opentext™

OpenText™ Documentum™ Server CE 23.2

Release Notes

1 Introduction

These Release Notes provide an overview of Documentum™ Server 23.2, including new features, delivery information, and supported platforms.

OpenText recommends that you read these Release Notes in conjunction with the documentation included with the software package. If any conflicts exist, the Release Notes supersede the other documentation.

We also recommend that you check OpenText My Support for any patches or documentation updates that may have been posted after the initial release of this product.

1.1 Release Notes revision history

Revision date	Sections revised	Description of revisions
April 2023	First release.	All new content.
May 2023	Improvements and new certifications in CE 23.2	Support for AWS Aurora Serverless PostgreSQL v2

2 About Documentum™ Server 23.2

This section provides an overview of Documentum™ Server 23.2.

Documentum Server is the core of the Documentum content management platform. Documentum Server governs the content repository and enables a set of content management services for controlling content and processes throughout distributed enterprises. Documentum Server lets you store, manage, and deploy all types of content, including HTML and XML, graphics, and multimedia. Documentum Server provides services such as the following:

- Integrated workflow
- Lifecycle and process automation
- Version control
- Security
- Data dictionary for capturing and configuring business rules

With Documentum Server, users can share and reuse trusted content on demand within and between business units. Administrators can define, organize, automate, and monitor all the functions and tasks of complex business processes. Documentum Foundation Services (DFS) is no longer installed with Documentum Server. You must install a DFS server on a machine that is different from the one on which Documentum Server is installed.

2.1 New features

Documentum™ Server 23.2 includes the following new features.

2.1.1 IPv6 certification

Documentum CE 23.2 has been enabled to support both IPV6 and IPv4 for modern deployments. IPv6 is the successor to the widely used Internet protocol version 4 (IPv4 or IP). IPv6 support enables you to easily integrate Documentum instances into your network, regardless of the IP version used. Documentum supports both mixed IPv4 and IPv6 environments as well as pure IPv6 setup.

Please refer to the product documentation for configuring the Documentum instance for IPv6.

2.1.2 Java 17 certification

Documentum CE 23.2 supports the latest LTS releases of Java 17. Documentum Platform supported Java 11 in releases prior to 23.2 and starting 23.2, Java 17 is supported as well at runtime across all Documentum components. All Documentum deployments can now use Java 17 JDK including the installation and configuration.

2.1.3 Optimization/reduction of pod restart time

Documentum pods startup times have been optimized and reduced significantly. For example: All Documentum Sever pods restart (other than during fresh install or upgrade) are optimized to come up in under few minutes for better resiliency and to better enable developers to be able to use cloud environments to develop on.

2.1.4 Supporting a custom Install Owner

Documentum deployments now support a custom install owner. Prior to Documentum CE 23.2, customers used "dmadmin" as Documentum install owner. Starting 23.2, they can now use a different account for improved security and easier Cloud Adoption from existing deployments.

2.1.5 Fetching images from Docker image registry using Pull Secrets

Administrators can pull Documentum images from a private container image registry or repository using a secret. A pull secret can be configured in the HELM Charts. Please refer to the product documentation and below link for more details:
https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/

2.1.6 AWS CSI Dynamic Provisioning

Documentum CE 23.2 supports AWS CSI dynamic provisioning of persistent volumes (PVs). Prior to CE 23.2, static provisioning was supported. AWS introduced dynamic provisioning support using EFS Access points, which are app specific entry points into an EFS file system and allow up to 120 PVs to be automatically provisioned within a single file system. Deploying Documentum into AWS Kubernetes environment allows cloud administrators to leverage dynamic provisioning of PVs using AWS EFS-CSI driver. Please refer to the below link for more details:
https://aws.amazon.com/blogs/containers/introducing-efs-csi-dynamic-provisioning/

2.1.7 Decoupling of Product and Base Images

Documentum CE 23.2 provides extensibility for a customer to upgrade the base image Operating System independent of the application. For applications that are deployed on an application server, a base image OS is provided along with the product image. This helps in keeping the OS image that has pre-configured application server and Java up to date.

2.1.8 Latest Kubernetes Platforms and Updated Helm Charts

Documentum CE 23.2 continues to provide improved capabilities and latest version support for Docker, Kubernetes, and Helm Charts. Documentum now supports latest Kubernetes platforms with K8s clients and K8s server versions of 1.23.x and 1.24.x for public clouds.

2.1.9 Improvements and new certifications in CE 23.2

Feature	**Benefit**
SQL Server 2022	Documentum CE 23.2 now supports the latest version of SQL Server Database
RHEL 9.x as the base Operating System container image	Documentum reference containers have RedHat Enterprise Linux 9.x certified as base OS image. Please refer to the *OpenText Documentum Platform Infrastructure Certification Guide* for supported databases with this RHEL version
Java Method Server (JMS) supports Apache Tomcat 9.0.71	Embedded JMS in Documentum Server has a newer hardened version of Apache Tomcat 9.0.71
Postgres 15.x	The latest version of Postgres database is certified in this release.
Latest JDK 17	Latest JDK 17.0.6 is certified in this release.
Ubuntu 22.04.x LTS	Documentum supports latest version of Ubuntu 22.04.x LTS as an operating system. Please refer to the *OpenText Documentum Platform Infrastructure Certification Guide* for supported databases with this Ubuntu version
AWS Aurora Serverless PostgreSQL v2	Documentum 23.2 CE now supports AWS Aurora Serverless PostgreSQL v2 given the scaling and cost benefits for production and peak capacity workloads. Also, customers can take advantage of the services Documentum supports in their chosen hyper scaler.

2.2 Discontinued and deprecated features

OpenText Documentum deprecates and discontinues software components and features in a phased approach. In the first stage, features are deprecated to inform Documentum customers. Deprecated features should not be used in new implementations. The functionality is retained but customers are encouraged to consider alternatives or plan to migrate in accordance with the migration path provided by Documentum. In the second stage, the feature is discontinued and is removed from the product and certain cross-product compatibility is no longer maintained.

With CE 21.4 and later versions, Documentum Workflow Designer and Process Engine, previously part of Business Process Manager (BPM), were included with Documentum Platform. This provided customers with advanced workflow capabilities. Documentum Workflow Manager and related plug-ins that are packaged with Documentum Composer are now replaced with the advanced workflow capabilities described in this section. Documentum Workflow Manager may be removed in a future release and customers are recommended to plan accordingly.

In Documentum Server CE 20.3, traditional mechanisms of Single Sign On (SSO) supported by Documentum Server were deprecated with a go-forward replacement option with OpenText Directory Services (OTDS). OTDS offers industry standard SSO and user/group management capabilities. The older authentication plugins are removed from the released binaries of CE 21.4. OTDS integration with Documentum provides a more flexible alternative with support for multiple SSO and identity providers and with native cloud support.

Documentum supported LDAP synchronization and authentication are now deprecated in lieu of the synchronization and SSO support offered by OTDS. The LDAP synchronization functionality is still accessible for customers to plan their migration. Starting CE 21.4, Documentum offers leading practices for customers to migrate from traditional LDAPv3 providers to OTDS.

2.2.1 Discontinued

The following features have been discontinued in this release:

Documentum CE 23.2 no longer supports Postgres 10.x and 11.x as a database since these versions of the database are out of standard support in November 2023. Documentum provides options to use Postgres 12.x up to the latest version of Postgres 15.x. Also, SQL Server 2016 is out of standard support by its vendor and no longer supported by Documentum.

Documentum CE 23.2 no longer supports RHEL 6.x, Ubuntu 16.04.x LTS, Ubuntu 18.04.x LTS and Windows Server 2016 as operating systems. Customers are provided with latest options of these operating systems. RHEL 7.x, 8.x and 9.x is certified. Ubuntu 20.04.x LTS and Ubuntu 22.04.x LTS versions are supported. Windows Server 2019, 2020, and 2022 is certified with the latest Documentum CE release. Please refer to the *OpenText Documentum Platform Infrastructure Certification Guide* for supported operating systems and databases.

Starting Documentum CE 22.4, reference docker images and HELM charts for Ubuntu operating system have been deprecated and discontinued. Customers can build their own images using the docker scripts and other packaging artifacts that have provided.

3 Downloads

Downloads for Documentum™ Server is available on My Support.

To search and download the list of software binaries on OpenText My Support, perform the following steps:

1. For product releases 22.4 or later, on the Home page, click **Knowledge** > **Software Downloads**.
2. In the **Search the Knowledge Base** box, type **#DocumentumServer23.2SoftwareDownloads** and then click **Search**.

Notes

For product releases prior to 22.4, on the Home page, click **Knowledge** > **Software Downloads** and use the additional filters.

4 Documentation

Documentation for Documentum™ Server is available on My Support.

To search and download the list of documentation on OpenText My Support, perform the following steps:

1. For product releases 22.4 or later, on the Home page, click **Knowledge** > **Product Documentation**.
2. In the **Search the Knowledge Base** box, type **#DocumentumServer23.2Documentation** and then click **Search**.

Note

For product releases prior to 22.4, on the Home page, click **Knowledge** > **Product Documentation** and use the additional filters.

5 Supported environments and compatibility

For information, see *OpenText Documentum Platform Infrastructure Certification Guide*.

6 Installation and upgrade notes

This section provides additional installation and upgrade information, including related or third-party product information and any required critical patches.

Before beginning installation, ensure that your system meets the requirements listed in Chapter 4, *Supported environments and compatibility*. After installation, be sure to update your software to the latest patched release, if any patches are available.

The *OpenText Documentum Platform and Platform Extensions Installation Guide* contains installation instructions for your product. The *OpenText Documentum System Upgrade and Migration Guide* contains upgrade information for your product. These documents are available on My Support.

7 Fixed issues

This section provides information about past issues that have been fixed in this release.

Issue number	Issue description
CS-142980	Documentum deployment on Kubernetes supports importing only one SSL S3 certificate into the JAVA trust store. This is an issue with chain of certificate from different S3 vendors. These chains of certificates must be imported manually with an application server restart.
CS-142902	DMFILESCAN deletes non-orphan content when the storage path contains uppercase characters.
CS-142862	Workflow agent writes huge amount of error message to Documentum Server log files and eventually brings down the server.
CS-142807	The DMOTDSREST running on the JMS allows unauthenticated access to all operations (list all users/groups, update or create users/groups) by any remote http client after a successful authentication has been performed by the OTDS resource connector.
CS-142797	D2 electronic sign-in failed if password contains "+".
CS-142782	dmqdocbroker.awk is not able to process command line input arguments. Changing the target host using -t argument is not working.
CS-142730	dmqdocbroker.awk is not able to process command line input arguments. In this defect, changing the target host using -t argument is not working.
CS-142587	Mail notification fails after upgrading to 22.4 with [DM_SESSION_E_NOT_SUPERUSER]error: "The operation you requested, fetch dm_smtp_config, was not executed because the current user is not superuser".
CS-142513	LDAP directory connection/validation issues seen from Documentum Administrator. Try to import multiple certificates (CER format) into LDAP certificate database and not all certificates are copied. Documentum Server dependency is resolved in this defect.

Issue number	Issue description
CS-142372	DQL with repeating attributes and dm_relation type is translated to an invalid SQL.
CS-140331	AEK key upgrade fails upgrade from 22.2 to 22.4 in scenarios where the AEK passphrase is not a very strong password as per the new password complexity guidelines.
CS-142301	Documentum Server upgrade has errors when ACS_BASE_URL has the load balancer URL.
CS-141998	MIGRATION_CONTENT job fails when the target store is set to S3 with error code DM_STORAGE_E_S3_PUSH_CONTENT_METADATA_FAIL (CS0021756).
CS-141956	Using "distinct" in I_ALL_USERS_NAMES query causes performance issues in Postgres database when the group count is high.
CS-141885	DQL query having RETURN_RANGE and ROW_BASED hints fail on SQL Server because dm_repeating1_2 could not be bound.
CS-141687	Extending Documentum attributes in Life Sciences pre-install script stalls the installation process.
CS-141463	Issue in Documentum Server 21.4, I_ANCESTOR_ID is not updated after move folder.
CS-141127	Role permission missing in Documentum Server container image.
CS-141117	Docbase ID for Documentum Server cloud deployments must be a 6-digit number.
CS-140996	Prod Docbase services down frequently.
CS-140985	Using the alias DM_DBO should not be mandatory in queries on registered tables.
CS-140856	Documentum Server with seek API for streaming support for external stores was introduced where in there was a mismatch in HTTP POST request parameter name which ACS could not recognize. The fix is to use the correct parameter name 'offset' instead of 'seek_offset'.

Issue number	Issue description
CS-140669	Documentum Server 20.x/21.x/22.x only accepts 1 of 3 certificates from certificate chain, and Documentum Server 16.4 show 3 of 3 certificate for DFC SSL.
CS-140317	Documentum Server after startup fails to obtain socket for xPlore host and hence does not start IA.
CS-139693	Documentum process consuming memory and then swap - reinit or restart to release.
CS-139355	Connection broker binding not happening to the right IP when server is attached with multiple Network Interface.

8 Known issues

The following known issues exist in this release.

8.1 Known issues specific to installation and upgrade

Issue number	Issue description
CS-137870	Populating data_dictionary_pt_BR.txt file before data_dictionary_pt.txt results in a failed deployment. **Workaround:** Please refer to the below workaround: data_dictionary_pt_BR.txt deployment will fail only if you don't have data_dictionary_pt.txt installed on your Documentum Server . In case you have data_dictionary_pt.txt installed, these errors don’t not appear. The sequence is to populate data_dictionary_pt.txt first, then proceed with data_dictionary_pt_BR.txt.

Issue number	Issue description

CS-143684	Docbroker externalisation in GCP is not pointing to the correct external targetPort numbers.
	Workaround: After dctm-server is installed and configured in GCP with externalisation, the following steps are required to access docbroker outside the cluster.
	1. Edit the external docbroker load balancer service and update the targetPort value of csnative to 1491 and targetPort value of csssl to 1492 under ports section as below and save it.
	Example:
	`kubectl edit svc csext-cedbr`
	2. Update ports and Documentum Server can be accessed externally using the external docbroker load balancer service's External IP with port 80.
	`name: csnative`
	`nodePort: 32241`
	`port: 80`
	`protocol: TCP`
	`targetPort: 1491`
	`name: csssl`
	`nodePort: 30856`
	`port: 81`
	`protocol: TCP`
	`targetPort: 1492`

CS-139907	Unable to deploy Documentum Server in FIPS-enabled Red Hat Enterprise Linux operating system with Red Hat provided OpenJDK. This is a Red Hat OpenJDK limitation. This limitation is also applicable to Docker Compose provided for Red Hat Enterprise Linux with packaged OpenJDK. **Workaround:** It is recommended to use OpenJDK from other Java providers that are supported by Documentum
CS-135504	Repository logs contain additional messages - “Unable to load monitor library" **Workaround**: Create a soft link from libpcre.so.1->libpcre.so.0 using the following command: ln -s /usr/lib64/libpcre.so.1 /usr/lib64/libpcre.so.0

	The library is seen using the following command: find / -name libpcre.so.1 /usr/lib64/libpcre.so.1
Issue number	**Issue description**
CS-137870	Populating custom locale (pt_BR locale) directly results in errors. **Workaround:** Populating of data_dictionary_pt_BR.txt file before data_dictionary_pt.txt results in errors. data_dictionary_pt_BR.txt deployment fails only if you do not have pt installed on Documentum Server. In case you have pt installed, these errors will not appear. First populate data_dictionary_pt.txt and then data_dictionary_pt_BR.txt file in the same environment and deployment succeeds.
CS-137902	With Docker containers, seamless upgrade configuration to CE 22.2 version fails due to mismatch of RSA key length. **Workaround**: Server.ini from the older version contains RSA key length value as 1024. With 22.2 this value is 2048. During a seamless upgrade, errors are seen at startup and the upgrade fails. It is recommended to manually update RSA key length to 2048 in 22.1 container before seamless configuration and run seamless upgrade again.
CS-133965	When you create a repository after the installation of Documentum Server, installation of DAR files results in an error. **Workaround**: Add `'dfc.date_format=<correct-local-date-format>'` in `C:\Documentum\config\dfc.properties`. If you are installing DAR files with dardeployer.ini or if you get an error while using composer.exe, then add the `'-Djava.locale.providers=COMPAT,SPI'` property after `-vmargs` in dardeployer.ini/composer.ini. Note: The <correct-local-date-format> is different for different localized Windows.
CS-133005	Java configurations are updated incorrectly when Documentum Server is upgraded to 21.2. **Workaround**: Before upgrading Documentum Server, you must manually delete JAVA_LINK from the %Documentum%\java64 directory.
CS-135462	Documentum Server upgrade from 20.4 to 22.1 shows older references of log4j2. **Workaround:** You need to first patch 20.4 and make sure no references of older log4j libraries are present before 22.1 upgrade.

Issue number	Issue description
CS-128912	Authentication fails intermittently for Documentum client applications when you deploy the DAR files in the Kubernetes platform. This happens when headless composer is invoked for installing the DAR files on the same Documentum Server host. **Workaround**: Ensure that you include the password in the client application scripts. For example, in Documentum Server, the *kube_cs.sh* script contains the password details as CLI arguments as follows: `java -Ddar="$darFile" -Dlogpath=$tempdarlogs -Ddocbase=$DOCBASE_NAME -Duser=$INSTALL_OWNER -Dpassword=$INSTALL_OWNER_PASSWORD -Ddomain= -cp $DM_HOME/install/composer/ComposerHeadless/startup.jar org.eclipse.core.launcher.Main -data $DM_HOME/install/composer/workspace -application org.eclipse.ant.core.antRunner -buildfile $DM_HOME/install/composer/deploy.xml >> ${DOCUMENTUM}/dba/config/$DOCBASE_NAME/dars.log` If the DAR files are installed by installer, you must modify the installer scripts to include the password.

CS-128870	On Linux, when you try to configure IJMS in the same host as Documentum Server, it results in the *"Failed to include persistent preferences from "<IJMS install directory>/config/dfc.properties"* error in the ACS log file resulting in failure to access the ACS URL.
	
	Workaround:
	1. Stop IJMS.
	2. Navigate to the location where the *dfc.properties* file exist in the IJMS ACS installation directory. For example, *<IJMS installation directory>/tomcat<version>/webapps/ ACS/WEB-INF/classes*.
	3. Open the *dfc.properties* file and replace the *<IJMS installation directory>* with *<Documentum installation directory>* as specified in **bold** and save the *dfc.properties* file.
	
	For example, change
	From
	`#include /home/<installowner>/`**`<IJMS installation directory>`**`/config/dfc.properties`
	To
	`#include /home/<installowner>/`**`<Documentum installation directory>`**`/config/dfc.properties`
	4. Restart IJMS.

Issue number	Issue description
CS-127896	ServerApps, ACS, and other URLs do not get generated in an RCS secondary environment. **Workaround**: Enable the privileged clients using DA.
CS-126854	Unable to invoke the CFS configuration program installer when using AdoptOpenJDK. This is a design limitation of InstallAnywhere software with AdoptOpenJDK. **Workaround**: In the command prompt window, navigate to *%DOCUMENTUM%\product\20.4\install* and then run the following command: `Server_Configuration_Program.exe LAX_VM "%JAVA_HOME%\bin\java.exe"` where JAVA_HOME represents AdoptOpenJDK.
CS-125750	Installation of DAR files are slow and may take more time in a Documentum Server/SQL Server 2019 environment. This is a Microsoft limitation. **Workaround**: Install the SQL Server 2019 for Microsoft Windows latest cumulative update.
CS-125094	In a Red Hat Enterprise Linux 8.1 or 8.2/Red Hat OpenJDK 11 environment, when you try to configure the repository and connection broker in the SSL mode without certificates, the configuration of the repository fails. **Workaround**: Configure the repository and connection broker in the SSL mode without certificates using the supported version of Oracle JDK or use the certificate-based Documentum Server.
CS-121167	The CFS configuration program installer may not be able to connect to the repository of primary Documentum Server while configuring on a dual-stack Windows environment. This is a design limitation of InstallAnywhere software with Java 11 while connecting to another dual-stack environment. **Workaround**: You must manually invoke the CFS configuration program through the Java 8 process and provide the IPv4 address of the primary Documentum Server to connect to its repository.
Issue number	**Issue description**
CS-120767	Java methods does not run when IJMS is installed on a different host of IPv6.

CS-120520	dm_bof_registry user is not created while configuring the global repository using the external connection broker on a dual-stack environment. **Workaround**: 1. Configure the connection broker in one host. 2. Create a repository in another host. The installation complains about dm_bof_registry user creation. 3. When the installation finishes, you must manually create a dm_bof_registry user with the following details: user_name: dm_bof_registry user_login_name: dm_bof_registry user_source: inline password user_password: <bof registry user password> user_state: 0 default_folder: /dm_bof_registry user_privileges: 0 client_capability: 0
Issue number	**Issue description**
CS-120209	While configuring the repository, the *Unable to register the Accelerated Content Services Administration URL* error message is displayed intermittently.
CS-48939	After consolidation of repositories, the *user_rename* operation does not rename the user on the migrated repository.

Issue number	Issue description
CS-41937	When you install Documentum Server on multiple hosts, the *DM_SESSION_E_AUTH_FAIL* exception occurs in *server.log* and *ServerApps.log* on the remote Documentum Server side. **Workaround**: Perform the following steps: 1. Navigate to Documentum Administrator > Client Rights Management > Privileged Clients > Manage Clients. All clients for both hosts are displayed. 2. For the appropriate client on the secondary host, select the following options: *a. Enable trusted login* *b. Enables trusted server privilege*
CS-41733	Logging through IAPI when handling several login requests within a short time frame takes a long time. This is because the *DEVRANDOM* variable is not added in the startup script on Linux for remote Documentum Server. **Workaround**: Add the following lines in *DM_HOME* /bin/dm_set_server_env.sh before starting RCS: *DEVRANDOM=/dev/urandom* *export DEVRANDOM*
CS-41543	When you configure the global repository after installing Documentum Server, the *DFC_DOCBROKER_EXCLUDED* warning message occurs in the JMS, DFC, and ACS log files. This is because the Teredo Tunneling Pseudo-Interface is enabled. **Workaround**: Perform the following step: From the command prompt, type *netsh interface teredo set state disabled* Or Disable the IP Helper service from the *Services* dialog to disable the tunneling permanently. Restart the machine.
CS-41332	UCF function fails when you upgrade Documentum Server and RMA. This is because the UCF installer adds the following line to the network configuration file causing UCF to use IPv6 which is not supported: *<option value="-Djava.net.preferIPv6Addresses=true"/>*

Issue number	Issue description
CS-40415	Unable to install Documentum Server on some localized Windows operating systems. **Workaround**: Create a group "Everyone" on the localized server operating system manually. Proceed with the Documentum Server installation. This is a limitation.
CS-34238	Warnings are displayed in the log directory of DAR (*IndexAgentDefaultFilters.dar* and *MessaginApp.dar*) installations in the upgrade environment. However, you can ignore these warnings since the version label is not used anywhere in the BOF service class.
DC-7495	Warning messages are displayed in the server log directory while deploying ACS, BOCS, and DMS. For example: Class Path entry <JAR1 NAME> in <JBOSS 7.x HOME>/server/DctmServer_DMS/deployments/DMS.ear/dms-ws.war/WEB-INF/lib/<JAR2 NAME>" does not point to a valid jar for a Class-Path reference. However, you can ignore these warnings. The JBoss website contains more information.

8.2 Known issues specific to server and administration

Issue number	Issue description
CS-128600	When Google Cloud Platform (GCP) releases a new certificate, the old certificate stops working even though the expiry date is not reached. This is because the public certificate from GCP expires every 90 days or earlier for various reasons. If the old certificate stops working, then you must obtain the new certificate from GCP and import it manually to the location of *dfc.keystore*. This is a GCP limitation.
CS-128074	Authentication fails with OTDS when the password contains double quotes.

Issue number	Issue description
CS-125376	Content compression does not work when both the compression and encryption are enabled for the REST store. This is a limitation. However, the compression works correctly when only content compression is enabled for the REST store.

Issue number	Issue description
CS-122988	When you launch the *dm_mailwrapper.sh* script in Red Hat Enterprise Linux 8.x operating system, it results in the */bin/mail: relocation error: /bin/mail: symbol SSLv3_client_method version OPENSSL_1_1_0 not defined in file libssl.so.1.1 with link time reference* error. **Workaround**: Add the lines (shown in **bold**) in *dm_mailwrapper.sh* script and then launch: #!/bin/sh … subject=$1 address=$2 content_file=$3 … **LD_LIBRARY_PATH=/lib64** **export LD_LIBRARY_PATH** /bin/mail -s "$subject" "$address" < $content_file status=$? … if [$delete_contents = 1] ; then # remove the temporary content file once it is sent \rm $content_file fi … **unset LD_LIBRARY_PATH** exit $status
CS-122754	LDAP user authentication is not supported with the TLS 1.3 protocol.
CS-120157	Limited support for the data partition feature on PostgreSQL.
CS-119448	Member repository unable to use the global repository which is projected to other connection broker. **Workaround**: The global repository and the new repository must be projected to the same connection broker.
CS-56179	Setting *HA_SETUP_ENABLED* is causing a workflow to have Documentum Server affinity for its whole activities, even if they are sequential or parallel. If a Documentum Server crashes, all associated workflows are stuck or in paused state. **Workaround**: Manual steps are required to move these workflows/workitems to an available Documentum Server. Fetch all completed workitems of associated crashed Documentum Server's workflows and then set *a_wq_name* of workitem to available Documentum Server config name. Then, rest of workitems are processed through the configured Documentum Server.

Issue number	Issue description
CS-55842	Email copied from sent items can be imported twice in same repository folder. This is an Aspose limitation.
CS-53868	Unable to move the existing objects data from the non-partitioned table to the partitioned table on a data partition enabled CentOS/PostgreSQL environment.
CS-53307	When you invoke the RPC method, MIGRATE_TO_LITE with RECOVERY_MODE on a CentOS/PostgreSQL environment, it results in an error.
CS-52847	Delay in executing drop_index call on a CentOS/PostgreSQL environment. This occurs only when select queries are frequently being executed on dm_sysobject types. Since read commit does not happen by default, drop index call hangs until the selects are not executed. **Workaround**: Set *lock_timeout* parameter in *postgresql.conf* to a value in millisecond (preferably to a lower value) so that any query statement waits only for the time as indicated in this parameter while attempting to acquire a lock on a table, index, row, or other database object. This is required if there is any exclusive lock on the tables in the database.
CS-52769	In a Windows/PostgreSQL environment, when closeBatch and flushBatch methods are run, batch [isBatchActive()] and implicit transaction [isTransactionActive()] are both still open.
CS-52561	Creating a blob store with names in uppercase on a CentOS/PostgreSQL environment is not supported.
CS-51940	UpdateStatsDoc job is not supported on a CentOS/PostgreSQL environment.
CS-51822	When dm_document is updated, attribute_list is not getting populated. This results in object IDs in dm_audittrail not returning in ascending order of its creation in the PostgreSQL database.
CS-48801	When you run the nested groups incremental LDAP synchronization job on Sun ONE directory server, it fails for the *user_rename* and *group_rename* operations and reports an error in the JMS log.
CS-48516	In the Microsoft Cluster environment, LDAP synchronization job does not work with Microsoft Cluster virtual host name.

Issue number	Issue description
CS-45744	The dm_policy object that is attached with the dm_procedure object can only be deleted by a superuser irrespective of the owner of the dm_policy object. **Workaround**: 1. Unlink the dm_procedure object from the dm_policy object. Then, delete the dm_policy object using the privileges used to create the dm_policy object. 2. Delete the dm_procedure object using the superuser privileges.
CS-43925	When you attempt to transfer content through ACS and BOCS with the Asynchronous Write Job turned 'ON', the DFC deployed in the application context sends a message to DMS instructing it to store the content located in BOCS. The size of the message is directly proportional to the number of ACS server configuration objects and the number of base URLs in the ACS config objects. If the number of configuration objects or URLs exceeds 2, the message may get truncated when it gets stored in the DMS database. Therefore, it is recommended to avoid such configurations of ACS config object(s). This is a limitation.
CS-43570	If the number of file stores in Documentum Server are more than 100, any additional file stores created do not work and results in the following error: *[DM_SESSION_E_STORESTAT_OVERFLOW]error: "The shared memory segment for caching the ONLINE/OFFLINE status of the Documentum Storage areas has reached its maximum size (100). Update access may be incorrectly given to Offline or ReadOnly storage area (28003039800002b7)."*. The file store status of some of the stores may be incorrect. This is a limitation.
CS-42094	Change object type to a subtype does not work for lightweight objects.
CS-41576	LDAP synchronization fails when you try to synchronize a high count of user data from the Microsoft Active Directory with the *java.net.ConnectException: Connection timed out* exception. **Workaround**: Set the value of the *method_arguments* attribute in the LDAP synchronization job to *ignore*. *API> retrieve,c,dm_job where object_name='dm_LDAPSynchronization'* *API> append,c,l,method_arguments* *SET> -referral <follow/ignore>* *API> save,c,l* If you do not set this value, or specify some other value, the default value *follow* is set.

Issue number	Issue description
CS-41252	When querying, agent_exec loose time because it also goes through jobs that are dedicated to another server. **Workaround**: To avoid time loss, set the value of the *target_server* attribute to current server or ANY SERVER.
CS-41027	Redundant joins in newly created SDT views. **Workaround**: Create an environment variable *DM_NO_EXTRA_JOINS* and set its value as T. Then, restart Documentum Server. To update the existing views, do the following in SQLplus: *UPDATE dm_type_s* *SET views_valid = 0;* *commit;* The view gets updated whenever you use a *type* object for the first time in Documentum Server. Otherwise, the view remains the same.
CS-40838	When two users perform a move operation of two folders simultaneously, the *r_folder_path* and *i_ancestor_id* parameters contain incorrect values causing folder inconsistencies in Oracle and SQL Server. **Workaround**: Add *disable_folder_synchronization = T* in the *server.ini* file. By default, the value is F.
CS-40701	When running the dm_event_sender_java method using the DO_METHOD directly, the <argument_name>:<argument_value> pair needs to be passed in while executing the method. Passing only the argument_value (as done in the dm_event_sender docbasic method) does not work, unless the queue API is called. With queue API, DFC appends the argument_name before the argument_value during the execution of the Java method. All argument names are mandatory and need to be passed to the Java method. If a particular argument name has no value, pass an empty string.
CS-40474	Performance issue is encountered when promoting a document in lifecycle, within a transaction. This occurs due to concurrent access to the dmc_tcf_activity object.

Issue number	Issue description
CS-40238	Unable to edit or perform a search based on the definition of the *a_retention_date* attribute for immutable objects. You must run the *UpdateDDInfoForRetentionDate.ebs* script manually to update the data dictionary information for *a_retention_date* attribute and republish the data dictionary information for the *a_retention_date* attribute of the sysobject and subtypes of the sysobjects for existing repositories. Execute the *UpdateDDInfoForRetentionDate.ebs* script on the Documentum Server machine where the repository is created, using the following command: • On Windows: dmbasic -f %DM_HOME%\bin\UpdateDDInfoForRetentionDate.ebs -eEntry_Point -- <docbaseName> <installOwner> <password> • On Linux: dmbasic -f $DM_HOME/bin/UpdateDDInfoForRetentionDate.ebs -eEntry_Point -- <docbaseName> <installOwner> <password> If you have a new 7.1 or later installation, you do not have to execute the *UpdateDDInfoForRetentionDate.ebs* script. You must execute the *UpdateDDInfoForRetentionDate.ebs* script only if you have upgraded repositories and if you want to allow users to edit or perform a search using the *a_retention_date* attribute definition of immutable objects. For downloading the *UpdateDDInfoForRetentionDate.ebs* script or the latest Documentum Server patch containing the *UpdateDDInfoForRetentionDate.ebs* script, refer to the Support site.
CS-40207	DoMail requests fail when static IP address is configured for JMS listen address. This is because DoMail class runs the validateRequestIPAddress method against the localhost's IP address. **Workaround**: To prevent DoMail requests from another Documentum Server (on a different host) from failing, you must add an init parameter to DoMail's web.xml. The name of this parameter must start with the keyword 'ip-' and its value must be the IP address of a trusted host. For example: *<servlet>* *<servlet-name>DoMail</servlet-name>* *<description>Documentum Mail Servlet</description>* *<servlet-class>com.documentum.server.impl.mailservlet.DoMail</servlet-class>* *<init-param>* *<param-name>ip-192.168.0.1</param-name>* *<param-value>192.168.0.1</param-value>* *<//init-param>* *</servlet>*

Issue number	Issue description
CS-39933	Using comma in the LDAP binding password results in an error. **Workaround**: Use the single quote if the password has a comma. For example: API> encrypttext,c,'password,123'
CS-39775	Renaming and deleting users and groups fail in the LDAP synchronization with the Oracle Internet Directory (OID) Server.
CS-39553	Deletion of nested groups from the LDAP directory server is not properly synchronized to Documentum Server. **Workaround**: Explicitly provide a value for input argument -full_sync for the LDAP synchronization job through Documentum Administrator before running it: TRUE for full sync; FALSE for incremental sync.
CS-39232	acl_check_db cannot be set to TRUE with QBS. This is because DFC does not support setRange with double security check in Documentum Server.
DFC-11836	[Internationalization] *dd_populate.ebs* for Loaddatadictionary populates labels only in two-letter locale names even though the data dictionary file contains locale_name with five-letter locale.
DFC-10894	Invalid license exception occurs during multi-domain authentication when Documentum Server internal JDK is used.
DA-10459	Unable to access DFC client application when Kerberos SSO is configured using Sun Login module "com.sun.security.auth.module.Krb5LoginModule required" on the SUSE Linux environment. This happens when the application server is configured with the SUSE Linux environment. The following error message is displayed when you try to access Documentum Administrator: *SEVERE [http-nio-8080-exec-8] org.apache.catalina.core.StandardWrapperValve.invoke Servlet.service()for servlet [ComponentDispatcher] in context with path [/da] threw exception [Servlet execution threw an exception] with root cause java.lang.ClassNotFoundException: com.dstc.security.kerberos.NotYetDecryptedException*

8.3 Known issues specific to Docker and Kubernetes

Issue number	Issue description
CS-136126	When you enable multiple languages during an upgrade from 21.4 to 22.1, it results in warnings in the logs of pods. **Workaround**: Ignore the warnings as English is enabled by default.
CS-134636	When you upgrade Documentum Server 21.4 to 22.1 in a cloud environment, some of the repositories and EBS scripts are not installed. **Workaround**: Rerun the scripts manually and then run the Helm upgrade command.
CS-130688	User authentication is successful even when the user state is set to 1 and INACTIVE_UNSUBSCRIBED_USER is enabled. **Workaround**: Modify the value of *upd_last_chg_time_from_db* to *T* in *server.ini* for all the replicas.
CS-128717	User authentication fails when OTDS is in SSL mode with certificate-based Documentum Server pod in a Kubernetes platform. **Workaround**: 1. Obtain the OTDS certificate from https://<ingress-prefix.ingress-host>/otdsws. 2. Copy the certificate in the Base64 encoded format (.CER or .PEM) and place it in the Documentum Server pod. 3. Import the certificate in *dfc.keystore* located at *$DOCUMENTUM/certificate/* using the following command format: `keytool -importcert -keystore $DOCUMENTUM/certificate/dfc.keystore -file <file path of certificate to be imported> -alias otds.`hostname` -storepass $DFC_SSL_TRUSTSTORE_PASSWORD -noprompt`
CS-121973	When you try to perform any operations after installing IJMS on Docker, it results in the *ACS_ERROR_PROJECTING_DOCBROKER* error. This occurs only when Documentum Server and IJMS are installed on different Docker hosts. This is because IJMS container does not have access to the hostname of the Documentum Server container. **Workaround**: Install the Documentum Server and IJMS on the same Docker hosts.
CS-59040	Repository configuration fails with the *use existing docbase* option in the Docker container.

Issue number	Issue description
CS-53709	Bundled Java does not work with CAS plug-in in a Docker container. **Workaround**: Ensure that the Docker container exports the port number 64443. Install the latest Java and generate the client server certificates and then copy the UnlimitedJCEPolicy jar files to Documentum Server Java, CAS Server Java and client server Java if you get the *java.security.InvalidKeyException:Illegal key size* error.

9 Contact information

OpenText Corporation
275 Frank Tompa Drive
Waterloo, Ontario
Canada, N2L 0A1

For more information, visit the OpenText or My Support websites.