Kony Cloud

Architecture and Security Overview

Table of Contents

kony ❋

Overview

The Kony Cloud is comprised of the following cloud types, each of which comes with a collection of cloud services and functionality. Each instance of a Kony Cloud environment is production-grade infrastructure, highly available across two data centers, and automatically scales based on user traffic. Each of the various clouds is offered as a free trial, typically for 90 days. In the case of a trial cloud, the environment is not highly available or auto-scaling and not intended for production use.

Visualization Cloud – Quickly define, prototype, design, and develop stunning multi-channel apps.

Development Cloud – Develop and deploy multi-channel apps on a single code base.

Management Cloud – Manage your apps, devices and content with best-in-class enterprise mobility management (EMM).

Kony Cloud functionality

Each Kony Cloud offering comes with a set of cloud services to enable the following associated functionality.

Kony Visualization Cloud comprises Kony Visualizer, a downloadable client tool, and a set of app prototype sharing and collaboration services in the cloud. These services allow you to publish an app prototype to the cloud so users can view the app on their mobile devices using the Kony Functional Preview app.

Kony Development Cloud offers the following services to support the development and runtime components required to operate a production-grade multi-channel application:

- App Services provide a dedicated, single-tenant instantiation of the Kony Middleware Server platform. This runs the mobile web version of the application and integration services that are used by both the native version of the app and the mobile web version of the app.

- Messaging Services is a multi-tenant service that provides a single console to manage your customer messaging via your deployed app. Each time an instance of your native app is downloaded and installed on a device, that device registers with Messaging Services, including the user's preference for receiving push notifications. Push notifications can then be sent to users based on segmentation or geolocation.

- Sync Services provides a dedicated, single-tenant instantiation of the Kony Sync platform. It enables an app to keep a local copy of a database or web service-enabled system on a native device for offline app access. Any changes on the local device or the back-end data source are synchronized via the cloud service. Conflict resolution rules and administration is managed with an admin console.

Kony Management Cloud is a multi-tenant device management and app management service for enterprises. Employees start by registering their devices with the system and gain access to corporate apps through an enterprise app store. Administrators can manage device security policies and app-specific security polices at a user and group level. If a customer already has an existing device management and/or app management solution, they can still use the other Kony cloud services with their existing MDM or MAM provider.

Registration

To use the Kony Cloud, users must create a Kony user account by submitting a registration request online at either http://kony.com or https://manage.kony.com/registration. The user's email address will serve as their login ID and they will be required to set a password after clicking an account activation link sent via email.

Authentication

A user will use their Kony user account credentials to authenticate in to the following components (all cloud services are secured using OAuth 1.0 user authentication.)

- Kony Cloud Portal – The Kony Cloud Portal provides product information, downloads, documentation, and tutorials related to the Kony Cloud offering.

- Kony Community – The Kony Community allows customers to connect with other Kony customers and with the Kony Support team to discuss questions or issues regarding the products and services offered on the Kony Cloud.

- Kony Studio –Kony Studio is a development tool for creating cross-platform multi-channel apps and deploying them to the Kony Cloud. It is available for download on the Kony Cloud Portal.

- Kony Cloud Console – The Kony Cloud Console allows customers to create and manage their cloud services. This includes creating new cloud environments, inviting other users to use their cloud services, managing their billing and payment, and accessing various standard cloud reports on the usage of their cloud services.

Authorization and role provisioning

Owner authorization

Each user who registers for a Kony user account has "owner" rights on their account. The owner is authorized to create one or more clouds within their account. Each cloud can contain one or all of the following features:

- Visualization Cloud
  - Kony Visualizer (downloadable app design tool)
  - Visualization Management Console

- Development Cloud – Consumer Apps
  - App Services
  - Messaging Services

- Development Cloud – Enterprise Apps
  - App Services
  - Messaging Services
  - Management Services (Kony EMM)
  - Sync Services (Optional add-on)

- Management Cloud
  - Management Services (Kony EMM)

Each feature has its own independent administration console that can be accessed from the Kony Account Management web application or directly using a custom URL. The owner uses the Kony user account credentials to authenticate the selected cloud features. The administration console authorizes the owner via integration with the Kony accounts platform. The account owner is always authorized to the administration console of each feature as an administrator with full control.

Privileged user authorization

The account owner can invite other users to join the account and grant access to each of the cloud features. For users with an existing Kony user account, the owner can invite them to the account using their email address and then grant predefined roles for that user at the cloud feature level.

For users that do not have a Kony user account, the owner can invite them to the account in the same manner by entering their email address and granting predefined roles for those users at the cloud feature level. Because they do not have an existing account, they will receive an email to activate their Kony user account.

The invited users will see the clouds to which they have privileged user access after logging in to the Kony Cloud Portal and accessing the Kony Cloud Console.

Kony Cloud API

Each account management function available in the Kony Cloud Console and each cloud deployment action available in Kony Studio is also exposed as an OAuth 1.0 protected REST API. An OAuth access token can be acquired from the authentication service and used to execute other APIs on behalf of the user. These Kony Cloud APIs enforce authentication and authorization.

Data storage, collection, and archiving (retention)

Overview

Each cloud environment tracks usage data for reporting and license management. The following information is collected by each of the cloud services. The information is retained in the active data warehouse for 18 months and archived for a total of seven years.

Customer rights

The customer retains all rights to any and all data collected from the cloud services they purchase. This data can be accessed at any time online using the Kony Cloud Console to view a set of standard reports. Additionally, the customer may request via a support ticket to export all data related to their cloud services to a CSV file. Such requests are limited to once per month and the CSV file will be hosted on a secure FTP site for a period of seven days for the customer to download. Customers may request a final data export upon cancelation of service for up to three months from the day of cancelation.

Kony Middleware and App Services

The Kony Middleware and App Services within the Kony Cloud host the web application and the integration services components of a deployed application. Requests are made from the end-user device to the cloud over a secure SSL connection. Any additional data required for the request is then retrieved by the cloud services from the customer's back-end systems outside the cloud environment. This data is also secured over an SSL connection. *No customer data or user-supplied data is retained within the Kony Cloud for Kony Middleware and App Services.* All data remains within the customer's enterprise except when in transit through the cloud via secure SSL connections. Although there is no enterprise or customer-specific data stored in the cloud, usage and analytical information is collected for billing and reporting.

For each request from an end-user app, the following information is published to a message queue and stored in a Kony data warehouse for reporting and billing purposes.

Field	Description
kaid	KonyAccountID – This is a value generated by Kony to represent the customer's Kony account.
eid	EnvironmentID – This is a value generated by Kony to uniquely identify this cloud environment within the customer's account.
awsid	Amazon Account ID – This value is an Amazon ID to identify the Amazon AWS subaccount number that the customer has been assigned.
ebid	Elastic Beanstalk ID - This will be a unique ID that directly correlates to an Amazon AWS ID for the beanstalk.
did	Device ID – A unique identifier for a device exposed by the underlying SDKs. For SPA , DesktopWeb, and MobileWeb it will be empty.
aid	App ID - A unique identification given to the app by the developer.
aname	App Name - A friendly name for the app given by the app developer.
aver	App Version – App version number.
rid	RequestID - A unique ID generated for this request.

Field	Description
sid	Session ID - A unique ID for this session. All requests to the server executed within the same session will have the same session ID.
chnl	Channel - [mobile, tablet, desktop] – Future applicability.
atype	App Type - [Native, MixedMode, Hybrid, SPA, MobileWeb] – Future applicability.
plat	Platform - [iOS, Android, Blackberry, Windows, J2ME] – Future applicability.
tdur	Total Duration - A numeric value in milliseconds calculated by the server of how long it took to service the request from the time it reached the server from the client to the time the server sent a response to the client. This includes any time taken to call out to other third party services.
idur	Internal Duration - A numeric value in milliseconds calculated by the server of how long it took to service the request (tdur) minus the time waiting on any external calls to other third party services.
predur	Preprocessor Duration – A numeric value in milliseconds that denotes time taken to execute any custom pre-processor logic for the service.
prsdur	Parse Duration – A numeric value in milliseconds that denotes time taken to execute any parsing logic on response including Xpath on XML or HTML on web scraping for the service.
exdur	External Duration – A numeric value in milliseconds that denotes time taken to execute any external calls for the service.
Postdur	Postprocessing Duration – A numeric value in milliseconds that denotes time take to execute any custom post processing logic for the service.
rip	Remote IP - The remote IP from the HTTP header. Should be the public-facing IP of the client.
ts	Time Stamp - A string representation of the server date and time when the request was received including time zone of the request.
dm	Device Model - The device model such as iPhone 5. This is a string that comes from the device and could be anything. This will be blank in the case of AppType=SPA or MobileWeb.
os	Operating System - Operating system version such as 5.1.2. It is some string value from the OS. This will be blank in the case of AppType=SPA or MobileWeb.
ua	User Agent - The Useragent of the client browser. This will be only populated for AppType=SPA or MobileWeb.
svcid	Service ID - A unique ID of the service the client called.
fid	Form ID - A unique ID of the mobile web or SPA web page the user accessed. This is only populated for AppType=SPA or MobileWeb.
stype	Session Type -- [B2C, B2E] -- Identifies if the user's app came from a licensed B2E source such as MAM.
Kuid	KonyUserID – Optional string inserted by the application typically to denote userID.
country	Country Code – data derived from remote IP with an IP to geo location mapping table, to give a representation of geo location of usage for analytics.
city	City name – data derived from remote IP with an IP to geo location mapping table, to give a representation of geo location of usage for analytics.
region	Region Code – data derived from remote IP with an IP to geo location mapping table, to give a representation of geo location of usage for analytics.
zip	Postal Code – data derived from remote IP with an IP to geo location mapping table, to give a representation of geo location of usage for analytics.
lat	Latitude – data derived from remote IP with an IP to geo location mapping table, to give a representation of geo location of usage for analytics.
lon	Longitude – data derived from remote IP with an IP to geo location mapping table, to give a representation of geo location of usage for analytics.
dmacd	Metro Code – data derived from remote IP with an IP to geo location mapping table when available, to give a representation of geo location of usage for analytics.
areacd	Area Code – data derived from remote IP with an IP to geo location mapping table, to give a representation of geo location of usage for analytics.

Kony enterprise mobility management

The Kony EMM solution publishes the following information daily to a message queue that is stored in a Kony data warehouse for reporting and billing purposes.

Field	Description
kaid	KonyAccountID – This is a value generated by Kony to represent the customer's Kony account.
eid	EnvironmentID – This is a value generated by Kony to uniquely identify this cloud environment within the customer's account.
awsid	Amazon Account ID – This value is an Amazon ID to identify the Amazon AWS subaccount number that the customer has been assigned.
dt	Date - A string representation of the server date when the request was received.
ldusr	Loaded Users – Total user accounts available for EMM activation from the connected enterprise LDAP or Active Directory.
mamusr	MAM Users – Total number of users that have downloaded that MAM App Manager.
mdmusr	MDM Users – Total number of users that are actively managed via MDM.
mcmusr	MCM Users – Total number of users that have downloaded the MCM Content Locker.
emmusr	EMM Users – Total number of users of the EMM.
mdmdev	MDM Devices – Total number of devices that are actively managed via MDM as a delimited string identifying device platform breakdown (i.e. iOS_Phone=XX|iOS_Tablet=XX|Android_Phone=XX|Android_Tablet=XX|etc).
mcmdev	MCM Devices – Total number of devices that have downloaded the MCM Content Locker as a delimited string identifying device platform breakdown
mamapp	(i.e. iOS_Phone=XX|iOS_Tablet=XX|Android_Phone=XX|Android_Tablet=XX|etc).
plat	MAM Apps – Total number of apps loaded in MAM as a delimited string identifying device platform breakdown (i.e. iOS_Phone=XX|iOS_Tablet=XX|Android_Phone=XX|Android_Tablet=XX|etc).
chnl	Platform - [iOS, Android, BlackBerry, Windows, J2ME] – Could be new values in future.
lon	Channel - [mobile, tablet, desktop] – Could be new values in the future.
dmacd	Metro Code – data derived from remote IP with an IP to geo location mapping table when available, to give a representation of geo location of usage for analytics.
areacd	Area Code – data derived from remote IP with an IP to geo location mapping table, to give a representation of geo location of usage for analytics.

Kony Sync

Kony Sync operates in two data transfer modes. "Over the air sync," or OTA, provides a direct sync between the enterprise data source and the end-user devices. In this scenario, no customer data is retained in the cloud. "Persistent sync" keeps a local copy of the data in the cloud. In this scenario, it is possible that customer data is stored in the cloud at rest depending on what data is selected to use persistent sync.

Kony Sync publishes the following information daily to a message queue that is stored in a Kony data warehouse for reporting and billing purposes

Field	Description
kaid	KonyAccountID – This is a value generated by Kony to represent the customer's Kony account.
eid	EnvironmentID – This is a value generated by Kony to uniquely identify this cloud environment within the customer's account.
awsid	Amazon Account ID – This value is an Amazon ID to identify the Amazon AWS subaccount number that the customer has been assigned.

Field	Description
ebid	Elastic Beanstalk ID - This will be a unique ID that directly correlates to an Amazon AWS ID for the beanstalk.
dt	Date - A string representation of the server date when the request was received.
ldusr	Loaded Users – Total user accounts available for EMM activation from the connected enterprise LDAP or Active Directory.
ausr	Active Users – Total number of users that have connected to the Sync server.
adev	Active Devices – Total number of devices that have connected to the Sync server as a delimited string identifying device platform breakdown
appid	(i.e. iOS_Phone=XX|iOS_Tablet=XX|Android_Phone=XX|Android_Tablet=XX|etc).
syncses	Application Identifier – A string that uniquely identifies the application that the data in this message describes. The remaining message fields are calculated only for this AppID.
con	Sync Sessions – Total number of Sync sessions for the day (or period of time since the last posted usage message).
data	Sync Conflicts – Total number of Sync conflicts for the day (or period of time since the last posted usage message).
plat	Data – Total persistent data storage size in GB per app in the format (<AppID>=XX|<AppID>=YY).
chnl	Platform - [iOS, Android, BlackBerry, Windows, J2ME] – Could be new values in future.

Kony Messaging Service

The Kony Messaging Service helps deliver notifications and alerts to all channels using a single interface. It also provides campaign management capabilities to target specific user segments or geo-locations for messages.

Field	Description
kaid	KonyAccountID – This is a value generated by Kony to represent the customer's Kony account.
eid	EnvironmentID – This is a value generated by Kony to uniquely identify this cloud environment within the customer's account.
dt	Date – Date when the message was generated. These messages are generated once a day for every environment.
appid	Application Identifier – This field is created by the developer to uniquely identify the application for which the notification is sent.
susr	Subscribed Users – Total number of users that have allowed the receipt of push notifications from this app.
sdev	Subscribed Devices – Total number of devices that have allowed the receipt of push notifications from this app.
tdev	Total Devices – Total device IDs received and associated to this app regardless of their push notification acceptance status (includes active and inactive devices).
smsg	Sent Messages – Total number of messages sent to the app across all users/devices for the current day.
omsg	Opened Messages – Total number of messages opened by the user across all users/devices for the current day.
plat	Platform - [iOS, Android, BlackBerry, Windows, J2ME) – Could be new values in future.
chnl	Channel - [mobile, tablet, desktop] – Could be new values in the future.
susrdev	Subscribed Users – Total number of users that have allowed the receipt of push notifications from this app broken down by platform and channel.
smsgdev	Sent Message Detail -- The total number of sent messages from the smsg value above, but broken out by channel and platform.
omsgdev	Opened Message Detail -- The total number of opened messages from the omsg value above, but broken out by channel and platform.

Visualization Service

The Visualization Service stores customer prototypes and related user notes within Amazon's S3 file storage. It also provides the ability to share a project between Visualizer and Kony Studio. Unlike the other services, the Kony Cloud captures no additional data for reporting and analytics except for running a daily report of the number of shared prototypes and projects for the billing system.

Kony access to customer data

The Kony Support team does not have direct system access to the production systems that may contain customer-specific data. If a customer needs the Kony Support team to investigate an issue related to a system that contains customer data, they must explicitly grant access to the support team by placing a comment in the associated support ticket, and temporarily inviting "support.kony.com" to their Kony Cloud account using the Cloud Management Console. The Kony Corporate Security group will first verify this access grant by viewing the support ticket. Access to these systems is protected with dual passwords requiring both the Kony Support management team and a Kony Corporate Security officer to provide their individual passwords before these systems can be accessed. Passwords are rotated once the support ticket is closed or the customer access grant is revoked in the ticket.
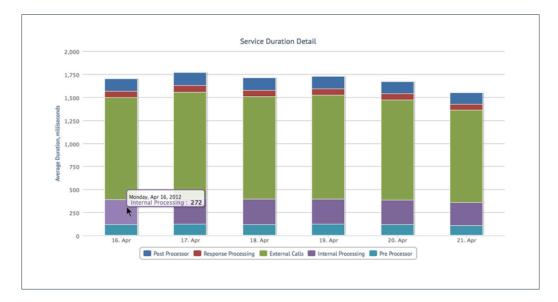
Monitoring cloud performance

The collection of the data described in the "Data storage, collection, and archiving" section above enables the cloud administrator to review the performance of their app services hosted on the cloud using standard cloud reports.

The duration of each service call to the cloud is tracked across five phases:

- Preprocessor Phase – The developer can create custom Java code that executes once the request is received by the cloud, but before any outbound service calls are made. This is typically used to make a decision on what service to call or to perform data validation on the request.

- External Calls Phase – This is the phase of the cloud service that makes calls to external systems hosted outside the cloud.

- Response Processing Phase – Once a response is received from an external service, the response has to be parsed. This is typically a very fast operation, but in some cases, external services return very large and complex responses that impact the performance of the service.

- Postprocessor Phase – The developer can create custom Java code that executes once the external calls return their response. This is typically used to post-process the data before it is returned to the device or determine if additional service calls should be made to retrieve additional data.

- Internal Processing Phase – The remaining time taken to execute a service call outside the four phases described above is considered internal server processing. This includes the work performed by the cloud framework to execute the service call and orchestrate across the various phases of the service call.

The following report shows an example of how a cloud administrator can review the duration of a specific service broken down by the five phases of the service call. The specific value of each segment can be viewed by positioning the mouse over the segment.

Capacity and auto-scaling

The resources deployed on the Kony Cloud are in an active-active configuration that is distributed across two Amazon AWS Availability Zones located in Ashburn, VA. These systems are engineered to automatically add server capacity based on an increase in user traffic and load. There is no additional cost for any additional server capacity added due to increased user load.

App Services and Sync Services are deployed as single-tenant environments dedicated to a specific customer. The initial configuration of a base environment supports between 20 and 40 transactions per second (TPS) depending on the individual characteristics of the app(s) deployed.

Customers may open a support ticket and request that a specific cloud environment is manually scaled up to support an anticipated sharp increase in user traffic to ensure optimal system performance during the spike. A minimum of seven days' notice is required to manually scale up an environment. The environment can be scaled up as much as seven days in advance to provide additional time for customer verification. Kony will scale the environment back down after notifying the customer if the user traffic does not justify the environment size for seven straight business days.

Event monitoring

Informational logging within the Kony PaaS infrastructure is pushed into a centralized logging repository. Event monitoring and reporting for certain security alerts and security compliance reporting are configured and executed against the logging repository.

Penetration testing

Each of the cloud services available on the Kony Cloud has completed at least one round of security penetration testing as of December 1, 2013. These security tests are repeated continuously and include at least one round of testing on each cloud service per quarter.

Firewall policy management

The Kony Cloud infrastructure components and each Kony Cloud customer environment are secured using Amazon AWS security groups that block all incoming IP traffic except ports explicitly opened and configured for specific IPs or IP ranges.

Configuration and software patch management

Kony Studio

Each Kony application is developed within Kony Studio. The version of Kony Studio is managed via an Eclipse update site that hosts all the Kony Eclipse plugins that enable Kony IDE functionality. The Kony Studio user will be automatically notified within Kony Studio if an update is available. The Kony Studio user can accept this update and install it at any time, but is not forced to immediately take upgrades. Kony only maintains support for two major versions of Kony Studio. As of December 2013, Kony Studio 5.0 and 5.5 are officially supported.

App Services - Kony Middleware and deployed apps

When an application is compiled using the ant build scripts within Kony Studio, the developer can manage the version of the Kony platform the app should run on when it is deployed to the Kony Cloud environment from within Kony Studio. During deployment, the application WAR will be updated with the Kony Platform libraries that match the version specified during compile time. This provides complete control to the developer over Kony Platform version management. Kony will maintain the various versions of the Kony Platform within the Kony Cloud infrastructure.

Any critical patches to Kony Platform for deployed apps will be posted on the Kony Cloud Portal and communicated to customers via email. A developer can manage when they update their application by executing a publish command that will redeploy the application and receive the updated Kony Platform libraries with the latest patches.

Since App Services is offered as a dedicated instance to each cloud (single tenant), the customer can manage the timing of maintenance windows and upgrades. In the case of apps built on

Kony, the customer must update Kony Studio to the desired version, recompile the app, and deploy the new app version to the cloud. Kony typically releases two major versions each year and will maintain support for the last two major versions released.

App Services also comes with an independent administrative console. The upgrade of this component is managed by the Kony Support team but is an independent application from the Kony built app.

Kony Visualization, Messaging, Management (EMM) and Sync Services

Kony Visualization, Messaging, Management, and Sync environments will be kept current during a monthly release patch schedule. Maintenance periods that have any impact to environment performance or availability will be scheduled and communicated to customers via email. In most cases, patches and upgrades will be applied without any service impact.

In the case of Sync Services, which is single tenant, the customer will have at least four weeks of notice of any required maintenance and at least a two week window to schedule their update based on their preferred maintenance time. These updates can be applied to different cloud environments at different times. This allows the customer to apply the maintenance in one cloud environment used for regression testing before applying to a different cloud environment used for production.

Physical security

The Kony Cloud infrastructure is hosted within Amazon's AWS data center infrastructure and protected by their physical security polices. These undisclosed data center locations are protected with military-grade external physical security. All personnel entering the facility must present proper identification and pass two-factor authentication at each entry point, which is video recorded, monitored, logged, and audited. Any visitors or contractors must be registered and are escorted by authorized staff at all times.

Tours or inspections of the data center facilities are not permitted by Amazon AWS, but an overview of their security can be reviewed on their website at http://aws.amazon.com/security/ and their latest security compliance reports can be viewed on their website at http://aws.amazon.com/compliance/.

Data disposal

Customer data resides in the following locations and is disposed in the methods outlined:

Kony Accounts Platform – Users with Kony user accounts have their account information stored in Kony's secure LDAP within the Kony Accounts Platform. A user can open a support ticket to have their information removed from the underlying LDAP. The Kony Support team will remove the user's data by issuing a delete command against the Kony Accounts Platform and underlying LDAP. The physical storage of the Kony LDAP is hosted within Amazon AWS data center facilities.

Cloud environments – Upon deletion of a cloud feature or an entire cloud environment, the associated servers and storage are "terminated" via Amazon AWS standard processes. This includes automatically wiping every block of associated storage per their posted security policies.

Kony Reporting Platform – 18 months of server usage data is retained within the Kony Reporting Platform data warehouse to support reporting and billing. This information is also replicated to the Kony billing partner, Aria, for managing invoicing and online payments. The data is purged from these systems after 18 months using a data deletion query in Amazon's RedShift product for the data warehouse and issuing a purge command within Aria's billing platform. Any customer can request that their data be purged from the Kony Reporting Platform via the support ticketing system and the signature on a request form from an official officer of the customer.

Kony usage backup retention – Kony will maintain seven years of compressed raw usage data within Kony-owned storage inside a RackSpace data center. The exact mechanism for disposing of this data is undefined at this time, but is expected to utilize a secure erase method on the SAN storage component.

High availability

High availability is achieved on the Kony Cloud by running a minimum of two instances of every system component that runs a customer cloud service or application. These redundant systems are spread across two Amazon data centers referred to as "AWS Availability Zones." The system utilizes the two data centers in active-active mode, which means the default runtime configuration is to evenly distribute the user traffic between both data centers. In the event of a data center outage, 100 percent of the user traffic will be routed to the remaining data center automatically by the Amazon AWS infrastructure capabilities. Additionally, within each data center, components are highly available by either running a minimum of two instances of the component or placing a single instance in an Amazon AWS scalability group with a minimum size of 1 that effectively immediately replaces the system component with a new instance if it becomes unresponsive.

Disaster recovery

The Kony Cloud infrastructure is hosted in Amazon's US-EAST-1 region located in Ashburn, Virginia across a minimum of two independent data centers. Instead of operating in a single active data center with a passive disaster recovery data center, the Kony Cloud operates across two active data center to achieve immediate recovery in the event of a total data center loss.

Customers will soon have the option, targeted for late Q2 2014, to pick additional Amazon AWS regions outside of the Virginia location when provisioning cloud services. In addition to selecting which region the cloud runs in, this will provide the opportunity to purchase a backup cloud environment for app deployments. The second cloud in a different region could serve as a dark disaster recover environment. In the event of two simultaneous data center outages in

the first region, app traffic could be re-routed to the backup region by changing a DNS entry.

This multi-region disaster recover approach applies to both App Services (Kony Server) and Sync Services (Kony Sync Server) since these are single-tenant offerings dedicated to the customer. The other services are multi-tenant and managed by Kony to be highly available even in the event of a disaster.

In the case of creating two independent clouds in different regions for disaster recover, the production user traffic would only route to the production cloud environment and no traffic would route to the disaster recover cloud environment under normal operating conditions.

In the case of App Services, the customer would be required to deploy their app to both environments and would have access to test their app in both environments. No data is persisted by App Services in the cloud, so no data replication would occur between the production and disaster recover cloud environment for App Services.

In the case of Sync Services, a database does exist and contains meta-data to manage the sync sessions and an optional configuration to persist a cache of the enterprise data for higher performance and availability. The meta-data and persistent data will be replicated between the production and disaster recover cloud environment in the case of Sync Services.

An automatic failover to the disaster recovery environment will occur if the production cloud is completely unresponsive for 5 minutes (configurable). The customer will be automatically notified by the system in the event of a DR failover. A fall back to the production cloud environment will be a manual process coordinated between the customer and the Kony support team. Customers can schedule two disaster recovery tests per year where the Kony support team can simulate a complete failure and monitor the recover.

Once a failover is triggered, the DNS entry for the cloud environment will be automatically reconfigured to point app traffic to the DR environment. The DNS change will only take effect on the device when the current DNS name cache on the device expires. This on-device DNS cache is configurable using the time-to-live (TTL) setting in DNS. The default will be set to 5 minutes, but a customer can request a different setting.

Service uptime commitment

The service uptime of the Kony Cloud infrastructure is dependent on the service level agreements provided by Amazon of the core infrastructure components that affect the availability of the Kony Cloud services. The following Amazon SLAs are used to calculate the Kony Cloud uptime percentage of 99.95% monthly.

http://aws.amazon.com/ec2-sla/ (99.95%)
http://aws.amazon.com/rds-sla/ (99.95%)
http://aws.amazon.com/route53/sla/ (100%)
http://aws.amazon.com/s3-sla/ (99.9%)

Note that the S3 uptime percentage of 99.9% is below the Kony Cloud uptime percentage of 99.95%. This is because the Kony Cloud services can continue servicing requests during an S3 outage. The deployment of new apps or services to the Kony Cloud by the customer may be affected during an outage of S3.

For more information on the service level agreement for Kony Cloud, please visit http://www.kony.com/service-level-agreement.

Enterprise data center connectivity and bandwidth

The services available on Kony Cloud typically require connectivity to data and services in an enterprise data center operated by the customer. In most cases, this data connection will route across the public internet and can be secured using a VPN and/or SSL connections. Establishing this connection can also be accomplished using Amazon AWS's Direct Connect capability at an additional charge. This capability provides a private and dedicated network circuit between the Amazon data center and the enterprise data center in partnership with the ISP providing connectivity to the enterprise data center.

Customers can perform basic bandwidth testing between their enterprise data center and the AWS data center hosting the Kony Cloud by accessing our FTP server hosted in the same location.

For download testing, access ftp-download.kony.com as anonymous and download the following file:

/installer/studio/latest/KonyStudioSetup_x64.exe

For upload testing, please contact support@kony.com to request a user account to write files to the FTP temporarily to test upload speeds.

Using Kony Cloud for non-production and on-premises for production

All Kony Cloud environments are production grade, offering high availability across two physically separate data centers and auto-scaling to add capacity in response to increased user traffic. The only exception to this is the trial environments that are single data center and do not automatically scale.

Many customers will choose to utilize several cloud environments to host their non-production testing environments. In these cases, the cloud environments used for testing are no different from the production clouds. They only differ in how the customer is using them.

Customers may also prefer to use the Kony Cloud only for non-production environments and utilize an on-premises environment for production. The following links provide information on an on-premises installation.

App Services (Kony Server):

http://docs.kony.com/KonyOnPremises/#../Subsystems/KonyServerSystemReference/
Content/System%20Requirements.htm%3FTocPath%3DKony%20Development%20
Cloud%7CKony%20Server%20Systems%20Reference%20Guide%7C_____4

Messaging Services (KMS):

http://docs.kony.com/KonyOnPremises/#../Subsystems/KMS_Console_Installer_Guide-
Linux/Content/Overview.htm%3FTocPath%3DKony%20Development%20Cloud%7CKony%20
Messaging%20Services%7CKony%20Messaging%20Services%20Console%20Installer%20
Guide-Linux%7C_____3

Kony Sync:

http://docs.kony.com/KonyOnPremises/#../Subsystems/Kony_Sync_On-Premises_Server_
Planning_Guide/Content/Homepage.htm%3FTocPath%3DKony%20Development%20
Cloud%7CKony%20Sync%7CKony%20Sync%20User%20Guides%7CKony%20Sync%20
On-Premises%20Server%20Planning%20Guide%7C_____1

Management Services – Enterprise Mobility Management (EMM):

http://docs.kony.com/KonyOnPremises/#../Subsystems/EMM_Installation_Guide/Content/
Home.htm%3FTocPath%3DKony%20Management%20Cloud%7CEMM%20Installation%20
Guide%7C_____1

App Services (Kony Server) sizing examples

Additionally, for Kony Server the following table provides some examples of production
applications and the hardware needed to support various size deployments. This is only a
guide as each application is different.

Field	Description	Sessions per Month	Count of Physical Servers (Dell - Intel Xeon E5-4640 2.4GHz)	CPU Cores per Server	Server RAM	JVMs per server* Physical Servers=Count of JVM's	Memory per JVM	CPU Usage at Peak
Airline	Native & Web	50M	6	6	128 GB	15 * 6 = 90	2.5 GB	80%
Travel	(HTML APIs)	250K	3	3	16 GB	1 * 3 = 3	2.5 GB	55%
Insurance	Web Only	1.2M	2	2	16 GB	3 * 2 = 6	2.5 GB	35%
Airline	Native & Web	200K	2	2	16 GB	3 * 2 = 6	2.5 GB	62%
Financial	Native Only	3M	2	2	16 GB	3 * 2 = 6	2.5 GB	59%
Cross-Industry	Native Only	100K	2	2	48 GB	6 * 2 = 12	2.5 GB	16%

About Kony, Inc.

Kony is the fastest growing cloud-based mobile application development platform (MADP) in the industry with over 600 live multi-channel apps, serving over 20 million end users across 45 countries, and generating over 1 billion sessions. The Kony Experience Platform is an integrated software development lifecycle (SDLC) platform to define, design, develop, test, deploy, and manage multi-channel applications from a single code base. With Kony, you can deliver stunning user-first experiences, get to market faster, and lower your application TCO. Kony also offers a suite of more than 33 ready-to-run B2E and B2C apps that enable customers to quickly extend their business.

For more information, please visit **www.kony.com** and connect with Kony on **Twitter**, **Facebook**, and **LinkedIn**.