Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
# Table of Contents

- Disclaimer: 1
- Introduction: 1
  - Intended Audience: 1
- The Oracle Service Cloud: 2
- The Oracle Service Cloud Platform: 2
  - Hosting Architecture: 2
  - Locations of Hosting Facilities: 3
  - Hardware and Operating System Configuration: 4
  - Deployment Automation: 4
  - HMS: 5
  - Multi-Tenancy / Multi-Version Innovation: 5
- Types of Clouds: 6
  - Commercial Cloud: 6
  - PCI Certified Cloud: 6
- HIPAA: 6
- U.S. Government Cloud: 6
- U.K. Government Cloud: 6
- DoD Cloud: 7
- Comparison of Offerings: 7
- Optional Certification and Accreditation Services for U.S. Government and DoD Customers: 7
- Data Management / Data Custodians: 8
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability</td>
<td>8</td>
</tr>
<tr>
<td>Facility Resilience</td>
<td>8</td>
</tr>
<tr>
<td>Availability</td>
<td>9</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>9</td>
</tr>
<tr>
<td>Operational Excellence</td>
<td>10</td>
</tr>
<tr>
<td>Operational Transparency / Portal Overview</td>
<td>10</td>
</tr>
<tr>
<td>Global Nerve Centers</td>
<td>11</td>
</tr>
<tr>
<td>Service Maintenance</td>
<td>11</td>
</tr>
<tr>
<td>Service Upgrades</td>
<td>13</td>
</tr>
<tr>
<td>Security</td>
<td>14</td>
</tr>
<tr>
<td>Physical Security</td>
<td>14</td>
</tr>
<tr>
<td>Environmental Controls</td>
<td>15</td>
</tr>
<tr>
<td>Logical Security</td>
<td>15</td>
</tr>
<tr>
<td>Data Security Standards</td>
<td>15</td>
</tr>
<tr>
<td>Intrusion Detection &amp; Anti-Virus</td>
<td>15</td>
</tr>
<tr>
<td>Security Audits, Testing, and Assessments</td>
<td>16</td>
</tr>
<tr>
<td>Compliance</td>
<td>16</td>
</tr>
<tr>
<td>Cryptographic Protection of User Passwords in Storage</td>
<td>16</td>
</tr>
<tr>
<td>Employee Screening</td>
<td>16</td>
</tr>
<tr>
<td>Customer Portal Framework</td>
<td>17</td>
</tr>
<tr>
<td>Custom Objects</td>
<td>17</td>
</tr>
<tr>
<td>Business Rules</td>
<td>17</td>
</tr>
<tr>
<td>Custom Process Models</td>
<td>18</td>
</tr>
<tr>
<td>Syndicated Widgets</td>
<td>18</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Add-In Framework</td>
<td>18</td>
</tr>
<tr>
<td>Enterprise Integration</td>
<td>18</td>
</tr>
<tr>
<td>Integration Frameworks</td>
<td>18</td>
</tr>
<tr>
<td>Open Standard APIs</td>
<td>19</td>
</tr>
<tr>
<td>Telephony Integration</td>
<td>19</td>
</tr>
<tr>
<td>Cross-Channel Integrations</td>
<td>19</td>
</tr>
<tr>
<td>SSO and SLO Integration</td>
<td>20</td>
</tr>
<tr>
<td>Conclusion</td>
<td>21</td>
</tr>
</tbody>
</table>
Companies that aim for exceptional customer service seek out and embrace the tools and technology that integrate through open standards with their existing systems and which can adapt to rapidly-changing business requirements. The Oracle Service Cloud Platform is built on the bedrock practices of security, reliable distributed architecture, and first-class cloud operations. This provides companies with the foundation for meaningful and unequaled customer service experiences.

Introduction

The Oracle Service Cloud is a suite of capabilities that allow organizations to connect with their customers and facilitate the experience in the customer’s channel of choice. Oracle Service Cloud continues to evolve to meet the ever-growing demands of the market, made possible by the platform on which it is architected. The Oracle Service Cloud Platform is the foundation that enables great customer experience. Built on proven Oracle hardware and the time-tested resilience of Linux, Java, WebLogic, Apache, MySQL, and PHP, the Platform offers customers robust security, scalability, extensibility, and demonstrated upgradability. Oracle’s global commitment to the Cloud ensures the Platform is designed to be resilient with high availability. Open Standards-based integration and extensibility of the Platform includes easy-to-configure SAML-based Single Sign-On, database schema extensibility, an Add-in Framework, and a rich array of Syndicated Widgets and Open Standards-based APIs.

Intended Audience

This publication is aimed at members of IT and Customer Care organizations who expect best-in-class capabilities that optimize their customers’ experiences.
The Oracle Service Cloud

To provide customer experience excellence, companies require the ability to rapidly adapt to evolving business needs, provide consistent and insightful customer interactions, and have the confidence of proven, reliable delivery. The Oracle Service Cloud is designed for this with the flexibility of open standards integration, business administration extensibility, transparent cloud management, and security.

The Oracle Service Cloud is comprised of Web Customer Service, Cross-Channel Contact Center, Knowledge Management, and Policy Automation, all integrated and running on the best-in-class Service Cloud Platform which this white paper describes in detail. It should be noted this white paper excludes Oracle Field Service Cloud as this product is not operating within the Oracle Service Cloud platform.

Figure 1. The Oracle Service Cloud

The Oracle Service Cloud Platform

The Service Cloud Platform is a unique and extensive foundation purposely built for service from the ground up on the time-tested Java and proven LAMP (Linux/Apache/MySQL/PHP) technology stack with security, extensibility, enterprise integration, and performance.

Hosting Architecture

The Oracle Service Cloud Platform is centrally administered and built to, be scalable, and to improve fault isolation. With this in mind, components are redundant and protected by a defense in depth architecture. Database clusters are protected with additional firewalls which further isolate them from other components. In addition to database clusters and firewalls, arrays of other servers like Chat, Email, Utility, and File Attachment function together to comprise what is known as a “pod” which houses multiple customers. A customer’s presence on a pod is called a customer site, and a customer site exists within a single pod. One or more pods exist in each physical data center, and each pod will have a corresponding disaster recovery – or DR – pod to which its data is replicated and which can be activated in the event of fault in the primary pod.
Locations of Hosting Facilities

The Oracle Service Cloud Platform has many hosting facilities distributed across the globe, and it is possible for data to be stored in-country or in-region. Current locations are illustrated below. Typically, customers will be hosted in the facility nearest their region. Customers who must comply with PCI requirements will be hosted in a facility specially configured to support PCI certification; PCI certified services may not be available in all regions.

![Hosting facilities map](image)
This table lists current data center locations, highlighting the types of pods available in each data center and whether it is a Production or DR pod.

CURRENT DATA CENTER LOCATIONS

<table>
<thead>
<tr>
<th>Location</th>
<th>Commercial</th>
<th>PCI</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chicago, IL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ashburn, VA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US Gov</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DoD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toronto, Canada</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calgary, Canada</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>London, UK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amsterdam, NL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frankfurt, Germany</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Munich, Germany</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kitakyushu-Shi, JP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sydney, AU</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Hardware and Operating System Configuration

The Oracle Service Cloud Platform is built on Oracle hardware running Enterprise Linux, Apache, and MySQL connected to RAID-0 local storage, and network-attached storage for file-attach storage, all engineered for performance. The servers consist of high-end Intel-based Sun hardware serviced by Oracle Field Services. Database servers employ flash-cache for added performance and encryption for data security. Oracle ZFS-engineered systems provide the backbone network-attached storage which forms the core of each pod.

The Service Cloud Platform’s multi-tiered architecture is optimized for performance and includes:

» Web servers are physically separated from database servers which are behind a separate physical firewall.

» Redundant fail-over firewalls separate the environment from the Internet.

» Redundant fail-over load balancers provide load-balancing, application-layer firewalls, and fail-over capabilities for HTTPS and CGI services.

Deployment Automation

The Oracle Service Cloud can be expanded quickly to scale with the customer base and handle large surges of traffic. Pods can quickly be expanded in order to host more customers or sites as needed.

Spare equipment is generally kept on site and virtual machines can be spun-up quickly. Capacity of the environment is continually monitored. New services are brought online as specific thresholds are approached. The capacity of a pod can expand horizontally by adding hardware where it is needed. If the web pool is heavily loaded,
more servers can be deployed to the pool. If a database cluster is approaching maximum connections allowed, additional database nodes and clusters can be added.

The decision to expand within an existing data center or to additional data centers is based on Oracle’s assessment of the current capacity within the pod(s), customer requirements, availability, and compliance requirements.

HMS

The Hosting Management System, or HMS, is the heart of the Oracle Service Cloud Management Platform. HMS is used by Oracle Service Cloud Operations personnel to manage all aspects of the environment. HMS serves as the register for all sites and services in the Oracle Service Cloud. A highly-automated and customized suite of tools, HMS is responsible for site and service provisioning, comprehensive site and service administration, customer-controllable upgrades, and multi-tenancy management capabilities that span all data centers. As capabilities in the Oracle Service Cloud grow, the HMS framework allows integration of new products and features.

Multi-Tenancy / Multi-Version Innovation

Multiple customers exist per database server cluster and each customer has their own database schema, isolated and secured from other customers’ data with schema-specific user accounts solely managed by the customer. Web sites are secured with a “chroot jail” which isolates each customer’s configuration, look, and feel. Requests in the Apache-based Web tier can be routed to any web server. Web servers are stateless and have no customer or user affinity.

The Oracle Service Cloud Platform is also multi-version. Customers who upgrade to the most recent Oracle Service Cloud software versions have consistent access to Oracle Service Cloud’s most advanced product capabilities. By standardizing on a release lifecycle of 24 months, Oracle offers a predictable upgrade path to facilitate each customer’s upgrade planning. While this approach requires customers to periodically upgrade, it still offers customers substantial flexibility and control over the timing of their upgrades.

The illustration above shows how multi-tenancy / multi-version architecture differs from other types of cloud implementations. With Oracle Service Cloud, tenants get both application and database isolation. This isolation
means customers enjoy the benefits of having their upgrades performed on a per-customer basis with no impact from other customers.

Types of Clouds

The Oracle Service Cloud Platform supports four distinct types of clouds, each tailored to specific needs to ensure our customers’ environments are fine-tuned to deliver to their business needs.

Commercial Cloud

The Commercial Cloud is the default cloud, delivering a secured and robust environment that serves thousands of customers globally throughout our geographically dispersed data centers. It is intended to support important environments complete with backups, redundancy, disaster recovery, and scalability.

These statistics showcase the capabilities of the Commercial Cloud:

» 2.7 million tickets created per day
» 8.8 million searches per week
» 208 million answers viewed per month
» 8 million answers maintained
» 2 billion contacts maintained
» Over 180 billion database transactions each week
» 600+ custom objects in use

PCI Certified Cloud

Safeguarding credit card information and maintaining compliance with the PCI Data Security Standards (PCI DSS) is a requirement for many organizations that processes, transmits, or stores credit card information.

For customers with these compliance requirements or for customers who want the additional benefits of a PCI-certified site, the Oracle Service Cloud Platform offers a PCI-certified Cloud which is a PCI Level I Service Provider, the highest level possible for Service Providers. Oracle continually invests in and improves the resources and infrastructure for a PCI-certified Cloud.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Oracle offers customers a solution that helps organizations that handle protected health information (PHI) meet the stringent privacy and security requirements under the HIPAA regulations.

U.S. Government Cloud

Oracle offers U.S. government customers a hosting environment that is designed to help them meet their requirements under the Federal Information Security Management Act (FISMA). This is an environment that offers the logical separation of tenants and other operational controls to provide the security, high availability, and redundancy, equivalent to our Commercial Cloud. The U.S. Government Cloud has been designed to implement the control requirements for the NIST 800-50 Moderate Baseline. Control implementation and compliance status has been independently verified and documented by a third party auditor.

U.K. Government Cloud

Oracle offers U.K. government customers a hosting option certified to ISO27001 and aligned with HMG Cloud Security Principles Assertion Level 3. This pod is located within the EEA (European Economic Area) and is
accessed by Oracle via secure VPN. Control implementation and compliance status has been independently verified and documented by a third party.

DoD Cloud

Oracle is a pioneer in bringing the SaaS delivery model to government agencies and has successfully served the U.S. government for more than a decade. Nearly 200 public sector customers – including members of the Department of Defense – rely on the Oracle Service Cloud Platform to deliver information.

Built to DIACAP standards designed to implement the requirements contained in DoD Instruction 8500.2, the DoD Cloud is hosted at a government-approved data center location that has been implemented with FedRAMP, MAC III, and Sensitive Information Assurance (IA) control requirements, including Certification and Accreditation (C&A) performed by third party accreditation consultants.

Comparison of Offerings

Here is a side-by-side comparison of the various Oracle Service Cloud offerings.

<table>
<thead>
<tr>
<th>Optional Certification and Accreditation Services for U.S. Government and DoD Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each U.S. Government Cloud and DoD customer needs their own System Security Plan (SSP), and some customers may need additional Certification and Accreditation (C&amp;A) services due to requirements above and beyond the NIST 800-53 baseline. Some customers may have configurations or customizations that deviate from the baseline. To meet those specific needs, Oracle can provide optional C&amp;A services for Oracle Consulting Services (OCS) engagements, or customer-specific product customizations for Government Cloud offerings:</td>
</tr>
<tr>
<td>» Security Engineering Support:</td>
</tr>
</tbody>
</table>
» Security engineering is integrated into OCS engagements to help understand customer application security/software assurance requirements and address them for customizations and/or integrations.

» Tailored C&A Package for OCS engagements for customer-specific product customizations:
  » Appendix for Major Application System Security Plan (SSP)
  » NIST 800-53A Security Assessment Report (SAR)
  » NIST 800-30 Risk Assessment Report (RAR)
  » Plan of Actions and Milestones (POA&M)

Data Management / Data Custodians
Oracle facilitates access to customer data acting only as a data processor, claiming no ownership of customer data. As a processor, Oracle provides encrypted data access to customers to modify their data securely through the Oracle Service Cloud products and Service Cloud APIs.

Reliability

Facility Resilience
The facilities that house the Oracle Service Cloud Platform are built and managed by wholesale and retail co-location vendors with varying combinations of certifications and characteristics of resilience. All facilities meet the following criteria:

» Construction, Power, and Cooling:
  » Concrete, stone, and/or steel construction
  » Redundant utility feeds
  » Redundant UPS
  » Redundant standby power
  » Excess power capacity
  » Cooling capacity that matches or exceeds power capacity
  » Redundant ISPs

» Physical Security:
  » 24x7 human guards
  » Secure ingress/egress always includes multiple levels of physical technology, including:
    • Man traps
    • Biometric scanners
    • Proximity card readers and identification badges
    • Audible alarms when security is breached
    • Access limited by defined access lists
    • Physical access logging
    • Cage space secured by physical key or hand scanner
    • Compulsory visitor escort
  » Closed circuit TVs and recorders
Certifications for physical facilities may include:

» ISO 9001
» ISO 27001
» ISAE 3402
» SSAE16 (U.S. facilities only)

Availability
Availability of your site and data is a high priority, and our web servers are configured into load-balanced clusters with spare capacity. If a web server experiences a failure the remaining web servers within that cluster can continue to service requests. Once the affected server is taken offline and its problem is resolved, it can be re-introduced into the cluster. Other components that make up the Oracle Service Cloud Platform infrastructure are mirrored with hot standby configurations. Those components include switches, firewalls, load balancers, NFS, and database servers. Network paths into and out of the data center are redundant and provided by multiple carriers.

Disaster Recovery
Oracle maintains a Service Cloud DR Plan designed to protect customer productivity and Oracle’s commitment to customer support in the event that all, or part, of its hosting operation is rendered “unusable”. If a disaster is declared, each primary site can be recovered at a disaster recovery data center. The RTO is 12 hours from the disaster declaration, and RPO is 1 hour, excluding any data loads that may be underway. Chroot snapshots are taken every 4 hours at both the production site and the DR site.

![Disaster recovery architecture](image)

Figure 5. Disaster recovery architecture

The plan incorporates recovery strategies that address varying levels of failure and are intended to reduce risk. These strategies include:

» Backups stored encrypted at both the primary and DR facilities
» Near real-time replication of data from the primary facility to the DR facility
» 24 hour automated monitoring service
» 4 hour response hardware service agreements
» Re-routable data transmissions
» Redundant on-site “hot” and “cold” spare equipment
» Uninterruptible Power Supply (UPS) systems
» High availability system configurations
» Multiple environment control systems (HVAC)
» Remote employees at all data center locations

The Oracle Service Cloud DR Plan is tested at least annually. Testing is carried out with the intention of minimizing impact to the production hosting environment. The results of each test, including criteria and details, are documented and reviewed by Operations and Customer Support staff.

Oracle currently uses this data backup schedule:
» Every 24 hours: Incremental
» Every 7 days: Full
» Every 14 days: Offsite, vaulting service

As part of our proprietary Data Center standard, Oracle utilizes an advanced data replication system that is designed to keep customer data in sync with online disaster recovery systems in our Disaster Recovery data center location. Continual data replication also allows us to pull the same data from numerous servers and spread the load across the environment. The Platform is designed to write data to one database, but read data from multiple copies. Long running reports can be processed on other servers to reduce impact on primary operations.

The DR system’s capabilities include:
» Full-scale duplication of production data in a geographically diverse carrier class data center
» Combining continual data replication and periodic storage snapshots designed to keep customer data up-to-date
» DR pods are updated during every maintenance window with the changes applied to the production pods to keep them current and ready with the same software versions as production

For additional information on Disaster Recovery, customers under NDA may request a copy of Oracle’s Service Cloud DR Plan by submitting a service request.

Operational Excellence

Operational Transparency / Portal Overview

Our Virtual CIO (VCIO) Portal gives IT personnel detailed visibility into key operational metrics.

With VCIO, customers have visibility into their Oracle Service Cloud Platform. Customers can even alert Operations about a critical issue from the VCIO dashboard.
Information and features currently available in VCIO includes:

» Current and historical service status

» Detailed service statistics about visits, bandwidth, end-user page hits, admin page hits, and storage for database, file attachments, and web content

» Operations information including incident service level targets (SLT), service events that affect your sites, and uptime of your sites

» Ability to perform digital certificate configuration

» Ability to manage system mailboxes

Global Nerve Centers

Our state-of-the-art operation centers (GNCs) follow the sun 24 hours a day every day. We have three GNCs which are located in the United States, United Kingdom, and a third GNC in Bangalore. GNCs are staffed 24x7x365 and are connected to all production pods worldwide, providing up-to-the-minute visibility into components of the environment. Our GNCs are responsible for monitoring and ensuring stability of the pods and customer sites, managing customer events, and handling proactive communications with customers.

Detection and prevention capabilities are marked by a dedicated 24x7x365 team of database and systems administrators at each GNC, and hand-offs between GNCs are both written and verbal at the end of every shift. Multiple individuals on the Operations Team have U.S. government clearance to support government sites.

Service Maintenance

Oracle is committed to providing a reliable hosting service for the cloud Platform. Efforts to improve the value customers receive from the Platform sometimes involves system maintenance that could result in planned downtime for a customer's site.

Scheduled maintenance currently can occur on the first or third Friday night of every month. Additionally, Oracle typically alternates maintenance dates between data centers so that only one data center is affected during a given
Maintenance window. Furthermore, because Oracle assigns customers to the pod most geographically aligned for them, we can often perform most maintenance to coincide with off hours.

Announcements for maintenance and service packs are generally distributed via both email and VCIO and according to the following schedule. Communications indicate date, time and expected impact to customers.

- Normal maintenance: 14 days in advance
- Emergency maintenance: 24 hours in advance
- Service packs: 7 days in advance

Emergency maintenance is sometimes necessary to apply critical updates or security patches in order to prevent security breaches or service interruption. Any hardware maintenance to be performed is carried out by the co-location facility and on-site personnel.

Figure 7. Service events

The Cloud Operations team adheres to a multi-level change management process in which all changes world-wide are tracked centrally in a single system. All changes are categorized into one of six levels based on the change’s expected impact and the deployment complexity where L6 is the smallest impact and complexity and L1 is the highest impact and complexity. The number of approvals required and visibility increases as the impact and complexity rises. L1 and L2 changes require two levels of management review as well as approval from the Change Advisory Board.
THE CURRENT STANDING SCHEDULE FOR MAINTENANCE IN THE ORACLE SERVICE CLOUD IS AS FOLLOWS:

<table>
<thead>
<tr>
<th>Location</th>
<th>Maintenance Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chicago, IL</td>
<td>10 PM – 2 AM CT</td>
</tr>
<tr>
<td>Ashburn, VA</td>
<td>10 PM – 2 AM ET</td>
</tr>
<tr>
<td>Toronto</td>
<td>10 PM – 2 AM ET</td>
</tr>
<tr>
<td>Brazil</td>
<td>10 PM – 2 AM BRT</td>
</tr>
<tr>
<td>London, UK</td>
<td>10 PM – 2 AM UTC/GMT</td>
</tr>
<tr>
<td>Amsterdam, NL</td>
<td>10 PM – 2 AM CET</td>
</tr>
<tr>
<td>Germany</td>
<td>10 PM – 2 AM CET</td>
</tr>
<tr>
<td>Kitakyushi-Shi, JP</td>
<td>1 AM – 5 AM JT</td>
</tr>
<tr>
<td>Sydney, AU</td>
<td>12 AM – 4 AM AET</td>
</tr>
</tbody>
</table>

Figure 9. Current standing maintenance schedule

Service Upgrades

When innovative new features and performance improvements become available on the Oracle Service Cloud Platform, Oracle wants customers to be able to take advantage of them quickly. To support that interest, the Oracle Service Cloud has spent considerable time and resources improving features, components and processes that enhance our customers’ experience when upgrading from one version of Oracle Service Cloud to another.

In addition to these improvements, Oracle has recently introduced the Auto Upgrade Program. Customers who enroll in the Auto Upgrade Program upgrade automatically to the latest product release each quarter. With the Auto Upgrade Program, an upgrade can be completed more quickly so you can spend more of your time delivering value to your customers instead of engaging in the upgrade process.
Security

Physical Security

Full-time 24/7 local operations and security staff are tasked with ensuring that only authorized individuals have access to the data center. Data center access doors, including shipping and parking areas, are monitored and video recorded. Data center access is secured by access cards, biometric devices (e.g. hand scanners), man-traps, portals, or a combination thereof. Design of exterior walls, doors and windows are taken into careful consideration in order to protect from natural hazards including lightening and wind.

Server and network equipment is physically secured within locked cages/suites separate from other data center tenants. The listing of employees and cages are updated frequently so that access is limited to authorized personnel. Each data center provides centralized security operations and monitoring on a 24/7 basis, including prompt response to actual or suspected physical security incidents. In addition to administering and monitoring access to the data center, the operations and security teams monitor and enforce other security policies and environmental sensors and alarms. Security and environmental systems are supported by redundant power, uninterruptible power supply (UPS) devices, and stand-by generators.

Hosting facilities currently meet the following physical security standards:

» Physical access to servers is limited to a defined access list. Physical access to the server area is authenticated with picture ID and/or biometrics. Physical access to the server area is logged.
» Alarms sound if physical hosting data center security has been breached.
» Visitor access to data centers is granted with the accompaniment of someone on the approved physical access list.
» Guards at designated stations to validate IDs based upon ACLs defined by the Oracle team. Data center entrances are guarded 24/7.
» Video surveillance cameras are in place. Recorded data is stored for 30 days.

To learn more about the Oracle Service Cloud process or about the benefits of the Auto Upgrade Program, please contact your Account Executive or Client Success Manager.
» Cage space is accessible only via a biometric scanner.
» Single point of entry to hosting areas.
» Building access points are monitored or controlled by one or more of the following: surveillance cameras, man-traps, biometric scanners, and/or guards.

Environmental Controls
Each data center facility has redundant generators and UPS systems. Load is handled by the battery backup until the generators take over the load. Facility fire protection is built around a pre-action dry pipe system. Structured cabling runs within overhead cable trays. Cages are built on either concrete slab or raised floor. Power is installed overhead. Oracle has a data center administrator at most locations.

Logical Security
The Oracle Service Cloud Platform requires management authorization for employee access via HMS to any critical applications and systems, and additional approval levels are required for all Cloud Services access. Access is granted on an as-needed and on-going basis according to a user's role and business need, like Cloud Operations, Customer Care, and Engineering. Logical and physical access is required to be promptly revoked from employees who have resigned or are terminated. The Oracle Service Cloud Platform audits system and network activities, including access, or attempted access, to customer data. This includes monitoring and auditing of systems for unauthorized or inappropriate access to customer data by Oracle employees.

When deploying new systems into a pod, hosts are first imaged from known secure OS images, and before being integrated into the pod, the new systems are hardened further using hardening guidelines based on CIS, NIST and DISA standards, according to Oracle policies.

Oracle employs software VPN, two-factor authentication, and encrypted protocols like SFTP and TLS for systems administrators accessing the environments. Host administration is performed via either encrypted SSH or TLS, and multi-factor authentication is required for external command-line access to all systems. Oracle retains security logs for between one and seven years, depending on the environment.

Auditing of the environments includes daily and quarterly infrastructure and application scans, quarterly patching and version reviews, quarterly formal access reviews that include justifying privileged access, and ethical hacking reviews both before and after GA release of new software versions. Third-party application security tests are performed for every new release, and advanced event correlation and vulnerability detection is done using a SIEM solution.

Data Security Standards
The Oracle Service Cloud implements various methods and practices to ensure world-class security of your data across external connections, including:

» Connections are negotiated for 128-bit encryption or stronger.
» Cipher key generation uses at least a 2,048-bit private key.
» Segregation in networks is deployed in a layered approach designed to protect customer data at the physical, data link, network, transport, and program levels.

Intrusion Detection & Anti-Virus
Oracle Service Cloud utilizes Network Intrusion Detection Systems (nIDS) to protect the environment. Packet inspection is done at the firewall layer. nIDS sensors are deployed in either Intrusion Prevention Mode or Intrusion Detection Mode on the network, to monitor and block suspicious network traffic from reaching the internal network.
nIDS alerts are routed to a centralized monitoring system that is managed by the security operations teams 24x7x365. Oracle uses a SIEM solution to monitor events and respond to incidents.

For anti-virus protection, Oracle Service Cloud employs industry standard anti-virus software to scan uploaded files. Virus definitions are configured to update daily. Attachments are scanned before being uploaded into the database. Infected attachments are automatically quarantined. Oracle Service Cloud scans inbound email messages for viruses and spam, and any detected are quarantined. Customers have the ability to manage the email quarantine and to adjust their own spam controls.

Security Audits, Testing, and Assessments
The internal controls of the Oracle Service Cloud are subject to periodic testing by independent third party audit organizations. Such audits may be based on SSAE 16 (Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization), ISAE 3402 (International Standard on Assurance Engagements No. 3402, Assurance Reports on Controls at a Service Organization), or other such third party auditing standards or procedures applicable to the Oracle Service Cloud. Audit reports for the Oracle Service Cloud are periodically published by Oracle’s third party auditors, and customers may request a copy.

The audit reports of Oracle Service Cloud, and the information they contain, are Oracle confidential information, and must be handled by customers accordingly. Such reports may be used solely by Customer to evaluate the design and operating effectiveness of defined controls applicable to the Oracle Service Cloud and are provided without any warranty.

Many audit reports are available to customers. Customers may submit a service request via their Account Executive or Client Success Manager to obtain available reports.

Compliance
The Oracle Service Cloud is aligned with ISO (International Organization for Standardization) 27001:2013 security controls. The ISO security framework includes a comprehensive set of security controls that are used as a baseline for the operational and security controls utilized to manage and secure the Oracle Service Cloud, but this does not include ISO 27001 certification.

The customer is solely responsible for its regulatory compliance in its use of the Oracle Service Cloud and must make Oracle aware of any requirements that result from its regulatory obligations prior to contract signing.

For more information about Compliance, see Oracle Cloud Enterprise Hosting and Delivery Policies.

Cryptographic Protection of User Passwords in Storage
Passwords are protected in storage by storing an industry-standard cryptographic hash in place of the plain-text password. Protections are also in place to ensure all hashes are unique. Passwords at rest in the Government and DoD Clouds adhere to the appropriate NIST 800-53 requirements. To discuss the specific protections in place for your version, customers can contact their Account Executive or Client Success Manager.

Employee Screening
Beginning with recruiting and hiring, and throughout the tenure of employment, Oracle is committed to developing and retaining a dedicated and competent professional workforce. Ongoing training opportunities are provided to Oracle employees on a regular basis throughout their careers. This means that Oracle employees can stay abreast of the latest professional developments.
As further evidence of its commitment to ongoing compliance with both the law and fundamental principles of ethical conduct, Oracle employs full-time recruiting staff, as well as a highly-trained professional dedicated to EEO/AA compliance, both internally and externally.

Extensibility

Customer Portal Framework

Customer Portal provides a full-featured framework for delivering great web self-service experiences. The framework uses PHP, YUI and other standard technologies to power a best practice reference implementation which enables desktop, mobile smart phone, and basic mobile page-sets. End Users are automatically directed to the appropriate experience based on configuration without duplication of effort. Customers extend the reference implementation to meet their specific needs using the IDE of their choice. Within a single administrative console, development, staging and production environments may be managed.

Features of the Customer Portal Framework include:

» Highly reusable template and widget-based customization
» Sitemap support for search engine optimization
» Configuration based rules for online interactions
» Content syndication allowing support experiences to extend beyond your own support site
» Extension wizards for creating new widgets or extending any current widget
» Web-based administration
» Industry-standard permission-specific security
» Ability to deploy your knowledge content in 34 languages (including double-byte languages) for easy localization

Custom Objects

Oracle Service Cloud provides a configuration-based approach to schema management through Custom Objects (COs).

Once created, COs can be leveraged as native objects within Oracle Service Cloud, and they are supported through the upgrade process. Therefore, they are accessible in Customer Portal, Reporting, APIs, Agent Desktop, Surveys and Marketing. An example where COs might be used is RMA processing. End users might initiate a product return via Customer Portal, and that request can be processed by an agent via the Agent Desktop with a customized workspace integrated into already familiar workflows. It would also be easy to allow end users to query status of their RMA from the Customer Portal.

Business Rules

Business rules allow automation of common business tasks. They link data from Oracle Service Cloud knowledge base, resulting in a responsive and consistent customer experience. Business rules can route incidents to the most suitable support person, notify an engineer when answers in the knowledge base should be reviewed, and automatically answer some customer questions. They can send marketing emails and surveys, escalate overlooked opportunities and set strategies based on conditions you define. Rules can also be written to update contacts and organizations, set custom fields, and assign tasks.

Besides the many advantages of keeping the knowledge base accurate and current, business rules also let staff members work efficiently and consistently. When you create rules to answer routine customer questions, customers enjoy an immediate response. At the same time, staff members work more productively without the distraction of repetitive tasks. As a result, they can deliver more responsive customer service and follow-up.
A Business Rule is simply an “if-then-[else]” statement: If these conditions apply, then take this action, else (optionally) take some other action. Some examples of Business Rules might include if a customer has a billing question, then route the incident to an accounting staff member, else route it to technical support; or, if a new contact is from the East coast, then send a marketing email about the grand opening of a New York store.

Custom Process Models

Custom Process Models (CPM) allows customers to implement custom business logic through Object Event Handlers (PHP scripts). An object event handler can be associated with create/update/destroy events on an object and is automatically triggered when the respective operation is performed on the object. Object Event Handlers can also be invoked from the Business Rules UI, allowing integration of custom business logic with business rules. For instance, an object event handler can be written to create a contact in an external system whenever a contact is created in the Oracle Service Cloud.

Syndicated Widgets

With the Customer Portal Framework, you can achieve Knowledge Syndication, Chat, and Surveys on your commerce web pages. The goal of this capability is to provide relevant knowledge content outside of your support area without losing the artificial intelligence and relevance inherent in the Oracle Service Cloud Platform. A common example might be to provide product knowledge overlaid on commerce pages for a shopping experience. Inclusion of syndicated knowledge components into your commerce site is as easy as loading the Oracle Service Cloud widget into your storefront pages with a few lines of code.

Add-In Framework

The Add-In Framework, based on the Microsoft .NET framework, enables customers and partners to extend the agent desktop with custom features and capabilities which may be important to their business. The power and flexibility offered by the Add-In Framework enables developers to create custom solutions that range from simple data validation to complex telephony integrations. In addition, the framework supports multiple add-in types allowing the developer to extend functionality of any aspect of the Agent Desktop. Because it is based on the Microsoft .NET framework, it looks and feels similar to Microsoft Word or Outlook. Further, since many customers leverage Microsoft Outlook in their contact center, the Agent Desktop has a pre-built Outlook integration which can be configured by the client. This integration allows two-way synchronization of contacts and tasks, and allows agents to append email messages to incidents in the Oracle Service Cloud.

Extending reporting capabilities to include external data sources is also accomplished using the Add-In Framework. Developers can create virtual tables which can be used to create analytics reports that can retrieve external data at run time.

Enterprise Integration

Integration Frameworks

At its core, the Oracle Service Cloud Platform is standards-based and not proprietary, so it can be integrated with your existing IT landscape. Whether simple or complex, the integrations you require can be assessed, developed, and implemented by customers themselves, by Oracle Partners, by Oracle Consulting Services, or a combination of the three. Knowing how to capitalize on the Oracle Service Cloud’s native integration capabilities, pre-built services and APIs is essential to developing a solution while reducing risk and adhering to industry best practices. If working with OCS or an Oracle Partner, customers are likely to take advantage of pre-designed and pre-built integrations to other Oracle applications because OCS works closely with Oracle Product Development to bring new packaged
integration solutions in areas like quoting, sales planning, data quality, marketing automation, ERP, and compensation management, but customers are also enabled to develop and manage integrations independently.

Open Standard APIs
The ability to integrate with other applications is one of the important benefits of the Oracle Service Cloud Platform. The Platform provides a robust set of backwards-compatible open standards-based public APIs to build integrations on both the server side and the client side. Connect REST API (REST API) allows customers and partners to integrate with the Oracle Service Cloud platform using representational state transfer (REST) web services. Connect REST API is a public API that leverages the Connect Common Object Model version 1.3. It follows the Oracle REST standard and supports CRUD operations. PHP-based Connect for PHP APIs enable server-side integrations, while Connect Web Services for SOAP enable client-side integrations. WS-I compliant Connect Web Services follow SOAP 1.1 and WSDL 1.1 specifications, allowing developers to build integrations using a choice of development platforms. Both Connect for PHP and Connect Web Services for SOAP follow the Common Object Model, providing a unified developer experience and accessibility to customer’s data stored in the Platform’s extensible schema. Connect for PHP APIs allow for customizing the customer experience using Customer Portal Framework and for developing business logic in Custom Process Models. In addition, a SQL like query subsystem – ROQL (RightNow Object Query Language) – available through Connect for PHP and Connect Web Services, allows developers to extract data from Oracle Service Cloud’s database in CSV (comma separated values) format using simple queries.

Telephony Integration
The Oracle Service Cloud inherently integrates web, email, and social media channels, but it also provides a comprehensive toolkit for telephony-based integration, called the Oracle Multi-Channel Toolkit. This is a framework for creating CTI (Computer Telephony Integration) solutions for Oracle Service Cloud customers. The toolkit facilitates the implementation of common patterns and enables a common CTI experience for agents and administrators.

The toolkit is based on the Managed Extensibility Framework (MEF) which is part of the .NET framework, and is comprised of four programming assemblies. Features provided by the Oracle Multi-Channel Toolkit include:

» An extensible and customizable media bar
» Automatic active record synchronization with contact number detection for outbound dialing
» Support for multiple simultaneous interactions
» Support for voice, email, web and generic incidents
» Built in transfer support
» Interaction and agent state control
» Extensible screen pop capabilities, with built in screen pop handlers

More information on telephony integration can be found in the Multi-Channel Toolkit.

Cross-Channel Integrations
Oracle Service Cloud recognizes the value of integrating the various channels used by end users and gives companies the ability to communicate with those end users regardless of the particular channel. We do this by providing numerous integration capabilities, including Universal Queuing, Chat APIs, co-browse, RTC, Fax, and SMS integration.

Universal Queuing provides a set of consistent routing and service rules to apply across communication channels and which are surfaced to the agent in the Oracle Service Cloud’s unified Agent Console. With universal queuing
and unified agent capabilities, agents are empowered to use telephony, chat, and email in concert with a core common knowledge base to deliver a superior problem identification and resolution experience. All interaction and tool usage history is stored with agents’ notes into a universal customer experience record. With universal queuing, agent staffing across channels can be predicted and re-staffing can occur more quickly which improves service levels.

Oracle Service Cloud co-browse capability is a powerful online collaboration tool that enables your agents to see what your customers see. By creating an instant screen sharing experience without the installation required by other co-browsing products, companies further improve the experiences of their customers.

Chat third-party queue routing integrations can be implemented in the Oracle Service Cloud using open standards-based APIs that allow customers or partners to build integration solutions between Oracle Service Cloud Chat and third-party or universal routing and queuing platforms. Fax is also easy to integrate using the RightNow Connect API.

More information on Chat technologies can be found in our Chat APIs documentation and our Connect PHP API Cloud Service Developer’s Guide, and your Account Executive or Client Success Manager can provide additional details about all of our telephony or cross-channel integration capabilities.

SSO and SLO Integration

As Cloud-based computing becomes more prevalent and relied upon, and as the number of integration points expands for a typical customer, single sign-on becomes more necessary to the efficiency of your business. The Oracle Service Cloud Platform offers both Single Sign-On (SSO) as well as Single Log-Out (SLO) between Oracle Service Cloud applications and applications external to the Cloud.

When SSO and SLO are configured, a user can navigate from an application to any other application in the ecosystem. The Agent Desktop can become a unified gateway to other applications.

Figure 11. Agent Desktop

The Oracle Service Cloud supports integration with Service Providers existing within the Cloud as well as SPs external to the Cloud. That includes apps residing in other clouds. This integration is based on industry-standard SAML 2.0 for increased compatibility and, therefore, easier adoption. Setup is quick and easy, requiring just an
exchange of metadata between the external SP and the Oracle Service Cloud IdP, and some configuration verb settings to be made by the customer administrator.

In addition to SSO integration, Oracle Service Cloud Platform also allows for Single Log-Out (SLO) which provides improved security, enhanced usability, and easy implementation. With SLO, logging out of an Oracle Service Cloud session (IdP-initiated) will automatically terminate other SP sessions that were initiated by Oracle Service Cloud.

Oracle Service Cloud can also act as a Service Provider (SP), depending on a different application acting as the IdP. Simply stated, customers can continue to use their existing Identity Management system and access Oracle Service Cloud with the same set of credentials.

Since SLO is built into the SSO framework, SLO is automatically pre-configured for Oracle Service Cloud apps. Setup of SLO with external SPs is similar to and just about as easy as setting up SSO and requires just a few lines of code and a digital certificate.

**Conclusion**

The Oracle Service Cloud Platform gives organizations a dynamic, best-in-class tool set for creating a great customer experience. The Platform is purposely built for exceptional customer experiences. From the well designed global architecture, to the reliability and security controls, to the enterprise integration, extensibility, and operational maturity, the Oracle Service Cloud Platform provides organizations with the value they desire and the service their customers deserve.
Integrated Cloud Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

The Oracle Service Cloud Platform
May 2016
Author: Sean Montgomery
Contributing Authors: Steve Fangman