WHITE PAPER

OpenText OT2 Fundamentals
A technical overview of the OT2 platform
Contents

Executive Summary 3
OT2 Tenancy and Concepts 3
OT2 Platform Infrastructure 3
  Deployment 3
  Storage 3
  Data Centers 4
  Platform Backing Services 4
Service Level Agreements 5
  Incident Response 5
  Disaster Recovery 5
  Availability 5
  Maintenance 5
  Recovery 5
  Data Retention 6
Secure Communication and File Encryption 6
  Secure File Encryption in Transit 6
  Secure File Encryption at Rest 6
  Security Scanning 6
  Geo Blocking 7
Admin Center 7
  Authentication, Authorization, and User Synchronization 8
  Auditing and Eventing 8
  Webhook Support 9
Compliance and Governance 10
About OpenText 10
Connect with us 10
Executive Summary

OpenText OT2 is a next-generation Information Management as a Service platform. OT2 is purpose-built for delivering Information Management applications and services in a highly secure and highly available multi-tenant architecture. This white 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 operation of the platform.

Security of content, transactions and access is an essential element of the platform's design. This white 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.

OT2 Tenancy and Concepts

OT2 is a fully multi-tenant platform where customer data in one tenant is fully isolated from customer data in a different tenant. Multi-tenancy is built into multiple layers of the platform for isolation of:

- Users and roles
- Authentication and authorization
- Foundational services
- OpenText Core applications

OT2 Platform Infrastructure

Deployment

OpenText Core applications are web-based content management applications created on the OT2 platform and run on Cloud Foundry, an open-source enterprise platform designed to run cloud applications (with the exception of OpenText Core Capture, which is Windows based). Cloud Foundry is deployed through BOSH, which orchestrates VM and software deployment to VMware vCenter. All Cloud Foundry applications in production are software-virtualized Linux containers with additional support for Windows Docker containers.

BOSH VMs are deployed by the BOSH director using YAML manifest files that provide all of the parameters necessary to deploy the VMs and BOSH stemcells, which are minimal OS templates with BOSH agents installed. The director stores the configuration state of the VMs it deploys, including the path to the persistent disks of all of the VMs. The configuration of the BOSH director and all manifest files are saved under source control.

Storage

BOSH VMs have a minimum of two disks. The first disk is the OS disk and the second disk is used for software packages and logs. Any necessary persistent data is stored on a third persistent disk. While the first two disks can be destroyed and recreated with the VM at any time, the persistent disk is always unmounted and remounted to the new VM. The persistent disks hold critical data such as databases and indices. The persistent .vmdk disk files are backed up at the vSphere datastore cluster level. The datastores are mounted to vCenter via NFS from NetApp appliances. The data is protected by snapshots, incremental and full backups and replication to the secondary site.
Data Centers

The OT2 platform runs on Cloud Foundry and is deployed with BOSH on VMWare vSphere. BOSH VMs are ephemeral and are designed to be recreated at any time with new, unique UUIDs and hostnames.

OT2 is deployed in paired data centers located in the North America and EMEA regions and employs an active/passive data center approach to ensure high availability. All OT2 applications and services run within the primary data center. The secondary data center is a clone of the primary with identical infrastructure and networks. Data is replicated every 5 minutes to the secondary site. DNS is configured to send users to the primary site unless access to the platform in that facility is disrupted or degraded, in which case customer traffic is re-routed to the secondary facility.

The primary and secondary OT2 data center locations are as follows:

**North America**
- Lithia Springs, Georgia (LI3) production environment
- Allen, Texas (AL3) disaster recovery environment

**EMEA**
- Amstelveen, NL (AM3) production environment
- Munich, DE (MU4) disaster recovery environment

Separate test and development environments are operated in the OpenText data center in Brook Park, Ohio.

Platform Backing Services

Core applications leverage OT2 Foundation and Platform Backing Services. These Backing Services along with Cloud Foundry form our Platform as a Service (PaaS) layer which sits on top of the infrastructure layer.

Some of these backing services are:
- Cassandra (NoSQL)
- Graylog (logging)
- Apigee (API management)
- Solr (search)
- PostgreSQL (database service)
- Kafka, RabbitMQ (messaging, eventing)
Service Level Agreements

Incident Response

OpenText makes a commitment to not only respond to a service request promptly and regularly report on its status, but to also 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

In the event OpenText declares a disaster event that impacts delivery of the OT2 applications or services from the primary data center facility, OpenText 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 12 hours and the target Recovery Point Objective (RPO) is 4 hours.

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% 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).
- Current RTO = 72 hours
- Recovery Point Objective (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

Maintenance

Upgrade and patching of the backing data and infrastructure components of the OT2 platform occurs during a standard maintenance window every Friday 9pm - 2am, local data center time.

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

Recovery

In the event of the loss of the primary data center, the datastores replicated to the secondary data center are mounted and made accessible. The Domain Name System (DNS) is updated to point to the secondary site instead of the primary site. The BOSH director is bootstrapped into the secondary data center using the saved configuration files, stemcells and binaries. After the director has been bootstrapped in the secondary site, all of the VMs deployed by the director are recreated using the director's saved configuration data and identical stemcells. Once all of the BOSH VMs are recreated, the apps and services are started in the secondary site. After the apps and services have been started, the secondary site is promoted to the primary site, and the original primary site becomes the new secondary site once access to the facility is restored.
OpenText provides a disaster recovery service to customers to ensure the continuity of the cloud services in a disaster situation (as declared by OpenText in accordance with the company's disaster recovery policies and procedures). The disaster recovery service will be used to reinstate the 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 Recovery Time Objective and Recovery Point Objective specified in the Order. OpenText will test the applicable disaster recovery processes once annually to ensure technical and operational readiness.

**Data Retention**

Various national and state 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.

<table>
<thead>
<tr>
<th>Storage</th>
<th>Snapshots</th>
<th>Incremental Backups</th>
<th>Full Backups</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Clusters</td>
<td>• Snapshot taken every 4 hours (1,5,9,13,17,21 at 5 minutes)</td>
<td>Daily</td>
<td>Weekly</td>
<td>3 months</td>
</tr>
<tr>
<td></td>
<td>• Retain 7 snapshots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Oldest snapshot is 24 hours old</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trident SVM</td>
<td>• Snapshot taken every 4 hours (1,5,9,13,17,21 at 5 minutes)</td>
<td>Daily</td>
<td>Weekly</td>
<td>3 months</td>
</tr>
<tr>
<td></td>
<td>• Retain 7 snapshots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Oldest snapshot is 24 hours old</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Secure Communication and File Encryption**

**Secure File Encryption in Transit**

Transport Layer Security (TLS) provides file encryption in transit between the user and the OT2 platform. The benefits of TLS include strong authentication, message privacy and integrity, enabling the detection of message tampering, interception and forgery.

**Secure File Encryption at Rest**

OT2 Content Storage is protected via Data Encryption Keys (DEK) as well as Role Based Access Control (RBAC) to protect the DEKs themselves. Every piece of content ingested into OT2 is secured and protected. Hardware key management is also employed to encrypt data.

**Security Scanning**

Digital reputations and signature recognition are used to detect threats and prevent malicious content from being uploaded to the OT2 platform.
**Geo Blocking**

OpenText commercial environments are protected with next generation and advanced threat prevention firewalls that have extended capabilities beyond traditional security access lists, including the ability to restrict certain countries to access the environments based on geo protection. This mechanism allows the firewalls to maintain a database that maps IP addresses to countries, satellite providers and anonymous proxies. This database is updated periodically, fetched from different sources and IP intelligence feeds. The mechanism to implement such protection is similar to a traditional access list, with the ability to block certain countries as a source, as a destination or both.

Within OpenText commercial environments we are currently blocking the following embargoed countries from access to our platforms: Cuba, Sudan, North Korea, Venezuela and Iran.

**Admin Center**

Admin Center is the management console for OT2 administration. Admin Center provides customer administrators with a single control point to configure OT2 applications, users, integrations with other OT2 applications or on-premises systems and view reports on the applications and users. Using Admin Center, administrators manage:

- Users and groups
- Authentication and authorization platforms, either built into the OT2 cloud or SAML authentication integration
- Password and 2-factor authentication policies (for native OT2 cloud authentication)
- Application role management
- API integration management
Authentication, Authorization, and User Synchronization

OT2 authentication (AuthZ), authorization (AuthN) and user synchronization are provided by internal and heavily integrated OTDS. Leveraging OTDS, the platform is capable of handling all industry standards including Oauth, SAML, OpenID Connect, and Multi-Factor Authentication. Extended, OT2 also supports third party cloud providers such as AzureAD, Ping and Okta. This is accomplished by 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. Audit is handled automatically via direct integration into the OT2 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.
OT2 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 OT2 or hybrid. OT 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 said integration.

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.

### 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 to be the toughest privacy and security law in the world. The OT2 platform is GDPR compliant, providing protection for personal data, the data subject, the data controller, the data processor, as well as any action or processing of the data. OT2 upholds PII and data sovereignty standards, and customer data is not directly accessible by OpenText.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn