opentext™

WHITE PAPER

OpenText OCP Fundamentals

A technical overview of the OpenText Cloud Platform

Contents

Executive summary

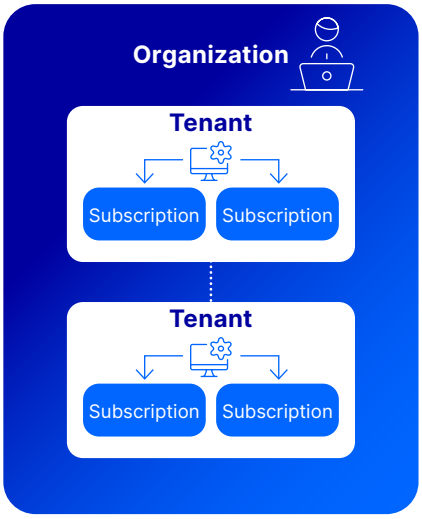
The OpenText™ Cloud Platform (OCP) is a next-generation Information Management as a Service platform powering the OpenText Core family of multi-tenant Software as a Service (SaaS) applications and services. OCP delivers information management applications and services in a highly secure and highly available multi-tenant architecture. This paper outlines the platform's key design characteristics, including its infrastructure components, platform tools, tenancy model, and administrative functions. It also describes the SLAs that govern platform operation.

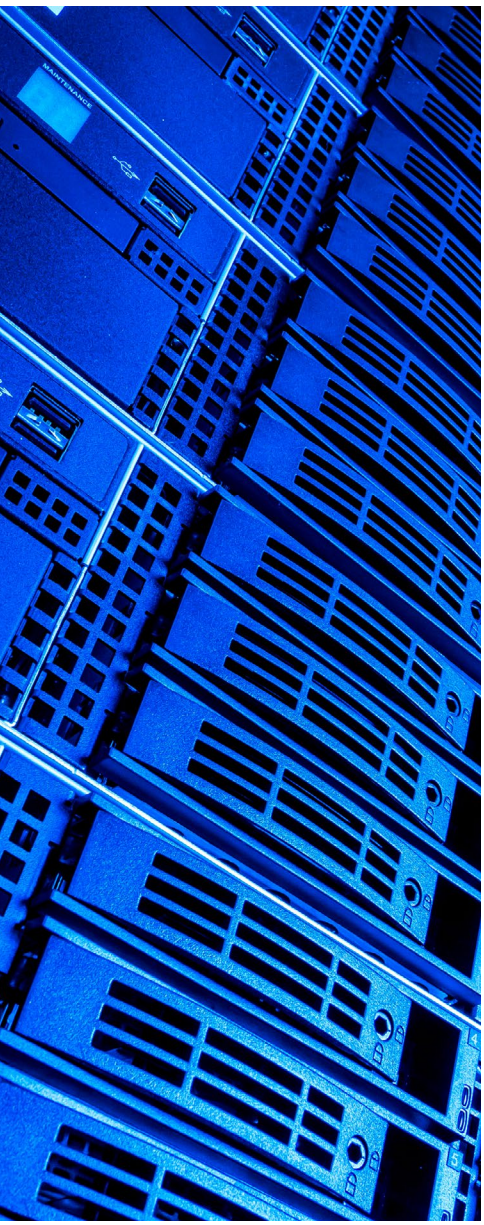
Security of content, transactions, and access is an essential element of the platform's design. This paper describes the platform technology that secures and protects content and communication and the additional compliance and governance measures in place on the platform to further protect customer content.

Core applications and services built on OCP include:

- OpenText™ Core Capture
- OpenText™ Core Capture for SAP® Solutions
- OpenText™ Core Capture - Thrust API
- OpenText™ Core Process Automation
- OpenText™ Core Content Management
- OpenText™ Core Journey
- OpenText™ Core Content Management for SAP® SuccessFactors®
- OpenText™ Core Collaboration for Engineering
- OpenText™ Signature Service - Thrust API

OCP tenancy and concepts



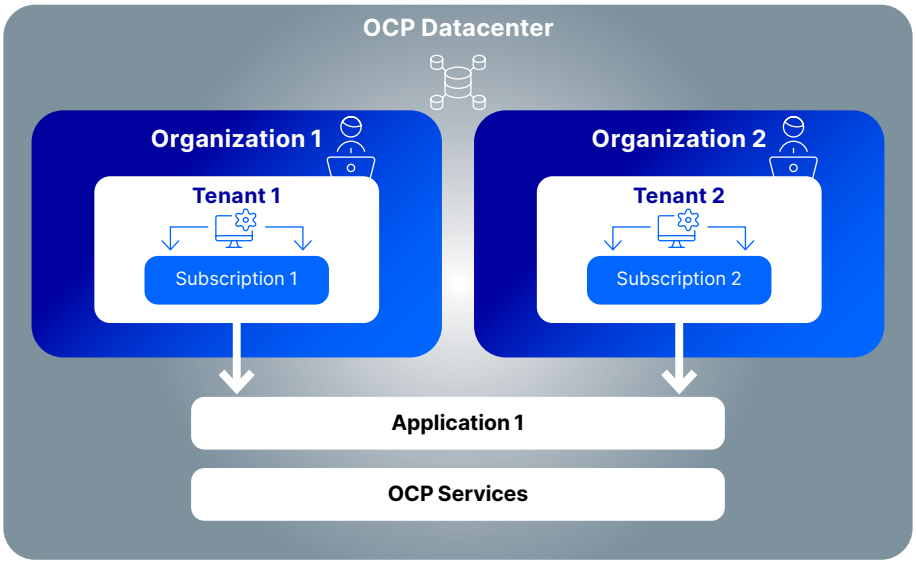


OCP is a fully compliant multi-tenant platform, where customer data in one tenant is isolated from customer data of other tenants. Multi-tenancy is built into multiple layers of the platform for isolation of:

- **Tenants**
  A tenant is a boundary for user and application subscription management.
- **Organizations**
  An organization is a collection of tenants scoped to a single customer.
- **Subscriptions to OCP applications**
  A subscription is a set of entitlements provided to a tenant for an OCP application.
- **Users and roles**
  Users are scoped within a tenant and roles are applied by administrators.
- **Authentication and authorization**
  Authentication in OCP is facilitated by OpenText Directory Services and based on roles scoped within a tenant and subscription.
- **Foundational Services**
  Foundational services underpin OCP and support a secure, highly available, and compliant platform.
- **Information Management Services**
  OCP Information Management Services provide applications high-value, re-usable capabilities that span across all OpenText technologies.

OCP platform infrastructure

Deployment



OpenText Core applications are multi-tenant SaaS applications created on OCP and run hosted in highly available public cloud data centers managed by OpenText or Google (GCP).

Storage

OCP offers foundational data storage for OpenText Core applications and customer developers.

OCP storage services are:

- Highly available
- Secure
- Redundant
- Backed up and available for recovery

Data center regions

OCP is deployed in data center regions located in North America, EMEA, and Asia-Pacific regions, with high availability between regions. All OCP applications and services run within the primary data center. Secondary data centers are clones of the primary with identical infrastructure and networks and aim to ensure high availability.

The OCP data center regions are as follows:

OCP geography	Data center region
North America	Canada
North America	United States
Asia-Pacific	Australia
EMEA	European Economic Area

Service level agreements (SLAs)

Incident response

OpenText makes a commitment to not only respond to service requests promptly and regularly report on their status, but also to restore service to affected users within a specific period of time following a service incident. Service restoration time objectives are linked to incident severity. Restoration may take the form of a root cause resolution or application of a workaround that enables users to access the system while troubleshooting and implementation of a permanent solution continues.

Disaster recovery

If OpenText declares a disaster event that impacts delivery of the OCP applications or services from the primary data center facility, we will restore service in the designated alternate facility for that data center region. The

target recovery time objective (RTO) following an OpenText declared disaster is 8 hours* and the target recovery point objective (RPO) is 4 hours.

- Current RTO = 8 hours*
- RPO is the age of files/data that must be recovered for normal operations to resume in the event of disaster or disruption.
- Current RPO = 4 hours

In the event of the loss of the primary data center, the data stores replicated to the secondary data center are mounted and made accessible.

OpenText provides a service with high availability to customers to ensure the continuity of cloud services in case of operational disruption (as declared by OpenText in accordance with the company's availability definition and policies). The service high-availability procedures will be used to reinstate production instance service levels by failing over to a secondary data center employing redundant facilities, systems, networks, hardware, and software.

The most recent available backups of the production instance will be used to restore content. All recoverability services are designed to support the RTO and RPO. OpenText will test the applicable high availability processes once annually to ensure technical and operational readiness.

*RTO may differ in EMEA. Please refer to your contract for specific details.

Availability

Availability SLAs may vary by type of cloud service being provided; however, the following is standard guidance for application SLAs:

- Availability is measured monthly and excludes scheduled downtime.
- 99.9 percent high availability with redundancy of major solution components is the targeted duration of time and a service level within which a service must be restored after a disaster (or disruption).

Maintenance

Upgrade and patching of the backing data and infrastructure components of OCP occurs during a standard maintenance window, Friday 21:00-2:00 EST for North America data centers, Saturday 2:00-6:00 UTC for the EMEA data center, and Friday 10:30-14:30 UTC for the Asia-Pacific data center.

During this scheduled maintenance window, the platform may be partially or completely unavailable.

Data retention

Various national, state, and country-specific laws require OpenText to maintain certain types of records for particular periods. Failure to maintain such records could subject OpenText and its personnel to penalties and fines. Applicable laws and regulations may also require that certain types of records

be destroyed within an appropriate time period. This can include certain health-related data and personal privacy data of OpenText or its customers. In general, such regulations require that sensitive data be retained no longer than is necessary for the purpose for which the data was obtained.

All services and their stored data are backed up multiple times per day. Additionally, all OCP backup storage repositories have a three-month retention period.

Secure communication and content encryption

Data encryption in transit

Transport Layer Security (TLS) provides data encryption in transit between the user and OCP. The benefits of TLS include data confidentiality and data integrity.

Data encryption at rest

The primary OCP Content Storage is protected by AES 128-bit encryption. The Data Encryption Keys (DEK) are encrypted with Key Wrapping Keys before being persisted.

Security scanning

Digital reputations and signature recognition are used to detect threats and to detect malicious content being uploaded to OCP.

User-level security

Enterprise users need to collaborate with others both within and outside the organization without security concerns hampering productivity. OCP's robust security infrastructure and advanced, yet simple security controls allow users to work productively without hassle.

When collaborating in OCP, users can protect content by specifying permissions at a granular level, for example, allowing certain users "view only" access while giving others the ability to modify.

Enterprises can leverage existing single sign-on (SSO and SAML) infrastructure, so users don't need to remember another username and password. These user-level features allow businesses to strike the appropriate balance between productivity and IT control with minimal maintenance overhead.

Network security

OCP provides robust solutions to detect and address network security threats as information flows between OCP and customer and any third-party systems. OCP continuously monitors its entire network stack. When events are detected, alerts are sent to on-call operations staff for immediate resolution.

To protect the systems from DoS (denial of service) attacks and ensure availability, OCP employs carrier-grade network equipment and redundant

internet links, as well as native secure networking infrastructure and application gateways. To ensure the security of the platform against increasingly sophisticated threats, OCP performs weekly vulnerability scans and engages with third-party security firms to perform penetration and application vulnerability testing.

Internal development process

The OCP application is designed with security as a key consideration at every stage. The web application is multi-tiered into logical segments (front-end, mid-tier, and database). This provides maximum protection while giving developers the flexibility of a multi-layer architecture.

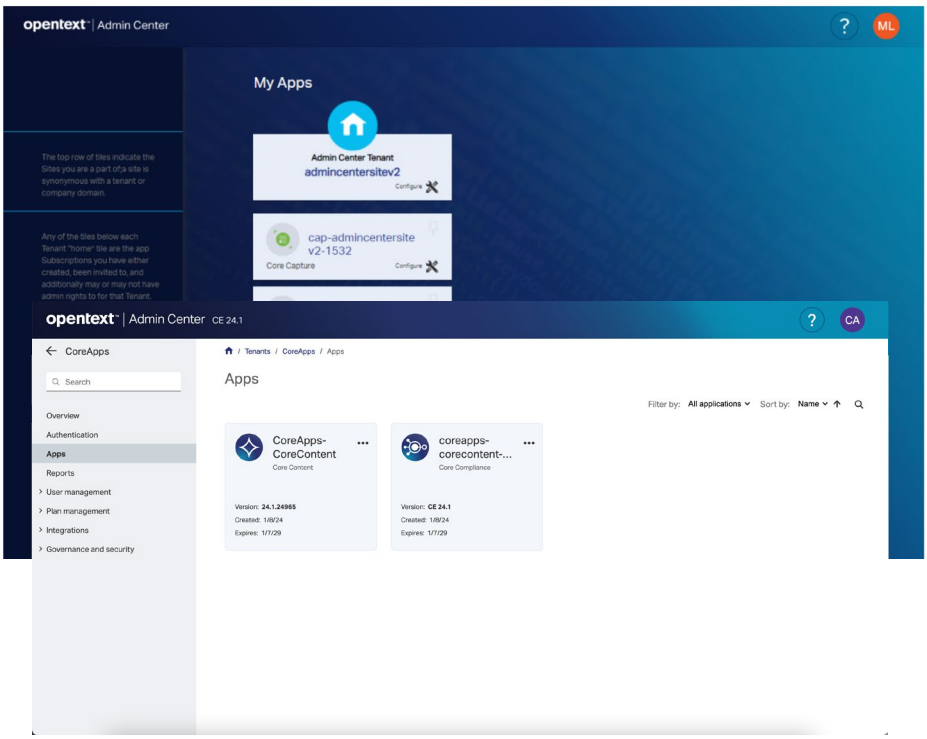
OCP application development goes through multiple checks and balances to ensure that development or testing processes do not impact the production systems and data. These checks include putting every change through a formal release engineering process, maintaining logically separate development environments and performing full functional testing of all changes in a QA environment before deployment to production. Following this rigorous development and release process allows OpenText to deliver new features and improvements while maintaining a solid and secure foundation.

Admin Center

Admin Center is the management console for OCP administration. Admin Center provides customer administrators with a single control point to configure OCP applications, users, and integrations with other OCP applications or on-premises systems, as well as view reports on the applications and users.

Using Admin Center, administrators can manage:

- Users and groups
- Authentication and authorization platforms, either built into OCP or via SAML authentication integration
- Password and two-factor authentication policies (for native OCP authentication)
- Application role management
- API integration management

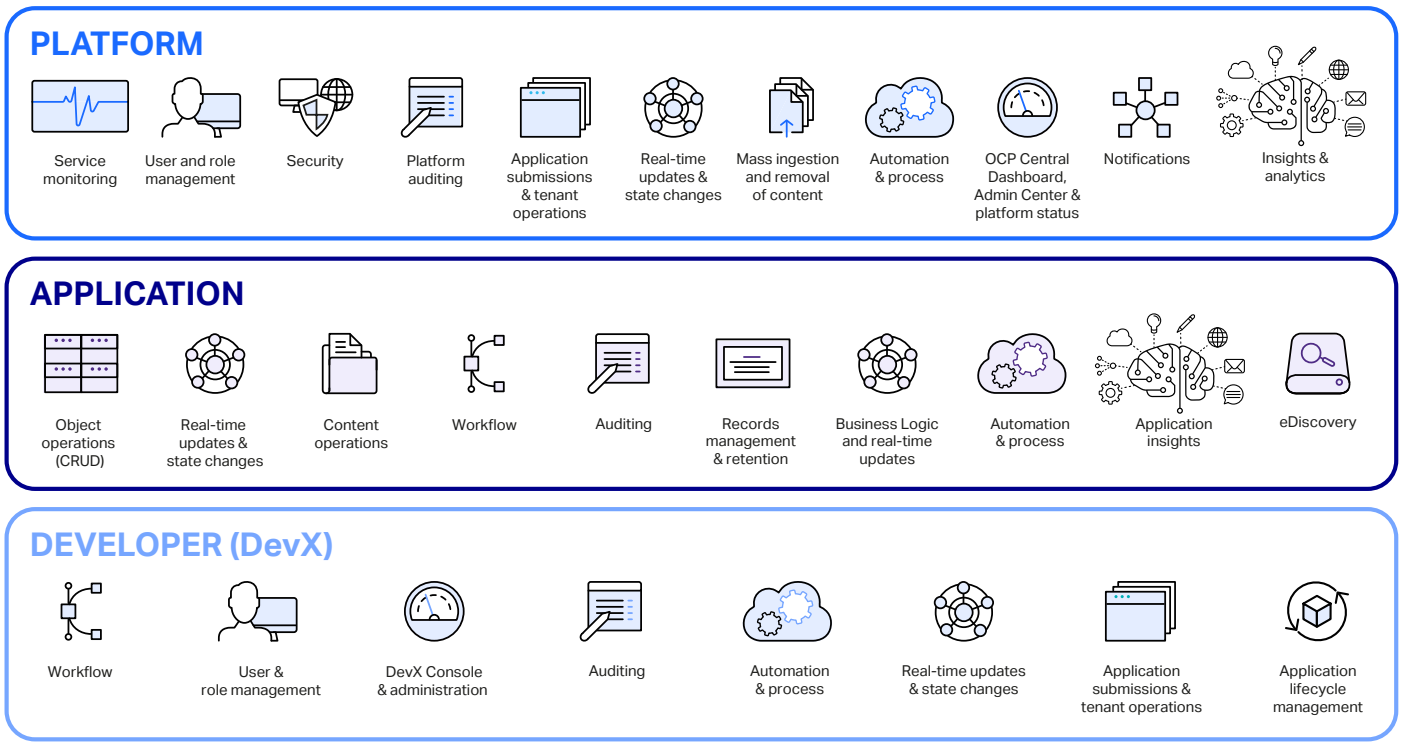


Authentication, authorization, and user synchronization

OCP authentication (AuthN), authorization (AuthZ), and user synchronization are provided by OpenText Directory Services (OTDS). OTDS is an industry leading authentication technology, capable of handling all industry standards including OAuth, SAML, OpenID Connect, and multi-factor authentication. Additionally, OCP also supports third-party cloud providers such as AzureAD®, PingIdentity®, and Okta®. This is accomplished through OTDS' support of the SCIM provisioning standard. All AuthZ, AuthN and user synchronization is provided via Admin Center.

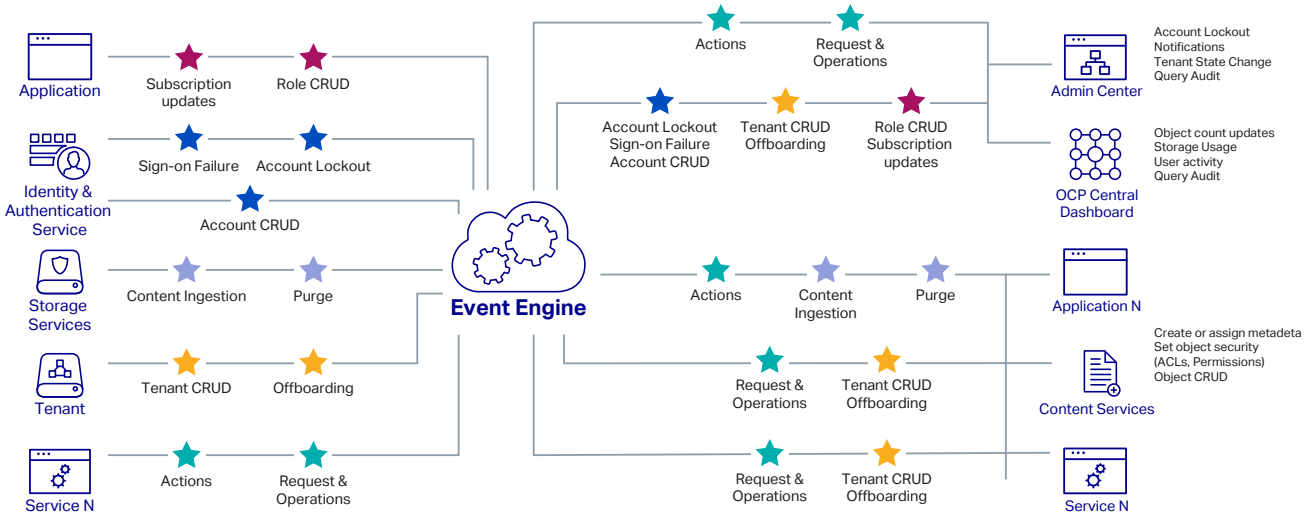
Auditing and eventing

Modern day IoT, communications, housekeeping, and analytic architectures depend on and use event frameworks at their core. Event-driven architecture decouples service to service communication and relies on a common microservice approach. Decoupling of service integration allows for independent scaling and minimizes impact of failures. Audits are handled automatically via direct integration into the OCP eventing subsystem. This requires no direct integration between other services with audit. On-demand, push-based architecture allows for reactive operations without continuous polling needed, resulting in lower costs and higher efficiency.



OCP eventing is a feature-rich subscription and consumption framework that allows for the creation of any event, at any time, with any information. Those events can then be consumed by any service or application deployed on OCP or hybrid. OCP eventing offers the ability to build customized business logic and triggers tailored directly to business requirements and use cases. Once an integration has been completed no additional maintenance is required to uphold it.

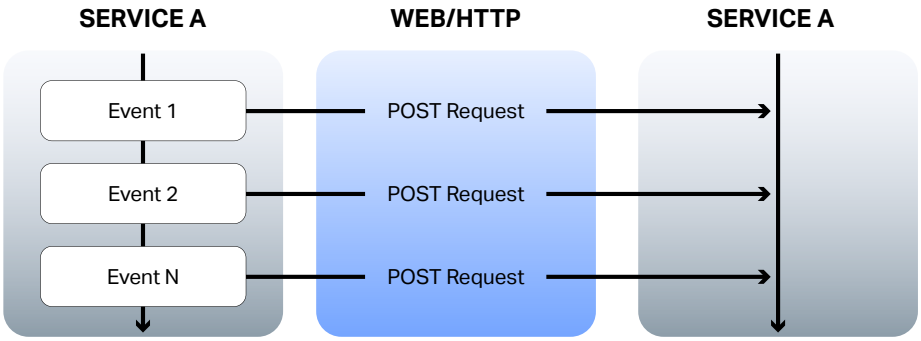
Furthermore, communications are dynamic and asynchronous, allowing for tasks and jobs to be completed after the request has been made. There are no API dependencies on versioning, further decoupling service to service communications. This reduces the dependency on API changes of consuming services as no direct integration is required.



Platform, security, and inter-service communications (Bi-directional)

Webhook support

Webhooks provide and allow for real-time status and reactions via HTTP web requests. This removes the requirement for redundant status requests, queries, and unnecessary polling.



Compliance and governance

OpenText is committed to customer success and protecting client information through both product design and the definition and application of policies that govern delivery of those products as cloud services.

The General Data Protection Regulation (GDPR) is considered the toughest privacy and security law in the world. OCP is GDPR compliant, providing protection for personal data, the data subject, the data controller, and the data processor, as well as any action or processing of the data. OCP upholds PII and data sovereignty standards and customer data is not directly accessible by OpenText.

OpenText holds the following certifications:

- ISO 27001
- ISO 27017
- ISO 27018
- SOC2 Type II