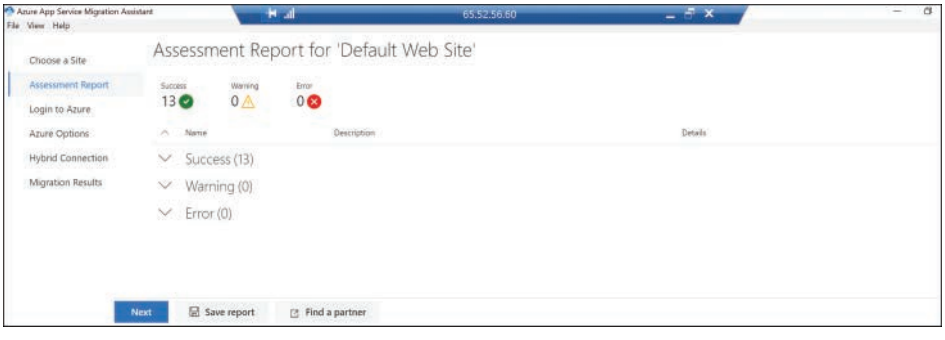

FIGURE 2-11 Website Assessment for migration to Azure App Services

9. Once the assessment tool has reviewed the chosen web applications, click **Next** to log in to Azure using the provided device code and link provided in the wizard, show in Figure 2-12.

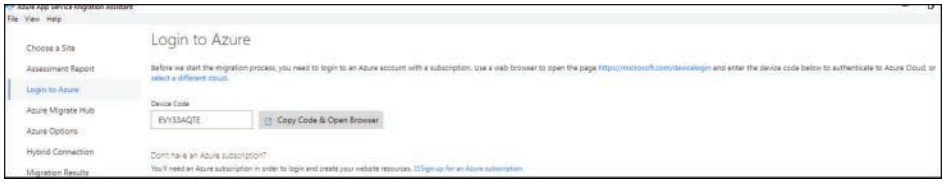

FIGURE 2-12 Use the link provided to open a browser and log in to your Azure Migrate project

10. Click Azure Options in the left-side navigation pane and set the **Subscription**, **Resource Group**, **Destination Site Name**, **App Service Plan**, **Region**, **Azure Migrate Project**, and **Databases** options, as shown in Figure 2-13.

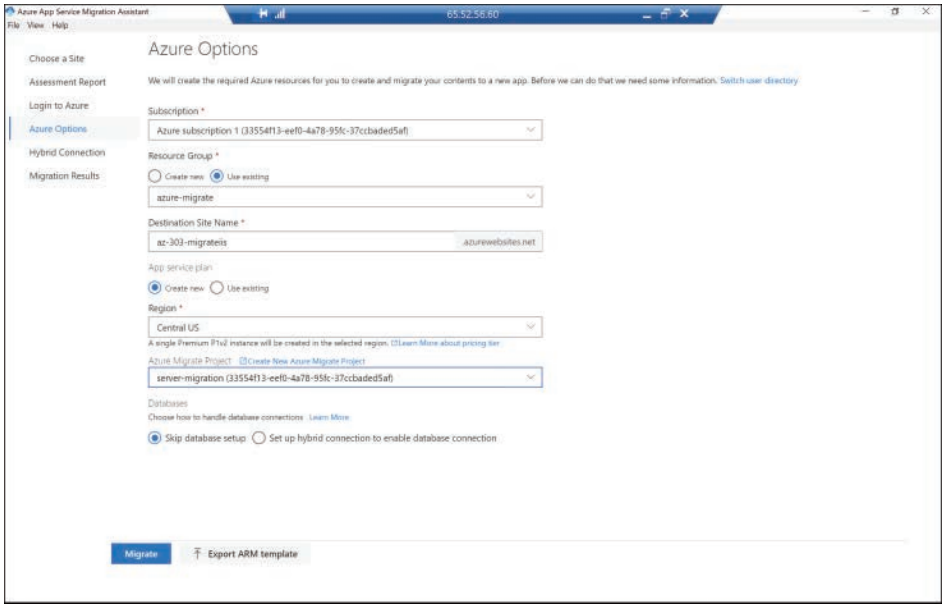

FIGURE 2-13 Options for Azure Migrate web app utility

11. If your application has a database back end, select the **Set Up Hybrid Connection To Enable Database Connection** option and enter the name of the on-premises database server and the port on which to connect in the On-Premises Database Server field shown when the option is selected.
12. Click **Migrate** to migrate the application as is or click the **Export ARM Template** button on the **Azure Options** screen to produce the JSON-based ARM template for the application for later deployment to Azure.
13. The migration progress is shown in Figure 2-14. You will also be able to see the resources once they are migrated in the Azure portal.

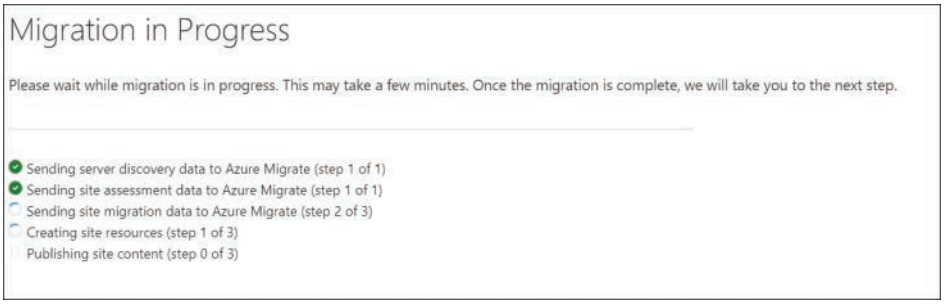

FIGURE 2-14 Migration in process

Complete a SQL database assessment and migration using the following steps:

1. Within the Azure Migrate project, select **Databases** > **Add Tool(s)**.
2. Select the **Azure Migrate: Database Assessment** tool and click **Next**, as shown in Figure 2-15.

FIGURE 2-15 Database Assessment tool selection in Azure Migrate

3. To proceed with a migration if the assessment produces the expected outcome, select the **Azure Migrate: Database Migration** tool.
4. If you are assessing production workloads and/or extremely large databases, select the **Skip Adding A Migration Tool For Now** check box to allow further review of the assessment to correct any issues found.
5. Once the tools have been added to the migration project, as shown in Figure 2-16, click the **Download** link to download the Database Migration Assessment tool to start the assessment.

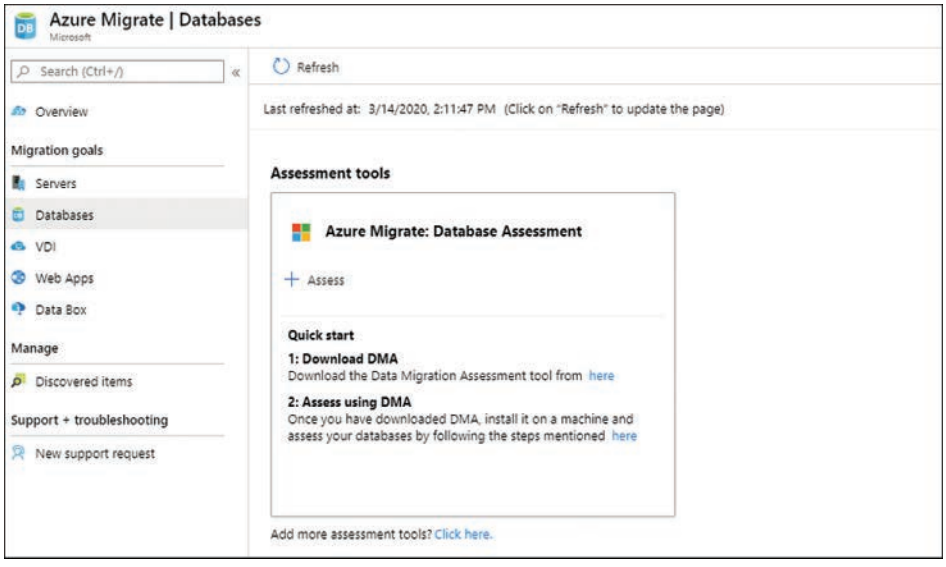

FIGURE 2-16 Database Assessment and Migration tools

6. Install and run the Data Migration Assistant Tool on the SQL server(s) to be migrated to Azure.
7. In the Data Migration Assistant tool, as shown in Figure 2-17, click **New** to add a new project.

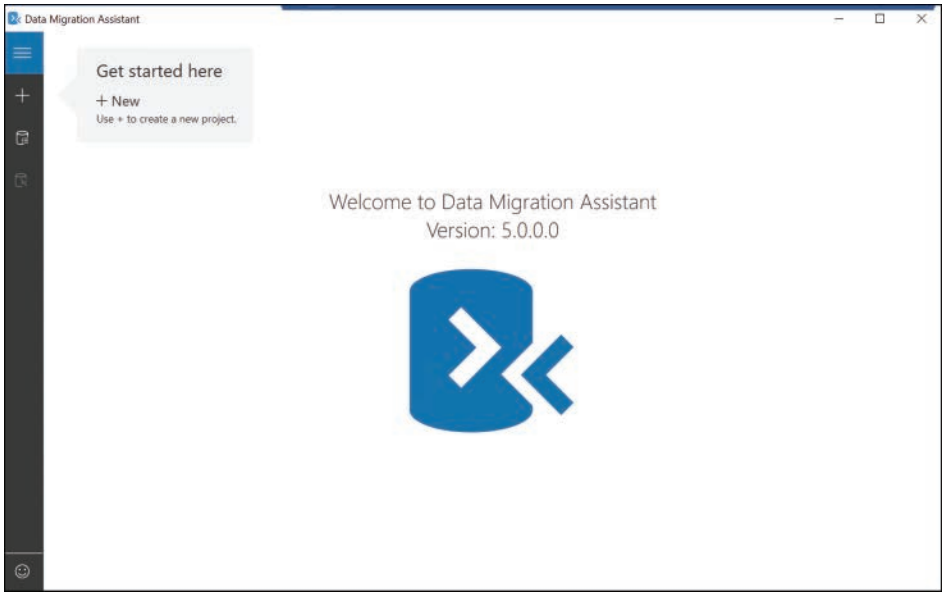

FIGURE 2-17 Azure Migration Assistant

8. Enter a name for the project and select the following for the SQL server data being migrated:
   - **Assessment Type.** Choose either database engine or integration services.
   - **Source Server Type.** Choose either SQL Server or AWS RDS For SQL Server.
   - **Target Server Type.** Choose from Azure SQL Database, Azure SQL Database Managed Instance, SQL Server On Azure Virtual Machines, or SQL Server.
9. On the **Options** screen within the created project, following are the selected (and default) options:
   - **Check Database Compatibility.** This will check an existing database for any issues that would prevent it from running in Azure SQL.
   - **Check Feature Parity.** This option looks for unsupported features in the source database.
10. Select the SQL server(s) and choose the appropriate authentication method(s) for the SQL server:
   - **Windows Authentication.** Use the currently logged-in Windows credentials to connect.
   - **SQL Server Authentication.** Use specific credentials stored in the SQL server to connect.
   - **Active Directory Integrated Authentication.** Use the logged-in Active Directory user for authentication.
   - **Active Directory Password Authentication.** Use a specific Active Directory user or service account to authenticate.
11. Select the properties for the connection:
   - **Encrypt connection.** Check this box if the SQL Server (and/or your organization's information security team) requires connections to be encrypted.
   - **Trust Server Certificate.** If the SQL Server is using certificates, the Data Migration Assistant can trust these certificates to simplify future connections.
12. Click **Connect**.
13. From the list of databases found, select any that should be included in the assessment, as shown in Figure 2-18.
14. Click **Add**.

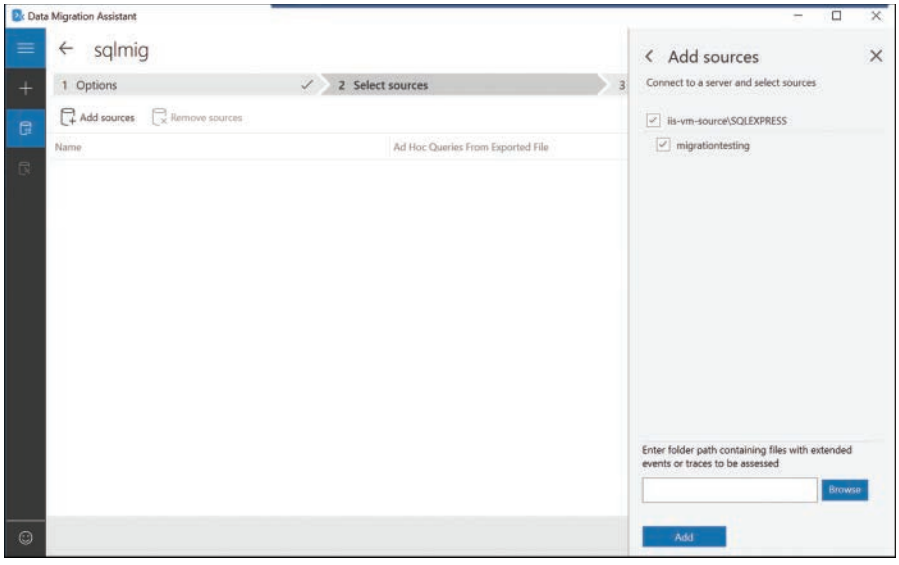

FIGURE 2-18 Include selected databases in Assessment

15. Once the databases are added to the assessment, if there are log files or extended events to include, click **Browse** to locate and include them, as shown in Figure 2-19.

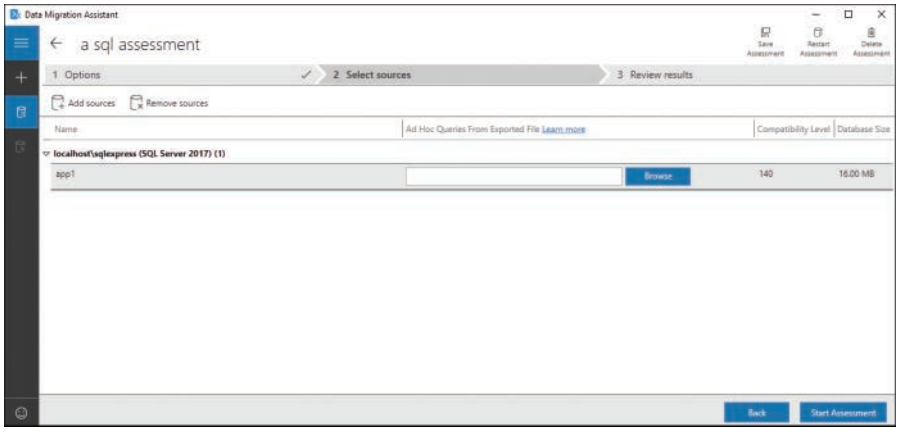

FIGURE 2-19 Include log files or extended events

16. Review the assessment for both feature parity and compatibility and fix any issues found. If there are discrepancies, they will need to be resolved before the migration can proceed.

> ***NOTE*** **SOME ITEMS MAY REQUIRE ADDITIONAL WORK**
>
> **The assessment will return items that are unsupported by Azure SQL but are in use within the source database(s). It will also find any compatibility issues within the data in the source database. These items will need to be remedied before migrating the data to Azure SQL.**

17. Click **Upload To Azure**.
18. You will be prompted to sign in if you are not already signed in on the computer where the assessment is running.
19. Select the **Subscription** and **Resource Group** and then click **Upload**.

Migrating information is straightforward as well, though there must be an existing Azure SQL database in which to migrate the SQL data. You should create this Azure SQL database beforehand because the tools will not build Azure SQL or other types of SQL in Azure as part of the process.

To complete a migration after the assessment of SQL databases, complete the following steps:

1. In the Data Migration Assessment tool, select the **Migrations** option.
2. Specify the source SQL instance and log-in method.
3. Specify the target Azure SQL Server name and credentials, and then click **Connect**.

> ***NOTE*** **ACCESS REQUIRED TO PROCEED**
>
> **You will need to ensure the system where the migration is running has access to the Azure SQL DB by allowing access from the IP address of the client within the Azure SQL Server networking details.**

4. Select the database to migrate and click **Next**, as shown in Figure 2-20.

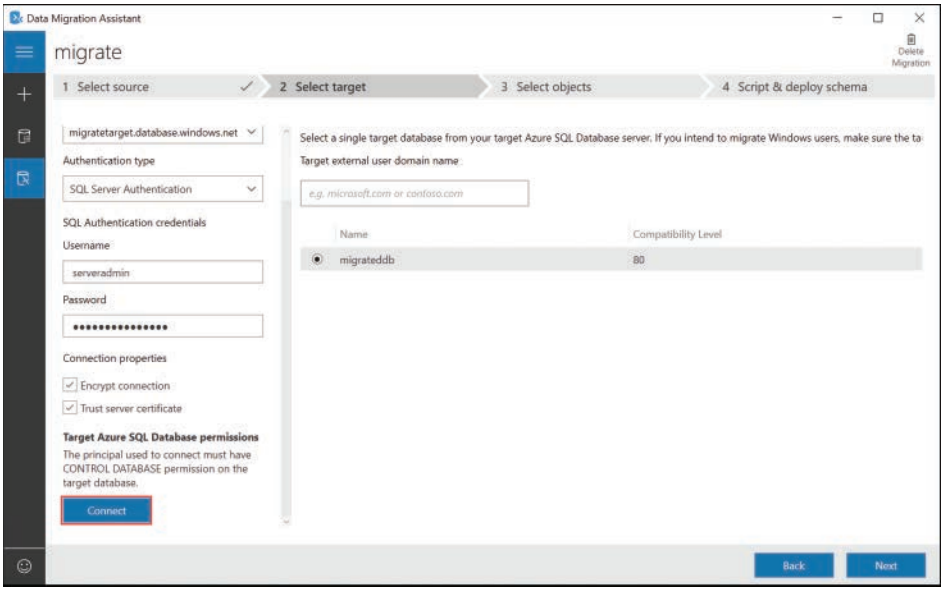

FIGURE 2-20 Connect to Azure to migrate source data to Azure SQL Database

5. Once the preparation completes and has been reviewed, click **Generate SQL Script** to create a script. A generated script is shown in Figure 2-21.

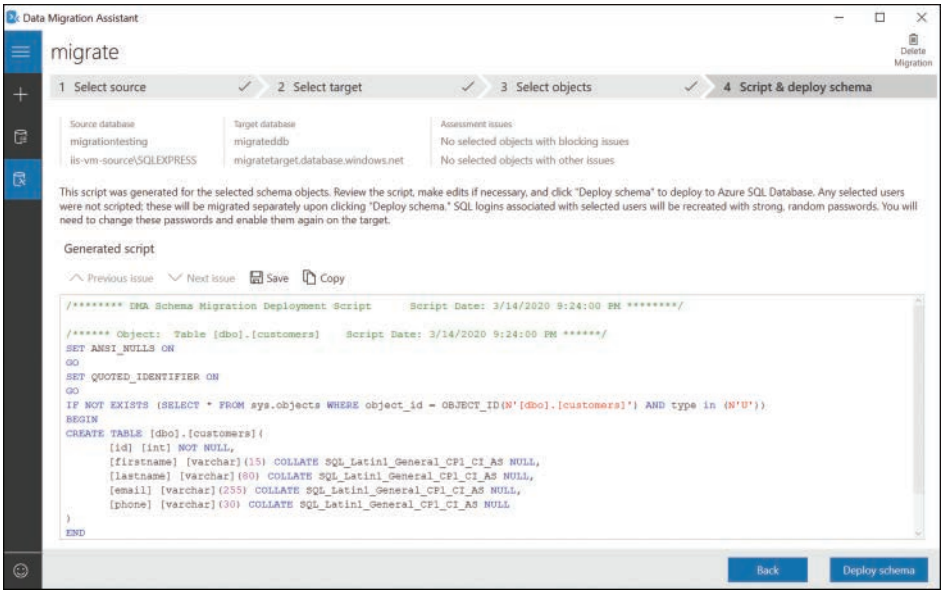

FIGURE 2-21 An SQL Script generated for migration work

6. To push this data to a specified instance of Azure SQL Database using the Data Migration Assistant, click **Deploy Schema**.

Migrate virtual desktop infrastructure to Azure

Azure Migrate also allows you to bring virtual desktop infrastructure (VDI) into Azure. The assessment of VDI requires the use of Lakeside: Systrack, a third-party tool, to complete the assessment of VDI environments. The migration process, however, follows the same path as a server migration, allowing workloads from VMware or Hyper-V to be migrated.

Azure Data Box allows offline migration of existing data to Azure. The Data Box itself is a ruggedized NAS that is capable of storing up to 100 TB of data with AES 256 encryption for transporting your data physically to the Azure datacenter(s) for ingestion.

To complete a Data Box offline migration of workloads to Azure, complete the following steps:

1. From within an Azure Migrate project, select **Data Box** as the **Migration Goal**.
2. Provide the following details about the data being ingested:
   - **Subscription.** Select the name of the Azure Subscription where the data will be transferred.
   - **Resource Group.** Select the resource group where the data will be transferred.
   - **Transfer Type.** Select the type of transfer being performed.
   - **Source Country/Region.** Select the country or region where the data lives today.
   - **Destination Azure Region.** Select the region in Azure where the data should reside after transfer.

3. Click **Apply**.
4. Select the appropriate Data Box option for your migration, as shown in Figure 2-22.

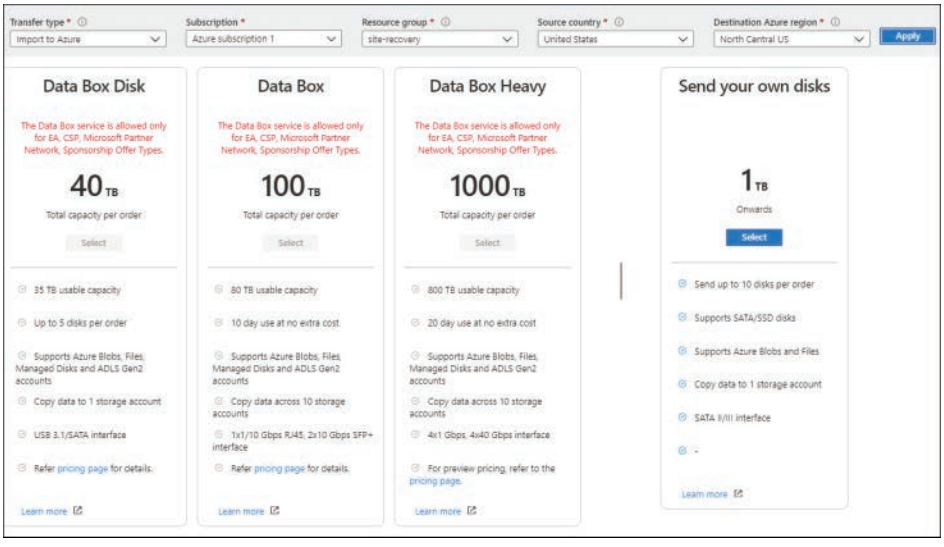

FIGURE 2-22 Select the appropriate Data Box size for your migration

Note that Data Box disks provided by Microsoft are only allowed with the following subscription offers:

- **EA.** Enterprise Agreement
- **CSP.** Cloud solution provider partnership
- **Microsoft Partner Network.** Partner organizations
- **Sponsorship.** A limited, invite-only Azure subscription offer provided by Microsoft

If you do not have an offer tied to your Azure subscription that meets the above requirements to use a provided Data Box, you can send in data on your own disks. If you provide your own disk, the following requirements apply:

- Up to 10 disks per order
- 1 TB per disk
- Copying data to one storage account
- $80 per disk import fee

These Data Box options are for offline transfers to Azure. Using the Data Box Gateway, a virtual appliance within your environment, will perform an online data migration to Azure.

5. Once you have selected a disk option, you will be able to configure the options for your environment (see Figure 2-22). You will choose the following options shown in figure 2-23:
   - **Type.** Import to or export from Azure.
   - **Name.** The name of the job to identify it to Azure.

- **Subscription.** Select the subscription for the job.
- **Resource Group.** Select an existing resource group or create a new one for the job.

6. After clicking **Next: Job Details**, you will supply the following information, shown in Figure 2-24:
   - **Upload Journal Files.** Specify the path to the journal file for each drive being used for import.
   - **Import Destination.** Specify a storage account to consume ingested data and the region the data will be stored in.
   - **Provide Return Shipping Information.** Specify the name and address details to allow your disk to be returned along with carrier information as shown in Figure 2-24.

Review and confirm your choices.

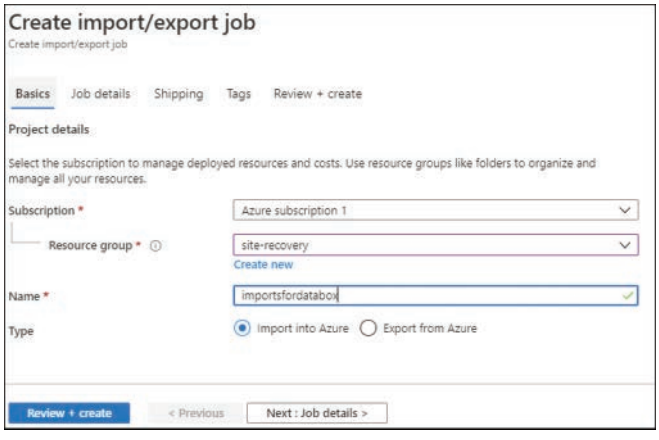

FIGURE 2-23 Configuration options for migration environment

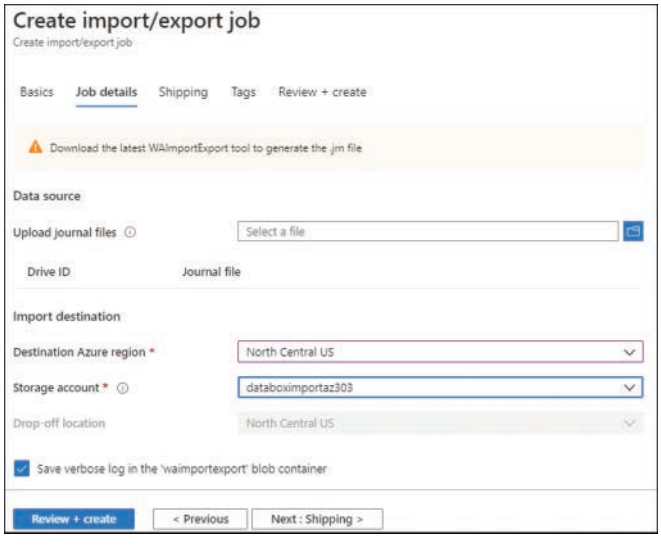

FIGURE 2-24 Provide job details

If you have shipped your own drives for this process, you will need to supply return information.

> ***NOTE*** **ONLY OPTION**
>
> **Supplying your own drives is the only option available for some Azure subscription types.**

As discussed above, if you are not using a EA,CSP, Partner, Sponsorship subscription in Azure, or one with a special offer designation, you might be required to use your own drive(s) with Data Box. If that is the case, return shipping information is required, as shown in Figure 2-25.

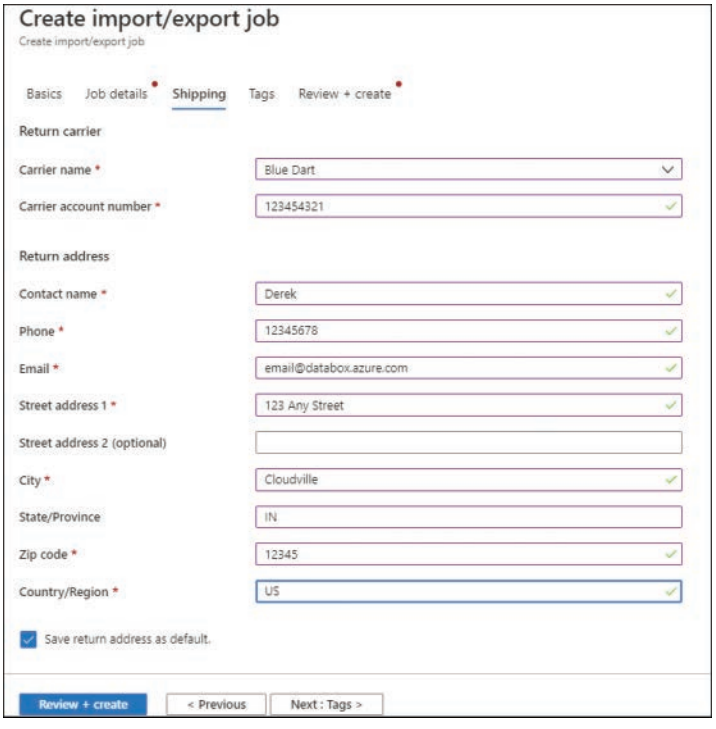

FIGURE 2-25 Return shipping information

There are other assessment and migration tools such as Movere or other third-party tools. These tools might require additional spend to assess your environment. Movere is free and can be used as part of this process because it was acquired by Microsoft, but this book focuses on the Azure tools for assessment and migration.

Implementing Azure Update Management

An organization that is seeking to move workloads to the cloud is probably (hopefully) already ensuring these servers are patched regularly and kept as close to truly up to date as their governance and infosec organizations will allow. Migrating a server to Azure does not necessarily

remove this burden from server administration teams. The last thing to cover in this section on workload management and migration is managing updates in the cloud. As you might expect, Azure has a method for that, and here, we will look at the implementation of this feature set.

> ***NOTE*** **IF IT IS WORKING, MAYBE IT SHOULD STAY WORKING**
>
> **Just because Azure brings an update management tool to the party does not mean it will be the best patch management strategy for your organization. In the event your organization has mostly Windows domain-joined systems or a well-oiled strategy for patching Linux, there might be no reason for you to change the way things are. Sure, you should evaluate the situation, but make sure the new tools fit the needs of your organization.**

To configure Azure Update Management, complete the following steps:

1. Log in to the Azure portal and navigate to a running virtual machine.
2. In the **Operations** section of the left navigation menu for the VM, select **Update Management**.
3. Supply the following information:
   - **Log Analytics Workspace Location.** Select the region for the account.
   - **Log Analytics Workspace.** Choose (or create) a log analytics workspace.
   - **Automation Account Subscription.** Select the Azure subscription to house this resource.
   - **Automation Account.** Choose or create an automation account for Update Management.
4. Click **Enable** and wait for the deployment to complete (between 5 and 15 minutes).

> ***NOTE*** **BE PATIENT WITH DATA COLLECTION**
>
> **Once the solution is enabled, the solution will need to collect data about your system(s) to help ensure the best update management plan. This can take several hours to complete. The Azure portal dialog box recommends allowing this to run overnight.**

5. Once the solution has finished onboarding virtual machines, revisiting the **Update Management** blade for one or more VMs will display information as it becomes available.
6. Selecting the **Update Agent** readiness troubleshooter will help determine which items might interfere with the use of the Update Management solution (see Figure 2-26).

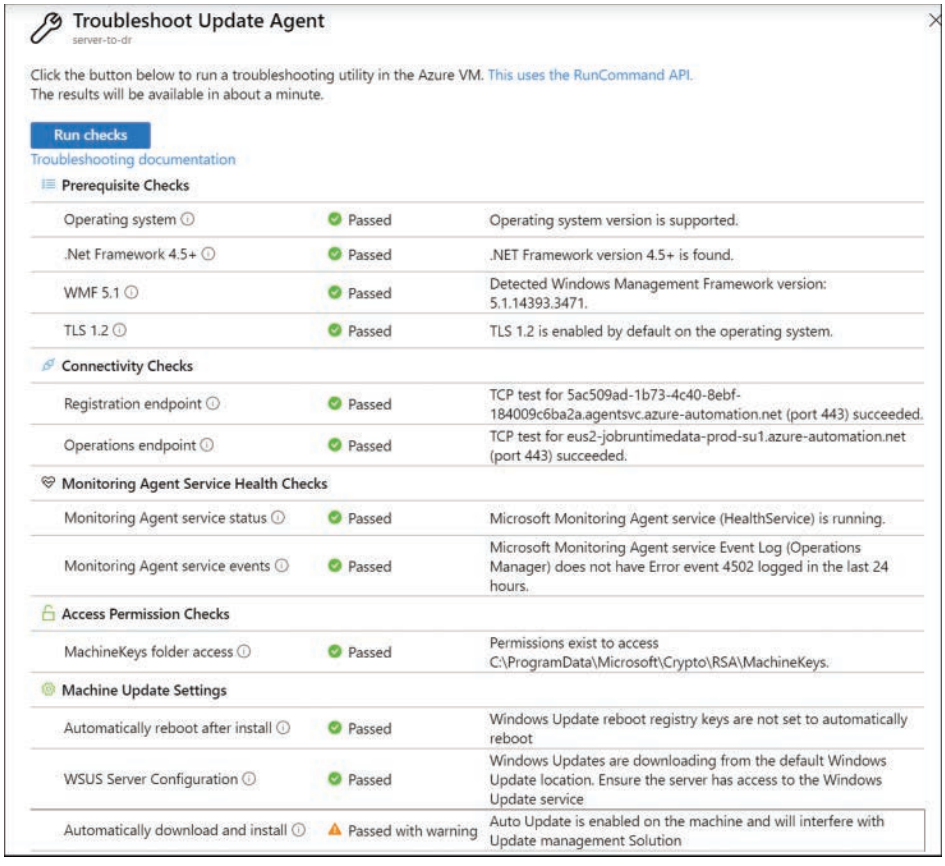

FIGURE 2-26 Update Agent Readiness configuration

7. If your VM is running Windows Auto Update, you will want to disable it before proceeding with Update Management in Azure.

Once the onboarding process has completed and after waiting for configuration to complete, visit the **Update Management** blade for a VM to see the **Missing Updates** for the system, which are broken out by **Critical**, **Security**, and **Others**, as shown in Figure 2-27.

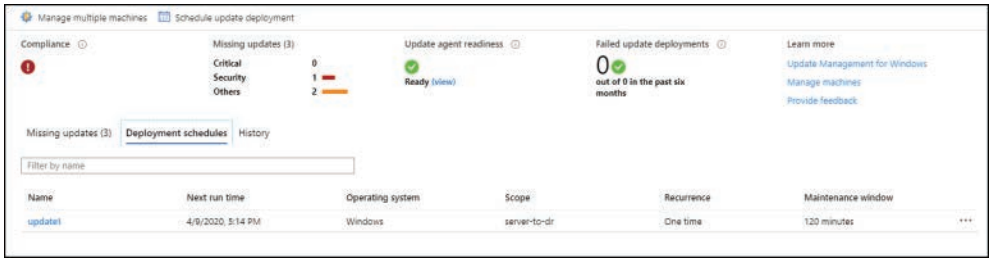

FIGURE 2-27 Security fixes needed before migration can proceed

Selecting an update from the **Missing Updates** list will open Log Analytics and insert a query looking for that update; running the query will display the update as a result.

When a server has onboarded into Update Management, it can be patched by configuring a schedule for update deployment. To do that, complete the following steps:

1. From the **Update Management** blade, click **Schedule Update Deployment**.
2. Enter the following information about the schedule:
   - **Name.** A name for the deployment.
   - **Update Classification.** The update types to be included.
   - **Include/Exclude Updates.** Optionally, select the updates to include or exclude.
   - **Schedule Settings.** When the deployment should happen.
   - **Pre/Post Scripts.** Any scripts that should run before or after deployment.
   - **Maintenance Window.** Specify the length of the maintenance window for deploying updates.
   - **Reboot Options.** Choose the reboot options for the update(s).
3. Click **Create** on the update deployment schedule.

The deployment that has been scheduled will be listed on the **Deployment Schedule** tab. Also, any deployments will be defaulted to 30 minutes after the current time to allow the schedule to push to Azure.

After these items are configured, the updates will be applied as per the schedule that has been set up.

This section took a high-level overview covering the various types of migrations to Azure using built-in Azure tools. As this technology changes and Azure evolves, this will surely expand.

NEED MORE REVIEW? **AZURE MIGRATE**

Check out these resources:

- **Azure Migrate Guidelinesfor Hyper-V.** ***https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-Hyper-V#assessment-appliance-requirements***
- **Azure Migrate Overview.** ***https://docs.microsoft.com/en-us/azure/migrate/***
- **Update Management Solution in Azure.** ***https://docs.microsoft.com/en-us/azure/automation/update-management/overview***
- **An Overview of Azure VM Backup.** ***https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction***

Skill 2.2: Implement disaster recovery using Azure Site Recovery

With the growing number of organizations moving to Azure, one of the first things that comes to mind is leveraging the cloud as a target for disaster recovery. If an organization has an existing co-location for DR data, Azure can provide some or all the services needed to replace this secondary (or multiple secondary) datacenter(s). In this section, the use and configuration of Azure Site Recovery are covered.

NOTE **BEFORE THERE WAS MIGRATE, THERE WAS SITE RECOVERY**

Before Azure Migrate, Azure Site Recovery was the Microsoft solution for both disaster recovery and migration of servers to Azure.

This skill covers:

- Configure Azure components of Site Recovery
- Configure on-premises components of Site Recovery
- Replicate data to Azure
- Migrate by using Azure Site Recovery

Configure Azure components of Site Recovery

Azure Site Recovery provides a way to leverage the scale of Azure while allowing Resources to be failed back to your on-premises datacenter should the need arise as part of a business continuity and disaster recovery (BCDR) scenario. Since the introduction of Azure Migrate and the additional workloads covered previously in this chapter, Site Recovery has become the primary disaster recovery tool for use with Azure.

Follow these steps to configure the Azure resources to use Site Recovery for DR to Azure:

NOTE **CONSIDER CREATING THE AZURE RESOURCES FIRST**

Creating the Azure resources first prepares the destination and ensures that nothing is missed. Because the process moves files into Azure, this can minimize issues when the transfer begins because the target resources will be identified up front.

1. Log in to your Azure subscription.
2. Create a resource group to hold your Azure Backup Vault.

Index

A

access control, Azure SQL Database, 302
access keys
  managing, 35–36
  rotating, 36
access policies, creating, 177–178
access tiers, 32
  blobs, 31–32
accounts. *See also* user accounts
  Cosmos DB, 277, 278–279
  ACI (Azure Container Instances), 22, 264
ACR (Azure Container Registry), 262
  creating resources for container images, 262–264
ACS (Azure Container Service). *See* AKS (Azure Kubernetes Service)
action groups, creating, 26–27
Activity Log, 5
ADE (Azure Disk Encryption), 53–56
advanced threat protection, Azure SQL Database, 303–304
AKS (Azure Kubernetes Service), 22
  configuring, 266
  creating a cluster with Azure CLI, 266–267
  policy services, 231–232
alerts
  creating, 28–29
  viewing, 29
APIs
  Cosmos DB, 281–282
    Cassandra, 283–284
    Gremlin, 284
    MongoDB, 283
    SQL, 282–283
    Table, 283
  selecting, 286
APM (Application Performance Management), Application Insights, 20–21
application gateways, 188–189
  Azure Load Balancer, 195
    back-end pools, 197
    configuring, 195–197
    health probes, 198
    rules, 198–199
  front-end configuration, 190–191
  load balancing, 191–192
  URL path-based routing, 192–195
Application Insights, 20–21
  availability, 21
  failures, 21
Application Map, 20
application registration, 183–186
  creating a client secret, 186–187
archive tier, Azure Storage, 32
ARM (Azure Resource Manager) templates, 63–64
  and Azure Blueprint, 235
  blank, 67
  deploying from, 70–73
  expressions, 69–70
  modifying, 66–68
  parameters, 67–68
  saving a deployment as, 64–66
  VHD (virtual disk), 73–74
ASGs (Application Security Groups), 211, 214
  assigning members, 215
  creating, 214–215
assessment tools, server migration, 132–133
assigning
  members to ASGs (Application Security Groups), 215
  policies, 229–230
  roles, 240–241
auditing, Azure SQL Database, 304–305
authentication
  application registration, 183–186
  managed identity, 181–183

authentication, *continued*
multi-factor, 93–95, 131
bypass options, 97–98
configuring verification methods, 100–101
trusted IPs, 98–99
storage accounts, 42–46
two-step verification, 93, 97
auto-failover groups, 311–314
automation runbook, creating, 75–79
autoscaling, 62
availability sets, 56–59
availability zones, 59–60
Azure Active Directory Log, 5
Azure AD (Active Directory), 86, 176
adding custom domains, 87–88
application registration, 183–186
creating a client secret, 186–187
conditional access, 108–111
configuring user accounts for MFA, 93–95
Connect Health, 125–127
fraud alerts, 96–97
guest accounts
adding, 101–102
managing, 102–105
Identity Protection, 106–108
implementing self-service password reset, 89–91
managed identity, 181–183
managing multiple directories, 88–89
seamless SSO, 123–125
storage accounts, authentication, 42–46
tiers, 86–87
Azure AD Connect
identity synchronization options, 118–119
installing and configuring, 112–118
Azure Advisor, recommendations, 9–10
Azure App Service, 249
ACI (Azure Container Instances), creating, 264
deployment slots, 254
creating, 254–255
enabling managed identity, 182–183
VNet integration, 253–254
web apps, 250
for containers, 251–252
creating, 250–251
Azure Bastion, 215–216
configuring, 216
connecting to a server, 217–218
Azure Blueprint, 232
and ARM templates, 235
configuring, 232–234
CosmosDB backend, 232
Azure CLI
commands for managing containers, 266
creating an AKS cluster, 266–267
documentation, 273
Azure Cosmos DB, 276–277
accounts, 277
configurations, 287–288
creating, 278–279
APIs, 281–282
Cassandra, 283–284
Gremlin, 284
MongoDB, 283
selecting, 286
SQL, 282–283
Table, 283
data consistency options, 279–280
setting up replicas, 287
Azure Cost Management, 15
budgets, 16
spending, 16
reports, 17
Azure Data Box, offline migration, 146–149
Azure Dedicated Hosts, 63
Azure Firewall, 199
configuring on a virtual network, 199–200
rules, 201–203
service tags, 202–203
threat intelligence, 203
Azure Front Door, 204
configuring, 204–205
WAF policies, 206–208
Azure Functions, 168, 257
function apps, creating, 168–170, 258–259
functions, 257–258
creating, 259–260
Azure Key Vault, 176
access policy, creating, 177–178
accessing an endpoint, 181
creating resources, 176–177
cryptographic operations, 179
key management operations, 179
privileged key operations, 179–180
Soft Delete, 177

Azure Load Balancer, 195
back-end pools, 197
configuring, 195–197
health probes, 198
rules, 198–199
Azure Logic Apps, 255
creating a logic app, 255–256
logic apps
creating an email action, 257
creating an RSS trigger, 256–257
Azure Migrate, 132
assessment tools, 132–133
Server Assessment tool, 133–138
SQL database assessment and migration, 141–144, 145–146
virtual desktop infrastructure migration, 146
Azure Monitor
action groups, creating, 26–27
alerts
creating, 28–29
viewing, 29
baselining, 8–9
for containers, 12–22
Insights, 18
Log Analytics workspace, creating, 18–19
monitoring performance capacity, 10–11
visualizing diagnostics data, 12–13
Azure Monitor Log, 10
Azure Network Watcher, 14
topology, monitoring, 14–15
Azure Policy, 228–229
assigning a policy, 229–230
Azure portal
exporting templates, 64–66
template library, 74–75
Azure Security Center, 3
free tier, 3
Log Analytics Agent, 3, 10
standard tier, 3
core features, 3–4
Azure Sentinel, 4
Azure Service Bus, 174
message queue, 175
service bus namespace, 174
Azure Service Health, 13–14
Azure Site Recovery, 132, 153
migrating to Azure, 163
on-premises components, configuring, 155–159, 160
recovery plan configuration, 161–162
replicating data to Azure, 160–161
resources, creating, 153–154
test failover, 162
cleanup, 163
Azure SQL Database, 289, 318–319
backups, 294
manual, 297
BCDR (business continuity and disaster recovery), 310
creating, 291–294
flavors, 289
high availability, 309–310, 311
configuring an auto-failover group, 311–314
geo-replication strategy, 311
models, 310
LTR (long-term backup retention) backups, 294–296
creating, 296
restoring, 296–297
Managed Instance, 305–306
creating, 306–308
specifying connection type, 307–309
publishing, 314–321
data migration, 315–318
DMA (Database Migration Assistant), 314, 315
DMS (Database Migration Service), 314–321
methods, 314
online migration, 318–319
phases, 314
purchasing models, 290
read scale-out, 299
scaling, 297–300
security, 299–300
access control, 302
advanced threat protection, 303–304
auditing, 304–305
configuring server-level firewall rules, 300–302
data protection and encryption, 302–303
defense-in-depth strategy, 299
Azure Storage, 30
access keys, managing, 35–36
account failover, implementing, 48
Azure files, configuring, 32–34
blobs
access tiers, 31–32
storage, 34–35
core services, 30–31, 32
disks, 31, 51
encryption, 53–56
roles, 51–52
queues, 31
replication, 46–47

Azure Storage, *continued*
storage accounts
authentication, 42–46
configuring network access, 36–38
private endpoints, 39
SAS (shared access signature), 39–42
types, 31
tables, 31
Azure Table storage, 270–271
configuring table storage data access, 274–276
and Cosmos DB Table API, 276
creating a storage service, 273–274
data model, 271–272
documentation, 273
partition key, 272
row key, 272
SAS (shared access signature), 274–275
stored access policy, 275–276
Timestamp property, 272
Azure Traffic Manager, 208. *See also* NSGs (Network Security Groups)
adding endpoints, 209–210
configuring, 208–209
configuring traffic monitoring, 210–211
real user measurements, 211
traffic view, 211
Azure Update Management, 149–150
configuring, 150–151
Azure VMs
diagnostics extension, 7–8
high availability, 56
availability sets, 56–59
availability zones, 59–60
JIT (just-in-time) access, 4

B

Backup and Site Recovery, 154–155
backups
managing on Azure SQL Database, 294
manual, 297
baselining, 8–9
BEK (BitLocker encryption key), 55
blobs, 30
access tiers, 31–32
storage, 34–35
budgets, creating, 16

C

Cassandra API, 283–284
client secret, creating, 186–187
cmdlets, 33, 35
Get-AzStorageBlobContent, 43
New-AzWebApp, 252
Set-AzDiagnosticSetting, 7
column-family databases, 270
conditional access, 108–111
Configuration as Code, 64
configuring
ADE (Azure Disk Encryption), 53–56
AKS (Azure Kubernetes Service), 266
Azure AD Connect, 112–118
Azure Bastion, 216
Azure Blueprint, 232–234
Azure files, 33–34
Azure Firewall
rules, 201–203
service tags, 202–203
threat intelligence, 203
Azure Front Door, 204–205
WAF policies, 206–208
Azure Load Balancer, 195–197
back-end pools, 197
health probes, 198
rules, 198–199
Azure Site Recovery, on-premises components, 155–159, 160
Azure Table storage, storage data access, 274–276
Azure Traffic Manager
endpoints, 209–210
real user measurements, 211
traffic monitoring, 210–211
traffic view, 211
Azure Update Management, 150–151
guest accounts, 101–105
Log Analytics workspace, 18–19
NoSQL databases, storage account tables, 270
recovery plan, 161–162
resources, diagnostic settings, 5–7
scale sets, 60–61
autoscaling, 62
storage accounts
network access, 36–38
SAS (shared access signature), 39–42

VM storage, 50–53
VPNs
ExpressRoute, 225–226, 227–228
site-to-site, 221–222
Connect Health, 125–127
Connection Monitor, 15
consistency options, Cosmos DB, 279–280
container images
building a storage resource, 262–264
creating, 261–262
containers, 261
blobs, 34–35
commands for managing, 266
creating a web app, 251–252
metrics, 22
monitoring, 12–22
cookie-based affinity, 191–192
cool tier, Azure Storage, 32
Cosmos DB, 276–277
accounts, 277
configurations, 287–288
creating, 278–279
APIs, 281–282
Cassandra, 283–284
Gremlin, 284
MongoDB, 283
selecting, 286
SQL, 282–283
Table, 283
data consistency options, 279–280
disaster recovery, 281
setting up replicas, 287
Table API, 276
Cost Management, 15
budgets, 16
reports, 17
spending, 16
creating
ACI (Azure Container Instance), 264
action groups, 26–27
ASGs (Application Security Groups), 214–215
automation runbook, 75–79
Azure SQL Database, 291–294
Azure Table storage service, 273–274
budgets, 16
container images, 261–262
Cosmos DB account, 278–279
deployment slots, 254–255
function apps, 168–170, 258–259
functions, 259–260
General-purpose V2 account, 31
Log Analytics workspace, 18–19
logic apps, 164–166, 255–256
email action, 257
RSS trigger, 256–257
LTR (long-term backup retention) backups, 296
migration projects, 132
resources, 153–154
Azure Key Vault, 176–177
storage resource for container images, 262–264
web apps, 250–252
custom domains, adding, 87–88

D

databases. *See also* Azure SQL Database; NoSQL
databases; SQL databases
column-family, 270
Cosmos DB, 276–277
dirty reads, 279
document, 270
graph, 270
key-value, 269–270
relational, 288
selecting, 288–289
deploying, from ARM template, 70–73
deployment slots, 254
creating, 254–255
diagnostics extension, Azure VMs, 7–8
dirty reads, 279
disaster recovery, Cosmos DB, 281
disks
Azure Storage, 31, 51–52
encryption, ADE (Azure Disk Encryption), 53–56
DMA (Database Migration Assistant), 314, 315
DMS (Database Migration Service), 314–321
Docker toolset
ACR (Azure Container Registry), 262
creating container images, 261–262
documentation, 262
document databases, 270
documentation
Azure CLI, 273
Azure Table storage, 273
Docker toolset, 262
governance, 237
load balancing, 218
logic apps, 257
DTUs (Data Transaction Units), 290

E

edges, creating for graph database, 285–286
editing, ARM templates, 66–68
encryption
  ADE (Azure Disk Encryption), 53
  Azure SQL Database, 302–303
  SSE (server-side encryption), 53
endpoints
  adding to Azure Traffic Manager, 209–210
  Azure Key Vault, accessing, 181
  configuring network access, 36–38
  private, 39
ephemeral OS disks, 51–52
Event Grid, 172
  features, 173–174
  subscriptions, 173
  topics, 172–173
events, monitoring, 13–14
exporting
  resources, 65–66
  templates, 64–66
expressions, ARM templates, 69–70
ExpressRoute, 218–219, 225
  configuring, 225–226, 227–228
  configuring a virtual network gateway, 227
  peering settings, 226

F

failover
  auto-, 311–314
  storage account, 48
files, Azure, configuring, 32–34
fraud alerts, 96–97
function app
  creating, 168–170
  Kudu troubleshooting console, 171–172
  Overview blade, 169–170
  Platform Features blade, 170–171
function apps, creating, 258–259
functions, 257–258
  creating, 259–260

G

General-purpose V2 account, creating, 31
Get-AzStorageBlobContent cmdlet, 43
GitHub, 66
Global VNet peering, 83–84
governance, 228. *See also* Azure Policy
  documentation, 237
  policies
    access, 177–178
    AKS policy add-on, 231–232
    Azure Front Door, 206
    conditional access, 108–111
    stored access, 275–276
    WAF, 206–208
  RBAC (role-based access control), 237
    configure access to resource by assigning roles, 240–241
    configure management access to Azure, 241–242
    creating a custom role, 237–240
    troubleshooting, 243–245
graph databases, 270, 284
  creating edges, 285–286
  creating vertices, 284–285
Gremlin API, 284. *See also* graph databases
  graph database
    creating edges, 285–286
    creating vertices, 284–285
guest accounts, 101–105

H

health probes, 189–190, 198
high availability, 56
  availability sets, 56–59
  availability zones, 59–60
  Azure SQL Database, 309–310, 311
    configuring an auto-failover group, 311–314
    geo-replication strategy, 311
    models, 310
  Azure Storage, 46–47
hot tier, Azure Storage, 32
hybrid identities, 111–112

I

IaaS (Infrastructure as a Service), 7
IaC (Infrastructure as Code), 63–64, 71
Identity Protection, 106–108
Insights, 18
  Application, 20–21
  Network, 22
installing, Azure AD Connect, 112–118

J-K

JIT (just-in-time) access, 4
Key Metrics workbook template, 12
Key Vaults, 180. *See also* Azure Key Vault
key-value databases, 269–270
KQL (Kusto Query Language), 10, 11–12
Kudu troubleshooting console, 171–172

L

latency, monitoring, 15
Linux VMs
  sizing, 49–50
  storage, configuring, 50–53
Live Metrics, 21
load balancing, 187, 191–192
  back-end pools, 197
  documentation, 218
  health probes, 198
  read scale-out, 299
  rules, 198–199
Log Analytics workspace, creating, 18–19
logging, 8
  VM workload, 24–26
logic apps
  building, 164–166, 255–256
  creating an email action, 257
  creating an RSS trigger, 256–257
  documentation, 257
LTR (long-term backup retention) backups, 294–295
  creating, 296
  restoring, 296–297

M

managed identity, 181–183
management groups, 235–236
  adding subscriptions, 236
  changing, 237
  top-level access, 236
managing
  access keys, 35–36
  containers, 266
  guest accounts, 101–105
  hybrid identities, 111–112
  on-premises connectivity, 224
manual backups, 297
  metrics, 8–9, 22
MFA (multi-factor authentication), 131
  bypass options, 97–98
  configuring, 93–95
  configuring verification methods, 100–101
  fraud alerts, 96–97
  trusted IPs, 98–99
migration projects. *See also* Azure Site Recovery; server migration
  creating, 132
  Data Box offline migration, 146–149
  server environment assessment, 133–138
  SQL databases
    assessment, 133, 141–144, 145, 314
    migration, 145–146
    publishing an Azure SQL database, 314–321
  update management, 150–152
  web app assessment and migration, 138–145
modifying, ARM templates, 66–68
MongoDB API, 283
monitoring, 1. *See also* Azure Front Door; Azure Traffic Manager; Connection Monitor
  containers, 12–22
  costs, 15
    budgets, 16
    spending, 16
  networks, 14
    latency, 15
    topology, 14–15
  performance, 4
    capacity, 10–12
    unused resources, 9–10
  security, 2
  service health, 13–14
Movere, 133
My Apps portal, SSPR (self-service password reset), 90–91

N

Network Insights, 22
networks
  latency, 15
  monitoring, 14
  topology, monitoring, 14–15
New-AzWebApp cmdlet, 252

NoSQL databases, 269
and Azure Table storage, 270–271
Cosmos DB Table API, 276
data models, 269–270
storage account tables, configuring, 270
NPM (Network Performance Monitor), 15
NSGs (Network Security Groups), 211, 214, 224, 225
adding to a VM, 211–212
associating with resources, 214
placement, 212
rules, 212–214

O-P

OneDrive, connecting to, 166–167
OSI networking model, 195
PaaS (platform as a service), configuring diagnostic settings on resources, 5–6
password writeback, 119–122
peering
ExpressRoute, 226
VNet, 83–85
performance
baselining, 8–9
metrics, 8–9
monitoring, 4
capacity, 10–12
unused resources, 9–10
visualizing diagnostics data, 12–13
Performance Analysis workbook template, 12
platform logs, 5
policies
access, creating, 177–178
AKS (Azure Kubernetes Service), 231–232
assigning, 229–230
Azure Front Door, 206
conditional access, 108–111
stored access, 275–276
WAF, 206–208
PowerShell, 43, 265
cmdlets, 33, 35
Get-AzStorageBlobContent, 43
New-AzWebApp, 252
Set-AzDiagnosticSetting, 7
configuring diagnostic settings on resources, 7
configuring URL path-based routing, 193–195
creating a client secret, 187
creating an application registration, 185–186
storage accounts, 39–42
authentication, 42–46
on-premises components of Azure Site Recovery, configuring, 155–159, 160
on-premises SQL database, migrating to Azure SQL database, 314–315
assessment phase, 314, 315
private endpoints, 39
publishing an Azure SQL database
data migration, 315–318
DMA (Database Migration Assistant), 314, 315
DMS (Database Migration Service), 314–321
methods, 314
online migration, 318–319
phases, 314
purchasing models, Azure SQL Database, 290

Q-R

queues, Azure Storage, 31
RBAC (role-based access control), 237
configure access to resource by assigning roles, 240–241
configure management access to Azure, 241–242
creating a custom role, 237–240
troubleshooting, 243–245
read scale-out, 299
recovery plan, configuring, 161–162
relational databases, 288. *See also* Azure SQL Database
replication
Azure Storage, 46–47
database, 287
enabling on Azure Site Recovery, 160–161
reports, Cost Management, 17
resource logs, 5
resources, 1, 153
assigning roles, 240–241
associating with NSG (Network Security Group), 214
Azure Key Vault, creating, 176–177
baselining, 8–9
configuring diagnostic settings, 5
using PaaS, 5–6
using PowerShell, 7
creating in Azure Site Recovery, 153–154
deploying from ARM template, 70–73
exporting, 65–66

serverless, 164
Azure Functions, 168
logic app, 164–166
service health, monitoring, 13–14
unused, 9–10
restoring, LTR (long-term backup retention) backups, 296–297
rotating, access keys, 36
rules
Azure Firewall, 201–203
firewall, 300–302
load balancing, 198–199
NSG (Network Security Group), 212–214
runbooks, creating, 75–79

S

SAS (shared access signature), 39–42, 274–275
scale sets
autoscaling, 62
configuring, 60–61
scaling, Azure SQL Database, 297–300
scheduling, updates, 151–152
SDKs, 265
seamless SSO, 123–125
security. *See also* ASGs (Application Security Groups); authentication; Azure Firewall; Azure Security Center; NSGs (Network Security Groups)
Azure Key Vault, 176
creating resources, 176–177
Azure Sentinel, 4
Azure SQL Database, 299–300
access control, 302
advanced threat protection, 303–304
auditing, 304–305
configuring server-level firewall rules, 300–302
data protection and encryption, 302–303
defense-in-depth strategy, 299
managed identity, 181–183
monitoring, 2
selecting, APIs, 286
Server Assessment tool, 133–138
server migration
assessment tools, 132–133
Server Assessment tool, 133–138
serverless resources, 164
Azure Functions, 168–172
service health, monitoring, 13–14
Set-AzDiagnosticSetting cmdlet, 7
site-to-site VPNs
configuring, 221–222
verifying on-premises connectivity, 222–223
sizing VMs, 49–50
SLA (service-level agreement), 56
spending
budgets, 16
monitoring, 16
reports, 17
SQL API, 282–283
SQL databases. *See also* NoSQL databases
assessment, 141–144, 145
migrating, 133, 145–146
SSE (server-side encryption), 53
SSE (Storage Service Encryption), 30
SSPR (self-service password reset)
implementing, 89–91
password writeback, 119–122
storage
blobs, 34–35
creating resources for container images, 262–264
tables, 274–276
VMs, 50–53
storage accounts, 160
access keys, 35–36
authentication, 42–46
configuring network access, 36–38
failover, 48
keys, 274
private endpoints, 39
SAS (shared access signature), 39–42
types, 31
stored access policies, 275–276
subscriptions, 173
management groups, 235–236
system-assigned managed identity, 181

T

Table API, 283
tables, Azure Storage, 31
template library, 74–75
threat intelligence, configuring on Azure Firewall, 203
topology
networks, 14–15
VNet peering, 84–85
traffic management. *See* Azure Traffic Manager

troubleshooting, RBAC (role-based access control), 243–245
trusted IPs, 98–99
two-step verification, 93, 97
  bypass options, 97–98
  configuring verification methods, 100–101

U

unused resources, monitoring for, 9–10
updates, scheduling, 151–152
URL path-based routing, 192–195
user accounts
  fraud alerts, 96–97
  guest, 101–105
  hybrid identities, 111–112
  Identity Protection, 106–108
  MFA (multi-factor authentication), 93–95
    bypass options, 97–98
  password writeback, 119–122
  risk reports, 106–108
  seamless SSO, 123–125
user-assigned managed identity, 181

V

VDI (virtual desktop infrastructure)
  Data Box offline migration, 146–149
  migrating to Azure, 146
vertices, creating for graph database, 284–285
viewing, alerts, 29
visualizations
  Application Insights, 20
  diagnostics data, 12–13
VMs. *See also* Azure VMs
  adding a Network Security Group, 211–212
  alerts
    creating, 28–29
    viewing, 29
  Azure Dedicated Hosts, 63
  on-boarding, 24
  high availability, 56
    availability sets, 56–59
    availability zones, 59–60
  monitoring performance capacity, 10–11
  preparing for migration, 155–160
  and private endpoints, 39
  replicating data to Azure, 160–162
  scale sets, 60–61
    autoscaling, 62
  sizing, 49–50
  storage, configuring, 50–53
  workload, logging, 24–26
VMSS (virtual machine scale set), 60–61
VNet(s)
  App Service integration, 253–254
  configuring Azure Firewall, 199–200
  peering, 83–85
  -to-VNet connections, 80–83
VPNs, 218
  creating a virtual network gateway, 219–220
  ExpressRoute, 225
    configuring a virtual network gateway, 227
    peering settings, 226
  managing on-premises connectivity with Azure, 224
  NSGs (Network Security Groups), 224, 225
  site-to-site
    configuring, 221–222
    verifying on-premises connectivity, 222–223

W-X-Y-Z

WAF (web application firewall) policies, 206–208
web app assessment and migration, 138–145
web apps, 250
  for containers, 251–252
  creating, 250–251
Windows VMs
  ADE (Azure Disk Encryption), 53–56
  sizing, 49–50
  storage, configuring, 50–53
workbook templates
  Key Metrics, 12
  Performance Analysis, 12
workload management
  assessment tools, 132–133
  Azure Migrate Server Assessment tool, 133
    server environment assessment, 133–138
  Azure Update Management
    configuring, 150–151
    scheduling updates, 152
  migrating VDI infrastructure to Azure, 146–149
  SQL database migration, 145–146
  web app assessment and migration, 138–145