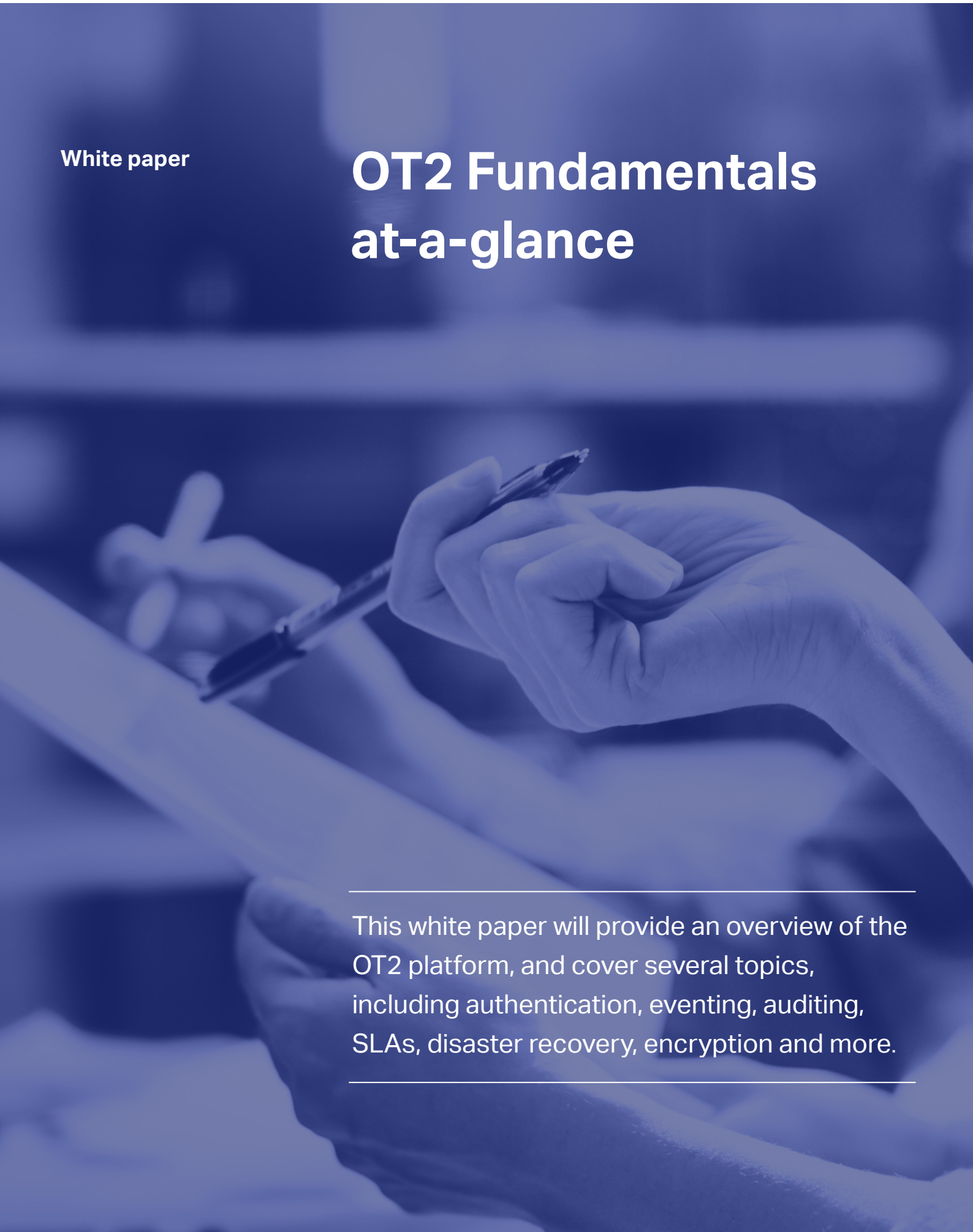
opentext™

White paper

# OT2 Fundamentals at-a-glance



This white paper will provide an overview of the OT2 platform, and cover several topics, including authentication, eventing, auditing, SLAs, disaster recovery, encryption and more.

opentext™

## Contents


| | |
|---|---|
| Executive summary | 3 |
| OT2 Platform infrastructure guide | 3 |
| Secure communication and file encryption | 6 |
| OT2 Tenancy and Concepts | 7 |
| Admin Center | 7 |
| Authentication, authorization, and user synchronization | 7 |
| Eventing and auditing | 8 |
| Compliance and governance | 8 |

opentext™

## Executive summary

This white paper will outline the basic concepts of the OT2 Platform including the architecture and design of OpenText's data centres, and the various authentication and authorization mechanisms of the platform. This also includes the steps to remediation covered under the disaster recovery, and the multi-scale abilities of the OT2 highly available platform.

Security of content, transactions, and access is a top priority of the platform. This paper will cover how all content and communication on the platform is secured and kept safe, how the technology ensures this, and additional measures in place to protect content.

The document will describe the tenancy concepts of OT2, along with the platform's administration, provided by OpenText Admin Center. Lastly, compliance implementations such as GDPR, PII, and other data compliance and sovereignty topics will be covered along with the corresponding current SLAs.

## OT2 Platform Infrastructure Guide

### 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 every time the VMs are recreated. The OT2 platform uses an active/passive data center approach. All Core applications and services (ETS, OTDS, etc.) run within the primary data center. The secondary data center is a clone of the primary, with identical infrastructure and networks. DNS is configured to send users to the primary site. All customer traffic is sent to the primary site and the only VMs running on the secondary site are the infrastructure VMs used to keep the secondary site operational.

The development and test deployments are in the Brook Park data center, while the OT2 production environments are as follows:

**North America**

- Lithia (LI3) production environment
- Allen (AL3) disaster recovery environment

**EMEA**

- Amstelveen (AM3) production environment
- Munich (MU4) disaster recovery environment

### Service Level Agreements (SLAs)

OpenText makes a commitment to not only respond to a service request promptly and regularly report on its 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.

In the event OpenText declares a disaster event that impacts delivery of the Core Cloud 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 24 hours and the target Recovery Point Objective (RPO) is 8 hours.

Specific SLAs may vary by type of cloud service being provided, however, in general 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 hrs.
- 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 hrs.

### 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 Bidirectional-Streams over Synchronous HTTP (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 Virtual Machines (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.

### Testing

OpenText shall provide a disaster recovery service to customers to assure the continuity of the Cloud Services in a disaster situation (declared by OT's sole discretion in accordance with OT'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.

### Deployment

Core applications on OT2 are web-based content management applications created on the platform and run on Cloud Foundry an open source enterprise platform designed to run cloud applications. 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.

opentext™

### Maintenance

The backing data components and infrastructure for OT2 still have a need for standard maintenance windows for upgrades and patching.  OT2 follows the OpenText standard by having an optional-use maintenance window every **Friday 9pm - 2am**, local data center time.

During this time, service may be partially or completely unavailable.

### 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 Retention

Legal Retention Requirements and Limitations

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 such sensitive data be retained no longer than is necessary for the purpose for which such data was obtained.

| Storage | Snapshots | Incremental Backups | Full Backups | Retention Period |
|---|---|---|---|---|
| **vSphere Clusters** | • Snapshot taken every 4 hours (1,5,9,13.17,21 at 5 min)<br>• Retain 7 snapshots<br>• Oldest snapshot is 24 hours old | • Daily | Weekly | 3 months |
| **Trident SVM** | • Snapshot taken every 4 hours (1,5,9,13.17,21 at 5 min)<br>• Retain 7 snapshots<br>• Oldest snapshot is 24 hours old | • Daily | Weekly | 3 months |

### Platform Tools

Anything deployed on Cloud Foundry is considered a service, with services and tools available to provide persistence, storage, logging, and search.

The following as a minimum will be deployed in the OT2 platform:

RabbitMQ (messaging broker, will be superseded by Kafka based service in future)

PostGreSQL

1. Cassandra (NoSQL)
2. xDB (XML Database)
3. Graylog (logging)
4. Apigee (API Management)
5. Solr (search)

## Secure communication and file encryption

### Secure file encryption in transit

Transport Layer Security (TLS) is leveraged for file encryption in transit. 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 the OT2 platform is secure and protected. During transmission of data, all content is encrypted and scanned from a software perspective. Hardware key management is also leveraged to provide complete data coverage. Digital reputations and signature recognition are used to detect threats and prevent malicious content from being uploaded into any part of OT2.

## 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
- Core Applications

## Admin Center

Admin Center is the management console for OT2 administrations. Admin Center provides customers with a single control point to configure OT2 applications, users, integrations with other OT2 application 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 Authorization (AuthZ) and Authorization (AuthN) along with user synchronization is provided by internal and heavily integrated OTDS. Leveraging OTDS, the platform is capable of handling all industry standard including Oauth, SAML, OpenID Connect, and Multi-Factor Authentication. Extended, OT2 also supports 3rd 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.

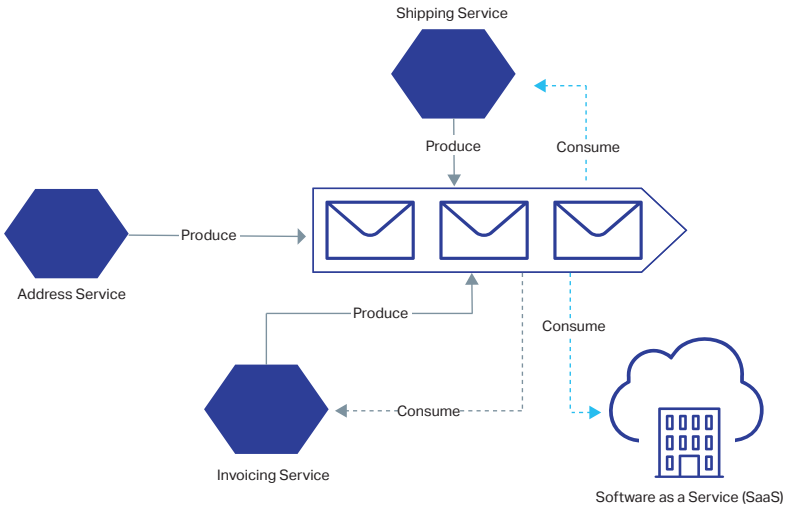
opentext™

OpenText OT2 Webpage

Read the blog posts

## Eventing and Auditing

Eventing and Auditing capabilities are provided by a heavily platform integrated eventing subsystem and framework. These components manage events, consumers, and producers. Every service within OT2 will generate corresponding events, that can be acted upon by other services or applications. Auditing capabilities are also integrated into this system to log every instance of an action and corresponding objects. Audi trails keep activity records for objects, files, and content. An audit trail provides assurance of the integrity of the electronic content and its record(s). Complete audit tracking of all instances, objects, transactions, and administration actions on the platform are logged accordingly.




## Compliance and Governance

OpenText™ is committed to customer success and protecting client information, both in the product portfolio and in the approach taken within its corporate policies.

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, meaning that it provides protection for personal data, the data subject, the data controller and the data processor, as well as any action or processing of the data. OT2 upholds PII and data sovereignty standards, and your data is not directly accessible by OpenText.


GDPR

## 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

**opentext.com/contact**