ORACLE CLOUD

ORACLE INDUSTRY CLOUD SERVICES PILLAR

CONTRACTUAL DOCUMENTATION | JULY 2017

ORACLE

Table of Contents

.

Scope

This document applies to Oracle Cloud Services for Industry (OCI).

OCI supports the cloud offerings provided by the Communications Global Business Unit, Financial Services Global Business Unit, the Health Sciences Global Business Unit, the Hospitality Global Business Unit, the Construction and Engineering Global Business Unit, the Retail Global Business Unit, and the Utilities Global Business Unit.

This document is a supplement to the *Oracle Cloud Hosting & Delivery Policies*. Its purpose is to account for exceptions and additional terms specific to the Oracle Global Business Units. The content of this document takes precedence over the *Oracle Cloud Hosting & Delivery Policies*.

Service Availability

For purposes of calculating the Service Availability Level of the Oracle Cloud Services, "Available" or "Availability" means that You and Your Users are able to log in and access the OLTP or transactional portion of Cloud Services.

Target Service Availability Level objectives are as outlined in the Oracle Cloud Service Level Objective Policy section in the Oracle Cloud Hosting & Delivery Policies document, or in the applicable Service Description related to the specific Global Business Unit cloud service.

Oracle works to meet a Target System Availability Level for the measurement period of each calendar month, commencing at Oracle's activation of the production environment.

Change Management

Application Upgrades and Updates

Oracle requires all Cloud Services customers to keep their Services current with the software versions that Oracle designates as generally available (GA) for such Services. Software updates or upgrades will follow the release of every GA release and are required for the Services in order to maintain version currency. For certain Cloud Services, Oracle performs upgrades by upgrading Your non-production environment to the latest version of the Cloud product before upgrading the production environment.

Oracle Cloud Hosting and Delivery Policies, such as Service Levels Objective Policy, and the Support Policy, are dependent on You maintaining GA version currency. Oracle is not responsible for performance or security issues encountered with the Cloud Services that may result from running earlier versions. Oracle will provide prior notice for updates or upgrades that involve service interruption to You.

Oracle typically schedules application upgrades every 2nd and 4th Friday of the month between 21:00-06:00 (Saturday) data center local time. For some sectors such as Hospitality and Retail, Oracle will schedule the application upgrade on a weekday to accommodate Your business operations.

If You are eligible to select Your own upgrade window, You will either be contacted by Oracle to coordinate the upgrade change window, or You will be able to select target hour and date with the exception of blocked time periods that Oracle reserves for core system maintenance.

Application Changes

Access to production servers at the operating system and database level is restricted to Oracle Cloud for Industry Services and Application Management groups. Customer changes to the application are allowed only via the defined user interface, web service, or a standardized API. Alteration or extension of the underlying base application code is not allowed as a mechanism of customizing the application.

Core System Maintenance

Core system maintenance involves changes to hardware, network systems, security systems, operating systems, storage systems, or general supporting software of the cloud infrastructure. Core system maintenance may result in service interruption. Oracle works to limit any service interruption due to core system maintenance to less than 2 hours during a scheduled service period. Oracle may elect not to schedule a core system maintenance event.

Oracle typically schedules core system maintenance on Fridays between 21:00- 06:00 (Saturday) data center local time.

Routine Infrastructure Maintenance

Oracle manages routine infrastructure maintenance activities for the purpose of providing environment currency, capacity, and stability. Routine maintenance is not expected to result in a service interruption. When possible, routine infrastructure maintenance will be performed during the Core System Maintenance window and follow the same notification policy.

GA and End of Life (EOL) for Oracle Business Unit Cloud Services

If Oracle is no longer supporting or otherwise making any of the Originally Ordered Cloud Services generally available to its commercial customers "End of Life Products", Oracle will provide You with no less than twelve (12) months advance notice prior to the date when the Originally Ordered Cloud Services are no longer generally available.

Specific Cloud Services have published GA and EOL practices information. Where applicable, the documentation is available here: http://www.oracle.com/us/corporate/contracts/cloud-services

Disaster Recovery

Disaster Recovery services are intended to provide service restoration capability in the case of a major disaster, as declared by Oracle that leads to loss of a data center and corresponding service unavailability. For the purposes of this Policy, a “disaster” means an unplanned event or condition that causes a complete loss of access to the primary site used to provide the Oracle Cloud Services such that Your production environments at the primary site are not available.

The Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) do not apply to Your customizations that depend on external components or third-party software. During an active failover event, non-critical fixes and enhancement requests are not supported. You will be solely responsible for issues arising from third party software and customizations to Oracle programs and services.

The RTO and RPO Level objectives are as outlined in the applicable Service Description related to the specific Global Business Unit cloud service.

Upon Oracle's declaration of a disaster, Oracle will commence the Disaster Recovery Plan to recover production data to the most recent available state to reconstitute the production environments of the affected Cloud Services with the Recovery Time and Recovery Point Objectives as defined in the Service Description for the applicable Global Business Unit cloud service. Production services may operate in a degraded state of performance for the duration of the disaster event.

A Recovery Time Objective (RTO) is Oracle's objective for the maximum period of time between Oracle's decision to activate the recovery process to the secondary site due to a declared disaster, and the point at which You can resume production operations in the secondary production environment. If the decision to failover is made during the period in which an upgrade is in process at the secondary site, the RTO extends to include the time required to complete the upgrade. A Recovery Point Objective (RPO) is Oracle's objective for the maximum possible length of time during which data could be lost in the event of a disaster. The RPO time excludes any data loads that may be under way when the disaster is occurring.

Oracle Hospitality Cloud Services Disaster Recovery

In the event of a declared disaster, Oracle may recover and restore the production environment of the affected Hospitality Cloud Service and work to restore production data using a recent backup made prior to the onset of the disaster. Oracle may elect to restore the production environment in an alternate, available data center of Oracle's choice. When using a backup for recovery and restoration of the production environment and production data, published RTOs and RPOs, if any, will not apply.

Information Transfer

Secure File Transfer Protocol (SFTP)

The secure file transfer protocol (SFTP) services are limited-access systems for the purpose of uploading or downloading data files in a secure manner. SFTP downloads/uploads are recorded in an electronic audit log that includes: date and time, user name, and name of file up/downloaded.

Traceability of user requests for SFTP access and modifications to access rights is provided through change control processes.

Account Usage

Oracle reserves the right to restrict access, limit use of the SFTP Service, or remove access for any nonconforming users, sites, or customers, without prior notification, whenever the use of the service is not in compliance with the terms of use. Access is granted on each account to specific directories using the principle of least privilege. Customer accounts have full read-write access to the data in each directory to which the user has access.

Technical controls in place are designed to ensure confidentiality of data and to prevent unauthorized access to other accounts' data. Attempts to access directories not authorized for a given account are a violation of the terms of use, and the account may be suspended. Oracle is not responsible for unauthorized customer access to data within a directory by an account which has authorized and approved access.

Account Provisioning

Currently, SFTP accounts are created with a strong 10-character password. The account password will be sent in an email to the address associated with the account. For this reason, the email address associated with an account must be a valid individual email and may not be a shared account or company e-mail distribution list. Inactive accounts will be disabled, and then deleted under the following schedule:

Accounts that are inactive for 3 months will be disabled.

Accounts that are inactive for 6 months will be deleted.

You must submit a request via the ticketing system to terminate accounts that are no longer required or need to be revoked.

Account Authentication

Passwords are automatically generated and cannot be changed by the account holder or recovered by Oracle. If a password needs to be changed or reset, the account holder must submit a formal change request via the ticketing system to have a new password generated. The updated account password will be sent in an email to the address associated with the account.

Account Authentication – Alternate Automation Methods

The SFTP service supports public key authentication; a method of automatic password-less login. Each account has a public key directory. By generating a local private and public key pair, uploading the public key file to this directory, and configuring the client software to use public key authentication, an account user can log in without being prompted for a password. Multiple public key files per account are supported by Oracle.

Acceptable Usage

All data transferred via the SFTP service must be for the specific business purpose and function of supporting Your hosted environment(s). The SFTP service may not be used for data backups, temporary storage, unlicensed copyrighted materials, or other illegal materials. Your integrations employing the use of automated data transfer agents or 'scripts' are permitted, however they should either run manually or on a periodic schedule not to exceed a SFTP connection rate of 10 times per hour. The use of automated processes that aggressively connect, or that do not properly connect, authenticate, perform an appropriate file transfer operation, or properly disconnect, is a violation of the terms of use.

Data Storage

Data stored on the SFTP server will automatically be deleted after 60 days. All incoming and outgoing SFTP data is considered transient data and not subject to backup retention. The only exception is that the directory structure and any ssh login key file information is retained and not automatically deleted

Payload Encryption Requirements – Data-at-Rest

If the service offering is subject to external regulatory requirements such as PCI DSS that mandates data-at-rest encryption, the configuration of the Oracle SFTP service for the deployment will employ the use of whole disk encryption, or the service will be designed to accept incoming encrypted data files with an Oracle provided public key or x.509 certificate. Conversely, if the service offering has outbound data and file transfer integrations, then You must provide Oracle with a bonafide x.509 certificate for SFTP data integrations.

Encryption Requirements – Transport

Industry security standards and Oracle security policies mandate end-to-end (socket-to-socket) based transport encryption for data exchange. Use of FTP over SSL (FTPS) and FTP does not guarantee transport encryption is either properly enforced or negotiated during the initiation of the data connection, and the latter protocol (FTP) is completely lacking any transport encryption. Therefore, Oracle data transfer standards is limited to SFTP with the goal of ensuring confidentiality of data transfers between Oracle and You.

Compliance

Audit Reports

Audit reports and letters of compliance for Oracle Cloud Services are periodically published by Oracle's third party auditors. Reports and letters may not be available for all services or at all times. You may request a copy of the current published audit report or letter available for a particular Oracle Cloud Service, as applicable, by contacting the Oracle Sales Representative or designated Oracle account contact and providing the following information:

- Company name
- Contact name
- Title
- Recipient e-mail address
- Request justification (e.g., purpose and intended use description)

Oracle Utilities Opower Cloud Services

For details regarding specific Oracle Utilities Opower Cloud Services, please refer to the Oracle Utilities Opower Service Descriptions.

Change Management

Application Upgrades and Updates

For Oracle Utilities Opower Cloud Services, Oracle schedules application upgrades between 11:00 – 15:00 Eastern US time every third Sunday. Customer notifications are sent 72 hours in advance of such upgrades.

Core System Maintenance

For Oracle Utilities Opower Cloud Services, Oracle schedules core system maintenance between 03:00 – 07:00 Eastern US time on the last Thursday of each month. Customer notifications are sent 72 hours in advance of such upgrades.

Access Control

Privilege Management

In lieu of a bastion host, Oracle Administrative access to the Oracle Utilities Opower Cloud Services environment requires administrators to first connect to a trusted network to be able to access the systems. Access to the trusted network requires physical access to the network or authentication to the network by means of a username and password. All access to the trusted network from remote locations requires multifactor authentication.

Communication and Operations Management

Backups

The Data Integration Platform components of the Oracle Utilities Opower Cloud Services includes customer AMI (or “smart meter”) data which is not backed up to disk or tape. Instead, disaster resiliency for this component relies on a data replication strategy. Non-personally identifiable AMI data resident within this component is automatically replicated to a standby cluster within the same jurisdictional region on a daily basis. Personally-identifiable information is handled in a manner consistent with the requirements specified in the Backups section of the Oracle SaaS Security Practices document.

Daily backups are used to recover Oracle Utilities Opower Services in the event of a disaster. Oracle operates only one data center in Canada. Backups for disaster recovery purposes are stored in an encrypted format at a secondary site in the United States.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200