



ОСНОВЫ Microsoft Azure

Подготовка к экзамену

AZ-900



Джим Чешир

DEVS UNIVERSE



Джим Чешир



Основы Microsoft Azure. Подготовка к экзамену AZ-900





Exam Ref AZ-900

Microsoft Azure

Fundamentals



Jim Cheshire



ОСНОВЫ 
Microsoft Azure.
Подготовка
к экзамену AZ-900

Джим Чешир



ДМК
ИЗДАТЕЛЬСТВО
Москва, 2022

УДК 004.01
ББК 32.972
Ч34



Чешир Дж.

Ч34 Основы Microsoft Azure. Подготовка к экзамену AZ-900 / пер. с англ. А. Д. Ворониной; ред. В. Н. Черников. – М.: ДМК Пресс, 2021. – 306 с.: ил.

ISBN 978-5-97060-869-2

Экзамен AZ-900 является базовым для всех технических специалистов, осваивающих облачную платформу Microsoft Azure. В рамках данного экзамена рассматриваются основные концепции облачных платформ, а также современные ИТ-технологии (искусственный интеллект, большие данные, интернет вещей). Книга содержит полное и подробное описание всех тем, необходимых для успешной сдачи экзамена AZ-900: Microsoft Azure Fundamentals. Удобная структура глав облегчает поиск нужной информации: каждый раздел посвящен отработке определенного навыка.

Данная книга будет полезна при обучении основам работы с облачной платформой Microsoft Azure.

УДК 004.01
ББК 32.972

Authorized Translation from the English language edition, entitled EXAM REF AZ-900 MICROSOFT AZURE FUNDAMENTALS, 2nd Edition by JIM CHESHIRE, published by Pearson Education, Inc, publishing as Microsoft Press, Copyright © 2021 by Pearson Education, Inc. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc. Electronic RUSSIAN language edition published by DMK PRESS PUBLISHING LTD., Copyright © 2021 by DMK Press. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.



ISBN 978-0-13-687718-9 (англ.)
ISBN 978-5-97060-869-2 (рус.)

© Pearson Education, Inc., 2021
© Перевод, оформление, издание, ДМК Пресс, 2021

*Я посвящаю эту книгу моей жене Бекки,
моей дочери Хоуп и моему сыну Джеймсу.*

– Джим Чешир



Содержание

https://t.me/it_books

<i>Благодарность</i>	10
<i>Об авторе</i>	11
<i>О переводе</i>	12
<i>Введение</i>	13
Глава 1 Описание основных понятий облачных технологий	17
Навык 1.1: описание преимуществ и особенностей использования облачных сервисов.....	18
Высокая доступность.....	18
Масштабируемость, эластичность и гибкость.....	21
Отказоустойчивость и аварийное восстановление.....	23
Экономические преимущества облака.....	24
Навык 1.2: описание различий между Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) и Software-as-a-Service (SaaS).....	25
Модель разделения ответственности.....	26
Инфраструктура как услуга (IaaS).....	26
Платформа как услуга (PaaS).....	29
Программное обеспечение как услуга (SaaS).....	31
Сравнение типов сервисов.....	32
Навык 1.3: описание различий между моделями общедоступного, приватного и гибридного облаков.....	33
Облачные вычисления.....	34
Общедоступное облако.....	34
Частное облако.....	36
Гибридное облако.....	37
Мысленный эксперимент.....	38
Ответы на мысленный эксперимент.....	39
Краткое содержание главы.....	40
Глава 2 Описание основных служб Azure	43
Навык 2.1: описание основных компонентов архитектуры Azure.....	44
Регионы Azure.....	45

Зоны доступности	46
Группы ресурсов	49
Подписки Azure.....	52
Группы управления.....	56
Диспетчер ресурсов Azure (Azure Resource Manager, ARM)	57
Навык 2.2: описание ключевых ресурсов, доступных в Azure	61
Виртуальные машины Azure	61
Служба приложений Azure	70
Экземпляры контейнеров Azure (Azure Container Instances, ACI)	75
Служба Azure Kubernetes (Azure Kubernetes Service, AKS)	78
Виртуальный рабочий стол Azure	78
Виртуальные сети	80
ExpressRoute	82
Хранилище BLOB-объектов	83
Дисковое хранилище	84
Файлы Azure (Azure Files).....	85
Уровни доступа к хранилищам	86
Azure Cosmos DB	86
База данных Azure SQL.....	89
База данных Azure для MySQL.....	92
База данных Azure для PostgreSQL.....	92
Azure Marketplace и сценарии его использования.....	93
Мысленный эксперимент.....	95
Ответы на мысленный эксперимент	97
Краткое содержание главы.....	99

Глава 3 Опишите основные решения и средства управления Azure

Навык 3.1: описание основных решений, доступных в Azure	103
Центр интернета вещей (Azure IoT Hub).....	103
IoT Central.....	109
Azure Sphere.....	116
Azure Synapse Analytics.....	118
HDInsight.....	119
Azure Databricks.....	122
Машинное обучение Azure	128
Служба когнитивных вычислений.....	134
Служба Azure Bot.....	135
Бессерверные вычисления	137
Функции Azure (Azure Functions).....	138
Logic Apps.....	146
Event Grid	152
Azure DevOps	153

Azure DevTest Labs.....	157
Навык 3.2: описание средств управления Azure.....	163
Портал Azure (Azure Portal).....	164
Azure и PowerShell.....	171
Интерфейс командной строки Azure.....	173
Azure Cloud Shell.....	176
Azure mobile app.....	181
Помощник по Azure (Azure Advisor).....	183
Azure Monitor.....	186
Azure Service Health.....	195
Мысленный эксперимент.....	197
Ответы на мысленный эксперимент.....	199
Краткое содержание главы.....	201
Глава 4 Описание общих функций безопасности и обеспечения безопасности сети.....	203
Навык 4.1: описание функций безопасности Azure.....	204
Центр безопасности Azure (Azure Security Center).....	204
Хранилище ключей Azure (Azure Key Vault).....	209
Azure Sentinel.....	213
Навык 4.2: описание безопасности сети в Azure.....	219
Глубокая защита.....	220
Группы сетевой безопасности (Network Security Group).....	220
Брандмауэр Azure.....	226
Защита от DDoS.....	233
Мысленный эксперимент.....	235
Ответы на мысленный эксперимент.....	236
Краткое содержание главы.....	236
Глава 5 Описание функций идентификации, управления, конфиденциальности и соответствия нормативным требованиям.....	238
Навык 5.1: описание основных служб идентификации Azure.....	239
Аутентификация и авторизация.....	239
Azure Active Directory.....	240
Условный доступ и многофакторная аутентификация.....	246
Управление доступом на основе ролей.....	249
Навык 5.2: описание основных функций управления Azure.....	253
Политика Azure.....	254
Блокировки.....	259
Теги.....	262
Azure Blueprints.....	263



Навык 5.3: описание конфиденциальности и соответствия нормативным требованиям	269
Заявление о конфиденциальности Microsoft	270
Cloud Adoption Framework для Azure	271
Центр управления безопасностью	271
Service Trust Portal	272
Суверенные регионы Azure	275
Мысленный эксперимент	276
Ответы на мысленный эксперимент	277
Краткое содержание главы	278

**Глава 6 Описание ценообразования, соглашений о качестве
предоставляемых услуг и жизненный цикл служб Azure** 280

Навык 6.1: описание методов планирования и управления затратами	281
Факторы, влияющие на затраты	281
Калькулятор цен	283
Калькулятор совокупной стоимости владения	285
Управление затратами Azure	288
Навык 6.2: описание соглашений о качестве предоставляемых услуг и жизненных циклов служб	292
Соглашение об уровне обслуживания	293
Интерпретация терминов SLA	294
Жизненный цикл службы Azure	297
Мысленный эксперимент	300
Ответы на мысленный эксперимент	300
Краткое содержание главы	301
<i>Предметный указатель</i>	303





Благодарность

Я хотел бы выразить глубокую благодарность следующим людям, без которых эта книга была бы невозможна.

Спасибо Лоретте за то, что привела меня в этот проект. После двадцати лет совместной работы над многочисленными проектами вы по-прежнему способны привнести в них новизну и вдохновение. Спасибо тебе, Рик, за тщательное редактирование каждого уголка этой книги, что помогло сделать процесс чтения лучше. Спасибо Тиму за те моменты, когда он заставлял меня взглянуть на мой подход с другой стороны, и за его ценные идеи. Спасибо Чарви за внимание к деталям, которые способствовали дальнейшему развитию проекта. А также спасибо сотрудникам Microsoft Press, чей труд помог воплотить из цифровой рукописи данную книгу.





Об авторе

ДЖИМ ЧЕШИР – любитель новых технологий с опытом работы в различных ИТ-областях более 25 лет. Джим является автором более 15 книг по технологиям, он провел многочисленные учебные занятия по Microsoft Azure как в частных предприятиях, так и в рамках учебной онлайн-программы Safari (Safari's Live Training program). Джим активно занимается Azure и уже более 22 лет работает в Microsoft. В настоящий момент трудится над дизайном и внедрением учебной платформы для обучения инженеров технической поддержки Microsoft. Вы можете подписаться на его страничку в Твиттере @az900examref и общаться с ним.



О переводе

Облачные технологии все глубже входят в повседневную деятельность ИТ-специалистов, и Microsoft является одним из лидеров на этом рынке со своей платформой Azure. Не всегда перевод данной книги был простым, но мы старались использовать те же термины и названия, которые доступны на официальных русскоязычных ресурсах Microsoft. Осталось добавить, что сам сертификационный экзамен AZ-900 можно сдавать как на русском, так и на английском языках, поэтому мы часто указывали ключевые термины и оригинальные названия на английском, чтобы вам было проще ориентироваться.

Над переводом этой книги работали специалисты компании Devs Universe:

- **Алина Воронина** – переводчик, специалист по обучению разработчиков английскому языку в компании Devs Universe;
- **Вячеслав Черников** – редактор перевода, к. т. н. в области разработки ПО, основатель компании Devs Universe, автор книги «Разработка мобильных приложений на C# для iOS и Android», в прошлом один из Microsoft MVP, Nokia Champion, Qt Certified Specialist, Qt Ambassador, автор статей для «Хабрахабр», «Хакера», Microsoft Developer Blogs, говоритель для конференций;
- **Марина Королькова** – помощь с редактурой, специалист компании Devs Universe.

Мы надеемся, что наши переводы помогут вам глубже понять суть современных технологий и стать первоклассными специалистами.





Введение

Как компании, так и частные лица внедряют облачные технологии с головокружительной скоростью. Зачастую для облачных приложений и служб выбирают именно Microsoft Azure. Цель экзамена AZ-900 заключается в проверке понимания основ Azure. В экзамен входят как широко применяемые в Azure высокоуровневые, так и другие важные концепции, уникальные для конкретных служб Azure. Подобно экзамену, предназначение этой книги состоит в том, чтобы дать вам широкое представление о самой платформе, а также о многих ключевых службах и компонентах Azure.

Несмотря на приложенные усилия для передачи достоверной информации с нашей стороны, Azure не стоит на месте, поэтому есть вероятность, что некоторые экраны на портале Azure будут немного отличаться от тех, что были в момент написания этой книги. Также, возможно, будут и другие незначительные изменения, например в названиях служб и сервисов.

В этом издании мы тщательно пересмотрели содержание первого издания и доработали данную книгу под сегодняшний Azure. Мы изменили порядок в книге и добавили новую информацию, которая отражает современный экзамен AZ-900. Недавно Microsoft внесла изменения в экзамен AZ-900, добавив туда новые концепции, службы и функции Azure. Мы также это учли. Благодаря обратной связи по первому изданию книги мы отредактировали некоторые детали и внесли изменения во второе издание.

Здесь вы найдете основные темы, которые можно встретить на экзамене, однако сама книга не дает ответов на все вопросы. Только у экзаменационной группы Microsoft есть доступ ко всем вопросам. К тому же Microsoft постоянно добавляет новые вопросы для экзамена, из-за чего становится невозможно охватить конкретные вопросы. Рассматривайте эту книгу в качестве дополнения к вашему реальному практическому опыту и другим учебным материалам. Практически везде вы найдете ссылки в разделах «Дополнительная информация», которые являются хорошим источником для дополнительного обучения.

Структура книги

Структура книги представлена списком «Оцениваемые навыки», опубликованным для экзамена. Этот список доступен для каждого экзамена на веб-сайте Microsoft Learning: <http://aka.ms/examlist>. Каждая глава книги соответствует основной тематической области в списке, а технические задачи в каждой области определяют организацию главы. Экзамен представлен шестью основными тематическими областями, которые и составляют главы в данной книге.

Подготовка к экзамену

Благодаря сертификационным экзаменам Microsoft вы сможете дополнить свое резюме и поделиться с миром своим уровнем квалификации. Данные экзамены подтверждают ваш опыт работы и базу знаний по продуктам. Конечно, ничто не заменит практический опыт работы, однако подготовка через обучение и выполнение практических заданий помогут вам для экзамена. При подготовке мы рекомендуем вам использовать разные доступные учебные материалы и курсы. Например, изучая руководство к экзамену (Exam Ref) или любое другое учебное пособие для «самостоятельного» обучения, вы можете приобрести курс Microsoft Official Curriculum для учебного опыта. Подберите для себя наиболее подходящую комбинацию.

Обратите внимание, что данная книга основана на общедоступной информации об экзамене и личном опыте автора. Целостность экзамена гарантируется тем, что авторы не обладают доступом к экзаменационным вопросам.

Сертификация Microsoft

Сертификаты Microsoft отличат вас от других специалистов, подтвердив, что вы владеете широким набором навыков и опытом работы с текущими продуктами и технологиями Microsoft. Экзамены и соответствующие сертификаты разработаны для подтверждения вашего владения критически важными компетенциями при проектировании и разработке, внедрении и поддержке решений с продуктами и технологиями Microsoft как в локальной среде, так и в облаке. Сертификация предоставляет различные преимущества и для отдельных лиц, и для работодателей, и для организаций.

ДОПОЛНИТЕЛЬНО СЕРТИФИКАТЫ MICROSOFT

Сведения о сертификатах Microsoft с полным списком доступных экзаменов расположены на сайте <https://microsoft.com/learn/>.

Быстрый доступ к онлайн-справочникам

Во всей книге приведены адреса веб-страниц, рекомендованные автором для получения дополнительной информации. Некоторые из них могут быть громоздкими для ввода в веб-браузер, поэтому мы сократили их и собрали в единый список, к которому вы можете обращаться во время чтения.

Загрузить список можно на следующем сайте: <https://MicrosoftPressStore.com/ExamRefAZ900SecondEdition/downloads>.

URL-адреса структурированы по главам и заголовкам. При виде URL-адреса вы можете найти гиперссылку в списке для перехода на веб-страницу.

Ошибки, обновления и поддержка

Мы сделали все, чтобы обеспечить точность данной книги и ее содержания. Вы можете получить последнюю информацию по книге в виде списка выявленных ошибок и связанных с ними исправлений:

<https://MicrosoftPressStore.com/ExamRefAZ900SecondEdition/errata>.

Если вы обнаружите ошибку, которая еще не представлена в списке, отправьте ее нам с той же страницы.

Дополнительную поддержку и информацию о книгах можно найти на сайте <https://MicrosoftPressStore.com/Support>.

Обратите внимание, что поддержка программного обеспечения и оборудования Microsoft не предоставляется по указанным выше адресам. Для получения справки по программному или аппаратному обеспечению Microsoft перейдите по ссылке <https://support.microsoft.com>.

До контакта

Давайте продолжим общение! Мы есть в Твиттере:

<http://twitter.com/MicrosoftPress>.

Там вы также можете найти и автора книги, Джима Чешира: @az900examref.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Скачивание исходного кода примеров

Скачать файлы с дополнительной информацией для книг издательства «ДМК Пресс» можно на сайте www.dmkpress.com на странице с описанием соответствующей книги.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Pearson Education очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.



ГЛАВА 1



Описание основных понятий облачных технологий

https://t.me/it_books

Облачные вычисления являются частью информационных технологий (ИТ) уже более 20 лет. За это время они превратилась в сложную коллекцию облачных сервисов и моделей. Перед тем как начать процесс перехода в облако, для начала важно понять ключевые концепции и услуги, связанные с облаком.

Для перехода в облако есть много причин, при этом одним из главных преимуществ является снятие части ИТ-нагрузки с вашей компании. Облако позволяет использовать преимущества инфраструктуры облачного провайдера, а также упрощает обеспечение согласованного доступа к приложениям и данным. Кроме того, у вас появятся преимущества готовых решений для резервного копирования данных, а ваши приложения смогут выдерживать аварийные ситуации и другие проблемы доступности. Размещение данных и приложений в облаке зачастую более экономично, чем инвестиции в собственную инфраструктуру и локальные ИТ-ресурсы.

После того как вы решите воспользоваться преимуществами облака, вам нужно разобраться в доступных вам предложениях. Некоторые облачные службы обеспечивают практически автоматическую работу, в то время как другие требуют от вас самостоятельного управления. Поиск правильного баланса с учетом ваших потребностей предполагает полное понимание каждого вида служб.

В этой главе рассматриваются преимущества использования облака, различные доступные облачные службы и модели, позволяющие использовать многообразие конфигураций.

Навыки этой главы:

- описание преимуществ и особенностей использования облачных сервисов;
- описание различий между Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) и Software-as-a-Service (SaaS);

- описание различий между моделями общедоступного (public), приватного (private) и гибридного (hybrid) облаков.

Навык 1.1: описание преимуществ и особенностей использования облачных сервисов

Современные компании в значительной степени полагаются на программные решения и доступ к данным. Действительно, нередко наиболее ценные активы компании напрямую связаны с данными и приложениями. Благодаря этому инвестиции в ИТ значительно выросли за последнюю пару десятилетий.

Зависимость от локальных ИТ-отделов хорошо работала в первые дни ИТ, но доступ к данным и приложениям стал настолько важной частью повседневной деятельности, что локализованные ИТ-системы стали неэффективными на многих уровнях.

Принимая решение о том, что вы хотите перенести в облако, оценивайте эти решения с учетом возможностей, которые предоставляют облачные вычисления.

Этот раздел охватывает:

- высокую доступность;
- масштабируемость, эластичность и гибкость;
- отказоустойчивость и аварийное восстановление;
- экономические преимущества облака.

Высокая доступность

Доступность данных и приложений является основным требованием для любого приложения, локального или облачного. Есть много причин, по которым вы можете потерять доступ к приложению. Наиболее распространенными проблемами являются следующие:

- перебои в работе сети;
- ошибка в приложении;
- прекращение работы системы (например, отключение виртуальной машины);
- перебои с электропитанием;
- проблема с внешней системой, например базой данных.

В идеальном мире вы обладаете 100%-ной доступностью, но если возникнет какая-либо из вышеперечисленных проблем, этот процент будет уменьшаться. Поэтому крайне важно, чтобы инфраструктура свела к минимуму риск возникновения проблем, влияющих на доступность приложения.

Поставщики облачных технологий предлагают *соглашение об уровне обслуживания* (service-level agreement, SLA), гарантирующее процентный уровень доступности. SLA, как правило, гарантирует почти стопроцентную безотказную работу, но это распространяется только на системы, которые контролируются поставщиком облачных услуг.

Размещенное в облаке приложение может быть как разработано вашей компанией, так и предоставлено облачным провайдером.

Перебои в работе сети

Всем приложениям необходимо сетевое подключение. Пользователям нужно сетевое подключение к компьютерам, которые выполняют приложение, а приложению необходимо подключение к серверным системам, таким как базы данных. С помощью сети приложения могут подключаться друг к другу. Если произошел сбой любого из сетевых подключений, это может привести к отсутствию доступа.

ДОПОЛНИТЕЛЬНО ПЛАНИРОВАНИЕ ПРИ ОТКАЗЕ СЕТИ

Ошибки в работе сети не обязательно означают недоступность приложения или данных. Во многих случаях тщательное планирование помогает избежать проблем, возникающих из-за неполадок в сети. Мы подробнее это рассмотрим, когда будем обсуждать отказоустойчивость в данной главе.

Облачные провайдеры вкладывают большие денежные средства в сетевую инфраструктуру, и при переходе в облако у вас появляются ее преимущества в комплекте с дополнительной надежностью. Если что-то в этой инфраструктуре выходит из строя, поставщик облачных вычислений диагностирует и исправляет неполадку, зачастую даже до того, как вы об этом узнаете.

Сбой приложения

Нередко сбоем приложения является результат ошибки ПО, или же причина может быть в архитектуре самого приложения.

ДОПОЛНИТЕЛЬНО АРХИТЕКТУРА ПРИЛОЖЕНИЙ И ОБЛАКО

Для AZ-900 вам не нужно разбираться в концепциях проектирования приложений, но если вы хотели бы больше узнать об архитектурах приложений и облаке, то у Microsoft на этот счет есть хорошая ссылка: <https://bit.ly/cloudappdesign>.

В некоторых облачных сценариях вы сами определяете сбои приложений, однако ваш поставщик облачных услуг, вероятнее всего, уже разработал и предоставляет средства, использование которых облегчает диагностику этих сбоев. Например, у Azure есть служба Application Insights, которая интегрируется с приложением для передачи подробной информации по его производительности и надежности.

Разработчики приложений могут использовать эту информацию для быстрого перехода к коду, в котором возникает проблема, что значительно сокращает время, необходимое на устранение неполадок.

Облачные провайдеры предлагают и другие возможности для уменьшения проблем с доступностью, вызванных из-за сбоев приложения. Как правило, вы можете протестировать новые версии приложения в защищенной среде без воздействия на реальных пользователей. Когда у вас все будет готово для перевода пользователей на новую версию, для начала вы можете перевести небольшую их часть, чтобы проверить, что все исправно работает. В случае проблем облако упрощает процесс возврата к предыдущей версии.

Отключение системы

Отключение системы происходит, когда компьютер, на котором выполняется определенная служба, становится недоступным. В локальной среде этот компьютер может быть сервером с базой данных или другой частью приложения. В облаке эти системы работают внутри *виртуальных машин* (virtual machines), или VM.

VM – это программно реализованные компьютеры, которые работают на физическом компьютере. На одном компьютере может работать несколько VM, при этом у каждой VM есть собственная операционная система и приложения. Все виртуальные машины, работающие на одном хост-компьютере, совместно используют центральный процессор (ЦП), оперативную память и файловое хранилище.

ПРИМЕЧАНИЕ VM НЕ ТОЛЬКО ДЛЯ ОБЛАКА

Виртуальные машины упрощают добавление дополнительных компьютеров и позволяют лучше управлять такими ресурсами, как ЦП, дисковое пространство и память. По этой причине VM – это обычное явление на большинстве предприятий.

Будете ли вы ответственны за обслуживание VM, зависит от выбранной вами облачной службы. Тем не менее независимо от того, кто поддерживает работу VM, поставщик облачных ресурсов будет постоянно следить за их работоспособностью и держать у себя в арсенале системы для восстановления отказавшей VM.

Отключение электропитания

Надежное электроснабжение имеет решающее значение для обеспечения доступности. Даже быстрый скачок мощности может привести к перезагрузке компьютеров и систем. В этом случае приложение будет недоступно до тех пор, пока не будут восстановлены все системы.

Облачные провайдеры вкладывают значительные средства в резервное питание на аккумуляторных батареях и другие избыточные системы для предотвращения проблем доступности, вызванных перебоями электропитания. В ситуации, когда отключение электропитания затрагивает огромную территорию, поставщики облачных вычислений предлагают возможность запуска приложения из другого региона, который не входит в область отключения.

Проблемы с внешней системой

Приложение может использовать системы, находящиеся вне облака или управляемые другим облачным провайдером. Если эти системы выйдут из строя,

приложение может стать недоступным. Размещение приложения в облаке дает вам преимущества инструментов устранения неполадок, оповещения и диагностики, предлагаемые поставщиком облачных услуг.

Теперь, когда вы разбираетесь в проблемах, способных повлиять на доступность, и особенностях облачных вычислений, помогающих устранить эти проблемы, давайте рассмотрим несколько способов, с помощью которых облако может обеспечить для вас высокий уровень доступности.

Масштабируемость, эластичность и гибкость

Вычислительные ресурсы не бесплатны. Это касается и виртуальных машин, базовые ресурсы которых (дисковое пространство, ЦП и память) стоят денег. Лучшим способом минимизации затрат станет использование только необходимых для вас ресурсов. Проблема лишь в том, что потребности в ресурсах могут часто и быстро меняться.

Рассмотрим ситуацию, при которой вы размещаете приложение в облаке, которое отслеживает данные о продажах компании. Если торговый персонал вносит информацию о ежедневных звонках по продажам в конце рабочего дня, то для обработки нагрузки могут потребоваться дополнительные вычислительные ресурсы. Однако потребность в подобных ресурсах в течение дня будет отсутствовать, так как персонал в это время осуществляет звонки с предложением продажи и не использует приложение.

Можно также разместить в облаке веб-приложение, используемое внешними клиентами. В зависимости от шаблона использования вы можете добавить дополнительные вычислительные ресурсы в установленные дни или в определенное время.

Допускайте и то, что вам нужно будет быстро подстроиться под большое количество пользователей, если ваша компания получит неожиданную рекламу в СМИ или каким-либо иным способом.

Масштабирование и эластичность позволяют легко справляться с такими сценариями. Под масштабированием понимается процесс добавления дополнительных ресурсов или мощности для приложения. Существует два варианта масштабирования: горизонтальное (часто называемое масштабированием наружу, *scaling out*) и вертикальное (часто называемое масштабированием вверх, *scaling up*).

При горизонтальном масштабировании для приложения добавляются дополнительные ВМ, каждая из которых идентична другим, обслуживающим ваше приложение виртуальным машинам. Горизонтальное масштабирование располагает вспомогательными ресурсами для обработки дополнительной нагрузки.

При вертикальном масштабировании вы переходите на новую ВМ с дополнительными ресурсами. Например, можно определить, что приложению необходим более мощный процессор и больше памяти. В этом случае вертикальное масштабирование позволит вам переместить приложение на более мощную ВМ.

ПРИМЕЧАНИЕ ВЕРТИКАЛЬНОЕ МАСШТАБИРОВАНИЕ ЧАСТО ДОБАВЛЯЕТ НОВЫЕ ВОЗМОЖНОСТИ

Нередко при масштабировании «вверх» вы не только увеличиваете мощность процессора и памяти, но и получаете дополнительные возможности. Например, вертикальное масштабирование позволяет вам использовать твердотельные накопители (Solid-State Disk Drive, SSD) и другие опции.

На рис. 1.1 показан пример вертикального масштабирования веб-приложения в Azure.

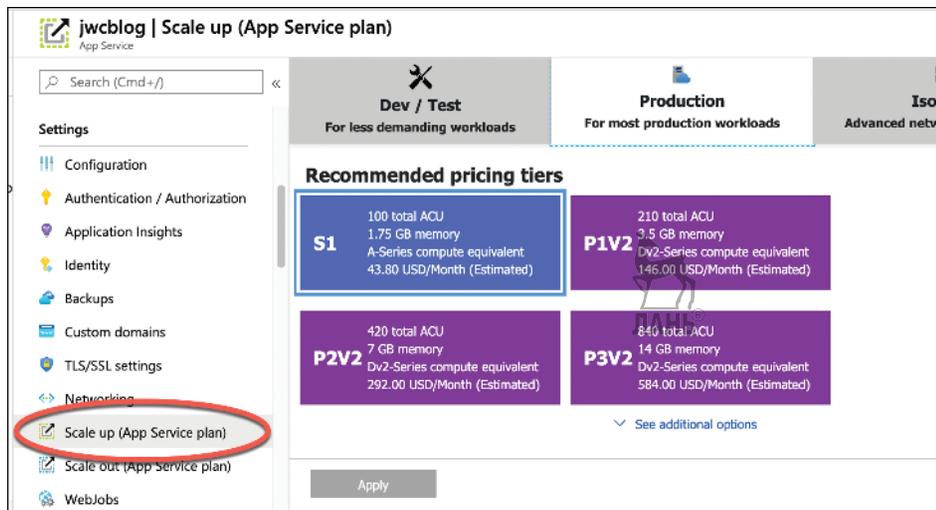


Рис. 1.1 Вертикальное масштабирование веб-приложения в Azure

НА ПРАКТИКЕ МАСШТАБИРОВАНИЕ ИДЕТ В ОБОИХ НАПРАВЛЕНИЯХ

Помимо горизонтального и вертикального масштабирований, вы также можете использовать *чередование* для сокращения потребления ресурсов. В реальной ситуации вам, скорее всего, понадобится при необходимости увеличивать и уменьшать вычислительные ресурсы.

Облачные провайдеры упрощают масштабирование приложений и предлагают возможности автоматического масштабирования на основе шаблона использования. Автоматически масштабировать можно на основе таких параметров, как использование ЦП и оперативной памяти, а также других метрик, специфичных для определенного типа приложения. Возможность автоматического масштабирования называется *эластичностью* (elasticity).



СОВЕТ К ЭКЗАМЕНУ

В Azure можно активировать автоматическое масштабирование с помощью Auto-Scale, службы Azure, которая позволяет автоматически масштабировать приложения на основе шаблонов использования, потребления ресурсов, времени суток и многих других параметров.

Одним из основных преимуществ облака является возможность быстрого масштабирования. Например, запуская веб-приложение в Azure, вы обнаружили, что вам нужно еще две ВМ для его выполнения, при этом их можно увеличить до трех за считанные секунды. Azure выделяет ресурсы за вас. Все, что вам нужно, – это сообщить Azure, сколько ВМ требуется, и все остальное происходит автоматически. Такую совокупность мобильности и скорости облаков часто называют *гибкостью* (agility).

ДОПОЛНИТЕЛЬНО ПОДРОБНЕЕ О НАИЛУЧШИХ ПРАКТИКАХ МАСШТАБИРОВАНИЯ

Дополнительные сведения о масштабировании в Azure смотрите в документации по ссылке: <https://docs.microsoft.com/azure/architecture/best-practices/auto-scaling>.



Отказоустойчивость и аварийное восстановление

Иногда в комплексном облачном окружении что-то может пойти не так. Для сохранения высокого уровня доступности поставщики облачных инструментов внедряют системы, отслеживающие работоспособность вычислительных ресурсов в облаке и принимающие меры при их неработоспособности, обеспечивая тем самым *отказоустойчивость* (fault tolerance).



СОВЕТ К ЭКЗАМЕНУ

Не путайте отказоустойчивость и масштабирование. Масштабирование позволяет вам реагировать на дополнительные нагрузки или потребности в ресурсах, при этом все используемые ВМ являются работоспособными. Отказоустойчивость обеспечивается без вашего участия, и в случае сбоев она автоматически перемещает приложение из неисправной в работоспособную систему.

Помимо мониторинга работоспособности ВМ и других ресурсов, поставщики облачных технологий проектируют инфраструктуру таким образом, чтобы обеспечить отказоустойчивость. Например, если у вас есть приложение, работающее на двух ВМ в Azure, Microsoft гарантирует, что эти машины будут распределены в отказоустойчивой инфраструктуре без подверженности системным ошибкам.

ДОПОЛНИТЕЛЬНО ОТКАЗООУСТОЙЧИВОСТЬ В AZURE

Для сдачи AZ-900 вам необязательно разбираться в технических деталях работы отказоустойчивости в Azure, но если вам это интересно, вы можете обратиться к информации по теме по ссылке: <https://docs.microsoft.com/en-us/archive/msdn-magazine/2015/september/microsoft-azure-fault-tolerance-pitfalls-and-resolutions-in-the-cloud>.

Отказоустойчивость предназначена для небольших устранений неисправностей; так, например, происходит перемещение приложения с неисправной на работоспособную ВМ. Однако бывают ситуации, когда происходят сбои посущественнее. Например, природные катаклизмы в регионе могут

оказать воздействие на все ресурсы в его дата-центрах. Это может не только повлиять на доступность, но и без особого плана действий может привести к потере данных.

НА ПРАКТИКЕ АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ И ПРАВИТЕЛЬСТВО

В зависимости от хранимых данных может потребоваться наличие плана аварийного восстановления. Облачные провайдеры, как правило, соблюдают стандарты, установленные такими законами, как HIPAA, и часто предоставляют инструменты, которые можно использовать для проверки степени соответствия. Вы узнаете подробнее о соответствии нормативным требованиям и Azure в главе 5 «Функции идентификации, управления, конфиденциальности и соответствия нормативным требованиям».

Аварийное восстановление означает не только надежное резервное копирование важных данных, но и способность облачной инфраструктуры дублировать ресурсы приложения в незатронутый регион в целях безопасности данных и обеспечения доступности приложения. Планы аварийного восстановления обычно называются планами непрерывности бизнес-процессов и аварийного восстановления (Business Continuity and Disaster Recovery, BCDR). Большинство облачных провайдеров имеют службы, помогающие разработать и реализовать план, отвечающий вашим конкретным потребностям.

Экономические преимущества облака

До сих пор мы обсуждали только преимущества доступности перехода в облако, не затрагивая экономическую выгоду. Далее рассмотрим локальную и облачную модели.

Локальная модель

В локальной модели компания закупает физическое компьютерное оборудование, которое будет использоваться для удовлетворения ИТ-потребностей. Поскольку эти компьютеры являются материальными активами, предназначенными для многолетнего использования, они обычно приобретаются в качестве *капитальных вложений*.

У этой модели есть несколько недостатков. Когда организация закупает компьютерное оборудование, она, как правило, старается поддерживать его в эксплуатации до тех пор, пока оно себя не окупит. В быстро развивающейся компьютерной сфере это может означать, что аппаратное обеспечение устареет задолго до того, как его замена будет финансово целесообразна. Другим важным недостатком этого подхода является ригидность. Закупка и настройка нового оборудования может занять целые месяцы, а в эпоху современных информационных технологий такой подход себя не оправдывает.

ПРИМЕЧАНИЕ ВКЛАДЫ

Предприятиям необходимы финансы для повседневной деятельности. Когда у вашей организации имеются крупные денежные средства, рассчитанные на капитальные расходы, это значительно сокращает объем средств на оперативные задачи.

Облачная модель

Работая в облаке, вы уже не зависите от собственного оборудования: вы берете его в аренду у поставщика облачных услуг. Поскольку вы не приобретаете физические активы, вы переносите расходы на ИТ из капитальных затрат в *операционные расходы* или ежедневные. В отличие от капитальных затрат, операционные расходы ежемесячно отслеживаются, поэтому их гораздо проще корректировать в зависимости от потребностей.

Еще одним важным преимуществом облачной модели является снижение затрат. При использовании облачных платформ необходимые ресурсы выделяются из огромного пула, принадлежащего облачному провайдеру. Поставщик облачных технологий предварительно платит за эти ресурсы, но из-за больших объемов, которые он приобретает, их стоимость значительно снижается. Снижение стоимости при покупке большого количества ресурсов называется *принципом экономии за счет масштаба*, и эта экономия ощущается потребителями облака.

Облачные провайдеры идут дальше, предлагая возможность использования только необходимых ресурсов в конкретный промежуток времени. Обычно такую модель называют *моделью на основе потребления* (consumption-based model). Ее часто применяют на многих уровнях в облачных вычислениях. Как мы уже ранее отмечали, вы можете масштабировать приложение, чтобы использовать только необходимое количество ВМ, а также выбирать их мощность. Вы можете настроить под себя как их количество, так и производительность. Многие облачные провайдеры также позволяют вам оплачивать лишь фактически потребленные ресурсы. Например, если код вашего приложения размещен на облачной платформе, то вы можете платить только за то время, за которое код фактически выполняется на ВМ. Если приложение не используется, то вы ничего не платите.

ДОПОЛНИТЕЛЬНО ВЫЧИСЛЕНИЯ НА ОСНОВЕ ПОТРЕБЛЕНИЯ

Пример модели на основе потребления показан в разделе «Бессерверные вычисления» главы 3 «Ключевые решения и инструменты управления Azure».

Как видите, облачная модель предлагает множество экономических преимуществ по сравнению с традиционной моделью, и это лишь одна из причин, по которой компании быстро переходят на облачные решения.

Навык 1.2: описание различий между Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) и Software-as-a-Service (SaaS)

Как вы теперь уже знаете, одним из преимуществ перехода в облако является то, что часть ответственности за инфраструктуру ложится на поставщика об-

лачных услуг. Однако переход в облако не является чем-то категоричным (или так, или никак). В зависимости от того, как вы используете облако, вам нужно будет найти золотую середину между самостоятельным управлением ресурсами и удобством предоставления подобных услуг от облачного провайдера.

В этом разделе мы рассмотрим три основных типа облачных служб модели разделения ответственности: инфраструктура как услуга (Infrastructure-as-a-Service, IaaS), платформа как услуга (Platform-as-a-Service, PaaS) и программное обеспечение как услуга (Software-as-a-Service, SaaS).

Содержание раздела:

- модель разделения ответственности;
- инфраструктура как услуга (Infrastructure-as-a-Service, IaaS);
- платформа как услуга (Platform-as-a-Service, PaaS);
- программное обеспечение как услуга (Software-as-a-Service, SaaS);
- сравнение типов сервисов.



Модель разделения ответственности

Любому типу сервиса необходим свой уровень ответственности, и такое понимание вещей часто относят к *модели разделения ответственности*. Простым способом визуализации модели является использование облачной пирамиды (рис. 1.2). Нижняя часть пирамиды представляет наибольший уровень контроля за работой ресурсов и, следовательно, наибольшую ответственность. А верхняя часть пирамиды представляет наименьший уровень контроля наряду с наименьшей ответственностью.

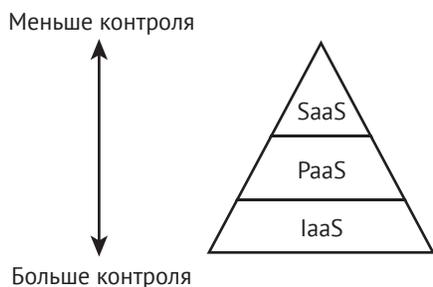


Рис. 1.2 Облачная пирамида

Для выбора правильного соотношения контроля и ответственности вам нужно знать все типы сервисов, их плюсы и минусы.

Инфраструктура как услуга (IaaS)

Инфраструктура (infrastructure) в целом относится к оборудованию, используемому приложением, а IaaS – к виртуализированной инфраструктуре, предлагаемой облачным провайдером. При создании IaaS-ресурса облачный про-

вайдер выделяет вам VM для использования. Иногда поставщики облачных вычислений могут самостоятельно установить операционную систему, однако вы и сами можете сделать это. В любом случае, вы устанавливаете другие необходимые вам службы и приложение.

Поскольку вы управляете установкой операционной системы и других сервисов, IaaS предоставляет вам полный контроль над облачными ресурсами. Однако это также означает, что на вас ложится ответственность за обновление системы безопасности ОС, а также за поиск и устранение неполадок при их возникновении.

Облачный провайдер отвечает только за предоставление VM. Тем не менее благодаря базовой инфраструктуре вы получаете преимущества отказоустойчивости и аварийного восстановления, рассмотренные нами выше.

ДОПОЛНИТЕЛЬНО УДАЛЕННЫЙ ДОСТУП К VM в модели IAAS

Удаленный доступ к VM в модели IaaS позволит вам взаимодействовать с машинами так же, как если бы вы это делали в локальной среде. При переходе на сервисы PaaS и SaaS эта возможность обычно теряется, поскольку инфраструктура управляется облачным провайдером.

На рис. 1.3 изображена VM в IaaS на портале Azure, для которой была выбрана операционная система Ubuntu Server на базе Linux. Как только VM будет успешно запущена на выполнение, на нее автоматически установится Ubuntu Server 18.04. Если обновления не будут устанавливаться, то VM всегда будет работать под управлением ранее установленной версии ОС, и Microsoft уже не будет устанавливать исправления или обновления за вас.

После запуска VM IaaS в облаке вы получаете доступ ко многим услугам облачных провайдеров. Например, Microsoft предлагает сервисы Azure Security Center (Центр безопасности) для обеспечения безопасности VM, Azure Backup для упрощения резервного копирования данных, Azure Log Analytics для выявления и устранения проблем в работе и многое другое.

ДОПОЛНИТЕЛЬНО ПОДРОБНЕЕ ОБ IAAS И AZURE

Дополнительные сведения по IaaS в Azure смотрите по адресу: <https://bit.ly/az900-what-is-iaas>.

Сервисы IaaS позволяют эффективно контролировать расходы, так как оплачиваете вы их только по факту использования. При прекращении работы с VM IaaS выставление счетов за ресурс сразу останавливается. Именно поэтому IaaS – это идеальная платформа для тестирования приложения во время запуска в производство. Команда разработки может запустить VM IaaS, протестировать приложение и по завершении работ прекратить использование.

IaaS часто используют, когда временно нужна одна или несколько мощных VM. Например, представьте, что нужно проанализировать большой объем данных по проекту. Используя VM IaaS в таком случае, можно минимизировать затраты, при необходимости быстро создавать ресурсы и получать всю необходимую вычислительную мощность.

Create a virtual machine

Basics | Disks | Networking | Management | Guest config | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? [Create VM from Azure Marketplace](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription ? ▼

* Resource group ? ▼
[Create new](#)

INSTANCE DETAILS

* Virtual machine name ? ✓

* Region ? ▼

Availability options ? ▼

* Image ? ▼
[Browse all images and disks](#)

* Size ? **Standard D2s v3**
 2 vcpus, 8 GB memory
[Change size](#)

[Review + create](#) [Previous](#) [Next : Disks >](#)

Рис. 1.3 Создание VM IaaS в Azure

Службы IaaS используют возможности масштабирования и эластичности, о которых мы говорили ранее. При надобности количество VM без проблем можно увеличить, а когда потребность в них исчезнет, затем быстро удалить. Для получения большей мощности ЦП, памяти или дискового пространства или ее уменьшения вы можете изменять параметры конфигурации VM.

Словом, службы IaaS являются отличным выбором, если вы хотите, чтобы кто-то за вас осуществлял управление аппаратной инфраструктурой (которая может включать как компьютеры, так и сеть), связанной с вашим приложением, и при этом вы сами могли контролировать установленные и запущенные приложения. В среде IaaS облачный провайдер ничего не устанавливает на VM, поэтому вы всегда знаете ее текущее состояние. Если для вас это важно, то IaaS вам, возможно, подойдет. Еще IaaS предоставляет высокопроизводительные VM под конкретные задачи.

Плюс IaaS также в том, что при размещении приложения и конфигурации в облаке вы платите за них, только когда они активны. Останавливая VM, вы уменьшаете лишние расходы; когда вам снова потребуется приложение, вы можете просто запустить VM с того места, где остановились.

Платформа как услуга (PaaS)

При использовании среды PaaS облачные провайдеры по-прежнему предоставляют вам инфраструктуру, а также еще и операционную систему вместе с установленным программным обеспечением для доступа к базам данных и сетевым системам (часто называемым промежуточное ПО, *middleware*). Также предоставляются дополнительные возможности для создания сложных облачных приложений и управления ими.

PaaS находится в середине облачной пирамиды. Сервисы PaaS обеспечивают гибкость управления приложением, при этом исчезает необходимость в ручной настройке базовых систем на VM. Если при развертывании своего приложения в облаке вы хотите свести к минимуму инвестиции в управление, без колебаний обращайтесь к PaaS.

ПРИМЕЧАНИЕ PaaS И VM

PaaS также использует VM облачных провайдеров, и, как правило, у пользователей нет к ним доступа. В основном управление VM полностью осуществляется облачными провайдерами.



Предположим, вам нужно запустить веб-приложение, использующее фреймворк PHP для подключения к вспомогательной системе управления базой данных. Используя для приложения IaaS, вам сначала нужно убедиться, что вы устанавливаете и настраиваете PHP на своей VM. Следующим шагом станет установка и настройка программного обеспечения, необходимого для подключения к серверной базе данных. В сценарии PaaS вы просто разворачиваете веб-приложение в облачной инфраструктуре, а обо всем остальном позаботится облачный провайдер.

На рис. 1.4 показано веб-приложение в Azure App Service, одно из предложений PaaS в Azure. Данное приложение было размещено на VM, поддерживаемой Microsoft. Обратите внимание, что есть выбор Linux или Windows, однако операционная система управляется Microsoft. Кроме этого, на выбор можно включить Application Insights – службу Azure, которая помогает разобраться в работе приложения и упрощает устранение неполадок, если они возникают.

Любопытным моментом на рис. 1.4 является возможность публикации кода или образа Docker. Docker – это технология, упрощающая процесс упаковки приложения и необходимых для него компонентов в образ, который затем можно развернуть и запустить на другом компьютере в другой среде, при условии что на этом компьютере установлен Docker. Работая с Azure App Service, вам не нужно беспокоиться об установке или настройке Docker: он автоматически входит во все VM App Service как часть предложения PaaS и полностью управляется и поддерживается Microsoft.

Некоторые службы PaaS:

- Azure CDN;
- Azure Cosmos DB;
- Azure SQL Database;
- Azure Database for MySQL;



- Azure Storage;
- Azure Synapse Analytics.

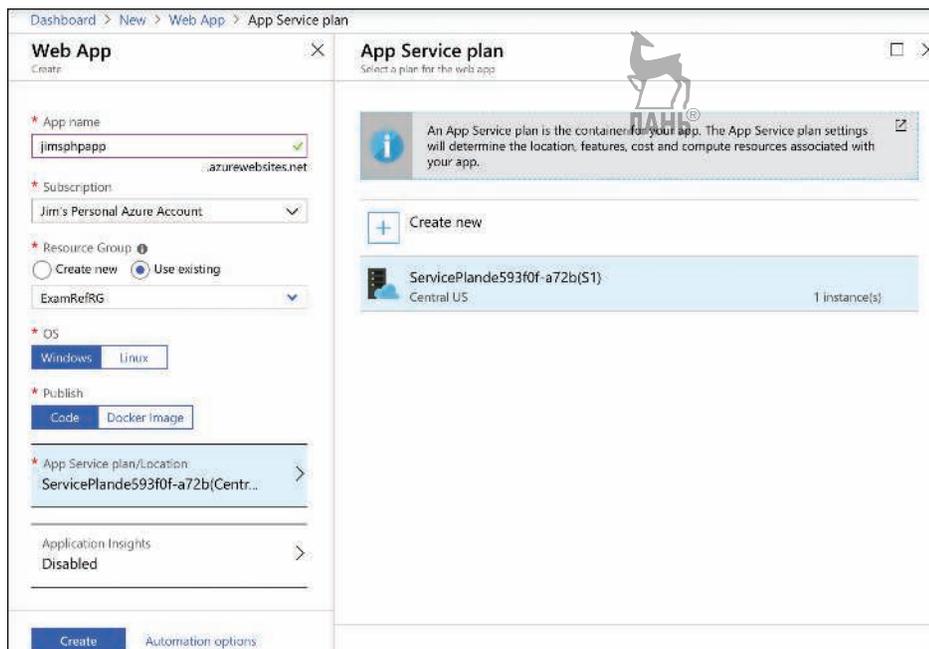


Рис. 1.4 Создание веб-приложения в Azure App Service

В предложение PaaS поставщики облачных вычислений заложили множество фреймворков приложений, таких как PHP, Node.js, ASP.NET, .NET Core, Java, Python и др. Они обычно предлагают несколько вариантов каждого фреймворка, делая возможным выбор той версии, которая совместима с вашим приложением. Облачный провайдер также обеспечивает установку и настройку общих компонентов, необходимых для подключения данных приложения к другим системам. Обычно это означает, что для работы кода в вашем приложении от вас не требуются сложные манипуляции по его настройке, что, несомненно, можно отнести к одному из основных преимуществ сервиса PaaS. Зачастую вы можете перенести приложение из локальной среды в облачную, просто развернув его в облаке. Такую концепцию часто называют простым перемещением (*lift-and-shift*).

Поскольку облачные провайдеры обеспечивают контроль операционной системы и установленных на ВМ компонентов, они могут предложить дополнительные возможности, добавив свои функции. Предположим, что вы хотите добавить возможность входа в веб-приложение, позволив пользователям входить в систему с помощью учетной записи Microsoft, Facebook или Google. Если вы хотите сделать это локально или в среде IaaS, вам понадобится помощь разработчиков в реализации данной функциональности, поскольку подобная задача требует специальных знаний. Либо в вашей компании найдутся разработчики, обладающие соответствующими компетенциями, либо вам нужно бу-

дет их подыскать. Обычно облачные провайдеры уже предлагают такие функции в своих сервисах PaaS, и их включение не сложнее, чем переключение сети и выполнение небольшой конфигурации, характерной для вашего приложения.

В службе PaaS вы найдете и другие преимущества, которые заимствуются ею из облака: отказоустойчивость, эластичность, простое и быстрое масштабирование, функции резервного копирования и аварийного восстановления и многое другое. В действительности возможности, такие как резервное копирование и восстановление данных, часто оказываются более удобными в использовании и функциональными именно в среде PaaS, поскольку облачный провайдер устанавливает на VM PaaS заказное ПО для расширения функциональности.

Как видите, есть настоящий плюс от того, что облачным провайдером контролируются элементы, установленные на выполняющих приложение VM. Однако есть и минусы: например, провайдер контролирует установку исправлений и обновлений ОС и других компонентов.

Обычно о крупных изменениях вам сообщают заранее, чтобы вы смогли сначала протестировать свое приложение на локальном компьютере во избежание сбоев, но вы также лишаетесь возможности выбора момента обновления VM.

ДОПОЛНИТЕЛЬНО ПОДРОБНЕЕ О PAAS И AZURE

Больше о предложениях PaaS в Azure вы найдете тут: <https://bit.ly/az900-whatispaas>.

Программное обеспечение как услуга (SaaS)

Как вам уже известно, для IaaS необходимо, чтобы вы контролировали операционную систему и компоненты промежуточного ПО (middleware) наряду с приложением. При переходе на ступень PaaS вы передаете управление ОС и компонентами промежуточного ПО облачному провайдеру, а сами при этом отвечаете только за код приложения. В верхней части облачной пирамиды, в области SaaS, провайдер занимается обслуживанием сервиса. Другими словами, SaaS – программное обеспечение, предоставляемое и полностью контролируемое облачным провайдером.

Оплата за услуги SaaS гибкая – система оплаты по мере использования. По сути, вы арендуете программное обеспечение у поставщика услуг. Пользователи ПО обычно получают доступ к нему из веб-браузера с возможностью установки приложений, которые будут работать, только пока поступает оплата за подписку SaaS. Одним из главных преимуществ ПО на базе веб-технологий является то, что оно работает практически на любом устройстве, даже на смартфонах. Именно поэтому SaaS-приложения позволяют сотрудникам подключаться при помощи своих устройств.

При использовании служб SaaS вы не только получаете преимущество уже написанного и поддерживаемого ПО, но вместе с этим поставщик облачных услуг будет сам обслуживать и настраивать ваши приложения. Например, если в вашей компании предлагают корпоративную электронную почту, вы можете использовать SaaS-службу Microsoft Office 365. Благодаря службе Exchange On-

line в Microsoft 365 вы можете использовать готовые программные решения электронной почты, пригодные для промышленной эксплуатации, без найма IT-специалистов, и создавать инфраструктуру для ее поддержки. Компания Microsoft сама обслуживает систему. Вы не только выигрываете за счет гибкости и надежности облака, но и можете расслабиться, зная, что Microsoft гарантирует доступность службы Exchange для своих пользователей.

Услуги SaaS предназначены не только для корпоративных целей. Большинство из нас уже используют SaaS-приложения, даже не осознавая этого. Пользуясь Hotmail, Gmail или другим сервисом электронной почты, вы уже являетесь пользователем службы SaaS. Поставщик облачных услуг размещает программное обеспечение электронной почты в облаке, а вы авторизуетесь и используете это ПО с помощью веб-браузера. Для этого вам не требуется ничего знать о ПО. Облачный провайдер может предложить новый функционал с обновлениями, который автоматически будет доступен для вас – вам даже делать ничего не придется. Если облачный провайдер обнаружит в ПО проблему, он сможет решить ее с помощью патча, а вы даже не узнаете, что она была.

Некоторые сервисы SaaS, предоставляемые Microsoft:

- Microsoft 365;
- Xbox Live;
- OneDrive;
- Power Automate (ранее Microsoft Flow).

ДОПОЛНИТЕЛЬНО ПОДРОБНЕЕ О SAAS И AZURE

Больше о сервисах SaaS и Azure смотрите по адресу: <https://bit.ly/az900-whatissaas>.

Сравнение типов сервисов

Мы уже рассмотрели некоторые преимущества и недостатки каждого из трех типов облачных сервисов. Облачная пирамида дает наглядное представление того, как эти типы различаются по уровню ответственности и возможностям контроля. Для закрепления материала давайте теперь рассмотрим типы сервисов в сравнении.

Как вам известно, IaaS предоставляет максимум гибкости. Вы можете установить свое программное обеспечение и компоненты, а еще именно вы осуществляете полный контроль обновлений программного обеспечения и операционной системы. Дополнительным преимуществом является и то, что вы платите за необходимые ресурсы только по факту их использования, поэтому IaaS позволяет вам сократить операционные расходы. Несмотря на экономию, полученную от отключения неиспользуемой VM, другие существенные затраты, связанные с установкой и обслуживанием ПО, могут перекрыть это преимущество.

Paas предлагает гибкость, подобную IaaS, – без необходимости в управлении инфраструктурой. В службе Paas вы отвечаете только за свое приложение, установленное в облаке. Приложение может быть как вашим собственным, так и разработанным другими программистами (например, система WordPress или

готовое решение e-commerce), но в любом случае вы несете за него ответственность. Услуги PaaS пользуются спросом среди команд разработчиков, которые стремятся легко и быстро переместить существующие приложения в облако. Эти услуги зачастую предлагают множество вариантов, максимально упрощающих процесс развертывания. Облачный провайдер PaaS устанавливает на платформу собственное ПО и дополнительные функции, поэтому и функционал сервисов PaaS обширнее, чем у IaaS. Однако обновления и изменения версий базового ПО могут повлиять на приложения: это может сказаться на увеличении затрат, вызванных необходимостью в их дополнительном тестировании, поскольку облачный провайдер может опубликовать изменения уже после проведенного тестирования.

Службы SaaS немного отличаются от IaaS или PaaS, так как они полностью управляются и поддерживаются поставщиком услуг. Вы не можете установить свое ПО, используя сервис SaaS, поэтому решающим фактором станет соответствие предоставленного ПО вашим потребностям. Преимущество службы SaaS в том, что она в значительной степени снимает ИТ-нагрузку с вашей компании и позволяет всем сотрудникам организации получать доступ к ПО на нескольких устройствах, имеющих доступ в интернет. Вы также можете воспользоваться преимуществами резервного копирования данных, которые облачный провайдер включает в свою инфраструктуру. Однако SaaS не позволяет вам настраивать приложение, а также не дает ни малейшего контроля над его конфигурацией.

НА ПРАКТИКЕ РАЗБИРАЕМСЯ СО СЛОЖНОСТЯМИ СОВРЕМЕННОГО МИРА ИТ

В зависимости от ваших потребностей выбор конкретного типа облачной службы может быть как простым, так и сложным. Например, вы можете работать в отрасли, где часть данных должна храниться только локально. У вас также могут быть старые системы, которые не готовы к переносу в облако, но вам нужны облачные приложения для использования этих старых систем. В следующем разделе навыков вы узнаете больше о том, как справиться с такими сложностями.

Навык 1.3: описание различий между моделями общедоступного, частного и гибридного облаков

Говоря простым языком, облако предоставляет инфраструктуру и приложения через интернет. Ранее говорилось о простых примерах, которые можно отнести к «традиционным» облачным технологиям, когда любой пользователь в интернете может получить доступ к вашему приложению. Несмотря на то что в вашем приложении могут использоваться средства проверки подлинности пользователей (аутентификация, authentication), чтобы «неправильные» люди не получили доступ, ваше приложение все еще работает на ВМ, подключенных к интернету и доступных через публичные сети.

ДОПОЛНИТЕЛЬНО РАЗБИРАЕМСЯ СО СЛОЖНОСТЯМИ СОВРЕМЕННОГО МИРА ИТ

Вы можете встретить ссылки на четвертую облачную модель, называемую общественным облаком (community cloud). Общественное облако похоже на частное, но вместо ресурсов, предназначенных для одной компании, они предназначены для сообщества компаний или отдельных лиц, которые совместно им управляют. Например, больницы могут использовать общественное облако, специально разработанное для исполнения закона HIPAA или других нормативных актов в области здравоохранения. Финансовые учреждения также могут использовать общественное облако, обеспечивающее соблюдение нормативных положений, касающихся банков и финансовой торговли.

Общественные облака не являются частью AZ-900, но если вы вдруг столкнетесь с этим термином во время подготовки к экзамену, вам нужно понимать, что он означает.

Традиционная облачная модель называется *общедоступным облаком* (public cloud). Помимо модели общедоступного облака, предприятия также могут использовать *частное облако* (private cloud) с локальной инфраструктурой. И последняя модель – модель *гибридного облака* (hybrid cloud), которая представляет собой сочетание моделей публичного и частного облаков.

Содержание раздела:

- облачные вычисления;
- общедоступное облако;
- частное облако;
- гибридное облако.

Облачные вычисления

В начале главы я упомянул, что облако *обычно* представляет собой инфраструктуру и приложения, доступные через интернет. Большинство людей воспринимают концепт «облако» именно в таком контексте, однако облачные ресурсы не всегда связаны с общедоступным интернетом.

Лучше всего понимать облачные вычисления в качестве вычислительных ресурсов, взаимосвязанных сетью, но даже это определение не до конца описывает само облако. Под облачными вычислениями также понимают масштабируемые и гибкие системы. Объединив эти концепции с распределительными вычислительными ресурсами, доступными в сети, вы получите возможности облачных вычислений.

Как видите, точно определить облачные вычисления не совсем просто. Исследование разных моделей поможет вам понять, что такое облачные вычисления.

Общедоступное облако

Наиболее распространенной облачной моделью является общедоступное облако. В этой модели используется общая инфраструктура, доступная в публичной сети. Сеть, хранилище и ВМ, используемые приложением, предоставляют

ся облачным провайдером и совместно используются всеми потребителями публичного облака. Microsoft Azure, Amazon Web Services (AWS), а также Google Cloud Platform – все это примеры общедоступных облаков.

ПРИМЕЧАНИЕ ОБЛАКО И ИНТЕРНЕТ

Многие облачные сервисы предоставляют доступ из интернета, но это не означает, что они будут доступны всем. Практически всегда для доступа требуется аутентификация.

Вы узнаете больше о безопасности облачных ресурсов в главе 4 «Описание функций общей и сетевой безопасности».

Модель общедоступного облака выгодна тем, что позволяет легко и быстро мигрировать в облако. Поскольку у облачного провайдера уже есть настроенная инфраструктура, то все, что вам нужно сделать, – это выбрать нужный тип облачного сервиса. Вы также получаете преимущества от возможности быстрого и эффективного масштабирования, поскольку у облачного провайдера все ресурсы уже готовы к использованию по первому запросу.

Как уже ранее говорилось, еще одно преимущество модели общедоступного облака заключается в эффективном контроле ресурсов, поскольку вы платите только за те ресурсы, которые используете. Если вам нужно увеличить количество ВМ, облачный провайдер готов вам их предоставить. Вам не нужно самостоятельно поддерживать пул ресурсов. Вы можете воспользоваться ресурсами, в которые инвестировал сам облачный провайдер.

ВАЖНО ОКРУЖЕНИЕ С НЕСКОЛЬКИМИ АРЕНДАТОРАМИ

Поскольку вы используете ресурсы в общедоступном облаке совместно с другими людьми, общедоступное облако еще иногда называют «окружением с несколькими арендаторами» (multitenant environment).

В то время как гибкость и удобство общедоступного облака являются явными плюсами, также имеются и недостатки. Прежде всего вы отказываетесь от контроля над инфраструктурой. Степень контроля зависит от расположения в облачной пирамиде, но, несмотря ни на что, облачный провайдер будет контролировать часть вашей инфраструктуры.

При работе в общедоступном облаке также могут возникнуть проблемы с безопасностью. Задействованная в облаке сеть является общедоступной частью интернета, которая доступна любому, у кого есть интернет-соединение. Во избежание несанкционированного доступа к вашему приложению и данным вам необходимы меры безопасности. Облачные провайдеры осознают данную необходимость и обеспечивают такую безопасность, однако не всегда предоставляемые меры соответствуют вашим требованиям безопасности.

Другим недостатком общедоступного облака является то, что оно привязывает вас к конкретной конфигурации, определенной облачным провайдером. Предположим, у вас есть приложение, которому требуется большой объем дискового хранилища, но для его запуска нужна только однопроцессорная система. Чтобы удовлетворить требования к дисковому пространству, облачный

провайдер может потребовать масштабирование до мощной, многопроцессорной ВМ, что приведет к ненужному увеличению затрат.

ДОПОЛНИТЕЛЬНО ПОДРОБНЕЕ ОБ ОБЩЕДОСТУПНОМ ОБЛАКЕ

Дополнительно об общедоступном облаке и Azure смотрите по ссылке: <https://bit.ly/az900-publiccloud>.

Частное облако

Модель частного облака предоставляет многие заманчивые преимущества облака (например, простое масштабирование и эластичность) в специальной среде, предназначенной для одной компании. Частное облако может размещаться как в локальной среде, так и на стороннем хостинг-провайдере.

ВАЖНО ОКРУЖЕНИЕ С ОДНИМ АРЕНДАТОРОМ

Поскольку ресурсы в частном облаке предназначены для одной организации, то частное облако нередко называют «окружением с одним арендатором» (single-tenant environment).

Две основные причины, по которым компании выбирают частное облако: конфиденциальность и вопросы отраслевого регулирования. В отличие от общедоступного, частное облако работает в частной сети, доступной только для одной организации. Такие предприятия, как банки и медицинские учреждения, могут иметь правила, которые предписывают недоступность некоторых данных через интернет. В подобных ситуациях частное облако может стать хорошим выбором. Еще одним примером пользователей частных облаков является индустрия круизных судов. Круизные суда плавают в отдаленных районах без доступа в интернет. Однако их владельцам необходимы преимущества облаков для повседневной работы сложных судовых систем.



СОВЕТ К ЭКЗАМЕНУ

Иногда вы можете услышать о том, что частное облако состоит из инфраструктуры, принадлежащей отдельной компании, но это не всегда так. Если компания локально использует частное облако, она обычно владеет оборудованием и инфраструктурой, необходимыми для частного облака.

Однако эта же компания может также разместить частное облако в стороннем центре обработки данных. В этом случае инфраструктура принадлежит хостинг-провайдеру, но она по-прежнему полностью выделена под задачи одной компании, оплачивающей это частное облако. Суть в том, что разница между публичным и частным облаками заключается в конфиденциальности инфраструктуры и данных. Не имеет значения, кто владеет инфраструктурой.

У частного облака есть и свои недостатки. При его локальном размещении вы, вероятнее, потратите столько же информационных технологий, сколько бы потратили в необлачной среде. Вам придется платить за оборудование и вир-

туализированные системы. Вам также понадобится ИТ-персонал, который сможет управлять программным обеспечением и инфраструктурой вашего облака.

Предотвращение расходов на ИТ является одной из основных причин, по которым компании предпочитают использовать сторонних хостинг-провайдеров для частных облаков. Однако у этого выбора есть и свои недостатки. Так, передавая управление частным облаком сторонней компании, вы теряете контроль над важными аспектами (например, над безопасностью данных). Зачастую достичь полной прозрачности при работе со сторонними провайдерами невозможно, при этом нет гарантий того, что ваши данные всегда будут в надлежащей безопасности.



ДОПОЛНИТЕЛЬНО ПОДРОБНЕЕ О ЧАСТНОМ ОБЛАКЕ

Дополнительную информацию о частных облаках вы получите по ссылке <https://bit.ly/az900-privatecloud>.

Гибридное облако

Вы, наверное, уже догадались, что под гибридным облаком понимается сочетание публичного и частного. В гибридной облачной среде приложение может быть запущено в общедоступном облаке и при этом получать доступ к данным, которые надежно хранятся в локальной среде. Или сценарий, в котором ваше приложение и большинство его ресурсов расположены в частном облаке, но вы хотели бы использовать службы или инфраструктуру из общедоступного облака. На самом деле количество сценариев, которые подходят для гибридной модели, почти бесконечно.

Нередко модели гибридного облака являются для компаний первым опытом работы с облаком. Большинство организаций используют устаревшие локальные системы, перенос которых в облако – не из дешевых удовольствий. Но если компания все же захочет воспользоваться преимуществами облачных сервисов, она может переместить в облако лишь часть определенной системы, оставив устаревшую систему локально до определенного момента.

Не все компании внедряют гибридную облачную модель из-за устаревших систем. В некоторых случаях компаниям нужно сохранить полный контроль над частью своей инфраструктуры или данных. Они также могут принять решение о создании локальной инфраструктуры параллельно с созданием своего общедоступного облака.

ВАЖНО ГИБРИДНЫЕ РЕШЕНИЯ НЕ ВСЕГДА ВКЛЮЧАЮТ ЛОКАЛЬНЫЕ СИСТЕМЫ

Вспомним, что частное облако – это облако, предназначенное для одной организации. Оно необязательно находится на территории предприятия: оно может размещаться в стороннем центре обработки данных, поэтому гибридная облачная модель может сочетать сторонний центр обработки данных и общедоступное облако.

Зачастую при использовании гибридной модели компаниям необходима возможность подключения частной локальной сети к сети общедоступного

облака. Для этого облачные провайдеры предлагают множество технологий. Примерами таких технологий в Microsoft Azure являются виртуальные сети (virtual networks), гибридные подключения (hybrid connections) и сервисные шины (service buses).

ДОПОЛНИТЕЛЬНО ПОДРОБНЕЕ О СЕТЕВЫХ ВОЗМОЖНОСТЯХ AZURE

Сетевые возможности Azure мы рассмотрим в разделе «Навык 2.2» главы 2 и разделе «Навык 4.2» главы 4.

Может показаться, что у гибридной облачной модели нет недостатков, но это не так. Прежде всего команды разработчиков приложений должны убедиться, что данные, совместно используемые общедоступным и частным облаками, совместимы между собой. Для этого могут потребоваться специальные навыки разработки и сложные способы устранения неполадок. Устройство сети в гибридной модели также может быть довольно сложным, особенно потому, что сетевая инфраструктура сторонних провайдеров может вызвать проблемы, которые не так просто устранить. Наконец, распространение ресурсов между общедоступным и частным облаками может привести к замедлению работы приложений из-за географической удаленности между системами, на которых выполняется приложение, и данными, используемыми приложением. Все эти особенности должны быть тщательно взвешены при принятии решения об использовании гибридного облака.

Чтобы упростить использование гибридного облака для своих клиентов, корпорация Microsoft предоставляет Azure Stack. Azure Stack продается в виде пакета, включая программное обеспечение и проверенные аппаратные средства для его запуска. Azure Stack позволяет локально запускать службы Azure, что упрощает перенос приложений в облако с минимальным объемом работы. Поскольку оборудование является частью Azure Stack, Microsoft сама проверяет его совместимость с Azure, а вам остается только управлять им.

Мысленный эксперимент

Давайте применим полученные в этой главе знания. Смотрите ответы в следующем разделе.

Вы работаете в компании Contoso Medical Group (CMG), и ваш менеджер разочарован одним из ваших часто используемых приложений. ИТ-отдел CMG ограничен в ресурсах и испытывает трудности в обеспечении доступности приложения.

Команда разработчиков часто обновляет приложение, но из-за отсутствия знаний о методах развертывания у них есть возможность только прямого копирования файлов, что вызывает проблемы с отслеживанием вносимых изменений. В то же время команда разработчиков не обладает данными, которые бы показывали корректность работы приложения.

Два дня назад, как раз перед обновлением медицинской документации, ситуация приобрела критический характер. Активность приложения была не-

типично высокая, из-за чего произошла перегрузка системы, и она перестала отвечать на запросы. IT-специалисты определили, что серверу не хватает ресурсов, однако создание второго сервера заняло бы два часа.

Для поиска решения проблем к вам может обратиться ваш менеджер. Независимо от предложенного вами решения необходимо учитывать, что медицинские данные в этом приложении подпадают под закон HIPAA (действует в США). Вашему менеджеру нужно, чтобы CMG сохранил весь контроль над данными, а также чтобы был тщательный контроль расходов.

Вы пришли к выводу, что CMG следует перенести приложение в облако, но вам нужно убедить в этом своего менеджера.

Ответьте на следующие вопросы:

1. Какой тип облачной службы вы бы порекомендовали?
2. Как бы вы обосновали свой выбор относительно проблем, с которыми сталкивается ИТ-команда?
3. Как бы вы обосновали свой выбор относительно проблем, с которыми сталкивается команда разработчиков?
4. Какие еще преимущества порадуют вашего менеджера, если будет реализована ваша рекомендация?
5. Что вы можете сделать для соответствия требованиям, связанным с медицинской документацией и необходимостью их контроля?

Ответы на мысленный эксперимент

В этом разделе мы обсудим ответы на вопросы из предыдущего раздела.

1. В данной ситуации наиболее разумным станет использование службы PaaS. Для среды IaaS необходимо, чтобы ИТ-отдел производил управление ВМ, что вам не подходит. Сервис SaaS же предоставляет готовое программное обеспечение, а вам нужно будет запускать свое приложение компании в облаке.
2. ИТ-отдел испытывает нехватку ресурсов, ему трудно поддерживать доступность приложения. В службе PaaS управление ВМ, выполняющих приложение, передается облачному провайдеру, который также предлагает вам соглашение об уровне обслуживания (SLA), обеспечивая тем самым круглосуточную доступность приложения. ИТ-специалисты получают преимущества от простого масштабирования в облачной среде. Они смогут добавлять новые серверы практически мгновенно, а не за два часа.
3. В службе PaaS облачный провайдер предлагает гибкие варианты развертывания, которые упрощают обновление приложения с помощью выбранного вами метода. Провайдер также обеспечивает ведение журнала, чтобы команда разработчиков могла отслеживать внесенные в приложение изменения. Функции диагностики службы PaaS (например, Azure Application Insights) предоставляют подробные сведения о работе приложения, также они могут предупреждать о проблемах с кодом.

4. Ваш менеджер желает снизить расходы, и переход в облако должен отвечать данной потребности. Ваш ИТ-отдел уже настроил второй сервер, делая возможным использование дополнительной мощности (при необходимости). Однако такое увеличение нагрузки носит временный характер. Данное решение было принято из-за дедлайна для подачи записей. В следующий раз, когда наступит крайний срок, вам опять понадобится второй сервер. Переход в облако дает вам преимущества простого масштабирования и эластичности, позволяя запускать второй сервер при необходимости, а после без труда его отключать для экономии расходов.
5. Используя гибридную облачную модель, вы можете хранить конфиденциальные медицинские данные в локальной среде, используя при этом преимущества приложения, работающего в облаке.

Краткое содержание главы

В этой главе вы познакомились с общими понятиями, связанными с облаком. Вы узнали о преимуществах перехода в облако, о различных типах и о доступных моделях облачных служб. Ниже представлены ключевые понятия главы.

- Облачные провайдеры предлагают соглашения об уровне обслуживания (SLA), которые гарантируют определенный уровень доступности, но только для подконтрольных систем.
- Переход в облако может помочь избежать простоев, вызванных перебоями в работе сети, систем и электроснабжения. Также он может помочь, если вам необходимо диагностировать проблемы с приложением или с внешней системой, используемой приложением.
- Приложения можно масштабировать вертикально с помощью более мощной ВМ, если требуется добавить дополнительные процессоры или больше памяти.
- Можно масштабировать горизонтально, если вам нужно добавить больше ВМ для обработки дополнительной нагрузки.
- Облачные провайдеры предоставляют способы автоматического масштабирования на основе использования шаблонов и ресурсов, времени суток. Это называется *эластичностью*.
- Облачные провайдеры следят за состоянием инфраструктуры. Когда ВМ выходит из строя, облачный провайдер может автоматически перенести ваше приложение на работоспособную ВМ без вашего участия. Это называется *отказоустойчивостью*.
- Облачные провайдеры также работают в нескольких центрах обработки данных, расположенных в разных регионах мира. Если стихийное бедствие (или другое ЧП) происходит в одном регионе, то при активации возможности дублирования своей среды в других регионах вы можете переключиться на другой. Такого рода планирование называется непрерывностью бизнес-процессов и аварийного восстановления (Business Continuity and Disaster Recovery), и зачастую облачные провайдеры обладают

функциями, облегчающими реализацию плана. Все это нередко называют аварийным восстановлением.

- Поскольку вы используете инфраструктуру, принадлежащую облачному провайдеру, переход в облако снижает ваши *капитальные затраты*, где основные расходы связаны с обслуживанием инфраструктуры и другими крупными покупками. Облачные провайдеры используют *принцип экономии за счет масштаба*, покупая большое количество инфраструктуры для использования потребителями облачных технологий.
- Ежедневные расходы (*производственные затраты*) в облаке могут уменьшиться, так как вы платите только за те ресурсы, которые используете. Эта *модель, основанная на потреблении*, является ключевым преимуществом облака.
- В облачной пирамиде отражается идея о том, что усиление контроля над ресурсами означает повышение вашей ответственности. Снижение контроля приводит к повышению ответственности для облачного провайдера. Данная концепция называется *моделью разделения ответственности*.
- Инфраструктура как услуга (Infrastructure-as-a-Service, IaaS) предлагает инфраструктуру, работающую в облаке, но вам будет необходимо самостоятельно поддерживать операционную систему и установленные приложения. Службы IaaS предлагают наибольший контроль в облаке, но вместе с этим и наибольшую нагрузку с точки зрения управления.
- Платформа как услуга (Platform-as-a-Service, PaaS) передает облачному провайдеру управление инфраструктурой, операционной системой и дополнительными компонентами, установленными на ВМ. А вы отвечаете только за свое приложение. Сервисы PaaS также предлагают множество дополнительных возможностей, которые упрощают добавление новой функциональности в приложение без написания сложного кода. Команды разработки имеют широкий спектр доступных методов развертывания, а облачный провайдер зачастую автоматизирует большую часть процесса.
- Программное обеспечение как услуга (Software-as-a-Service, SaaS) предоставляет готовое приложение в облаке, к которому обычно подключаются с помощью веб-браузера. В сервисе SaaS облачный провайдер самостоятельно всем управляет. Вы всего лишь арендуете программное обеспечение у облачного провайдера. Большим преимуществом SaaS является то, что он делает приложения легкодоступными для сотрудников на местах с любых устройств.
- Модель общедоступного облака иногда называют «окружением с множеством арендаторов». Несколько компаний и пользователей используют одну и ту же инфраструктуру. ВМ и другая инфраструктура выделяются пользователям по мере необходимости, а когда они больше не нужны, они возвращаются в пул для использования другими арендаторами. Сеть публично доступна через интернет, но вы также можете использовать механизмы обеспечения безопасности для контроля доступа к вашим ресурсам.
- Модель частного облака иногда называют «окружением для одного арендатора». Вся инфраструктура является частной для отдельного лица или

компании, а сеть доступна только в частном облаке. Она не выходит в интернет. Во многих случаях инфраструктура, используемая в частном облаке, принадлежит самой компании, но не всегда. Частное облако можно разместить в стороннем центре обработки данных.

- Модель гибридного облака представляет собой сочетание моделей публичного и частного облаков. Гибридные облака часто применяются, когда компании необходимо использовать локальные ресурсы в облачном приложении.



ГЛАВА 2

Описание основных служб Azure

https://t.me/it_books



В главе 1 «Концепции облачных технологий» вы узнали об облаке и о пользе использования облачных служб. Microsoft Azure лишь упоминалась нами в качестве примера облачных служб.

В этой главе мы подробнее расскажем о многих службах и решениях, которые предлагает Azure. Вы получите представление о ключевых концепциях архитектуры Azure, которые применяются ко всем службам Azure. Мы затронем центры обработки данных Azure и механизмы реализации отказоустойчивости и аварийного восстановления благодаря размещению инфраструктуры Azure во всех странах мира. Вы также познакомитесь с зонами доступности, предоставляемыми Microsoft для обеспечения работоспособности в случае, когда в отдельном центре обработки данных Azure возникает проблема.

Вы узнаете о том, как управлять ресурсами Azure и отслеживать их, а еще о том, как работать с группой ресурсов при помощи групп ресурсов Azure (Azure Resource Groups). Вы научитесь использовать группы ресурсов Azure не только для планирования и управления ими, но и для классификации операционных расходов.

Чтобы понять, как работают группы ресурсов и как работает Azure «под капотом», важно осознать базовую систему Azure Resource Manager (ARM), используемую Azure для управления всеми ресурсами. Вы узнаете о преимуществах ARM и увидите, как ARM открывает широкие возможности для быстрого и простого развертывания реальных решений в Azure.

Получив базовое понимание платформы Azure, вы познакомитесь с основными продуктами, предлагаемыми Microsoft, такими как Azure VM, Azure App Service, службах, которые упрощают процесс работы с хранилищем и сетевыми технологиями, памятью и службами баз данных. Вы также узнаете об Azure Marketplace и о том, как с его помощью создавать и развертывать сложные решения в несколько кликов. Благодаря знаниям, полученным в начале главы, Azure Marketplace не будет выглядеть как колдовство.

Если вам кажется, что это слишком много для одной главы, то вы правы! Для того чтобы сдать экзамен AZ-900, важно иметь понимание всех обозначенных тем. Благодаря базовым знаниям об облачных технологиях из главы 1

«Концепции облачных технологий» вам будет проще понять вещи, специфичные для Azure.

Навыки, описанные в этой главе:

- описание основных компонентов архитектуры Azure;
- описание ключевых ресурсов, доступных в Azure.



Навык 2.1: описание основных компонентов архитектуры Azure

Попросив любого руководителя перечислить пять наиболее важных активов своей компании, вы, вероятнее всего, получите ответ, в котором данные компаний займут первые строки списка. Мир, в котором мы живем, вращается вокруг данных. Взгляните на такие компании, как Facebook и Google. Они предлагают услуги, которые нам интересны. Все любят смотреть на фотографии друзей и семьи на Facebook (вперемежку с другой неприятной информацией). А кто из вас не гуглил что-либо в интернете? Facebook и Google предлагают эти услуги не потому, что они хотят быть хорошими, а потому, что для них это способ собрать большой объем данных о своих клиентах, и именно эти данные являются их самым ценным активом.

Facebook и Google не одни такие. Многие компании располагают огромными объемами данных, имеющих ключевое значение для их бизнеса, и обеспечение безопасности этих данных является краеугольным камнем бизнес-решений. Вот что останавливает многие компании от перехода в облако. Они боятся потерять контроль над своими данными. Их пугает не только то, что злоумышленники могут завладеть конфиденциальными данными, но и то, что эти данные могут быть навсегда утеряны – их будет либо сложно, либо невозможно воссоздать.

В Microsoft хорошо осведомлены о подобных опасениях. Платформа Azure была полностью создана с нуля как раз для того, чтобы люди начали доверять облачным технологиям. Давайте рассмотрим основные архитектурные компоненты, благодаря которым мы можем доверять облачным услугам от Microsoft.

Содержание раздела:

- регионы Azure;
- зоны доступности;
- группы ресурсов;
- подписки Azure;
- группы управления;
- Azure Resource Manager (ARM).

Регионы Azure

Термин «облако» иногда заставляет людей думать об Azure как о чем-то туманном, неясно видимом, но это ошибочно. Хотя при описании Azure и используются абстрактные понятия, сама платформа работает на физических устройствах. В конце концов, мы же говорим о компьютерах!

Чтобы службами Azure смогли воспользоваться широкие массы, Microsoft создала границы, называемые *географическими*. Географические границы часто совпадают с границами той или иной страны, и для этого есть веские основания. В различных странах существуют свои правила обработки и хранения данных, которые должны поддерживаться в дата-центрах Azure. Многим компаниям (особенно тем, которые обрабатывают конфиденциальные данные) гораздо удобнее, если их данные хранятся в пределах страны, в которой они осуществляют свою деятельность.

В Azure существует множество географических регионов. Например, есть географическое расположение США, Канады, Великобритании и других стран. Любая территория разбита на несколько регионов, каждый из которых, как правило, находится на расстоянии нескольких сотен километров друг от друга. Например, на территории Соединенных Штатов есть несколько регионов, в том числе Центральная часть США в Айове, восточная часть США в Вирджинии, западная часть США в Калифорнии и южно-центральная часть США в Техасе. Из-за дополнительных нормативных положений по отношению к государственным данным Microsoft также управляет изолированными регионами, полностью под них предназначенными.

На каждой территории Microsoft создала еще одну логическую границу под названием *региональная пара*, где каждая содержит по два региона. Когда Microsoft нужно обновить платформу Azure, она это делает в одном регионе региональной пары. Обновив платформу, она переходит в следующий регион региональной пары для обновления. Такой способ гарантирует, что обновления не окажут воздействия на ваши службы, работающие в рамках региональной пары.

ДОПОЛНИТЕЛЬНО РЕГИОНАЛЬНАЯ ПАРА

Чтобы воспользоваться преимуществами региональных пар, вам необходимо обеспечить избыточное развертывание ресурсов под каждый регион в паре. Со списком всех региональных пар вы можете ознакомиться на следующем сайте: <https://bit.ly/az900-regionpairs>.



СОВЕТ К ЭКЗАМЕНУ

Важное значение имеет тот факт, что любая территория содержит как минимум два региона, разделенных большим расстоянием. Именно так Azure поддерживает аварийное восстановление, и, скорее всего, вопросы об этом будут включены в экзамен. Мы подробнее рассмотрим данный аспект позже.

В каждом регионе Microsoft создала центры обработки данных (реальные здания), содержащие настоящее оборудование, используемое Azure. Эти цент-

ры имеют охлаждаемые системы в зданиях, где размещаются серверные стойки с физическим компьютерным оборудованием. Каждый регион работает на своей собственной сетевой инфраструктуре, и Microsoft создает сетевые структуры с низким значением задержки. Таким образом, все службы Azure, которые есть в определенном регионе, соединены между собой надежным и быстрым сетевым подключением.

ДОПОЛНИТЕЛЬНО КЛИЕНТЫ ВИДЯТ ТОЛЬКО РЕГИОНЫ

Когда клиент создает ресурсы Azure, отображается только регион. Концепция географических регионов – это внутренняя реализация Azure, о которой клиенты ничего не знают, когда используют Azure. Клиенты также не имеют представления о концепции региональных пар, но они видят регионы пары.

Любой центр обработки данных содержит изолированный источник питания и генераторы на случай отключения электроэнергии. Весь сетевой трафик, входящий и исходящий из центра обработки данных, проходит через пассивную оптоволоконную сеть Microsoft по кабелю, принадлежащему или арендованному корпорацией. Даже данные, передающиеся между регионами на разных континентах, проходят по оптоволоконным кабелям Microsoft, проложенным по дну океанов.

ДОПОЛНИТЕЛЬНО МОЩНОСТЬ ЦЕНТРА ОБРАБОТКИ ДАННЫХ

По состоянию на 2018 год все центры обработки данных Microsoft использовали более 50 % возобновляемой энергии (солнечной, ветряной и т. д.). К 2020 году планировали использовать 60 %, а в долгосрочной перспективе рассматривалось стопроцентное применение экологически чистой энергии.

Чтобы не зависеть от сторонних поставщиков электроэнергии, Microsoft также инвестирует в разработку полностью интегрированных топливных элементов, работающих на природном газе. Топливные элементы не только обеспечивают чистую электроэнергию, но и устраняют колебания мощности и другие неудобства, связанные с использованием электросети.

В целях защиты данных в Azure от различных ЧП и сбоях, возникших из-за возможных проблем в отдельном регионе, клиентам рекомендуется реплицировать данные (размещать их копии) в нескольких регионах. Если, например, южно-центральная часть США пострадала от разрушительного торнадо (к сожалению, частое явление в Техасе), данные, копии которых были перенесены в североцентральный регион США в штате Иллинойс, будут вне опасности и доступны вам. Для уверенности в том, что скорость работы приложений по-прежнему останется высокой, Microsoft обеспечивает процесс отправки, обработки и возврата сигнала в 2 миллисекунды между регионами или даже быстрее.

Зоны доступности

Тот факт, что регионы физически разделены сотнями километров, защищает пользователей Azure от потери данных и простоев приложения в связи с ката-

строфами в отдельных регионах. Однако важно, чтобы данные и приложения оставались доступны при возникновении проблем в центре обработки данных конкретного региона. По этой причине Microsoft разработала зоны доступности (availability zones).

ПРИМЕЧАНИЕ НАЛИЧИЕ ЗОН ДОСТУПНОСТИ

Зоны доступности поддерживаются не во всех регионах и не для всех служб Azure. Актуальный список регионов с поддержкой зон доступности вы найдете здесь: <https://bit.ly/az900-azones>.

В каждом регионе есть минимум три зоны доступности, и поскольку все зоны существуют в своих собственных центрах обработки данных, у каждой из них свое водоснабжение, система охлаждения, сеть и изолированный от других зон источник питания. Размещая службу Azure в двух или более зонах, вы можете получить высокую доступность тогда, когда возникает проблема в одной зоне.



СОВЕТ К ЭКЗАМЕНУ

Зоны доступности обеспечивают высокую доступность и отказоустойчивость, но не аварийное восстановление. При локализованной аварии, например при пожаре в центре обработки данных с одной зоной, вам очень пригодятся зоны доступности.

Поскольку зоны доступности расположены в одном и том же регионе Azure, в случае крупномасштабного стихийного бедствия, такого как торнадо, вы можете оказаться незащищенными. Другими словами, зоны доступности – это лишь один из элементов общей системы аварийного восстановления и отказоустойчивости.

Поскольку зоны доступности предназначены для обеспечения повышенной доступности инфраструктуры, не все службы их поддерживают. Например, в Azure есть сервис под названием сертификат службы приложений, или же App Service Certificate, который позволяет вам приобретать SSL-сертификат и управлять им через Azure. Смысла в размещении App Service Certificate в отдельной зоне доступности нет, потому как он не является компонентом инфраструктуры.

На данный момент зоны доступности поддерживаются следующими службами Azure:

- виртуальные машины Windows;
- виртуальные машины Linux;
- масштабируемые наборы виртуальных машин;
- служба Azure Kubernetes;
- управляемые диски;
- хранилище, избыточное между зонами;
- стандартные балансировщики нагрузки;
- общедоступный IP-адрес;
- VPN-шлюз;

- шлюз ExpressRoute;
- шлюз приложений V2 (Application Gateway V2);
- брандмауэр Azure;
- обозреватель данных Azure;
- база данных SQL;
- кеш Azure для Redis;
- Azure Cosmos DB;
- центры событий (Event Hubs);
- служебная шина (Service Bus, только уровень «Премиум»);
- сетка событий (Event Grid);
- доменные службы Azure AD;
- среды службы приложений внутреннего балансировщика нагрузки (App Service Environments ILB).



ПРИМЕЧАНИЕ БУДЬТЕ В КУРСЕ ИЗМЕНЕНИЙ В AZURE

Следите за новостями, связанными с обновлениями Azure, благодаря блогу Azure: <https://azure.com/blog>.

Разворачивая службу в двух или более зонах доступности, вы обеспечиваете максимальную доступность для этого ресурса. Вообще, Microsoft гарантирует соглашение об уровне обслуживания в 99,99 % времени работоспособного состояния для виртуальных машин Azure, только если две или более ВМ развернуты в двух или более зонах. На рис. 2.1 показаны преимущества использования нескольких зон. Как видите, даже несмотря на то, что третья зона доступности по неизвестной причине была отключена от интернета, зоны 1 и 2 еще работают.

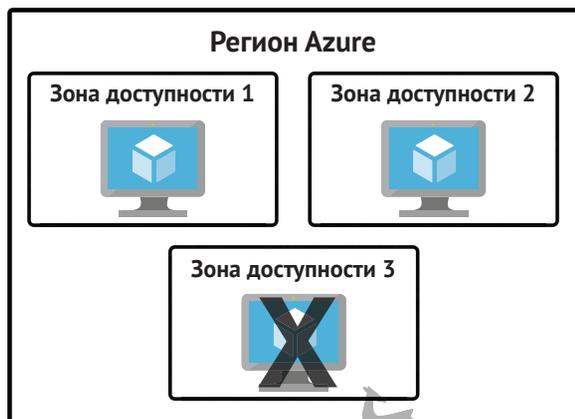


Рис. 2.1 Виртуальная машина Azure в трех зонах доступности



ПРИМЕЧАНИЕ СОСТОЯНИЕ AZURE

Microsoft поддерживает веб-сайт с информацией о состоянии сервисов Azure. Если вы обнаружите проблему с ресурсами, можно воспользоваться страницей Azure Status для проверки: <https://status.azure.com>.



СОВЕТ К ЭКЗАМЕНУ

Не путайте зоны доступности (availability zones) с наборами доступности (availability sets). Наборы доступности позволяют создавать две или более виртуальных машин в разных физических серверных стойках центра обработки данных Azure. Microsoft гарантирует 99,95%-ное SLA при использовании набора доступности.

Зона доступности позволяет развернуть две или более службы Azure в двух отдельных центрах обработки данных в пределах региона. Microsoft гарантирует 99,99%-ное SLA при использовании зон доступности.

Существуют две категории служб, поддерживающих зоны доступности: *зональные* (zonal) и *избыточные* в пределах зоны (zone-redundant). Зональные службы – это службы, такие как виртуальные машины, и используемые в них управляемые диски и публичные IP-адреса. Для обеспечения высокой доступности необходимо явным образом развернуть службы в двух или более зонах.

ПРИМЕЧАНИЕ УПРАВЛЯЕМЫЕ ДИСКИ И ПУБЛИЧНЫЕ IP-АДРЕСА

При создании виртуальной машины в Azure и ее развертывании в зоне доступности Azure автоматически создает управляемые диски и публичный IP-адрес (если таковой настроен) в той же зоне доступности.

Службы, избыточные в пределах зоны, – это службы наподобие хранилища, избыточного между зонами, и базы данных SQL. Чтобы использовать зоны доступности с этими службами, вам необходимо указать специальный параметр при их создании. Для хранилища эта функция называется ZRS (zone-redundant storage), а для базы данных SQL – база данных, избыточная между зонами (database zone redundant). Azure берет всю работу на себя, автоматически реплицируя данные в несколько зон доступности.

Группы ресурсов

Теперь вы понимаете, что переход в облако может оказаться не таким уж простым, как вы сначала думали. Создание единичного ресурса в Azure – довольно простой процесс, но когда вы имеете дело с приложениями корпоративного уровня, тогда речь уже идет о сложном наборе сервисов. Кроме этого, вы можете иметь дело с несколькими приложениями, использующими множество служб, плюс они могут быть распространены по нескольким регионам Azure. Безусловно, размещение ресурсов может быстро стать хаотичным.

К счастью, Azure предоставляет функцию, которая помогает решить подобные проблемы: группу ресурсов (resource group). Группа ресурсов – это логический контейнер для служб Azure. Создав все службы Azure, связанные с кон-

кретным приложением, в одной группе ресурсов, можно разворачивать все эти службы и управлять ими как единым целым.

Групповая организация ресурсов Azure имеет множество преимуществ. Прежде всего можно без особого труда настроить развертывание при помощи функции шаблона ARM. Развертывания *шаблона ARM* обычно предназначены для одной группы ресурсов. Вы также можете выполнять развертывание в нескольких группах ресурсов, но для этого необходимо настроить сложную цепочку шаблонов ARM.

ДОПОЛНИТЕЛЬНО ПОДРОБНЕЕ О ШАБЛОНАХ ARM

В этой главе вы узнаете больше о шаблонах ARM, когда мы позже будем говорить об Azure Resource Manager.



Другим преимуществом группы ресурсов является возможность присвоения ей своего уникального и узнаваемого имени, чтобы можно было сразу увидеть все ресурсы Azure, используемые в конкретном приложении. Это может показаться не столь важным, пока вы не начнете разворачивать ресурсы Azure и не поймете, что у вас их гораздо больше, чем вы думали изначально. Например, при создании одной виртуальной машины Azure создает не только саму машину, но и дисковый ресурс, сетевой интерфейс, общедоступный IP-адрес и группу сетевой безопасности. При просмотре всех ресурсов Azure могут возникнуть трудности с определением ресурсов, которые идут с приложением. И группы ресурсов решают эту проблему.

На рис. 2.2 показано множество служб Azure. Некоторые из них были автоматически созданы Azure для поддержки других служб. Зачастую Azure назначает ресурсу неузнаваемое имя.

На рис. 2.3 показаны ресурсы, входящие в группу ресурсов **WebStorefront**. Это ресурсы Azure, используемые в магазине электронной коммерции.

Удобно, что все ресурсы приложения у нас на глазах, но на этом все не ограничивается. Выше расположен хороший пример, поскольку в нем отображено обычное использование групп ресурсов. Однако вы можете сформировать свои группы ресурсов так, как захотите. Обратите внимание на рис. 2.3: там ресурсы отображаются в нескольких разных регионах Azure (регионы находятся в столбце **Location**). Обладая доступом к нескольким подпискам Azure, вы можете получить ресурсы этих подписок в качестве цельной группы.

Если вы посмотрите на левую часть рис. 2.3, то увидите меню операций, доступных к выполнению над группой ресурсов. Мы не будем вдаваться в детали, потому что это не входит в экзамен AZ-900, но есть здесь и полезная информация, объясняющая преимущества группы ресурсов.

При нажатии на **Resource Costs** отобразится стоимость всех ресурсов этой группы. Наличие подобной информации особенно полезно, когда вы хотите убедиться, что определенные отделы вашей компании тратят корректные суммы за использованные ресурсы. В действительности некоторые компании создают группы ресурсов под каждый отдел, а не для отдельных приложений. Например, наличие группы ресурсов по продажам и маркетингу или IT-поддержки может значительно помочь вам в составлении отчетов и контроле расходов.

<input type="checkbox"/>	NAME	TYPE	RESOURCE...	LOCATION	SUBSCRI...
<input type="checkbox"/>	900rgdiag	Storage acc...	900RG	South Centr...	Jim's Perso...
<input type="checkbox"/>	900RG-vnet	Virtual netw...	900RG	South Centr...	Jim's Perso...
<input type="checkbox"/>	EComVM	Virtual mac...	WebStorefr...	South Centr...	Jim's Perso...
<input type="checkbox"/>	EComVM_OsDisk_1_1d...	Disk	WEBSTORE...	South Centr...	Jim's Perso...
<input type="checkbox"/>	ecomvm34	Network int...	WebStorefr...	South Centr...	Jim's Perso...
<input type="checkbox"/>	EComVM-ip	Public IP ad...	WebStorefr...	South Centr...	Jim's Perso...
<input type="checkbox"/>	EComVM-nsg	Network sec...	WebStorefr...	South Centr...	Jim's Perso...
<input type="checkbox"/>	greatappalready	App Service	Test	Central US	Jim's Perso...
<input type="checkbox"/>	jwc900	SQL server	WebStorefr...	Central US	Jim's Perso...
<input type="checkbox"/>	900StoreDB (jwc900/...	SQL database	WebStorefr...	Central US	Jim's Perso...
<input type="checkbox"/>	ServicePlan9dbd216e...	App Service ...	WebStorefr...	Central US	Jim's Perso...
<input type="checkbox"/>	UbuVM	Virtual mac...	900RG	South Centr...	Jim's Perso...
<input type="checkbox"/>	UbuVM_OsDisk_1_973...	Disk	900RG	South Centr...	Jim's Perso...
<input type="checkbox"/>	ubuvm97	Network int...	900RG	South Centr...	Jim's Perso...

Рис. 2.2 Это все мои ресурсы Azure

Dashboard > Resource groups > WebStorefront

WebStorefront

Resource group

Search (Ctrl + F)

+ Add Edit columns Delete resource group Refresh Move Assign tags Delete

Subscription (change) Jim's Personal Azure Account Deployments 3 Succeeded

Subscription ID 2ed0e6a0-aaf7-4f5f-aff6-bf25ffdef188

Tags (change) Click here to add tags

Filter by name... All types All locations No grouping

11 items Show hidden types

<input type="checkbox"/>	NAME	TYPE	LOCATION
<input type="checkbox"/>	EComVM	Virtual machine	South Central US
<input type="checkbox"/>	EComVM_OsDisk_1_1dae8c7f45b4205b14c5c93a5546...	Disk	South Central US
<input type="checkbox"/>	ecomvm34	Network interface	South Central US
<input type="checkbox"/>	EComVM-ip	Public IP address	South Central US
<input type="checkbox"/>	EComVM-nsg	Network security group	South Central US
<input type="checkbox"/>	jwc900	SQL server	Central US
<input type="checkbox"/>	900StoreDB (jwc900/900StoreDB)	SQL database	Central US
<input type="checkbox"/>	ServicePlan9dbd216e-8674	App Service plan	Central US
<input type="checkbox"/>	webstore900	App Service	Central US
<input type="checkbox"/>	webstorefrontdiag	Storage account	South Central US

Рис. 2.3 Группа ресурсов Azure



СОВЕТ К ЭКЗАМЕНУ

Ресурс Azure может существовать только в одной группе ресурсов. Другими словами, виртуальная машина не может одновременно находиться в группах ресурсов *Web-Storefront* и *SalesMarketing*: либо она находится в первой, либо во второй. Ресурсы Azure можно перемещать из одной группы ресурсов в другую.

ДОПОЛНИТЕЛЬНО ПЕРЕМЕЩЕНИЕ РЕСУРСОВ AZURE

Перемещение ресурсов Azure между группами ресурсов или подписками не лишено риска. Microsoft описала для вас несколько советов, следуя которым, вы не столкнетесь с проблемами при перемещении ресурсов. Вы можете ознакомиться с руководством по ссылке: <https://bit.ly/az900-movingresources>.

Нажав на **Automation Script** (Скрипт автоматизации), вы получите созданный Azure шаблон ARM, который можно будет использовать для автоматического развертывания всех ресурсов в Azure. Это пригодится, когда вам впоследствии нужно будет развернуть ресурсы или же когда вы планируете развернуть их в другой подписке Azure.

При удалении группы ресурсов все ее ресурсы автоматически удалятся. Это сводит удаление множества ресурсов Azure в одно простое действие. Скажем, вы тестируете сценарий, и вам нужно создать пару виртуальных машин, базу данных, веб-приложение и многое чего еще. Поместив все перечисленные ресурсы в одну группу, вы можете легко ее удалить после тестирования, а Azure автоматически удалит за вас все находящиеся в ней ресурсы. Это прекрасное решение по избеганию непредвиденных затрат, связанных с неиспользуемыми ресурсами.

Подписки Azure

Подписавшись на Azure, вы автоматически получаете там подписку, и теперь все создаваемые вами ресурсы будут в ней располагаться. Однако вы можете создавать и дополнительные подписки, которые привязываются к вашему аккаунту в Azure. Дополнительные подписки полезны в случаях, когда требуется создать логические группировки ресурсов Azure или если вам нужно отчитаться о ресурсах, используемых соответствующими группами лиц.

Каждой подписке Azure назначены ограничения, иногда называемые квотами. Например, в подписке может содержаться до 250 учетных записей хранения Azure и до 25 000 виртуальных машин на регион, также на одну подписку вы получаете до 980 групп ресурсов во всех регионах.

ДОПОЛНИТЕЛЬНО ОГРАНИЧЕНИЯ ПОДПИСКИ

Подробнее об ограничениях на подписки вы узнаете на сайте: <https://bit.ly/az900-sublimits>.



СОВЕТ К ЭКЗАМЕНУ

В некоторых ситуациях служба поддержки Microsoft может увеличить ограничения, если у вас есть этому хорошее бизнес-обоснование. Однако некоторые ограничения увеличить нельзя.

На рис. 2.4 показана подписка в портале Azure.

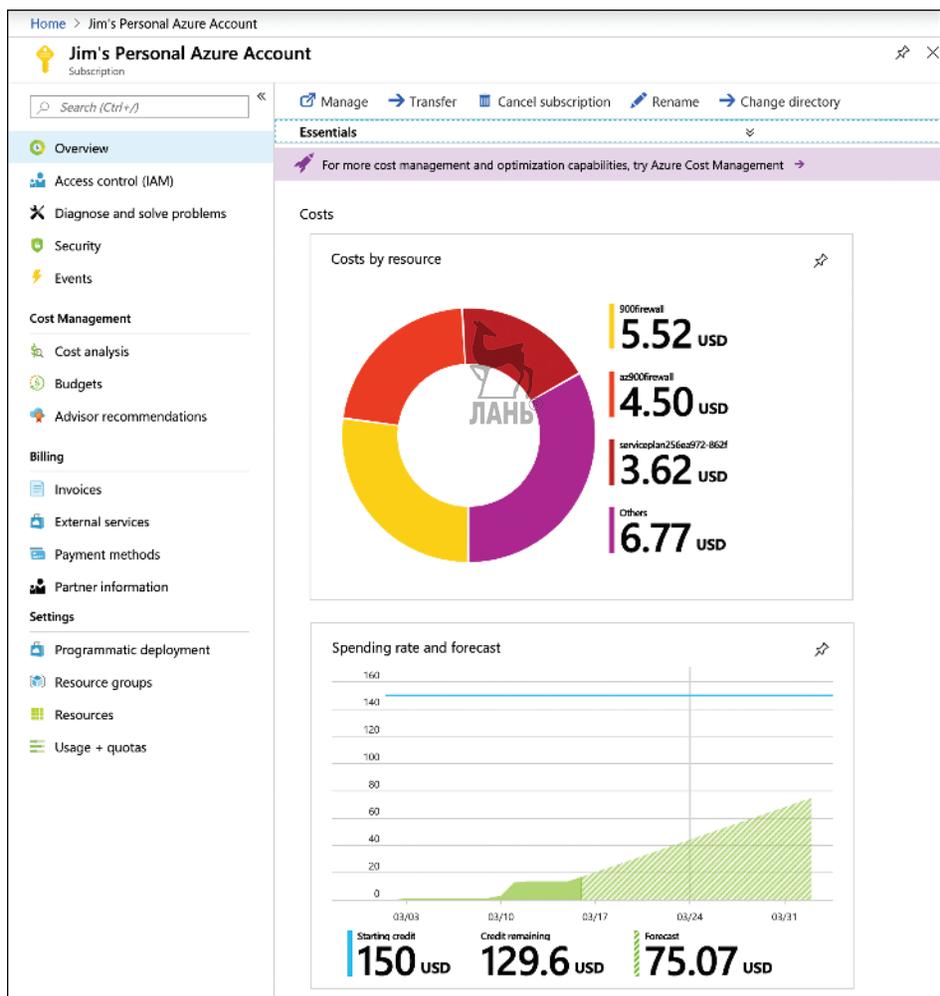


Рис. 2.4 Подписка в портале Azure

В разделе **Overview** (Обзор) перед вами открывается разбивка затрат по каждому из ресурсов. Вы также можете увидеть тариф расходов на подписку и прогнозируемую стоимость к концу текущего месяца. Нажав на плитку **Costs by resource** (Затраты по ресурсам), можно увидеть дальнейшую разбивку расходов Azure, как показано на рис. 2.5. В данном случае отображаются затраты по имени службы (Service Name), местоположению (регион Azure) и группе ресурсов, также отображен график затрат за месяц.

На портале Azure вам доступны счета-фактуры для каждой подписки. Вы можете посмотреть прошлые счета-фактуры, щелкнув на **Invoices** в меню подписки, как показано на рис. 2.6.

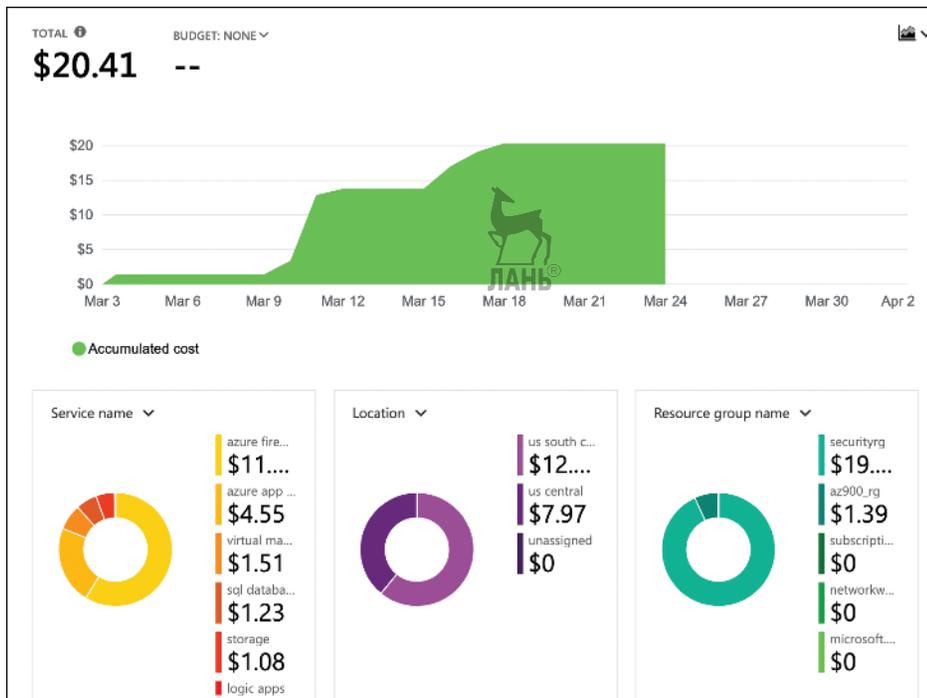


Рис. 2.5 Анализ расходов подписки Azure

ДОПОЛНИТЕЛЬНО ПЛАНИРОВАНИЕ БЮДЖЕТА

Вы можете управлять своими расходами в Azure при помощи бюджета. Об этом мы поговорим с вами в главе 6 «Ценообразование, соглашения о качестве предоставляемых услуг и жизненные циклы Azure».

Jim's Personal Azure Account - Invoices

Subscription

Search (Ctrl+F)

Older invoices Email invoice Access to invoice

Your selected payment method (AMEX *) will automatically be charged.

Azure services Azure Marketplace and Reservations

View invoices for Azure services.

Subscription ⓘ

Jim's Personal Azure Account [2ed0efa...]

Grid Chart

BILLING PERIOD	CHARGE DATE	AMOUNT (USD)	INVOICE
2/3/2019-3/2/2019	3/3/2019	176.34	Download invoice
1/3/2019-2/2/2019	2/3/2019	228.13	Download invoice
12/3/2018-1/2/2019	1/3/2019	184.94	Download invoice
11/3/2018-12/2/2018	12/3/2018	211.20	Download invoice
10/3/2018-11/2/2018	11/3/2018	168.43	Download invoice
9/3/2018-10/2/2018	10/3/2018	124.59	Download invoice

Рис. 2.6 Счета-фактуры Azure

Вы можете создать дополнительные подписки Azure в своей учетной записи. Это пригодится вам при разделении расходов или когда наступит ограничение подписки на ресурс. Для создания новой подписки Azure введите **subscription** в поле поиска и нажмите **Subscriptions** (Подписки), как показано на рис. 2.7.

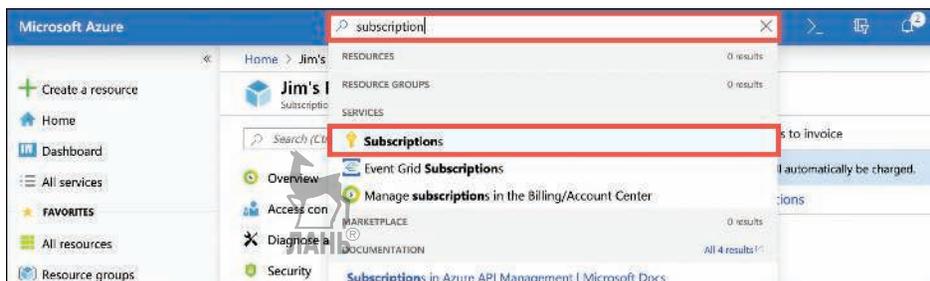


Рис. 2.7 Подписки Azure

Для создания новой подписки нажмите кнопку **Add** (Добавить) в разделе **Subscriptions** (Подписки), как показано на рис. 2.8.

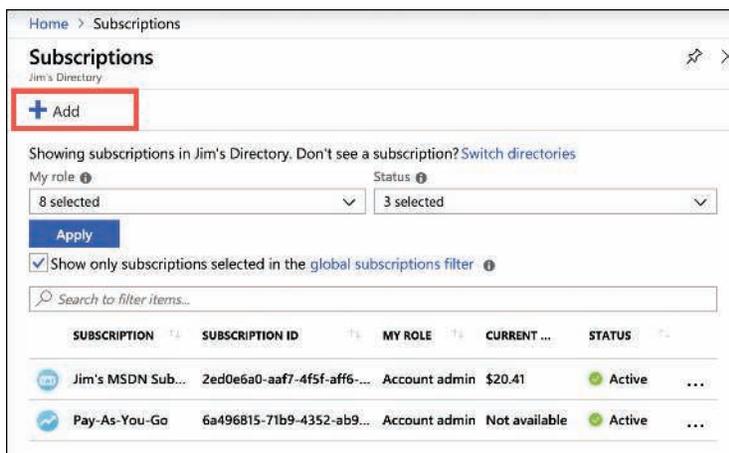


Рис. 2.8 Создание новой подписки

Создав новую подписку, вам нужно выбрать ее тип. Вообще, существует несколько типов подписок Azure.

- **Бесплатная пробная версия.** Предоставляет бесплатный доступ к ресурсам Azure на определенное время. Для каждой учетной записи доступен только одна бесплатная подписка. Нельзя создать новую бесплатную пробную версию, если срок действия предыдущей истек.
- **Оплата по мере использования.** Вы платите только за те ресурсы, которые используете в Azure. Предоплата не взимается, и вы можете отменить подписку в любое время.

- **Для разработки/тестирования.** Специальная подписка для подписчиков на Visual Studio, которую можно использовать для разработки и тестирования. Эта подписка предлагает скидки на VM, однако использовать их для реальных приложений нельзя.

ПРИМЕЧАНИЕ ТИПЫ ПОДПИСОК AZURE

Некоторые типы учетных записей Azure предлагают дополнительные возможности подписки.



СОВЕТ К ЭКЗАМЕНУ

У каждой подписки есть свой уникальный идентификатор – *идентификатор подписки*. Вы можете присвоить подписке и описательное имя, что облегчит вам поиск, однако Azure всегда будет использовать ее ID. Взаимодействуя с Microsoft по поводу вашей учетной записи в Azure, у вас наверняка запросят идентификатор подписки.

Теперь вы знаете о подписках Azure и о том, как при необходимости создавать дополнительные подписки. Создав дополнительные подписки вместе с ресурсами, вы можете обнаружить, что управление этими самыми ресурсами – это довольно трудоемкий процесс. Microsoft позаботилась об этом: вам в помощь разработаны группы управления.

Группы управления

Группы управления – это удобный способ применения политик и контроля доступа к ресурсам Azure. Подобно группе ресурсов, группа управления – это контейнер для организации ваших ресурсов. Однако группы управления могут содержать только подписки Azure или другие группы управления.

ПРИМЕЧАНИЕ ИДЕНТИФИКАЦИЯ И УПРАВЛЕНИЕ AZURE

На данный момент вам не нужно разбираться в таких понятиях, как политика и контроль доступа. Они будут позже представлены в главе 5 «Функции идентификации, управления, конфиденциальности и соответствия нормативным требованиям».

На рис. 2.9 для компании были созданы три группы управления. Группа управления **Sales Dept.** содержит подписки для отдела продаж. Группа управления **IT Dept.** содержит подписку и еще одну группу управления, и две дополнительные подписки, находящиеся в данной группе управления. Группа управления **Training Dept.** содержит две подписки для отдела профессиональной подготовки.

Организуя подписки с помощью групп управления, вы можете более точно контролировать доступ к ресурсам. Также можно будет управлять конфигурацией ресурсов, созданных в рамках этих подписок.

После создания группы управления вы можете переместить любую из своих подписок в эту группу. Вдобавок можно переместить одну группу управления в другую. Однако есть несколько нюансов:

- ограничение в общей сложности к 10 000 групп управления;
- иерархия группы управления может поддерживать только до шести уровней;
- в одной группе управления или подписке может содержаться только одна родительская группа или подписка.

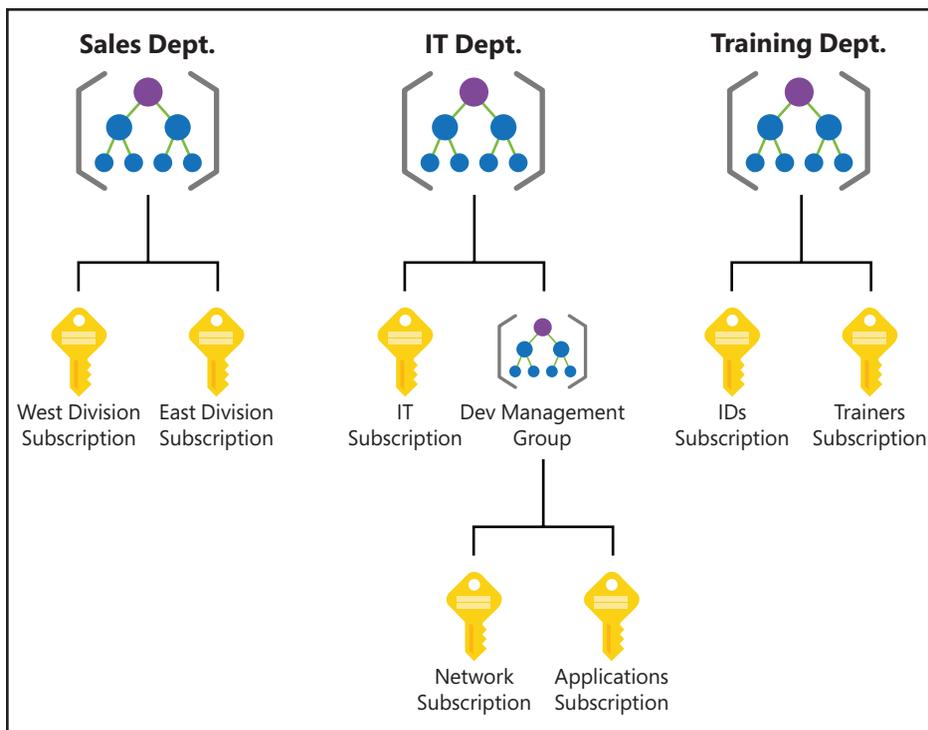


Рис. 2.9 Группы управления, организующие подписки и другие группы управления

Диспетчер ресурсов Azure (Azure Resource Manager, ARM)

Почти все системы, мигрированные в облако, состоят из нескольких служб Azure. Например, у вас может быть виртуальная машина Azure для одной части приложения; данные могут находиться в базе данных SQL Azure; некоторые конфиденциальные данные могут храниться в хранилище Azure Key Vault, а веб-часть приложения может быть размещена в службе приложений Azure (Azure App Service).

Раздельное управление этими службами Azure может превратиться в еще ту головную боль. А если у вас будет несколько приложений в облаке, то ситуация может стать еще хуже. Мало того, что отслеживание принадлежности служб к приложениям было бы весьма сложным занятием, так еще и добавление механизмов развертывания обновлений для приложения могло бы действительно все запутать.

Чтобы упростить развертывание служб Azure и управление ими, в Microsoft разработали Azure Resource Manager, или же ARM. ARM – это служба, которая работает в Azure и отвечает за все взаимодействие со службами Azure. При создании новой службы Azure ARM проверяет наличие у вас прав доступа для создания этого ресурса, а затем общается с поставщиком ресурсов (resource provider) для создаваемой вами службы. Например, если вы создаете новое веб-приложение в службе приложений Azure, ARM передает ваш запрос поставщику ресурсов *Microsoft.Web*, поскольку он знает все о веб-приложениях и способах их создания.



СОВЕТ К ЭКЗАМЕНУ

Для каждой службы Azure существуют свои поставщики ресурсов, но их имена иногда могут быть бессмысленны. Например, *Microsoft.Compute* отвечает за создание ресурсов виртуальной машины.

Для экзамена AZ-900 вам не нужно глубокое познание о поставщиках ресурсов, наоборот, вам нужно понимать общую концепцию, так как предполагается, что вы знакомы со службой Azure Resource Manager.

В главе 3 мы поговорим об использовании портала Azure для создания служб Azure и управления ими. Вы также узнаете, как при помощи инструментов командной строки сделать то же самое. Как портал, так и инструменты командной строки работают с помощью ARM, и они взаимодействуют с ARM с помощью программного интерфейса приложений (application programming interface, или API). API-интерфейс ARM является одинаковым вне зависимости от того, используете вы портал или инструменты командной строки. Это означает, что результат всегда будет неизменным. Плюс вы можете создать ресурс Azure с помощью портала, а затем внести в него изменения с помощью командной строки, обеспечивая необходимую гибкость для потребителей облака.

ДОПОЛНИТЕЛЬНО VISUAL STUDIO И ARM

Visual Studio, среда разработки Microsoft для написания приложений, также может создавать ресурсы Azure и разворачивать для них код. Она делает это, используя тот же ARM API, который упоминался ранее. Фактически ARM API можно считать своим интерфейсом в мире Azure. Вы действительно не можете создавать службы Azure или управлять ими без использования ARM API.

Поток обычного запроса ARM для создания ресурса или его управления прост. Такие средства, как портал Azure, средства командной строки или Visual Studio, делают запрос к ARM API. API передает, что запрос к ARM выполняется авторизованным и аутентифицированным пользователем. Затем ARM передает запрос поставщику ресурсов, который, в свою очередь, создает новый ресурс или изменяет существующий. На рис. 2.10 показан этот поток и представлена небольшая выборка из множества доступных служб Azure.

Запрос в ARM не является сложным запросом на основе программного кода. Напротив, ARM использует *декларативный синтаксис*. Это означает, что, будучи потребителем Azure, вы делитесь с ARM информацией о своих действиях,

и ARM делает это за вас. При этом не нужно объяснять ARM, как именно выполнять то, что вам необходимо: вы говорите, ARM делает. Для этого данная служба использует файлы, закодированные в JavaScript Object Notation (или JSON), называемые *шаблонами ARM*.

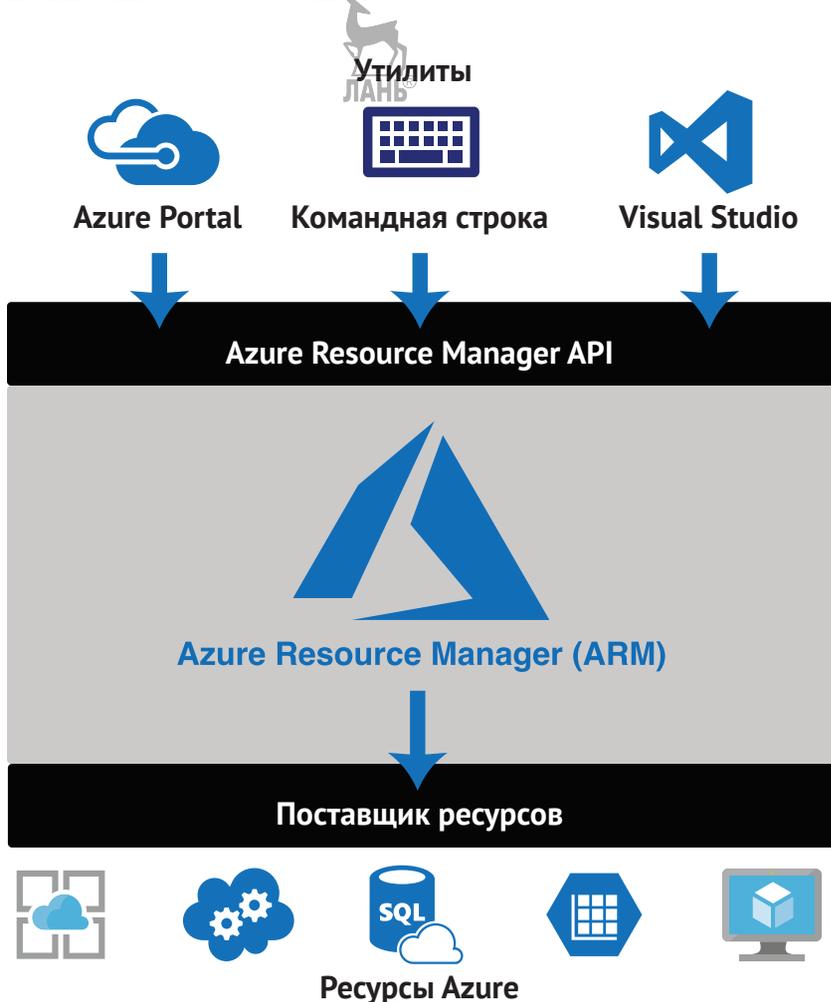


Рис. 2.10 Диспетчер ресурсов Azure

ПРИМЕЧАНИЕ ШАБЛОНЫ ARM

Для экзамена AZ-900 вам не нужны знания об использовании шаблонов ARM, но, чтобы понять принцип работы ARM, вам нужно хотя бы немного о них узнать.

Простым языком: шаблон ARM содержит список ресурсов, которые вы хотите либо создать, либо изменить. Каждый ресурс обладает свойствами, скажем своим именем и особыми параметрами. Например, если вы использовали шаблон ARM для разворачивания веб-приложения в службе приложений, то он

запросит у вас желаемый для создания приложения регион, имя приложения, тарифный план, доменные имена, которые вам хотелось бы использовать для приложения, и т. д. Разбираться в установке всех этих свойств необязательно. Вы попросту даете ARM установку на это (заявляете о своем намерении), и ARM берет всю работу на себя.



ДОПОЛНИТЕЛЬНО ПОДРОБНЕЕ О ШАБЛОНАХ ARM

Несмотря на свою простоту, шаблоны ARM весьма мощные. При желании больше узнать об их использовании вы можете ознакомиться со следующей документацией: <https://bit.ly/az900-armtemplates>.

Есть еще один важный аспект использования шаблонов ARM. Разворачивая несколько ресурсов (обычный сценарий из реальной практики), у вас практически всегда будет зависимость служб. Другими словами, вы разворачиваете одну или несколько служб, которые полагаются на другие сервисы, которые уже создаются.

Подумайте, например, о ситуации, когда вы публикуете сертификат, который будет использоваться вместе с веб-приложением. Одним из необходимых к установке в веб-приложении свойств является сертификат, который вам хотелось бы использовать, но если этот сертификат еще не развернут, то и публикация веб-приложения завершится неудачей. ARM позволяет вам указывать зависимости во избежание подобных проблем. Вы просто сообщаете ARM, что веб-приложение находится в зависимости от сертификата, и ARM гарантирует, что публикация сертификата завершится до развертывания веб-приложения.

Как видите, у ARM много преимуществ, и для экзамена вы должны о них знать.

- ARM позволяет легко разворачивать сразу несколько ресурсов Azure.
- ARM дает возможность воспроизводить разворачивание с последующими неизменными результатами в любой момент.
- ARM позволяет создавать декларативные шаблоны для разворачивания вместо написания и поддержки сложных скриптов.
- ARM дает возможность настраивать зависимости так, чтобы каждый раз ваши ресурсы разворачивались и создавались в правильном порядке.

В этом разделе навыков вы узнали о некоторых преимуществах использования Azure. Поскольку регионы Azure разбросаны по всему миру по разным континентам и странам, вы можете быть уверены, что ваши данные и приложения разместятся в нужном вам месте, а также что все правила или требования по отношению к данным будут соблюдены. Теперь вы знаете, что в каждом регионе есть несколько центров обработки данных, и, разворачивая свои приложения в зонах доступности, вы можете обезопасить себя от последствий сбоя в определенном центре обработки данных.

Мы также поговорили об использовании групп ресурсов для организации ваших ресурсов Azure и о том, как использовать подписки Azure. В конце вы узнали о группах управления и об Azure Resource Manager, или иначе ARM. В следующем разделе навыков мы подробнее поговорим о некоторых основных продуктах рабочей нагрузки Azure.

Навык 2.2: описание ключевых ресурсов, доступных в Azure

Когда мы перешли к основным архитектурным компонентам Azure, вы могли заметить упоминания на некоторые продукты, доступные в Azure. В этом разделе навыков мы поговорим об основных рабочих компонентах в Azure.

Содержание раздела:

- виртуальные машины Azure;
- служба приложения Azure (Azure App Service);
- экземпляры контейнеров Azure (Azure Container Instances, ACI);
- служба Azure Kubernetes (Azure Kubernetes Service, AKS);
- виртуальный рабочий стол Windows (Windows Virtual Desktop);
- виртуальные сети (Virtual networks);
- ExpressRoute;
- хранилище двоичных объектов (контейнеров) (Container (Blob) Storage);
- дисковое хранилище (Disk Storage);
- файлы Azure (Azure Files);
- уровни доступа к хранилищам (Storage tiers);
- Cosmos DB;
- база данных SQL Azure (Azure SQL Database);
- база данных Azure для MySQL (Azure Database for MySQL);
- база данных Azure для PostgreSQL (Azure Database for PostgreSQL);
- Azure Marketplace и сценарии его использования.

Виртуальные машины Azure

Виртуальная машина, VM (Virtual Machine, VM) – это программный компьютер, работающий на физическом компьютере. Под физическим компьютером понимается узел (иначе *хост*, host). Он обеспечивает основные физические компоненты, такие как дисковое пространство, память, процессор и т. д. На хост-компьютере работает программное обеспечение, называемое гипервизором (hypervisor), которое может создавать и управлять одной или более VM, а эти VM, в свою очередь, обычно называются *гостями* (guests).

Операционная система на гостевом компьютере может отличаться от операционной системы на хост-машине. Если у вас хост работает под управлением Windows 10, то на нем можно запустить гостевую систему Windows Server 2016, Linux или многие другие. Подобная гибкость делает VM крайне популярными. Однако поскольку VM, работающие на хост-компьютере, используют его физические системы, то если вам нужна мощная VM, для ее размещения потребуется мощный физический компьютер.

Используя виртуальные машины Azure, вы можете задействовать мощные хост-компьютеры, если вам нужна вычислительная мощность, а когда вы больше не нуждаетесь в этой мощности, вам и не придется за нее платить.

ПРИМЕЧАНИЕ ИСПОЛЬЗОВАНИЕ AZURE

В этом разделе вы создадите виртуальную машину Azure, поэтому вам понадобится подписка Azure. Если у вас ее нет, вы можете получить бесплатную пробную версию, перейдя по ссылке: <https://azure.microsoft.com/en-us/free/>.

Чтобы создать виртуальную машину Azure, войдите на портал Azure, используя свою учетную запись, а затем выполните следующие действия, как показано на рис. 2.11–2.13.

1. Нажмите **Create A Resource** (Создать ресурс).
2. Нажмите кнопку **Compute** (Вычисления).
3. Нажмите **See All link** (Посмотреть все ссылки).
4. Нажмите **Ubuntu Server**.
5. Нажмите кнопку **Create** (Создать).
6. Рядом с пунктом **Resource Group** (Группа ресурсов) нажмите кнопку **Create New** (Создать новую) для создания новой группы ресурсов.
7. Введите **TestRG** в качестве имени группы ресурсов и нажмите **ОК** (Принять).
8. Введите **TestVM** в качестве имени виртуальной машины.
9. Прокрутите вниз и выберите **Пароль** (Password) для типа аутентификации.

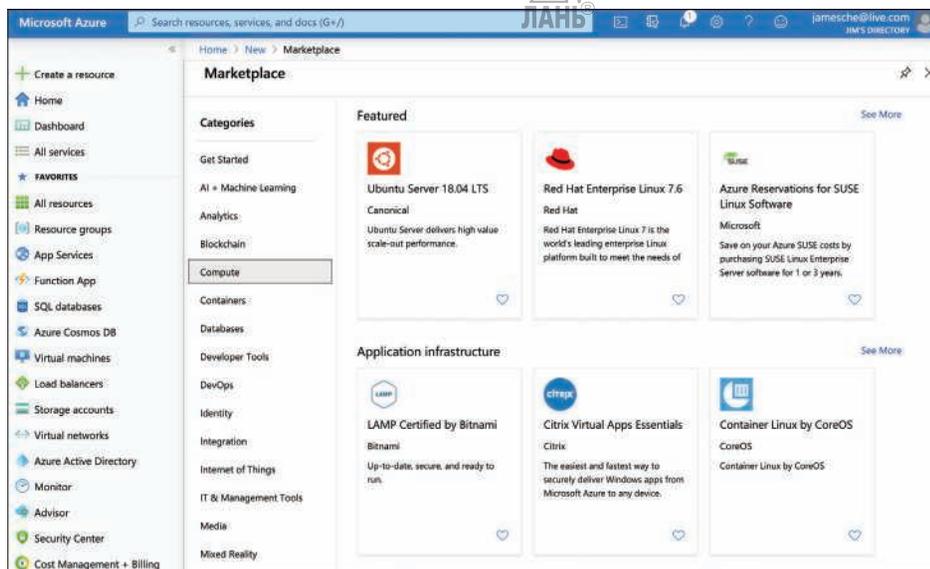


Рис. 2.11 Создание виртуальной машины

10. Введите имя пользователя для учетной записи администратора.
11. Введите пароль, который вы хотите использовать для учетной записи администратора.
12. Подтвердите пароль.
13. Оставьте стандартные настройки и нажмите кнопку **Next** (Далее) три раза, чтобы перейти на экран управления (**Management**).
14. В разделе **Monitoring** (Мониторинг) установите для параметра **Boot diagnostics** (Диагностика загрузки) значение **Off** (Выкл).
15. Нажмите **Review** (Обзор) + **Create** (Создать) для создания своей VM.

После того как вы нажали кнопки **Review** (Обзор) + **Create** (Создать), Azure проверит ваши параметры, чтобы убедиться, что вы ничего не забыли. После успешной проверки вы увидите кнопку **Create** (Создать). Вам нужно на нее нажать, чтобы началось создание новой виртуальной машины.

ДОПОЛНИТЕЛЬНО КАК AZURE РАЗВОРАЧИВАЕТ VM

При нажатии кнопки **Create** (Создать) портал Azure использует шаблон ARM для разворачивания VM. Этот шаблон содержит параметры, которые заменяются информацией, введенной пользователем. Все VM в Azure создаются при помощи ARM-шаблона, что гарантирует неизменность разворачивания.

Home > New > Marketplace > Ubuntu Server 18.04 LTS > Create a virtual machine

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Jim's MSDN Subscription

Resource group * ⓘ (New) TestRG [Create new](#)

Instance details

Virtual machine name * ⓘ TestVM

Region * ⓘ (US) Central US

Availability options ⓘ No infrastructure redundancy required

Image * ⓘ Ubuntu Server 18.04 LTS [Browse all public and private images](#)

Рис. 2.12 Параметры виртуальной машины

Home > New > Marketplace > Ubuntu Server 18.04 LTS > Create a virtual machine

Create a virtual machine

Size * ⓘ

Standard D2s v3
2 vcpus, 8 GiB memory (\$80.30/month)
[Change size](#)

Administrator account

Authentication type ⓘ SSH public key Password

Username * ⓘ ✓

Password * ⓘ ✓

Confirm password * ⓘ ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ None Allow selected ports

Select inbound ports * ✓

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

[Review + create](#) [< Previous](#) [Next : Disks >](#)

Рис. 2.13 Параметры виртуальной машины

Как только ваша VM будет развернута, вы увидите состояние, отображенное на портале Azure (см. рис. 2.15). Также можно посмотреть ресурсы Azure, которые были созданы для поддержки VM. Еще там есть информация об имени и типе ресурса (который начинается с поставщика ресурсов), а также о состоянии каждого ресурса.

После создания всех ресурсов, необходимых для VM, она будет считаться полностью развернутой. Затем можно нажать кнопку **Go To Resource** (Перейти к ресурсу), чтобы увидеть интерфейс управления VM на портале Azure, как показано на рис. 2.16.

Созданная нами VM будет являться гостевой, работающей на физическом компьютере в центре обработки данных Azure. В этом центре находится физическая стойка компьютерных серверов, и наша VM размещается на одном из них. Host-компьютер управляется Microsoft, а управление VM осуществляет именно вы из-за выбранного предложения IaaS.

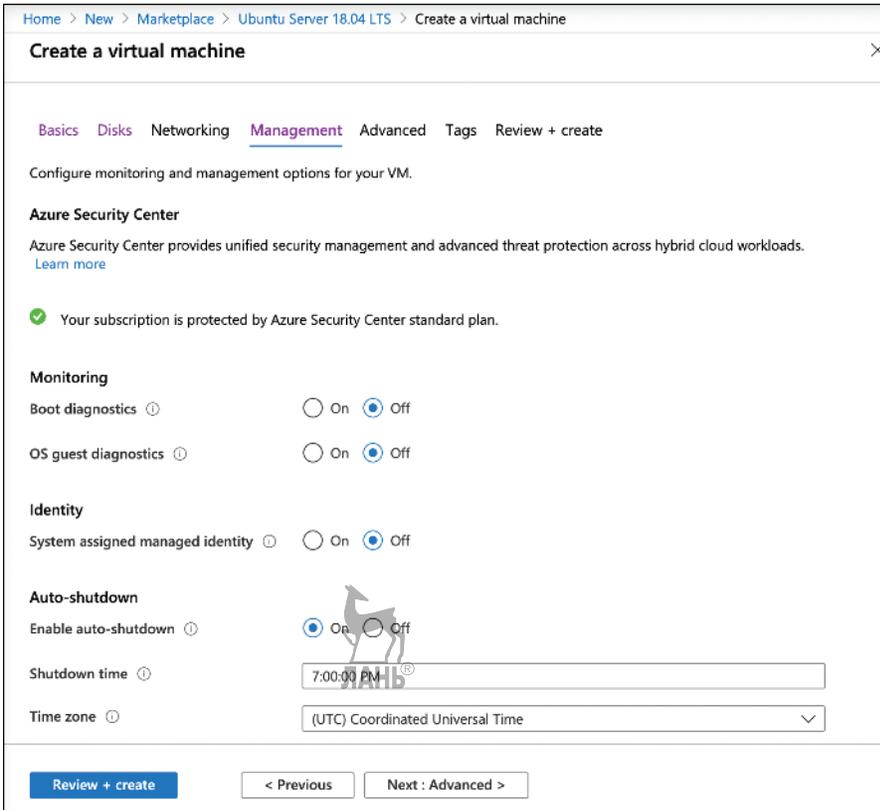


Рис. 2.14 Параметры управления виртуальной машины

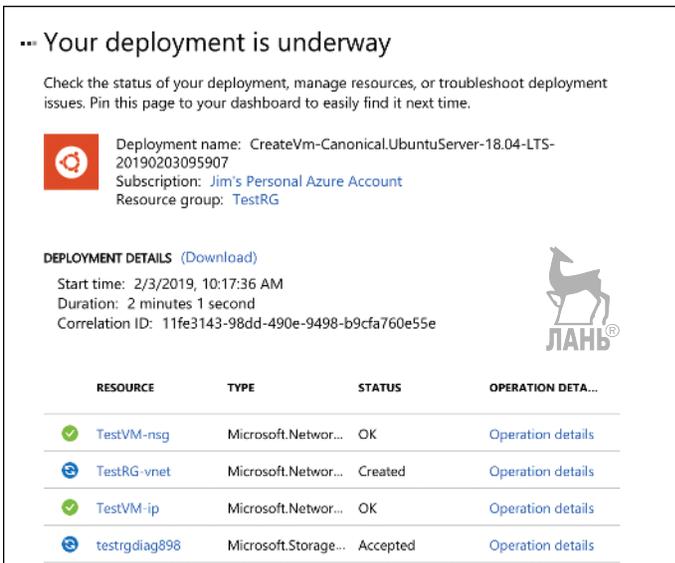


Рис. 2.15 Разворачивание виртуальной машины

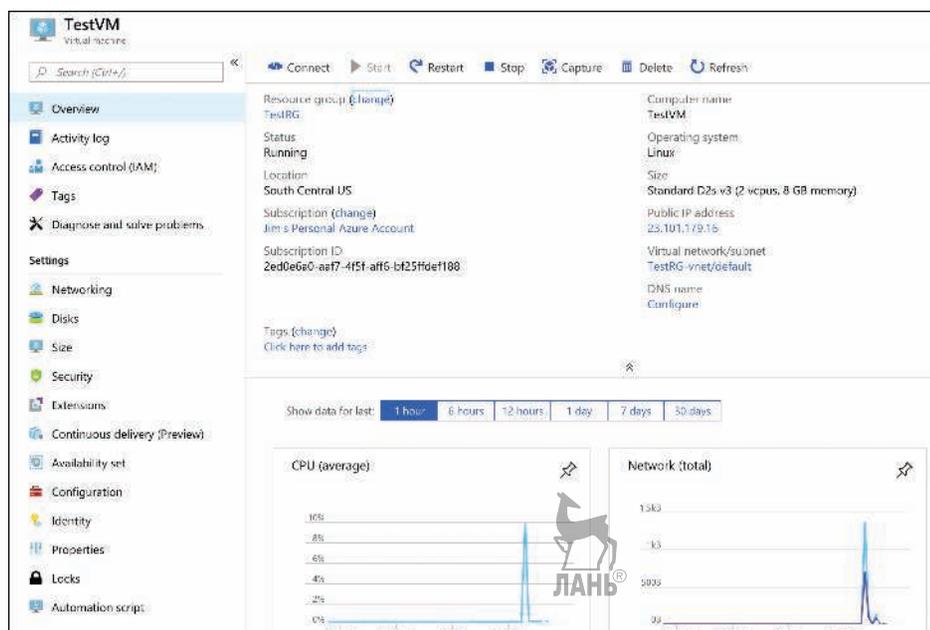


Рис. 2.16 Просмотр виртуальной машины

ПРИМЕЧАНИЕ **ВМ И СЧЕТА НА ОПЛАТУ**

Плата за ВМ Azure взимается до тех пор, пока они запущены, и использование стандартных настроек, как у нас сейчас, может привести к дорогостоящим последствиям. Чтобы остановить выставление счетов за данную ВМ, нажмите кнопку **Stop** в верхней части экрана (рис. 2.15). Azure сохранит текущее состояние ВМ, и выставление счетов будет приостановлено. Вы не сможете использовать приостановленную ВМ, однако и счета за нее вы также не получите. Учтите, что если вы не настроите статический IP-адрес для своей ВМ, то ваш IP-адрес, скорее всего, изменится при следующем запуске.

Вы также можете остановить ВМ из гостевой операционной системы, но при этом с вас все равно будет взиматься плата за ресурсы, которые использует ВМ, поскольку она по-прежнему развернута на хост-компьютере. Это означает, что плата за управляемые диски и другие ресурсы по-прежнему будет взиматься. Далее мы поговорим об удалении группы ресурсов *TestRG*, благодаря чему с вас не будет взиматься плата за ВМ.

Сейчас данная ВМ подвержена простою из-за трех типов событий: *планового обслуживания, внепланового обслуживания и неожиданного простоя*.

Плановое обслуживание относится к запланированным обновлениям, которые Microsoft производит на хост-компьютере. Оно включает в себя обновления операционной системы, драйверов и т. д. Во многих случаях обновления не влияют на ВМ, но если Microsoft установит обновление, требующее перезагрузки главного компьютера, ВМ отключится во время перезагрузки.

Azure имеет низкоуровневые системы, которые постоянно отслеживают работоспособность компонентов компьютера. Если одна из этих систем обнаружит, что компонент на главном компьютере скоро выйдет из строя, Azure пометит компьютер для внепланового обслуживания. В случае незапланиро-

ванного обслуживания Azure попытается переместить VM на другой работоспособный хост-компьютер. При этом сохранится состояние VM вместе с тем, что находится в памяти, а также все открытые файлы. Перемещение VM, которая в этот момент находится в приостановленном состоянии, для Azure не занимает много времени. В случае сбоя операции перемещения VM столкнется с неожиданным простоем.

Чтобы обеспечить защиту от сбоев в отдельных стойках центров обработки данных Azure, вы можете (и должны) воспользоваться функцией наборов доступности. *Наборы доступности* (availability sets) защищают вас от событий технического обслуживания и от простоев, вызванных сбоями оборудования. Для этого Azure создает основообразующие сущности в наборе доступности, называемые *доменами обновлений* (update domains) и *доменами сбоя* (fault domains). (Чтобы защититься от возможных сбоев и простоев, необходимо развернуть не менее двух взаимозаменяемых VM в наборе доступности.)

Домен сбоя представляет собой логическое представление физической серверной стойки, в которой установлен хост-компьютер. По умолчанию два домена сбоя связаны с одним набором доступности в Azure. Если проблема возникает в одном домене сбоя (в одной серверной стойке), то будут затронуты VM в этом домене сбоев, а в другом не будут. Это защищает вас от незапланированного технического обслуживания и непредвиденных простоев.

Домены обновлений направлены на защиту от ситуаций, которые возникают при перезагрузке хост-компьютера. При создании набора доступности Azure по умолчанию формирует пять доменов обновлений. Данные домены обновлений распределяются по доменам сбоя в наборе доступности. При необходимости в перезагрузке компьютеров в наборе доступности, будь то хост-компьютер или VM, Azure будет одновременно перезагружать компьютеры только в одном домене обновлений. После перезагрузки Azure сперва ожидает восстановления работоспособности компьютеров в течение получаса, а потом переходит к следующему домену обновления. Домены обновлений защищают вас от простоев, связанных с запланированными операциями обслуживания.

На рис. 2.17 показана схема, которую Microsoft использует для отображения набора доступности. На этой схеме домены сбоев FD0, FD1 и FD2 охватывают три физические компьютерные стойки. UD0, UD1 и UD2 являются доменами

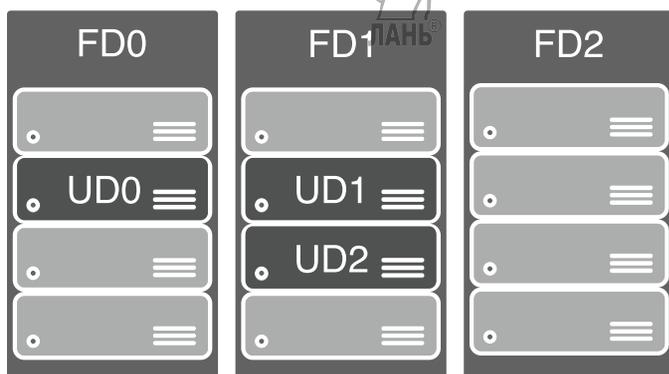


Рис. 2.17 Представление набора доступности в документации Microsoft

обновления в доменах сбоя. Такую же схему набора доступности вы увидите и в других учебных программах Azure. Однако она немного вводит в заблуждение, потому как домены обновлений не привязаны к конкретному домену сбоя.

На рис. 2.18 показано более наглядное представление набора доступности с пятью VM. Вы видите два домена сбоя и три домена обновлений. Когда в этом наборе доступности создавались VM, их распределение было следующим:

- первой VM назначается домен сбоя 0 и домен обновления 0;
- второй VM назначается домен сбоя 1 и домен обновления 1;
- третьей VM назначается домен сбоя 0 и домен обновления 2;
- четвертой VM назначается домен сбоя 1 и домен обновления 0;
- пятой VM назначается домен сбоя 0 и домен обновления 1.

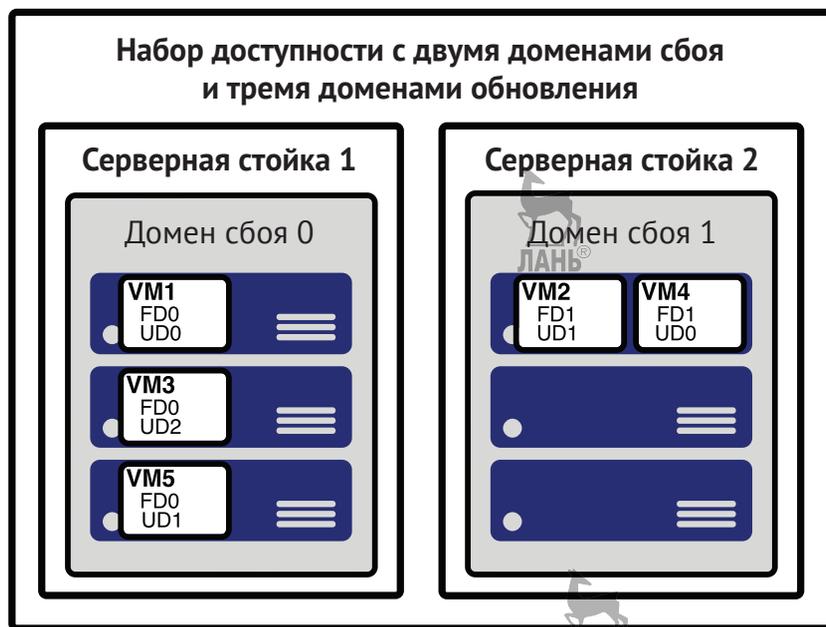


Рис. 2.18 Более наглядное представление набора доступности

Вы можете проверить размещение доменов сбоев и обновления, создав в наборе доступности пять VM с двумя доменами сбоя и тремя доменами обновления. Если посмотреть на набор доступности, созданный на портале Azure, как показано на рис. 2.19, то можно увидеть ту же конфигурацию, что и на рис. 2.18.

На рис. 2.19 вы видите, что набор доступности называется *WebAvailability-Set*. В этом наборе доступности мы запускаем пять VM, на которых работает веб-сервер, и размещаем веб-сайт для приложения. Предположим, вам необходима база данных для этого приложения, которую вы также хотите разместить на VM. Для этого потребуется разделить VM базы данных на их собственный набор доступности. Всегда лучше разделять сценарии разработки приложения на отдельные наборы доступности.

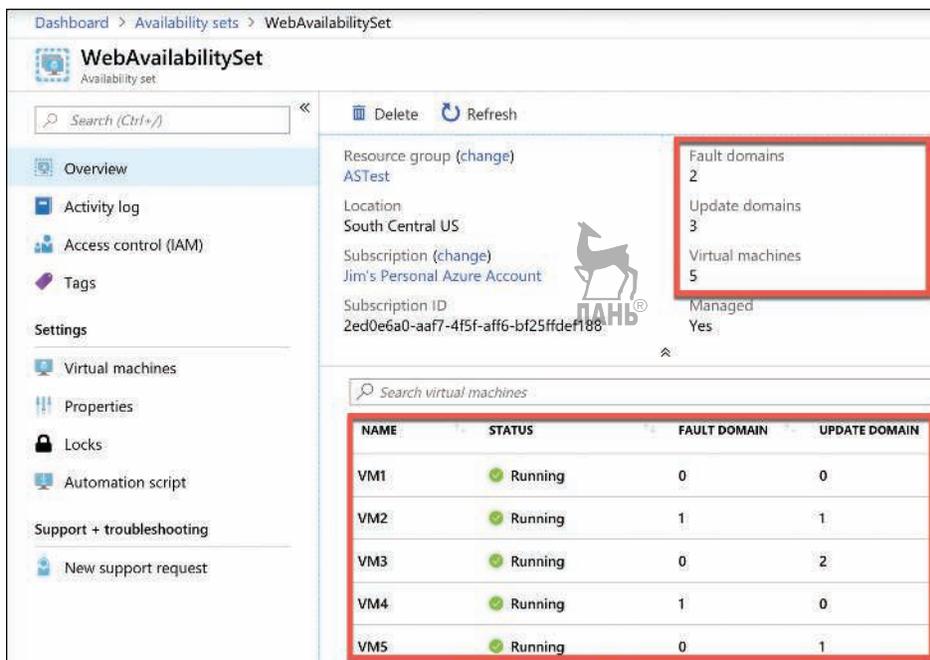


Рис. 2.19 Набор доступности на портале Azure с доменами сбоя и обновлений

У наборов доступности есть несомненное преимущество, которое заключается в защите от простоев, однако есть и свои недостатки. Прежде всего необходимо, чтобы все компьютеры в наборе доступности были явно созданы. Несмотря на то что шаблон ARM можно использовать для создания одновременно нескольких виртуальных машин, вам нужно будет самим настроить ПО и конфигурацию на этих машинах для корректной работы приложения.

Также важно, чтобы в наборе доступности дополнительно было настроено распределение трафика между этими VM. Например, если набор доступности обслуживает веб-сайт, размещенный на VM, вам необходимо настроить балансировщик нагрузки для распределения пользовательских запросов.

Еще одним недостатком наборов доступности является их стоимость. В условиях, когда ваши потребности в VM часто меняются в зависимости от таких факторов, как нагрузка на приложение, вы можете столкнуться с тем, что платите за их ненужное количество.

ДОПОЛНИТЕЛЬНО ИСПОЛЬЗОВАНИЕ ПОЛЬЗОВАТЕЛЬСКОГО ОБРАЗА

По умолчанию наборы шаблонов для VM базовые и включают только операционную систему. Однако можно создать VM, установить все необходимые компоненты (вместе с собственными приложениями), а затем создать образ, который можно использовать при создании масштабируемых наборов.

Дополнительные сведения об использовании пользовательских образов вы найдете по ссылке <https://bit.ly/az900-customvmimages>.

Azure предлагает еще одну функцию для ВМ, называемую *наборами масштабирования* (scale sets), которая прекрасно решает эти проблемы. При создании такого набора вы сообщаете Azure, какую операционную систему вы хотите запустить, а затем указываете необходимое количество ВМ в наборе масштабирования. У вас также есть множество других вариантов, например использование балансировщика нагрузки или *иных* инструментов. Azure создаст столько ВМ, сколько вы указали (до 1000), за одно легкое движение.

Наборы масштабирования разворачиваются в наборах доступности автоматически, поэтому вы получаете преимущества от нескольких доменов сбоя и обновления. В отличие от ВМ в наборе доступности, ВМ в наборе масштабирования также совместимы с зонами доступности, что защищает вас от возможных проблем в центрах обработки данных Azure.

Наборы масштабирования можно масштабировать в зависимости от потребности в большем или меньшем количестве ВМ. Вы можете начать работать только с одной ВМ в наборе масштабирования, но по мере увеличения нагрузки на нее может потребоваться автоматическое добавление новых ВМ. Наборы масштабирования обеспечивают данную функциональность с помощью автоматического масштабирования Azure. Вы определяете правила масштабирования, которые используют такие метрики, как загрузка ЦП, использование диска, сети и т. д. Вы также можете настроить условия, при которых Azure должна добавлять новые экземпляры, уменьшать их или отключать. Это отличный способ обеспечить доступность при одновременном снижении затрат благодаря эластичности от автомасштабирования.

ДОПОЛНИТЕЛЬНО МАСШТАБИРОВАНИЕ И НАБОРЫ ДОСТУПНОСТИ

До появления наборов масштабирования вы могли самостоятельно настраивать правила автоматического масштабирования для набора доступности. Информацию и учебные материалы по масштабированию наборов доступности все еще можно встретить, хотя данная функциональность уже была заменена наборами масштабирования.

Microsoft гарантирует SLA на 99,95% для сценария развертывания нескольких ВМ, что обычно является наиболее предпочтительным вариантом. Однако если вы используете единственную ВМ и premium-хранилище, Microsoft гарантирует SLA на 99,9%. Для повышения производительности и уменьшения ошибок в работе premium-хранилище использует SSD-диски (solid state drive), расположенные на том же физическом сервере, на котором запущена и сама ВМ.

Служба приложений Azure

Как уже говорилось в главе 1, служба приложений Azure (Azure App Service) представляет собой предложение PaaS в Azure для размещения веб-сайтов. Помимо базовой услуги по размещению сайтов, служба приложений Azure также предлагает многие дополнительные функции, которые можно без труда добавить в веб-приложение несколькими кликами на портале Azure.

Когда вы создаете веб-приложение в службе приложений Azure, ваше приложение работает на виртуальных машинах Azure, которые заранее настраиваются под службу приложений. В зависимости от уровня сервиса, который вы используете для создания приложения, оно будет работать либо на общей для пользователей ВМ, либо на ВМ, специально отведенной для вас.

На рис. 2.20 показана схема базовой архитектуры службы приложений. Эта упрощенная версия схемы, но, несмотря на это, там отображены основы того, как функционирует служба приложений. Балансировщик нагрузки Azure распределяет трафик на специальную ВМ в службе приложений, называемую *внешним интерфейсом* (front end). Внешний интерфейс работает на специальном ПО, позволяющем эффективно распределять трафик на ВМ, на которых в данный момент работает приложение. Работа этих ВМ происходит в плане службы приложений (App Service plan), логическом контейнере для одной или более ВМ веб-приложения.

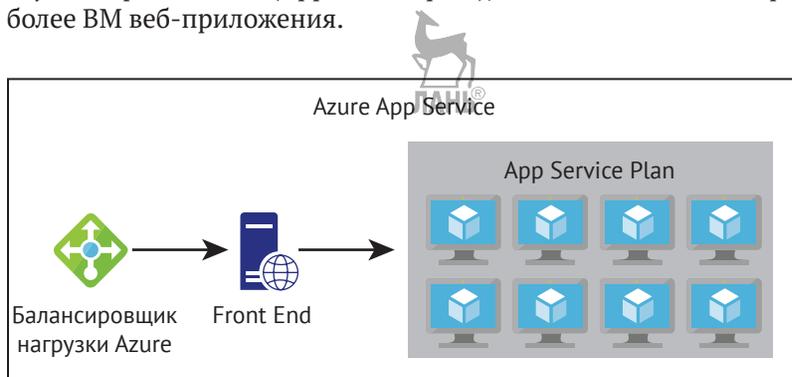


Рис. 2.20 Высокоуровневое представление службы приложений Azure

Планы службы приложений

Любое веб-приложение, созданное в службе приложений, работает внутри плана службы приложений. План службы приложений создается в определенном регионе Azure, и это определяет количество ВМ, на которых работает приложение, и их возможности.

ПРИМЕЧАНИЕ ПЛАН СЛУЖБЫ ПРИЛОЖЕНИЙ

В приведенном примере этой главы было запущено одно приложение в плане службы приложений. В рамках одного плана службы приложений может выполняться несколько приложений. Все приложения в плане будут использовать одни и те же ВМ.

На рис. 2.21 изображен план службы приложений под названием *AZ900-Plan*, создаваемый в Центральном регионе США. ВМ в этом плане службы приложений будут работать на Windows, а также будут создаваться в стандартном уровне цен S1 службы приложений. Вы можете изменить ценовую категорию нажатием на кнопку **Change Size** (Изменить размер) перед созданием плана службы приложений. Вы всегда можете масштабировать план службы приложений для изменения его размера.

App Service Plan

App Service plans give you the flexibility to allocate specific apps to a given set of resources and further optimize your Azure resource utilization. This way, if you want to save money on your testing environment you can share a plan across multiple apps. [Learn more](#)

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource Group * [Create new](#)

App Service Plan details

Name *

Operating System *

Region *

Pricing Tier

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. [Learn more](#)

Sku and size * **Standard S1**
100 total ACU, 1.75 GB memory
[Change size](#)

[Review + create](#) [< Previous](#) [Next : Tags >](#)

Рис. 2.21 Создание плана службы приложений в Центральном регионе США

В службе приложений доступны следующие ценовые категории:

- **бесплатный уровень** для тестирования, выполняющегося на VM, которые совместно используются разными клиентами службы приложений;
- **общий доступ** – недорогой уровень для тестирования с некоторыми дополнительными функциями, которые не предлагаются на бесплатном уровне. Работает на VM, совместно используемых разными клиентами службы приложений;
- **базовый, стандартный, премиальный и премиальный V2** – дорогостоящие уровни, предлагающие множество дополнительных функций. Работают на выделенных индивидуально под клиентов VM.



СОВЕТ К ЭКЗАМЕНУ

Плата за планы служб приложений продолжит с вас взиматься даже при незапущенных веб-приложениях. За приостановленные веб-приложения также придется платить. Единственным способом избежать списания средств за план службы приложений является его удаление.

При переходе с более низкой ценовой категории на более высокую вы прибегаете к вертикальному масштабированию. В любой момент можно обратиться к горизонтальному масштабированию путем снижения ценовой категории. Работая на базовом, стандартном, премиальном или премиальном V2 уровнях, можно горизонтально масштабироваться до нескольких ВМ. Базовый уровень позволяет вам масштабировать максимум до 3 ВМ (или экземпляров), стандартный уровень дает возможность создавать 10 экземпляров, а уровни премиум и премиум V2 – до 20 экземпляров.

ДОПОЛНИТЕЛЬНО ВИРТУАЛЬНЫЕ МАШИНЫ СЛУЖБЫ ПРИЛОЖЕНИЙ

Создание веб-приложения в службе приложений и его горизонтальное масштабирование до нескольких экземпляров не занимает много времени. Это связано с тем, что ВМ, на которых запущены веб-приложения службы приложений, готовы и уже работают. Когда вы создаете веб-приложение, вы просто выделяете для использования существующую ВМ.

Веб-приложения

Для создания нового веб-приложения вы можете использовать существующий план службы приложений или же создать новый. Все приложения в плане службы приложений работают на тех же ВМ, поэтому если вами уже используются ресурсы существующего плана службы приложений, то лучше создать новый план для нового веб-приложения.

Служба приложений позволяет вам выбрать между предварительно настроенной ВМ для различных сред выполнения (например, Java, .NET, PHP и т. д.) для запуска приложения или контейнера Docker. Если вы решите выбрать предварительно настроенную среду выполнения, то вам на выбор будет даваться одна из нескольких версий окружения, предоставляемых службой приложений.

ДОПОЛНИТЕЛЬНО КОНТЕЙНЕР DOCKER

О содержимом Docker вы узнаете в следующем разделе, когда мы будем говорить о контейнерах в Azure.

На рис. 2.22 показано веб-приложение, создаваемое в плане службы приложений AZ900-Plan. Это новое веб-приложение будет работать на ВМ, настроенной для запуска приложений .NET Core 3.0 на ВМ под управлением Windows.

Настройка и управление веб-приложением довольно просты. Поскольку служба приложений является службой PaaS, вы ответственны только за свой код. Microsoft управляет доступными вам функциями. На рис. 2.23 вы видите многие доступные в службе приложений функции, включая и возможность быстрого и простого горизонтального масштабирования.



Web App

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource Group * [Create new](#)

Instance Details

Name * [.azurewebsites.net](#)

Publish * Code Docker Container

Runtime stack *

Operating System * Linux Windows

Region *
 ⓘ Not finding your App Service Plan? Try a different region.

App Service Plan

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. [Learn more](#)

Windows Plan (Central US) * [Create new](#)

[Review + create](#) [< Previous](#) [Next: Monitoring >](#)

Рис. 2.22 Создание веб-приложения для запуска веб-сайта на базе .NET Core 3.0

cheshireaz900 | Scale out (App Service plan)

App Service

Search (Cmd+/) Save Discard Refresh Provide feedback

Settings

- Configuration
- Authentication / Authorization
- Application Insights
- Identity
- Backups
- Custom domains
- TLS/SSL settings
- Networking
- Scale up (App Service plan)
- Scale out (App Service plan)**
- WebJobs
- Push
- MySQL In App
- Properties
- Locks
- Export template

Configure Run history JSON Notify Diagnostics settings

Autoscale is a built-in feature that helps applications perform their best when demand changes. You can choose to scale your resource manually to a specific instance count, or via a custom Autoscale policy that scales based on metric(s) thresholds, or scheduled instance count which scales during designated time windows. Autoscale enables your resource to be performant and cost effective by adding and removing instances based on demand. [Learn more about Azure Autoscale](#)

Choose how to scale your resource

Manual scale

Maintain a fixed instance count

Custom autoscale

Scale on any schedule, based on any metrics

Manual scale

Override condition

Instance count

Рис. 2.23 Параметры веб-приложения упрощают добавление функций и масштабирование приложения

Экземпляры контейнеров Azure (Azure Container Instances, ACI)



Экземпляры контейнеров Azure (Azure Container Instances, ACI) являются службой PaaS, которая позволяет легко запускать контейнерные приложения. Для того чтобы понять, как работает ACI, вам необходимо иметь базовое представление о контейнерах.

Контейнеры

Для многих компаний становится обычным делом перемещать приложения между различными «окружениями», и этот подход начинает все больше преобладать в облачных сервисах. Одним из самых сложных аспектов перехода в облако является миграция в новое окружение. Чтобы помочь в решении этой проблемы и облегчить перенос приложений в новые окружения, была предложена концепция *контейнеров*.

Контейнер создается с помощью заархивированной версии приложения, называемого *образом*, и включает в себя все необходимые компоненты для запуска этого приложения. Такой образ может включать в себя ядро базы данных, веб-сервер и прочее. Образ можно развернуть в любом окружении, поддерживающем использование контейнеров. После этого образ используется для запуска контейнера, в котором, в свою очередь, будет запущено приложение.

Для запуска приложения в контейнере на компьютере должна быть установлена специальная среда выполнения. Самой популярной средой для запуска контейнеров в настоящее время является Docker, разрабатываемая и поддерживаемая компанией Docker. Docker не только знает, как запускать приложения в контейнерах, но и обеспечивает соблюдение высоких требований безопасности.

ДОПОЛНИТЕЛЬНО DOCKER-ОБРАЗЫ

Вы можете создавать свои или использовать уже готовые образы. Docker создает и поддерживает репозиторий образов, которые можно использовать в своих приложениях. Репозиторий вы найдете по ссылке: <https://hub.docker.com>.

Каждый контейнер работает в изолированной среде. У него своя сеть, собственное хранилище и т. д. Другие контейнеры, работающие на том же компьютере, не могут получить доступ к данным и системам, используемым вашим контейнером (если только не были предприняты явные действия, разрешающие это). Это делает контейнеры идеальным решением, когда важна безопасность.

Работа контейнеров на ACI

ACI упрощает запуск контейнеров с минимальной конфигурацией. Вы просто указываете ACI, где найти образ (используя тег Docker или URL-адрес) и базовую конфигурацию VM, на которой хотите, чтобы работал контейнер.

Azure создает серверные ресурсы, необходимые для запуска контейнера, но вы платите не за базовую VM, а за память и процессор, которые использует ваш контейнер. В большинстве случаев это приводит к минимальным затратам. Например, если приложение ACI работает на компьютере с 1 процессором и 1 ГБ памяти и вы используете приложение в течение 5 минут в день, в конце месяца ваша стоимость составит менее 5 центов!

ПРИМЕЧАНИЕ У КОНТЕЙНЕРОВ СВОЯ ОС

Операционная система для контейнера, по сути, является частью образа. VM, которую вы настраиваете при создании приложения ACI, — это VM, на которой работает среда выполнения контейнера. Важно, чтобы операционная система была совместима с вашим контейнером. Образ Docker, созданный для Linux, не будет работать на хосте Windows, и наоборот.

ACI предназначен для работы с простыми приложениями. Вы можете объединить несколько контейнеров в группу и запустить их в качестве единого экземпляра ACI, но сам ACI не позволит вам масштабировать приложение в случае увеличения нагрузки. Для масштабирования контейнерных приложений лучше подойдет служба Azure Kubernetes Service (AKS).

ДОПОЛНИТЕЛЬНО СЛУЖБА AZURE KUBERNETES

Подробнее о службе Azure Kubernetes мы поговорим в следующем разделе.

При создании экземпляра контейнера ACI вы указываете имя контейнера, используемый образ и размер VM, на которой будет запускаться контейнер. При отсутствии у вас образа Microsoft предоставит несколько шаблонов. На рис. 2.24 показан экземпляр ACI с именем *jimsaciapp*, который создается в восточном регионе США с использованием одного из шаблонов образа для быстрого запуска (Quickstart).

Чтобы этот экземпляр был доступным через интернет, вам нужно установить для него имя метки DNS. Эти параметры вы получите, нажав на кнопку **Next** (Далее): **Networking** (Сеть) в нижней части экрана (см. рис. 2.24). На рис. 2.25 имя DNS (DNS name) для данного экземпляра имеет значение *jimsaciapp*. После создания экземпляра к нему можно получить доступ по следующей ссылке: <http://jimsaciapp.eastus.azurecontainer.io>.



СОВЕТ К ЭКЗАМЕНУ

Изменить имя DNS после создания экземпляра нельзя. Аналогичным образом вы не сможете изменить образ, используемый экземпляром. Если вы все-таки захотите поменять данные настройки, то вам понадобится удалить экземпляр, а потом создать его заново. Однако такие действия приведут к потере публичного IP-адреса, поэтому лучше всего заранее все распланировать.

Create container instance

Azure Container Instances (ACI) allows you to quickly and easily run containers on Azure without managing servers or having to learn new tools. ACI offers per-second billing to minimize the cost of running containers on the cloud.
[Learn more about Azure Container Instances](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Container details

Container name * ⓘ

Region * ⓘ

Image source * ⓘ Quickstart images
 Azure Container Registry
 Docker Hub or other registry

Image * ⓘ

Size * ⓘ [Change size](#)

[Review + create](#) [< Previous](#) [Next : Networking >](#)

Рис. 2.24 Создание экземпляра ACI с образом из **Quickstart** (Быстрый запуск)

Create container instance

[Basics](#) [Networking](#) [Advanced](#) [Tags](#) [Review + create](#)

Choose between three networking options for your container instance:

- **'Public'** will create a public IP address for your container instance.
- **'Private'** will allow you to choose a new or existing virtual network for your container instance. This is not yet available for Windows containers.
- **'None'** will not create either a public IP or virtual network. You will still be able to access your container logs using the command line.

Networking type Public Private None

DNS name label ⓘ .eastus.azurecontainer.io

Ports ⓘ

Ports	Ports protocol
80	TCP

Рис. 2.25 Установка имени DNS для последующего перехода к экземпляру по URL-адресу

Служба Azure Kubernetes (Azure Kubernetes Service, AKS)

Kubernetes – это служба управления контейнерами. Это означает, что данный сервис отвечает за мониторинг и запуск контейнеров, а также гарантирует их работоспособность. Он также может автоматически масштабировать необходимое количество контейнеров в случае увеличения или уменьшения нагрузки.

Kubernetes создает контейнеры в *подах* (*pod* – «стручок, кокон»). Под является группой связанных контейнеров, которые могут совместно использовать различные ресурсы. Это одно из преимуществ Kubernetes, поскольку он освобождает вас от ограничения совместного использования ресурсов, характерного для среды со множественностью контейнеров. Тем не менее контейнер в одном поде не может совместно использовать ресурсы с контейнером в другом поде.

Компьютер, на котором запущены поды Kubernetes, называется *узлом* (*host*) или *работником* (*worker*). На этом компьютере должна быть запущена среда выполнения контейнера, например Docker. В дополнение к подам узел также запускает несколько служб, которые необходимы Kubernetes для управления подами. Обычно в одном экземпляре Kubernetes находится несколько узлов, и все они управляются главным компьютером, называемым *мастером*. Среда мастера и его узлы называются *кластером* Kubernetes.

Мастер Kubernetes содержит все настройки и службы, необходимые для управления подами и другими объектами. Настройка мастера является непростой и самой трудоемкой задачей при создании кластера Kubernetes. По этой причине такие службы, как Azure Kubernetes (AKS), становятся все более популярными.

AKS переносит сложность настройки кластера Kubernetes на Microsoft. При создании кластера Kubernetes AKS создает для вас мастера и узлы Kubernetes. Все, что вам останется сделать, – это развернуть ваши контейнеры внутри готового кластера Kubernetes.

AKS упрощает не только создание кластера Kubernetes, но и управление им (рис. 2.26). Операции, связанные с обновлением или масштабированием кластера, заметно упрощаются с помощью веб-портала Azure. Вы также можете получить подробную информацию как о работе кластера в целом, так и о каждом узле в отдельности.

AKS облегчает использование и управление Kubernetes, при этом его не усложняя. Чтобы развернуть приложения, вам все равно необходимо понять, как работает Kubernetes, а в некоторых случаях даже использовать командную строку. Azure, однако, заметно упрощает работу и обслуживание кластера. И что немаловажно, AKS в Azure бесплатен. Оплата производится только за вычислительные ресурсы, используемые самим кластером.

Виртуальный рабочий стол Azure

У множества компаний есть такие приложения, которыми пользуются все сотрудники. Например, если нужен доступ к Microsoft Word, Microsoft Excel, Microsoft Outlook и т. д.

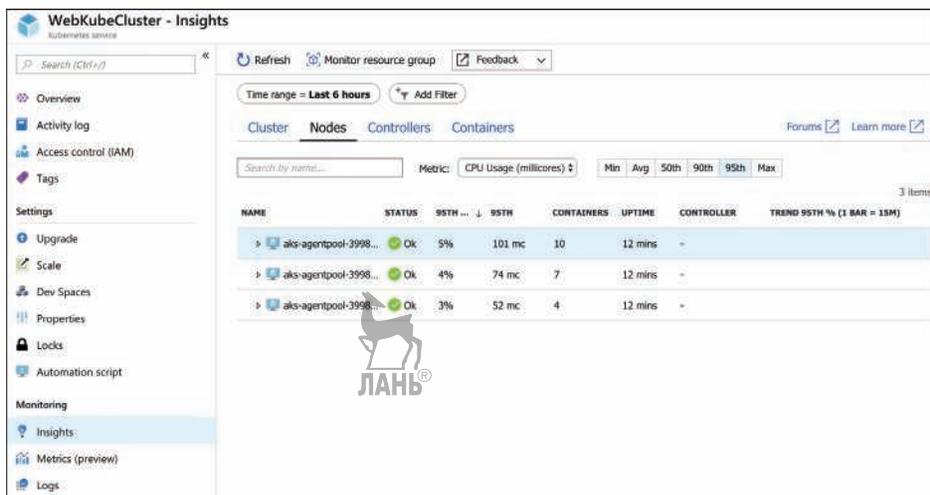


Рис. 2.26 Кластер AKS на портале Azure

Зачастую это решается покупкой лицензионного Microsoft Office на всех с установкой Office на компьютер каждого сотрудника.

Классическая модель, при которой сотрудником используется один компьютер с установленными приложениями, не только неэффективна, но и небезопасна. Во-первых, компании нужно покупать лицензии на операционную систему и приложения для каждого. Также понадобится ИТ-отдел, который будет следить за устранением неполадок. У пользователей локальных приложений есть данные, хранящиеся на жестком диске, что ставит под угрозу безопасность, если нежелательные лица получают доступ к компьютеру.

По этим и многим другим соображениям многие компании используют виртуализацию настольных ПК. В данной модели компания устанавливает операционную систему и приложения на одном центральном сервере. Инфраструктура виртуализации настольных ПК позволяет сотрудникам получать доступ к операционной системе и приложениям практически с любого устройства, при условии что есть доступ к сети. ОС и приложения загружаются на девайс сотрудника, который использует приложения в виртуализированной среде, имитирующей локальное выполнение приложений.

ДОПОЛНИТЕЛЬНО ВИРТУАЛИЗАЦИЯ НАСТОЛЬНЫХ ПК

Если вы уже использовали удаленный рабочий стол Windows (Windows Remote Desktop) для удаленного доступа к другому компьютеру, то вы имели дело с чем-то похожим на виртуализацию рабочего стола. Разница лишь в том, что виртуализация позволяет вам виртуально получить доступ к операционной системе и приложениям, настроенным для удаленного доступа на VM.

Виртуализация настольных ПК может показаться идеальным решением для многих компаний, но на самом деле ее довольно сложно настроить, и для обеспечения безопасной среды потребуется множество компонентов. По этой

причине Microsoft разработала службу в Azure, которая называется виртуальный рабочий стол Windows (Windows Virtual Desktop, WVD).

Виртуальный рабочий стол Windows – это PaaS-предложение Azure, которое обеспечивает виртуализацию рабочих столов, управляемую Microsoft. Для этого вам понадобится расширенная конфигурация, но сразу после ее настройки инфраструктура будет полностью управляться Microsoft.

Чтобы использовать виртуальный рабочий стол Windows, для начала создайте WVD-клиента. Клиентом является набор из одного или нескольких пулов хостов, которые, в свою очередь, состоят как из хостов сеансов, так и из одной или нескольких групп приложений, представляющих приложения и рабочие столы ОС, к которым у пользователей должен быть доступ. Эти хосты сеансов – всего лишь виртуальные машины в Azure, настроенные вами под WVD.

После настройки клиента вы можете добавить пользователей из Azure Active Directory, чтобы они могли получать доступ к операционным системам и приложениям в клиенте, и назначить им права доступа. После этого пользователи могут получить доступ к WVD при помощи следующих методов:

- используя клиентское приложение WVD для Windows;
- применяя клиентское приложение WVD для MacOS;
- при помощи клиента WVD для iOS;
- используя веб-клиента для Android;
- веб-клиентом любого веб-браузера.

ДОПОЛНИТЕЛЬНО ВИРТУАЛЬНЫЙ РАБОЧИЙ СТОЛ WINDOWS

За дополнительной информацией о виртуальном рабочем столе Windows, требованиях по его использованию и руководстве по настройке обращайтесь по ссылке: <https://bit.ly/AZ900-winvirtualdesktop>.

Конечный пользователь, получающий доступ к WVD, видит список доступных ему ОС и приложений. Нажав на ОС, он сможет взаимодействовать с ней так же, как если бы запускал ее на своем локальном компьютере. Нажав на приложение, пользователь запустит его в виртуальном сеансе, при этом создается впечатление, будто оно запущено локально. Благодаря приобретенной Microsoft технологии FSLogix WVD обеспечивает локальный профиль, пока пользователем используется приложение. Данная возможность даже позволяет использовать файлы в Microsoft OneDrive вместе с WVD.

ДОПОЛНИТЕЛЬНО WINDOWS 10 MULTI USER

Microsoft разработала специальную версию Windows 10 – многопользовательскую (multi user) Windows 10, для поддержки функциональности виртуального рабочего стола Windows.

Виртуальные сети

Виртуальная сеть Azure (часто называемая VNet) позволяет службам Azure взаимодействовать друг с другом и интернетом. VNet можно даже использовать для взаимодействия между локальными ресурсами и ресурсами Azure.

При создании виртуальной машины в Azure для нее создается VNet. Без VNet вы не сможете удаленно подключаться к VM или использовать для приложений. Однако можно создать собственную VNet и настроить ее любым удобным для вас способом.

Azure VNet является такой же компьютерной сетью, как и любая другая. Она состоит из сетевых адаптеров (network interface card, NIC), IP-адресов и других компонентов. Вы можете разбить VNet на несколько подсетей и настроить пространство IP-адресов сети для каждой подсети. После можно настроить правила, которые будут регулировать подключение между этими подсетями.

На рис. 2.27 показана Azure VNet, которую можно использовать для многоуровневого приложения. VNet использует IP-адреса в диапазоне 10.0.0.0, и у каждой подсети есть свой собственный диапазон адресов. Диапазоны IP-адресов в VNet задаются с помощью бесклассовой междоменной маршрутизации (classless inter-domain routing, CIDR), но обсуждение этого вопроса не входит в рамки экзамена. Однако при конфигурации, указанной на рис. 2.27, в нашей VNet доступно 65 536 IP-адресов, и каждой подсети выделено 256 IP-адресов. (Первые четыре и последний в диапазоне IP-адреса зарезервированы под использование Azure, поэтому на самом деле у вас только 251 адрес для использования в каждой подсети.) Это стандартная конструкция, поскольку в сети по-прежнему имеется большое количество адресов для последующего расширения в дополнительной подсети.

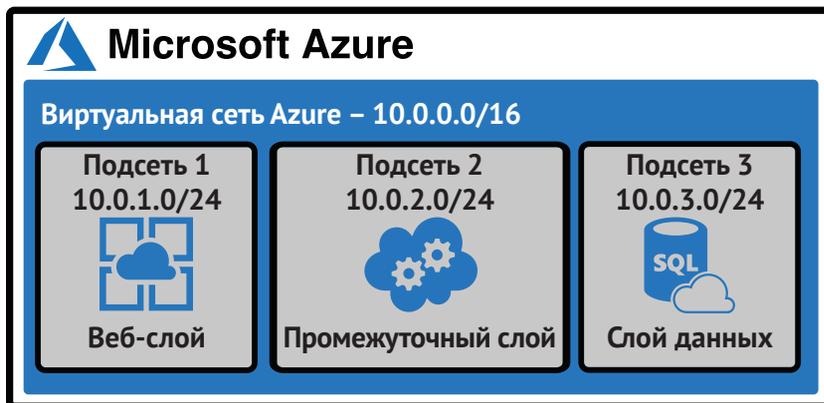


Рис. 2.27 Многослойное приложение в виртуальной сети Azure

В подавляющем большинстве случаев сперва вы создаете VNet, а потом ресурсы, которые использует сеть. Как я уже выше говорил, когда мы создаем VM в Azure, автоматически создается и VNet. Это происходит потому, что использовать VM, пока она не связана с сетью, невозможно. Можно подключить создаваемую VM к существующей VNet, однако если VM уже создана, то нельзя. Поэтому если вы хотите использовать свою VNet, а не ту, которую Azure создает автоматически, вам нужно создать свою VNet до создания VM.

С другой стороны, веб-слой на рис. 2.27 работает на базе PaaS-решения в Службе приложений Azure. Наше приложение выполняется на VM, которой

управляет Microsoft, поэтому именно Microsoft создает и управляет VM и ее сетью. Для использования данного слоя с VNet Служба приложений также предлагает функцию **VNet Integration** (Интеграция виртуальной сети), которая позволяет интегрировать веб-приложение в Службе приложений с существующей VNet.

IP-адреса в VNet на данный момент являются частными. Они позволяют ресурсам VNet взаимодействовать друг с другом, но вы не можете использовать частный IP-адрес в интернете. Для того чтобы предоставить доступ в интернет для веб-приложения, вам нужен общедоступный (публичный) IP-адрес.

ДОПОЛНИТЕЛЬНО ИСХОДЯЩЕ ИНТЕРНЕТ-ПОДКЛЮЧЕНИЕ

Для того чтобы отдельный ресурс мог сам посылать данные в интернет, ему не нужен общедоступный IP-адрес. Azure поддерживает пул общедоступных IP-адресов, которые могут динамически назначаться ресурсу, если ему необходимо установить исходящее соединение. Этот IP-адрес не привязывается к ресурсу, поэтому его нельзя использовать для получения входящих интернет-соединений.

Поскольку веб-слой работает в Службе приложений Azure (служба PaaS), Microsoft управляет общедоступной сетью. Вы автоматически получаете доступ к приложению через интернет. Если же требуется запустить веб-слой на VM IaaS, то вам придется самостоятельно настраивать для нее общедоступный IP-адрес. В таком случае Azure позволяет создать общедоступный IP-адрес в виде отдельного ресурса и назначить его виртуальной сети.

ДОПОЛНИТЕЛЬНО ГРУППЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

Azure предлагает функцию **Network Security Groups** (Группы сетевой безопасности), которая позволяет настраивать правила фильтрации трафика в VNet. Мы рассмотрим группы сетевой безопасности в главе 4 «Особенности общей и сетевой безопасности».

ExpressRoute

Виртуальные сети Azure предоставляют возможность подключения к локальным сетям с использованием подключения виртуальной частной сети (virtual private network, VPN). Многие используют этот метод для подключения локальных ресурсов к Azure. Однако есть некоторые аспекты применения VPN, которые подойдут не для всех клиентов. Например, существует ограничение скорости сети для VPN, равное 1,25 Гбит/с. Если клиенту нужна более высокая скорость, то VPN – не лучшее решение.

Azure предлагает службу ExpressRoute, которая может обеспечивать скорость до 10 Гбит/с по выделенным волоконно-оптическим соединениям. При использовании ExpressRoute вы подключаетесь из локальной сети к маршрутизатору Microsoft Enterprise Edge (MSEE), который затем подключает вас к Azure. Маршрутизатор MSEE находится на периферии сети Microsoft, и в большинстве случаев ваше соединение также будет осуществляться с маршрутизатора в локальной сети, находящегося на периферии сети.

ДОПОЛНИТЕЛЬНО ПЕРИФЕРИЙНЫЕ СЕТЕВЫЕ УСТРОЙСТВА

Периферийное устройство в сети относится к устройству, которое работает как точка доступа в сеть. Представьте сеть кругом; устройства этой сети будут находиться внутри этого круга. А теперь представьте периферийное устройство, которое располагается на линии круга.

Очень часто клиенты подключаются к маршрутизатору MSEE при помощи стороннего провайдера услуг. Эти провайдеры являются крупными поставщиками сетевых услуг и нередко интернет-услуг. У провайдеров есть сетевые подключения прямо к маршрутизатору MSEE, а у сетевых подключений имеются выделенные полосы пропускания. На рис. 2.28 показана стандартная конфигурация ExpressRoute.

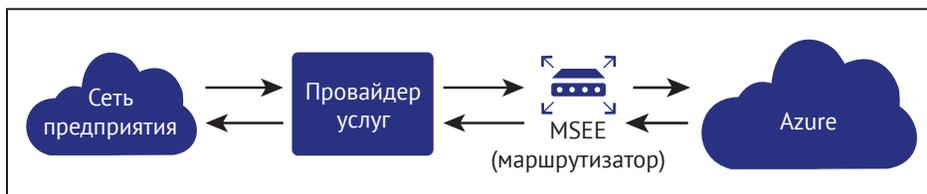


Рис. 2.28 Стандартная конфигурация ExpressRoute



СОВЕТ К ЭКЗАМЕНУ

Microsoft именует соединение ExpressRoute *цепью (chain)*.

Данные в ExpressRoute не пересекают общедоступный интернет, поэтому пропускная способность намного надежнее. Однако для конфигурации ExpressRoute, которую вы видите на рис. 2.28, необходимо, чтобы вы поручали провайдеру данные, которые проходят по цепи. Если вам нужно удалить провайдера с картинки, то вы можете воспользоваться предложением ExpressRoute Direct, которое позволяет напрямую подключиться к физическому порту маршрутизатора MSEE.

ДОПОЛНИТЕЛЬНО EXPRESSROUTE И ДОСТУПНОСТЬ

ExpressRoute рассчитан на высокую доступность. Все цепи используют резервные соединения, поэтому если вы создадите цепь со скоростью 5 Гбит/с, то фактическая пропускная способность, выделенная для цепи, составит 10 Гбит/с. Microsoft даже позволит вам использовать эту дополнительную пропускную способность для коротких очередей.

Хранилище BLOB-объектов

Хранилище BLOB-объектов Azure (Azure Blob Storage) предназначено для хранения данных без определенной структуры. Такими объектами могут быть текстовые файлы, изображения, видео, документы и многие другие типы файлов. Сущность, хранящаяся в BLOB-хранилище, называется *блором (blob, Bina-*

ry Large Object – двоичный большой объект). В Azure Storage поддерживаются три типа блобов:

- **блочные BLOB-объекты** (*block blobs*) используются для хранения файлов приложения;
- **добавочные BLOB-объекты** (*append blobs*) аналогичны блочным, но оптимизированы для операций добавления. По этой причине они часто используются для хранения постоянно обновляемых данных, таких как журналы диагностики;
- **страничные BLOB-объекты** (*page blobs*) используются для хранения файлов виртуальных жестких дисков (virtual hard disk, .vhd), которые подключаются к виртуальным машинам Azure. Мы рассмотрим их в дисковом хранилище Azure (Azure Disk Storage).

Блобы хранятся в специальных *контейнерах*. Контейнер используется как средство структурирования блобов, поэтому существуют их разные типы: контейнеры для видеофайлов, для файлов изображений и т. д. Только вы выбираете, что в них хранить.

Перенести данные из локальной среды в хранилище Azure можно несколькими способами. Для загрузки данных можно использовать Azure Storage Explorer, бесплатное приложение от Microsoft. Можно также использовать средства командной строки, которые Microsoft предоставляет для загрузки файлов в Azure Storage.

Microsoft предлагает сервис *Data Box* для перемещения большого объема данных. В Data Box есть онлайн-служба Data Box Edge, которая упрощает копирование данных в хранилище Azure – весь процесс становится похожим на несложное копирование файлов на жесткий диск в системе. Для более крупных объемов данных Microsoft предлагает автономную службу Data Box (офлайн), при которой в комплекте поставляются жесткие диски. Вы просто копируете свои данные на эти жесткие диски, шифруете их с помощью BitLocker, а затем отправляете обратно в Microsoft. Они даже предлагают сервис Data Box Heavy, когда вам отправляется защищенное устройство на колесиках с вместимостью аж до 1 петабайта данных!

Дисковое хранилище

Дисковое хранилище (Disk storage) в Azure относится к дискам для виртуальных машин. При создании VM Azure формирует диск, который автоматически назначается для временного хранения данных. Это значит, что при обслуживании VM данные на этом диске будут потеряны. Если вам нужно долгосрочное хранение данных, которые будут сохраняться между развертыванием VM и событиями обслуживания, то вы можете создать диск с помощью образа, находящегося в хранилище Azure.

Диски Azure доступны как в виде традиционных жестких дисков (HDD), так и твердотельных накопителей (SSD). Жесткий диск Azure дешевле и предназначен для хранения некритических данных. SSD-накопители уровня Standard предназначены для невысоких нагрузок, а на уровне Premium – для интенсивного использования.

Диски Azure могут быть управляемыми и неуправляемыми. Все диски Azure базируются на BLOB-объектах хранилища Azure. Неуправляемые диски используют вашу учетную запись хранилища Azure, которой вы должны самостоятельно управлять. Это может создать проблемы, так как хранилище Azure имеет свои ограничения, и при высокой нагрузке на диски вы можете в итоге столкнуться с простоем вследствие ограничений.

При переходе на управляемые диски Microsoft изменяет учетную запись хранилища, и все ограничения по памяти снимаются. Ваш ресурс – используемый диск. Также вы можете доверить свою учетную запись хранилища Microsoft.

ДОПОЛНИТЕЛЬНО УПРАВЛЯЕМЫЕ ДИСКИ

Microsoft рекомендует управляемые диски для всех новых и уже существующих ВМ с неуправляемыми дисками.

Наиболее веской причиной для использования управляемых дисков является то, что таким образом вы избегаете ситуации возникновения сбоев в ВМ. При использовании неуправляемых дисков существует вероятность того, что учетные записи хранилища Azure, создающие резервные копии дисков, могут находиться в одном и том же хранилище. Если в этой единице масштабирования произойдет сбой, то вы потеряете все свои диски. За счет того, что каждый управляемый диск находится в отдельном блоке масштабирования, возникновение подобных сбоев исключается.

Файлы Azure (Azure Files)

Диски Azure хорошо подходят для добавления диска на виртуальную машину, но если вам просто нужна область дисковой памяти в облаке, то и нет смысла брать на себя бремя по управлению виртуальной машиной и ее операционной системой. В подобных ситуациях идеальным выходом станут файлы Azure (Azure Files).

ПРИМЕЧАНИЕ ФАЙЛЫ И ХРАНИЛИЩЕ AZURE

Общие ресурсы службы файлов Azure также поддерживаются хранилищем Azure, поэтому для создания общего ресурса данной службы вам понадобится учетная запись хранения.

Файлы Azure – полностью управляемый общий файловый ресурс, который можно подключать так же, как и любой другой файловый ресурс по протоколу SMB (Server Message Block). Это означает, что существующие приложения, использующие сетевые устройства хранения данных (network attached storage, NAS) или общие файловые ресурсы SMB, могут использовать файлы Azure без дополнительных инструментов. А при наличии множества приложений, которым нужен доступ к одному и тому же общему ресурсу, все будет работать, как и раньше, но только со службой файлов Azure.



СОВЕТ К ЭКЗАМЕНУ

Можно подключить общие ресурсы службы файлов Azure на VM Azure и локально в Windows, Linux и MacOS. Однако использовать Windows 7 или Windows Server 2008 для локального подключения общего ресурса файлов Azure нельзя, поскольку эти операционные системы поддерживают только протокол SMB 2.1.

Кроме того, файлы Azure использует протокол SMB, поэтому необходимо убедиться, что TCP-порт 445 открыт в сети. В Windows можно использовать команду PowerShell `Test-NetConnection` для проверки подключения через порт 445. За дополнительной информацией обращайтесь по следующей ссылке: <https://bit.ly/az900-azurefiles>.

Удаленное расположение файлов – одна из возможных проблем использования файлов Azure. Если пользователи или приложения применяют хранилище в сервисе Azure Files, то на передачу файлов уходит больше времени, чем при использовании локальных хранилищ данных. Для решения данной проблемы в Microsoft разработали инструмент синхронизации файлов Azure (Azure File Sync).

Установка инструмента синхронизации файлов Azure на одном или более серверах в локальной сети способствует синхронизации файлов Azure с локальным хранилищем. Когда пользователям или приложениям потребуется доступ к этим файлам, они смогут быстро получить их локальные копии. Любые изменения, внесенные в облачное хранилище файлов Azure, синхронизируются со всеми серверами, на которых настроен инструмент синхронизации.

Уровни доступа к хранилищам

Microsoft предлагает множество уровней хранения BLOB-объектов, стоимость которых зависит от частоты доступа к данным и от срока их хранения и т. д. Уровень «горячего» хранения предназначен для данных, к которым требуется частый доступ. У него самая высокая стоимость хранения, но низкая стоимость доступа к данным. Уровень «холодного» хранения предназначен для данных на долгое хранение и без частого доступа к ним. Стоимость такого хранилища ниже, чем у «горячего», но вот затраты на доступ к данным – выше. Вы также обязаны хранить данные в таком хранилище не менее 30 дней.

Microsoft еще предлагает уровень архивного хранилища для долгосрочного хранения данных. Хранимые таким способом данные имеют самые низкие затраты на хранение и самые высокие затраты на доступ. Хранить заархивированные данные в хранилище положено минимум 180 дней, а иначе вас могут обвинить в досрочном удалении и нарушении условий работы. Поскольку заархивированные данные не предназначены для быстрого и частого доступа, их извлечение может занять очень много времени. В то время как уровни «горячего» и «холодного» доступа гарантируют доступ к первому байту данных в течение миллисекунд, уровень архива гарантирует доступ к первому байту лишь в течение 15 часов.

Azure Cosmos DB

Многие системы баз данных используют реляционные данные. Реляционная база данных содержит связанные таблицы данных. Часть структуры базы дан-

ных определяет взаимосвязь между таблицами. И новые данные, поступающие в базу данных, должны соответствовать *схеме* (способу настройки базы данных).

Существуют и нереляционные системы баз данных – *базы данных NoSQL* (NoSQL databases). В системах NoSQL вы не привязаны к определенной схеме данных.

В реляционной системе, например, для расширения клиентской базы информацией о днях рождения вам нужно будет отредактировать схему базы данных. А в нереляционных системах вы просто заносите день рождения в данные и добавляете их в базу данных. Такой базе данных непринципиален тип данных и поля.

Существует четыре типа систем баз данных NoSQL: ключ-значение, колончатая, документоориентированная и графовая. В табл. 2.1 представлены эти типы и некоторые сведения о них.

Таблица 2.1 Системы баз данных NoSQL

Система	Описание	Использование
БД «ключ-значение» (Key-value)	Хранит данные, привязанные к уникальному ключу. Ключ передается, а база данных возвращает данные	Поскольку значение может представлять собой что угодно, у этой базы данных есть множество применений
Столчатые, или колоночные, БД (Column)	Базы данных NoSQL называют <i>пространствами ключей</i> (keyspaces). Они содержат семейства столбцов. Колонки содержат строки и столбцы, как в реляционной таблице, но у каждой строки может быть свой собственный набор столбцов. Вы не привязаны к определенной схеме	Хранение данных профиля пользователя для веб-сайта. Кроме того, колончатые базы данных хорошо масштабируют и работают довольно быстро, поэтому они хорошо подходят для хранения больших объемов данных
Документоориентированная БД (Document)	Данные хранятся в виде структурированной строки текста – он называется «документ». Документы могут быть HTML, JSON и многое другое. Эти системы похожи на БД ключ-значение, только вот документ является структурированным значением	Документоориентированные БД обладают такими же преимуществами, как и системы пары ключ-значение. Они неплохо масштабируют горизонтально и позволяют делать запросы по значениям, получая часть данных. Запрос к БД ключ-значение возвращает значение целиком, связанное с ключом
Графовая БД (Graph)	Хранит данные и связи между ними. Данные хранятся в узлах, а связи строятся уже между узлами	Многие системы используют графовые базы данных, потому что они очень быстрые. Социальная сеть может использовать графовую базу данных, потому что в ней легко хранить связи между людьми, а также вещи, которые нравятся этим людям, и т. д.

Существует множество различных систем NoSQL, и большинство из них ориентированы на конкретную модель базы данных. Microsoft предлагает систему баз данных NoSQL, размещенную в Azure, под названием Cosmos DB, и эта служба поддерживает все типы баз данных NoSQL. Microsoft создала программные библиотеки для доступа к Cosmos DB, чтобы разработчики смогли использовать свой опыт работы с другими системами баз данных при пере-

ходе на Cosmos DB. Это позволяет существующим приложениям использовать преимущества Cosmos DB без необходимости в доработке кода приложений.

При создании базы данных Cosmos DB выберите API, который вы хотели бы использовать, и это определит тип базы данных. Существуют следующие типы API БД:

- **Core (SQL).** Создает документоориентированную базу данных, к которой можно делать запросы с помощью синтаксиса SQL, знакомого разработчикам реляционных баз данных;
- **Azure Cosmos DB для API MongoDB.** Используется для переноса данных из системы MongoDB в базу данных Cosmos DB. База данных MongoDB является документоориентированной;
- **Cassandra.** Используется для переноса данных из системы Cassandra в базу данных Cosmos DB. База данных Cassandra является колоночной;
- **Azure Table.** Применяется для переноса данных из Azure Table Storage в Cosmos DB. Azure Table – это база данных ключ-значение;
- **Gremlin.** Используется для переноса баз данных Gremlin в Cosmos DB. Базы данных Gremlin являются графовыми.

Названия API соответствуют их назначению. Эти программные интерфейсы (application programming interfaces, API) позволяют разработчикам, использующим базы данных NoSQL, мигрировать в Cosmos DB, не изменяя при этом свой код.

Еще одним заметным преимуществом Cosmos DB является функция «глобальное распределение под ключ» (turnkey global distribution). Эта функциональность использует горизонтальную масштабируемость систем NoSQL и позволяет всего в несколько кликов реплицировать данные по всему миру. На портале Azure можно выбрать регион(ы), где нужна будет репликация данных, как показано на рис. 2.29. После нажатия на **Save** (Сохранить) Cosmos DB начнет реплицировать данные, которые будут доступны в выбранных регионах, что позволяет обеспечить максимально быстрое взаимодействие пользователей и приложения.



Рис. 2.29 Простая репликация по всему миру с помощью Cosmos DB

База данных Azure SQL

База данных Azure SQL (Azure SQL Database) – это предложение PaaS для размещения баз данных SQL Server. Так как Microsoft управляет платформой, вашей областью ответственности становится сама БД и ее данные.

База данных SQL Server хранит *реляционные базы данных*, состоящие из таблиц данных, и каждая таблица имеет схему, которая определяет ее структуру. Например, схема может установить, что данные должны содержать идентификационный номер (ID), имя, фамилию и дату рождения. Все данные таблицы должны придерживаться схемы, поэтому добавляемые данные не должны содержать полей, которые не указаны в схеме.

База данных содержит множество таблиц, связанных друг с другом. Используя специализированные запросы, разработчики смогут возвращать данные, которые будут собираться из разных таблиц. Например, могут быть две таблицы **Customers** (Клиенты) и **Orders** (Заказы), у каждой из которых свое поле, идентифицирующее клиента. Запрашивая и объединяя данные из обеих таблиц, вы можете предоставить пользователю счет со всеми заказами. Эта связь между таблицами объясняет, как реляционные базы данных получили свое название. Обратимся к рис. 2.30.

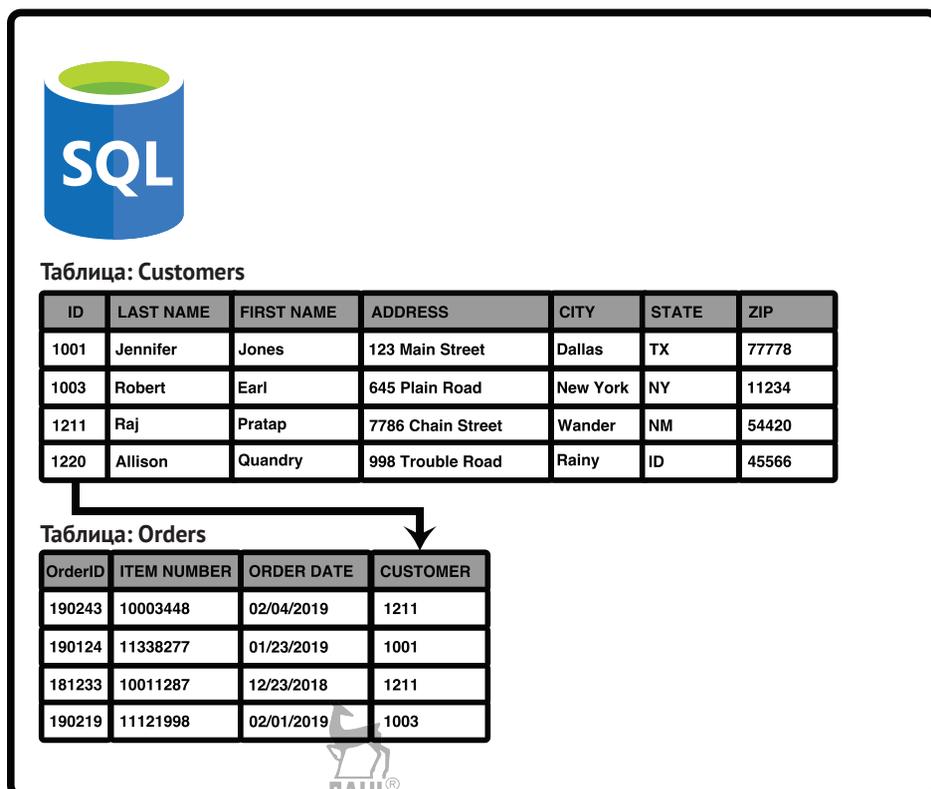


Рис. 2.30 Две таблицы в реляционной базе данных

ПРИМЕЧАНИЕ РЕЛЯЦИОННЫЕ БАЗЫ ДАННЫХ

SQL Server не является единственной системой реляционных баз данных. Существует множество других, в том числе и Oracle, PostgreSQL и MySQL.

Azure предлагает три различных варианта реализации базы данных Azure SQL: отдельная база данных, эластичный пул и управляемый экземпляр.

Отдельная база данных (single databases) – это обычная база данных, работающая в экземпляре SQL Server, запущенном в Azure. Microsoft управляет сервером баз данных, а на вас лежит ответственность за саму базу данных. Microsoft предоставляет две различные модели приобретения такой базы данных: база данных на основе количества транзакций (Database Transaction Unit, DTU) и база данных на основе виртуального ядра (virtual core, vCore).

Модель приобретения на основе единиц DTU представляет собой процессор, память, считываемые и записываемые данные. Существует три уровня DTU модели: базовый, стандартный и премиум. Каждый уровень предлагает более высокое значение процессора, памяти и передачи данных.

ДОПОЛНИТЕЛЬНО ВЫБОР МОДЕЛИ ПРИОБРЕТЕНИЯ

За дополнительной информацией по доступным моделям приобретения и по вопросам выбора между ними перейдите по ссылке: <https://bit.ly/az900-sqlpurchasingmodels>.

Модель приобретения на основе виртуального ядра использует виртуальный процессор, что облегчает настройку необходимой вам конфигурации оборудования. Эта модель предлагает вам уровень общего назначения (General Purpose) и уровень, критически важный для бизнеса (Business Critical). Вы можете выбрать как подготовленный уровень (где вы выбираете процессор, память и другие доступные всегда ресурсы), так и бессерверный, в котором вы задаете диапазон необходимых ресурсов для более эффективного контроля затрат.

В табл. 2.2 показаны эти модели и их различия.

Эластичный пул (elastic pool) состоит из нескольких баз данных (зачастую из множества БД), при этом все они управляются одним и тем же SQL-сервером. Это решение класса SaaS, которое позволяет разным пользователям получить свои базы данных. Вы можете легко перемещать базы данных в эластичный пул и извлекать их, что идеально подходит для SaaS.

Иногда достаточно уметь масштабировать отдельную базу данных для добавления дополнительной мощности. Однако если использование приложения сильно варьируется и вам трудно его предсказать (например, при помощи службы SaaS), то лучше добавить в пул больше экземпляров базы данных. В эластичном пуле взимается плата за использование ресурсов всего пула, а не отдельных баз данных, при этом вы полностью контролируете то, как отдельные БД используют эти ресурсы. Это позволяет не только управлять расходами, но и обеспечивать БД необходимыми ресурсами, при этом сохраняя предсказуемость бюджетов. Более того, вы можете легко преобразовать отдельные базы данных в эластичный пул их простым перемещением в пул.

Таблица 2.2 Модели приобретения отдельной базы данных

Модель DTU	Модель vCore
Хороший выбор для пользователей, которым не нужна высокая степень гибкости в настройке и которые хотят фиксированную цену	Хороший выбор, если вам нужен высокий уровень прозрачности и контроля отдельных ресурсов (таких как память, хранилище и мощность процессора), используемых вашей базой данных
Предварительно настроенные ограничения для транзакций с базой данных и заранее настроенные конфигурации хранилища, процессора и памяти	Гибкость в использовании мощности процессора, памяти и хранилища, которое тарифицируется на основе фактического потребления
Доступны предложения Basic и Standard, а также Premium для баз данных с большим количеством транзакций	Предложения General Purpose (общего назначения) и Business Critical (критически важные для бизнеса) позволяют при необходимости снизить затраты и обеспечивают высокий уровень производительности и доступности
Возможность масштабирования до более высокого уровня при необходимости	Возможность и гибкость масштабирования процессора, памяти и хранилища по мере необходимости
Резервное (backup) и долгосрочное хранения предоставляются за дополнительную плату	Резервное (backup) и долгосрочное хранения предоставляются за дополнительную плату

ПРИМЕЧАНИЕ МОДЕЛИ ЦЕНООБРАЗОВАНИЯ ЭЛАСТИЧНЫХ ПУЛОВ

Информация о модели ценообразования (табл. 2.2) относится и к эластичным пулам. Ваши ресурсы применяются не к отдельной базе данных, а к целому пулу.

**СОВЕТ К ЭКЗАМЕНУ**

Вы легко можете повысить или понизить производительность Azure SQL Database, перейдя на более дорогой тариф или добавив вычислительные ресурсы, память, хранилище. Однако реляционные базы данных вообще не масштабируются горизонтально. Существует несколько вариантов масштабирования копий БД, доступных только для чтения, но, как правило, реляционные базы данных не предлагают возможности предоставления копий данных в нескольких регионах.

Управляемый экземпляр (managed instance) предназначен для клиентов, которым нужен простой путь миграции из локальной среды (или другой, отличной от Azure) в Azure. Управляемые экземпляры полностью совместимы с локальным SQL Server. Поскольку ваш сервер баз данных объединен с изолированной виртуальной сетью и имеет частный IP-адрес, то он может находиться в вашей частной виртуальной сети Azure. Эти функции предназначены для пользователей, желающих перенести локальную базу данных в Azure с минимальными усилиями и хлопотами. Доступны оба уровня обслуживания – General Purpose и Business Critical.

Microsoft разработала службу миграции баз данных Azure (Database Migration Service, DMS), чтобы упростить клиентам преобразование локальных баз данных (или баз данных, размещенных в облаке в другом месте) в управляемый экземпляр Azure. DMS работает с помощью пошагового мастера, позволяющего определить, какие базы данных и таблицы вы хотите перенести из

исходной базы данных в базу данных Azure SQL. Затем он будет использовать виртуальную сеть Azure для миграции данных. После переноса данных DMS настраивает синхронизацию между исходной базой данных и базой данных Azure SQL. Это означает, что до тех пор, пока исходная база данных остается в сети, любые изменения, внесенные в нее, будут синхронизированы с управляемым экземпляром в базе данных Azure SQL.

ДОПОЛНИТЕЛЬНО DMS И ЛОКАЛЬНЫЕ БАЗЫ ДАННЫХ

Для переноса локальной базы данных необходимо иметь подключение между Azure и локальной сетью через VPN или с помощью службы, например ExpressRoute.

База данных Azure для MySQL

Подобно SQL Server, базы данных MySQL являются реляционными. MySQL – это самая популярная в мире система с открытым исходным кодом.

База данных Azure для MySQL – полностью управляемое облачное предложение от MySQL Community Edition. Используя БД Azure для MySQL, вы не беспокоитесь об управлении сервером баз данных, о безопасности или выполнении сложных задач, скажем настройки производительности. Microsoft берет все в свои руки.



СОВЕТ К ЭКЗАМЕНУ

БД Azure для MySQL защищает ваши активные и неактивные данные. Это означает, что вместе с вашими базами данных в безопасности находятся и данные, передаваемые клиентам.

База данных Azure для MySQL предлагает несколько тарифных планов под особые нужды каждого. План с увеличенной производительностью (Burstable) подойдет для минимального использования; план общего назначения (General Purpose) больше подойдет для коммерческих целей; а план, оптимизированный для операций в памяти (Memory Optimized), подходит для тех, кому нужна высокая производительность. С переходом от низшего к высшему ценовому плану вы соответственно получаете больше процессорных ядер и памяти. Каждый тарифный план содержит несколько уровней, поэтому можно все спланировать, как вам нужно.

Поскольку база данных Azure для MySQL основана на MySQL Community Edition, вы можете без труда переместить локальную базу данных MySQL в облако, не беспокоясь о совместимости.

База данных Azure для PostgreSQL

PostgreSQL – это еще одна реляционная система базы данных с открытым исходным кодом. Изначально PostgreSQL создавался для Unix или Linux, а сейчас он доступен и на MacOS, Linux, OpenBSD, FreeBSD, Windows.

PostgreSQL разрабатывался с учетом интересов предприятий. Он позволяет множеству пользователей выполнять сложные операции. База данных Azure для PostgreSQL – это управляемая версия PostgreSQL в Azure. Базы данных Azure для PostgreSQL, как и Azure для MySQL и Azure SQL, позволяют использовать мощные системы баз данных, где вам не нужно управлять сервером, безопасностью базы данных, производительностью и другими задачами администрирования.

Ценообразование БД Azure для PostgreSQL схоже с БД Azure для MySQL. Доступны планы с увеличенной производительностью, общего назначения и оптимизированный для операций в памяти, а цены возрастают по мере добавления дополнительных ресурсов баз данных, типа процессора и памяти.

Azure Marketplace и сценарии его использования

Вы уже узнали о многих продуктах и службах, доступных в Azure, но есть и множество дополнительных сервисов, выходящих за рамки обсуждаемого ранее. Кроме того что Microsoft предлагает множество своих дополнительных служб, сторонние поставщики также предоставляют широкий спектр сервисов, которые можно использовать в Azure. Все эти ресурсы доступны в одном месте – Azure Marketplace.

Чтобы получить доступ к Azure Marketplace, нажмите **Create A Resource** (Создать ресурс) на портале Azure, как показано на рис. 2.31. У вас отобразится список категорий на выбор, а также список популярных предложений по всем категориям. Вы можете нажать на категорию, чтобы посмотреть в ней все шаблоны. Также можно выбрать шаблон из списка популярных, ввести поисковый запрос или нажать **See All** (Посмотреть все) для просмотра всех доступных шаблонов.

Нажав на **See All** (Посмотреть все), вы перейдете к полному списку предложений Marketplace, где можно отсортировать шаблоны по ценам, операционным системам и издателю, как показано на рис. 2.32.



СОВЕТ К ЭКЗАМЕНУ

Продукты Azure Marketplace являются ARM-шаблонами. Они разворачивают одну или несколько служб Azure. Помните, ранее мы обсуждали Azure Resource Manager и говорили, что все ресурсы Azure разворачиваются с использованием шаблонов ARM. Marketplace не исключение.

Некоторые шаблоны в Marketplace разворачивают только один ресурс. Например, если выбрать шаблон Web App, то он создаст веб-приложение, работающее в Службе приложений Azure. Другие шаблоны создают несколько ресурсов, которые объединяются для создания единого решения. Например, можно создать кластер базы данных DataStax Enterprise, а шаблон создаст 1–40 узлов DataStax Enterprise. Предложения Azure Marketplace оплачиваются целиком, поэтому при создании кластера DataStax Enterprise с 40 узлами вы не увидите отдельных счетов на 40 виртуальных машин, сетей и т. д. Вам выставят счет за кластер DataStax Enterprise. Это значительно упрощает понимание процесса формирования счетов.

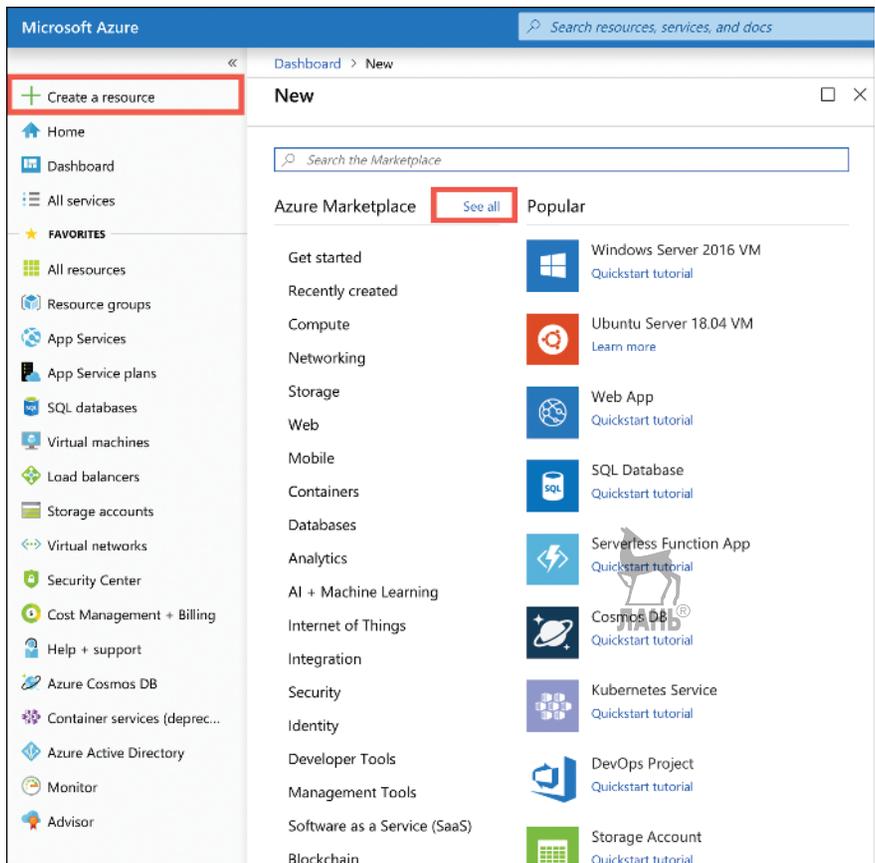


Рис. 2.31 Azure Marketplace

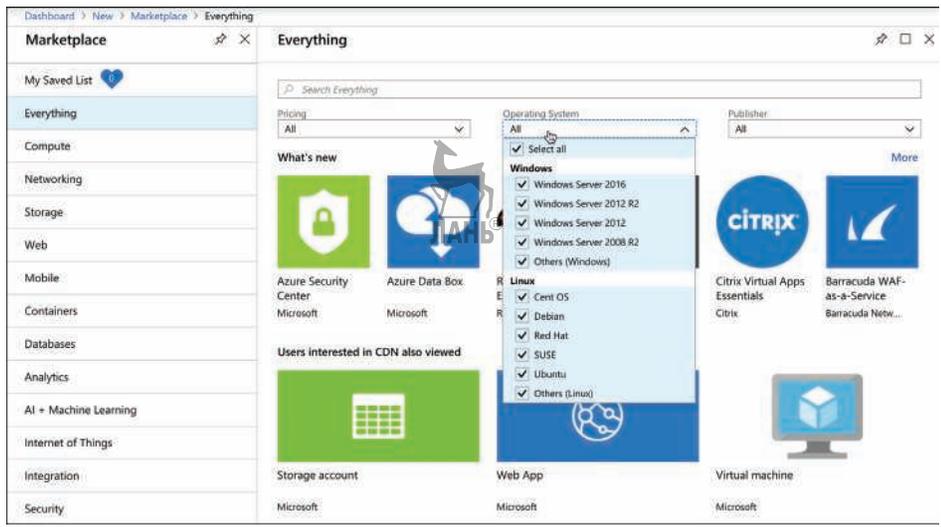


Рис. 2.32 Фильтрация в Azure Marketplace

Как показано на рис. 2.33, многие шаблоны Marketplace содержат ссылки на документацию и другую информацию, способствующую максимально эффективному использованию шаблона. Если вы решите, что сейчас вам не нужны новые ресурсы, вы можете нажать кнопку **Save For Later** (Отложить), и шаблон будет добавлен в список, к которому вы можете вернуться в любое время, выбрав **My Saved List** (Сохраненные шаблоны), как показано в левом верхнем углу на рис. 2.32.

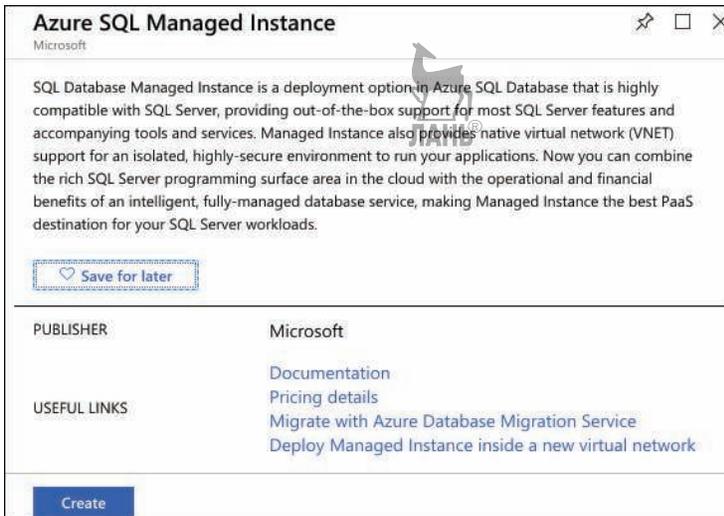


Рис. 2.33 Ссылки на Marketplace и список сохраненных шаблонов

Мысленный эксперимент

Теперь, когда вы познакомились с основными службами Azure, мы применим ваши новые знания. Ответы на мысленный эксперимент находятся в следующем разделе.

Компания ContosoPharm обратилась к вам за помощью в настройке виртуальных машин Azure для размещения корпоративных служб в Azure. Им необходимы гарантированные высокая доступность служб и защита при ЧП, которые могут произойти в центре обработки данных в каком-либо регионе Azure. Кроме того, им нужны гарантии, что отключение питания в каком-либо центре обработки данных не повлияет на их обслуживание в этом регионе.

В планах у ContosoPharm большое количество виртуальных машин, размещенных лишь на трех разных службах в облаке. С каждой из этих служб будут связаны и другие службы Azure в дополнение к ВМ. Компания весьма заинтересована в возможности свободно просматривать на портале Azure ресурсы, связанные с конкретной службой.

Две планируемые службы будут принадлежать отделу маркетинга, а третья – отделу разработки. Компании нужен способ для ведения отчетности по каж-



дому из отделов, поэтому был выбран способ логически объединить данные службы.

Наряду с этим технический директор хотел бы управлять доступами сотрудников к службам в каждом отделе, а также настройкой данных служб.

Виртуальные машины ContosoPharm будут использовать определенные конфигурации для виртуальных сетей. Компании необходимо, чтобы эти ресурсы без труда разворачивались в новых регионах Azure. Для них крайне важно, чтобы у поздних развертываний была та же конфигурация, что и у уже работающих копий сервисов, поскольку любые различия могут привести к несовместимости приложений.

Технический директор также обеспокоен тем, что ВМ могут быть недоступны из-за сбоев оборудования. Он слышал, что у пользователей услуг облачных вычислений могут возникнуть проблемы, когда их провайдер почему-то перезагружает базовый хост-компьютер. Необходимо, чтобы перечисленное не случилось в ContosoPharm, поэтому вас просят дать рекомендации.

В ContosoPharm было замечено, что приложения вызывают экстремально высокую загрузку центрального процессора. Компании нужна система, которая будет это учитывать и, возможно, добавлять ВМ в периоды пиковой нагрузки. Однако для компании также важно вести учет контроля расходов, поэтому им не хотелось бы платить за эти дополнительные ВМ, когда они не используются. Любой предложенный вами совет для решения этой ситуации будет приятным бонусом для компании.

В одном из сервисов ContosoPharm есть веб-портал, написанный на PHP. Его нужно перенести в облако, но возиться с большой конфигурацией у компании нет никакого желания. Компании нужна стабильная доступность портала для пользователей, возможность обновления в нем кода и, учтите, удобное масштабирование портала при его повышенном использовании в разгаре месяца. От вас ждут лучшее Azure-решение.

Другая часть одной из служб должна существовать в виде Docker-образа, который будет запускаться в Azure, но технический директор обеспокоен подобными расходами. Эта часть службы нужна только для определенных операций и будет выполняться всего несколько минут в месяц. Тем не менее это важнейший компонент, поэтому нужно, чтобы он был надежным. Технический директор хочет, чтобы вы предложили наиболее экономичный вариант Azure.

Одна служба также упакована в контейнер, но немного сложнее. Использование этой службы осуществляется повсеместно. Иногда требуется много вычислительных ресурсов, а иногда нет. Важно, чтобы в случае необходимости все работало как часы.

У менеджеров в отделе продаж компании ContosoPharm должен быть надежный доступ к приложениям Office, но руководитель департамента информационных технологий очень обеспокоен тем, что конфиденциальные данные по продажам хранятся на жестких дисках. Он хотел бы, чтобы вы предложили его сотрудникам необходимый для них способ доступа к приложениям, который при этом не нарушит безопасность данных. Возможность доступа к этим приложениям с любого устройства (или даже веб-браузера) станет по-настоящему революционным продуктом.

Большая часть инфраструктуры, которую ContosoPharm перемещает в облако, состоит из многоуровневых приложений, где все уровни взаимодействуют друг с другом, а также могут подключаться к интернет-сети. Локальные сетевые инженеры ContosoPharm прекрасно понимают, как работает и настраивается локальная сеть, но у них нет ни малейшего понятия, как перевести ее в облако. Вам нужно будет поделиться с ними своими рекомендациями для решения данного вопроса.

У ContosoPharm есть еще локальная система, которую нельзя перенести в облако. Она как была локальной, так и останется ею. Эта система использует 3D-анимацию клеточных структур, а также анимацию того, как на них действуют лекарства. Размеры файлов весьма велики, и ContosoPharm опасается, что передача таких объемов данных из облака замедлит работу приложения. Из-за того, что конфиденциальность данных может быть нарушена, они предпочли бы, чтобы по возможности передача файлов не осуществлялась через интернет.

От компании ContosoPharm требуют, чтобы все копии счетов-фактур от клиентов хранились у них по порядку. Эти счета загружаются на веб-сайт в PDF-формате, и необходимо, чтобы они сохранялись в облаке. Отчетность по счетам компании не нужна. Данные копии необходимы на тот случай, если регулирующие государственные органы потребуют их в будущем.

Также им нужна возможность сохранения данных VM даже при событии обслуживания Azure или при перемещении на другую VM. Подобные данные весьма ценные, поэтому компания должна быть уверена, что сделала правильный выбор.

Другая часть приложения должна сохранять данные, к которым можно будет получить доступ из локального сервера, работающего на сервере Windows Server 2016. А устанавливать дополнительные программы на сервер для доступа к файлам в облаке компания не хотела бы.

Все химические вещества и фармацевтические препараты ContosoPharm хранятся в большом исследовательском учреждении. Они хотели бы интегрировать базу данных учреждения со своими службами Azure, и им нужно, чтобы это соединение было зашифровано и защищено. Разработчики существующей системы использовали MySQL Community Edition для разработки базы данных. ContosoPharm заинтересована в простейшем решении для размещения этой БД в облаке с автоматической настройкой и обслуживанием.

Предоставьте ContosoPharm рекомендации, которые бы отвечали всем установленным требованиям. Давать конкретные технические подробности о том, как это реализовать, вам не нужно. Предоставьте компании правильное направление, если у вас нет полностью проработанного предложения.

Ответы на мысленный эксперимент

В этом разделе мы рассмотрим ответы на мысленный эксперимент.

Чтобы обеспечить защиту VM от чрезвычайных происшествий в центре обработки данных в отдельном регионе Azure, вам следует порекомендовать ContosoPharm использование зон доступности. Разворачивание VM в зонах

доступности может гарантировать распределение ВМ по разным физическим зданиям в пределах одного региона Azure. У каждого здания будет своя система подачи электроэнергии, водоснабжения, система охлаждения и сеть.

Для просмотра ресурсов Azure, связанных с определенной службой, ContosoPharm может создавать отдельные группы ресурсов и ресурсы для каждой службы в своей группе ресурсов. Чтобы логически группировать службы подразделений маркетинга и разработки для отчетности, они могут создавать отдельные подписки Azure для каждого подразделения.

Чтобы развеять опасения технического директора по поводу того, у кого есть доступ к службам и как эти службы настроены, вы можете порекомендовать использование групп управления. Поскольку вы уже предложили, чтобы каждое подразделение имело свою собственную подписку, логичнее использовать группы управления, так как каждую подписку можно будет переместить в отдельную группу.

Для текущего и будущего последовательного развертывания ContosoPharm может создать шаблон ARM, с использованием которого обеспечивается идентичная конфигурация всех создаваемых ресурсов.

Для защиты приложения от ситуаций, при которых у ВМ возникает аппаратная проблема, или при ее перезагрузке компании следует использовать набор доступности (availability set). Набор доступности предоставит несколько доменов сбоя (fault domain) и обновлений (update domain). И в случае перезапуска одной ВМ в другом домене обновлений будет находиться другая, рабочая ВМ.

Чтобы у компании всегда было достаточное количество ВМ во время пиковых нагрузок на процессор, ей следует использовать наборы масштабирования (scale set). Это позволит ContosoPharm настраивать правила автоматического горизонтального масштабирования для управления затратами.

Лучшим вариантом для размещения веб-портала PHP в облаке является служба приложений Azure. Поскольку это служба PaaS, ContosoPharm не придется беспокоиться о сложной конфигурации. Также служба приложений предоставляет возможности масштабирования, что отвечает требованию по реагированию на увеличение использования.

Лучшим вариантом для размещения Docker-образа в облаке являются экземпляры контейнеров Azure (Azure Container Instances, ACI). Вообще, у Azure для этого есть и другие решения, но так как технического директора волнуют затраты на это, плюс в месяц этот компонент запускается лишь на некоторое время, то в таком случае ACI – самый экономичный вариант.

Для второго контейнерного компонента лучше всего подойдет служба Azure Kubernetes (Azure Kubernetes Service, AKS). Тот факт, что этот компонент более сложный и иногда требует много вычислительных ресурсов, делает его идеальным вариантом для AKS. Особенно потому, что Kubernetes может обеспечить постоянную работу и доступность контейнера.

Чтобы у менеджеров по продажам был доступ к приложениям MS Office, который не ставит под угрозу безопасность хранения файлов на ноутбуках, порекомендуйте компании виртуальный рабочий стол Windows. Так сотрудники впоследствии смогут подключаться к приложениям с любого устройства или веб-браузера.

Вам следует порекомендовать сетевым инженерам настройку виртуальной сети. Они без труда смогут настроить подсети в данной сети, подобно тем, что у них есть локально, и все привычные сетевые функции будут им доступны.

Системе 3D-анимации ContosoPharm явно не хватает пропускной способности. При такой ситуации ExpressRoute – похоже, хороший вариант, особенно если учитывать, что для компании важно, чтобы передача файлов осуществлялась не через интернет. С помощью ExpressRoute данные передаются по частному соединению. В зависимости от потребностей приложения регулируется и пропускная способность (макс. до 10 Гбит/с).

Чтобы хранить счета в облаке, ContosoPharm может использовать хранилище Azure Blob Storage. Они могут хранить файлы в виде двоичных BLOB-объектов в хранилище Azure, но поскольку им не нужно генерировать отчеты или выполнять сложные запросы к БД, хранилище BLOB-объектов Azure будет дешевле.

Дисковое хранилище позволит компании сохранять данные на VM при их перезагрузках или перемещениях. Возможно, вам еще следует порекомендовать и использование управляемых дисков для простоты и надежности. Для части приложения, которая должна сохранять данные, доступные локальным серверам Windows Server 2016, посоветуйте использование файлов Azure. Для доступа к файлам впоследствии можно будет использовать SMB, а существующие локальные системы смогут работать с файлами без установки дополнительных приложений.

А если компании нужны базы данных, то лучшим выбором на сегодняшний день является БД Azure для MySQL (Azure Database for MySQL). Поскольку это управляемая служба, ContosoPharm не придется беспокоиться о техническом обслуживании или настройке. И так как эта БД основана на версии MySQL Community Edition, то перенос БД прямо в облако упрощается.

ЛАНЬ®

Краткое содержание главы

В этой главе было рассмотрено множество тем! Вы не только изучили основы Azure, связанные с регионами и группами ресурсов, но и узнали о многих ключевых службах, предоставляемых Azure.

Это краткое описание того, что было описано во второй главе.

- Регион Azure – это область в пределах определенной географической границы, и каждый регион, как правило, находится в сотнях миль друг от друга.
- Под «географией» обычно подразумевается отдельная страна, и в каждой такой географии содержится минимум два региона.
- Центр обработки данных – это физическое здание в регионе, и каждый центр обработки данных имеет свои собственные источники питания, системы охлаждения, системы водоснабжения, генераторы и сеть.
- Задержка в отправке данных между двумя регионами не должна превышать 2 мс, поэтому регионы иногда определяются как «границы задержки» (latency boundary).

- Клиенты должны разворачивать ресурсы Azure в нескольких регионах для обеспечения доступности.
- Зоны доступности обеспечивают развертывание ресурсов в отдельных центрах обработки данных в регионе. В каждом регионе существует минимум три зоны доступности.
- Группы ресурсов позволяют логически разделять ресурсы Azure. Также можно использовать теги для упрощения управления.
- Ресурсы Azure создаются в рамках подписки Azure. Можно создавать и дополнительные подписки, если вы хотите упростить группировку ресурсов или отчетность по ним.
- Подписки Azure имеют свои ограничения.
- С помощью групп управления можно назначать политики и управлять доступом к ресурсам Azure
- Добавлять в группу управления можно только подписки или другие группы управления.
- Менеджер ресурсов Azure (Azure Resource Manager, ARM) – это инструменты управления Azure, которые создают ресурсы и управляют ими.
- ARM использует поставщиков ресурсов для создания и управления ресурсами.
- Шаблон ARM позволяет обеспечить согласованность крупных развертываний в Azure.
- Виртуальные машины Azure – это предложение IaaS, позволяющее управлять операционной системой и конфигурацией.
- Наборы доступности защищают ВМ с помощью доменов сбоя и обновлений. Домены сбоя защищают ВМ от сбоя оборудования в стойке. Вы защищаетесь от перезагрузки ВМ доменами обновлений.
- Наборы масштабирования (scale sets) позволяют настраивать правила автоматического горизонтального масштабирования.
- Служба приложений Azure упрощает размещение веб-приложений в облаке, поскольку является службой PaaS, снимающей с пользователя бремя управления.
- Приложения Службы приложений запускаются в рамках плана службы приложений (App Service plan), в котором определяется количество ВМ и их конфигурация.
- Контейнеры позволяют создавать образ приложения и все необходимое для его запуска.
- Экземпляры контейнеров Azure (Azure Container Instances, ACI) позволяют запускать контейнеры за минимальную оплату.
- Служба Azure Kubernetes (AKS) является управляемой службой, упрощающей размещение кластера Kubernetes в облаке.
- Виртуальный рабочий стол Windows предоставляет доступ к приложениям и ОС множеству пользователей практически с любого устройства.
- Виртуальная сеть Azure (VNet) позволяет службам Azure взаимодействовать друг с другом и с интернетом.

- В виртуальной сети можно добавить публичный IP-адрес для входящего подключения через интернет. Это полезно, если веб-сайт работает в виртуальной сети и вы хотите предоставить доступ к нему для внешних пользователей.
- Балансировщик нагрузки Azure (Azure Load Balancer) может распределять трафик из интернета между несколькими VM в виртуальной сети.
- ExpressRoute предоставляет подключение с высокой пропускной способностью до 10 Гбит/с к Azure, подключаясь к роутеру Microsoft Enterprise Edge (MSEE).
- Трафик ExpressRoute не передается через интернет.
- Хранилище BLOB-объектов Azure (Azure Blob Storage) – это хороший вариант для хранения неструктурированных данных, таких как двоичные файлы.
- Если вам нужно переместить большой объем данных в хранилище BLOB-объектов, то можно использовать Azure Data Box. На ваш адрес могут отправить жесткие диски любой емкости. Просто запишите на них свои данные и отправьте посылку обратно в Microsoft, где эти данные будут перенесены в учетную запись хранилища.
- Дисковое хранилище Azure (Azure Disk Storage) – это виртуальное дисковое хранилище для VM Azure. Управляемые диски (managed disks) позволяют снять с вас обязательства по управлению дисками.
- Файлы Azure (Azure Files) позволяют получить дисковое пространство в облаке, которое можно локально подключить на диск.
- Хранилище BLOB-объектов предлагает уровни «горячего», «холодного» и «архивного» хранения данных. Каждый уровень предлагает свои условия по срокам хранения данных, частоты обращения к ним и т. д.
- Azure Cosmos DB – это облачная БД NoSQL для неструктурированных данных.
- База данных Azure SQL (Azure SQL Database) – реляционная система баз данных в облаке, полностью управляемая Microsoft.
- База данных Azure для MySQL основана на версии Community Edition с открытым исходным кодом системы базы данных MySQL. Она является управляемой службой, которая снимает с плеч пользователей бремя управления.
- База данных Azure для PostgreSQL – это управляемая служба для размещения БД PostgreSQL.
- Azure Marketplace – источник шаблонов для создания ресурсов Azure. Некоторые из них предоставляются Microsoft, а некоторые – сторонними компаниями.

ГЛАВА 3

Опишите основные решения и средства управления Azure

В главе 2 вы узнали об основных продуктах Azure. В этой главе мы поговорим о самых современных технологиях, доступных в Azure сегодня. Мы затронем несколько многообещающих технологий: искусственный интеллект (artificial intelligence), интернет вещей (Internet of Things, IoT), большие данные (big data) и бессерверные вычисления (serverless computing).

Если вы действительно хотите научиться использовать Azure, тогда вам нужно знать, как можно управлять ресурсами Azure. Вы уже знакомы с порталом Azure, но это не единственное возможное решение для управления и создания ресурсов в Azure. Существует несколько инструментов для командной строки, которые упрощают создание сценариев взаимодействия с ресурсами Azure. Управлять ресурсами Azure можно даже со смартфона!

После создания и настройки служб Azure важно отслеживать их работу в случае необходимости смены настроек таким образом, чтобы использование облачных ресурсов осуществлялось по максимуму. Однако идти в ногу с лучшими практиками и рекомендуемыми конфигурациями может оказаться не таким простым занятием, особенно когда у вас несколько служб. К счастью, у Azure есть Azure Advisor. Связав Azure Advisor с Azure Monitor, вы можете отслеживать работу всех служб Azure.

Отслеживание работоспособности определенных облачных приложений – это только половина всей истории, когда речь заходит об обеспечении доступности ваших облачных ресурсов. Хотя Microsoft Azure – это высоконадежная облачная платформа, есть вероятность, что что-то может работать с ошибками, и когда это случится, веб-сайт службы работоспособности Azure (Azure Service Health) проинформирует вас о происходящем.

Ниже представлены навыки, которые мы рассмотрим в третьей главе.

Навыки, рассматриваемые в главе:

- описание основных решений, доступных в Azure;
- описание средств управления Azure.

Навык 3.1: описание основных решений, доступных в Azure

Несмотря на то что облачные вычисления являются относительно новой технологией, они становятся важнейшей составляющей многих компьютерных решений. Сфера облачных вычислений стремительно разрастается, и наряду с этим Microsoft Azure также расширяет свои возможности. С момента публикации первого издания книги, уже спустя несколько месяцев, были представлены новые службы Azure, а изменения к уже существующим службам стали намного обширнее. Древнегреческий философ Гераклит сказал: «Единственная постоянная вещь – это переменны». Безусловно, Гераклит не мог предвидеть появление Azure несколько тысяч лет назад, но он так точно описал постоянство Azure!

Количество служб Azure может повергнуть вас в шок, но эта глава поможет в них разобраться.

Содержание раздела:

- центр интернета вещей (Azure IoT Hub);
- IoT Central;
- Azure Sphere;
- Azure Synapse Analytics;
- HDInsight;
- Azure Databricks;
- машинное обучение Azure (Azure Machine Learning);
- Cognitive Services;
- Служба Azure Bot (Azure Bot Service);
- бессерверные вычисления (Serverless computing);
- функции Azure (Azure Functions);
- Logic Apps;
- сетка событий (Event Grid);
- Azure DevOps;
- Azure DevTest Labs.

Центр интернета вещей (Azure IoT Hub)

Многие из нас **не** живут в высокотехнологичных умных домах, поэтому нам сложно понять, насколько большую роль начинает играть IoT. Чтобы лучше понять всю важность этой технологии, мы обратимся к цифрам. Популярный статистический портал Statista сообщает, что на сегодня существует более 25 млрд подключенных устройств интернета вещей (IoT). И ожидается, что их количество возрастет до шокирующей цифры в 75 млрд к 2025 году. На сегодня количество интернет-пользователей составляет примерно 3,2 млрд человек.

А всего на планете проживает около 8 млрд. Эти IoT-устройства превосходят человеческую расу по количеству, а объем информации, которую они собирают и передают, невероятный.

Для того чтобы лучше понять сервисы IoT в Azure, давайте рассмотрим теоретически существующую компанию ContosoPharm. Она представляет собой фармацевтическую компанию с большим многоэтажным зданием, где хранятся разрабатываемые лекарства и чувствительные к внешним условиям компоненты, используемые в исследованиях. Эти предметы должны находиться под строгим климат-контролем. Если температура или влажность выходят за пределы очень узкого диапазона, это приводит к потере бесценных материалов.

Чтобы защитить свои инвестиции, ContosoPharm использует связанные с IoT системы климатического контроля, а также генераторы и осветительные системы. Эти системы постоянно следят за окружением и отправляют оповещения, если что-то идет не так. В здании имеется порядка 5000 IoT-устройств. ContosoPharm обязана соблюдать следующие требования для всех этих устройств:

- прошивки на устройствах IoT должны обновляться легко и поэтапно (по очереди);
- необходимо реализовать возможность изменения настроек устройств, например изменять уровни оповещений, но эти параметры специфичны для физического расположения устройств в здании;
- любое подключение к устройствам должно быть полностью безопасным.

Центр интернета вещей (IoT Hub) может легко решить все эти проблемы. IoT-устройства добавляются в IoT Hub, и вы сами можете управлять ими, отслеживать и отправлять им сообщения, как индивидуально, так и в создаваемые вами группы. В один центр интернета вещей можно добавить до 1 000 000 IoT-устройств.

На рис. 3.1 показано IoT-устройство, добавленное в IoT Hub для ContosoPharm.

Из IoT Hub можно отправлять сообщения на устройства (канал «облако-устройство»/cloud-to-device или «обмен сообщениями C2D»/C2D-messaging) или с устройства в IoT Hub (канал «устройство-облако»/device-to-cloud или «обмен сообщениями D2C»/D2C-messaging). Можно также интеллектуально перенаправлять сообщения в Центр событий (Event Hub), хранилище Azure (Azure Storage) или служебную шину (Service Bus) на основе содержимого сообщения.

При добавлении нового IoT-устройства IoT Hub создает строку подключения, использующую общий ключ доступа (shared access key) для проверки подлинности. Этот ключ предотвращает несанкционированный доступ к вашему центру интернета вещей. После подключения устройства к IoT Hub сообщения между ними шифруются для дополнительной безопасности.

Помимо сообщений, вы также можете использовать IoT Hub для отправки файлов на свои устройства. Это позволяет легко обновлять прошивку на ваших устройствах безопасным способом. Чтобы обновить прошивку на устройстве интернета вещей, просто скопируйте ее на устройство. Устройство обнаружит прошивку, перезагрузит и запишет обновление на устройство.

Одной из важных концепций в центре интернета вещей является концепция так называемого *двойника устройства* (device twin). Каждое IoT-устройство

в центре интернета вещей имеет логический эквивалент, который хранится в IoT Hub в формате JSON. Это JSON-представление устройства называется двойником устройства, и оно обеспечивает работу важных функций.

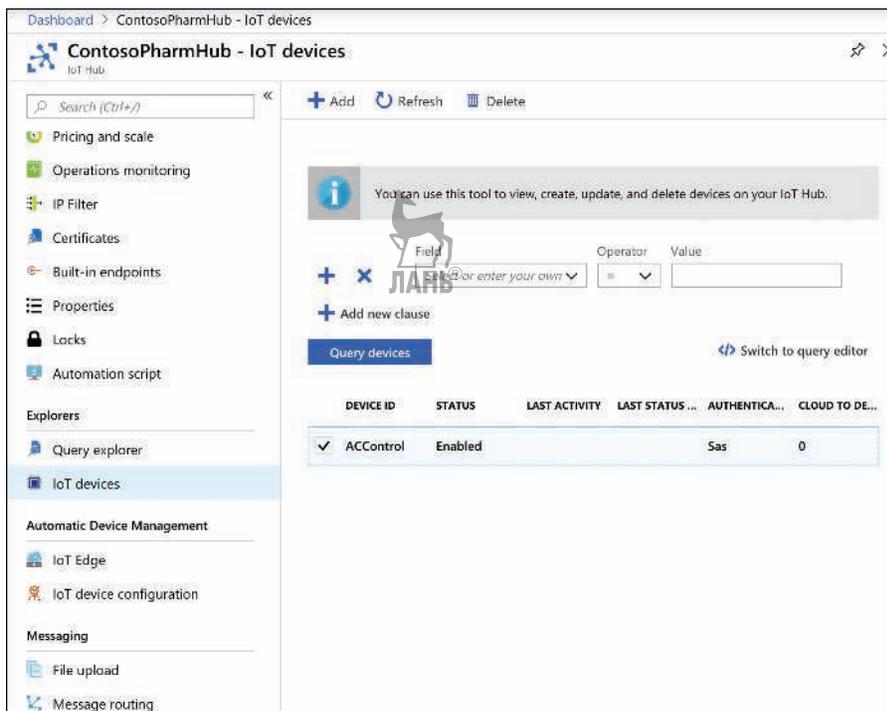


Рис. 3.1 IoT-устройство в центре интернета вещей

Каждый двойник устройства может содержать метаданные, которые добавляют дополнительную категоризацию для устройства. Эти метаданные хранятся в виде тегов в JSON для двойника устройства, и они неизвестны фактически устройству. Только центр интернета вещей может видеть эти метаданные. Одним из требований ContosoPharm было поэтапное обновление прошивки вместо одновременного обновления всех устройств. Это может быть реализовано путем добавления тегов для двойников устройств, образ которых может быть следующим:

```
"tags": {
  "deploymentLocation": {
    "departament": "researchInjectibles",
    "floor": "14"
  }
}
```

Затем они могут отправить файлы прошивки только на устройства, например на 14-м этаже или, скажем, на устройства в отделе *researchInjectibles*. На рис. 3.2 показана конфигурация двойников устройств в IoT Hub с тегами, уста-

новленными на местоположение устройства. Обратите внимание на тег «*building*» со значением «*null*». Это тот самый тег, который ранее был установлен для двойника. Установив его значение в *null*, мы удалим тег.

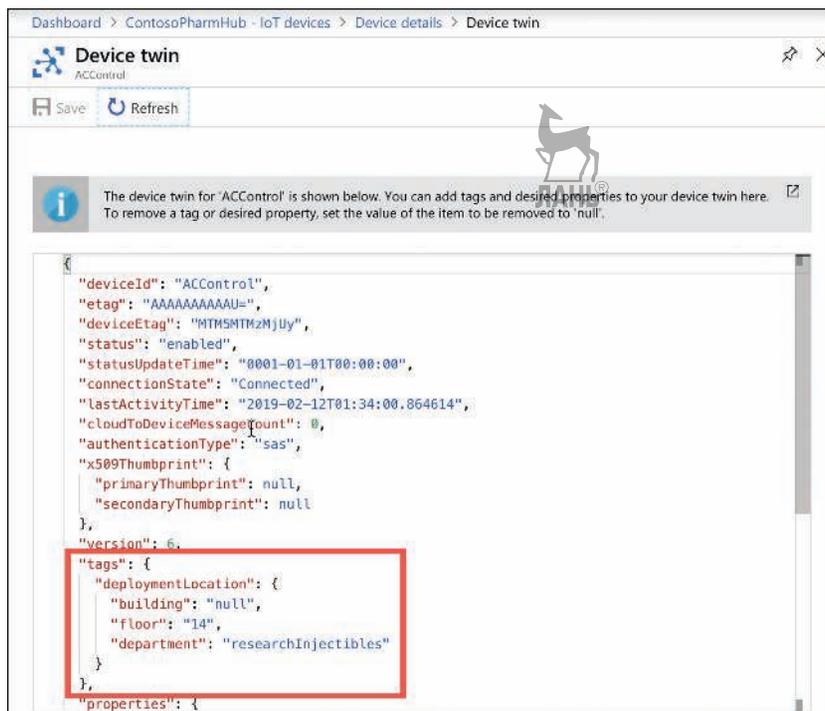


Рис. 3.2 Двойник устройства, показывающего установленные в JSON теги

Двойник также содержит свойства IoT-устройства. Есть две копии каждого объекта. Один из них – «*сообщаемое*» (*reported*) свойство, а другой – «*желаемое*» (*desired*) свойство. Вы можете изменить свойство устройства в IoT Hub, изменив «*желаемое*» свойство на новое значение. При следующем подключении устройства к IoT Hub это свойство будет на нем установлено. До тех пор, пока этого не произойдет, *reported*-свойство будет содержать последнее значение, переданное в центр интернета вещей. Как только свойство обновится, «*сообщаемое*» и «*желаемое*» значения будут равны.

Причина, по которой IoT Hub использует этот метод для установки новых свойств, в том, что у него не всегда есть подключение к устройству. Например, если устройство переведет себя в спящий режим для экономии энергии, IoT Hub не сможет записать на него изменения. Сохраняя «*желаемую*» и «*сообщаемую*» версии каждого свойства, IoT Hub всегда знает, нужно ли записывать свойство на устройство при его следующем подключении к IoT Hub.

Чтобы помочь пользователям, которые хотят добавить большое количество устройств в IoT Hub, Microsoft предлагает службу подготовки устройств (Device Provisioning Service, DPS). DPS использует группы регистрации (*enrollment groups*) для добавления устройств в IoT Hub. Концепция заключается в том, что

как только устройство просыпается (обычно при первом подключении, если это новое устройство), оно должно знать, что ему необходимо подключиться к вашему IoT Hub. Для этого DPS должен однозначно идентифицировать устройство, и он делает это либо с сертификатом, либо с помощью чипа доверяемого модуля платформы (trusted platform module).

Как только служба DPS подтвердит идентификацию устройства, она может использовать сведения о группе регистрации, чтобы определить, в какой IoT Hub устройство должно быть добавлено. Затем он предоставит устройству информацию о подключении для связи с этим IoT Hub. Кроме того, группа регистрации также может предоставить начальную конфигурацию устройства двойника. Это позволяет установить такие свойства, как версия прошивки, которую должно иметь устройство при запуске.

Когда ваши устройства отправляют сообщения в центр интернета вещей, их можно перенаправить в хранилище Azure, центр событий и другие сервисы. Можно выбрать тип сообщений для маршрутизации, а также написать запрос для фильтрации сообщений, которые будут перенаправлены. На рис. 3.3 настроен маршрут, который отправляет сообщения в Azure Blob Storage. Вы можете видеть в запросе, что мы будем маршрутизировать только те сообщения, которые приходят от устройства с двойником, содержащим тег для нашего исследовательского отдела.



Рис. 3.3 Добавление маршрута сообщений в центр интернета вещей

Для центра интернета вещей существует два уровня ценообразования: **Basic** (Базовый) и **Standard** (Стандартный). Каждый уровень предлагает несколько вариантов, которые выбираются в зависимости от количества сообщений в день для каждого подразделения центра интернета вещей. При масштабировании центра интернета вещей добавляются дополнительные модули. Это дает возможность обрабатывать больше сообщений за более высокую стоимость.

В табл. 3.1 показаны варианты и цены для уровня **Basic** (Базовый). В табл. 3.2 показаны варианты и цены для уровня **Standard** (Стандартный).



СОВЕТ К ЭКЗАМЕНУ

Ценообразование в центре интернета вещей (IoT Hub) является прозрачным. Большинство предприятий выбирают тариф **Standard** (Стандартный) из-за дополнительных функциональных возможностей, доступных на этом уровне. Затем они выбирают вариант, удовлетворяющий их минимальным потребностям в количестве сообщений. Когда во время пиковых нагрузок им нужны дополнительные сообщения, они будут масштабироваться до большего количества узлов IoT Hub.

Например, предположим, что потребности ContosoPharm составляют приблизительно 5 000 000 сообщений в день. Они выбирают ценовой уровень S2 и платят 250 долларов в месяц, если работает 1 узел центра интернета вещей. Если количество сообщений увеличится до 8 000 000 (в результате изменения конфигурации или добавления новых IoT-устройств), они, скорее всего, предпочтут масштабироваться до 2 узлов центра интернета вещей. Это даст им 12 000 000 сообщений в день по цене 500 долларов США в месяц.

Таблица 3.1 Ценообразование центра интернета вещей уровня Basic

Тариф	Ежемесячная плата за IoT Hub Unit	Сообщений в день за IoT Hub Unit
B1	\$10 US	400 000
B2	\$50 US	6 000 000
B3	\$500 US	300 000 000

Таблица 3.2 Ценообразование центра интернета вещей Standard

Тариф	Ежемесячная плата за IoT Hub Unit	Сообщений в день за IoT Hub Unit
Free	Бесплатно	8000
S1	\$25 US	400 000
S2	\$250 US	6 000 000
S3	\$2500 US	300 000 000



ПРИМЕЧАНИЕ ИЗМЕНЕНИЕ УРОВНЯ ЦЕНООБРАЗОВАНИЯ

Вы не можете перейти на более низкий ценовой уровень после разворачивания центра интернета вещей. Если вы создаете центр интернета вещей на уровне **Standard** (Стандартный), его нельзя изменить на уровень **Basic** (Базовый). Если вы создаете центр интернета вещей на уровне **Standard** (Стандартный) с использованием вариантов S1, S2 или S3, то перейти на бесплатную версию уже нельзя.

Важно также отметить, что следующие функции доступны только на уровне **Standard**:

- потоки устройств (Device Streams) для потоковой передачи сообщений в режиме «облако–устройство», почти в реальном времени;
- обмен сообщениями с устройствами через облако;
- управление устройствами, двойники устройств или модулей;

- служба IoT Edge для обработки IoT-устройств на границах сети, в которой они находятся.

При использовании Device Provisioning Service (DPS) взимается плата в размере 0,1 доллара США за каждые 1000 операций.

IoT Central

IoT Hub – отличный способ управления и подготовки устройств, который обеспечивает надежные механизмы работы с сообщениями. Вы даже можете использовать Azure Stream Analytics для отправки сообщений в Power BI для мониторинга в режиме, близком к реальному времени, но для этого требуется дополнительная конфигурация. Если вы ищете удобный инструмент мониторинга IoT-устройств без сложного конфигурирования, то IoT Central – хороший выбор.

IoT Central – это предложение SaaS для IoT-устройств. В отличие от IoT Hub, вам не нужно создавать ресурсы Azure для использования IoT Central. Вместо этого перейдите по адресу <https://apps.azureiotcentral.com/> и создайте приложение с помощью веб-браузера, как показано на рис. 3.4.

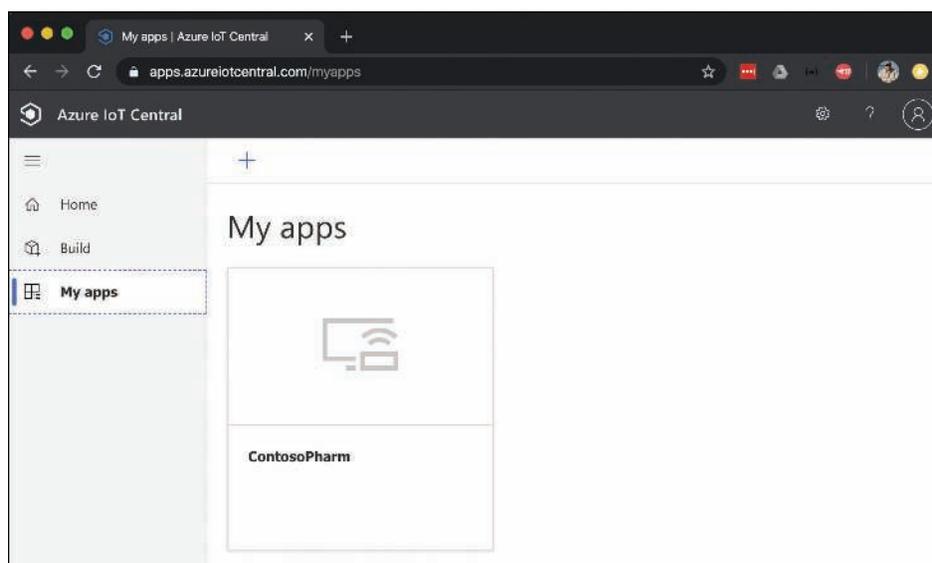


Рис. 3.4 Главная страница Azure IoT Central

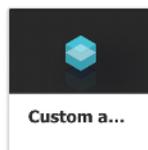
Чтобы создать приложение интернета вещей, нажмите **New Application** (Новое приложение). Откроется экран создания приложения, показанный на рис. 3.5.

Вы также можете выбрать шаблон или создать пустой шаблон. Для удобства шаблоны классифицируются на **Retail** (розничная торговля), **Energy** (энергетика), **Government** (государственные и муниципальные структуры) и **Health-care** (медицина).

Build your IoT application

Test drive with a 7 day trial (limited to one per account), or build your own app that scales and grows with you.

Featured



Custom a...

Retail Energy Government Healthcare



Connected logistics

Track your shipment in real-time across air, water and land with location and condition monitoring.

Create app

[Learn more](#)



Digital distribution center

Improve warehouse output efficiency by digitalizing key assets and actions.

Create app

[Learn more](#)

Рис. 3.5 Создание нового приложения IoT Central

После выбора шаблона прокрутите страницу вниз, чтобы указать имя приложения и URL-адрес. Вы можете использовать имена по умолчанию или указать свои собственные, но рекомендуется использовать свои собственные, чтобы вы могли легко идентифицировать свое приложение. Кроме того, как только ваше приложение было создано, вы получаете доступ к нему напрямую, используя указанный вами URL-адрес, поэтому лучше использовать понятные для вас названия.

Если вы используете **Pay-As-You-Go** (оплата по мере использования), необходимо выбрать службу Azure Active Directory, связанную с подпиской, саму подписку Azure и регион, в котором вы хотите создать приложение. (Лучше всего выбрать регион, географически близкий к вашим IoT-устройствам, если это возможно.) Нажмите кнопку **Create** (Создать), чтобы завершить создание приложения.

На рис. 3.4 видно, что мы уже создали приложение под названием Contoso-Pharm. При нажатии на это приложение в левой части страницы отображается меню, и при нажатии на **Device Explorer** (Обозреватель устройств) отображаются все устройства, добавленные, как показано на рис. 3.7.

Build > **New application**

New application Custom

Answer a few quick questions and we'll get your app up and running.

About your app

Application name * ⓘ

URL * ⓘ

 .azureiotcentral.com

Application template * ⓘ

Pricing plan *

Free

Try for **7 days** with no commitment
5 free devices

Standard 1

For devices sending a **few messages per hour**
2 free devices **5,000** messages/mo

Standard 2 (most popular)

For devices sending **messages every few minutes**
2 free devices **30,000** messages/mo

We've got you cov...

Pricing

No termination fees. Pay only for what you need. [Get pricing details](#)

Security

Protect your connected products with built-in, end-to-end IoT security. Keep control of your data with privacy features like role-based access and integration with your Active Directory permissions.

Рис. 3.6 Указание имени приложения, URL-адреса и сведений о подписке Azure

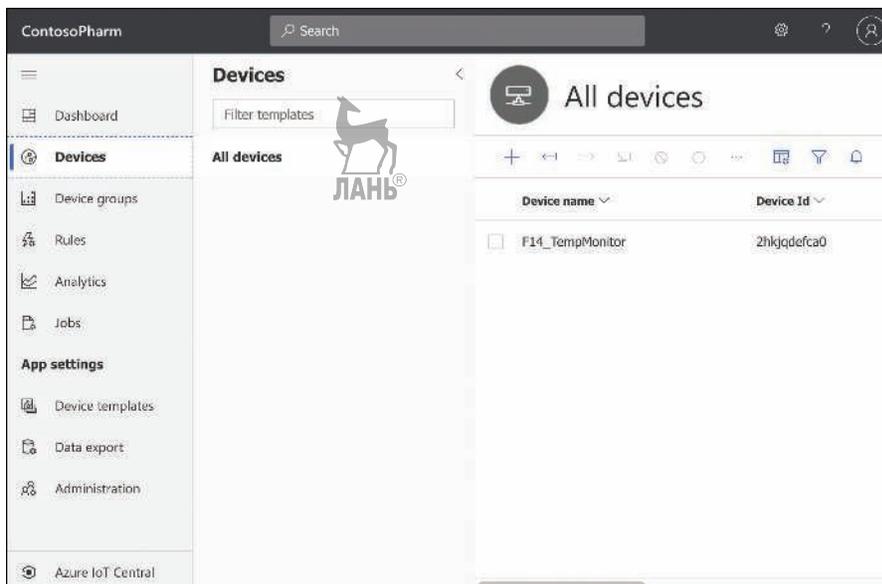


Рис. 3.7 IoT-устройство в IoT Central

Добавьте новое устройство, нажав на знак «плюс», как показано на рис. 3.8. У вас есть возможность добавить реальное устройство, если оно у вас есть, но вы также можете добавить имитируемое (simulated) устройство. Добавление simulated-устройств – хороший способ настроить все в IoT Central так, как вы хотите, а добавить реальные устройства вы сможете позже.

ПРИМЕЧАНИЕ ИМИТАЦИЯ УСТРОЙСТВ – ФУНКЦИЯ, ДОСТУПНАЯ ТОЛЬКО ДЛЯ ИОТ

Возможность создания simulated-устройства характерна только для IoT Central. Центр интернета вещей (IoT Hub) не предлагает эту возможность.

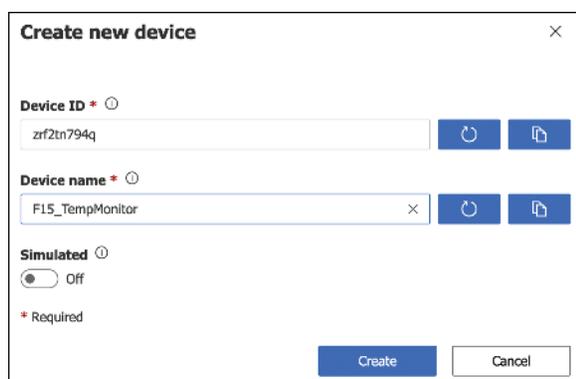


Рис. 3.8 Добавление устройства в IoT Central

Каждая страница в вашем приложении может быть отредактирована непосредственно в браузере. На рис. 3.9 показана домашняя страница приложения IoT Central. Если нажать кнопку **Edit** (Изменить), вы сможете добавить/удалить плитки, отредактировать в них информацию и настроить интерфейс напрямую в веб-браузере.

Причина, по которой мы видим кнопку **Edit**, заключается в том, что этот пользователь установлен в качестве администратора приложения. IoT Central дает вам контроль над тем, кто и что может делать в приложении, используя роли. Существует три встроенные роли, которые можно назначить пользователю:

- **администратор** приложений (Application Administrator). Пользователи с этой ролью имеют полный доступ к приложению, могут редактировать страницы и добавлять новых пользователей;
- **конструктор** приложения (Application Builder). Пользователи с этой ролью могут редактировать страницы, но не могут выполнять административные задачи, такие как добавление пользователей, изменение ролей пользователей, изменение параметров приложения и т. д.;
- **оператор** приложений (Application Operator). Пользователи с этой ролью могут использовать приложение, но они не могут редактировать страницы и не могут выполнять административные задачи.

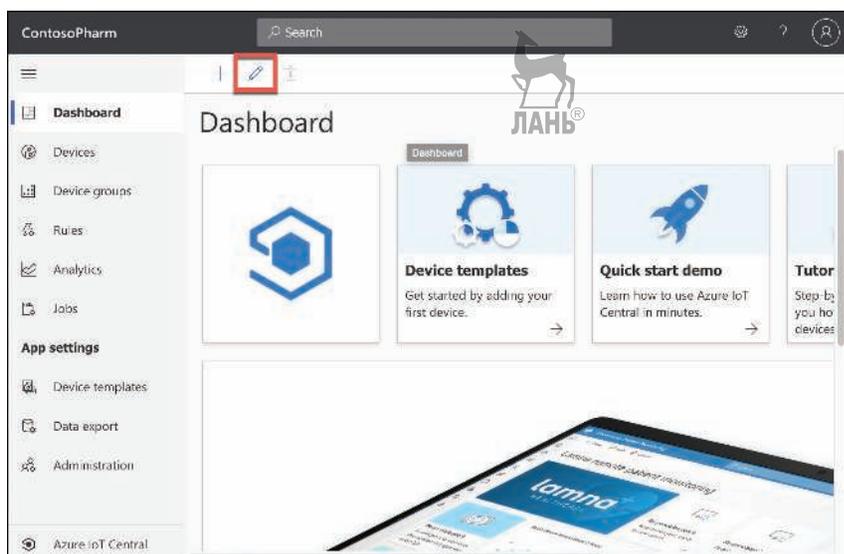


Рис. 3.9 Редактирование страницы в IoT Central

В некоторых ситуациях эти встроенные роли могут не обеспечить необходимую гибкость, поэтому Microsoft работает над тем, чтобы вы могли определять свои собственные роли с настраиваемыми разрешениями.

Для администрирования приложения нажмите **Administration** (Администрирование) в меню слева, как показано на рис. 3.10. Затем можно добавлять и удалять пользователей, настраивать роли пользователей, изменять имя приложения или URL-адрес, добавлять свой образ (custom image) для приложения и т. д. Вы также можете скопировать или удалить приложение с этого экрана.

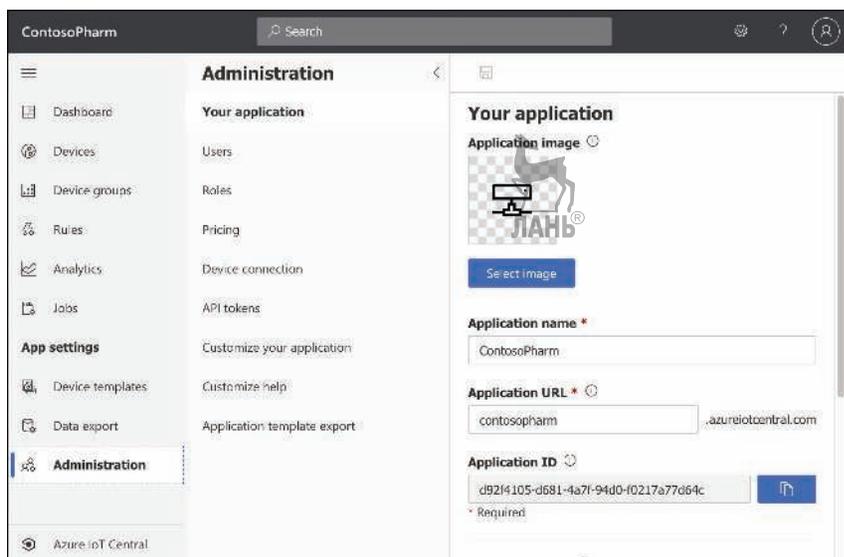


Рис. 3.10 Администрирование приложения в IoT Central

Если вы нажмете на устройство, то можете посмотреть информацию, поступающую от его датчиков. На рис. 3.11 представлены датчики влажности и температуры на устройстве *F14_TempMonitor*.

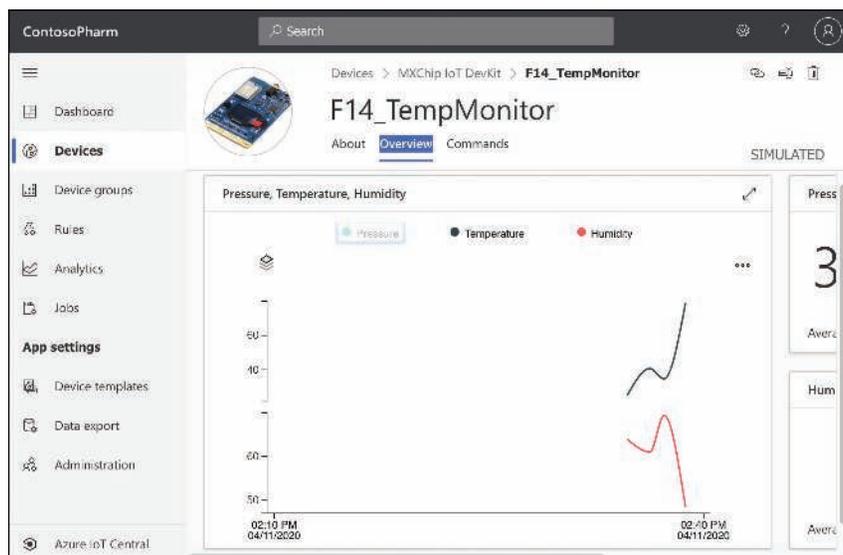


Рис. 3.11 Просмотр данных датчиков с устройства в IoT Central

IoT Central также позволяет легко настраивать правила, которые будут отслеживать ваши устройства и выполнять действия, выбираемые при активации правила. На рис. 3.12 мы настраиваем правило, которое будет активироваться, когда влажность достигнет 60 или выше.

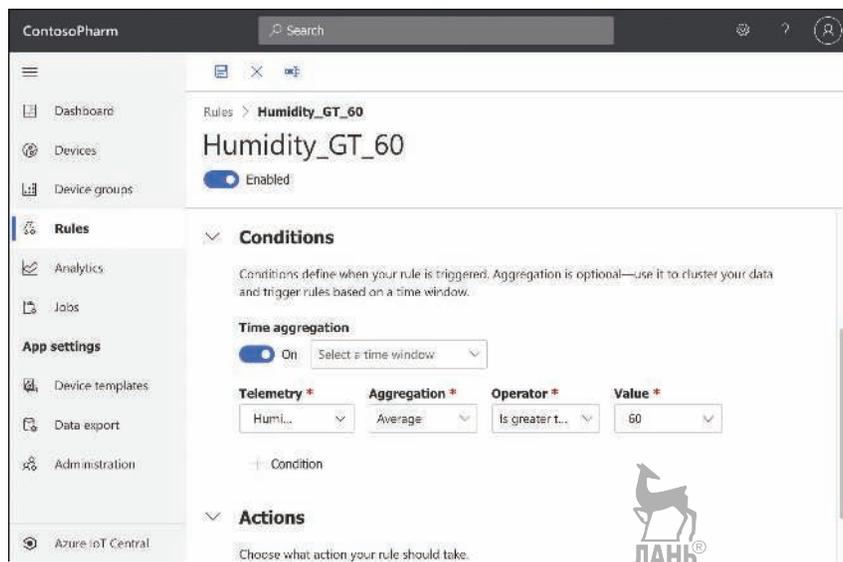


Рис. 3.12 Создание правила

При срабатывании правила IoT Central может отправить электронное письмо с подробностями произошедшего. Можно также вызвать `webhook` (отправить данные на указанный URL), сделать запрос к Azure Function, запустить `workflow` в приложениях Azure Logic и Microsoft Flow. Эти параметры обеспечивают гибкость для выполнения практически любой задачи при срабатывании правила.

Когда у вас большое количество устройств, удобно группировать устройства в наборы (`device set`), чтобы вы могли выполнять действия на многих устройствах одновременно. Чтобы создать `device set`, укажите условие, которое должно быть выполнено для добавления устройства в набор. На рис. 3.13 мы создаем набор для всех устройств, которые содержат подстроку `F14` в названии. Если имя содержит `F14`, устройство автоматически добавляется в набор. Даже при добавлении нового устройства позднее оно станет частью данного набора, если имя содержит `F14`.

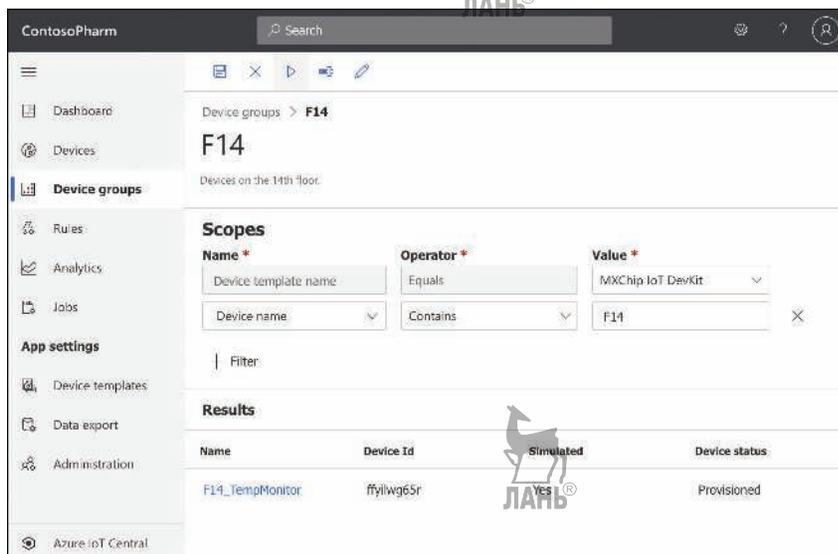


Рис. 3.13 Создание группы устройств

После создания набора вы можете выполнить действия на всех устройствах, находящихся в нем, создав задание (`job`). Нажмите на **Jobs** (Задания) в главном меню приложения, чтобы настроить ваше задание. Задание может изменять свойства, изменять настройки или отправлять команды на устройства. На рис. 3.14 мы создаем задание, которое будет включать ИК-датчик для всех устройств в нашем наборе.

IoT Central также позволяет выполнять аналитику по метрикам со всех устройств в наборе. Например, вы можете смотреть на все устройства, которые зарегистрировали температуру выше определенного уровня. Для более расширенной аналитики данных можно настроить IoT Central на непрерывный экспорт данных с устройств в Azure Blob Storage, Azure Event Hub или Azure Service Bus.

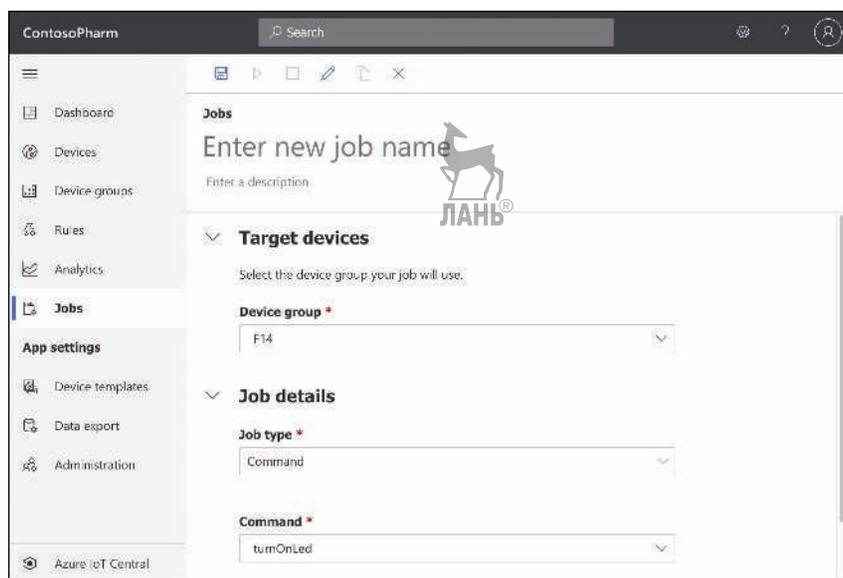


Рис. 3.14 Создание задания

Azure Sphere

Несомненно, устройства с интернет-подключением предлагают вам множество преимуществ. Находясь в магазине и не помня, нужно ли вам молоко или нет, ваш умный холодильник может вам это подсказать. Если вы куда-то отправились и думаете, что оставили духовой шкаф включенным, вашу умную духовку можно будет выключить с телефона. Вы поняли принцип. В общем, возможность подключения – это хорошая вещь, но также в этом есть и недостатки, как минимум в безопасности. Последнее, что вам нужно, – так это взломщики, получающие контроль над замками дверей вашего дома через интернет.

IoT-устройства подобны другим вычислительным устройствам в том, что они работают на программном обеспечении, которое разработано для особых целей. Любое устройство, которое работает на ПО, неустойчиво к багам в ПО, и IoT-устройства не исключение. Однако в ПО IoT-устройства встроен чип, создавая уникальные проблемы при исправлении багов и обновления ПО. Когда вы добавляете факт, что в IoT-устройстве нет ни малейшей стандартизации, в конечном итоге вы столкнетесь с кошмаром, который выражен в безопасности.

Обратившись к аспекту безопасности, Microsoft разработала Azure Sphere. Azure Sphere основывается на десятилетнем опыте Microsoft и тщательном исследовании, которое Microsoft проводила на защищенных устройствах.

ДОПОЛНИТЕЛЬНО 7 СВОЙСТВ НАИБОЛЕЕ ЗАЩИЩЕННЫХ УСТРОЙСТВ

Microsoft написала статью на тему «7 свойств наиболее защищенных устройств», которая раскрывает исследование по защищенным устройствам. Со статьей вы можете ознакомиться по ссылке <https://aka.ms/7properties>.

Azure Sphere – это в действительности целая экосистема и начинается с чипа или микропроцессорного устройства (MCU). Microsoft разработала Azure Sphere MCU, которая содержит компоненты безопасности, встроенные в чип. Третьи лица могут использовать MCU для запуска кода, особенно под их нужды, и этот код работает на ОС Azure Sphere, которая является кастомизированной версией Linux под Azure Sphere.

В Azure служба безопасности Azure Sphere обеспечивает безопасность микроконтроллеров (microcontroller unit, MCU), предоставляет возможность обновлять встроенную ОС Azure Sphere и приложения, работающие на микроконтроллерах, и позволяет формировать отчеты о сбоях и другой аналитике. Одним из значимых преимуществ экосистемы Azure Sphere является возможность исправлять ошибки во встроенных чипах, которые могут послужить причиной проблем с безопасностью.

Эта экосистема обеспечивает безопасную среду для запуска встроенного кода, но также и безопасную связь между устройствами. Вполне вероятно, что ваш умный холодильник может взаимодействовать с другими умными устройствами в доме, и, обеспечивая надежную аутентификацию между этими устройствами, Azure Sphere может помочь обеспечить безопасную среду для всех ваших умных устройств.

На момент написания книги был доступен только один сертифицированный микроконтроллер Azure Sphere, но Microsoft ожидает, что производители умных устройств продолжат использование Azure Sphere для своих микроконтроллеров. Чтобы упростить процесс, наборы разработки Azure Sphere доступны по низкой цене. Комплект для разработки включает оборудование, готовое для Azure Sphere, и комплект разработчика ПО Azure Sphere (software developer's kit , SDK) для Microsoft Visual Studio.

ДОПОЛНИТЕЛЬНО AZURE SPHERE DEVELOPER KITS

С комплектом разработчика Azure Sphere можно ознакомиться по ссылке: <https://aka.ms/AzureSphereDevKitsAll>.

Чтобы воспользоваться преимуществами Azure Sphere, вы приобретаете ее у дистрибьютера Microsoft. Дистрибьютер продает пакет, который включает сертифицированный для Azure Sphere контроллер и лицензию на ОС Azure Sphere. Текущая цена MediaTek MT3620 AN (в настоящее время единственный сертифицированный Azure Sphere MCU) составляет менее 8,65 доллара. Цены варьируются в зависимости от того, сколько микроконтроллеров вы покупаете, но цена не превышает 8,65 доллара за одну штуку.



СОВЕТ К ЭКЗАМЕНУ

В цену Azure Sphere входят обновления ОС и службы безопасности вплоть до июля 2031 года.

Azure Synapse Analytics

Предприятия собирают огромные объемы данных из различных источников. Как вы уже узнали, Microsoft предлагает SLA для служб Azure, в рамках которого уровень доступности составляет 99,9%+. Microsoft не просто заявляет эту цифру, а затем скрещивает пальцы, чтобы ничего не поломалось. Она хранит огромные объемы данных о том, как работает инфраструктура Azure, и использует эти данные для прогнозирования проблем и реагирования на них до того, как они повлияют на клиентов.

ДОПОЛНИТЕЛЬНО ИСПОЛЬЗОВАНИЕ ДАННЫХ

Огромное количество данных, которые аккумулирует предприятие, часто используется для машинного обучения, о котором вы узнаете далее.

Из-за огромных масштабов инфраструктуры Azure вам сложно представить, сколько данных собирается для каждой отдельной системы. Для выполнения заявленных SLA специалисты Microsoft должны иметь возможность надежно анализировать эти данные в режиме реального времени. Как именно они это делают? Вы не можете просто скопировать этот объем данных на виртуальную машину или пул виртуальных машин.

Проблема использования огромных объемов данных, которые мы собираем, является общей для всех предприятий, и это то, что мы имеем в виду под *большими данными*. Большие данные (Big Data) означают, что у вас имеется больше данных, чем вы можете проанализировать с помощью обычных средств за необходимый временной отрезок. Для анализа больших данных требуется мощная система хранения данных, возможность запрашивать данные несколькими способами, огромные возможности для выполнения больших запросов, гарантия безопасности данных и многое другое. Это именно то, что предоставляет служба аналитики Azure Synapse.

ПРИМЕЧАНИЕ AZURE SYNAPSE

Azure Synapse является следующим шагом в развитии другой службы Azure – SQL Data Warehouse. Это правда, что Azure Synapse является заменой для SQL Data Warehouse, но здесь важно отметить, что Azure Synapse предоставляет намного больше функциональностей.

SQL Data Warehouse нацелен в основном на хранение больших объемов данных на так называемых «складах» (warehouse), однако у Azure Synapse есть подобная функциональность в дополнении к мощным функциям аналитики.

Azure Synapse работает на кластере Azure Synapse (cluster). Кластер – это набор четырех компонентов:

- Synapse SQL;
- интеграция Apache Spark;
- интеграция данных Spark и хранилище Azure Data Lake Storage;
- пользовательский веб-интерфейс Azure Synapse Studio.



СОВЕТ К ЭКЗАМЕНУ

На момент написания данной книги Azure Synapse только начинают рассматривать, а также он часто меняется. Большая часть информации, которую вам нужно знать для экзамена AZ-900, высокоуровневая, но все еще есть вероятность, что Azure Synapse поменяется после выхода данного издания. Перепроверьте информацию по Azure Synapse на сайте, доступном по ссылке: <https://azure.microsoft.com/en-us/services/synapse-analytics/>.

Synapse SQL – это часть хранилища данных Azure Synapse. Используя Synapse SQL, вы можете выполнять запросы к своим большим данным. Эти запросы выполняются на вычислительных узлах, и несколько вычислительных узлов осуществляются одновременно, что позволяет параллельно выполнять несколько запросов. Каждый вычислительный узел также запускает компонент, называемый Службой перемещения данных (Data Movement Service, DMS), которая перемещает данные между вычислительными узлами.

Очереди выполняются на вычислительных узлах, чтобы отделить работу с запросами от хранения данных. Это позволяет легко масштабировать количество вычислительных узлов, когда вашим запросам требуется больше мощности. Это дает вам возможность приостанавливать использование вычислительной мощности, чтобы платить за хранилище только тогда, когда вам не нужно выполнять запросы.

Многие клиенты больших данных используют сторонний механизм обработки больших данных, называемый Apache Spark. Azure Synapse тесно взаимодействует с двигателем Spark. Функции Spark автоматически встроены в Azure Synapse при создании кластера.

Azure Synapse интегрирует функциональность Apache Spark с хранилищем Azure Data Lake Storage. Хранилище Azure Data Lake предназначено для хранения больших объемов данных, которые вам нужно проанализировать, однако это хранилище предназначено для широких массивов данных, а не для реляционных. В озере данных (от data lake) данные хранятся в *контейнерах*. При этом каждый контейнер обычно содержит связанные данные.

ПРИМЕЧАНИЕ НЕ ТОЛЬКО AZURE

Понятия «озеро данных» (data lake) и «склад данных» (data warehouse) относятся не только к Azure. Это общие термины. Озеро данных относится к хранилищу неупорядоченных данных, а склад данных относится к хранилищу упорядоченных данных.

Azure Synapse упрощает анализ данных и управление ими с помощью веб-портала под названием Azure Synapse Studio. После создания рабочей области Azure Synapse вы просто нажимаете кнопку для запуска Synapse Studio, и оттуда вы можете легко управлять и анализировать свои данные.

HDInsight

HDInsight позволяет легко создавать кластеры компьютеров и управлять ими с помощью единого фреймворка, предназначенного для выполнения распре-

деленной обработки больших данных. HDInsight, по сути, является управляемой службой Microsoft, которая обеспечивает облачную реализацию популярной платформы аналитики данных Hadoop, но также поддерживает и многие другие типы кластеров, как показано в табл. 3.3.

Таблица 3.3 Поддерживаемые типы кластеров HDInsight

Тип кластера	Описание
Hadoop	Крупномасштабная обработка данных, которая может включать дополнительные компоненты Hadoop, такие как Hive (для SQL-подобных запросов), Pig (для использования скриптовых языков) и Oozie (система планирования рабочего процесса)
HBase	Чрезвычайно быстрая и масштабируемая база данных NoSQL
Storm	Быстрая и надежная обработка неограниченных потоков данных в реальном времени
Spark	Чрезвычайно быстрая аналитика с использованием кеша в памяти при одновременном выполнении нескольких операций
Interactive Query (интерактивные запросы)	Аналитика данных, размещенных в оперативной памяти с помощью Hive и LLAP (процессы, выполняющие фрагменты запросов Hive)
R Server	Аналитика корпоративного уровня с использованием языка R, который предназначен для анализа больших данных
Kafka	Чрезвычайно быстрая обработка огромного количества синхронных потоков данных, часто с IoT-устройств

Создание собственного кластера занимает много времени и является непростой задачей, если ранее у вас не было подобного опыта. С помощью HDInsight Microsoft выполняет всю тяжелую работу на собственной инфраструктуре. Вы получаете преимущества от безопасной среды, которая легко масштабируется для выполнения обработки данных.

Кластер HDInsight выполняет аналитику, разбивая большие блоки данных на сегменты, которые затем передаются узлам кластера. Узлы затем выполняют аналитику данных и сводят их до набора результатов. Вся эта работа происходит параллельно, так что операции выполняются значительно быстрее, чем на одной виртуальной машине. Добавляя дополнительные узлы в кластер, вы можете увеличить мощность и обрабатывать данные еще быстрее.

При создании кластера HDInsight укажите тип кластера, который требуется создать, и присвойте ему имя, как показано на рис. 3.15. Вы также укажете имя пользователя и пароль для доступа к кластеру и пользователя SSH для безопасного удаленного доступа.

После нажатия кнопки **Next** (Далее) необходимо настроить учетную запись хранилища и доступ к Data Lake Storage при необходимости. Обратите внимание, что на рис. 3.16 вы видите только Data Lake Storage Gen1. Чтобы использовать Data Lake Storage Gen2, сначала нужно создать учетную запись хранилища и выполнить дополнительную конфигурацию, описание которой вы найдете на сайте <https://docs.microsoft.com/en-us/azure/hdinsight/hdinsight-hadoop-use-data-lake-storage-gen2>.

Create HDInsight cluster

Resource group * (New) AZ900 [Create new](#)

Cluster details
Name your cluster, pick a region, and choose a cluster type and version. [Learn more](#)

Cluster name * jwc ✓

Region * (US) East US ✓

Cluster type * **Hadoop** [Change](#)

Version * Hadoop 2.7.3 (HDI 3.6) ✓

Cluster credentials
Enter new credentials that will be used to administer or access the cluster.

Cluster login username * ⓘ admin

Cluster login password * 🔒

Confirm cluster login password * 🔒

Secure Shell (SSH) username * ⓘ sshuser

Use cluster login password for SSH

[Review + create](#) « Previous Next: Storage »

Рис. 3.15 Создание кластера HDInsight Hadoop

Microsoft Azure Search resources, services, and docs (G+)

Home > New > Azure HDInsight > Create HDInsight cluster

Create HDInsight cluster

Selection method * ⓘ Select from list Use access key

Primary storage account * (New) jwchdistorage [Create new](#)

Container * ⓘ jwc-2020-04-12t14-21-49-349z ✓

Data Lake Storage Gen1
Provide details for the cluster to access Data Lake Storage Gen1. The cluster will be able to access any Data Lake Storage Gen1 accounts that the chosen service principal has access to.

Data Lake Storage Gen1 access [Configure access settings](#)

Additional Azure Storage
Link additional Azure Storage accounts to the cluster.

[Add Azure Storage](#)

[Review + create](#) « Previous Next: Security + networking »

Рис. 3.16 Настройка учетной записи хранилища для кластера HDInsight

После того как вы запустите создание кластера Hadoop, это может занять до 20 минут, в зависимости от конфигурации. После того как кластер будет готов, вы можете начать анализ данных, написав запросы к нему. Даже если ваши запросы анализируют миллионы строк, HD Insight может справиться с этим, и если вам нужно больше вычислительной мощности, вы можете добавить дополнительные узлы.

Кластеры HD Insight оплачиваются на почасовой основе, но стоимость также зависит и от мощности машин в вашем кластере. Подробные сведения о ценах см. по ссылке <https://azure.microsoft.com/pricing/details/hdinsight/>.

Azure Databricks

Данные, хранящиеся в этих службах, как правило, являются неструктурированными, и их трудно использовать для построения модели машинного обучения. Для нашей ML-модели нам также могут понадобиться данные, поступающие из нескольких источников, некоторые из которых могут находиться вне Azure. Azure Databricks – идеальное решение для накопления данных и формирования данных (так называемое моделирование данных, data modeling), чтобы они были оптимальными для моделей машинного обучения.

ДОПОЛНИТЕЛЬНО МОДЕЛЬ МАШИННОГО ОБУЧЕНИЯ

О модели машинного обучения вы узнаете в следующем разделе данной главы.

На рис. 3.17 показан новый экземпляр Azure Databricks. Все ваши взаимодействия с Databricks осуществляются через рабочую область (workspace), специальный веб-портал, для доступа к которому необходимо нажать на кнопку **Launch Workspace**, как показано на рис. 3.17.

ДОПОЛНИТЕЛЬНО DATABRICKS

Databricks – это на самом деле название компании, которая изначально разрабатывала Apache Spark. Сейчас она управляет платформой анализа данных под названием Databricks. Возможно, вы подумаете, что Azure Databricks является платформой Databricks, работающей в качестве службы в Azure, но за этим стоит гораздо большее. Фактически Microsoft изначально создали Databricks Runtime для работы в Azure. Azure Databricks предоставляет множество других уникальных функций вне платформы Databricks, разработанной компанией Databricks.

При нажатии на кнопку **Launch Workspace** вы переходите в рабочую область Databricks. Для входа в рабочую область Databricks будет использоваться ваша учетная запись Azure. Мой экземпляр Databricks пока пуст. В левой части страницы (рис. 3.18) расположены ссылки для доступа ко всем сущностям Databricks, таким как рабочие области, таблицы и задания. Существует еще раздел **Common Tasks** (Общие задачи), который позволяет вам получить доступ к этим сущностям, а также создавать новые записные книжки, о которых мы еще поговорим в ближайшее время.

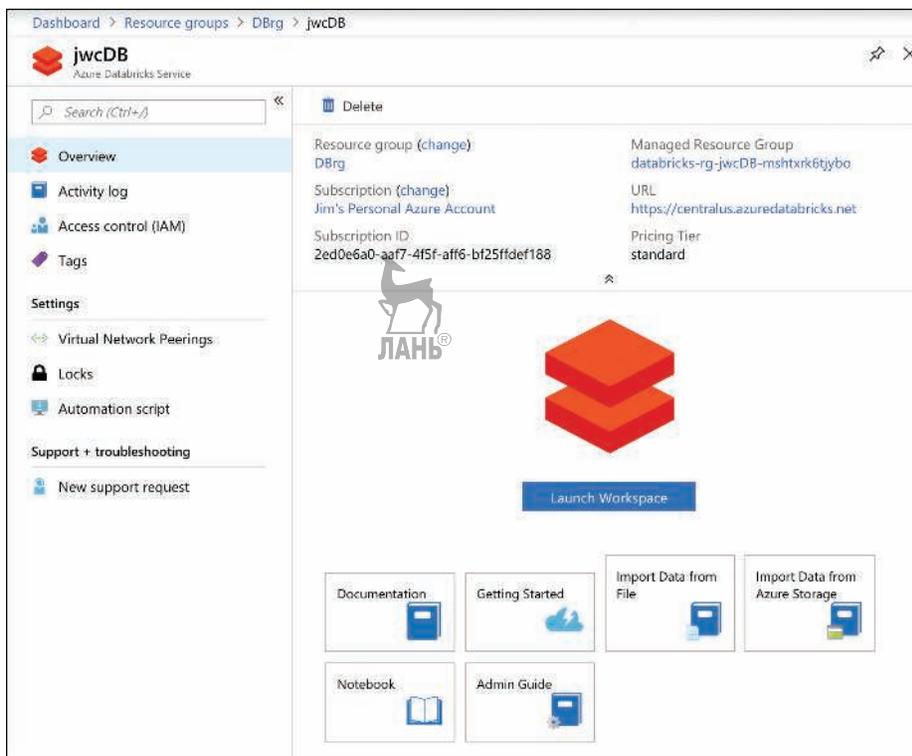


Рис. 3.17 Экземпляр Azure Databricks на портале Azure

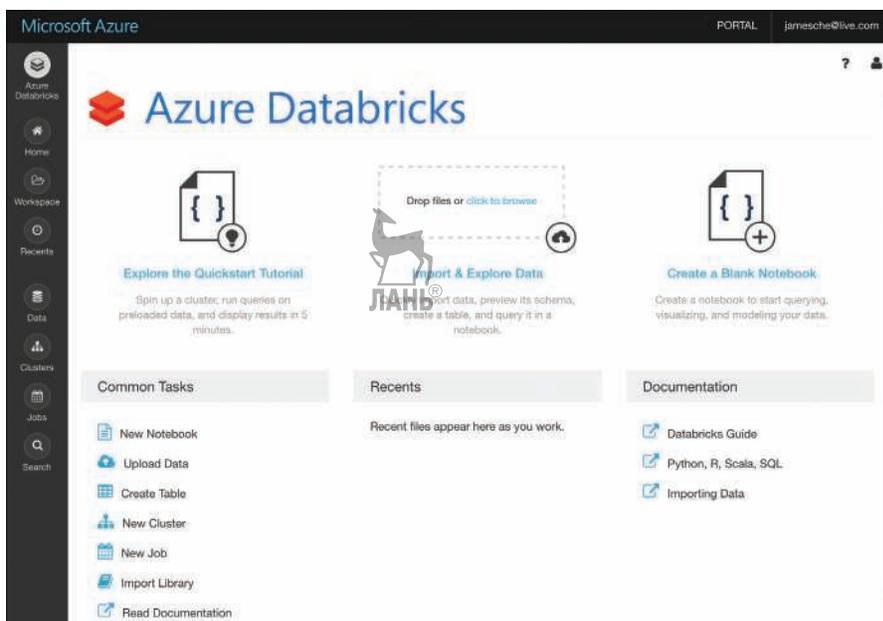


Рис. 3.18 Рабочее пространство Azure Databricks

Давайте теперь создадим кластер. Databricks выполняет всю работу с помощью кластеров, которые являются вычислительными ресурсами. Чтобы создать кластер, вы можете нажать на **New Cluster** (Новый кластер) в разделе **Common Tasks** (Общие задачи). После этого вы увидите экран создания кластера, показанный на рис. 3.19, где новый кластер был назван *jcCluster*, а все остальные параметры оставлены по умолчанию.

Create Cluster

New Cluster 2-8 Workers: 28.0-112.0 GB Memory, 8-32 Cores, 1.5-6 DBU
1 Driver: 14.0 GB Memory, 4 Cores, 0.75 DBU

Cluster Name UI | JSON

Cluster Mode

Pool

Databricks Runtime Version [Learn more](#)

Now This Runtime version supports only Python 3.

Autopilot Options

Enable autoscaling

Terminate after minutes of inactivity

Worker Type 14.0 GB Memory, 4 Cores, 0.75 DBU | Min Workers Max Workers

Driver Type 14.0 GB Memory, 4 Cores, 0.75 DBU |

► Advanced Options

Рис. 3.19 Создание кластера Databricks

Далее мы создадим записную книжку (notebook). Записные книжки являются мощным способом представления и взаимодействия с данными, которые связаны между собой. Каждая записная книжка содержит не только данные, но и графическое представление, а также описание, чтобы помочь нам лучше понять эти данные. Как только ваши данные окажутся в записной книжке, вы сможете запускать команды ML-фреймворков, чтобы построить свою ML-модель.

Нажатие кнопки **Azure Databricks** в меню слева (показано на рис. 3.18) позволяет вам затем нажать на **New Notebook** (Новая записная книжка) для создания новой книжки. На рис. 3.20 мы создаем новую записную книжку, использующую SQL в качестве основного языка. Databricks будет исходить из того, что код, написанный в этой записной книжке, будет на языке SQL, если специально не указан другой язык. Можно также указать языки Python, Scala или R.

ДОПОЛНИТЕЛЬНО ЯЗЫКИ ПРОГРАММИРОВАНИЯ

Python, Scala, и R – это все языки программирования, которые обычно используются для программирования моделей машинного обучения.

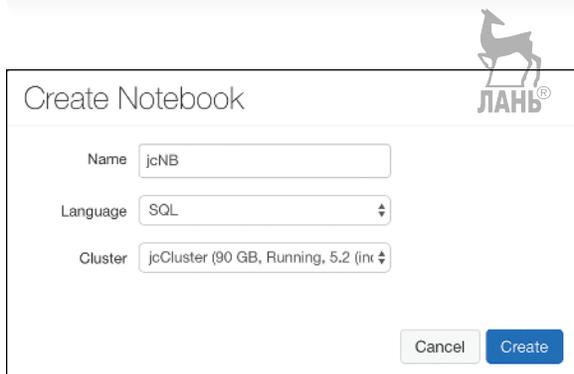


Рис. 3.20 Создание записной книжки

После создания новой записной книжки вы увидите новую запись с одной ячейкой. Внутри этой ячейки вы можете ввести любые данные, которые вы хотите. Например, может потребоваться документация, описывающая содержание этого блокнота. Такой текст в записной книжке вводится с помощью разметки Markdown, языка, который хорошо подходит для написания документации. На рис. 3.21 показана новая записная книжка с разметкой Markdown, которая описывает данные. Обратите внимание, что описание начинается с «%md». Это говорит Databricks, что следующий текст написан в разметке Markdown, а не на языке SQL.



Рис. 3.21 Документирование записной книжки с использованием разметки Markdown

Если кликнуть за границами этой ячейки, то код разметки Markdown будет отображаться в формате HTML. Чтобы добавить данные в эту записную книжку, необходимо создать новую ячейку, нажав **B** на клавиатуре или наведя курсор на существующую ячейку и нажав **+**.

ПРИМЕЧАНИЕ СОЧЕТАНИЕ КЛАВИШ

Сочетания клавиш являются самым быстрым способом работы в Databricks. Полный список сочетаний клавиш можно найти по ссылке **Shortcuts** (Сочетания клавиш), показанной на рис. 3.21.

После нажатия кнопки **В** на клавиатуре в конец записной книжки добавляется новая ячейка. Вы можете ввести код SQL в эту ячейку, чтобы заполнить таблицу данными, как показано на рис. 3.22. (Этот код был взят из учебника Databricks по адресу <https://docs.azuredatabricks.net/getting-started/index.html>.) После ввода кода вы можете запустить его, нажав кнопку **Run** (Выполнить).

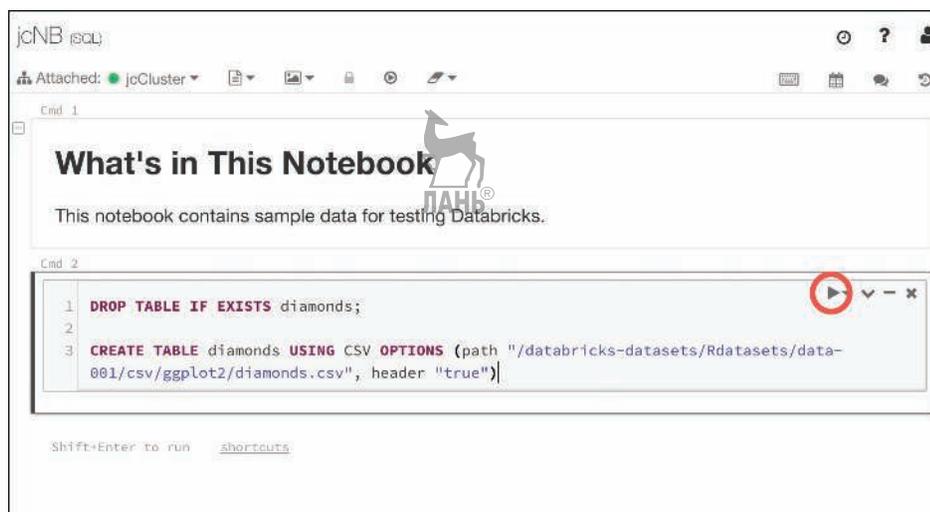


Рис. 3.22 Добавление кода и выполнение команды

ДОПОЛНИТЕЛЬНО ОТКУДА БЕРУТСЯ ДАННЫЕ

Обратите внимание, что путь, введенный для данных, начинается с /databricks-datasets. При создании кластера вы получаете доступ к коллекции наборов данных, называемых Azure Databricks Datasets. В эти наборы данных включены примеры данных в формате значений, разделенных запятыми, и введенный путь указывает на эти данные. Когда эта команда запускается, она извлекает данные в записную книжку.

Можно выполнить запрос к данным с помощью команды на языке SQL в новой ячейке, как это показано на рис. 3.22. На рис. 3.23 показаны результаты запроса к данным.

Для выполнения команд Databricks создает задание, которое выполняется на вычислительных ресурсах, выделенных кластеру. Databricks использует бессерверную (serverless) модель вычислений. Это означает, что когда вы не выполняете никаких заданий, у вас нет виртуальных машин или вычислительных ресурсов. При выполнении заданий Azure временно выделяет виртуальные машины в кластер для обработки. После завершения задания эти ресурсы освобождаются.

Данный пример довольно прост, но как все это относится к машинному обучению? Azure Databricks включает среду для машинного обучения Databricks Runtime for Machine Learning (Databricks Runtime ML), позволяющую использовать данные в Databricks для обучения ML-моделей. Databricks Run-

time ML включает в себя несколько популярных библиотек для машинного обучения, в том числе Keras, PyTorch, TensorFlow и XGBoost. Это также позволяет использовать фреймворк Horovod для распределенных алгоритмов глубокого обучения. Вы можете использовать эти компоненты и без Databricks Runtime ML. Эти фреймворки являются проектами с открытыми исходными кодами, но Databricks Runtime ML избавляет вас от работ по их установке и настройке.

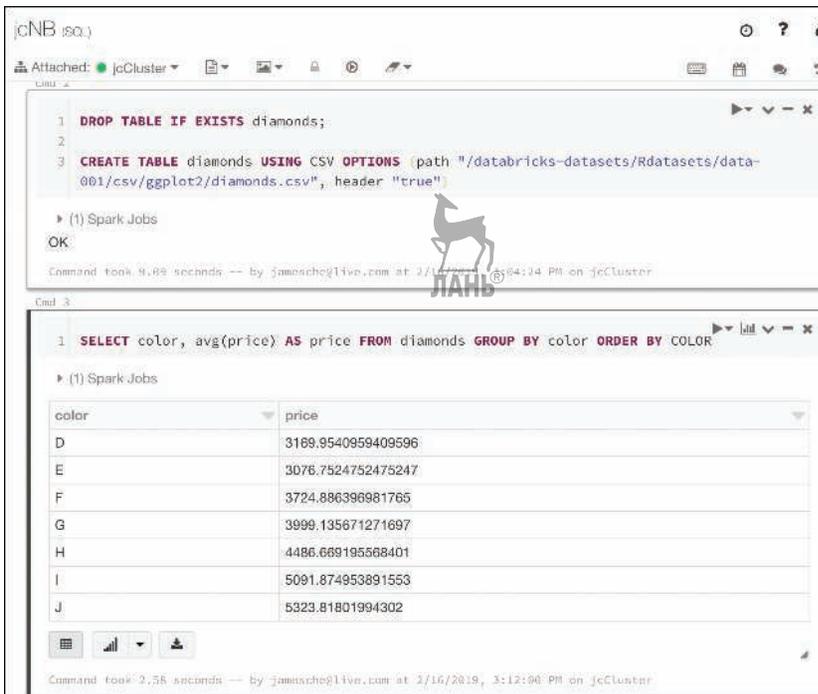


Рис. 3.23 Запрос данных



СОВЕТ К ЭКЗАМЕНУ

Обсуждение того, как программировать и обучать ML-модели, выходит далеко за рамки экзамена AZ-900, поэтому мы не будем рассматривать это в деталях. Важно помнить, что Databricks работает со сторонними инструментами машинного обучения, чтобы позволить вам создавать ML-модели.

Чтобы использовать Databricks Runtime ML, можно указать его либо при создании нового кластера, либо в настройках существующего. Это можно сделать, выбрав одну из ML-сред, как это показано на рис. 3.24.

Вы не ограничены библиотеками, включенными в Databricks Runtime ML. Вы можете подключить большинство сторонних средств машинного обучения к Azure Databricks, как это описано в документации по ссылке: <https://bit.ly/az900-thirdpartyml>.

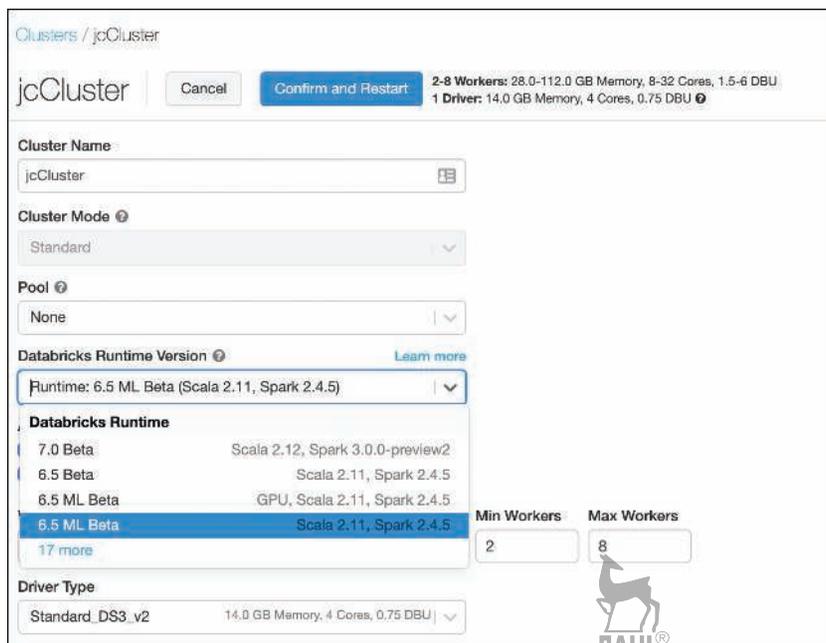


Рис. 3.24 Databricks Runtime ML в настройках кластера



СОВЕТ К ЭКЗАМЕНУ

Возможно, вы заметили отсылки к сервису Spark в документации Databricks. Это связано с тем, что Databricks основан на Apache Spark, системе с открытым исходным кодом для распределенной обработки больших данных.

После того как вы создали ML-модель в Databricks, вы можете экспортировать ее для использования во внешней ML-системе. Этот процесс называется «выводом в производство» (productionalizing) конвейера машинного обучения, и Databricks позволяет делать это помощью двух различных методов: MLeap и Databricks ML Model Export.

MLeap – это система, которая может исполнять модель машинного обучения и делать прогнозы на основе этой модели. Databricks позволяет экспортировать модель в так называемый пакет (bundle) MLeap. Затем вы можете использовать этот пакет для запуска модели с новыми данными.

Databricks ML Model Export предназначен для экспорта конвейера и ML-моделей для использования в других платформах машинного обучения. Он специально разработан для экспорта моделей и конвейеров на основе Apache Spark.

Машинное обучение Azure

Azure Machine Learning – это служба, которая позволяет вам интегрироваться в мир *искусственного интеллекта* (artificial intelligence, AI). Чтобы действительно разобраться в Azure Machine Learning, вам сначала нужно понимать основы искусственного интеллекта и машинного обучения.

Искусственный интеллект

Прежде чем мы погрузимся в ИИ, давайте сначала договоримся о том, что мы подразумеваем под ИИ. Когда многие думают о компьютерном ИИ, то образ, который приходит на ум, – это убивающий людей андроид или другая враждебная технология, одержимая избавлением мира от людей. Вы будете рады узнать, что на самом деле это ошибочное представление.

ИИ сегодня называется искусственным ограниченным интеллектом (Artificial Narrow Intelligence), или иногда слабым ИИ (weak AI), и он относится к ИИ, способному выполнять лишь одну конкретную задачу гораздо эффективнее человека. Весь ИИ, который мы разработали до сих пор, является слабым ИИ. На другом конце спектра ИИ – искусственный интеллект общего уровня (Artificial General Intelligence), или сильный ИИ (strong AI). Это тип ИИ, который показан в фильмах и научно-фантастических книгах, однако в настоящее время у нас нет таких возможностей.

Применение термина «слабый» по отношению к существующим технологиям ИИ может сбивать с толку. Если вы сравните их с возможностями воображаемого «сильного» ИИ, они, безусловно, имеют ограничения, но и слабый ИИ может решать сложные задачи, с которыми вы сталкиваетесь каждый день. Например, если вы общаетесь со своим телефоном или умной аудиоколонкой, то ИИ распознает то, что вы сказали.

В издании «Profiles of the Future» 1973 года известный писатель-фантаст Артур Кларк сказал: «Любая достаточно развитая технология неотличима от магии». Хотя ИИ еще не было, когда Кларк сделал это утверждение, возможности, которые доступны ИИ, безусловно, имеют широкое применение, а сам ИИ не является магией. ИИ – это математика, а как вам скажет любой компьютерный специалист, компьютеры очень сильны в математике.

Чтобы развивать возможности ИИ, инженеры поставили перед собой цель дать компьютерам возможность «учиться» так же, как и человеческий мозг. Наш мозг состоит из нейронов и синапсов. Каждый нейрон взаимодействует со всеми другими нейронами в мозге, и вместе они образуют так называемую нейронную сеть. В то время как отдельный нейрон решает лишь простую задачу, вся сеть способна на необычные вещи.

ИИ работает на основе цифровой нейронной сети. Каждая часть этой нейронной сети может общаться и обмениваться информацией с любой другой частью сети. Как и наш мозг, компьютерная нейронная сеть принимает входные данные, обрабатывает их и предоставляет результат. ИИ может использовать множество методов для обработки входных данных, и каждый метод является подмножеством ИИ. Двумя наиболее распространенными задачами являются понимание естественного языка и машинное обучение.

Понимание естественного языка является технологией ИИ, которая разработана, чтобы понимать человеческую речь. Если бы мы попытались запрограммировать компьютер традиционным способом, чтобы понять произнесенное слово, то потребовались бы целая армия программистов и несколько десятилетий, чтобы приблизиться к работающему приложению. Они не только должны были бы учитывать акценты и различия словарного запаса, которые имеются в разных географических регионах, но и должны были бы учитывать тот факт, что люди часто произносят слова по-разному даже в одних и тех же

регионах. Люди также имеют разные речевые ритмы, и поэтому некоторые слова произносятся вместе. Компьютер должен знать, как различать отдельные слова. В дополнение ко всей этой сложности компьютер должен учитывать тот факт, что язык постоянно меняется.

ДОПОЛНИТЕЛЬНО COGNITIVE SERVICES

У Azure есть множество опций для понимания естественного языка. Эти службы входят в Cognitive Services. Мы их рассмотрим в данном разделе.



Учитывая эту сложность, как в Amazon смогли создать аудиоклонку Echo? Как Siri от Apple понимает то, что вы говорите? Как Cortana от Microsoft разгадывает хитроумную шутку, когда вы спрашиваете ее о Siri? Ответ во всех случаях – ИИ. У нас есть миллионы часов аудиозаписи, и у нас есть миллионы часов видео, которые включают аудио. Существует так много данных, что ни один человек никогда не может обработать их все, но компьютер обрабатывает данные гораздо быстрее. Он не только имеет больше аналитических алгоритмов, чем люди, но и обрабатывает информацию гораздо быстрее.

ДОПОЛНИТЕЛЬНО КОМПЬЮТЕРЫ РАБОТАЮТ БЫСТРО

Когда я говорю, что компьютеры могут обрабатывать информацию быстрее, чем люди, я действительно имею это в виду! Информация в человеческом мозге перемещается между нейронами со скоростью, которая чуть ниже скорости звука. Хотя это достаточно быстро для наших нужд, это ничто по сравнению с компьютерами. Информация в нейронной сети ИИ перемещается со скоростью света, и именно это позволяет компьютерам обрабатывать огромные объемы данных. Фактически компьютерная система на базе ИИ может обработать за одну неделю столько же информации, сколько человек за 20 000 лет.

Если мы загрузим все эти записи в механизм понимания естественного языка, у него будет множество примеров, чтобы определить, какие слова мы говорим, когда что-то говорим в умный динамик или смартфон, и определение значения этих слов – простой шаблон распознавания. Когда Apple, Amazon и Microsoft разрабатывали эту технологию, они постоянно ее улучшали на основе отзывов реальных пользователей. Иногда голосовые помощники могут спросить вас, правильно ли они поняли ваш запрос, а иногда могут предположить, что что-то не так, если вы прервали диалог раньше времени. Со временем система становится все лучше и лучше, поскольку она получает больше данных.

Машинное обучение (Machine learning, ML) работает похожим образом и использует нейронные сети для обучения, но предназначено не для понимания речи. Фактически машинное обучение имеет множество применений. Одним из распространенных видов машинного обучения является распознавание изображений. Как оказалось, нейронные сети ИИ особенно хорошо распознают закономерности в изображениях, и, как и аудио, у нас есть огромный объем данных, с которыми нужно работать.

Мы все знаем, что спутники фотографируют поверхность Земли уже долгое время. У нас есть подробные изображения почти с каждого квадратного дюйма

нашей планеты, и эти изображения ценны во многих отношениях. Например, ученые, которые занимаются охраной природы, получают возможность следить за тем, как наша планета меняется с течением времени. Так, инженеры лесного хозяйства должны знать о здоровье лесов. А специалисты по охране дикой природы должны знать, где животные подвергаются наибольшему риску. Применяя машинное обучение к изображениям со спутников, Microsoft может помочь собрать нужные данные.



ДОПОЛНИТЕЛЬНО MICROSOFT AI ДЛЯ ЗЕМЛИ

Дополнительные сведения о том, как Microsoft использует искусственный интеллект для сохранения природы, смотрите по адресу: <http://aka.ms/aiforearth>.

Анализ изображений с помощью ИИ не ограничивается планетарными задачами. Эта технология также может быть полезной, когда мы, например, хотим проанализировать наши собственные фотографии. Возможно, вы хотите найти все фотографии с нужным человеком, или заинтересованы в том, чтобы найти все фотографии цветов. Ваш телефон, скорее всего, уже может сделать это, и он делает это с помощью искусственного интеллекта и машинного обучения. Например, Google Photos может идентифицировать конкретных людей на фотографиях, сделанных с разницей в десятилетия. Все это реализуется с помощью машинного обучения (ML).

ML использует алгоритм обучения, который является основой для ИИ. После разработки алгоритма вы передаете в него тестовые данные и проверяете результат. Основываясь на промежуточном результате, вы улучшаете алгоритм. Как только алгоритм начинает выдавать результаты с необходимой точностью, он разворачивается в среде с большой вычислительной мощностью. Затем вы можете подавать в него огромные объемы данных для обработки. Поскольку алгоритм имеет дело с большим количеством данных, он может улучшать себя с помощью выявления шаблонов.

Когда вы тестируете ML-модель, вы настраиваете сценарий так, чтобы только часть полного набора данных использовалась для обучения. После того как ваша модель обучена, вы используете оставшуюся часть данных для оценки результата. Поскольку вы имеете дело с заранее подготовленным набором данных, вы уже знаете, какого результата ожидать от ML-модели. Это позволяет определить точность результатов ее работы. После достижения желаемой точности модели ее можно начать использовать с новыми реальными данными.

Даже после тщательной настройки модели алгоритмы машинного обучения могут ошибаться. В статье о машинном обучении, опубликованной в 2016 году, Марко Рибейро, Самир Сингх и Карлос Гестрин написали об ML-эксперименте, который был разработан для того, чтобы различать собак и волков на фотографиях. Как оказалось, алгоритм совершал множество ошибок, но люди не могли понять, почему.

Когда они вернулись назад и протестировали алгоритм машинного обучения, чтобы определить, как он принимает неверные решения, они обнаружили, что алгоритм пришел к выводу, что фотографии с волками имеют снежный

фон, а фотографии с собаками – траву. Поэтому каждая собака на фотографии с заснеженным фоном классифицировалась (иногда неправильно) как волк.

ДОПОЛНИТЕЛЬНО ИИ И ДОВЕРИЕ

История с волками и собаками иллюстрирует одну из основных проблем ИИ, а именно как определить, что ИИ-модели можно доверять. Если вы хотите больше узнать об этом эксперименте, то можете найти статью по адресу: <https://arxiv.org/pdf/1602.04938.pdf>.

Теперь, с базовыми знаниями, вы лучше понимаете, что именно предлагает Azure своим машинным обучением.

Машинное обучение Azure

Машинное обучение Azure делает ML-модели доступными практически для каждого. Обучение предлагает комплекты разработки ПО как на Python, так и на R, среду с поддержкой перетаскивания объектов мышью и автоматизированный режим работы для более легкого создания и наглядного обучения по использованию ML-моделей.

Машинное обучение Azure доступно в двух версиях: базовой (Basic) и универсальной (Enterprise). Базовая версия предлагает доступ только к комплекту разработки ПО ML-моделей и записные книжки. Универсальная же версия предлагает функции базовой, но и многие дополнительные, в том числе визуальные, конструкторы.

ДОПОЛНИТЕЛЬНО MACHINE LEARNING STUDIO

У Microsoft есть автономная студия Machine Learning Studio, которая работает на своем собственном портале, однако лучше использовать машинное обучение Azure. Может сбить с толку то, что машинное обучение Azure также предлагает студию, однако это совсем другое.

Для начала вы должны создать рабочую среду машинного обучения Azure, после создания которой вы сможете создавать модели, обучающие модели, проводить эксперименты и т. д. На рис. 3.25 видно, что вы направляетесь в студию машинного обучения Azure для выполнения большинства операций.

Нажав на кнопку **Launch Now** (Загрузить), как показано на рис. 3.25, вы загрузите студию, где сможете создать ML-модели. На рис. 3.26 показано, что в студию могут быть загружены образцы, так что вы сможете экспериментировать с машинным обучением Azure.

Оплата за машинное обучение Azure построена на том, как вы используете его. Вам выставляют счет за VM, на которой установлена работа машинного обучения Azure. Вам также назначат машину обучения за дополнительно взимаемые суммы и небольшое количество в час за использование. Если вы хотите сэкономить, то можете настроить использование на год по сниженной стоимости или три года по еще более выгодной цене.

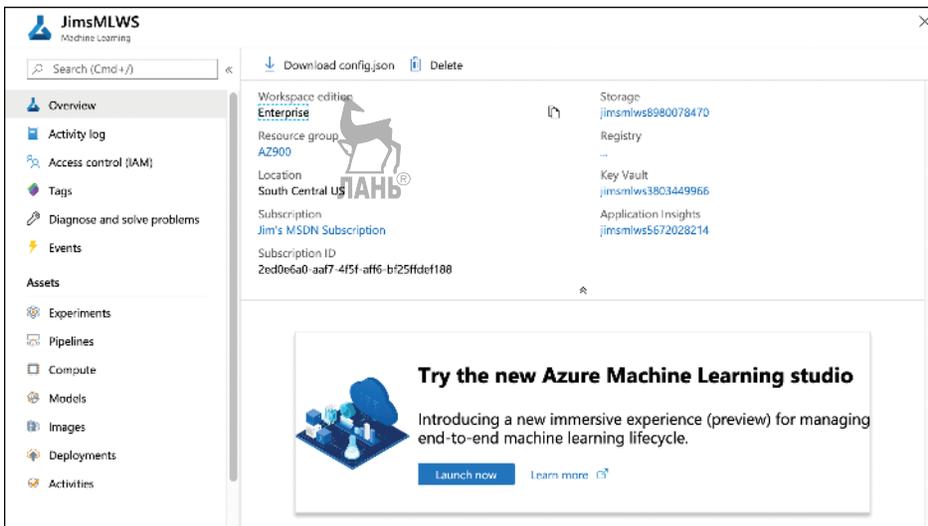


Рис. 3.25 Рабочая среда машинного обучения Azure

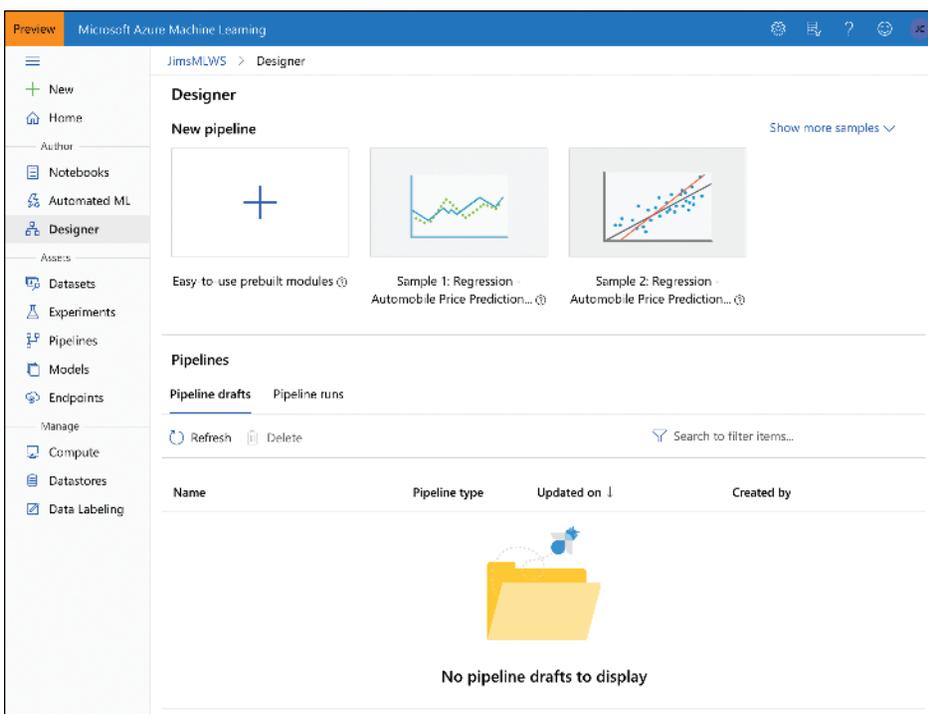


Рис. 3.26 Студия машинного обучения Azure, показывающая страницу конструктора



Служба когнитивных вычислений

Microsoft предлагает большое количество прикладных программных интерфейсов (application programming interface, API), которые способствуют быстрому созданию решений машинного обучения. Эти предложения позволяют ускорить возможности ML благодаря преимуществам работы Microsoft для поддержки собственных сервисов, таких как Bing, Microsoft 365 и др. Служба когнитивных вычислений подобна модели SaaS ML, которую вы можете напрямую использовать в решениях ML без необходимости создавать свою.

ДОПОЛНИТЕЛЬНО СЛУЖБЫ КОГНИТИВНЫХ ВЫЧИСЛЕНИЙ

Microsoft предлагает множество API в службе когнитивных вычислений, число которых постоянно увеличивается. В этой книге мы рассмотрим лишь некоторые из интерфейсов, так как у нас попросту не хватит страниц, чтобы уместить их все. Если у вас есть желание прочитать обо всех существующих API, то вы можете воспользоваться следующим сайтом: <https://bit.ly/az900-cognitiveapis>.

Службы когнитивных вычислений включают API, называемый компьютерным зрением (Computer Vision), который упрощает создание механизма ML, способного извлекать информацию из изображений. Компьютерное зрение может распознавать объекты или сцены, а также неподходящий контент, чтобы у вас была возможность модернизировать изображения. Чтобы увидеть компьютерное зрение в действии, вы можете ввести URL-адрес изображения или загрузить свое собственное изображение для анализа по адресу <https://bit.ly/az900-computervision>.

По тому же принципу Video Indexer API анализирует видеоконтент и извлекает из него информацию. Можно без особого труда добавлять субтитры на нескольких языках, распознавать людей и объекты, а также искать видео, содержащие определенные слова, людей или даже эмоции.

Также доступны и многочисленные речевые API-интерфейсы, от перевода речи (Speech Translation), который осуществляет перевод в режиме реального времени, до распознавания говорящего (Speaker Recognition), API, способный анализировать речь и идентифицировать говорящего. Языковые API-интерфейсы предоставляют возможность понимания введенных команд (полезно для создания автоматического агента чата и подобного) или текстовую аналитику, улавливающую настроения пользователей в тексте.

Службы когнитивных вычислений также предоставляют API-интерфейсы для принятия решений, которые позволяют вам выполнять такие действия, как уменьшение контента в изображениях, тексте или видео. Вы можете предложить пользователям персонализированный пользовательский интерфейс с помощью персонализированного API (Personalizer API).

Цены на службы когнитивных вычислений Azure являются транзакционными. Это значит, что вы платите небольшую сумму за транзакции, которые обрабатываются в службе. Детальный обзор по ценообразованию служб когнитивных вычислений расположен на сайте: <https://azure.microsoft.com/en-us/pricing/details/cognitive-services/>.

Служба Azure Bot

Одним из распространенных вариантов использования служб когнитивных вычислений является создание интерактивного искусственного интеллекта, способного на взаимодействие (AI conversational experiences). Этот опыт широко распространен в интернете. В действительности большинство компаний, которые предлагают тот или иной тип взаимодействия в чатах, нередко начинают его с автоматизированного агента. Когнитивные службы вычислений могут способствовать достижению качественного опыта в этой сфере.

Чтобы упростить процесс создания производительного взаимодействия на основе искусственного интеллекта, Microsoft предлагает службу Azure Bot (Azure Bot Service). Эта служба является предложением PaaS, работающим в службе приложений Azure. Это означает, что она наследует все функции службы приложений, такие как простое масштабирование и конфигурация.

Вы создаете службу Bot при помощи шаблона Web App Bot на портале Azure. Как показано на рис. 3.27, у вас есть выбор между C# и Node.js для языка программирования SDK. Вы можете выбирать между разными шаблонами ботов в зависимости от особых потребностей.

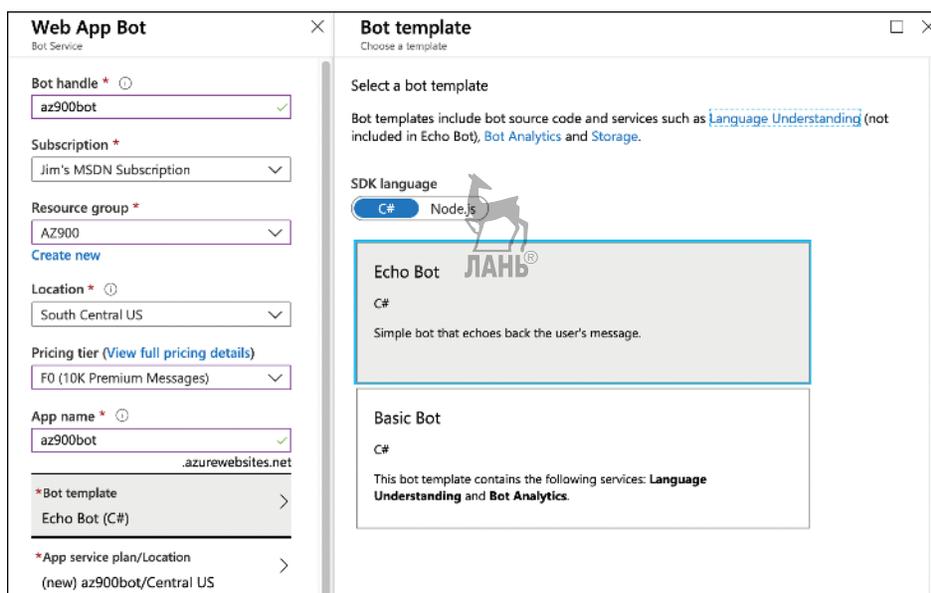


Рис. 3.27 Создание бота в службе Azure Bot Service

После создания Bot-службы вы можете загрузить код для его настройки, как показано на рис. 3.28. Портал Azure покажет вам все, что необходимо будет сделать для начала работы с вашим ботом. В такой инструктаж входит редактирование исходного кода, создание исходного кода, просмотр аналитики и многое другое. Все эти задачи являются частью *Bot Framework*, платформы, разработанной Microsoft для упрощения создания ботов.

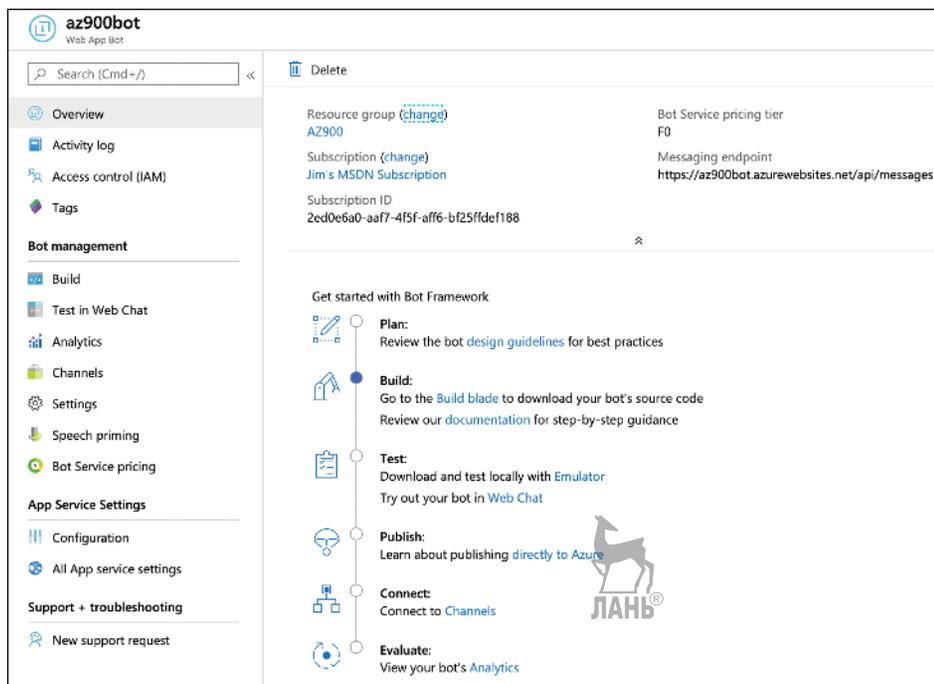


Рис. 3.28 Служба Azure Bot Service на портале Azure

Разрабатывая свою программу-бота, вы можете использовать пункт меню **Test In Web Chat** (Тест в веб-чате), расположенного в левой части портала (показан на рис. 3.28), чтобы проверить работоспособность. После того как вы нажмете на эту кнопку, вы сможете указать команды на выбор для программы. На рис. 3.29 показано взаимодействие, доступное из базового шаблона программы-бота (Basic Bot), предоставленного корпорацией Microsoft.

Службу Azure Bot можно подключить ко многим популярным сервисам, таким как Slack, Facebook Messenger, Microsoft Teams и др. Каждый из них считается *каналом* внутри службы Bot. Каналы, предоставляемые Microsoft, называются *стандартными*. Однако можно использовать и то, что Microsoft называет *прямой линией* (Direct Line) для подключения бот-программы к вашему приложению или веб-сайту. Прямая линия считается *премиум-каналом*, и за сообщения, используемые ею, вы заплатите небольшую сумму.



СОВЕТ К ЭКЗАМЕНУ

Поскольку служба Bot работает в службе приложений Azure, с вас будет взиматься плата за план службы приложений при создании службы Bot.

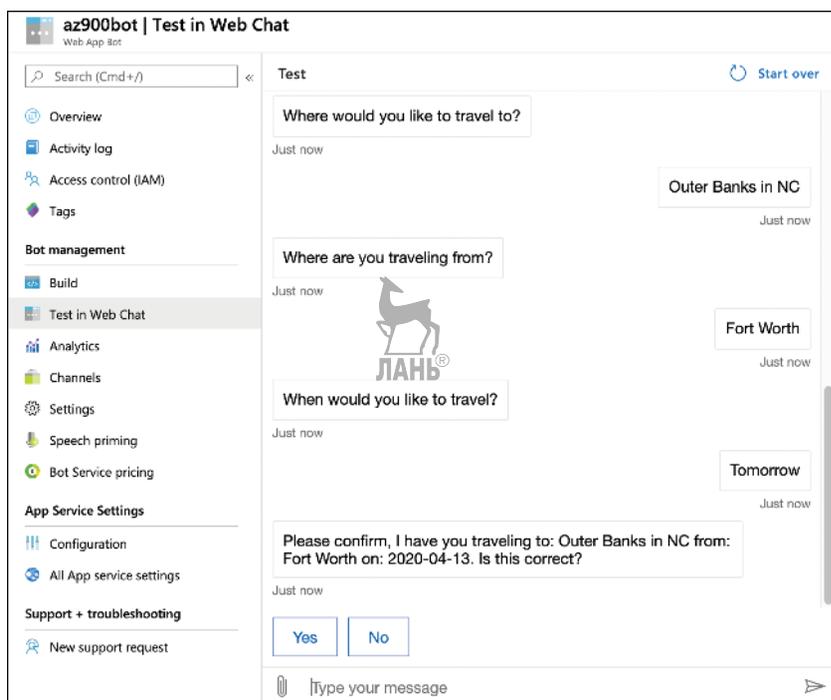


Рис. 3.29 Взаимодействие с ботом с помощью функции тестирования на портале Azure

Бессерверные вычисления

Как вы уже узнали, одним из преимуществ перехода в облако является то, что вы можете воспользоваться большими объемами инфраструктуры, в которую вложены средства облачного провайдера.

Вы можете создавать виртуальные машины в облаке и оплачивать только время их работы. Иногда вам просто нужно арендовать компьютер, чтобы провести вычисления или выполнить быструю задачу. В таких ситуациях идеально подходят так называемые бессерверные (serverless) вычисления. При использовании serverless-решений вы платите только за время работы вашего кода на виртуальной машине. Когда ваш код не работает, вы ничего не платите.

Концепция бессерверных вычислений возникла потому, что облачные провайдеры имели неиспользуемые виртуальные машины в своих центрах обработки данных, и они хотели монетизировать их. Всем облачным провайдерам требуется избыточная емкость, чтобы они могли удовлетворить потребности клиентов, но когда виртуальные машины простаивают, ожидая клиента, это приводит к потере дохода. Чтобы решить эту проблему, облачные провайдеры создали тарифные планы на основе фактического потребления, которые позволяют запускать код на избыточных виртуальных машинах и оплачивать только время его работы.



СОВЕТ К ЭКЗАМЕНУ

Важно понимать, что «бессерверный» не означает, что виртуальные машины и физические серверы не используются. Это просто означает, что виртуальная машина, на которой работает ваш код, за вами не закреплена. Ваш код перемещается на виртуальную машину, выполняется, а затем удаляется.

Поскольку ваш «бессерверный» код работает на избыточной емкости, облачные провайдеры обычно предлагают большие скидки на такие тарифные планы. На самом деле за небольшие рабочие нагрузки вы можете вообще ничего не платить.

Azure имеет множество бессерверных служб. Мы уже обсуждали, что примерами таких служб являются Azure Databricks и Azure Machine Learning Service. Однако есть и другие бессерверные службы, которые мы еще не обсуждали. Это Azure Functions для вычислений, Azure Logic Apps для автоматизации рабочих процессов и Azure Event Grid для маршрутизации событий.

Функции Azure (Azure Functions)

Azure Functions – это компонент бессерверных вычислений в Azure. Это означает, что вы можете использовать Functions для написания кода, не беспокоясь о его развертывании или создании виртуальных машин. Приложения на основе Azure Functions часто называются приложениями-функциями (Function Apps).

ДОПОЛНИТЕЛЬНО FUNCTION APPS ИСПОЛЬЗУЮТ СЛУЖБУ ПРИЛОЖЕНИЙ

Function Apps не являются в прямом смысле бессерверными, а работают на базе Azure App Service. Вы можете самостоятельно создать Function App на базе App Service, но в этом случае вам придется платить за все время работы сервиса, а не только за время работы вашего кода. Мы рассмотрим это подробнее позже в данной главе.

Функции могут быть созданы различными способами. Вы можете создать приложение-функцию, используя:

- Microsoft Visual Studio;
- Microsoft Visual Studio Code;
- Maven для Java Function Apps;
- командную строку Python для Python Function Apps;
- интерфейс командной строки Azure (command line interface, CLI) в Windows или Linux;
- портал Azure.

Предположим, что вы не создаете Function App при помощи метода, особенно для определенного языка, вы можете выбрать между .NET Core, Node.js, Python, Java или PowerShell Core при использовании Code option (вариантов кода). Можно также создать Function App с помощью контейнера Docker на VM Linux.

На рис. 3.30 показано создание Function App на портале Azure. Мы выбрали .NET в качестве среды выполнения, чтобы использовать язык C# для написания функций.

Function App

Basics Hosting Monitoring Tags **Review + create**

Create a function app, which lets you group functions as a logical unit for easier management, deployment and sharing of resources. Functions lets you execute your code in a serverless environment without having to first create a VM or publish a web application.

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Jim's MSDN Subscription

Resource Group * ⓘ AZ900
[Create new](#)

Instance Details

Function App name * contosopharmfunc .azurewebsites.net

Publish * Code Docker Container

Runtime stack * .NET Core

Version * 3.1

Region * Central US

[Review + create](#) < Previous Next : Hosting >

Рис. 3.30 Создание нового Function App на портале Azure

После выбора стека среды выполнения и версии вы можете настроить способ размещения Function App. В качестве операционной системы можно выбрать между Linux и Windows, хотя некоторые варианты стека среды выполнения допустимы только для одной из ОС. Можно будет выбрать запуск в бессерверном плане (используемом по умолчанию) или запуск в плане обслуживания приложений. На рис. 3.31 Function App настраивается для запуска в Windows в соответствии с типом плана потребления (бессерверный).

Как только Function App будет создано, вы можете открыть его на портале, чтобы начать писать код. На рис. 3.32 показано новое Function App на портале Azure.

Начиная с этого момента вы можете создать новую функцию, новый прокси или новый слот. Функция – это код, который запускается, когда срабатывает триггер. (Мы скоро посмотрим на триггеры.) Прокси (proxy) позволяет настроить несколько конечных точек для вашего Function App, но использовать при этом один URL-адрес. Слоты позволяют создавать копии ваших Function App, скрытых от пользователей. Вы можете написать код и протестировать новую

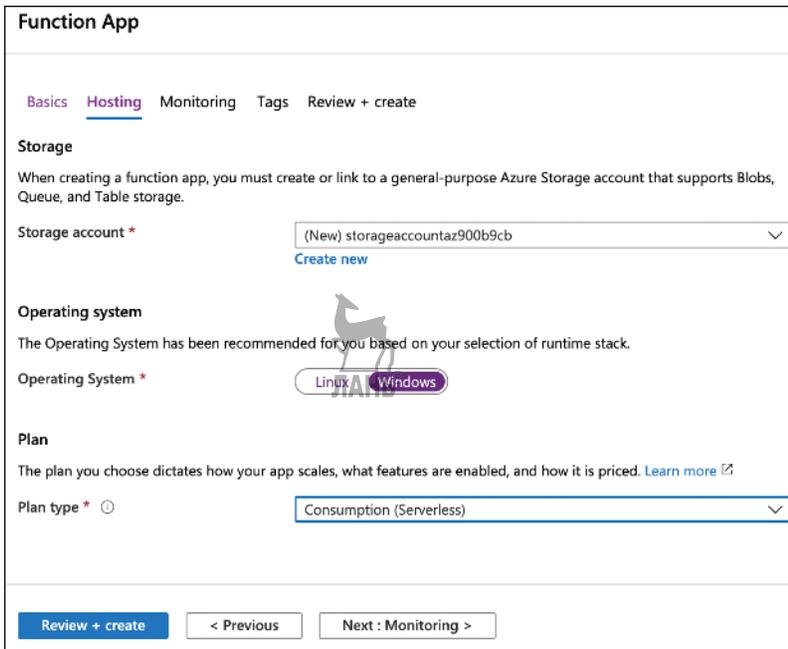


Рис. 3.31 Настройка параметров размещения для Function App

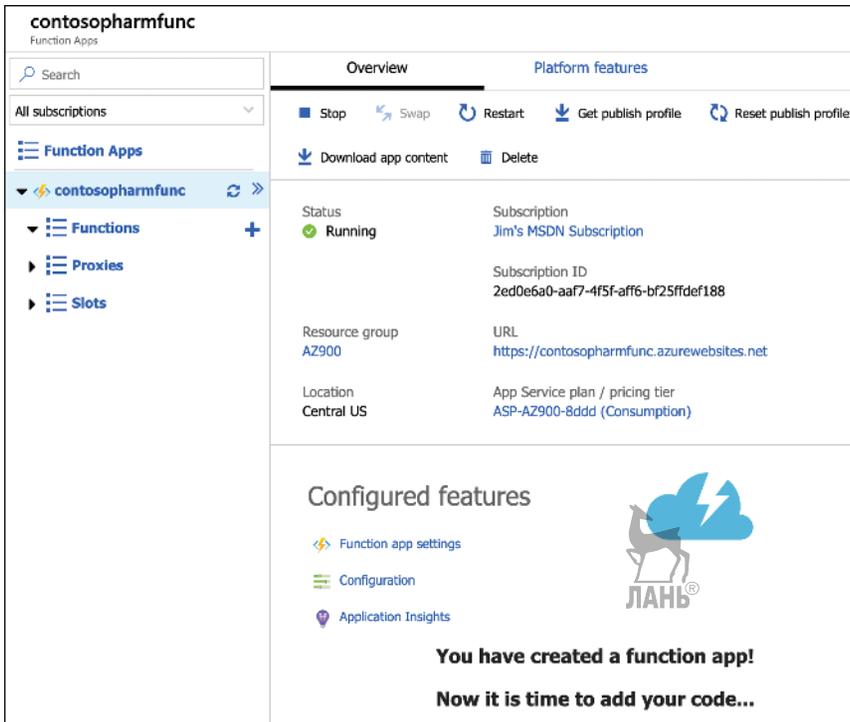


Рис. 3.32 Новое Function App на портале Azure

версию в рабочей среде, и если она работает корректно, то вы можете переключиться между старым и новым кодами одним нажатием кнопки. Эта функциональность в App Service называется слотами развертывания (Deployment Slots).

Если вы нажмете кнопку **Function App Settings** в разделе **Configured Features** (см. рис. 3.32), то сможете изменить настройки для приложения, как это показано на рис. 3.33.

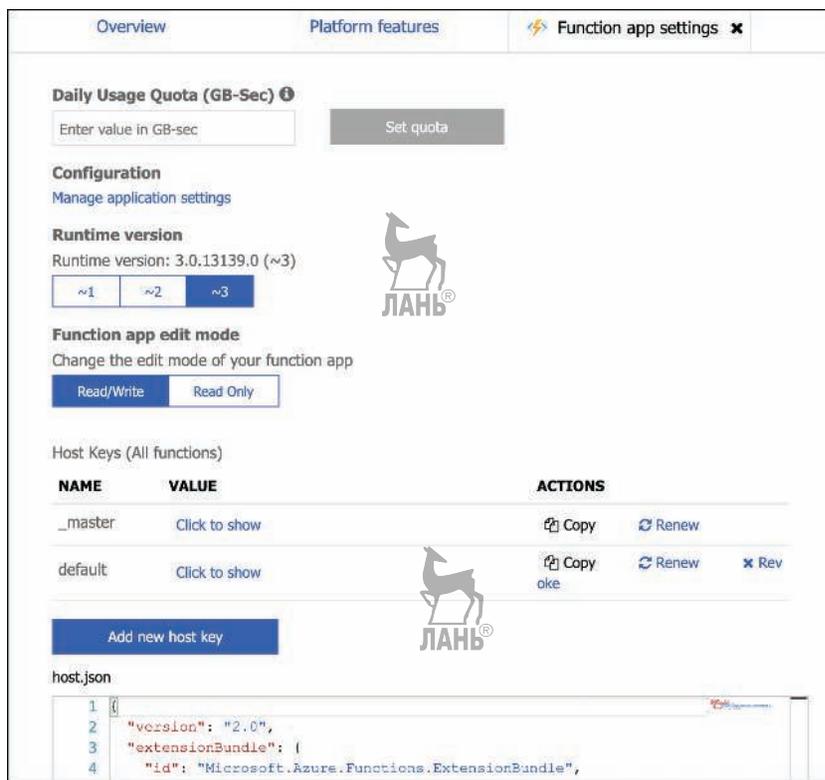


Рис. 3.33 Параметры Function App

На этом экране вы можете настроить ежедневную квоту для вашего приложения-функции. Как только вы достигнете квоты, Azure остановит приложение до следующего дня. Вы также можете изменить версию среды выполнения приложения. Это версия среды выполнения Azure Functions, и обычно рекомендуется использовать последнюю версию, но если ваша функция была написана в более ранней версии среды, то вы не сможете обновить ее, просто изменив версию в настройках. Изменение версии может привести к поломке приложения, поэтому Microsoft предотвратит вас от изменения версии, если у вас есть существующие функции в вашем Function App.

Вы также можете изменить Function App на режим только для чтения, чтобы предотвратить любые изменения в нем. Это полезно, если у вас есть несколько разработчиков, пишущих код вашего приложения, и вы не хотите, чтобы кто-

то изменил что-либо без вашего ведома. Наконец, вы можете просматривать, продлевать, отзываться и добавлять новые ключи хоста. Ключи хоста используются для контроля доступа к вашим функциям. Когда вы создаете функцию, то можете указать, будет ли она доступна открыто или потребуется ключ.



СОВЕТ К ЭКЗАМЕНУ

Хотя ключ может защитить ваши функции, он не предназначен для обеспечения полной безопасности Function Apps. Если вы хотите защитить свое приложение от несанкционированного доступа, то должны использовать механизмы аутентификации, доступные в App Service. Вы также можете использовать Microsoft API Management для добавления требований безопасности в Function App.

Если вы нажмете **Application Settings** (показано на рис. 3.32), то можете настроить параметры приложения. Эти параметры специфичны для службы приложений. На рис. 3.34 показаны некоторые из этих параметров, в том числе работает ли приложение в 32-разрядной или 64-разрядной среде, версию HTTP, возможность доступа к файлам с помощью FTP и многое другое. На этой странице можно также настроить строки подключения к базе данных.

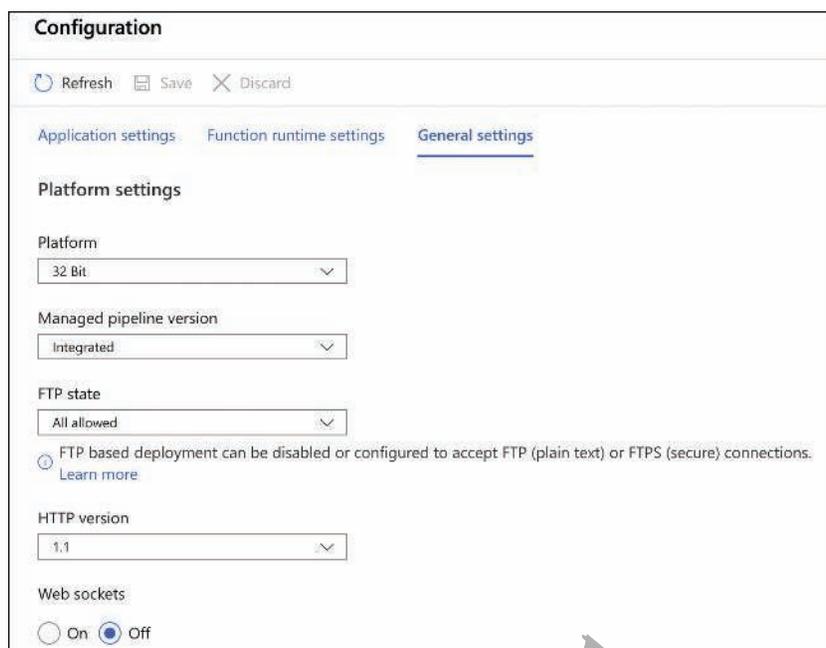


Рис. 3.34 Некоторые настройки Function App

Наконец, если вы перейдете на вкладку **Platform Features** (Свойства платформы), то увидите все доступные вам функции в App Service, как показано на рис. 2.83. Здесь можно настроить SSL-сертификаты, пользовательские имена доменов, аутентификацию и многое другое.



Рис. 3.35 Свойства платформы App Service, доступные Function App

Чтобы создать новую функцию, нажмите на знак +, как показано на рис. 3.36. Затем можно выбрать среду разработки. Вы можете выбрать Visual Studio, Visual Studio Code, среду разработки внутри портала Azure (In-Portal), или можете использовать редактор кода по вашему выбору наряду с основными инструментами Azure Functions Core Tools.

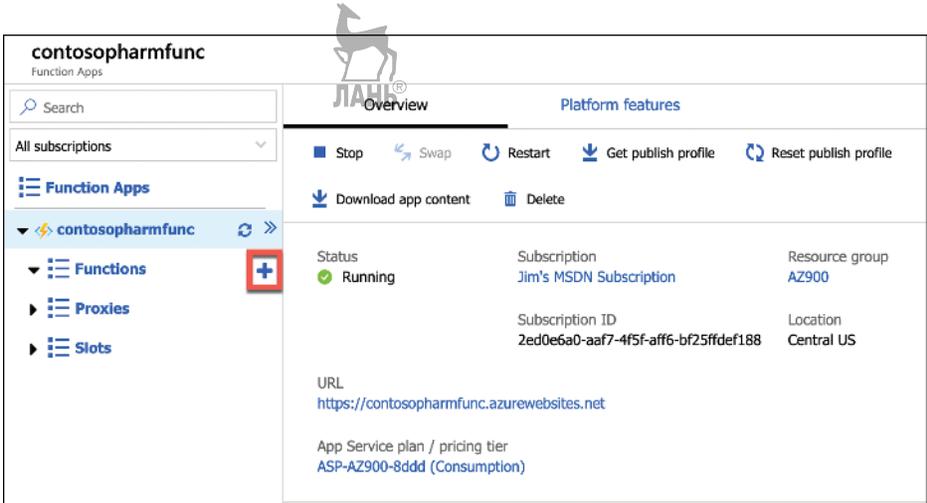


Рис. 3.36 Создание функции

Если вы выберете какой-либо вариант, отличный от In-Portal, вам нужно указать, как вы хотите развернуть свою функцию в App Service. Варианты зависят от выбранной среды разработки, но обычно это включает либо использование возможностей вашей среды для отправки функции непосредственно в App Service, либо вам потребуется использовать центр развертывания службы приложений (App Service Deployment Center). В любом случае развертывание происходит быстро и просто.

В зависимости от того, какую среду разработки вы выберете, вам, скорее всего, придется выполнить предварительные шаги перед написанием кода функции. Вы увидите экран, в котором точно указано, что делать, чтобы все работало правильно. На рис. 3.37 вы можете увидеть, что требуется для использования VS Code для разработки функций. В большинстве случаев вам потребуется установить основные средства Azure Functions Core Tools.

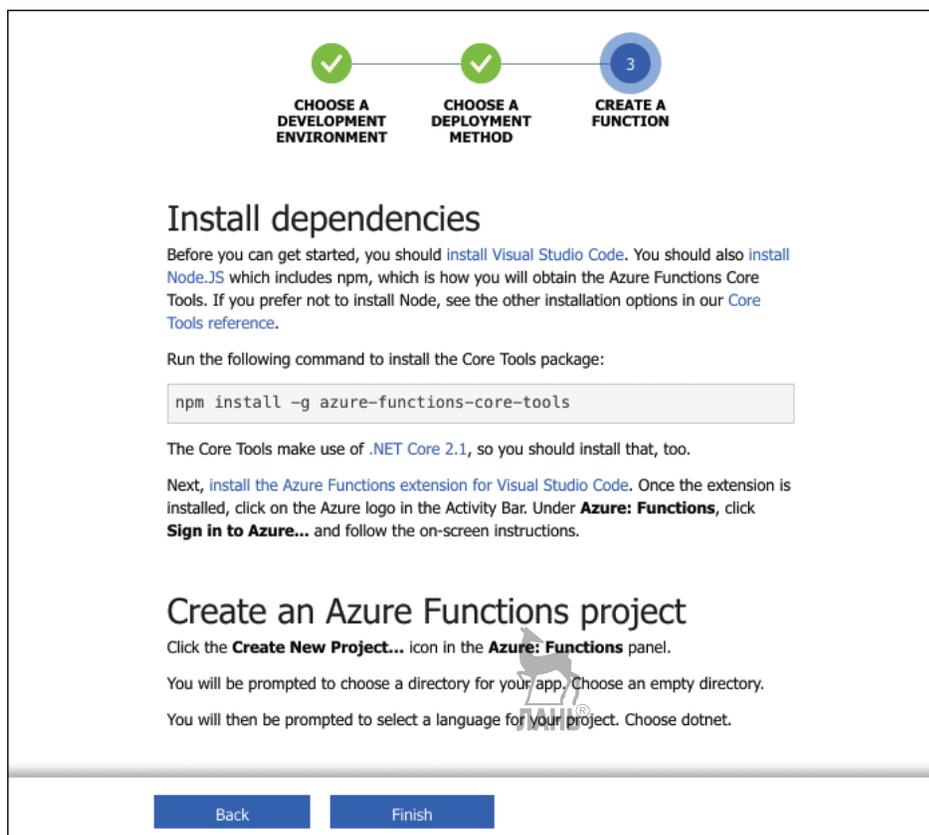


Рис. 3.37 Создание функции с помощью Visual Studio Code и Azure Functions Core Tools

Функции работают с помощью системы, основанной на триггерах. Когда вы создаете свою функцию, вы выбираете триггер, который ее запустит. Когда он срабатывает, ваш код функции будет запущен. Обычно функции пред-

назначены для простых задач. Если вам нужно решить более сложную задачу, вы можете использовать прокси-функцию (Function Proxy) для объединения нескольких простых функций, которые работают вместе над различными частями задачи. Такой подход к разработке называется микросервисами (microservices), и он позволяет быстро менять функциональность, просто изменив отдельную функцию.

После того как триггер сработал и код запустился, вы можете выбрать то, что произойдет далее, используя так называемую привязку вывода (output binding). Тип привязок, которые вы можете использовать, зависит от типа создаваемых функций. На рис. 3.38 показаны некоторые из привязок вывода, доступных при использовании триггера `HttpTrigger`. Эта функция будет запускаться сразу после запроса определенного URL-адреса.

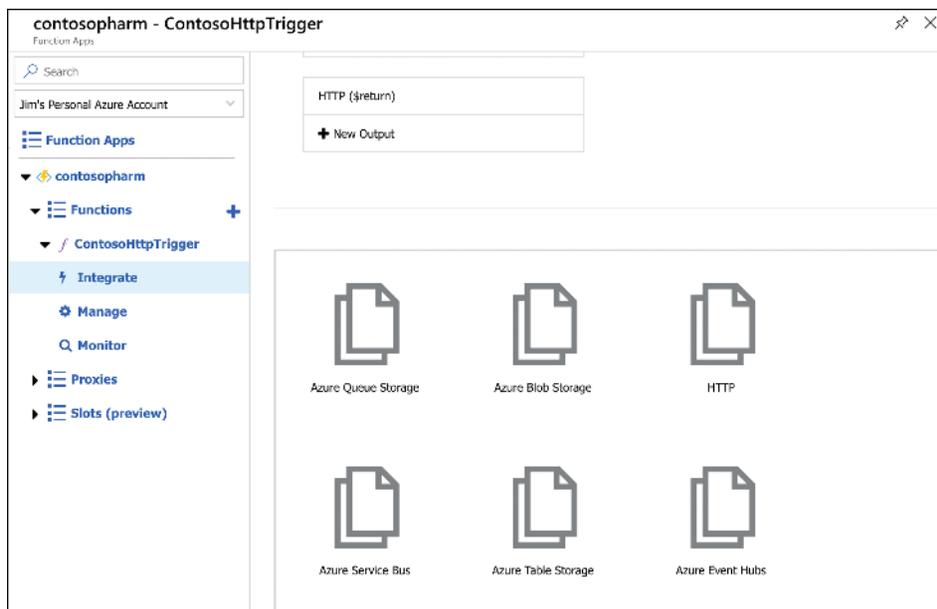


Рис. 3.38 Привязки вывода в функциях Azure

ДОПОЛНИТЕЛЬНО ФУНКЦИИ HTTPTRIGGER

Функции `HttpTrigger` очень удобны, потому что они могут быть вызваны как веб-перехватчики (webhook). Многие онлайн-сервисы поддерживают веб-перехватчиков. В сценарии веб-перехватчика вы можете настроить внешнюю службу, чтобы она сделала запрос на определенный URL-адрес в ответ на событие. Если вы настроили этот веб-перехватчик для вызова URL-адреса функции Azure, то можете легко добавить мощные функциональные возможности в свой рабочий процесс.

Вы также можете настроить несколько выводов для вашей функции. Однако для более сложных задач Logic Apps являются более подходящим выбором, и вы можете интегрировать Logic Apps напрямую с Azure Functions.

Logic Apps

Logic Apps (Логические приложения) похожи на приложения-функции тем, что они запускаются триггером, но после этого запускается другая цепочка действий. В отличие от приложений-функций, вам не нужно писать код для рабочих процессов на базе Logic Apps.

ПРИМЕЧАНИЕ POWER AUTOMATE

Вы, возможно, знакомы с Power Automate, ранее известной как Microsoft Flow. В основе технологии Power Automate на самом деле лежат **Logic Apps** (Логические приложения). Вот почему конструктор Power Automate очень похож на Logic Apps.

Рабочий процесс приложений Logic Apps описывается как цепочка простых действий, таких как отправка электронной почты, передача данных в базу данных и прочее. Он может выполнять эти действия по порядку, но он также может делать две вещи одновременно. Например, у вас может быть сайт электронной коммерции, и когда клиент заказывает продукт, вы можете:

- обновить оставшееся количество товара;
- создать счет для оплаты;
- отправить счет клиенту по электронной почте;
- подписать клиента на свою новостную рассылку;
- создать этикетку для товара.

Приложения Logic Apps позволяют легко создавать сложные рабочие процессы, и поскольку они интегрируются с более чем сотней других служб (как служб Azure, так и сторонних), вы можете сделать что угодно.

В приложениях логики есть три компонента, которые делают рабочие процессы возможными: соединители (connectors), триггеры (triggers) и действия (actions).

- Соединитель – это компонент, который соединяет ваше приложение Logic App с внешним сервисом. Это может быть другая служба Azure, сторонняя служба, FTP-сервер и т. д. Каждый соединитель будет иметь один или несколько триггеров и действий, специфичных для этого соединителя.
- Триггер – это конкретное действие, которое запустит рабочий процесс.
- Действие – это то, что ваше приложение сделает в качестве вывода.

Можно комбинировать несколько действий для соединителя, а также комбинировать несколько соединителей для создания сложных рабочих процессов.

Logic Apps создаются на портале Azure. После создания такого приложения вам отобразится специальный конструктор (designer). В этом конструкторе вы можете выбрать триггер, как показано на рис. 3.39. Показанный список представляет собой краткий набор распространенных триггеров, но есть из чего выбрать. Там также есть триггер для Azure Functions, поэтому вы можете запустить рабочий процесс Logic App во время работы функции.

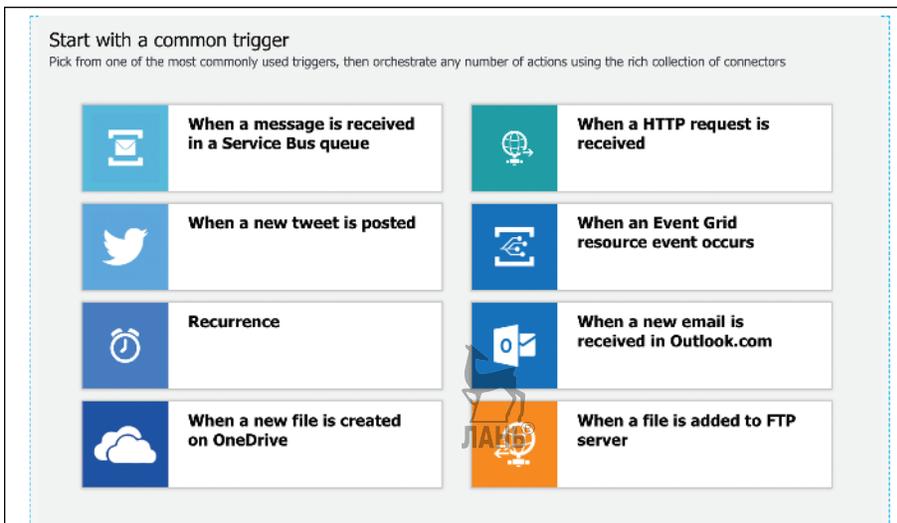


Рис. 3.39 Основные триггеры Logic App



СОВЕТ К ЭКЗАМЕНУ

Важно понимать разницу между соединителями и триггерами. Все элементы, показанные на рис. 3.40, являются триггерами, связанными с определенными соединителями. Например, **When A New File Is Created On OneDrive** (Когда создан новый файл в OneDrive) является триггером для соединителя к OneDrive. Существуют и другие триггеры OneDrive, в том числе **When A File Is Modified** (Когда файл изменен) и **When A File Is Deleted** (Когда файл удален).

Если вы прокрутите вниз, то увидите большое количество шаблонов, которые можно использовать для создания Logic App, как показано на рис. 3.40. Эти шаблоны автоматически настраивают приложение Logic App, содержащее полный рабочий процесс, который можно изменить для собственных целей. Это самый быстрый способ начать работу, но имеющиеся шаблоны могут быть не совсем тем, что вы хотите, поэтому вы можете создать пустое приложение Logic App и начать с нуля.

После создания пустого приложения можно выбрать один из нескольких способов создания рабочего процесса. Можно выбрать триггер из списка, найти триггер или соединитель по запросу либо просто выбрать соединитель из списка и посмотреть, какие триггеры для него доступны. Как показано на рис. 3.41, существует множество доступных вариантов.

На рис. 3.41 показан лишь небольшой фрагмент доступных соединителей в Logic Apps. Эти соединители охватывают широкий спектр сложных задач: от реагирования на файловые операции в папке OneDrive до запуска сложных и мощных операций на сторонних платформах, таких как Salesforce. В этом и есть настоящая ценность Logic Apps. Как правило, если команда разработчиков хочет интегрировать приложение с такой платформой, как Salesforce, то им придется долго изучать Salesforce и то, как программируется приложение для его использования. Многие компании просто нанимают разработчиков

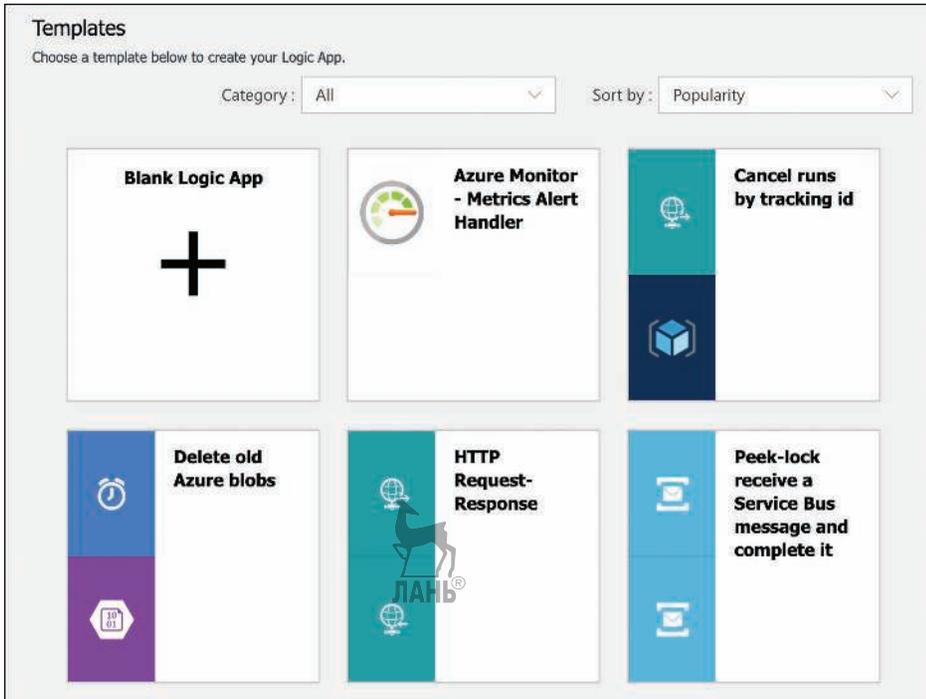


Рис. 3.40 Шаблоны приложений Logic App

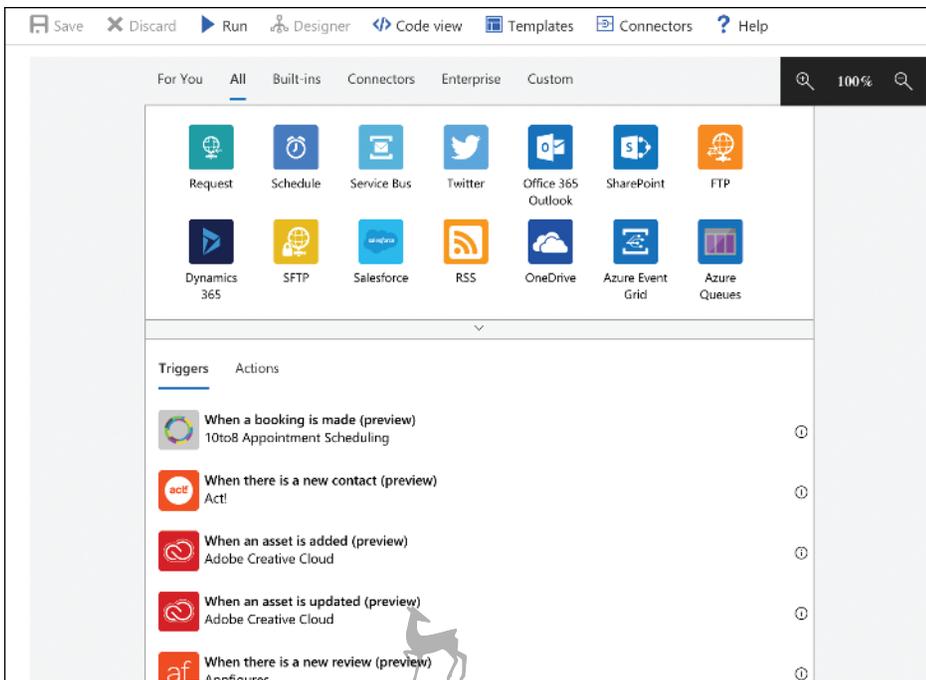


Рис. 3.41 Добавление триггеров в приложение Logic App

с необходимыми для этого знаниями и, как правило, по высокой цене. Используя Logic Apps, компания может обеспечить интеграцию с такими платформами, как Salesforce, или другими даже без разработчиков! Трудно переоценить ценность такой легкой интеграции.

Не всякий сценарий интеграции будет сложным, с нетривиальными платформами. На рис. 3.42 мы настроили коннектор к OneDrive для отслеживания папки в OneDrive. Когда файл будет изменен в этой папке, это запустит рабочий процесс приложения Logic App. Чтобы что-то сделать при изменении файла, нажмите **New Step** (Новый шаг) для добавления действия.

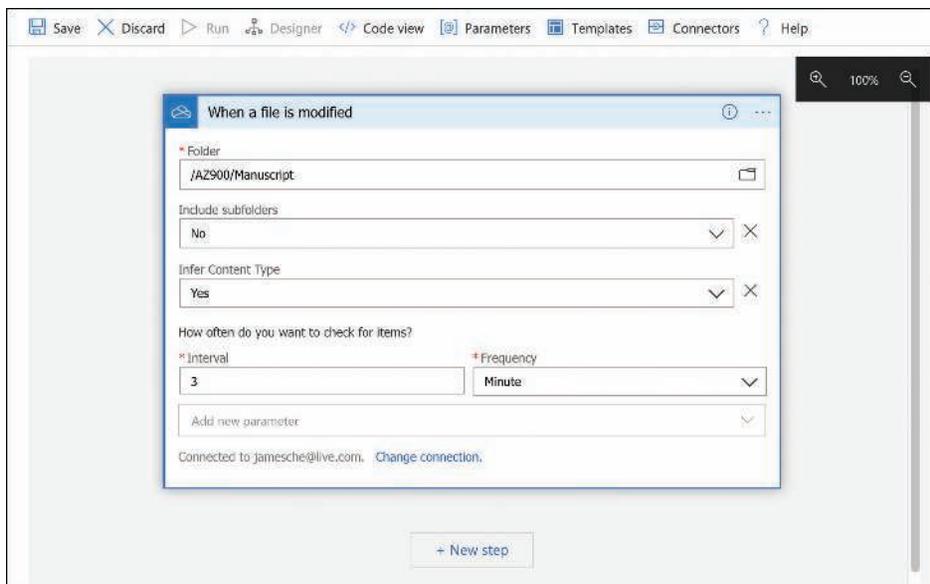


Рис. 3.42 Использование соединителя OneDrive

Когда вы нажмете на **New Step**, то увидите тот же экран, который отображается при запуске приложения. Поскольку мы добавили шаг к рабочему процессу, который уже имеет триггер, то вам отобразятся действия, которые вы можете предпринять при запуске приложения. Существует множество действий для выбора, как показано на рис. 3.43.

На рис. 3.44 мы настроили Logic App для вызова Function App при изменении файла в папке OneDrive. Вы можете передать имя файла, который был изменен, внутрь Function App в виде динамического содержимого (dynamic content). Просто нажмите на **File Name** (Имя файла) из списка. Конечно, можно передать только один элемент динамического содержимого в ваше действие (action).

ДОПОЛНИТЕЛЬНО ПЕРЕДАЧА ПАРАМЕТРОВ В FUNCTION APPS

При вызове Function App из приложения Logic App убедитесь, что функция предназначена для приема данных, которые Logic App передает ему. В противном случае приложение-функция сообщит об ошибке.

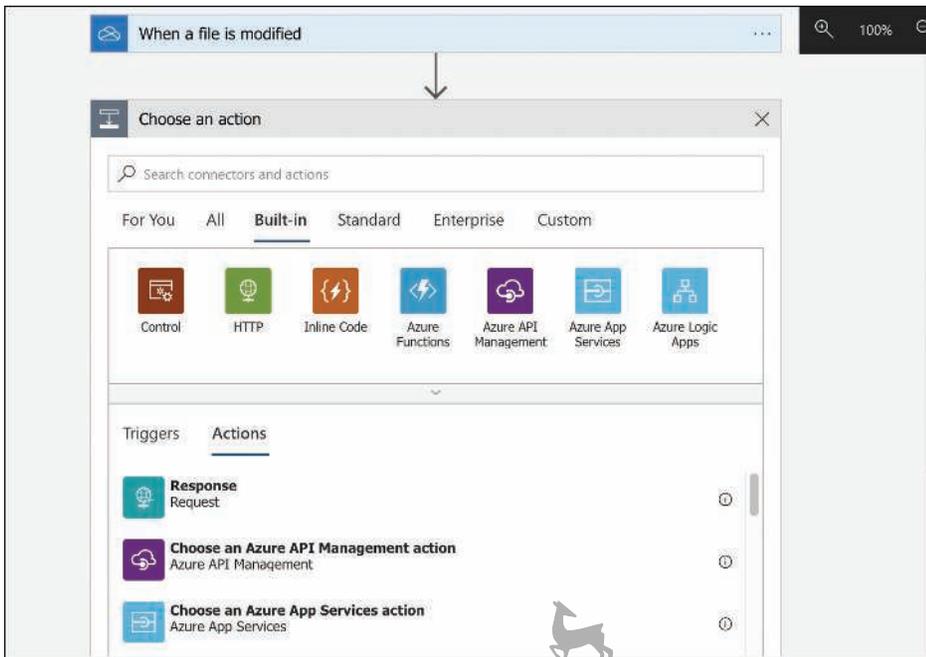


Рис. 3.43 Добавление действия в приложение Logic App

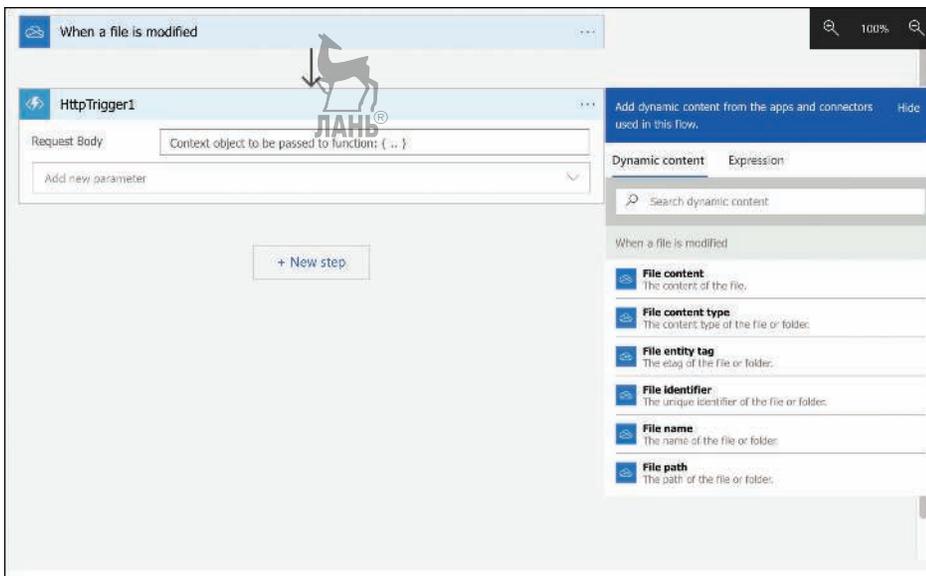


Рис. 3.44 Настройка действия Function App



СОВЕТ К ЭКЗАМЕНУ

Когда вы настраиваете триггеры и действия в конструкторе Logic Apps, приложения логики автоматически генерируют код, который будет реализовывать ваш рабочий процесс. Рабочие процессы приложений Logic App описываются с помощью файлов JSON, и конструктор генерирует этот код JSON при настройке приложения.

Теперь у вас есть работающее приложение Logic App. Чтобы проверить рабочий процесс, нажмите кнопку **Save** (Сохранить) в верхней части конструктора. Соединитель OneDrive настроен на проверку изменений в файлах каждые три минуты (см. рис. 3.42), поэтому вам потребуется подождать несколько минут, пока рабочий процесс запустится. Вы также можете нажать **Run Trigger** (Запустить триггер) в верхней части конструктора, чтобы вручную запустить триггер.

Вы можете отслеживать свои приложения логики с помощью портала Azure. Откройте приложение и нажмите **Overview** (Обзор), чтобы узнать, когда был активирован триггер и запускался ли рабочий процесс, как показано на рис. 3.45.

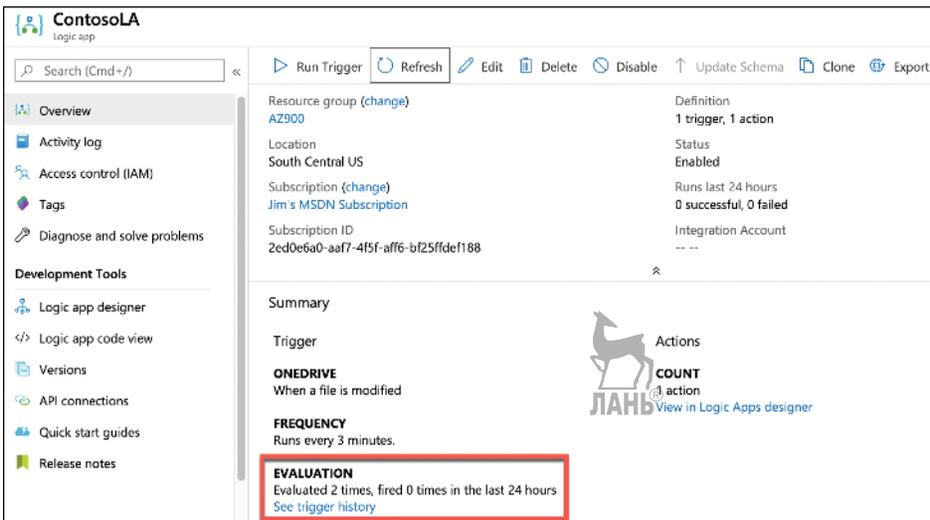


Рис. 3.45 Портал Azure отображает, когда Logic App было запущено

Если вы нажмете **See Trigger History** (Посмотреть историю триггера), то увидите всю историю того, когда триггер сработал и когда он запустил рабочий процесс Logic App.

В нашем примере мы использовали Logic App для вызова функции Azure, но вы могли бы записать лог-файл в хранилище Azure или сохранить информацию в базе данных Azure SQL. Если вы хотите, чтобы приложение логики интегрировалось с другими службами Azure, то можете подключить Azure Event Grid.

Event Grid

Концепция взаимодействия различных служб Azure друг с другом должна быть вам уже знакома. Существует множество способов интеграции служб, и в некоторых случаях требуется, чтобы один ресурс Azure узнал об изменениях другого ресурса Azure. Для этого вы можете использовать метод опроса (polling), аналогичный тому, как Logic App проверяет OneDrive каждые три минуты в поисках изменений. Однако более эффективный способ – разрешить одной службе Azure создавать специальное событие (event) и настроить другую службу Azure для прослушивания этого события, чтобы она могла на него отреагировать. Event Grid предоставляет такую функциональность.

Функции Azure и приложения логики интегрированы с Event Grid. Можно настроить функцию для запуска при возникновении события в Event Grid. На рис. 3.46 представлен список ресурсов Azure, которые могут быть триггером событий Event Grid. Не все службы Azure представлены в Event Grid, но со временем этот список увеличивается.

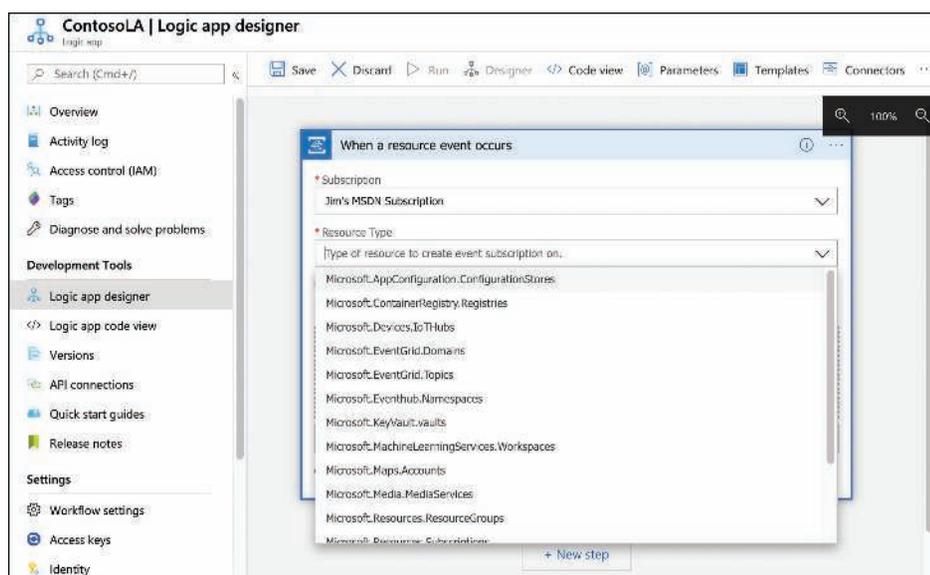


Рис. 3.46 Ресурсы, доступные в Event Grid

После того как вы выбрали тип ресурса, настройте событие, которое вы хотите прослушать. Доступные события могут отличаться в зависимости от выбранного ресурса. На рис. 3.47 мы создаем событие для подписки Azure.

ДОПОЛНИТЕЛЬНО СОБЫТИЯ

Подробную информацию обо всех событиях и о том, что они означают, смотрите на сайте: <https://bit.ly/az900-eventschema>.

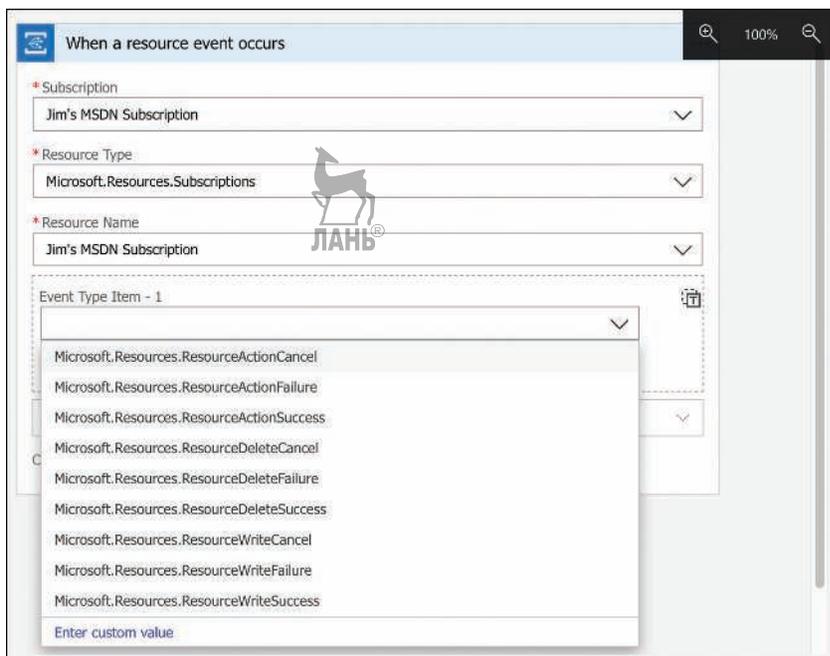


Рис. 3.47 События для подписки Azure

При возникновении события можно выполнить действие с ресурсом Azure с помощью соединителя Azure Resource Manager в Logic App. Можно также запустить сценарий, который взаимодействует с ресурсом Azure, чтобы, например, добавить тег (tag) для ресурса или настроить его определенным образом.

Основным преимуществом использования Event Grid является быстрая разработка решений. Бонусом вы также получаете гарантии того, что Event Grid запустит ваши события. Если событие Event Grid не срабатывает по какой-либо причине, то Event Grid продолжит повторные попытки запуска в течение 24 часов. Event Grid также чрезвычайно эффективна с точки зрения затрат. Первые 100 000 операций в месяц бесплатны, и после этого вы платите 60 центов за каждый миллион операций.

Azure DevOps

Отслеживание работы может быть сложной задачей, особенно если работа делегируется отдельным сотрудникам в многочисленной команде. При возникновении сложностей, возникающих тогда, когда команда разрабатывает непростое приложение (или даже простое), и проблемы могут вырасти в геометрической прогрессии. Azure DevOps предлагает набор инструментов, которые значительно упрощают планирование, отслеживание и управление подобными проектами.

Azure DevOps состоит из нескольких служб, которые помогают в работе, таких как:

- **Azure Boards** – это визуальный способ управления и отслеживания работы команды с помощью карточек, отображаемых в интерфейсе с поддержкой перетаскивания объектов мышью;
- **Azure Repos** – управление исходным кодом и версиями с использованием либо системы управления версиями Team Foundation, либо Git;
- **Azure Pipelines** – управление релизами ПО с помощью автоматизации сборки, тестирования и выпуска;
- **Azure Test Plans** – создают и отслеживают тесты для обеспечения надежных релизов программного обеспечения;
- **Azure Artifacts** – используют популярные каналы пакетов как из общедоступных, так и из частных источников.

Azure Boards позволяют легко отслеживать и управлять не только релизами программного обеспечения, но и практически любым проектом, связанным с работой. Вы можете без труда создавать новые задачи одним щелчком, и у вас есть возможность гибкой настройки внешнего вида плитки каждой задачи на основе мощных правил форматирования. На рис. 3.48 показан простой проект Azure Boards, который я создал для отслеживания работы, которую выполнял во время написания этой книги.

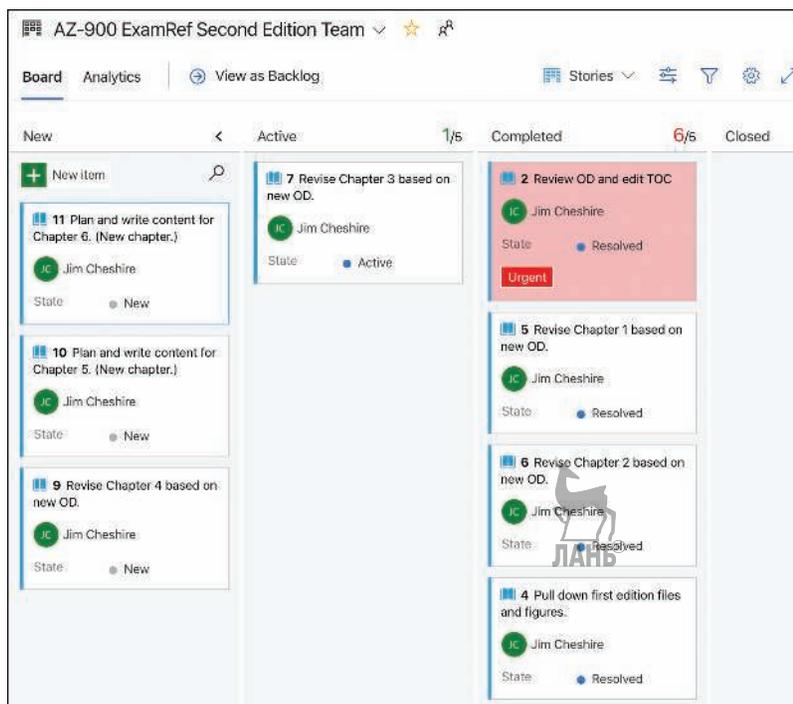


Рис. 3.48 Azure Boards, показывающие отслеживание простого проекта

Каждая плитка в Azure Boards поддерживается рабочим элементом DevOps, который включает в себя больше деталей. При открытии плитки отображается базовый рабочий элемент, как показано на рис. 3.49.

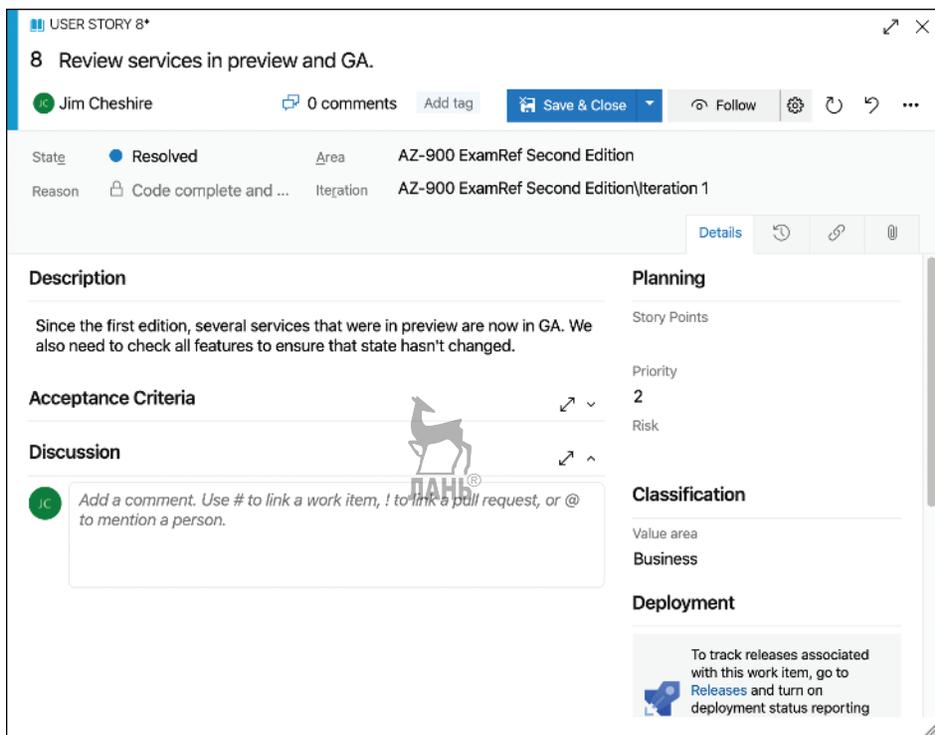


Рис. 3.49 Рабочий элемент для плитки в Azure Boards

Azure Repos (Репозитории Azure) предоставляют исходный код и управленческие версиями для группы разработчиков, использующих Git (решение с открытым исходным кодом для системы управления версиями) или Team Foundation Version Control (TFVC). У разработчиков, применяющих Git, будут отображаться все версии файлов репозитория на локальных компьютерах, и им будет также доступна история каждого изменения. У разработчиков, использующих TFVC, будет только одна версия файла на компьютере, а все остальное будет расположено на сервере.

Стандартное приложение, над которым может работать команда, состоит из тысячи файлов, содержащих исходный код. По мере хода развития приложения разработчики будут работать над изменениями этих файлов с помощью нового кода с изменением существующего. Система управления версиями позволяет команде разработчиков отслеживать все изменения, и если изменение вызовет проблему, без труда можно будет откатить эти изменения, даже если они затрагивают большое количество исходных файлов.

Бывает также, что разработчикам нужно усовершенствовать текущее приложение добавлением новых функций, но при этом им важно оставить прежний код. Системы управления версиями позволяют команде работать над новой функциональностью отдельно от существующего источника, и, будучи уверенными в правильной работе и готовыми включить новую функцию, разработчики могут включить ее в исходную версию.

На рис. 3.50 файлы проекта разработки показаны в репозиториях Azure. Исходный файл открыт, и исходный файл виден. Поскольку была нажата **History** (История) в верхней части представления источника, то можно увидеть все изменения. При нажатии **Compare** (Сравнить) отображается представление, демонстрирующее различия между двумя версиями.

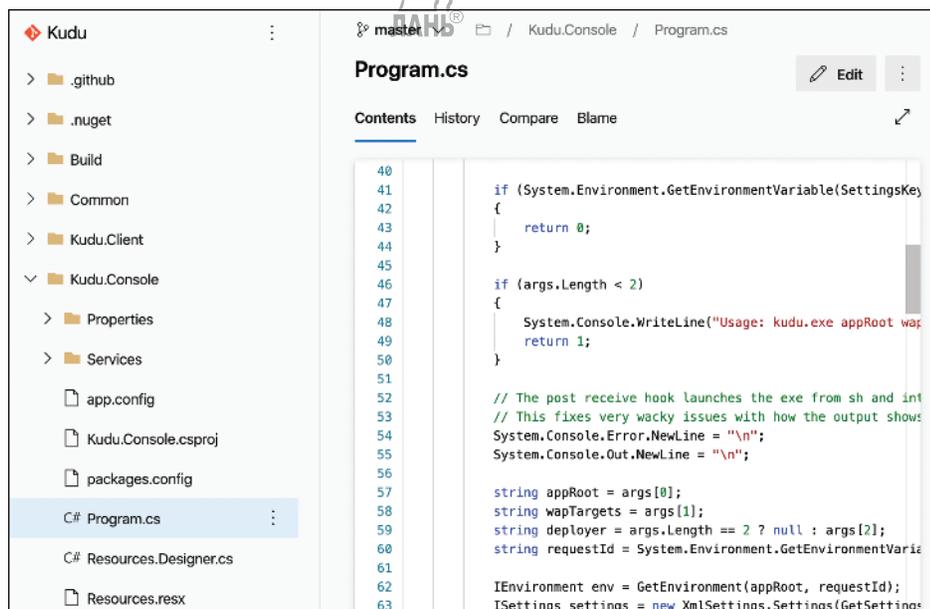


Рис. 3.50 Репозиторий в Azure Repos с содержимым исходного файла

Azure Pipelines представляют собой службы непрерывной интеграции и развертывания для проектов. Вы можете настроить Azure Pipelines для автоматической интеграции изменений в исходный код и создания новой сборки программного обеспечения для развертывания. Вы также можете настроить процесс сборки таким образом, чтобы тесты запускались сразу же после завершения сборки, что позволит вам находить проблемы до того, как их обнаружит пользователь.

Azure Test Plans (Планы тестирования Azure) предоставляют функции, упрощающие тестирование программного обеспечения на наличие проблем. Разработчики могут создавать сложные тесты, которые зачастую основаны на рабочих элементах, содержащих сведения об ошибке в ПО. После создания теста его можно запустить в Azure Test Plans из веб-браузера, поэтому тесты могут запускаться на любом устройстве.

Многие программные приложения используют упакованные компоненты от третьих сторон или из собственной организации. Эти упакованные компоненты часто называют *артефактами*, и артефакты Azure (Azure Artifacts) предоставляют простой способ их упорядочения. Azure Artifacts также предоставляют возможность интеграции этих пакетов в процесс сборки, включая сборки, которые выполняются в Azure Pipelines.

Azure DevTest Labs

Когда мы рассматривали Azure DevOps, мы затронули понятие тестирования. Стандартный тестовый сценарий может включать в себя создание разработчиков VM для запуска средств тестирования и разработки. Разработчику может также потребоваться настройка VM с различными пакетами, необходимыми для запуска тестируемого приложения. В более сложных сценариях приложению может потребоваться множество VM с соответствующими конфигурациями.

Создание разработчиками виртуальных машин для тестирования несет в себе следующие недостатки. Во-первых, ручное создание VM может занять довольно много времени, особенно если разработчику нужно установить обязательные пакеты на данную VM. Во-вторых, компания может дорого заплатить разработчику за создание более мощной VM или понести убытки, если разработчик допустит ошибку, оставив или удалив VM после тестирования.

Azure DevTest Labs прекрасно справляется с двумя этими проблемами и добавляет немало других функций, которые будут полезны как разработчикам, так и ИТ-отделам. VM могут создаваться в DevTest Lab, которые предварительно будут настроены для определенных целей. Когда разработчикам необходимо использовать VM для тестирования, они просто просматривают список доступных VM и выбирают нужную VM. Затем эта VM выделяется им до тех пор, пока ее не освободят. Утверждение VM занимает все несколько секунд, потому что VM не нужно создавать снова, когда ее уже утвердили.

На рис. 3.51 показано быстрое и легкое создание DevTest Lab. Вы просто даете название своей лаборатории, выбираете группу ресурсов (Resource Group) и указываете несколько параметров. Обычно DevTest Lab создается ИТ-отделом, ведущим разработчиком или ответственным за конкретный проект.

После создания DevTest Lab в ней нужно будет создать еще VM, чтобы разработчики могли их использовать для тестирования. Для создания VM нажмите кнопку **Add** (Добавить), как показано на рис. 3.52.

При добавлении VM в DevTest Lab сначала выбирается база для нее. Основой может послужить шаблон VM из Azure Marketplace или других источников. Это также может быть VM, которая изначально настроена для конкретного проекта и сохранена в виде *формулы* или *пользовательского образа*. Мы рассмотрим их подробнее далее в этом разделе.

На рис. 3.53 показано создание VM, которая использует базовый образ центра обработки данных Windows Server 2016. Вы можете создать VM только с установленным базовым образом, в который также сами можете добавить дополнительные компоненты путем добавления *артефакта*. Как уже ранее говорилось, связанные с Azure DevOps артефакты – это упакованные компоненты, которые могут потребоваться для определенной конфигурации. Вы можете добавить их в VM, нажав **Add Or Remove Artifacts** (Добавить или удалить артефакты) в нижней части экрана, как показано на рис. 3.53.

Create a DevTest Lab

Lab name *
AZ900Lab ✓

Subscription *
Jim's MSDN Subscription ▼

Resource group * ⓘ
 Create new Use existing
 AZ900 ▼

Location *
South Central US ▼

Auto-shutdown
Enabled >

Public environments ⓘ
 On Off

ⓘ Lab policies don't apply to lab environments. Click here for more information.

Tags

Name	Value
<input type="text"/>	<input type="text"/>

Create [Automation options](#)

Рис. 3.51 Создание DevTest Lab на портале Azure

AZ900Lab
DevTest Lab

Search (Cmd+Z) 🔍

Refresh **Add** Claim any Delete MSDN forum Feedback

Resource group [\(change\)](#)
AZ900

Status
Ready

Location
South Central US

Subscription [\(change\)](#)
Jim's MSDN Subscription

Subscription ID
2ed0e6a0-aaf7-4f5f-aff6-bf25ffdef188

My virtual machines

Name	Status	Auto-start	Auto-shutdown	Base
Nothing to display				

Рис. 3.52 Нажмите **Add** (Добавить), чтобы добавить новую VM в DevTest Lab

Рис. 3.53 Добавление новой VM в DevTest Lab

ДОПОЛНИТЕЛЬНО ДОБАВЛЕНИЕ VM

Как правило, IT-отделы или ведущие разработчики создают VM для DevTest Lab. При необходимости разработчики, работающие в команде, смогут выбрать одну из добавленных в DevTest Lab VM.

Крайне важно осознавать, что созданная в DevTest Labs VM по умолчанию предназначена для одного пользователя и не подлежит утверждению. Если вы создаете VM, которой бы вам хотелось поделиться с другими пользователями, то для этого вам нужно нажать **Advanced Settings** (Расширенные настройки) в верхней части экрана, показанного на рис. 3.53, и настроить машину так, чтобы другие пользователи могли ее использовать (рис. 3.54).



СОВЕТ К ЭКЗАМЕНУ

Добавление существующей VM в DevTest Lab – не совсем простой процесс. Чтобы сделать это, вам нужно постараться скопировать VHD-образ VM в контейнер хранилища Azure, который используется DevTest Lab, и затем создать новую VM из пользовательского образа.

Create lab resource
Virtual machine

Basic Settings **Advanced Settings**

Network Settings

Virtual network * DtlAZ900Lab

Subnet Selector * DtlAZ900LabSubnet

IP address Public Private **Shared**

Virtual machine expiration

Expiration date Will not expire h:mm:ss A
Central Daylight Time

Claim options

Make this machine claimable Yes No

Number of instances 1

Automation

[View ARM template](#)

Рис. 3.54 Настройка VM с доступом для других пользователей

Иногда базовые изображения не содержат нужную вам конфигурацию, даже с учетом добавленных артефактов. Например, у вас может быть свой пакет программного обеспечения, используемый в компании, который вы хотели бы включить в образ VM, или у вас может быть определенная конфигурация ОС, необходимая для вашей VM. В этих случаях вы можете создать пользовательский образ или формулу, на основе которых будут создаваться ваши новые VM.

Пользовательские образы и формулы похожи, но есть одно ключевое отличие между ними. Пользовательский образ – это образ, основанный на виртуальном жестком диске существующей VM. В основе формулы также лежит виртуальный жесткий диск, но формула содержит параметры, характерные для DevTest Labs: размер VM, включенные артефакты и т. д. Однако формула часто использует пользовательский образ в качестве основы.

ДОПОЛНИТЕЛЬНО СОЗДАНИЕ ПОЛЬЗОВАТЕЛЬСКИХ ОБРАЗОВ И ФОРМУЛ

Одной из причин, по которой вы можете создать невостребованную VM, является то, что вы настраиваете ее с помощью определенных параметров и программного обеспечения, а затем сохраняете ее как пользовательский образ или формулу для применения другими пользователями.

Чтобы создать пользовательский образ, настройте VM, как вам необходимо, а затем выберите ее из списка VM в DevTest Lab. Нажмите кнопку **Create Custom Image** (Создать пользовательский образ) и заполните поля, как показано на рис. 3.55.

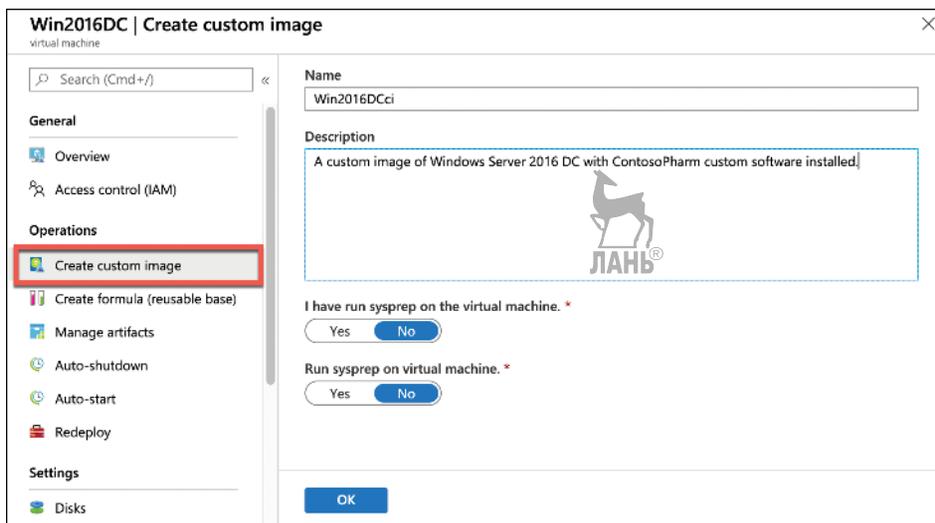


Рис. 3.55 Создание пользовательского образа в DevTest Labs

Нажав кнопку **ОК** для создания пользовательского образа, вам нужно будет какое-то время подождать, пока образ станет доступным в качестве основы для других ВМ.

Чтобы создать формулу, нажмите **Formulas** (Формулы) в меню, показанном на рис. 3.52, а затем нажмите кнопку **Add** (Добавить), чтобы создать новую формулу. Выберите основу для своей формулы. На рис. 3.56 первый базовый образ в списке – это пользовательский образ, созданный ранее из ВМ в DevTest Lab.

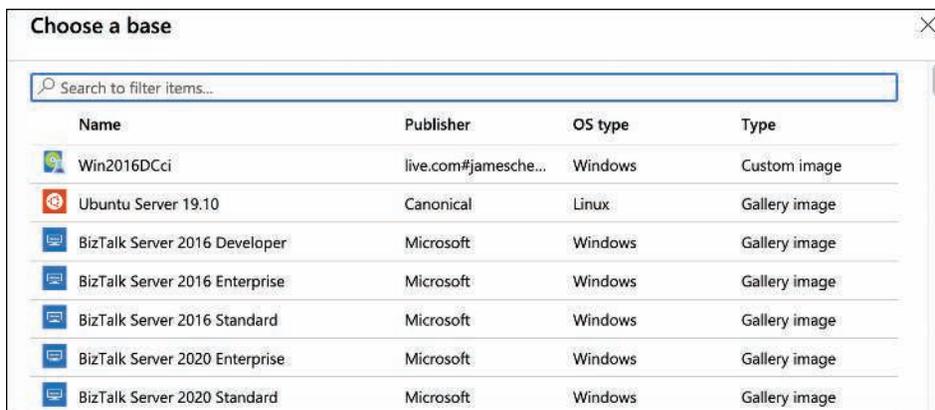


Рис. 3.56 Выбор базового образа для формулы

После того как основа для формулы выбрана, можно настроить желаемые параметры DevTest Lab, как показано на рис. 3.57. На ВМ, созданных с помощью этой формулы, эти параметры будут заранее настроены.

Create formula (reusable base)

Create a formula to capture the settings used to create this virtual machine.

Basic Settings Advanced Settings

User Settings

Formula name ✓

Description ✓

Disk and Size

Virtual machine size ⓘ

Size

Standard_A3

[Change Size](#)

OS disk type ⓘ ▼

Artifacts

Artifacts Selection

Artifact

0 artifact(s) selected

[Add or Remove Artifacts](#)

[Create formula](#)

Рис. 3.57 Указание настроек для формулы DevTest Lab

Другой экономичной функцией DevTest Labs является свойство автоматического выключения ВМ. По умолчанию все ВМ создаются с включенным автоматическим отключением, и это означает, что по истечении определенного периода времени неиспользуемые ВМ отключаются, так что вам не нужно будет за них платить.

IT-администраторы или другие пользователи также могут определять политики в DevTest Labs. Эти политики позволяют управлять размерами создаваемых ВМ, их количеством на пользователя и на лабораторию и т. д. Чтобы настроить политики, выберите **Configuration And Policies** (Конфигурация и политики) в меню вашей DevTest Lab.

Политики можно настроить, выбрав нужную в меню, а затем настроив ее. На рис. 3.58 показана настройка политики, ограничивающей доступные размеры ВМ: Standard_A0, Standard_A1 и Standard_A2. В сохраненной политике пользователи не смогут создавать ВМ других размеров.



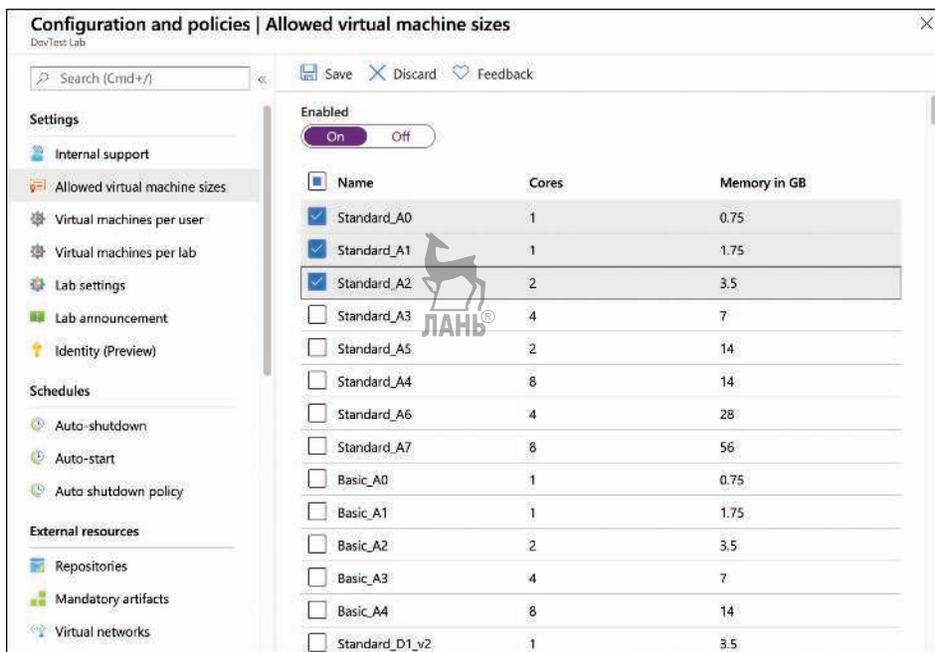


Рис. 3.58 Конфигурация политики для допустимых размеров виртуальной машины

Навык 3.2: описание средств управления Azure

Мы много обсуждали портал Azure ранее, и вы уже использовали его при взаимодействии с несколькими службами Azure. Однако существуют и другие способы создания и управления службами Azure.

Многие пользователи Azure создают сценарии взаимодействия со своими службами Azure, особенно когда требуется взаимодействие с несколькими ВМ или другими ресурсами Azure. Для этого Azure предлагает средства командной строки.

Пользователям Azure также необходимо убедиться, что они получают максимальную отдачу от своих служб Azure, а такие инструменты, как Azure Advisor и Azure Monitor, помогают информировать пользователей о последних событиях в соответствии с лучшим опытом Azure, а также способствуют тому, чтобы у пользователей была информация по тому, как работают их ресурсы Azure. При возникновении проблемы служба работоспособности Azure (Azure Service Health) также помогает определить причину возникновения проблемы: связана ли она с приложением или же с самим Azure.

Содержание раздела:

- портал Azure;
- Azure PowerShell;
- интерфейс командной строки Azure (Azure CLI);
- Azure Cloud Shell;
- Azure Mobile app;
- Azure Advisor;
- Azure Monitor;
- Azure Service Health.

Портал Azure (Azure Portal)

Портал Azure, который используется сегодня, является третьей итерацией портала Azure, и это произошло, когда Microsoft перешла на ARM. Все, что вы делаете в портале Azure, реализуется с помощью ARM.



СОВЕТ К ЭКЗАМЕНУ

Для экзамена AZ-900 вам, вероятно, не нужно знать, что портал Azure просто делает вызовы ARM на бэкенде, но знать об этом не помешает. Однако для остальной части этого раздела мы рассмотрим только различные части портала, а также способы навигации и настройки его. Эта информация необходима для экзамена AZ-900.

При первом открытии портала Azure вам будет предложено совершить экскурсию по portalу. Если вы еще незнакомы с порталом, то экскурсия позволит вам узнать, как он работает. Если вы решите этого не делать, то позже можете щелкнуть вопросительный знак на верхней панели инструментов, чтобы получить доступ к экскурсии в любое время.

По умолчанию на портале отображается домашняя страница (Home), как показано на рис. 3.59. Здесь вы можете увидеть значки для различных служб Azure, и если вы нажмете на один из этих значков, то он покажет вам любые ресурсы этого типа, которые вы создали. Меню слева содержит те же значки и многое другое.

Если у вас уже имеются созданные ресурсы Azure, то вы без труда сможете к ним перейти, нажав одну из ссылок в разделе **Navigate** (Навигация). Если вы недавно просматривали свой ресурс, то вы увидите другой раздел с вашими недавно доступными ресурсами, так что можете легко получить к ним доступ, снова нажав на них.

Вдоль верхней цветной панели вы найдете строку поиска, где можно искать службы Azure, документы или ресурсы Azure. Справа от поля поиска расположена кнопка, которая запускает Azure Cloud Shell. Cloud Shell – это веб-оболочка, в которой можно взаимодействовать с Azure из командной строки. Вы можете создавать ресурсы Azure и многое другое. Когда вы читаете документацию Azure, то можете увидеть кнопку **Try** (Попробовать), и эти кнопки используют **Cloud Shell**, чтобы помочь вам протестировать различные службы и функции.

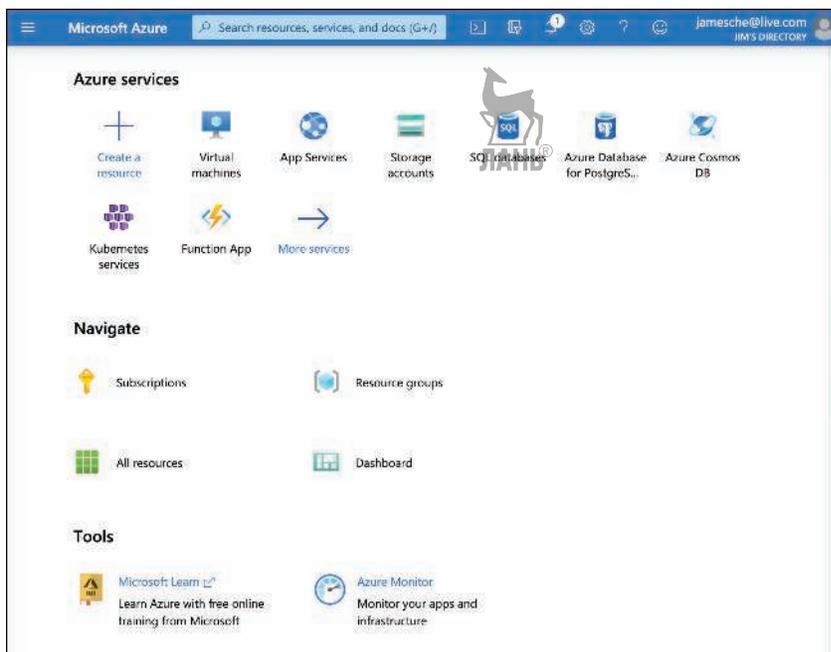


Рис. 3.59 Главный экран портала Azure

Справа от кнопки **Cloud Shell** расположена кнопка фильтра, позволяющая настроить портал на отображение ресурсов только в определенной подписке Azure или Azure Active Directory. Справа от этого находится кнопка **Notification** (Уведомления). Здесь вы увидите уведомления от Azure, связанные с вашей службой и подпиской.

Справа от кнопки уведомлений находится кнопка **Settings** (Настройки). При нажатии на нее откроется панель, в которой можно изменить настройки портала, как показано на рис. 3.60.

В разделе **Settings** (Настройки) можно изменить вид по умолчанию, цветовую схему портала, отключить всплывающие уведомления или уведомления, которые Microsoft может отображать вам время от времени. Также предоставляются ссылки, позволяющие восстановить стандартные настройки, экспортировать настройки или удалить их вместе с панелью мониторинга. (Мы поговорим о панелях мониторинга далее.)

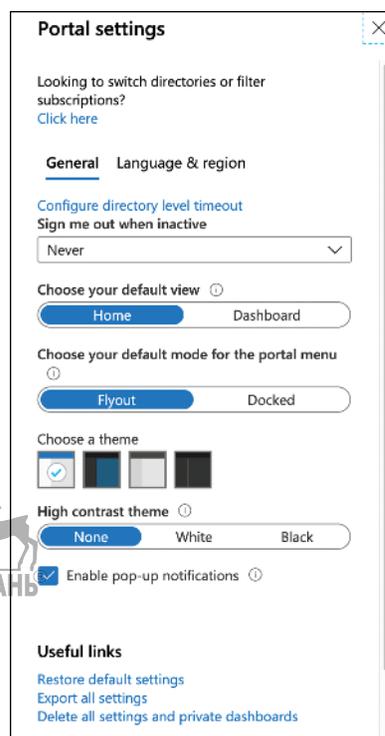


Рис. 3.60 Настройки портала

Если щелкнуть на ваше имя в правом верхнем углу (показано на рис. 3.59), то можно выйти из системы или переключиться на другие учетные записи Azure. Можно также изменить учетную запись Azure Active Directory для доступа к ресурсам в другом каталоге. Это полезно, если ваша компания имеет корпоративный каталог и у вас также есть личный каталог.

ДОПОЛНИТЕЛЬНО AZURE ACTIVE DIRECTORY

Azure Active Directory будет рассмотрено в разделе «Навык 5.1» главы 5.

Меню слева от портала содержит список ресурсов Azure по умолчанию. При нажатии на один из них будут отображены все ресурсы этого типа. Если вы не нашли службу в списке, которую вы хотите добавить, щелкните **All Services** (Все службы), найдите нужную и щелкните на звездочке справа от нее, чтобы пометить ее как избранную, как показано на рис. 3.61.

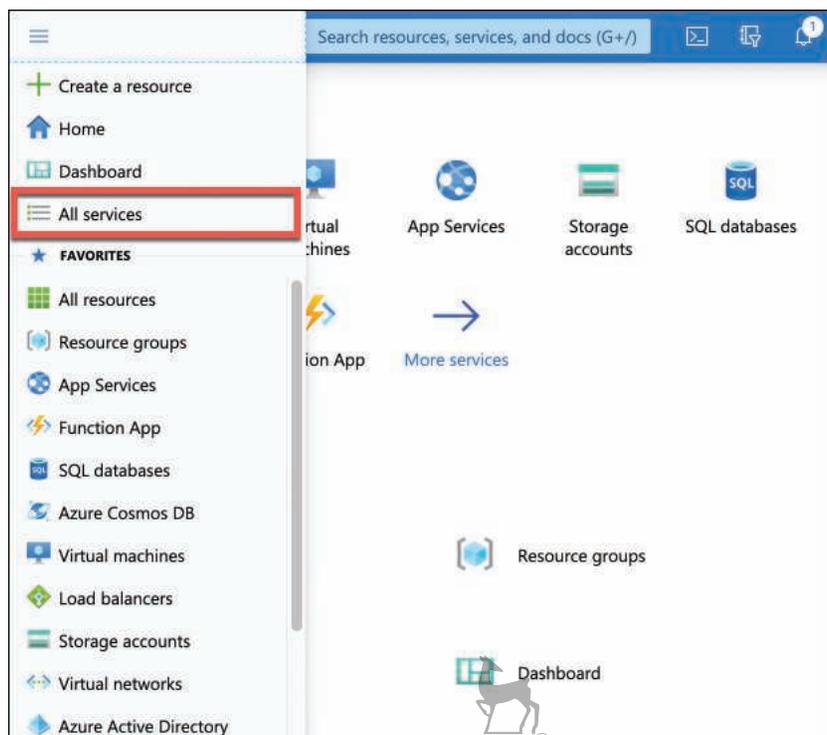


Рис. 3.61 Меню портала Azure, отображающее пункт меню **All Services**

ПРИМЕЧАНИЕ ПЕРЕМЕЩЕНИЕ ПУНКТОВ МЕНЮ

Вы можете изменить порядок пунктов в меню. Нажмите и удерживайте элемент и перетащите его в новое место в меню.

В списке служб Azure найдите службу, которую вы хотите добавить в список, и нажмите звездочку справа от службы, чтобы пометить ее как избранную (см. рис. 3.62).

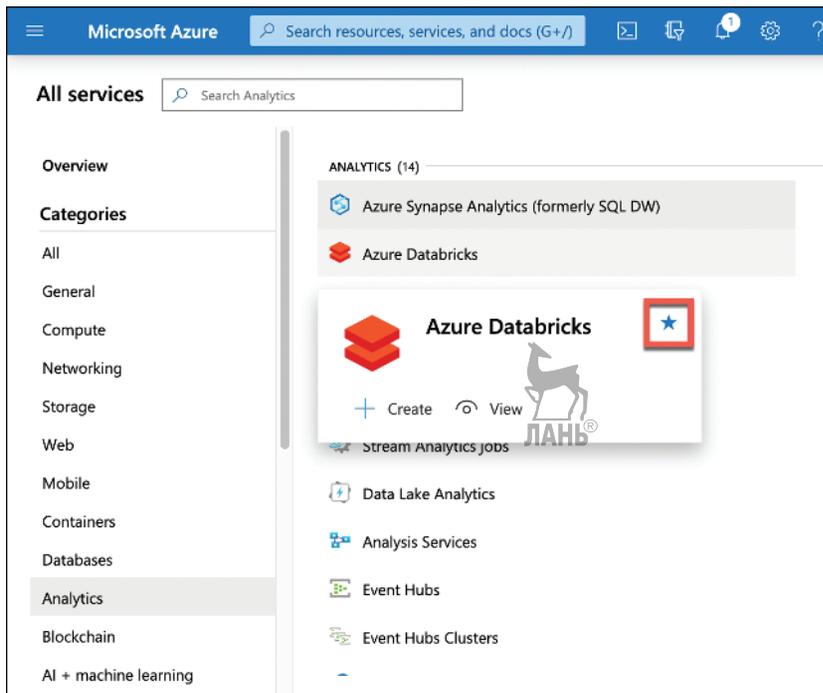


Рис. 3.62 Отметить службу Azure как избранную для ее отображения в главном меню

На рис. 3.63 мы нажали кнопку **App Service Plans** (Планы службы приложений) в меню, чтобы увидеть все планы. Из этого списка вы можете увидеть ресурс, нажав на него. Вы также можете щелкнуть на заголовке столбца для сортировки по нему, предполагая, что у вас есть несколько ресурсов этого типа. Нажмите **Manage View** (Управление видом), чтобы отредактировать отображаемые столбцы, сохранить текущее представление и многое другое. Чтобы создать новый ресурс такого типа, нажмите кнопку **Add** (Добавить).

Когда вы нажмете на определенный ресурс, он откроется на портале. Вдоль левой стороны будет меню, специфичное для типа ресурса, который вы открыли. В главном окне вы увидите различные элементы в зависимости от типа просматриваемого ресурса. Эти области на портале часто называются блейдами (blades).

На рис. 3.64 вы увидите приложение App Service Web App на портале. Блейд **Overview** (Обзор) является общим для большинства ресурсов Azure, но отображаемая там информация будет отличаться в зависимости от ресурса. В веб-приложении вы можете увидеть группу ресурсов, в которой она находится, статус, регион и многое другое. В правом верхнем углу этих плиток находится кнопка прикрепления (pin). Если вы нажмете на эту кнопку, она добавит плитку на панель мониторинга портала.

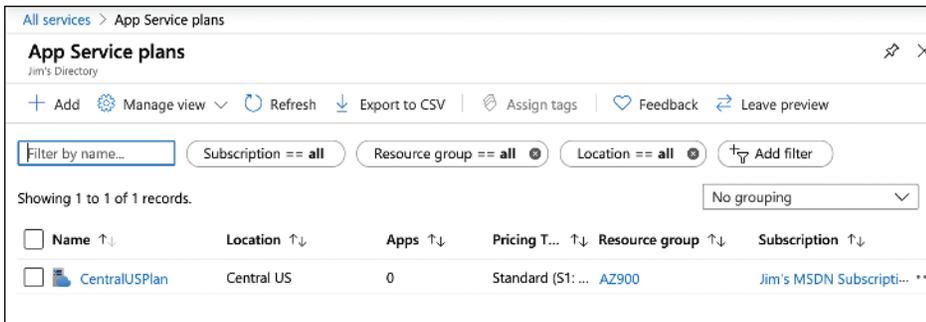


Рис. 3.63 Просмотр плана службы приложений на портале

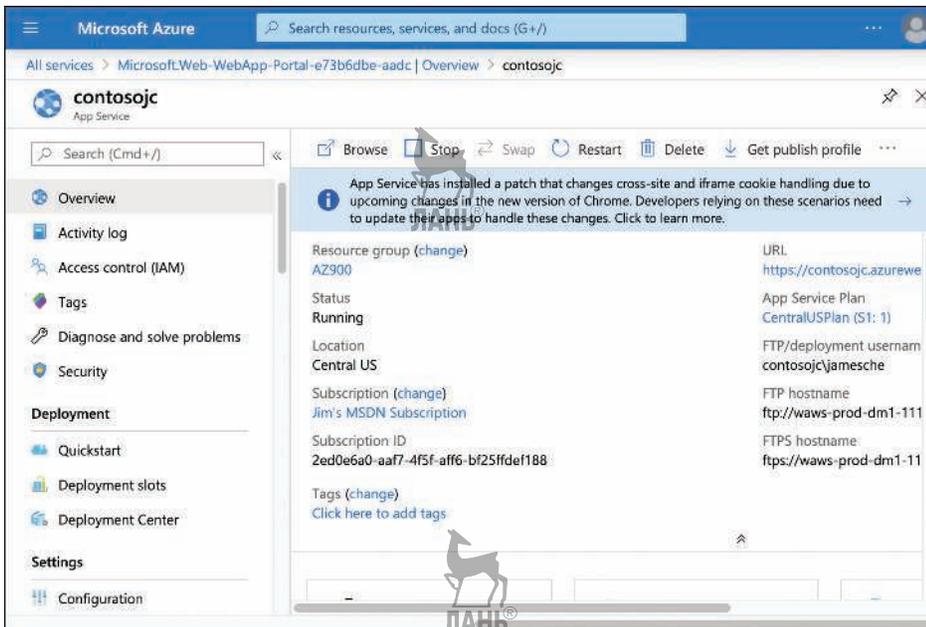


Рис. 3.64 Просмотр веб-приложения на портале

Вдоль верхней части лезвия для веб-приложения расположены несколько кнопок для взаимодействия с ресурсом. Для веб-приложения у вас есть кнопка **Browse** (Обзор), которая откроет приложение в браузере, кнопка **Stop** (Стоп) для остановки приложения, кнопка **Swap** (Поменять) для изменения слотов развертывания и т. д. Каждый тип ресурсов будет иметь различные кнопки, чтобы вы могли легко взаимодействовать с ресурсом из блейда **Overview** (Обзор).

Если нажать на элемент в меню слева, содержимое из блейда **Overview** (Обзор) заменится выбранным новым элементом. На рис. 3.65 мы нажали кнопку **Diagnose And Solve Problems** (Диагностика и решение проблем), которая заменяет блейд **Overview** (Обзор) новым содержимым из блейда **Diagnose And Solve Problems** (Диагностика и решение проблем).

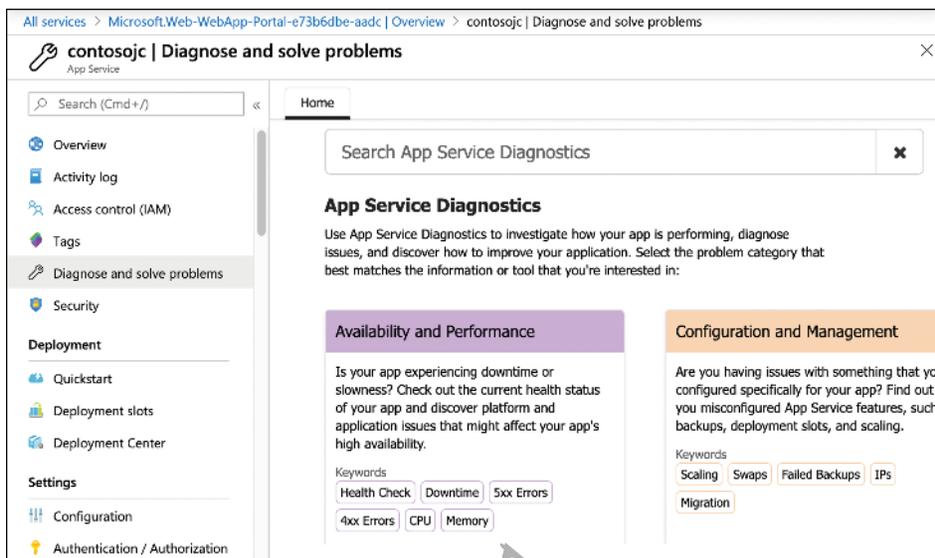


Рис. 3.65 Новый блейд

При использовании портала вы обнаружите, что между различными сервисами существует несоответствие. У каждой команды Microsoft есть своя подгруппа по разработке портала, и они, как правило, разрабатывают интерфейсы портала, которые имеют смысл для их собственной команды. По этой причине вы можете видеть кнопки сверху в одних блейдах и кнопки снизу в других.

Вы можете настроить работу портала с помощью панели мониторинга. Если вы нажмете **Dashboard** (Панель мониторинга) на начальном экране, то увидите панель мониторинга по умолчанию. При управлении ресурсами нажмите на **pin** (булавка), чтобы закрепить плитки на панели мониторинга (как показано на рис. 3.64). Затем можно перемещать эти плитки и настраивать их разными способами, чтобы создать уникальный вид, отвечающий вашим потребностям.

Для настройки панели мониторинга щелкните **Dashboard** (Панель мониторинга) в меню, чтобы отобразить ее, а затем нажмите кнопку **Edit** (Изменить), как показано на рис. 3.66.

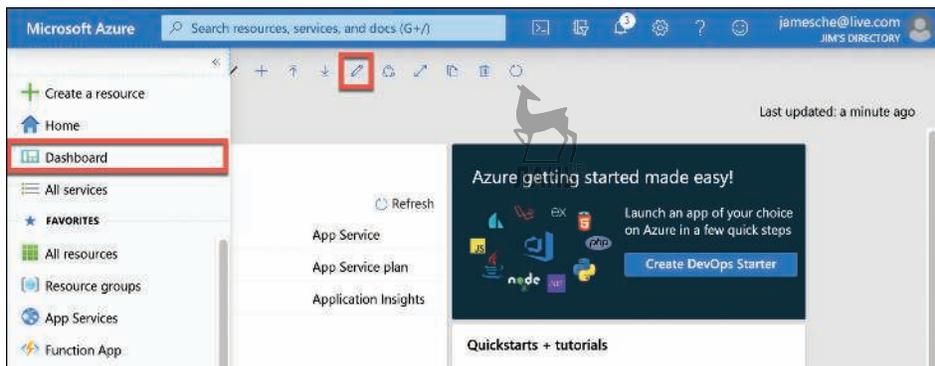


Рис. 3.66 Редактирование панели мониторинга

На экране настройки, показанном на рис. 3.67, можно изменить название панели мониторинга, щелкнув на текущее имя и изменив его на новое. Вы можете добавить плитки на панель мониторинга, выбрав одну из сотен плиток, доступных в галерее в левой части портала. При необходимости можете выполнить поиск и отфильтровать список. Если вы наведете курсор на существующую плитку, то увидите кнопку **Delete** (Удалить) и кнопку меню, представленную тремя точками. Нажмите на кнопку **Delete** (Удалить), чтобы удалить плитку с панели мониторинга. Нажмите кнопку меню, чтобы открыть контекстное меню, в котором можно изменить размер плитки.

Когда панель мониторинга вас устроит, нажмите на **Done Customizing** (Завершить настройку), чтобы закрыть экран настроек.

Вы можете создать новые панели мониторинга для определенных целей, щелкнув на значке «плюс» (показанном на рис. 3.66) рядом с названием панели мониторинга. Это действие приведет вас на экран настройки новой панели мониторинга, как показано на рис. 3.67.

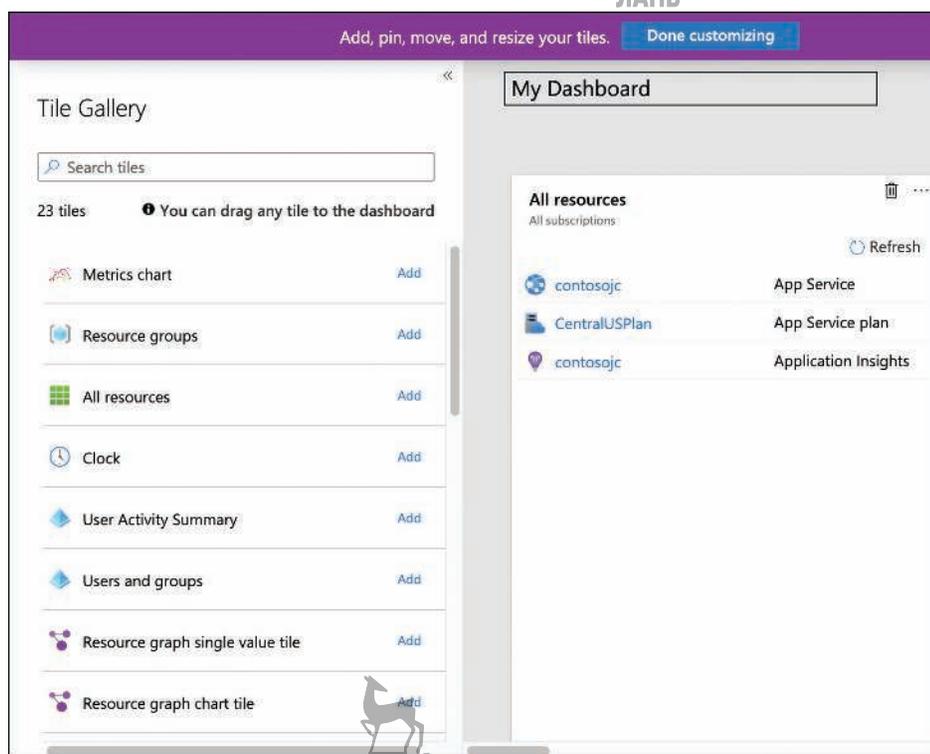


Рис. 3.67 Настройка панели мониторинга

На рис. 3.68 мы создали панель мониторинга для веб-приложений. Вы можете легко переключаться между этой панелью мониторинга и панелью по умолчанию, щелкнув стрелку вниз рядом с названием панели мониторинга.

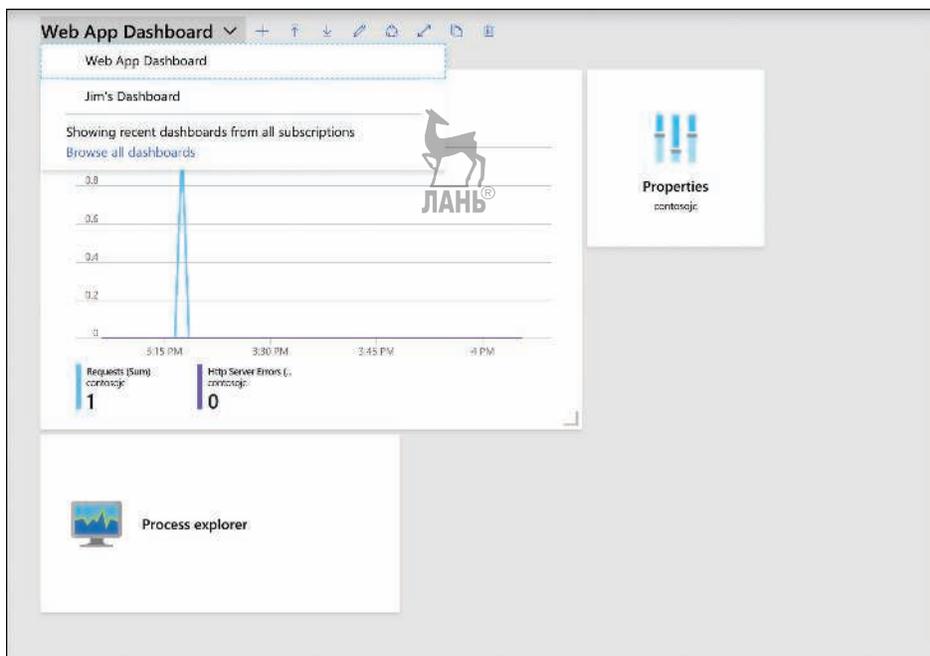


Рис. 3.68 Переключение между панелями мониторинга

Azure и PowerShell

Если вы являетесь пользователем PowerShell, то можете воспользоваться этими знаниями для управления ресурсами Azure с помощью модуля Azure PowerShell Az. Этот модуль обеспечивает кросс-платформенную поддержку, поэтому независимо от того, используете ли вы Windows, Linux или macOS, вы можете использовать модуль PowerShell Az.

ДОПОЛНИТЕЛЬНО AZURERM И AZ

Модуль PowerShell Az является относительно новым. До этого все команды PowerShell использовали модуль AzureRm. Команды, используемые с обоими модулями, идентичны. Единственное отличие – это имя модуля.

ДОПОЛНИТЕЛЬНО УСТАНОВКА POWERSHELL НА LINUX ИЛИ MACOS

Если вы используете Linux, то можете найти подробную информацию об установке PowerShell по адресу <https://bit.ly/az900-powershellonlinux>. Пользователи macOS могут найти пошаговую инструкцию по адресу <https://bit.ly/az900-powershellonmac>.

Прежде чем использовать модуль PowerShell Az, его необходимо установить. Для этого сначала нужно запустить PowerShell с повышенными правами. В Windows это означает запуск его от имени администратора. В Linux и macOS вам нужно запустить его с привилегиями суперпользователя, используя Sudo.



СОВЕТ К ЭКЗАМЕНУ

Модуль PowerShell Az использует библиотеку .NET Standard для своей работы, что означает, что он будет работать с PowerShell версии 5.x или 6.x. PowerShell 6.x является кросс-платформенным и может работать в Windows, Linux или macOS.

Если вы используете Windows 7 или более поздние версии и PowerShell 5.x, то вам также необходимо установить .NET Framework 4.7.2.

Чтобы установить модуль, выполните следующую команду:

```
Install-Module -Name Az -AllowClobber
```

При установке нового модуля PowerShell проверяет все существующие модули на предмет наличия имен команд, совпадающих с именем команды в новом модуле. Если будут найдены совпадения, то установка нового модуля завершится неудачей. Указывая *-AllowClobber*, вы сообщаете PowerShell, что модуль Az может иметь приоритет для любых команд, которые существуют в других модулях.

Если не удастся запустить PowerShell с повышенными правами, можно установить модуль для пользователя только с помощью следующей команды:

```
Install-Module -Name Az -AllowClobber -Scope CurrentUser
```

После установки модуля необходимо выполнить вход с учетной записью Azure. Для этого выполните следующую команду:

```
Connect-AzAccount
```

Эта команда отобразит токен в окне PowerShell. Вам нужно будет перейти на <https://microsoft.com/devicelogin> и ввести код, чтобы удостоверить подлинность сеанса PowerShell. Если вы закроете PowerShell, вам придется снова запустить команду в следующем сеансе.

ДОПОЛНИТЕЛЬНО СОХРАНЕНИЕ УЧЕТНЫХ ДАННЫХ

Можно настроить PowerShell для сохранения учетных данных. Дополнительную информацию об этом см. по адресу: <https://docs.microsoft.com/powershell/azure/context-persistence>.

Если у вас несколько подписок Azure, то необходимо настроить активную подписку так, чтобы введенные команды повлияли на желаемую подписку. Вы можете сделать это с помощью следующей команды:

```
Set-AzContext -Subscription «subscription»
```

Замените *subscription* на имя или идентификатор подписки Azure, которую вы хотите использовать с модулем Az.

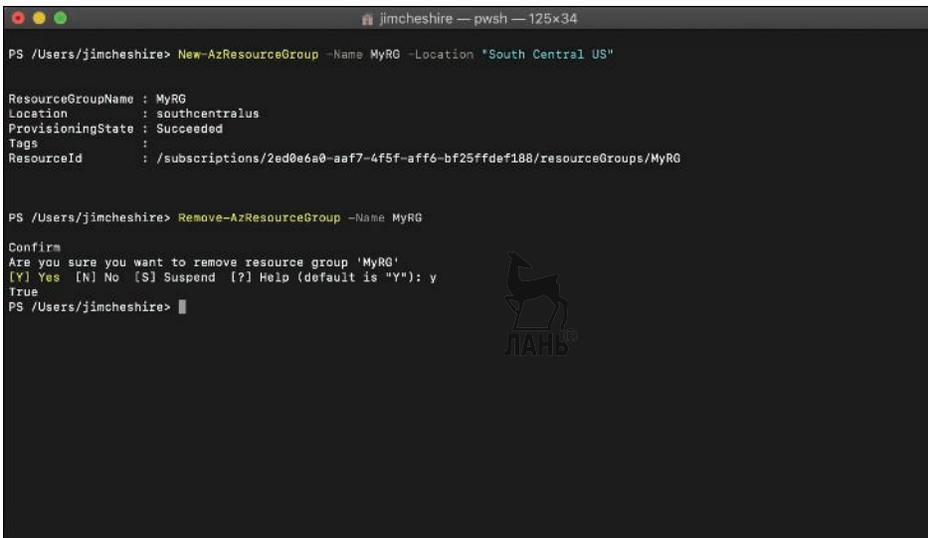
Все команды модуля Az будут иметь общий синтаксис, который начинается с глагола и объекта. Глаголы – это такие слова, как *New*, *Get*, *Move* или *Remove*. Объект – это тот ресурс, на который воздействует глагол. Например, следующая команда создаст группу ресурсов *MyRG* в южно-центральной зоне США:

```
New-AzResourceGroup -Name MyRG -Location «South Central US»
```

Если это сработает, то вы увидите сообщение об успешном выполнении. Если команда не сработает по какой-либо причине, то вы увидите ошибку. Чтобы удалить группу ресурсов, выполните следующую команду.

```
Remove-AzResourceGroup -Name MyRG
```

Когда эта команда будет введена, вам будет предложено подтвердить, хотите ли вы удалить группу ресурсов. Введите у (сокр. от yes, да), и группа ресурсов будет удалена, как показано на рис. 3.69.



```
PS /Users/jimcheshire> New-AzResourceGroup -Name MyRG -Location "South Central US"

ResourceGroupName : MyRG
Location           : southcentralus
ProvisioningState  : Succeeded
Tags               :
ResourceId         : /subscriptions/2ed0e6a0-aaf7-4f5f-aff6-bf25ffdef188/resourceGroups/MyRG

PS /Users/jimcheshire> Remove-AzResourceGroup -Name MyRG

Confirm
Are you sure you want to remove resource group 'MyRG'?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
True
PS /Users/jimcheshire> █
```

Рис. 3.69 Создание и удаление группы ресурсов с помощью модуля Az

Зачастую вы будете объединять команды PowerShell в скрипт, чтобы можно было выполнять несколько операций одновременно. В этом случае вы не сможете подтвердить команду, введя у, поэтому вам будет необходимо использовать параметр *-Force* для обхода этих подтверждений. Например, можно удалить группу ресурсов с помощью следующей команды, и запрос не будет выдан.

```
Remove-AzResourceGroup -Name MyRG -Force
```

Все команды, доступные в модуле PowerShell Az, можно найти по ссылке <https://bit.ly/az900-powershellaz>. Нажмите **Reference** (Ссылки) в левом меню.

Интерфейс командной строки Azure

Как я уже отмечал ранее, одним из основных преимуществ PowerShell является возможность написания сценариев взаимодействия с ресурсами Azure. Однако если вы хотите создать скрипт с помощью PowerShell, вам понадобится

ся кто-то, кто знает PowerShell. Если у вас нет никого, кто мог бы это сделать, отличный выбор – интерфейс командной строки (command-line interface, CLI) Azure. С помощью Azure CLI можно создавать скрипты для командной строки на различных языках, таких как Python, Ruby и т. д.

Как и модуль PowerShell Az, интерфейс командной строки Azure является кросс-платформенным и работает на Windows, Linux и macOS начиная с версии 2.0. Этапы установки различаются в зависимости от платформы. Шаги для всех операционных систем можно найти по адресу: <https://bit.ly/az900-installcli>.

После установки интерфейса командной строки вам будет необходимо войти в учетную запись Azure. Для этого выполните следующую команду:

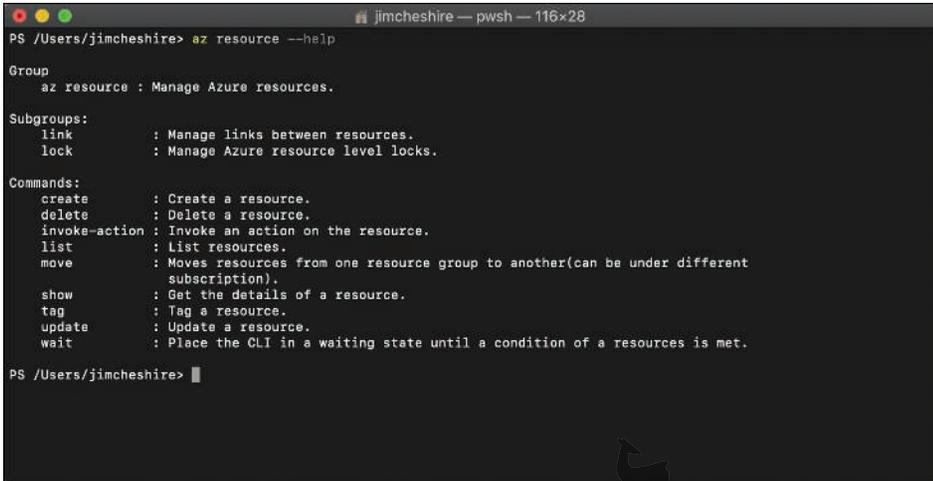
```
az login
```

При выполнении этой команды интерфейс командной строки автоматически откроет браузер для входа в систему. После входа в систему, если у вас несколько подписок Azure, вы можете указать подписку по умолчанию, введя следующую команду:

```
az account set --subscription «subscription»
```

Замените *subscription* на имя или идентификатор подписки, которые вы хотите использовать.

Чтобы просмотреть список команд, которые можно выполнить с помощью CLI, введите **az** и нажмите клавишу **Enter**. Вы увидите список всех команд, которые вы можете запустить. Подробную справку по любой команде можно найти, введя команду и добавив параметр `--help`. На рис. 3.70 отображена справочная информация *no az resource*.



```
PS /Users/jimcheshire> az resource --help
Group
  az resource : Manage Azure resources.

Subgroups:
  link       : Manage links between resources.
  lock      : Manage Azure resource level locks.

Commands:
  create    : Create a resource.
  delete    : Delete a resource.
  invoke-action : Invoke an action on the resource.
  list     : List resources.
  move     : Moves resources from one resource group to another(can be under different
            subscription).
  show     : Get the details of a resource.
  tag      : Tag a resource.
  update   : Update a resource.
  wait     : Place the CLI in a waiting state until a condition of a resources is met.

PS /Users/jimcheshire> █
```

Рис. 3.70 Справка Azure CLI

Вы можете обратиться к справке, если не уверены, что делает та или иная команда. Например, можно выполнить показанную команду, чтобы получить справку по синтаксису для *az resource create*.

```
az resource create --help
```

Команда предоставит вам справку и примеры команд для понимания синтаксиса.



СОВЕТ К ЭКЗАМЕНУ

Как и в PowerShell, большинство команд в Azure CLI имеют параметр `--force`, который можно включить, чтобы запросы на подтверждение не отображались. При написании скриптов PowerShell или CLI необходимо включить этот параметр, иначе скрипт не будет работать. Следите за примерами на экзамене AZ-900, которые проверяют такие знания.

Более простым способом изучения интерфейса командной строки является переход в интерактивный режим. Это предоставит вам возможности автоматического заполнения, области действия команд и многое другое. Для переключения в интерактивный режим введите **az interactive** в командной строке. Интерфейс командной строки установит расширение для добавления этой функции. На рис. 3.71 показан интерфейс командной строки Azure с активным интерактивным режимом. Вы ввели `we` в командной строке, и она отображает остальную часть команды в затемненном тексте. Можно нажать клавишу со стрелкой вправо, чтобы ввести затемненный текст одним нажатием клавиши.

```
az>> we app create

*
*
*

#[cmd]          : use commands outside the application
#[cmd] + [param] + "??[query]": Inject jmespath query from previous command
"??[query]"     : Jmespath query of the previous command
#[cmd] :: [num] : do a step by step tutorial of example
$              : get the exit code of the previous command
%%[cmd]        : set a scope, and scopes can be chained with spaces
%% ..         : go back a scope

[F1]Layout      [F2]Defaults  [F3]Keys       [Ctrl+D]Quit   Subscription: Jim's Personal Azure Account
```

Рис. 3.71 Интерактивный режим командной строки

Вы можете установить дополнительные расширения для новой функциональности. Поскольку интерфейс командной строки использует архитектуру расширений, команды Azure могут обеспечить поддержку новых функциональных возможностей, не дожидаясь нового выпуска CLI. Вы можете найти

список всех доступных расширений, которые Microsoft предоставляет, выполнив следующую команду:

```
az extension list-available --output table
```

Это не только отобразит вам доступные расширения, но и покажет, есть ли у вас уже установленные расширения и есть ли для них обновления. Чтобы установить расширение, выполните следующую команду:

```
az extension add --name extension_name
```

Замените *extension_name* на имя расширения, которое вы хотите установить.

Azure Cloud Shell

Мы с вами убедились, что доступ командной строки к ресурсам Azure при помощи PowerShell и Azure CLI является мощным и гибким решением. Мы также узнали, что можно установить расширения для увеличения мощности командной строки. Однако если вы используете более одного компьютера, то вам потребуется установка данных расширений на каждом из них. Необязательно запускать их на телефоне или планшете, когда рядом нет компьютера.

Единственным решением этих проблем является предоставление вам средства командной строки в облаке. Это именно то, что сделала Microsoft, предоставив Azure Cloud Shell.

Чтобы получить доступ к Cloud Shell, нажмите кнопку **Cloud Shell** на портале Azure, как показано на рис. 3.72.

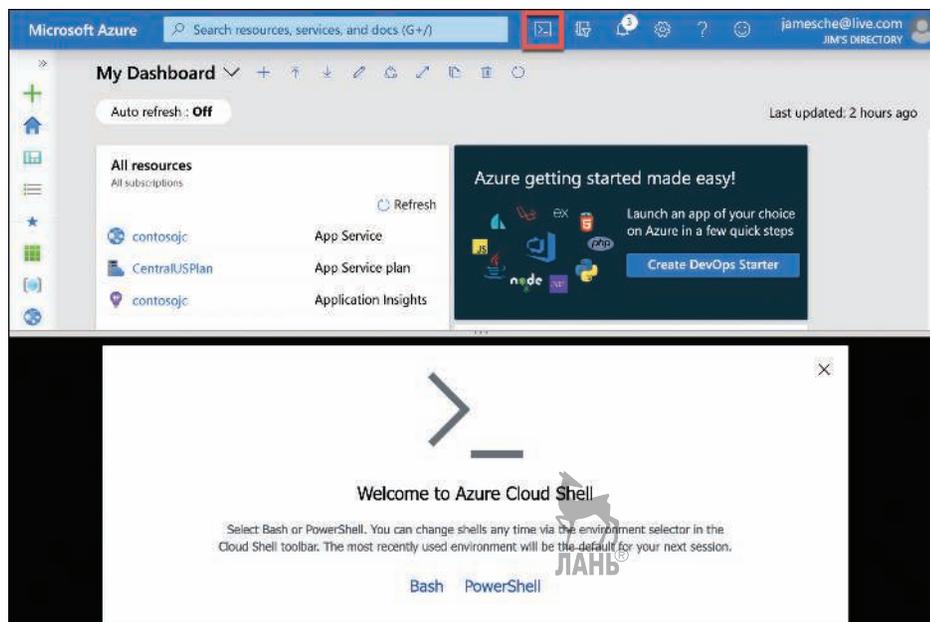


Рис. 3.72 Cloud Shell на портале Azure

При первом запуске Cloud Shell вам нужно будет выбрать среду, которую вы будете использовать. У вас есть выбор между Bash и PowerShell. Выбрав среду, вы можете изменить ее в любое время. Затем вам также нужно будет создать учетную запись хранилища Azure. Cloud Shell хранит все установленные компоненты, ваши настройки на устройствах, поэтому для их сохранения вам потребуется учетная запись хранилища. На рис. 3.73 показано создание учетной записи хранилища для Cloud Shell.

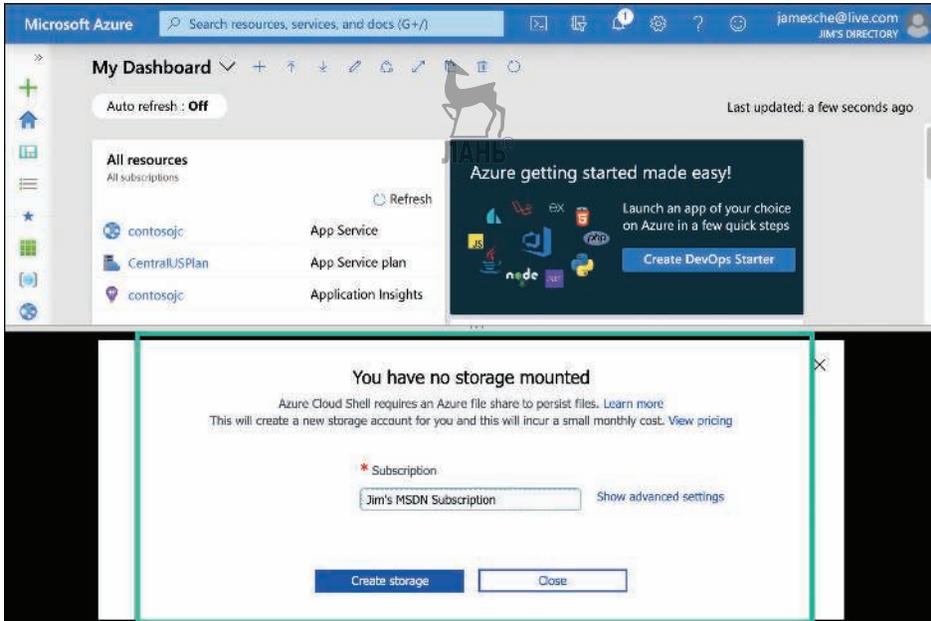


Рис. 3.73 Создание учетной записи хранилища для Cloud Shell

Как только учетная запись хранилища будет создана, Cloud Shell запустит сеанс, как показано на рис. 3.74.

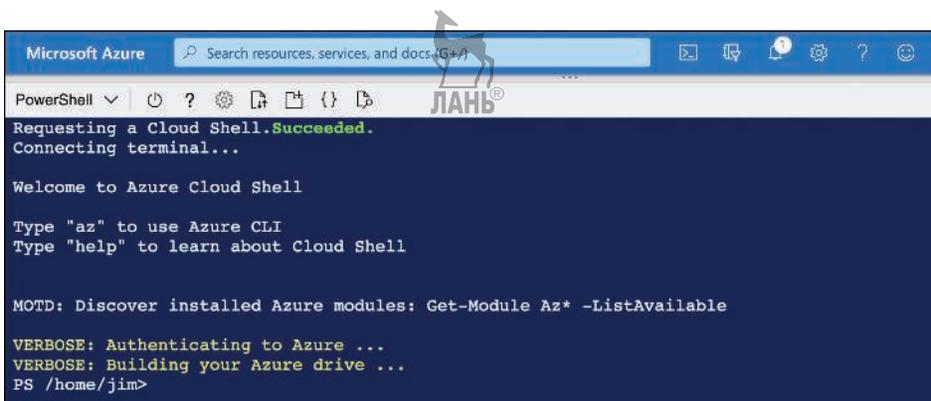


Рис. 3.74 Сеанс Cloud Shell

Из Cloud Shell вы можете выполнить любую команду, которая выполняется в Azure CLI. Если вы используете PowerShell, вы также можете использовать команды из модуля Az PowerShell. В верхней части окна Cloud Shell находится панель инструментов. Для переключения между PowerShell и Bash выберите необходимую вам среду в раскрывающемся меню. Рядом с этим меню находится кнопка **Power** (Питание), которая перезапускает сеанс Cloud Shell, за которой следует кнопка **Help** (Помощь) и кнопка **Settings** (Настройки) для изменения текста и шрифта. Справа от кнопки **Settings** (Настройки) находится кнопка, которая позволяет загружать и скачивать файлы в общий файловый ресурс для Cloud Shell. За ней следует кнопка, открывающая новый сеанс Cloud Shell в новой вкладке браузера.



СОВЕТ К ЭКЗАМЕНУ

Файлы, которые вы загружаете, будут доступны вам в Cloud Shell на любом устройстве. Это связано с тем, что ваши файлы хранятся в учетной записи хранилища Azure. Когда вы открываете Cloud Shell, Azure выбирает экземпляр Cloud Shell для подключения и копирует файлы из хранилища в этот экземпляр.

Кнопка **Open Editor** (Открыть редактор) на панели инструментов откроет экземпляр Monaco Editor, редактор кода, упрощающий редактирование сценариев и других файлов. На рис. 3.75 в редакторе открыт JSON-файл, а слева показан файловый браузер.

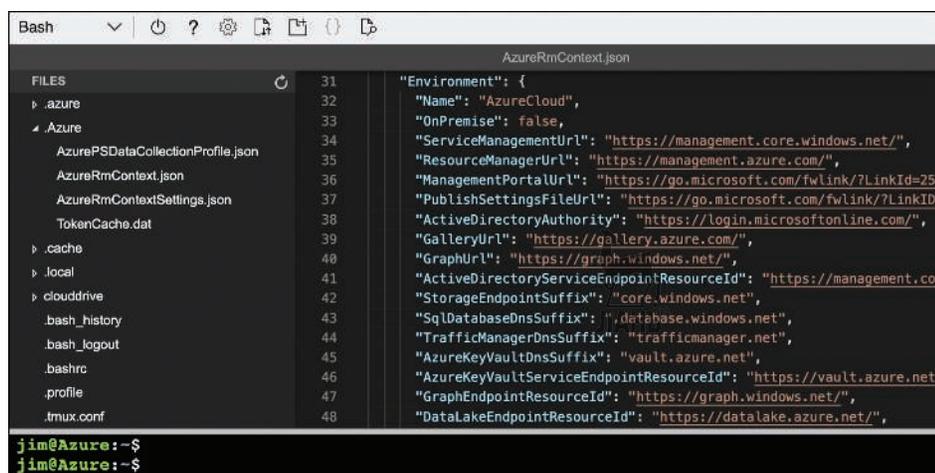


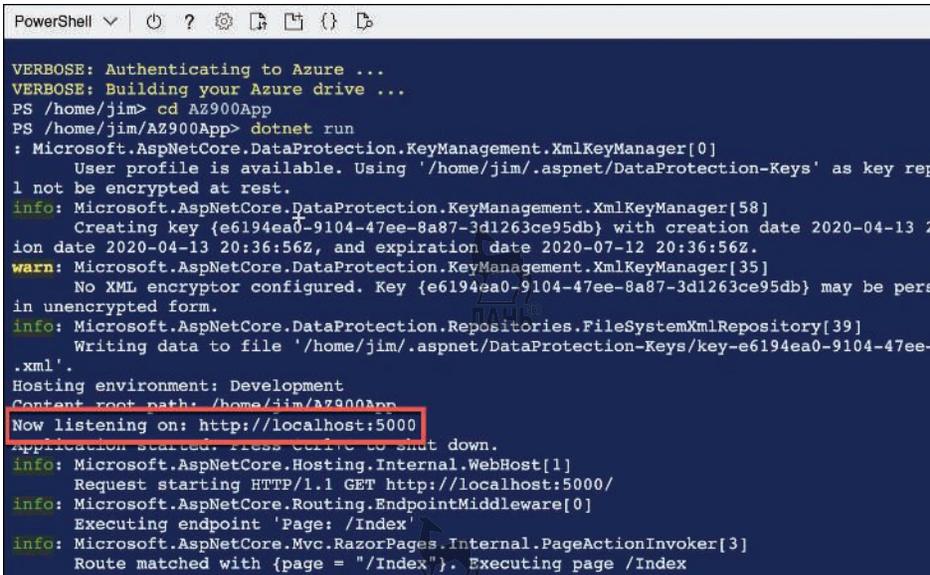
Рис. 3.75 Редактор файлов в Cloud Shell

ПРИМЕЧАНИЕ ЗАКРЫТИЕ РЕДАКТОРА

Чтобы выйти из редактора, щелкните правой кнопкой мыши на заголовке окна и нажмите **Quit** (Выйти).

Последняя кнопка на панели инструментов – это кнопка предварительного просмотра веб-страниц (Web Preview). Она позволяет запускать веб-приложение, используя файлы в текущей папке внутри веб-браузера. Это мощный инструмент для разработчиков, который дает возможность им разрабатывать веб-приложения при помощи Cloud Shell.

На рис. 3.76 я запускаю веб-приложение .NET Core в Cloud Shell, используя команду `dotnet run`. (Приложение `dotnet` применяется для запуска приложений, написанных для .NET Core.) После этого я вижу, что приложение запущено в экземпляре Cloud Shell на порте 5000.



```
PowerShell
VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/jim> cd AZ900App
PS /home/jim/AZ900App> dotnet run
: Microsoft.AspNetCore.DataProtection.KeyManagement.XmlKeyManager[0]
  User profile is available. Using '/home/jim/.aspnet/DataProtection-Keys' as key re
  pl not be encrypted at rest.
info: Microsoft.AspNetCore.DataProtection.KeyManagement.XmlKeyManager[58]
  Creating key (e6194ea0-9104-47ee-8a87-3d1263ce95db) with creation date 2020-04-13 2
  ion date 2020-04-13 20:36:56Z, and expiration date 2020-07-12 20:36:56Z.
warn: Microsoft.AspNetCore.DataProtection.KeyManagement.XmlKeyManager[35]
  No XML encryptor configured. Key {e6194ea0-9104-47ee-8a87-3d1263ce95db} may be pers
  in unencrypted form.
info: Microsoft.AspNetCore.DataProtection.Repositories.FileSystemXmlRepository[39]
  Writing data to file '/home/jim/.aspnet/DataProtection-Keys/key-e6194ea0-9104-47ee-
  .xml'.
Hosting environment: Development
Content root path: /home/jim/AZ900App
Now listening on: http://localhost:5000
Application started. Press Ctrl+C to shut down.
info: Microsoft.AspNetCore.Hosting.Internal.WebHost[1]
  Request starting HTTP/1.1 GET http://localhost:5000/
info: Microsoft.AspNetCore.Routing.EndpointMiddleware[0]
  Executing endpoint 'Page: /Index'
info: Microsoft.AspNetCore.Mvc.RazorPages.Internal.PageActionInvoker[3]
  Route matched with {page = "/Index"}. Executing page /Index
```

Рис. 3.76 Запуск веб-приложения .NET Core из Cloud Shell

Если вы хотите открыть его в браузере и просмотреть, нажмите Web Preview в Cloud Shell и выберите **Configure** (Настроить). Введите номер порта (в нашем случае **5000**), как показано на рис. 3.77.



Рис. 3.77 Конфигурация порта для Web Preview в Cloud Shell

После этого я могу нажать кнопку **Open And Browse** (Открыть и просмотреть) и увидеть свое веб-приложение в браузере, как показано на рис. 3.78. По сайту видно, что с оформлением CSS-файла у меня есть проблемы. Предварительный просмотр позволяет мне устранить эту и другие проблемы приложения.

ПРИМЕЧАНИЕ WEB PREVIEW

Зачем же просматривать приложение в Cloud Shell, если можно просто производить его отладку локально? Многие разработчики пишут приложения, которые взаимодействуют с другими службами Azure, и им может потребоваться отладка приложений во время работы в Azure. Для разработчиков командной строки этот метод в Cloud Shell является эффективным.

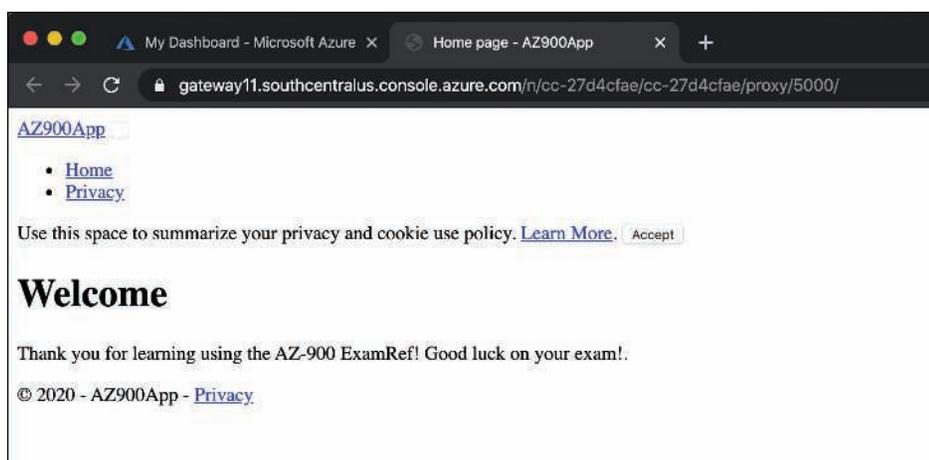


Рис. 3.78 Просмотр веб-приложения с помощью Web Preview

До этого мы рассматривали только использование Cloud Shell из портала Azure, но это не единственный способ для доступа к Cloud Shell. В документации Azure приводится множество примеров сценариев PowerShell и Azure CLI, и зачастую имеется кнопка **Try** (Попробовать), которую вы можете нажать, чтобы опробовать сценарий в своем браузере. Когда вы нажмете ее, откроется экземпляр Cloud Shell, чтобы вы могли легко ввести сценарий и выполнить команды, как показано на рис. 3.79.

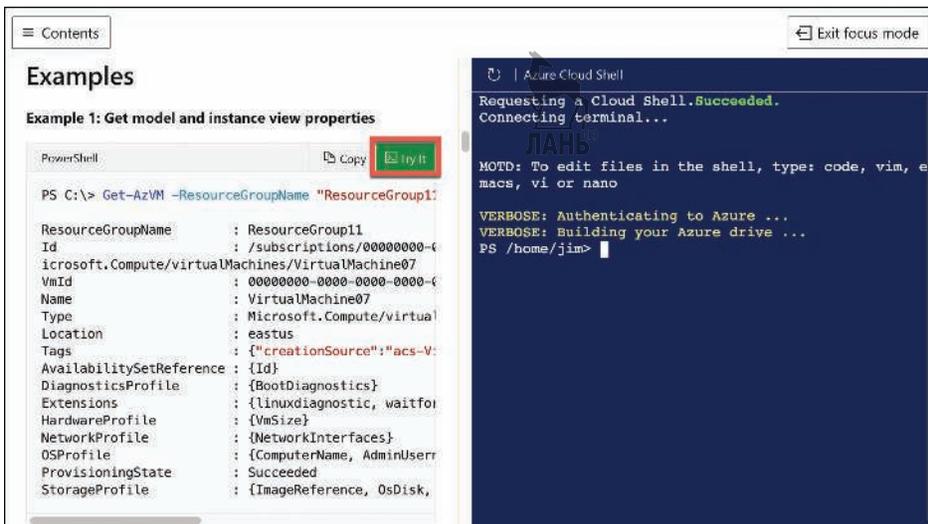


Рис. 3.79 Интеграция Cloud Shell с документацией Microsoft

Azure mobile app

Если у вас есть устройство Android или iOS, вы сможете загрузить мобильное приложение Azure для управления ресурсами Azure со своего устройства. Вы всегда можете перейти на портал Azure на своем устройстве, и вы получите возможности, настроенные под небольшие экраны. Однако, как и в случае с другими веб-сайтами, которые вы можете использовать, приложение обеспечивает лучший и более удобный интерфейс на мобильном устройстве.

При первом запуске мобильного приложения Azure вам будет предложено войти в свою учетную запись Azure. Затем вы увидите экран, подобный тому, что изображен на рис. 3.80.

На главном экране вы можете просмотреть свои службы Azure, проверить работоспособность служб, чтобы определить, произошел ли сбой в Azure, и многое другое. Если вы нажмете на службу Azure, то увидите список всех ресурсов этого типа службы. Нажатие на ресурс позволит вам взаимодействовать с ним. У вас не будет полной функциональности портала Azure, но вы сможете просматривать подробные сведения о ресурсе и выполнять с ним основные функции.

На рис. 3.81 виртуальная машина Azure отображается в мобильном приложении Azure. Внизу показаны ссылки **Stop** (Остановить), **Restart** (Перезапустить) и **Connect** (Подключиться).

ПРИМЕЧАНИЕ ПОДКЛЮЧЕНИЕ К ВМ

Для того чтобы подключиться к ВМ, вам потребуется установленное приложение Microsoft Remote Desktop. Его можно бесплатно скачать на Apple Store или Google Play.

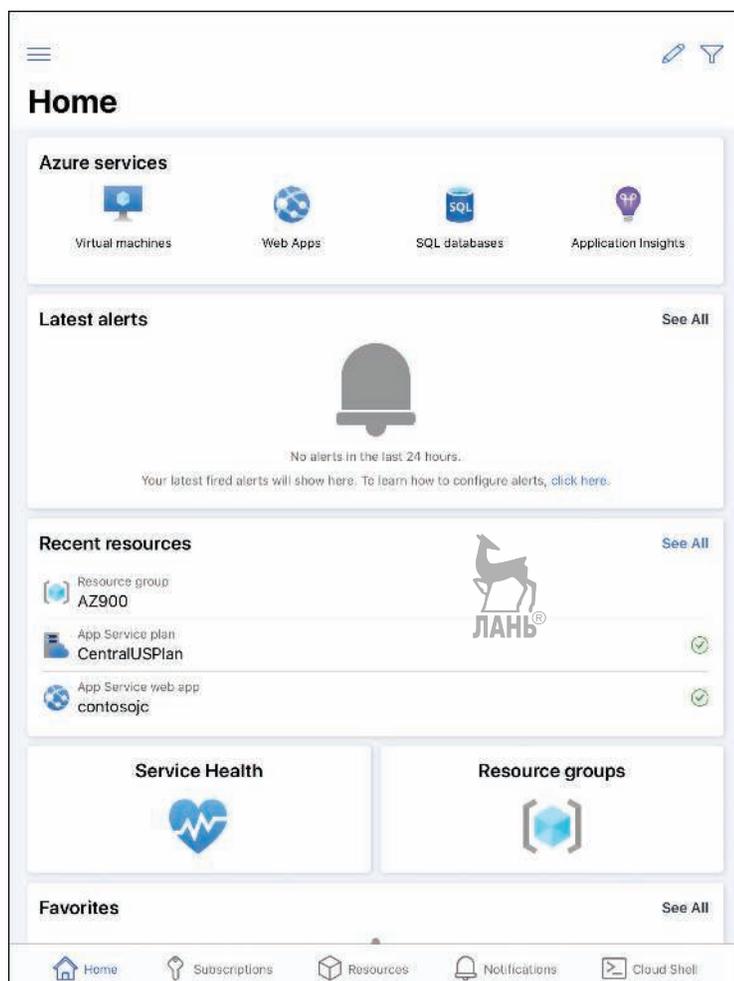


Рис. 3.80 Мобильное приложение Azure

Даже без наличия профессиональных умений при работе с порталом Azure в мобильном приложении Azure у вас есть много возможностей. Если вы нажмете на кнопку **Cloud Shell** в правом нижнем углу (как показано ранее на рис. 3.80), запустится экземпляр Cloud Shell, как показано на рис. 3.82. Отсюда вы сможете выполнять те же команды, которые вы выполняли в Cloud Shell на компьютере. Вы можете переключиться с PowerShell на Bash, выполнить команды **Azure CLI** и **Az PowerShell** и т. д.

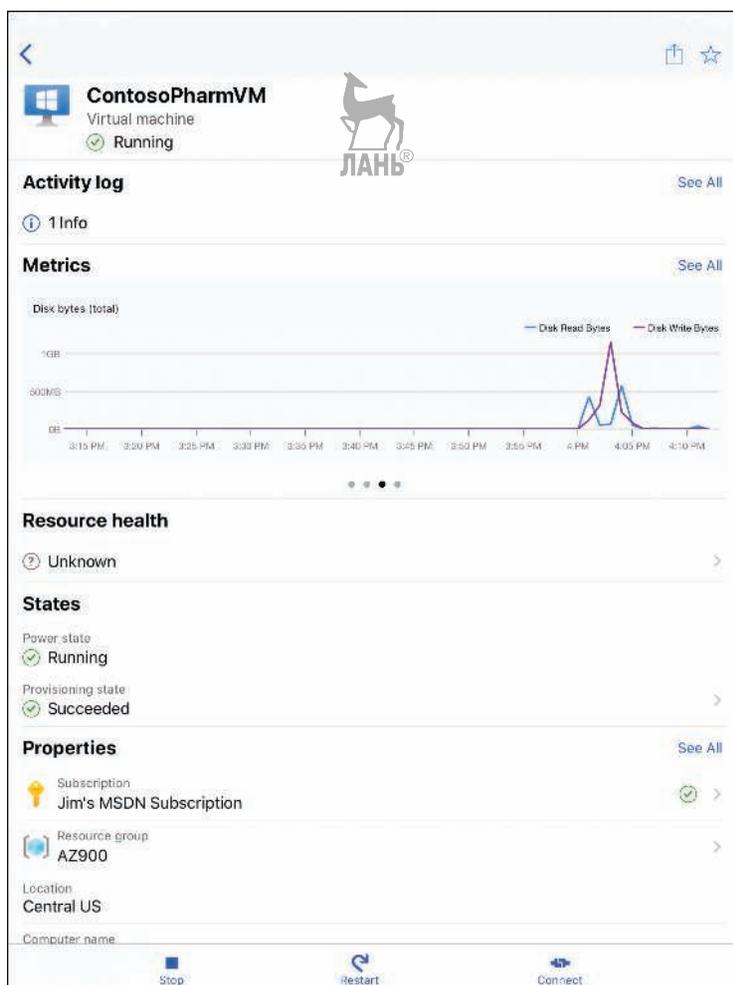


Рис. 3.81 VM Azure в мобильном приложении Azure

Помощник по Azure (Azure Advisor)

Управление ресурсами Azure включает не только создание и удаление ресурсов. Это также означает, что ваши ресурсы настроены правильно для обеспечения высокой доступности и эффективности. Разобраться с тем, как именно это сделать, является непростой задачей. Были написаны целые книги по передовым практикам для облачных развертываний. К счастью, Azure может уведомлять вас о проблемах в конфигурации, чтобы избежать проблем. Он делает это через Помощника Azure.

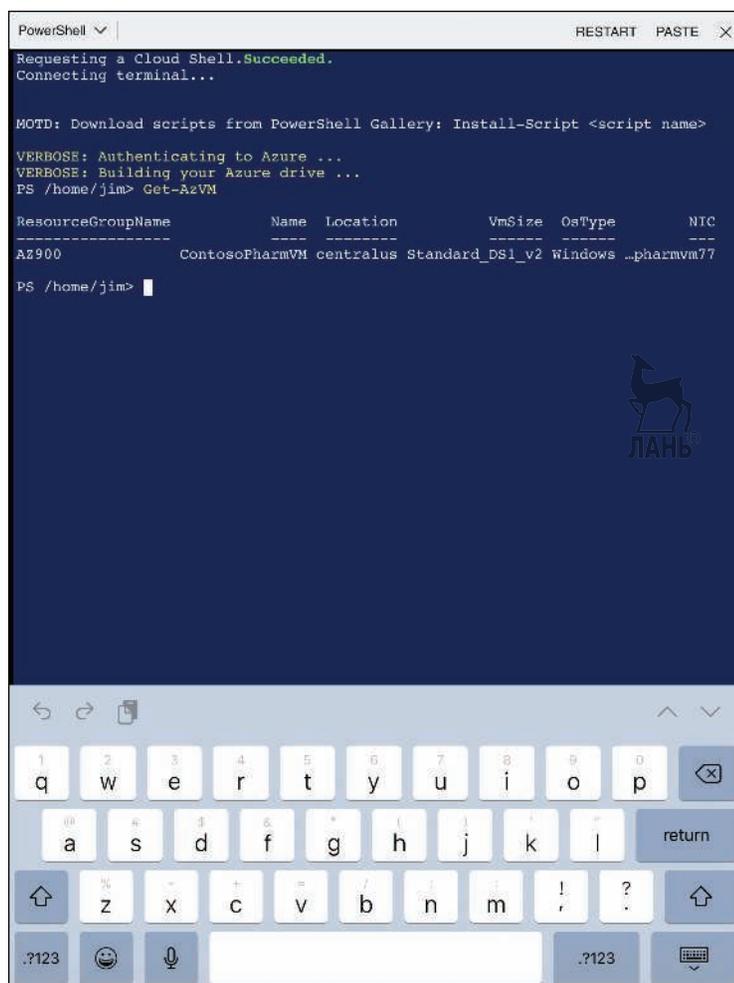


Рис. 3.82 Работа Cloud Shell в мобильном приложении Azure

Помощник по Azure (Azure Advisor) может предложить рекомендации в области высокой доступности, безопасности, производительности и стоимости. Чтобы получить доступ к Помощнику по Azure, зайдите на портал Azure и выберите пункт **Advisor** (Помощник) в меню слева. На рис. 3.83 показана служба Помощник по Azure с двумя рекомендациями для обеспечения безопасности.

Чтобы просмотреть сведения по рекомендации, нажмите на плитку. На рис. 3.84 мы выбрали плитку безопасности (Security tile) и получили рекомендацию по активации MFA (multifactor authentication), или же многофакторной аутентификации, и добавили другого владельца в подписку.

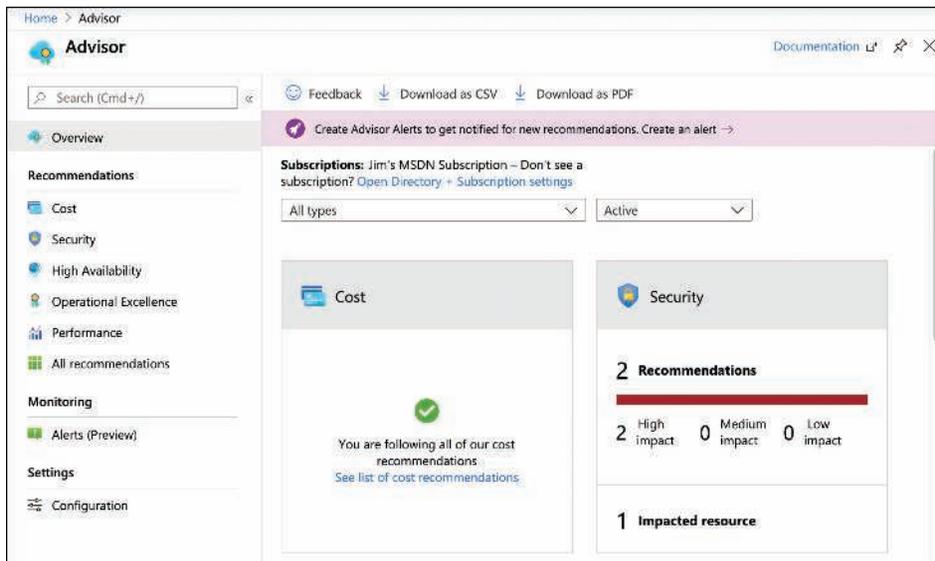


Рис. 3.83 Помощник по Azure

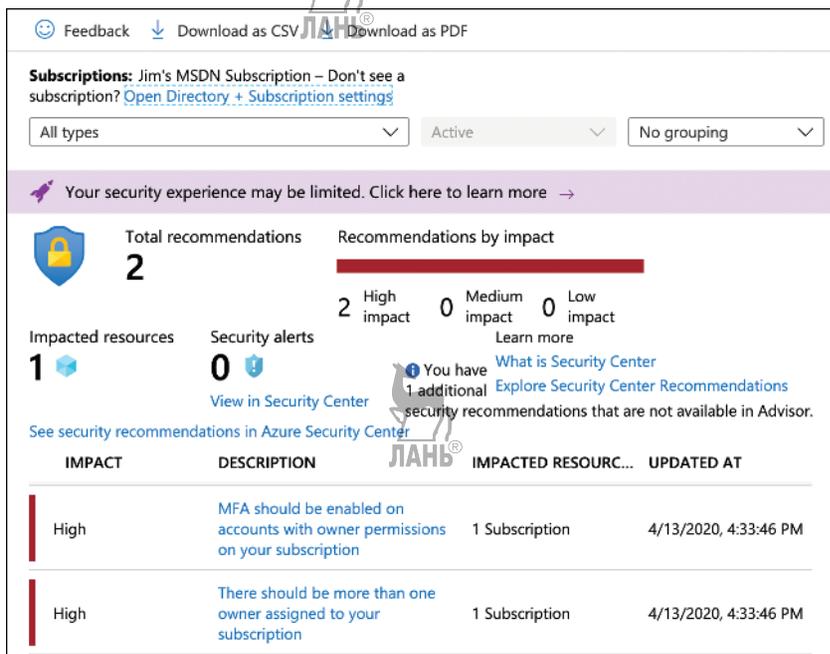


Рис. 3.84 Рекомендации Помощника

Вам не обязательно делать то, что рекомендует Помощник по Azure. Если вы нажмете на описание, то можете отложить или отклонить предупреждение, как показано в нижнем левом углу на рис. 3.85. Если вы решите отложить оповещение, то можете получить повторное напоминание через 1 день, 1 неделю, 1 месяц или 3 месяца.

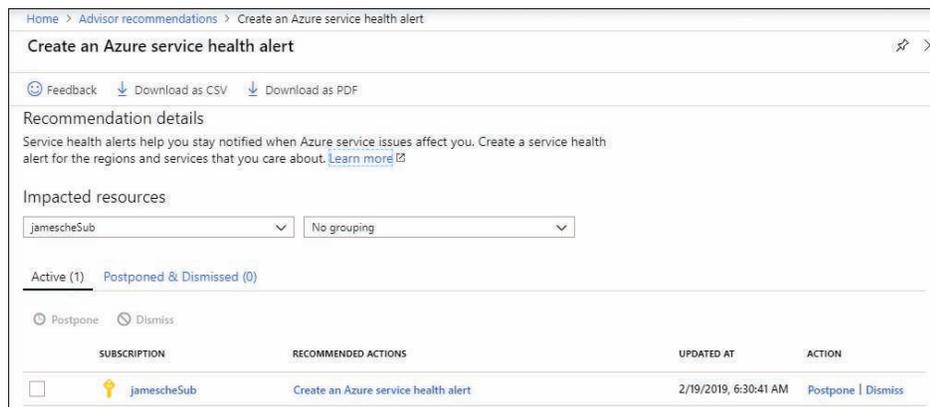


Рис. 3.85 Действия по рекомендации

Если у вас имеется большое количество рекомендаций или если вы не являетесь уполномоченной персоной для их выполнения, то можете скачать рекомендации Помощника по Azure в виде CSV-файла или PDF-файла. Нажмите кнопку **Download As CSV** (Скачать как CSV) или **Download As PDF** (Скачать как PDF), как показано на рис. 3.83. Вы также можете скачать файл с конкретными рекомендациями, нажав соответствующую кнопку загрузки при просмотре подробностей, как показано на рис. 3.84 и 3.85.

Azure Monitor

Azure Monitor объединяет метрики для служб Azure и предоставляет их в одном интерфейсе. Вы также можете создавать оповещения, которые будут уведомлять вас или другого пользователя о проблемах, которые вам нужно будет устранить.

Чтобы получить доступ к Azure Monitor, нажмите на **Monitor** на портале Azure, чтобы отобразилась кнопка **Azure Monitor**, как показано на рис. 3.86. Azure Monitor находится в процессе настройки, где отображены наиболее интересные вас моменты. По этой причине Azure Monitor не отображает метрики до тех пор, пока вы их не настроите. Для просмотра метрик нажмите **Metrics** (Метрики), а после выберите область.

На рис. 3.87 для мониторинга была выбрана ВМ в группе ресурсов AZ900.

После выбора ресурса вам будет представлен список связанных с ним метрик. Метрики для ВМ представлены на рис. 3.88.

Когда вы выберете метрику, график обновится с ее отображением. Вы можете добавить дополнительные метрики в свою диаграмму, нажав кнопку **Add Metric** (Добавить метрику), как показано на рис. 3.89.

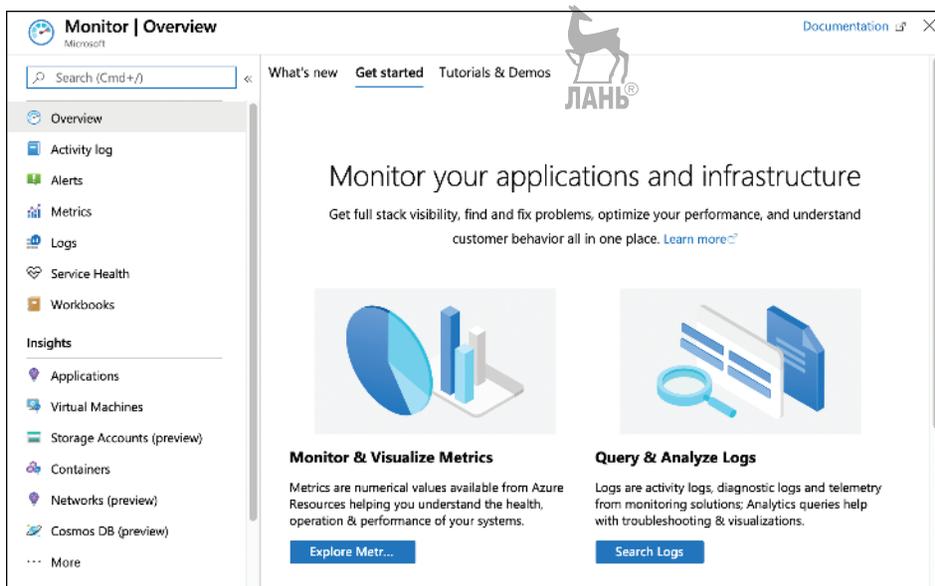


Рис. 3.86 Azure Monitor

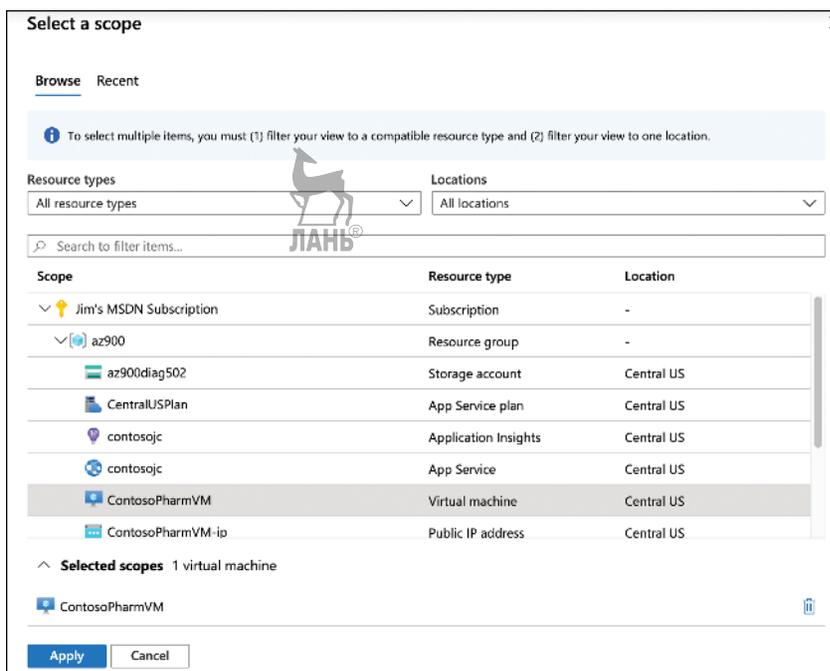


Рис. 3.87 Выбор ресурса для мониторинга

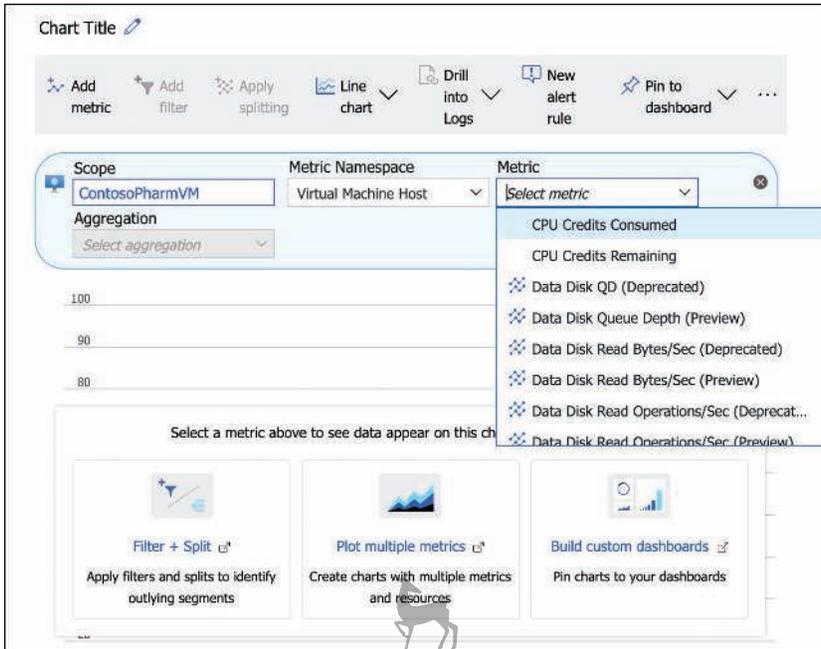


Рис. 3.88 Метрики для ВМ

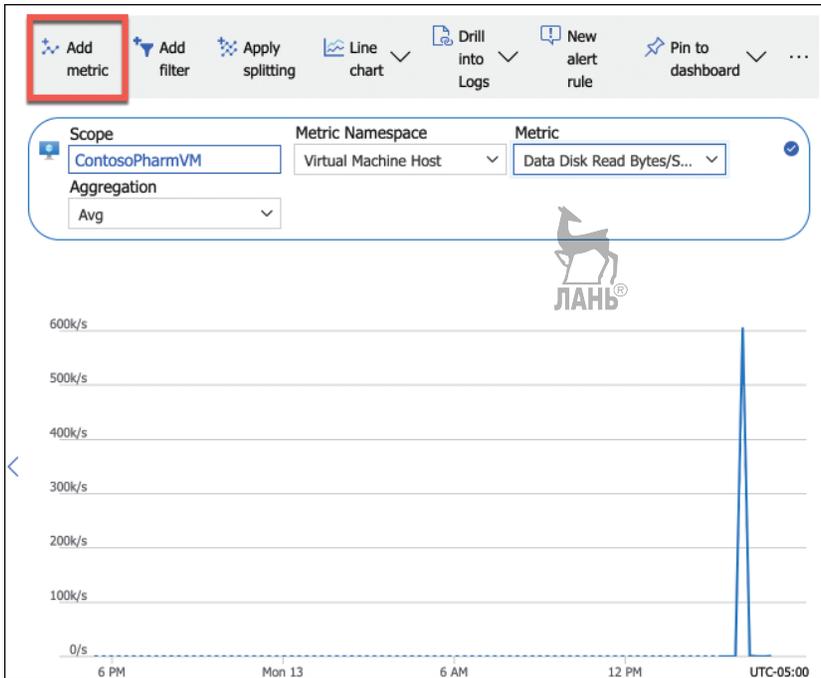


Рис. 3.89 Мониторинг использования диска ВМ

При добавлении нескольких метрик вам потребуется включить только те, которые имеют общую единицу измерения. Например, если бы вам пришлось добавить метрику ЦП в диаграмму, представленную на рис. 3.89, это бы не имело большой значимости, потому что процент ЦП измеряется в процентах, а дисковые единицы измеряются в байтах.

На рис. 3.90 мы добавили байты записи на диск (Disk Write Bytes) в диаграмму. Azure Monitor автоматически кодирует каждую метрику, чтобы их можно было различить. Мы также выбрали диаграмму области (Area Chart) в качестве типа диаграммы, чтобы закономерности были лучше видны.

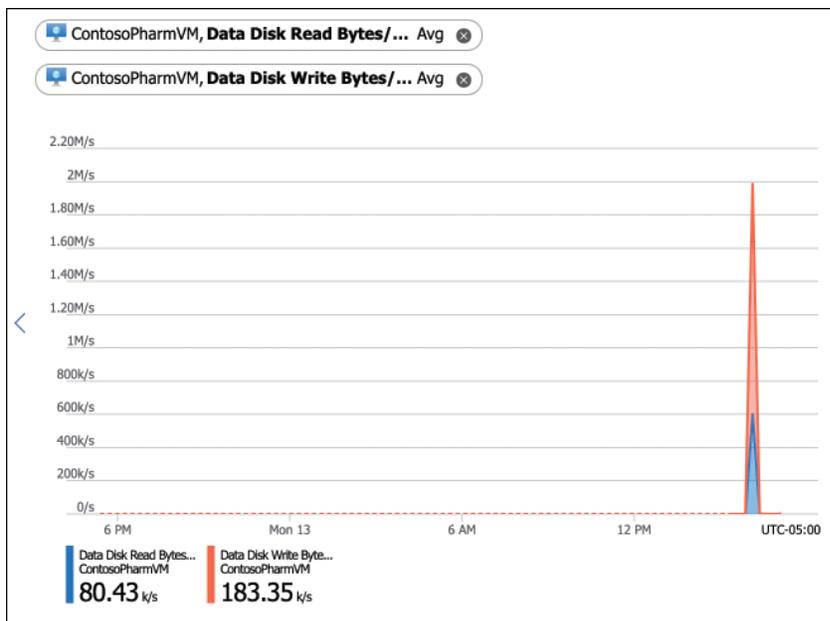


Рис. 3.90 График использования диска

Диаграммы отображаются за последние 24 часа по умолчанию, а значение в режиме реального времени отображается в правом краю диаграммы. Однако вы можете настроить отображаемый временной интервал, нажав на него и настроив по своему усмотрению, как показано на рис. 3.91.

Как только у вас появится диаграмма, которая будет вам необходима, вы можете закрепить ее на панели мониторинга портала, нажав **Pin To Dashboard** (Закрепить на панели мониторинга). Как показано на рис. 3.92, вы можете выбрать **Pin To Current Dashboard** (Закрепить на текущей панели мониторинга) или же закрепить на определенной панели мониторинга, выбрав **Select Another Dashboard** (Выбрать другую панель мониторинга), чтобы создать панель мониторинга на портале, настроенном под особые цели.

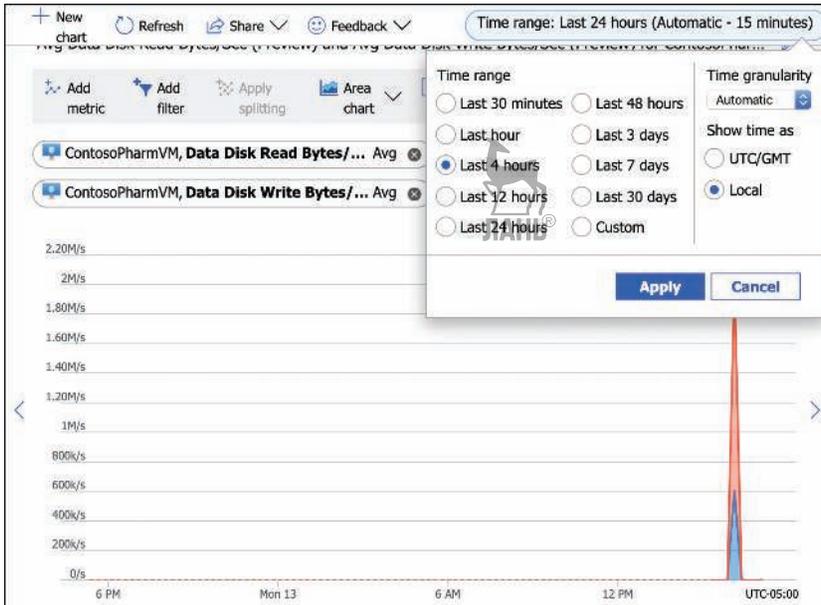


Рис. 3.91 Изменение временного интервала графика

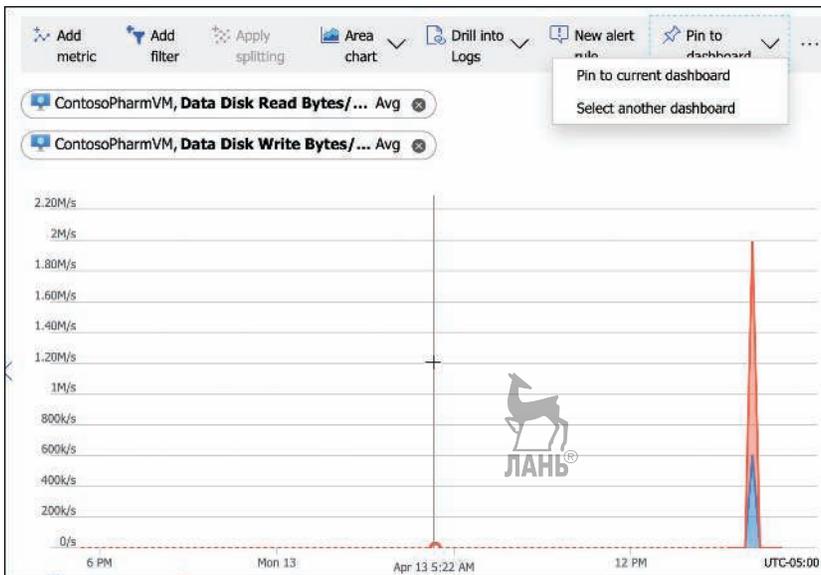


Рис. 3.92 Закрепление графика

Azure Monitor Alerts уведомляет своих пользователей посредством электронной почты или же текстовых сообщений, запускает поток **Logic App** (приложения логики), вызывает **Function App** (приложение-функцию), отправляет запрос на веб-перехватчик (webhook) и многое другое, когда выполняется определенное условие. Оповещения основаны на определенных вами прави-

лах, и при выполнении условия правила оповещения выполняют указанное вами действие.

Вы можете создать правило оповещения, которое автоматически настраивается для выбранных вами метрик на диаграмме, нажав **New Alert Rule** (Новое правило оповещений) в верхней части диаграммы. Вы также можете создать его с чистого листа, нажав **Alerts** (Оповещения) в меню Azure Monitor, как показано на рис. 3.93, а затем нажав **New Alert Rule** (Новое правило оповещения).

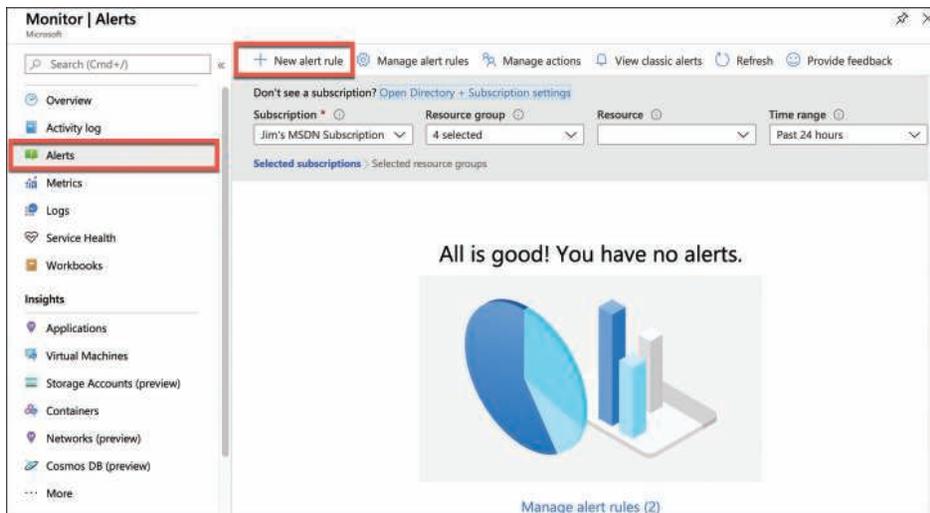


Рис. 3.93 Создание правила оповещения

Чтобы запустить правило, нажмите кнопку **Select** (Выбрать) и выберите ресурс, для которого вы хотите настроить оповещение. На рис. 3.94 ВМ выбрана для нового правила оповещения.

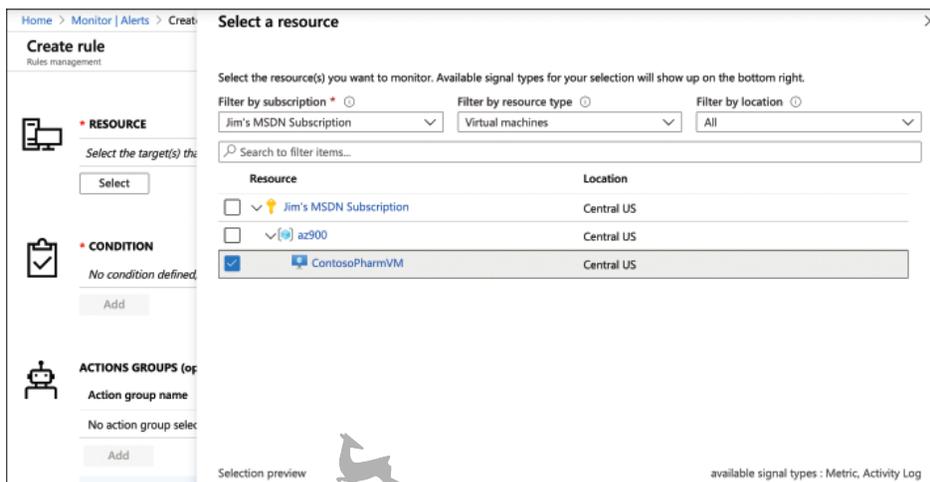


Рис. 3.94 Выбор ресурса для оповещения

Затем вам нужно будет указать условие для вашего оповещения. Нажмите кнопку **Add Condition** (Добавить условие), а затем выберите сигнал, который вы хотите отслеживать для своего оповещения. На рис. 3.95 оповещение настроено на основе сигнала изменения процента загрузки процессора VM (Percentage CPU signal).

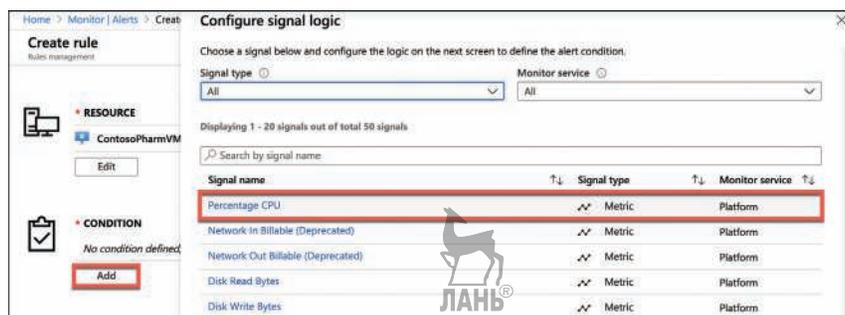


Рис. 3.95 Настройка условия

После выбора сигнала для него настраивается логика. На рис. 3.96 Monitor отображает интерактивный график выбранного вами сигнала, который помогает вам получить представление о том, как именно работал ваш ресурс. По умолчанию отображены шесть часов, при этом вы можете настроить период графика, указать оператора, тип агрегации и пороговое значение. Или нажать кнопку **Done** (Готово) для создания логики оповещения.

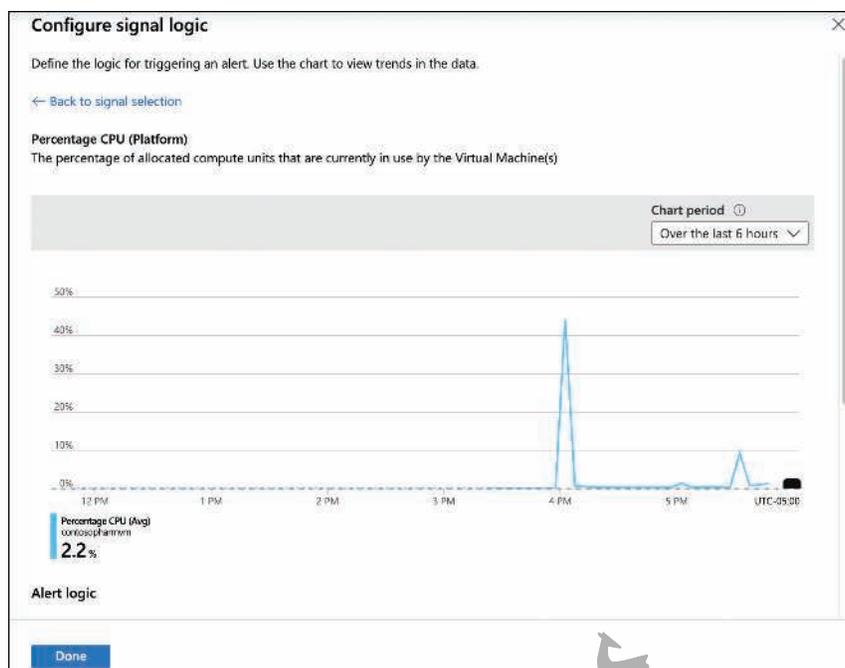


Рис. 3.96 Логика правила оповещения



ПРИМЕЧАНИЕ НЕСКОЛЬКО УСЛОВИЙ

Правило оповещения может состоять из нескольких условий. Например, у вас может быть правило, которое срабатывает только в том случае, если среднее значение процессора превышает 70 % и при высокой загрузке диска. Выбор всегда за вами.

Когда срабатывает оповещение, оно выполняет действие, указанное вами с помощью *группы действий*. Группа действий содержит список действий, которые необходимо выполнить при вызове оповещения. Чтобы создать новую группу действий, нажмите кнопку **Create** (Создать), как показано на рис. 3.97.

The screenshot shows the 'Create rule' interface in Azure. It is titled 'Create rule' and 'Rules management'. The interface is divided into three main sections: **RESOURCE**, **CONDITION**, and **ACTIONS GROUPS (optional)**.
1. **RESOURCE**: Shows 'ContosoPharmVM' with an 'Edit' button.
2. **CONDITION**: Shows 'Whenever the percentage cpu is greater t... \$ 0.10' with a green checkmark and a trash icon. Below it, 'Total \$ 0.10' is displayed. An 'Add' button is present.
3. **ACTIONS GROUPS (optional)**: Shows 'No action group selected' with an 'Add' button and a 'Create' button. The 'Create' button is highlighted with a red box.

Рис. 3.97 Создание группы действий

На рис. 3.98 мы создаем действие для уведомления ИТ-директора. В этом случае действие отправит директору текстовое сообщение и push-уведомление посредством мобильного приложения Azure.

Группы действий предназначены для включения в себя нескольких действий, которые выполняются при срабатывании оповещения. Чтобы добавить новое действие, нажмите **Manage Actions** (Управление действиями) (см. рис. 3.93), а затем выберите свою группу действий. На рис. 3.99 мы добавили дополнительное действие в группу, которое вызывает Function App, выполняющее код для перезагрузки VM.



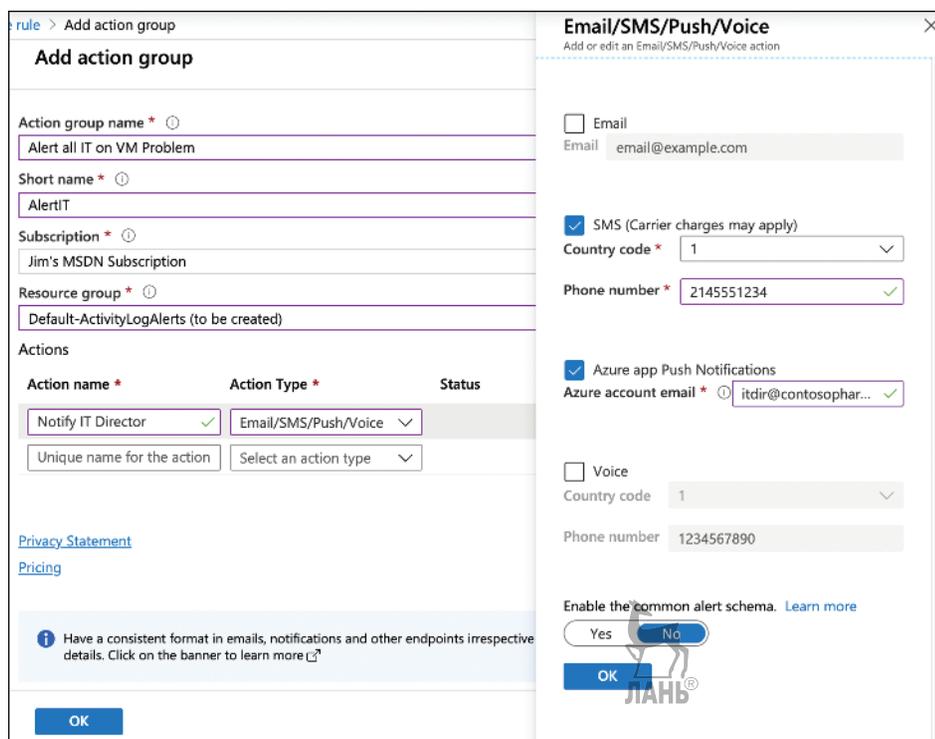


Рис. 3.98 Создание действия

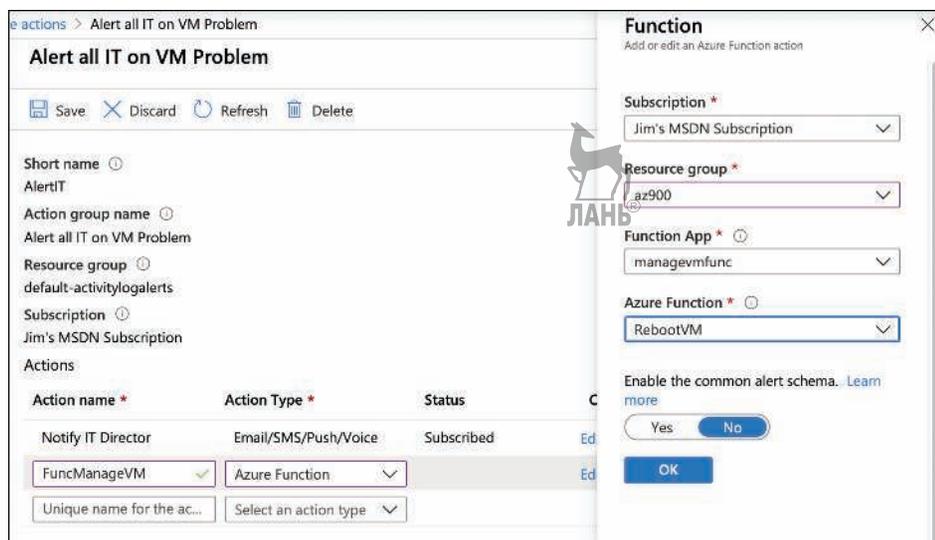


Рис. 3.99 Добавление другого действия

Azure Service Health

Microsoft управляет веб-страницей состояния Azure (Azure Status), на которой вы можете просматривать текущее состояние служб Azure в тех регионах, где работает Azure. Несмотря на то что она является довольно полезным представлением по общей работоспособности Azure, большой объем веб-страницы не позволяет назвать ее самым эффективным способом получения общего представления о работоспособности служб. Служба работоспособности Azure может предоставить вам представление конкретно под ваши определенные ресурсы.

Чтобы получить доступ к Service Health, нажмите **All Services > All > Service Health**, как показано на рис. 3.100.

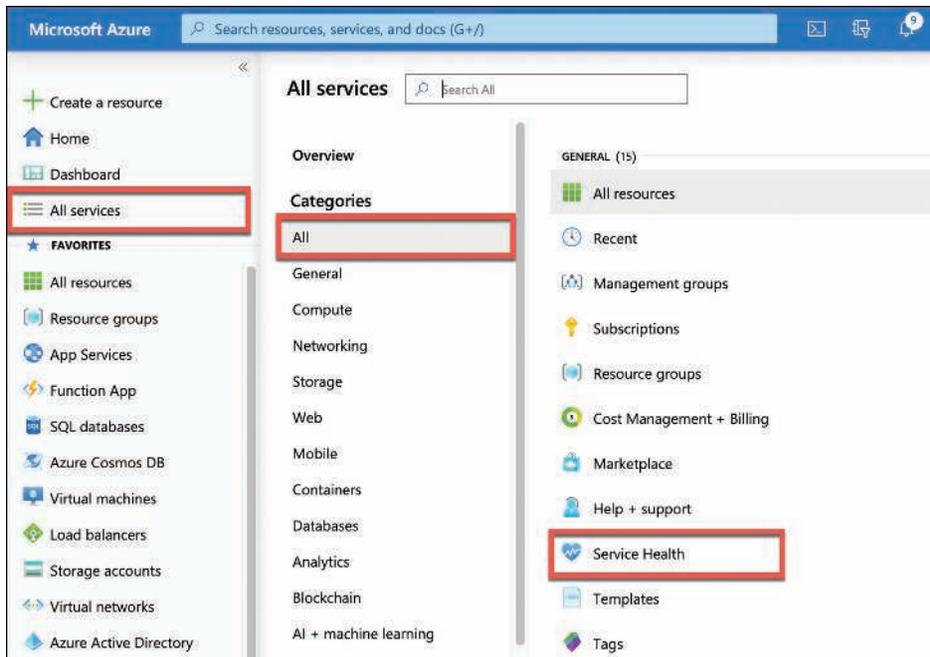


Рис. 3.100 Azure Service Health

На рис. 3.101 показан блейд Service Health, отображающий работоспособность и состояние ресурсов. На представленной карте есть три зеленые точки, которые олицетворяют работоспособность трех регионов Azure, в которых развернуты ресурсы. Эта карта специфична, и, нажав иконку булавки, вы получите краткую справку о работоспособности Azure только для тех регионов, где у вас имеются ресурсы.

Вы также можете просмотреть любое предстоящее плановое техобслуживание (оно может повлиять на вашу работу), нажав на **Planned Maintenance** (Плановое обслуживание) в левой части меню. Нажав **Health Advisories** (Рекомендации по работоспособности), вы можете просмотреть информацию о работоспособности, возможно связанную с вашей собственной конфигурацией, а не с проблемами в Azure.

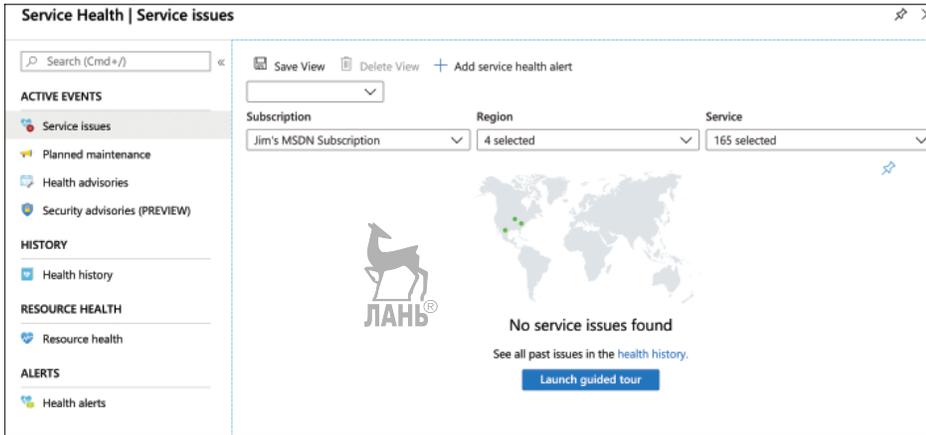


Рис. 3.101 Проблемы с обслуживанием в Service Health

Когда у вас возникнет проблема с обслуживанием, вы получите подробную информацию о ней, как показано на рис. 3.102. Вам также придет ссылка с подробной информацией об инциденте. Вы сможете загрузить PDF-файл с официальным уведомлением от Microsoft о случившемся.

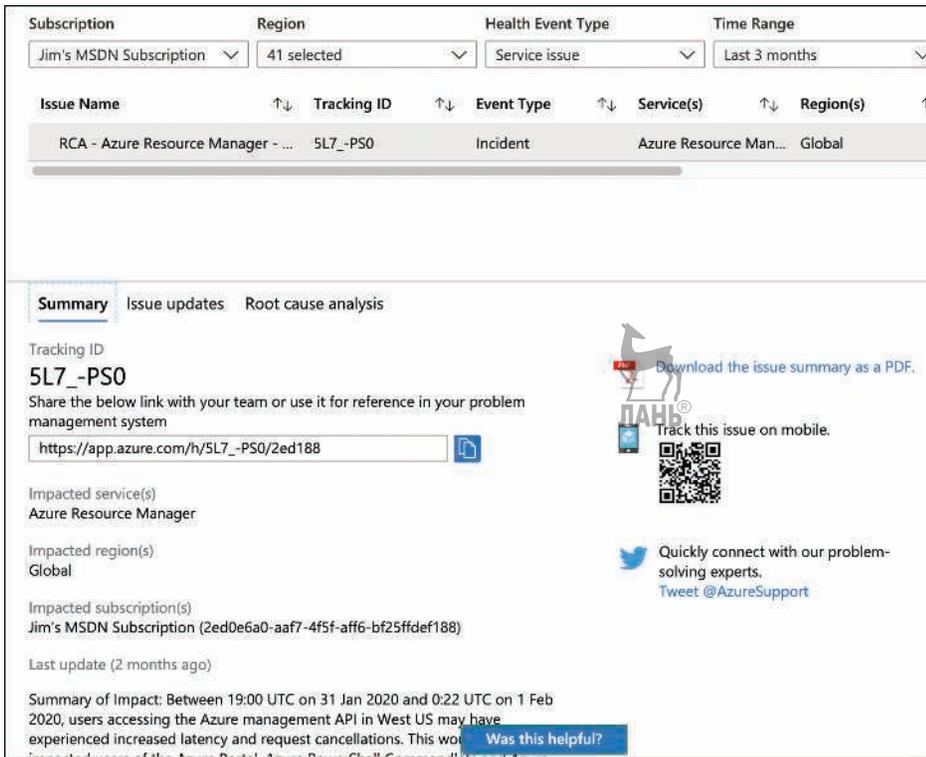


Рис. 3.102 Инцидент Azure Service Health

Azure Monitor и служба работоспособности Azure (Azure Service Health) приносят значительный вклад в общее представление о ресурсах Azure. Azure Monitor предназначен для мониторинга стоимости и производительности ресурсов. Он оповещает пользователей, когда это задается условиями. А вот служба работоспособности Azure предоставляет достоверную информацию о работоспособности самого Azure и о том, какое влияние оказывают происходящие в Azure инциденты на ресурсы. В совокупности эти две службы предоставляют вам необходимые инструменты, благодаря которым вы знаете о своих ресурсах и насколько хорошо они работают.

Мысленный эксперимент

В этой главе вы многому научились, поэтому давайте теперь применим эти знания на практике – в мысленном эксперименте. Ответы на него вы можете найти в следующем разделе.

ContosoPharm заинтересованы в модернизации своих систем, и они обратились к вам за помощью. Компания хотела бы отслеживать изменения условий микроклимата на складах, поэтому они установили несколько термостатов с доступом в интернет. Одним из требований компании является возможность предупреждения персонала о наличии определенных отклонений касаясь температуры и степени влажности. ИТ-отделу требуется способ эффективного обновления встроенного ПО на этих термостатах, и поскольку их количество достигает сотни и сотни устройств, компания обеспокоена затратами на нужных специалистов-инженеров для выполнения подобной работы. Компании важна уверенность в том, что все термостаты будут обновлены, даже при отсутствии у них доступа в интернет. Посоветуйте компании хорошее решение, которое будет отвечать всем заявленным требованиям.

Еще одним требованием к устройствам является обеспечение их безопасности. ИТ-директор обеспокоен подключением систем к интернету из-за опасений того, что злоумышленники могут взять под контроль системы климат-контроля. Предоставьте компании рекомендации, использование которых обезопасит устройства.

ContosoPharm также интересна возможность использования машинного обучения в целях повышения эффективности проводимых компанией исследований. У компании уже накоплен достаточный объем данных в хранилище Data Lake Storage. Им необходим эффективный способ для анализа этих данных, а также способ для построения моделей машинного обучения. У ContosoPharm имеются огромные объемы данных, поэтому в их случае требуется масштабируемое решение, способное обрабатывать миллионы строк данных. Если вы сможете предоставить им решение для включения неструктурированных данных в уравнение, то это будет большим плюсом. В ходе ваших предварительных обсуждений с компанией выяснилось, что специалисты компании по обработке и анализу данных заинтересованы в возможностях использования знаний по Jupyter Notebooks. Предоставьте компании рекомендации о том, как лучше всего реализовать это в Azure.

Имея в своем штате квалифицированных специалистов по обработке и анализу данных и разработчиков, в планах которых использование R для создания моделей машинного обучения, компания ContosoPharm также хотела бы предоставить возможность другим сотрудникам, не имеющим знаний по R или Python, разрабатывать модели. Если у вас есть предложение, которое бы вы могли им предоставить по этому вопросу, то это стало бы отличным коммерческим аргументом.

ИТ-директор осознает, что эти задачи будут нагружать ресурсы, и его беспокоит то, что менеджеры по продажам будут тормозить работу ИТ-специалистов службы поддержки. Проблемы, с которыми они сталкиваются, не такие сложные, однако на их решение требуется много времени со стороны ИТ-персонала. Директор попросил вас порекомендовать способ, благодаря использованию которого они могли бы оказать базовую поддержку без вовлечения ценных ИТ-ресурсов.

Единственное, что вызывает проблемы с поддержкой Azure VM, – это то, что она работает с устаревшим приложением ContosoPharm. В приложении имеются утечки памяти, что в итоге приводит к его замедлению до такой степени, что осуществляются автоматические вызовы службы поддержки. У компании сейчас нет доступных ресурсов для устранения неполадок и проблем, поэтому, получая вызовы, они перезагружают VM, временно устраняя проблему. Если вы можете порекомендовать им способ для контроля используемой памяти и для автоматической перезагрузки VM без участия пользователя, то это значительно помогло бы сократить количество вызовов службы поддержки.

Размер VM, на которой размещено приложение, иногда приходится изменять из-за увеличения использования. Когда эта VM масштабируется до большого размера, то это значит большие расходы для ContosoPharm. Директор по информационным технологиям готова на увеличение стоимости, только если об этом ей будут приходить информационные уведомления об изменениях в виде текстовых сообщений. Она предложила эту идею ИТ-директору, но он не может предоставить решение из-за ограниченного количества разработчиков, которые бы создали такое решение. Было бы большим плюсом, если бы вы смогли помочь найти им выход из сложившейся ситуации, который бы не задействовал рабочие силы, способные на создание кода.

Вместе с рекомендацией по созданию решения для директора по информационным технологиям компания ContosoPharm хочет получить хороший способ по отслеживанию выполняемой работы. Есть беспокойство, что придерживаться графика не всегда будет получаться, так как у сотрудников, работающих над проектом, может быть много других обязанностей. Предоставьте им рекомендации о том, как отслеживать работу и обеспечивать ее выполнение.

Один из разработчиков компании думает, что мог бы устранить неисправность приложения по утечке информации, однако на это он не может потратить много времени. При работе над этим приложением одной из проблем станет необходимость задействовать другие VM с установленными на них специальными инструментами, а также сотруднику потребуются символьные файлы для отладки, которые будут установлены на этих VM. Установка таких файлов занимает порядка пары часов после запуска новой VM. Если бы вы могли порекомендовать какой-либо способ для экономии времени на это, то это

бы позволило ContosoPharm выполнить работу по исправлению приложения и в решении проблемы в долгосрочной перспективе.

Другой серьезной проблемой в устранении неисправностей приложения является то, что в нем используется три разных веб-приложения, запущенных в службе приложений Azure. Разработчик не хотел бы устранять проблемы, используя при этом веб-приложения, поэтому у него должна быть возможность для создания новых приложений для тестирования. Поскольку оплата за эти веб-приложения осуществляется ContosoPharm независимо от их эксплуатации, то когда разработчик не будет активно заниматься устранением проблем, компании придется удалить эти веб-приложения. Снова приступив к работе над проблемным приложением, сотруднику придется потратить время на повторное создание приложений. Посоветуйте ContosoPharm решение, которое бы позволило им без труда создавать такие веб-приложения, а при их ненужности удалять.

Разработчик, который будет работать над приложением, сообщил, что приложение использует объемную коллекцию сценариев Bash, установленных на ВМ. Эти сценарии взаимодействуют с ресурсами Azure, поэтому и должны выполняться в ее среде. Он считает, что эти сценарии могут быть частью проблем с приложением, поэтому ему нужен способ, который бы позволил ему легко редактировать эти сценарии в среде Azure. Проблема еще в том, что у сотрудника может и не быть доступа к компьютеру. Большую часть работы, выполняемой над сценариями, он осуществляет вне офиса – в дороге, и единственным устройством, которое он берет с собой в дорогу, является iPad. Если вы сможете предложить компании способ, при помощи которого разработчик сможет продуктивно работать, то это будет большим плюсом для ContosoPharm.

ИТ-директор читал об облачных технологиях. У него есть сомнения, что основная часть проблем ContosoPharm заключается лишь в том, что они не используют передовой опыт Azure. Он попросил вас обсудить с ним нововведения, чтобы у компании не возникало проблем. Вы понимаете, что потратите на это время, а также осознаете, что и нововведения могут вскоре стать устаревшими. Предоставьте компании наилучшую рекомендацию, благодаря которой ContosoPharm смогут соответствовать наилучшим практикам в Azure. Поскольку компания встает на путь перемен, они хотели бы также узнать, существует ли способ тщательного контроля производительности ВМ и других ресурсов. Чтобы сэкономить потраченное время, они также хотят быть в курсе любых инцидентов в Azure, влияющих на их ресурсы.

Ответы на мысленный эксперимент

В этом разделе мы рассмотрим ответы на мысленный эксперимент.

Лучшим вариантом для управления термостатами ContosoPharm является применение центра интернета вещей (IoT Hub). Они могли бы использовать IoT Central для выполнения большинства задач, однако одним из требований компании является возможность обновления встроенного ПО для устройств, даже при временном отсутствии интернета. Функция двойника устройства

в IoT Hub специально разработана для подобных ситуаций, поэтому IoT Hub будет лучшим вариантом.

Чтобы обеспечить безопасность термостатов, вы можете порекомендовать Azure Sphere. Однако тогда понадобятся и предназначенные для Azure Sphere микроконтроллеры. Но если такие устройства будут не доступны на рынке, то Azure Sphere является лучшим решением для обеспечения безопасности устройств интернета вещей, и ContosoPharm должна об этом знать.

Для компании лучшим способом для анализа данных и создания моделей будет аналитика Synapse. Это комплексное решение, которое хорошо работает с хранилищем Data Lake Storage. Поскольку компании необходимо масштабируемое решение, которое будет способно обрабатывать миллионы строк данных, HDInsight будет лучшей для них рекомендацией. Компания говорила, что желает работать с неструктурированными данными. Azure Databricks – это идеальное решение для использования неструктурированных данных, и его поддержка блокнотов отлично совпадает с желанием об использовании знаний Jupyter Notebooks.

Чтобы пользователи, которые не знают основ программирования, могли создавать ML-модели, вы можете порекомендовать компании машинное обучение Azure. Для этого ContosoPharm нужно будет использовать версию Enterprise, чтобы у них был доступ к визуальным конструкторам, это позволит им создавать ML-модели с помощью нескольких кликов.

Для уменьшения нагрузки на ИТ-отдел вы можете порекомендовать Службы когнитивных вычислений Azure и Службу Azure Bot для создания агента поддержки ИИ. Используя этот метод, они смогут легко понимать естественный язык и предоставлять предложения при помощи чат-бота.

Для отслеживания использования памяти и вынужденной перезагрузки VM ContosoPharm может использовать Azure Monitor и настраивать оповещения для вызова Function App с целью запуска кода, перезагружающего машину. Поскольку директор по информационным технологиям хотел бы получать информацию при изменении размера VM в связи с нехваткой памяти, вы можете предложить им использование Logic Apps для создания рабочего процесса. Вы можете использовать Event Grid для прослушивания события при изменении размера VM, а затем Logic Apps могут запустить поток, отправляющий текстовое сообщение директору по информационным технологиям.

Для отслеживания работы, которая выполняется в приложении для устранения ошибок утечки памяти, вы можете порекомендовать Azure DevOps и Azure Boards. Это позволит легко отслеживать различные задачи и их текущее состояние.

Разработчик, которому нужен доступ к VM с установленными специальными инструментами, может использовать Azure DevTest Labs. Создав пользовательский образ, включающий все необходимые инструменты и символы отладки, он всегда сможет моментально получить доступ к VM.

Для того чтобы легко и быстро создавать и удалять веб-приложения, вы можете порекомендовать сотруднику использовать модуль Az в PowerShell или Azure CLI. Используя их, разработчик может написать сценарий этих операций, позволяющий легко создавать веб-приложения и настраивать их под себя.

Для работы над своими сценариями Bash разработчик должен использовать Azure Cloud Shell. Поскольку Cloud Shell применяет встроенную файловую

систему, используемые сотрудником файлы будут доступны в любом сеансе Cloud Shell, а встроенный редактор Monaco упростит редактирование и разработку сценариев. Cloud Shell также решает проблему повышения производительности работы сотрудника, пока он находится в дороге. Установив мобильное приложение Azure на свой iPad, разработчик сможет получить доступ к сессии Cloud Shell на этом устройстве и выполнить свою работу.

Для того чтобы ContosoPharm были уверены, что используют самый современный передовой опыт, они могут использовать помощник Azure. Помощник укажет на несоответствия и предложит шаги по исправлению ситуации. Они смогут отслеживать возможные инциденты по обслуживанию в Azure при помощи службы работоспособности Azure на портале Azure.

Краткое содержание главы

В этой главе мы рассмотрели много вопросов. Вы узнали о некоторых новейших технологиях облачных вычислений и о способах управления ресурсами Azure.

Ниже представлено краткое изложение содержания главы.

- Интернет вещей (IoT) относится к устройствам и датчикам, которые взаимодействуют друг с другом и с интернетом.
- Azure IoT Hub позволяет управлять IoT-устройствами и отправлять на них сообщения.
- Служба Azure IoT Hub Provisioning упрощает подготовку большого количества устройств к работе в IoT Hub.
- Azure IoT Central является SaaS-предложением для осуществления мониторинга IoT-устройств.
- Azure Sphere является службой для защиты IoT-устройств.
- Azure Sphere состоит из микроконтроллеров, ОС и службы безопасности Azure Sphere.
- Большие объемы данных относятся к данным, которые необходимо проанализировать с помощью стандартных средств за какое-то время.
- Azure Synapse является заменой для хранилища данных SQL.
- Azure Synapse хранит огромные объемы данных, а также обеспечивает анализ данных в кластере.
- Кластер Azure Synapse состоит из Synapse SQL, интеграций Apache Spark, интеграции данных Apache Spark и хранилища Azure Data Lake, пользовательского веб-интерфейса Azure Synapse Studio.
- Хранилище Data Lake подходит для любого типа данных, поскольку в нем хранятся неструктурированные данные.
- HDInsight является решением Microsoft для обработки объемных данных кластером Hadoop.
- Azure Databricks представляет собой хорошее решение для моделирования данных из хранилища данных, чтобы его можно было эффективно использовать в ML-моделировании.

- Кластеры Azure Databricks состоят из блокнотов, в которых могут храниться все типы информации.
- Процесс принятия решения ИИ в нескольких точках нейронной сети называется ML-конвейером.
- Машинное обучение Azure использует облачные ресурсы для более быстрого обучения ML-моделей.
- Корпоративная версия машинного обучения Azure предлагает конструкторы, которые позволяют создавать, обучать и оценивать ML-модели в графическом интерфейсе.
- Службы когнитивных вычислений предоставляют множество API-интерфейсов, позволяющих быстро разрабатывать решения для машинного обучения.
- Служба Azure Bot работает в службе приложений Azure и упрощает создание эффективного взаимодействия с помощью ИИ.
- Бессерверные вычисления означают использование избыточных VM в Azure для выполнения клиентского кода. Вы оплачиваете только его выполнение.
- Функции Azure представляют собой вычислительный компонент бессерверной службы Azure.
- Azure Logic Apps являются бессерверным решением для рабочих процессов, использующим коннекторы (соединители), триггеры и действия.
- Azure Event Grid позволяет создавать и обрабатывать события по мере взаимодействия с ресурсами Azure.
- Azure DevOps – это простой способ планирования, отслеживания и управления проектами, а также командами.
- Azure DevTest Labs упрощает доступ к готовым VM, настроенным под вас.
- Портал Azure – это веб-интерфейс для взаимодействия со службами Azure. Он использует обращения к ARM API во внутренней структуре для взаимодействия с ресурсами Azure.
- Azure PowerShell Az – кросс-платформенный модуль PowerShell, упрощающий управление ресурсами Azure в PowerShell.
- Azure CLI является кросс-платформенным средством командной строки, оно может быть написано на разных языках.
- Azure Cloud Shell предоставляет доступ к Azure из командной строки практически с любого устройства.
- Cloud Shell сохраняет все скопированные файлы при помощи учетной записи хранилища Azure.
- Мобильное приложение Azure позволяет управлять ресурсами Azure с устройства на базе iOS или Android.
- Помощник Azure предоставляет рекомендации по передовым практикам в области высокой доступности, безопасности, производительности и стоимости.
- Azure Monitor объединяет показатели для ресурсов Azure. Вы можете создавать оповещения на основе этих показателей.
- Служба работоспособности Azure предоставляет информацию, связанную с инцидентами Azure, влияющими на ваши ресурсы.



ГЛАВА 4

Описание общих функций безопасности и обеспечения безопасности сети

До этого момента мы затрагивали аспекты безопасности Azure, но не погружались в эту тему. Мы поговорим о безопасности в данной главе. По понятным причинам безопасность представляет собой весомый интерес для тех пользователей, которые осуществляют миграцию в облако. Таким образом в облако перемещаются большие объемы данных, некоторые из которых являются строго конфиденциальными, из-за чего важно обеспечить их защиту от посторонних глаз. Компании также хотят обеспечить контроль доступа своих сотрудников к облачным ресурсам. Кроме того, многие предприятия имеют свои стандарты и политики, которым они должны соответствовать, и им необходимо удостовериться, что облачный провайдер тоже отвечает этим стандартам.

Azure помогает разобраться со всеми необходимыми требованиями. Центр безопасности Azure (Azure Security Center) позволяет убедиться пользователям в том, что рекомендации по обеспечению безопасности соблюдаются. Хранилище ключей Azure (Azure Key Vault) дает гарантии шифрования секретной информации. Azure Sentinel помогает отслеживать ваши ресурсы Azure на предмет угроз и реагировать на них.

Угрозы безопасности являются серьезной проблемой для большинства предприятий, и Azure также затрагивают эту область. В данной главе мы поговорим об углубленной защите данных. Мы рассмотрим группы безопасности сети (Network Security Groups, NSG) для управления трафиком сети, брандмауэр Azure (Azure Firewall) для защиты сети от злоумышленников, защиту от DDoS-атак (Azure DDoS Protection) в качестве решения, предотвращающего вредоносную атаку, которая оказывает влияние на доступ к сетевым ресурсам.

Навыки, описанные в этой главе:

- описание функций безопасности Azure;
- описание безопасности сети в Azure.



Навык 4.1: описание функций безопасности Azure

Задайте вопрос пользователям, мигрирующим в облако, о том, что их беспокоит больше всего. Вы наверняка получите ответ – безопасность. Но что же именно значит «безопасность»? Понятие безопасности многогранно. Оно начинается с проверки правильности настроек ресурсов для обеспечения безопасности. Однако даже при корректной настройке вы все равно рискуете попасть под атаки злоумышленников. Другие угрозы могут исходить изнутри, поскольку сотрудники получают доступ к конфиденциальным данным и системам. Некоторые сотрудники могут преднамеренно нарушить требуемые меры безопасности, другие – могут случайным образом создать проблему безопасности.

Содержание раздела:

- центр безопасности Azure (Azure Security Center);
- хранилище ключей Azure (Key Vault);
- Azure Sentinel.

Центр безопасности Azure (Azure Security Center)

Многие компании имеют специалистов, чьей работой является изучение передового опыта и обеспечение его соответствия для организации. Когда дело касается Azure, то это ставит специалистов в затруднительное положение из-за большого количества доступных служб. Поскольку Azure постоянно развивается и меняется, то это еще больше усложняет задачу.

Центр безопасности Azure (Azure Security Center) предлагает вам условия для освоения передового опыта, а также дает вам инструкции, для того чтобы ваши ресурсы были настроены корректно с точки зрения безопасности. Центр безопасности даже обеспечивает для вас безопасность локальных ресурсов.

Центр безопасности предлагает два уровня обслуживания:

- **Free** (Бесплатный) – предоставляет общую оценку и рекомендации по обеспечению безопасности ресурсов Azure и охватывает только виртуальные машины и службу приложений;
- **Standard** (Стандартный) – добавляет покрытие баз данных Azure SQL, MySQL, PostgreSQL и хранилища BLOB-объектов, а также дополнительные функции, такие как расширенное обнаружение угроз, Microsoft Threat Intelligence и управление соответствием нормативным требованиям ваших

ресурсов Azure. Уровень Standard тарифицируется по часам, а подробную информацию о ценах можно найти на сайте <https://azure.microsoft.com/en-us/pricing/details/security-center>.

Чтобы начать работу с центром безопасности, выберите пункт **Security Center** (Центр безопасности) в меню портала Azure. Вам откроется блейд **Overview** (Обзор), где вы можете увидеть обзор всех ваших ресурсов, защищенных центром безопасности, как показано на рис. 4.1.

Существует три основные области покрытия в центре безопасности:

- **Policy & Compliance** (Политика и соответствие требованиям). Обеспечивает безопасность и общую оценку надежности ресурсов. Эта область также охватывает ваше соответствие нормативным стандартам;
- **Resource Security Hygiene** (Гигиена безопасности ресурсов). Предоставляет общий обзор состояния ресурсов с точки зрения безопасности. Проблемы безопасности классифицируются как имеющие высокую, среднюю или низкую степень серьезности;
- **Threat protection** (Защита от угроз). Показывает все активные или прошлые атаки, а также угрозы для ваших ресурсов.

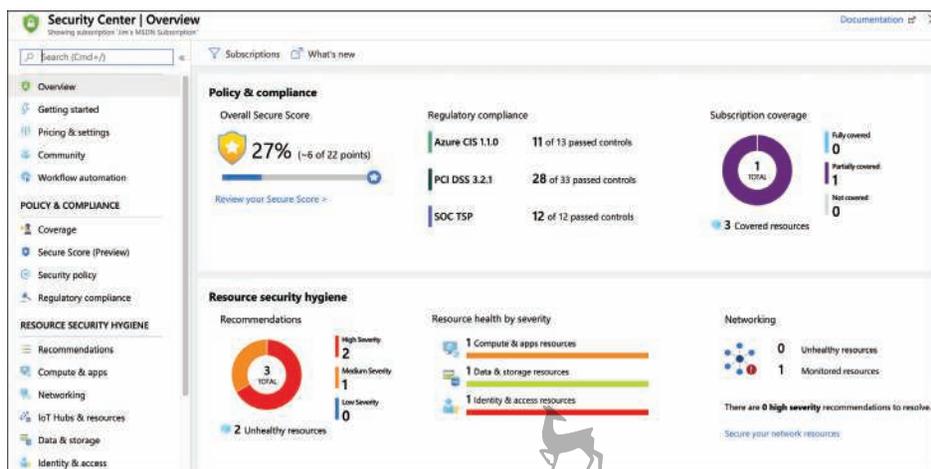


Рис. 4.1 Центр безопасности Azure

Информация по первым двум областям предоставляется охраняемой службой. Эта информация часто связана с лучшими практиками. Защита от угроз, с другой стороны, специально направлена на анализ как сетевого трафика, так и поведения пользователей ваших ресурсов. Если что-то выглядит подозрительно, об этом сообщает Центр безопасности.

Microsoft Threat Intelligence применяется для идентификации угроз безопасности. Threat Intelligence использует исторические данные Microsoft и машинное обучение для выявления возможных угроз. Эти угрозы могут оказаться хакером, пытающимся получить доступ к ресурсу, или они могут быть связаны с подозрительной деятельностью пользователя. Например, если пользователь повышает свои привилегии на виртуальной машине и запускает неизвестный

процесс, это, скорее всего, будет помечено как инцидент, который должен быть расследован.

Нажав на элемент в блейде **Overview** (Обзор), вы можете ознакомиться с деталями. На рис. 4.2 мы нажали кнопку **Compute & Apps** (Вычисления и приложения) в блоке **Overview** (Обзор). Такое представление отображает для вас доступные рекомендации. Вы также можете увидеть, насколько улучшится ваш показатель защиты (secure score) при обращении к каждой рекомендации.

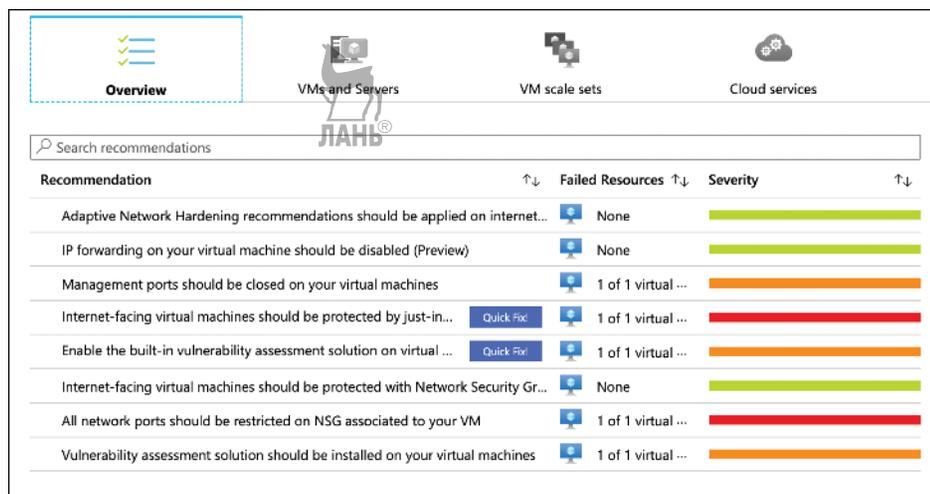


Рис. 4.2 Обзор рекомендаций по вычислительным ресурсам Azure в центре безопасности

Нажатие на одну из рекомендаций позволит получить дополнительную информацию. В большинстве случаев вы увидите ссылку на инструкции по выполнению рекомендации, но Центр безопасности и сам умеет автоматически исправлять их. Возле рекомендаций, которые могут быть автоматически исправлены, отобразится значок **Quick Fix** (Быстрое исправление), как показано на рис. 4.2.

Одной из главных угроз безопасности облачных ресурсов являются открытые сетевые порты на VM. Доступ к VM с помощью удаленного рабочего стола для VM Windows или SSH для VM Linux является необходимой частью управления этими ресурсами, но хакеры обычно используют сетевые порты для удаленного управления, чтобы взломать VM. Центр безопасности предоставляет функцию, называемую доступом по принципу «точно в срок» (just-in-time, JIT), которая помогает защитить VM от атак на порты управления.

Если включен JIT-доступ, пользователи должны запросить доступ к VM, чтобы удаленно войти в нее. До тех пор, пока кому-либо не будет предоставлен доступ, порты управления на VM закрываются. После того как пользователь получает доступ, порты открыты в течение определенного периода времени в соответствии с запросом пользователя. По истечении этого периода времени порты управления снова закрываются.

Чтобы включить JIT-доступ на VM, нажмите кнопку **Just In Time VM Access** (JIT-доступ к VM) в Центре безопасности, как показано на рис. 4.3. Перейдите

на вкладку **Recommended** (Рекомендуемые), чтобы просмотреть ВМ, которые в настоящее время не настроены для JIT-доступа. Выберите одну или более ВМ и нажмите **Enable JIT** (Включить JIT) для активации этой функции.

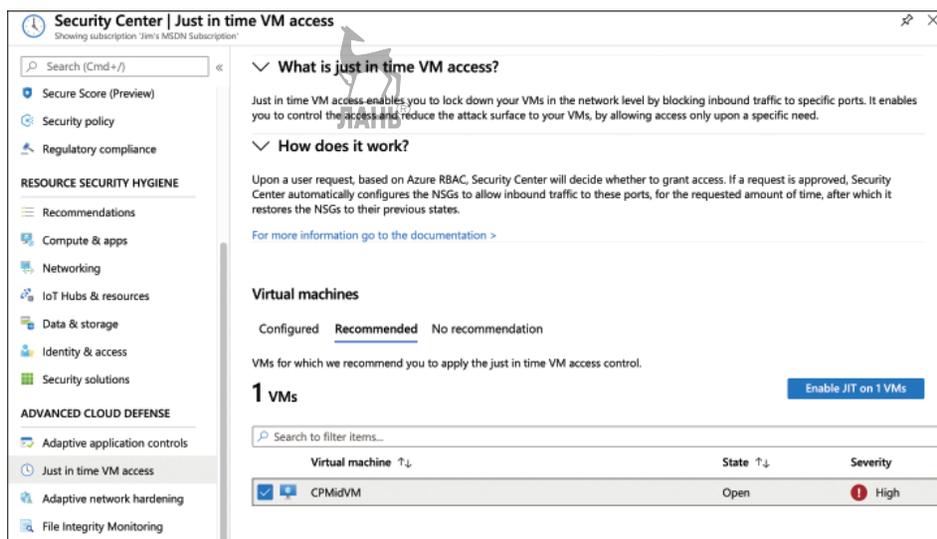


Рис. 4.3 Включение доступа JIT на ВМ

При включении JIT-доступа можно выбрать порты, которые вы хотите защитить, как показано на рис. 4.4. В списке перечислены рекомендуемые порты для управления, но вы можете добавить и свои собственные. Например, если вы изменили конфигурацию ВМ, чтобы управление происходило на нетипичном порту, вы можете добавить этот порт для JIT-доступа.

Помимо указания порта, вы также можете контролировать, какие IP-адреса и протоколы разрешены через порт. Если для разрешенных IP-адресов установлено значение **Per Request** (По запросу), пользователь, запрашивающий доступ, будет иметь возможность указать IP-адрес или блок IP-адресов в бесклассовом формате (Classless Inter-Domain Routing, CIDR). В противном случае можно указать блок CIDR самостоятельно, чтобы разрешить доступ только из определенного диапазона IP-адресов.

Когда пользователь запрашивает доступ, то количество часов, в течение которых предоставляется доступ, может быть не более максимального значения, указанного в конфигурации порта. Максимальное время запроса может быть настроено от 1 до 24 часов, по умолчанию оно равно 3 часам.

После настройки ВМ для JIT-доступа пользователи запрашивают доступ из Центра безопасности. После нажатия кнопки **Just In Time VM Access** (JIT-доступ к ВМ) выберите ВМ и нажмите кнопку **Request Access** (Запросить доступ), как показано на рис. 4.5.

Как уже было показано на рис. 4.6, пользователи, запрашивающие доступ, должны указать порты для открытия, разрешенные IP-адреса (при условии что они не были указаны при включении JIT-доступа для ВМ) и на какое время по-

требуется доступ (вплоть до максимально возможного). После нажатия кнопки **Open Ports** (Открыть порты) запрашиваемые порты остаются открытыми в течение указанного периода времени.

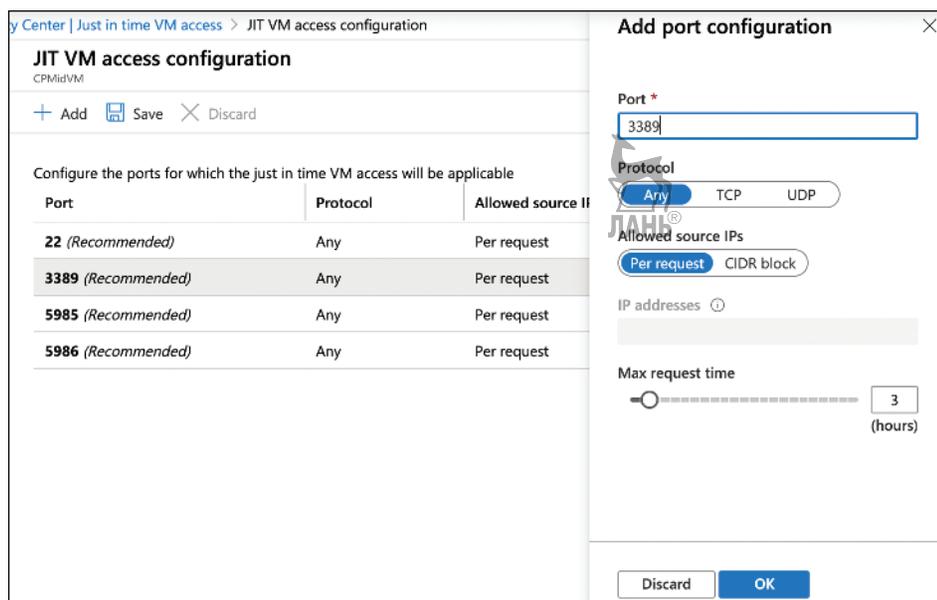


Рис. 4.4 Конфигурация JIT-доступа

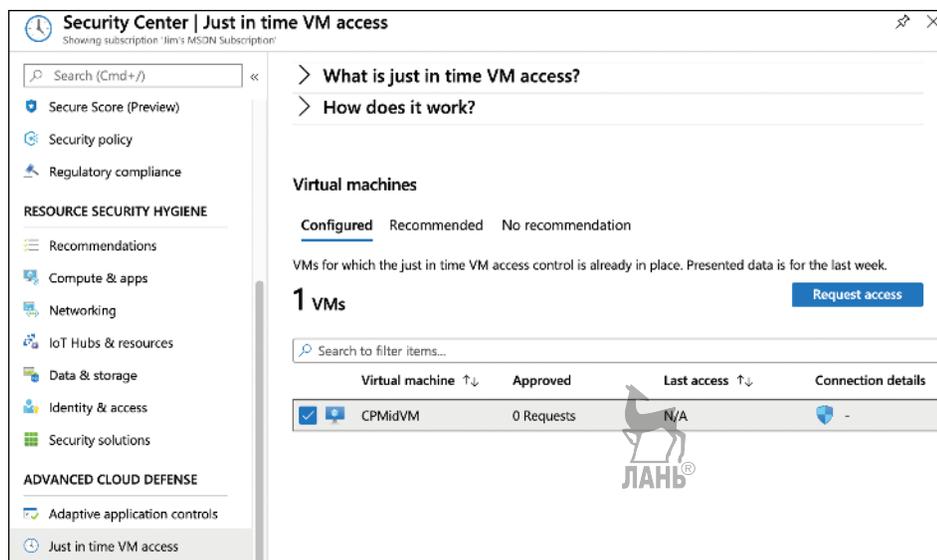


Рис. 4.5 Запрос JIT-доступа

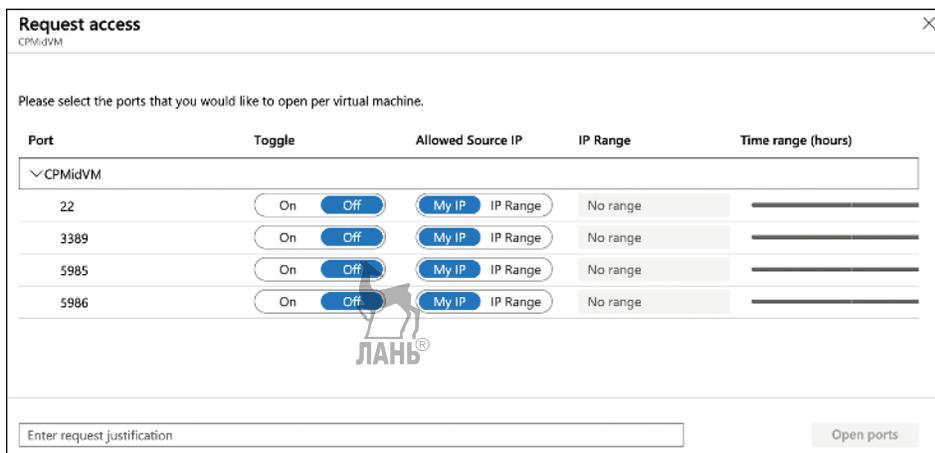


Рис. 4.6 Сведения по запросу JIT-доступа

Хранилище ключей Azure (Azure Key Vault)

Большинство приложений используют конфиденциальную или секретную информацию. Например, приложение, использующее базу данных, должно знать, как подключиться к этой базе данных, и эта информация о подключении хранится в строке подключения. Строка подключения может содержать имя пользователя и пароль, защищающие базу данных, и сохранение этого имени пользователя и пароля в текстовом файле будет представлять собой очевидную угрозу безопасности.

Хранилище ключей Azure предоставляет безопасный способ хранения секретов, ключей и сертификатов. После сохранения элемента в хранилище ключей можно применить политики безопасности, определяющие, какие пользователи и приложения могут получить к нему доступ. Azure Key Vault шифруется с помощью ключей шифрования, но Microsoft не имеет доступа к этим ключам или зашифрованным данным.

Хранилища ключей создаются на портале Azure, как показано на рис. 4.7.

В хранилище ключей доступно два уровня ценообразования: стандартный и премиум. Единственное различие между ними заключается в том, что ключи хранятся в аппаратных модулях безопасности (hardware security module, HSM) на уровне премиум. HSM – это отдельная часть оборудования, предназначенная для безопасного хранения зашифрованного содержимого, а также для обработки криптографических данных.



СОВЕТ К ЭКЗАМЕНУ

Хранение ключей шифрования в границе HSM требуется для Федерального стандарта обработки информации США (Federal Information Processing Standard, FIPS) 140-2, поэтому компании, которым необходимо поддерживать соответствие стандарту FIPS 140-2, могут сделать это с помощью уровня премиум.

Create key vault ✕

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Key vault name *

Region *

Pricing tier *

Soft delete Enable Disable

Retention period (days) *

Purge protection Enable Disable

Рис. 4.7 Создание хранилища ключей

Вы можете импортировать ключ, секрет или сертификат в хранилище ключей, но это хранилище также может сгенерировать для вас ключи безопасности и сертификаты. Например, может потребоваться создать ключ безопасности, который ваша компания может использовать для подписи сертификатов. Если вы хотите создать для этой цели 4096-битный ключ безопасности и сохранить его в хранилище ключей, нажмите кнопку **Keys** (Ключи), а затем нажмите кнопку **Generate/Import** (Создать или импортировать), как показано на рис. 4.8.

На рис. 4.9 изображен 4096-битный ключ RSA, который создается и добавляется в хранилище ключей.

Как показано на рис. 4.10, после сохранения ключа можно просмотреть запись, чтобы получить идентификатор ключа, URL-адрес, который можно использовать для получения ключа авторизованными пользователями или приложениями. Однако вы можете получить ключ только через его идентификатор, поскольку он зашифрован и недоступен.

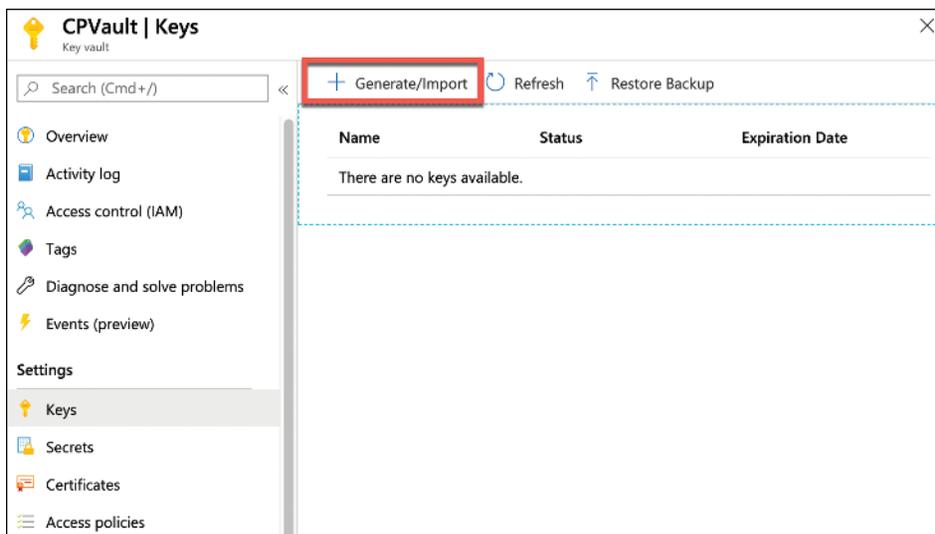


Рис. 4.8 Добавление ключа в хранилище ключей

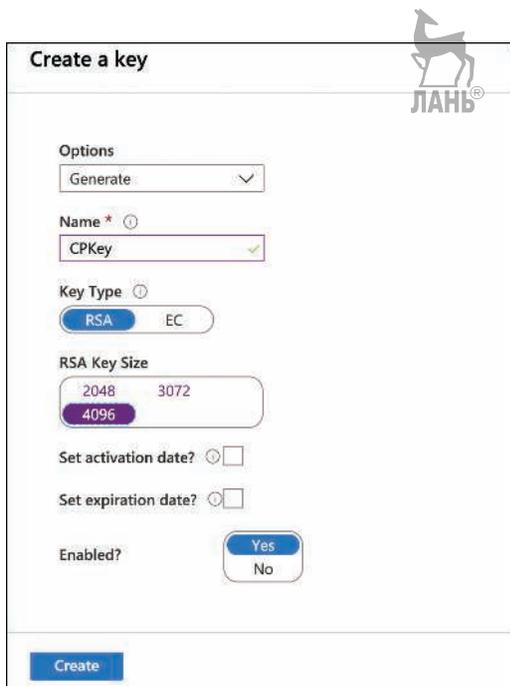


Рис. 4.9 Создание ключа RSA



СОВЕТ К ЭКЗАМЕНУ

Ключ, хранящийся в Azure Key Vault, обычно предоставляется приложением программно. Чтобы защитить ключ, разработчики приложений могут извлекать его каждый раз, когда он нужен, вместо того чтобы извлекать его один раз и сохранять в памяти. Это гарантирует, что ключ остается безопасным.

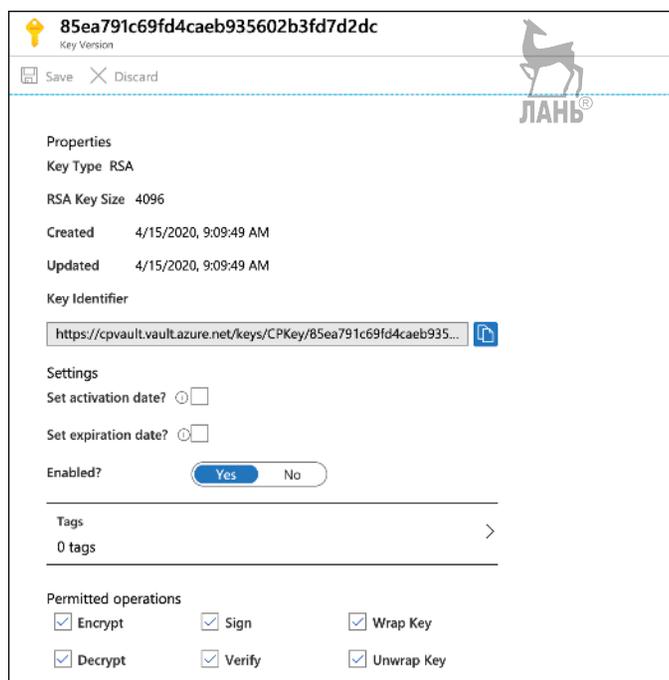


Рис. 4.10 Подробные сведения о ключе

Другим распространенным сценарием использования хранилища ключей является хранение ключей шифрования для виртуальных машин Azure. Одна из рекомендаций по безопасности, предлагаемых Security Center, заключается в шифровании дисков виртуальной машины. Диск виртуальной машины хранится в виде файла VHD, и когда он зашифрован, операционная система хоста, на котором выполняется виртуальная машина, должна иметь доступ к ключу безопасности, чтобы расшифровать VHD и запустить виртуальную машину. Key Vault предлагает возможности, специально предназначенные для такого рода сценариев.

Для использования хранилища ключей для ключей шифрования диска политики доступа должны быть настроены таким образом, чтобы разрешить шифрование диска в хранилище. Если этого не было сделано при создании хранилища, эту настройку можно изменить, выбрав **Access Policies** (Политики доступа) и включив доступ к шифрованию дисков Azure **Azure Disk Encryption For Volume Encryption**, как показано на рис. 4.11.

Шифрование дисков Azure включается на VM с помощью Azure PowerShell или интерфейса командной строки Azure либо шаблона ARM.

ДОПОЛНИТЕЛЬНО ВКЛЮЧЕНИЕ ШИФРОВАНИЯ

Чтобы включить шифрование и хранить ключи в хранилище ключей, виртуальные машины и Key Vault должны находиться в одной подписке Azure и одном регионе Azure. Дополнительные сведения о требованиях к шифрованию диска и действиях по его включению смотрите в разделе <https://bit.ly/az900-keyvaultvm>.

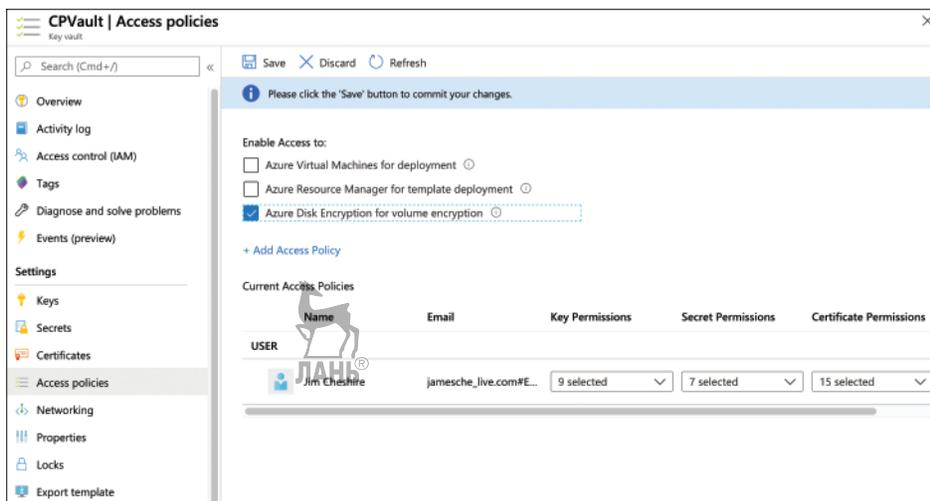


Рис. 4.11 Настройка политик доступа для разрешения доступа к шифрованию дисков Azure

Azure Sentinel

Говоря о защите данных и ресурсов, многие компании используют проверенные платформы, предназначенные для наиболее важных моментов, таких как SOAR, Security Orchestration, Automation, and Response (управление безопасностью, автоматизация и реагирование) или SIEM, Security Information and Event Management (управление безопасностью информации и событиями). В действительности многие компании используют комбинацию SOAR и SIEM.

Внедрение SOAR и SIEM может вызвать много сложностей. Большинство компаний нанимают экспертов по безопасности для их внедрения на предприятии. Microsoft хотела упростить внедрение SOAR и SIEM даже для обычных пользователей. Результатом этой работы стало появление Azure Sentinel.



СОВЕТ К ЭКЗАМЕНУ

Azure Sentinel предназначен не только для Azure. Azure Sentinel способен формировать отчеты об угрозах, проводить анализ для локальных и облачных ресурсов.

Перед началом использования Azure Sentinel вам нужно создать рабочую область Sentinel. Сделав это, вы увидите экран рабочих пространств Azure (Azure Sentinel Workspaces screen), изображенный на рис. 4.12. Нажмите на **Connect Workspace** (Подключить рабочее пространство) для создания экземпляра Azure Log Analytics (аналитики журналов) и добавьте его в рабочее пространство Sentinel. Если у вас уже имеется экземпляр Log Analytics, вы можете выбрать его для добавления в Azure Sentinel.

После добавления Log Analytics в Azure Sentinel вы подключаете источники данных к Sentinel, используя *коннекторы* при помощи нажатия на кнопку **Connect** (Подключить), как видно на рис. 4.13.

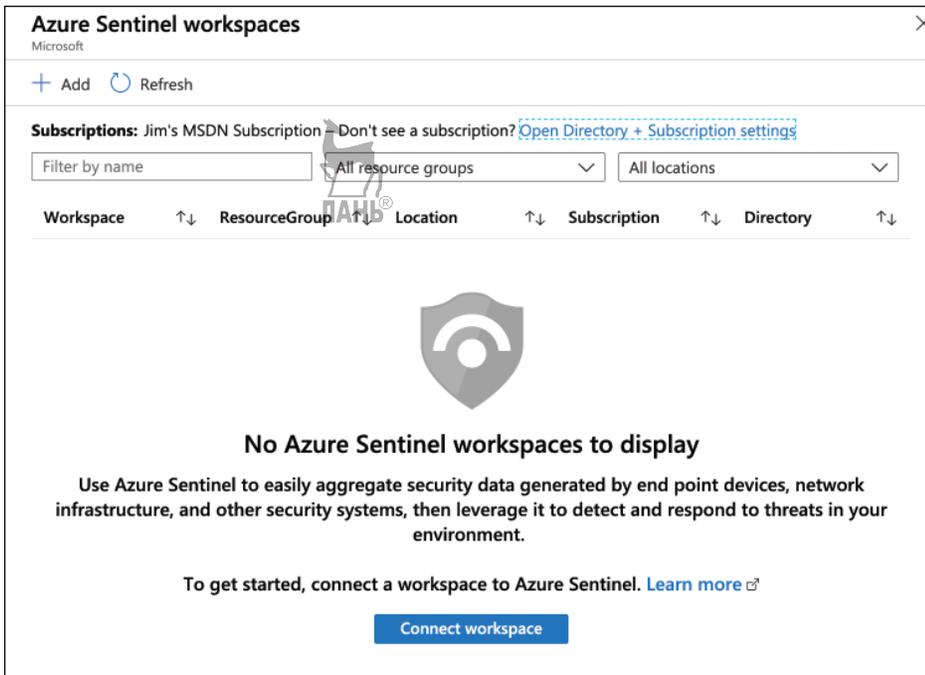


Рис. 4.12 Создание рабочего пространства Azure Sentinel

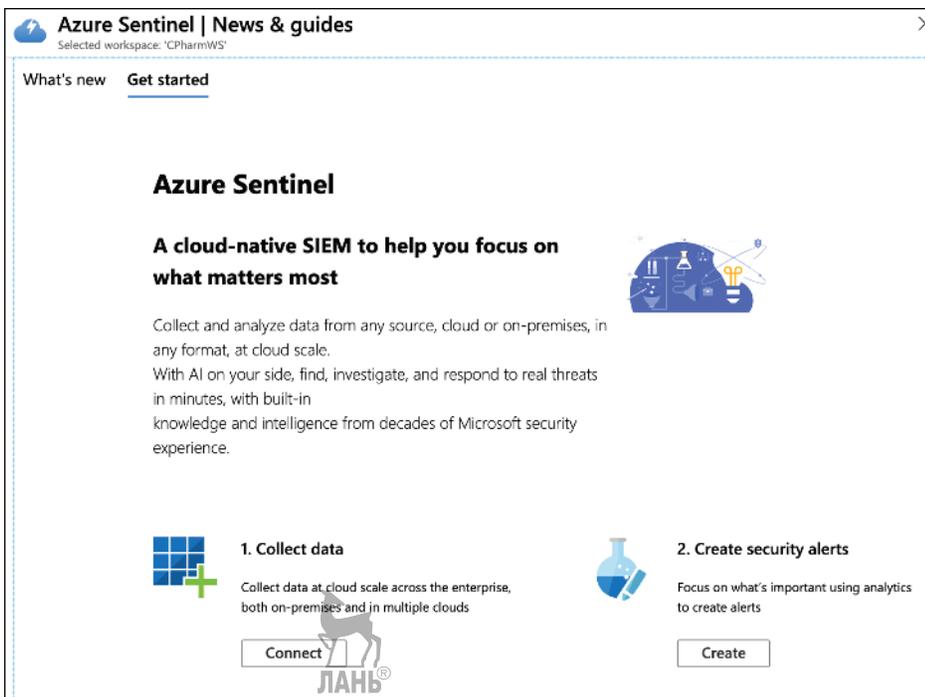


Рис. 4.13 Сбор данных при помощи Azure Sentinel

ПРИМЕЧАНИЕ AZURE SENTINEL И LOG ANALYTICS

Azure Sentinel находится выше Log Analytics. Поскольку Log Analytics собирает информацию из ресурсов Azure, служба Azure Sentinel отслеживает данные на предмет наличия угроз.

Microsoft предоставляет коннекторы для Azure и других своих продуктов, но есть и сторонние коннекторы. На рис. 4.14 показан коннектор для веб-служб Амазона (Amazon Web Services).

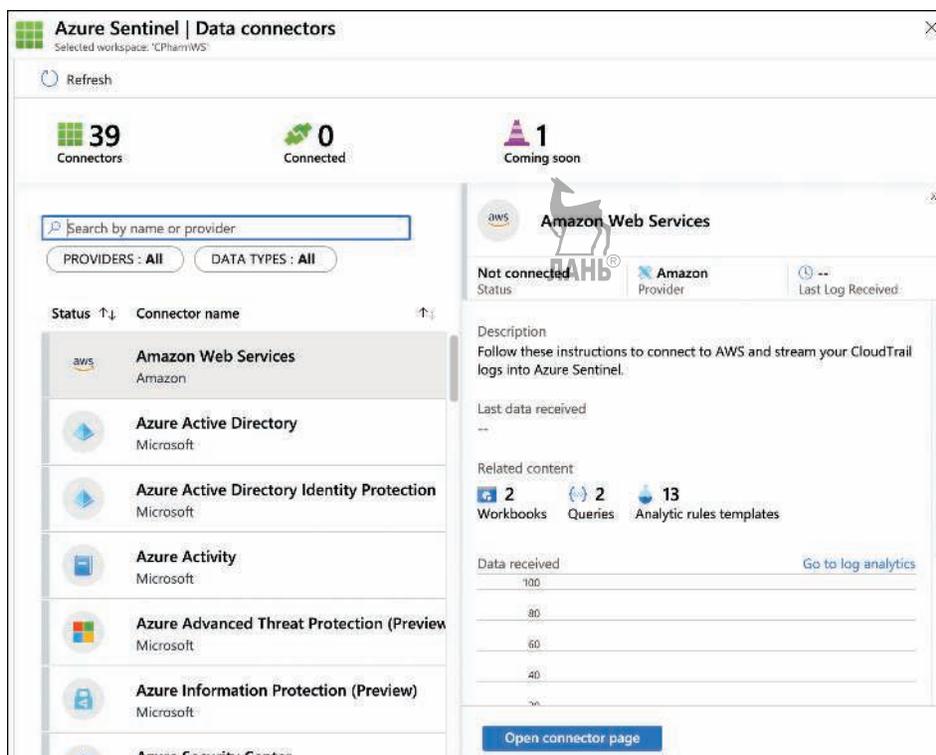


Рис. 4.14 Добавление коннектора в Sentinel

Добавив коннектор, вы увидите обязательные для него условия вместе с этапами, которые нужно выполнить. На рис. 4.15 показано, как мы добавили коннектор для Azure Active Directory.

Список обязательных условий – это активный список, в котором отображено текущее состояние условий. На рис. 4.15 показано, что все обязательные условия были выполнены, кроме требования к лицензии Azure Active Directory, что и обозначено значком X.

Кнопка **Next Steps** (Дальнейшие шаги) позволяет вам выполнить действия, необходимые для завершения процесса добавления коннектора. На рис. 4.16 вы видите дальнейшие шаги по настройке коннектора Azure Active Directory.

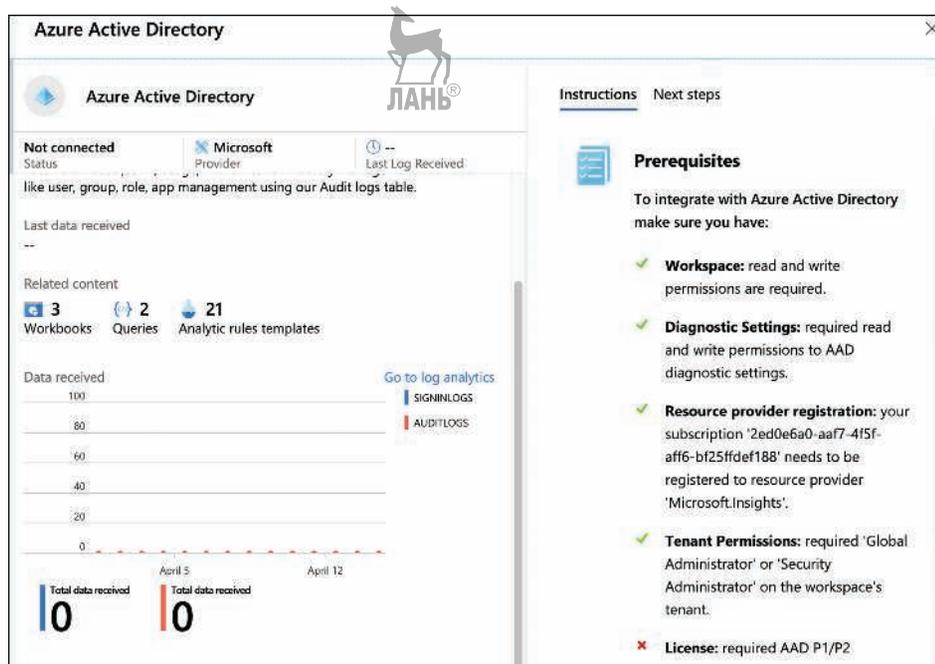


Рис. 4.15 Коннектор Azure Active Directory в Sentinel

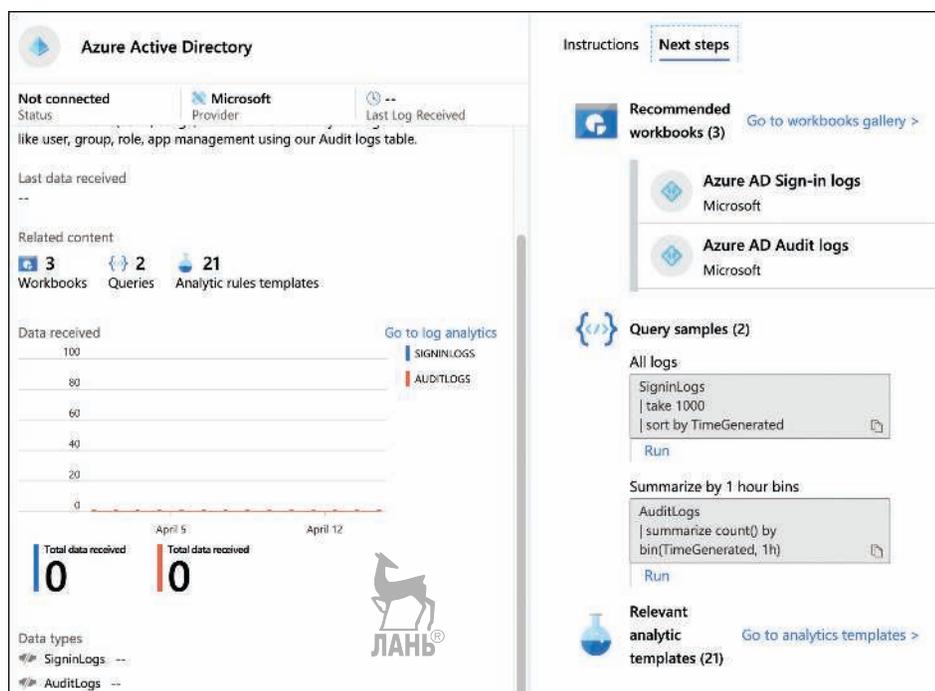


Рис. 4.16 Дальнейшие шаги по конфигурации коннектора Azure Active Directory в Sentinel

После добавления коннектора сохраните конфигурацию в рабочей книге Azure Monitor (Azure Monitor Workbook). Рабочие книги позволяют вам легко агрегировать данные для более простого использования.

Azure Sentinel способен выискивать определенные угрозы безопасности. Он знает несколько запросов для поиска всевозможных угроз. Кнопка **Hunting** (Поиск, от англ. охота) позволяет вам выбрать запрос, который вам нужно выполнить со своими ресурсами, как показано на рис. 4.17.

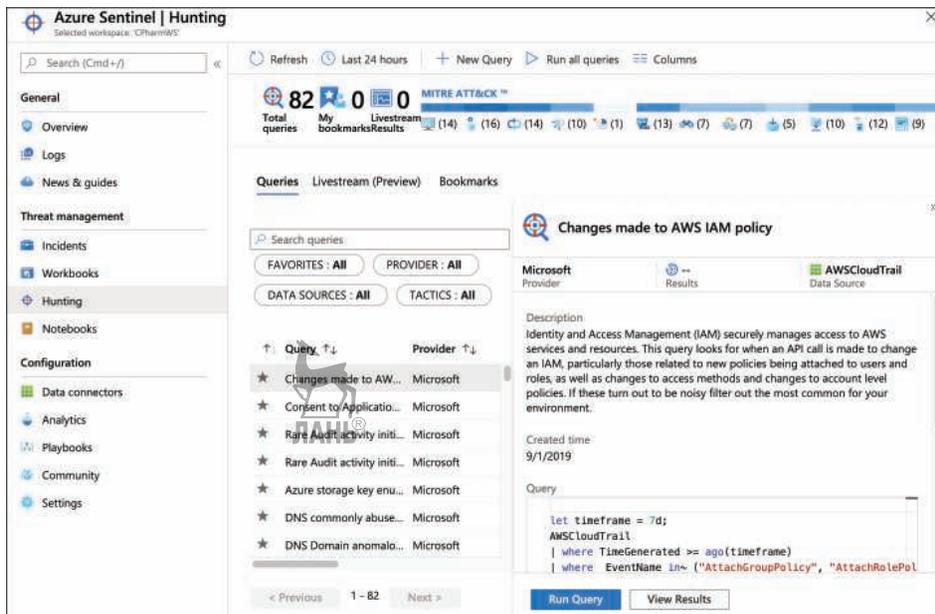


Рис. 4.17 Поиск угроз в Azure Sentinel

Когда Sentinel находит проблему, вы можете задать ему ответное действие на нее при помощи *набора сценариев* (Playbook). Playbook – это рабочий процесс, который выполняется в ответ на оповещение в Sentinel. Для его создания нажмите **Playbook**, а затем **Add Playbook** (Добавить набор сценариев), как показано на рис. 4.18.

При создании нового набора сценариев Sentinel запросит у вас создание нового Logic App, потому как он использует Logic Apps для своих рабочих процессов. На момент написания книги было мало пользовательского опыта. После создания Logic App вам нужно будет нажать **Blank Logic App** (Пустой Logic App), как показано на рис. 4.19.



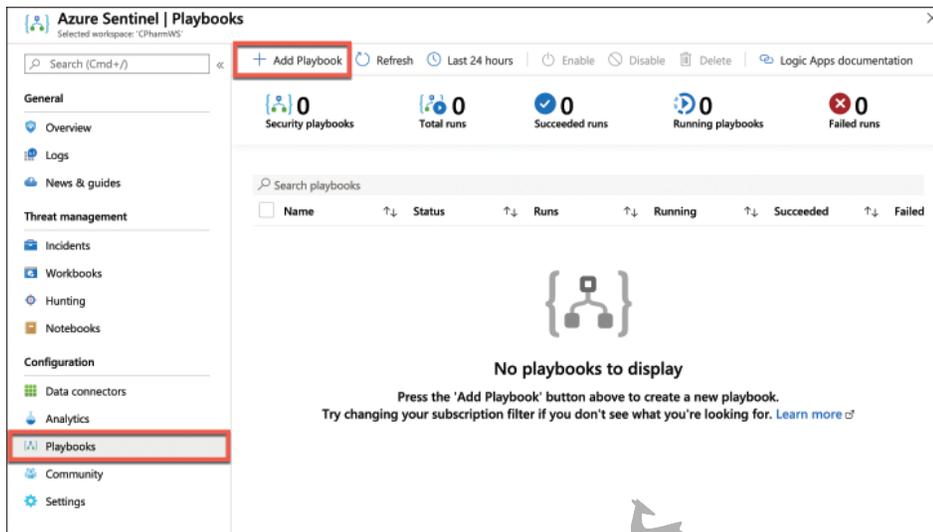


Рис. 4.18 Добавление набора сценариев в Sentinel

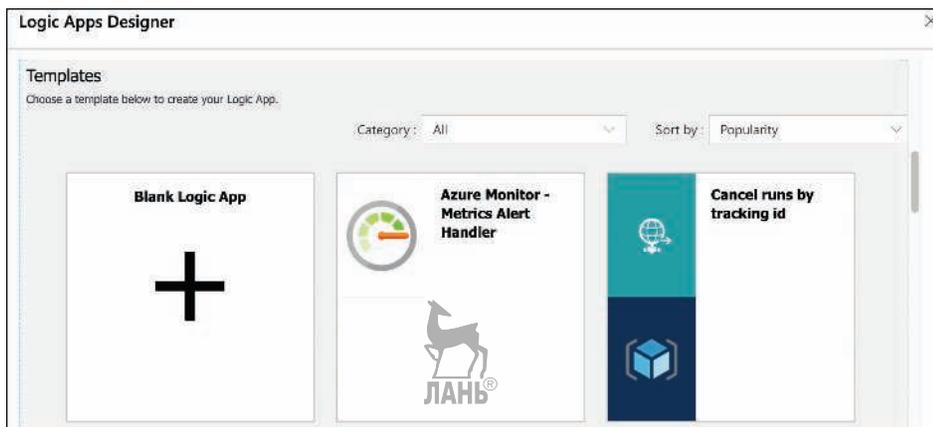


Рис. 4.19 Создание новой логики приложения для набора сценариев Sentinel

Введите **sentinel** в поле поиска и нажмите **When A Response To An Azure Sentinel Alert Is Triggered** (Появление ответа на появившееся оповещение Azure Sentinel), как показано на рис. 4.20. После этого вы можете продолжить построение рабочего процесса и добавить действия, которые бы вы хотели выполнять при появлении оповещения (предупреждения).

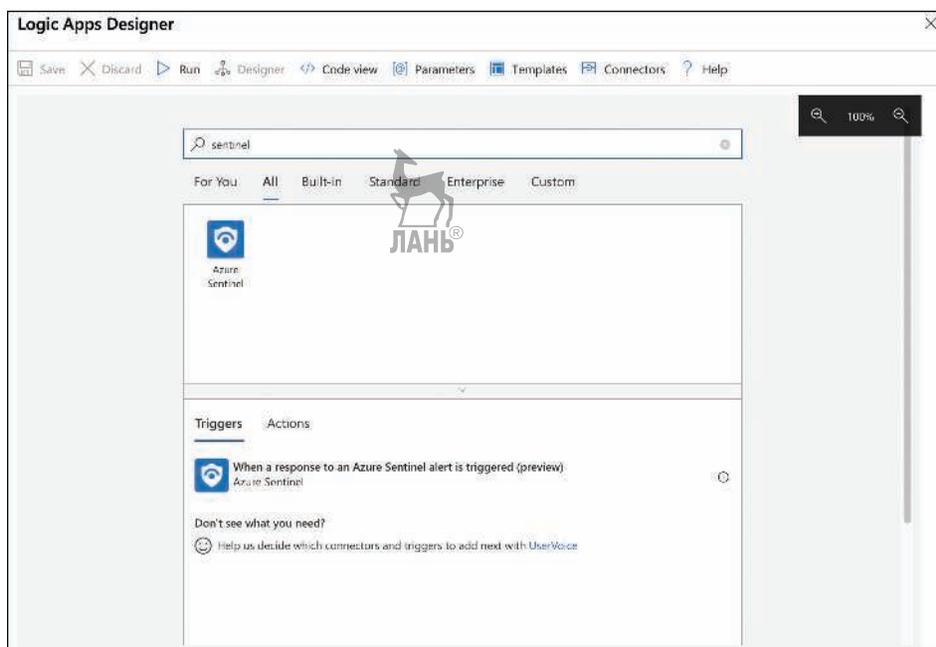


Рис. 4.20 Добавление переключающего события для Azure Sentinel в логике приложения

Навык 4.2: описание безопасности сети в Azure

Другой компонент безопасности связан с сетевыми подключениями. Для обеспечения такой безопасности требуется совершенно другой набор инструментов и навыков. Как и при планировании безопасности данных и ресурсов, предприятия часто тратятся на специалистов, которые обеспечивают им сетевую безопасность. Однако в Azure большая часть безопасности сетевых подключений должна обеспечиваться за вас. Несмотря на это, вам все же придется предпринять некоторые действия, чтобы себя обезопасить.

Содержание раздела:

- глубокая защита (Defense in depth);
- группы сетевой безопасности (Network Security Groups, NSGs);
- брандмауэр Azure (Azure Firewall);
- защита от DDoS-атак (Azure DDoS Protection).

Глубокая защита

Перенесемся на мгновение в Средневековье. Представьте, каково это было – жить в замке. Непростое время во всех отношениях. Всегда была некая враждебная сила, которая пыталась проникнуть в крепость. Чтобы предотвратить вторжение, вокруг замков строили рвы, целью которых было помешать вражеским силам проложить туннель под стеной и проникнуть внутрь.

Еще до того, как враг достигал рва, вдоль высокой стены замка его поджидали лучники, которые представляли для нападающих большую опасность. Скажем, враги смогли пережить лучников и преодолеть ров, далее их поджидали высокая стена с крепкими воротами. Пройдя через ворота, они бы встретили вооруженную армию противника.

У средневековых людей было очень хорошее представление о безопасности. Они поняли, что для того, чтобы как-то себя обезопасить, одной преграды для атакующих будет недостаточно. Им необходима была многоуровневая оп-позиция, чтобы, преодолевая один метод безопасности, врагам пришлось бы столкнуться с другим.

Описанный выше пример прекрасно иллюстрирует суть «глубокой обороны», которую иногда даже именуют «замковым подходом». В рамках безопасности сетевых подключений этот многоуровневый подход является лучшим способом для защиты. Брандмауэр Azure помогает предотвратить проникновение злоумышленников в вашу сеть, группы сетевой безопасности помогают вам контролировать сетевой трафик в сети, а защита от DDos-атак Azure способствует идентификации и уменьшению воздействия вредоносного трафика, который на первый взгляд может показаться обычным.

Группы сетевой безопасности (Network Security Group)

Группа сетевой безопасности (Network Security Group, NSG) позволяет фильтровать трафик в сети и применять правила для этого трафика. NSG содержит несколько встроенных правил, предоставляемых Azure, которые позволяют вашим ресурсам в виртуальной сети взаимодействовать друг с другом. Затем можно добавить собственные правила в NSG для управления трафиком в сеть и из сети, а также между ресурсами в сети.

На рис. 4.21 представлено многослойное приложение.

Ниже представлен поток трафика данного приложения:

- подсеть 1 получает данные из другой виртуальной сети, на которой работает брандмауэр Azure;
- подсеть 1 взаимодействует с подсетью 2 для обработки запросов;
- подсеть 2 взаимодействует с сервером базы данных в подсети 3 для доступа к данным.

Если вы хотите обеспечить безопасную среду, подсеть 1 не должна иметь возможности напрямую взаимодействовать с ресурсами в подсети 3. Анало-

гичным образом нельзя, чтобы подсеть 3 напрямую взаимодействовала с ресурсами в подсети 1. Только у подсети 1 должна быть возможность взаимодействия с виртуальной сетью, в которой работает брандмауэр Azure. Можно использовать NSG для реализации правил, которые будут применять эти политики.

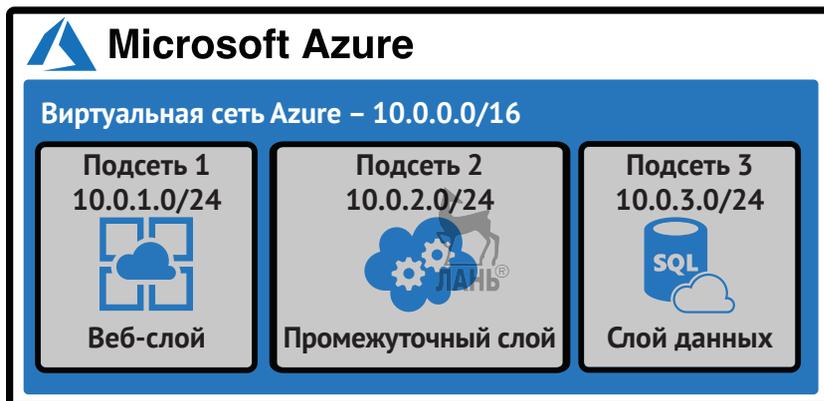


Рис. 4.21 Многослойное приложение

NSG могут быть связаны с подсетью или сетевым интерфейсом, подключенным к ВМ. Каждый сетевой интерфейс или подсеть может иметь только одну NSG, но вы можете создать до 1000 правил в одной NSG, поэтому вы легко можете реализовать логику любой сложности, необходимую для любой задачи. Если вы связываете NSG с подсетью и с одним или несколькими сетевыми интерфейсами внутри этой подсети, то сначала применяются правила для сетевых интерфейсов, а затем – правила подсети.



СОВЕТ К ЭКЗАМЕНУ

NSG, связанная с подсетью, влияет на ВМ внутри этой подсети, а также на трафик в подсеть и из нее. Например, если настроить NSG для блокировки всего трафика, кроме трафика из интернета, и затем связать эту NSG с подсетью, содержащей две ВМ, то эти две виртуальные машины больше не смогут взаимодействовать друг с другом, поскольку только трафик из интернета разрешен NSG.

Чтобы правила не мешали друг другу, они должны иметь различный приоритет от 100 до 4096. Правила с более низким числом приоритета важнее правил с более высоким числом. К сетевому трафику применяется в первую очередь правило с наименьшим числом приоритета. Если трафик соответствует этому правилу, то оно применяется, и дальнейшая обработка прекращается. Если трафик не соответствует правилу, он проверяется по следующему в порядке приоритета. Это продолжается до тех пор, пока трафик не будет соответствовать одному из правил или пока все правила не кончатся.

ДОПОЛНИТЕЛЬНО ПРИОРИТЕТ ПРАВИЛ ПО УМОЛЧАНИЮ

Правила по умолчанию, применяемые Azure ко всем сетевым группам безопасности, имеют приоритет в диапазоне 65 000. Это позволяет избежать ситуации, когда правила по умолчанию имеют тот же приоритет, что и созданные вами. Вы также можете при необходимости переопределить правила по умолчанию.

Чтобы создать NSG, выполните поиск **Network Security Group** (Группа сетевой безопасности) в Azure Marketplace. При создании NSG присвойте ей имя, выберите или создайте группу ресурсов и укажите расположение для NSG из раскрывающегося меню **Region** (Регион), как показано на рис. 4.22.

Create network security group

Basics Tags Review + create

Project details

Subscription * Jim's MSDN Subscription

Resource group * AZ900
[Create new](#)

Instance details

Name * Subnet-1-NSG

Region * (US) East US

[Review + create](#) < Previous Next : Tags > [Download a template for automation](#)

Рис. 4.22 Создание NSG

После создания NSG можно добавить правила входящего и исходящего трафика для NSG. После открытия NSG на портале Azure щелкните **Inbound Security Rules** (Правила безопасности входящего трафика), чтобы добавить их, и **Outbound Security Rules** (Правила безопасности исходящего трафика), чтобы добавить и правила отправки данных.

На рис. 4.23 были выбраны **Inbound Security Rules** (Правила безопасности входящего трафика) для добавления нового правила, разрешающего трафик из виртуальной сети с брандмауэром Azure. После этого NSG будет связана с подсетью 1. Обратите внимание, что вы можете связать NSG с подсетью или сетевым интерфейсом перед добавлением правил.

Нажмите **Add** (Добавить), чтобы добавить новое правило NSG. На рис. 4.24 показано добавляемое правило, разрешающее трафик в эту подсеть из адресного пространства другой виртуальной сети, на которой работает брандмауэр Azure.

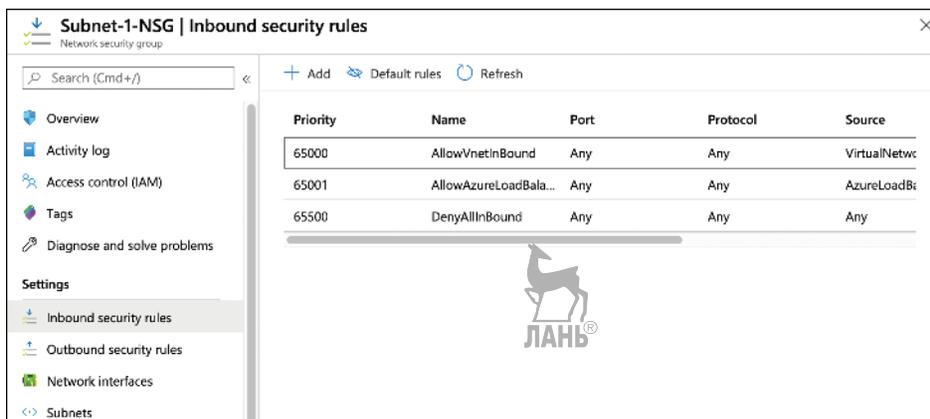


Рис. 4.23 Правила безопасности входящего трафика для NSG

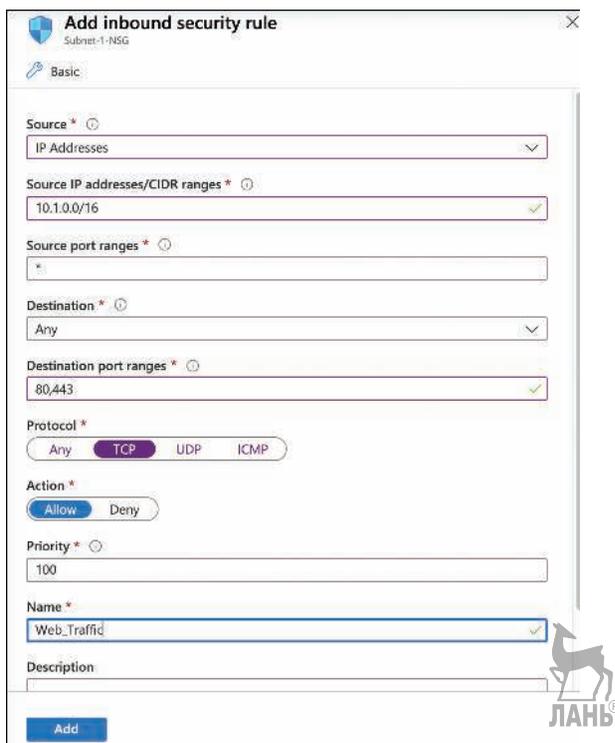


Рис. 4.24 Создание правила входящего подключения NSG

Правило, настроенное на рис. 4.24, использует нотацию CIDR для IP-адресов источника. Вы также можете ввести определенный IP-адрес или изменить раскрывающийся список **Source** (Источник) на **Any** (Любой), если необходимо, чтобы правило применялось ко всем IP-адресам. Нажмите **Add** (Добавить) для создания правила.

Создав правило, нажмите **Subnets** (Подсети), чтобы связать NSG с подсетью, или **Network Interfaces** (Сетевые интерфейсы) для связи с сетью, используемой ВМ. Затем нажмите **Associate** (Связать), как показано на рис. 4.25.

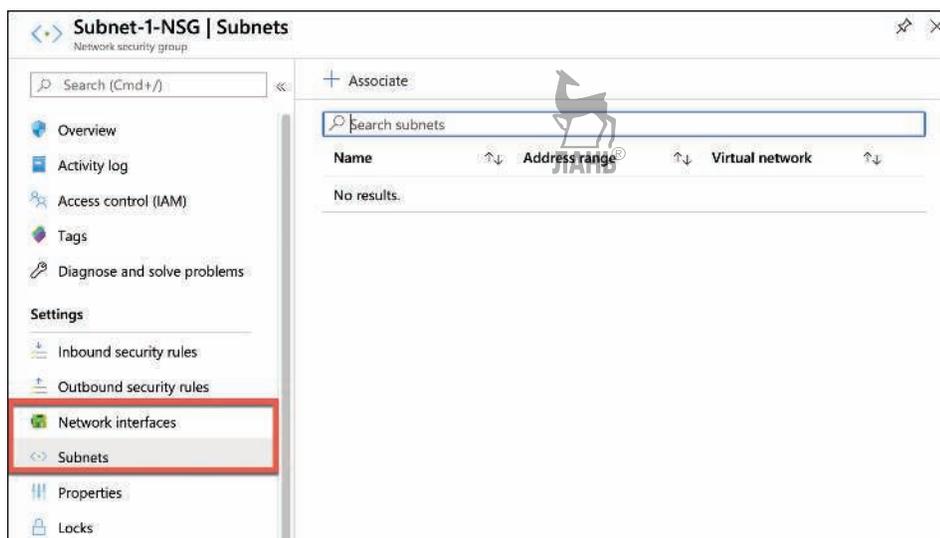


Рис. 4.25 Связывание NSG

На рис. 4.26 изображен блейд, на котором NSG связана с подсетью.

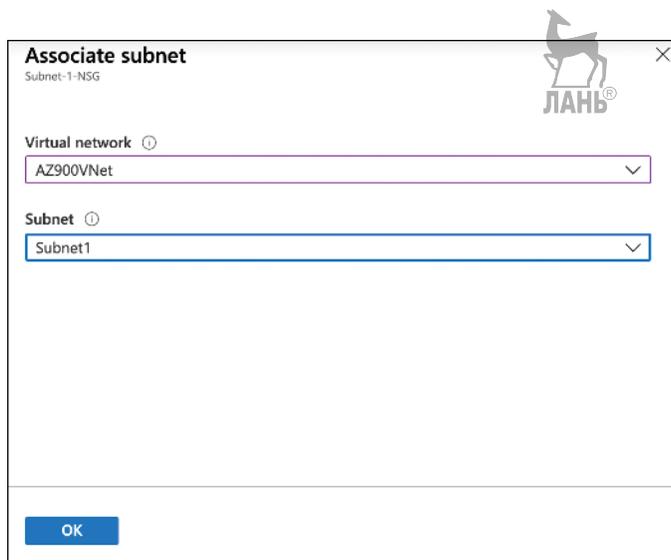


Рис. 4.26 Связывание NSG с подсетью

Правила безопасности исходящего трафика создаются таким же образом, как и входящего. Однако не требуется одновременно создавать парные прави-

ла для входящего и исходящего трафиков. NSG поддерживают так называемую *запись потока* (flow record), которая хранит состояние соединения и разрешает трафик, соответствующий этой записи, без необходимости создавать конкретное правило. Если правило безопасности разрешает входящий трафик на порт 80 с IP-адресов в диапазоне 10.1.0.0/16 (как, например, правило, настроенное на рис. 4.24), NSG также разрешает исходящий трафик с порта 80 адресам в том же диапазоне, используя запись потока. Только после того, как трафик остановится в течение нескольких минут, запись потока больше не будет действовать.

Есть случаи, когда вы не будете знать конкретный диапазон IP-адресов. Например, если вы хотите настроить правило NSG в виртуальной сети, разрешающее весь трафик из интернета, вы не указываете точный диапазон адресов. Чтобы справиться с этим, NSG позволяют использовать *теги службы* (service tags) при настройке правил.

Тег службы – это специальный идентификатор, созданный Microsoft, который применяется к определенному типу службы в Azure или в интернете. Например, если у вас есть веб-приложения, запущенные в службе приложений Azure, и вы хотите разрешить им взаимодействовать с подсетью, то можете использовать тег AppService в правиле входящего трафика, чтобы разрешить обмен данными. Службы Azure также имеют теги служб для регионов, поэтому трафик можно разрешить или запретить только из определенных регионов.

Чтобы использовать тег службы, установите для параметра **Source** (Источник) правила значение **Service Tag** (Тег службы). Затем можно выбрать тег службы из раскрывающегося списка. На рис. 4.27 тег службы *AppService.CentralUS* используется для разрешения трафика из ресурсов службы приложений Azure в Центральном регионе США.

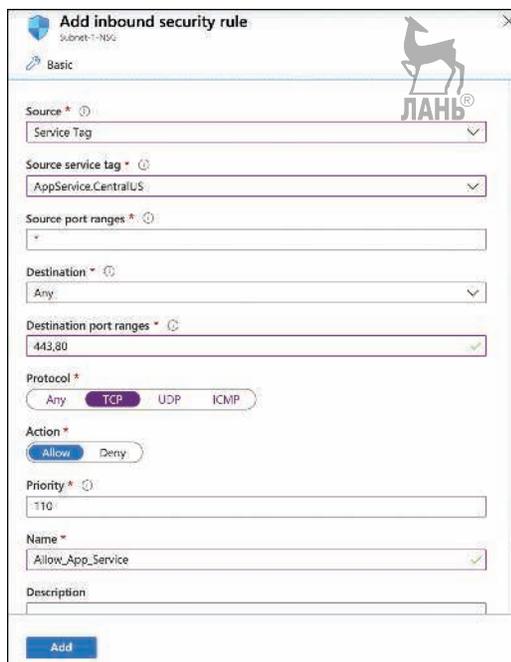


Рис. 4.27 Использование тега службы в правиле NSG

Брандмауэр Azure

На компьютерном жаргоне брандмауэр (firewall) – это устройство, через которое проходит сетевой трафик в определенную сеть и из нее. Цель брандмауэра состоит в том, чтобы разрешить только желаемый трафик в сети и отклонить любой трафик, который может быть злонамеренным или исходит из неизвестного источника. Брандмауэр устанавливает контроль над сетью с помощью правил, определяющих диапазон IP-адресов отправителя и получателя, а также комбинацию портов.

В типичной конфигурации брандмауэра весь трафик по умолчанию запрещен. Чтобы через брандмауэр мог проходить трафик, правило должно соответствовать этому трафику. Например, если требуется разрешить пользователям публичного интернета доступ к веб-приложению, запущенному на определенном сервере, создайте правило брандмауэра, позволяющее осуществлять связь с портами 80 и 443 (портами для трафика HTTP и HTTPS). Затем настройте правило для отправки этого трафика на веб-сервер.

Существует несколько брандмауэров от сторонних разработчиков, доступных в Azure Marketplace, но Microsoft также предлагает свой собственный брандмауэр под названием **Azure Firewall** (Брандмауэр Azure). Azure Firewall – это PaaS-сервис в Azure, который легко управляется и обеспечивает соглашение об уровне обслуживания (SLA) на уровне 99,95 %. Брандмауэр Azure масштабируется в соответствии с потребностями сети, поэтому вам не придется беспокоиться о всплесках трафика, вызывающих задержку или простой приложений.

ПРИМЕЧАНИЕ БРАНДМАУЭР AZURE – БРАНДМАУЭР С КОНТРОЛЕМ СОСТОЯНИЯ

Брандмауэр Azure – это брандмауэр с контролем состояния. Это означает, что он хранит в памяти данные о состоянии сетевых подключений, которые проходят через него. Когда новые сетевые пакеты для существующего подключения попадают в брандмауэр, он может определить, представляет ли состояние этого подключения угрозу безопасности.

Например, если кто-то подменяет ваш IP-адрес и пытается получить доступ к вашей виртуальной сети в Azure, брандмауэр распознает, что аппаратный адрес используемого компьютера изменился, и отклонит подключение.

Обычная настройка брандмауэра Azure состоит из следующих компонентов:

- централизованная сеть хабов, содержащая брандмауэр Azure и ВМ, работающую как *инсталляционный сервер* (jumpbox). У брандмауэра есть общедоступный IP-адрес, у ВМ jumpbox его нет;
- одна или несколько дополнительных сетей (называемых *оконечными сетями*, или *spoke networks*), которые не имеют общедоступных IP-адресов. Эти сети содержат различные ресурсы Azure.

Инсталляционный сервер (jumpbox) – это виртуальная машина, с которой можно удаленно управлять другими ВМ в сетях. Все остальные ВМ настроены таким образом, чтобы разрешить удаленный доступ только с IP-адреса виртуальной машины jumpbox. Если вы хотите получить доступ к ВМ в оконечной сети, сначала удаленно подключитесь к jumpbox, а затем с него подключитесь к нужной ВМ. Эта конфигурация называется *hub-and-spoke* (сеть со звездо-

образной топологией), и она обеспечивает дополнительную безопасность для сетевых ресурсов.



ПРИМЕЧАНИЕ ДРУГИЕ КОНФИГУРАЦИИ СЕТИ

Звездообразная топология – это не единственная конфигурация, в которой можно использовать брандмауэр Azure. Например, и в единичной виртуальной сети можно использовать брандмауэр Azure для фильтрации интернет-трафика. Сеть со звездообразной топологией является наиболее распространенной в реальных бизнес-приложениях.

На рис. 4.28 показана типичная конфигурация сети со звездообразной топологией, которая также включает брандмауэр Azure. Трафик, поступающий из интернета через порт 443 (HTTPS-трафик), направляется брандмауэром на веб-сервер, работающий в Spoke VNet 1. Трафик, поступающий через порт удаленного рабочего стола, направляется на VM jumpbox, с которой по протоколу RDP (Remote Desktop Protocol) идет подключение к виртуальной машине в Spoke VNet 2.

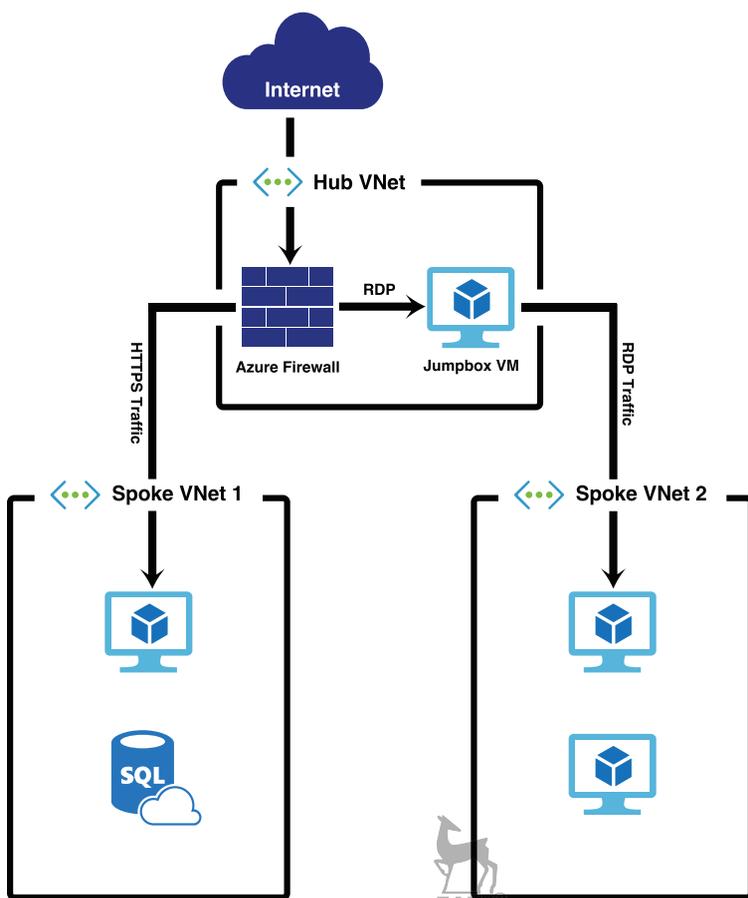
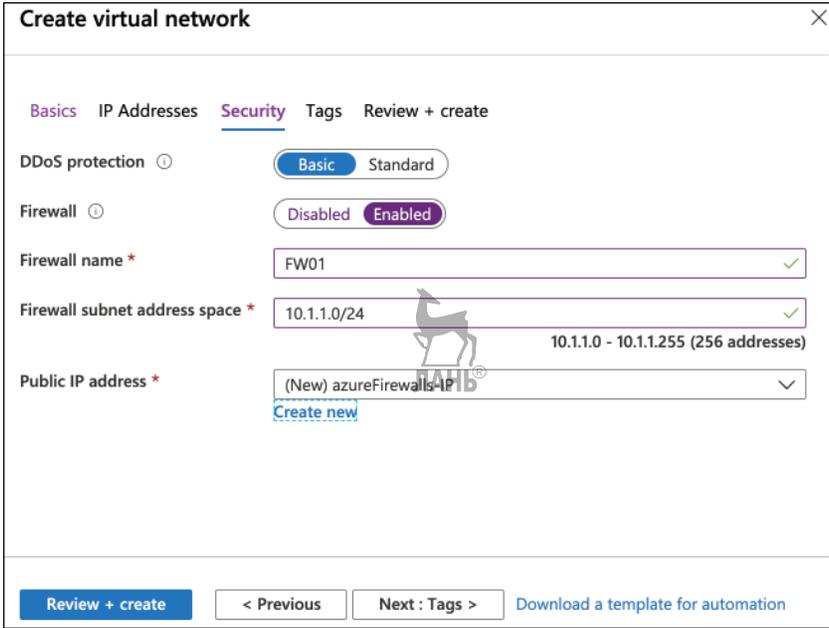


Рис. 4.28 Пример конфигурации сети со звездообразной топологией с брандмауэром Azure

Перед настройкой брандмауэра для обработки сетевого трафика необходимо создать экземпляр брандмауэра Azure. Можно включить брандмауэр Azure при создании виртуальной сети в Azure, или вы можете создать межсетевой экран и добавить его в существующую виртуальную сеть. На рис. 4.29 показан брандмауэр Azure, создаваемый в новой виртуальной сети.



The screenshot shows the 'Create virtual network' wizard in Azure, specifically the 'Security' tab. The 'DDoS protection' is set to 'Basic'. The 'Firewall' is set to 'Enabled'. The 'Firewall name' is 'FW01'. The 'Firewall subnet address space' is '10.1.1.0/24', which corresponds to the IP range '10.1.1.0 - 10.1.1.255 (256 addresses)'. The 'Public IP address' is set to '(New) azureFirewalls-IP', with a 'Create new' link below it. At the bottom, there are buttons for 'Review + create', '< Previous', 'Next : Tags >', and 'Download a template for automation'.

Рис. 4.29 Создание брандмауэра Azure

При создании брандмауэра в новой виртуальной сети Azure создает в ней подсеть с именем *AzureFirewallSubnet* и использует адресное пространство, указанное для этой подсети. Для брандмауэра также создается публичный IP-адрес для доступа к нему из интернета.

ДОПОЛНИТЕЛЬНО AZURE BASTION

В этом примере мы используем *jumpbox* и JIT-доступ, чтобы продемонстрировать вам преимущества брандмауэра Azure. Но лучшим подходом к удаленному доступу для ваших VM будет использование Azure Bastion. Azure Bastion в настоящее время не входит в экзамен AZ-900, но вы можете узнать о нем больше по ссылке: <https://bit.ly/az900-azure-bastion>.

Несмотря на то что брандмауэр Azure является PaaS-решением, его не просто нужно добавить в виртуальную сеть, но еще и настроить. Вам также будет необходимо сконфигурировать отправку трафика на брандмауэр, а затем настроить правила управления этим трафиком.

Чтобы отправить трафик на брандмауэр, необходимо создать таблицу маршрутов (*route table*). Таблица маршрутов – это ресурс Azure, связанный с под-

сеть. Он содержит правила (называемые *маршрутами*), определяющие способ обработки сетевого трафика в подсети.

Таблица маршрутов создается с помощью элемента **Route Table** (Таблица маршрутов) в Azure Marketplace. После создания новой таблицы маршрутов необходимо связать ее с одной или несколькими подсетями. Чтобы сделать это, нажмите сперва **Subnet** (Подсеть), а затем **Associate** (Связать), как показано на рис. 4.30.

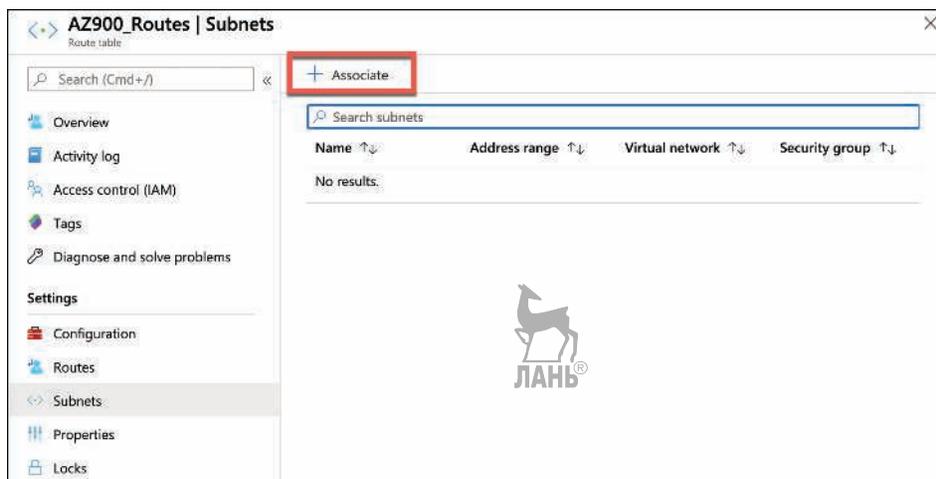


Рис. 4.30 Связывание таблицы маршрутов с подсетью

После кнопки **Associate** (Связать) выберите виртуальную сеть (Virtual Network) и подсеть (Subnet), как показано на рис. 4.31.

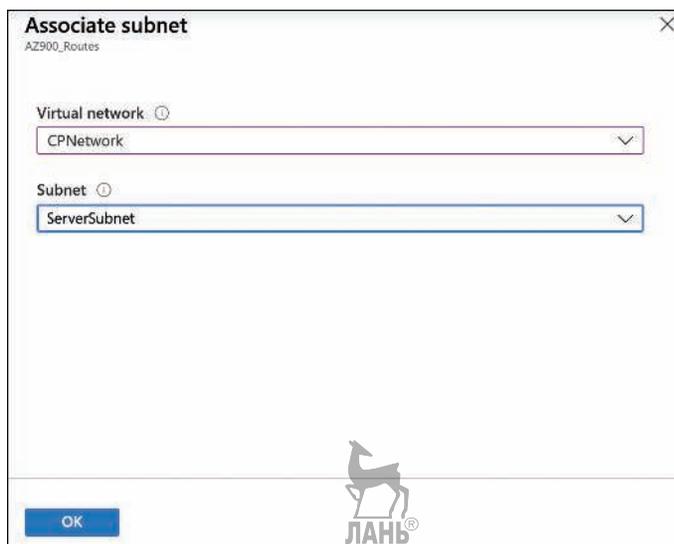


Рис. 4.31 Выбор подсети для связывания

ПРИМЕЧАНИЕ РЕГИОН ТАБЛИЦЫ МАРШРУТОВ

Ваша таблица маршрутов должна быть расположена в том же регионе, что и ваша виртуальная сеть. В противном случае вы не сможете связать подсеть с таблицей маршрутов.

Конкретно в нашем случае настроек мы хотим связать обе сети *JumpboxSubnet* и *ServerSubnet* с таблицей маршрутов. Это гарантирует, что брандмауэр будет обрабатывать весь сетевой трафик на VM *jumpbox* и весь трафик из *ServerSubnet*.



СОВЕТ К ЭКЗАМЕНУ

Важно понимать, что брандмауэр может (и должен) использоваться для фильтрации трафика, поступающего в сеть и исходящего из нее. Например, вы хотите, чтобы брандмауэр обрабатывал трафик в *jumpbox*, но при этом вам нужны гарантии, что трафик, поступающий из подсети, в которой расположены другие серверы, является безопасным и данные не отправляются из сети ненадлежащим образом.

После того как мы связали таблицу маршрутов с подсетями, мы создаем новый маршрут, чтобы трафик направлялся через брандмауэр Azure. Для этого нажмите кнопку **Routes** (Маршруты), а затем кнопку **Add** (Добавить), как показано на рис. 4.32.

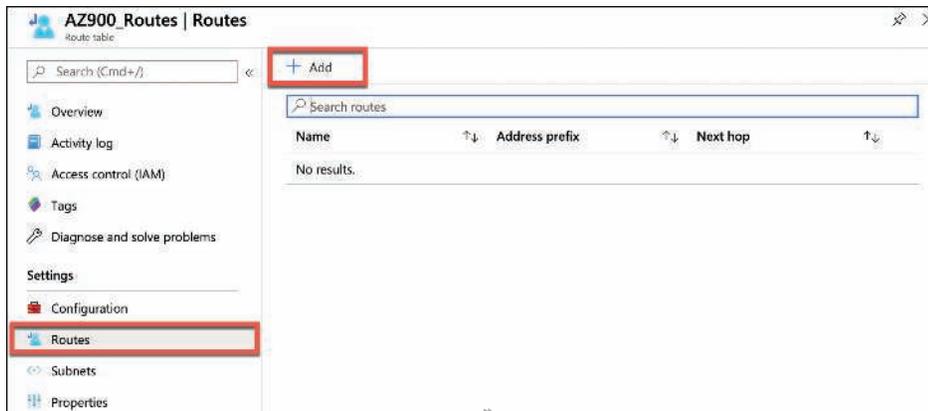


Рис. 4.32 Добавление пользовательского маршрута в таблицу маршрутов

На рис. 4.33 показана конфигурация нового маршрута с именем *ToFirewall*. Этот маршрут настроен на *0.0.0.0/0*, что охватывает весь трафик. Затем маршрут перенаправляет этот трафик на виртуальное устройство (в данном случае брандмауэр Azure), расположенное по IP-адресу *10.1.1.4*, он же внутренний IP-адрес этого брандмауэра. Как только данный маршрут будет настроен, он сразу же начнет применяться ко всем устройствам в подсетях, связанных с таблицей маршрутов.

Add route
AZ900_Routes

Route name *
ToFirewall ✓

Address prefix * ⓘ
0.0.0.0/0 ✓

Next hop type ⓘ
Virtual appliance ✓

Next hop address * ⓘ
10.1.1.4 ✓

ⓘ Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

OK

Рис. 4.33 Добавление пользовательского маршрута

Вспомним, что брандмауэр Azure блокирует по умолчанию весь трафик, поэтому на данный момент нет возможности добраться до VM jumpbox, находящейся в *JumpboxSubnet*. Чтобы получить доступ к этой VM, необходимо настроить правило брандмауэра в Azure Firewall, которое будет перенаправлять соответствующий трафик на VM jumpbox.

Чтобы добавить правило брандмауэра, откройте Azure Firewall на портале Azure и нажмите **Rules** (Правила), выберите тип правила и нажмите кнопку **Add** (Добавить), чтобы добавить новую коллекцию правил, как показано на рис. 4.34.

FW01 | Rules

Search (Cmd+/) << Refresh

NAT rule collection Network rule collection Application rule collection

+ Add NAT rule collection

Priority	Name	Action	Rules
No results			

ⓘ When a DNAT rule is matched, an implicit corresponding network rule to allow the translated traffic is added. [Learn more.](#)

Рис. 4.34 Наборы правил брандмауэра Azure на портале Azure

Существует три типа наборов правил, доступных в брандмауэре Azure:

- **правила преобразования сетевых адресов** (Network address translation, NAT Rule Collection). Эти правила используются для пересылки трафика с брандмауэра на другое устройство в сети;
- **сетевые правила** (Network Rules Collection). Правила, разрешающие трафик по определенным диапазонам IP-адресов и указанным портам;
- **правила приложений** (Application Rules Collection). Правила приложений используются, чтобы разрешить таким приложениям, как Центр обновления Windows, обмениваться данными по сети. Они также могут использоваться для разрешения определенных доменных имен, таких как *azure.com* и *microsoft.com*.

Брандмауэр Azure объединяет все правила определенного типа и приоритета в набор правил. Приоритет – это число от 100 до 65 000. Меньшие числа представляют собой более высокий приоритет и обрабатываются в первую очередь. Другими словами, если необходимо убедиться, что правило всегда применяется перед всеми другими правилами, включите это правило в коллекцию с приоритетом 100.

Когда сетевой трафик приходит в брандмауэр, то сначала применяются правила NAT. Если трафик соответствует правилу NAT, брандмауэр Azure применяет имплицитное сетевое правило для корректной маршрутизации трафика, и вся дальнейшая обработка правил останавливается.

Если правило NAT не соответствует трафику, применяются сетевые правила. Если сетевое правило соответствует трафику, вся дальнейшая обработка правил прекращается. Если сетевое правило не применяется к трафику, применяются правила приложения. Если ни одно из правил приложения не соответствует трафику, трафик отклоняется брандмауэром.

Чтобы разрешить удаленный доступ к VM jumpbox, можно настроить правило NAT, которое пересылает любой трафик с входящего порта 55000 на порт 3389 (порт удаленного рабочего стола) на внутренний IP-адрес виртуальной машины jumpbox, как показано на рис. 4.35. Поскольку порт 55000 является общим, который обычно не используется для удаленного рабочего стола, то злоумышленники вряд ли это обнаружат.

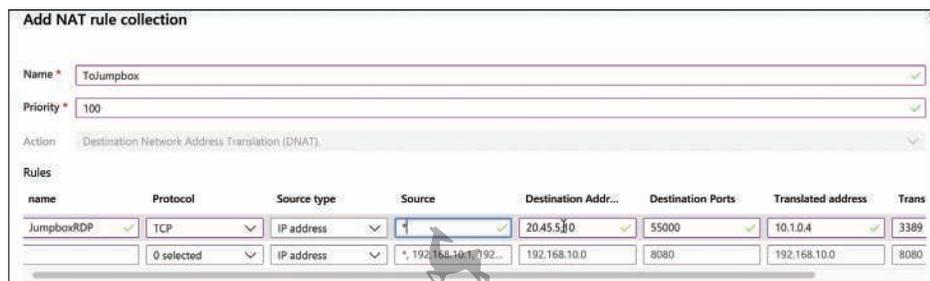


Рис. 4.35 Добавление правила NAT

В дополнение к настраиваемым правилам имеется также функция аналитики угроз в брандмауэре Azure, которая может защитить вас от заведомо вре-

доносных IP-адресов и доменных имен. Microsoft постоянно обновляет свой список известных вредоносных участников, а собранные данные содержатся в ленте Microsoft Threat Intelligence.

При включении аналитики угроз можно настроить оповещение Azure, если трафик с известного вредоносного IP-адреса или доменного имени пытается попасть в сеть. Вы также можете выбрать автоматическое блокирование трафика брандмауэром, как показано на рис. 4.36.

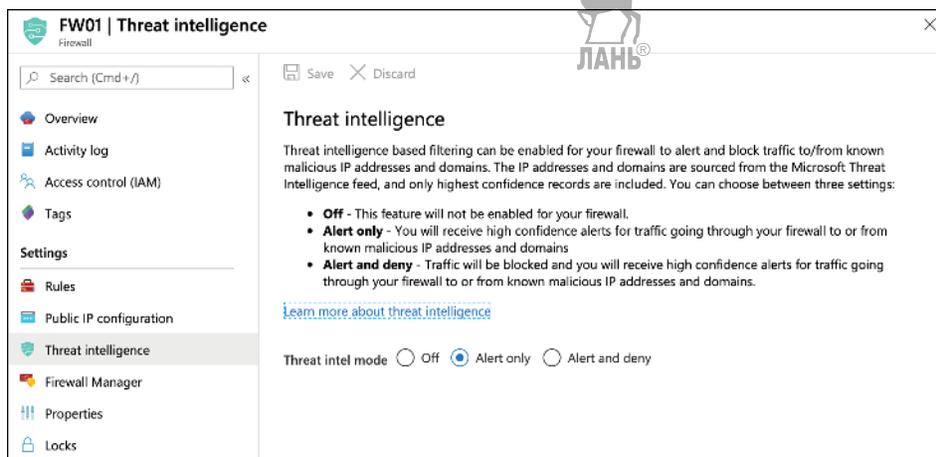


Рис. 4.36 Аналитика угроз помогает защитить виртуальную сеть Azure

Защита от DDoS

Облачные приложения, доступные из интернета по публичному IP-адресу, подвержены атакам *распределенного отказа в обслуживании* (distributed denial of service, DDoS). DDoS-атаки могут перегружать серверы приложения и часто делают онлайн-сервис полностью недоступным до тех пор, пока атака не будет устранена. DDoS-атаки также могут применяться для использования недостатков в безопасности приложения и атаковать системы, к которым подключается приложение.

Azure может помочь защитить от DDoS-атак с помощью защиты от DDoS. Защита от DDoS (DDoS protection) – это функция виртуальных сетей Azure. Существует два уровня защиты от DDoS: Basic и Standard.

- **Basic** (Базовый уровень) защищает вас от объемных (volume-based) DDoS-атак, распределяя большие объемы трафика по всей сетевой инфраструктуре Azure. Базовая защита от DDoS применяется к публичным IP-адресам, как к IPv4, так и к IPv6. Уровень Basic не имеет журнала или отчетов о любых мерах по устранению DDoS, и не существует пока способ по настройке оповещения, чтобы вы получали уведомления, если обнаружена проблема. Однако уровень Basic является бесплатным и обеспечивает базовую защиту;
- **Standard** (Стандартный уровень) обеспечивает защиту не только от объемных DDoS-атак, но и при использовании в сочетании со шлюзом

приложений Azure (Azure Application Gateway), он также защищает от атак, направленных на безопасность приложений. Он предлагает ведение журнала и оповещение о событиях DDoS, и если вам нужна помощь во время DDoS-атаки, Microsoft предоставляет доступ к экспертам, которые могут помочь вам. Уровень DDoS Standard применяется только к публичным IP-адресам IPv6. Уровень Standard предназначен для корпоративных клиентов и обходится в 2994 доллара в месяц плюс небольшая плата за гигабайт обрабатываемых данных. Фиксированная ежемесячная цена покрывает до 100 ресурсов. Если вам нужно покрыть дополнительные ресурсы, вы платите дополнительно 30 долларов за ресурс в месяц.

Чтобы включить уровень **Standard** (Стандартный уровень), нажмите **DDoS Protection** (Защита от DDoS) в настройках виртуальной сети на портале Azure и выберите **Standard** (Стандартный уровень), как показано на рис. 4.37.

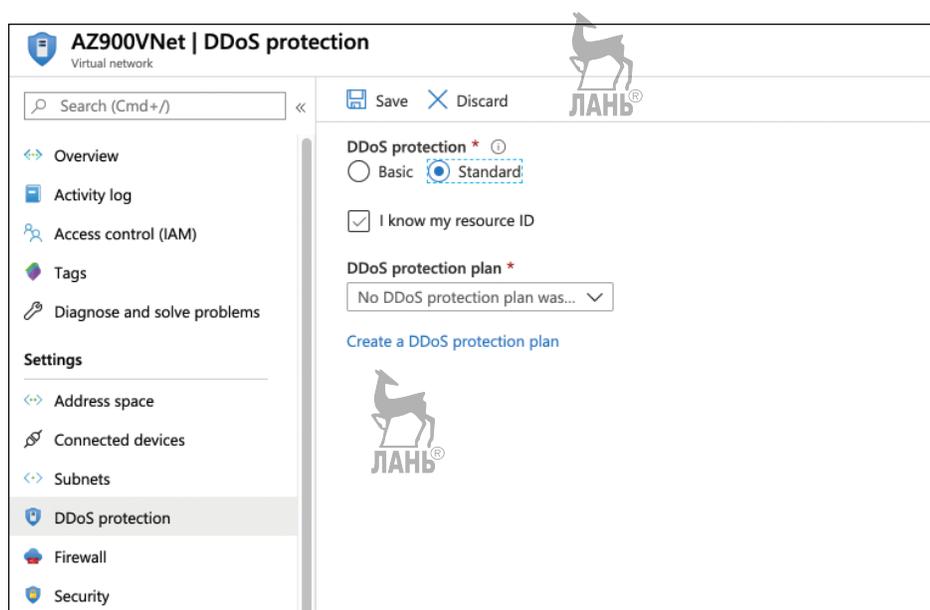


Рис. 4.37 Защита от DDoS на портале Azure

Чтобы включить уровень **Standard** (Стандартный уровень), вам понадобится план защиты от DDoS (DDoS Protection plan). Если в данный момент его нет, кликните **Create A DDoS Protection Plan** (Создать план защиты от DDoS), чтобы создать его на портале Azure. Этот план защиты от DDoS можно применить к вашей и другим виртуальным сетям, к которым у вас есть доступ в Azure. Виртуальные сети, использующие план защиты от DDoS, не должны находиться в одной подписке, поэтому в большинстве случаев организации потребуется только один план защиты от DDoS для всех своих виртуальных сетей.



СОВЕТ К ЭКЗАМЕНУ

Тот факт, что вы можете добавлять виртуальные сети из нескольких подписок Azure на тот же план защиты от DDoS, является важной концепцией. С вас взимается большая ежемесячная плата за защиту от DDoS, и если вы создаете два таких плана, то просто удваиваете свои расходы.

Защита от DDoS уровня **Standard** (Стандартный) отслеживает ваш сетевой трафик 24/7 и использует машинное обучение для профилирования трафика по времени, затем подстраивается под профиль вашей сети. Во ходе DDoS-атаки уровень **Standard** (Стандартный) позволяет передавать журналы в систему управления информацией по безопасности и событиями (security information and event management, SIEM). Системы SIEM предназначены для агрегирования данных из большого числа источников для анализа и проверки соответствий политикам и стандартам хранения данных.

После настройки оповещений и мониторинга для защиты от DDoS можно моделировать событие DDoS с помощью учетной записи BreakingPoint Cloud по адресу: <https://www.ixiacom.com/products/breakingpoint-cloud>. Это позволит вам проверить, что защита от DDoS-атак работает.

Мысленный эксперимент

Теперь вы можете разбираться в вопросах безопасности в облаке. Давайте проверим ваши знания при помощи мысленного эксперимента. Ответы на этот мысленный эксперимент вы найдете в следующем разделе.

ContosoPharm узнали, что вы теперь довольно хорошо разбираетесь в безопасности. У компании есть несколько проблем, которые вы как раз способны решить. Прежде всего имеется большой объем ресурсов Azure, которые только что развернули при помощи нового приложения, которое имеет доступ к конфиденциальной информации. Компании нужны гарантии, что соблюдаются наилучшие методы обеспечения безопасности. Также у компании имеется несколько локальных серверов, которые используют приложение, поэтому важно, чтобы компания знала, так ли они безопасны, как должны быть.

Еще одной проблемой, с которой сталкивается ContosoPharm, является доступ к используемым приложением VM Azure. ИТ-директор хочет быть уверен, что только компьютеры корпоративной сети ContosoPharm могут удаленно подключаться к VM в определенное время.

Одна часть приложения ContosoPharm использует сертификаты для аутентификации, и компании нужны гарантии, что они будут безопасно храниться. Им также нужна возможность хранения зашифрованных ключей, которые бы отвечали требованиям FIPS 140-2.

ИТ-директор ContosoPharm сказала своим сотрудникам о необходимости внедрения в среду SOAR и SIEM. Им нужно, чтобы это внедрение смогло работать как для ресурсов Azure, там и для ресурсов веб-служб Amazon. Дорогостоящие консультации им не нужны. Нужен простой способ, позволяющий это реализовать.

Приложение, развернутое в облаке, является многоуровневым. Директор по информационным технологиям обеспокоен, что инженеры по сетям обеспечили недостаточную защиту приложения. Ему нужны гарантии, что правила передачи трафика реализованы на разных уровнях приложения, а также в том, что поступающий извне трафик будет отклоняться.

Поскольку приложение значимо для работы ContosoPharm, компания готова финансово вкладывать средства, сэкономленные на ваших консультациях, в предотвращение потенциальных DDoS-атак, которые вызывают проблемы с доступностью.

Что же вы порекомендуете ContosoPharm в этих случаях?

Ответы на мысленный эксперимент

Здесь мы рассмотрим ответы на мысленный эксперимент.

Чтобы убедиться, что ContosoPharm использует оптимальные службы и настройки, вы можете ей посоветовать Службу безопасности Azure. Она способна не только сообщать о службах Azure, но и получать подробные сведения о локальных ресурсах. Используя функции доступа к ВМ «just-in-time» Центра безопасности, у них появятся гарантии, что доступ к ВМ будет заблокирован для использования вне корпоративной сети. Может быть также ограничено время, в которое будут доступны ВМ.

Для безопасного хранения сертификатов должно использоваться хранилище ключей Azure. Там можно будет хранить зашифрованные ключи, но поскольку компании необходимо соответствие требованиям FIPS 140-2, потребуется премиум-уровень.

Для несложной реализации SOAR и SIEM в своей среде ContosoPharm следует использовать Azure Sentinel. Он способен настроить коннекторы для служб Azure и AWS.

Для внедрения правил сетевого трафика для виртуальных сетей должен быть настроен NSG. Чтобы нежелательный трафик не попадал в сеть, компании нужно использовать брандмауэр Azure и настроить правила, которые будут разрешать только «правильный» входящий трафик. Создаваемые ими NSG также должны устанавливать правила, по которым определяется, как приложения принимают трафик из интернета.

Чтобы предотвратить DDoS-атаки, компания может приобрести защиту от DDoS по тарифу **Standard** (Стандартный). Хотя его стоимость довольно высока, он способен обеспечить полноценную защиту от DDoS-атак.

Краткое содержание главы

В этой главе мы познакомились со средствами безопасности, которые могут быть использованы для защиты локальных сервисов и ресурсов в Azure, а также виртуальных сетей. Вы познакомились с некоторыми концепциями безопасности, которые помогли вам лучше разобраться с тем, как настраиваются инструменты Azure.

Ниже представлено краткое содержание главы.

- Центр безопасности Azure представляет собой инструмент для анализа соответствия локальных сервисов и ресурсов Azure передовым практикам.
- Центр безопасности включает три основные области: политика и соответствие нормативным требованиям, поддержание безопасности ресурсов и защита от угроз.
- Доступ к ВМ «just-in-time» может ограничить доступ к удаленному рабочему столу ВМ в определенных сетях и в конкретное время.
- Хранилище ключей Azure обеспечивает безопасный способ хранения секретной информации, ключей и сертификатов.
- Хранилище ключей Azure премиум-уровня хранит ключи в аппаратных модулях (HSM), что делает его совместимым с FIPS 140-2.
- Azure Sentinel является решением для внедрения в среду SOAR и SIEM.
- Sentinel помогает отслеживать угрозы безопасности в Azure, облаке и локально.
- Sentinel может выполнять действия в отношении предупреждения системы безопасности с помощью наборов сценариев, которые надстраиваются над Azure Logic Apps.
- Глубокую защиту зачастую называют «замковым подходом» (castle approach), поскольку она представляет собой многоуровневые стратегии безопасности.
- Группы сетевой безопасности (NSG) представляют собой правила, позволяющие фильтровать трафик сети и осуществлять управление им.
- Правила NSG имеют приоритет от 100 до 4096, и правила с самым низким значением будут применяться первыми.
- Брандмауэр Azure запрещает весь трафик в определенные подсети, если не настроено правило, разрешающее это.
- Брандмауэр Azure – это брандмауэр с отслеживанием состояния, который «запоминает» состояние подключений. Это позволяет ему распознавать вредоносный трафик, который может показаться обычным.
- Защита от DDoS-атак состоит из базового и стандартного уровней.
- Базовый уровень бесплатен, он относится к защите от DDoS-атак, которую Microsoft использует для предотвращения воздействия DDoS-атак на саму платформу Azure.
- Стандартный уровень можно использовать со шлюзом приложений Azure.



ГЛАВА 5

Описание функций идентификации, управления, конфиденциальности и соответствия нормативным требованиям

В книге мы уделили много времени безопасности, но когда дело касается миграции в облако, не только безопасность начинает волновать большинство компаний. Для них также важно контролировать используемые ресурсы и обеспечивать конфиденциальность данных после их загрузки в экосистему облачного провайдера. Кроме того, многие предприятия должны соблюдать определенные правила и стандарты, и, переходя в облако, они перекладывают часть этой ответственности на поставщиков облачных услуг. Поэтому компаниям нужны надежные гарантии, что поставщики смогут обеспечить должный уровень соответствия требованиям.

Microsoft подходит со всей серьезностью ко всем перечисленным проблемам и предоставляет эффективные инструменты для потребностей своих клиентов. В этой главе мы поговорим об этих инструментах и о том, как их использовать.

Навыки, описанные в этой главе:

- описание основных служб идентификации Azure;
- описание основных функций управления Azure;
- описание конфиденциальности и соответствия нормативным требованиям.

Навык 5.1: описание основных служб идентификации Azure

Безопасность – это не только управление сетевым трафиком. Чтобы обеспечить безопасную среду, вам нужны средства идентификации того, как вообще можно получить доступ к вашему приложению. Идентифицировав пользователя, вам нужно будет убедиться, что ему не разрешен доступ к данным или другим ресурсам, к которым он априори не должен иметь доступ.

Этот раздел охватывает следующие продукты:

- **Authentication and authorization** (Аутентификация и авторизация);
- **Azure Active Directory** (Служба каталогов Azure);
- **Conditional Access and multifactor authentication, MFA** (Условный доступ и многофакторная аутентификация);
- **Role-based access control, RBAC** (Управление доступом на основе ролей).

Аутентификация и авторизация

Во многих бизнес-приложениях не у всех пользователей имеются одинаковые привилегии. Например, веб-сайт может позволить ограниченному числу пользователей добавлять и редактировать свое содержание. Другие пользователи могут иметь возможность назначать тех, кто может добавлять контент. Однако подавляющее большинство пользователей – всего лишь потребители. Они не могут изменять содержание сайта или предоставлять другим людям возможность доступа к его содержанию.

Для реализации подобного рода контроля вам нужно знать, кто использует приложение, чтобы вы могли определить степень их привилегий. Для этого вам потребуется, чтобы пользователи вошли в систему, нередко это происходит при помощи логина (имя пользователя, username) и пароля (password). Предположим, пользователь предоставил верные учетные данные, и он проходит *проверку подлинности (authenticated)* в приложении.

После того как пользователь аутентифицируется и начнет взаимодействовать с приложением, могут быть и дополнительные проверки, используемые для подтверждения степени полномочий пользователя. Такой процесс называется *авторизацией (authorization)*, и проверка авторизации выполняется в отношении того, кто уже прошел аутентификацию.

Аутентификация и авторизация могут быть не только на веб-сайте. Когда вы входите на портал Azure, вы проходите аутентификацию. При работе с ресурсами Azure вы также получаете разрешение на выполнение действий. В зависимости от уровня ваших привилегий вам будет разрешено выполнять только определенный ряд операций. Например, вам может быть разрешено создание ресурсов Azure, но у вас нет прав предоставлять другим пользователям доступ к используемой вами подписке Azure.

Azure использует службу Azure Active Directory для принудительной проверки подлинности и авторизации в Azure, но, кроме этого, у этой службы есть ряд и других возможностей.

Azure Active Directory

Если у вас есть опыт работы с локальной Windows Active Directory, вы можете столкнуться с непониманием механизмов работы Azure Active Directory (Azure AD). Это связано с тем, что Azure AD не является облачным эквивалентом Windows Active Directory. Это совершенно другая служба.

Azure AD – это облачная служба идентификации в Azure, которая помогает аутентифицировать и авторизовать пользователей. Azure AD можно использовать для предоставления пользователям доступа к ресурсам Azure. Вы также можете предоставить пользователям доступ к сторонним ресурсам, используемым компанией, или локальным, используя такое же имя пользователя и пароль.

ДОПОЛНИТЕЛЬНО ПРЕДОСТАВЛЕНИЕ ДОСТУПА К РЕСУРСАМ AZURE

Вы узнаете о том, как предоставить другим пользователям доступ к ресурсам Azure, когда мы рассмотрим управление доступом на основе ролей чуть позже в этом навыке.

Ядро Azure AD – это каталог пользователей. Каждый пользователь имеет *удостоверения* («личность», identity), состоящие из ID пользователя, пароля и других свойств. Пользователи также имеют одну или несколько *ролей каталога* (directory role). Идентификатор и пароль используются для аутентификации пользователя, а роли – для авторизации при выполнении определенных действий в Azure AD.

ДОПОЛНИТЕЛЬНО СУБЪЕКТ-СЛУЖБЫ И УПРАВЛЯЕМЫЕ ИДЕНТИФИКАЦИИ

Двумя другими сущностями, доступными в Azure AD, являются субъект-службы (service principal) и управляемые удостоверения (managed identities). Субъект-службы предоставляют приложение в Azure AD, о котором мы поговорим чуть позже.

Управляемые удостоверения – это особый тип субъект-службы, который можно использовать только с ресурсами Azure. О них вы можете прочитать дополнительно по ссылке <https://bit.ly/az900-managedidentities>.

При регистрации в Azure для вас автоматически создается Azure AD, который используется для управления доступом к ресурсам Azure в рамках вашей подписки. На рис. 5.1 показана Azure AD на портале Azure.

Чтобы просмотреть пользователей в Azure AD или управлять ими, щелкните **Users** (Пользователи) в меню в левой части страницы. Откроется блейд **All Users** (Все пользователи), показанный на рис. 5.2.

Azure AD на рис. 5.2 содержит двух пользователей. Первый пользовательский источник – это пользователь Azure Active Directory, который был добавлен вручную. Вторым пользователем используется учетная запись Microsoft для входа в каталог.

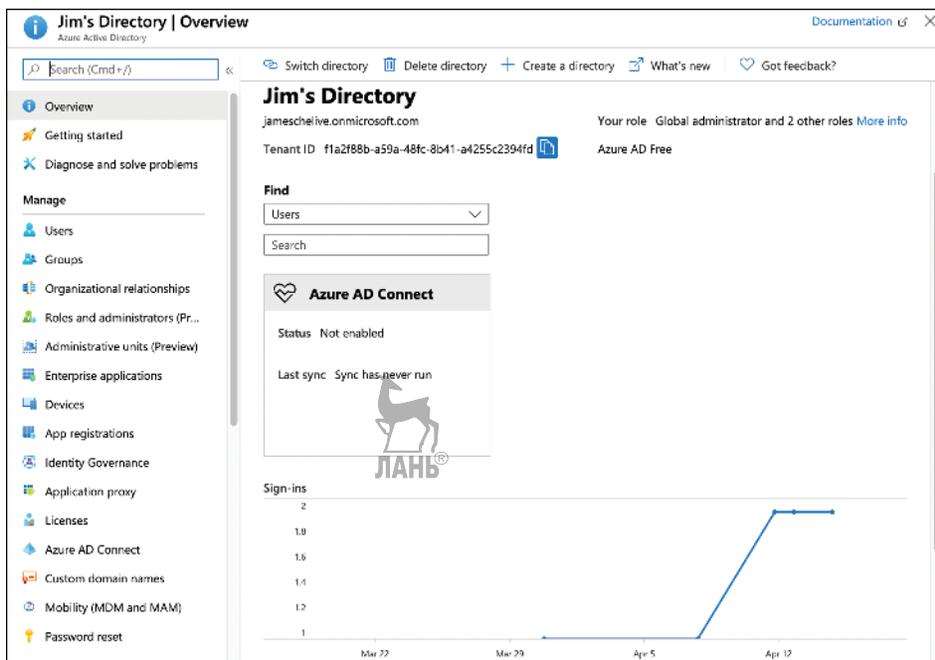


Рис. 5.1 Azure AD на портале Azure

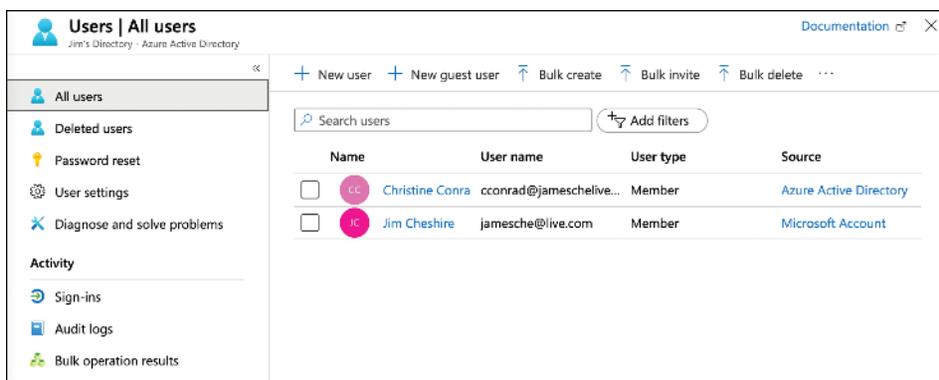


Рис. 5.2 Блейд **All Users** (Все пользователи) на портале Azure

Чтобы добавить нового пользователя из вашей компании в Azure AD, нажмите **New User** (Новый пользователь), чтобы отобразить блейд, показанный на рис. 5.3.

Указанное имя пользователя потребуется для входа в Azure AD. Используемое доменное имя должно быть именем, которое принадлежит вам и которое связано с Azure AD. Вы также можете нажать на **Groups** (Группы), чтобы выбрать группу для этого пользователя. Группы упрощают управление большим количеством схожих учетных записей.

New user

Jim's Directory

♥ Got feedback?

Identity

User name * ⓘ ✓ @ ✓

The domain name I need isn't shown here

Name * ⓘ ✓

First name ✓

Last name ✓

Password

Auto-generate password

Let me create the password

Initial password

Show Password

Groups and roles

Groups 0 groups selected

Roles User

Create

Рис. 5.3 Добавление нового пользователя Azure AD

Azure AD предлагает функцию Azure AD B2B (business to-business), которая позволяет добавлять пользователей, не принадлежащих компании. Таким образом, вы можете пригласить других пользователей, не принадлежащих компании, стать участниками Azure AD. Эти пользователи могут получить доступ к вашим ресурсам. Пользователи, не входящие в компанию, называются *гостевыми* (guest users). Чтобы добавить гостевых пользователей, нажмите **New Guest User** (Новый гостевой пользователь), как показано на рис. 5.2. Откроется блейд **New Guest User** (Новый гостевой пользователь), как показано на рис. 5.4.

Когда вы добавляете гостевого пользователя, приглашение присоединиться к Azure AD отправляется на указанный вами адрес электронной почты. Чтобы принять приглашение, адрес электронной почты пользователя должен быть связан с учетной записью Microsoft (Microsoft Account). Если пользователь не имеет такой учетной записи, ему будет предоставлена возможность создать ее, чтобы присоединиться к Azure AD.

Пользователь, показанный на рис. 5.4, может получить доступ к корпоративным учетным записям социальных сетей, добавив эти приложения в Azure AD. Приложения для добавления включают не только приложения социальных сетей, такие как Facebook и Twitter, но и тысячи других. Чтобы добавить приложение, откройте Azure AD на портале Azure, нажмите сперва **Enterprise Applications** (Корпоративные приложения), а затем **New Application** (Новое приложение), как показано на рис. 5.5.

New user
Jim's Directory

♥ Got feedback?

Identity

Name ✓

Email address * ✓

First name ✓

Last name ✓

Personal message

Groups and roles

Groups 0 groups selected

Roles User



Рис. 5.4 Добавление нового гостевого пользователя

Enterprise applications | All applications
Jim's Directory Azure Active Directory

+ New application Columns

Application Type: Enterprise Applications Applications status: Any

Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID	Application ID
Azure DevOps	http://azure.com/devops	bd2d9884-ddb8-47c8-...	499b84ac-1321-427f-...
AzureCards	http://azurecardsjwc.azurewe...	a39f1bcf-ccb7-4ca4-8...	88070b0c-6961-4a2...
jwcaetest	http://localhost	83db4d25-0d59-4416-...	2cc5bf99-103b-45f0-...
Office 365 Exch	http://office.microsoft.com/o...	a8be4da9-ceae-4f21-b...	00000002-0000-0ff1...
Office 365 Man		4ed586fa-858d-4317-...	c5393580-f805-4401...
Office 365 Shar	http://office.microsoft.com/s...	45fc3986-c1ae-40de-b...	00000003-0000-0ff1...
Outlook Group		65a5cfe3-0379-4443-b...	925eb0d0-da50-460...
Skype for Busin		d2b6e155-cd1a-41ce-...	00000004-0000-0ff1...

Рис. 5.5 Корпоративные приложения в Azure AD

После нажатия кнопки **New Application** (Новое приложение) можно выбрать одно из списка популярных облачных провайдеров, как показано на рис. 5.6. Вы можете найти приложение путем ввода имени приложения в поле поиска, а также отфильтровать представление с помощью кнопок фильтрации справа от поля поиска.

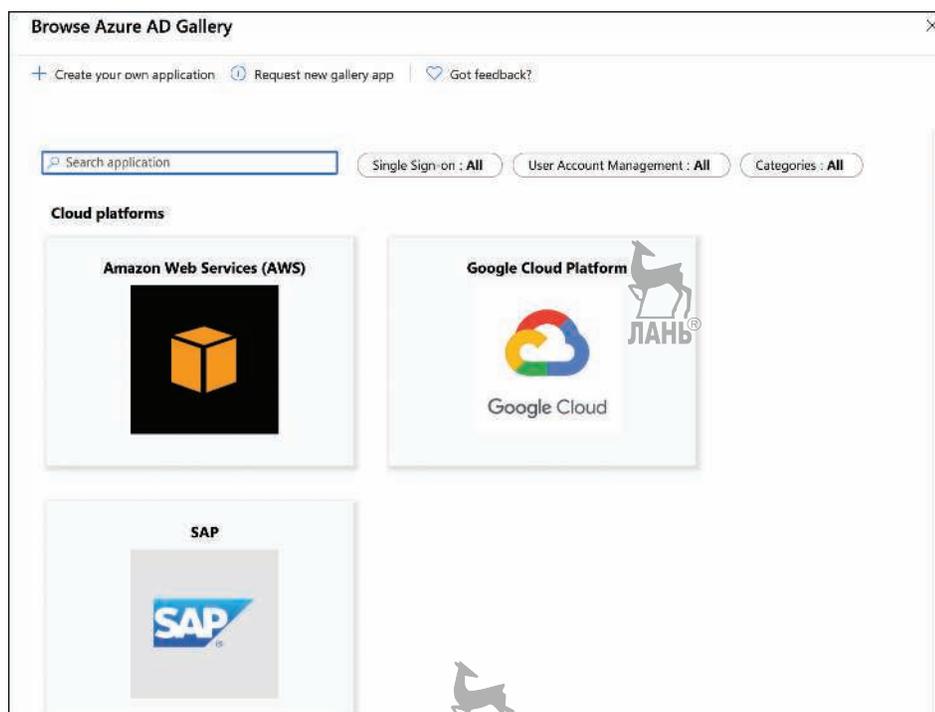


Рис. 5.6 Облачные провайдеры галереи корпоративных приложений

Если вы прокрутите вниз, то увидите список и других приложений, которые можно будет добавить, как показано на рис. 5.7.

Можно также добавить собственное приложение, существующее локально приложение или интегрировать любое другое приложение. Добавляемому приложению необходимо предоставить страницу входа в систему, на которую будет перенаправлять Azure AD для ее интеграции.



СОВЕТ К ЭКЗАМЕНУ

Вы можете настроить доступ приложения к определенным ресурсам при помощи *субъект-службы* (service principal). Эта служба создается, когда вы предоставляете приложению доступ к ресурсам Azure при помощи управления доступом на основе ролей (role-based access control), о чем мы с вами поговорим в следующем разделе.

После добавления приложения можно настроить Azure AD таким образом, чтобы пользователи, имеющие доступ к этому приложению, могли пройти

аутентификацию с использованием тех же учетных данных, которые они используют для входа в Azure AD. Такой вид аутентификации известен как *единый вход* (single sign-on, SSO), и он является одним из ключевых преимуществ использования Azure AD.

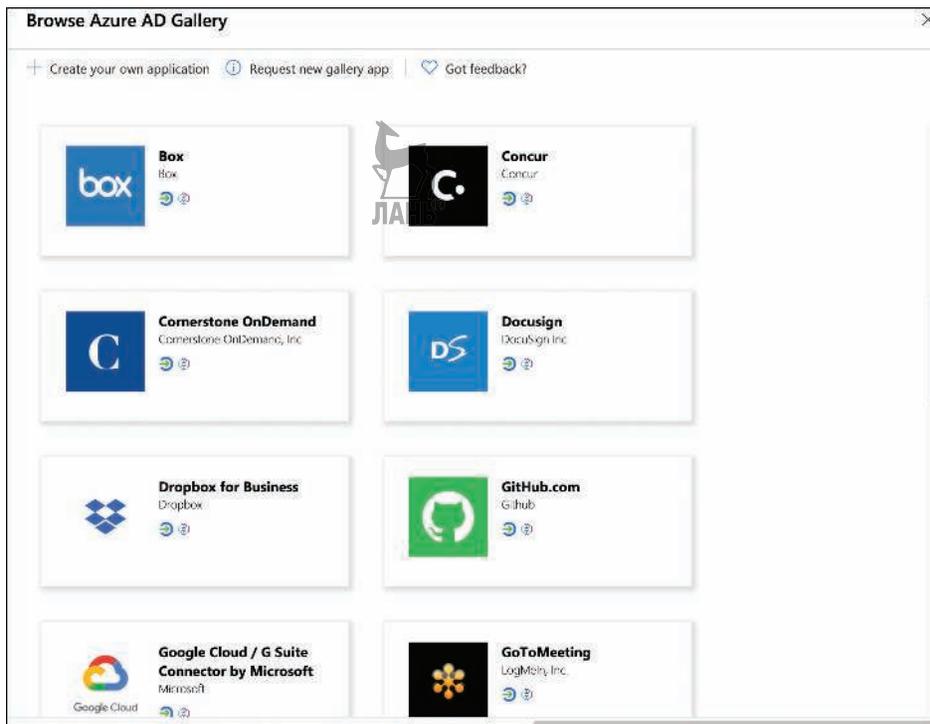


Рис. 5.7 Галерея корпоративных приложений



СОВЕТ К ЭКЗАМЕНУ

Azure AD B2B позволяет приглашать гостей пользователей в Azure AD из других компаний. Другая функция AD, называемая Azure AD B2C, позволяет предоставлять пользователям доступ к приложениям Azure AD путем входа в существующие учетные записи, такие как Facebook или Google.

Еще одним важным преимуществом использования Azure AD для управления доступом пользователей к другим приложениям является то, что вы легко можете отозвать этот доступ из единого интерфейса. Например, когда вы даете внешнему специалисту имя пользователя и пароль вашей учетной записи в социальных сетях, чтобы он мог публиковать посты от вашего имени, то если вы передумаете, вам придется изменить имя пользователя и пароль в этой социальной сети. Однако если вы предоставите им доступ с помощью Azure AD с настроенным единым входом, вы можете легко удалить этот доступ на портале Azure. Пользователь не должен знать имя пользователя и пароль, используемые для учетной записи в социальных сетях.

Все функции Azure AD, которые мы рассмотрели, включены в бесплатную версию Azure AD, которую получает любой пользователь с подпиской Azure. В Azure AD есть еще три платных уровня: Office 365 apps, Premium P1 и Premium P2. Перейдя на один из тарифных планов премиум-класса, вы можете включить многофакторную аутентификацию для пользователей.

ДОПОЛНИТЕЛЬНО ЦЕНООБРАЗОВАНИЕ AZURE ACTIVE DIRECTORY

Дополнительные сведения о тарифных планах Azure AD и о том, что входит в каждый из них, вы найдете по ссылке <https://aka.ms/aadpricing>.



Условный доступ и многофакторная аутентификация

Простыми словами: администраторы Azure AD могут запросить у пользователя прохождение аутентификации с помощью имени пользователя и пароля, а также авторизации для проверки доступа к определенному ресурсу. Однако большинству администраторов необходим больший уровень контроля для обеспечения безопасности ресурсов.

Предположим, что вы предоставили пользователю по имени Кристина доступ к своей учетной записи Microsoft 365 при помощи Azure AD. Поскольку ваши конфиденциальные данные хранятся в Microsoft 365, вам нужны гарантии, что никто не сможет взломать пароль Кристины и получить к вашим данным доступ. Условный доступ Azure (Azure Conditional Access) и многофакторная аутентификация (multifactor authentication, MFA) помогают сделать учетную запись Кристины безопаснее. Давайте начнем с условного доступа.

Условный доступ

Условный доступ Azure позволяет создавать политики, которые применяются по отношению к пользователям. Эти политики используют назначения и средства управления доступом для настройки доступа к ресурсам.

Назначения определяют пользователей, группы пользователей, роли в Azure AD или гостевых пользователей, к которым применяется политика. Также можно указать применение политики к конкретным приложениям, таким как Microsoft 365 в нашем примере.

Назначения могут определять и условия, обязательные к выполнению (например, требуется определенная платформа, скажем iOS, Android, Windows и т. д.), особое расположение по IP-адресу и многое другое.

Элементы управления доступом определяют, как применяется политика условного доступа (Conditional Access policy). Наиболее строгий контроль доступа – это его блокировка. Но вы можете использовать средства контроля доступа, чтобы потребовать от пользователя использование устройства, отвечающего определенным условиям, использование одобренного приложения для доступа к вашим ресурсам, использование MFA и т. д.

Чтобы создать политику условного доступа, найдите на портале Azure условный доступ Azure AD. Затем нажмите кнопку **New Policy** (Новая политика) для создания политики, как показано на рис. 5.8.



СОВЕТ К ЭКЗАМЕНУ

Условный доступ возможен только на премиум-уровнях Azure AD. Поскольку в примерах мы пользуемся бесплатной версией Azure AD, то **New Policy** (Новая политика) у нас отключена на рис. 5.8.

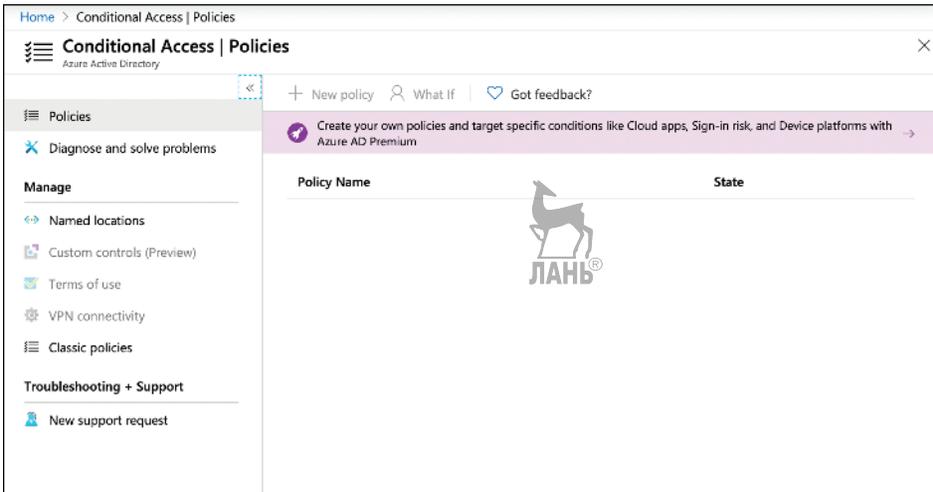


Рис. 5.8 Блейд политик условного доступа на портале Azure

Многофакторная аутентификация (Multifactor authentication, MFA)

По умолчанию пользователи могут входить в Azure AD, используя только имя пользователя и пароль. Даже если вы требуете от них использования надежных паролей, предоставление доступа к вашим ресурсам только с именем пользователя и паролем ставит под угрозу безопасность. Если злоумышленник получает пароль с помощью программного обеспечения, угадывающего пароли, или с помощью фишинга (phishing), или же других средств, то ваши ресурсы перестают быть под защитой.

Многофакторная аутентификация решает эту проблему. Концепция многофакторной аутентификации заключается в том, что вы должны пройти аутентификацию, используя комбинацию:

- что-то, что вы знаете, например имя пользователя и пароль;
- что-то, что у вас есть, например телефон или мобильное устройство;
- то, что привязано к вашему телу, например распознавание лица или отпечаток пальца.

Если многофакторная аутентификация требует всех трех ключей, она называется трехфакторной аутентификацией. Если требуются только первые два, это называется двухфакторной аутентификацией. (Microsoft называет это *двухэтапной проверкой*.) Многофакторная проверка подлинности Azure – это двухфакторная проверка.

ПРИМЕЧАНИЕ **БИОМЕТРИЯ В МОБИЛЬНЫХ УСТРОЙСТВАХ**

Несмотря на то что многофакторная проверка подлинности Azure является двухфакторной, если вы используете мобильное устройство, включающее биометрические функции, вы можете пройти проверку подлинности с использованием трехфакторного варианта. Однако третий фактор может запросить ваше мобильное устройство, а не Azure. Многофакторная аутентификация Azure не требует трехфакторной проверки подлинности.

Чтобы включить многофакторную аутентификацию для одного или нескольких пользователей Azure AD, откройте блейд **All Users** (Все пользователи) и выберите **Multi-Factor Authentication** (Многофакторная аутентификация), как показано на рис. 5.9. (Если у вас монитор большой, то кнопка многофакторной проверки подлинности будет видна по умолчанию.)

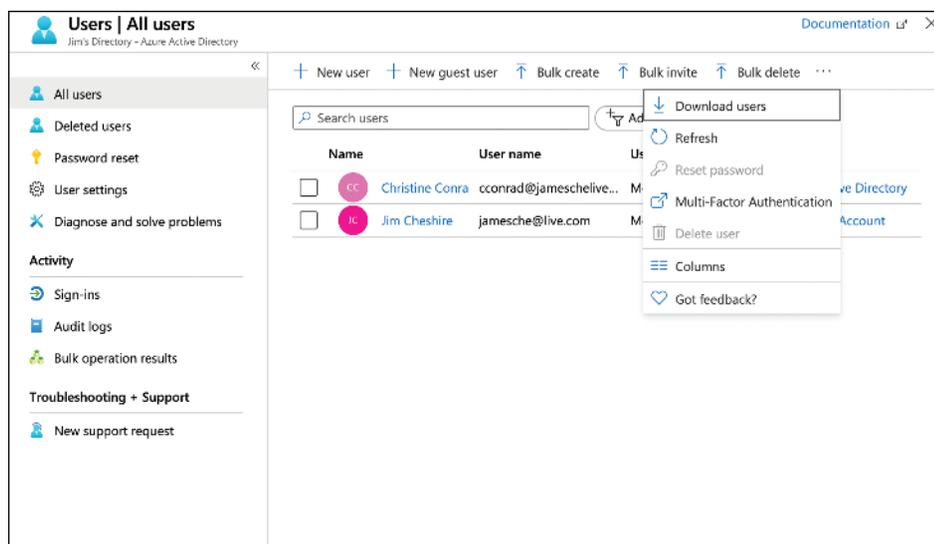


Рис. 5.9 Включение многофакторной аутентификации

ДОПОЛНИТЕЛЬНО **ОБЪЕДИНЕННАЯ РЕГИСТРАЦИЯ ИНФОРМАЦИИ О ЗАЩИТЕ**

Для улучшения работы пользователей Microsoft рекомендует использовать объединенную регистрацию, которая позволяет пользователям регистрироваться в MFA со сбросом предложенного пароля. Вы можете ознакомиться с этим подробнее на сайте <https://bit.ly/az900-combinedregistration>.

При нажатии **Multi-Factor Authentication** (Многофакторная аутентификация) открывается новое окно браузера, на котором отображается сайт управления пользователями Azure AD. Выберите одного или нескольких пользователей, для которых требуется включить многофакторную проверку подлинности, и нажмите кнопку **Enable** (Включить), как показано на рис. 5.10.



СОВЕТ К ЭКЗАМЕНУ

MFA проще всего настроить с помощью политики условного доступа. Помимо не-сложного использования, настройка MFA при помощи условного доступа также позволяет настраивать ее для гостевых пользователей, чего нельзя сделать при помощи сайта, показанного на рис. 5.10.

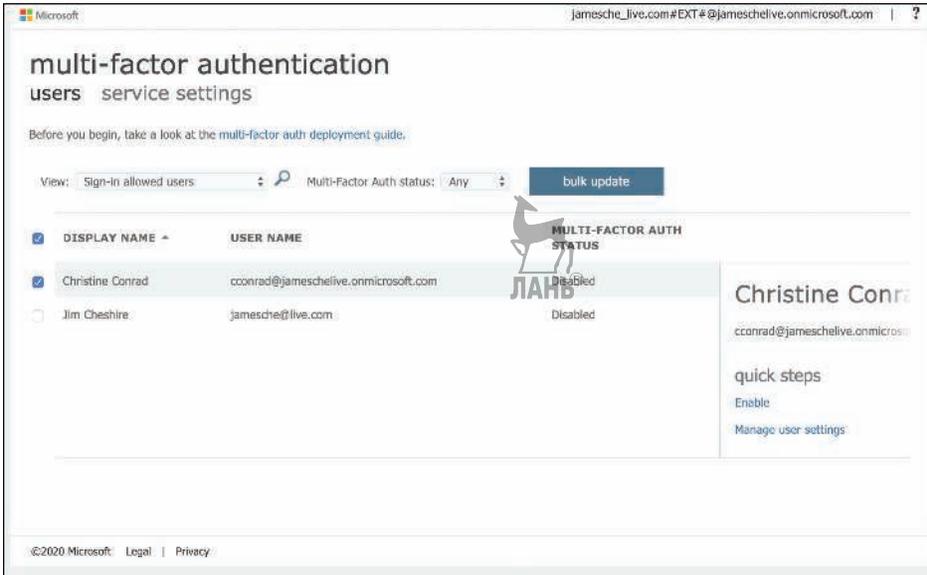


Рис. 5.10 Включение многофакторной проверки подлинности

Как только пользователю потребуется MFA, он должен будет выполнить второй этап при входе на портал Azure. Это может быть и запрос (prompt) из приложения Microsoft Authenticator (доступно для iOS и Android), смс с номером доступа, телефонный звонок, требующий ввода кода доступа, или же аппаратный ключ защиты OAUTH.

ДОПОЛНИТЕЛЬНО АППАРАТНЫЙ КЛЮЧ ЗАЩИТЫ OAUTH

OAUTH – это небольшое устройство, которое отображает номер доступа. При появлении запроса в вашем браузере быстро введите этот номер доступа, чтобы завершить аутентификацию.

Управление доступом на основе ролей

Управление доступом на основе ролей (Role-based access control, RBAC) – это общий термин, который относится к концепции авторизации пользователей в системе на основе определенных ролей, к которым принадлежит пользователь. Azure внедряет RBAC во всех ресурсах Azure, чтобы вы могли контролировать взаимодействие пользователей и приложений с ресурсами Azure.

Возможно, вы захотите разрешить пользователям, которые администрируют ваши базы данных, доступ к базам данных в определенной группе ресурсов, но вы не хотите разрешать этим людям создавать новые базы данных или удалять существующие. А может, вам будет нужно, чтобы некоторые веб-разработчики могли разворачивать новый код в ваших веб-приложениях, но вам не нужно, чтобы они могли масштабировать приложение по более дорогостоящему тарифному плану. Это всего лишь два примера того, что можно сделать с помощью RBAC в Azure.

RBAC состоит из четырех элементов:

- **Security principal** (Субъект безопасности). Представляет отдельную идентичность. Это может быть пользователь, группа, приложение (которое называется субъект-службой) или специальный объект AAD, называемый *управляемым удостоверением* (managed identity). Управляемое удостоверение – это способ авторизации другой службы Azure для доступа к вашему ресурсу Azure;
- **Role** (Роль) – это то, что определяет, как субъект безопасности может взаимодействовать с ресурсом Azure (иногда называют определением роли). Например, роль может определить, что субъект безопасности может читать свойства ресурса, но не может создавать новые или удалять существующие;
- **Scope** (Область действия). Определяет уровень, на котором применяется роль, и определяет, какие рычаги управления доступны субъекту безопасности. Например, если область относится к группе ресурсов, роль определяет действия, которые могут выполняться со всеми ресурсами в этой группе;
- **Role assignments** (Назначения ролей). Роли назначаются субъекту безопасности в определенной области, и именно это определяет уровень доступа для субъекта.

RBAC включает множество встроенных ролей. Три из них применяются ко всем ресурсам Azure:

- **Owner** (Владелец). Члены этой роли имеют полный доступ к ресурсам;
- **Contributor** (Участник). Члены этой роли могут создавать ресурсы и управлять ими, но они не могут делегировать это право кому-либо другому;
- **Reader** (Читатель). Члены этой роли могут просматривать ресурсы Azure, но не могут создавать, удалять или управлять этими ресурсами.

Все остальные встроенные роли относятся к определенным типам ресурсов Azure.

Чтобы предоставить кому-то доступ к ресурсу с помощью RBAC, откройте этот ресурс на портале Azure. Нажмите **Access Control (IAM)** (Управление доступом) на портале для настройки RBAC. На рис. 5.11 RBAC настраивается для веб-приложения, размещенного в службе приложений Azure. Нажатие **Add** (Добавить) в поле **Add a Role Assignment** (Добавить назначение ролей) позволяет добавить роль.

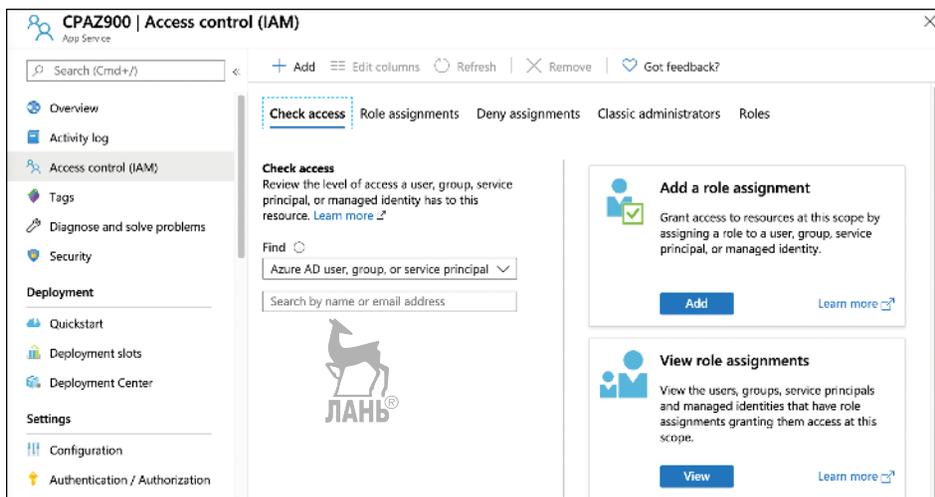


Рис. 5.11 Настройка RBAC для веб-приложения



СОВЕТ К ЭКЗАМЕНУ

Область действия RBAC определяется местом назначения роли RBAC. Например, если открыть группу ресурсов на портале и назначить пользователю роль RBAC, то область будет находиться на уровне группы ресурсов. С другой стороны, если вы открываете веб-приложение в этой группе ресурсов и назначаете роль, то областью действия будет только это веб-приложение. Этот пользователь не будет иметь доступа к другим приложениям в группе ресурсов, если к нему не будут применены иные назначения ролей. Роли RBAC могут быть ограничены группой управления, подпиской, группой ресурсов или уровнем ресурсов.

После нажатия кнопки **Add** (Добавить) выберите роль, которую вы хотите назначить. Список ролей будет отличаться в зависимости от типа ресурса. Выберите, кому или чему вы хотите назначить роль, а затем нажмите кнопку **Save** (Сохранить), как показано на рис. 5.12.

На рис. 5.12 показан список пользователей в AAD, так как в выпадающем списке **Assign Access To** (Назначить доступ к) представлены объекты AAD. Список других типов объектов можно просмотреть, выбрав другой тип ресурса. Например, на рис. 5.13 мы выбираем встроенный тип управляемого удостоверения, который добавит виртуальные машины Azure к роли **Website Contributor** для этого веб-приложения.



СОВЕТ К ЭКЗАМЕНУ

Важно понимать, что назначения ролей суммируются. Ваша конечная роль в любой области является результатом назначения ролей вплоть до этого уровня. Другими словами, если у меня уже есть роль **Owner** (Владелец) в группе ресурсов и вы назначите мне роль **Website Contributor** в веб-приложении в этой группе ресурсов, то назначение **Website Contributor** не будет иметь никакого эффекта, так как роль **Owner** (Владелец) уже наделяет меня всеми правами, доступными для участника (contributor).

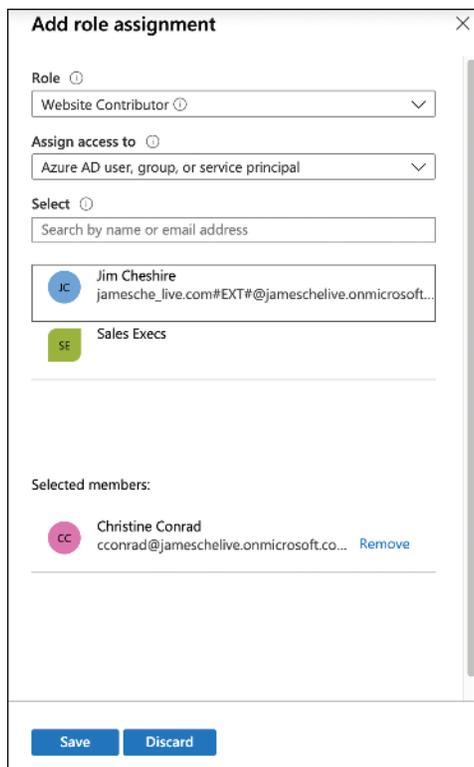


Рис. 5.12 Добавление роли

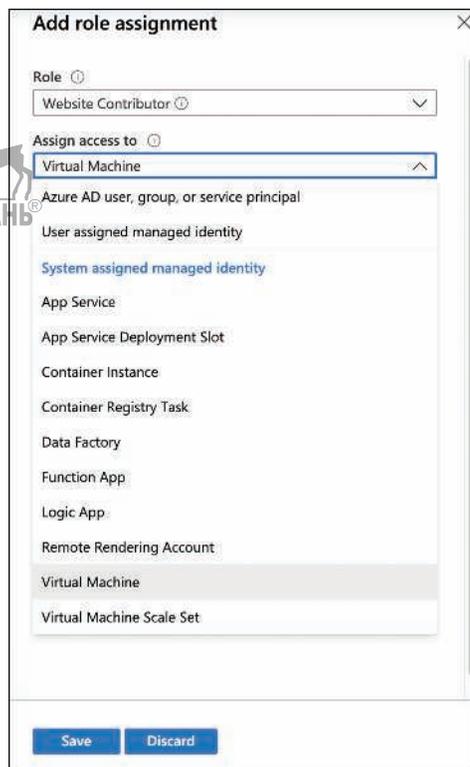


Рис. 5.13 Назначение управляемого удостоверения роли

RBAC применяется Azure Resource Manager (ARM). При попытке взаимодействия с ресурсом Azure, будь то на портале Azure или с помощью инструмента командной строки, ваша учетная запись проверяется с помощью ARM, и метка (token) генерируется для вас. Эта метка соответствует вашей учетной записи и всем назначенным ролям, и она включается во все операции, которые вы выполняете в Azure. ARM может определить, разрешено ли выполняемое действие ролям, которые вам назначены. Если это так, вызов завершается успешно. Если нет, вам будет отказано в доступе.

Вы можете убедиться в том, что у кого-то есть необходимые права, проверив доступ на портале Azure. Откройте ресурс и нажмите **Access Control (IAM)** (Контроль доступа (IAM)). Перейдите на вкладку **Check Access** (Проверить доступ) и найдите пользователя или ресурс, к которому предоставлен доступ, как показано на рис. 5.14.

Для получения более подробной информации о том, какие точные операции разрешены и не разрешены, нажмите на отображаемую роль. Это позволит просмотреть подробный список операций и комбинацию прав на чтение, запись, удаление и другие действия, которые может выполнять субъект безопасности.

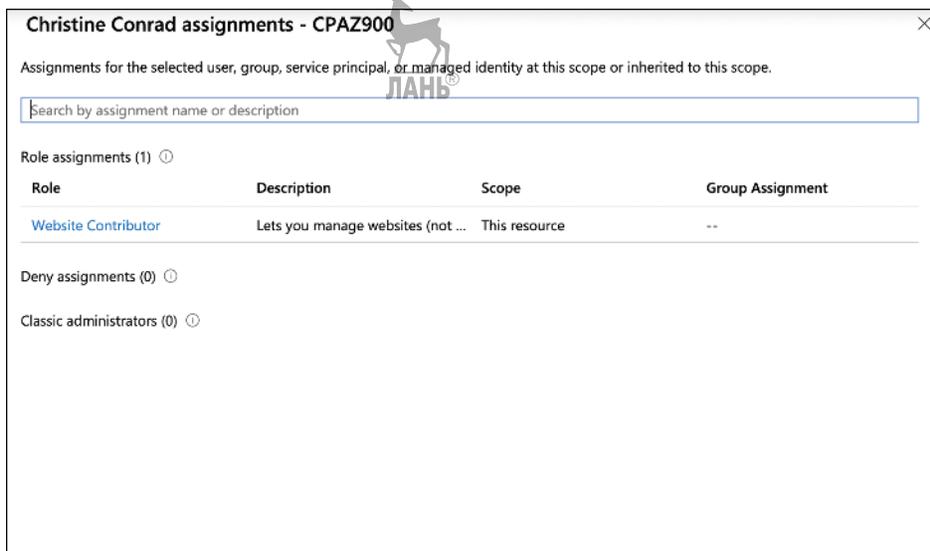


Рис. 5.14 Просмотр назначений ролей для пользователя



СОВЕТ К ЭКЗАМЕНУ

Ранее мы немного затронули субъект-службы, поскольку они относятся к приложениям Azure AD. Субъект-службы представляют собой субъекты безопасности в лице приложения. Субъект безопасности, который представляет собой пользователя, называется *субъектом-пользователем* (user principal). Важно не забывать, что и субъект-пользователь, и субъект-служба являются субъектами безопасности.

Навык 5.2: описание основных функций управления Azure

Чем дольше вы пользуетесь облаком, тем выше вероятность, что количество ваших ресурсов Azure, охватывающих множество различных служб Azure, будет увеличиваться. Если вы не контролируете создание и управление ресурсов, то ваши затраты также могут стать неконтролируемыми. Кроме этого, на вас могут свалиться и другие ограничения вроде определения регионов, в которых будут создаваться ресурсы, как они будут помечаться и т. д.

Традиционный способ решения подобных проблем управления состоял бы в рассылке пользователям памятки с объяснением требований и скрещении пальцев в надежде, что все будут их соблюдать. К счастью, политика Azure может гарантировать вам соблюдение нормативных требований и политик.

В этом разделе описаны следующие продукты:

- политика Azure (Azure Policy);
- блокировки ресурсов (Resource locks);
- теги (Tags);
- Azure Blueprints.



Политика Azure

Политика Azure (Azure Policy) позволяет определять правила, которые применяются при создании и управлении ресурсами Azure. Например, можно создать политику, указывающую, что может быть создана ВМ только определенного размера и что все ВМ должны быть созданы в южно-центральной зоне США. Azure возьмет на себя применение данного алгоритма, чтобы соблюдались корпоративные политики.

Чтобы получить доступ к политике Azure, введите **policy** (политика) в поле поиска на портале Azure и нажмите **Policy** (Политика). Кроме того, вы можете нажать **All Services** (Все службы) и найти **политику** в списке. Действие отобразит блейд **Policy** (Политика), как показано на рис. 5.15.

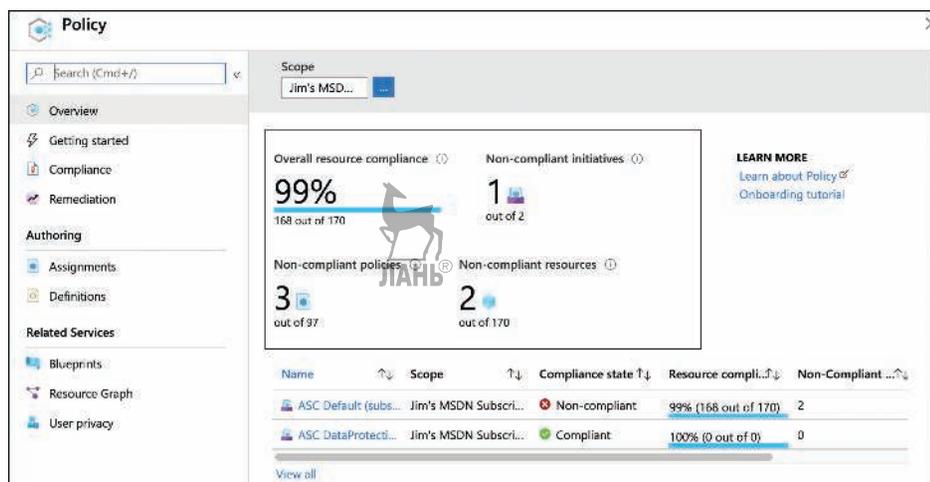


Рис. 5.15 Политика Azure на портале Azure

По умолчанию политика Azure показывает соответствие политикам, определенным в подписке Azure. Если вы хотите, то можете использовать это представление для другой подписки или группы ресурсов, нажав на многоточие (...) рядом с областью работы и выбрав новую область, как показано на рис. 5.16.

Несоответствие требованиям, показанное на рис. 5.15, основано на политиках, реализованных Центром безопасности Azure (Azure Security Center). Нажав на элемент, не соответствующий требованиям, вы можете увидеть полную информацию о том, что входит и не входит в политику, как показано на рис. 5.17.

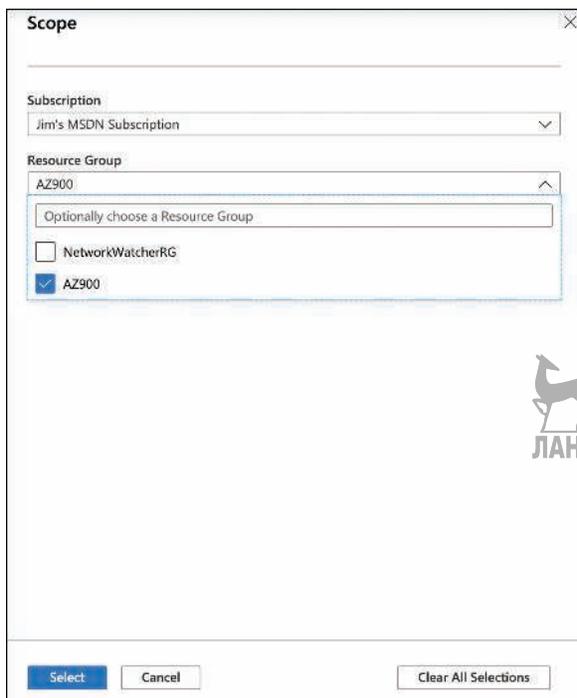


Рис. 5.16 Изменение области действия блейда Policy (Политика) на портале

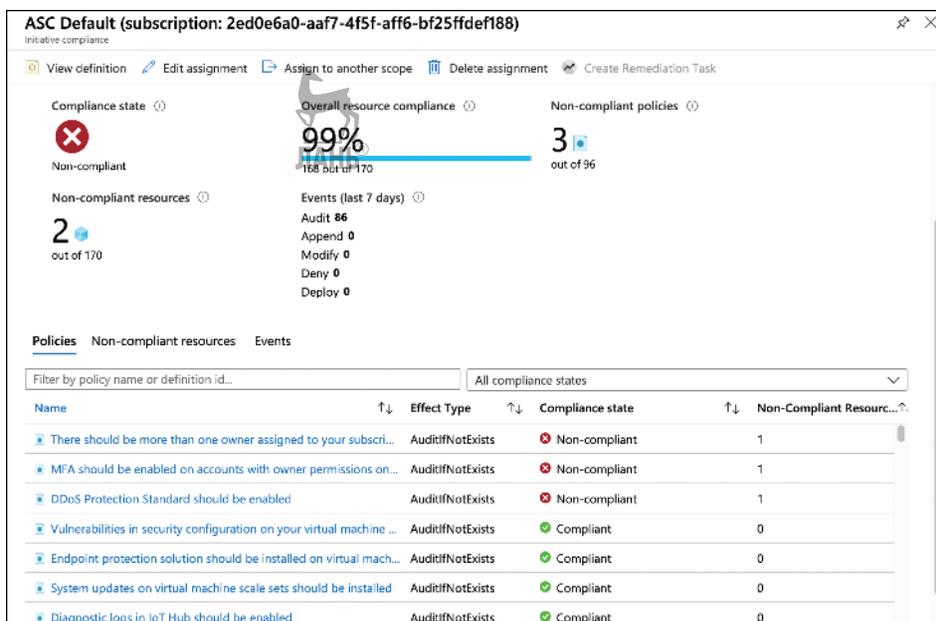


Рис. 5.17 Подробные сведения о соответствии требованиям

Обратите внимание, что название элемента – *ASC Default*, за которым следует идентификатор подписки. *ASC Default* представляет собой совокупность нескольких политик, определенных Центром безопасности Azure. Политика Azure позволяет легко вводить полный набор политик, объединяя их в группу, называемую *инициативой* (initiative). Определяя такую группу, вы можете легко определить сложные правила, обеспечивающие управление политикой компании.

Можно назначить новую политику путем выбора политики из списка уже включенных по умолчанию или же путем создания собственной политики. Чтобы назначить политику из списка включенных, нажмите **Assignments** (Назначения), затем выберите **Assign Policy** (Назначить политику), как показано на рис. 5.18.

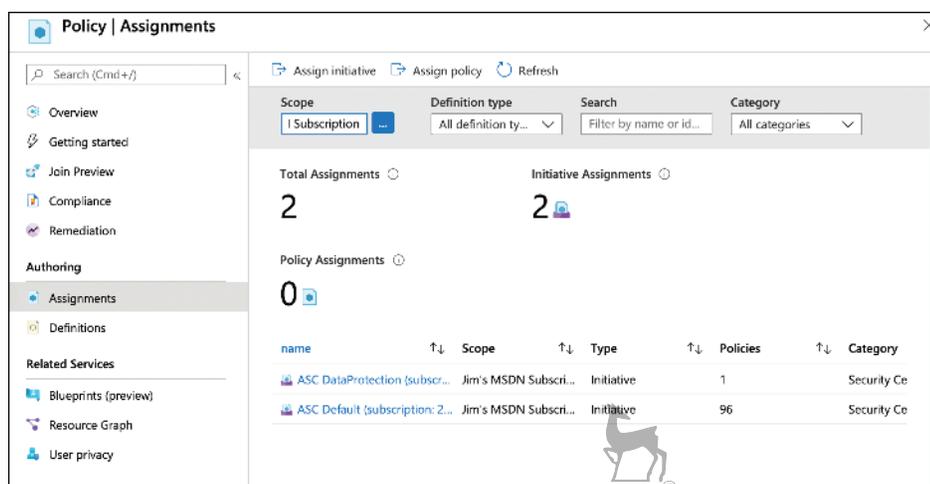


Рис. 5.18 Назначение политики

Для выбора политики нажмите на многоточие рядом с **Policy Definition** (Определение политики), как показано на рис. 5.19.

В этом случае применяется политика, которая помечает любое приложение службы приложений, не настроенное под использование службы виртуальной сети конечного устройства. Это можно сделать, введя **app service** (служба приложений) в поле поиска и выбрав встроенную (built-in) политику, как показано на рис. 5.20.

После того как вы нажали кнопку **Select** (Выбрать), как показано на рис. 5.20, появится подробная информация по выбранной политике. Если вы перейдете на вкладку **Parameters** (Параметры), то увидите влияние политики. Как показано на рис. 5.21, результатом данной политики является *AuditIfNotExists*.

Home > Policy | Assignments > Assign policy

Assign policy

Basics Parameters Remediation Review + create

Scope
 Scope [Learn more about setting the scope *](#)
 ...

Exclusions
 ...

Basics
 Policy definition *
 ...

Assignment name * ⓘ
 ...

Description

Review + create Cancel Previous Next

Рис. 5.19 Выбор определения политики

Available Definitions

Type: Search:

Policy Definitions (2)

App Service should use a virtual network service endpoint
 Built-in
 This policy audits any App Service not configured to use a virtual network service endpoint.

Diagnostic logs in App Services should be enabled
 Built-in
 Audit enabling of diagnostic logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised

Select Cancel

Рис. 5.20 Добавление встроенного определения политики

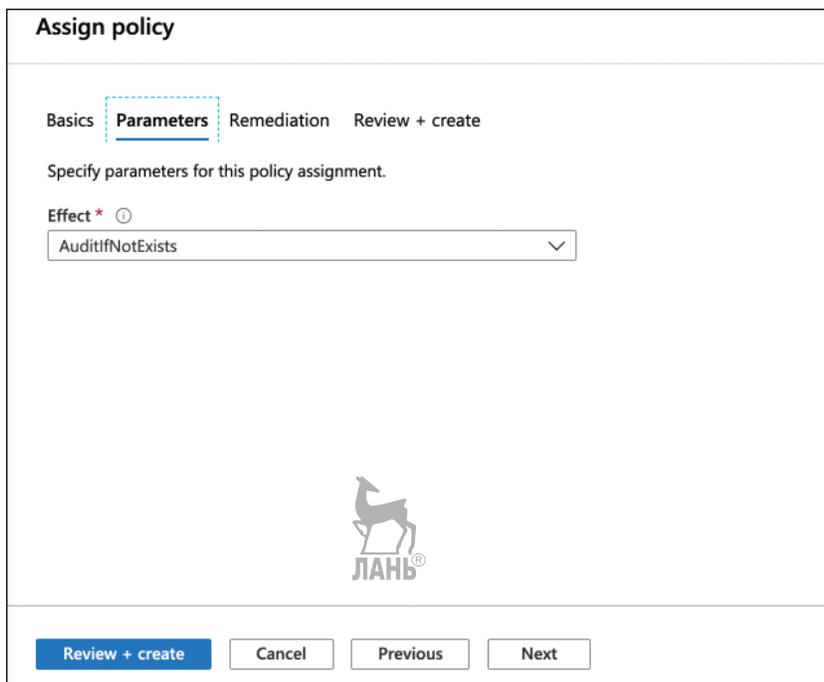


Рис. 5.21 Завершение назначения политик

В политике Azure поддерживается шесть различных результатов. Однако не все они доступны для встроенных политик. Результаты действия политик:

- **Append** (Добавить) – добавляет дополнительные свойства к ресурсу; может быть использован для добавления к ресурсам тега с определенным значением;
- **Audit** (Аудит) – регистрируется предупреждение, если политика не соблюдается;
- **AuditIfNotExists** (Аудит, если не существует) – позволяет указать дополнительный тип ресурса, который должен существовать вместе с создаваемым или обновляемым ресурсом. Если этот тип ресурса не существует, регистрируется предупреждение;
- **Deny** (Запретить) – запрещает операции создания или обновления;
- **DeployIfNotExists** (Развернуть, если не существует) – позволяет указать дополнительный тип ресурсов, который требуется развернуть вместе с создаваемым или обновляемым ресурсом. Если этот тип ресурса не создан, он разворачивается автоматически;
- **Disabled** (Отключено) – политика не действует.

ДОПОЛНИТЕЛЬНО РЕЗУЛЬТАТЫ ПОЛИТИК

Более подробную информацию о результатах действия политик, включая примеры каждого из них, смотрите по ссылке <https://bit.ly/az900-policyeffects>.

Помимо использования встроенных политик, можно также определять собственные политики, создавая определение пользовательской политики, которое представляет собой ARM-шаблоны. Дополнительные сведения о создании определения пользовательской политики смотрите в разделе: <https://bit.ly/az900-custompolicy>.

Блокировки

RBAC – отличный способ управления доступом к ресурсу Azure, но лишь в тех случаях, когда вам нужно предотвратить изменения или удаление ресурса. В этом случае блокировки (resource locks или locks) являются наиболее простым решением. В отличие от RBAC, блокировки применяются ко всем, кто имеет доступ к ресурсу.



СОВЕТ К ЭКЗАМЕНУ



Для того чтобы создать блокировку, вы должны быть либо в роли **Owner** (Владелец), либо **User Access Administrator** (Администратор доступа пользователей) в RBAC. Кроме того, администратор может создать настраиваемую роль, предоставляющую право на создание блокировки.

Блокировки могут быть применены на уровне ресурса, группы ресурсов или на уровне подписки. Чтобы применить блокировку к ресурсу, откройте ресурс на портале Azure и выберите **Locks** (Блокировки) в разделе **Settings** (Настройки) в меню слева, как показано на рис. 5.22.

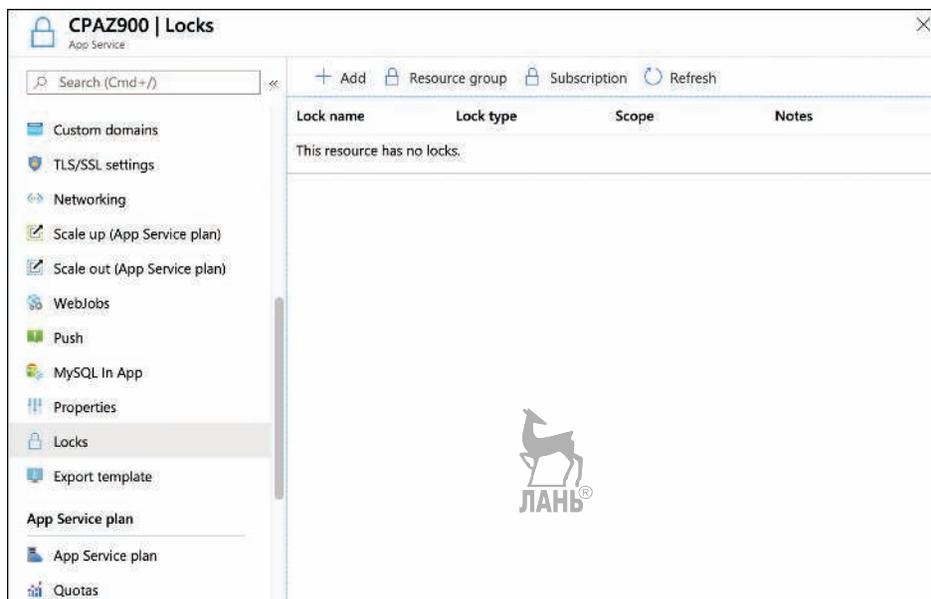


Рис. 5.22 Блокировка ресурса

Чтобы добавить блокировку ресурса, нажмите кнопку **Add** (Добавить). (Вы также можете просмотреть и добавить блокировки в группу ресурсов или подписку.) В строке **Lock Name** (Имя блокировки) укажите ее имя, задайте ее тип (**Lock Type**) и добавьте дополнительное примечание, как показано на рис. 5.23.

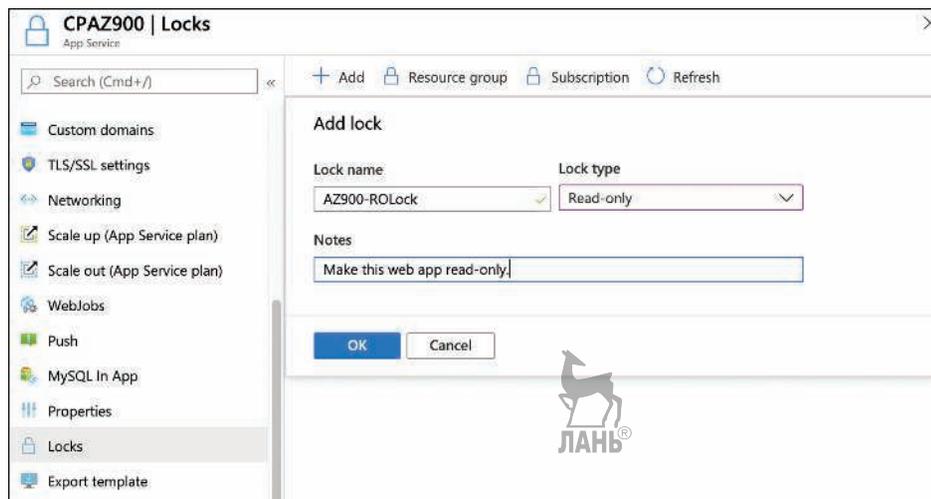


Рис. 5.23 Добавление блокировки **read-only** (только чтение)

Блокировка **read-only** (только чтение) является наиболее ограничивающей. Она предотвращает изменение свойств или удаление ресурса. Блокировка **delete lock** (удаление) предотвращает удаление ресурса, при этом его свойства могут быть изменены. Результат блокировки **read-only** (только чтение) часто непредсказуем из-за того, как эти блокировки обрабатываются Azure.

Блокировки применяются только к операциям, которые обрабатываются ARM, а некоторые операции, специфичные для ресурса, обрабатываются внутри самого ресурса. Например, блокировка **read-only** (только чтение), примененная к хранилищу ключей Azure, не позволит пользователю изменять политики доступа к хранилищу, но пользователи все равно могут добавлять и удалять ключи, информацию и сертификаты, поскольку эти операции обрабатываются самим хранилищем ключей.

Существуют и другие ситуации, когда блокировка **read-only** (только чтение) может предотвратить выполнение неожиданных операций. Например, если вы разместите блокировку **read-only** (только чтение) на учетной записи хранилища, это не позволит пользователям получить ключи доступа к учетной записи хранилища, так как операция получения списка ключей делает их доступными для записи.

Если блокировка применяется к группе ресурсов, то все ресурсы этой группы наследуют блокировку. Аналогично если блокировка применяется на уровне подписки, все ресурсы подписки наследуют блокировку. Возможны вложенные блокировки, и в таких ситуациях срабатывает наиболее результативная блокировка. Например, если у вас есть блокировка **read-only** (только чтение) для

группы ресурсов и блокировка **delete lock** (удаление) для отдельного ресурса в этой группе, то к ресурсу применится блокировка **read-only** (только чтение). Эксплицитная блокировка **delete lock** (удаление) в этом случае не нужна.



СОВЕТ К ЭКЗАМЕНУ

Блокировки также наследуются вновь созданными ресурсами. Если применить блокировку удаления к группе ресурсов и после добавить новый ресурс в группу, то этот ресурс автоматически унаследует блокировку удаления.

При попытке выполнить запрещенную блокировкой операцию на портале появляется сообщение об ошибке, как показано на рис. 5.24.



СОВЕТ К ЭКЗАМЕНУ

Не все типы ресурсов оповещают вас, что блокировка предотвратила операцию, предпринятую на портале. Бывает и такое, что вы получаете уведомление с общим сообщением об ошибке. При попытке выполнить ту же операцию в Azure CLI или при помощи модуля Az в PowerShell вы должны получить подробную информацию о блокировке.

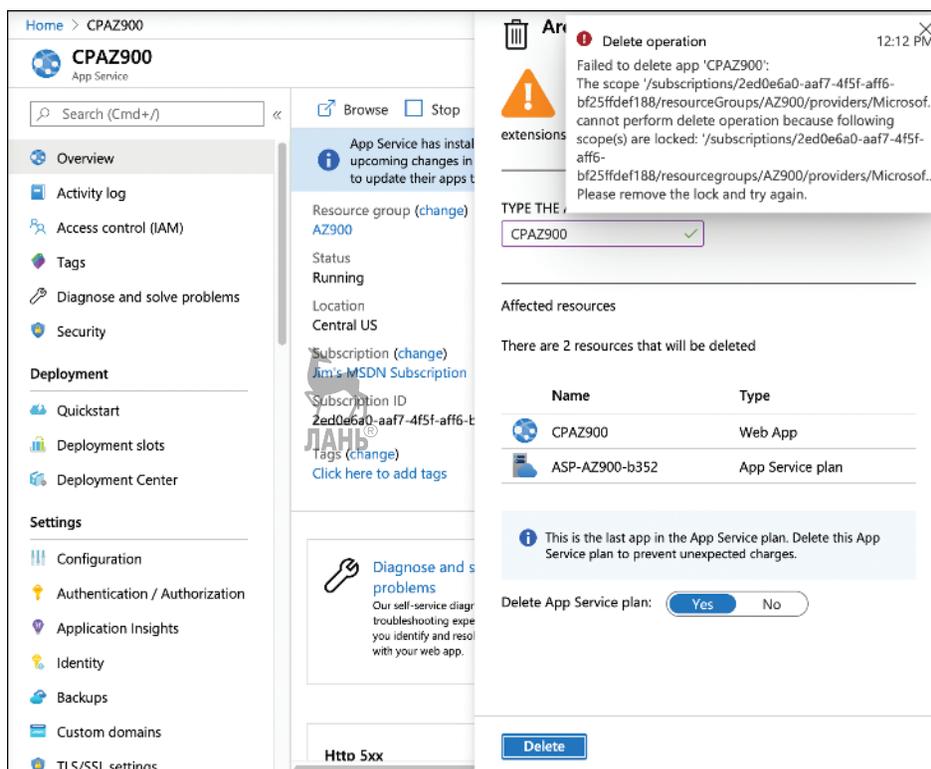


Рис. 5.24 Отказ блокировкой

Вы можете отредактировать или удалить блокировку на портале, нажав на соответствующие иконки, как показано на рис. 5.25. Зачастую вам не нужно будет прокручивать вправо, чтобы увидеть кнопки **Edit** (Редактирование) и **Delete** (Удаление).

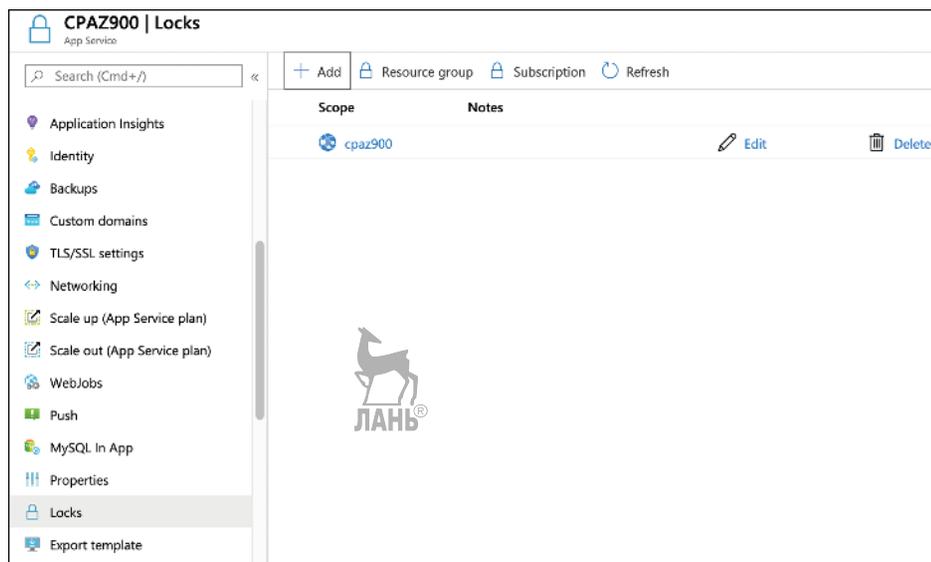


Рис. 5.25 Редактирование или удаление блокировки

Теги

Еще одной функцией Azure, упрощающей организацию ресурсов, являются теги (tags). Тег состоит из имени и значения. Например, компания участвует в двух торговых мероприятиях: одно проводится в Техасе, другое – в Нью-Йорке. Для поддержки этих событий было создано множество ресурсов Azure. Вам нужно посмотреть все ресурсы Azure, касающиеся одного события, однако они распределены по нескольким группам ресурсов. Добавив в каждую группу тег, идентифицирующий событие, с которым она связана, вы можете решить сложившуюся проблему.

На рис. 5.26 вы видите теги, связанные с группой ресурсов *WebStorefront*. Группе был присвоен тег *EventName*, значение которого равно *Contoso-Texas*. Нажав на значок куба справа от тега, вы сможете просмотреть все ресурсы, имеющие такой тег.

ПРИМЕЧАНИЕ ОТОБРАЖЕНИЕ ТЕГОВ

Чтобы просмотреть все теги, выберите **All Services** (Все службы) в главном меню портала, а затем выполните поиск **Tags** (Теги) в списке служб.

Тег можно будет применить и ко многим другим ресурсам Azure, а не только к группе ресурсов. Важно понимать, что добавление тега в группу ресурсов

не значит, что он будет добавляться к ресурсам в самой группе. При наличии веб-приложения в группе ресурсов *WebStorefront* приложение не будет наследовать примененный к группе ресурсов тег. Поэтому теги привносят дополнительный уровень гибкости и эффективности при просмотре ресурсов Azure.

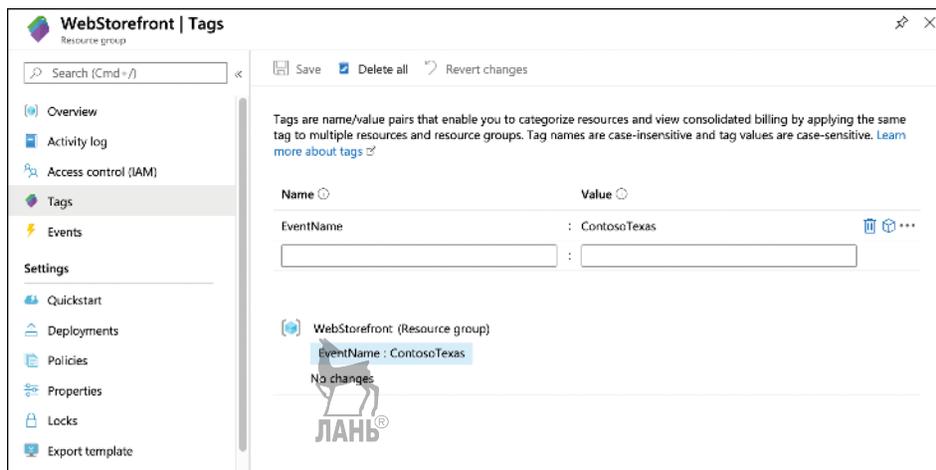


Рис. 5.26 Маркирование группы ресурсов



СОВЕТ К ЭКЗАМЕНУ

Теги также помогают вам контролировать расходы на Azure. При загрузке счета Azure в столбце появятся теги ресурсов. Поскольку счета Azure можно загружать в виде разделенных запятыми значений, вы можете использовать подобные Microsoft Excel инструменты для фильтрации по тегам.

Azure Blueprints

Принимая решение о создании облачного приложения, компания прежде всего тщательно планирует создание даже одного ресурса Azure, вместо того чтобы сразу приступить к действию. В такое планирование входит план обеспечения соответствия всей архитектуры облачного приложения необходимым стандартам, а также концепции (подобные планированию топологий виртуальных сетей) и назначение прав пользователям приложения. Помимо этого, передовой опыт также является частью планирования.

Компания сильно рискует при неправильном планировании, и поэтому многие компании приглашают на работу квалифицированных специалистов, компетентных в этом вопросе. Такие действия могут стать причиной дополнительных финансовых и временных затрат для компании.

Azure Blueprints является службой, которая упрощает процесс развертывания в облаке. **Blueprint** (план, чертеж) позволяет настроить среду необходимым вам образом наряду со всеми существующими политиками и другими

асpekтами управления. Настройки можно будет сохранить для дубликации при дальнейших развертываниях.

Элементы, которые вы добавляете в *blueprint*, называются *артефактами*. Артефактом может быть и группа ресурсов, ARM-шаблон, назначение политики или роли. Создав *blueprint*, его можно будет затем сохранить либо в подписке, либо в группе управления. Потом сохраненный в группе управления *blueprint* может быть использован любой подпиской в иерархии этой группы управления.



СОВЕТ К ЭКЗАМЕНУ

Вам наверняка будет интересно узнать, что чертежи (*blueprints*) отличаются от ARM-шаблонов. Мы с вами говорили, что ARM-шаблоны используются для облегчения предсказуемого и воспроизводимого разворачивания. Чертежи же предлагают множество преимуществ по сравнению с ARM-шаблонами.

Поскольку чертежи являются реальными ресурсами Azure, а не просто файлами, предназначенными для определения разворачивания, Azure поддерживает связь между чертежами и ресурсами, которые их используют. Это позволяет компаниям проводить итерацию по чертежам и улучшать их, что значительно облегчает разработку проекта в соответствии с требованиями компании. Помимо перечисленного, чертежи версионированы (имеют версии) и могут храниться в системе управления версиями электронных материалов, поэтому процесс отслеживания чертежей прост и эффективен.

Вдобавок чертежи не могут заменить ARM-шаблоны. Во многих чертежах широко используются ARM-шаблоны как артефакты.

Для создания чертежа найдите **чертежи** на портале Azure и откройте **Blueprints | Getting Started page** (Начало работы с чертежами Azure), как показано на рис. 5.27.

На странице **Blueprints | Getting Started page** (Начало работы с чертежами Azure) нажмите кнопку **Create** (Создать), для того чтобы запустить процесс по созданию чертежа. Как показано на рис. 5.28, Microsoft предоставляет множество образцов шаблонов, которые могут быть использованы в качестве основы для вашего чертежа, плюс вы всегда можете начать с пустого чертежа.

Нажмите на ссылку, чтобы начать с пустого чертежа. Введите имя чертежа, описание и укажите место, где будет сохранено определение вашего чертежа. Это может быть либо подписка, либо группа управления. На рис. 5.29 создается чертеж, который затем будет сохранен в подписке.



СОВЕТ К ЭКЗАМЕНУ

Изменять имя или определение местоположения чертежа после его создания вы уже не можете.

Для добавления артефактов в чертеж нажмите **Next: Artifacts** (Далее: Артефакты), как показано на рис. 5.29. Нажмите **Add Artifact** (Добавить артефакт), чтобы добавить первый артефакт. Выберите **Artifact Type** (Тип артефакта) и введите необходимую информацию для добавления артефакта. На рис. 5.30 показано добавление артефакта группы ресурсов.

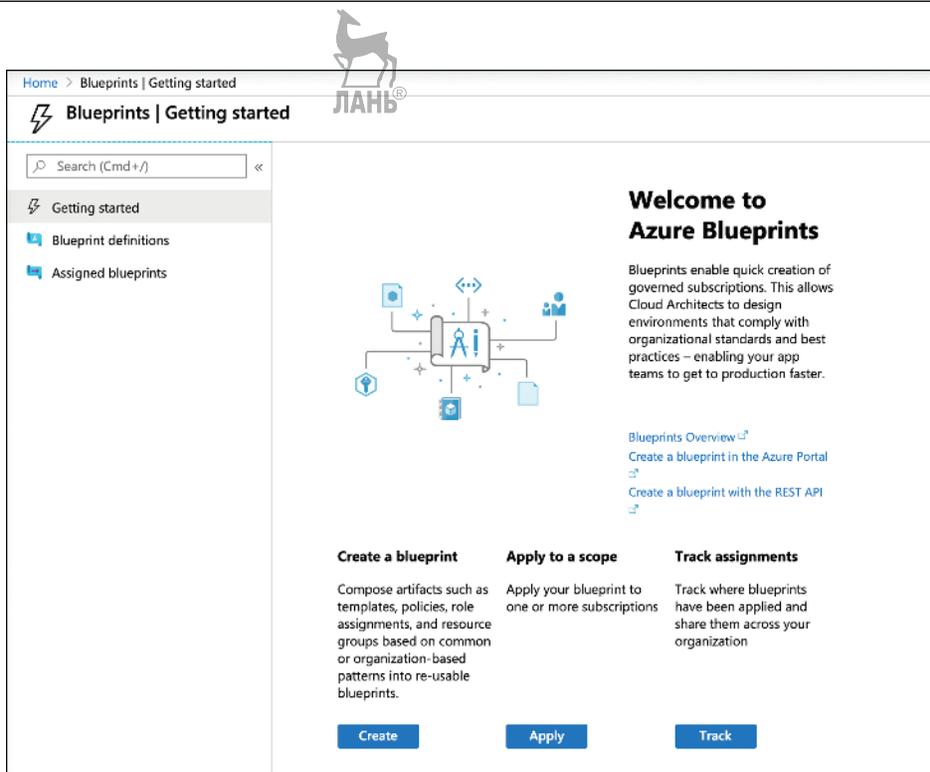


Рис. 5.27 Начало работы с чертежами Azure

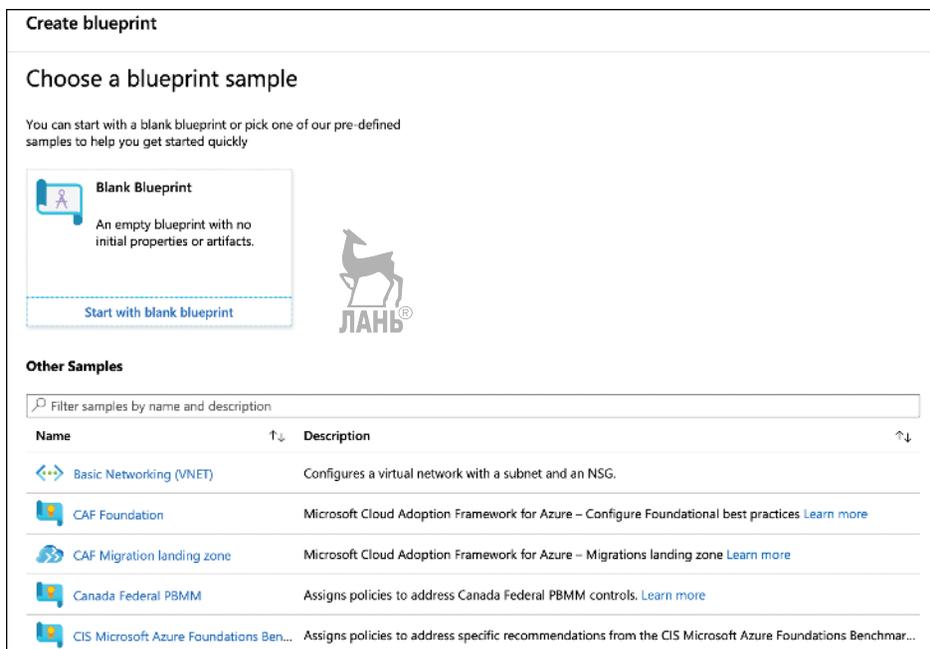


Рис. 5.28 Создание чертежа

Create blueprint

Basics Artifacts

Blueprint name * ⓘ
AZ900WebAppBlueprint ✓

Blueprint description
Sample web app with policies applied. ✓

Definition location * ⓘ
Jim's MSDN Subscription ✓

The management group or subscription where the blueprint is saved. The definition location determines the scope that the blueprint may be assigned to. Learn more at aka.ms/BlueLocation.

Save Draft Discard Next : Artifacts >

Рис. 5.29 Указание основных параметров чертежа

Home > Blueprints | Getting started > Create

Create blueprint

Basics Artifacts

Add artifacts to the blueprint. Add resource

Name

- Subscription
 - + Add artifact...

Add artifact

Artifact type *
Resource group

Artifact display name ⓘ
WebAppResourceGroup

i You can choose to fill these parameters in now or when assigning the blueprint.

Resource Group Name
Set value(s)

This value should be specified when the blueprint is assigned

Location
East US

This value should be specified when the blueprint is assigned

Resource Group Tags (Optional):

Tag Name	Tag Value
Enter tag name	:

Save Draft Discard « Pre Add Cancel

Рис. 5.30 Добавление артефакта



Чтобы ваш чертеж был универсален, вы можете его настроить так, что имя группы ресурсов и локация будут указываться при назначении чертежа посредством отметки **This Value Should Be Specified When The Blueprint Is Assigned** (Это значение следует указать при назначении чертежа), расположенной рядом с **Resource Group Name and/or Location** (Имя группы ресурсов и/или локация). Мы рассмотрим назначение чертежа немного позже. Нажмите **Add** (Добавить), после чего ваш артефакт будет добавлен в чертеж.

Закончив добавление артефактов, нажмите **Save Draft** (Сохранить черновик), как показано на рис. 5.30. Черновик чертежа можно будет редактировать и обновлять. Когда чертеж будет готов, вы можете его опубликовать.

Чтобы опубликовать чертеж, нажмите **Blueprint Definitions** (Определение чертежа) и нажмите чертеж, как показано на рис. 5.31.

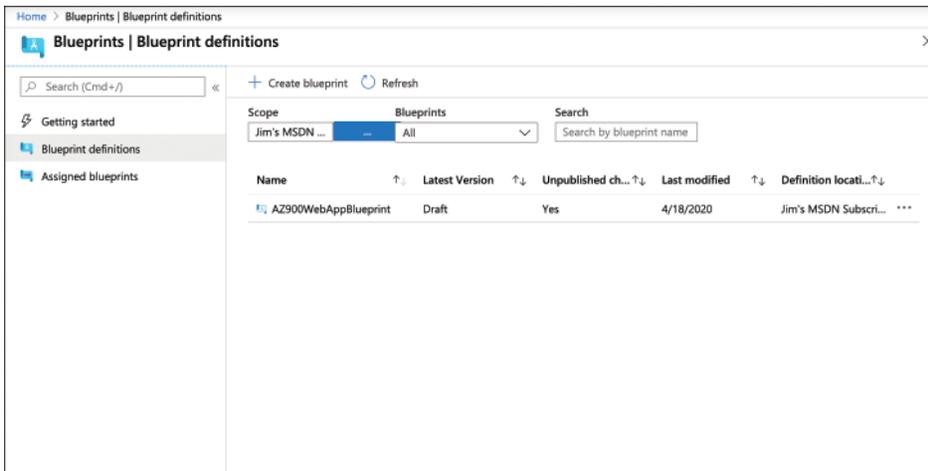


Рис. 5.31 Просмотр определений чертежа

Нажмите кнопку **Publish Blueprint** (Опубликовать чертеж), как показано на рис. 5.32.

Когда вы опубликуете чертеж, вам нужно будет указать номер версии. Желательно добавить еще примечания об изменениях. На рис. 5.33 наш чертеж публикуется как *Version 1.0*. Нажмите кнопку **Publish** (Опубликовать) для завершения.

Как только чертеж будет опубликован, его можно будет назначить подписке. Нажмите на чертеж, а затем **Assign Blueprint** (Назначить чертеж), как показано на рис. 5.34.

Чтобы назначить чертеж, введите имя, выберите местоположение и версию определения чертежа. (Можно также принять настройки по умолчанию.) Вы можете указать назначение блокировки для ресурсов, которые создает чертеж, нажав желаемый параметр назначения блокировки.

Нажатие на **Assign** (Назначить) завершит назначение чертежа.

Когда чертеж будет назначен подписке, определенные чертежом ресурсы начнут в ней создаваться.

AZ900WebAppBlueprint ✕

Blueprints

↑ Publish blueprint
✎ Edit blueprint
🗑 Delete blueprint

Name
 AZ900WebAppBlueprint 📄

State
 Draft

Definition location
 Jim's MSDN Subscription

Description
 Web app with policies

Definition location ID
 2ed0e6a0-aaf7-415f-aff6-bf25ffdef188

Version
 Draft

⤴

Latest artifacts

Artifact name	Resource type	Parameters
⌵ Assigned subscription	Subscription	
WebAppResourceGroup	Resource group	0 out of 2 parameters popula...

Рис. 5.32 Чертеж готов для публикации

Publish blueprint

Version * ⓘ
 1.0 ✓
 No previous versions

Change notes ⓘ
 Original version ✓



Publish
Cancel

Рис. 5.33 Публикация чертежа

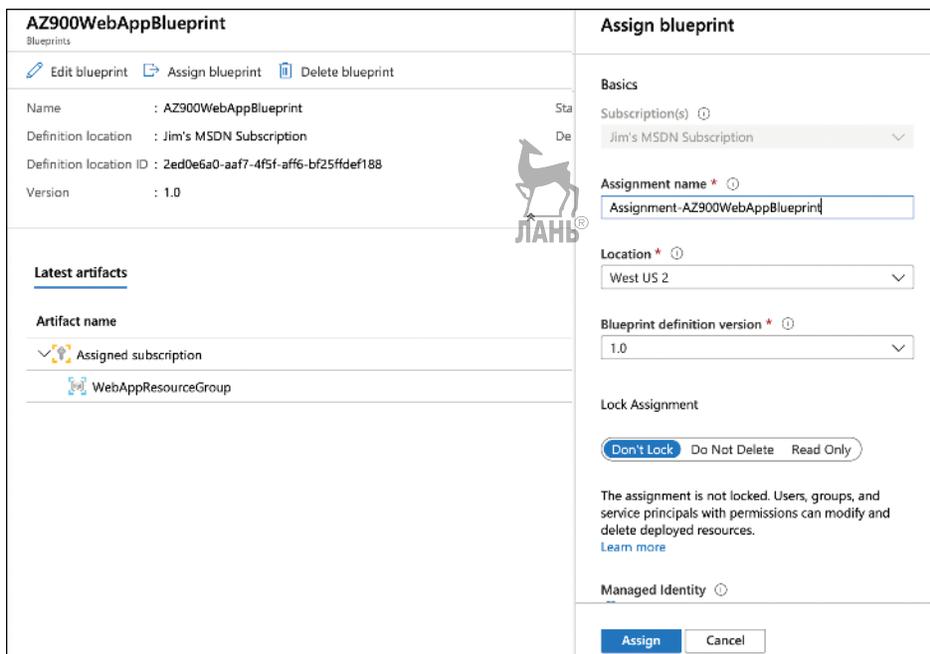


Рис. 5.34 Назначение чертежа

ПРИМЕЧАНИЕ ПАРАМЕТРЫ BLUEPRINT

Когда мы создавали чертеж, то указали, что имя группы ресурсов и местоположение должны будут выбираться при назначении чертежа. Поэтому вам нужно будет заполнить пробелы этими значениями.

Навык 5.3: описание конфиденциальности и соответствия нормативным требованиям

Когда вы переходите в облако, то перекладываете долю ответственности за свои сервисы и данные на облачного провайдера, в область которого также входит ответственность за соблюдение стандартов защиты данных. Облачный провайдер берет на себя часть этой работы, и вы должны ему доверять и верить, что он сможет обеспечить соответствие нормативным требованиям.

ПРИМЕЧАНИЕ МОДЕЛЬ РАЗДЕЛЕНИЯ ОТВЕТСТВЕННОСТИ

Вы же помните, что о модели разделения ответственности мы с вами говорили еще в навыке 1.2? Абзац выше представляет собой идеальный пример того, в чем суть модели разделения ответственности.

Существует множество стандартов, которые компании обязаны соблюдать. Например, в 2016 году Европейский союз принял **General Data Protection Regulation** (Общий регламент по защите данных), или GDPR. GDPR регулирует порядок обработки персональных данных физических лиц в ЕС, но и контролирует любые персональные данные, экспортируемые из ЕС. Компании, ведущие бизнес в странах ЕС, юридически обязаны соблюдать GDPR.

Одним из способов обеспечения того, что организации соблюдают GDPR и другие нормативные акты, регулирующие данные, является соблюдение отраслевых стандартов, направленных на оказание помощи организациям в обеспечении безопасности информации. Одним из таких стандартов является стандарт Международной организации стандартов (International Organization of Standards, ISO) 27001. Компании, которые соответствуют стандарту ISO 27001, могут быть уверены в том, что они придерживаются лучших практик, необходимых для обеспечения безопасности информации. Фактически многие компании не будут работать с облачным провайдером, если он не сможет доказать соответствие стандарту ISO 27001.

Системы, занимающиеся государственными данными, должны обеспечивать соответствие стандартам, которые поддерживаются Национальным институтом стандартов и технологий (National Institute of Standards and Technology, NIST). NIST SP 800-53 – это документ NIST, в котором изложены все требования к информационным системам, работающим с государственными данными. Для того чтобы государственное учреждение смогло использовать сервис, он должен сначала доказать соответствие NIST SP 800-53.

Microsoft выполняет эти требования соответствия в своей инфраструктуре различными способами.

Содержание раздела:

- заявление о конфиденциальности Microsoft (Microsoft privacy statement);
- Cloud Adoption Framework для Azure;
- центр управления безопасностью (Trust Center);
- портал доверия служб (Service Trust Portal);
- суверенные регионы Azure (Azure sovereign regions).

Заявление о конфиденциальности Microsoft

Заявление о конфиденциальности Microsoft (Microsoft Privacy Statement) – это всеобъемлющее заявление Microsoft, в котором описываются вопросы, касающиеся обработки информации и персональных данных:

- персональные данные, собираемые Microsoft;
- как Microsoft использует персональные данные;
- причины, по которым Microsoft предоставляет персональные данные;
- как получить доступ и управлять вашими персональными данными, собираемыми Microsoft;

- как Microsoft использует куки-файлы и аналогичные технологии;
- что организации, предоставляющие вам программное обеспечение Microsoft, могут делать с вашими данными;
- какие данные предоставляются сторонним компаниям при использовании учетной записи Microsoft;
- сведения о том, как Microsoft защищает данные, где они обрабатываются, и о политиках хранения.

Microsoft добавляет ссылки на заявление о конфиденциальности во всех официальных коммуникациях, и вы можете получить доступ к заявлению о конфиденциальности по ссылке <https://aka.ms/privacystatement>.

Cloud Adoption Framework для Azure

Как вы уже успели понять, за переходом в облако лежат более сложные действия, чем простое нажатие кнопок на портале Azure. Необходимо все тщательно спланировать, при этом вам нужно заблаговременно иметь представление успешного перехода в облако. Вам нужно знать о передовом опыте, об архитектуре облачных приложений, правильном способе миграции ресурсов, настройке и политиках и т. д.

Как вы могли догадаться, Microsoft располагает такими знаниями, распространенными среди команд Azure. Microsoft не только заимствует опыт от работы со своими клиентами, но и сама является крупным потребителем Azure. Она обладает достаточным уровнем компетенций в планировании, организации, разворачивании и управлении ресурсами Azure.

Желая поделиться с миром своими обширными знаниями, Microsoft создала **Cloud Adoption Framework для Azure** (Платформа внедрения облачных технологий). Эта платформа объединяет в себе лучшие передовые практики сотрудников и партнеров Microsoft, знания, полученные из опыта работы с клиентами. Всю эту информацию вы сможете найти на довольно информативном веб-сайте. Сведения из платформы четко организованы, вы даже можете загружать такие ресурсы, как инфографика, которая способствует визуализации Cloud Adoption Framework для Azure.

Вы можете получить доступ к Cloud Adoption Framework для Azure, перейдя по ссылке <https://aka.ms/cloudadoptionframework>.

Центр управления безопасностью

Центр управления безопасностью (Trust Center) – это веб-портал, на котором можно узнать все о подходе Microsoft к обеспечению безопасности, конфиденциальности и соответствию нормативным требованиям. Вы можете получить доступ к Центру управления безопасностью, перейдя по адресу <https://aka.ms/microsofttrustcenter>.

Центр управления безопасностью предоставляет информацию по решениям в области безопасности, о продуктах безопасности, об используемых Microsoft способах по вопросам конфиденциальности, управления данными и т. д. Центр также предоставляет техническую документацию и контрольные

выписки в качестве инструментов для обеспечения безопасности и соответствия нормативным требованиям.

С учетом развития облачной среды и эволюции угроз Microsoft обновляет Центр управления безопасностью актуальной информацией, поэтому следите за изменениями.

Service Trust Portal

Портал доверия служб (Service Trust Portal, STP) – это портал, предоставляющий доступ к различным средствам обеспечения соответствия, которые Microsoft предоставляет для отслеживания соответствия приложений, работающих на различных платформах Microsoft. Доступ к STP можно получить по адресу <https://aka.ms/STP>. На рис. 5.35 вы видите домашнюю страницу STP.

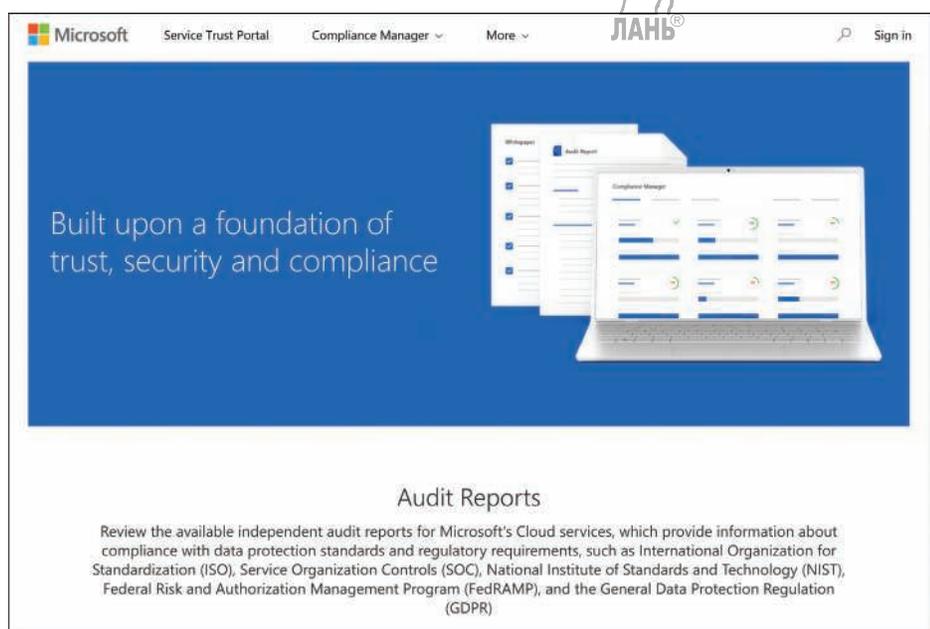


Рис. 5.35 Service Trust Portal

STP является отправной точкой для **Compliance Manager** (Менеджера по соответствию требованиям), инструмента для управления соответствием нормативных требований в облаке. Compliance Manager позволяет легко визуализировать ваше соответствие отраслевым стандартам. Этот менеджер также предоставляет подробную информацию о том, как вы можете улучшить соответствие стандартам, а в тех областях, где ответственность за обеспечение соответствия лежит на Microsoft, менеджер дает подробные сведения о способах, предпринимаемых Microsoft, для обеспечения соответствия стандартам.

Для доступа к менеджеру по соответствию требованиям нажмите **Compliance Manager** (Менеджер по соответствию) в верхней части страницы STP. Compliance Manager позволяет отслеживать соответствие требованиям у приложений, объединяя их в группы, которым вы можете дать любое имя группы. Каждая созданная группа представлена плиткой в **Manager** (Менеджере), и вы можете увидеть, как далеко вы продвинулись в достижении соответствия в каждой группе (см. рис. 5.36).

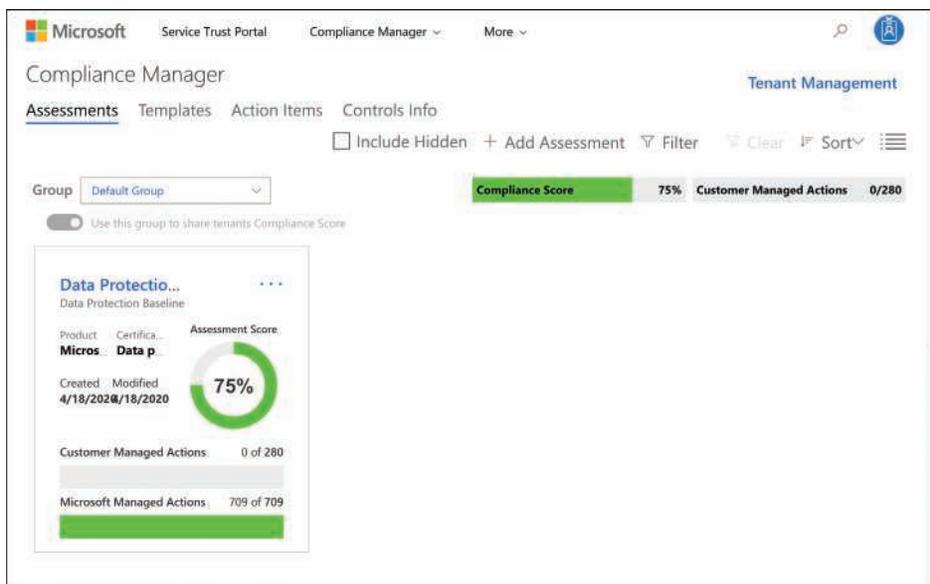


Рис. 5.36 Compliance Manager (Менеджер по соответствию требованиям)

С выбором **Data Protection Baseline** (Требования для защиты данных) вы попадаете на экран с подробной информацией по вашей оценке. Как показано на рис. 5.37, существует множество действий, которые Microsoft рекомендует применять для защиты данных.

Нажав **Review** (Просмотреть) на любое действие, вас перекидывает на панель, где отображен статус действия. Потом вы сможете записать статус реализации, назначить действие определенному пользователю и т. д. Вы также можете ввести дату плана внедрения для отслеживания результатов и дату тестирования внедрения, как показано на рис. 5.38.

Assessed Actions	0/280	Compliance Score	75%
Action Title	Compliance Score	Owner	Implementation Date & Status
Activate Azure Rights Management Your organization should use Azure Rights Management ... Read More	27	Customer	Review
Add an Android App Protection Policy Your organization should create and assign an Android ap... Read More	27	Customer	Review
Alert Personnel of Information Spillage Your organization should alert organization personnel of L... Read More	1	Customer	Review
Allow Mailbox Delegation Only When Authorized Your organization should ensure that mailbox delegation L... Read More	27	Customer	Review
Anonymize Usage Activity Reports Your organization should anonymize personal data where ... Read More	27	Customer	Review

Рис. 5.37 Список действий по соблюдению требований по защите данных

Activate Azure Rights Management

ⓘ Please note that selecting 'Not in scope' excludes this customer action from the assessment score calculation

Assign User

Manage Documents

Implementation Status **Implementation Date**

Test Result **Test Date**

Implementation Notes | Test Plan | Additional Information

Enter implementation details for your organization, along with any notes you want to include. Information that you enter in this field can help others in your organization, as well as auditors and regulators, to understand your organization's implementation details and how your implementation can be tested and validated.

Рис. 5.38 Описание действия

Суверенные регионы Azure

Некоторые требования соответствия не могут быть выполнены простым применением политик в Azure. Иные сценарии соответствия требованиям правительства США требуют, чтобы данные оставались на территории США и чтобы только граждане Соединенных Штатов имели доступ к системам, используемым для хранения этих данных. Соблюдение этих требований невозможно ни в публичном облаке, ни при помощи политик. Поэтому Microsoft разработала полностью изолированные центры обработки данных Azure, которые составляют облако Azure для государственных организаций.

Центры обработки данных Azure для государственных организаций отделены от общедоступных центров обработки данных. Все сотрудники, работающие в Azure на государственные структуры, проходят проверку и являются гражданами США. Даже сотрудники Microsoft, оказывающие техническую поддержку клиентам Azure для государственных организаций, должны быть гражданами США.

Поскольку Microsoft хотела разрешить совместимое взаимодействие между облаком Azure для государственных организаций и локальными государственными системами, то также разработала выделенные местоположения Microsoft ExpressRoute, которые полностью изолированы от других сетей Azure и используют собственные выделенные оптоволоконные каналы.

Суверенные регионы Azure предназначены не только для федеральных правительственных учреждений. Города и муниципалитеты также используют преимущества Azure для государственных организаций для обеспечения соответствия нормативным требованиям. Когда клиент подписывается в Azure для государственных организаций, Microsoft проверяет этого пользователя, чтобы убедиться, что он является представителем государственного учреждения. Только тогда им предоставляется подписка на Azure для государственных организаций (Azure Government).

Облако Azure для государственных организаций имеет те же функции и службы, что и общедоступное облако, но есть небольшие различия. Например, портал Azure для государственных организаций находится по адресу <https://portal.azure.us>, а не <https://portal.azure.com>. URL-адреса служб Azure также используют домен `.us` верхнего уровня, поэтому если вы создаете веб-приложение службы приложений в Azure для государственных организаций, доменным именем по умолчанию будет <https://webapp.azurewebsites.us>. Тем не менее за пределами этой разницы все остальное остается прежним, поэтому разработчики, обладающие навыками облачной разработки в Azure, обнаружат, что их навыки применимы и к Azure для государственных организаций.

Министерство обороны (Department of Defense, DoD) США имеет дополнительные требования к соблюдению, называемые Временная авторизация DoD для 5-го уровня воздействий (DoD Impact Level 5 Provisional Authorization). Соблюдение этого требования относится к контролируемой несекретной информации, которая требует дополнительных уровней защиты. Эти дополнительные требования DoD удовлетворяются подмножеством центров обработки данных в Azure для государственных организаций, одобренных для использования Министерством обороны.

Специалисты Microsoft осознают, что строгие требования в ЕС требуют уникального подхода, поэтому и было разработано еще одно облако под назва-

нием Azure Germany. Как и Azure для государственных организаций, Azure для Германии (Azure Germany) – это отдельная облачная система, разработанная для удовлетворения конкретных требований национального регулятора. В случае Azure для Германии эти потребности связаны со строгими требованиями, установленными в ЕС. Azure для Германии доступен для клиентов, которые занимаются бизнесом в ЕС, Европейской ассоциации свободной торговли и Великобритании.

Центры обработки данных Azure для Германии физически расположены в Германии и управляются строгими мерами безопасности местной компанией T-Systems International (дочерняя компания Deutsche Telekom), которая работает в качестве доверенного лица данных. Доверитель данных имеет полный контроль над всеми данными, хранящимися в Azure для Германии, и всей инфраструктурой, используемой для размещения этих данных. Microsoft занимается управлением только теми системами, которые вообще не имеют доступа к данным клиентов.

Еще одним регионом, в котором Azure предъявляет особые требования, является Китай. Microsoft управляет еще одним отдельным облаком в Китае под названием Microsoft Azure China. Azure для Китая управляет компания Blue Cloud Technology (зачастую сокращенно именуемая BlueCloud). BlueCloud принадлежит компании Beijing 21Vianet Broadband Data Center (сокращенно 21Vianet), поставщику интернет-услуг и центров обработки данных в Китае. Ввиду таких взаимоотношений между компаниями Azure для Китая упоминается как «Microsoft Azure, управляемый 21Vianet» или просто «Azure 21Vianet».

Azure для Китая не предлагает вам полный набор функций, которые есть в других облаках Azure, но Microsoft сосредоточила все свои усилия для добавления дополнительных функций и служб. За детальной информацией по содержанию возможностей Azure для Китая перейдите по адресу <https://bit.ly/az900-azurechina>.

Мысленный эксперимент

Давайте применим концепции, связанные с идентификацией, безопасностью, конфиденциальностью и соответствием требованиям, которые вы узнали в этой главе, в мысленном эксперименте.

Ответы на этот мысленный эксперимент вы можете найти в следующем разделе.

Ваши старые знакомые связались с вами снова с просьбой помочь им в работе по облачным вычислениям. На этот раз у них есть парочка новых задач. Для начала у них создается новый портал для клиентов, который компания хочет интегрировать со своими учетными записями в социальных сетях. Им нужен внешний исполнитель, который будет помогать с аккаунтами в социальных сетях, публикуя сообщения подписчикам и отвечая на вопросы клиентов. ИТ-директора беспокоит момент передачи имен пользователей и паролей своих учетных записей в социальных сетях сторонним компаниям. Он хотел бы предотвратить исполнителю доступ к учетным записям социальных сетей без пароля, но ему нужна уверенность, что после окончания договора о подряде без особого труда можно будет удалить из учетных записей сторонних специалистов.

Также у них есть ресурсы Azure, к которым исполнителю потребуется доступ, однако ИТ-директора волнует безопасность. В целях безопасности ему нужны гарантии, что никто не сможет получить доступ к системам ContosoPharm, если кто-то узнает имя пользователя и пароль подрядчика. Ему также нужно убедиться, что один конкретный ресурс будет доступен, только если подрядчик войдет в систему с компьютера, работающего на Windows. Доступ с мобильных устройств он не предусматривает.

Также нужны гарантии, что подрядчик сможет просматривать несколько ресурсов Azure на портале на случай, если что-то пойдет не по плану, но директор не хотел бы, чтобы подрядчик мог изменять какие-либо настройки.

В ходе работы разработчиков над этим решением будут создаваться ВМ в Azure. Эти ВМ должны располагаться в Центральном регионе США, для того чтобы они находились в той же зоне, что и сервис кеширования. ИТ-директор отправил памятку своим специалистам, в которой обращался к ним с просьбой о создании ВМ только в центральной части США, но он обеспокоен, что кто-то может об этом забыть, а также что низкая производительность сервиса кеширования повлияет на показатели тестирования. Кроме этого, если кто-либо удалит компонент кеширования, это может полностью нарушить работу приложения, поэтому нужны гарантии, что никто не сможет его удалить.

За некоторые ВМ, созданные для приложения, счет приходит ИТ-отделу, ответственному за разработку, но за большинство других ВМ счет приходит отделу продаж. Директор по информационным технологиям хотел бы, чтобы осуществлялась разбивка расходов по отделам после получения счета от Azure.

У ContosoPharm есть еще одна огромная проблема, в решении которой им нужна помощь. В ближайшее время планируется еще одно разворачивание в облаке, это будет сложное приложение. Было много времени потрачено на планирование реализации. Они точно знают, как должна быть настроена сеть, имеется запись обо всех ресурсах, которые нужно будет создать, а также ARM-шаблон, который должен будет выполнить всю работу по публикации. Конфигурация сети, которая была разработана для виртуальных сетей Azure, соответствует потребностям и позволяет им интегрироваться с локальными системами. Здесь мы видим довольно сложную настройку. Им нужна возможность легкого воссоздания данной настройки в Azure, когда им потребуется развернуть другие приложения, которые будут использовать ту же топологию сети.

Ответы на мысленный эксперимент

В этом разделе рассматриваются ответы на мысленный эксперимент.

Для предоставления подрядчику доступа к учетным записям социальных сетей без имени пользователя и пароля компания может предоставить подрядчику гостевой доступ в своей Azure Active Directory. После этого они смогут добавлять корпоративные приложения для желаемых платформ социальных сетей и предоставлять пользователям доступ с помощью Azure AD business-to-business или B2B. Когда договор с подрядчиком потеряет свою силу, они могут просто удалить подрядчика из Azure AD, и доступ к учетным записям в социальных сетях у подрядчика пропадет.

Чтобы обеспечить невозможность получения доступа к системам извне, если имя пользователя и пароль подрядчика будут скомпрометированы, они могут использовать многофакторную аутентификацию. Поскольку подрядчик является гостевым пользователем в Azure AD, ему потребуется использовать политику условного доступа, что также решит проблему с запретом доступа к ресурсу, если подрядчик не использует Windows, посредством определения условия, основанного на ОС устройства, с которого осуществляется вход.

Для того чтобы у подрядчика была возможность просмотра некоторых ресурсов Azure без доступа к внесению изменений в настройки, можно использовать роли – роль читателя для ресурсов. Это позволит подрядчику видеть ресурсы, но не удалять или изменять настройки.

Чтобы разработчики создавали VM только в центральном регионе США, они могут использовать политики Azure. Для того чтобы была уверенность, что никто не сможет удалить компонент кеширования, они могут установить блокировку «только чтение» или запретить «удаление».

Чтобы директор по информационным технологиям мог видеть разбивку использования VM для ИТ-отдела и для отдела продаж, они могут использовать теги на VM. Теги отображаются в счете от Azure. Поскольку счет можно экспортировать в формат, который можно будет открыть в Microsoft Excel, это позволит легко проводить по ним сортировку и фильтрацию.

Для того чтобы перевести тяжелую работу по планированию и обеспечить простоту воспроизведения сложной конфигурации сети в последующих развертываниях, можно будет использовать Azure Blueprints. Создав чертеж, который добавляет артефакты для необходимых политик, групп ресурсов, ARM-шаблонов и т. д., они могут без труда убедиться в корректности настроек.

Краткое содержание главы

В этой главе мы рассмотрели много тем, связанных с идентификацией и управлением. Мы завершили с подробной информацией по конфиденциальности и соблюдению требований, а также инструментами, которые Microsoft предоставляет в этих областях.

Ниже представлен краткий обзор того, что было рассмотрено в данной главе.

- Аутентификация – это процесс определения того, кто получает доступ к ресурсу.
- Авторизация – это действие по обеспечению того, что может и чего не может делать аутентифицированный пользователь.
- Azure Active Directory – это облачная служба идентификации в Azure.
- В основе Azure AD лежит каталог пользователей.
- Можно пригласить и других пользователей в ваш домен Azure AD.
- Приглашенные пользователи, как правило, находятся за пределами организации и приглашаются в Azure AD отдельно.
- Корпоративные приложения позволяют интегрировать Azure AD с другими службами и облачными платформами.

-
- Политики условного доступа применяются к пользователям, использующим средства управления доступом.
 - Многофакторная аутентификация – это двухфакторная аутентификация, которая требует ввода кода из SMS-сообщения наряду с именем пользователя и паролем.
 - Управление доступом на основе ролей (Role-based access control, RBAC) позволяет управлять тем, как пользователи и приложения могут взаимодействовать с ресурсами Azure.
 - Политика Azure позволяет определять правила, которые применяются при создании и управлении ресурсами Azure.
 - Блокировки ресурсов позволяют предотвращать изменение и удаление ресурсов.
 - Теги позволяют упорядочивать ресурсы, назначая имя и значение, которые можно увидеть на портале Azure и счете от Azure.
 - Azure Blueprints позволяют сохранять конфигурации и ресурсы в чертежах, которые можно будет после легко развернуть.
 - Элементы, добавленные в чертежи, называются артефактами. Артефакт может представлять собой группу ресурсов, ARM-шаблон, назначение политики или роли.
 - Заявление о конфиденциальности Microsoft – всеобъемлющее заявление Microsoft, в котором описывается, как корпорация использует, обрабатывает и защищает данные и персональную информацию.
 - Cloud Adoption Framework для Azure объединяет передовой опыт и информацию от сотрудников Microsoft, их партнеров и клиентов Microsoft, чтобы упростить внедрение облачных технологий.
 - Центр доверия описывает подход Microsoft к безопасности, конфиденциальности и соблюдению нормативных требований.
 - Портал доверия служб предоставляет доступ к различным инструментам обеспечения соответствия требованиям, имеющимся у Microsoft.
 - Портал доверия служб является отправной точкой для **Compliance Manager** (Менеджер по соответствию требованиям), инструментом по соблюдению нормативных требований в облаке.
 - Azure для государственных учреждений – частное облако для государственных учреждений, доступное только для граждан США. Он обладает собственными центрами обработки данных, которые полностью отделены от общедоступного облака.
 - Подсистема государственных центров обработки данных Azure одобрена Министерством обороны, поскольку содержит дополнительные соответствия нормативным требованиям, связанным с DoD Impact Level 5 Provisional Authorization.
 - Azure для Германии предоставляет частное облако, разработанное в соответствии с правилами ЕС.
 - Azure для Китая – это отдельное облако в Китае, которое в настоящее время не предлагает все службы, доступные в Azure.



Описание ценообразования, соглашений о качестве предоставляемых услуг и жизненный цикл служб Azure

Несмотря на то что мы уже изучили множество различных тем в этой книге, нам еще предстоит рассмотреть основные проблемы при переходе в облако: ценообразование, соглашения об уровне обслуживания и жизненный цикл служб Azure.

Ценообразование предполагает не только знание стоимости ресурсов Azure. Компании часто хотят знать, сколько будут стоить облачные ресурсы до размещения приложений в облаке, а после развертывания приложения им необходимо максимально сократить затраты и получить прозрачность расходов на ресурсы Azure.

Мы уже рассматривали высокую доступность в облаке, и Microsoft вам в этом может помочь своими рекомендациями, представленными в соглашениях о качестве предоставляемых услуг (Service Level Agreement, SLA). Когда что-то идет не так и это влияет на ваши службы, крайне важно получить поддержку, необходимую для обеспечения доступности приложений.

Очень важно, чтобы вы понимали жизненные циклы служб, особенно потому, что некоторые сервисы не предполагают наличия SLA или поддержки от Microsoft.

Навыки, описанные в этой главе:

- описание методов планирования и управления затратами;
- описание соглашений о качестве предоставляемых услуг и жизненных циклов служб.

Навык 6.1: описание методов планирования и управления затратами

Когда вы начинаете думать о переходе в облако, первое, что вы, скорее всего, захотите сделать, – это определить, как ваши расходы будут зависеть от ваших потребностей в ресурсах. Как только вы начнете создавать и использовать ресурсы Azure, управление затратами становится важным для того, чтобы оставаться в пределах бюджетов. В Azure есть инструменты, которые помогут вам с планированием и управлением затратами.

Содержание раздела:

- факторы, влияющие на затраты;
- калькулятор цен;
- калькулятор совокупной стоимости владения (total cost ownership, TCO);
- управление затратами Azure.

Факторы, влияющие на затраты

При планировании развертывания Azure следует учитывать факторы, которые могут повлиять на стоимость. Основными факторами, влияющими на затраты, являются тип ресурса, способ приобретения ресурса, регионы Azure, которые вы используете, и зона выставления счетов, в которой находятся ресурсы.

Плата за службы Azure взимается в соответствии со *счетчиками* (meters), связанными с ресурсами. Эти счетчики отслеживают, сколько конкретной метрики было использовано ресурсом. Например, плата за виртуальную сеть Azure не взимается, как и за трафик внутри этой сети, но оплачиваются гигабайты входящего и исходящего трафика, даже при соединении нескольких одноранговых виртуальных сетей.



СОВЕТ К ЭКЗАМЕНУ

Каждая служба Azure имеет страницу цен, в которой приводится оценка стоимости этого ресурса на основе типичного использования.

При определении ресурсов, которые необходимо использовать в Azure, подумайте о том, как эти ресурсы будут использовать метрики, за которые взимается плата. Например, если можно спланировать виртуальные сети таким образом, чтобы количество одноранговых сетей было меньше, можно существенно сэкономить в долгосрочной перспективе.

Вы также можете обнаружить, что приобретение ресурсов Azure по-разному может обеспечить экономию средств. Если вы согласны внести предоплату по Корпоративному соглашению (Enterprise Agreement), Microsoft предложит вам сниженную ставку. Долгосрочные соглашения предлагают еще больше скидок. Партнеры по облачным решениям также могут предоставить вам комплекс-

ные решения, которые являются более экономичными, чем покупка всех ресурсов самостоятельно.

Расходы Microsoft на эксплуатацию служб Azure различаются в зависимости от региона, даже если эти регионы находятся в пределах одной географической границы. Таким образом, цены будут отличаться в зависимости от того, какой регион Azure вы используете. Например, ВМ, развернутая в регионе Центральной Америки, будет стоить дороже, чем та же ВМ, развернутая в восточном регионе США. Microsoft не предоставляет разбивку по их затратам, но можно предположить, что электричество и другие ресурсы, необходимые для центра обработки данных Azure, стоят дороже в регионе Центральной Америки, чем в восточном регионе США.



СОВЕТ К ЭКЗАМЕНУ

Выбор наименее дорогостоящего региона для каждого из ресурсов Azure обычно не является хорошим способом контроля затрат. В конечном итоге вам придется платить за сетевой трафик в разных регионах, и это может привести к увеличению ваших затрат выше суммы, которую вы экономите. Многие ресурсы Azure не взимают плату за сетевой трафик в пределах одного региона, но они взимают плату за трафик между регионами.

Также важно иметь в виду, что плата за сетевой трафик в центре обработки данных Azure не взимается, но взимается за его пределами. Тем не менее ваши первые 5 ГБ исходящих данных бесплатны. После этого объема с вас взимается заданная сумма за многоуровневую модель.

ДОПОЛНИТЕЛЬНО ЦЕНЫ НА ПРОПУСКНУЮ СПОСОБНОСТЬ

Дополнительные сведения о ценах на пропускную способность сети в Azure вы найдете по адресу: <https://bit.ly/az900-bandwidthpricing>.

География Azure разбита на четыре отдельные группы для выставления счетов. Эти группы называются *зонами выставления счетов*, или чаще всего просто *зонами*. Затраты Microsoft на сетевой трафик вне каждой зоны различаются, поэтому ваши затраты также будут отличаться.

В табл. 6.1 перечислены зоны в Azure и соответствующие регионы.

Таблица 6.1 Зоны и география

Имя зоны	Входящие РЕГИОНЫ
Зона 1	Центральная Австралия, Центральная Австралия 2, Центральная Канада, Восточная Канада, Северная Европа, Центральная Франция, Южная Франция, Северная Германия (общедоступная), Западно-центральная Германия (общедоступная), Восточная Норвегия, Западная Норвегия, Северная Швейцария, Западная Швейцария, Южная Великобритания, Западная Великобритания и все регионы США
Зона 2	Восточная Азия, Юго-Восточная Азия, Восточная Австралия, Юго-восточная Австралия, Центральная Индия, Южная Индия, Западная Индия, Восточная Япония, Западная Япония, Центральная Корея и Южная Корея
Зона 3	Южная Бразилия, Северо-южная часть Африки, Юго-западная часть Африки, Центральная часть Объединенных Арабских Эмиратов, Северная часть Объединенных Арабских Эмиратов
DE Зона 1	Центральная Германия (суверенная) и Северо-Восточная Германия (суверенная)

Минимальные затраты на исходящий трафик расположены в Зоне 1. На втором месте по минимальной стоимости – DE 1, за которой следуют Зона 2 и Зона 3.

Как вы можете видеть, существует множество факторов, которые влияют на расходы в Azure, и оценить затраты на основе всех этих факторов может быть непросто. К счастью, Microsoft предлагает калькулятор цен, который поможет вам оценить свои расходы при переходе на облачные сервисы.

Калькулятор цен

Azure Pricing Calculator (Калькулятор цен Azure) поможет вам получить оценку расходов на основе продуктов, которые вы собираетесь использовать, а также регионов развертывания этих продуктов и т. д. Вы можете получить доступ к калькулятору цен, перейдя по адресу <https://bit.ly/az900-pricingcalculator>.

Первым шагом при оценке расходов Azure является выбор продуктов, которые вы хотите использовать. Как показано на рис. 6.1, некоторые из наиболее распространенных продуктов Azure отображаются по умолчанию, и вы можете добавить любой из них, нажав на его плитку.

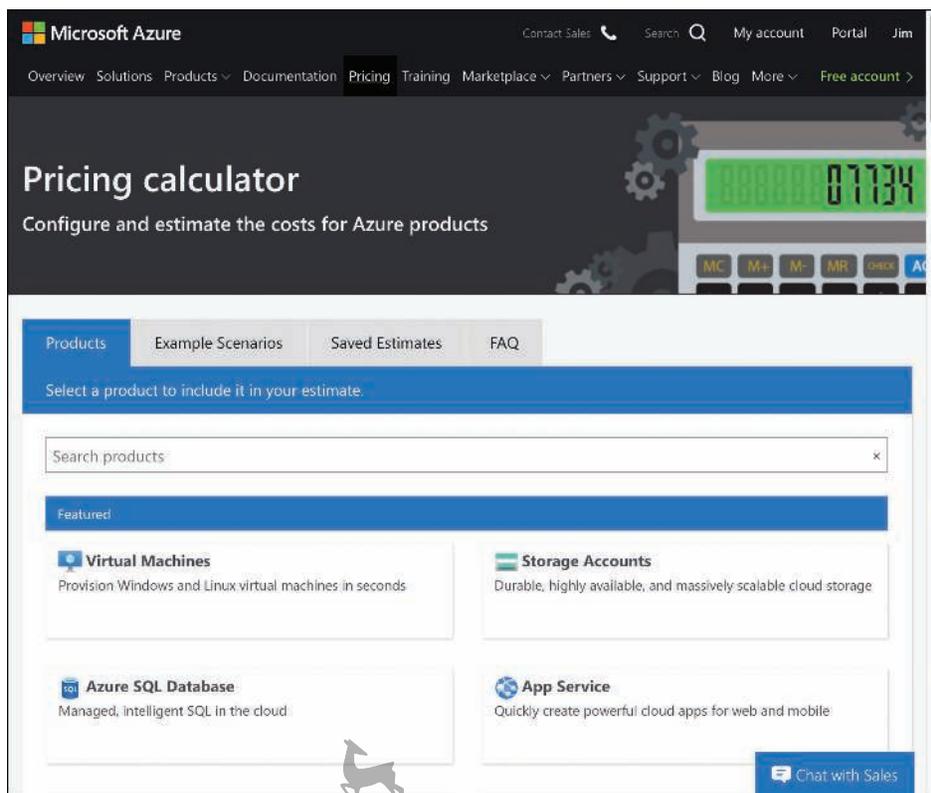


Рис. 6.1 Калькулятор цен



Если нужный товар отсутствует в списке, вы можете либо щелкнуть по категории товаров в списке слева, либо найти продукт, введя его название в поле поиска.

После добавления продуктов, которые вы хотите использовать, прокрутите вниз, чтобы настроить параметры каждой службы. Эти сведения различаются в зависимости от того, как Microsoft взимает плату за продукт. На рис. 6.2 показаны параметры для базы данных Azure SQL.

При нажатии на кнопку **Pricing Details** (Сведения о ценах), справа от названия продукта, откроется страница ценообразования для продукта в новой вкладке. Вы также можете нажать на **Product Details** (Сведения о продукте) или **Documentation** (Документация), чтобы узнать больше о сервисе и принять более подходящие решения о выбранных опциях.

После настройки продукта в соответствии с вашими потребностями можно нажать кнопку в верхней правой части окна + (**Clone** (Клонировать)), чтобы добавить другой экземпляр этого продукта в оценку. Например, предположим, что вам нужны две базы данных Azure SQL для вашего приложения, и каждая из них будет использовать один и тот же уровень обслуживания, размер экземпляра и т. д. Самый простой способ добавить их – добавить один продукт базы данных Azure SQL в оценку, настроить его с нужными параметрами цены, а затем нажать кнопку **Clone** (Клонировать), чтобы добавить второй экземпляр.

▼ Azure SQL Database ⓘ Single Database, vCore Purchase Mo... 🗑️ 📄

Azure SQL Database

REGION: ▾

TYPE: ▾

BACKUP STORAGE TIER: ▾

PURCHASE MODEL: ▾

SERVICE TIER: ▾

COMPUTE TIER: ▾

GENERATION: ▾

INSTANCE: ▾

Savings Options

Save up to 73% on pay as you go prices with 1 year or 3 year reserved options.

Compute	SQL License
<input checked="" type="radio"/> Pay as you go	<input checked="" type="radio"/> Pay as you go
<input type="radio"/> 1 year reserved	<input type="radio"/> Azure Hybrid Benefit
<input type="radio"/> 3 year reserved	
\$888.95	\$583.80
Average per month	Average per month
(\$0.00 charged upfront)	(\$0.00 charged upfront)

\$1,472.75
Average per month
(\$0.00 charged upfront)

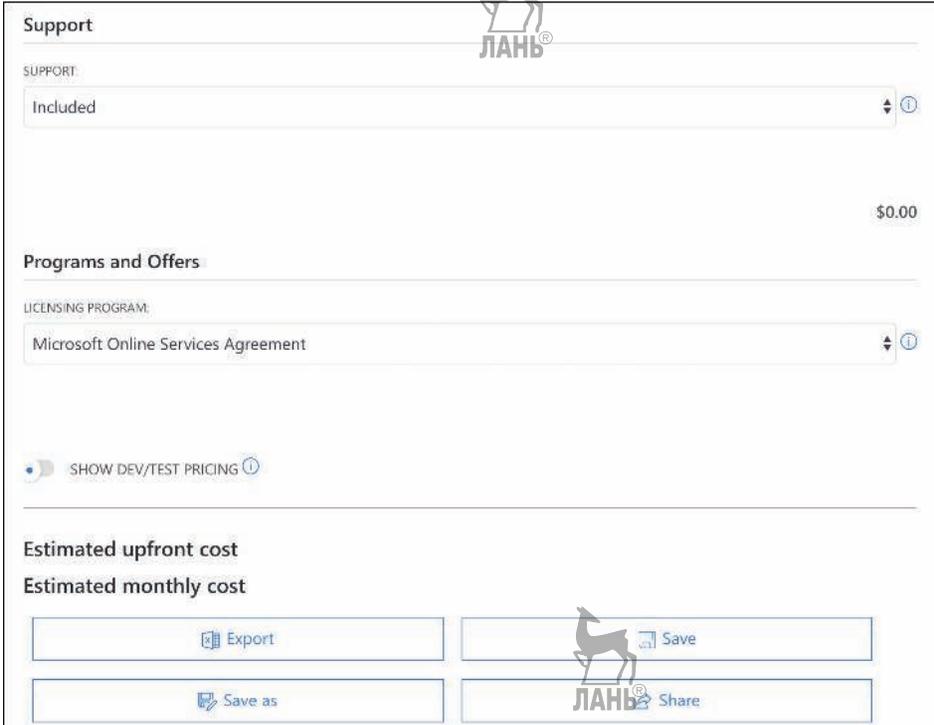
[Chat with Sales](#)

Рис. 6.2 Параметры ценообразования для базы данных Azure SQL

Чтобы просмотреть оценку стоимости, прокрутите страницу вниз. Как показано на рис. 6.3, вы можете выбрать план поддержки для добавления в свою оценку. Если у вас есть **Microsoft Online Services Agreement** (Соглашение об онлайн-службах Microsoft), **Enterprise Agreement** (Корпоративное) или **Microsoft Customer Agreement** (Клиентское соглашение с Microsoft), вы можете выбрать их для того, чтобы эта цена применялась к оценочной стоимости. Затем нажмите кнопку **Export** (Экспорт), чтобы сохранить оценку в виде файла Excel, потом нажмите кнопку **Save** (Сохранить), чтобы сохранить оценку в калькуляторе цен и внести изменения позже, или выберите **Share** (Поделиться), чтобы создать ссылку для совместного использования, дабы другие могли просмотреть ее.

ПРИМЕЧАНИЕ СОХРАНЕННЫЕ ОЦЕНКИ

Если вы сохраните оценку в калькуляторе цен, вы можете получить доступ к ней позже, нажав вкладку **Saved Estimates** (Сохраненные оценки) в верхней части страницы.



The screenshot shows a web interface for a pricing calculator. At the top right, there is a logo for 'ЛАНЬ' (Lan) featuring a deer. The main content area is titled 'Support' and contains a dropdown menu labeled 'SUPPORT:' with 'Included' selected. Below this, the price is shown as '\$0.00'. A section titled 'Programs and Offers' contains a dropdown menu labeled 'LICENSING PROGRAM:' with 'Microsoft Online Services Agreement' selected. There is also a toggle switch for 'SHOW DEV/TEST PRICING'. At the bottom, there are two rows of buttons: the first row has 'Export' and 'Save', and the second row has 'Save as' and 'Share'. The 'ЛАНЬ' logo is also present on the 'Share' button.

Рис. 6.3 Завершение оценки в калькуляторе цен

Калькулятор совокупной стоимости владения

Калькулятор совокупной стоимости владения (total cost of ownership, TCO) полезен для оценки затрат на новые приложения в Azure, но если у вас есть ло-

кальные приложения, которые вы хотите перенести в Azure, и вы хотите оценить, сколько можете сэкономить в Azure, калькулятор совокупной стоимости владения является лучшим выбором. Вы можете получить доступ к калькулятору совокупной стоимости владения, перейдя по ссылке <https://bit.ly/az900-tco-calculator>.

Первым шагом при использовании калькулятора совокупной стоимости владения является добавление сведений о локальных серверах, базах данных, хранилище и использовании сети. На рис. 6.4 локальный сервер настроен для веб-приложения. Вы можете настроить все сведения о сервере, включая ОС, будь то VM или физический сервер, и многое другое.

Define your workloads

Enter the details of your on-premises workloads. This information will be used to understand your current TCO and recommended services in Azure.

Servers

Enter the details of your on-premises server infrastructure. After adding a workload, select the workload type and enter the remaining details.

Web Server

Workload	Environment	Operating system	Servers	Procs per server	Core(s) per proc
Web App	Physical Servers	Windows	1	2	4

RAM (GB) Optimize by CPU Auto scaling

+ Add server workload

Рис. 6.4 Настройка локального сервера в калькуляторе TCO

Кроме того, необходимо добавить локальные базы данных и системы хранения данных, а также любое использование сети для вашего приложения. На рис. 6.5 добавлена система хранения данных и указано использование сети для приложения.

После ввода всех локальных ресурсов можно просмотреть предположения (assumptions), используемые калькулятором TCO, нажав кнопку **Next** (Далее). Калькулятор совокупной стоимости владения использует полный список допущений о расходах на инфраструктуру предприятия, которые Microsoft собрала на основе многолетнего опыта, и эти предположения используются для предоставления вам наилучшей возможной оценки экономии средств. Как показано на рис. 6.6, допущения включают в себя такие элементы, как приобретение плана страховки программного обеспечения (Software Assurance) для локальных серверов, сведения о текущих расходах на локальную инфраструктуру, затраты на рабочую силу ИТ и многое другое. Для точной оценки совокупной стоимости владения лучше тщательно регистрировать ваши расходы перед формированием отчета.

Storage

Enter the details of your on-premises storage infrastructure. After adding storage, select the storage type and enter the remaining details.

Image storage 🗑️

Storage type	Capacity	Backup	Archive
NAS/file share	3 TB (1 - 5000)	3 TB (0 - 5000)	6 TB (0 - 5000)

[+ Add storage](#)

Networking

Enter the amount of network bandwidth you currently consume in your on-premises environment.

Outbound bandwidth

GB
(1 - 2000)

[Next](#)

Рис. 6.5 Настройка хранилища и сети

Storage costs

Storage procurement cost/GB for local disk/SAN-SSD	<input type="text" value="3"/> (USD)
Storage procurement cost/GB for local disk/SAN-HDD	<input type="text" value="2"/> (USD)
Storage procurement cost/GB for NAS/file storage	<input type="text" value="2"/> (USD)
Storage procurement cost/GB for Blob storage	<input type="text" value="2"/> (USD)
Annual enterprise storage software support cost	<input type="text" value="10"/> (%)
Cost per tape drive	<input type="text" value="4500"/> (USD)

IT labor costs

Number of physical servers that can be managed by a full time administrator	<input type="text" value="387"/>
Number of virtual machines that can be managed by a full time administrator	<input type="text" value="516"/>
Hourly rate for IT administrator	<input type="text" value="50"/> (USD)

Other assumptions

The following assumptions also affect the TCO model, but typically require less adjustment by customers. You can come back to this section at any time and adjust the assumptions.

- Hardware costs
- Software costs

Рис. 6.6 Корректировка допущений, сделанных TCO-калькулятором

После корректировки предположений прокрутите вниз экрана и нажмите кнопку **Next** (Далее), чтобы просмотреть отчет о совокупной стоимости владения. Отчет о совокупной стоимости владения показывает, сколько можно сэкономить в течение следующих 5 лет, переместив приложение в Azure, как показано на рис. 6.7.

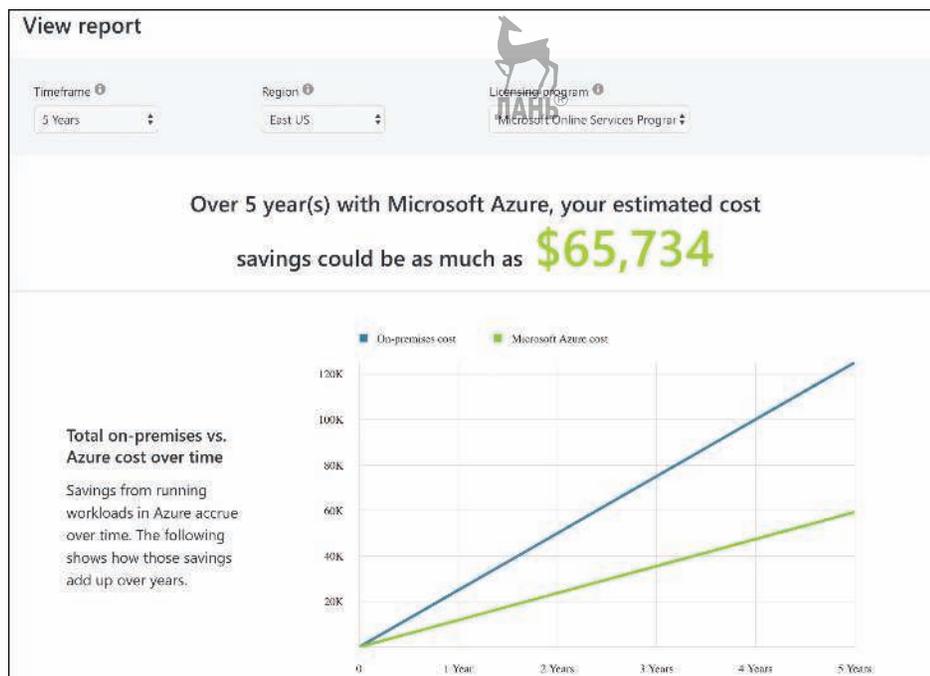


Рис. 6.7 Отчет об экономии совокупной стоимости владения

Отчет о совокупной стоимости владения содержит подробные диаграммы экономии расходов, а в нижней части отчета вы найдете разбивку локальных затрат и затрат Azure, чтобы вы могли легко определить, где сэкономите деньги. Как и в случае с калькулятором цен, отчеты, созданные калькулятором ТСО, можно скачать, сохранить или скопировать, нажав соответствующую кнопку, как показано на рис. 6.8.

Управление затратами Azure

Azure Cost Management (Управление затратами Azure) – это инструмент в Azure, который позволяет легко анализировать затраты на детальном уровне. Управление затратами позволяет создать бюджет для расходов Azure, настраивать оповещения, чтобы вы знали, приближаетесь ли вы к установленному в бюджете лимиту, и подробно проанализировали свои расходы.

Чтобы начать работу с этим инструментом, откройте портал Azure и найдите пункт **Cost Management** (Управление затратами), нажмите **Cost Management + Billing** (Управление затратами + выставление счетов).

On-premises cost breakdown summary		Azure cost breakdown summary	
Category	Cost	Category	Cost
Compute	\$87,396.15	Compute	\$17,556.60
Hardware	\$17,296.00	Data Center	\$0.00
Software	\$4,808.75	Networking	\$0.00
Electricity	\$2,102.40	Storage	\$41,748.90
Database	\$63,189.00	IT Labor	\$0.00
Data Center	\$10,187.10		
Networking	\$6,655.43		
Storage	\$18,216.00		
IT Labor	\$2,585.00		
Total	\$125,040.00	Total	\$59,306.00

Estimated on-premises cost (5 year(s))		Estimated Azure cost (5 year(s))	
<input checked="" type="checkbox"/> Compute cost <input checked="" type="checkbox"/> Data center cost		Azure compute cost	
		Azure data center cost	
Total on-premises cost over five year(s)	\$125,040.00	Total Azure cost over five year(s)	\$59,306.00

A total savings of **\$65,734.00** with Microsoft Azure

[Download](#)
[Share](#)
[Save](#)

Рис. 6.8 Сводные данные о локальных расходах и расходах на Azure



СОВЕТ К ЭКЗАМЕНУ

Вы также увидите раздел Cost Management в Azure Marketplace. Это другое предложение, основанное на Cloudfy, компании по управлению расходами в облаке, которую приобрела Microsoft. Функции из Cloudfy переносятся в службу управления затратами Azure, и к концу 2020 года Microsoft полностью откажется от Cloudfy.

После открытия блейда **Cost Management + Billing** (Управление затратами + выставление счетов) нажмите **Cost Management** (Управление затратами), как показано на рис. 6.9.

Для эффективного мониторинга затрат необходимо создать бюджет в разделе **Cost Management** (Управление затратами). Создание бюджета не требуется, но это позволит вам визуализировать ваши расходы для сравнения с запланированными.

1. Нажмите кнопку **Budgets** (Бюджеты), а затем нажмите кнопку **Add** (Добавить), как показано на рис. 6.10.
2. Введите имя бюджета.

3. Введите сумму расходов и период, в течение которого ваши расходы сбрасываются.
4. Введите дату начала бюджета.
5. Введите дату истечения срока действия (см. рис. 6.11).
6. Нажмите **Next** (Далее), чтобы завершить бюджет.

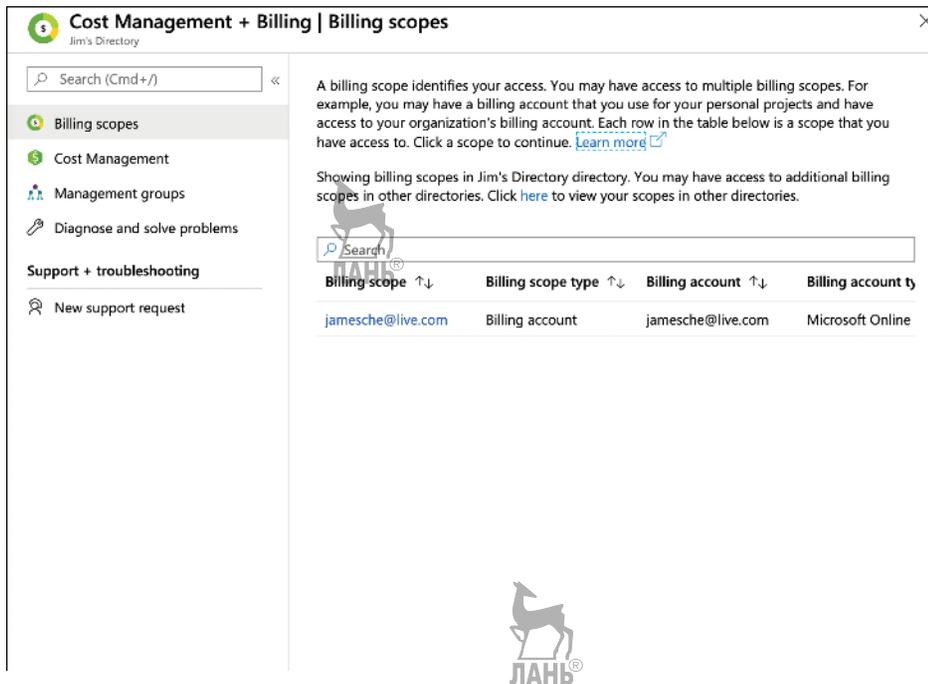


Рис. 6.9 Cost Management + Billing (Управление затратами + выставление счетов) на портале Azure

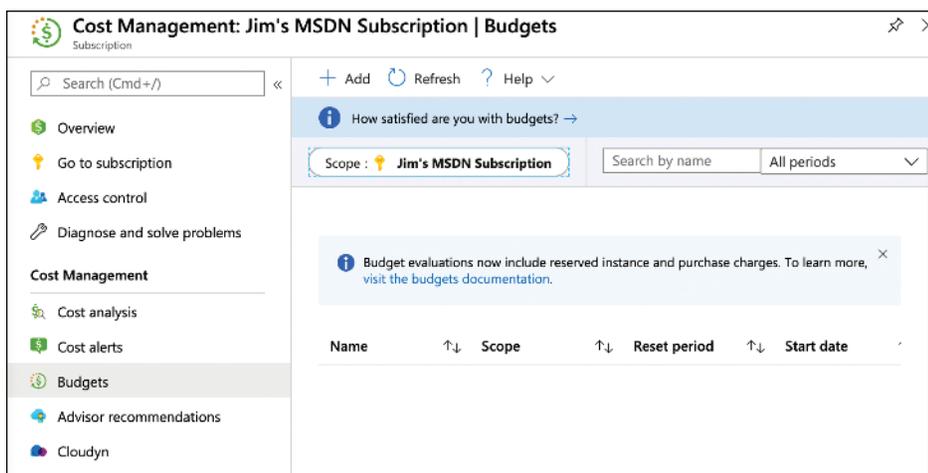


Рис. 6.10 Добавление нового бюджета

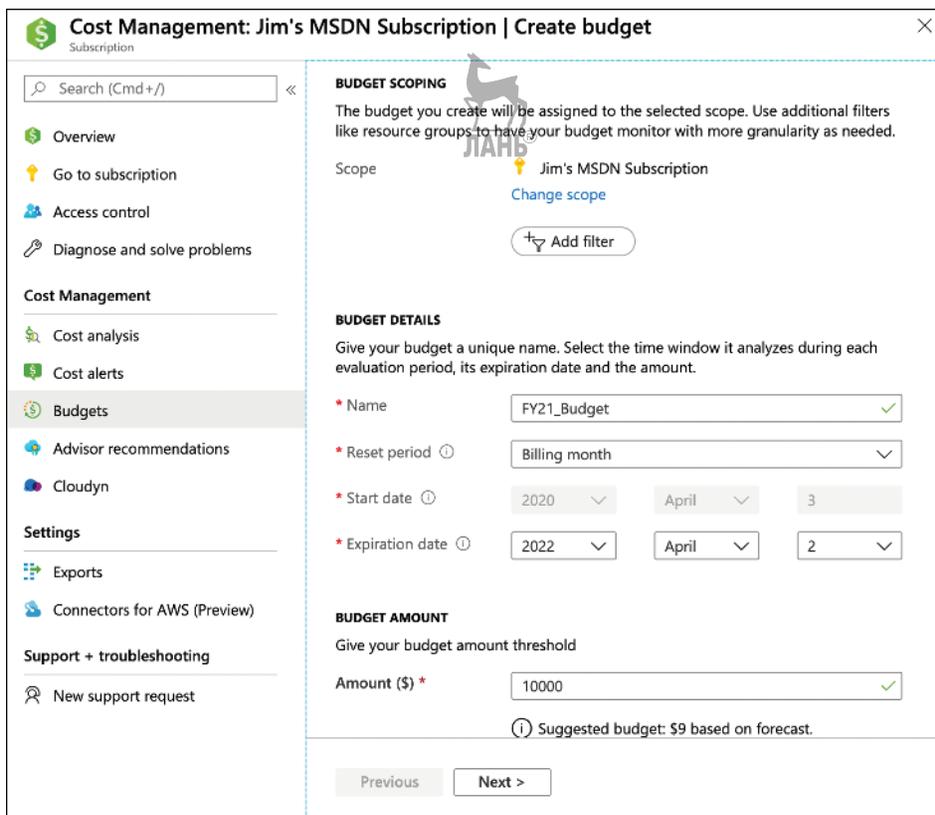


Рис. 6.11 Создание бюджета

7. Настройте все оповещения для вашего бюджета.
8. Введите адреса электронной почты людей, которым следует отправлять любую информацию о срабатывании оповещений, как показано на рис. 6.12.
9. Нажмите кнопку **Create** (Создать), чтобы завершить создание бюджета.

После создания бюджета нажмите **Cost Analysis** (Анализ затрат), чтобы увидеть, как ваши расходы сравниваются с бюджетом.



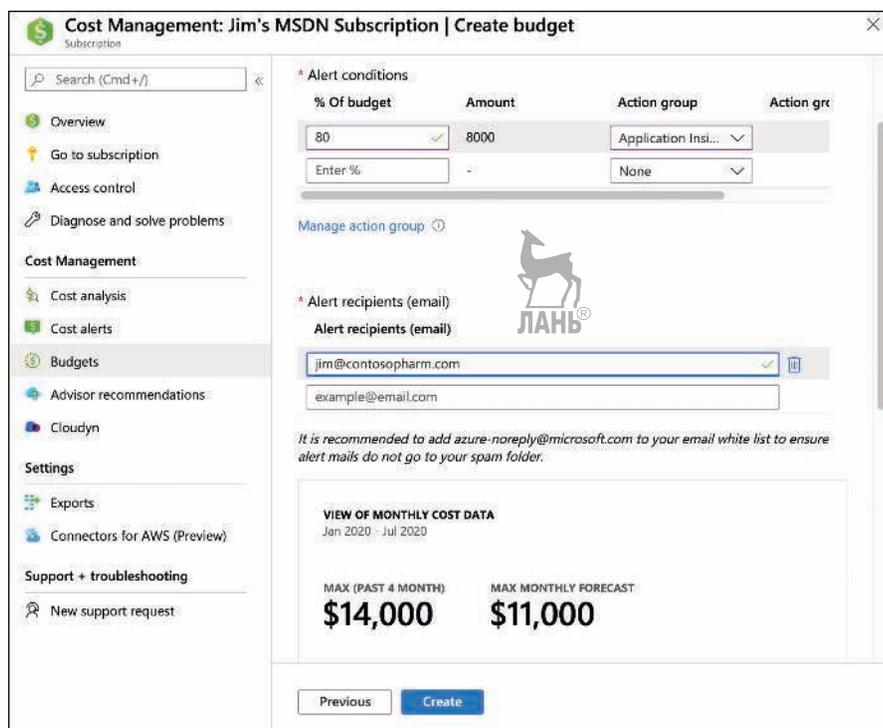


Рис. 6.12 Настройка уведомлений для бюджета

Навык 6.2: описание соглашений о качестве предоставляемых услуг и жизненных циклов служб

Многие из услуг, используемых сегодня, включают *соглашение об уровне обслуживания* (service level agreement, SLA), которое служит контрактом между вами и поставщиком услуг на определенный уровень обслуживания. Microsoft предоставляет соглашение об уровне обслуживания в Azure, а также документацию о том, как рассчитывается SLA. Однако не все службы поставляются с SLA. Microsoft часто делает службы доступными в режиме предварительного просмотра (preview), прежде чем пускает продукты в производство. Такие службы нередко идут без SLA.

Содержание раздела:

- соглашение об уровне обслуживания (Service Level Agreement, SLA);
- интерпретация терминов SLA;
- жизненный цикл служб.

Соглашение об уровне обслуживания

Соглашения об уровне обслуживания устанавливают конкретные целевые показатели доступности, а также определяют, что будет делать поставщик услуг, если эти цели не будут выполнены. Соглашение об уровне обслуживания выражается в процентах и почти всегда составляет 99 % или выше. Самый высокий уровень доступности, выраженный в SLA, составляет 99,999 %, обычно именуемый «5 девяток» (5 nines). Чтобы вам было проще понять, услуга с SLA на уровне «5 девяток» гарантирует, что время простоя в течение года не превысит 5,56 минуты. Более разумное SLA в размере 99,9 % гарантирует, что время простоя в течение месяца не превысит 43,2 минуты.

Важный пункт соглашения об уровне обслуживания для облачных служб заключается в том, что облачный провайдер считает только время простоя, вызванное проблемой на стороне облачной платформы, а не самого приложения. Другими словами, если вы разворачиваете новый код своего приложения и это приводит к аварийному завершению его работы, облачный провайдер не будет рассматривать это в качестве нарушения SLA. Если вы устанавливаете компонент на виртуальную машину и это приводит к отключению компьютера, то это также не входит в зону контроля облачного провайдера и не классифицируется как нарушение SLA.

Поскольку SLA относятся только к проблемам, которые находятся под контролем облачного провайдера, то в случае недоступности приложения важно определить, связана ли проблема с облачной платформой, или проблемой с кодом, или конфигурацией. Ответить на этот вопрос может быть сложнее, чем вы думаете.

Azure – это очень сложная среда, включающая большое количество служб, работающих вместе. Например, Служба приложений Azure (одна из самых популярных служб Azure) использует системы DNS, хранилище, базу данных и другие службы Azure. Снижение производительности любой из этих служб может повлиять на доступность приложения, работающего в Службе приложений. Если вы сообщаете, что приложение Службы приложений недоступно, Microsoft должна определить, является это проблемой Azure или вашего приложения.

Microsoft собирает огромный объем диагностических данных для операций во всех службах Azure. При открытии обращения в службу поддержки, чтобы сообщить о недоступности приложения, Microsoft может выполнить анализ этих данных, чтобы определить, была ли проблема с самой платформой Azure.

Если вы считаете, что доступность вашего приложения ниже уровня SLA, вы несете ответственность за подачу претензии в Microsoft. Вы можете сделать это, открыв обращение в службу поддержки. Если Microsoft определит, что соглашение об уровне обслуживания не было выполнено, вы можете получить кредит на счет Azure. Сумма кредита зависит от срока, в течение которого SLA не было соблюдено, и от политики SLA конкретной службы Azure.



СОВЕТ К ЭКЗАМЕНУ

Чтобы иметь право на получение кредита в связи с невыполнением SLA, необходимо подать заявку в Microsoft не позднее двух месяцев после окончания цикла выставления счетов, в течение которого произошел сбой.

Большинство служб Azure предлагают SLA не менее 99,9 %, и более высокие значения SLA могут быть достигнуты с помощью дополнительной конфигурации. Например, одна виртуальная машина, использующая хранилище Premium для всех дисков, имеет SLA 99,9 %. При развертывании двух или более виртуальных машин в одном наборе доступности SLA увеличивается до 99,95 %. Развертывание нескольких экземпляров в двух или более зонах доступности в одном регионе Azure – и соглашение об уровне обслуживания повышается до 99,99 %.



СОВЕТ К ЭКЗАМЕНУ

Microsoft иногда изменяет соглашения об уровне обслуживания. Если условия соглашения об уровне обслуживания изменятся, новые условия вступят в силу только после продления подписки Azure. До этого времени вы будете попадать под SLA, которое действовало при последнем продлении подписки или при оформлении подписки Azure.

Интерпретация терминов SLA

Поскольку SLA различается между службами Azure и поскольку определенные конфигурации могут повлиять на SLA отдельной службы, важно определить конкретное SLA для служб Azure, которые вы используете. Microsoft предоставляет веб-страницу с подробными сведениями об уровне обслуживания для каждой службы Azure. Вы можете найти его по адресу: <https://bit.ly/az900-azuresla>.

Как показано на рис. 6.13, один раз на веб-странице SLA можно выбрать категорию, чтобы просмотреть все службы Azure в этой категории. Вы также можете ввести имя службы в поле поиска, чтобы найти SLA для этой службы.

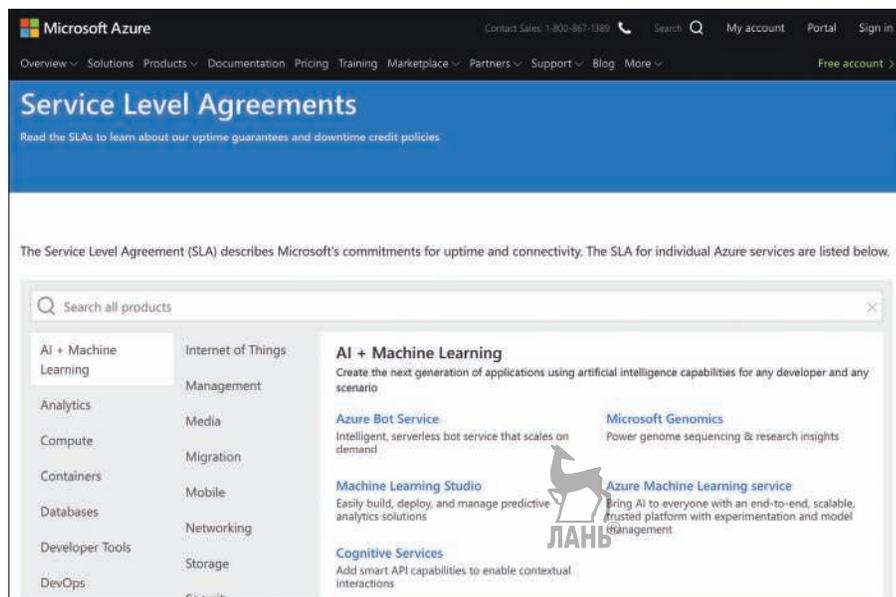


Рис. 6.13 Веб-страница соглашения об уровне обслуживания Azure

После того как вы найдете интересующую вас службу, щелкните на нее, чтобы прочитать подробные сведения об уровне обслуживания.

Когда вы нажмете на службу, то увидите подробную информацию об уровне обслуживания, предоставляемом этой службой. На рис. 6.14 показана страница соглашения об уровне обслуживания для виртуальных машин Azure. Три маркера в верхней части страницы описывают соглашение об уровне обслуживания для виртуальных машин Azure.



SLA for Virtual Machines

Last updated: January 2020

- For all Virtual Machines that have two or more instances deployed across two or more Availability Zones in the same Azure region, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.99% of the time.
- For all Virtual Machines that have two or more instances deployed in the same Availability Set or in the same Dedicated Host Group, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.95% of the time.
- For any Single Instance Virtual Machine using Premium SSD or Ultra Disk for all Operating System Disks and Data Disks, we guarantee you will have Virtual Machine Connectivity of at least 99.9%.

Introduction	∨
General Terms	∨
SLA details	∧

Additional Definitions

"**Availability Set**" refers to two or more Virtual Machines deployed across different Fault Domains to avoid a single point of failure.

"**Availability Zone**" is a fault-isolated area within an Azure region, providing redundant power, cooling, and networking.

Рис. 6.14 SLA-соглашение об обслуживании Azure VM

В разделе **Introduction** (Введение) описываются соглашения об уровне обслуживания Azure в целом. В разделе **General Terms** (Общие условия) описываются условия SLA, такие как **Management Portal** (Портал управления), **Service Level** (Уровень обслуживания) и **Downtime** (Время простоя), которые относятся ко всем службам Azure. В нем также объясняется, как можно сделать требования и ограничения для соглашений об уровне обслуживания Azure.

Раздел **SLA Details** (Сведения об уровне обслуживания) относится к конкретному сервису Azure, который вы просматриваете. Например, в этом разделе на странице соглашения об уровне обслуживания виртуальных машин определяются термины, относящиеся к соглашению об уровне обслуживания для виртуальных машин. Если вы прокрутите вниз, то увидите дополнительные сведения, показанные на рис. 6.15, в том числе как рассчитать доступность и сумму кредита, которую вы можете получить в случае невыполнения соглашения об уровне обслуживания.

Monthly Uptime Calculation and Service Levels for Virtual Machines in Availability Zones

"Maximum Available Minutes" is the total accumulated minutes during a billing month that have two or more instances deployed across two or more Availability Zones in the same region. Maximum Available Minutes is measured from when at least two Virtual Machines across two Availability Zones in the same region have both been started resultant from action initiated by Customer to the time Customer has initiated an action that would result in stopping or deleting the Virtual Machines.

"Downtime" is the total accumulated minutes that are part of Maximum Available Minutes that have no Virtual Machine Connectivity in the region.

"Monthly Uptime Percentage" for Virtual Machines in Availability Zones is calculated as Maximum Available Minutes less Downtime divided by Maximum Available Minutes in a billing month for a given Microsoft Azure subscription. Monthly Uptime Percentage is represented by the following formula:

$$\text{Monthly Uptime \%} = (\text{Maximum Available Minutes} - \text{Downtime}) / \text{Maximum Available Minutes} \times 100$$

The following Service Levels and Service Credits are applicable to Customer's use of Virtual Machines, deployed across two or more Availability Zones in the same region:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.99%	10%
< 99%	25%
< 95%	100%

Рис. 6.15 Подробные сведения об уровне обслуживания виртуальных машин Azure

Если ваше приложение использует несколько служб Azure, то несколько соглашений об уровне обслуживания будут применяться к вам. Если у вашего приложения возникают простои, необходимо подать заявку на все службы Azure, которые подпадают под SLA, если вы хотите получить кредит. Однако денежный кредит не является вашей единственной заботой, связанной с доступностью вашего приложения. Простои в приложении негативно влияют на ваш бизнес, поэтому вы всегда хотите иметь максимально высокий уровень обслуживания, и когда вы имеете дело с несколькими службами Azure с разными соглашениями об уровне обслуживания, важно понимать, как это влияет на общее SLA.

При расчете SLA для приложения, использующего несколько служб Azure, необходимо рассчитать составное соглашение об уровне обслуживания на основе используемых служб. Например, если у вас есть App Service Web App, которое также использует одну виртуальную машину Azure с хранилищем Premium, необходимо объединить SLA для обеих служб, чтобы определить общее SLA вашего приложения.

ПРИМЕЧАНИЕ СОСТАВНЫЕ СОГЛАШЕНИЯ SLA

Важно понимать, что отдельные соглашения об уровне обслуживания по-прежнему применяются к вам при использовании нескольких служб Azure. Однако понимание составных соглашений об уровне обслуживания имеет важное значение, поскольку позволяет определить, когда конкретная конфигурация повышает вероятность простоя.

Соглашение об уровне обслуживания для службы приложений составляет 99,95 %, а SLA для одной виртуальной машины с хранилищем Premium – 99,9 %. Таким образом, общее соглашение об уровне обслуживания для вашего приложения составляет $99,95 \% \times 99,9 \%$, или 99,85 %. Разворачивая две виртуальные машины в двух зонах доступности в одном регионе, можно получить соглашение об уровне обслуживания на уровне 99,99 % для виртуальных машин, что увеличивает общий уровень обслуживания до 99,94 %.

Жизненный цикл службы Azure

По мере того как группы по продуктам Azure разрабатывают новые службы и возможности, им важно получать отзывы от клиентов, использующих эти службы и возможности в реальной среде. По этой причине Microsoft часто предлагает клиентам новые услуги и возможности в рамках предложений с предварительным просмотром. В то время как официальным термином Microsoft является «предварительный просмотр» (preview), вы часто увидите, что люди ссылаются на эти службы и возможности как «предложение для бета-тестирования» (beta offering).

Как только функция наполняется необходимым содержанием, она переходит на этап *общедоступности*. Это именно тот этап, на котором уже будет поддерживаться SLA.



СОВЕТ К ЭКЗАМЕНУ

Службы и возможности, которые находятся в режиме предварительного просмотра, не предлагают SLA и не предназначены для использования в качестве приложений в производственной среде. Возможности в режиме предварительного просмотра также обычно предлагаются не во всех регионах Azure. Microsoft предоставит документацию о том, какие регионы доступны для определенного preview-функционала.

Службы и возможности в режиме preview

Службы и возможности в режиме preview иногда сначала предлагаются в качестве частного предварительного просмотра (private preview). В частном предварительном просмотре услуга или функция становятся доступной для тестирования небольшому набору клиентов. Доступ к частному предварительному просмотру иногда осуществляется по приглашению инженеров, разрабатывающих службу или возможность. В других случаях Microsoft может предоставить любому клиенту возможность зарегистрироваться для доступа к private preview. Если регистрация открыта для всех, Microsoft закрывает регистрацию после набора целевого числа клиентов.

ПРИМЕЧАНИЕ СЛУЖБЫ ИЛИ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Многие случаи private preview предназначены для новых функций существующих сервисов. Например, Служба приложений может получить новую функциональную возможность, и до того, как эта функция будет выпущена, она будет проходить некоторое время через этап предварительного просмотра.

Возможности и службы в режиме `private preview` обычно предоставляют только часть функциональности, которая в конечном итоге превратится в сервис или функцию. Microsoft часто просит клиентов с помощью частного предварительного просмотра протестировать конкретные сценарии и предоставить обратную связь. Это помогает инженерным командам выявлять ошибки и проблемы с удобством работы в сложных реальных средах, которые используются заказчиками.



СОВЕТ К ЭКЗАМЕНУ

Не все услуги или функции предлагают частный предварительный просмотр. Если `private preview` не предлагается, служба или функция сначала становится доступной в режиме публичного предварительного просмотра (`public preview`). Все сервисы и функции проходят через определенный период `public preview`. В режиме `private preview` новинки могут быть предложены клиентам бесплатно, но чаще они предлагаются со значительной скидкой.

После того как сервис или функция удовлетворяет определенным критериям, установленным командой инженеров, она будет переходить к публичному предварительному просмотру. Обычно это происходит после того, как сервис или функция полностью реализованы или очень близки к этому. Однако если есть ошибки в определенной части функциональности, которую инженерная команда считает критической, они могут задержать стадию `public preview` до тех пор, пока эти ошибки не будут исправлены.

Функции и службы, которые находятся в `public preview`, предоставляются со скидкой, но, как и в случае с `private preview`, они обычно не предлагают SLA и предоставляются «как есть» (`as-is`).

Клиентам, участвующим в `private preview`, иногда предоставляется секретная ссылка на портал Azure, который включает службу или функциональную возможность. Когда клиент использует эту ссылку, Microsoft может использовать идентификатор подписки Azure, чтобы определить, зарегистрированы ли они и утверждены для предварительного просмотра. В противном случае функция или сервис будут недоступны, даже если они используют секретную ссылку.

Также бывают и сценарии, которые нельзя реализовать с помощью портала Azure. В этих случаях клиентам предоставляются инструкции к командной строке по использованию службы или функциональности. Чаще всего пользовательский интерфейс портала разрабатывается на этапе `private preview`, поэтому первым пользователям обычно предоставляется доступ только через командную строку.

Как только служба или функция попадает в `public preview`, она становится доступной для всех клиентов в определенных регионах, и регистрация не требуется для ее использования. Значок предварительного просмотра будет отображаться на портале Azure, чтобы пользователи знали, что служба или функция доступны в режиме `preview`. На рис. 6.16 показаны функции контейнера Docker в веб-приложении App Service, работающем в Windows, и каждый параметр контейнера содержит значок `preview`.

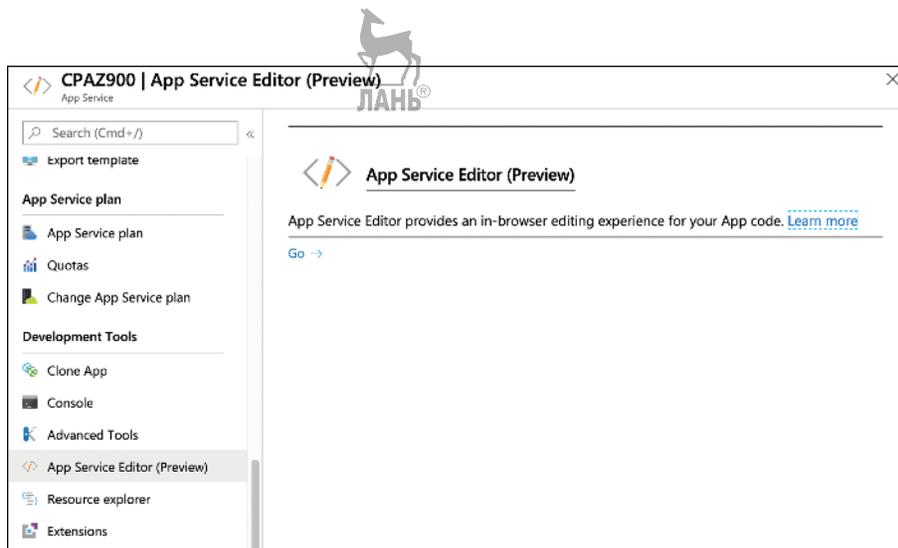


Рис. 6.16 Функции в предварительном просмотре в Службе приложений

Службы и функции, которые находятся в общедоступной предварительной версии, обычно поддерживаются Microsoft так же, как если бы они были полностью выпущены. Однако SLA не применяются к preview-функциональности, и есть ситуации, когда служба или функция не будут поддерживаться инженерами технической поддержки Microsoft во время предварительного просмотра. В таких случаях вы можете обратиться на форумы для поддержки.

Общая доступность

После того как услуга или функция в режиме preview достигнет качества и доступности, подходящей для инженерной команды, они объявят об общей доступности (general availability, GA). На этом этапе сервис или функция полностью поддерживаются.

Как только служба или функция достигает GA, она попадает под соглашение об уровне обслуживания, предоставляемое Microsoft. Если это новый сервис, новое соглашение об уровне обслуживания будет опубликовано на веб-странице SLA. Для новых возможностей существующих сервисов SLA наследуется от SLA самого сервиса.

Если вы использовали функцию или сервис во время public preview, вам обычно не нужно ничего делать, чтобы получить официальную поддержку в рамках GA. Однако в некоторых ситуациях Microsoft попросит удалить все ресурсы, созданные во время preview, и создать их заново. Обычно это происходит, когда оставшийся код от preview может вызвать проблемы с сервисом или функцией, запущенной в GA.

Когда служба или функция достигает GA, она не обязательно будет доступна в режиме GA во всех географических регионах Azure. В таких случаях другие регионы обычно будут на более позднем этапе жизненного цикла сервиса или функции. Ценообразование в режиме preview также может оставаться в силе в течение определенного периода времени после GA. Такие сведения опубликованы в официальном объявлении GA на веб-сайте Azure.

Мысленный эксперимент

Мы рассмотрели множество положений, и настало время применить полученные знания на практике. Как всегда, мы это сделаем при помощи мысленного эксперимента, ответы на который вы найдете в следующем разделе.

Вот уже несколько месяцев ContosoPharm планирует масштабное разворачивание в облако. Компания уже готова спустить курок и начать работу. ИТ-директор – тот единственный сотрудник компании, который больше всего обеспокоен таким переходом. У директора строго ограничен бюджет, поэтому ей важно понимать, о каких финансовых затратах будет идти речь. ИТ-директор должна будет предоставить подробный финансовый прогноз финансовому директору, поэтому необходимо получить точный отчет по затратам. ContosoPharm обратились к вам за решением.

ContosoPharm столкнется с комплексным сетевым разворачиванием при работе с новой облачной службой. Планируется большое количество подключенных к сети ВМ. Необходимо снизить затраты, свести к минимальным расходам. Какие рекомендации вы можете дать для этого? А что вы можете посоветовать в отношении ВМ?

ИТ-директор может вам предоставить сводную ведомость с подробным описанием ресурсов, которые компания хотела бы использовать в облаке. Туда нужно будет внести приблизительную стоимость, но у директора нет уверенности в вопросах ценообразования. Что бы вы ей могли посоветовать?

На данном этапе ContosoPharm размещает службу локально. Переход в облако обусловлен экономией денежных средств. Финансовому директору нужно получить прогноз по разнице в затратах от использования технологии облачных вычислений и при локальном использовании. Какой вы видите самый лучший способ для сбора подобной информации?

После того как ContosoPharm развернет службу в облаке, ИТ-директору нужно будет осуществлять мониторинг затраченных средств, чтобы убедиться, что затраты не выходят за рамки дозволенного. Если это произойдет, ИТ-директору нужно будет отчитаться перед финансовым директором за перерасходы. Как это можно будет сделать проще всего?

Директор по информационным технологиям запросил у ИТ-директора информацию касательно надежности облака, на что получил положительный ответ. Однако ИТ-директору потребуются соответствующие аргументы, подкрепленные реальными данными. Было бы неплохо, если бы она смогла предоставить подробную информацию по настройке сервисов для повышения надежности. Что вы порекомендуете тут?

Ответы на мысленный эксперимент

В этом разделе представлены ответы на мысленный эксперимент.

Чтобы снизить затраты на сети и виртуальные машины (ВМ), можно поступить следующим образом. Для начала тщательно спланировать то, в каких регионах будут создаваться службы. От региона к региону затраты разнятся,

поэтому выбор региона с наименьшими затратами поможет в этой ситуации. Однако не забывайте, что за трафик виртуальных сетей Azure, идущий из центра обработки данных, вам будет выставлен счет, поэтому нужно тщательно спланировать, как этого можно будет избежать (по возможности). Нужно принимать во внимание и зоны, потому как в зависимости от зон будет отличаться и сетевой трафик.

Чтобы получить приблизительную цену по стоимости ресурсов, ContosoPharm может воспользоваться калькулятором цен. Он позволит добавлять и настраивать используемые продукты Azure. После чего вы получите смету расходов за месяц, которую как раз ИТ-директор и сможет включить в сводную ведомость.

Чтобы понять, какую сумму сэкономит ContosoPharm от использования облака, ИТ-директор может воспользоваться калькулятором TCO. Используя его, ИТ-директор может внести все сведения о локальных системах ContosoPharm, персонале и т. д. А потом можно будет получить полное представление об экономии.

Для непрерывного отслеживания расходов и уведомлений о потенциальных причинах по превышению бюджета ContosoPharm может использовать Управление затратами Azure. Компания может составить бюджет на основе ожидаемой степени использования, а служба Azure по управлению затратами – позволить компании управлять и отслеживать расходы, а также отчетываться по ним.

ИТ-директор может найти информацию по надежности облачных служб на страницах об SLA по каждой службе, что даст точную информацию по тому, что предлагает Microsoft. Там также будет расписано, какую конфигурацию ContosoPharm нужно выполнить для наивысшего уровня обслуживания. И поскольку ИТ-директор собирает данные по надежности облачных вычислений, эти сведения могут оказаться для нее полезными.

Краткое содержание главы

В этой главе мы затронули множество тем: от ценообразования до затрат, от уровней обслуживания до жизненного цикла служб. Ниже представлен краткий обзор главы.

- Ключевыми факторами ценообразования являются тип ресурсов и способ их приобретения, используемые регионы Azure и зоны выставления счетов, в которых расположены ваши ресурсы.
- Оплата служб Azure осуществляется в соответствии со счетчиками определенного ресурса.
- Приобретение Корпоративного соглашения или же приобретение продуктов у партнера по облачным решениям поможет сэкономить денежные средства на услугах Azure.
- Цены Microsoft варьируются в зависимости от региона, поэтому ваши расходы будут также отличаться.
- Регионы Azure разбиты по зонам выставления счетов, поэтому с вас будет взиматься разная плата.



- Калькулятор цен помогает рассчитать расходы в Azure, предоставляя приблизительную смету на основе необходимых ресурсов.
- Калькулятор общей стоимости владения позволяет вводить сведения о ваших локальных ресурсах. Затем он предоставляет вам оценку того, сколько можно будет сэкономить при переходе в облако.
- Управление затратами Azure дает возможность более детально анализировать затраты.
- Управление затратами позволяет создавать бюджет и настраивать оповещения на основе бюджета.
- Соглашение об уровне обслуживания (Service Level Agreement, SLA) – это гарантия, предоставляемая Microsoft на бесперебойную работу служб.
- SLA часто включают требования к необходимой конфигурации. Они задокументированы на веб-странице соглашения об уровне обслуживания.
- Служба, не попадающая под SLA, считается только тогда, когда возникающая в ней проблема находится вне юрисдикции Microsoft.
- Службы предварительного просмотра предлагаются заблаговременно до релиза продукта. Зачастую идут без SLA и продаются со скидкой.
- Служба, готовая к использованию, считается общедоступной и включает в себя SLA.



Предметный указатель

A

Azure Active Directory, 240
Azure Advisor, 183
Azure Blueprints, 263
Azure Bot, 135
Azure Cloud Shell, 176
Azure Cost Management, 288
Azure Databricks, 122
Azure DevOps, 153
Azure DevTest Labs, 157
Azure Files, 85
Azure Firewall, 226
Azure Functions, 138
Azure IoT Hub, 103
Azure Key Vault, 209
Azure Machine Learning, 128
Azure Marketplace, 93
Azure mobile app, 181
Azure Monitor, 186
Azure Policy, 254
Azure Portal, 164
Azure PowerShell Az, 171
Azure Pricing Calculator, 283
Azure Security Center, 204
Azure Sentinel, 213
Azure Service Health, 195
Azure Sphere, 116
Azure Synapse Analytics, 118
Azure Test Plans, 156

C

Cloud Adoption Framework, 271

Cosmos DB, 86

D

DDoS protection, 233

E

Event Grid, 152
ExpressRoute, 82

H

HDInsight, 119

I

IoT Central, 109

L

Logic Apps, 146

N

Network Security Group, 220

P

Playbook, 217
PostgreSQL, 92

S

Service Trust Portal, 272

A

Аварийное восстановление, 24
Авторизация, 239
Аутентификация, 239

Б

База данных Azure
SQL, 89
Блокировка, 259
Большие данные, 118
Брандмауэр Azure, 226

В

Виртуальная машина (VM), 20, 61
Виртуальная сеть Azure, 80
Виртуальный рабочий стол Azure, 78
Внешний интерфейс, 71

Г

Гибкость, 23
Гостевые пользователи, 242
Границы географические, 45
Группа действий, 193
Группа ресурсов, 49
Группы управления, 56

Д

Декларативный синтаксис, 58
Дисковое хранилище, 84
Домен
обновлений, 67
сбоя, 67
Доступность, 18

Е

Единый вход, 245

З

Защита от DDoS, 233
Заявление о конфиденциальности
Microsoft, 270
Зоны
выставления счетов, 282
доступности, 46

И

Инициатива, 256
Инсталляционный сервер, 226
Инфраструктура как услуга
(IaaS), 26
Искусственный интеллект, 128

К

Калькулятор
совокупной стоимости
владения, 285
цен Azure, 283
Кластер, 78, 118
Концепция контейнеров, 75

Л

Локальная модель, 24

М

Масштабируемость, 21
Многофакторная
аутентификация, 247
Модель
на основе потребления, 25
разделения ответственности, 26

Н

Наборы доступности, 67

О

Облако
гибридное, 37
общедоступное, 34
частное, 36
Облачная модель, 25
Облачные вычисления, 34
Образ, 75
Отказоустойчивость, 23

П

Платформа как услуга (PaaS), 29
Под, 78
Подписки Azure, 52
Политика Azure, 254
Поставщик ресурсов, 58
Принцип экономии за счет
масштаба, 25
Проверка подлинности, 239
Программное обеспечение как услуга
(SaaS), 31

Р

Региональная пара, 45



Регионы Azure, 45
суверенные, 275

С

Служба когнитивных вычислений, 134
Соглашение об уровне
обслуживания, 19, 293
Счетчик, 281

Т

Таблица маршрутов, 228
Тег, 262

У

Управление доступом на основе
ролей, 249
Управление затратами Azure, 288
Условный доступ, 246

Х

Хранилище
ключей Azure, 209
BLOB-объектов, 83

Ц

Центр управления
безопасностью, 271

Ш

Шаблон ARM, 50, 59

Э

Эластичность, 22

Я

Ядро Azure AD, 240



Книги издательства «ДМК ПРЕСС»
можно купить оптом и в розницу
в книготорговой компании «Галактика»
(представляет интересы издательств
«ДМК ПРЕСС», «СОЛОН ПРЕСС», «КТК Галактика»).

Адрес: г. Москва, пр. Андропова, 38;
тел.: (499) 782-38-89, электронная почта: books@aliants-kniga.ru.

При оформлении заказа следует указать адрес (полностью),
по которому должны быть высланы книги;
фамилию, имя и отчество получателя.

Желательно также указать свой телефон и электронный адрес.

Эти книги вы можете заказать и в интернет-магазине: <http://www.galaktika-dmk.com/>.



Джим Чешир

Основы Microsoft Azure. Подготовка к экзамену AZ-900

Главный редактор *Мовчан Д. А.*
dmkpress@gmail.com

Зам. главного редактора *Сенченкова Е. А.*

Редактор *Черников В. Н.*

Перевод *Воронина А. Д.*

Корректор *Синяева Г. И.*

Верстка *Чаннова А. А.*

Дизайн обложки *Мовчан А. Г.*

Гарнитура PT Serif. Печать цифровая.

Усл. печ. л. 24,86. Тираж 200 экз.

Веб-сайт издательства: www.dmkpress.com

Сдайте экзамен Microsoft Exam AZ-900 и продемонстрируйте ваши знания облачной платформы Microsoft Azure!

Темы, рассмотренные в книге:

- облачные концепции;
- ключевые сервисы Azure;
- безопасность, приватность, соответствие требованиям регуляторов и механизмов обеспечения доверия;
- ценообразование в Azure;
- соглашение об уровне обслуживания и жизненный цикл служб Azure.



Данное руководство:

- организовано в соответствии с темами экзамена;
- содержит интересные упражнения на стратегическое мышление;
- предполагает, что вы хотите овладеть основами облачных сервисов на базе Microsoft Azure;
- не требует от читателя реального опыта работы в IT.

Издание подходит не только техническим специалистам, но и сотрудникам отделов продаж, служб поддержки и других нетехнических направлений.

Интернет-магазин:
www.dmkpress.com

Оптовая продажа:
КТК «Галактика»
books@aliens-kniga.ru

DMK
ИЗДАТЕЛЬСТВО
www.dmk.pf

Экзамен AZ-900

Экзамен AZ-900 сфокусирован на проверке базовых знаний по облачным технологиям, включая различия между IaaS/PaaS/SaaS и публичными/частными/гибридными облачными моделями. Также от вас потребуется знание основных архитектурных компонентов, продуктов и решений в Azure, инструментов управления сервисами, безопасностью и функциями отдельных служб. Дополнительно проверяется знание инструментов мониторинга, обеспечения приватности, соответствия требованиям регуляторов, механизмов защиты данных. Последний блок вопросов относится к подпискам Azure, управлению затратами, уровням обслуживания и рассмотрению жизненного цикла служб в Azure.

ISBN 978-5-97060-869-2



9 785970 608692 >