Introduction

Businesses today are being challenged by the proliferation of handheld devices and new corporate policies for BYOD (Bring Your Own Device). Users want to be able to access their productivity applications from anywhere, from any device — a laptop, smartphone or tablet — and use only one username and password to access it all. This creates a challenge for IT. How do they give users what they want, while maintaining a secure environment?

To accomplish this, businesses need to have a robust, hybrid infrastructure that allows users to seamlessly access their applications whether they are deployed in their on-premises data center or in the cloud. This white paper focuses specifically on Microsoft’s approach, featuring Office 365 and Azure. It demonstrates how to configure and deploy Active Directory in a hybrid architecture. We’ll discuss why hybrid makes sense, common concerns, pitfalls to consider, and best practices for setting up your hybrid infrastructure leveraging Azure Active Directory Services with Office 365.

ABOUT OFFICE 365:

Microsoft Office 365 provides secure anywhere access to professional email, shared calendars, instant messaging (IM), video conferencing and document collaboration. It represents the cloud version of Microsoft Office, a suite of communication and collaboration productivity tools for businesses of all sizes.

ABOUT AZURE:

Azure is Microsoft’s cloud computing platform for building, deploying and managing applications and services through a global network of Microsoft data centers. Azure consists of a growing collection of integrated services including identify management, analytics, computing, database, mobile, networking, storage and web.
Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft’s multi-tenant, cloud-based directory and identity management service. Azure Active Directory extends on-premises Active Directory into the cloud, enabling users to use their primary organizational account to not only sign in to their domain-joined devices and company resources, but also all of the web and SaaS applications needed for their job.

Without Active Directory integration, users have to manage multiple sets of usernames and passwords. In addition, application access can be mistakenly provisioned or de-provisioned — automatically — based on organization group membership or employee status. Azure Active Directory introduces security and access governance controls that enable administrators to centrally manage user access across SaaS applications such as Office 365. It also gives users the ease of a single sign-on for access to their productivity applications.

The architecture of the integration has the following four main building blocks:

1. Single sign-on enables users to access their SaaS applications based on their organizational account in Azure AD. Single sign-on enables users to authenticate to an application using their single organizational account.

2. User provisioning and de-provisioning into a target SaaS occur based on changes made in Windows Server Active Directory and/or Azure AD. A provisioned account enables a user to be authorized to use an application after they have authenticated through single sign-on.

3. Centralized application access management in the Azure Management Portal enables single-point SaaS application access and management, with the ability to delegate application access decision-making and approvals to anyone in the organization.
HOW DOES SINGLE SIGN-ON WITH AZURE ACTIVE DIRECTORY WORK?

When a user “signs in” to an application, they go through an authentication process that requires them to prove their identity. Without single sign-on, this is typically done by entering a password that is stored within each and every application. The user is required to know each password for each application.

Azure AD supports three different ways to sign in to applications:

1. **Federated Single Sign-on** enables each application to redirect to Azure AD for user authentication instead of prompting for its own password. This works for applications that support protocols such as SAML 2.0, WS-Federation or OpenID Connect, and is the richest mode of single sign-on.

2. **Password-based Single Sign-on** enables secure application password storage and replay using a web browser extension or mobile app. This leverages the existing sign-in process provided by the application, but enables an administrator to manage the passwords and does not require the user to know the password.

3. **Existing Single Sign-on** enables Azure AD to leverage any existing single sign-on that has been set up for the application. The application can be linked to the Office 365 or Azure AD access panel portals; additional reporting can also be enabled in Azure AD when the application is launched there.

Once users have authenticated with an application, they also need to have an account record provisioned within the application. This tells the application where their user permissions and level of access are located inside the application. The provisioning of this account record can occur automatically, or it can occur manually by an administrator before the user is provided single sign-on access.

For security, Azure AD also includes a full suite of identity management capabilities, including:

- multi-factor authentication
- device registration
- self-service password management
- self-service group management
- privileged account management
- role-based access control
- application usage monitoring
- rich auditing
- security monitoring and alerting
These capabilities can help secure cloud-based applications, streamline IT processes, cut costs and ensure corporate compliance goals are met.

Additionally, with just four clicks, Azure AD can be integrated with an existing Windows Server Active Directory, giving organizations the ability to leverage their existing on-premises identity investments to manage access to cloud-based SaaS applications.

Below is a visual representation of the Azure Active Directory:

![Diagram of Azure Active Directory](https://azure.microsoft.com/en-us/documentation/articles/active-directory-whatis/)

**WHAT ARE THE BENEFITS OF AZURE AD?**

Your organization can use Azure AD to improve employee productivity, streamline IT processes, improve security and cut costs in many ways:

- Quickly adopt cloud services, providing employees and partners with an easy single sign-on experience powered by Azure AD’s fully automated SaaS app access management and provisioning services capabilities.
- Empower employees with access to world-class cloud apps and self-service capabilities from wherever they need to work, on the devices they love to use.
- Easily and securely manage employee and vendor access to your corporate social media accounts.
- Improve application security with Azure AD multifactor authentication and conditional access.
• Implement consistent self-service application access management, empowering business owners to move quickly while cutting IT costs and overhead.
• Monitor application usage and protect your business from advanced threats with security reporting and monitoring.
• Secure mobile (remote) access to on-premises applications.

COMPARING YOUR ON-PREMISES ACTIVE DIRECTORY TO AZURE ACTIVE DIRECTORY

The Active Directory capabilities that are part of Windows Server actually include several different roles, such as Active Directory Domain Services (AD DS), Active Directory Certificate Services (AD CS), Active Directory Lightweight Directory Services (AD LDS), Active Directory Federation Services (AD FS) and Active Directory Rights Management Services (AD RMS).

Many people think of “Active Directory” as Active Directory Domain Services when comparing AD with Azure Active Directory. But Active Directory Domain Services (henceforth just Active Directory) in Windows Server is completely different from Azure Active Directory (Azure AD), and they have different focus areas.

Active Directory is a true directory service that has a hierarchical structure (based on X.500) that uses DNS as its locator mechanism and can be interacted with via LDAP. In addition, Active Directory primarily uses Kerberos for authentication. Active Directory enables organizational units (OUs) and Group Policy Objects (GPOs) in addition to actually joining machines to the domain. It allows trusts to be created between domains.

Azure AD, while having some aspects of a directory service, is really an identity solution and allows users and groups to be created, but in a flat structure without OUs or GPOs. You can’t join a machine to Azure AD unless you are running Windows 10 and ADFS. There’s no Kerberos authentication, and you can’t query it via LDAP. These missing elements are acceptable for Azure AD on-premises, where all types of communication are possible. However, Azure AD is particularly focused on identity throughout the internet, where the types of communication are typically limited to HTTP (port 80) and HTTPS (port 443) and are used by all types of devices — not just corporate assets. Authentication is performed through a number of protocols such as SAML, WS-Federation and OAuth. It’s possible to query Azure AD but instead of using LDAP you use a REST API called AD Graph API. These all work over HTTP and HTTPS.
Why Hybrid Architecture?

In the context of this white paper, a hybrid architecture is one that integrates your Windows Server Active Directory with Azure Active Directory, allowing you to extend your on-premises infrastructure into the cloud. Because it makes use of your existing setup, it allows you to unlock cloud services that you currently consume in the easiest way possible.

A hybrid architecture provides an ideal experience for your Office 365 deployment. For a seamless user experience, you might think about combining your on-premises Active Directory with Azure AD by setting up directory synchronization (including password sync) and federation. This allows users on their corporate assets to log on with their AD account, and when they access internet services, such as Office 365, authentication with Azure AD happens seamlessly via the federation. This allows access to all the different services that Azure AD is federated with. This is actually a great benefit of federating your on-premises AD with Azure AD. While it’s possible for your organization to federate with various companies out on the internet, it requires a lot of manual effort to set up and maintain. However, if you federate with Azure AD, you’ve federated by proxy with all the organizations that Azure AD is federated with — pretty much all of the major service providers on the internet today. Think of Azure AD as a federation hub.

A hybrid architecture may also be necessary for compliance with regulations that require authentication take place behind your firewalls. So, for example, when signing into a third-party SaaS application, users are authenticated using your on-premises Active Directory Domain Services instead of Azure Active Directory.

When you think about maximizing Azure AD, you’ll want to use it for authentication for internet-based services such as Office 365, as well as thousands of services (e.g., Facebook) that are already federated with Azure AD. By default, they trust Azure AD without you having to do anything beyond enabling the application or service for your user base. In order to accomplish this, you need to deploy Azure Active Directory Federated Service (Azure ADFS). This can be a challenging undertaking if you don’t have the right resources. To give you an idea of the complexity, we’ll walk through the steps in the next section.
THE FOLLOWING TABLE WILL HELP YOU CHOOSE
THE CORRECT MODEL AND IDENTITY TO BE USED WITH AZURE AD.

<table>
<thead>
<tr>
<th>I need to...</th>
<th>Synchronized identity model</th>
<th>Federated identity model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DirSync</td>
<td>Azure AD Sync/ Azure AD Connect**</td>
</tr>
<tr>
<td>Sync new user, contact, and group accounts created in my on-premises AD to the cloud in a single-forest scenario</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sync new user, contact, and group accounts created in my on-premises AD to the cloud in a multi-forest scenario</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Enable users to sign in with the same identity and password</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Immediately disable user accounts</td>
<td>✓***</td>
<td>✓***</td>
</tr>
<tr>
<td>Enable cloud-based multi-factor authentication solutions</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enable self-service password reset with AD write-back option</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Customize the user sign-in page to Azure AD/Office 365</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enable users to sign in once using corporate credentials without password caching</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable use of on-premises third-party multi-factor authentication solutions</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do not replicate password hashes to the cloud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restrict access based on location or group membership</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Allow authentication with non-MS identity providers</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Enable SSO for SaaS applications, hybrid applications, etc.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Audit users sign-in to Azure AD/Office 365</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

* With password sync  
** Including Azure AD Basic or Premium capabilities  
*** Using user password reset
How to Implement Azure AD Federated Service in a Hybrid Environment

Setting up the Azure AD Federated Service can be a complex undertaking. The following steps provide high-level guidance on successfully configuring your environment to:

- deploy Azure AD FS
- set up Azure AD/Office 365 single sign-on
- start using Azure AD FS to provide a seamless sign-in experience for end users accessing Azure AD and Office 365 resources.

For a more details, please refer to www.rackspace.com/Azure.

We’ll start by building a highly available test environment for the directory synchronization with a single sign-on (SSO) scenario. The goal is to provide users with the most seamless authentication experience possible as they access Microsoft cloud services (and/or other cloud-based applications) while logged on to the corporate network.

For the sake of simplicity, and in order to focus on the key aspects that relate to the directory synchronization with an SSO scenario, the test environment features:

- In the cloud: Azure AD/Office 365 tenant and cloud-based applications that leverage Azure AD for identity management and access control
- On-premises: Active Directory single-forest environment
- Two Active Directory Federated Services (ADFS) servers integrated with Active Directory for authentication
- Two Wireless Application Protocol (WAP) proxies to publish on the internet the AD FS server endpoints
- A third-party SSL certificate with the appropriate SAN names to be used by ADFS

AZURE SECURITY

If you invest in a cloud service, you must be able to trust that your customer data is safe, that the privacy of your data is protected, and that you retain ownership of and control over your data — that it will only be used in a way that is consistent with your expectations. Microsoft has built Azure with industry-leading security measures and privacy policies, and participated in international compliance programs with independent verification. Azure conforms to global standards including ISO 27007, PCI DSS, HIPAA, SOC 1, SOC 2, FedRAMP and UK G-Cloud.

To find out more out Azure’s built in security, visit: http://azure.microsoft.com/en-us/support/trust-center/
The following diagram provides an overview of the production environment with the software and service components that need to be deployed and configured.

Figure 1. Typical Azure Deployment
CREATE A TEST AZURE AD/OFFICE 365 TENANT AND LOCAL ENVIRONMENT*

For the purpose of testing and familiarizing yourself with ADFS, the easiest way to provision environments for both Azure AD and Microsoft Office 365 Enterprise (including related Office application workloads) is to sign up for the appropriate free trial accounts from Microsoft. For Office 365, there is a free 30-day Enterprise E3 trial. And if you don’t already have an Azure account, you can sign up for a free one-month trial.

Then you will add your Azure trial subscription to your Office 365 account. This is done by utilizing your Office 365 global administrator account.

Next, set up a local environment for Azure using Azure PowerShell. Microsoft Azure PowerShell is the module for Windows PowerShell that you can use to control and automate the deployment and management of the workloads in Azure. The configuration of Azure PowerShell on a local computer consists of:

- Installing Azure PowerShell
- Verifying that Azure PowerShell can run scripts, and enabling scripts to run in Windows PowerShell
- Verifying that WinRM allows Windows PowerShell to connect, and configuring WinRM to support basic authentication
- Creating external DNS records for adfs, enterprise registration, and www

Your local environment will include six computers, one for each role (these roles will be configured later in the process).

a. **Group Managed Services Account (gMSA):** A Windows Server 2012 (or higher) on at least one DC computer, i.e. the DC1 computer in our illustration. This is used for creating a group Managed Service Account (gMSA) that will be required during the AD FS installation and configuration.

b. **Sync Server:** A Windows Server 2008 R2 (or higher) computer, i.e. the ADFS1 computer in our illustration.

c. **AD FS Server:** A Windows Server 2012 R2 computer, i.e. the ADFS1 computer in our illustration.

d. **Web Application Proxy (WAP) Server:** A Windows Server 2012 R2 computer, i.e. the EDGE1 computer in our illustration.
SET UP SINGLE SIGN-ON WITH THE AZURE AD/OFFICE 365 TENANT

This section discusses how to set up single sign-on between your on-premises Active Directory (e.g., yourcompanydevserver.com) and the Azure AD/Office 365 tenant (e.g., yourcompany.onmicrosoft.com) to offer a seamless user experience in accessing cloud resources like an Office 365 Enterprise E3 subscription.

For the sake of simplicity, we will leverage the Azure Active Directory Connect (Azure AD Connect) wizard. We’ll set up the directory synchronization and the federation between the on-premises infrastructure of your test environment and the Office 365 (yourcompany.onmicrosoft.com) tenant in the cloud.

1. To begin, add a domain to your Azure AD/Office 365 tenant that will be later federated with your on-premises Active Directory.

2. Next, you’ll integrate your on-premises Active Directory forest(s) with your Azure AD/Office 365 tenant to configure the Azure-based infrastructure from an identity perspective. This will establish the identity bridge between it and your Azure AD/Office 365 subscription with the following steps:
   a. Procure a third-party SSL/TSL certificate: The AD FS role service requires a server SSL/TLS certificate.
   b. Download Azure AD Connect.
   c. Execute Azure AD Connect.

Azure AD Connect is the one-stop shop for connecting your on-premises directories to Azure AD, whether you are evaluating, piloting, or in production. Azure AD Connect provides a single and unified wizard that streamlines the overall onboarding process for both directory synchronization (single or multiple directories) AND single sign-on (if desired). It automatically performs the following steps:

- download and setup of all the prerequisites
- download, setup and guided configuration of the synchronization with the Azure AD Sync tool
- activation of the sync in the Azure AD tenant
- setup and/or configuration of AD FS
Azure AD Connect replaces DirSync and Azure AD Sync. It leverages Azure AD Sync as the synchronization engine, and includes a rich set of sync and write-back capabilities:

- Enable your users to perform self-service password reset in the cloud with write-back to on-premises AD.
- Enable provisioning from the cloud with user write-back to on-premises AD.
- Enable write-back of “Groups in Office 365” to on-premises distribution groups in a forest with Exchange.
- Enable device write-back so that your on-premises access control policies enforced by AD FS can recognize devices that registered with Azure AD. This includes the recently announced support for Azure AD Join in Windows 10.

3. You will use Azure AD Connect to:

- Install prerequisites like the Azure Active Directory Module for Windows PowerShell (64-bit version) and Microsoft Online Services Sign-In Assistant.
- Install and configure the Azure AD Sync tool, as the sync engine, and enable directory synchronization in the customer’s Azure tenant.
- Configure either password sync or AD FS, depending on which sign-on option is preferred. Includes any required configuration in Azure.
- Verify everything is working.

4. After executing Azure AD Connect, you may wish to add scale or refine your options right away, or after some time has passed. Additional tasks you may want to configure include the following:

- **View the selected scenario.** This allows you to view data about your current configuration.
- **Customize synchronization options.** This allows you to add additional AD forests to your connection. In addition, you can specify or further refine sync options, including write-back options.
- **Enable Staging Mode.** The sync engine will no longer export any data to Azure AD and on-premises identity infrastructure.
5. The final step will be to verify your work. You’ll need to verify that your Office 365 user information is being synchronized on the Azure AD tenant through the Azure Management Portal. Then you will also verify that single sign-on is configured correctly.

At the end of this process, you should have seamless access to the signed-in user settings in Office 365. If not, you will need to troubleshoot the configuration to resolve the issue.

As we said at the beginning of this section, this is a very high-level look at the steps needed to configure single sign-on for Azure AD and Office 365 resources to make access simple and easy, increase security and compliance, and ease manageability of your applications, no matter where they are hosted.

For more details, please visit www.rackspace.com/Azure. Rackspace can also provide assistance with the planning, architecture and deployment of Azure AD and Office 365.

*This paper assumes that your on-premises AD is cloud ready.*
Common Mistakes When Moving to Azure ADFS

According to a THINKstrategies and INetU survey on enterprise migration to the cloud:

- 70 percent of respondents admitted they had to change their cloud design during the migration
- More than half made adjustments within the first six months
- 43 percent of the cloud projects failed or stalled
- Close to half required an increase in budget within six months

This highlights why a thoughtful, upfront strategy is essential when implementing any hybrid architecture. We see these issues every day with customers who may have started a project and run into complex issues they can’t solve. We also see it with customers who don’t have the right technical resources and don’t know where to begin. To make sure your project doesn’t become one of the statistics above, here are some common mistakes to avoid.

NOT GETTING HELP TO INTEGRATE AZURE ADFS

While integrating Azure ADFS is not an overwhelming task, it is complex and requires specific knowledge and skills. While you and your team are probably very knowledgeable about your own AD infrastructure and IT environment, how much experience do you have with Azure and Azure ADFS? Hiring an outside expert typically provides better value than spending time learning a new technology. It’s not uncommon to get in over your head with this integration and you can avoid this mistake by getting help at the beginning of your project.

TREATING A CLOUD DEPLOYMENT AS AN EXTENSION OF YOUR ON-PREMISES ENVIRONMENT

One of the biggest mistakes a company can make is to treat a new cloud addition the same way they would treat adding new hardware or storage. Deploying Azure adds an entirely different infrastructure and associated set of tools and processes to manage. It may require you to think about your environment differently. Without the proper knowledge and expertise to architect, deploy and manage this new environment, your organization may not realize the expected benefits or potential cost savings.
AVOIDING HYBRID SOLUTIONS

Companies without the right skills and expertise tend to avoid hybrid solutions; this can keep them locked into an expensive, outdated environment. A hybrid architecture leveraging the latest cloud computing technologies gives your business greater flexibility, greater cost control, and increases the options for your end users to access productivity tools whenever they need them, wherever they are.

POOR CLOUD DEPLOYMENT PLANNING

If you don’t take the time to fully understand your business needs and unique IT environment, the result can be a deployment that costs more than expected, is vulnerable to security risks, and doesn’t perform reliably and efficiently. Without cloud expertise and best practices, it’s difficult to put together the sound upfront planning necessary for a successful deployment. Again, your IT team knows your infrastructure, but do they have the experience needed to plan, architect and deploy a complex hybrid environment? You’ll want to be sure your plan takes into account your unique environment, as well as cloud and hybrid best practices.
Conclusion

The business environment has changed dramatically and your users are more demanding today than ever before. They need access to their applications wherever they are, in real time, so they can be more productive. You can provide your users with a seamless experience with single sign-on for all their applications, whether hosted on-premises or in the cloud. This will meet their mobility needs, increase productivity, and give your business a great foundation for easily adding new cloud-based productivity applications in the future. It also can help your organization meet security and regulatory requirements, as well as help simplify IT administration and reduce your help-desk load for password-based requests.

Make sure you take a thoughtful, strategic approach to this deployment to ensure you maximize the power of Azure. Start with a plan built on best practices and integration expertise to ensure a reliable, secure integration.

WHY RACKSPACE FOR MICROSOFT WORKLOADS?

Rackspace is the leader in the Gartner Magic Quadrant for Cloud Enabled Managed Hosting, an accolade we received for exceptional customer service on industry-leading technologies for over 15 years. We have teams of Microsoft Certified Professionals that can help you architect, design, deploy and manage your applications, whether they are on dedicated servers, private clouds, SaaS platforms like Office 365 or even Microsoft Azure itself.

We offer support on a number of technology stacks and applications, including the following:

- **Microsoft Azure**
- **Office 365**
- **Microsoft Cloud Platform on System Center and Windows Azure Pack**
- **Microsoft SQL Server**
- **Microsoft Exchange**
- **Microsoft Windows Server**
- **Microsoft SharePoint**
- **Skype for Business**
About Rackspace

Rackspace (NYSE: RAX), the #1 managed cloud company, helps businesses tap the power of cloud computing without the challenge and expense of managing complex IT infrastructure and application platforms on their own. Rackspace engineers deliver specialized expertise on top of leading technologies developed by OpenStack®, Microsoft®, VMware® and others, through a results-obsessed service known as Fanatical Support®.

GLOBAL OFFICES

Headquarters Rackspace, Inc.
1 Fanatical Place | Windcrest, Texas 78218 | 1-800-961-2888 | Intl: +1 210 312 4700
www.rackspace.com

UK Office
Rackspace Ltd.
5 Millington Road
Hyde Park Hayes
Middlesex, UB3 4AZ
Phone: 0800-988-0100
Intl: +44 (0)20 8734 2600
www.rackspace.co.uk

Benelux Office
Rackspace Benelux B.V.
Teleportboulevard 110
1043 EJ Amsterdam
Phone: 00800 8899 00 33
Intl: +31 (0)20 753 32 01
www.rackspace.nl

Hong Kong Office
9/F, Cambridge House, Taikoo Place
979 King’s Road,
Quarry Bay, Hong Kong
Sales: +852 3752 6488
Support +852 3752 6464
www.rackspace.com.hk

Australia Office
Rackspace Hosting Australia PTY LTD
Level 1
37 Pitt Street
Sydney, NSW 2000
Australia

© 2015 Rackspace US, Inc. All rights reserved.

This white paper is for informational purposes only. The information contained in this document represents the current view on the issues discussed as of the date of publication and is provided “AS IS.” RACKSPACE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS DOCUMENT AND RESERVES THE RIGHT TO MAKE CHANGES TO SPECIFICATIONS AND PRODUCT/SERVICES DESCRIPTION AT ANY TIME WITHOUT NOTICE. USERS MUST TAKE FULL RESPONSIBILITY FOR APPLICATION OF ANY SERVICES AND/OR PROCESSES MENTIONED HEREIN. EXCEPT AS SET FORTH IN RACKSPACE GENERAL TERMS AND CONDITIONS, CLOUD TERMS OF SERVICE AND/OR OTHER AGREEMENT YOU SIGN WITH RACKSPACE, RACKSPACE ASSUMES NO LIABILITY WHATSOEVER, AND DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO ITS SERVICES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

Except as expressly provided in any written license agreement from Rackspace, the furnishing of this document does not give you any license to patents, trademarks, copyrights, or other intellectual property.

Rackspace, Fanatical Support, and/or other Rackspace marks mentioned in this document are either registered service marks or service marks of Rackspace US, Inc. in the United States and/or other countries. OpenStack is either a registered trademark or trademark of OpenStack, LLC in the United States and/or other countries. Third-party trademarks and tradenames appearing in this document are the property of their respective owners. Such third-party trademarks have been printed in caps or initial caps and are used for referential purposes only. We do not intend our use or display of other companies’ tradenames, trademarks, or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.