



# Managing Microsoft SharePoint Server 2016



Exam Ref 70-339

Troy Lanphier

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



# **Exam Ref 70-339: Managing Microsoft SharePoint Server 2016**

Troy Lanphier

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

Copyright © 2016 by Troy Lanphier

All rights reserved. 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: 2016934335  
ISBN: 978-1-5093-0294-9

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Support at [mspinput@microsoft.com](mailto: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 website 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” webpage 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:** Cohesion, Inc.

**Technical Reviewer:** Jeremy Taylor; Technical Review services provided by Content Master, a member of CM Group, Ltd.

**Copyeditor:** Teresa Horton

**Indexer:** Lucie Haskins

**Cover:** Twist Creative • Seattle

*To my kids and my wife: Thanks for sharing my evenings with the occasional writing effort. I appreciate your love and support - KBO.*

—TROY LANPHIER

*This page intentionally left blank*

# Contents at a glance

	<i>Introduction</i>	<i>xvii</i>
<b>CHAPTER 1</b>	<b>Design SharePoint Infrastructure</b>	<b>1</b>
<b>CHAPTER 2</b>	<b>Authentication and security</b>	<b>77</b>
<b>CHAPTER 3</b>	<b>Workload optimization</b>	<b>157</b>
<b>CHAPTER 4</b>	<b>Productivity solutions</b>	<b>223</b>
<b>CHAPTER 5</b>	<b>Manage search capabilities</b>	<b>279</b>
<b>CHAPTER 6</b>	<b>Plan and configure cloud services</b>	<b>339</b>
<b>CHAPTER 7</b>	<b>Monitor and optimize a SharePoint environment</b>	<b>363</b>
	<i>Index</i>	<i>415</i>

*This page intentionally left blank*

# Contents

<b>Introduction</b>	<b>xvii</b>
<i>Organization of this book</i>	<i>xviii</i>
<i>Microsoft certifications</i>	<i>xviii</i>
<i>Acknowledgements</i>	<i>xviii</i>
<i>Free ebooks from Microsoft Press</i>	<i>xix</i>
<i>Microsoft Virtual Academy</i>	<i>xix</i>
<i>Errata, updates, &amp; book support</i>	<i>xix</i>
<i>We want to hear from you</i>	<i>xx</i>
<i>Stay in touch</i>	<i>xx</i>

<b>Chapter 1 Design SharePoint Infrastructure</b>	<b>1</b>
Skill: Design information architecture . . . . .	1
Design information architecture	2
Design a logical architecture	27
Design a physical architecture	37
Skill: Plan an installation. . . . .	49
Identifying and configuring installation prerequisites	49
Implement scripted deployment	53
Plan Access Services deployment	56
Implement patch slipstreaming	57
Plan and install language packs	58
Plan and configure service connection points	60
Plan installation tracking and auditing	62
Plan and install Office Online Server	63
Implement managed paths for Office 365 migrations	65
Configure SharePoint hybrid cloud settings	66

---

**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/](http://www.microsoft.com/learning/booksurvey/)

Skill: Plan a hybrid cloud environment . . . . .	66
Plan for deployment of Office Online . . . . .	67
Configure server-to-server authentication . . . . .	67
Configure OAuth . . . . .	68
Configure audiences and hybrid features . . . . .	68
Summary . . . . .	74
Thought experiment . . . . .	75
Thought experiment answer . . . . .	76

## **Chapter 2 Authentication and security 77**

Skill: Plan and configure authentication . . . . .	77
Plan and configure Windows authentication . . . . .	78
Plan and configure anonymous authentication . . . . .	81
Plan connection encryption . . . . .	82
Plan and configure identity federation . . . . .	85
Configure claims providers . . . . .	86
Configure S2S intraserver and OAuth authentication . . . . .	87
Configure connections to the Access Control Service . . . . .	90
Configure authentication for hybrid cloud deployments . . . . .	91
Skill: Plan and configure authorization . . . . .	93
Plan and configure SharePoint users and groups . . . . .	93
Plan and configure People Picker . . . . .	95
Plan and configure sharing . . . . .	97
Plan and configure permission inheritance . . . . .	100
Plan and configure anonymous access . . . . .	101
Plan web application policies . . . . .	104
Skill: Plan and configure platform and farm security . . . . .	107
Plan and configure security isolation . . . . .	108
Plan and configure services lockdown . . . . .	110
Plan and configure antivirus settings . . . . .	111
Plan and configure certificate management . . . . .	113
Plan for Kerberos support for service applications . . . . .	117
Plan and configure Information Rights Management . . . . .	118
Plan and configure delegated farm administration . . . . .	120

Plan and configure delegated service application administration	122
Plan and configure managed accounts	123
Plan and configure blocked file types	125
Plan and configure Web Part security	126
Skill: Create and configure a User Profile service application (UPA) . . . .	128
Configure a UPA application	128
Configure social permissions	129
Plan and configure sync connections of MIM 2016 synchronization	131
Configure profile properties	134
Configure claims integration with UPA	136
Skill: Manage site and site collection security . . . . .	137
Manage site access requests	137
Manage app permissions	139
Manage anonymous access	141
Manage permission inheritance	142
Configure permission levels	144
Configure HTML field security	147
Skill: Provision and configure web applications. . . . .	148
Create managed paths	148
Configure alternate access mappings	152
Configuring SharePoint Designer settings	153
Summary. . . . .	154
Thought experiment. . . . .	155
Thought experiment answer. . . . .	155

### **Chapter 3 Workload optimization 157**

Skill: Create and maintain site collections. . . . .	157
Configure Fast Site Collection Creation	158
Configure host header site collections	159
Configure self-service site creation	162
Maintain site owners	163
Maintain site quotas	164

Configure site policies	167
Configure a team mailbox	168
Plan Sites page pinning	170
Skill: Plan SharePoint high availability and disaster recovery . . . . .	172
Plan for service distribution	172
Plan for service instance configuration	173
Plan for physical server distribution	174
Plan for network redundancy	176
Plan for server load balancing	177
Plan for SQL Server aliases	178
Plan for SQL Server clustering	180
Plan for SQL Server AlwaysOn Availability Groups	181
Plan for SQL Server Log Shipping	182
Plan for storage redundancy	182
Plan for login replication	183
Skill: Plan backup and restore . . . . .	184
Establish a SharePoint backup schedule	185
Establish an SQL Server backup schedule	186
Plan a nonproduction environment content refresh	186
Plan for farm configuration recovery	187
Plan for service application recovery	187
Plan for content recovery	188
Configure a recovery solution by using SQL Database running in Azure and other Azure backup solutions	190
Skill: Plan and configure social workload . . . . .	191
Plan communities	191
Plan My Sites	193
Plan OneDrive redirection	194
Plan social permissions	194
Plan user profiles	195
Plan activity feeds	196
Plan connections	196
Configure Yammer settings	197
Skill: Plan and configure a Web Content Management workload . . . . .	199
Plan and configure channels	199

Plan and configure product catalog and topic pages	200
Plan and configure Design Manager	202
Plan and configure content deployment	203
Plan and configure display templates	204
Plan and configure variations	205
Skill: Plan and configure an Enterprise Content Management workload	205
Plan and configure eDiscovery	206
Plan and configure document routing	208
Plan and configure co-authoring	209
Plan and configure durable links	211
Plan and configure record disposition and retention	211
Plan large document repositories	213
Plan and configure software boundaries	214
Plan and configure data loss prevention	216
In-place holds and document deletion features	218
Summary	219
Thought experiment	220
Thought experiment answer	221

## **Chapter 4 Productivity solutions 223**

Skill: Evaluate content and customizations	223
Perform migration precheck tasks	224
Analyze content database test results	226
Configure web application authentication for upgrade	228
Resolve orphan objects	230
Resolve missing file system components	231
Resolve configuration conflict issues	232
Skill: Plan an upgrade process	233
Plan removal of servers in rotation	233
Configure a parallel upgrade	236
Configure read-only access for content	236
Configure upgrade farms	237
Measure upgrade performance	238

Plan an installation sequence	241
Migrate SharePoint on-premises to SharePoint Online or a hybrid topology	241
Skill: Create and configure app management	243
Configure DNS entries	244
Configure wildcard certificates	245
Create and configure subscriptions	245
Create and configure the App Store	247
Configure marketplace connections	248
Skill: Create and configure productivity services	250
Create and configure Office Online Server and optional SharePoint services	251
Configuring hybrid OneDrive for Business with Profile Redirection and Extensible App Launcher	258
Plan and install SharePoint Insights and SharePoint Server Telemetry features	259
Skill: Create and configure a Business Connectivity Services (BCS) and Secure Store application	260
Import and configure BCS models	260
Configure BCS model security	262
Generate a Secure Store master key	264
Create Secure Store Target Applications	266
Manage Secure Store Target Application permissions	268
Configure BCS for search	269
Configure hybrid BCS	269
Skill: Manage SharePoint solutions and applications	271
Manage sandbox solution quotas	271
Configure sandbox solution management	272
Deploy farm solutions	273
Upgrade farm solutions	274
Deploy Apps	274
Upgrade Apps	276
Summary	276
Thought experiment	277
Thought experiment answer	278

<b>Chapter 5</b>	<b>Manage search capabilities</b>	<b>279</b>
	Skill: Create and configure enterprise search . . . . .	279
	Plan and configure a Search topology	280
	Plan and configure content sources	286
	Plan and configure crawl schedules	287
	Plan and configure crawl rules	290
	Plan and configure crawl performance	291
	Plan and configure security trimming	293
	Choose and configure hybrid search	295
	Skill: Create and configure a managed metadata service (MMS) application . . . . .	298
	Configure proxy settings for managed service applications	299
	Configure content type hub settings	301
	Configure sharing term sets	302
	Plan and configure content type propagation schedules	303
	Configure custom properties	304
	Configure term store permissions	305
	Configure MMS imports	307
	Skill: Manage search . . . . .	307
	Manage result sources	308
	Manage query rules	310
	Manage display templates	312
	Manage Search Engine Optimization settings	314
	Manage result types	316
	Manage a search schema	317
	Manage federated search, including integration with Delve and Office Graph	319
	Skill: Manage taxonomy. . . . .	320
	Manage site collection term set access	320
	Manage term set navigation	321
	Manage topic catalog pages	324
	Configure custom properties	326
	Configure search refinement	327
	Configure list refinement	330

Skill: Plan and configure a search workload . . . . .	330
Plan and configure search result relevancy . . . . .	331
Plan and configure index freshness . . . . .	332
Plan and configure result sources . . . . .	333
Plan and configure the end-user experience . . . . .	334
Plan and configure a search schema . . . . .	335
Analyze search analytics reports . . . . .	336
Summary . . . . .	336
Thought experiment . . . . .	337
Thought experiment answer . . . . .	338

## **Chapter 6 Plan and configure cloud services 339**

Skill: Plan and configure a BI infrastructure . . . . .	339
Plan and configure PerformancePoint . . . . .	340
Plan and configure Reporting Services . . . . .	344
Plan and configure Power Pivot . . . . .	345
Plan and configure Excel Services (Office Online only) . . . . .	350
Plan and configure Power View . . . . .	351
Plan and configure BI security . . . . .	352
Skill: Create and configure work management . . . . .	354
Configure a connection to Exchange . . . . .	355
Activate and configure a connection to Microsoft Project Server 2016 . . . . .	355
Manage trusts . . . . .	356
Plan Exchange configuration for eDiscovery . . . . .	357
Skill: Plan and configure cloud and hybrid federated search . . . . .	358
Plan and configure on-premises and Office 365 search and encrypted metadata when content is transferred to the search index in Office 365 . . . . .	359
Configure user-specific queries and inbound and outbound or bidirectional hybrid topologies . . . . .	360
Summary . . . . .	361
Thought experiment . . . . .	362
Thought experiment answer . . . . .	362

**Chapter 7 Monitor and optimize a SharePoint environment 363**

Skill: Monitor a SharePoint environment . . . . .	363
Define monitoring requirements	364
Configure performance counter capture	368
Configure page performance monitoring	375
Configure usage and health providers	377
Monitor SharePoint hybrid cloud deployments	384
Skill: Tune and optimize a SharePoint environment . . . . .	384
Plan and configure SQL optimization	385
Implement database maintenance rules	390
Plan for capacity software boundaries	391
Estimate storage requirements	392
Plan and configure caching and a caching strategy	393
Tune network performance	398
Plan and configure Zero Downtime Patching	398
Skill: Troubleshoot a SharePoint environment . . . . .	401
Establish baseline performance	401
Perform client-side tracing	402
Perform server-side tracing	404
Analyze usage data	404
Enable a developer dashboard	407
Analyze diagnostic logs	408
Troubleshoot SharePoint hybrid cloud issues	409
Summary . . . . .	411
Thought experiment . . . . .	412
Thought experiment answer . . . . .	412
<i>Index</i>	415

---

**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/](http://www.microsoft.com/learning/booksurvey/)

# Introduction

---

Although this book was written primarily to help you prepare for Exam 70-339: “Managing Microsoft SharePoint Server 2016,” it is also intended to be a reference that you can refer to during your experiences with SharePoint Server 2016. In several cases, the steps to perform the more advanced tasks are shown in this book to help you feel comfortable with related questions on the exam, as well as provide a reference on how to perform the task in a real-life situation.

The 70-339 is an advanced solutions examination, although the level of detail in this book might exceed content required for the exam. This does not mean there won't be specific questions about steps required to perform a task or requirements needed to install a service application; what it does mean is that you should not focus on minutia such as being able to spell out a command correctly or knowing every possible parameter for the command. Instead, focus on the concepts, the overall steps involved with a task, and the required components needed for a solution.

If you focus on these concepts and go through the tasks in this book, you will be well on your way to passing the exam. It should be noted that this 2016 exam requires a broader spectrum of experience, as it combines concepts that were previously covered in two separate tests: 70-331 (Core Solutions of Microsoft SharePoint Server 2013) and 70-332 (Advanced Solutions of Microsoft SharePoint Server 2013) exams. If you didn't previously take these tests, don't worry; just expect that there are a lot of potential topics to be covered.

This book is generally intended for exam candidates who have four or more years working with SharePoint Server and related technologies such as SQL Server and Windows Server. Candidates should have hands-on experience with a multiserver SharePoint farm, specifically focusing on planning, implementing, and maintaining this farm. This experience includes (but is not limited to) the areas of high availability, disaster recovery, capacity planning, and exposure to Office 365 and hybrid implementations.

Despite having multiple years of experience with a multiserver SharePoint farm, it is doubtful that exam candidates will automatically have experience with each and every technology set covered by the exam; thus, they should focus on the areas in which they have the least experience or understanding. Also, any of the newer features recently added to SharePoint Server 2016 will likely receive additional coverage on the exam.

This book will help you prepare for the exam, but nothing can take the place of real-life experience. In an effort to make the exam content an accurate measure of product knowledge, the test might include a series of case studies along with the standard multiple-choice questions. Expect to see questions that present you with a business and technical problem, then require you to place steps in order and answer questions in which you have to choose

the right set of items from a large list of possible answers. In these cases, previous practice with the actual implementation of the functionality covered in this book will help you far more than just trying to memorize facts and answers.

This book covers every exam objective, but it does not necessarily cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, thus making it impossible to cover specific questions and answers. 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 reference links provided in the text to find more information, then take the time to research and study topics in which you lack experience or understanding. A great deal of planning and implementation for SharePoint is available on MSDN, TechNet, and other blogs and forums.

## 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 Learning website: <http://aka.ms/examlist>. Each chapter in this book corresponds to a major topic area in the list, and the techniques 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.

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

## Acknowledgements

Several people are involved in the development of a book such as this; from an author standpoint, I'd like to thank Karen Szall as well as Lisa Flinchbaugh and Kim Spilker who helped to finish this project. Jeremy Taylor of Content Master was my technical reviewer, and provided

top-notch feedback, particularly around the hybridization of SharePoint. Finally, thanks to Mary Stone and Chris Norton for helping close this effort out.

On the home front, I'd like to thank my family and friends for putting up with me being the occasional writing hermit. In particular, I want to thank Marlene Lanphier, who always seems to be available when I need someone to listen to a particular portion of this text.

## 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>*

Check back often to see what is new!

## 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 at *<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/ER399/errata>*

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

If you need additional support, email Microsoft Press Book Support at *[mspinput@microsoft.com](mailto: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>*

We know you're busy, so we've kept it short with just a few questions. Your answers go directly to the editors at Microsoft Press. (No personal information will be requested.) Thanks in advance for your input!

## **Stay in touch**

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

# Productivity solutions

This chapter shifts the focus away from the purely technical aspects of the farm, moving instead toward SharePoint farm users. Each of the solutions covered can comprise a major portion of the user's day-to-day interaction with SharePoint, including upgrade methods, customizations, and functionality provided within the farm itself to improve productivity and business process.

## Skills in this chapter:

- Skill: Evaluate content and customizations
- Skill: Plan an upgrade process
- Skill: Create and configure app management
- Skill: Create and configure productivity services
- Skill: Create and configure a Business Connectivity Services (BCS) and Secure Store application
- Skill: Manage SharePoint solutions and applications

## Skill: Evaluate content and customizations

---

Implementing a successful migration from one version of SharePoint to another requires a great deal of planning and coordination on the part of the SharePoint administration team. This planning effort will concentrate on the roles and responsibilities required to carry out the four upgrade stages:

- Creating the SharePoint 2016 farm
- Copying databases to the new farm
- Upgrading service applications
- Upgrading the content databases and site collections

The coordination effort concentrates on (1) what other systems will be affected by the upgrade (for example, SQL, Storage, Exchange, Skype, and Infrastructure), and (2) what steps are required to communicate with each of these teams. The level of interaction required with these teams is greatly influenced by how much integration SharePoint 2013 previously had with each of these environments (for instance, existing server-to-server (S2S)

protocol trusts, authentication mechanisms, high availability and disaster recovery (HADR), and User Profile service application (UPA) configurations with Active Directory).

This skill pays particular attention to the documentation and verification of the existing farm's suitability for upgrade, concentrating on the health of the databases, authentication mechanisms, and file systems of the servers themselves.

**This section covers how to:**

- Perform migration precheck tasks
- Analyze content database test results
- Configure web application authentication for upgrade
- Resolve orphan objects
- Resolve missing file system components
- Resolve configuration conflict issues

## Perform migration precheck tasks

Before beginning the process of migrating or upgrading the SharePoint 2013 environment, the existing environment must be assessed. This assessment should concentrate on documentation and evaluation efforts.

### Documenting the existing farm

When SharePoint implementations are first carried out, documentation that describes the initial state of the farm is usually included. As time passes and farm requirements change, configuration and functional changes are often not captured in updated documentation.

The documentation created for the upgrade effort should be able to capture the current state and interactions of the existing farm, including:

- Server topology and the resulting configuration of service applications and roles
- The resiliency capability at each layer or service of the farm
- Existing S2S relationships with other server types (SharePoint, Exchange, Skype, Office 365)
- Configuration and capacity metrics for web applications and content databases

**NEED MORE REVIEW?** The upgrade from SharePoint Server 2013 to 2016 uses the same database attach method that was used to upgrade from SharePoint Server 2010 to 2013. Reviewing and documenting the existing SharePoint environment prior to an upgrade requires quite a bit of time, but can be expedited by using a planning worksheet, such as the "Upgrade worksheet for SharePoint 2013," which can be found at <https://www.microsoft.com/download/details.aspx?id=30370>.

## Evaluating the existing farm

With the documentation effort complete, the results can now be evaluated for upgrade suitability. The evaluation effort allows the upgrade team to determine the current health and upgrade potential of the existing farm, including:

- Current patch state of the farm and content databases
- Orphaned items in content databases
- Compatibility level of site collections in content databases
- Alignment with published boundary, threshold, and supported limits

The eventual result of this effort should be a remediation plan that details steps required to get from the existing farm state to that of a prepared farm migration environment.

## Introducing Test-SPContentDatabase

One mechanism for comprehensive evaluation of a content database is to use the Test-SPContentDatabase PowerShell cmdlet. This cmdlet is used to evaluate each content database for use with SharePoint Server 2016 prior to upgrade.

**NEED MORE REVIEW?** Over the next few sections, we will repeatedly refer to the Test-SPContentDatabase cmdlet. For a complete listing of the optional switches available for use, review the TechNet article entitled “Test-SPContentDatabase” at [https://technet.microsoft.com/library/ff607941\(v=office.16\).aspx](https://technet.microsoft.com/library/ff607941(v=office.16).aspx).

Evaluating a content database for upgrade is always done from the destination system (SharePoint 2016, in this case), and requires the following steps:

- **From SQL Server Management Studio**
  - Back up a copy of the SharePoint 2013 content database and restore it to the SQL instance used with SharePoint 2016.
- **From SharePoint 2016 farm**
  - Create a new web application and supporting content database.
  - Match the authentication mode of the SP2013 content database, either classic or claims-mode.
  - Discard the supporting content database (we won't be using it).
  - Run the Test-SPContentDatabase cmdlet, specifying the SP2013 content database to be tested against the web application. Output the test results to a text file.

**IMPORTANT** Although Test-SPContentDatabase makes no changes in a content database, it nonetheless can cause a significant server load. If you already have users on your SharePoint 2016 farm, it is recommended that this test be carried out after hours or during times of minimal load.

As we progress through this chapter, understand that Test-SPContentDatabase cmdlet can indicate (but not correct) issues with the SharePoint 2013 content databases. These corrections are usually carried out on the farm to be migrated (SharePoint 2013) prior to being migrated, although some (such as authentication) can be remedied in the destination environment (SharePoint 2016).

## Analyze content database test results

Upgrades to SharePoint 2016 are directly dependent on the state of the underlying content databases; as a result, each content database must be inspected and tested prior to upgrade.

### Version status

The version of the SharePoint content database should be inspected from within the SharePoint 2013 environment. When a content database is attached to a SharePoint 2016 environment, the environment reviews the attached content database to obtain its version status. If the version status is not up to the minimum upgradable status, the attachment of the content database will be blocked outright.



---

#### **EXAM TIP**

All content databases to be migrated must be first upgraded to a minimum level of 15.0.4481.1005, or Service Pack 1 and the March 2013 PU. If the farm was originally installed by using combination SharePoint 2013 and Service Pack 1 media, then the content databases are already at this updated level.

---

Checking a content database for its version status is a fairly straightforward (but commonly overlooked) process, involving only three steps:

1. Determining the farm patch level.
2. Determining if one or more content databases has not upgraded.
3. Determining what the actual schema of the content database is.

**IMPORTANT** Don't confuse the configuration database version with the version of a content database. It's entirely possible to have a farm that is patched to a higher level (configuration database) with a content database that has not fully upgraded.

From Central Administration on the original SharePoint environment, from System Settings, select Manage Servers In This Farm. The Farm Information items (Figure 4-1) show the configuration database version (the patch level applied to the configuration database, and perhaps the entire SharePoint farm), as well as the configuration database server and name.

**NEED MORE REVIEW?** The Configuration database version is not always a certain indication of the current update level within the farm, but can quickly point you in the right direction. This number should be compared with the individual patches shown in the Check Product And Patch Installation Status menu of Upgrade and Migration, to get a clear

picture of the overall patch level. For more specific information, review the TechNet blog post “SharePoint patching demystified” at [https://blogs.technet.microsoft.com/stefan\\_gossner/2014/08/18/sharepoint-patching-demystified/](https://blogs.technet.microsoft.com/stefan_gossner/2014/08/18/sharepoint-patching-demystified/).



FIGURE 4-1 The Servers In Farm page

Now that the update level for the configuration database has been captured, it can be compared to that of an individual content database. Selecting Review Databases Status from Upgrade and Migration in Central Administration presents the Manage Databases Upgrade Status page. On this page, you will see the content databases (indicated in blue text and hyper-linked) and their current status, as well as the configuration and service application databases.

Note that the screenshot shown in Figure 4-2 shows a status of Database Is In Compatibility Range And Upgrade Is Recommended for the WSS\_Content\_MeasureMe database, indicating that this database is not currently upgraded to the same level as the other content databases and the configuration database.

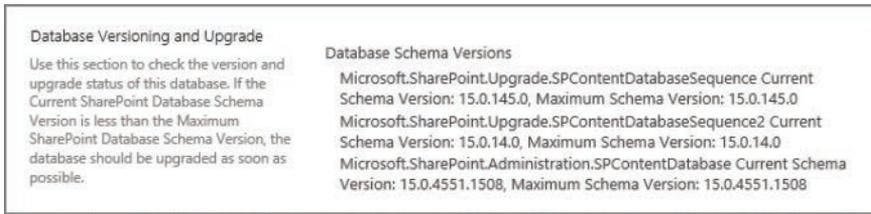
SQL Instance	Database	Type	Status
WingtipDB01	SP2013_SharePoint_AdminContent	Content Database	No action required
WingtipDB01	WSS_Content	Content Database	No action required
WingtipDB01	WSS_Content_MeasureMe	Content Database	Database is in compatibility range and upgrade is recommended
WingtipDB01	MMS_TEMP	MetadataWebServiceDatabase	No action required
WingtipDB01	SP2013_SharePoint_Config	Configuration Database	No action required
WingtipDB01	SP2013_CMS_...management	App Management Database	No action required

FIGURE 4-2 Manage Databases Upgrade Status page

Selecting the content database on the Manage Databases Upgrade Status page allows us to inspect the update levels. When the Manage Content Database Settings page opens (partially shown in Figure 4-3), the last line under Database Schema Version indicates two values:

- **Microsoft.SharePoint.Administration.SPContentDatabase Current Schema Version** This value represents the current SharePoint database schema version for the selected content database.
- **Maximum Schema Version** Also known as the Maximum SharePoint Database Schema Version, this indicates the current update level of the farm or configuration database.

A current schema version that is lower than the maximum schema version indicates that this content database has not successfully upgraded to the current update level of the farm, whereas a match between these two values indicates that the database has been successfully made current.



**FIGURE 4-3** Partial view of the Manage Content Database Settings page, showing values in the Database Versioning And Upgrade section

## SharePoint 2010 site collections

During the process of upgrading to SharePoint 2016, content databases will also be inspected to see if they have any SharePoint 2010 mode site collections (compatibility level 14) requiring upgrade. If these site collections are not upgraded to SharePoint 2013 mode (compatibility level 15), the content database attach will be blocked and not upgraded to SharePoint 2016.

SharePoint 2010 site collections can be identified by using the `Get-SPSite` PowerShell command and inspecting the compatibility level:

- To test all site collections in a farm:

```
Get-SPSite -Limit All | ? { $_.CompatibilityLevel -eq 14 }
```

- To test site collections within a specific content database:

```
Get-SPSite -ContentDatabase <database name> -Limit All | ? {  
    $_.CompatibilityLevel -eq 14 }
```

**IMPORTANT** Shortly, we'll be covering the `Test-SPContentDatabase` command, which also checks for the presence of SharePoint 2010 site collections in a content database. Unfortunately, there's no way to upgrade these site collections from the SharePoint 2016 environment, so it's simply easier to locate and correct these site collections in SharePoint 2013 (prior to beginning the upgrade test process).

## Configure web application authentication for upgrade

In Chapter 1, "Infrastructure," we discussed the different authentication modes, types, and methods. The authentication types (Windows authentication, forms-based authentication, and Secure Application Markup Language [SAML] token-based authentication) and methods (for Windows authentication only: NTLM, Kerberos, Digest, and Basic) are unchanged from SharePoint 2016.

## Authentication mode

The largest change in SharePoint 2016 with regard to authentication has to do with the authentication mode. As was the case with the upgrade from SharePoint 2007 to SharePoint 2010, the upgrade from SharePoint 2010 to SharePoint 2013 didn't *necessarily* require that you alter the authentication method in a web application from classic-mode authentication to claims-mode. Unfortunately, this means that there are still SharePoint farm environments in use that do not use claims-mode authentication, even though this configuration is not recommended going forward.



---

### **EXAM TIP**

Windows classic-mode authentication is no longer supported in SharePoint Server 2016. Prior to upgrade, examine the Health Analyzer in the SharePoint 2013 farm being upgraded; provided the rule hasn't been suspended or removed, there is a daily timer job that indicates web applications that are still using classic-mode authentication.

---

If your environment happens to be among those still using classic-mode authentication and you are planning for the upgrade to SharePoint 2016, you will need to make the conversion from classic-mode to claims-mode authentication to configure the new farm in a supported state.

**IMPORTANT** As you are preparing to run Test-SPContentDatabase, don't forget to match the authentication mode from your SharePoint 2013 environment when creating the SharePoint 2016 environment. If the 2013 web application was set to classic mode, set the 2016 mode to classic when creating the new web application (and vice versa for claims mode).

## Converting a web app from classic-mode to claims-mode authentication

Although the process for converting to claims mode isn't terribly difficult, you have two options to consider. Either:

- Convert SharePoint 2013 classic-mode web applications to claims-based authentication in the SharePoint 2013 farm, then attach copies of these content databases to SharePoint 2016 claims-mode web applications,

or

- Configure SharePoint 2016 classic-mode web applications, attach copies of the SharePoint 2013 classic-mode content databases, and then convert the SharePoint 2016 classic-mode web applications to claims-based authentication.



### **EXAM TIP**

Perform a backup before proceeding with this conversion; after you convert a web app to claims-based authentication, you cannot revert it back to classic-mode authentication.

---

**NEED MORE REVIEW?** Although this conversion is not very difficult, it is somewhat complex. Detailed instructions on how to convert a web app from classic-mode to claims-mode authentication can be found in the TechNet article entitled “Migrate from classic-mode to claims-based authentication in SharePoint 2013” at [https://technet.microsoft.com/library/gg251985\(v=office.16\).aspx](https://technet.microsoft.com/library/gg251985(v=office.16).aspx).

## Resolve orphan objects

Orphaned objects are items in a database that are lacking a hierarchical relationship; for instance:

- Child sites without a reference to a parent site
- Lists or libraries without a site reference
- Apps that are not accessible within a content database

These orphans can be created by any number of causes, including site collections failing to fully provision, incomplete or halted restore operations, features not deploying properly, and so on. Orphans in the content database cannot be reassigned to a reference; thus, they should be deleted from the affected content database.

**IMPORTANT** Ensure that you have a full backup of the content database prior to correcting issues with orphans, in case there are issues with removing orphaned items.

SharePoint 2013 has two built-in Health Analyzer Rule Definitions (in the Availability category) that help identify these issues prior to upgrade, one of which looks for orphaned apps, and one that looks for all other orphan types. Both of these rules are run on a monthly basis, although you can run them ad hoc before copying a content database.

**IMPORTANT** When the orphan rules are run against a content database, the resulting notice gives you the option to simply Repair Automatically. Although this can be a reasonable solution to removing orphans, the fact remains that it places a significant load on the SharePoint content databases and can take quite a bit of time to run (on large content databases).

An alternate solution to allowing the health rule to repair content databases is to use PowerShell cmdlets. This allows you to repair one content database at a time, providing for finer control of this process.

1. Get the content database, assigning it to a variable.  

```
$cdb = Get-SPContentDatabase -Identity <content database name>
```
2. Inspect the content database to see if repairs are needed.  

```
$cdb.Repair($false)
```

At this point, you should receive output from the SharePoint PowerShell console (Figure 4-4). If the OrphanedObjects count is zero, then the database is ready for

upgrade. If there are orphaned objects in the content database, a full backup of that database should be completed before proceeding.



```
Administrator: SharePoint 2013 Management Shell
PS C:\Users\svc_spfarm> $cdb = Get-SPContentDatabase -Identity WSS_Content
PS C:\Users\svc_spfarm> $cdb.repair($false)
<OrphanedObjects Count="0" />
PS C:\Users\svc_spfarm>
```

FIGURE 4-4 Verifying that there are no orphaned objects in a content database

3. (Optional) If the content database has orphaned objects, then these must be removed.  
`$cdb.repair($true)`

Regardless of why these orphans exist, the fact remains that their existence in content databases can prevent the upgrade of a content database from SharePoint 2013 to SharePoint 2016.

## Resolve missing file system components

Missing file system components won't necessarily prevent an upgrade to SharePoint 2016, but they will gladly replicate existing errors and issues found in your SharePoint 2013 farm. Although missing file system components appear on occasion within the Unified Logging Service (ULS) logs of the SharePoint 2013 farm, they are not usually viewed in a group until `Test-SPContentDatabase` is run from the SharePoint 2016 farm.

Essentially, missing file system components are those needed by solutions, branding, Add-ins (apps), and other components that are referenced in the content database. These file system components are expected on the local drives of the individual SharePoint farm servers, and are obviously missing.

### Correcting missing files

A first best effort at correcting these issues is ensuring that solutions, assemblies, and third-party products have been installed in the newly configured SharePoint 2016 farm. Remember that it's not only possible but sometimes necessary to run the `Test-SPContentDatabase` cmdlet several times, each time capturing the output of what files a content database is expecting but not receiving.

**NEED MORE REVIEW?** It's quite possible that Add-in functionality was added to the SharePoint 2013 environment and could have been installed or removed improperly, leaving artifacts behind in the content database. Add-in removal is detailed in the TechNet article entitled "Remove app for SharePoint instances from a SharePoint 2013 site" at <https://technet.microsoft.com/library/fp161233.aspx>.

## Removing solutions and features

Solutions and features that are not necessary (or available) in the new SharePoint 2016 environment should be removed prior to copying the SharePoint 2013 content database. This action can have severe consequences in the SharePoint 2013 environment, so a backup of the farm is recommended (including the web applications) prior to the removal of any solution.

**NEED MORE REVIEW?** The removal of solution functionality is not something that SharePoint administrators do every day. As a result, review is often needed for this activity before proceeding. Essentially, a solution must first be uninstalled and then removed, all from within PowerShell. The Uninstall-SPSolution and Remove-SPSolution cmdlets are reviewed within the TechNet article “Features and solutions cmdlets in SharePoint 2016” at [https://technet.microsoft.com/library/ee906565\(v=office.16\).aspx](https://technet.microsoft.com/library/ee906565(v=office.16).aspx).

## Resolve configuration conflict issues

The discussion of configuration conflicts takes us all the way back to the beginning of this section. Documentation that describes the existing SharePoint 2013 environment and its configurations suddenly becomes the focus of our efforts.

This documentation forms the framework that describes the SharePoint farm integration topics such as these:

- **Server-to-Server (S2S) connectivity** Interactions between the SharePoint 2013 farm and other farms might have resulted in a significant arrangement of trusts between farms on premises (and potentially in the cloud). Each of these S2S relationships will need to be re-created between the new SharePoint 2016 farm and its counterparts.
- **Authentication mechanisms** Changes in the authentication architecture for the SharePoint 2016 farm might negate the need for certain authentication types. For instance, are external users going to continue to log in via Forms or are they being moved to an Active Directory Federation Services (AD FS)-connected authentication mechanism?
- **On-premises secure configurations** If your current SharePoint 2013 farm is part of a larger Business Intelligence (BI) infrastructure, it's likely that Kerberos has been implemented. If this is the case, Service Principal Names (SPNs) must be created in the new environment that allow the existing BI infrastructure to be implemented.
- **Moving away from Excel Calculation Services** Many organizations make regular use of Excel Calculation Services within their SharePoint 2013 configuration. Excel Calculation Services functionality has been moved away from being a service application and into the Office Online Server configuration (which is an on-premises server product outside SharePoint, superseding existing Office Web Application functionality).
- **Business Connectivity Services** Any existing Business Connectivity Services (BCS) connections must be re-established within the new environment, including the

creation of the appropriate external content types. This configuration might be affected by plans for utilizing BCS services available in Office 365.

- **User profile services and application changes** In SharePoint 2013, user profile information can be pushed from the SharePoint farm to Active Directory by way of the Forefront Identity Manager (FIM) component found within SharePoint 2013. In SharePoint 2016, this component is replaced by Microsoft Identity Manager 2016 (MIM). It might be desired to move the configuration of the FIM server into MIM to maintain functionality previously available in the SharePoint 2013 farm.
- **Load balancer configuration** External hardware load balancers are commonly in use with SharePoint 2013 farms. The configuration for the SharePoint 2016 farm will involve re-creating the SharePoint 2013 load balancer configuration, but could change based on the architecture chosen; for instance, changes in topology from traditional to streamlined (MinRole) might affect the configuration.

## Skill: Plan an upgrade process

---

Now that we've covered some of the planning and evaluation required for a SharePoint 2016 farm upgrade, we can begin to discuss how the actual implementation might proceed. Consideration at this point should be given to resourcing and which team members might be involved in the creation and migration efforts going forward.

### This section covers how to:

- Plan removal of servers in rotation
- Configure a parallel upgrade
- Configure read-only access for content
- Configure upgrade farms
- Measure upgrade performance
- Plan an installation sequence
- Migrate SharePoint on-premises to SharePoint Online or a hybrid topology

## Plan removal of servers in rotation

As more and more users are moved between SharePoint environments (from 2013 to 2016), the user load on the SharePoint 2013 environment will decrease and increase on the SharePoint 2016 environment. Combining this fact with the potential change in topology and need for resiliency, it becomes likely that some SharePoint 2013 servers might be repurposed as members in the SharePoint 2016 farm, if for no other reason than economy.

Prior to removing a server from any SharePoint 2013 farm, it's a good idea to see what role(s) and services the individual server is hosting. Part of the documentation you are doing for the actual migration comes in handy here, allowing you to ask questions like these:

- What role(s) did the server host (Front end, batch, and so on)?
- Can the availability requirements for certain tiers in the farm be reduced while the migration is taking place?
- Is there more than one server in this tier? If so, how many? Are they configured identically from a services perspective?
- Are there any specialized services or service applications in this tier that require PowerShell configuration before servers can be removed?

As users are migrated, a careful review of performance at each tier (along with answers to the preceding questions) will determine which servers (if any) can be removed from the SharePoint 2013 farm and repurposed.

## Specialized services and service applications

At first blush, removing a server from the SharePoint farm might seem straightforward because all you'd have to do is run the configuration wizard and unjoin it from the farm. This most often is not the case, however, as removing the role of the server in the farm might require extra steps to reconfigure:

- **Search servers** To remove a server from the search topology, you must first clone that topology, remove the server from the cloned topology, and then make it the active topology. Search servers often exist in both the web and application tiers of a traditional topology.

**NEED MORE REVIEW?** Altering the search topology in SharePoint 2016 isn't a difficult task, but if done incorrectly, it can cause the loss of the current search index or a failure in SharePoint Search. Prior to making any topology changes, review the TechNet article "Manage the search topology in SharePoint Server 2013" at <https://technet.microsoft.com/library/jj219705.aspx>.

- **User Profile servers** Two services are associated with the User Profile service application: User Profile Service and User Profile Synchronization Service. The latter "Sync" service is only installed on one server in the farm, and thus cannot be removed (unless you move this function to a different server in the farm).

**NEED MORE REVIEW?** As a SharePoint farm administrator, you might not often have the requirement to interact with or alter the User Profile Services or User Profile service application. Reviewing the TechNet article "Overview of the User Profile service application in SharePoint Server 2013" at <https://technet.microsoft.com/library/ee662538.aspx> will reacquaint you with the concepts required to alter these servers.

- **Servers in the distributed cache cluster** A single server can provide distributed cache services in a SharePoint farm. A cluster of these servers (3–16 per farm, a two-server installation is not allowed) can also exist. If you have multiple servers in the farm and wish to remove them from the cluster, you can do so via PowerShell. You cannot simply shut down this service from Services on Server, as this does not remove the server from the cluster and will render your farm in an unsupported state.

**NEED MORE REVIEW?** Removing a server from the distributed cache cluster is done via PowerShell, and can result in a nonfunctioning or unrecoverable configuration if performed improperly. Two major steps are required: Perform a graceful shutdown of the distributed cache service and then remove a server from the cache cluster. Carefully review and understand the TechNet article “Manage the Distributed Cache service in SharePoint Server 2013” at <https://technet.microsoft.com/library/jj219613.aspx> before proceeding with any change.

- **Workflow Manager servers** Workflow Manager servers may exist either inside or outside of the SharePoint farm itself. These servers would not be a good option for removal until the farm is being shut down. If you must remove a Workflow Manager server, ensure that the server is made to leave a farm before proceeding.

**NEED MORE REVIEW?** Workflow Manager is maintained outside the realm of the SharePoint Server farm, although it might exist on a SharePoint server (depending on your existing configuration). Information on how to remove a Workflow Manager server from a farm can be found in the MSDN article “Leaving a Farm” at [https://msdn.microsoft.com/library/jj193527\(v=azure.10\).aspx](https://msdn.microsoft.com/library/jj193527(v=azure.10).aspx).

- **Office Web App servers** If you have multiple Office Web Apps servers in your existing SharePoint 2013 farm, these are optimal servers for refit into Office Online servers for use in your 2016 farm. As these servers are likely behind a load balancer, each could be removed from the load balancer configuration before being removed from the Office Web Apps server farm and then shut down, as only one server is required in the Office Web Apps farm for it to be used with SharePoint (watch your performance characteristics as you remove each server).



---

**EXAM TIP**

Two PowerShell cmdlets exist for use in removing Office Web Apps functionality, `Remove-OfficeWebAppsHost` and `Remove-OfficeWebAppsMachine`. Only the latter removes the current server from an Office Web Apps server farm.

---

## Configure a parallel upgrade

Close coordination with your SQL administration team can provide opportunities for improving the SharePoint upgrade process. Working with the storage, storage area network (SAN), and network attached storage (NAS) teams, the SQL admins might be able to provide configurations that provide more processing, I/O, and storage resources. For example, they might be able to temporarily move the storage of your new farm over to a faster set of disks (say, from standard hard drives to solid-state drives [SSD]) to improve upgrade speed.

Upgrading the SharePoint farm, then, is directly dependent on the performance levels of the underlying SQL configuration. It could be that you have a constrained window of time in which to perform your upgrades, so it stands to reason that you take advantage of every possible optimization strategy.

It is likely that, while your SharePoint and SQL environments are upgrading a single content database, they are not fully utilizing the processing, memory, or I/O performance available in the farm. Fortunately, it is entirely possible (and fully supported) to attach and upgrade more than one content database at a time, a concept known as *parallel upgrades*.

There is no particular configuration requirement for performing parallel upgrades; however, there are a handful of recommendations.

- **PowerShell sessions** Use a separate PowerShell session to run each content database upgrade, giving you the opportunity to monitor each separately (and monitor the performance levels of the SQL and SharePoint servers performing the upgrade).
- **Start times** Separate the start time for each new database upgrade session by several minutes, especially when connecting multiple content databases to a single web application. This is necessary to avoid temporary locking, which will cause an error in the upgrade session.

**NEED MORE REVIEW?** Parallel upgrades are only a small portion of an overall content database migration strategy. More detailed information can be found in the TechNet article entitled “Upgrade content databases to SharePoint 2013,” which can be found at <https://technet.microsoft.com/library/cc263299.aspx>.



### EXAM TIP

Using SharePoint Central Administration to attach a content database is not supported for upgrading. Be familiar with the `Mount-SPContentDatabase` cmdlet and the available options used for upgrading content databases.

## Configure read-only access for content

It could be that your organization has a requirement for allowing users read access to content in your SharePoint 2013 system while you are upgrading to SharePoint 2016. This is actually not a limiting factor, but additional effort will be required to coordinate upgrade schedules

with the site collection administrators and business stakeholders associated with a particular content database.

If this configuration is required for your organization, then it's entirely possible to set an originating (SharePoint 2013) content database to read-only mode, copy it to the SharePoint 2016 environment, and then mount and upgrade the content database.

**IMPORTANT** At this point, we are not talking about setting a content database to read-only status from within SharePoint Central Administration. The content database will be set to read-only from within SQL Server Management Studio (SSMS) prior to copy.

Prior to the read-only and copy activities, verify the following:

- The account used to copy the databases has access to SSMS on both the SharePoint 2013 and SharePoint 2016 environments (data tier), and has access to a network location accessible by both environments.
- The account used to set the databases to read-only or read-write is a member of the db\_owner fixed database role on the content databases that you are upgrading.
- The content databases to be upgraded have been checked for database consistency errors (and repaired, if required).
- The appropriate service pack or cumulative update (CU) has been applied (and the update verified in the content databases) to the SharePoint 2013 environment.

**NEED MORE REVIEW?** Although the process of setting a content database to read-only, backing up the database, and restoring the database is specifically an SQL skill, a SharePoint administrator might be called on to either specify the particular actions or carry them out in SSMS. To gain a better understanding of this process, review the TechNet article entitled "Copy databases to the new farm for upgrade to SharePoint 2016" at [https://technet.microsoft.com/library/jj839720\(v=office.16\).aspx](https://technet.microsoft.com/library/jj839720(v=office.16).aspx).

## Configure upgrade farms

Although there were three versions of SharePoint 2013 (Foundation, Standard, and Enterprise), SharePoint 2016 only comes in two distinct versions: SharePoint Server 2016 Standard and SharePoint Server 2016 Enterprise. The upgrade path chosen for SharePoint 2016 will depend on the current version of SharePoint in use within your organization.

- **SharePoint 2010 and previous** SharePoint only allows an upgrade from the immediately preceding version. If your organization is upgrading from an older version of SharePoint to SharePoint 2016, you have two options: perform a step upgrade through previous versions (for example, upgrade to SharePoint 2013 and then upgrade again to SharePoint 2016), or use a third-party tool to extract information from your existing SharePoint environment and restore this information to your new environment.

- **SharePoint Foundation 2013** There is no similar product in the SharePoint 2016 product line, so you will use a content database attach upgrade to either a SharePoint 2016 Standard or Enterprise farm.
- **SharePoint 2013 Standard** Use a content database attach upgrade to SharePoint 2016 Standard and then optionally upgrade the license to SharePoint 2016 Enterprise farm.
- **SharePoint 2013 Enterprise** Use a content database attach upgrade to a SharePoint 2016 Enterprise farm. Although technically possible, it's not recommended to migrate from **SharePoint** 2013 Enterprise to **SharePoint** 2016 Standard, due to expected solution and feature functionality used in the content databases.

**NEED MORE REVIEW?** SharePoint is not the only component in your farm. When you are considering upgrade paths, don't forget to plan for other components such as Office Web Apps, Workflow Manager, and Project Server. In particular, a Project Server upgrade (Project Server is an additional functionality that can be activated in a SharePoint 2016 farm) requires a specific upgrade path, which is described in the TechNet article "Upgrade to Project Server 2016" at [https://technet.microsoft.com/library/gg502590\(v=office.16\).aspx](https://technet.microsoft.com/library/gg502590(v=office.16).aspx).

## Measure upgrade performance

If you've installed SharePoint in an enterprise on-premises setting, it's likely that you've built more than one SharePoint instance (development, staging, production). These environments are used to vet new development efforts, evaluate third-party solutions, and to test configuration and performance changes intended for production.

When it's time to evaluate an upgrade scenario, you might decide to repurpose the staging environment as a test environment for the new SharePoint farm. This environment usually has the same specifications as its production counterpart, and should be identical from a per-server processor, RAM, and I/O standpoint. If this option is chosen, you might want to add servers to this environment to more accurately reflect the MinRole configuration that will be used in the SharePoint 2016 production environment.

Whether you choose to repurpose or reconfigure the existing staging environment or build a new test environment for your SharePoint 2016 upgrade plans, the fact remains that the resulting environment should perform identically to the eventual SharePoint 2016 production farm.

**IMPORTANT** The test environment does not require the same resiliency levels as its production counterpart (no high availability, disaster recovery or load balancing), but affords you the opportunity to practice evaluating performance levels and estimating upgrade times.

## Storage evaluation

In addition to being memory- and resource-intensive, a SharePoint upgrade can require a significant amount of space. This space is manifested in two separate components:

- **Content database growth** A content database usually grows in size while the upgrade is taking place, causing growth of the database itself.
- **Transaction log growth** The matching transaction log can grow significantly during the upgrade process, as backups will likely not yet be configured.

**IMPORTANT** During the process of copying and restoring a content database, consider “pregrowing” the content database file in SSMS to reduce the amount of time SQL spends trying to add space for the upgrade process. Additionally, consider altering the growth rate for the transaction logs well beyond the default of 10 percent, so as to avoid a time-out during the content database upgrade.

## Performance evaluation

Upgrade performance should be evaluated for the entire test farm; however, some metrics will be captured explicitly from the SQL server (data tier), as it commits most of the effort from a resourcing standpoint to the upgrade effort. Environmental and database factors will both heavily influence the captured performance metrics.

Environmental factors that affect the performance of database and site collection upgrades have to do with the physical configuration of servers in the farm, and include the following:

- **Simultaneous (parallel) upgrades** As we discussed previously, every content database being upgraded requires resources from the SQL server attached to the farm.
- **SQL Server disk IOPS** The number of input/output operations per second (IOPS) provided by the storage layer to the SQL server has a direct correlation to the upgrade speed of the farm as a whole.
- **SQL Server database to disk layout** Multiple content databases may occupy the same physical set of disks; optimally, these disks will be spread across multiple I/O channels and sets of disks, thus minimizing the amount of load on any particular set of disks.
- **SQL Server temporary database optimizations** The TempDB database on the SQL database server itself should be optimized, with the correct number and size of TempDB files.
- **SQL Server CPU and memory characteristics** Sometimes the SQL data layer servers are on their own server, but sometimes the SQL layer is but a single instance of SQL on a larger SQL database server. The amount of processing power and memory available to the instance has a direct bearing on how transactions are carried out (and databases are upgraded).

- **Web server CPU and memory characteristics** The rest of the servers in a SharePoint installation have an influence (albeit a great deal smaller) on upgrade performance. As is the case within SQL, the processor and memory characteristics should be configured so as to not bottleneck performance (and slow or halt the upgrade process).
- **Network bandwidth and latency** While the upgrade is occurring, there will be a considerable amount of communication between the different tiers of the SharePoint server farm. If possible, consider having the intrafarm communications exist on a different virtual local area network (VLAN).

Database factors that affect the performance of database upgrades have to do with information contained within the content database itself, and include the following:

- **Site collections** Each site collection is itself upgraded as part of the content database upgrade process; if the upgrade of a single database will take too long, consider building another content database in the SharePoint 2013 environment prior to upgrade and move a portion of the site collections to the new database.
- **Subwebs** As site collections are subject to upgrade, the number of webs contained within the site collection has a direct effect on the upgrade speed for the site collection.
- **Lists** Lists within SharePoint can contain hundreds, thousands, or more individual items that are part of the upgrade process. Consider working with the site collection administrator to clean large lists if possible.
- **Rowspan within lists** Lists with a significant number of columns (known as *wide lists*) cause a phenomenon known as *rowspan* within the underlying SQL content database.
- **Document versions (number and size)** Although this is not as significant an issue as when upgrading from SharePoint 2010, upgrades from SharePoint 2013 to SharePoint 2016 nevertheless have to address each major and minor version of a document to be upgraded. Versions retained can be configured via the GUI or via the object model.
- **Documents** Documents within a SharePoint library can be fairly significant in size and number. Work with your site collection administrator and users to see about removing any outdated or discarded documents. Don't forget to empty the Recycle Bin for the library itself.
- **Links** Links function identically to lists, and are subject to the same corrective actions.

**NEED MORE REVIEW?** Several pieces of guidance exist on TechNet, specifically addressing upgrade performance and how to clean up an existing environment. For performance planning, review the TechNet article "Plan for performance during upgrade to SharePoint 2013" at <https://technet.microsoft.com/library/cc262891.aspx>. For tips on SharePoint environmental cleanup, review the TechNet article "Clean up an environment before

an upgrade to SharePoint 2013” at <https://technet.microsoft.com/library/ff382641.aspx>. Testing and troubleshooting information specific to SharePoint 2016 can be found in the TechNet article “Test and troubleshoot an upgrade to SharePoint Server 2016” at [https://technet.microsoft.com/library/ff382642\(v=office.16\).aspx](https://technet.microsoft.com/library/ff382642(v=office.16).aspx).

## Plan an installation sequence

The installation process for a new SharePoint farm is largely unchanged from previous versions. Essentially, the order of installation starts with the data tier and works its way up (even in a MinRole farm):

- 1. SQL servers** This environment is technically configured separately from the rest of a SharePoint environment, but sets the tone for the performance and operation of the entire farm. Items addressed at this level are high availability data recovery efforts and Business Intelligence Services.
- 2. Application servers** Once the SQL server is ready to present a database instance to SharePoint, the next step is to set up application servers. The first server set up in a SharePoint 2016 farm is the de facto Central Administration server (easily changed later if required).
- 3. Distributed cache servers** A SharePoint farm is not valid without at least one distributed cache server present. Remember that if you required resiliency at this tier that a farm with two distributed cache service boxes is not supported, so you must have a minimum of three (or up to 16 total).
- 4. Search servers** Although this MinRole is optional, this grouping of servers should be put in place prior to the Front-end servers if Search is to be required in the farm. The search topology can be configured after the Front-end servers have been configured.
- 5. Front-end servers** The Front-end servers require the least amount of interaction for setup, and would be the last servers required to complete the SharePoint farm.

## Migrate SharePoint on-premises to SharePoint Online or a hybrid topology

So far, we’ve been discussing the effort required to upgrade from SharePoint 2013 to SharePoint 2016 on premises. It might be that part of your upgrade strategy is to move portions of the environment to SharePoint Online and leave portions on premises, or you could decide that the entire environment should be moved to the cloud.

This conversation becomes important when talking about migrating an on-premises environment wholly to the cloud, because there might be custom functionality that is not supported by SharePoint Online or Office 365. If this is the case, the good news is that you can host the “custom” part of the environment in Azure; configuration and upgrade functions are identical for this environment to what they are on premises.

The remaining functionality can be hosted in SharePoint Online, and must be migrated from an on-premises environment by some means. This is the same effort as is required for moving certain hybrid content to the cloud.

**IMPORTANT** We are not really talking about My Sites or OneDrive for Business sites here. These are the standard, ordinary collaboration and publishing sites that we have consistently hosted in the on-premises SharePoint environment.

## Content migration mechanisms

Although we could task users with moving content manually (by using Sync for their libraries, and so on), this might not be efficient in the long run, either from an efficiency or accuracy standpoint. Instead, we have a series of migration methods to put content in the cloud:

- **Microsoft FastTrack** This is a service intended to help push content to the cloud by engaging a Microsoft Partner.
- **SharePoint Online Migration API** By using the object model, content can be moved from file shares and SharePoint Server sites to SharePoint Online and OneDrive Migration.
- **Windows PowerShell cmdlets** By using PowerShell cmdlets, content can be moved from file shares and SharePoint Server sites to SharePoint Online and OneDrive Migration.

**NEED MORE REVIEW?** The SharePoint Online Migration API and Windows PowerShell cmdlets are both covered as part of the TechNet article "SharePoint Online and OneDrive Migration Content Roadmap," at <https://technet.microsoft.com/library/mt203955.aspx>.

The SharePoint Online Migration API and PowerShell options are intended for importing files to Office 365 by network upload. Depending on the amount of data, both of these options might be inadequate for an efficient transfer to the cloud.

**IMPORTANT** Guidance from Microsoft suggests that you should consider shipping drives (versus uploading data) if you have more than 10 TB of data that will ultimately live in SharePoint Online. See "Import SharePoint data to Office 365" at <https://support.office.com/article/Import-SharePoint-data-to-Office-365-ed4a43b7-c4e3-45c8-94c8-998153407b8a> for more details.

If this is the case, there is another mechanism available: importing files to Office 365 by shipping drives. There are few requirements for this mechanism, specifically the types of drives and adapters and the requirement for BitLocker encryption.

This mechanism requires a connection to SharePoint Online to gather information and prepare the migration.

1. Download and install the drive preparation tool.
2. Download the SharePoint Online Management Shell.

3. Connect to the SharePoint Online tenant.
4. Get the storage account key.
5. Create a SharePoint Online Migration package manifest and data.
6. Prepare the drives.
7. Prepare a mapping file.
8. Upload the drive files and mapping file.
9. Ship the drives.
10. Enter shipping information in the Office 365 admin center.

Once this effort is complete and Microsoft has received the drive, information can be transferred to your Office 365 tenancy.

**NEED MORE REVIEW?** This is not a terribly difficult process, but it requires that the steps be carefully followed. More information about this process (including the required steps and the associated PowerShell cmdlets) can be found in the *support.office.com* article entitled "Import SharePoint data to Office 365," found at <https://support.office.com/article/Import-SharePoint-data-to-Office-365-ed4a43b7-c4e3-45c8-94c8-998153407b8a>. Note that this document shows steps for both network and drive upload mechanisms.



#### EXAM TIP

Although Office 365 is not necessarily part of the SharePoint test, it is important nonetheless to be familiar with the PowerShell cmdlets that allow these migrations to take place.

## Skill: Create and configure app management

In earlier versions of SharePoint, custom code and functionality were created and deployed via full trust solutions in the SharePoint farm. Although this was (and is) a valid way to add new functionality, this mechanism is being superseded by SharePoint apps and add-ins.

One reason for this change is simply that the apps can be created and deployed to both on-premises and cloud solutions. This reusability means that customizations can be developed once and deployed somewhat uniformly to both environments.

**IMPORTANT** The nomenclature for SharePoint (and Office) apps is currently changing; instead of Apps for SharePoint, they are now referred to as SharePoint Add-ins. App Parts and App Webs are also changing nomenclature, named Add-in part and Add-in web, respectively.

Regardless of how they are named, the functionality is the same; as the user interface still refers to these as Apps (Apps for Office, Apps for SharePoint, and so on), we will use the term *App* when called for in the interface but use the more current designation of Add-in when talking about the individual functionality.

### This section covers how to:

- Configure DNS entries
- Configure wildcard certificates
- Create and configure subscriptions
- Create and configure the App Store
- Configure marketplace connections

## Configure DNS entries

To configure Add-ins with SharePoint 2016, you will need to accomplish two tasks in Domain Name Services (DNS): creating a DNS zone for your Add-in domain, and creating a wildcard alias for the new domain name.

### Creating a DNS zone for the Add-in domain

By using the DNS console, you will need to create a new DNS zone (such as *http://www.wingtiptoyssaddins.com*). The new DNS zone should be created as a forward lookup zone, and should not be a subdomain of the existing domain that hosts the SharePoint sites (such as *http://www.addins.wingtiptoyss.com*), as this poses a potential security risk (such as cross-site scripting).

This zone is created by using the DNS console on a domain controller, and requires the user creating the zone to be a domain administrator.

### Creating a wildcard alias for the domain name

Once the DNS entry for the Add-in domain has been created, the next task is to create a wildcard alias record that points to the SharePoint domain. This record can be created as an Address (A) record, but is more often created as a Canonical Name (CNAME) record.

Using the previous example, you would create a record for *\*.wingtiptoyssaddins.com* and point to this by using a CNAME to the SharePoint domain (for example, *sharepoint.wingtiptoyss.com*).



#### **EXAM TIP**

Although DNS configuration is not necessarily a core skill for effective SharePoint administration, it is nonetheless a good idea to understand how to create the appropriate DNS entries required for your add-in domain.

If at all possible, practice the steps required to both create the forward lookup zone and the CNAME entry by using the DNS console. If this is unavailable, it is strongly suggested that you be familiar with how to start the DNS console and make these entries.

**NEED MORE REVIEW?** The steps for creating the forward lookup zone for the app domain as well as those required to create the wildcard entry are shown in the TechNet article entitled “Configure an environment for apps for SharePoint (SharePoint 2013)” at <https://technet.microsoft.com/library/fp161236.aspx>.

## Configure wildcard certificates

It’s technically possible to avoid using Secure Sockets Layer (SSL) with the Add-in functionality in SharePoint, but this is not a recommended configuration, particularly if either of the following is true:

- Existing SharePoint sites are using SSL.
- Any of the Add-ins to be used connect to data located external to SharePoint sites.

### Requesting a wildcard certificate

A new wildcard certificate can be requested from the Internet Information Server (IIS) console and then imported to the SharePoint web application where the App Catalog will be located. When the certificate is imported, it’s important that the Friendly Name entry includes the asterisk character (\*), indicating the wildcard (for example, \*.wingtiptoy.com).



---

#### **EXAM TIP**

Be familiar with the process of requesting a new certificate from the IIS console. In particular, remember that this certificate must be installed in IIS for each Front-end server of the farm.

---

**NEED MORE REVIEW?** The processes for both requesting and installing a new wildcard certificate are shown in the TechNet article entitled “Configuring Internet Server Certificates (IIS 7)” at [https://technet.microsoft.com/library/cc731977\(v=ws.10\).aspx](https://technet.microsoft.com/library/cc731977(v=ws.10).aspx).

## Create and configure subscriptions

Prior to the creation of the Add-in Catalog, two service applications must be configured in the SharePoint Server 2016 farm:

- **App Management** This service application is responsible for storing and providing SharePoint Add-in licenses and permissions, including those downloaded from the SharePoint and Office Store.
- **Subscription Settings** This service application enables the sharing of stored setting data within a set of site collections.

**IMPORTANT** Although it's technically possible to create a new App Management service application from Services Applications in Central Administration, Application Management, you might wish to simply go ahead and create this service application from PowerShell. The reason for this is simple: There is no provision for creating the other required service application, the SubscriptionSettingsServiceApplication.

Creating these two new service applications is a bit different in a MinRole-compliant SharePoint 2016 environment than it was in SharePoint 2013. Particularly, the supporting services for each service application (App Management Service and Microsoft SharePoint Foundation Subscription Settings Service) are automatically provisioned and started in servers holding the Front-end and Application roles within the SharePoint 2016 farm (Figure 4-5). No manual start and stop is required.

Service	Auto Provision	Action	Compliant
Access Services	No	Manage Service Application	Yes
Access Services 2010	No	Manage Service Application	Yes
App Management Service	Yes	Manage Service Application	Yes
Business Data Connectivity Service	No	Manage Service Application	Yes
Claims to Windows Token Service	Yes	Disable Auto Provision	Yes
Distributed Cache	Yes	Disable Auto Provision	Yes
Document Conversions Launcher Service	No	Enable Auto Provision	Yes
Document Conversions Load Balancer Service	No	Enable Auto Provision	Yes
Machine Translation Service	No	Manage Service Application	Yes
Managed Metadata Web Service	Yes	Manage Service Application	Yes
Microsoft SharePoint Foundation Sandboxed Code Service	No	Enable Auto Provision	Yes
Microsoft SharePoint Foundation Subscription Settings Service	Yes	Manage Service Application	Yes

**FIGURE 4-5** Newly started services in the SharePoint 2016 farm

**NEED MORE REVIEW?** The creation of these two service applications is identical to what it was in SharePoint 2013 (except the activating of the supporting services), and is shown in the article “Configure an environment for apps for SharePoint (SharePoint 2013)” on TechNet at <https://technet.microsoft.com/library/fp161236.aspx>.

## Configuring the Add-in URLs for use

The last step in the subscription process is to create the App domain prefix and the tenant name to use for Apps in this SharePoint environment. Within the Apps section of Central Administration, select Configure App URLs (under App Management, shown in Figure 4-6).

**FIGURE 4-6** Configuring the App URLs

**NEED MORE REVIEW?** Configuration of the Add-in URLs is detailed in the TechNet article “Configure an environment for apps for SharePoint (SharePoint 2013)” at <https://technet.microsoft.com/library/fp161236.aspx>.

## Create and configure the App Store

Apps for SharePoint (now called SharePoint Add-ins) are self-contained extensions of SharePoint websites (on premises or online) that are created without the need for custom code on the SharePoint server farm. Two types of these Add-ins exist:

- **SharePoint-hosted** Used for creating functionality scoped to a single-site collection, created entirely in JavaScript.
- **Provider-hosted** Used for more complex business requirements, this functionality can be used to reach across multiple sites and line-of-business apps, and does not necessarily have to be created in JavaScript.

These Add-ins can be developed in house or can be purchased from the Office Store, within the SharePoint Add-Ins section.

**IMPORTANT** The nomenclature can get a bit confusing here; since its inception, the ability to incorporate Add-ins and Apps to SharePoint has been provided both on premises in the App Catalog and Add-in Catalog. The online location for sourcing these Add-ins is currently referred to in Central Administration as simply SharePoint and Office Store; throughout different documentation efforts, you might also hear this location referred to as the SharePoint MarketPlace, App Store, or SharePoint Store.

## SharePoint Add-ins and the App Catalog

Before SharePoint Add-ins can be installed to a SharePoint farm, an App Catalog must be configured for use. This catalog hosts both locally created Add-ins as well as those hosted within SharePoint and Office Store (also known as the App Store).

Apps in the catalog site are stored in one of two document libraries: Apps for SharePoint or Apps for Office. As the administrator, you can choose which of these libraries can be utilized by your user base.



---

**EXAM TIP**

An App Catalog site is scoped to a single web application within SharePoint; as a result, farms that maintain multiple web applications can have distinct, matching App Catalog sites.

---

A new App Catalog can be created simply by selecting the Apps within Central Administration and then selecting Manage App Catalog. Once there, you can choose to either create a new App Catalog site (no different than creating a standard SharePoint site) or enter a URL for an existing App Catalog site.

**IMPORTANT** As we will cover in the section about configuring DNS entries, the site collection that hosts the App Catalog should be set up with its own fully qualified domain name (FQDN); additionally, this FQDN should not be a subdomain (for example, *apps.wingtiptoy.com*). The reason for using an FQDN is because newly added Add-ins have a unique URL, which is composed of the app domain name plus a prefix and an Apphash (a unique identifier for each app for use with SharePoint). Using a subdomain presents a security risk due to exposing information found in cookies.

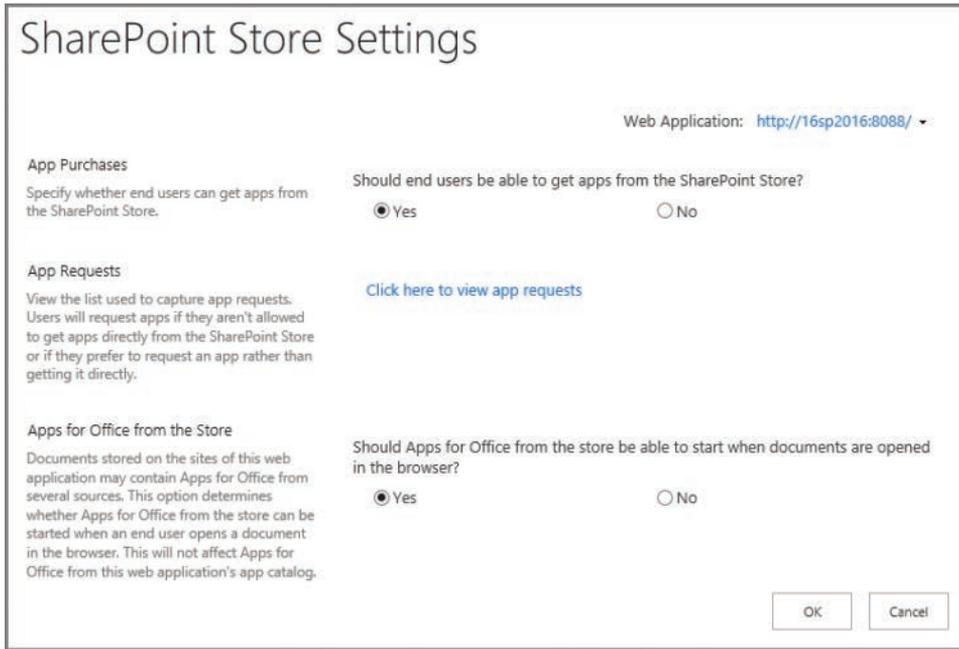
## Configure marketplace connections

Connections to the SharePoint Marketplace (now known as the Office and SharePoint Store) are configured in two distinct locations within Central Administration: SharePoint Store Settings and Application Management.

### SharePoint Store Settings

The first configuration that is required is to decide on a per-web-app basis whether users will be able to select SharePoint Apps, Office Apps, both, or neither for use within the SharePoint farm.

This selection is made within the SharePoint Store Settings page of the Apps section in Central Administration, and is configured on a per-web-app basis (shown in Figure 4-7).



**FIGURE 4-7** SharePoint Store Settings page

Selecting the appropriate web application then allows the admin to choose from three settings:

- **App Purchases** Choose whether users should be able to get apps from the SharePoint Store.
- **App Requests** View any pending app requests.
- **Apps For Office From The Store** Allow Apps for Office to start when users interact with documents in a web browser.

## Application management

If sites in a web app are configured to allow Internet-facing endpoints, you can turn on the Internet-facing endpoints feature to allow the use of Add-ins that support this functionality; otherwise, these Add-ins are unavailable in the SharePoint Store.

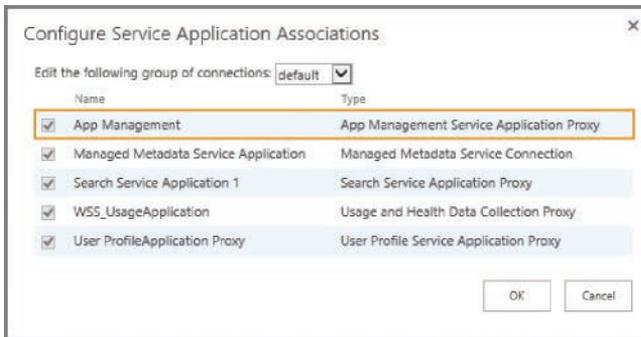
Selecting the web app and then selecting Manage Features (Figure 4-8) allows you to activate the feature called Apps That Require Accessible Internet Facing Endpoints. This can be useful when your users are unable to access the SharePoint Store with the message Sorry, We Can't Seem To Connect To The SharePoint Store.



**FIGURE 4-8** Manage Applications page, Web Applications tab, showing the Manage Features and Service Connections icons

## Service connections

Depending on how your environment was configured, you might have more than a single App Management service application. If this is the case, you might need to choose the service application connections used for your web application; in our case, we are concerned that we select the correct connection group and then select the App Management Service Application Proxy (see Figure 4-9).



**FIGURE 4-9** Ensuring that the App Management Service Application Proxy is selected

## Skill: Create and configure productivity services

Beyond the core services and service applications of a SharePoint farm lie the productivity services, which extend different features out to users in the farm. These features range in scope from MS Office centric (Access, Visio, Word, PowerPoint, and so on) to hybrid components (OneDrive and the App Launcher), and finally to the newly introduced management components within the SharePoint Insights and Telemetry feature set.

**This section covers how to:**

- Create and configure Office Online Server and optional SharePoint services
- Configure hybrid OneDrive for Business with Profile Redirection and Extensible App Launcher
- Plan and install SharePoint Insights and SharePoint Server Telemetry features

## Create and configure Office Online Server and optional SharePoint services

Extensible functionality is available in (but not fundamental to) the setup and creation of a SharePoint Server 2016 farm. Some of this functionality is provided by service applications, whereas other functionality exists in the form of an external, non-SharePoint environment.

This functionality is provided by:

- **Office Online Server** Office Online Server is an on-premises server (not a SharePoint farm server) that delivers browser-based versions of Office applications (such as Microsoft Word). This functionality can be provided to Exchange Server 2016, Skype for Business Server 2015, Lync Server 2013, and SharePoint environments.
- **Microsoft Access Services** Access Services enables the creation and customization of Access add-ins for SharePoint.
- **Microsoft Visio Services** Visio Services allows users to share and view Visio diagrams in a SharePoint site. These diagrams can be configured to be updated by using information from various data sources.
- **Microsoft Word Automation Services** Word Automation Services provides unattended, server-side conversion of documents into formats supported by Microsoft Word.
- **Microsoft PowerPoint Conversion Services** PowerPoint Conversion Services (also known as PowerPoint Automation Services) allows for the conversion of PowerPoint files (.pptx and .ppt) to a number of different formats, including .pptx, .pdf, .xps, .jpg, and .png.
- **Microsoft Translation Services** Translation Services allows for the automatic machine translation of files and sites. This is accomplished by sending these files to the Microsoft Translator cloud-hosted machine translation service, also used by the Office, Skype, Yammer, and Bing translation features.

### Office Online Server

- In Chapter 1, we discussed the planning and installation of Office Online Server. This server is an on-premises solution, exists out of the bounds of the SharePoint server farm, and can be configured to provide services to SharePoint, Skype for Business, and Exchange Server environments.

Configuration steps for this farm are largely unchanged from those required to set up Office Web Apps Server (replaced by Office Online Server), and can be broken down into three major groupings: installing prerequisites, installing Office Online Server binaries, and configuring the connection between Office Online Server and the SharePoint Server 2016 farm.

- **Install prerequisites** Once the physical servers have been built for Office Online Server, additional components and configuration are required before the Office Online Server components can be installed.
  - Install .NET Framework 4.5.2.
  - Install the supporting operating system features required by Office Online Server.
  - Reboot the Office Online Server server(s).
- **Install Office Online Server** This installation requires that you download Office Online Server binaries from the Volume License Service Center.
  - On the Office Online Server servers, run Setup.exe.
  - Obtain and install SSL certificates. If you are running split DNS, you will only need a single certificate; if you have different internal and external FQDNs, you will need two different certificates.
  - Configure DNS to point to the appropriate FQDNs.
  - Use the New-OfficeWebAppsFarm PowerShell cmdlet to build the new Office Online Server farm.
- **Configure SharePoint 2016** The newly created Office Online Server environment must be connected to SharePoint.
  - Use the New-SPWOPIBinding cmdlet to bind the two environments together.
  - Use the Set-SPWOPIZone cmdlet to configure the zone that the SharePoint will use to navigate the browser to Office Online Server.
  - Configure Office Online Server to allow HTTP OAuth connections (if required, *not* recommended for a production environment).



#### **EXAM TIP**

Installing Office Online Server isn't terribly difficult. The items that should be studied for the test are the prerequisites for installation, and the PowerShell cmdlets for configuration, along with their optional switches.

---

**NEED MORE REVIEW?** Detailed information concerning the installation and configuration of Office Online Server (including how to connect it to SharePoint, Exchange Server, and Skype for Business Server) can be found in the TechNet Wiki article "Install & Configure Office Online Server" at <http://social.technet.microsoft.com/wiki/contents/articles/34289.install-configure-office-online-server.aspx>.

## Microsoft Access Services

As was the case with SharePoint 2013, SharePoint 2016 hosts two service applications that provide Access Services functionality:

- **Access Services** Access add-ins for SharePoint allow you to build databases in Access 2016 and then share them with other users as an add-in for SharePoint in a web browser.
- **Access Services 2010** Access Services 2010 is still provided for backward compatibility, and provides the ability to view and edit web databases that were previously created by using Access 2010 and SharePoint Server 2010.



---

### **EXAM TIP**

Although SharePoint 2016 allows for the presentation and editing of Access Services 2010 databases, new web databases cannot be added to SharePoint 2016. Instead, you must use the newer Access Services functionality.

---

Access Services in SharePoint 2016 provides a series of add-in features, including the following:

- Cascading controls
- Datasheet filter improvements
- Related Item Control enhancements
- Image storage and performance improvements
- Office Add-ins integration with Access web apps
- Additional packaging and upgrade functionality for Access web app packages
- On Deploy macro action for upgrade scenarios
- Lock tables from editing functionality
- Download in Excel feature for datasheet views

The configuration of Access Services on a SharePoint server requires that a series of SQL Server Components be added to the SharePoint servers that host the Front-end role.. Once these components have been added to the SharePoint servers, Access Services configuration requires only five major configuration steps:

1. Configure the SharePoint Server farm for Add-ins (covered in the last section).
2. Configure SQL Server, used to store Access Add-in content.
3. Create a Secure Store service application (covered in the next section).
4. Create the Access Services service application (from either Central Administration or PowerShell).
5. Configure Security.

**NEED MORE REVIEW?** At the time of publication for this Exam Ref, detailed instructions for configuring Access Services in a SharePoint 2016 environment had not yet been released. Fortunately, SharePoint 2016 documentation on TechNet is maintained alongside the SharePoint 2013 documentation, and will be introduced in the TechNet article “Plan for Access Services in SharePoint Server 2013” at [https://technet.microsoft.com/library/ee683869\(v=office.16\).aspx](https://technet.microsoft.com/library/ee683869(v=office.16).aspx).

## Microsoft Visio Services

Prior to use, Visio Services requires that both a service application and the associated proxy be created. As is the case with many other service applications in SharePoint Server 2016, it is *not* necessary to attempt to start the Visio Graphics service prior to the creation of the actual Visio Graphics service application and proxy, due to MinRole service controls. When the Visio Graphics service application has been configured, the Visio Graphics service is activated automatically on SharePoint servers that host the Front-end role.

### CREATING THE VISIO GRAPHICS SERVICE APPLICATION

Creating a service application and proxy for the Visio Graphics service is fairly straightforward, requiring only that you select New, Visio Graphics Service on the Service Applications screen in Central Administration (alternately, you could use PowerShell for a scripted configuration).

Only four pieces of information are required to complete this process:

- **Name** The name of the Visio Graphics service application.
- **Application Pool And Credentials** Choose whether to reuse an existing application pool or create a new application pool, providing the managed account for security credentials.
- **Partitioned Mode** Choose whether or not to run in partitioned mode; this is used in multitenancy environments.
- **Add To Default Proxy List** Choose whether or not to add the service application’s proxy to the farm’s default proxy list.

### CONFIGURING THE VISIO GRAPHICS SERVICE APPLICATION

The Visio Graphics service allows you to configure two distinct sets of items: Global Settings and Trusted Data Providers. Configuring these items can influence both the performance and security of this service.

- **Global Settings** This menu allows for the management of performance, security, and data connection refresh rates.
- **Maximum Drawing Size** The maximum size in MB (default is 25) of a web drawing that can be rendered.
- **Minimum Cache Age** The minimum number of minutes (default is 5) that a web drawing is cached in memory.

- **Maximum Cache Age** The number of minutes (default is 60) after which cached web drawings are purged.
- **Maximum Recalc Duration** The number of seconds (default is 60) before data refresh operations time out.
- **Maximum Cache Size** The maximum cache size in MB (default is 5,120) that can be used.
- **External Data** Allows the administrator to assign the target Application ID used to reference Unattended Service Account Credentials.
- **Trusted Data Providers** A listing of trusted data providers available for use with Visio Graphics service, which includes SQL Server, Oracle, IBM, SharePoint, and Excel Web Services.

**NEED MORE REVIEW?** The use of Visio within SharePoint Server 2016 can range from very simple (rendering Visio drawings in the browser) to very complex (rendering Visio drawings that connect to external data sources). For a better understanding of this service application, review the TechNet article entitled “Visio Graphics Service administration in SharePoint Server 2013” at [https://technet.microsoft.com/library/ee524059\(v=office.16\).aspx](https://technet.microsoft.com/library/ee524059(v=office.16).aspx).

## Microsoft Word Automation Services

Word Automation Services is configured in a similar manner to Visio Services, requiring that both a service application and the associated proxy be created. Note that it is not necessary to attempt to start Microsoft Word Automation Services prior to the creation of the actual Word Automation service application and proxy, due to MinRole service controls.

When the Word Automation service application has been configured, the corresponding Word Automation service is activated automatically on SharePoint servers that host the application role (as this application runs a batch process).

### CREATING A WORD AUTOMATION SERVICE APPLICATION

Creating a service application and proxy for the Microsoft Word Automation service is a fairly standard SharePoint service application install, but does also require a supporting database.

To begin creating this service application, select New, Word Automation service from the Service Applications page in Central Administration (alternately, you could use PowerShell for a scripted configuration).

Five pieces of information are required to complete this process:

- **Name** The name of the Word Automation service application.
- **Application Pool And Credentials** Choose whether to reuse an existing application pool or create a new application pool, providing the managed account for security credentials.

- **Partitioned Mode** Choose whether or not to run in partitioned mode; this is used in multitenancy environments.
- **Add To Default Proxy List** Choose whether or not to add the service application's proxy to the farm's default proxy list.
- **Database** Specify the Database Server, Database Name, and Database authentication credentials.

## CONFIGURING A WORD AUTOMATION SERVICE APPLICATION

The Word Automation service provides several options having to do with both the document formats that can be converted by this service and tuning the performance (and service load) on the SharePoint farm.

- **Supported File Formats** Which file formats can be opened by the service application.
  - Open XML Documents (such as .docx, .docm, .dotx, .dotm).
  - Word 97-2003 (binary) documents (such as .doc, .dot).
  - Rich Text Format (.rtf).
  - Webpage (.htm, .html, .mht, .mhtml).
  - Word 2003 XML Document (.xml).
- **Embedded Font Support** Allows the choice of supporting embedded fonts in a document.
- **Maximum Memory Usage** The maximum percentage of system memory (default is 100 percent) made available in the service application.
- **Recycle Threshold** The number of documents (default is 100) converted by a conversion process before it is restarted.
- **Word 97-2003 Document Scanning** Word 97-2003 documents are a binary format, and can carry hidden payloads; this setting decides whether or not these documents should be scanned prior to conversion.
- **Conversion Processes** Specifies the number of conversion processes (default is 1) created on each server available to the service application.
- **Conversion Throughput** Determines both the frequency in minutes (default is 15) with which conversions are started and the number of conversions to start (default is 300) per conversion process.
- **Job Monitoring** Specifies the length of time before conversions are monitored (default is 5) and potentially restarted.
- **Maximum Conversion Attempts** Specifies the maximum number of times a conversion is attempted (default is 2) before its status is set to Failed.
- **Maximum Synchronous Conversion Requests** Specifies the maximum number of synchronous conversion requests (default is 25) that can be processed at a time on each server available to the service application.

## Microsoft PowerPoint Conversion Services

PowerPoint Conversion Services is very similar to Word Automation Services in concept. It is a service application that is responsible for taking content of one type (in this case, .ppt and .pptx PowerPoint files) and converting it into one of several formats.

From a creation point of view, PowerPoint Conversion Services is quite a bit different than the Word Automation or Visio Graphics services, as it must be configured in PowerShell. It does, however, require that both a service application and the associated proxy be created.



---

### **EXAM TIP**

**There is no mechanism for creating a new PowerPoint Conversion service application in Central Administration.**

---

Note that it is not necessary to attempt to start the PowerPoint Conversion service prior to the creation of the actual PowerPoint Conversion service application and proxy, due to MinRole service controls. When the PowerPoint Conversion service application has been configured, the corresponding service is activated automatically on SharePoint servers that host the Application role (as this application runs a batch process, similar to Word Automation Services).

### **CREATING A POWERPOINT CONVERSION SERVICE APPLICATION**

Creating a service application and proxy for the PowerPoint Conversion service is a very basic SharePoint service application install requiring that the following steps be carried out via a PowerShell script:

1. Create the service application by using the `New-SPPowerPointConversionServiceApplication` cmdlet.
2. Assign the service application to a specified Service Application Pool.
3. Create a matching service application proxy by using the `New-SPPowerPointConversionServiceApplicationProxy` cmdlet and assign the proxy to a group (usually default).

After the service application has been configured, a local folder named PowerPoint Conversion should be created on each Application role server, and the WSS\_WPG group should be given NTFS modify rights. The folder should be created in the `C:\ProgramData\Microsoft\SharePoint\` path.

### **CONFIGURATING THE POWERPOINT CONVERSION SERVICE APPLICATION**

Unlike other service applications, the PowerPoint Conversion service application does not provide the ability to manage or set properties from Central Administration. In fact, a custom application needs to be created to use this service.

**NEED MORE REVIEW?** On the TechNet site, there is an article called “SharePoint 2013: Configure PowerPoint Automation Services” that is useful for learning to configure and use this service application. This article can be found at <http://social.technet.microsoft.com/wiki/contents/articles/21627.sharepoint-2013-configure-powerpoint-automation-services.aspx>.

## Configuring hybrid OneDrive for Business with Profile Redirection and Extensible App Launcher

Hybrid OneDrive for Business and the Extensible App Launcher are both part of the hybrid functionality present in SharePoint 2016.

- **OneDrive for Business** OneDrive for Business provides services that had previously been considered part of the on-premises OneDrive for Business configuration (also known as My Sites).
- **Extensible Hybrid App Launcher** The Extensible Hybrid App Launcher is a visual component in the interface that allows Apps (Add-ins) to be pinned to your session in Office 365; as these modifications are made, they are pushed down to the on-premises SharePoint 2016 environment.

### Configuring OneDrive for Business with Profile Redirection

When configuring a SharePoint farm for a hybrid deployment, there are two options available from Office 365 in Central Administration:

- OneDrive and Sites
- OneDrive only

Regardless of the option chosen, the user will receive access to a OneDrive that replaces the on-premises version. The only configuration option available is the assignment of users to either an on-premises or cloud OneDrive via the use of Audiences.

**NEED MORE REVIEW?** To better understand how users can be granted access to Office 365 via Audiences, review the TechNet article entitled “How to redirect users to Office 365 for OneDrive for Business” at <https://technet.microsoft.com/library/dn627525.aspx>.

### Configuring the Extensible Hybrid App Launcher

The Extensible Hybrid App Launcher requires that OneDrive and Sites be configured on the Office 365 page in Central Administration. Once the App Launcher has been enabled, an administrator can log in to Azure Active Directory (either from the Azure Management Portal or from the Office 365 Admin Center) to configure new Apps on the launcher.

Two options exist for adding applications to the App Launcher:

- **Add An Application My Organization Is Developing** Uses the Add Application Wizard to capture fields including the App Name, Type, URI, and Sign-on URL.

- **Add An Application From The Gallery** Allows the user to search from and select an App in the Application Gallery.

In the case of applications added from the Gallery, each has a configuration menu that includes the ability to do the following:

- Enable single sign-on with Windows Azure Active Directory, including a selection from the following choices:
  - Windows Azure AD Single Sign-On
  - Password Single Sign-On
  - Existing Single Sign-On
- Enable automatic user provisioning to the App
- Assign users to the App

**NEED MORE REVIEW?** For more information about how the App Launcher can be customized, review the MSDN article entitled "Have your app appear in the Office 365 app launcher" at <https://msdn.microsoft.com/office/office365/howto/connect-your-app-to-o365-app-launcher>.

## Plan and install SharePoint Insights and SharePoint Server Telemetry features

SharePoint Insights allows SharePoint administrators to manage their on-premises infrastructure from Office 365 in a hybrid configuration. By using this service, Office 365 reports compile and relay information found in on-premises diagnostic and usage logs.

The Insights service taps local telemetry data to produce a dashboard showing SharePoint administrators which SharePoint features are being used and the actions users are taking, along with numerous advanced analytics about SharePoint use.

The Microsoft SharePoint Insights service will be configured in a similar fashion to hybrid OneDrive and Sites, from the Office 365 menu of Central Administration. The SharePoint Insights Hybrid scenario will be used to create the telemetry relationship between the on-premises SharePoint environment and Office 365. Should you attempt instead to start the Microsoft SharePoint Insights service from Central Administration, Services in Farm, you will be greeted with the following message:

*Authentication for Hybrid scenarios is not yet set. Please start the service after SharePoint Insights Hybrid scenario is enabled on your SharePoint farm.*

**NEED MORE REVIEW?** At the time of publication for this Exam Ref, detailed instructions for configuring Microsoft SharePoint Insights in a SharePoint 2016 environment had not yet been released. Once this functionality is made available, the supporting documentation will be found in the TechNet article entitled "Microsoft SharePoint Insights" at <https://technet.microsoft.com/library/86e0fc90-0ef8-4c22-9d3b-7af42bf882f1>.

# Skill: Create and configure a Business Connectivity Services (BCS) and Secure Store application

---

Business Connectivity Services (BCS) is a powerful feature that allows both SharePoint and non-SharePoint data and information to be represented within the same interface. Successfully presenting this data requires that the SharePoint administrator be familiar with both BCS itself as well as the Secure Store, which is required for storing credentials to these external systems.

## This section covers how to:

- Import and configure BCS models
- Configure BCS model security
- Configure BCS for search
- Generate a Secure Store master key
- Manage Secure Store Target Application permissions
- Create Secure Store Target Applications
- Configure hybrid BCS

## Import and configure BCS models

Designing a data connection for use with BCS requires the use of a model. This model is an XML file that contains sets of descriptions of one or more external content types, the related external systems, and other environment-specific information, such as authentication properties.

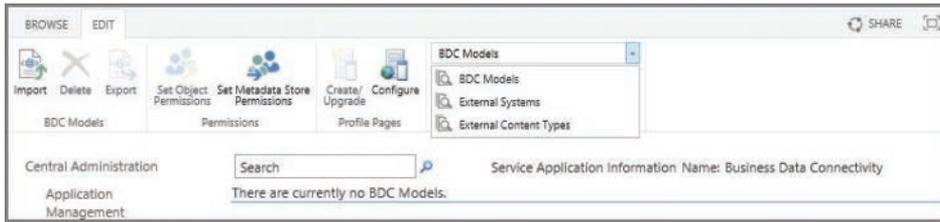
**IMPORTANT** BCS used to be called Business Data Catalog (BDC) in previous versions of SharePoint. Throughout this section, this functionality is referred to by its name in Central Administration for clarity. One of the places where this naming standard appears is in the naming of models; the XML model imported into BCS is still referred to as a BDC model.

Four main data sources are available for use within BCS:

- Windows Communication Foundation
- SQL Server
- SQL Azure
- OData sources (including SQL OData sources)

## Importing a BCS model

Once a BCS model has been made for the data source, it must be imported for use within SharePoint. Selecting the Business Data Connectivity service application allows for the management of the BDC service (Figure 4-10).



**FIGURE 4-10** Managing the BDC service application

Selecting the Import icon on the ribbon begins the import process, with the following options:

- **BDC Model** Browse to and upload a BDC model XML file.
- **File Type** Choose the file type (model or resource).
  - **Model** A BDC model definition file contains the base XML metadata for a system.
  - **Resource** A resource definition file enables you to import or export only the localized names, properties, permissions, or any combination of the three.
- **Advanced Settings** Advanced Settings allows you to do the following:
  - **Choose Which Resources To Import** It is possible to select more than one of the following: Localized names (selected by default), Properties (selected by default), and Permissions (not selected).
  - **Custom Environment Settings** If you imported a resource file type, it can include custom settings.

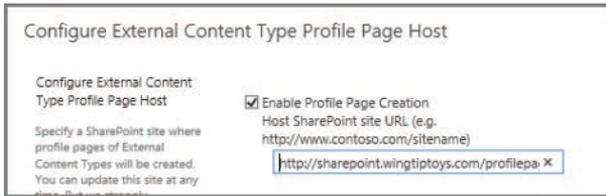


**EXAM TIP**

A BDC model can be imported using a combination of both the `Get-SPBusinessDataCatalogMetadataObject` and `Import-SPBusinessDataCatalogModel` cmdlets, as shown in the TechNet article “Import-SPBusinessDataCatalogModel” at <https://technet.microsoft.com/library/ff607757.aspx>. For the exam, be familiar with these cmdlets and also note that neither uses the phrase Business Connectivity Services or BCS.

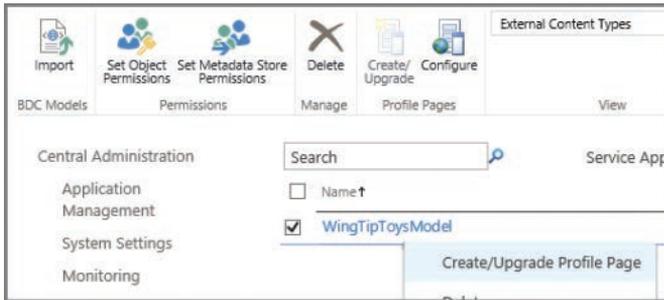
## Configuring an External Content Type Profile Page Host

Once the BCS model has been uploaded, Profile Pages can then be configured by selecting the Configure icon on the ribbon. The configuration process allows you simply to specify an External Content Type Profile Page Host, as shown in Figure 4-11.



**FIGURE 4-11** Configuring an External Content Type

Profile Pages are used to display information for an entity (External Content Type). New Profile Pages are added by selecting the External Content Type and then selecting Create/Upgrade Profile Page (Figure 4-12).



**FIGURE 4-12** Creating a new Profile Page

**NEED MORE REVIEW?** Creating and configuring BDC and BCS connections can be a very complex task. For a better understanding, review the TechNet article “Plan a Business Connectivity Services solution in SharePoint 2013” at <https://technet.microsoft.com/library/jj219580.aspx>.

## Configure BCS model security

BCS often connects to other line-of-business systems, which can contain sensitive data. As with any other system, security requires that we plan for the authentication to the data source as well as the authorization (permissions) for accessing the data source.

### Authentication

BCS supports three different authentication methods:

- **Credentials-based authentication** User name and password credentials are passed directly from BCS to the external system.
- **Claims-based authentication** The external system will accept credentials from a third-party authentication service (a security token provider). These credentials are comprised of assertions about the requestor (a claim).

- **Custom authentication** If neither credentials- nor claims-based authentication is supported by the external system, then a custom solution will be required to translate credentials from BCS to a format understood by the external system.

## Authorization

Once authentication has been performed, the next discussion is which roles will be assigned access to the solution. The security of this data should be assigned to three roles in a SharePoint farm:

- **Administrative roles** Administrators are responsible for permissions management, creating and managing the BDC service application, importing BDC models, and managing permissions. If Add-ins are also used, then administrators will also publish the Add-in and create and manage connection objects.
- **Developer or Designer roles** These roles create the external content types, BDC models, and the Add-ins for SharePoint by using BCS.
- **User roles** Multiple groupings of users may be assigned to consume and possibly manipulate external data in the BCS solution.

Permissioning in BCS needs to be managed for four distinct components of the BCS solution:

- **External system** The external system administrator will assign and manage permissions for the solution; if users are required to use their SharePoint credentials, the Secure Store service might need to be set up in SharePoint.
- **BCS central infrastructure** This has to do with the security of the service application contained within Central Administration on the SharePoint farm; permissions to this service application can be delegated (as can happen on a number of other service applications in SharePoint).
- **Development environment** As a development environment will likely be required for BCS design efforts, this environment can have fewer users but permissions can be a bit more relaxed, so as not to impede development efforts.
- **User environment** User permissions differ based on the mechanisms used for accessing BCS data. For instance, it is a different matter (in terms of scope and execution) to configure external lists and columns, than to assign permissions via Office and SharePoint Add-ins.

**NEED MORE REVIEW?** BCS security extends from the SharePoint user, through administration, and into the destination system. Ensuring that these data connections are secure is a fundamental requirement for implementing successful BCS solutions. For a better understanding of the detailed tasks required for securing a BCS solution, review the TechNet article “Overview of Business Connectivity Services security tasks in SharePoint 2013” at <https://technet.microsoft.com/library/jj683116.aspx>.

## Generate a Secure Store master key

The Secure Store service in SharePoint 2016 is a claims-aware service that stores authorization credentials in an encrypted database. These credentials can be used by other service applications in the farm, particularly to access external data sources.

### Creating the Secure Store service application

As service applications go, setting up the Secure Store service application is quite easy. After selecting Manage Service Applications from within Central Administration, all that must be provided is a handful of information:

- **Service Application Name** A name for the new service application.
- **Database** The server and database names, along with the authentication mechanism used (Windows or SQL).
- **Failover Server** Only used if you implement SQL mirroring.
- **Application Pool** Create a new application pool (or reuse an existing one).
- **Enable Audit** Choose whether or not to enable an Audit log for the Secure Store service (and how many days it spans), which will then be stored in the Secure Store database.

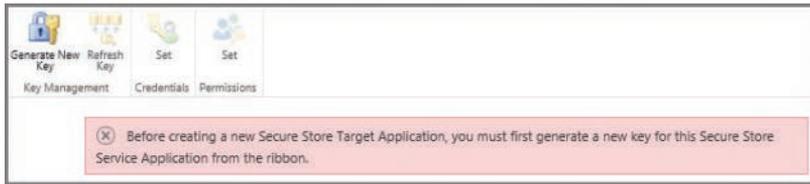
Several guidelines exist for the secure configuration of the Secure Store service application. These guidelines are designed to help secure this database, as it stores potentially sensitive credentials.

- Run the Secure Store service in a separate application pool from all other service applications.
- Run the Secure Store service in a separate application server not used for any other service.
- Deploy the Secure Store database to a different instance of SQL Server than is used for the SharePoint 2016 installation.

### Creating a new key

Aside from creating the Secure Store service application (created from Central Administration, Service Applications), the only other task that remains is to create a new encryption key for use with the Secure Store database.

On the initial installation of the Secure Store service application, the service will not allow you to create new Target Applications until this key has been generated (Figure 4-13).



**FIGURE 4-13** Warning message about generating a new key

Three guidelines exist for the creation and management of the encryption key:

- Back up the Secure Store database:
  - Before generating a new encryption key
  - After it's initially created
  - Each time credentials are re-encrypted
- Back up the encryption key (located in the Secure Store service application):
  - After initially setting up Secure Store
  - Each time it is regenerated
- Do not store the encryption key backup media in the same location as the backup media used for the Secure Store database.

Clicking the Generate New Key icon starts the process of generating and applying the encryption key. This process requires that you create a case-sensitive pass phrase for use with the encryption key, and which is used when adding new Secure Store service servers as well as restoring a backed-up Secure Store database (Figure 4-14).



**FIGURE 4-14** Creating a new pass phrase while generating a new encryption key

Once the key has been generated, make sure to record the pass phrase, as both it and the encryption key are required to successfully restore the Secure Store database.

**IMPORTANT** At this point, you should perform a full backup of both the Secure Store service application (under Shared Services in Central Administration, Backup and Restore) as well as the Secure Store database.

## Create Secure Store Target Applications

Creating a new Secure Store Target Application is a three-step process. On the ribbon, clicking the New icon begins this process.

### First Configuration page

On the first configuration page, shown in Figure 4-15, you have the opportunity to provide the following values:

- **Target Application ID (name)** A unique, unchangeable identifier for your Target Application.
- **Display Name** A friendly (display) name for the Target Application.
- **Contact E-mail** The e-mail for the primary contact for this Target Application.
- **Target Application Type** Choose from an Individual Ticket, Individual Restricted, Individual (Default), Group Ticket, Group Restricted, or Group.
- **Target Application Page URL** Choose whether to use Default Page, a Custom Page (specify), or None.

**Create New Secure Store Target Application**

**Target Application Settings**

The Secure Store Target Application ID is a unique identifier. You cannot change this property after you create the Target Application.

The display name is used for display purposes only.

The contact e-mail should be a valid e-mail address of the primary contact for this Target Application.

The Target Application type determines whether this application uses a group mapping or individual mapping. Ticketing indicates whether tickets are used for this Target Application. You cannot change this property after you create the Target Application.

The Target Application page URL can be used to set the values for the credential fields for the Target Application by individual users.

Target Application ID:

Display Name:

Contact E-mail:

Target Application Type:

Target Application Page URL:  Use default page,  Use custom page,  None

**FIGURE 4-15** Creating a new Secure Store Target Application (Page 1)

**NEED MORE REVIEW?** Target Application types have to do with the type of account used to map user credentials. More information on these items can be found in the MSDN article "How to: Use Secure Store Service to Connect to an External System" at [https://msdn.microsoft.com/library/office/ee554863\(v=office.14\).aspx](https://msdn.microsoft.com/library/office/ee554863(v=office.14).aspx).

## Second configuration page

On the second configuration page, you have the opportunity to provide both two field names and two matching field types (Figure 4-16). Field Name simply describes what the field is to be called, and is not a field for entering a user name or a password. The Masked check box can be selected to hide either the user name, password, or both when setting credentials, as you will see shortly.



Field Name	Field Type	Masked	Delete
Windows User Name	Windows User Name	<input type="checkbox"/>	X
Windows Password	Windows Password	<input type="checkbox"/>	X

Add Field

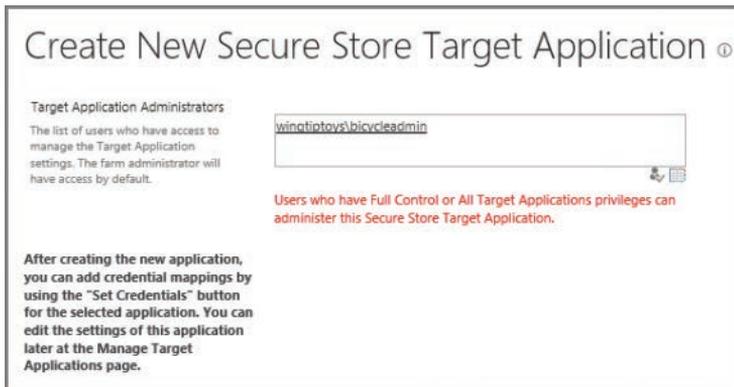
**Important: The field names and field types cannot be edited later.**

**FIGURE 4-16** Creating a new Secure Store Target Application (Page 2)

## Third configuration page

On the third and final configuration page, the Target Application Administrators can be selected. These users are then given privileges to manage the Target Application settings (Figure 4-17).

**IMPORTANT** Farm administrators automatically have access to the Target Application.



Target Application Administrators

The list of users who have access to manage the Target Application settings. The farm administrator will have access by default.

wintoptovs\bicyleadmin

**Users who have Full Control or All Target Applications privileges can administer this Secure Store Target Application.**

After creating the new application, you can add credential mappings by using the "Set Credentials" button for the selected application. You can edit the settings of this application later at the Manage Target Applications page.

**FIGURE 4-17** Creating a new Secure Store Target Application (Page 3)

**NEED MORE REVIEW?** The settings on this page depend greatly on which Target Application type was previously selected. For a clearer understanding of the effect this choice has on the Secure Store Target Application, review the TechNet article "Plan the Secure Store Service in SharePoint Server 2016" at [https://technet.microsoft.com/library/ee806889\(v=office.16\).aspx](https://technet.microsoft.com/library/ee806889(v=office.16).aspx).

# Manage Secure Store Target Application permissions

Permissions for the Secure Store Target Application have to do with two actions: setting credentials and setting permissions.

## Setting credentials

Once the Target Application has been created, user credentials need to be initially set. Selecting Target Application, Set Credentials provides the opportunity to specify a Credential Owner as well as individual or group user names and passwords (Figure 4-18).

**IMPORTANT** This credential entry provides no opportunity for user lookups or validation; be careful of the values you enter here, as it would be easy enough to accidentally include a typographical error.

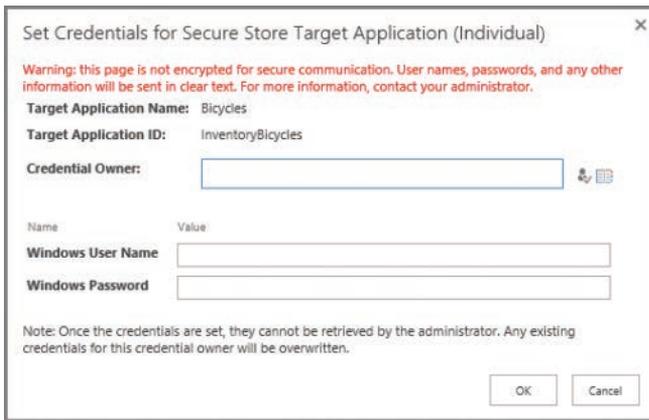


FIGURE 4-18 Setting credentials for the Secure Store Target Application

## Setting permissions

After the Target Application is created, user permissions can be applied after the fact. Selecting the Target Application ID and then choosing to Set Permissions will give the ability to specify one or more permission sets (Target Application Administrators shown in Figure 4-19), depending on the Target Application type previously chosen.

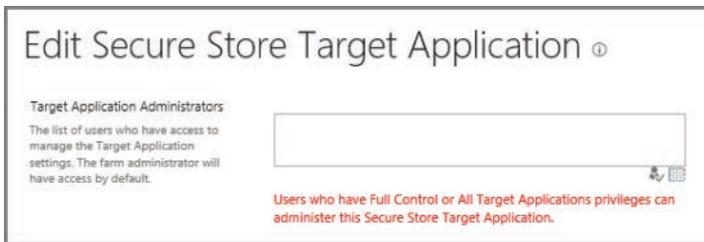


FIGURE 4-19 Setting permissions

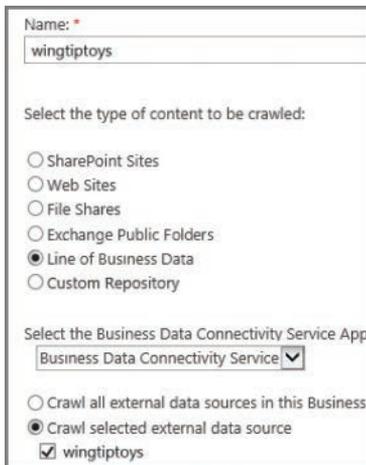
**IMPORTANT** As we will see shortly, the Search service account should be given member access at both the Secure Store Target Application as well as on the appropriate BDC External Content Type.

## Configure BCS for search

To surface a BDC External Content Type in Search, the External Content Type needs to be configured as a Content Source in the Search service application.

Within the Search service application, selecting New Content Source begins this process, requiring the following fields (shown in Figure 4-20):

- **Name** The name of the Search content source.
- **Type of content to be crawled** Selections include SharePoint Sites, Web Sites, File Shares, Exchange Public Folders, Line Of Business Data (selected), and Custom Repository.
- **Select The Business Connectivity Service Application** Allows for the selection of a BCS service application (assuming there is more than one).
- **Crawl** Either Crawl All External Data Sources or Crawl Selected External Data Source, in this case Wingtip toys.



The screenshot shows a configuration form for a BCS content source. It includes a text box for the name 'wingtip toys', a radio button selection for 'Line of Business Data', a dropdown menu for 'Business Data Connectivity Service', and a checked radio button for 'Crawl selected external data source' with 'wingtip toys' selected.

**FIGURE 4-20** Configuring a BCS content source

## Configure hybrid BCS

BCS is available both on-premises and in SharePoint online. By using the Microsoft BCS hybrid deployment scenario, you can publish on-premises data to an external list or add-in on SharePoint Online.

## Prerequisites

Prior to its use, an environment must be configured for use with the BCS hybrid scenario. This configuration has several prerequisites:

- There must be an S2S trust with Azure Access Control Service for inbound hybrid connections.
- Ensure that all on-premises user accounts accessing the BCS hybrid solution are federated accounts.
- Create a service account in the on-premises domain intended to access the OData service endpoint.
- Create a global security group in the on-premises domain.
- Add the federated accounts from the on-premises domain to the global security group.

## Configuration steps for hybrid BCS

Configuring the on-premises environment to use the hybrid BCS scenario requires several steps, intended to establish the relationship between the two environments:

- Create and configure a Secure Store Target Application, which links the global security group to the service account, both of which were created in the prerequisites section.
- Create and configure the OData service endpoint; this will also include the assignment of permissions to the data source represented by this endpoint.
- Prepare the SharePoint Online site and App Catalog, identifying the site through which the data will be offered, and configuring the App Catalog (if an Add-in for SharePoint will be used).
- Set permissions on the BDC Metadata Store in SharePoint Online (for use with manual imports of External Content Type method).
- Validate external access to the on-premises SharePoint environment using the URL published through your reverse proxy.
- Create and configure the External Content Type by using Visual Studio.
- From BCS in SharePoint Online, configure a connection settings object, which contains additional information used to establish the connection to the external system and OData source.

**NEED MORE REVIEW?** Establishing the relationship between environments is error-prone, often requiring a lot of troubleshooting. Fortunately, this process is documented in Chapter 3 (“BCS hybrid”) of the ebook *Configuring Microsoft SharePoint Hybrid Capabilities*, available for free download at [https://blogs.msdn.microsoft.com/microsoft\\_press/2016/07/06/free-ebook-configuring-microsoft-sharepoint-hybrid-capabilities/](https://blogs.msdn.microsoft.com/microsoft_press/2016/07/06/free-ebook-configuring-microsoft-sharepoint-hybrid-capabilities/).

## Skill: Manage SharePoint solutions and applications

---

From an extensibility standpoint, SharePoint has several options, depending on whether development efforts are specific to an on-premises deployment or meant for working in a hybrid situation. This skill begins with solutions (both sandboxed and full trust), then moves into the Add-in (previously referred to as App) model functionality.

### This section covers how to:

- Manage sandbox solution quotas
- Configure sandbox solution management
- Deploy farm solutions
- Upgrade farm solutions
- Deploy Apps
- Upgrade Apps

## Manage sandbox solution quotas

Sandbox solutions are code that runs in a very restricted execution environment. Maintaining these solutions in this space limits the amount of resources they consume from the SharePoint farm as a whole, perhaps preventing a poorly written solution from potentially taking down the entire SharePoint farm.

**IMPORTANT** Sandbox solutions were deprecated in SharePoint 2013, but this functionality is provided with backward compatibility in mind. No new development should be using a sandbox solution.

Sandbox solutions are monitored by SharePoint for resource usage on a per-site-collection basis, and assigned points (via quota) that can be used on a daily basis. If this limit is reached, all sandboxed solutions within the site collection are disabled for the rest of the day, then reset by the Solution Daily Resource Usage Update timer job.

## Creating a new quota template

A quota template provides a reusable mechanism for quickly assigning storage and resource limits to a series of site collections. Quota templates are assigned in Application Management, Site Collections, Specify Quota Templates, and require that the following fields be completed:

- **Template Name** Choose to either edit an existing quota template or create a new one.
- **Storage Limit Values** Limit site storage and set a warning threshold for an email notification in the site collection.
- **Sandboxed Solutions With Code Limits** Limit the maximum resource usage per day (default is 100 points), also setting a warning threshold for an email notification in the site collection.

## Altering a site collection quota

It might be the case that a particular site collection needs a temporary change in resources or perhaps will be receiving a custom site collection quota, assigned without the use of a quota template. These quotas are assigned in Application Management, Site Collections, Site Collection Quotas and Locks, and require the following fields be completed:

- **Site Collection** The site collection selected is the one for which the quota is being changed or unlocked.
- **Site Lock Information** This indicates the existing website collection owner as well as the current lock status for the site (which can be altered): Not Locked, Adding Content Prevented, Read Only, or No Access.
- **Site Quota Information** Allows for the selection of a predefined quota or the assignment of limits for both storage and resource quotas.

**NEED MORE REVIEW?** The creation, assignment, and alteration of quotas is described in the TechNet article “Create, edit, and delete quota templates in SharePoint 2013” at [https://technet.microsoft.com/library/cc263223\(v=office.15\).aspx](https://technet.microsoft.com/library/cc263223(v=office.15).aspx).

## Configure sandbox solution management

Sandbox solution management can be found in Farm Management, under Manage User Solutions. This page allows the administrator to accomplish one of two distinct tasks:

- **Solution Restrictions** Within this section, an administrator can do the following:
  - Name a solution that should be blocked and prevent it from running.
  - Optionally, display a message to the user, describing why this particular solution is disallowed in the farm.
- **Load Balancing** This section has to do with performance and the load on a particular server.
  - Choosing to run all sandboxed code on the same machine as a request might perform better for smaller deployments, but not be able to handle a larger number of simultaneous requests.
  - Choose instead to use solution affinity to balance requests across multiple servers running the Microsoft SharePoint Foundation Sandboxed Code service.

**NEED MORE REVIEW?** A bit of confusion exists around sandboxed solutions, and specifically their use. Many SharePoint administrators think that they are deprecated, but this is untrue; not all sandbox solutions are deprecated, only those that use custom code.

The Microsoft SharePoint Foundation Sandboxed Code Service is available in SharePoint 2016, although it's not provisioned or activated by default. For a better understanding of sandboxed solutions, review the TechNet article “Sandboxed solutions overview” at [https://technet.microsoft.com/library/ee721992\(v=office.14\).aspx](https://technet.microsoft.com/library/ee721992(v=office.14).aspx).

## Deploy farm solutions

Farm solutions are a type of on-premises code deployment wherein dynamic-link libraries (DLLs) can be added to the global assembly cache. This type of deployment means that the solutions are “trusted,” and therefore not subject to the same limitations placed on User (sandbox) solutions.

Although full trust solutions cannot be used in SharePoint Online, they are still a viable mechanism for deploying new functionality within an on-premises or cloud-hosted SharePoint farm, such as that found in Microsoft Azure. Before a solution package can be deployed in a SharePoint farm, it has to be submitted to the Solution Store in the configuration database by way of the `Add-SPSolution` cmdlet.

## Adding and installing solutions

The process of deploying a farm solution is fairly straightforward:

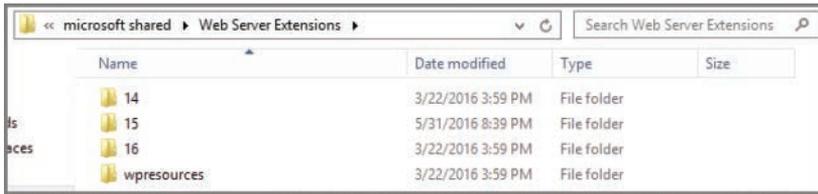
- 1. Add the farm solution** Before the solution can be deployed, it has to be added to the farm by using the `Add-SPSolution` cmdlet (there is no provision for adding a farm solution via Central Administration).
- 2. Deploy the farm solution** Once the solution has been added, it can be deployed:
  - Via PowerShell by using the `Install-SPSolution` cmdlet
  - Via Farm Management, Manage Farm Solutions in Central Administration

## Backward compatibility

As you are busily creating a new SharePoint 2016 environment, you might actually be ahead of the development curve. The full trust solutions you’ve maintained until now might be built for SharePoint 2013 (or even SharePoint 2010).

Fortunately, SharePoint has mechanisms in place that allow you to continue using older solutions, in the form of the `-CompatibilityLevel` switch, used with the `Install-SPSolution` cmdlet. On a SharePoint 2016 farm server, three folders exist at `C:\Program Files\Common Files\Microsoft shared\Web Server Extensions` (Figure 4-21), representing three different modes:

- **14 folder** Installing a solution into the 14 folder indicates SharePoint 2010 compatibility mode.
- **15 folder** Installing a solution into the 15 folder indicates SharePoint 2013 compatibility mode.
- **16 folder** Installing a solution into the 16 folder indicates SharePoint 2016 compatibility mode.



**FIGURE 4-21** The Web Server Extensions folder, with the 14, 15, and 16 folders

**IMPORTANT** There is no provision for specifying the compatibility level of a solution when deploying it from Central Administration. That said, obtain updated solutions for your farm whenever they become available, as older versions might not work as desired.

## Upgrade farm solutions

After you've completed your SharePoint 2016 deployment and upgrade, your development teams or vendors might produce newer versions of the solutions present in your farm. When this occurs, you will need to work with these groups to better understand the changes made to the solution, as the act of upgrading a solution has two distinct flavors:

- **Updating a SharePoint solution** When the version of a SharePoint solution has been updated, the existing solution can be upgraded in place, if and only if the files and features are exactly the same as in the previous version. This replacement is done by using the `Update-SPSolution` cmdlet.
- **Replacing a SharePoint farm solution** More often than not, an updated solution means that new components, functionality, and (perhaps) bug fixes are also rolled in for good measure. This type of an update requires that the existing solution be retracted (`Uninstall-SPSolution`) and redeployed (`Install-SPSolution`).

## Deploy Apps

Site Owners in a SharePoint farm have the ability to provide Add-ins in their sites from one of three locations:

- From a list of Add-ins that were already available for a site
- From the privately available App (Add-in) Catalog
- From the commercial Office Store

In particular, this section isn't about commercially available Add-ins from the SharePoint Store; it concentrates instead on in-house development and deployment of Add-ins. SharePoint Add-ins that are developed in house often provide a level of customization over and above what can be purchased in the store, but they must be maintained just like the older, full trust solutions. These Add-ins can be added to the organization's private Add-in Catalog.

**IMPORTANT** When developing a new Add-in from the Microsoft Developer Tools for Visual Studio, the Add-in can be directly deployed to a test SharePoint site. This mechanism should not be used in a production SharePoint farm.

## Installing an Add-in via the Add-in Catalog

Importing and installing an Add-in is as simple as uploading a document. Open the Add-in Catalog site for the particular web application, and then select the Apps for SharePoint library.

Within the library, the new Add-in can be uploaded. At this point, the Item Details box will appear, prompting for the Name, Title, Short Description, Icon URL, and other settings.



### EXAM TIP

If your Add-in is not available in users' sites, ensure that you have selected the Enabled check box. Additionally, if you'd like to have the Add-in shown in the Featured Content view, simply select the Featured check box.

## Importing and installing an Add-in via PowerShell

Prior to the installation of an Add-in, the installer must be a member of certain roles and groups:

- Securityadmin fixed role on the SQL server instance
- Db\_owner fixed database role on all databases that are to be updated
- Administrators group on the local server where PowerShell cmdlets are to be run
- Site Owners group on the site collection to which you want to install the Add-in

**IMPORTANT** Adding an individual by using the Add-SPShellAdmin cmdlet grants the ability to use SharePoint PowerShell cmdlets.

The process of deploying an App or Add-in in a farm via PowerShell is similar to deploying a solution:

- 1. Import the Add-in package** Before the Add-in can be installed, it has to be added to the farm by using the Import-SPAppPackage cmdlet (there is no provision for adding an Add-in via Central Administration).
- 2. Deploy the Add-in** Once the Add-in has been added, it can be deployed; in the case of Add-ins, there is no provision for installing them via Central Administration. Install the Add-in via PowerShell by using the Install-SPApp cmdlet.



### EXAM TIP

It is not uncommon to see tasks that regularly occur in Central Administration represented instead by PowerShell commands in the exam.

## Upgrade Apps

After an Add-in has been installed, development might begin on a newer version of the Add-in. At some point, you might wish to place this new Add-in within the Add-in Catalog. When this occurs, you will need to decide which of the following two mechanisms you will use:

- **Updating a SharePoint Add-in** When the version of a SharePoint solution has been updated, the existing solution can be upgraded in place if (and only if) the files and features are exactly the same as in the previous version. This replacement is done by using the Update-SPAppInstance cmdlet.
- **Migrating from an older Add-in to a newer Add-in** Depending on the need, you might decide to develop a new Add-in that replaces, rather than upgrades, the original Add-in. If this is the case, you will need to use the same friendly name and file name of the package, but have a different product ID in the manifest. This will allow the Add-in to effectively replace the original in the catalog.

**IMPORTANT** The process of updating SharePoint Add-ins obviously is a lot more involved than we've covered here, with nuances such as update schedules, migrated data, modified functionality, and so on. For a clearer understanding of the process, review the MSDN article "SharePoint Add-ins update process" at <https://msdn.microsoft.com/library/fp179904.aspx>.

## Summary

---

- The upgrade path to SharePoint Server 2016 uses the database attach method.
- The Test-SPContentDatabase indicates (but does not correct) issues with content databases.
- All content databases to be migrated must be first upgraded to a minimum level of 15.0.4481.1005, or Service Pack 1 and the March 2013 PU to be upgraded to SharePoint 2016. If the SharePoint 2013 farm was initially created with the combination SharePoint 2013 and Service Pack 1 media, then the farm is already at this version level.
- A correctly upgraded configuration database does not necessarily indicate that all the surrounding content databases are successfully upgraded.
- All SharePoint 2010 site collections in the SharePoint 2013 farm must be upgraded to 2013 site collections prior to the SharePoint 2016 upgrade process.
- Web Applications need to be upgraded from classic- to claims-aware authentication, as classic mode is no longer supported in SharePoint 2016.
- Consider making some content read-only and migrating content to expand migration scheduling opportunities.

- The installation sequence for a new SharePoint 2016 farm should begin at the data tier and work out, in accordance with MinRole guidance.
- Content can be migrated from SharePoint on-premises to SharePoint Online by using a Microsoft FastTrack partner, the SharePoint Online Migration API, or Windows PowerShell cmdlets. If you have a significant body of content (more than 10 TB), consider shipping the disk media to Microsoft for upload to your tenancy.
- Although you can create the App Management service application from Central Administration, you'll still have to create the Subscription Settings service application from PowerShell. You might as well build both at the same time from PowerShell.
- Building new service applications in a MinRole-compliant SharePoint 2016 farm does not require you to start the individual services (as you would have in 2013); the farm will start these for you.
- The App Catalog should live in its own DNS space, not in a subdomain or subsites or managed path because that introduces security issues. The FQDN is used with the app hash to create a unique URL.
- Office Online Server is an on-premises server, despite the name; it replaces the Office Web Apps Server in a SharePoint 2016 farm.
- SharePoint Insights and SharePoint Telemetry provide the ability to view on-premises server events and performance and user metrics from Office 365.
- BCS models are XML-based, and can represent four distinct data sources: Windows Communication Foundation, SQL Server, SQL Azure, and OData sources (including SQL OData sources).
- BCS supports three different authentication methods: Credentials-based authentication, Claims-based authentication, and Custom authentication.
- Hybrid BCS has four prerequisites: that all user accounts are federated, that there is a service account for the OData service endpoint, that there is a global security group in the on-premises domain, and that the federated accounts be added to the global security group.
- Apps (Add-ins) are available for deployment from three locations: a list of previously available Add-ins, from the Add-in Catalog, or from the Office Store.
- As is the case with solutions, Add-ins can be added from PowerShell.
- Add-ins can be either updated or migrated, depending on their complexity.

## Thought experiment

---

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find the answer to this thought experiment in the next section.

You are designing a migration plan for moving from SharePoint Server 2013 to a hybrid SharePoint 2016 and SharePoint Online environment. The adoption of the previous

environment was quite successful, and code-based customizations to the farm were fairly common. This environment has been in use since 2010, having been upgraded in 2013.

1. How would you approach the initial assessment of the SharePoint 2013 environment, particularly from a code standpoint?
2. What changes will be required from a productivity services standpoint to move the farm into the new hybrid configuration?
3. Management states that they cannot sustain an extended outage. How would you go about completing an upgrade?

## Thought experiment answer

---

This section contains the solution to the thought experiment.

1. It's likely that you will have a combination of code and solutions in this farm. Document both the user solutions (sandboxed) and farm solutions as they exist today (including compatibility version), also capturing the Apps (now Add-ins) that were previously deployed. Work with the development team to determine which solutions and apps are no longer in use, then provide a window of time required to update earlier versions of solutions (if possible). Document the solutions that cannot (or will not) be updated, so they can be installed in a previous compatibility mode.
2. On the whole, most of the productivity services will successfully make the transition between SharePoint 2013 and SharePoint 2016. Create a new Office Online Server, and then work with your user base to determine which Excel Calculation Services components should be replaced by the Office Online Services farm. Remove any other Excel Calculation Services components, as the service is unavailable in SharePoint 2016. Capture the settings of the other Office-based services, such as Visio, Word Automation, and others, for migration to the new environment.
3. Work with management to understand which components of the environment can be down for extended periods (if available). Consider planning a parallel upgrade for certain components of the farm, and then work with the user stakeholders to schedule a freeze, during which they can still access content from the SharePoint 2013 environment, but not write or make changes (this includes workflows). Test the migration for each series of content databases, working with the SQL team to temporarily optimize components in the data layer to handle the upgrade of more than one content database at a time.

# Index

## A

- AAD Connect mechanism, 198
- AADSync tool set, 91
- AAM (alternate access mappings)
  - about, 31
  - configuring, 152–153
  - planning, 36–37
- Access Request Settings page, 99, 138
- Access Services 2010, 56, 253
- Access Services 2010 (Microsoft), 56, 253
- Access Services (Microsoft)
  - about, 56–57, 251, 253–254
  - Kerberos delegation, 117
- accessibility, document library, 16
- ACS (Azure Access Control Service), 86–87, 90, 270
- Active Directory Direct Import option, 131–133
- Active Directory Domain Administrator, 296
- Active Directory Domain Services (AD DS)
  - authentication support, 78
  - Office Online Server, 65
  - preparing configuration accounts, 54
  - UPA support, 136
  - Yammer settings, 198
- Active Directory Federation Services (AD FS), 86–87, 90, 92
- Active Directory Rights Management Services (AD RMS), 118–119
- activity feeds (microblogging), 196, 198–199
- AD DS (Active Directory Domain Services)
  - authentication support, 78
  - Office Online Server, 65
  - preparing configuration accounts, 54
  - UPA support, 136
  - Yammer settings, 198
- AD FS (Active Directory Federation Services), 86–87, 90, 92
- AD RMS (Active Directory Rights Management Services), 118–119
- Add Crawl Rule page, 290
- Add-in Catalog, 245, 247, 274–276
- Add-in model, 48, 243–247
- Add Network Library Configuration dialog box, 179
- Add New Synchronization Connection page, 132
- Add Query Rule page, 311
- Add-RoleGroupMember cmdlet, 358
- Add-SPDiagnosticsPerformanceCounter cmdlet, 402
- Add-SPServiceApplicationProxyGroupMember cmdlet, 300
- Add-SPShellAdmin cmdlet, 121, 190
- Add-SPSolution cmdlet, 273
- Administration database type, 281
- Administrators group, 190, 275
- ADOMD.NET, 343, 348
- ADSIEdit tool, 60, 62–63
- Advanced Encryption Standard (AES) encryption, 80
- AES (Advanced Encryption Standard) encryption, 80
- aliases
  - SQL, 178–180
  - wildcard, 244
- alternate access mappings (AAM)
  - about, 31
  - configuring, 152–153
  - planning, 36–37
- Analysis Services scorecard template, 342
- Analysis Services (SQL Server), 346–348, 351
- Analytic Chart report template, 341
- Analytic Grid report template, 341
- Analytics processing component (Search), 280, 336
- Analytics reporting database type, 281, 336
- anonymous access
  - planning and configuring, 101–107, 111
  - sites and site collections, 141–142
  - web applications, 30, 82, 101, 142

## Anonymous Access icon

- Anonymous Access icon, 102
- anonymous authentication, 81–82, 101
- Anonymous policy, 104, 106–107
- Antivirus page, 112–113
- antivirus settings, configuring, 111–113
- App Catalog, 245, 247–248, 270
- app management
  - about, 243–244, 249–250
  - app hosting models, 48
  - app-only policy, 141
  - App Store, 247–248
  - authentication, 77
  - configuration conflict issues, 233
  - deploying apps, 274–275
  - DNS entries, 244–245
  - marketplace connections, 248–250
  - permissions, 139–141
  - sandbox solution quotas, 271–272
  - subscriptions, 245–247
  - upgrading apps, 276
  - wildcard certificates, 245
- App Management service application, 245–246
- App Store, 247–248
- Application Discovery and Load Balancer Servicer, 60, 62
- Application Management page, 150, 164–166
- application pools
  - considerations for building, 28–29
  - isolation considerations, 110
  - limits guidance, 28
  - planning, 27–29
- Application Proxy feature, 87
- Application server role
  - about, 37–38
  - configuring installation prerequisites, 50–51
  - defining server requirements, 42
  - defining service topologies, 43–46
  - designing for resiliency, 399
  - installation sequence, 241
  - planning server load balancing, 46
  - search resiliency and, 281
  - service instance configuration, 173–174
  - zero downtime patching, 399
- ASP.NET, 126, 377, 394–396
- audiences
  - configuring, 68–69, 73
  - OneDrive redirection, 194
  - term sets, 23–24
- audit logs, 209
- auditing installations, 62–63
- auditing policy features, 17
- authentication
  - about, 77–78
  - Access Control Service, 90
  - anonymous, 81–82, 101
  - basic, 30, 79–80
  - BCS model security, 262–263
  - business intelligence, 352–353
  - claims-based, 30, 35, 56, 63, 85, 136–137, 229–230, 262
  - claims providers, 85–86
  - classic mode, 30, 35, 56, 80, 229–230
  - configuration conflict issues, 232
  - connection encryption, 82–85
  - crawl rules, 291
  - credentials-based, 262
  - custom, 263
  - digest, 79, 81
  - domain controllers and, 398
  - Forms-based, 30, 78, 82, 85–86
  - hybrid cloud deployments, 91–93
  - identity federation, 85–86
  - Kerberos, 78–80, 117–118, 353–354
  - negotiate, 78, 80, 117–118
  - NTLM, 78–79
  - OAuth, 68, 83, 87–89
  - server-to-server, 67–68, 83, 87–89
  - SQL Server, 30
  - thought experiment, 155
  - user, 77, 136
  - web application support, 29–30, 228–230
  - Windows, 30, 35, 56, 78–81
- authorization
  - anonymous access, 101–104
  - app policies, 141
  - BCS model security, 263
  - defined, 93
  - People Picker control, 95–97
  - permission inheritance, 100–101
  - SharePoint users and groups, 93–95
  - sharing, 97–101
  - web application policies, 104–107
- autogrowing content databases, 389
- Autohosted model, 48
- Automatic Password Change settings, 123–124
- Available MBytes performance counter, 372

Avg. Disk Queue Length performance counter, 372  
 Azure Access Control Service (ACS), 86–87, 90, 270  
 Azure AD, 68, 87, 91–93  
 Azure AD Connect tool, 91–93  
 Azure Infrastructure Services, 190–191  
 Azure Workflow Manager, 114, 235  
 Azure Workflow Service, 83

## B

Background Intelligent Transfer Service (BITS), 47

backup and restore

- about, 184
- configuring recovery solution, 190–191
- content recovery, 188–190
- establishing backup schedule, 185–186
- farm configuration recovery, 187
- nonproduction environment content refresh, 186–187
- service application recovery, 187–188

backward compatibility

- Access Services 2010, 56, 253
- alternate access mappings, 152
- class mode authentication, 80
- content deployment, 203
- deploying farm solutions, 273–274
- in-place upgrade method, 400
- labeling policy feature, 18
- Online Web Part Gallery, 127
- SQL AlwaysOn Mirroring, 172
- zero downtime patching, 399–400

bandwidth and network latency, 47

bar code policy feature, 17

baseline performance, 401–402

basic authentication, 30, 79–80

BCS (Business Connectivity Services)

- configuration conflict issues, 232–233
- configuring for search, 269
- configuring hybrid, 269–270
- configuring security, 262–263
- external content types, 8–9, 197
- importing and configuring models, 260–262
- monitoring considerations, 410
- UPA support, 134

BCS Connector Framework, 287

BI (business intelligence)

- about, 339

- authentication mechanisms, 352–353

- Excel Online, 351

- Excel Services, 350–351

- Kerberos delegation, 353–354

- PerformancePoint, 340–344

- Power Pivot, 345–350

- Power View, 351–352

- security considerations, 352–354

- SQL Server Reporting Services, 344–345

bidirectional hybrid, 71

Binary Large Object (BLOB)

- antivirus software and, 111, 113

- BLOB cache, 396–397

- cache counters, 376

BitLocker encryption, 242

BITS (Background Intelligent Transfer Service), 47

Blank Scorecard scorecard template, 342

BLOB (Binary Large Object)

- antivirus software and, 111, 113

- BLOB cache, 396–397

- cache counters, 376

blocked file types, 125–126

Blocked File Types page, 125

boundaries, software. *See* software boundaries and limits

built-in query rules, 13

Business Connectivity Services (BCS)

- configuration conflict issues, 232–233

- configuring for search, 269

- configuring hybrid, 269–270

- configuring security, 262–263

- external content types, 8–9, 197

- importing and configuring models, 260–262

- monitoring considerations, 410

- UPA support, 134

Business Data Actions Web Part, 8

Business Data Connectivity Filter Web Part, 8

Business Data Connectivity Services service application, 117

Business Data Item Builder Web Part, 8

Business Data Item Web Part, 8

Business Data List Web Part, 8

Business Data Related List Web Part, 8

business intelligence (BI)

- authentication mechanisms, 352–353

- Excel Online, 351

- Excel Services, 350–351

- Kerberos delegation, 353–354

## Business Intelligence Center

- PerformancePoint, 340–344
- Power Pivot, 345–350
- Power View, 351–352
- security considerations, 352–354
- SQL Server Reporting Services, 344–345
- Business Intelligence Center
  - about, 340
  - PerformancePoint Content library, 340–341
  - reports and scorecards, 340
- business services integration, 197

## C

- c2WTS (Claims to Windows Token Service), 351, 354
- caching mechanisms, 375–376, 393–398
- Canonical Name (CNAME) record, 244
- cascading style sheets (CSS), 199–200
- catalog item pages, 202, 324
- Categories page, 318–319
- category pages, 202, 324
- Central Administration deployment design, 38
- certificate management
  - about, 113–114
  - establishing trust, 115–116
  - exporting root certificates, 114–115
  - exporting STS certificates, 115
  - trust creation, 114
  - wildcard certificates, 245
- channels (WCM), 199–200
- claims-based authentication
  - about, 30
  - BCS model, 262
  - converting from classic mode, 229–230
  - host-header site collections, 35
  - identity federation, 85
  - UPA support, 136–137
  - web applications, 56, 63
- claims providers, 85–86
- Claims to Windows Token Service (c2WTS), 351, 354
- classic hybrid search. *See* hybrid federated search
- classic mode authentication
  - about, 30
  - backward compatibility, 80
  - converting to claims-mode, 229–230
  - host-header site collections, 35
  - web applications, 56
- CLICONFG (SQL Server Client Network Utility), 178–179
- client-side tracing, 402–404
- closed communities, 192
- closed term sets, 23
- cloud hybrid search
  - about, 69–71, 295, 358
  - configuring, 297–298
  - preparing for, 295–297
- Cloud Search service application, 359–361
- cloud services
  - business intelligence infrastructure, 339–354
  - hybrid federated search, 358–361
  - thought experiment, 362
  - work management, 354–358
- CNAME (Canonical Name) record, 244
- co-authoring (collaboration), 209–210
- COD (critical on-demand) hotfixes, 57
- Code 39 standard, 17
- Cold Standby Recovery, 175, 191
- collaboration (co-authoring), 209–210
- collaborative large list or library, 214
- communities (social networking), 191–192
- Compliance Policy Center, 19, 217–218
- configuration conflicts, 232–233
- configuration-only backups, 185
- Configure App URLs page, 247
- Configure-EnterprisePartnerApplication.ps1 PowerShell script, 89, 206, 355
- Configure Service Application Associations page, 250
- Configure Usage And Health Data Collection page, 402
- Configuring Microsoft SharePoint Hybrid Capabilities*, 270
- Connect To Catalog page, 325
- connection encryption, 82–85
- Connector (Windows service), 87
- Container class, 61
- content access accounts, 293–295
- content databases
  - analyzing test results, 226–228
  - autogrowing, 389
  - boundary considerations, 32–33
  - evaluating existing, 225
  - maintenance rules, 390–391
  - migration strategies, 236
  - monitoring, 382
  - performance considerations, 390
  - pregrowing, 388
  - recovering content from, 189–190
  - scaling implementations, 33–34

- Site Master, 36
  - storage evaluation, 239
  - version status, 226–228
- Content Deployment Source feature, 203–204
- Content Farm (farm type), 38
- content management
  - about, 224–225
  - backward compatibility, 203
  - configuration conflict issues, 232–233
  - content database test results, 226–228
  - content deployment, 203–204
  - content recovery, 188–190
  - disaster recovery, 203
  - migration precheck tasks, 224–226
  - missing file system components, 231–232
  - nonproduction environment content refresh, 186–187
  - orphaned objects, 230–231
  - web application authentication, 228–230
- Content Organizer feature, 209
- Content Processing Activity report, 293
- Content processing component (Search), 280
- Content Search Web Part, 213, 312–313
- content sources, 286–289
- Content Type Hub timer job, 303
- content type hubs, 7–8, 301–302
- Content Type Publishing page, 301–302
- Content Type Subscriber timer job, 8, 303–304
- content types
  - about, 6
  - external, 8–9, 197, 261–262
  - hierarchy, 7
  - information management policies, 18
  - large document repositories, 213
  - propagation schedules, 303–304
  - publishing, 301–302
  - unpublishing, 302
- Continuous Crawl report, 293
- continuous crawls, 289, 333
- Contribute permission level, 144–146
- Contributor permissions, 93, 95
- Contributors role, 305–306
- Control templates, 312
- CPU and Memory Load report, 293
- Crawl component (Search), 280
- Crawl database type, 281
- Crawl Freshness report, 293
- crawl health reports, 293

- Crawl Latency report, 293
- crawl performance, 291–293, 333
- Crawl Queue report, 293
- Crawl Rate report, 293
- crawl rules, 290–291
- crawl schedules, 287–288
- crawled properties, 14–15, 317–319, 335
- Crawler Impact Rule, 292, 333
- Create A Folder page, 98–99
- Create All Child Object permission, 60
- Create and Share, 98–99
- Create New Data Collector Set page, 372
- Create Personal Site social permission, 194
- CreateCloudSSA.ps1 PowerShell script, 70–71, 296
- Creating New Secure Store Target Application page, 266–267
- credentials-based authentication, 262
- critical on-demand (COD) hotfixes, 57
- Cross-Site Collection Publishing feature, 324
- CSS (cascading style sheets), 199–200
- .csv files, 404
- current navigation (sites), 3
- current schema version, 227–228
- custom authentication, 263
- custom properties, 304–305, 326–327
- Custom Repository content source type, 287
- Custom server role
  - about, 37–38
  - defining service topologies, 44, 46
  - service instance configuration, 174
- custom zone, 36

## D

- DAS (direct-attached storage), 38–39, 385
- Dashboard Designer tool, 340–342
- data collector sets, 370–375
- data isolation, 110
- data loss prevention (DLP) policies, 19–20, 217
- data loss prevention (DLP) queries, 19, 109, 216
- dbcreator SQL fixed server role, 54
- db\_owner fixed database role, 190, 237
- Decomposition Tree report template, 342
- dedicated deployment mode (request management), 41
- default zone, 36
- Defined Managed Paths page, 149–150
- delegated farm administration, 119–122

## delegated service application administration

- delegated service application administration, 122
- Delete Unique Permissions icon, 143–144
- Delve app, 319
- Design Manager, 202–204, 313
- Design permission level, 144
- Detailed Term Set Planning Worksheet (Excel), 24
- Developer Dashboard icon, 407
- Developer Dashboard tool, 407–408
- DHCP (Dynamic Host Configuration Protocol), 177
- Diagnostic Logging feature, 402
- diagnostic logs, 408–409
- Diagnostic Providers feature, 402
- digest authentication, 78, 81
- direct-attached storage (DAS), 38–39, 385
- directory service integration, 197
- DirSync tool, 91–93
- disaster recovery. *See also* backup and restore
  - content deployment, 203
  - failover database server, 31
  - login replication, 183–184
  - network redundancy, 176–177
  - physical server distribution, 174–176
  - server load balancing, 177–178
  - service distribution, 172–173
  - service instance configuration, 173–174
  - SQL Server aliases, 178–180
  - SQL Server AlwaysOn Availability Groups, 181
  - SQL Server clustering, 180–181
  - SQL Server Log Shipping, 182
  - storage redundancy, 182–183
- Discovery Management role group, 357–358
- Discovery Search Mailbox, 357
- display templates
  - associated with result types, 317
  - configuring, 204, 312–313
  - creating, 313–314
  - user search experience, 335
- DisplayLevel property, 407
- disposition of records, 211–213
- Distributed cache server role
  - about, 37–38, 235
  - defining server requirements, 42
  - defining service topologies, 43–46
  - designing for resiliency, 399
  - installation sequence, 241
  - planning server load balancing, 46
  - search resiliency and, 281
  - service instance configuration, 173–174
  - zero downtime patching, 399
- DLLs (dynamic-link libraries), 273
- DLP (data loss prevention) policies, 19–20, 217
- DLP (data loss prevention) queries, 19, 109, 216
- DNS (Domain Name System), 177, 244–245
- DNS zone, 244–245
- docID (resource ID), 15, 64, 211
- Document Fingerprinting, 20
- document library. *See* lists and libraries
- document management
  - co-authoring, 209–210
  - Content Organizer, 209
  - document deletion, 218–219
  - document library accessibility, 16
  - document movement considerations, 211
  - document routing, 208–209
  - large document repositories, 213–214
  - measuring upgrade performance, 240
  - Open Document Format, 26
  - record disposition and retention, 211–213
- Documentum content source type, 287
- Domain Name System (DNS), 177, 244–245
- Downtime metric, 365
- durable links, 15, 64, 211
- Dynamic Host Configuration Protocol (DHCP), 177
- dynamic-link libraries (DLLs), 273

## E

- EAC (Exchange Admin Center), 358
- ECM (Enterprise Content Management) workload
  - about, 205–206
  - co-authoring, 209–210
  - data loss prevention, 216–218
  - document deletion, 218–219
  - document routing, 208–209
  - durable links, 211
  - eDiscovery, 206–208
  - in-place holds, 218–219
  - large document repositories, 213–214
  - record disposition and retention, 211–213
  - software boundaries, 215
- eDiscovery Center
  - DLP queries, 19, 216
  - Exchange configuration, 355, 357–358
  - in-place holds, 218
  - planning and configuring, 206–208

- Edit Managed Metadata Service Connection page, 302–303
- Edit permission level, 144
- Edit Secure Store Target Application page, 268
- Edit User Profile page, 134–135
- email
  - Discovery Search Mailbox, 357–358
  - outgoing, 84–85, 98–99, 138
  - team mailbox, 168–169
  - warning, 165
- Enable-ProjectServerLicense cmdlet, 356
- Enable-SPWebTemplateForSiteMaster cmdlet, 36, 158–159
- encryption
  - AES, 80
  - BitLocker, 242
  - connection, 82–85
  - Kerberos protocol, 117
  - SMTP, 84–85
  - SSL, 80, 82–85
  - TLS, 82–85
- end-user experience, 334–335
- Enterprise Content Management (ECM) workload
  - about, 205–206
  - co-authoring, 209–210
  - data loss prevention, 216–218
  - document deletion, 218–219
  - document routing, 208–209
  - durable links, 211
  - eDiscovery, 206–208
  - in-place holds, 218–219
  - large document repositories, 213–214
  - record disposition and retention, 211–213
  - software boundaries, 215
- enterprise searches
  - content sources, 286–287
  - crawl performance, 291–293
  - crawl rules, 290–291
  - crawl schedules, 287–289
  - Enterprise Search Center, 334–335
  - hybrid searches, 295–298
  - Search topology, 280–286
  - security trimming, 293–295
- event logging, 378–379
- Event Viewer, 153, 404
- Excel Calculation Services, 64, 232
- Excel (Microsoft), 24, 345–350
- Excel Online, 350–352

- Excel Services, 64, 350–351
- Exchange
  - configuring connection, 355
  - eDiscovery support, 355, 357–358
  - network infrastructure, 47
  - Office Online Server, 63, 65
  - S2S authentication, 67–68, 87
  - sensitive information types, 19
  - server farm connections, 83–84
  - Skype for Business connectivity and, 206–207
- Exchange Admin Center (EAC), 358
- Exchange Management Shell, 358
- Exchange Public Folders content source type, 287
- Exchange Server 2016, 88–89
- Exchange Web Services API, 169
- ExchangeArchivingPolicy property, 207
- Execute permission, 119
- explicit managed paths, 21, 148
- Export-SPWeb cmdlet, 21
- Extensible Hybrid App Launcher, 74, 258–259
- external content types, 8–9, 197, 261–262
- external resource mappings, 153
- extranet zone, 36

## F

- faceted navigation, 321–322
- Failover Cluster Instance (FCI), 180
- failover database servers, 31
- Farm Administrator, 120, 122
- Farm Administrators group, 121–122, 131
- Farm Configuration Wizard, 284
- Fast Site Collection Creation, 35–36, 158–159
- FCI (Failover Cluster Instance), 180
- FCP (Fibre Channel Protocol), 39
- Feature Administrators, 122
- feature limits, 215
- Federated Users, 296
- federation providers (FPs), 86
- Fibre Channel, 39–40
- Fibre Channel Protocol (FCP), 39
- Fiddler tool, 410
- file management
  - blocked file types, 125–126
  - Content Organizer, 209
  - document library accessibility, 16
  - large file support, 47–48

## File Shares content source type

- missing file system components, 231–232
- File Shares content source type, 287
- FIM (Forefront Identity Manager), 133, 233
- fine-grained permissions, 101
- Fixed Values Scorecard scorecard template, 342
- folksonomy, 10, 22–23, 25
- Follow People and Edit Profile social permission, 194
- Forefront Identity Manager (FIM), 133, 233
- Forms-based authentication
  - about, 30
  - identity federation, 85–86
  - IIS websites, 82
  - web applications, 78
- forward lookup zone, 245
- FPs (federation providers), 86
- FQDN (Fully Qualified Domain Name), 132, 159, 248
- Front-end server role
  - about, 37–38
  - defining server requirements, 42
  - defining service topologies, 43–46
  - designing for resiliency, 399
  - installation sequence, 241
  - planning server load balancing, 46
  - search resiliency and, 281
  - service instance configuration, 173–174
  - virus scanning software, 113
  - zero downtime patching, 399
- Full Control permission level, 95, 140, 144–145
- full crawls, 288–289, 333
- Full Read permissions, 295
- Fully Qualified Domain Name (FQDN), 132, 159, 248
- functional navigation (sites), 4

## G

- Get-PfxCertificate cmdlet, 116
- Get-SPBusinessDataCatalogMetadataObject cmdlet, 261
- Get-SPCertificateAuthority cmdlet, 114–115
- Get-SPContentDatabase cmdlet, 230, 382–383
- Get-SPDatabase cmdlet, 382
- Get-SPEnterpriseSearchCrawlContentSource cmdlet, 289
- Get-SPEnterpriseSearchServiceApplication cmdlet, 286, 289
- Get-SPEnterpriseSearchServiceInstance cmdlet, 285
- Get-SPEnterpriseSearchStatus cmdlet, 283
- Get-SPFarmConfig cmdlet, 61, 63

- Get-SPIRMSettings cmdlet, 119
- Get-SPLogEvent cmdlet, 366
- Get-SPSecurityTokenServiceConfig cmdlet, 115
- Get-SPServiceApplicationProxy cmdlet, 300
- Get-SPSite cmdlet, 228, 383
- Get-SPSiteSubscriptionIRMConfig cmdlet, 119
- Get-SPTopologyServiceApplication cmdlet, 62
- Get-SPTtrustedRootAuthority cmdlet, 116
- Get-SPWebApplication cmdlet, 96, 150–151
- Global Administrator, 296
- global navigation (sites), 3
- global term sets, 23–24
- Goßner, Stefan, 399
- Group Managers role, 305–306

## H

- HA (high availability)
  - failover database server, 31
  - login replication, 183–184
  - network redundancy, 176–177
  - physical server distribution, 174–176
  - server load balancing, 177–178
  - service distribution, 172–173
  - service instance configuration, 173–174
  - SQL Server aliases, 178–180
  - SQL Server AlwaysOn Availability Groups, 181
  - SQL Server clustering, 180–181
  - SQL Server Log Shipping, 182
  - storage redundancy, 182–183
- Health Analyzer
  - about, 366
  - classic-mode authentication, 229
  - content databases, 33, 390–391
  - Database rule, 390
  - implementing rules, 390–391
  - orphaned objects, 230, 400
- health reports
  - crawl, 293
  - usage and health providers, 377–384
- HHSC (Host-Header Site Collections)
  - alternate access mappings and, 37
  - configuring, 159–161
  - managed paths, 148–149
  - planning, 34–35
  - self-service site creation, 162
- hierarchy limits, 215

- high availability (HA)
  - failover database server, 31
  - login replication, 183–184
  - network redundancy, 176–177
  - physical server distribution, 174–176
  - server load balancing, 177–178
  - service distribution, 172–173
  - service instance configuration, 173–174
  - SQL Server aliases, 178–180
  - SQL Server AlwaysOn Availability Groups, 181
  - SQL Server clustering, 180–181
  - SQL Server Log Shipping, 182
  - storage redundancy, 182–183
- High-Performance Mode, 176
- Host-Header Site Collections (HHSC)
  - alternate access mappings and, 37
  - configuring, 159–161
  - managed paths, 148–149
  - planning, 34–35
  - self-service site creation, 162
- Hot Standby Recovery, 175, 190
- HTML field security, 147
- HTML5, 26
- HTTP/HTTPS, 68, 83, 87
- HTTP request throttling, 41
- hybrid BCS, 269–270
- hybrid cloud environment
  - audiences and hybrid features, 68–74
  - authentication, 67–68, 91–93
  - configuring settings, 66
  - monitoring deployments, 384
  - OAuth, 68
  - Office Online deployment, 67
  - troubleshooting issues, 409–411
- hybrid features
  - configuring, 69
  - Hybrid Picker tools, 72–73
  - OneDrive for Business, 72–74, 130–131
  - Search configurations, 69–72
  - Team Sites, 74
- hybrid federated search, 69, 71–72, 358–361
- Hybrid OneDrive for Business, 72–74, 130–131, 193–194
- Hybrid Picker tool set, 72–73
- Hybrid SharePoint Sites (Team Sites), 3, 74
- IaaS (Infrastructure as a Service), 356
- IDE (integrated drive electronics), 40
- identity federation, 85–86
- Identity Provider Security Token Service (IP-STs), 86
- identity providers (IdPs), 86
- IdPs (identity providers), 86
- IIS (Internet Information Services)
  - basic authentication and, 79–80
  - host header site collections, 159
  - logical design and, 27
  - site mailboxes, 169
  - wildcard certificates, 245
- IIS Manager, 27
- images, quick previews, 16
- Import-Module OfficeWebApps cmdlet, 347
- Import-SPAppPackage cmdlet, 275
- Import-SPBusinessDataCatalogModel cmdlet, 261
- Import-SPEnterpriseSearchThesaurus cmdlet, 12
- Import-SPWeb PowerShell cmdlet, 21
- In-Place Hold Policy Center, 218–219
- in-place holds, 218–219
- inbound hybrid, 71–72
- incremental crawls, 289, 333
- Index component (Search), 280
- index freshness, 332–333
- individual permissions, 94
- InfoPath Form Services service application, 117
- information architecture
  - compliance features, 19–20
  - content types, 6–9
  - document library accessibility, 16
  - durable links, 15
  - information management policies, 16–18
  - intersite navigational taxonomy, 2–4
  - keywords, 9–11
  - managed properties, 14–15
  - managed site structures, 20–22
  - mobile navigation, 26–27
  - Open Document Format, 26
  - Promoted Results, 13–14
  - searches for sensitive and nonsensitive content, 19
  - site columns, 4–6
  - synonyms, 11–12
  - term sets, 22–26
- information management policies
  - assigning, 18
  - auditing, 17

## Information Rights Management (IRM)

- bar code, 17
- creating new, 18
- disabling, 18
- labeling, 18
- planning, 16–18
- retention, 17
- Information Rights Management (IRM)
  - configuration-only backups, 185
  - data loss prevention, 20
  - Office Online Server, 64
  - physical isolation, 109
  - planning and configuring, 118–119
- Information Rights Management Services, 20
- information types
  - defined, 5
  - site columns, 6
- Infrastructure as a Service (IaaS), 356
- infrastructure design
  - hybrid cloud environment, 66–74
  - information architecture, 1–27
  - installation planning, 49–66
  - logical architecture, 27–37
  - physical architecture, 37–49
  - thought experiment, 75–76
- inheritance
  - permission, 100–101, 142–144
  - site columns, 5
- Initialize-SPResourceSecurity cmdlet, 56
- input/output operations per second (IOPS), 39, 392–393
- Install-SPApp cmdlet, 275
- Install-SPApplicationContent cmdlet, 56
- Install-SPFeature cmdlet, 56
- Install-SPHelpCollection cmdlet, 56
- Install-SPService cmdlet, 56
- Install-SPSolution cmdlet, 273–274
- installation planning
  - Access Services deployment, 56–57
  - installation prerequisites, 49–52
  - installation tracking and auditing, 62–63
  - language packs, 58–59
  - Office 365 migrations, 65–66
  - Office Online Server, 63–65
  - patch slipstreaming, 57–58
  - scripted deployment, 53–56
  - service connection points, 60–62
  - upgrade processes, 241
- integrated deployment mode (request management), 41

- integrated drive electronics (IDE), 40
- internal URLs, 36, 152
- Internet Information Services (IIS)
  - basic authentication and, 79–80
  - host header site collections, 159
  - logical design and, 27
  - site mailboxes, 169
  - wildcard certificates, 245
- Internet service providers (ISPs), 28
- Internet zone, 36
- interserver communication, 47
- intersite navigational taxonomy
  - about, 2–3
  - current navigation, 3
  - functional navigation, 4
  - global navigation, 3
  - organizational chart navigation, 4
  - scalability issues, 3
- intranet zone, 36
- IOPS (input/output operations per second), 39, 392–393
- IP-STS (Identity Provider Security Token Service), 86
- IRM (Information Rights Management)
  - configuration-only backups, 185
  - data loss prevention, 20
  - Office Online Server, 64
  - physical isolation, 109
  - planning and configuring, 118–119
- isolation
  - application pools, 110
  - data, 110
  - physical, 109
  - security requirements, 108–109
  - service application, 109
  - web application zones, 110
  - web applications, 110
- ISPs (Internet service providers), 28
- Item templates, 312

## J

- JavaScript Object Notation (JSON), 88–89, 355
- JBOD (just a bunch of disks), 40
- .js files, 204
- JSON (JavaScript Object Notation), 88–89, 355
- just a bunch of disks (JBOD), 40

**K**

KCD (Kerberos constrained delegation), 117–118, 353–354

KDC (Key Distribution Center), 80

Kerberos authentication, 78–80, 117–118, 353–354

Kerberos constrained delegation (KCD), 117–118, 353–354

Key Distribution Center (KDC), 80

key performance indicators (KPIs), 340

keyword metadata, 9

Keyword Query Language (KQL), 207

keyword set, 9

keywords

- adding to document library, 10–11
- default storage location, 9
- transforming into terms, 10–11

KPI Details report template, 341

KPIs (key performance indicators), 340

KQL (Keyword Query Language), 207

**L**

labeling policy feature, 17

language considerations

- language packs, 58–59
- variation labels, 205

large-scale archive, 214

latency and bandwidth, 47, 240

LDAP (Lightweight Directory Access Protocol), 63, 131

libraries. *See* lists and libraries

Lightweight Directory Access Protocol (LDAP), 63, 131

Limited Access permission level, 144–145

Limited-Access User Permission Lockdown Mode feature, 111

Line-of-Business Data content source type, 287

Link database type, 281, 336

list columns, 4–5

list-level searches, 334

list permission level, 94, 145

list refinement, 330

lists and libraries

- about, 2
- access requests, 99–100
- anonymous access, 103–107, 111, 141
- app hosting model, 48
- collaborative large list or library, 214

- configuring refinement, 330
- content deployment, 203
- Content Organizer, 209
- content types, 6–8
- designing accessibility, 16
- hierarchy limits, 215
- information management policies, 18
- keywords, 10–11
- managed properties, 14
- managed site structures, 20
- measuring upgrade performance, 240
- object cache, 397
- orphaned objects, 230
- People Picker control, 95
- permission inheritance, 100–102, 142, 144–145
- permission levels, 94, 140–141
- product catalogs, 200–201, 325
- refining, 330
- search interfaces, 334
- software boundaries, 391
- storage considerations, 213–214
- term sets, 22–23

load balancing

- alternate access mappings, 153
- configuration conflict issues, 233
- configuring request management, 40–41
- planning, 46, 177–178

local properties, 326

local term sets, 23–24

Log Parser tool, 410

logging database, 380–381

logging events, 378–379

logical architecture

- application pools, 27–29
- content databases, 32–34
- Fast Site Collection Creation, 35–36
- host-header site collections, 34–35, 37
- software boundaries, 31–32
- web applications, 29–31
- zones and access mapping, 36–37

login replication, 183–184

Lotus Notes content source type, 287

**M**

Manage Catalog Connection page, 325

Manage Catalog Connections page, 325

## Manage Content Database Settings page

- Manage Content Database Settings page, 227–228
- Manage Databases Upgrade Status page, 227
- Manage Parent icon, 142
- Manage permission level, 140
- Manage Permissions page, 102–104
- Manage Query Rules page, 311
- Manage The Promoted Sites Below dialog box, 171
- Manage User Properties page, 135
- managed accounts, 123–124
- Managed Metadata Service Connection, 302–303
- Managed Metadata Service (MMS)
  - about, 298
  - content type hub settings, 301–302
  - content type propagation schedules, 303–304
  - content types, 7–8
  - custom properties, 304–305
  - hybrid configurations, 69
  - import files, 307
  - keywords, 9
  - metadata-based navigation, 22
  - product catalogs, 201
  - sharing term sets, 302–303
  - term sets, 22–26
  - term store permissions, 305–306
- Managed Metadata term store, 10
- managed paths
  - creating, 148–151
    - Office 365 migrations, 65–66
    - path-based navigation, 21–22
    - removing, 150–152
- managed properties, 14–15, 317–319, 335
- marketplace connections, 248–250
- Master Page Gallery, 312–313, 317
- master pages, 202–204, 325
- MAXDOP (maximum degree of parallelism), 53–54
- maximum degree of parallelism (MAXDOP), 53–54
- maximum schema version, 227–228
- MD5 checksum (digest), 79, 81
- Members group, 93, 95, 143
- metadata
  - external content types, 8
  - keyword, 9
  - list columns, 4–5
  - planning communities, 192
  - site columns, 5
  - terms and term sets, 22–26
- metadata-based navigation, 22
- microblogging (activity feeds), 196, 198–199
- Microsoft Access Services
  - about, 56–57, 251, 253–254
  - Kerberos delegation, 117
- Microsoft Access Services 2010, 56, 253
- Microsoft Excel, 24, 345–350
- Microsoft FastTrack service, 242
- Microsoft Identity Manager (MIM)
  - configuration conflict issues, 233
  - creating connections, 196
  - directory service integration, 197
  - planning and configuring sync connections, 131–134
- Microsoft Network Monitor, 410
- Microsoft OLE DB Provider for Analysis Services (MSOLAP), 348
- Microsoft OneNote, 210
- Microsoft PowerPoint Conversion Services, 251, 257
- Microsoft Project Server 2016, 355–356
- Microsoft Translation Services, 251
- Microsoft Visio Services, 117, 251, 254–255
- Microsoft Word Automation Services, 251, 255–256
- migration precheck tasks
  - documenting existing farm, 224
  - evaluating content databases, 225–226
  - evaluating existing farm, 225
- MIM (Microsoft Identity Manager)
  - configuration conflict issues, 233
  - creating connections, 196
  - directory service integration, 197
  - planning and configuring sync connections, 131–134
- MIM Synchronization Service Manager, 133
- MinRole server roles
  - about, 37–38
  - defining server requirements, 41–43
  - defining service topologies, 43–46
  - designing for resiliency, 399
  - installation sequence, 241
  - planning server load balancing, 46
  - search resiliency, 281–282
  - service instance configuration, 173–174
  - zero downtime patching, 399
- missing file system components, 231–232
- MMS (Managed Metadata Service)
  - about, 298
  - content type hub settings, 301–302
  - content type propagation schedules, 303–304
  - content types, 7–8
  - custom properties, 304–305
  - hybrid configurations, 69
  - import files, 307

- keywords, 9
- managed service applications, 299–301
- metadata-based navigation, 22
- product catalogs, 201
- sharing term sets, 302–303
- term sets, 22–26
- term store permissions, 305–306
- mobile navigation, 26–27
- monitoring SharePoint environment
  - about, 363–364
  - baseline performance, 401–402
  - crawl performance, 291–293, 333
  - defining requirements, 364–368
  - hybrid cloud deployments, 384
  - key performance indicators, 340
  - monitoring levels, 365
  - monitoring tools, 365–368
  - network performance, 398
  - page performance monitoring, 375–377
  - performance counter capture, 368–375
  - RAM usage, 29
  - service guarantee metric, 364–365
  - thought experiment, 412–413
  - for upgrades, 238–241
  - usage and health providers, 377–384
- Monthly Uptime Percentage metric, 365
- MSOLAP (Microsoft OLE DB Provider for Analysis Services), 348
- My Sites, 131, 193

## N

- NAS (network-attached storage)
  - about, 38–39
  - Remote Blob Storage support, 385
  - storage redundancy, 183
  - upgrades and, 236
- navigation (sites)
  - about, 2–3
  - current, 3
  - eDiscovery, 207–208
  - faceted, 321–322
  - functional, 4
  - global, 3
  - metadata-based, 22
  - mobile, 26–27
  - organizational chart, 4
  - path-based, 21–22
  - scalability issues, 3
  - site, 321–322
- negotiate authentication, 78, 80, 117–118
- NetBIOS name, 285
- network-attached storage (NAS)
  - about, 38–39
  - Remote Blob Storage support, 385
  - storage redundancy, 183
  - upgrades and, 236
- network infrastructure, 46
- network interface cards (NICs), 177
- network latency, 47, 240
- Network Load Balancing feature, 177–178
- network performance, 398
- network redundancy, 176–177
- network resiliency, 177
- New-CSPartnerApplication cmdlet, 206
- New-OfficeWebAppsFarm cmdlet, 252
- New-SPCentralAdministration cmdlet, 56
- New-SPConfigurationDatabase cmdlet, 55
- New-SPEnterpriseSearchAdminComponent cmdlet, 286
- New-SPEnterpriseSearchAnalyticsProcessingComponent cmdlet, 286
- New-SPEnterpriseSearchContentProcessingComponent cmdlet, 286
- New-SPEnterpriseSearchCrawlComponent cmdlet, 286
- New-SPEnterpriseSearchIndexComponent cmdlet, 286
- New-SPEnterpriseSearchQueryProcessingComponent cmdlet, 286
- New-SPEnterpriseSearchTopology cmdlet, 286
- New-SPManagedPath cmdlet, 149, 151–152
- New-SPPerformancePointServiceApplication cmdlet, 343
- New-SPProfileServiceApplication cmdlet, 129
- New-SPProfileServiceApplicationProxy cmdlet, 129
- New-SPServiceApplicationProxyGroup cmdlet, 299
- New-SPSite cmdlet, 95, 158–159, 161
- New-SPSiteMaster cmdlet, 36, 158–159
- New-SPTrustedRootAuthority cmdlet, 116
- New-SPTrustedSecurityTokenIssuer cmdlet, 88, 357
- New-SPWeb cmdlet, 95
- New-SPWebApplication cmdlet, 35, 161
- New-SPWOPIBinding cmdlet, 252
- NICs (network interface cards), 177
- nonproduction environment content refresh, 186–187
- NT LAN Manager (NTLM) authentication, 78–79
- NTLM authentication, 78–79

## OAuth (Open Authorization)

### O

- OAuth (Open Authorization)
  - configuring, 68
  - S2S connection, 83, 87–89
  - site mailboxes, 169
- object cache, 377, 397
- ODC (Office Data Connection), 310
- ODF (Open Document Format), 26
- Office 365
  - App Launcher feature, 74
  - hybrid cloud environment, 67–68
  - hybrid federated search, 359–360
  - managed paths for migrations, 65–66
  - Search index, 70
  - server farm connections, 83
  - uploading thesaurus files, 12
  - Yammer online functionality, 196–199
- Office 365 Global Administrator, 131
- Office Data Connection (ODC), 310
- Office Graph, 319
- Office Online, 67, 350–351
- Office Online Server
  - creating and configuring, 251–252
  - installing Analysis Services, 346–348
  - planning and installing, 63–65, 68
  - resource IDs, 15, 211
- Office Web Apps servers, 235
- Onboard-CloudHybridSearch.ps1 PowerShell script, 70–71, 296
- One-Click Sharing, 98
- one-way inbound topology, 360
- one-way outbound topology, 360
- OneDrive for Business
  - about, 72–74
  - hybrid, 72–74, 130–131, 193–194
  - with redirection, 194, 258
- OneNote (Microsoft), 210
- Online Viewers, 64
- Online Web Part Gallery, 127
- OOB Farm Configuration Wizard, 27
- Open Authorization (OAuth)
  - configuring, 68
  - S2S connection, 83, 87–89
  - site mailboxes, 169
- open communities, 192
- Open Document Format (ODF), 26
- open term sets, 23

- Open XML structure, 26
- Opportunistic TLS (STARTTLS), 84
- optimizing SharePoint environment
  - about, 384–385
  - caching strategy, 393–398
  - database maintenance rules, 390–391
  - estimating storage requirements, 392–393
  - network performance, 398
  - performance prioritization, 387–388
  - software boundaries, 391–392
  - SQL optimization, 385–390
  - Zero Downtime Patching, 398–400
- organizational chart navigation (sites), 4
- orphaned objects, 230–231, 400
- Out-GridView cmdlet, 366–367
- outbound hybrid, 71–72
- outgoing email, 84–85, 98–99, 138
- Owners group, 95, 143

### P

- page output cache, 394–396
- page performance monitoring, 375–377
- parallel upgrades, 236
- Password Sync (Azure AD Connect), 92
- patch slipstreaming, 57–58
- path-based navigation, 21–22
- path-based site collections (PBSC), 148–151, 159–160
- PBSC (path-based site collections), 148–151, 159–160
- People Picker control, 95–97
- Peoplepicker-activedirectorysearchtimeout property, 96
- Peoplepicker-distributionlistsearchdomains property, 96
- Peoplepicker-nowindowsaccountsforonwindows authenticationmode property, 96
- Peoplepicker-onlysearchwithinsitecollection property, 96
- Peoplepicker-peopleeditoronlyresolvewithinsitecollecti on property, 96
- Peoplepicker-searchadcustomfilter property, 96
- Peoplepicker-searchadcustomquery property, 96
- Peoplepicker-searchadforests property, 96
- Peoplepicker-serviceaccountdirectorypaths property, 96
- performance considerations. *See* monitoring SharePoint environment
- performance counters, 368–375

- Performance Monitor (Perfmon.exe), 29, 367–377
- PerformancePoint Services
  - about, 352
  - configuring, 343–344
  - Kerberos delegation, 117
  - report templates, 341–342
  - reports and scorecards, 340
  - scorecard templates, 342
- permission inheritance, 100–101, 142–144
- permission levels
  - about, 94
  - adding, 145–146
  - anonymous access and, 140–141
  - configuring, 144–146
- Permission Levels screen, 94
- Permission policy, 104–105
- permissions
  - anonymous access, 107
  - app, 139–141
  - co-authoring controls, 210
  - configuring levels, 144–146
  - crawl performance, 333
  - deleting unique, 143–144
  - fine-grained, 101
  - importing thesaurus files, 12
  - manipulating SCP containers, 60–61
  - OneDrive redirection, 194
  - Secure Store Target Application, 268–269
  - SharePoint users and groups, 93–95
  - sites and site collections, 137–141
  - social, 129–131, 194–195
  - term store, 305–306
  - UPA support, 129–131
- Permissions Level icon, 145
- personal permission level, 94, 145
- physical architecture
  - app hosting models, 48
  - CentralAdministration deployment, 38
  - large file support, 47–48
  - network infrastructure, 46
  - physical isolation, 109
  - request management, 40–41
  - server distribution planning, 174–176
  - server farm topology using MinRole, 37–38
  - server load balancing, 46
  - server requirements, 41–43
  - service topologies, 43–46
  - storage architecture, 38–40
- PID (Product ID), 355
- policies
  - app authorization, 141
  - Compliance Policy Center, 19, 217–218
  - data loss prevention, 19–20, 217
  - information management, 16–18
  - property, 195
  - site, 167–168, 212–213
  - web application authorization, 104–107
- Power Pivot, 345–350
- Power Pivot for SharePoint, 348–349
- Power View, 351–353
- PowerPoint Conversion Services (Microsoft), 251, 257
- PowerShell cmdlets. *See specific cmdlets*
- pregrowing content databases, 388
- Prerequisiteinstaller.exe file, 52
- prerequisites for installations, 49–52
- private communities, 192
- % Processor Time performance counter, 368–369, 372
- product catalogs, 200–201, 325
- Product ID (PID), 355
- productivity solutions
  - configuring app management, 243–250
  - configuring BCS, 260–270
  - configuring productivity services, 250–259
  - configuring Secure Store application, 260–270
  - evaluating content and customizations, 223–233
  - managing solutions and applications, 271–276
  - planning upgrade process, 233–243
  - productivity services, 250–259
  - removing, 232
  - thought experiment, 277–278
- Profile database (UPA), 128
- Profile Pages, 261–262
- Promoted Results, 13
- propagation schedules, content types, 303–304
- properties
  - crawled, 14–15, 317–319, 335
  - custom, 304–305, 326–327
  - local, 326
  - managed, 14–15, 317–319, 335
  - policies for, 195
  - profile, 134–136
  - shared, 326
- Provider-hosted model, 48
- proxies
  - Application Proxy feature, 87
  - reverse, 86, 360

## proxy groups

- service applications, 31, 299–301
- proxy groups, 129, 299–301
- PSCConfig.exe file, 54–55
- public URLs, 36, 152
- Publishing Infrastructure feature, 20

## Q

queries

- data loss prevention, 19, 109, 216
- LDAP, 63
- user-specific, 360–361

Query processing component (Search), 280

query rules

- building, 13
- hybrid federated search, 71
- managing, 310–312
- search result rank, 332
- user search experience, 335

Quick Launch, 3

Quota Templates page, 165–166

quotas, site, 164–167, 193, 272

## R

RAID (redundant array of independent disks), 40, 182–183, 386–387

rank elevation, 331–332

RBS (Remote Blob Storage), 385

RBS (Remote BLOB Storage), 38–39

RDL (Report Definition Language), 310

Read-Only app permission level, 140, 236–237

Read permission, 61, 119, 144

Reader permissions, 93, 95

record disposition and retention, 211–213

recycle bins, 392

redundant array of independent disks (RAID), 40, 182–183, 386–387

Refiner Web Part, 327

ReFS (Resilient File System), 40

Remote Blob Storage (RBS), 385

Remote BLOB Storage (RBS), 38–39

Remote Connectivity Analyzer, 410

Remove-OfficeWebAppsHost cmdlet, 235

Remove-OfficeWebAppsMachine cmdlet, 235

Remove-SPCentralAdministration cmdlet, 38

Remove-SPManagedPath cmdlet, 151–152

Remove-SPServiceApplicationProxyGroupMember cmdlet, 300

Remove-SPSolution cmdlet, 232

Report Definition Language (RDL), 310

Reporting Services data source (RSDS) file, 353

Reporting Services report template, 341

reports

- audit log, 17
- health, 293
- PerformancePoint Services, 340–342
- search analytics, 336

repositories, large document, 213–214

Representational State Transfer (REST), 9, 64

request management, 40–41

Require Check Out feature, 210

Resilient File System (ReFS), 40

resource ID (docID), 15, 64, 211

REST (Representational State Transfer), 9, 64

Restore-SPFarm cmdlet, 189

result sources, 308–310, 333

result types, 316–317, 335

retention of records, 211–213

retention policy features, 17

reverse proxy, 86, 360

root certificates, 114–115

routing documents, 208–209

RSDS (Reporting Services data source) file, 353

## S

S2S (server-to-server) authentication, 67–68, 83, 87–89

S2S (server-to-server) trusts, 356–357

S2S (site-to-site) authentication, 77

SAML (Secure Application Markup Language)

- about, 30, 78, 228
- identity providers, 86

sandbox solution management

- backward compatibility, 271, 273–274
- configuring, 272
- deploying farm solutions, 273–274
- managing quotas, 271–272
- site quota templates, 165
- upgrading farm solutions, 274

SANs (storage area networks)

- about, 38–39, 385
- SQL Server clustering, 180

- storage redundancy and, 183
- upgrade process and, 236
- SAS (Serial Attached SCSI), 39–40
- SATA (Serial Attached ATA), 39–40
- Scheduled Downtime metric, 365
- schedules
  - backup, 185–186
  - content type propagation, 303–304
- scorecards, 342
- SCP containers, 60–61
- SCPs (service connection points), 60–63
- Script Editor Web Part, 199
- scriptable Web Parts, 127
- scripted deployment
  - configuring maximum degree of parallelism, 53–54
  - creating server farm, 54–56
  - developing installation script, 53
  - preparing configuration accounts, 54
- SCSI (small computer system interface), 39–40
- Search administration component (Search), 280
- Search Administration page, 284–285, 311
- search analytics reports, 336
- Search application
  - backing up, 185
  - BCS support, 269
  - changing topology, 284–286
  - cloud hybrid, 69–71, 295–298
  - components supported, 280
  - database types supported, 281
  - enterprise searches, 279–298
  - hybrid federated, 69, 71–72
  - managed properties, 14–15
  - managing, 307–319
  - managing taxonomy, 320–330
  - MMS application, 298–307
  - planning communities, 192
  - product catalogs, 201
  - Promoted Results, 13
  - search workload, 330–336
  - sensitive and nonsensitive content, 19
  - service application isolation, 109
  - service application recovery, 188
  - thought experiment, 337–338
  - viewing topology, 283
- Search Center (SharePoint Online), 70
- Search Engine Optimization (SEO), 314–316
- Search Engine Optimization Settings page, 315
- Search Farm (farm type), 38
- search management
  - about, 307
  - display templates, 312–314
  - enterprise searches, 279–298
  - federated search, 319
  - managing taxonomy, 320–330
  - MMS applications, 298–307
  - query rules, 310–312
  - result sources, 308–310
  - result types, 316–317
  - search schema, 317–319
  - search workload, 330–336
  - SEO settings, 314–316
  - thought experiment, 337–338
- search refiners, 327–329
- search relevancy, 331–332
- search schema, 317–319, 332, 335–336
- Search Schema page, 14
- search scopes, 308
- Search server role
  - about, 37–38, 234
  - defining server requirements, 42
  - defining service topologies, 45–46
  - designing for resiliency, 399
  - installation sequence, 241
  - planning server load balancing, 46
  - search resiliency, 282
  - service instance configuration, 173–174
  - zero downtime patching, 399
- Search Service Application Administrator permission, 12
- search verticals, 70
- Search Web Part, 204
- search workload
  - about, 330–331
  - end-user experience, 334–335
  - index freshness, 332–333
  - result sources, 333
  - search analytics reports, 336
  - search result relevancy, 331–332
  - search schema, 335–336
- Secure Application Markup Language (SAML)
  - about, 30, 78, 228
  - identity providers, 86
- Secure Sockets Layer (SSL)
  - about, 80
  - Add-in functionality, 245
  - certificate management, 114
  - connection encryption, 82–85

## Secure Store master key

- site mailboxes, 169
- Secure Store master key, 264–266
- Secure Store service
  - about, 188, 409
  - creating target applications, 266–267
  - managing application permissions, 268–269
  - Secure Store master key, 264–266
- Secure Store Target Application
  - creating, 266–267
  - managing permissions, 268–269
- security considerations
  - alternate access mappings, 152–153
  - antivirus settings, 111–113
  - BCS, 262–263
  - blocked file types, 125–126
  - business intelligence, 352–354
  - certificate management, 113–116
  - delegated farm administration, 120–122
  - delegated service application administration, 122
  - enterprise searches, 293–295
  - HTML field security, 147
  - Information Rights Management, 20, 64, 118–119
  - Kerberos protocol, 78, 80, 117–118
  - managed accounts, 123–124
  - managed paths, 148–152
  - security isolation, 108–110
  - services lockdown, 110–111
  - sites and site collections, 137–147
  - thought experiment, 155
  - UPA applications, 128–137
  - Web Parts, 126–127
- Security for Web Part Pages settings, 126–127
- security identifier (SID), 134, 136
- Security Token Service, 83
- security token service (STS) certificates, 114–115
- securityadmin fixed server role
  - delegated farm administration, 120
  - installing Add-ins, 275
  - preparing configuration accounts, 54
  - recovering content, 190
- Self-Service Site Collection Management page, 163
- self-service site collections, 162–163
- sensitive information, 19–20
- SEO Properties page, 316
- SEO (Search Engine Optimization), 314–316
- Serial Attached ATA (SATA), 39–40
- Serial Attached SCSI (SAS), 39–40

- server farms
  - antivirus settings, 111–113
  - basic request management, 40–41
  - certificate management, 113–116
  - configuration recovery planning, 187
  - configuring upgrade, 237–238
  - connecting to other systems, 83–85
  - creating via scripted deployment, 54–56
  - defining service topologies, 43–46
  - delegated administration, 120–122
  - deploying solutions, 273–274
  - designing storage architecture, 38–40
  - documenting existing, 224
  - evaluating existing, 225
  - hybrid cloud environment, 68
  - individual server requirements, 41–43
  - Kerberos protocol, 117–118
  - large file support, 47–48
  - load balancing, 46
  - managed paths, 65–66
  - MinRole concept, 37–38
  - monitoring levels, 365
  - network infrastructure, 47
  - registering in SCP container, 61
  - removal of servers in rotation, 233–235
  - S2S authentication, 88–89
  - search resiliency, 282
  - security isolation, 108–110
  - services lockdown, 110–111
  - stretched farms, 47, 175
  - upgrading solutions, 274
  - viewing SCPs, 62–63
  - web applications, 357
- Server Manager, 51
- server-side tracing, 404
- server-to-server (S2S) authentication, 67–68, 83, 87–89
- server-to-server (S2S) trusts, 356–357
- ServerCertification.aspx page, 119
- Servers In Farm page, 227, 282
- Service Application Administrators, 122, 131
- service applications
  - Access Services, 56–57, 253
  - delegated administration, 122
  - estimating storage, 393
  - isolation considerations, 109
  - Kerberos support, 117–118
  - monitoring levels, 365
  - proxy support, 31, 299–301

- query rules, 311
- recovery planning, 187–188
- UPA, 128–137
- service connection points (SCPs), 60–63
- service guarantee metric, 364–365
- service level agreements (SLAs), 110, 364
- Service Principal Names (SPNs), 78
- service topologies, 43–46
- Services In Farm page, 246
- Services Infrastructure, 409
- Session Initiation Protocol (SIP), 73, 136
- Set Service Principal Name (SetSPN) tool, 118
- Set-SPEnterpriseSearchCrawlContentSource cmdlet, 289
- Set-SPFarmConfig cmdlet, 61–62
- Set-SPIRMSettings cmdlet, 119
- Set-SPSiteSubscriptionIRMConfig cmdlet, 119
- Set-SPSiteUrl cmdlet, 36–37
- Set-SPTTrustedIdentityTokenIssuer cmdlet, 357
- Set-SPTTrustedRootAuthority cmdlet, 357
- Set-SPTTrustedSecurityTokenIssuer cmdlet, 357
- Set-SPTTrustedService-TokenIssuer cmdlet, 357
- Set-SPWebApplication cmdlet, 84
- Set-SPWOPIZone cmdlet, 252
- shared properties, 326
- Shared Services Administrator, 120
- Shared Services Farm (farm type), 38
- SharePoint 2010 site collections, 228
- SharePoint 2016 Products Preparation Tool, 50–51
- SharePoint Configuration Wizard, 59, 61, 399
- SharePoint Designer tool, 9, 153–154
- SharePoint Farm Administrator, 296
- SharePoint Foundation, 409
- SharePoint groups, 93–95
- SharePoint-hosted model, 48
- SharePoint Insights feature, 259
- SharePoint Management Agent, 134
- SharePoint Online Administrator, 131
- SharePoint Online Migration API, 242
- SharePoint Online Search Center, 70
- SharePoint Portal Server, 409
- SharePoint Products Configuration Wizard, 58, 60
- SharePoint Security Token Service certificate, 88
- SharePoint Server 2016, 88–89, 345, 410
- SharePoint Server Search, 410
- SharePoint Server Telemetry feature, 259
- SharePoint Sites content source type, 287
- SharePoint Store Settings page, 248–249
- SharePoint users, 93–95
- SharePoint VS (Virus Scan) API, 111
- SharePoint\_Shell\_Access role, 121
- Sharing hints, 98
- Shell Admin, 121–122
- SID (security identifier), 134, 136
- Simple Mail Transfer Protocol (SMTP), 73, 84–85, 136
- Simple Object Access Protocol (SOAP), 64
- Single-server farm server role, 37, 41–42, 44
- Single Sign-On (SSO), 92, 198
- SIP (Session Initiation Protocol), 73, 136
- Site Administration
  - configuring custom properties, 326
  - configuring MMS imports, 307
  - configuring page output cache settings, 396
  - configuring search refinement, 328
  - Content Organizer, 209
  - creating term sets, 26
  - Manage Catalog Connection page, 325
  - moving subsites, 20
  - Site Closure and Deletion page, 168
- Site Closure And Deletion page, 168
- Site Collection Administration
  - activating object cache, 397
  - assigning term sets, 24
  - audit log reports, 17
  - building query rules, 13
  - configuring SEO properties for site collections, 315
  - creating information management policy, 18
  - creating site policies, 168
  - enabling page output cache, 395
  - monitoring site collection content, 383
  - reviewing site collection cache profiles, 394
  - Search Schema page, 14
  - SharePoint Designer settings, 153–154
- Site Collection Administrators page, 164
- Site Collection Quotas And Locks page, 167
- site columns
  - content types, 7
  - designing, 5–6
  - managed properties, 14
- Site Content And Structure menu, 21
- site-level searches, 334
- Site Mailbox Site feature, 169
- Site Master, 36, 158–159
- site navigation, 321–322
- site owners, 163–164
- Site Owners group, 275
- site permission level, 94, 145

## Site Permissions page

- Site Permissions page, 99, 143
- site policies, 167–168, 212–213
- site quotas, 164–167, 193, 272
- site-to-site (S2S) authentication, 77
- sites and site collections
  - access requests, 99, 137–139
  - anonymous access, 102–103, 141–142
  - app permissions, 139–141
  - content types, 7–8
  - defined, 2
  - displaying Yammer feed, 198–199
  - eDiscovery, 207–208
  - Fast Site Collection Creation, 35–36, 158–159
  - HHSC, 34–35, 37, 148–149, 159–162
  - HTML field security, 147
  - information management policies, 18
  - intersite navigational taxonomy, 2–4
  - managed properties, 14
  - managing site structures, 20–22
  - managing term set access, 320–321
  - measuring upgrade performance, 240
  - monitoring, 365, 383–384
  - orphaned objects, 230
  - PBSC, 148–151, 159–160
  - PerformancePoint Services, 344
  - permission inheritance, 142–144
  - permission levels, 144–146
  - query rules, 311
  - self-service site creation, 162–163
  - SEO settings, 315
  - services lockdown, 110–111
  - SharePoint 2010 mode, 228
  - site access requests, 137–139
  - site closures and deletions, 168
  - site owners, 163–164
  - site policies, 167–168, 212–213
  - site quotas, 164–167, 193, 272
  - Sites page pinning, 170–171
  - team mailbox, 168–169
  - top-level sites, 2
- Sites page pinning, 170–171
- Skype for Business
  - Exchange connectivity and, 206–207
  - network infrastructure, 47
  - Office Online Server, 63, 65
  - S2S authentication, 67–68, 87, 89
  - server farm connections, 83
- SLAs (service level agreements), 110, 364
- slipstreaming process, 57–58
- small computer system interface (SCSI), 39–40
- SMTP (Simple Mail Transfer Protocol), 73, 84–85, 136
- Snippets (Design Manager), 203
- SOAP (Simple Object Access Protocol), 64
- Social database (UPA), 128
- social networking
  - activity feeds, 196
  - OneDrive redirection, 194
  - planning communities, 191–192
  - planning connections, 196–197
  - planning My Sites, 193
  - social permissions, 129–131, 194–195
  - user profiles, 195–196
  - Yammer settings, 197–199
- social permissions, 129–131, 194–195
- software boundaries and limits
  - classes of, 31–32
  - content database considerations, 32–33
  - ECM considerations, 214–215
  - planning for capacity, 391–392
- solid-state drive (SSD), 40, 236
- SPIInstall share, 58
- SPList permission request scope, 140–141
- SPNs (Service Principal Names), 78
- SPSite permission request scope, 140–141
- SPWeb permission request scope, 140–141
- SQL optimization, 385–386
- SQL Server
  - aliases, 178–180
  - AlwaysOn Availability Groups, 176, 181, 203
  - Analysis Management Objects, 348
  - Analysis Services, 346–348, 351
  - authentication, 30
  - backup schedule, 185–186
  - BCS support, 260
  - Client Network Utility, 178–179
  - clustering, 180–181
  - Failover Cluster Instance, 180
  - installation sequence, 241
  - Log Shipping, 176, 182, 203
  - mirroring, 31, 172, 176
- SQL Server Client Network Utility dialog box, 179
- SQL Server Integration Services (SSIS), 184
- SQL Server Management Studio (SSMS)
  - autogrowing content databases, 389
  - evaluating content databases for upgrade, 225, 239
  - farm level administrators, 121

- logging database, 380
  - maximum degree of parallelism, 53–54
  - pregrowing content databases, 388
  - read-only access for content, 237
  - viewing usage data, 404–405
  - SQL Server Reporting Services (SSRS), 117, 344–345, 351
  - SSD (solid-state drive), 40, 236
  - SSIS (SQL Server Integration Services), 184
  - SSL bindings, 82–83
  - SSL (Secure Sockets Layer)
    - about, 80
    - Add-in functionality, 245
    - certificate management, 114
    - connection encryption, 82–85
    - site mailboxes, 169
  - SSMS (SQL Server Management Studio)
    - autogrowing content databases, 389
    - evaluating content databases for upgrade, 225, 239
    - farm level administrators, 121
    - logging database, 380
    - maximum degree of parallelism, 53–54
    - pregrowing content databases, 388
    - read-only access for content, 237
    - viewing usage data, 404–405
  - SSO (Single Sign-On), 92, 198
  - SSRS (SQL Server Reporting Services), 117, 344–345, 351
  - Start-SPEnterpriseSearchServiceInstance cmdlet, 285
  - STARTTLS (Opportunistic TLS), 84
  - Stop Inheriting Permissions icon, 142
  - storage architecture
    - designing, 38–40
    - estimating requirements, 392–393
    - forecasting storage needs, 381
    - site limit values, 165
    - storage redundancy planning, 182–183
    - upgrade considerations, 239
  - storage area networks (SANs)
    - about, 38–39, 385
    - SQL Server clustering, 180
    - storage redundancy and, 183
    - upgrade process and, 236
  - Strategy Map report template, 341
  - streamlined topology, 172, 280
  - stretched farms, 47, 175
  - structural navigation (sites), 3
  - structured large repository, 214
  - STS (security token service) certificates, 114–115
  - Subscription Settings service application, 245
  - subscriptions, 245–247
  - subsites, 2, 167
  - supported limits, 32, 214
  - Synchronization database (UPA), 128
  - synonyms
    - creating thesaurus files, 11–12
    - designing, 11–12
    - importing thesaurus files, 12
  - System Center 2012 Operations Manager, 367–368
- ## T
- T-SQL scripts, 53–54, 184
  - taxonomy management
    - custom properties, 326–327
    - folksonomy comparison to, 10, 22–23, 25
    - intersite navigational, 2–4
    - list refinement, 330
    - search refinement, 327–329
    - site collection term set access, 320–321
    - term set navigation, 321–324
    - topic catalog pages, 324–326
  - team mailbox, 168–169
  - Team Sites (Hybrid SharePoint Sites), 3, 74
  - Tenancy permission request scope, 140–141
  - Term Property Web Part, 304
  - term set groups, 23, 25
  - Term Set Management Tool, 24
  - term set owners, 25
  - term sets
    - about, 22–23
    - creating new, 26
    - defining, 23, 25–26
    - defining functionality, 23
    - determining groups, 25
    - identifying, 25
    - identifying owners, 25
    - local versus global, 23–24
    - managing navigation, 321–324
    - managing site collection access, 320–321
    - planning core, 24
    - sharing, 302–303
  - Term Sets Planning worksheet (Excel), 24
  - Term Store Administrators role, 305–306
  - Term Store Management Tool
    - adding custom properties, 304–305
    - configuring custom properties, 326

## term store permissions

- configuring MMS imports, 307
- configuring search refinement, 328
- configuring term store permissions, 305–306
- creating term sets, 26
- Faceted Navigation tab, 328–329
- importing metadata planning worksheets, 24
- Navigation tab, 322–323
- Term-Driven Pages tab, 323–326
- term store permissions, 305–306
- terms, 22–23
- test environment, 238
- Test-SPContentDatabase cmdlet, 225–226, 229, 231
- thesaurus files
  - creating, 11–12
  - importing, 12
  - uploading, 12
- thresholds, 32, 214
- throttling
  - avoiding issues, 359
  - HTTP request, 41
- Timer Job Scheduling feature, 402
- timer jobs, 8, 303–304, 381
- TLS (Transport Layer Security), 82–85
- top-level sites, 2
- Top Link Bar, 3
- topic catalog pages, 200–201, 324–326
- trace logs
  - about, 402
  - client-side tracing, 402–404
  - server-side tracing, 404
- tracking installations, 62–63
- traditional topology, 172, 280
- transaction logs, 182, 189, 239
- Translation Services (Microsoft), 251
- Transport Layer Security (TLS), 82–85
- troubleshooting SharePoint environment
  - about, 401
  - analyzing diagnostic logs, 408–409
  - analyzing usage data, 404–406
  - client-side tracing, 402–404
  - enabling Developer Dashboard, 407–408
  - establishing baseline performance, 401–402
  - hybrid cloud issues, 409–411
  - server-side tracing, 404
  - thought experiment, 412–413
- trust management, 356–357
- trusted identity provider, 30
- trusted root authority, 116
- two-way, bidirectional topology, 360

## U

- ULS (Unified Logging Service)
  - about, 366, 410
  - alternate access mapping, 153
  - logging levels, 409
  - missing file system components, 231
- ULS Viewer, 410
- UNC (Universal Naming Convention), 12
- Unified Logging Service (ULS)
  - about, 366, 410
  - alternate access mapping, 153
  - logging levels, 409
  - missing file system components, 231
- uniform resource identifiers (URIs), 141
- Uninstall-SPSolution cmdlet, 232, 274
- Universal Naming Convention (UNC), 12
- unstructured document library, 214
- UPA (User Profile service application)
  - about, 128
  - claims integration, 136–137
  - configuring, 128–129
  - planning communities, 192
  - profile properties, 134–136
  - service application recovery, 188
  - social permissions, 129–131
  - synching connections, 131–134
- Update-SPSolution cmdlet, 274
- Updates directory, 57–58
- Upgrade-SPContentDatabase cmdlet, 399–400
- upgrades
  - apps, 276
  - configuring farms, 237–238
  - farm solutions, 274
  - installation sequence, 241
  - measuring performance, 238–241
  - migrating on-premises environment, 241–243
  - parallel, 236
  - read-only access for content, 236–237
  - removal of servers in rotation, 233–235
  - web application authentication for, 228–230
- Upload command, 16
- UPN (User Principal Name), 69, 136
- URIs (uniform resource identifiers), 141
- URLs
  - alternate access mapping, 31, 36–37, 151–152
  - host-header site collections, 34–35
  - My Sites, 131

- Usage Data Collection feature, 402
- Usage Data Import timer job, 381, 402
- Usage Data Maintenance timer job, 381
- Usage Data Processing timer job, 381
- % Usage Peak performance counter, 372
- % Usage performance counter, 372
- Use Tags and Notes social permission, 194
- useCacheProfileOverrides attribute, 395
- user and app policy, 141
- user authentication, 77, 136
- user-facing communication, 47
- user-only policy, 141
- User policy, 104–106
- User Principal Name (UPN), 69, 136
- User Profile Service, 234
- User Profile service application (UPA)
  - about, 128
  - claims integration, 136–137
  - configuring, 128–129
  - configuring social permissions, 129–131
  - planning communities, 192
  - profile properties, 134–136
  - service application recovery, 188
  - synching connections, 131–134
- User Profile Synchronization Service, 234
- user profiles, 195–197, 233

## V

- variation labels, 205
- version status (content databases), 226–228
- versioning controls, 210
- videos, quick previews, 16
- View Items permissions, 104
- View Only permission level, 144
- virtual local area networks (VLANs), 177
- Visio Services (Microsoft), 117, 251, 254–255
- Visitors group, 93, 95, 143
- VLANs (virtual local area networks), 177

## W

- Warm Standby Recovery, 175, 190
- warning emails, 165
- WCM (Web Content Management) workload
  - channels, 199–200

- content deployment, 203–204
  - Design Manager, 202–203
  - display templates, 204
  - planning variations, 205
  - product catalogs, 200–201
  - topic pages, 200–201
- Web Application Open Platform Interface (WOPI), 211
- web application zones
  - about, 31
  - associating, 36–37
  - isolation considerations, 110
  - SharePoint Designer settings, 153–154
- web applications
  - alternate access mappings, 31, 36–37, 152–153
  - anonymous access, 30, 82, 101, 142
  - anonymous authentication, 81
  - assigning proxy groups to, 301
  - authentication, 29–30, 228–230
  - authorization policies, 104–107
  - failover database servers, 31
  - isolation considerations, 110
  - managed paths, 148–152
  - Office Online Server, 63
  - planning, 29–31
  - planning application pools, 27–29
  - planning policies, 104–107
  - reverse proxy, 86
  - server farms, 357
  - service application connections, 31
  - SSL bindings, 82–83
- Web Content Management (WCM) workload
  - channels, 199–200
  - content deployment, 203–204
  - Design Manager, 202–203
  - display templates, 204
  - planning variations, 205
  - product catalogs, 200–201
  - topic pages, 200–201
- Web Page report template, 342
- Web Parts
  - Business Data, 8
  - Content Search, 213, 312–313
  - display templates, 204
  - establishing connections between, 127
  - Excel Services support, 64
  - Refiner, 327
  - Script Editor, 199
  - Search, 204

## Web Server (IIS) role

- security considerations, 126–127
- Term Property, 304
- Web Server (IIS) role, 50–51, 65
- Web Sites content source type, 287
- wildcard aliases, 244
- wildcard certificates, 245
- wildcard managed paths, 21–22, 148
- Windows Administrators group, 121–122
- Windows authentication
  - about, 30
  - host-header site collections, 35
  - planning and configuring, 78–81
  - web applications, 56
- Windows Communication Foundation, 260
- Windows Firewall, 347
- Windows PowerShell cmdlets. *See specific cmdlets*
- Windows Server Failover Clustering (WSFC), 180
- Windows SharePoint Services Timer Service, 120, 189
- WOPI (Web Application Open Platform Interface), 211
- Word Automation Services (Microsoft), 251, 255–256
- work management
  - about, 354–355
  - eDiscovery, 357–358
  - Exchange connection, 355
  - managing trusts, 356–357
  - Microsoft Project 2016, 355–356
- workload optimization
  - backup and restore, 184–191
  - disaster recovery solutions, 172–184
  - ECM, 205–219
  - high availability solutions, 172–184
  - site collections, 157–171
  - social workloads, 191–199
  - thought experiment, 220–221
  - WCM, 199–205
- Write permission, 60–61, 140
- WS-Federation standard, 86
- WSFC (Windows Server Failover Clustering), 180
- WSS\_UsageApplication database, 380, 405

## X

- X-SharePointHealthScore header, 41
- XML sitemap, 316

## Y

- Yammer Configuration page, 198
- Yammer online functionality, 196–199

## Z

- Zero Downtime Patching, 398–400
- zones
  - DNS, 244
  - forward lookup, 245
  - web application, 31, 36–37, 153–154