SERVICE OVERVIEW

MANAGED IDENTITY AND ACCESS FOR MICROSOFT AZURE

rackspace®

NOVEMBER 28, 2017

TABLE OF CONTENTS

OVERVIEW

In today's organizational landscape, the proliferation of different types of accounts and identities —including cloud, mobile, ecommerce and social networks — has many IT organizations scrambling to determine how to prioritize their digital initiatives. As employees bring their personal devices to work and adopt readily available SaaS applications, maintaining control over their applications across corporate data centers and public cloud platforms has become a significant challenge.

If your company is struggling to simplify its identity and access management (IAM) environment, you're not alone. Making an IAM solution cloud-ready requires effective governance of user access and necessitates that you find and retain specialists with IAM expertise.

The Rackspace Managed Identity and Access service reduces the complexity of IAM through a managed Microsoft® Azure® Active Directory (AD) solution that extends an enterprise customer's Active Directory (Synchronized or Federated) into Azure Active Directory. Rackspace blends technology and human expertise to provide design best practices and improved security through ongoing architectural and procedural guidance. Our team of Microsoft-certified experts monitor, alert and respond to any issues that may arise, 24x7x365.

REGION AVAILABILITY

Managed Identity and Access for Microsoft Azure is available to Rackspace customers in the U.S. deploying Rackspace Fanatical Support for Microsoft Azure Aviator service level as at the publication date of this document, with the exception of Microsoft Azure Government regions (e.g., U.S. Gov Iowa) and China.

Some Azure regions are available only to customers with specific billing addresses in that region. Certain Azure services are designed to operate globally and do not require customers to specify a particular region when using the service.

OUR SERVICE LEVEL

Our Managed Identity and Access solution is a fully featured, cloud-based, enterprise-grade and fully managed identity and access solution within our portfolio of Fanatical Support for Microsoft Azure services.

Federated Identities are usernames that are synchronized from an on-premises Active Directory to Azure Active Directory for integration with SaaS-based applications. The federation servers act as an intermediary for username and password validation directly against the customer's on-premises Active Directory. This provides Single Sign-On functionality, which means that: (i) each user logs into his or her workstation and that login is used automatically for each Azure tenant integrated SaaS application (for internal users); or (ii) each user logs in once to any Azure tenant integrated SaaS application, and that login is used automatically when the user connects to any additional integrated application (for users external to the customer's on-premises network).

CONFIGURATION REQUIREMENTS

All virtual machine (VM) infrastructure to support the Managed Identity and Access Services must be hosted within the Microsoft Azure public cloud. The licenses for the software referenced in these terms are not included in the Managed Identity and Access Services and must be separately purchased by Customer. Certain features and services are only available to you if you have the requisite Microsoft license.

You must purchase at least the Rackspace Fanatical Support for Azure Aviator service level and may not downgrade to the Navigator service level at any time.

"Deployed Solution": Means the Azure Services, including the additional Aviator services detailed in the Guide.

SERVICE MATRIX

SERVICES	FEDERATED IDENTITY
MONITORING AND ALERTING	
Azure AD Connect Health Status and Alerting	✔
AD FS Health Status and Alerting	✔
AD FS Proxy Health Status and Alerting	✔
Azure Synchronized Identity Solution Performance Monitoring and Alerting	✔
Azure Federated Identity Solution Performance Monitoring and Alerting	✔
AD FS Windows Event Monitoring and Alerting	✔
SUPPORT SERVICES	
24x7x365 Azure Support Team	✔
Updates and Patching of Solution	✔
APPLICATION INTEGRATION	
Multi-Factor Authentication (Cloud Only)*	✔
Integration with SaaS Applications (SAML) - ADFS 3.0*	✔
USER AND GROUP SYNCHRONIZATION TO AZURE AD	
Provisioning and Deprovisioning Users via Azure AD Connect	✔
Provisioning and Deprovisioning Groups via Azure AD Connect	✔

*Additional Fees

EXPANDED SERVICES DESCRIPTION

MONITORING AND ALERTING

Rackspace will monitor and address alert notifications received for the following features:

AD Connect; Azure Active Directory Federation Services (ADFS); Web Application Proxy servers; Azure AD Domain Controller; and Azure AD Replication.

Rackspace will monitor performance of the Deployed Solution for the following key metrics: Azure ADFS and Web Application Proxy server health; critical alerts; Azure AD Connect server health. In addition, Rackspace will monitor: (i) synchronization of user accounts into Azure AD and (ii) key Windows event logs of the Deployed Solution. Rackspace will address relevant alert notifications and notify customer of any issues.

APPLICATION INTEGRATION

Rackspace will provide integration services to the following Security Assertion Markup Language (SAML) applications: Office 365, Salesforce, Box, Zendesk, Dropbox, Workday, GoToMeeting, Webex, Amazon Web Services, Slack, Pagerduty, Google Apps, Concur, DocuSign and Service Now. Rackspace is responsible for ensuring stable sign-on functionality to integrated applications. Customer is responsible for general application administration including, but not limited to, changing application settings and adding/removing users, groups or permissions. At your request, Rackspace may provide assistance with additional SAML applications that are not listed here for an added fee.

SUPPORT

Rackspace live support for the Managed Identity and Access infrastructure and applications is available 24x7x365, including weekends and holidays. You may submit all Support Services requests directly to Rackspace by telephone, chat or ticket at the contact information provided in your Services Description, provided that the service level agreement in Section 3 above shall only apply to requests submitted by ticket.

Software Component Patching: Rackspace will perform required updates and patching of the relevant software components of the Deployed Solution and schedule time with Customer to perform any necessary actions. Relevant software components that will be patched include: Azure AD Connect; Azure ADFS; Web Application Proxy servers; and Microsoft Multi-Factor Authentication (MFA) Services.

USER GROUP SYNCHRONIZATION TO AZURE AD

Rackspace engineers will integrate and synchronize your on-premises directories users and groups into Azure Active Directory using Azure AD Connect for your cloud applications such as SaaS, Office 365 and Azure Active Directory. This allows for quick onboarding/off-boarding of your on-premises directories for your cloud applications to provide seamless communication between directories and cloud applications with proactive notification of issues with synchronization for quick remediation.

APPENDIX 1

ROLES AND RESPONSIBILITIES

There are two parties involved in supporting your Managed Identity and Access Management of Microsoft Azure environment, specifically:

You, the customer (including any in-house IT resources)

Rackspace, our Microsoft Certified support experts

R - Responsible for activity

I - Informed of service

O - Optional Rackspace service (for an additional monthly fee)

P - Active Participant/Collaboration in activity/Event

SERVICE LEVEL ACTIVITIES	RACKSPACE	CUSTOMER
MANAGED IDENTITY SOFTWARE COMPONENT PATCHING		
Azure AD Connect	R	I
Active Directory Federation Services	R	I
Web Application Proxy Services	R	I
Microsoft Multi-Factor Authentication (MFA) Services	R	I
AZURE AD CONNECT MONITORING		
Monitoring the Microsoft Azure AD Sync Service	R	I
Monitoring the Azure AD Connect Health Sync Insight Service	R	I
Monitoring Azure AD Connect Health Sync Monitoring Service	R	I
Monitoring for the Following Errors in the Azure AD Connect Sync Tool · Synchronization errors · Duplicate account identification · Missing attributes identification · Rule violations identification	R	I
MICROSOFT ACTIVE DIRECTORY FEDERATION SERVICE MONITORING		
Monitor the Active Directory Federation Services	R	I
Monitor the Azure AD Connect Health AD FS Diagnostic Service	R	I
Monitor the Azure AD Connect Health AD FS Insight Service	R	I
Monitor the Azure AD Connect Health AD FS Monitoring Service	R	I
Monitor the Active Directory Federation Services Application	R	I
Monitor the Windows Internal Database Service	R	I
Monitor the Microsoft SQL Server for ADFS Database only	R	I
Monitor the availability of the Active Directory Federation Metadata XML from the ADFS service.	R	I
Monitor the Active Directory Federation Certificate Management rollover	R	I

APPENDIX 1

ROLES AND RESPONSIBILITIES (CONT.)

R - Responsible for activity

I - Informed of service

O - Optional Rackspace service (for an additional monthly fee)

P - Active Participant/Collaboration in activity/Event

SERVICE LEVEL ACTIVITIES	RACKSPACE	CUSTOMER
MICROSOFT WEB APPLICATION PROXY SERVERS MONITORING		
Monitor the Active Directory Federation Services	R	I
Monitor the Azure AD Connect Health AD FS Diagnostic Service	R	I
Monitor the Azure AD Connect Health AD FS Insight Service	R	I
Monitor the Azure AD Connect Health AD FS Monitoring Service	R	I
Monitor the Active Directory Federation Farm Connection	R	I
Monitor the AD FS Proxy Operation Status	R	I
Monitor the Web Application Proxy Core Operation Status	R	I
Monitor the Web Application Proxy Application	R	I
ACTIVE DIRECTORY FEDERATION SERVICES EVENT MONITORING		
ADFS Event Log Health Alerts	R	I
ADFS Usage Analytics · Total Requests Grouped by Type of Request · Total Failed Requests Grouped by Type of Request · Top 50 Users with Failed Username and Password	I	R
SAML APPLICATION INTEGRATION		
Office 365	R	I
Salesforce	R	I
Box.Net	R	I
ZenDesk	R	I
Dropbox	R	I
Workday	R	I
GoToMeeting	R	I
Webex	R	I
Amazon Web Services	R	I
Slack	R	I
PagerDuty	R	I
Google Apps	R	I
Concur	R	I

APPENDIX 1

ROLES AND RESPONSIBILITIES (CONT.)

R - Responsible for activity

I - Informed of service

O - Optional Rackspace service (for an additional monthly fee)

P - Active Participant/Collaboration in activity/Event

SERVICE LEVEL ACTIVITIES	RACKSPACE	CUSTOMER
SAML APPLICATION INTEGRATION (CONT.)		
DocuSign	R	I
ServiceNow	R	I
CUSTOMER OBLIGATIONS		
Active Directory Administration	I	R
Active Directory Object Creation and Management	I	R
DNS Management and Configuration	I	R
Active Directory Sites and Services Configuration and Management	I	R
Active Directory Certificate Authority	I	R
General Day-to-Day IT Administration Activities	I	R

APPENDIX 2

SUPPORTED AZURE SERVICES

Fanatical Support for Microsoft Azure customers can select from the Azure product groups listed below to build their hosted infrastructure.

NOTE: Some products listed below may be subject to different Terms, Conditions, Service Level Agreements and levels of support.

Comprehensive Support: Rackspace has substantial support expertise and has developed specific support services.

Reasonable Effort: Reasonable activities undertaken to resolve issues but with no guarantee of resolution. Escalation management to Microsoft where required. Over time, best-effort features may transition into comprehensive support.

Customers can deploy resources outside the list documented below; however, Rackspace does not represent expertise in these areas. Rackspace support can be engaged for special escalation scenarios; however, feedback and responsiveness may be limited.

CS - Comprehensive Support **RE** - Reasonable Effort

FEATURE	CS	RE
COMPUTE		
Virtual Machines	●	
Virtual Machine Scale Sets	●	
Cloud Services	●	
RemoteApp		●
Batch		●
MEDIA & CDN		
CDN		●
WEB & MOBILE		
Web Apps	●	
Logic Apps		●
WEB & MOBILE		
SQL Database	●	
Storage	●	
Import /Export	●	
Redis Cache		●
DocumentDB		●
ANALYTICS		
HDInsight		●
NETWORKING		
Virtual Network	●	
Traffic Manager	●	
ExpressRoute	●	
Azure DNS	●	
Load Balancer	●	
VPN Gateway	●	
Application Gateway	●	
DEVELOPER SERVICES		
Visual Studio Application Insights		●
Azure DevTest Labs		●
HYBRID INTEGRATION		
Service Bus	●	
Backup	●	
Site Recovery	●	
IDENTITY & ACCESS MANAGEMENT		
Azure Active Directory	●	
Multi-Factor Authentication	●	
Azure Active Directory Domain Services		●
MANAGEMENT		
Scheduler		●
Automation	●	
Log Analytics	●	
Key Vault	●	
Security Center		●
INTERNET OF THINGS (IOT)		
Notification Hubs		●
Machine Learning		●
Event Hubs		●
Stream Analytics		●
Azure IoT Hub		●

APPENDIX 3

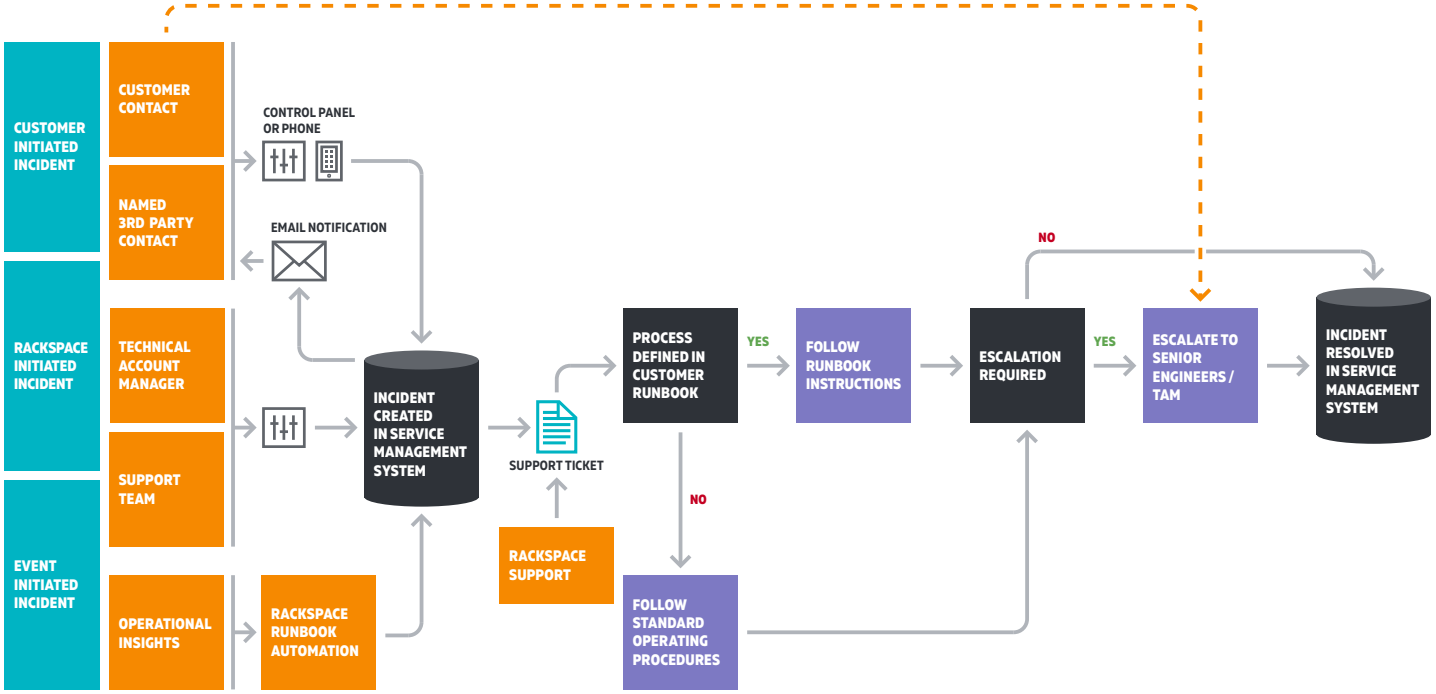
INCIDENT MANAGEMENT AND RESOLUTION PROCESS

Incident management refers to the management of incidents where restoration of the services is the primary objective. Rackspace endeavors to restore normal service as quickly as possible when a problem or incident occurs.

Rackspace will apply a consistent approach to all incidents, except where a specific approach is agreed upon with you in accordance with your account's custom runbook.

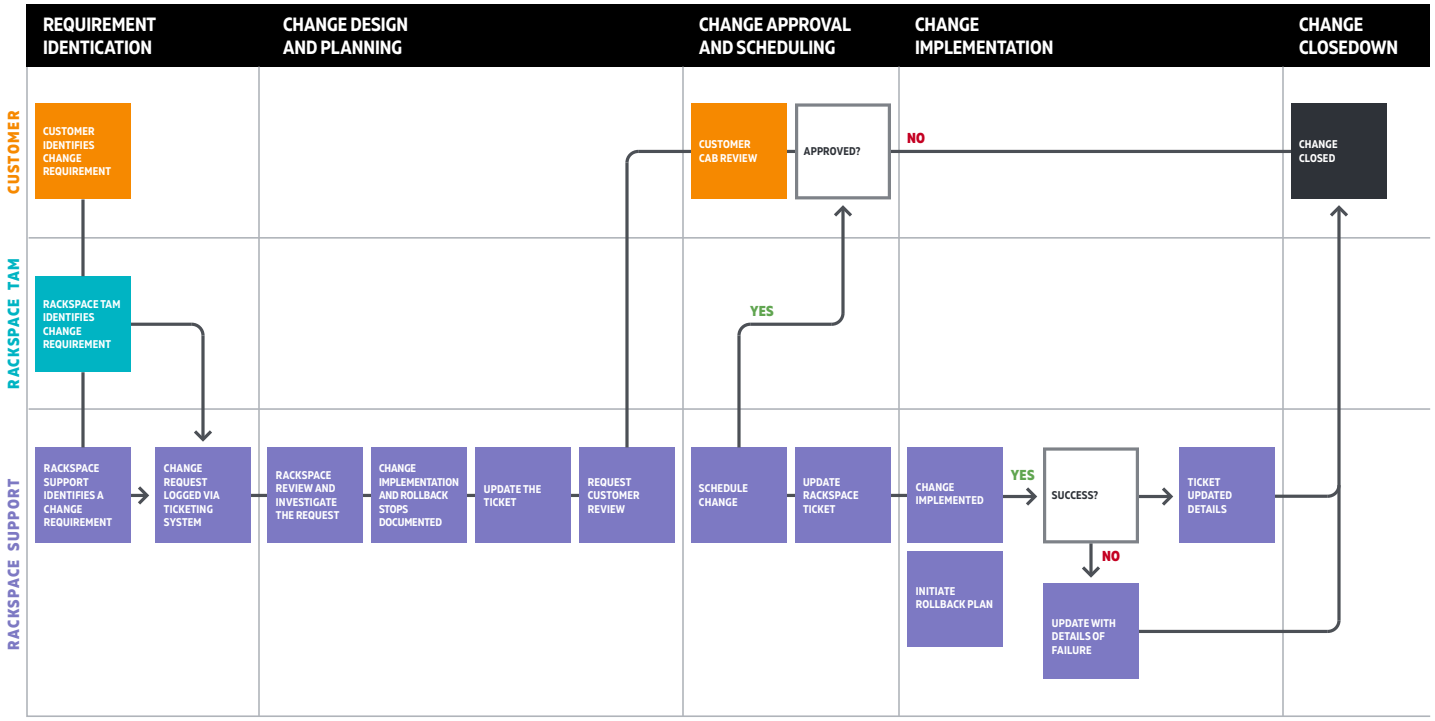
- Incidents can be initiated by either:
  - Named customer contacts
  - Rackspace
  - Event management tools (e.g., Azure Operational Insights)
- All incidents are logged in tickets accessible via the Fanatical Support for Microsoft Azure Control Panel. Rackspace Support teams will investigate the incident in accordance with the agreed service level once logged.
- The priority-level for tickets entered manually via the Fanatical Support for Microsoft Azure Control Panel is initially set to "Standard." Should you desire an escalation of priority, please phone your Rackspace Support team or your assigned TAM. Incidents logged with a specific priority will not be changed to another priority level without the agreement of all parties involved.
- Before investigation, Rackspace support will carefully review instructions on your account (documented via the Custom Runbook & Account Management guidelines).
- Rackspace will collaborate with you as well as with any third parties you nominate as technical contacts through the Fanatical Support for Microsoft Azure Control Panel to resolve the incident.
- At all times you will have visibility into which support engineer is working on the incident.
- The Rackspace Support teams will communicate regularly with you throughout the incident, detailing their findings and any actions taken.
- If a support engineer is unable resolve an incident, they may escalate the incident at any time until resolution is achieved. This escalation may be Hierarchical (e.g., to a more senior engineer or the Technical Account Manager) or it may be Functional (e.g., involving specialized technical expertise from other functional groups or Microsoft).
- The action required to resolve an incident will vary depending on investigative findings. In some cases, a proposed solution may be complex or cause additional disruptive impact to your Azure environments. In these cases, the incident will be handled as a change through the Rackspace change management process, and you will be consulted to determine the time window during which the solution or change may be implemented. Alternatively, you may be required to take action to resolve the incident, which will be communicated should such need occur.
- An incident is deemed closed when you confirm that it is resolved. This is achieved through the incident ticket being set to "Solved" status. You may close the ticket or reopen it if you believe that further work is required.

INCIDENT MANAGEMENT AND RESOLUTION PROCESS (CONT.)



APPENDIX 4

CHANGE MANAGEMENT PROCESS



APPENDIX 5

SUBSCRIPTION MANAGEMENT

CO-ADMINISTRATOR ACCESS

To enable full support for your Azure subscription, Rackspace requires co-administrator access. Depending on how you acquire your Azure subscription, this may require you to add Rackspace as a co-administrator directly.

Several of our support offerings require that the co-administrator account be an "organizational account" rather than a "Microsoft account." If you are unable or unwilling to provide an organizational account for co-administration use, some support services may not be available or may be limited in scope.

The co-administration account credentials will be stored within a secure password repository at Rackspace and utilized by our technicians during support, troubleshooting, deployment and other similar activities.

AZURE ACTIVE DIRECTORY SERVICE PRINCIPAL

Rackspace must deploy an Azure Active Directory Service Principal. Service Principals in Azure AD are used to assign permission levels to securable resources within the scope of a particular Azure subscription. When associated with an Azure AD Application, they can be used to enable programmatic access to Azure resources within that subscription.

When Fanatical Support for Microsoft Azure is enabled for a subscription, a Service Principal is created and granted reader access to the resources within that subscription. This allows Rackspace automation systems to interact with the subscription to facilitate management and integration tasks such as portal views and resources tracking.

Service Principals are granted a Role-Based Access Control (RBAC) security group. This allows a granular assignment of permissions to specific resources and access levels for the service principal. When a code-flow or programmatic access model is used with a Service Principal, a key is used to authenticate against Azure AD. This key is easily expired in case it ever becomes compromised or if access via the Service Principal should be revoked.

ABOUT RACKSPACE

Rackspace, the #1 managed cloud company, helps businesses tap the power of cloud computing without the complexity and cost of managing it on their own. Rackspace engineers deliver specialized expertise, easy-to-use tools, and Fanatical Support® for leading technologies developed by AWS, Google, Microsoft, OpenStack, VMware and others. The company serves customers in 150 countries, including more than half of the FORTUNE 100. Rackspace is a leader in the 2017 Gartner Magic Quadrant for Public Cloud Infrastructure Managed Service Providers, Worldwide, and has been honored by Fortune, Forbes and others as one of the best companies to work for.

Learn more at www.rackspace.com or call us at **1-800-961-2888**.

NOVEMBER 28, 2017

AZU-CSO-Managed_Identity_and_Access-9194

rackspace®