OpentText™ Web Experience Management Audit

Installation and Configuration Guide

Version 16.2.1

Contents

1. Introduction

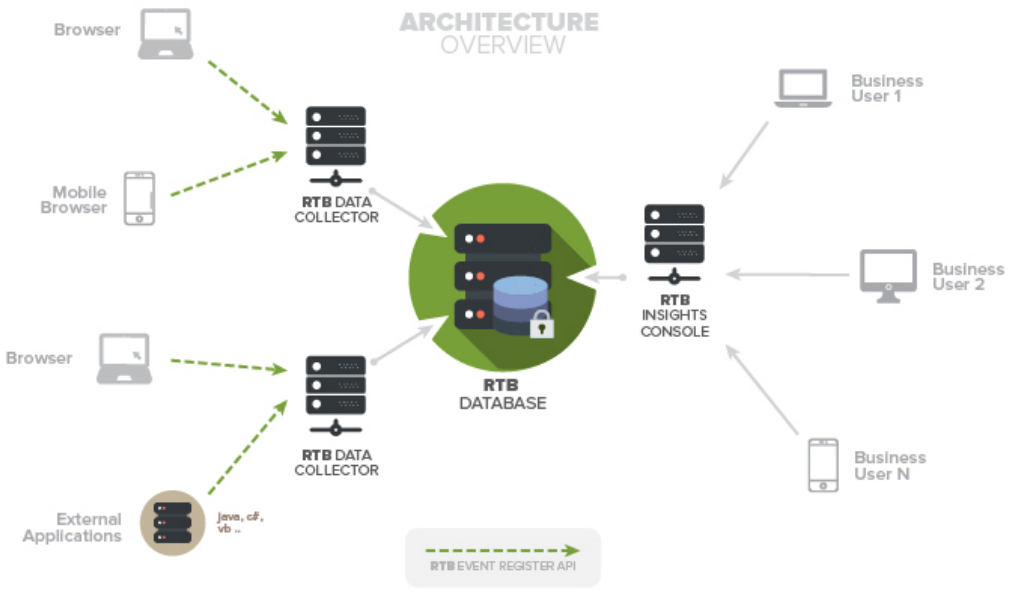
This guide provides an overview of OpenText™ Web Experience Management Audit 16.2.1 installation and configuration.

1.1. Document Revision History

Revision Number	Modification Date	Section Modified	Modifications
1.0	2017-07-07	All	Initial Release 16.2
1.1	2017-08-25	All	Release of 16.2.1

1.2. Architecture Overview

The following diagram shows the underlying RealTimeBiz (RTB) platform architecture:



The RealTimeBiz platform has three main system components:

- **RTB Database** – the data repository of RTB.
- **RTB Data Collector** – the component that receives the events from external systems and stores them in the RTB Database in real-time.
- **RTB Insights Console** – the web console where business users access parametric data reports.

WEM Audit complements the functionality of the RTB platform by monitoring the activity of Web

Experience Management. This module is specifically designed to gather information about events such as the creation of the channels, the modification of content types, and other activities, and make them available in the WEM Management Console.

These collected events are configured to be stored in a RTB database for a specified amount of time. Once this time is elapsed, the events are automatically removed from the system.

RTB Insights is an advanced tool to analyze all the audit information and to help improve your content management and delivery business processes.

1.3. Release Notes and Patch Notes

Read the WEM Audit Release Notes and the Patch Notes before you begin the procedures in this guide. The Release Notes and the Patch Notes contain installation and configuration notes, and other important information not contained in this guide.

1.4. Prerequisites

The following sections describe prerequisite for installing RealTimeBiz and the WEM Audit.

1.4.1. SMTP Server and Email Account

If you want to receive WEM Audit (RTB) reports or logs via email, you must have an SMTP Server, which must be accessible from the machine where the RTB Insights Console will be installed.

Make sure that you have the SMTP server, the administrative permissions, and the RTB email account.

1.4.2. Web Experience Management Audit Distrubution

You must have a distribution of OpenText™ Web Experience Management Audit 16.2.1, which contains the following files and directories.

File/Directory	Description
`antDir/`	Installer scripts
`bin/`	RealTimeBiz binaries
`config/`	Configurations files
`installLib/`	Installer libraries
`install.bat`	Windows installer wizard
`install.sh`	Linux/Unix installer wizard

File/Directory	Description
`uninstall.bat`	Windows uninstaller wizard
`unistall.sh`	Linux/Unix uninstaller wizard
`version.txt`	Version descriptor

1.4.3. General Configurations

Before proceeding with the WEM Audit installation, you must gather the following information.

If you wish to use **LDAP** for authentication, use the following prerequisites:

Prerequisite
LDAP URL (host + port)
LDAP user and Password with read privileges (complete DN)
LDAP user attribute (i.e. cn, uid)
LDAP user search base (root DN for users)
LDAP group search base (root DN for groups)
LDAP group object class
LDAP user object class
LDAP member attribute
Complete DN of groups and/or users with Audit privileges (access to Insights console)

If you wish to use **OpenText™ Directory Services (OTDS)** for authentication, use the following prerequisites:

Prerequisite
OTDS URL (host + port)
OTDS user and Password with read privileges (complete DN)
OTDS resource ID (previously created)

Prerequisite
Complete name of OTDS groups with Audit privileges (access to RTB Insights Console)

Other general configurations

Prerequisite
Retention Period desired for events and large attributes (1 year, 5 years, etc)
Database connection data (host, port, instance, user, password) for RTB
Database connection data (host, port, instance, user, password) for Web Experience Management
List of LDAP Groups that are going to be tracked with RTB (optional)
The host and port of Web Experience Management Server
User/groups/roles that will have the capability to see the event history at Web Experience Management Console
SMTP Host and port

1.4.4. OTDS Server Certificate

The communication between the installer and the OTDS server is usually done via `HTTPS`. This means that the OTDS Server Certificate needs to be added to the Java Key Store of the JVM where the installer is running.

To add a certificate to a key store, use the `keytool` command:

```
keytool -import -alias OTDS -file Example.cer -keystore examplekeystore
```

For additional information refer to the documentation of your JVM distribution.

1.4.5. OTDS Resource

If you wish to use OpenText Directory Services (OTDS) for authentication, you will need the OTDS Resource Identifier during the installation. You must create the Resource before proceeding with the installation.

Tip:

For more information on how to create an OTDS Resource, see Appendix 6 - Configuring a Resource in OTDS.

1.4.6. Pre-installation actions

You need to do this before installing OpenText™ Web Experience Management Audit. Skipping this may result in a faulty installation.

Edit cfgaction script

Make sure that the **cfgaction** script of the Web Experience Management installation has the **commons-lang** library added to its classpath. If not, it must be added.

Create database for RTB

The user and database for RTB must be created manually before the installation. The installer will not create them automatically.

1.4.7. System Requirements

The following table outlines the minimum requirements to install Web Experience Management Audit.

Requirement	
Web Experience Management Stage	100 MB
Memory:	See Web Experience Management Memory Requirements
Database Space	4K per collected event
Database Connection Pool	Two (2) connections per concurrent user of the RTB Insights Console, plus a minimum of five (5) connections for the RTB Data Collector.

2. Installation

This chapter describes the administrator's tasks for installing and configuring the RealTimeBiz platform, WEM Audit, and RTB Insights Console.

2.1. Installation Process Overview

The WEM Audit installation process has the following major installation steps:

- Create RTB Database
- Complete the Installation Wizard
- Configure Generic Resources
- Test Environment
- Update Roles
- Execute RTB Loader

> **Important:**
>
> Ensure you have read the section prerequisites before proceeding.

2.2. Creating RTB Database

You must create a database user in your database system (for example, RTB) before you begin the WEM Audit Installation. Follow the recommended steps for completing that task specific to your database vendor's documentation. The newly created user should have the same privileges/permissions to the Web Experience Management System user (ex: vgncms, vgnsys,…) such as:

- Create databases, stored procedures, and indexes
- Stored procedures execution
- Table insert, read, write, and others

Tables and other content will be created when executing the installer. Note the database IP, a port, instance name, user and a password.

It is recommended to provide a table space, or storage area, that can grow as event data is collected. The database size must be proportional to the number of events being recorded: you may start with a size of 5G-10GB, but be prepared to grow beyond that number, especially in production environments.

The database block size should be 8K at least to improve the performance. This is the default value in MS SQL Server, and you can check or set it in Oracle using the `db_block_size` parameter.

2.3. Launching the Installation Wizard

Before launching the RTB installer, be sure that you are using `Java 1.6` or above. Ensure that `JAVA_HOME/bin` is in the system path. You can use `<WEMinstallDir>/Content/16_2/java` dir path for the Java installation.

The following processes must be up and running:

- VgnVCMServer (and additional cluster nodes)
- VgnAdminServer
- Config Agents

Expand the WEM Audit distribution file in a directory of your choice (i.e. c:\tmp\WEMAudit) and execute the `install.bat`(or `install.sh`) file from that directory.

For UNIX:

```
chmod u+x install.sh
./install.sh
```

For Windows:

```
install.bat
```

The default language used for installation is defined by the language configured for your server. If you want to change the language used by the installer, for example from Engish to Spanish, follow these steps:

a. Edit the `install.bat` file using a text editor.
b. Add the language parameter at the end of the `install.bat` or `install.sh` file, for example -l es. Only `es` and `en` are supported in this version.

2.3.1. Selecting Installation Option

The WEM Audit 16.2.1 installer has a three (3) options:

- Install WEM Audit From Scratch
- Install Wem Audit Over WSA
- Upgrade WEM Audit Cumulative Patch

```
==========================================
WEM Audit Installer
==========================================
This application is going to install the WEM Audit application on the WEM
Server.
(Select one option [insert option number])

1)Install WEM Audit From Scratch

2)Install WEM Audit Over WSA

3)Upgrade WEM Audit Cumulative Patch

4)Exit
```

2.3.2. Installing WEM Audit From Scratch

This section describes how to do the fresh install of WEM Audit.

Select Installation Type

```
==========================================
Welcome to the Web Experience Management Audit install wizard
Please ensure that you have read the prerequisites chapter in the
documentation before going any further.

The following processes must be running before proceeding:
- VgnVCMServer (all cluster nodes), VgnAdminServer and Config Agents.

==========================================

Please, select the Installation Type that you will be using. Notice that
the installer should be launched at every machine running a Web Experience
Management cluster node. For installation with just one cluster node use
option 1.

(Select one option [insert option number])
1) Install on Web Experience Management cluster primary node.
2) Install on Web Experience Management cluster secondary node.
```

Chose the installation option that you want to perform. If you have just one cluster node, choose option **1) Install WEM Audit from Scratch**.

If you have a clustered installation, you must run the installer first in the primary node using the installer option 1, and then on all the secondary nodes using the option 2. For more information about installing in a Cluster, see Installing WEM Audit in a Web Experience Management Cluster

Selecting Installation Folders

After you choose the installation option, you can select the folders in which you will install the RTB platform and WEM Audit.

You cannot use non-alphanumerical or accentuated characters in neither Windows nor UNIX / Linux systems.

```
Please select a destination directory.
(this directory will store Web Experience Management Audit binaries and
configuration)
 >Default value [c:\audit]
 >Value: c:\OpenText\Content\Audit

Please select the Web Experience Management directory.
(this directory should contain the Content subfolder)
 >Default value [c:\OpenText]
 >Value: c:\OpenText
```

Creating Directory Structure

```
-----------------------------------------
Installing Directory structure
-----------------------------------------
In the next step the following components will be installed/configured:

- Data Collector properties file.
- Insights Console application files.
- RTB loader properties file.
- Insights Console properties file.
- Web Experience Management Audit Applications files.
- Data Collector application files.
- Audit libraries files.
- Client files.
- Uninstaller binaries.
- Folder structure.
- Client properties file.
- RTB Loader.

Do you want to continue with this step? (yes - continue, no - skip).
(only skip this step if you are doing a manual step by step setup over a
previous installation, otherwise the installation will fail)

 >Default value [yes]
 >Value:
[yes]

Installing ....
Creating folder structure ...
-->Folder structure created.
Copying Insights Console web application ...
-->Insights Console web application copied.
Copying collector application ...
-->Collector application copied.
Copying WEM applications ...
-->WEM Applications copied.
Copying Insights Console properties...
-->Open Insights Console properties copied.
Copying collector properties ...
-->Collector properties copied.
Copying client properties ...
-->Client properties copied.
Copying libraries ...
-->Libraries copied.
Install/uninstall libraries ..
-->Libraries installed/uninstalled.
Done.
```

Configuring Database

To execute this step, you need the connection details of two database users:

- The database user for Web Experience Management Audit (RTB)
- The system database user already in use for Web Experience Management

```
-----------------------------------------
System Database Installation
-----------------------------------------
In the next step the following components will be installed/configured:

- Auditor capability.
- Groups and company info.
- Open Text Web & Social indicators.
- RTB System Database.
- WEM Indicators.

Do you want to continue with this step? (yes - continue, no - skip).
(only skip this step if you are doing a manual step by step setup over a
previous installation, otherwise the installation will fail)
 >Default value [yes]
 >Value:
[yes]

Web Experience Management Audit database information
-----------------------------------------------------
(At this point a database user must be created before proceeding)
Database software
(Select one option [insert option number])
1)Oracle
2)MSSQL
3)Postgres
2

Database Host
 >Default value [localhost]
 >Value:
[localhost]

Database Port
 >Default value [1433]
 >Value:
[1433]

Database Instance Name
 >Default value [VIGN]
 >Value: VCMAUDIT

Database User
 >Default value [vcmaudit]
 >Value: audit

Database User Password


Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]

Company information
-------------------
Please enter the company name in which Web Experience Management Audit is
being installed
```

```
 >Default value [OpenText]
 >Value: OpenText

Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]


Events lifetime.
-----------------------------------------
Events lifetime into the database. (in days)
(This is the retention period for events.  After that period events will
be removed)
 >Default value [1095]
 >Value: 365

Large objects lifetime.
(This is the retention period for large attributes inside events. After
that period large attributes will be removed)
 >Default value [365]
 >Value: 30

Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]

Each user can belong to one or more groups when starting a session. A
session is a sequence of individual events performed by a user. To segment
by group, you should introduce the list of LDAP groups for which you are
interested to obtain reports.
Please type the list of groups that you are interested to report on
[separated by commas. For example: Administrators, DepartmentA,
Contributors].
 >Value: Administrators, Editors

Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]

Web Experience Management database system information
-----------------------------------------------------

Please provide the parameters needed for connecting to Web Experience
Management system database user.
Database software
(Select one option [insert option number])
1)Oracle
2)MSSQL
3)Postgres
2

Database Host
 >Default value [localhost]
 >Value:
[localhost]

Database Port
 >Default value [1433]
 >Value:
[1433]

Database Instance Name
 >Default value [VIGN]
 >Value: VCMMGMT
```

```
Database User
 >Default value [vcmsys]
 >Value: vcmmgmt

Database User Password

Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]

Installing ....
Creating RTB system tables...
-->RTB system tables created.
Creating Web Experience Management Audit data ...
-->Web Experience Management Audit data created.
Adding groups ...
-->Groups added.
Adding indicators ...
-->Indicators added.
Adding WEM indicators ...
-->WEM Indicators added.
Installing Auditor capability ...
-->Auditor capability installed.
done.
```

Web Experience Components Installer

```
-------------------------------------------------
Installing Web Experience Management configuration
-------------------------------------------------
In the next step the following components will be installed/configured:

- Audit libraries.
- Workflow listeners.
- Web Experience Management Automatic Task.
- Audit generic resource.
- History Button.
- Web Experience Management Audit property sheet.

Do you want to continue with this step? (yes - continue, no - skip).
(only skip this step if you are doing a manual step by step setup over a
previous installation, otherwise the installation will fail)

 >Default value [yes]
 >Value:
[yes]


Please type Web Experience Management (VgnVCMServer) connection info.
-------------------------------------------------------------------
Web Experience Management Server Host
 >Default value [localhost]
 >Value: localhost

Web Experience Management Port

 >Default value [27110]
 >Value:
[27110]

Admin User
 >Default value [vgnadmin]
 >Value:
[vgnadmin]
```

```
Admin User Password


Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]

Creating generic resource ...
-->Generic resource created.
Installing workflow listeners ...
-->Workflow listeners installed.
Installing Console buttons ...
Console buttons installed.
Committing changes ...
Doing deploy (configp) ...


##The next step requires configp execution.


Please press the "Enter" key

This action may take several minutes, please wait
->Deploy (configp) finished.
Creating Audit program task definition ...
-->Audit program task definition created.
Creating audit property sheet ...
-->Audit property sheet created.
done.
```

Configuring System Properties

```
-----------------------------------------------
Gathering system information (Properties file)
-----------------------------------------------
In the next step the following components will be installed/configured:
-RTB Data Collector properties.
-RTB Client properties.
-Insights Console properties.

Do you want to continue with this step? (yes - continue, no - skip).
(only skip this step if you are doing a manual step by step setup over a
previous
installation, otherwise the installation will fail)
 >Default value [yes]
 >Value:
[yes]

Define where you want to create the data collector log file
 >Default value [c:\OpenText\Content\Audit\logs\rtbcollector.log]
 >Value:
[c:\OpenText\Content\Audit\logs\rtbcollector.log]

Define the size for the data collector log file [KBs]
 >Default value [100]
 >Value: 1000

Define the port where the tool will be listening
 >Default value [26000]
 >Value:
[26000]


Please type the mail account information:
(this account will be used by the platform to send reports to business
users and
 log files to technical support)
-----------------------------------------
SMTP Host
 >Default value [localhost]
 >Value:
[localhost]

SMTP port
 >Default value [25]
 >Value:
[25]

Email Account
 >Default value [vcmaudit@yourcompany.com]
 >Value:
[vcmaudit@yourcompany.com]

Email Account Password


Enter a comma-separated list of email addresses. The product can send log
files
to these addresses:
 >Default value [rtb.support@vilt-group.com]
 >Value:
[rtb.support@vilt-group.com]
```

Authentication Properties

Configure the authentication provider. You can choose between LDAP and OpenText Directory Services.

```
Please set authentication properties:
(Authentication properties will be used for authentication and
authorization)
-----------------------------------------
Please select the authentication type
(Select one option [insert option number])

1)OTDS
2)LDAP
```

OTDS Properties

If you choose OTDS, you will be prompted to add the following properties:

- **OTDS Resource ID**, which is the identifier for the OTDS Resource created for the WEM Audit application. This resource should not be activated. The identifier can be obtained from the OTDS Administration Client by editing the resource. For example, 6e854917-6e78-4d38-a346-ac9f1625f3b0.
- **OTDS Rest services base URL**, which is the URL of the OTDS Web Services. The URL must use the `HTTPS` protocol and be in the following format: https://[host]:[sslport]/otdsws

Caution:

The OTDS resource created for WEM Audit and provided to the installer should not be activated.

When reinstalling WEM Audit ensure that the resource is inactive by deactivating it in the OTDS Administration client.

```
Please type the OTDS properties:
--------------------------------
OTDS Resource ID
 >Value: 6e854917-6e78-4d38-a346-ac9f1625f3b0

OTDS Rest services base URL
 >Value: https://myhost:8443/otdsws

The connection to OTDS has been made successfully

Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]
```

After configuring properties, the installer will perform a test to check the OTDS connection and the resource. If the test succeeds, the OTDS resource will be activated. If the connection test fails, you will be asked to setup the OTDS settings again.

Important:

If your connection fails, see Appendix 5 – OTDS Authentication for troubleshooting.

When the connection succeeds, configure the properties that define user privileges in RTB Insights Console. These privileges are defined using the mapping between the WEM Audit Roles and the OTDS Groups. The WEM Audit Roles grant users the right to access a resource or to perform certain actions.

By default, RTB Insights Console has the following two roles:

- **Audit:** Users with this role have access to the Audit information in the RTB Insights console and can consult reporting information.
- **Administrator:** – Users with this role have the Audit role access and access to the Admin tab in RTB Insights Console where they can perform administrator operations.

You must provide corresponding OTDS Groups for the Audit role and the Administrator role:

- **Role Audit:** The name of the OTDS Group for Audit users that should be associated to OTDS with the Resource created for WEM Audit through an Access Role.
- **Role Admin:** The name of the OTDS Group for Administrator users that should be associated to OTDS with the Resource created for WEM Audit through an Access Role.

The OTDS Groups are identified by its name. Note that the OTDS Groups name is case sensitive. If you want to provide multiple Groups, you should separate them with a semicolon (ex: “Audit Internal; Audit External”).

Important:

Groups must belong to the Access Role associated with the OTDS Resource. For more information, see Appendix 6 - Configuring a Resource in OTDS.

```
Please type group ids (separated by semicolons) for each role below:
---------------------------------------------------------------------

Role Admin: Users who will have access to the Administration Tab in RTB
Insights Console
 >Default value
[cn=Administrators,ou=Groups,dc=yourCompany,dc=com;cn=Contributo
rs,ou=Groups,dc=yourCompany,dc=com]
 >Value: Administrators

Role Audit: Users who will have access to the Audit tab in RTB Insights
Console console
 >Default value [Admin Access to Audit]
 >Value: Audit
```

Important:

If your role mapping validation fails, see Appendix 5 – OTDS Authentication for troubleshooting.

LDAP Properties

The installer will fetch the LDAP properties from Web Experience Management, and suggest them to you as your default options. If you do not want to use the same LDAP configuration you use in Web Experience Management, you must add them all manually.

The format of the LDAP properties depend directly on the LDAP server you are using. The table below contains the typical properties for some well-known LDAP servers: OpenLDAP, ActiveDirectory and Sun One.

Properties	OpenLDAP	ActiveDirectory	Sun LDAP
adminName	cn=admin,dc=vilt,dc=es	CN=Administrator, OU=Users, DC=localhost, DC=vilt,DC=dev	cn=Manager, dc=opentext,dc=com
adminPassword	XXX	XXX	XXX
groupObjectClass	groupOfNames	group	groupofuniquenames
groupSearchBase	ou=Groups,dc=vilt,dc=es	OU=VCM Groups,OU=Groups,DC=localhost,DC=vilt,DC=dev	ou=Groups,dc=opentext,dc=com
groupSearchMember	Member	member	uniqueMember
Ldapurl	ldap://localhost:389	ldap://localhost:3268	ldap://ldapdes01:389
searchBase	ou=People,dc=vilt,dc=es	OU=Users,DC=localhost,DC=vilt,DC=dev	ou=People,dc=opentext,dc=com
userObjectClass	person	User	person
userResolver	Cn	sAMAccountName	uid

```
Please type the LDAP properties:
--------------------------------
LDAP server URL:
 >Default value [ldap://lv111:27110]
 >Value:
[ldap://lv111:27110]

LDAP administrator username:
 >Default value [uid=vgnadmin,ou=people,ou=VgnLDAPRealm,dc=vgndomain]
 >Value: [uid=vgnadmin,ou=people,ou=VgnLDAPRealm,dc=vgndomain]

LDAP administrator password:
```

```
Testing LDAP connection...

Connection successful

Distinguished name where to begin the user search:
 >Default value [ou=People,dc=VgnLDAPRealm,dc=vgndomain]
 >Value: ou=VgnLDAPRealm,dc=vgndomain

Name of the property that defines a user in LDAP:
(this property depends directly on the LDAP server that you're using.
PLEASE READ THE INSTALLATION GUIDE FOR DETAILED INFORMATION ON THE
CORRECT PROPERTY NAME FOR THE MOST COMMON LDAP SERVERS)
 >Default value [uid]
 >Value:
[uid]

User Object Class:
(this property depends directly on the LDAP server that you're using.
PLEASE READ THE INSTALLATION GUIDE FOR DETAILED INFORMATION ON THE
CORRECT PROPERTY NAME FOR THE MOST COMMON LDAP SERVERS)
 >Default value [inetOrgPerson]
 >Value:
[inetOrgPerson]

Distinguished name where to begin the group search:
 >Default value [ou=groups,ou=VgnLDAPRealm,dc=vgndomain]
 >Value: [ou=groups,ou=VgnLDAPRealm,dc=vgndomain]

 Group Object Class:
(this property depends directly on the LDAP server that you're using.
PLEASE READ THE INSTALLATION GUIDE FOR DETAILED INFORMATION ON THE
CORRECT PROPERTY NAME FOR THE MOST COMMON LDAP SERVERS)
 >Default value [groupOfUniqueNames]
 >Value: [groupOfUniqueNames]

Name of the property that defines a group in LDAP:
(this property depends directly on the LDAP server that you're using.
PLEASE READ THE INSTALLATION GUIDE FOR DETAILED INFORMATION ON THE CORRECT
PROPERTY NAME FOR THE MOST COMMON LDAP SERVERS)
 >Default value [cn]
 >Value: [cn]

Name of the attribute that defines the membership relation:
(this property depends directly on the LDAP server that you're using.
PLEASE READ THE INSTALLATION GUIDE FOR DETAILED INFORMATION ON THE
CORRECT PROPERTY NAME FOR THE MOST COMMON LDAP SERVERS)
 >Default value [uniqueMember]
 >Value:
[uniqueMember]

Do you want to perform a test to check if the LDAP configuration is
correct?
 >Default value [yes]
 >Value:
[yes]

To start the test, it is necessary to enter an existing user in the LDAP
server
 >Default value [vgnadmin]
 >Value:
[vgnadmin]

Enter the password


The connection has been made successfully
```

```
Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]
```

The next step provides the ability for you to configure the user's privileges in the RTB Insights Console. These privileges are defined using roles. A role grants to a user the right to access a resource or to perform certain action.

By default, RTB has the following roles:

- **Administrators:** This role grants the access to the Admin tab in the RTB Insights Console and all the administration features within.
- **Web Experience Management Auditors:** This role grants access to the Audit tab in the RTB Insights Console, in which are displayed all the reports of the application. They also have the `xml_viewer` capability, allowing users to see the XML with the details of the events. This functionality is present on the Auditing tab of the properties of an object into WEM Content Console.

```
Please type users and groups (separated by semicolons) for each role
below:
------------------------------------------------------------------------
-
Role Admin: Users who will have total control on RTB Insights Console
 >Default value
    [cn=Administrators,ou=groups,dc=VgnLDAPRealm,dc=vgndomain]
 >Value:
    [cn=Administrators,ou=groups,dc=VgnLDAPRealm,dc=vgndomain]

Role Web: Users who will have access to the Web tab on RTB Insights
Console
 >Default value [cn=Administrators,ou=groups,dc=VgnLDAPRealm,dc=vgndomain]
 >Value:
[cn=Administrators,ou=groups,dc=VgnLDAPRealm,dc=vgndomain]

Role Audit: Users who will have access to the Audit tab on Insights
Console
 >Default value [cn=Administrators,ou=groups,dc=VgnLDAPRealm,dc=vgndomain]
 >Value:
[cn=Administrators,ou=groups,dc=VgnLDAPRealm,dc=vgndomain]


Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]
```

Web Experience Components Installer

```
-----------------------------------------
TomEE webapps deployment
-----------------------------------------
In the next step the following components will be installed/configured:
-WEM Audit Data Collector application.
-TomEE Start Parameters.
-RTB Insights console.
-WEM Audit Database Resource.

Do you want to continue with this step? (yes - continue, no - skip).
(only skip this step if you are doing a manual step by step setup over a
previou
s installation, otherwise the installation will fail)
 >Default value [yes]
 >Value:
[yes]

Installing ....

Installing Database Resource...

Setting start parameters ...

Installing Insights ...

Installing Web Experience Management Audit Data Collector App ...
-----------------------------------------------
-----------------------------------------------
--> Web Experience Management Audit Data Collector App installed.
```

Finishing the installation

```
The install process has finished successfully!
===============================================

In order to start registering events, it is necessary to restart Web
Experience
Management Server (all nodes in the cluster).

===============================================


-----------------------------------------
After restart is complete, please check your installation. You should
perform the following tests:
Web Experience Management Audit application:
http://localhost:27110/AuditVCMWeb/diagnosis/index.jsp
RTB Insights Console application: http://localhost:27110/Insights/dianosis
Web Experience Management Audit Data Collector:
http://localhost:27110/collector/diagnosis
-----------------------------------------


-----------------------------------------
The Web Experience Management Audit Loader application was installed in:
c:\OpenText\Content\Audit\rtbLoader

It's recommended to run Web Experience Management Audit Loader before
starting
to register system events. Please consult the documentation to learn more.
-----------------------------------------

Please press the "Enter" key
```

2.3.3. Upgrading WEM Audit with Cumulative Patch

This section will describe the steps you must perform to patch or upgrade to WEM Audit 16.2.1 using the cumulative patch.

Selecting Installation Type

```
=========================================
WEM Audit Cumulative Patch upgrader
=========================================
Welcome to the Web Experience Management Audit upgrade wizard
Please ensure that you have read the prerequisites chapter in the
documentation before going any further.
The following processes must be running before proceeding:
- VgnVCMServer (all cluster nodes), VgnAdminServer and Config Agents.
(Select one option [insert option number])

1)Apply the Audit Cumulative Patch on Web Experience Management cluster
principal node.

2)Apply the Audit Cumulative Patch on Web Experience Management cluster
secondary node.

3)Back to top menu
```

Choose the type of upgrade that you want to perform. If you have just one cluster node, choose option 1.

If you have a clustered installation, you must run the installer first in the primary node using the upgrader option 1, and then on all the secondary nodes with option 2. For more information, see Installing Audit in a Web Experience Management Cluster.

Selecting Installation Folders

When you start the upgrade, you must select the folders in which you installed the RTB platform and WEM Audit, as well as the folder where you have your WEM installation.

```
Principal Node Audit Cumulative Patch
-------------------------------------

Principal Node Audit Cumulative Patch
Please select a destination directory.
(all binaries, configurations and documentation will be stored in this
directory)
 >Default value [c:\audit]

Principal Node Audit Cumulative Patch
-----------------------------------------
Principal Node Audit Cumulative Patch
Please select a destination directory.
(all binaries, configurations and documentation will be stored in this
directory)
 >Default value [c:\audit]
 >Value: c:\OpenText\Content\Audit

Please select the Web Experience Management directory.
(this directory should contain the Content subfolder)
 >Default value [c:\OpenText]
 >Value: c:\OpenText\WEM

-----------------------------------------
Installing Directory structure
-----------------------------------------
In the next step the following components will be installed/configured:
- RTB Insights Console application files.
- Web Experience Management Audit Applications files.
- Data Collector application files.
- Audit libraries files.
- Client files.
- Uninstaller binaries.
- Folder structure.

Do you want to continue with this step? (yes - continue, no - skip).
(only skip this step if you are doing a manual step by step setup over a
previous installation, otherwise the installation will fail)
 >Default value [yes]
 >Value: yes

Installing ....
Creating folder structure ...
-->Folder structure created.
Copying RTB Insights Console web application ...
-->RTB Insights Console web application copied.
Copying collector application ...
-->Collector application copied.
Copying WEM applications ...
-->WEM Applications copied.
Copying libraries ...
-->Libraries copied.
Install/uninstall libraries ..
-->Libraries installed/uninstalled.
done.
```

Database Upgrade

You must provide the information of the WEM Audit Database.

```
-----------------------------------------
System Database installation
-----------------------------------------
In the next step the following components will be installed/configured:
-RTB System Database.

Do you want to continue with this step? (yes - continue, no - skip).
(only skip this step if you are doing a manual step by step setup over a
previous installation, otherwise the installation will fail)
 >Default value [yes]
 >Value: yes


Web Experience Management Audit database information
-----------------------------------------
(At this point you will need a database and a new user before proceeding)
Database software
(Select one option [insert option number])

1)Oracle

2)MSSQL

3)Postgres
1

Database Host
 >Default value [localhost]
 >Value:
[localhost]

Database Port
 >Default value [1521]
 >Value:
[1521]

Database Instance Name
 >Default value [VIGN]
 >Value: orcl

Database User
 >Default value [vcmaudit]
 >Value: VCM_AUDIT

Database User Password


Database connection succeeded.

Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value: yes

Installing ....
Creating RTB system tables...
it seems that this component has already been installed. It will be
ignored
done.
```

Upgrading Web Applications

This step will upgrade the Web Applications related to WEM Audit.

```
-----------------------------------------
TomEE webapps deployment
-----------------------------------------
In the next step the following components will be installed/configured:
-WEM Audit Data Collector application.
-RTB Insights console.

Do you want to continue with this step? (yes - continue, no - skip).
(only skip this step if you are doing a manual step by step setup over a
previous installation, otherwise the installation will fail)
 >Default value [yes]
 >Value:
[yes]


Installing ....

Installing Insights ...

Installing Web Experience Management Audit Data Collector App ...
done.
```

Updating Web Experience Management Configuration

Update the WEM configuration to allow the execution of the WEM Audit components. The installer will need the following information to access the VgnVCMServer:

- WEM Server Host
- WEM Server Port
- Admin User
- Admin User Password

```
------------------------------------------------
Installing Web Experience Management configuration
------------------------------------------------
In the next step the following components will be installed/configured:
- Audit libraries.

Do you want to continue with this step? (yes - continue, no - skip).
(only skip this step if you are doing a manual step by step setup over a
previous installation, otherwise the installation will fail)
 >Default value [yes]
 >Value: yes


Please type Web Experience Management (VgnVCMServer) connection info.
----------------------------------------
Web Experience Management Server Host
 >Default value [localhost]
 >Value: lw61

Web Experience Management Port
 >Default value [27110]
 >Value:
[27110]

Admin User
>Default value [vgnadmin]
 >Value:
[vgnadmin]

Admin User Password


Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value: yes

Installing ....
Deploying (configp) ...


##The next step requires configp execution.


Please press the "Enter" key

This action may take several minutes, please wait

->Deployment (configp) finished.
done.
Saving properties ...


The install process has finished successfully!

Please press the "Enter" key
```

2.4. Configuring the Web Experience Management Audit Resource

The installation process creates several Generic Resources in the WEM Configuration Console under the following nodes:

Content

→Delivery Services
→<for every stage, including management>
→Resources
→ResourceType-Generic
→Resource-RTBAudit
→GenericResource

The following tables summarize the properties included in this resource.

This first table contains the properties that are valid in the Management stage and in Delivery stages. If you have multiple delivery stages, you must configure the properties in each one of them.

Properties	Description	Default Value
`audit.config.refresh`	Web WEM Audit properties refresh time in minutes. Avoid the restart after configuration changes. You should wait until this interval is at maximum to see that the changes take effect.	5 minutes
`eventsDisabled`	Events that will not be audited are comma separated. You can specify the names of single events (like ContentSiteDelete) or you can specify a whole branch of events (like ContentSite). Using the ALL keyword will disable the auditing of all events for that stage. To disable all Auditing events, you must configure this parameter as ALL in all stages. In the Appendix 5 you can find a table containing all the possible events that can be filtered with this property.	Commented. Uncomment it and insert the event branches that you don't want to register.
`usersIgnored`	Users whose events are not going to be audited are comma separated. Using the ALL keyword would disable the auditing of all events.	Commented. Uncomment it and insert the users whose events you do not want to register.

Properties	Description	Default Value
`contentType.denied`	List of content types that are not going to be audited. By default, Web Experience Management Audit registers events for all content types. This property is useful to define a 'black list' of content types for which you do not want to register the events. Using the ALL keyword will disable the auditing of all content types. Use the Content Type XML name.	Commented. Uncomment it and insert the content types to be blacklisted.
`contentType.allowed`	List of content types that will be audited (only if contentType.denied is not set). This property is useful for the Web Experience Management installation if you only register events from few content types. Using the ALL keyword will enable the auditing of all content types. Use the Content Type XML name.	Commented. Uncomment it and insert the content types to be audited.
`workflows.denied`	A comma separated list of workflows that are not going to be audited. Using the ALL keyword will disable the auditing of all workflow events.	ALL
`workflows.allowed`	A comma separated list of workflows that will be audited.	Commented. Uncomment it and insert the workflows to be audited.
`task.<name_of_workflow>`	Used to specify a list of tasks to be audited for a concrete workflow. For example, if you are auditing a workflow named 'MyPublishing', but are only interested in the steps 'Begin' and 'End', you should add this parameter: task.MyPublishing=Begin,End	Commented. Uncomment it and insert the tasks to be audited.

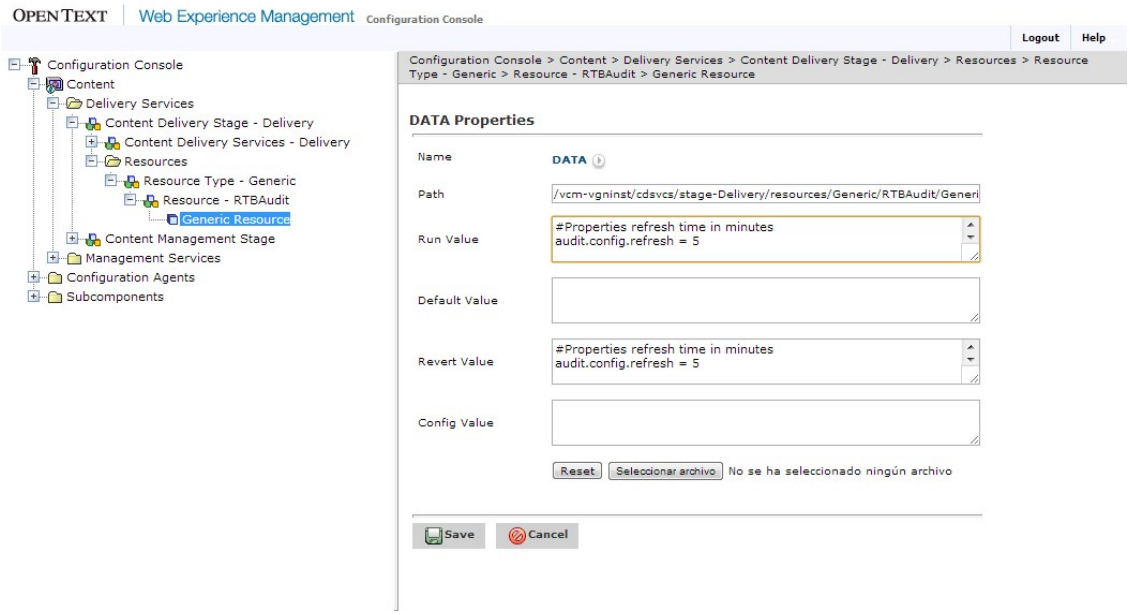
Properties	Description	Default Value
`job.var`	Name of the default publishing workflow. Do not change its value unless you explicitly have modified the default publishing workflows for Web Experience Management.	jobId
`job.task`	Name of the task invoked when starting the publishing workflow. Do not change this property unless you explicitly have modified the default publishing workflows for Web Experience Management.	BeginDeployment
`contentType.xml.denied`	Web Experience Management Audit can register, for content instances, not only generic information (user, date, etc.) but also the full XML data associated to every content instance. This parameter defines the Content types for which XML data should not be registered. By default, Web Experience Management Audit only registers generic information about the content instances (name, channel, etc.), but not the full information stored in the instance. Setting this property to a value is useful to register information of all the content instances except those listed in this property. Using the ALL keyword will disable the auditing of all XML associated with content types. Use the Content Type XML name.	Commented. Uncomment it and insert the content types whose xml should not be registered.

Properties	Description	Default Value
`contentType.xml.allowed`	Content types that allow XML to be registered (only if denied list does not exist). If set, this property has names of the content types that you need to register with WEM Audit. Using the ALL keyword will enable the auditing of all XML associated with content types. Use the Content Type XML name.	Commented. Uncomment it and insert the content types whose xml should be registered.
`contentinstance.details.preview`	If this property has the value true, the XML of ContentInstances that have the associated XSLT template for a preview in the WEM Management Console will be transformed when viewing the details of the event when a user clicks the WEM Audit History button. If the Content Type does not have a preview template, the XML will display. If this property has the value `false`, the XML will display despite the existence of the preview template for that Content Type.	true

The following properties will be created by default under this resource:

```
#Properties refresh time in minutes
audit.config.refresh = 5

#Ignored user list
#usersIgnored = robot1,robot2

#Ignored events list
#eventsDisabled = ContentChannel

#Worflows denied to register
#workflows.denied=[ALL|wf1,wf2,wf3]
workflows.denied=ALL

#Worflows to audit
#workflows.allowed=[ALL|wf1,wf2,wf3]
#workflows.allowed=ALL

#WorkFlow task to audit
#task.wf1=task1,task2

#Task who contains jobId, default BeginDeployment
#job.task=BeginDeployment

#Content types denied to register
#contentType.denied=[ALL|ct1,ct2,..]

#Content types allowed to register (only if denied list not exists)
#contentType.allowed=[ALL|ct1,ct2,..]

#Content types xml data denied to register
#contentType.xml.denied=[ALL|ct1,ct2,..]
contentType.xml.denied=ALL

#Content types xml data allowed to register (only if denied list not
exists)
#contentType.xml.allowed=[ALL|ct1,ct2,..]

contentInstance.details.preview = true
```

The following figure shows the location in the configuration console of this resource. Note that there is a resource for every stage:



When you change the DATA of the Generic Resource, you must restart the correspondent Deployment Agent if you want to see the changes immediately, otherwise it will be updated continuously according to the `audit.config.refresh` property.

2.5. Testing the Environment

WEM Audit includes several built-in tests that can be useful to verify that the installation process completed without errors. Before you perform tests, you must restart VgnVCMServer (and secondary servers at cluster) after the installation is finished, otherwise the results will not be accurate.

2.5.1. Testing RTB Insights Console

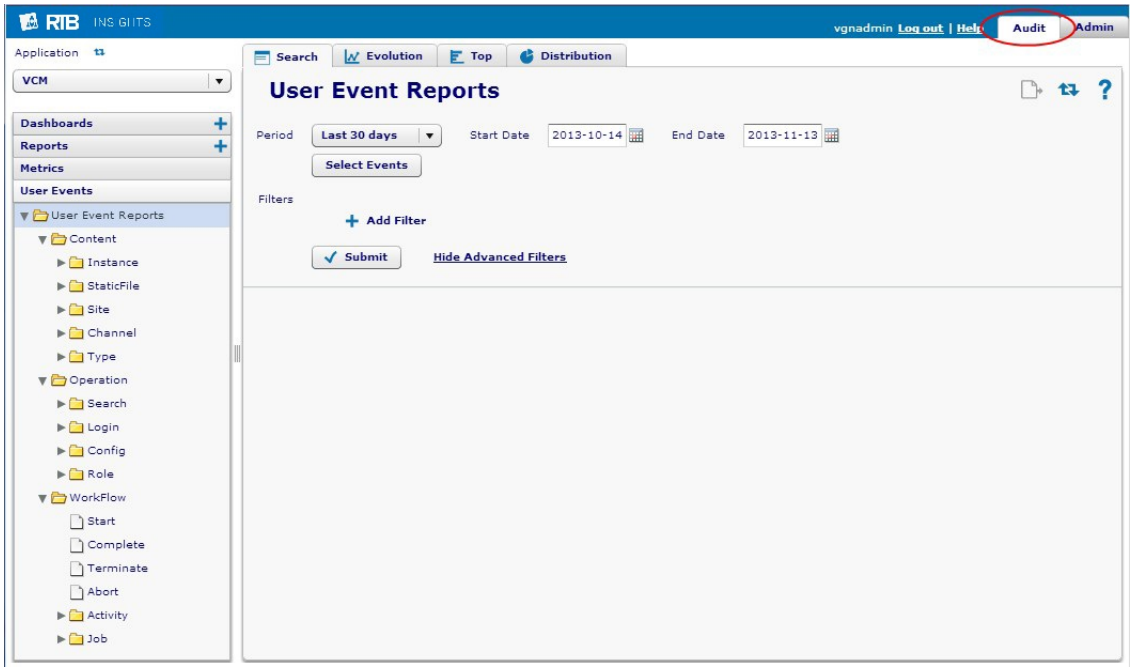
To test RTB Insights Console:

1. Open the RTB Insights Console diagnosis page (http://<VCM-host>:<port>/Insights/diagnosis) to ensure that the management console installation was successful.

RealTimeBiz ManagementConsole diagnosis

Test	Result
Testing kiron.js evaluation	✓
Testing Kiron entrypoint	✓
Testing ManagementConsole remoting	✓
Testing ManagementConsole DataBase connection	✓
Retrieving all ManagementConsole application names	VCM

2. If the test is successful, log in to the RTB Insights Console at this URL http://host:port/Insights. The Audit tab appears on the top right corner.

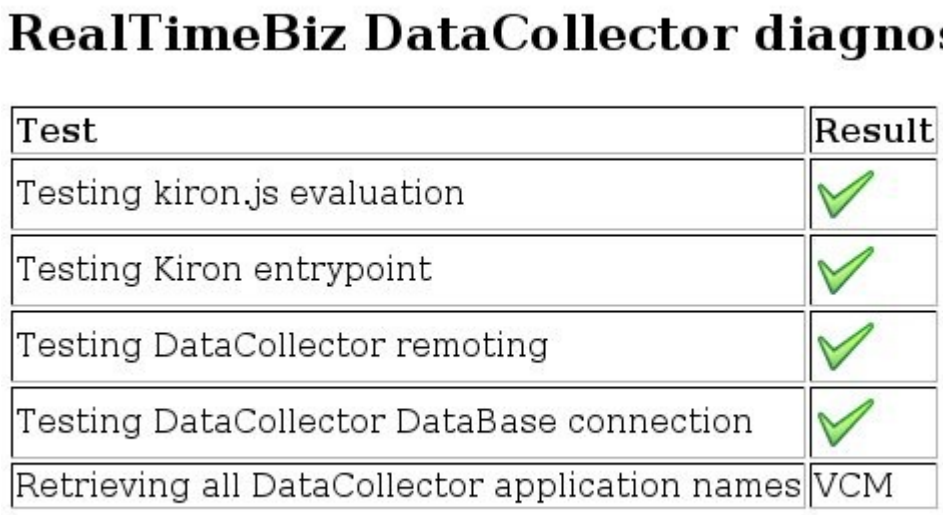


If you are unable to log in, see Access Denied to RTB Insights Console in Appendix 1 – Troubleshooting.

2.5.2. Testing the Collector Application

Open the Data Collector diagnosis page (http://<VCM-host>:<port>/collector/diagnosis) to

ensure that the Data Collector installation was successful.

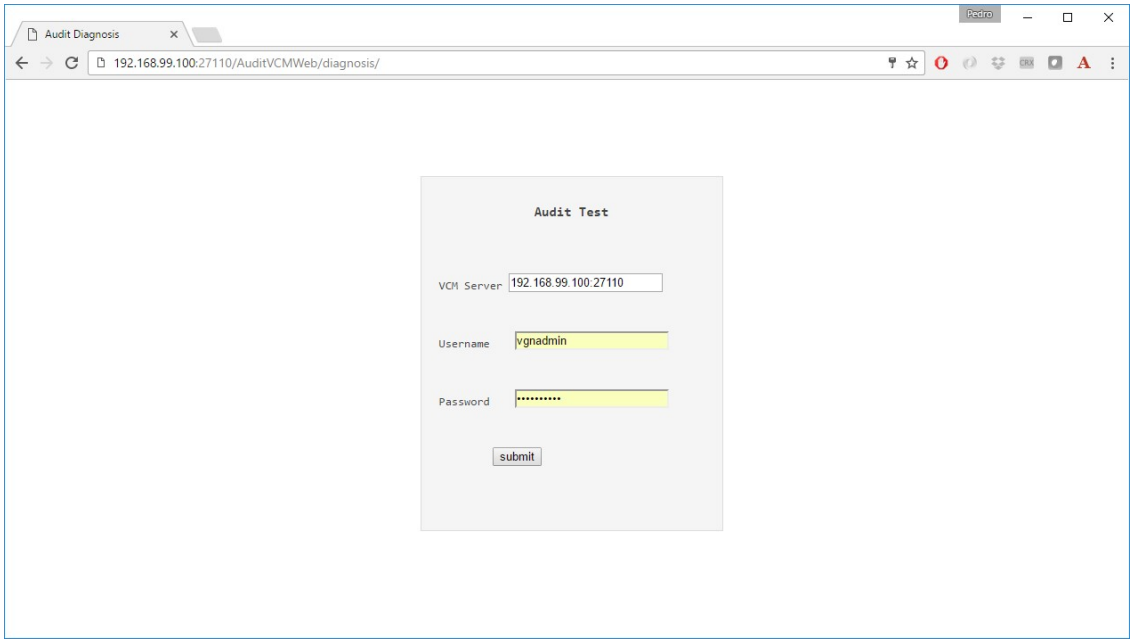


RealTimeBiz DataCollector diagnosis

Test	Result
Testing kiron.js evaluation	✓
Testing Kiron entrypoint	✓
Testing DataCollector remoting	✓
Testing DataCollector DataBase connection	✓
Retrieving all DataCollector application names	VCM

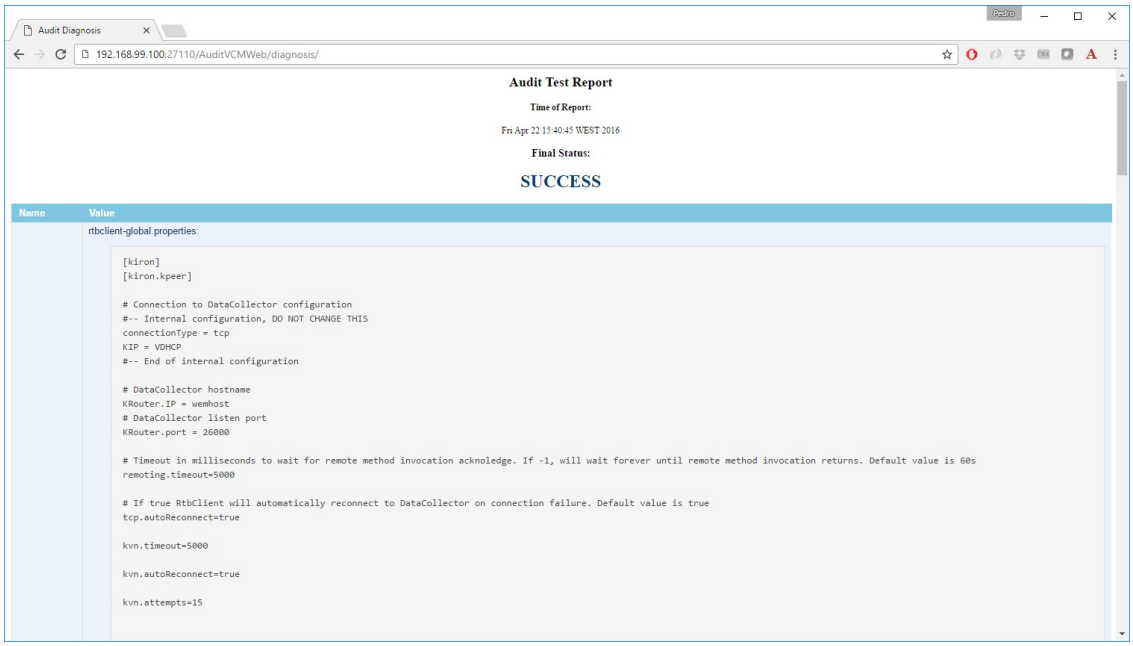
2.5.3. Testing the Audit System

The Audit Test tool is available at this URL: http://<VCM-host:port>/AuditVCMWeb/diagnosis .



To test the Audit System

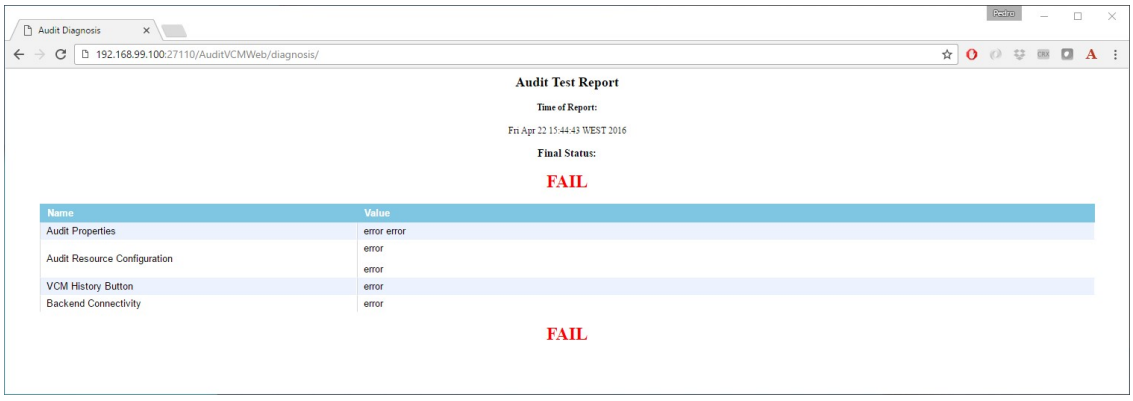
1. Enter the WEM hostname, a user name, and a password valid for VgnVCMServer. Click **Submit** to execute the test. When the test completes, the test results appear.



Note:

This test will fail if the hostname is not correct. You must have the full hostname where Web Experience Management Server is listening. If you have difficulties, you can perform the command `netstat -a` and check the `host:port` for Web Experience Management, and use it for the diagnosis.

2. If there are misconfigurations, the test will not succeed and a failure message will appear. The success message appears, if you correctly configure WEM Audit.



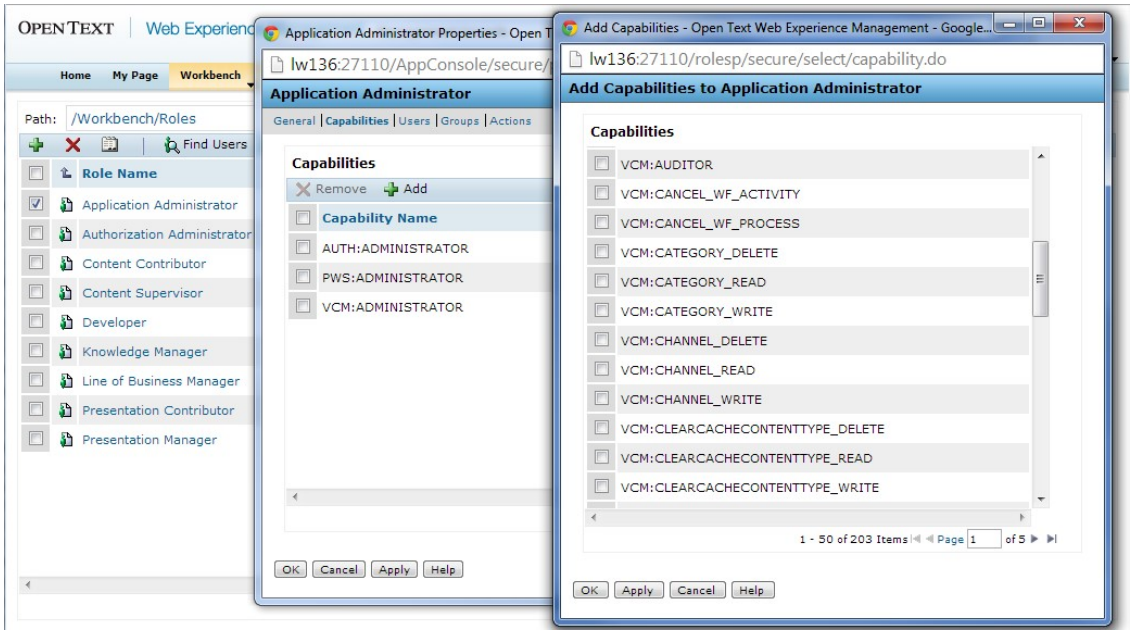
For more information, see the Troubleshooting section of this guide.

2.6. Updating Roles

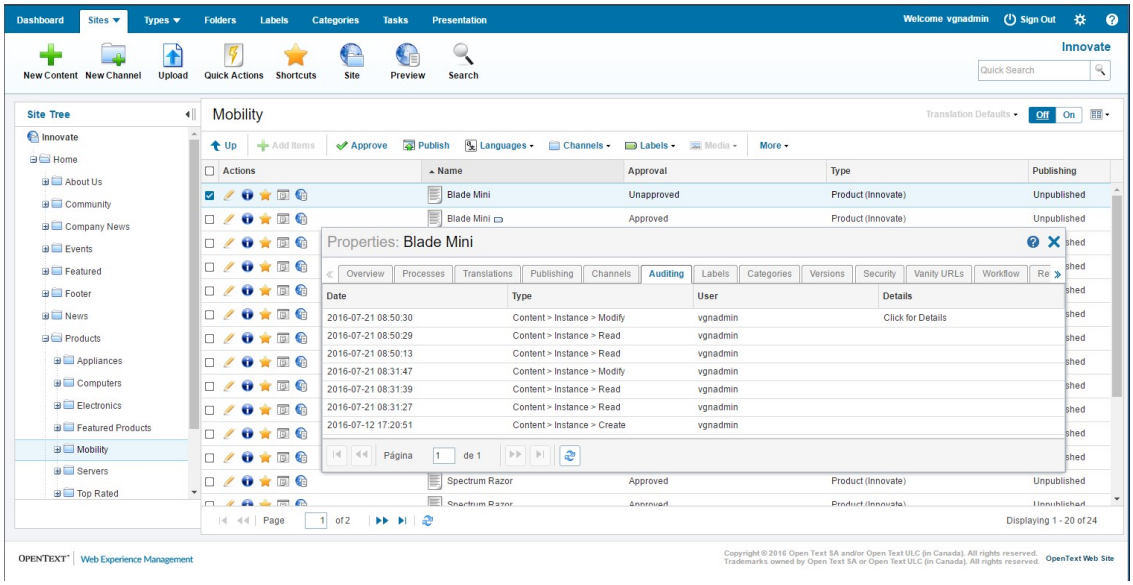
By default, all users can see the **Audit Events** button in the WEM Management Console and the **Auditing** tab in the Content Workspaces, but only users with the `VCM:AUDITOR` capability have the Audit Events button and the **Auditing** tab enabled. Note that the administrator with the `VCM:ADMINISTRATOR` capability always has the **Audit Events** button and the **Auditing** tab

enabled. To add this capability to other users, the WEM administrator must modify a user role and add the `VCM:AUDITOR` capability, using the following menu option in the WEM Management Console:

Workbench → Roles



Users with `VCM:AUDITOR` capability can see the **Auditing** tab in Content Workspaces. The following figure shows an example of the **Auditing** tab in Content Workspaces. Note that apart from having the capability, a user must belong to any of the groups that are authorized to make changes to the Web Experience Management object in question.



2.7. Executing RTB Loader

The RTB Loader utility takes the information stored in the content management system, and loads it in the event database of WEM Audit. All Content Instances, Sites, and Channels that already exist in WEM will generate their creation events, with the respective creation date.

RTB Loader also accepts filters, and registers events related to the WEM Configuration Console. The following steps are mandatory:

- Find RTBloader in `<AuditInstallDir>\rtbLoader` (i.e.: `C:\apps\wem audit\rtbLoader`)
- Launch the `load.bat` (or `load.sh`) script.
- Login into WEM as the Administrator user.

Although the script is configured to perform the typical execution of an initial load, it can be edited to modify one of the following parameters:

```
load -h host:port -u username -p password [-ldapFile ldap.properties |
-otdsFile otds.properties] [ -g outScript.out  | -o [ALL | SI | SF | RL |
CH | CV | CI  [-type XmlContentTypeName ]  ]  ]
```

Property	Description
`-h <host:port>`	Web Experience Management host and port
`-p <password>`	Web Experience Management user password
`-u <username>`	Web Experience Management username

Property	Description

`-ldapFile <ldap.properties>`	Path to properties files that contain the following attributes:
	
	groupAttribute=cn(Attribute of groups)
	groupObjectClass=groupOfNames
	userAttribute=cn(Attribute of users)
	userObjectClass=person
	## ALL | group1,group2,group3
	allowedGroups=ALL host=localhost:port
	userSearchBase=ou=People,dc=company,
	dc=es groupSearchMember=member
	# Please provider the password of ldap
	adminPassword=password
	adminName=cn=admin_name,dc=company
	,dc=es
	groupSearchBase=ou=Groups,dc=compan
	y,dc=es
	
	Note that the installation wizard generates a file with the above parameters adapted to your particular installation, except the password of the principal in LDAP.

`-otdsFile <otds.properties>`	Path to a properties file that contains the following attributes:
	
	#OTDS Configuration
	#OTDS REST Services URL
	otdsBaseURL=https://localhost:8443/otdsw
	s
	#OTDS Resource ID
	otdsResourceId=5261f244-71ed-4fe6-8d8f-
	b581b7976839
	#OTDS Secret Key
	otdsSecretKey=MwNod7vCBMxSgOAJbrfG
	0g==

`-g <outFileScript.sh>`	Generate command-line script with all possible exports. This is very useful in installations with hundreds of thousands of content instances, as the generated script can be split in several smaller scripts that can be launched in parallel to accelerate the event load.

Property	Description
`-o <WemObjectType>`	Web Experience Management Content Object to export:[ALL|CV|CT|CI|SI|SF|RL] Where ALL=All object types, CV=Configuration Values*, CT=Content Types, CI=Content Instances, SF=Static Files, CH=Channels, SI=Sites, RL=Roles
`-type <XmlNameOfContentType>`	XML name of the content type to load (only with CI)
`-interval <maxQueryValue>`	Maximum number of content instances committed in the same operation, [Default 300] (only with CI)
`-help`	Print a help message

There are two important points to remember:

- If the installation has a large number of content instances, it is recommended to use the `-g outputfileScript` parameter. This parameter is very useful to split the load in several steps. For example, a step to load channels, a step for every content type, and so on.
- If there are custom components in the installation, such as content types with a java class override, it is important to modify the `load.bat` (or `load.sh`) script to add in its classpath libraries where these classes reside. You must do this, so that the loader can successfully load custom components.

2.8. Installation on a Web Experience Management Cluster

```
================================================================================
==============================
Welcome to the Web Experience Management Audit install wizard
Please ensure that you have read the prerequisites chapter in the
documentation before going any further.

The following processes must be running before proceeding:
{blank}
    - VgnVCMServer (all cluster nodes), VgnAdminServer and Config Agents.
================================================================================
==============================

Please, select the Installation Type that you will be using. Notice that
the installer should be launched at every machine running a Web Experience
Management cluster node. For installation with just one cluster node use
option 1.

(Select one option [insert option number])
1) Install on Web Experience Management cluster primary node.
2) Install on Web Experience Management cluster secondary node.
```

If you are installing WEM Audit in a Web Experience Management cluster with several nodes, you must launch the installation wizard in each one of its machines. You must start with the installation on the primary node, and only then proceed to the secondary nodes.

3. Upgrading to OpenText™ Web Experience Management Audit 16.2.1

The following section provides information on how to upgrade to OpenText™ Web Experience Management Audit 16.2.1.

3.1. How to Upgrade

Proceed with the following steps:

- Make a backup of your OpenText™ Web Experience Management Audit Database, following the instructions from your provider.
- Launch the uninstaller for your current OpenText™ Web Experience Management Audit. Follow the instructions in Uninstalling Web Experience Management Audit.
- Launch the SQL script located under `config/dataModel/<DB_VENDOR>/migration/from_X_Y.sql`, where X_Y represents your current version. If the script does not exist for your version, then you do not need one.
- Launch the OpenText™ Web Experience Management Audit 16.2.1 installer, and perform a new installation on top of your current Audit Database. As the database already exists, the installer will not make modifications to it and the application will be upgraded without you losing any data.

4. Uninstalling Web Experience Management Audit

This section provides information on how to uninstall WEM Audit.

4.1. Launching Uninstall Wizard

Under the root of WEM Audit folder, the installer creates a folder named uninstaller. This folder contains the following uninstall scripts:

- `uninstall.sh` for UNIX
- `uninstall.bat` for Windows

Before launching the uninstaller ensure that you are using java 1.6, and `JAVA_HOME/bin` as a system path. You can use `<WEMinstallDir>/Content/16_2/java` dir as your Java installation. To launch the script execute the uninstall.* file.

For Unix:

```
$chmod u+x uninstall.sh
$./uninstall.sh
```

For Windows:

```
>uninstall.bat
```

The uninstaller seeks for the necessary information for the uninstall process. If you have installed WEM Audit in Delivery Stages on remote machines, you must run the uninstaller on each machine.

```
===============================================================
Welcome to the Web Experience Management Audit uninstall Wizard
The following processes must be running before proceeding:
    VgnVCMServer, VgnAdminServer and Config Agents.
===============================================================

----------------------------------------
Web applications uninstallation
----------------------------------------
In the next step the following components will be uninstalled:

- Web Experience Management Audit application.
- Web Experience Management Audit Data Collector application.
- Start Parameters.
- RTB Insights Console application.
- Pools and Datasources.

Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
>Value:
[yes]
```

```
Uninstalling ....
Removing connection pool ...
-->Connection pool removed.
Removing start parameters ...
-->Start parameters removed.

Uninstalling Web Experience Management Audit App ...
-----------------------------------------------
-----------------------------------------------
--> Web Experience Management Audit App Uninstalled.

Uninstalling Collector App ...
-----------------------------------------------

-----------------------------------------------
-->Uninstall Collector App Uninstalled.

Uninstalling RTB Insights Console...
-----------------------------------------------
-----------------------------------------------
-->Uninstall RTB Insights Console Uninstalled.
done.


----------------------------------------
Web Experience Management configuration
----------------------------------------
In the next step the following components will be uninstalled:

- Workflow listeners.
- Audit libraries.
- Web Experience Management Audit property sheet.
- Audit generic resource.
- Deployment Agent parameters.
- History Button.
- Web Experience Management Automatic Task.

Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]

Please type Web Experience Management (VgnVCMServer) connection info.
-----------------------------------------------------------------------

Web Experience Management Server Host
 >Default value [rtbtests]
 >Value:
[rtbtests]

Web Experience Management Port
 >Default value [27110]
 >Value:
[27110]

Admin User
 >Default value [vgnadmin]
 >Value:
[vgnadmin]

Admin User Password

Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]

Uninstalling ....
Removing data from Deployment Agents ...
```

```
-->Deployment Agents data removed.
Removing generic resource ...
-->Generic resource removed.
Removing workflow listener ...
-->workflow listener removed.
Removing buttons ...
-->Buttons removed.
Removing audit property sheet …
-->Audit property sheet removed.
Committing changes ...
Doing deploy (configp) ...

##The next step requires the execution of configp

Please press any key

This action may take several minutes, please wait
->Deploy (configp) finished.
Removing Audit program task definition ...
-->Audit program task definition removed.
done.


----------------------------------------
Web Experience Management Audit Database
----------------------------------------
In the next step the following components will be uninstalled:
-Auditor capability.
Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]


Web Experience Management database user information
----------------------------------------
Please provide the parameters needed for connecting to Web Experience
Management system database user.

Database software
(Select one option [insert option number])
1)Oracle
2)MSSQL
3)Postgres
2

Database Host
 >Default value [localhost]
 >Value:
[localhost]

Database Port
 >Default value [1433]
 >Value:
[1433]

Database Instance Name
 >Default value [VCMMGMT]
 >Value:
[VCMMGMT]

Database User
 >Default value [vcmmgmt]
 >Value:
[vcmmgmt]

Database User Password
```

```
Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
>Value:
[yes]

Uninstalling ....
Removing auditor capability ...
-->Capability removed.
done.


-----------------------------------------
Directory structure
-----------------------------------------
In the next step the following components will be uninstalled:
-Uninstaller binaries.
-Web Experience Management Audit Applications files.
-Web Experience Management Audit libraries files.
-Folder structure.
-Audit properties files.

Do you want to continue? (yes - continue / no - go back)
 >Default value [yes]
 >Value:
[yes]

Uninstalling ....

Removing libraries ...
-->Libraries removed.
Removing properties ..
-->Properties removed.
Removing applications ..
-->Aplications removed.
Removing folders
-->Folders removed.
done.

The uninstallation process has finished successfully. Please remove Web
Experience Management Audit folder manually and start all servers and
Config / Deployments Agents.


WARNING: This uninstallation process does not remove the database schema
of Web Experience Management Audit, so that you don't lose your data. If
you need to remove this database schema, please do it manually.

Please press any key
```

4.2. Final Steps

To completely remove WEM Audit you must manually complete the following manual steps:

- Remove the WEM Audit folder
- Delete the information stored in the WEM Audit database. After performing this step you will lose all the historic information. Do not perform this step if you plan to upgrade to another version with the intention to keep existing events.

4.3. Uninstalling from a Web Experience Management Cluster

If the product is installed on a Web Experience Management cluster with several nodes, the uninstall wizard must be launched at each node.

Launch the uninstaller wizard in the Primary node of the cluster (VgnVCMServer), following the steps from section Launching the Uninstall Wizard.

Once the wizard completes, you can proceed with uninstalling it in the Secondary nodes.

5. Appendix 1 - Troubleshooting

5.1. Access Denied to RTB Insights Console

If you try to access RTB Insights Console without success, you will receive one of the following error messages:

- **'Invalid username / password':** You have entered a wrong username or password.
- **'Insufficient privileges':** Your password is OK, but you don't belong to any LDAP group with privileges to access RTB Insights.
- **'Unable to check your privileges':** Audit was wrongly installed, so the LDAP connection is not well configured. Check the LDAP section in `<AuditInstallDir>\webapps\management.properties`. Once you have modified the management.properties file, you must restart the server in order to the changes take effect.

5.2. Using TAS

RTB Insights supports the OpenText Trusted Authentication Server (TAS) allowing you to use this tool. It is however supported in WEM Audit, so the event history can be viewed through a preview application server using TAS.

To use TAS with WEM Audit and RTB Insights Console, do the following:

- If TAS is defined as your default web application, there are no additional steps to perform; it should be working out-of-the-box.
- If TAS is not your default web application, you must create the `AuditVCMWeb.war` file and the `Insights.war` file following TAS instructions on how to create a proxy web application, available in the chapter Deploying Extensions for TAS in the Web Experience Management *Dynamic Portal and Site Configuration Guide 16.0*. Then you need to redeploy those WARs. `Insights.war` is deployed as a common webapp in you server's `webapps` folder. `AuditVCMWeb.war` is deployed using WEM `configp` utility.

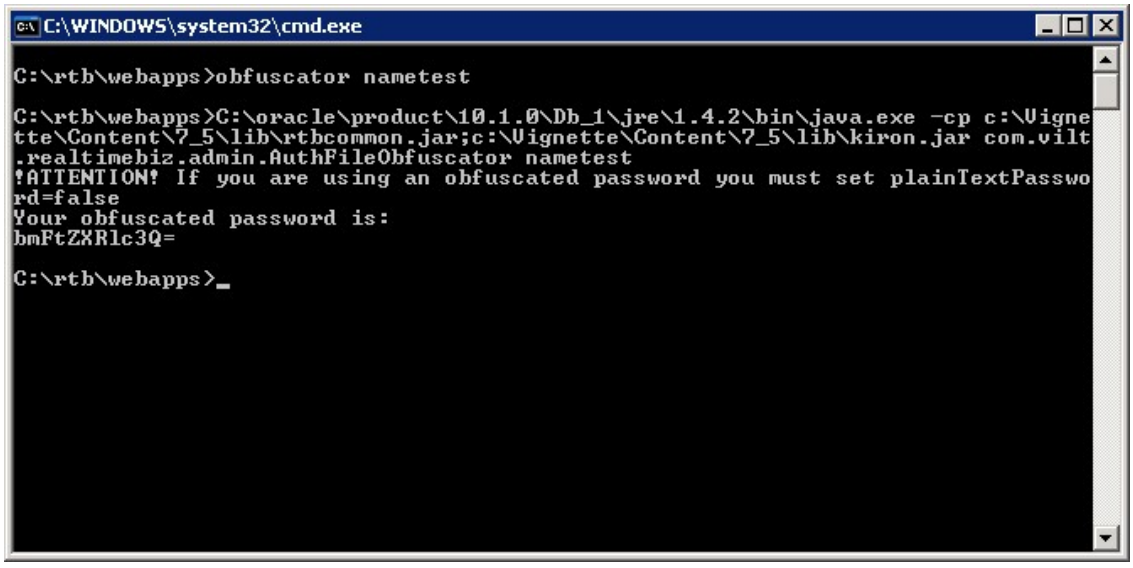
6. Appendix 2 - Properties Files

The properties files included in the WEM Audit 16.2.1 distribution have this structure:

- `<AuditInstallDir>/rtbclient/`
  - `rtbclient-global.properties`
- `<AuditInstallDir>/webapps/`
  - `collector.properties`
  - `management.properties`

> **Important:**
>
> In order to work properly, the files must be saved in UTF-8.

Both the password of the LDAP principal user and the password of the Email Account used by Web Experience Management Audit to send mails are obfuscated for enhanced security. In the installation process, the passwords requested to the user are obfuscated; in case of any of this passwords need to be changed in the future, the administrator must use the tool `obfuscator.bat/obfuscator.sh` to update the properties files. The following figure demonstrates how to do it.



The obfuscated password must be manually copied into the properties files at the appropriate location.

6.1. Collector Properties (`collector.properties`)

```
[main]

#The DataBase vendor: Oracle | MSSQL | Postgres
DB.type=MSSQL
```

```
#This property defines the timeout in milliseconds to keep alive a browser
RTB session upon inactivity. It has a default value of 5min. If set to -1
the session will remain alive until it is closed manually.
browserKRouterConnection.timeout=1800000

#Name of the JNDI Data Source to use
DB.poolDataSource=jdbc.RTBMMSQL

#Weblogic conection.The value should be t3://<server>:<port>
java.naming.provider.url=t3://localhost:27110

#Initial Factory for Weblogic pool
java.naming.factory.initial=weblogic.jndi.WLInitialContextFactory

#User that owns the DB schema. This must be set when there are multiple
RTB instalations on the same DBMS
#DB.schemaOwner=VILTSITE

#IP range database location
#geolocation=/home/geolocation

#Use plain text password
plainTextPassword=false

#The SMTP host used to send mails
SMTPHost=rtbtests

#The SMTP port used to send mails
SMTPPort=25

#The account used to send mails
emailSenderUsername=rtb@vilt.es

#The account's password
emailSenderPassword=cnRi

#The name that will appear as the sender. This has effect only in
MyReports module and represents the email sender name
#emailSenderPersonalName=RTB


[kiron]

[kiron.kpeer]


#This section defines kiron's internal configuration

#Internal configuration, DO NOT CHANGE THIS

connectionType=local
KIP=0

#DataCollector hostname
KRouter.IP=rtbtests

kvn.attempts=-1

#End of internal configuration

#Internal thread pool size. This pool is used to dispatch event
registration. Default size is 10
#remoting.threadPool=10

#Browser client identification cookie lifetime in milliseconds. -1 will
last until the user closes the browser
#http.cookie.age=-1

#Maximum time that pool conexion its open
```

```
#leaserReaper.timeout=10000

[kiron.krouter]

#DataCollector Kiron listen port
port=26000

[logging]

=WARN, RFile


[authentication]

#This section defines the properties related to the authentication
#Class used for authentication

authenticatorClass=com.vilt.realtimebiz.bousers.jndi.JNDIIntegration

#Enables/Disables authentication mechanism, default is enabled

authDisable=0

#Ldap Connection URL
ldapurl=ldap://rtbtests:27110


#LDAP Principal User
adminName=uid=vgnadmin,ou=people,ou=VgnLDAPRealm,dc=vgndomain
groupAttribute=cn

#Principal password
adminPassword=dmlnbmV0dGU=

#Base to search users. Root of LDAP tree where to begin the user lookup.
searchBase=ou=people,ou=VgnLDAPRealm,dc=vgndomain

#Base to search groups
groupSearchBase=ou=groups,ou=VgnLDAPRealm,dc=vgndomain

#Group class property
groupObjectClass=groupOfUniqueNames

#User group property
groupSearchMember=uniqueMember

#If true, will use complete user DN for authentication, otherwise the
username is used. Must be true in some LDAP implementations
principal.useDN=true

#Use DIGEST-MD5 for LDAP user authentication, default disabled
#java.naming.security.authentication=DIGEST-MD5

#User identification property
userResolver=uid

#User object class
userObjectClass=inetOrgPerson

#Use plain text password. Default true
plainTextPassword=false


[rolemapper]

#This section defines the rolemapper's properties
#Role mapping in file system (default)
rolemapperClass=com.vilt.realtimebiz.bousers.SimpleFileRoleMapper
```

```
#These properties define the AD attributes to use in role mapping. If you
are using the user fully qualified name to map roles you don't need this.
Just keep your properties as they are
#attributeNames=memberOf distinguishedName

#Role enumeration. Specify all needed roles
applicationRoles=Audit Admin xml_viewer scheduling VCM
role.scheduling=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain
role.Audit=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain
role.Admin=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain
role.VCM=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain
role.xml_viewer=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain

[support]

#This section is used to define the properties for the log sending
facilities

#The location of the log file
files=c:/program files/vcm audit/logs/rtbcollector.log

#The name that will appear as the sender
emailSenderPersonalName=RTB

#Destination mails, comma-separated
SendTo=admin@vilt.es
```

6.2. RTB Insights Console Properties (`management.properties`)

```
[main]

#The limit of search pages for file exports, each page has 10 results.
Default is 30. e.g. 50 = 500 results will be exported to file
searchExportPageLimit=50

#The DataBase vendor: Oracle | MSSQL | Postgres
DB.type=MSSQL

#Name of the JNDI Data Source to use
DB.poolDataSource=jdbc.RTBMMSQL

#Enables/Disables facts, default is false
facts.enabled=false

#Weblogic conection
java.naming.provider.url=t3://rtbtests:27110

#Enables/Disables property value caching, default is disabled
propertyValueCache=disabled

#If enabled will return null in case of a PV Cache miss. If disabled it
will not populate the cache. Default is enabled.
propertyValueReturnCacheOnly=enabled

#Initial Factory for Weblogic pool
java.naming.factory.initial=weblogic.jndi.WLInitialContextFactory

#If enabled will build the PV cache when the server starts up. Default is
disabled
propertyValueCacheStartup=disabled

#User that owns the DB schema. This must be set when there are multiple
RTB instalations on the same DBMS
#DB.schemaOwner=VILTSITE
```

```
#IP range database location
#geolocation=/home/geolocation

#Use plain text password
plainTextPassword=false

#The SMTP host used to send mails
SMTPHost=rtbtests

#The SMTP port used to send mails
SMTPPort=25

#The account used to send mails
emailSenderUsername=rtb@vilt.es

#The account's password
emailSenderPassword=cnRi

#The name that will appear as the sender
#emailSenderPersonalName=RTB


[kiron]

[kiron.kpeer]


#This section defines kiron's internal configuration
#Internal configuration, DO NOT CHANGE THIS

connectionType=local
KIP=0

#End of internal configuration

#DataCollector hostname
KRouter.IP=rtbtests

#Cookie name
cookieName=managementKIP

#This property defines the timeout in milliseconds to keep alive a browser
RTB session upon inactivity. It has a default value of 5min. If set to -1
the session will remain alive until the browser is closed
browserKRouterConnection.timeout=-1

[kiron.krouter]

#DataCollector Kiron listen port
port=26099

[logging]

#This section defines the properties related to the logging system. By
default the log levels are set to warning (WARN). If you are having
troubles, log levels should be set to DEBUG

 #RFile is set to be a FileAppender
log4j.appender.RFile=org.apache.log4j.RollingFileAppender

#RFile maximum sixe
log4j.appender.RFile.MaxFileSize=1000KB

#RFile max backup index
log4j.appender.RFile.MaxBackupIndex=10

#RFile log file
log4j.appender.RFile.File=c:/program files/vcm
audit/logs/rtbmanagement.log
```

```
#RFile layout. RFile uses PatternLayout
log4j.appender.RFile.layout=org.apache.log4j.PatternLayout

#RFile ConversionPattern
log4j.appender.RFile.layout.ConversionPattern=%d [%t] %-5p %c{2} %x - %m%n

#package com.vilt.kiron. Set it to DEBUG level to get details about the
underlying communication layer
log4j.logger.com.vilt.kiron=WARN, RFile

#package com.vilt.realtimebiz. Set it to DEBUG level to get details about
the handling of events
log4j.logger.com.vilt.realtimebiz=WARN, RFile


[authentication]

#This section defines the properties related to the authentication
 #Class used for authentication

authenticatorClass=com.vilt.realtimebiz.bousers.jndi.JNDIIntegration

authDisable=0


#Ldap Connection URL
ldapurl=ldap://rtbtests:27110


#LDAP Principal User
adminName=uid=vgnadmin,ou=people,ou=VgnLDAPRealm,dc=vgndomain


groupAttribute=cn

#Principal password
adminPassword=dmlnbmV0dGU=

#Base to search users
searchBase=ou=people,ou=VgnLDAPRealm,dc=vgndomain

#Base to search groups
groupSearchBase=ou=groups,ou=VgnLDAPRealm,dc=vgndomain

#Group class property
groupObjectClass=groupOfUniqueNames

#User group property
groupSearchMember=uniqueMember

#If true, will use complete user DN for authentication, otherwise the
username is used. Must be true in some LDAP implementations
principal.useDN=true

#Use DIGEST-MD5 for LDAP user authentication, default disabled
#java.naming.security.authentication=DIGEST-MD5

#User identification property
userResolver=uid

#User object class
userObjectClass=inetOrgPerson

#Use plain text password. Default true
plainTextPassword=false

[rolemapper]
```

```
#This section defines the rolemapper's properties
#Role mapping in file system (default)

rolemapperClass=com.vilt.realtimebiz.bousers.SimpleFileRoleMapper

#These properties define the AD attributes to use in role mapping. If you
are using the user fully qualified name to map roles you don't need this.
Just keep your properties as they are
#attributeNames=memberOf distinguishedName

#Role enumeration. Specify all needed roles
applicationRoles=Audit Admin xml_viewer scheduling VCM


role.scheduling=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain
role.Audit=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain
role.Admin=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain
role.VCM=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain
role.xml_viewer=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain

[scheduling]

#This section defines the scheduling properties

#cron format: seconds, minutes, hours, day of month, month, day of week,
(year)
#0 0 12 * * ?              Fire at 12pm (noon) every day
#0 15 10 ? * *          Fire at 10:15am every day
#0 15 10 * * ?          Fire at 10:15am every day
#0 15 10 * * ? *        Fire at 10:15am every day
#0 15 10 * * ? 2005     Fire at 10:15am every day during the year 2005
#0 * 14 * * ?           Fire every minute starting at 2pm and ending at
2:59pm, every day
#0 0/5 14 * * ?         Fire every 5 minutes starting at 2pm and ending at
2:55pm, every day
#0 0/5 14,18 * * ?      Fire every 5 minutes starting at 2pm and ending at
2:55pm, AND fire every 5 minutes starting at 6pm and ending at 6:55pm,
every day
#0 0-5 14 * * ?         Fire every minute starting at 2pm and ending at
2:05pm, every day
#0 10,44 14 ? 3 WED     Fire at 2:10pm and at 2:44pm every Wednesday in
the month of March.
#0 15 10 ? * MON-FRI    Fire at 10:15am every Monday, Tuesday, Wednesday,
Thursday and Friday
#0 15 10 15 * ?         Fire at 10:15am on the 15th day of every month
#0 15 10 L * ?          Fire at 10:15am on the last day of every month
#0 15 10 ? * 6L         Fire at 10:15am on the last Friday of every month
#0 15 10 ? * 6L         Fire at 10:15am on the last Friday of every month
#0 15 10 ? * 6L 2002-2005   Fire at 10:15am on every last friday of every
month during the years 2002, 2003, 2004 and 2005
#0 15 10 ? * 6#3            Fire at 10:15am on the third Friday of every
month
#0 0 12 1/5 * ?         Fire at 12pm (noon) every 5 days every month,
starting on the first day of the month.
#0 11 11 11 11 ?            Fire every November 11th at 11:11am.

crons=SegmentUpdater,PropertyValueUpdater,EventLifetime,PropertyValueCache
Reloader

#segment updater schedule class
SegmentUpdater.class=com.vilt.realtimebiz.scheduling.SegmentUpdaterJob

#segment updater schedule class
SegmentUpdater.cron=0 0 01 1/5 * ?

#Property value updater class
PropertyValueUpdater.class=com.vilt.realtimebiz.scheduling.PropertyValueUp
daterJob
```

```
#Property value updater class
PropertyValueUpdater.cron=0 0 02 * * ?

#Event lifetime class. This task is used to remove events older than its
associated lifetime
EventLifetime.class=com.vilt.realtimebiz.scheduling.EventLifetimeJob

#Event lifetime class. This task is used to remove events older than its
associated lifetime
EventLifetime.cron=0 0 0 1/5 * ?

#ManagementConsole cache job
PropertyValueCacheReloader.class=com.vilt.realtimebiz.reporting.PropertyVa
lueCacheReloaderJob

#ManagementConsole cache job
PropertyValueCacheReloader.cron=0 0 03 * * ?

[scheduling.quartz]

#Quartz scheduler internal configuration. Please do not modify this

org.quartz.scheduler.instanceName=Sched1
org.quartz.scheduler.instanceId=1
org.quartz.scheduler.rmi.export=false
org.quartz.scheduler.rmi.proxy=false
org.quartz.threadPool.class=org.quartz.simpl.SimpleThreadPool
org.quartz.threadPool.threadCount=3
org.quartz.jobStore.class=org.quartz.simpl.RAMJobStore

#End of quartz internal configuration

[support]

#This section is used to define the properties for the log sending
facilities
#The location of the log file

files=c:/program files/vcm audit/logs/rtbmanagement.log

#The name that will appear as the sender
emailSenderPersonalName=RTB

#Destination mails, comma-separated
SendTo=admin@vilt.es
```

6.3. Client Properties (`rtbclient-global.properties`)

```
[kiron]

[kiron.kpeer]

#This section defines kiron's internal configuration

#Internal configuration, DO NOT CHANGE THIS

connectionType=tcp
KIP=VDHCP

#End of internal configuration


#DataCollector hostname
KRouter.IP=rtbtests
```

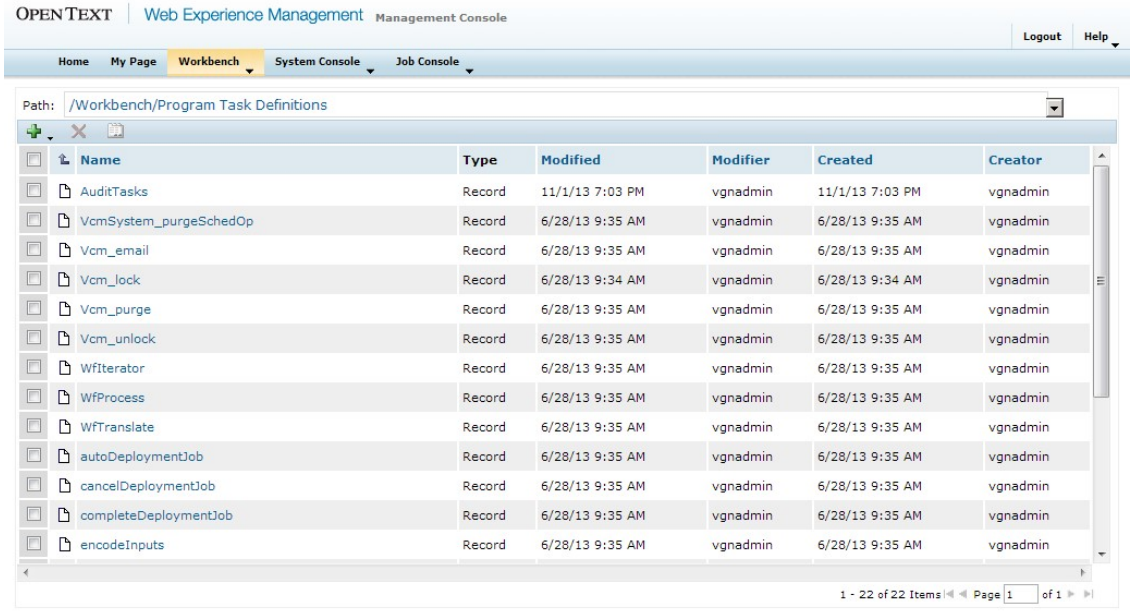
```
#DataCollector listen port
KRouter.port=26000

#Timeout in milliseconds to wait for remote method invocation acknowledge.
If -1, will wait forever until remote method invocation returns. Default
value is 5s
remoting.timeout=5000

#If true RtbClient will automatically reconnect to DataCollector on
connection failure. Default value is true
tcp.autoReconnect=true

#Internal configuration, DO NOT CHANGE THIS

kvn.timeout=5000
kvn.autoReconnect=true
kvn.attempts=15

#End of internal configuration

[rtbclient]

#This section defines the configuration of rtbclient

#If true, client will wait until RtbClient connects to DataCollector
waitForConnection=true

#Enable/Disable RtbClient. Enabled by default
#rtbclient.enable=true

#Timeoutto wait for DataCollector connection in milliseconds
waitForConnectionTimeout=60000

#If true, RtbClient will register events even if user HttpServletRequest
does not have cookies. True by default
#rtbclient.no_cookies=true


[logging]

#This section defines the properties related to the logging system. By
default the log levels are set to warning (WARN). If you are having
troubles, log levels should be set to DEBUG

#RFile is set to be a FileAppender
log4j.appender.RFile=org.apache.log4j.RollingFileAppender

#RFile maximum sixe
log4j.appender.RFile.MaxFileSize=1000KB

#RFile max backup index
log4j.appender.RFile.MaxBackupIndex=10

#RFile log file
log4j.appender.RFile.File=c:/program files/vcm audit/logs/rtbclient.log

#RFile layout. RFile uses PatternLayout
log4j.appender.RFile.layout=org.apache.log4j.PatternLayout

#RFile ConversionPattern
log4j.appender.RFile.layout.ConversionPattern=%d [%t] %-5p %c{2} %x - %m%n

#package com.vilt.kiron. Set it to DEBUG level to get details about the
underlying communication layer
log4j.logger.com.vilt.kiron=WARN, RFile

#package com.vilt.realtimebiz. Set it to DEBUG level to get details about
the handling of events
log4j.logger.com.vilt.realtimebiz=WARN, RFile
```

```
#file2 is set to be a FileAppender
log4j.appender.file2=org.apache.log4j.RollingFileAppender

#file2 maximum size.
log4j.appender.file2.MaxFileSize=10000KB

#file2 MaxBackupIndex
log4j.appender.file2.MaxBackupIndex=10

#file2 log file
log4j.appender.file2.File=c:/program files/vcm audit/logs/rtbVcmAudit.log

#file2 layout. file2 uses PatternLayout
log4j.appender.file2.layout=org.apache.log4j.PatternLayout

#file2 ConversionPattern
log4j.appender.file2.layout.ConversionPattern=%d [%t] (%F:%L) %-5p %c{2}
(%x) - %m%n

#package com.vilt.audit.listeners. Set it to DEBUG level to get details on
the event listener
log4j.logger.com.vilt.audit.listeners=WARN, file2

#package com.vilt.audit.wf. Set it to DEBUG level to get details on the
workflow listener
log4j.logger.com.vilt.audit.wf=WARN, file2

#package com.vilt.audit.utils
log4j.logger.com.vilt.audit.utils=WARN, file2

#package com.vilt.audit.history. Set it to DEBUG level to get details on
the event history popup in VCM
log4j.logger.com.vilt.audit.history=WARN, file2

#package com.vilt.audit.weblogic. Set it to DEBUG level to get details on
the weblogic auditor
log4j.logger.com.vilt.audit.weblogic=WARN, file2

#file3 is set to be a FileAppender.
log4j.appender.file3=org.apache.log4j.RollingFileAppender


#file3 Maximum size.
log4j.appender.file3.MaxFileSize=10000KB

#file3 MaxBackupIndex
log4j.appender.file3.MaxBackupIndex=10

#file3 log file
log4j.appender.file3.File=c:/program files/vcm audit/logs/rtbLoader.log

#file3 layout
log4j.appender.file3.layout=org.apache.log4j.PatternLayout

#file3 ConversionPattern
log4j.appender.file3.layout.ConversionPattern=%d [%t] (%F:%L) %-5p %c{2}
(%x) - %m%n

#RTBLoader log
log4j.logger.com.vilt.audit.load=DEBUG, file3


[support]
#This section is used to define the properties for the log sending
facilities
#The location of the log file
files=c:/program files/vcm audit/logs/rtbclient.log
```

7. Appendix 3 – Audit Task

7.1. About the Audit Task

The workflow automated task is part of a set of tools included in the RTB extensibility. AuditTasks is used to log the events generated in the workflows. You must use it if you want to audit existing custom workflows whose events are not registered by the WorkFlow Listener. When running the installer, the application AuditVCMApp will be automatically installed. It automatically creates a new Program Task Definition named AuditTasks.

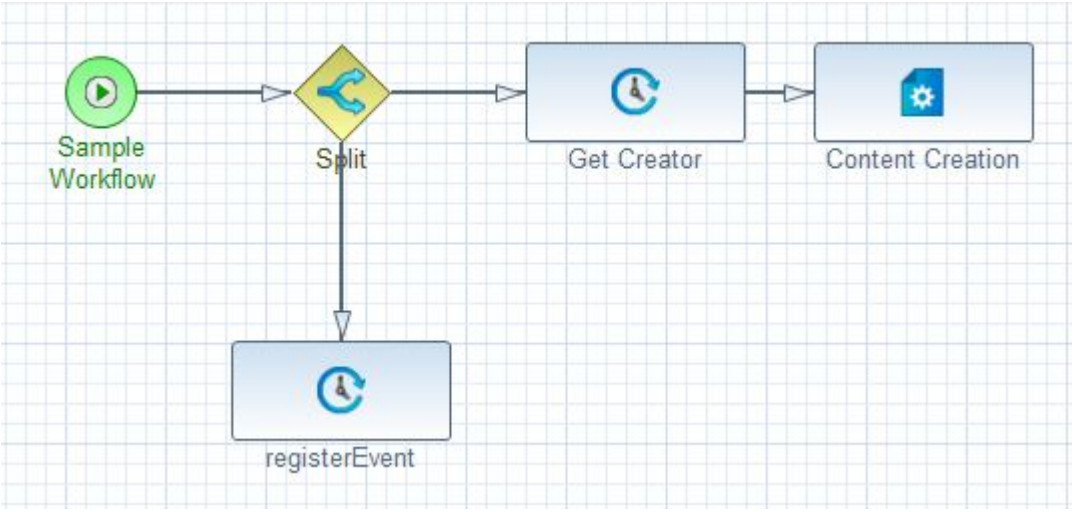


[Audit Task] | *auditTask2.jpg*

An automatic task named **registerEvent** is created. You need to place it in specific points of the WorkFlows's diagrams in order to audit them.

7.2. Workflows Update

The custom WorkFlows developed by the costumer can be audited using the program task **registerEvent**. To use it, it is necessary to add a new automatic task in the workflow diagram. This task receives as input the event name that is going to be audited and its properties as parameters, described in the next section. In the diagram below, the only required change is to add a new split that redirects the exit of the task to be audited to the **registerEvent** task.



7.3. Parameters

The task registerEvent receives the following 16 parameters:

1. **taskType:** Type of the task that can have the values **escalation**, **manual**, or **auto**, depending on how the user is obtained:
    - **escalation or manual:** The user is obtained from a parameter named user.
    - **auto:** The user is obtained automatically.
2. **user:** Used to define the user when **taskType** is **escalation** or **manual**.
3. **eventName:** A name used to register the event. By default, the event is registered with the following concatenation of properties:
    - taskType
    - workflowId

If the task has an associated payload, there will be as many events registered as the contents that the payload has. By default, the following attributes will be added:

- vcmId
- name

Along with these attributes, the attributes defined by the following parameters, with the syntax **paramX=valueX**, will always try to be registered:

4. **pBool1**
5. **vBool1**
6. **param1**
7. **value1**
8. **param2**
9. **value2**

10. **param3**
11. **value3**
12. **param4**
13. **value4**
14. **param5**
15. **value5**
16. **result** (Not used).

8. Appendix 4 - Events

The following table shows the complete list of events that WEM Audit registers. If you want to refer to a branch in a secondary level (for example to filter it), compose its name by appending its path along the branches, without any spaces. For example, ContentInstanceRead or OperationConfigVarCreate.

Level 1 Branch	Level 2 Branch	Level 3 Branch	Level 4 Branch
Content	Instance	Create, Modify, Delete, Publish, Unpublish, Read	
	Static File	Create, Modify, Delete, Publish, Unpublish, Read	
	Site	Create, Modify, Delete, Publish, Unpublish	
	Channel	Create, Modify, Delete, Publish, Unpublish	
	Type	Create, Modify, Delete, Publish	
Operation	Search	Simple, Advanced	
	Login	Success, Failure	
	Config	Commit	
		Var	Create, Modify, Delete
	Role	Create	
		Modify	Add Capability, Delete Capability, Add User, Delete User, Add Group, Delete Group
Workflow	Start		
	Complete		

Level 1 Branch	Level 2 Branch	Level 3 Branch	Level 4 Branch
	Terminate		
	Abort		
	Activity	Start, Complete, Terminate, Abort, Accept, Decline	
	*Job	Publish, Unpublish	

Note:

WorkflowJob cannot be filtered except if eventsDisabled=ALL, as it is a system event.

9. Appendix 5 – OTDS Authentication

OpenText WEM Audit supports the authentication using OpenText Directory Services (OTDS). This means that the same OTDS installation is used to authenticate users in WEM and in WEM Audit. The OTDS Administration Client attributes a Resource created previously in OTDS to authenticate WEM Audit users through OTDS.

Tip:

For more information on how to create an OTDS Resource, see Appendix 6 – Configuring a Resource in OTDS.

9.1. Installer - Provide OTDS Properties

When you choose the OTDS authentication, the WEM Audit installer needs to provide two configurations:

- **OTDS Resource ID:** Is the Resource Id of the resource created for the WEM Audit application and in the inactive state. The Resource Id can be verified in the OTDS Administration client.
- **OTDS Rest services base URL:** The URL of the OTDS Web Services must use HTTPS protocol and usually has the form: https://<server>:<port>/otdsws

After this configuration, the installer will test the OTDS connection to the Resource.

9.1.1. Error troubleshooting

If the connection to OTDS fails, one of the following error messages may appear:

Message	Reason
error: myhost	OTDS server unreachable, check network
error: Connection refused: connect	Invalid OTDS URL, check **OTDS Rest services base URL for errors**
`error: sun.net.www.protocol.http.HttpURLConnection cannot be cast to javax.net.ssl.HttpsURLConnection`	**OTDS Rest services base URL** must use SSL (start with https://)
`error: com.opentext.otds.OtdsException: The resource is already activated`	The OTDS resource is already activated, you may need to deactivate the resource by using the OTDS Administration client
`error: com.opentext.otds.OtdsException:` The resource doesn't exist.	**The OTDS Resource ID** provided was not found in the OTDS server provided. Check the Resource ID in the OTDS Administration client

If none of these messages match the error, check the file `install.log` located in the installation directory. After successful connection to OTDS, the installer will automatically activate the OTDS resource and issue the message **"The connection to OTDS has been made successfully."**

9.2. Installer - Provide authorization Roles

After successful connection and activation of the OTDS Resource created for WEM Audit, the installer will require the OTDS Access Role ID's for the two possible authorization roles in WEM Audit: Audit and Administrator. To provide an authorization role, you must use the full name of the OTDS Groups.

> **Important**
>
> The OTDS Group Names are case sensitive.

The provided OTDS Groups must be associated with the configured OTDS Resource. To check the Groups associated with a Resource, you can use the OTDS Administration Client by selecting the resource provided, checking the list of Access Roles, and then checking the Groups associated with those Access Roles. If you want to provide multiple Groups you should separate them with semicolons (ex: "Audit Internal;Audit External")

> **Important**
>
> Only users of the groups belonging to the OTDS Access Roles associated in the configured OTDS Resource will have access to the RTB Insights Console. You can check users and groups associated to the Access Role in the OTDS Administration Client.

10. Appendix 6 - Configuring a Resource in OTDS

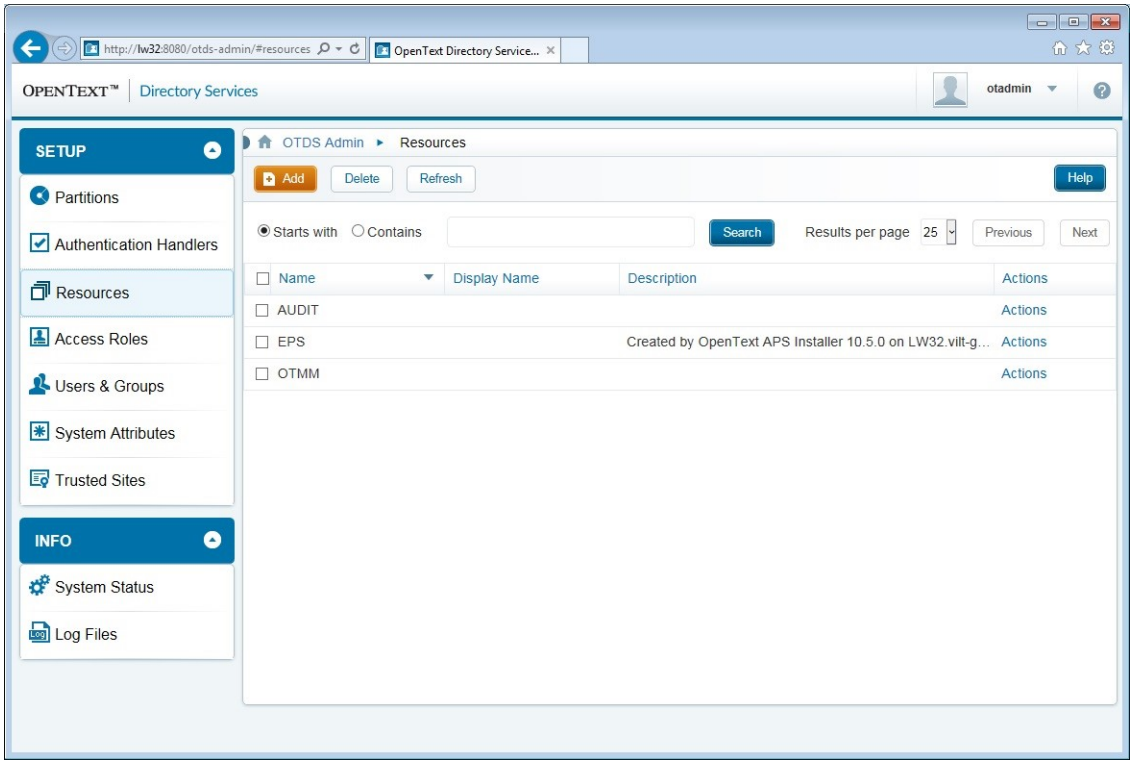
This section provides a quick guide on how to create and configure a Resource in OpenText Directory Services (OTDS) and use it for authentication in WEM Audit. You can configure a Resource in the OpenText Directory Services Administration Console.

10.1. Configuring a Resource using the OTDS Administration Console

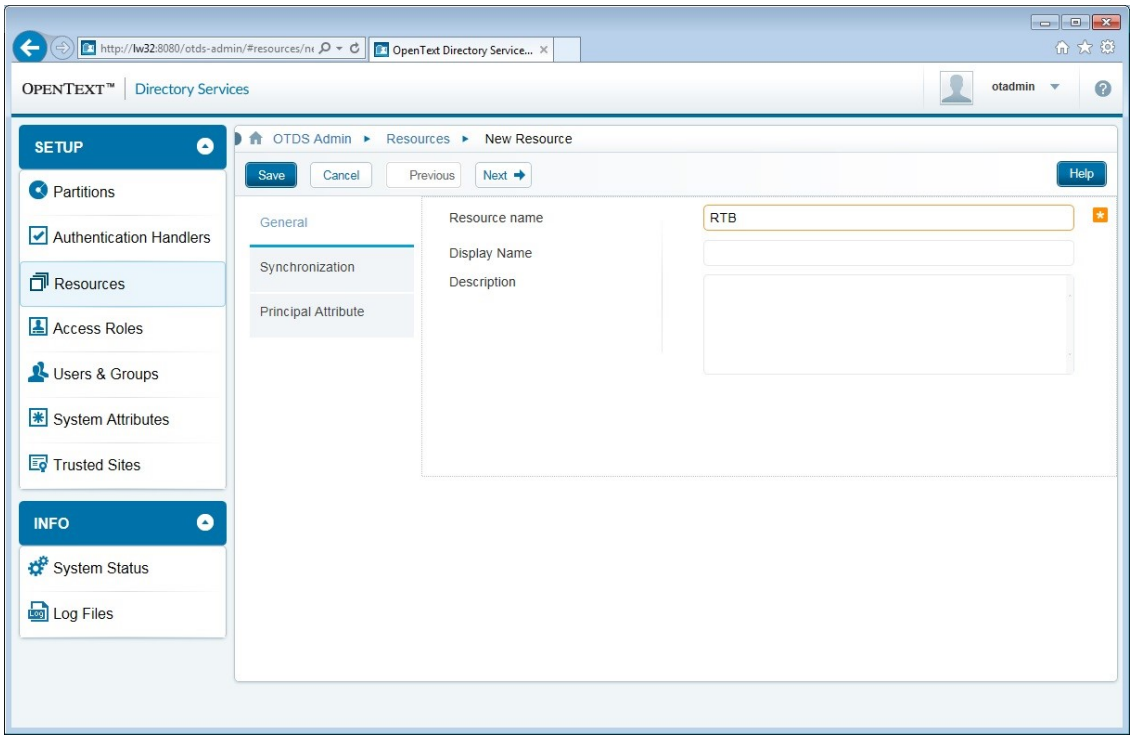
The OpenText Directory Services Administration Console is available at this URL: http://<OTDSServer>:<Port>/otds-admin.

10.1.1. To create the Resource:

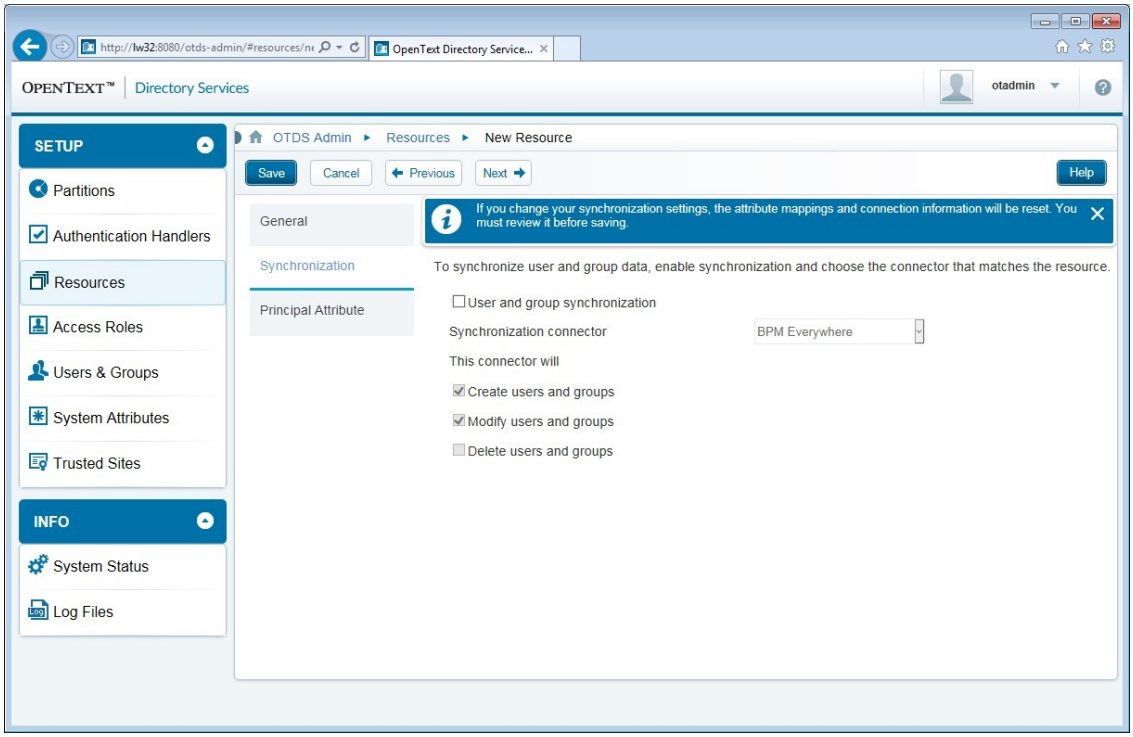
1. Log in to the OTDS Server as the administration user (usually otadmin@otds.admin).
2. Navigate to **Resources** and click **Add**.



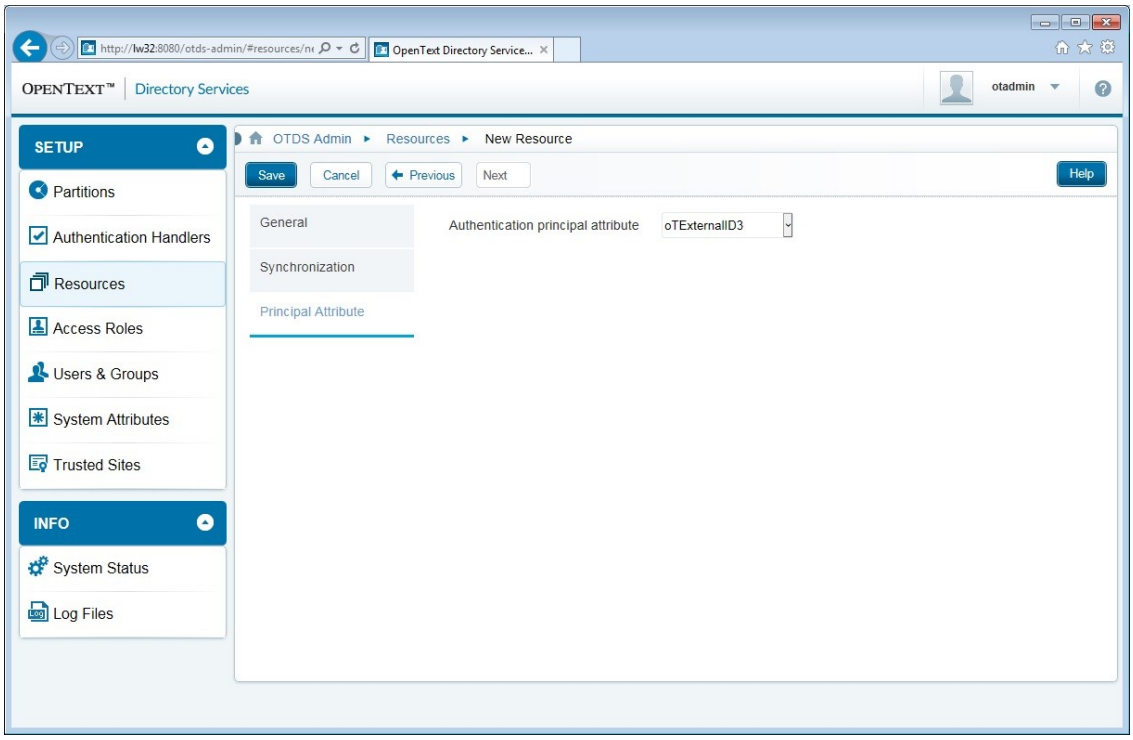
3. In the **General** area, enter a **name** of a Resource, and then click **Next**. The name of your resource can be whatever the name you want. You can optionally add a **Display Name** and a **Description**.



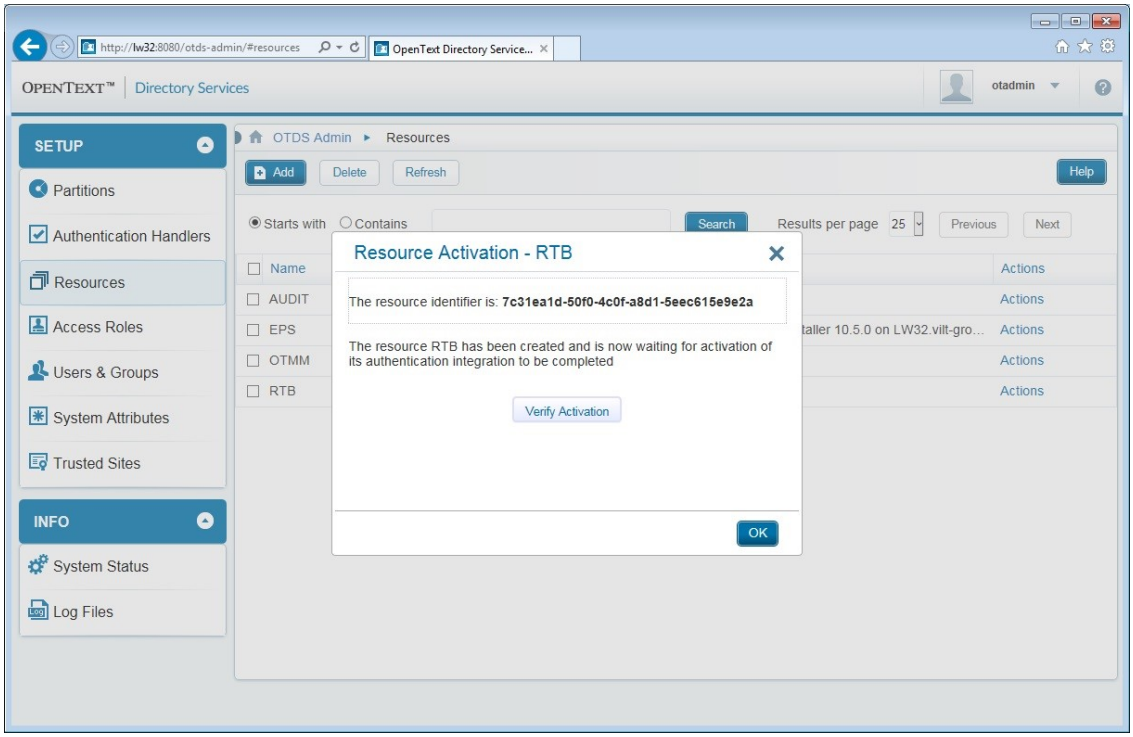
4. In the **Synchronization** area, clear the **User and group synchronization** option, and then click **Next**.



5. In the **Principal Attribute** area, select **oTExternalID3** as your authentication principal attribute. Click **Save** to save your new Resource.



6. In the **Resource Activation** window, click **Verify Activation** to verify that the new Resource is in the inactive state, and then click **Close**.



Note:

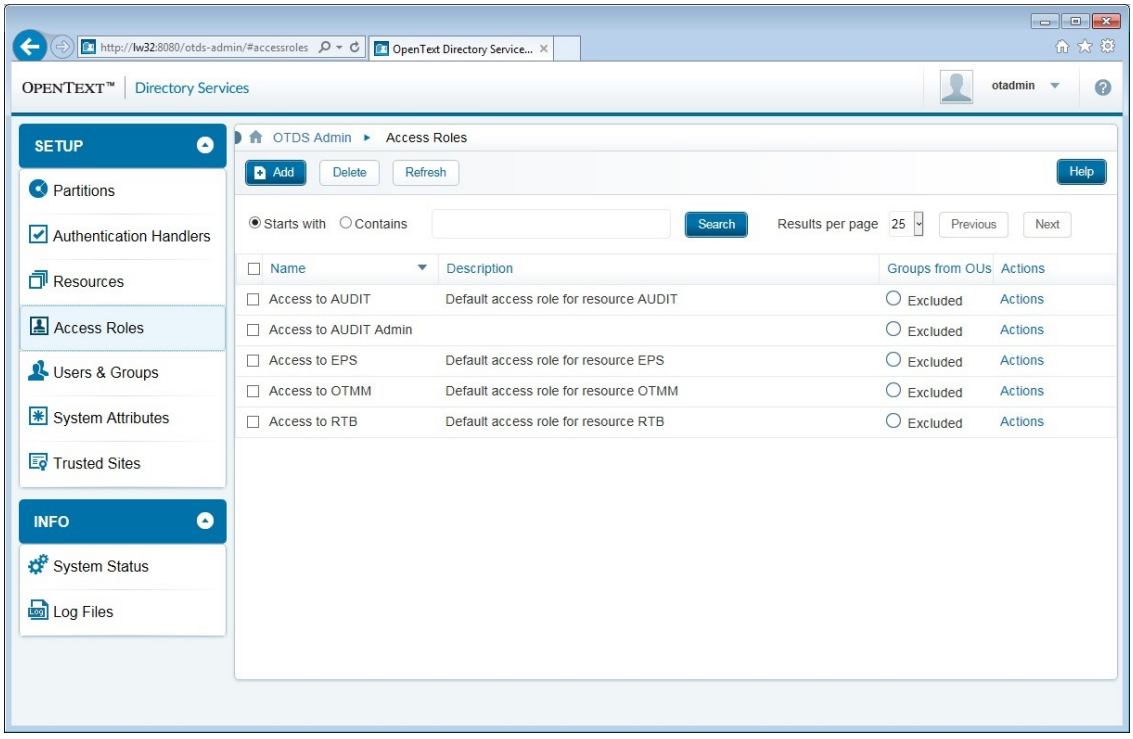
Resources should be inactive before installing WEM Audit. The installation process will activate them. OpenText recommends to store the resource identifier (Resource ID) in a temporary note, because you will need it later in the installation process.

10.1.2. Configuring Access Roles

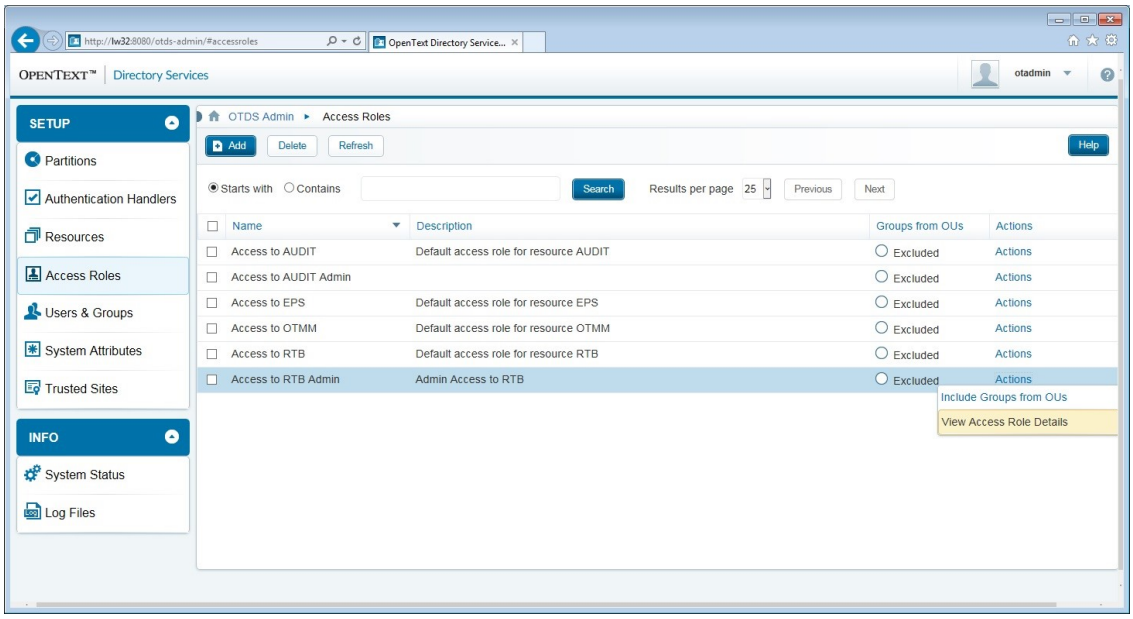
You will need to configure at least one Access Role to associate the Groups and/or Users with the Resource you have created and grant them access to the RTB Insights Console.

To configure Access Roles

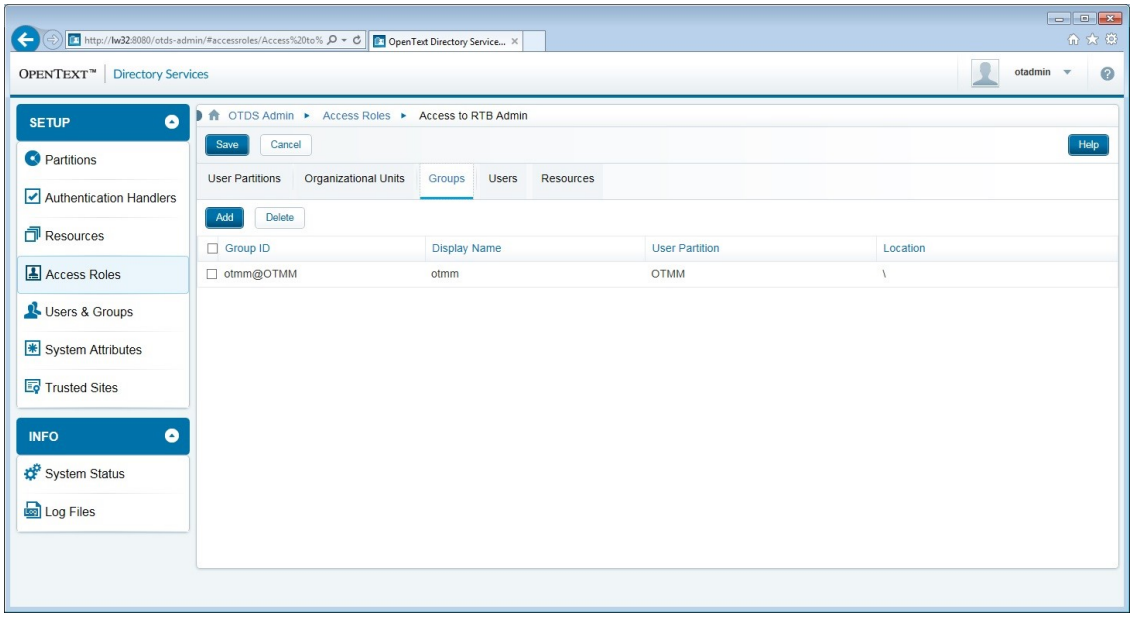
1. Navigate to Access Roles. The Access Role will be created automatically when you create the Resource, with the name **"Access to «ResourceName»"**. You can edit this resource or create a new one. The examples use a resource that was already created.



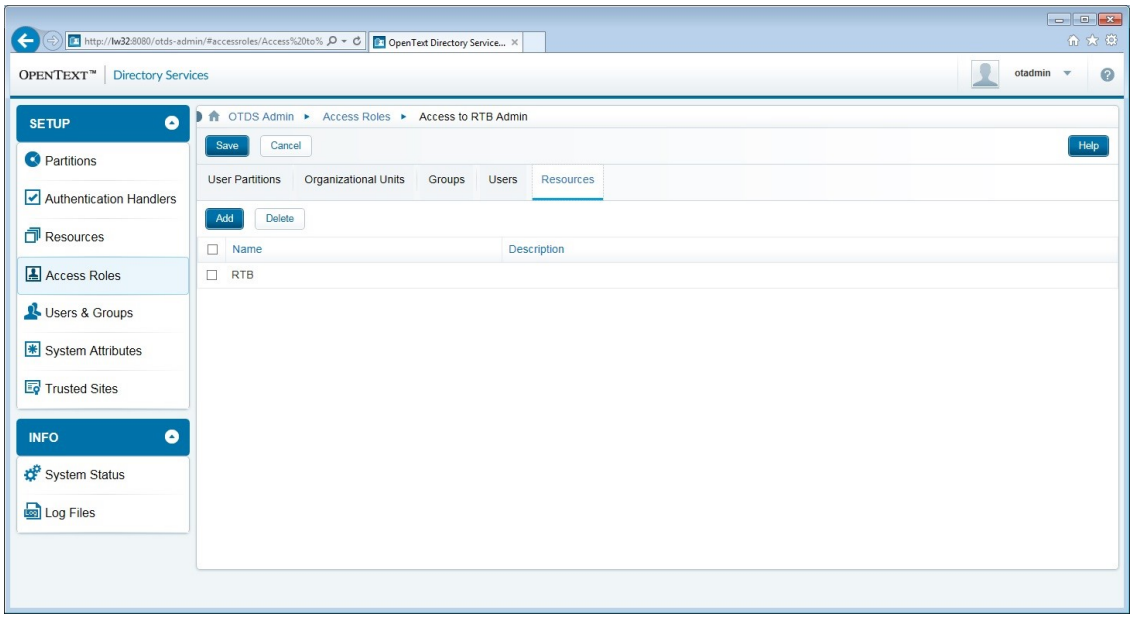
2. Click **View Access Role Details** on the **Actions** menu of Access Role.



3. In the Access Roles Details page, associate User Partitions, Organizational Units, Groups, Users and/or Resources to the Access Role. For WEM Audit purposes, you need to associate Groups and/or Users and the Resource that you created.
4. Navigate to the **Groups** section, click **Add**, and then add groups that you will use for Audit purposes.



5. In the **Add Groups to Access** Role pop-up window, click add **Add to Access Role** to add groups.
6. Click **Ok**. Use **2 different groups**: one for **normal** access to Insights, and another for **administration** access. These 2 groups will be prompted during the WEM Audit installation.
7. Navigate to the Resources section and add the Resource that you created.



8. **Select** the Resource and click **Add to Access Role.**
9. Click **Ok**.
10. Click **Save to** store details of your Access Role.

The Access Role will function as a bound between the Groups and/or Users and the Resource that you created, which will guarantee access to RTB.

Important

The access to RTB Insights console will always depend on the groups that the user belongs to. RTB uses groups to categorize users and uses them as RTB Roles. So, the simplest way to guarantee access to RTB is always adding groups of users that you will provide in the installation process to the Access Role associated with the Resource you will use.

11. Contact Information

VILT Portugal
Rua Ivone Silva, 6 - 7° Esq
1050-124 Lisboa
Portugal
Email: product.support@vilt-group.com
For more information, visit https://www.vilt-group.com