OPENTEXT™

Web Experience Management Audit

Installation and Configuration Guide

Version 10.5.1

OpenText Web Experience Management Audit Installation and Configuration Guide

Rev.: 2015-Apr-24

This documentation has been created for software version 10.5.1.
It is also valid for subsequent software versions as long as no new document version is shipped with the product or is published at https://knowledge.opentext.com.

Open Text SA

40 Avenue Monterey , Luxembourg, Luxembourg L-2163

Tel: 35 2 264566 1

Open Text Corporation

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

Tel: +1-519-888-7111
Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440
Fax: +1-519-888-0677
Support: http://support.opentext.com
For more information, visit https://www.opentext.com

Contents

1 Introduction

This guide provides an overview of Web Experience Management Audit version 10.5.1 installation and configuration. OpenText recommends that you read this Installation and Configuration Guide in conjunction with the documentation included with the software package.

We also recommend that you check the OpenText Knowledge Center (https://knowledge.opentext.com/) for any patches or documentation updates that may have been posted after the initial release of Web Experience Management Audit version 10.5.1.

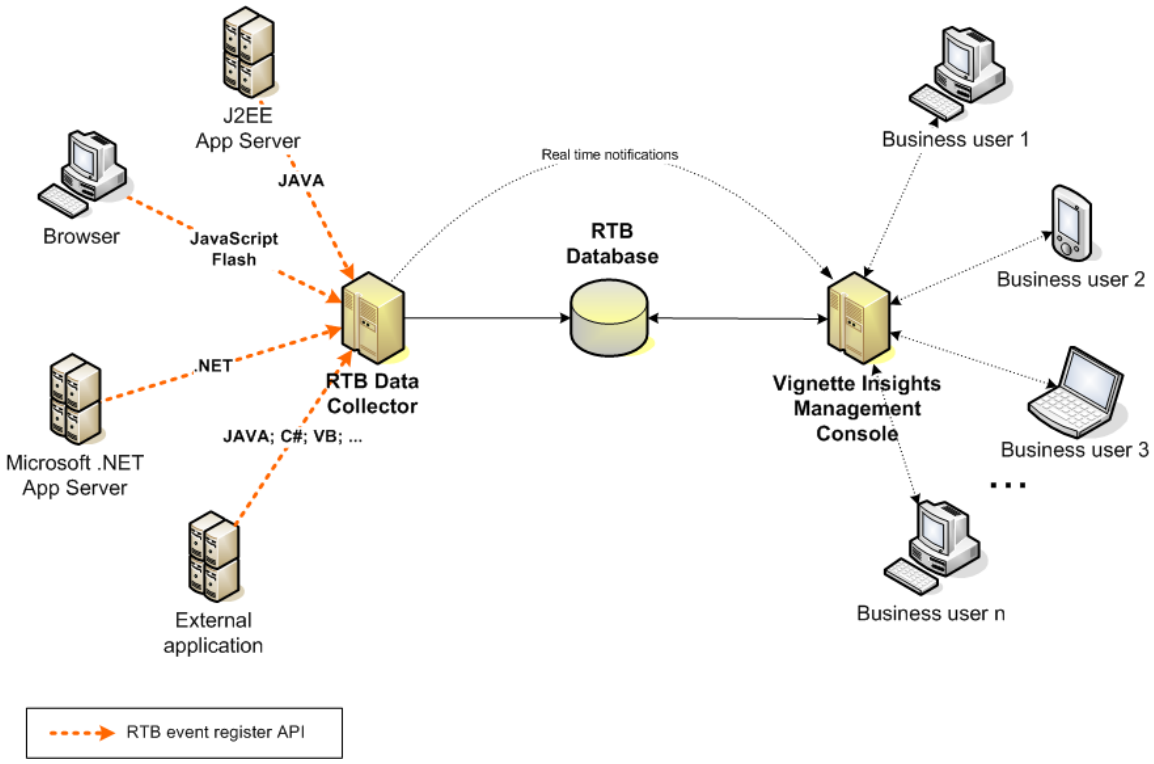
This document is the installation guide for *OpenText Insights*, *Web Experience Management Audit and Web Experience Management Audit Enhanced modules*. OpenText Insights is a real-time reporting console built on top of the flexible and extendable VILT RealTimeBiz (RTB) platform that allows your organization to register content management events connected to specific actions that your organization deems relevant and wants the ability to report on.

1.1 Document Revision History

Topic	Modifications	Revision Number
All	Initial release	10.5.1

1.2 Architecture Overview

The diagram below 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.
- **OpenText Insights Management Console** – the web console where business users access parametric data reports. This component is only available with “WEM Audit Enhanced” license.

The Web Experience Management Audit Module 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, etc., and making them available within the Web Experience Management Console.

These collected events are configured to be stored in a RTB database for a configured amount of time. Once this time is elapsed, the events are automatically removed from the system. This retention schedule feature is currently available only at Web Experience Management Audit Enhanced.

Web Experience Management Audit Enhanced Module is supplied as a separated component. It provides you OpenText Insights, an advanced tool to analyze all the audit information and to help you

to improve your content management and delivery business processes.

1.3 Consulting the Release Notes and Patch Notes

Read the Web Experience Management Audit Release Notes and Patch Notes before you begin the procedures in this guide. The Release Notes and Patch Notes contain installation and configuration notes, and other important information not contained in this guide. See the *Web Experience Management Audit Supported Platforms Matrix Web Experience Management, version 10.5* (available on http://knowledge.opentext.com) for details about supported versions of required software.

1.4 Supported Platform Matrix

OpenText supports platforms only when used in combination as described in the *Web Experience Management Audit Supported Platforms Matrix, version 10.5*. Running Web Experience Management Audit in a configuration not listed in the document is not supported and may result in unpredictable performance.

1.5 Prerequisites

Each section below describes a prerequisite to install R*ealTimeBiz* and *Web Experience Management Audit Module*.

1.5.1 SMTP Server and Email Account

If you want to receive Web Experience Management Audit (RTB) reports or logs via email, you must have an SMTP Server and it must be accessible from the machine where OpenText Insights Management Console will be installed. This option is only available if you have a license for Web Experience Management Audit Enhanced.

Make sure you have your SMTP server available and that you have administrative permissions and the email account to be used by RTB.

1.5.2 Web Experience Audit Distribution (RTB 3.4.25)

You must have a distribution of *RealTimeBiz Web Experience Management Audit 10.5.1*. It contains the files and directories shown below.

File / Directory	Description
antDir/	Installer scripts
bin/	Realtimebiz binaries
config/	Configuration files
doc/	Documentation
installLib/	Installer libraries
install.bat	Windows installer wizard
install.sh	Linux/Unix installer wizard
uninstall.sh	Windows uninstaller wizard
uninstall.sh	Linux/Unix uninstaller wizard

1.5.3 General Configurations

Before proceeding with the *Web Experience Management Audit Module* installation, the following information should be gathered:

If you wish to use LDAP for authentication:

Prerequisite	**X**
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 OpenText Insights)	

If you wish to use OpenText Directory Services (OTDS) for authentication:

Prerequisite	**X**
OTDS URL (host + port)	
OTDS user and password with admin privileges	
OTDS resource ID (previously created)	
Complete name of OTDS groups with Audit privileges (access to OpenText Insights)	

General information:

Host Name or IP where RTB Collector will be installed	
Retention Period desired for events and large attributes (1 year, 5 years, etc)	
Database user and password for RTB tables	

Database user and password for Web Experience Management system tables	
Database URL (host + port + instance)	
List of LDAP Groups that are going to be tracked with RTB	
The host and port of Web Experience Management Connection Server	
User/groups/roles that will have the capability to see the event history at Web Experience Management Console	
Max. number of pages to be exported to excel or CSV (each page has 10 events)	
Workflows that should be audited and the activities inside those workflows	
SMTP Host and port	
RTB account mail and password to this account	

1.5.4 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, you can use the `keytool` command.

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

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

1.5.5 OTDS Resource

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

> **Tip:** For more information on how to create an OTDS Resource, please refer to Appendix 6 – Configuring a Resource in OTDS.

1.5.6 System Requirements

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

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

2 Installation

This contains administrator tasks for installing and configuring RealTimeBiz 3.4.25 platform, Web Experience Management Audit and OpenText Insights

2.1 Installation Process Overview

Web Experience Management 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
- Upgrade to Web Experience Management Audit Enhanced (optional)

Each one of these steps is described in the following sections.

Important

Ensure that you have read previous chapters (prerequisites) before proceeding

2.2 Create RTB Database

You must create a database user in your database system (ex: AUDIT, RTB…) prior to begin Audit installation. Follow the recommended steps for doing that task specific to your database vendor's documentation. The newly created user should have the same privileges/permissions of the Web Experience Management System user (ex: vgncms, vgnsys,..). Permissions like:

- Create databases, stored procedures, indexes
- Stored procedures execution
- Table insert, read write, etc…

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

It is recommended to provide a table space or storage area that can grow as event data is collected because it is difficult to make an upfront estimation of the required database size. The database occupation is proportionally to the number of events being recorded, you may start with a size of 5GB-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/set it in Oracle using the `db_block_size` parameter.

2.3 Complete the Installation Wizard

Before launching the RTB installer, be sure that you are using Java 1.6. Ensure that JAVA_HOME/bin is at system path. You can use *<WEMinstallDir>*/Content/10_5/java dir as your Java installation.

Also, it is necessary to have up and running the following processes:

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

Expand the Web Experience Management Audit distribution file in a directory of your choice (i.e. c:\tmp\WEMAudit) and execute 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 switch the language used by the installer, for example to the Spanish language, you can follow these steps:

1. Edit the install.bat with a text editor.
2. Add this parameter at the end of the install.bat or install.sh file: -l es (only *es* and *en* *are supported at this version*).

If you prefer, you have a silent installation mode that is explained in the Silent Installation point.

2.3.1 Select Installation Option

WEM Audit 10.5.1 Installer gives you the option to perform 3 different things: Install WEM Audit from scratch, Install WEM Audit over OTWSA or Upgrade WEM Audit Cumulative Patch (upgrade from WEM Audit 10.5 to WEM Audit 10.5.1).

```
==========================================
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 OTWSA

3)Upgrade WEM Audit Cumulative Patch

4)Exit
```

2.3.2 Install WEM Audit from Scratch

This section will describe the steps needed to perform in order to install WEM Audit from scratch.

2.3.2.1 Select Installation Type

In this first step you must choose the type of installation 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 every secondary node using installer option 2, and then on the primary node with option 1. More information about installing in an OpenText Content Cluster can be found in Installing Audit in 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:
-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.
```

2.3.2.2 Select Installation Folders

When starting the desired installation, you have the option to select the folders in which you will install the *RTB platform* and *Web Experience Management Audit* product.

The parent folder, of the one that you want to create, must exist. And 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
```

2.3.2.3 Create Directory Structure

```
-----------------------------------------
Installing Directory structure
-----------------------------------------
In the next step the following components will be installed/configured:
-Data Collector properties file.
-Open Text Insights application files.
-RTB loader properties file.
-Open Text Insights 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 Open Text Insights web application ...
-->Open Text Insights web application copied.
Copying collector application ...
-->Collector application copied.
Copying WEM applications ...
-->WEM Applications copied.
Copying Open Text Insights properties...
-->Open Text Insights 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.
```

2.3.2.4 Database Configuration

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

You also need to have in mind the lifetime that your events will have, and the LDAP groups that you will want to monitor.

```
-----------------------------------------
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
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, Auditores

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
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.
```

2.3.2.5 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: 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]
```

```
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.

 ***  WARNING: Before proceed, check that Runtime Services configuration is not
locked in any browser ***



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.
```

2.3.2.6 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.
-Open Text Insights 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]
```

2.3.2.7 Authentication Properties

Configure the authentication provider used for authentication.
Choose your authentication provider between LDAP and OpenText Directory Services (OTDS 10.5)

```
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
```

2.3.2.7.1 OTDS Properties

When selecting OTDS, you will be prompted for the following properties:

- **OTDS Resource ID:** Identifier of the OTDS Resource created for the WEM Audit application, this resource should not be activated (identifier can be obtained in OTDS Administration Client by editing the resource. ex: 6e854917-6e78-4d38-a346-ac9f1625f3b0)
- **OTDS Rest services base URL** The URL of the OTDS Web Services. It must use HTTPS protocol and usually has the form: https://<otdshost>:<otdsport>/otdsws

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

When reinstalling WEM Audit make sure 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 being provided with this configuration the installer will perform a test to check the OTDS connection and 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 please refer to Appendix 5 – OTDS Authentication for troubleshooting.

When the connection succeeds, you are asked to configure the properties that define user privileges in OpenText Insights. These privileges are defined using a mapping between WEM Audit Roles and OTDS Groups. WEM Audit Roles grant users the right to access a resource or to perform certain actions.
By default there are two different roles for OpenText Insights:

- **Audit** users with this role have access to the Audit information at Insights console being allowed to consult reporting information.
- **Administrator users** with this role have *Audit* role access and also access to the Admin tab in OpenText Insights being allowed to perform administration operations.

You will be prompted to provide corresponding OTDS Groups for the Audit and Administrator roles:

- **Role Audit:** Name of the OTDS Group for Audit users. Should be associated in OTDS with the Resource created for WEM Audit through an Access Role.
- **Role Admin:** Name of the OTDS Group for Administrator users. Should be associated in OTDS with the Resource created for WEM Audit through an Access Role

The OTDS Groups are identified by its name. Please remember that the OTDS Group's name is case sensitive. If you want to provide multiple Groups, you should separate them with semi-commas (ex: "Audit Internal;Audit External")

Important

The Groups provided must belong to an Access Role associated with the OTDS Resource configured previously. If you need more details on how to configure the Resource, the Access Roles and the Groups associated with it, please refer to 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 Open Text In
sights 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 Open Text Insights console
 >Default value [Admin Access to Audit]
 >Value: Audit
```

Important

If your role mapping validation fails please refer to Appendix 5 – OTDS Authentication for troubleshooting.

2.3.2.7.2 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 insert 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:


Distinguished name where to begin the user search:
 >Default value [ou=people,ou=VgnLDAPRealm,dc=vgndomain]
 >Value: [ou=people,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 of OpenText Insights management 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 there are 2 different roles in RTB:

- Administrators: Grants access to the **Admin** tab in the OpenText Insights Management Console and all the administration features within.
- Web Experience Management Auditors: Grants access to the **Audit** tab in the OpenText Insights Management Console, in which are displayed all the reports of the application. They also have the capability `xml_viewer`, allowing them to see the XML with the details of the events in the history button of Web Experience Management console.

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

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


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

2.3.2.8 Web Experience Components Installer

```
-----------------------------------------
Installing Web applications configuration
-----------------------------------------
In the next step the following components will be installed/configured:
-Web Experience Management Audit application.
-Web Experience Management Audit Data Collector application.
-Start Parameters.
-Pools and Datasources.
-Open Text Insights application.

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]


Please provide information for the connection to runtime services
(VgnAdminServe
r)
-----------------------------------------
Admin Server Host
 >Default value [localhost]
 >Value:
[localhost]

Admin Port
 >Default value [27001]
 >Value:
[27001]

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 ....
```

```
Installing connection pool ...
-->Connection pool installed.
Setting start parameters ...
-->Start parameters configured.


##To continue the process it is necessary to restart:
 VgnVCMServer (all nodes in the cluster)
Please restart the server(s) manually and do not close this wizard.
Did the server(s) complete the reboot?
 >Default value [no]
 >Value: yes


Installing Web Experience Management Audit application ...
-------------------------------------------------
-------------------------------------------------
-->Web Experience Management Audit application installed.

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

Installing Open Text Insights ...
-------------------------------------------------
-------------------------------------------------
-->Open Text Insights installed.
done.
```

Note: In some cases, you can find an error while installing the connection pool. If you find that error, you need to retry this part of the installation and pay attention in the next connection pool installation message.

If the next message is something like “the connection pool is already installed”, enter to the Web Experience Management Runtime Services console and review in “Services > JDBC > Data Sources”. If there is one data source named auditPool and it is targeted in the cluster, the installation has been done successfully. But if the data source exists and it is not targeted, you should select the auditPool and target it onto all servers in the cluster.

2.3.2.9 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
Open Text Insights 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
```

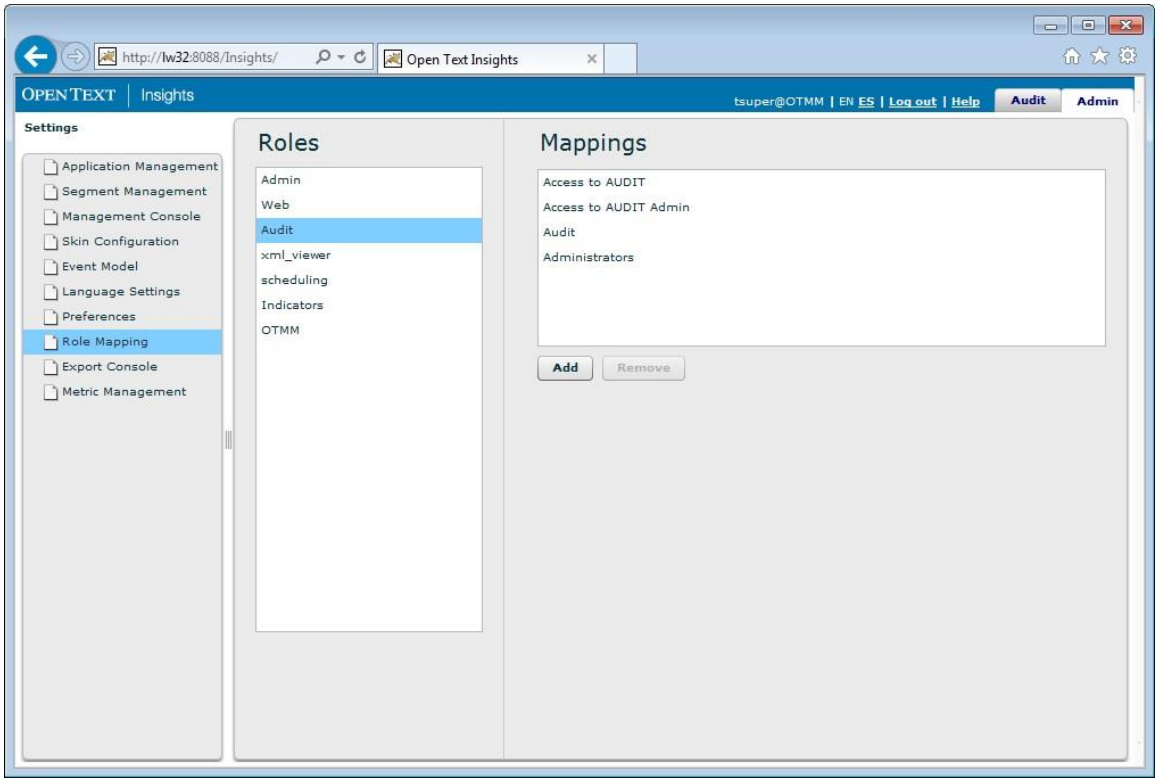
2.3.3 Upgrade WEM Audit Cumulative Patch

If you already have an installation of Web Experience Management Audit 10.5, you can upgrade it to version 10.5.1. This section will describe the steps needed to patch/upgrade WEM Audit 10.5.

2.3.3.1 Before the upgrade

If you're going to upgrade Web Experience Management Audit 10.5 to version 10.5.1, and you are using OpenText Directory Services for authentication, take in consideration the new feature of using OTDS Groups instead of OTDS Access Roles for role mapping in RTB.

Before the upgrade, you must map the OTDS Groups in Insights Admin tab. If you don't do that, you will not have access to Insights after the upgrade, as you don't have the OTDS Groups mapped to the RTB roles.



So, you must follow these steps:

1. Open Insights console, login with a user with administration privileges and navigate to the Admin tab.
2. Navigate to the Role Mapping section and provide OTDS Groups for each one of the roles, accordingly to your needs.

a. **Tip:** We advise you to use 2 different groups: one for normal access and another one for administration purposes. Probably, you're already using 2 Access Roles for that, you just need now to use Groups instead of Access Roles.

3. Perform the upgrade as described in OpenText Web Experience Management Audit 10.5.1 (Installation and Configuration guide).
4. You can delete the Access Roles mapped to the RTB roles after the upgrade.

If you wish to continue using Access Roles in order to map the RTB roles and categorize the users after the upgrade, you can use the option **auth_groups=disabled** in the table **TBRTB_PROPERTIES**. You can use this script to update it:

```
INSERT INTO tbrtb_properties (propkey,propvalue)
VALUES('auth_groups','disabled');
```

2.3.3.2 Select Installation Type

In this first step you must 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 every secondary node using upgrader option 2, and then on the primary node with option 1. More information about installing in an OpenText Content Cluster can be found in Installing Audit in a Web Experience Management Cluster.

```
========================================
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
```

2.3.3.3 Select Installation Folders

When starting the desired upgrade, you have to select the folders in which you installed the *RTB platform* and *Web Experience Management Audit* product, as well as the folder where you have your *Web Experience Management* 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]
 >Value: /opt/audit

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

-----------------------------------------
Installing Directory structure
-----------------------------------------
In the next step the following components will be installed/configured:
-Open Text Insights 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 Open Text Insights web application ...
-->Open Text Insights 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.
```

2.3.3.4 Database Upgrade

You will now need to 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
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.
```

2.3.3.5 Upgrade Web Applications

This step will upgrade the Web Applications related with Web Experience Management Audit. You will need to provide information in order to access the Web Experience Management Runtime Services Console (VgnAdminServer), such as:

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

```
-----------------------------------------
Installing Web applications configuration
-----------------------------------------
In the next step the following components will be installed/configured:
-Web Experience Management Audit application.
-Upgrading Open Text Insights console.
-Upgrading the collector application.

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 provide information for the connection to runtime services
(VgnAdminServer)
-----------------------------------------
Admin Server Host
 >Default value [lw61]
 >Value:
[lw61]
```

```
Admin Port
 >Default value [27001]
 >Value:
[27001]

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 ....

Installing Web Experience Management Audit application ...
-----------------------------------------------
-----------------------------------------------
-->Web Experience Management Audit application installed.

Deploying Open Text Insights ...
-----------------------------------------------
-----------------------------------------------
-->Open Text Insights installed.

Deploying Data Collector ...
-----------------------------------------------
-----------------------------------------------
-->Data Collector installed.
done.
```

2.3.3.6 Update Web Experience Management Configuration

This step will update the configuration of Web Experience Management in order to allow the execution of the Audit components. The installer will need the information to access the VgnVCMServer, such as:

- 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.

 ***  WARNING: Before proceed, check that Runtime Services configuration is not
locked in any browser ***



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
```

2.3.3.7 Upgrade Finish

At this point you have now Web Experience Management Audit upgraded to version 10.5.1. No restarts are necessary.

2.4 Silent installation

This version includes a silent installation mode to make a faster installation. To enable this mode you need to rename *<INSTALL_DIR>*\installation.properties file to *<INSTALL_DIR>*\silent.properties. The file contains the following properties:

```
#################################################################
##                                                             ##
## VCM Audit silent installation properties                    ##
##                                                             ##
## This is the main properties file for the VCM Audit silent installation   ##
##                                                             ##
## You need to populate the properties to perform a silent installation   ##
## of this Audit tool.                                         ##
##                                                             ##
#################################################################

#Installation type (please don't change this property)
installer.type=principal_node

#################################################################
## Common properties                                           ##
#################################################################

#Path where the VCM is installed
common.vcmPath=c:\\OpenText

#Path where the Audit tools will be installed
common.installPath=c:\\OpenText\\Audit

#Company to associate the application to be audited
common.company=VILT

#common.internalHosts=

# Number of days that you want to store the events in the database
common.eventLifeTime=365

# Number of days that you want to store the content instance XML associated to the events
common.xmlLifeTime=30

# Mail to send reports in case of problems
common.mailSendTo=rtb@vilt-group.com

# Host where the collector application is going to be installed
common.collectorHost=localhost

# Port where the collector will be listening for events (not the webapp server port)
common.collectorKRouterPort=26000

# Port where the management will be listening for events (not the webapp server port and different
```

```
to the collectorKRouterPort)
common.managementKRouterPort=26099

# Mail account to send mail from the tool
common.managementAccounts=rtb.support@vilt-group.com

# Folder where the properties will be cached
common.propertiesCacheFile=c:\\OpenText\\AuditSilent\\cache

#################################################################
## Logging properties                                          ##
#################################################################

# Log file to store traces of events generation
logging.rtbClientLogFile=c:\\OpenText\\Audit\\logs\\rtbclient.log

# Log file to store traces of the tool that retrieves and store events generated by the tool
logging.collectorLogFile=c:\\OpenText\\Audit\\logs\\rtbcollector.log

# Size of the collector log file before rotation (without the KB suffix)
logging.collectorLogFileSize=1000

# Log file to store traces of the tool that generates reports from events generated by the tool
logging.managementLogFile=c:\\OpenText\\Audit\\logs\\rtbmanagement.log

# Size of the management log file before rotation (without the KB suffix)
logging.managementLogFileSize=1000

#################################################################
## Audit events database properties (where events will be stored)  ##
#################################################################

# Audit events database software (MSSQL or Oracle)
database.rtbSoftware=MSSQL

# Audit events database host
database.rtbHost=localhost

# Audit events database port
database.rtbPort=1433

# Audit events database name
database.rtbDBName=RTB

# Audit events database user
database.rtbUser=rtb

# Audit events database password
database.rtbPassword=rtb

# Open Text user groups
```

```
database.groups=Administrators

#########################################################################
## VCM database properties (if you have split the database use the System one)  ##
#########################################################################

# VCM system database software (MSSQL or Oracle)
database.vcmSoftware=MSSQL

# VCM system database host
database.vcmHost=localhost

# VCM system database port
database.vcmPort=1433

# VCM system database name
database.vcmDBName=VCMMGMT

# VCM system database user
database.vcmUser=vcmmgmt

# VCM system database password
database.vcmPassword=vcmmgmt

#################################################################
## Role mapping properties (enabling users and/or groups for Insights)     ##
#################################################################

# Enabling the Admin tab for these users and/or groups
rolemapping.admin=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain

# Enabling the Audit tab for these users and/or groups
rolemapping.audit=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain

# Enabling the Web tab for these users and/or groups
rolemapping.web=cn=Administrators,ou=groups,ou=VgnLDAPRealm,dc=vgndomain

#################################################################
## VCM connection properties                                   ##
#################################################################

# VCM host
vcm.host=localhost

# VCM port
vcm.port=27110

# VCM user
vcm.user=vgnadmin

# VCM password
```

```
vcm.password=vignette

# VCM node name
vcm.nodeName=VgnVCMServer

#################################################################
## Runtime Services connection properties                      ##
#################################################################

# Runtime Services host
rtsvcs.host=localhost

# Runtime Services port
rtsvcs.port=27001

# Runtime Services user
rtsvcs.user=vgnadmin

# Runtime Services password
rtsvcs.password=vignette

#################################################################
## LDAP authentication properties                              ##
#################################################################

# LDAP URL
ldap.url=ldap://localhost:27110

# LDAP admin full name
ldap.adminFullName=uid=vgnadmin,ou=people,ou=VgnLDAPRealm,dc=vgndomain

# LDAP admin name
ldap.adminName=vgnadmin

# LDAP admin password
ldap.adminPassword=vignette

# LDAP user search base
ldap.userSearchBase=ou=people,ou=VgnLDAPRealm,dc=vgndomain

# LDAP user resolver
ldap.userResolver=uid

# LDAP user object class
ldap.userObjectClass=inetOrgPerson

# LDAP group search base
ldap.groupSearchBase=ou=groups,ou=VgnLDAPRealm,dc=vgndomain

# LDAP group resolver
ldap.groupResolver=cn
```

```
# LDAP group object class
ldap.groupObjectClass=groupOfUniqueNames

# LDAP group search member
ldap.groupSearchMember=uniqueMember

################################################################
## SMTP configuration properties (for reports sending)        ##
################################################################

# SMTP host
smtp.host=localhost

# SMTP port
smtp.port=25

# SMTP user
smtp.user=test@vilt-group.com

# SMTP password
smtp.password=test
```

You should replace the properties values for those from your environment and run the installation scripts.

For Unix:

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

For Windows:

```
install.bat
```

This is a silent installation so the installer will show the process information in the "<INSTALL_DIR>\install.log" file. If you have any error during the installation process, you will be able to see it there.

The first step will be the properties validation, so if you have any error, it will appear in the log file. The common problem that you could find in this step is a mistake on any connection property (database, LDAP, WEM, Runtime Services).

Note: Ensure that the Runtime Services configuration is not locked, because some steps will need to apply some changes to the configuration using the Runtime Services.

2.5 Configure the Web Experience Management Audit Resource

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

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, don't forget you have to configure the properties in each one of them.

Properties	**Description**	**Default Value**
audit.config.refresh	Web Experience Management Audit properties refresh time in minutes. Avoids restart after configuration changes. The user should wait this interval (at maximum) to see the changes take effect.	5 minutes
eventsDisabled	Events that will not be audited, comma separated. You can specify the names of single events (like ContentSiteDelete) or you can specify a whole branch of events (like ContentSite). Using 'ALL' keyword would disable the auditing of all events for that stage. In order to disable all Auditing, you must configure this parameter as 'ALL' in all stages. In 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, comma separated. Using 'ALL' keyword would disable the auditing of all events.	Commented. Uncomment it and insert the users whose events you don't want to register.

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 which we don't want to register events. Using 'ALL' keyword would disable the auditing of all content types. Use Content Type xml name.	Commented. Uncomment it and insert the content types to be blacklisted.
contentType.allowed	List of content types that are going to be audited (Only if contentType.denied is not set). This property is useful if in a Web Experience Management installation where we are only interested in registering events from few content types. Using 'ALL' keyword would enable the auditing of all content types. Use Content Type xml name.	Commented. Uncomment it and insert the content types to be audited.

This table shows the properties that are only valid for the management stage.

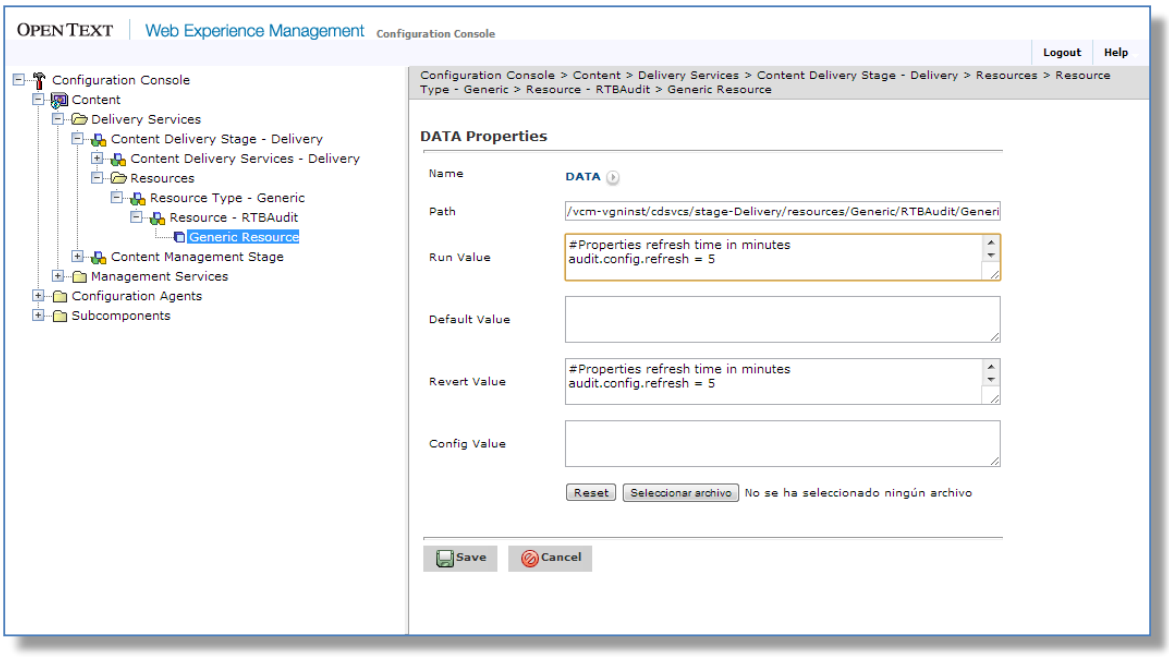
Properties	Description	Default Value
workflows.denied	Comma separated list of workflows that are not going to be audited. Using 'ALL' keyword would disable the auditing of all workflow events	ALL
workflows.allowed	Comma separated list of workflows that are going to be audited	Commented. Uncomment it and insert the workflows to be audited.
task.<name_of_workflow>	Used to specify 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.
job.var	Name of the default publishing workflow. Please, don't' change its value unless you explicitly have modified the default publishing workflows of Web Experience Management	jobId
job.task	Name of the task invoked when starting the publishing workflow. As before, don't change this property unless you explicitly have modified the default publishing workflows of 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 about the full information stored in the instance. Setting this property to a value is useful to register information of all the content instances but the ones listed in this property. Using 'ALL' keyword would disable the auditing of all XML associated with content types. Use Content Type xml name.	Commented. Uncomment it and insert the content types whose xml should not be registered.
contentType.xml.allowed	Content types that allow XML to be registered (only if denied list does not exist). If set, this property has the names of the content types that we need Web Experience Management Audit to register its complete information. Using 'ALL' keyword would enable the auditing of all XML associated with content types. Use Content Type xml name.	Commented. Uncomment it and insert the content types whose xml should be registered.
contentinstance.details.preview	If true, the XML of ContentInstances that have an associated XSLT template for preview at Web Experience Management Console will be transformed when viewing the details of the event at Web Experience Management Audit History Button. If the Content Type do not have a preview template the XML will be displayed. If this property has the value false, the XML will be displayed despite the existence of preview template for that Content Type.	true

These are the properties 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 only have to 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.

2.6 Testing the Environment

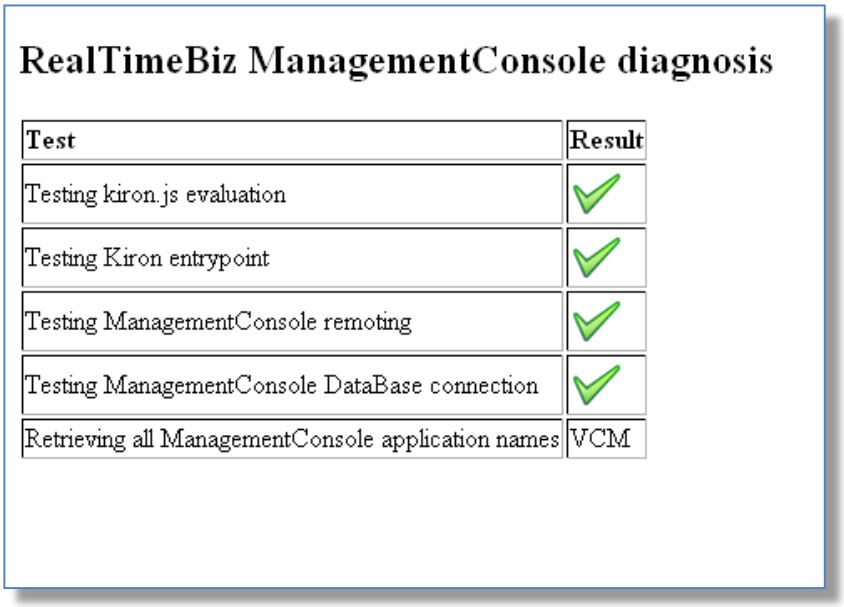
Web Experience Management Audit includes several built-in tests that can be useful to verify that the installation process has been done without errors. Don't forget to restart VgnVCMServer (and secondary servers at cluster) after the installation is finished, before you perform the tests, or its results won't be accurate.

2.6.1 Testing OpenText Insights

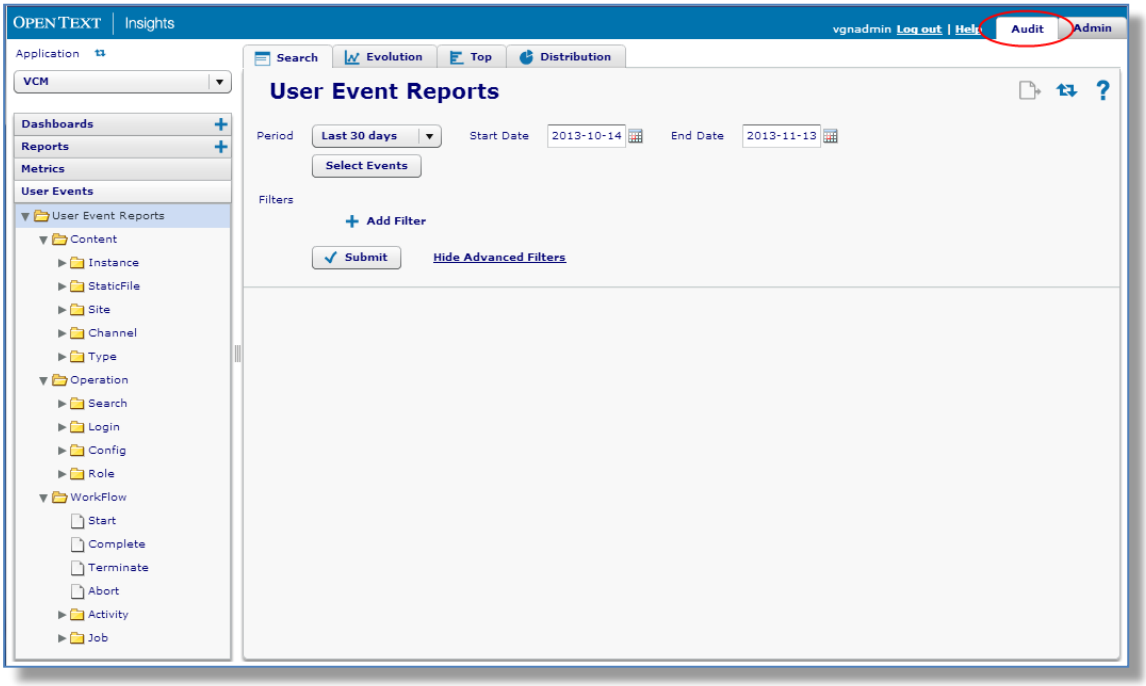
Important

This step only applies if you have purchased Web Experience Management Audit Enhanced and have previously installed it. To install Web Experience Management Audit Enhanced, see the 'Web Experience Management Audit Enhanced Installation' section later in this document.

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



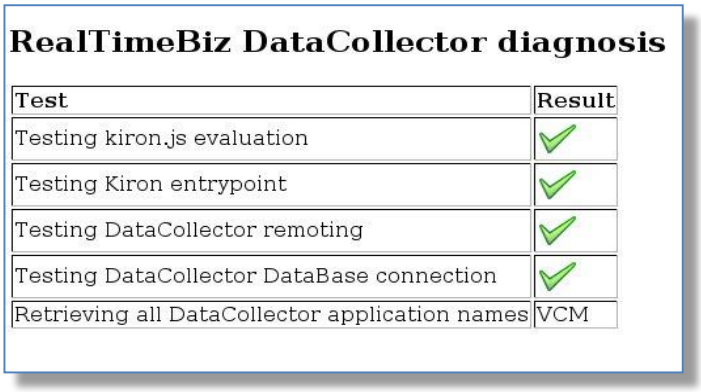
2. If this test has been successful you can open the OpenText Insights management console page (http://host:port/Insights). You should be able to login and see the Web Experience Management Audit Enhanced modules tabs (on the top right corner) according to your user roles:



If you are unable to login, check the section Access Denied to OpenText Insights in Appendix 1 – Troubleshooting.

2.6.2 Testing the Collector Application

1. Open Data Collector diagnosis page (http://<VCM-host>:<port>/collector/diagnosis) to ensure the data collector installation was successful.

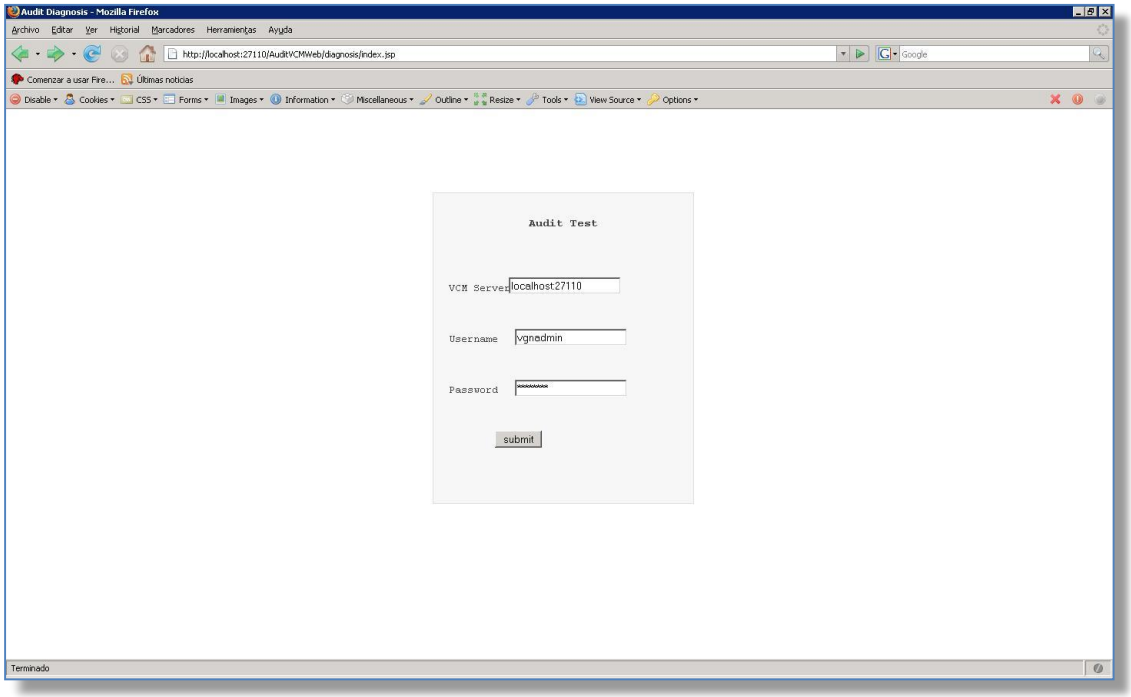


RealTimeBiz DataCollector diagnosis

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

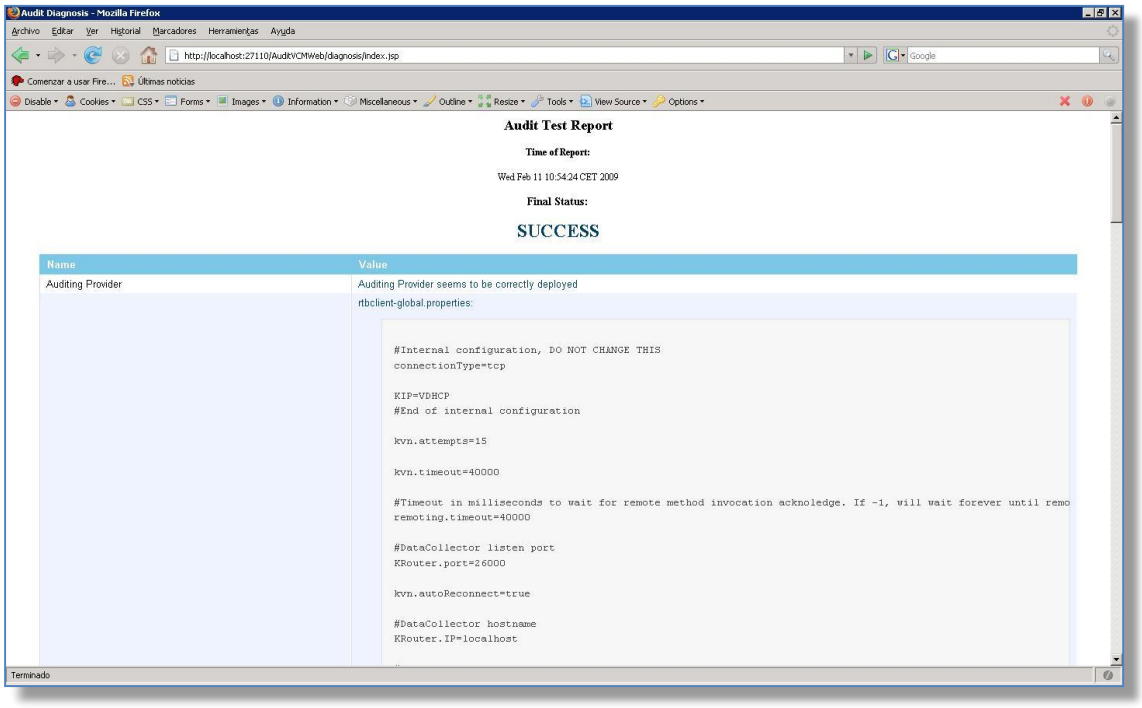
2.6.3 Testing the Audit System

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

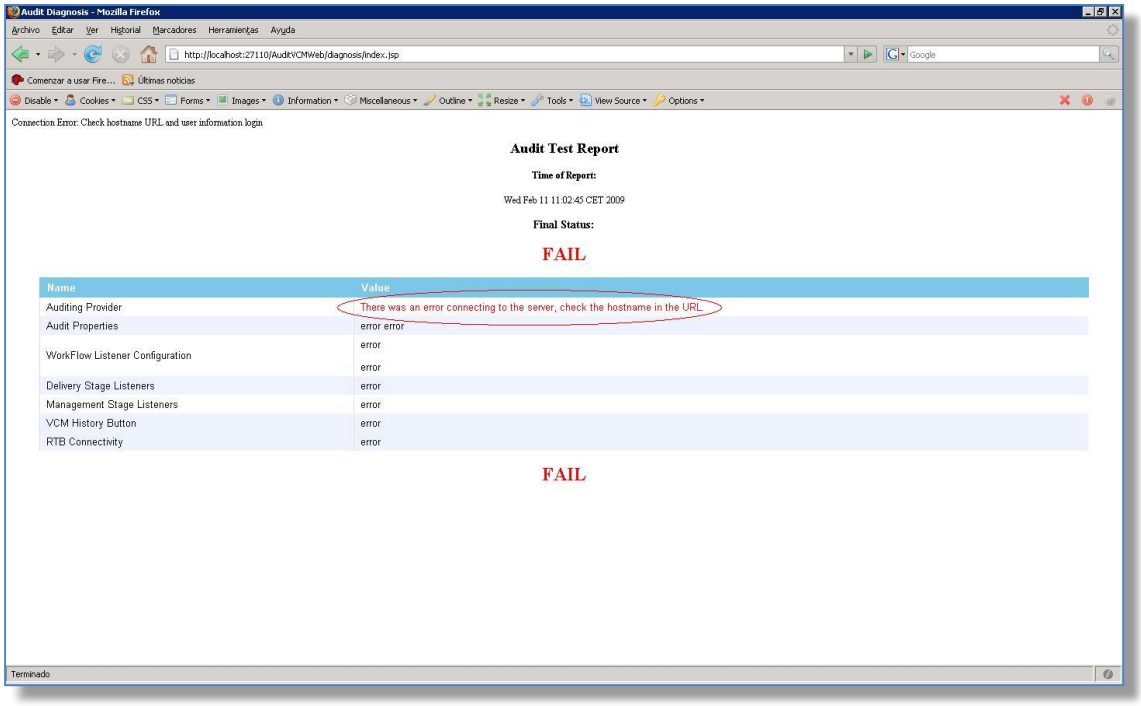


1. Enter the hostname that is used in Web Experience Management, and a user and a password valid for VgnVCMServer. After entering your login information click the ‘Submit’ button to execute the test. When the test completes, the test results will be displayed.

Note: This test will fail if the hostname is not correct, as it must reflect the complete hostname where Web Experience Management Server is listening. If you are having difficulties with this, you can perform the command *netstat -a* and check at which `host:port` Web Experience Management is attached and use it for the diagnosis.



2. If there are misconfigurations, the test will not succeed and a failure message will be displayed listing all the possible errors. If a success message is displayed, Web Experience Management Audit is correctly configured.

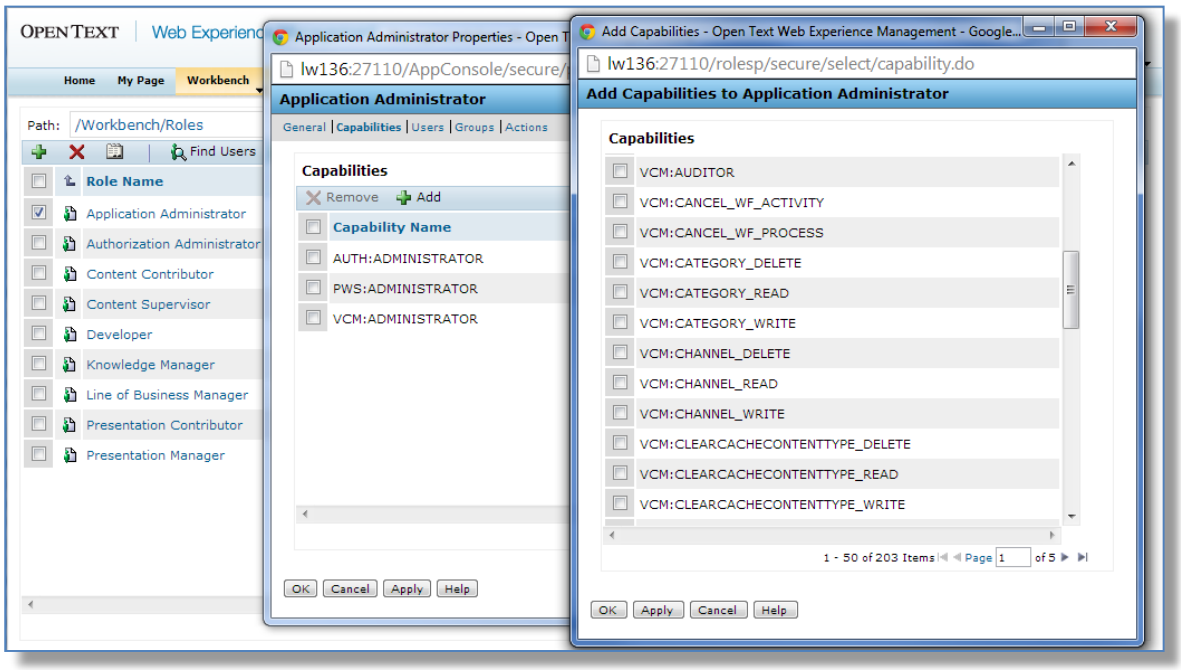


Note: If you experience any errors, see the Troubleshooting section of this guide.

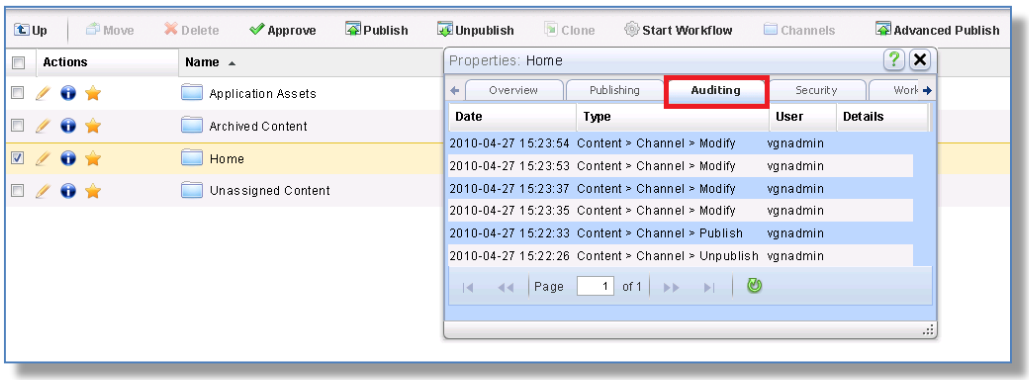
2.7 Update Roles

By default, all the users can see the Audit “Events” button in the Web Experience Management Console and the “Audit” tab in the Content Console, but only the users that have the capability VCM:AUDITOR have the button/tab enabled (please, note that the administrator user (those with VCM:ADMINISTRATOR capability) always has this button enabled). To add this capability to other users, the administrator user of Web Experience Management must modify an existing role to add the capability VCM:AUDITOR, using the next menu option in the management console:

Workbench -> Roles



Now, users that have this capability should see the **Audit** tab in Content Workspaces. The following figure shows an example. Note that apart from having the capability, a user must belong to any of the groups that are authorized to the Web Experience Management object (channel, site, etc.) that the user wants to audit.



2.8 Execute RTB Loader

The utility RTB Loader takes the information stored in the content management system, and loads it in the event database of Web Experience Management Audit. All the Content Instances, Sites, Channels existing in your Web Experience Management Server will generate its creation events, with the respective creation date.

It also accepts filters, and registers events related to the configconsole.
The steps required to execute RTBLoader are:

- You will find RTBloader in `<AuditInstallDir>\rtbLoader` (i.e.: `C:\apps\wem audit\rtbLoader`)
- The configuration will be read from the existing Audit's configuration files.
- Launch script load.bat (or load.sh) from `<AuditInstallDir>\rtbLoader`.
- Before starting the process, it will ask the password of the administrator user in Web Experience Management

Although the script is configured to fit 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 a properties files that contains the following attributes (please note that the installation wizard generates a file with the following parameters adapted to your particular installation, except the password of the principal in LDAP):
	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=company,dc=es

-otdsFile <otds.properties>	Path to a properties file that contains the following attributes:
	#OTDS Configuration
	#OTDS REST Services URL
	otdsBaseURL=https://localhost:8443/otdsws
	#OTDS Resource ID
	otdsResourceId=5261f244-71ed-4fe6-8d8f-b581b7976839
	#OTDS Secret Key
	otdsSecretKey=MwNod7vCBMxSgOAJbrfG0g==

-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>	Max 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 really large number of content instances, it is recommended to use the parameter '-g outputfileScript'. This is very useful to split the load in several steps (one step to load channels, a step for every content type, etc.).
- If there are custom components in the installation (content types with a java class override), it is important to modify the script load.bat (or load.sh) to add in its classpath the libraries where these classes reside. If you don't do it, the loader won't be able to successfully load them.

2.9 Upgrade to Web Experience Management Audit Enhanced

You can skip this paragraph if you are not upgrading to Web Experience Management Audit Enhanced. Note that Web Experience Management Audit Enhanced is purchased separately.
If you are installing Web Experience Management Audit Enhanced from scratch, and not updating an existing Web Experience Management Audit installation, please follow the steps beginning at the chapter "Launch Installation Wizard".

If you want to upgrade a preexisting Web Experience Management Audit, perform the following steps:

- Extract the file `bin/rtbserver/management.war` from the Web Experience Management Content Audit Enhanced distribution file (i.e. VCM Audit Enhanced.zip) to `<AuditInstallDir>\webapps`
- Deploy management.war using the runtime services console (`http://<VCMhostname>:port/console`): Left panel -> Deployments -> Install (Right Panel).
- Test the installation conform to the instructions in the chapter; “Testing the Environment”

2.10 Installation on a Web Experience Management Cluster

If you are going to install Web Experience Management 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 installations on every Secondary node, and only then proceed to the Primary node.

2.10.1 Installation on Secondary Nodes

When the installer is launched, it will require you to choose the type of installation. Choose the option 2, Installation in a secondary node of a Web Experience Management Cluster. Once the installation is finished for every secondary node, you must proceed with the installation on the Primary node.

2.10.2 Installation on Primary Node

When the installer prompts for the installation type, choose the option 1, Installation on a Primary node of a Web Experience Management cluster.

Then, the steps in Chapter 2 - Installation, must be followed.

3 Upgrading to Web Experience Management Audit 10.5.1 from WEM Audit 7.6

Information to assist you with upgrading from Audit 7.6 to Audit 10.5.1.

3.1 How to Upgrade

If you already have a working copy of Vignette Content Audit 7.6 and you have upgraded from Vignette Content 7.6 or Vignette Content 8.0 or 8.0.1 or Web Experience Management 8.1 or 8.5 to Web Experience Management 10.5, you must upgrade to Web Experience Management Audit 10.5.1.

To do so, proceed with the following steps:

- Make a backup of your Vignette Content Audit Database, following the instructions from your provider.
- Launch the uninstaller for your current Vignette Content Audit 7.6, 8.0, 8.1 or 8.5. Follow the instructions in Uninstalling Web Experience Management Audit.
- Launch the SQL script located under `config/dataModel/<DB_VENDOR>/migration/from_7_6.sql`
- Launch the Web Experience Management Audit 10.5.1 installer, following Installation. As the database already exists, the installer won't touch it and the application will be upgraded without you losing any data.

4 Uninstalling Web Experience Management Audit

Information to assist you with uninstalling Web Experience Management Audit.

4.1 Launch Uninstall Wizard

Under the root of Web Experience Management Audit folder, the installer creates a folder named uninstaller. This folder contains the uninstaller scripts:

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

Before launching the uninstaller be sure that you are using java 1.6, and JAVA_HOME/bin is at system path. You can use *<WEMinstallDir>/*`Content/10_5/java dir` as your Java installation. To launch the script execute 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 Web Experience Management Audit in Delivery Stages in remote machines, you must run the uninstaller in each one of them.

```
==========================================
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.
-Open Text Insights application.
-Pools and Datasources.

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

```
Please provide information for the connection to runtime services
(VgnAdminServer)
---------------------------------------
Admin Server Host
 >Default value [rtbtests]
 >Value:
[rtbtests]

Admin Port
 >Default value [27001]
 >Value:
[27001]

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 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 Open Text Insights ...
-----------------------------------------------
-----------------------------------------------
-->Uninstall Open Text Insights 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

 ***  WARNING: Before proceed, check that Runtime Services configuration is not
locked in any browser ***

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
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 ....


##To continue the process it is necessary stop:  VgnVCMServer, VgnAdminServer
and all Deployments and Configuration Agents (Some Web Experience
Management Audit libraries are going to be removed now; these libraries may
be used in other process actually.) . Please stop the server(s) manually and do
not close this wizard.
Did the server(s) complete the stop?
 >Default value [no]
 >Value: yes

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 Web Experience Management Audit you will need to complete the following manual steps.

- Remove the Web Experience Management Audit folder

Delete the information stored in the Web Experience Management Audit database. After performing this step you will lose all the historic information. Don’t do it if you plan to upgrade to another version keeping 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 uninstaller wizard must be launched at each node.

You must start launching it in the primary node of the cluster (VgnVCMServer), following the steps from Section 4.1, Launching the Uninstall Wizard.

Once that wizard has finished, you can proceed with uninstalling it in the secondary nodes.

5 Appendix 1 – Troubleshooting

The setup process generates a running installation of Web Experience Management Audit; in case of problems, the following sections describe how to manually install or uninstall some of the components of Web Experience Management Audit. This can be helpful if some of the tests included in Audit fail or the installer failed to perform some specific action.

Please note that all the following steps are usually executed by the setup process, not needing any kind of intervention by the user. The steps are shown here just to document how to perform them manually in case of exceptional scenarios.

5.1 Launch Installation Wizard

Before launching the Web Experience Management Audit installer, be sure that you are using Java 1.6. Ensure that JAVA_HOME/bin is at system path. You can use `<WEMinstallDir>/Content/10_5/java dir` as your Java installation.

Also, it is necessary to have the following processes up and running:

- VgnVCMServer
- VgnAdminServer
- Config Agents

5.2 Adding libraries and Classpath manually

5.2.1 Libraries installation in Web Experience Management

To install libraries in Web Experience Management you must copy the following files to the lib directory of OpenText (<WEMinstallDir>/Content/10_5/lib):

- kiron.jar
- json.jar
- rtbclient.jar
- rtbcommon.jar
- AuditVCMLib.jar
- aspectjrt.jar
- aspectjweaver.jar
- backport-util-concurrent.jar

5.2.2 Classpath and Arguments

Web Experience Management Servers must be instructed to use both the libraries and the properties files included with Web Experience Management Audit. Both the Web Experience Management Server and the AppSvcs deployment agents must be configured as follows:

Using the runtime services console, there are two parameters that must be changed:

Classpath: The following libraries must be added at the end of the classpath:

```
<WEMinstallDir>/Content/10_5/lib/kiron.jar
<WEMinstallDir>/Content/10_5/lib/rtbcommon.jar
<WEMinstallDir>/Content/10_5/lib/rtbclient.jar
```

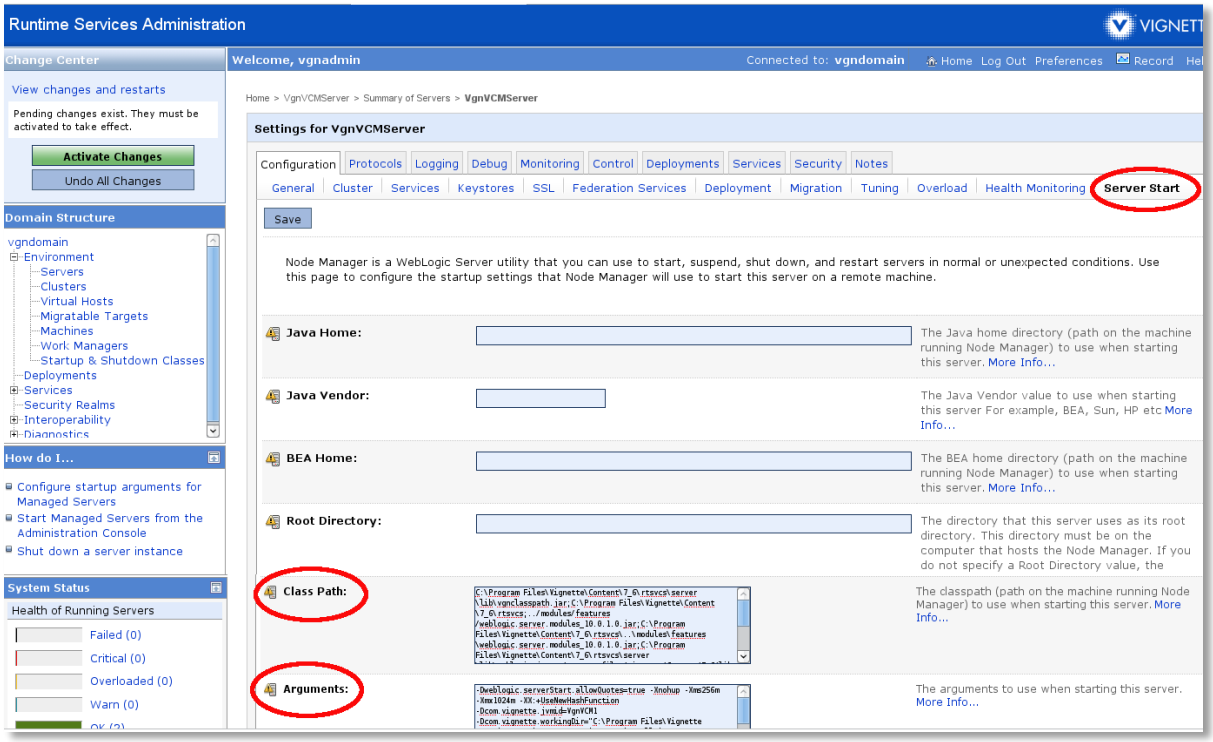
```
<WEMinstallDir>/Content/10_5/lib/log4j.jar
<WEMinstallDir>/Content/10_5/lib/json.jar
<WEMinstallDir>/Content/10_5/lib/aspectjrt.jar
```

Arguments: The following variables must be added at the end of this parameter.

```
-DRTBCLIENT-PROPERTIES=<AuditInstallDir>/rtbclient
-DCOLLECTOR-PROPERTIES=<AuditInstallDir>/webapps/collector
-DMANAGEMENT-PROPERTIES=<AuditInstallDir>/webapps/management
-javaagent:<WEMinstallDir>/Content/10_5/lib/aspectjweaver.jar
```

NOTE: The directory *<AuditInstallDir>* must refer to the **exact path** where the files are installed.

The following figure shows where to do it:



5.3 Installation of WF Listener

There is a variable in the Configuration Console that needs to be configured to monitor workflows. In the Configuration Console navigate to the path:

Content->
Management Services->
Management Server

And set:

WF_EVENT_LISTENER_CLASS_NAMES=com.vilt.audit.wf.event.RTBWfEventAudit

Note: This class replaces the default value. Do not append it to the default one.

5.4 Deployment of AuditVCMApp

The AuditVCMApp application contains the following utilities:

- Audit diagnosis
- Audit Task for the workflows, a task that allows monitoring of any workflow. For details on how to use it, check Appendix 3.

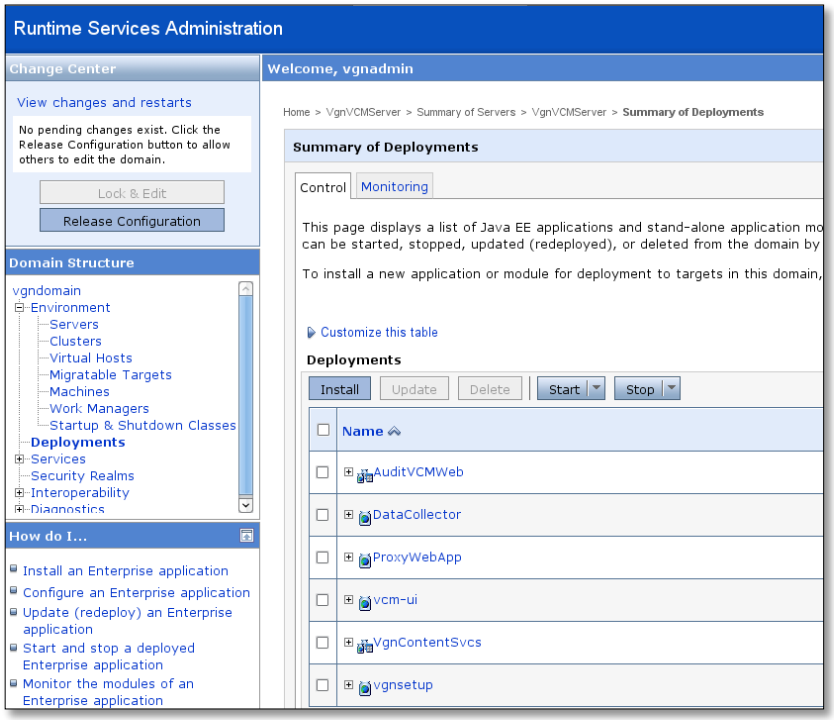
The application `AuditVCMWeb.ear` must be configured as any other OpenText extension. The EAR file must be edited, so the libraries `thirdparty-combined.jar` and `vgn-appsvcs-cma.jar` are copied inside its folder APP-INF/lib. Besides, the file `AuditVCMLib.war` included in `AuditVCMWeb.ear` must be also edited, so the library `vgnconfigapp.jar` is copied inside its folder WEB-INF/lib. Please use the libraries `thirdparty-combined.jar`, `vgn-appsvcs-cma.jar` and `vgnconfigapp.jar` located in your Web Experience Management installation.

Only after this file is updated with these libraries, it must be deployed in Weblogic.

To deploy this application, is necessary to copy the file `AuditVCMApp.ear` to a directory of the machine, for example:

*/<AuditInstallDir>/*webapps/

Then the application can be deployed in Runtime Services, using his console: Deployments → Install



5.5 Configuration of Web Experience Management Console “Events” Button, “Events” Tab and “Audit” Tab in the Content Console

This section explains how to configure the Web Experience Management console **Events History** button.

This web application shows the history of events when a Web Experience Management element is selected (Site, Channel, ContentType, Content Instance, Rol...).

The steps needed to install this application are:

- Add the configuration of the button.
- Add the configuration of the **Events** tab.
- Add the configuration of the **Audit** tab (in the Content Console).
- Set the visualization rights for the buttons.

5.5.1 Add the Configuration of the Button

The button that shows the history of events must be properly configured in the Configuration Console. Navigate to:

Content >
Management Services >
Management Console >
Service Provider Framework >
Type Specification Registry >
Customer Extensions Type Specification Registry >

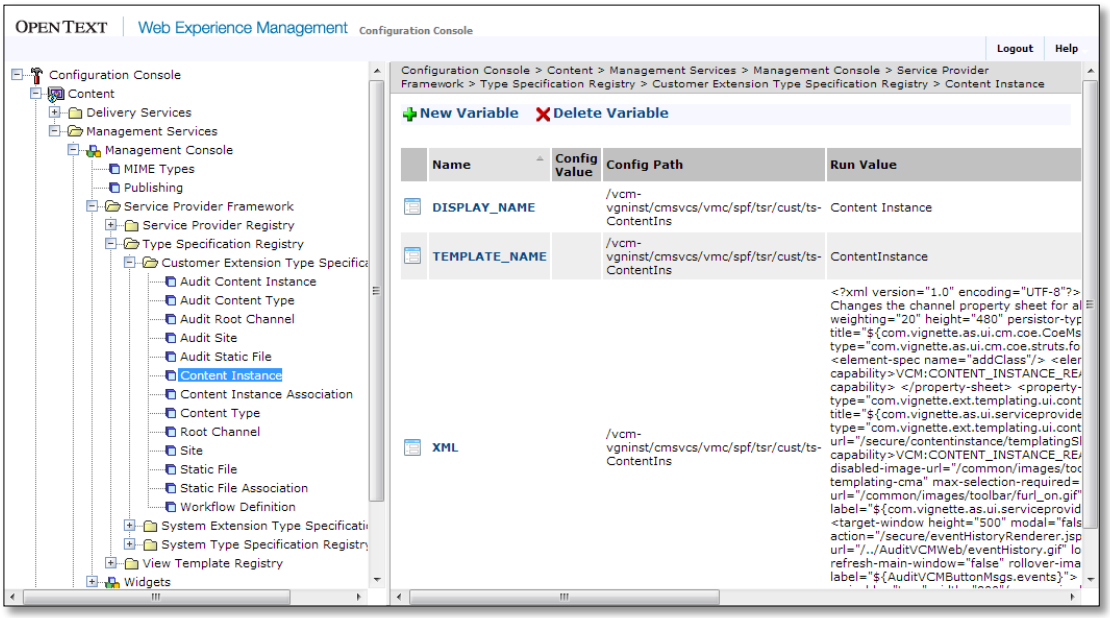
In this location, the next type specifications will be created or modified:

Display Name	Template Name	XML
Content Instance	ContentInstance	config_button_history.xml
Static File	Static File	config_button_history.xml
Root Channel	RootChannel	config_button_history.xml
Site	Site	config_button_history.xml
Content Type	ContentType	config_button_history.xml
Content Instance Association	ContentInstanceAssociation	cia_config_button_history.xml
Static File Association	StaticFileAssociation	cia_config_button_history.xml

The XML field is created by the following procedure:

If the node previously exists in the folder **Customer Extensions** or **System Extension**, it must be modified, adding the content of the file `config_button_history.xml` of `cia_config_button_history.xml` at the end, just before the tag `</service-provider-asset-type-specification>`

If the node did not exist in any of those folders, the initial tag will be taken from any other item, and the content of the file `config_button_history.xml` of `cia_config_button_history.xml` will be added inside.



To add the button for watching the history of the roles, the following node must be modified:

Content >
Management Services >
Management Console >
Service Provider Framework >
View Template Registry>
Customer Extensions View Template Registry>

In this location, a new node will be added with the following characteristics:

Display Name	Template Name	XML
Roles	ROLES_TOOLBAR_TEMPLATE	roles_config_button_history.xml

5.5.2 Add the Configuration of the Events Tab

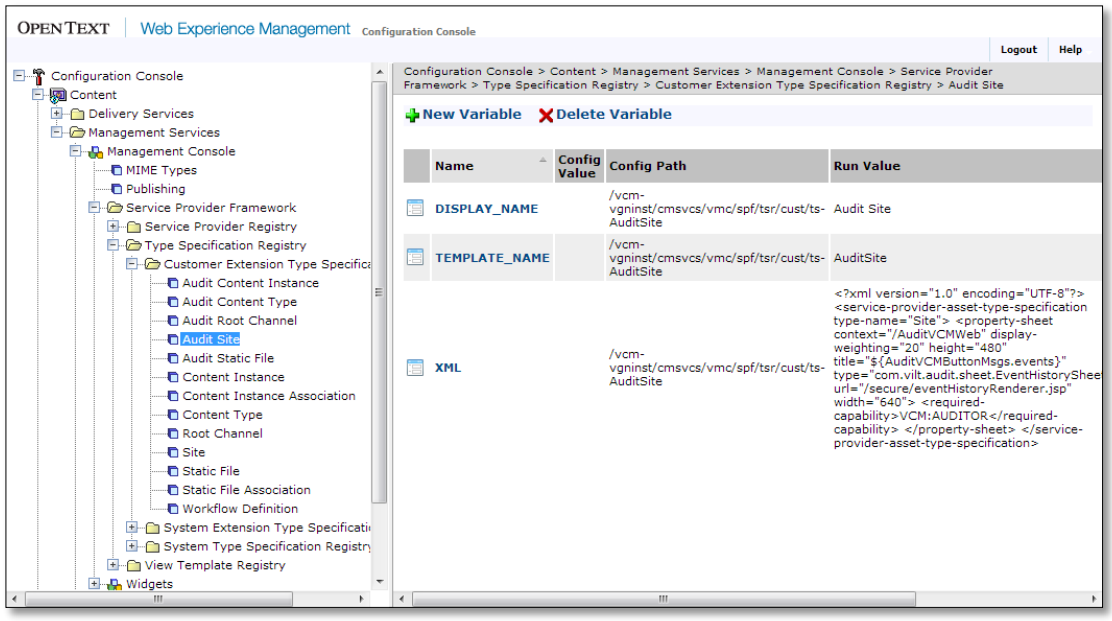
The tab that shows the history of events must be properly configured in the Configuration Console. Navigate to:

Content >
Management Services >
Management Console >
Service Provider Framework >
Type Specification Registry >
Customer Extensions Type Specification Registry >

In this location, you should see the next type specifications:

Display Name	Template Name
Audit Content Instance	AuditContentInstance
Audit Static File	AuditStaticFile
Audit Root Channel	AuditRootChannel
Audit Site	AuditSite
Audit Content Type	AuditContentType

If nodes don't exist you should run a `vgnimport` to import the "InstallPropertySheet.zip" file that you can find in the Web Experience Management Audit distribution file in the `config/sheet` folder. This import will generate the nodes shown before.



5.5.3 Add the Configuration of the Audit Tab (on Content Console)

The **Audit** tab shows the history of events in the Content Console.

In order to install it, manually, you should deploy `xr_vilt_cc_audit.jar` library that you can found in the Web Experience Management Audit distribution file. To do that, you should perform a `configp`.

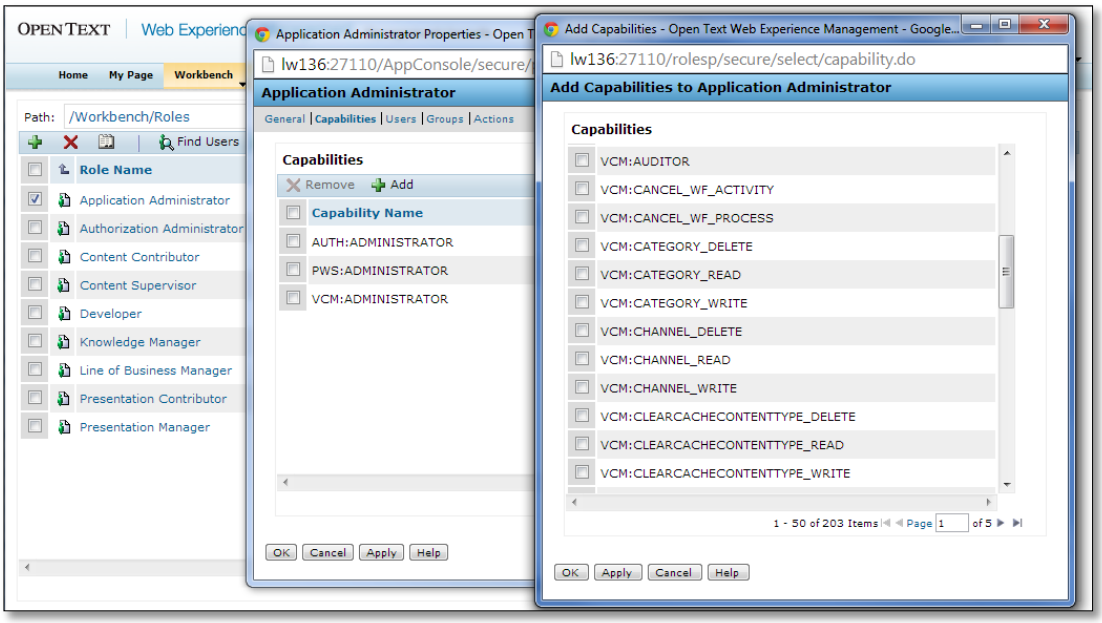
5.5.4 Visualization Permissions for the Buttons

A new capability must be added in Web Experience Management. The following SQL statement could be used to update the database table of Web Experience Management system schema:

INSERT INTO VGNCAPABILITIES VALUES ('VCM','AUDITOR');

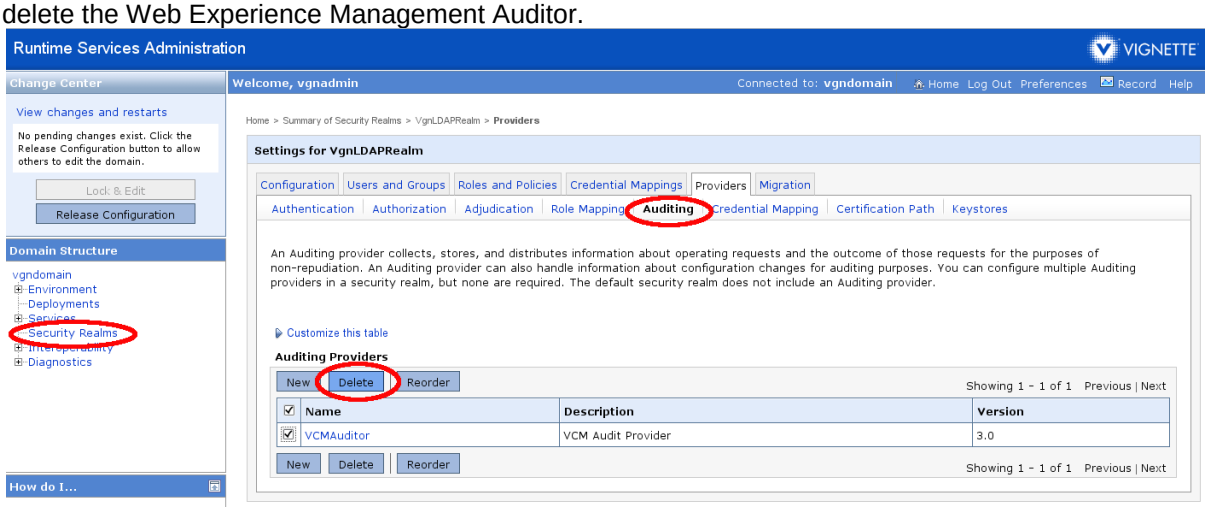
Once the capability has been added, the next step is to modify any existing role to add the capability VCM:AUDITOR, using the next node in the management console:

Workbench -> Roles



5.6 Removing Weblogic Auditor

This is not used since this version, so if you have it installed, you should uninstall it. In the Runtime Services Console, just click in Security Realms in the Left Menu, then click in Auditing, and select and delete the Web Experience Management Auditor.



5.7 Access Denied to OpenText Insights

If you try to access OpenText Insights (included with Web Experience Management Audit Enhanced) 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 your group is not in the rolemapper section of `<AuditInstallDir>\webapps\management.properties`. Make sure the LDAP groups and users are correctly spelled, including upper and lower case.
- **'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 stop and redeploy the management web application from the Runtime Services Console. Go to Deployments (left panel), select management application from the list (right panel), stop it, update it and start it.

5.8 Restarting the DataCollector in Runtime Services

If you need to restart the DataCollector, you must perform the action 'update' instead of stopping and starting, otherwise the classes won't be reloaded and DataCollector will not work.

If the application is running and you perform an 'update', the application is redeployed and reloaded. If it is stopped, you need to 'update' it and then 'start' it.

5.9 Using TAS

OpenText's Trusted Authentication Server, TAS, is supported by OpenText Insights, so you can use this tool through it. It is however supported in Web Experience Management Audit, so the event history can be viewed through a preview application server using TAS.

If you want to use TAS with Web Experience Management Audit and OpenText Insights, proceed as follows:

- 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 an `AuditVCMWeb.war` and an `Insights.war` following TAS instructions on how to create a proxy web application, available in the chapter Deploying Extensions for TAS in the *Dynamic Portal and Dynamic Site Configuration Guide 10.5*.

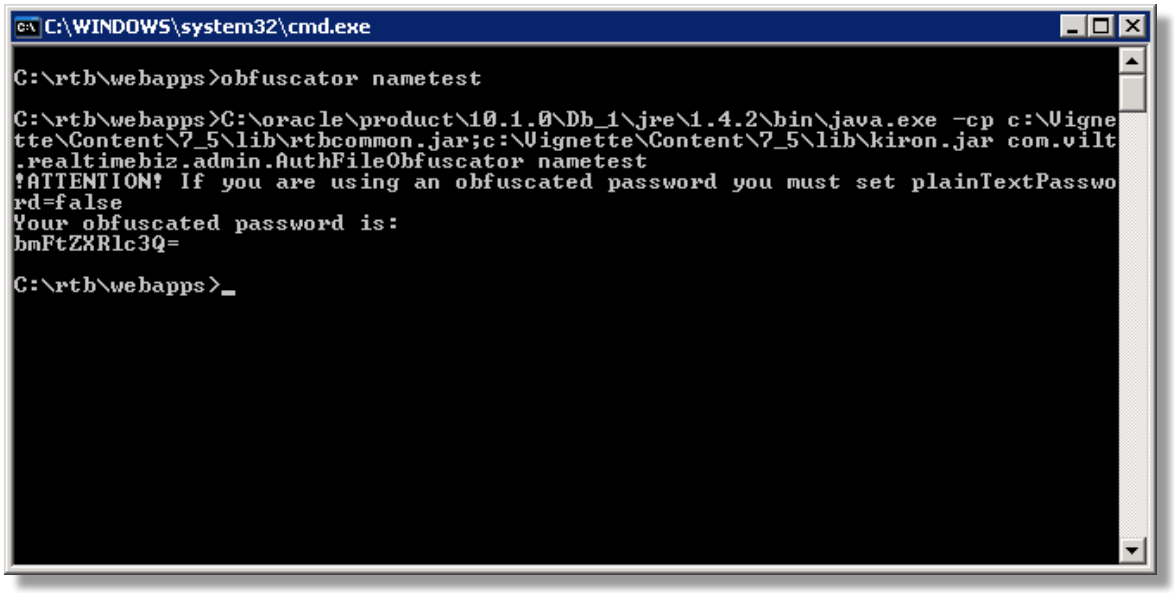
6 Appendix 2 – Properties Files

The properties files included in the Web Experience Management Audit 10.5.1 distribution have this structure:

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

IMPORTANT NOTE: 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 picture shows you how to do it.



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

6.1 Collector Properties (collector.properties)

```
[main]

#The DataBase vendor: Oracle | MSSQL
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]

#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/rtbcollector.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

#Interceptors package. Set it to DEBUG level to get details on VCM Audit's interceptors
included in collector
log4j.logger.com.vilt.audit.interceptors=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 OpenText Insights 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
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=vgndomai
n
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=vgndomai
n

[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,PropertyValueCach
eReloader

#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.PropertyValueUpdat
```

```
erJob

#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.PropertyValue
CacheReloaderJob

#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
```

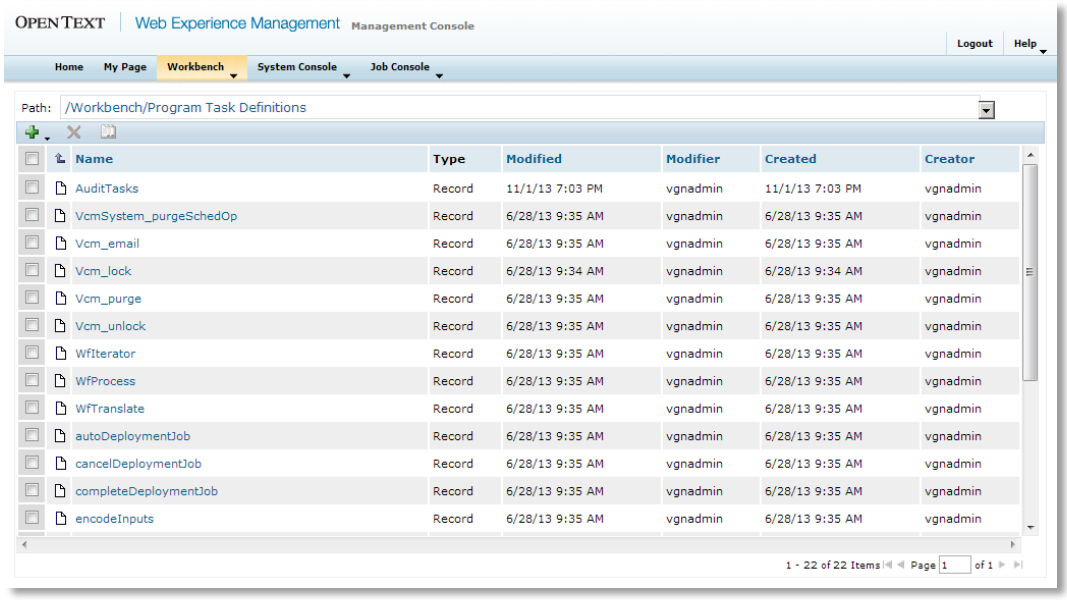
```
#file2 log file
log4j.appender.file2.File=c:/program files/vcm audit/logs/rtbVcmAudit.log

#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) -
```

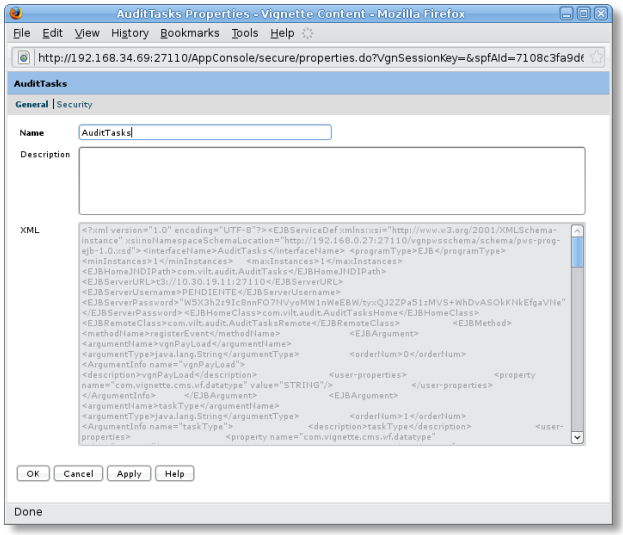
```
%m%n

#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

This workflow automated task is part of a set of tools included in an extensibility package of RTB. Contact your OpenText Sales representative for more information about extensibility capabilities. AuditTasks is used to log the events generated in the workflows. You need to use it if you want to audit existing custom Workflows whose events are not being 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.

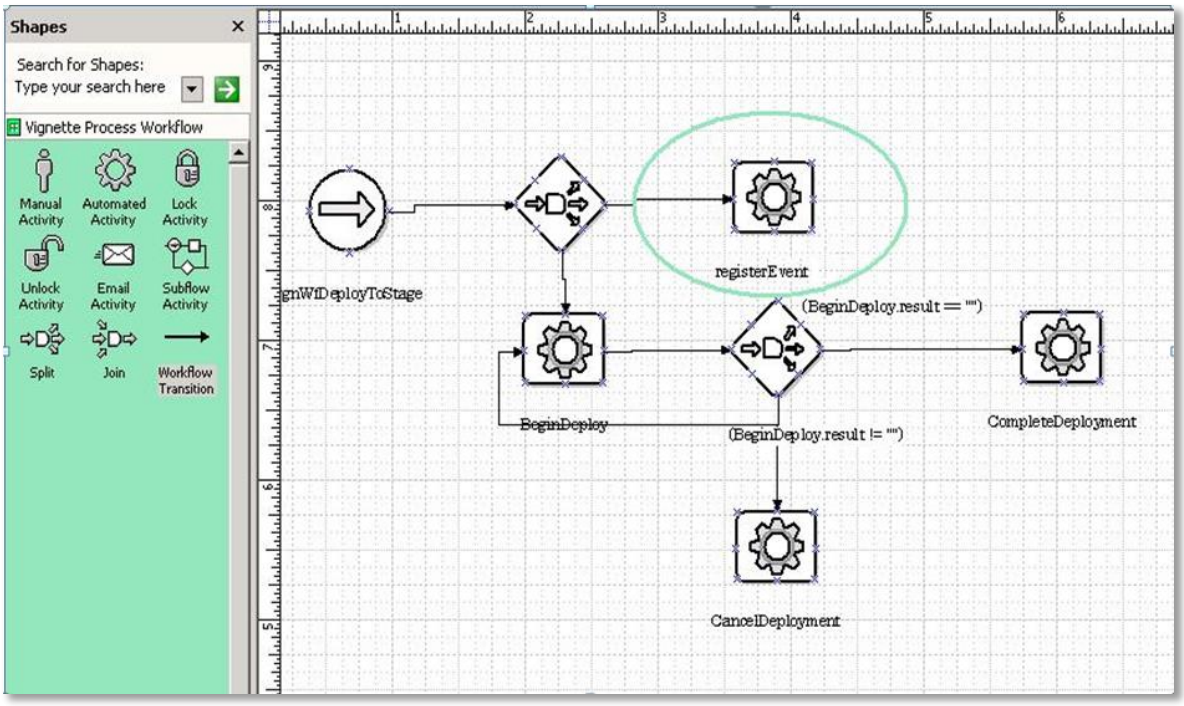




An automatic task named **registerEvent** is created. You need to place it in specific points of the WorkFlows's diagrams in order to audit them.

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. As shown 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:** Name with which the event will be registered. By default, the event is registered with the following properties:
   - **taskType**
   - **wf_id**

If the task has an associated payload, there will be registered as many events as the contents that the payload has, and there are also added the following attributes:

- **vcm_id**
- **ci_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 Web Experience Management 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, like 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		
	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 authentication using OpenText Directory Services (OTDS) 10.5. OpenText WEM uses OTDS for its authentication, making it possible to use the same OTDS installation to authenticate users in WEM and in WEM Audit.
WEM Audit in order to authenticate users through OTDS should be attributed a **Resource** created previously in OTDS by using the OTDS Administration Client.

> **Tip:** For more information on how to create an OTDS Resource, please refer to Appendix 6 – Configuring a Resource in OTDS.

After creation the Resource is identified by a **Resource Id** and is set to inactive state.

9.1 Installer - Provide OTDS Properties

When OTDS authentication is chosen the WEM Audit installer needs to be provided two configurations:

- **OTDS Resource ID**: Is the Resource Id of the resource created for the WEM Audit application and in 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://<otdshost>:<otdsport>/otdsws

After this configuration the installer will test the OTDS connection to the resource

9.1.1Error troubleshooting

If there was an error connecting to OTDS the message "**The connection to OTDS failed.**" is shown followed by an error message:

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 this messages match the error experienced, please 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

Please note that OTDS Group Names are case sensitive

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

Important

Only the users of the groups belonging to the OTDS Access Roles associated with the OTDS Resource configured will have access to the Insights console. You may check the users and groups associated to a Access Role in the OTDS Administration Client´

10 Appendix 6 – Configuring a Resource in OTDS

In this appendix we provide a quick guide on how to create and configure a Resource in OpenText Directory Services (OTDS) 10.5 in order to use it for authentication in WEM Audit.

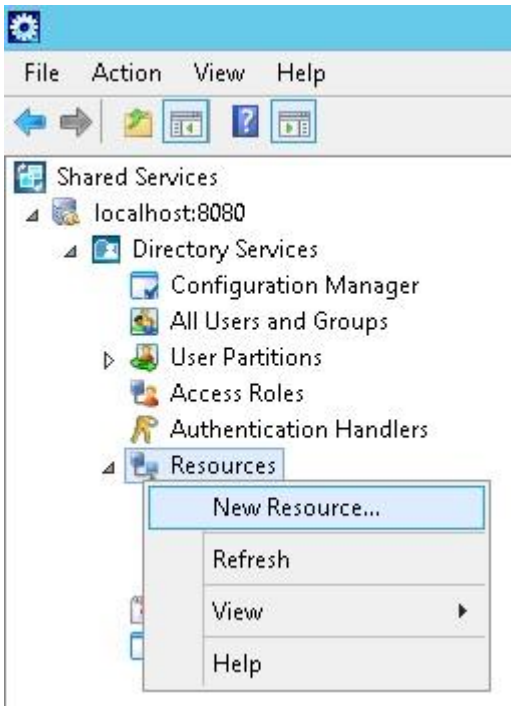
You can do this using 2 different tools:

- OpenText Administration Client
- OpenText Directory Services Administration Console

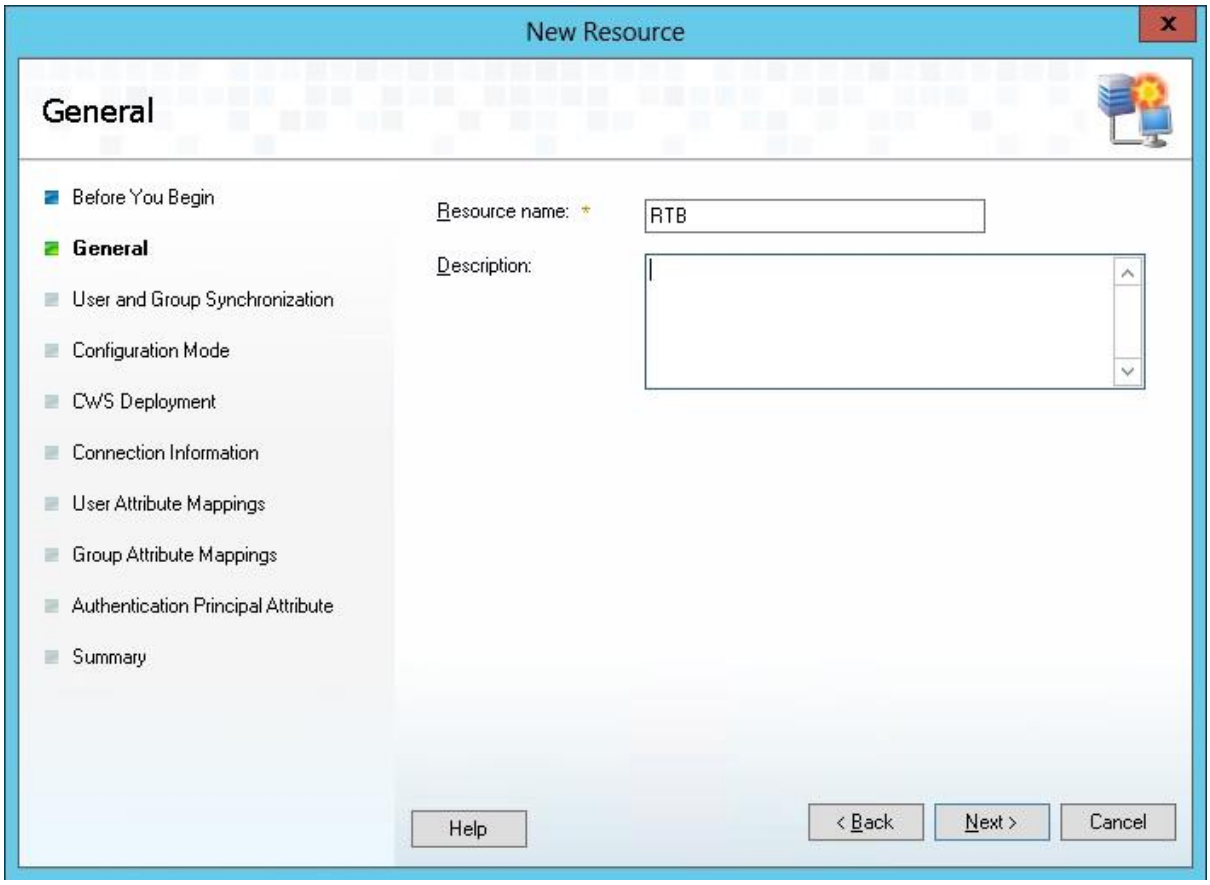
10.1 Configure a Resource using OpenText Administration Client

10.1.1 Creating the Resource

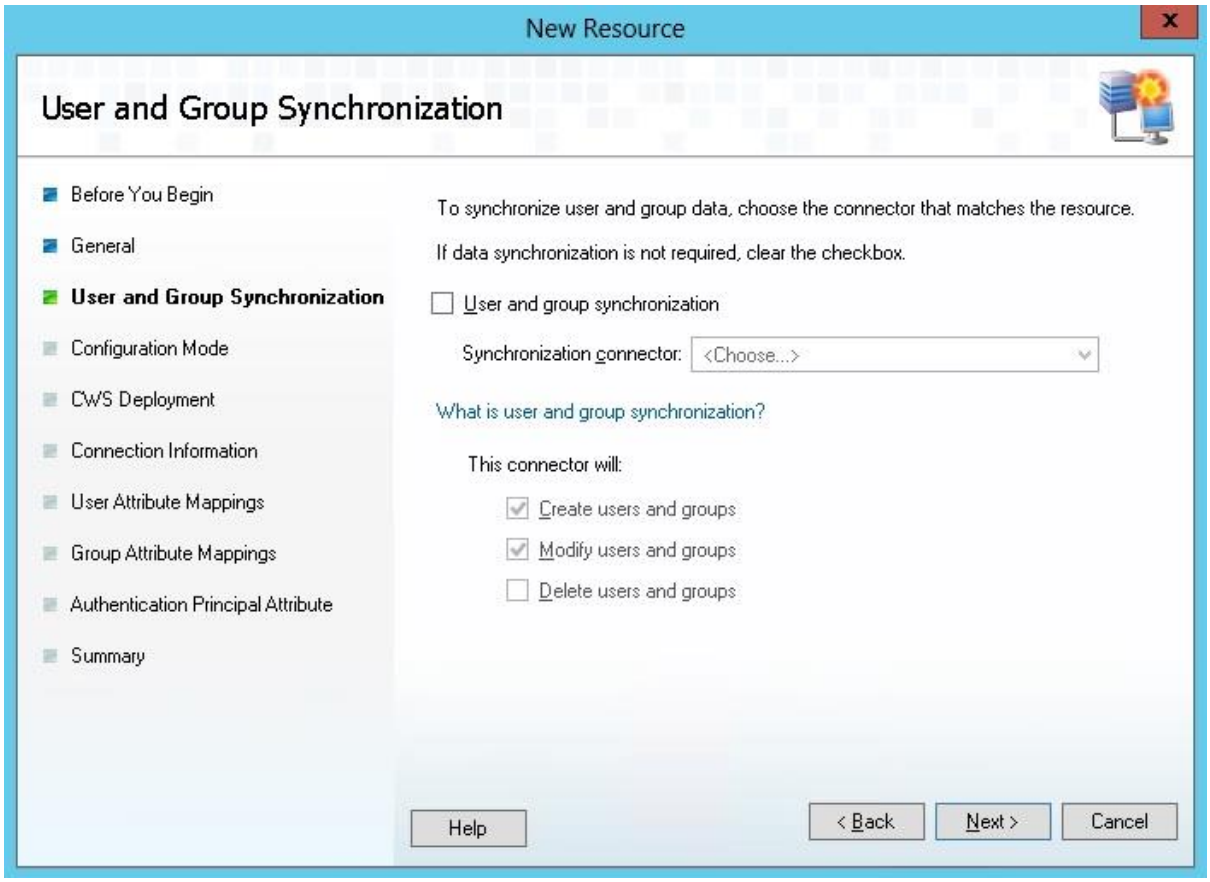
Open Administration Client and login to your OTDS server with a user with administration privileges (usually otadmin@otds.admin).



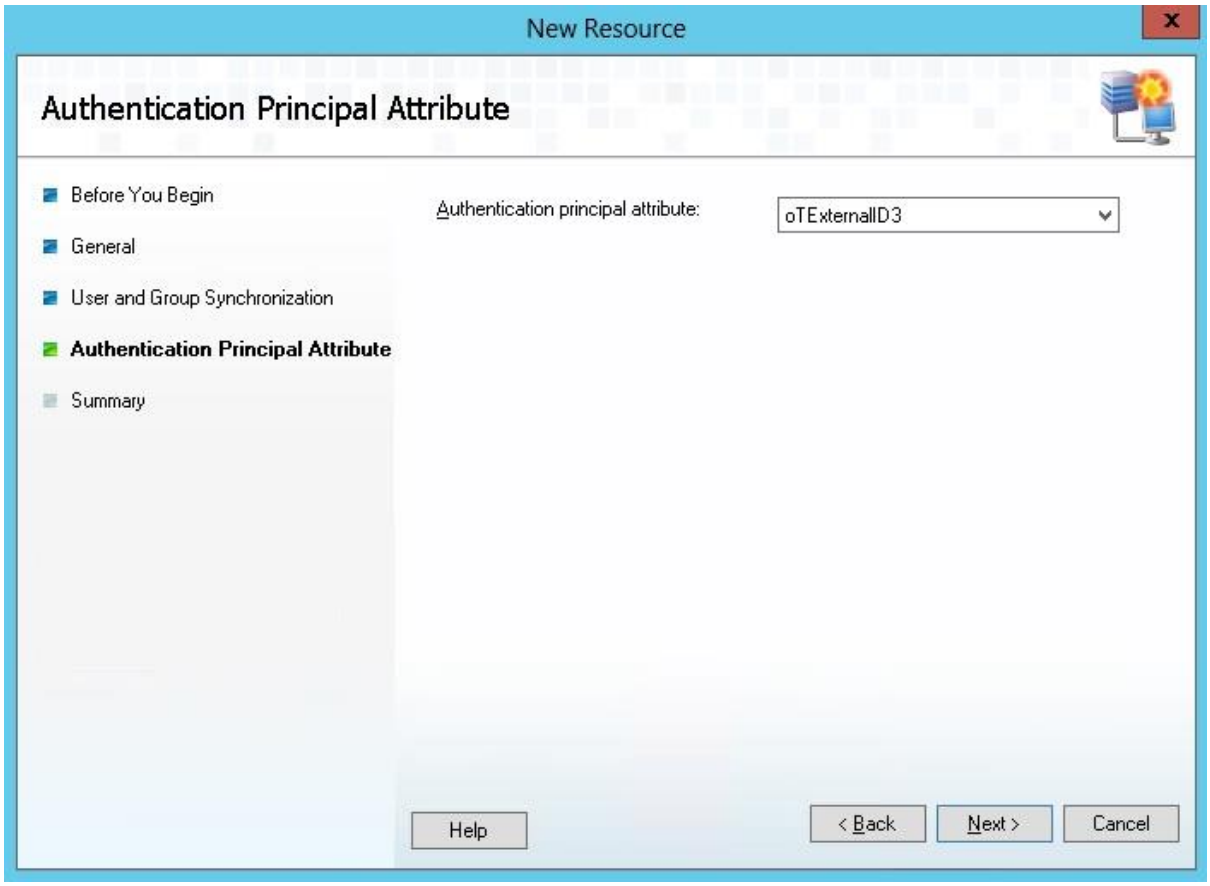
Navigate to **Shared Services > «Your Server» > Directory Services > Resources**. Right click over **Resources** and select **New Resource…**



In the **New Resource window**, in the **Before You Begin** section, click **Next**.
In the General section, please enter the **Resource name**. You can choose any name you want. You can optionally insert a **Description** for the resource. Click **Next**.



In the **User and Group Synchronization** section, make sure you deselect the option **User and group synchronization** and click **Next**.



In the **Authentication Principal Attribute** section and property, make sure you've selected **oTExternalID3** and click **Next**.

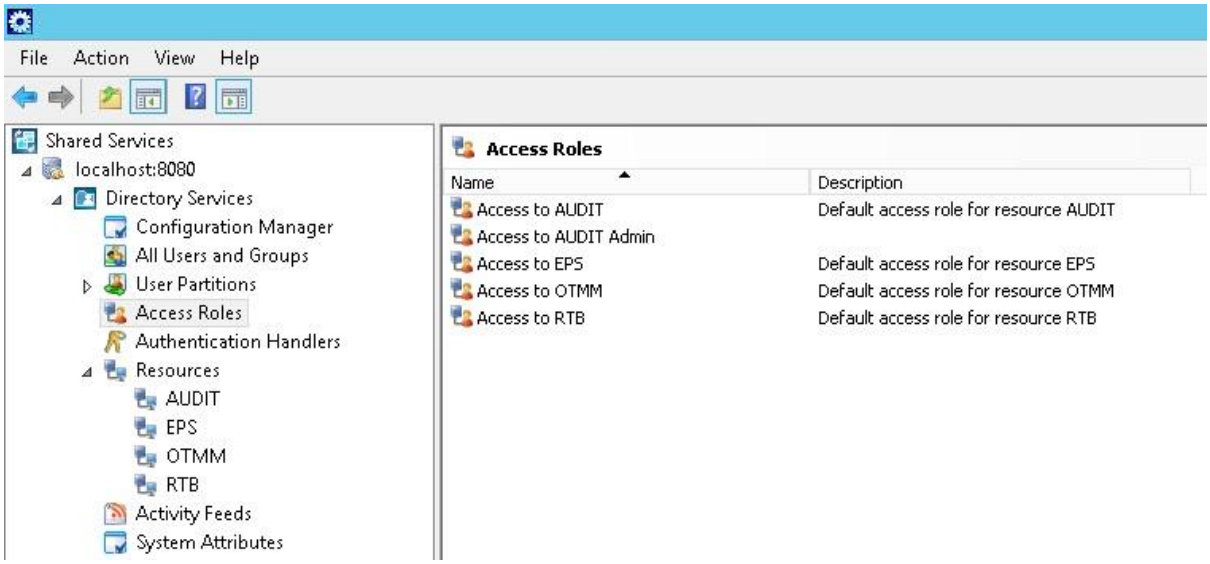
In the **Summary** section, just click **Finish**. You will be redirected to the **Resource Activation** window. In this window you can verify that the resource is in inactive state, by clicking on **Verify Activation**. Please remember that the resource should be inactive before installing WEM Audit. The install process will activate it.

We advise you to store the resource identifier (Resource ID) in a temporary note, because you will need it later in the installation process. You can use the option **Copy to Clipboard** to copy the Resource ID.

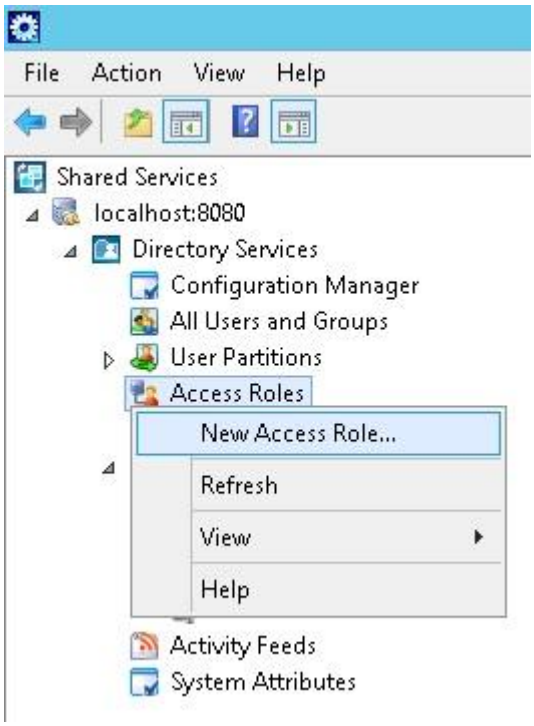
You can then close the Resource Activation Window.

10.1.2 Configuring Access Roles

You will need to configure at least one Access Role in order to associate the Groups and/or Users with the Resource you've just created and grant them access to Insights console. Navigating to **Shared Services > «Your Server» > Directory Services > Access Roles** you can see that an Access Role was automatically created with the creation of your Resource, with the name "**Access to «ResourceName»**".

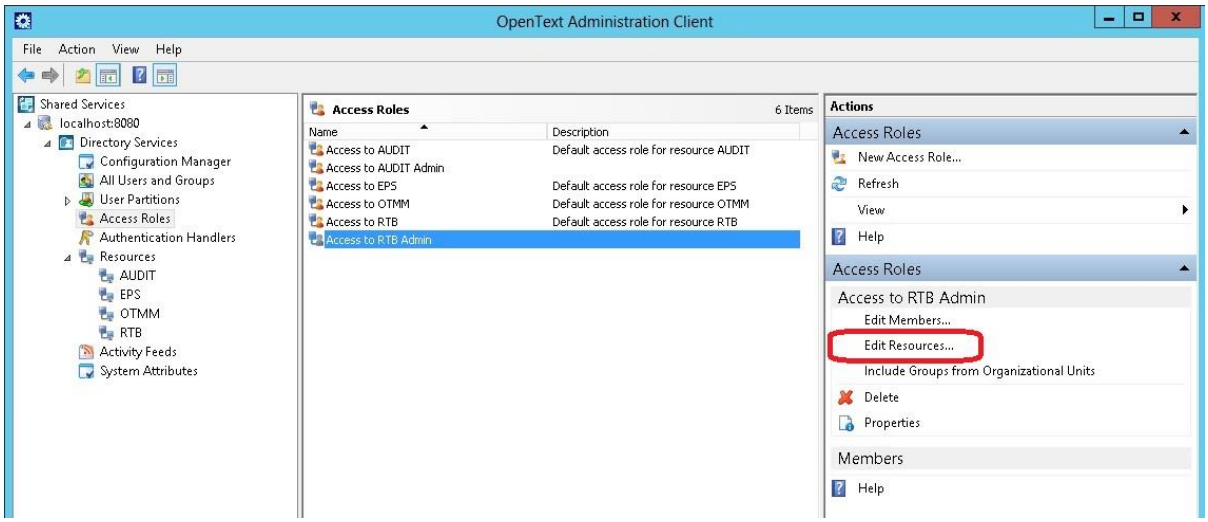


You can edit this resource or create a new one. In this guide we will explain how to create a new Access Role from scratch.



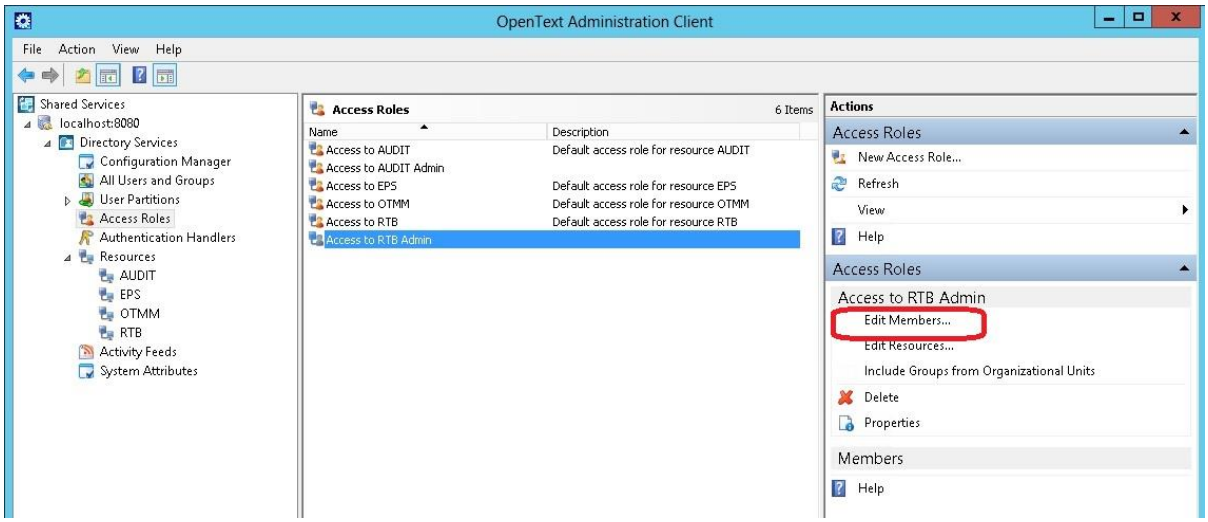
Right click on **Access Roles** and select **New Access Role…**

In the **General** section, insert the **Access Role name** (mandatory) and **Description** (optional). Click **OK**.

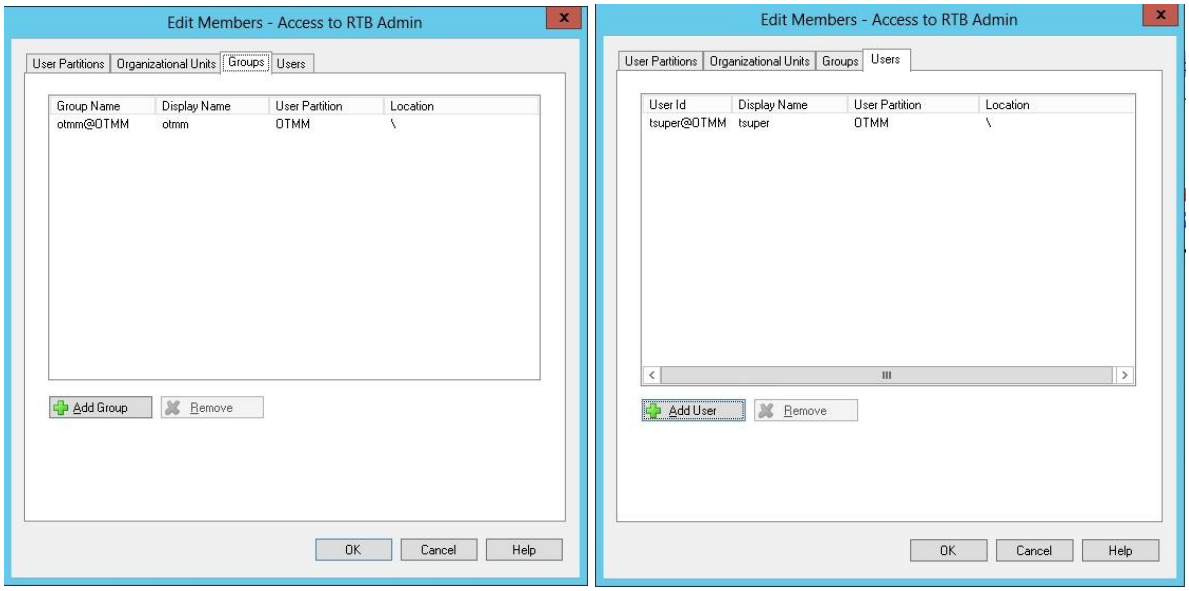


In the Access Roles, you can now see the access role newly created. Now you need to associate the Resource and the Users and Groups to it, in order to create the bound between them. Select your Access Role and click the option **Edit Resources** in the **Actions** panel.

Select the Resources you want to associate to this Access Role. For WEM Audit you just need to select the Resource created for it. Click **OK**.



Back to the Access Roles page, select your Access Role and click on **Edit Members** in the **Actions** panel.



You can add Groups and/or Users to the Access Roles. That will guarantee that the Groups and/or Users will have access to the Resource. We advise you to use 2 groups to map Insights access: one for regular access and another one to administration access. This two groups will be prompted during the installation wizard.

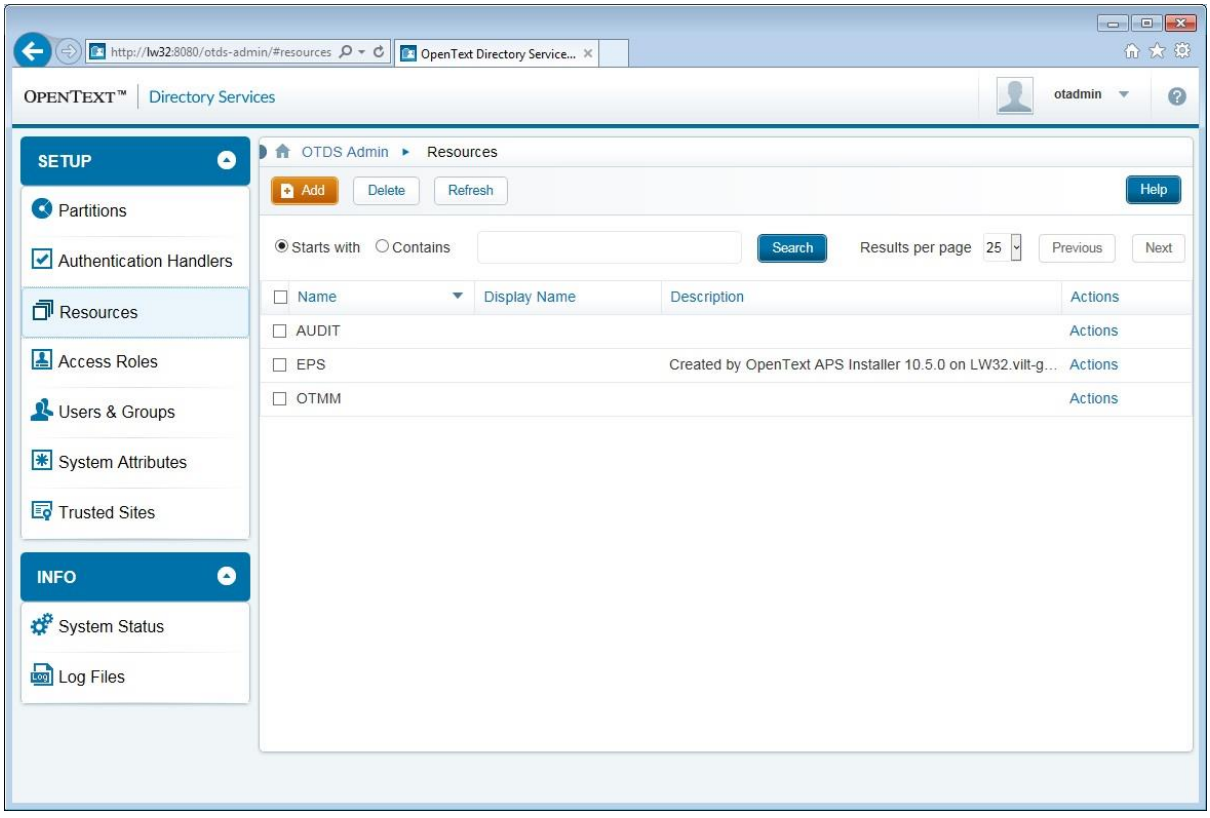
Please remember that the access to Insights console will always depend on the groups that the user belong, as the groups are what RTB uses in order to categorize the users and uses them as RTB Roles. So, the simplest way to guarantee access to RTB is always adding the groups of users that you will provide in the installation process

10.2 Configure a Resource using OTDS Administration Console

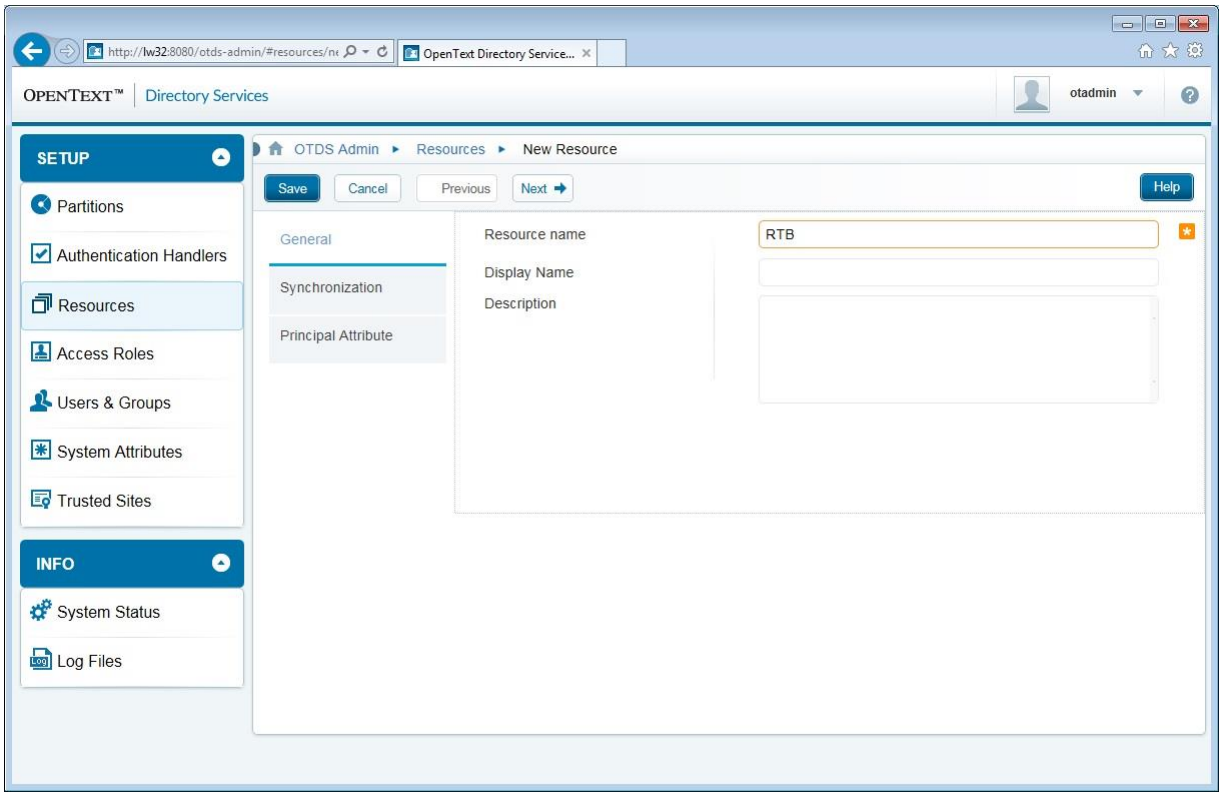
The OpenText Directory Services Administration Console is available on *http://<OTDSServer>:<Port>/otds-admin*.

10.2.1 Creating the Resource

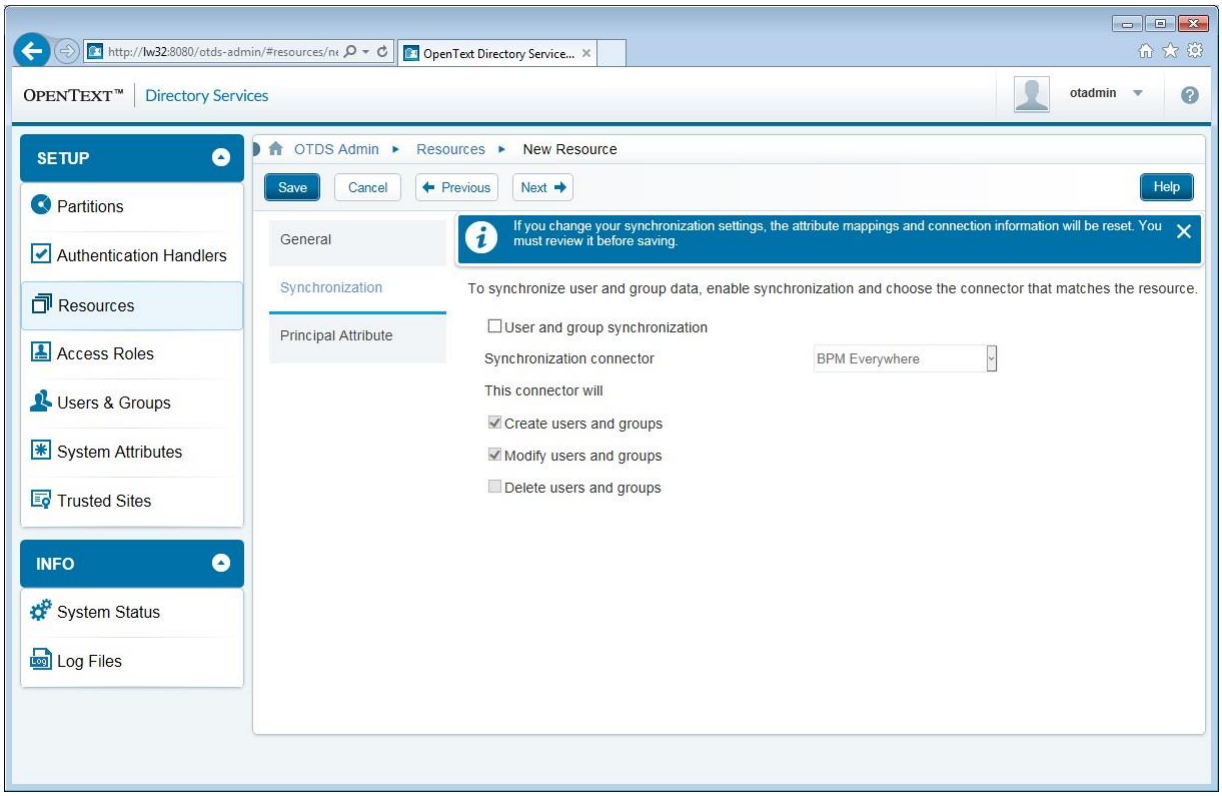
Open the Administration Console and login to your OTDS server with a user with administration privileges (usually otadmin@otds.admin).



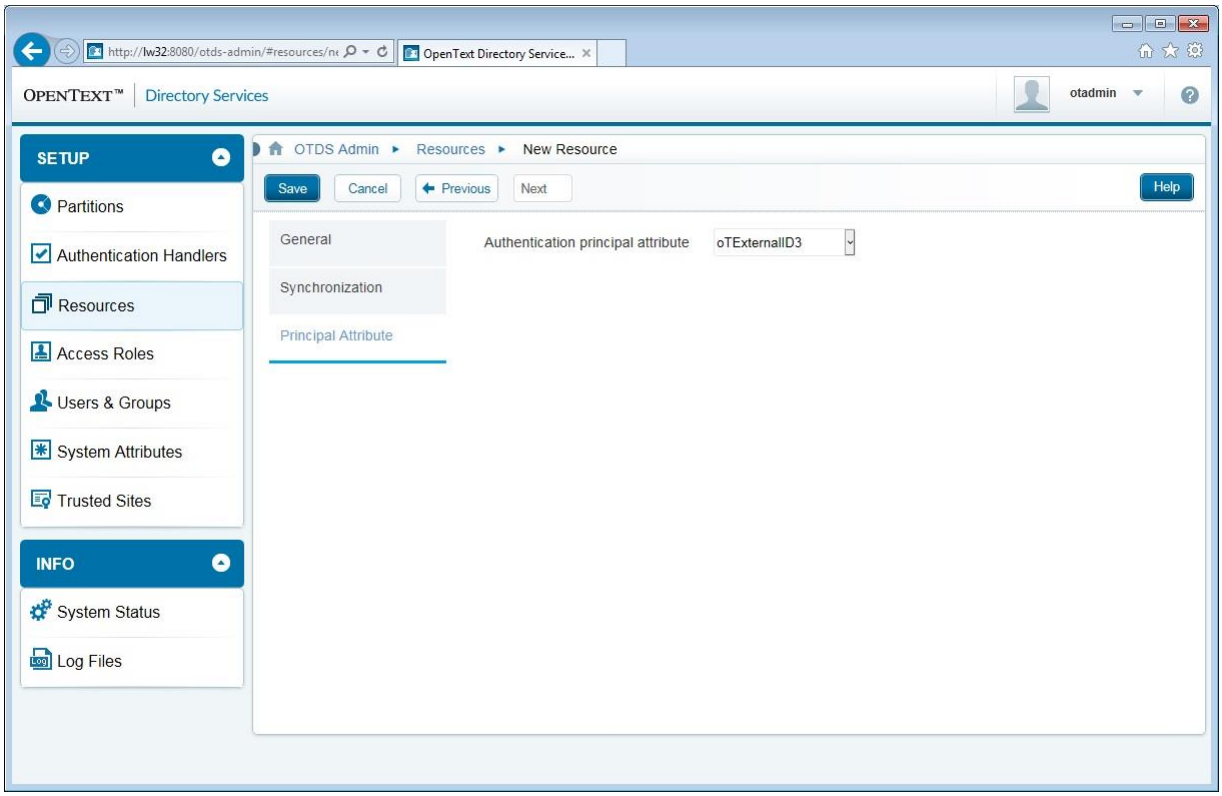
Navigate to **Resources** and **click** on the option **Add**, in order to create a new Resource.



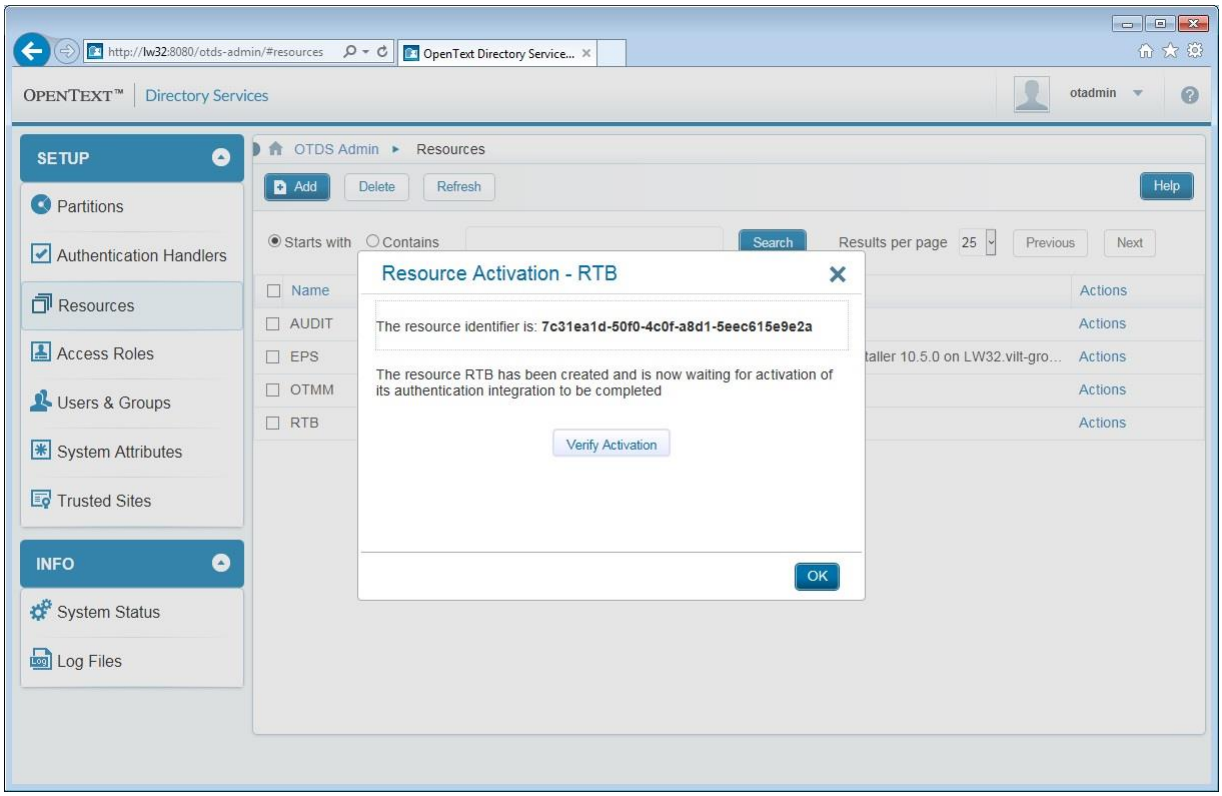
On the **General** section, give a **name** to your Resource and click **Next**. The name of your resource can be whatever the name you want. You can optionally add a **Display Name** and a **Description**.



On the **Synchronization** section, make sure you **deselect** the option **User and group synchronization** and click **Next**.



On the **Principal Attribute** section, make sure you select **oTExternalID3** as your **authentication principal attribute**. Click **Save** in order to save your new Resource.



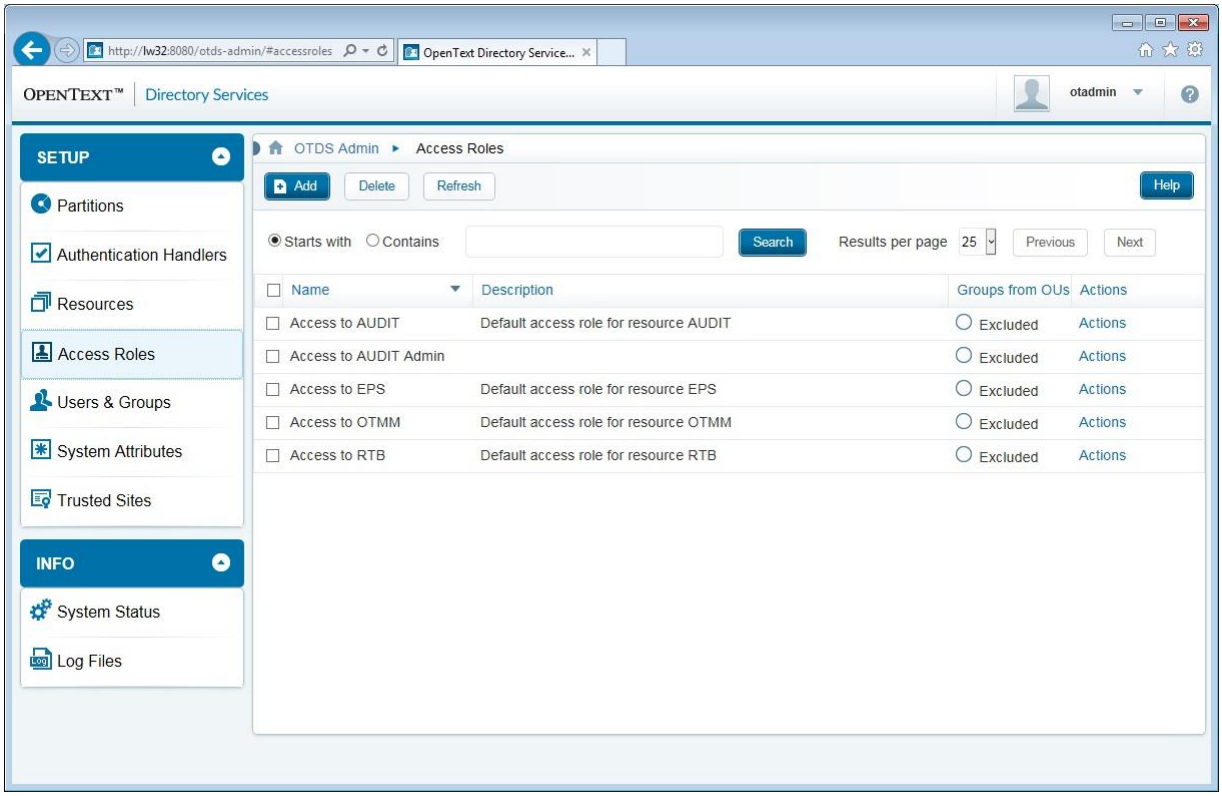
You will see a **Resource Activation** pop-up where you can verify that the resource is in inactive state, by clicking on **Verify Activation**. Please remember that the resource should be inactive before installing WEM Audit. The install process will activate it.

We advise you to store the resource identifier (Resource ID) in a temporary note, because you will need it later in the installation process.

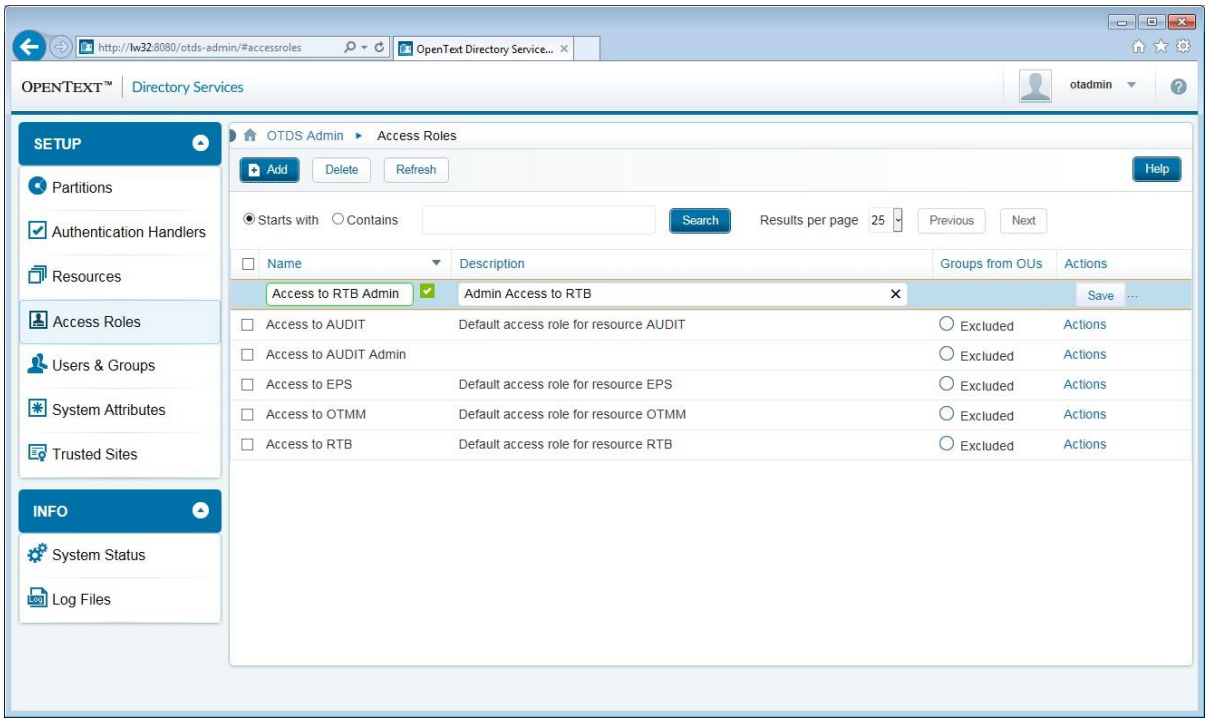
You can then close the Resource Activation pop-up.

10.2.2 Configuring Access Roles

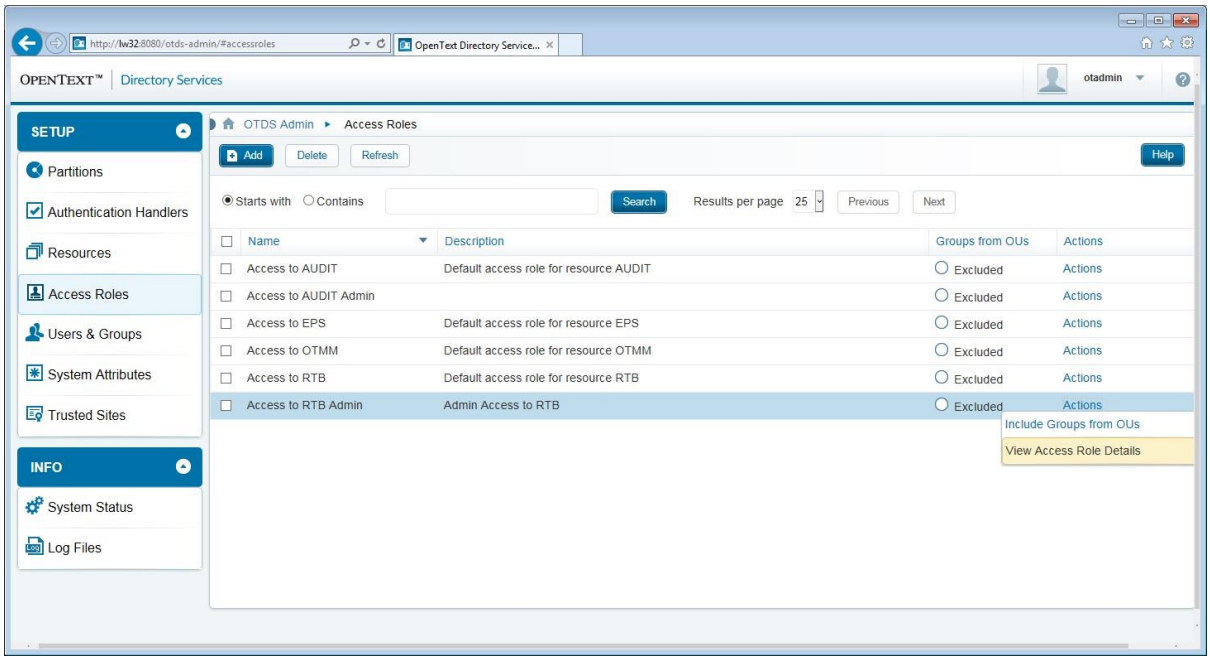
You will need to configure at least one Access Role in order to associate the Groups and/or Users with the Resource you've just created and grant them access to Insights console. Navigate to **Access Roles** and you can see that an Access Role was automatically created with the creation of your Resource, with the name "**Access to «ResourceName»**".



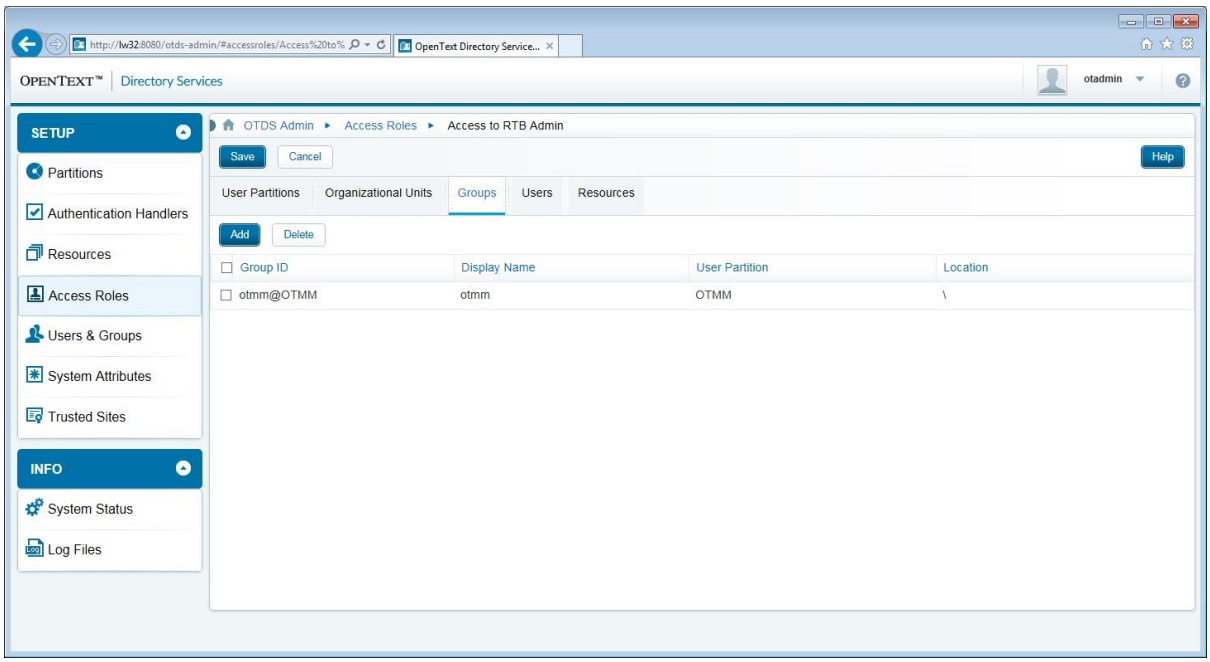
You can edit this resource or create a new one. In this guide we will explain how to create a new Access Role from scratch.



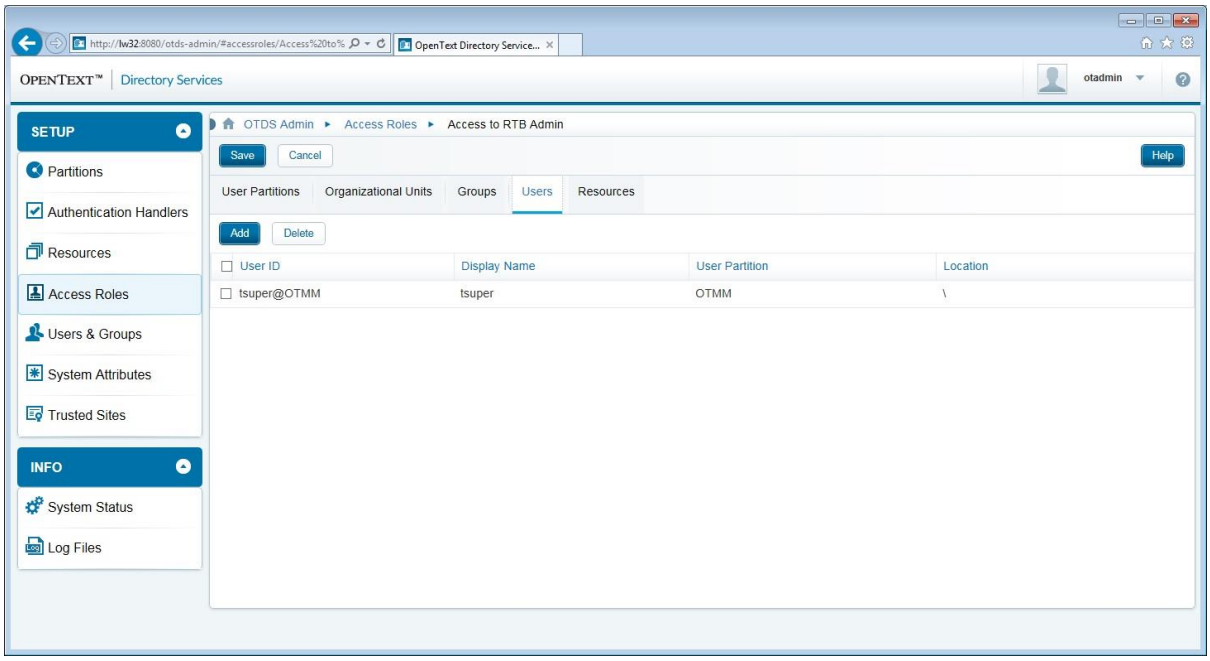
On the Access Roles page, click on the option **Add**. It will create a new line on the Access Roles list to create a new Access Role. Give it a **Name** and optionally a **Description** and click **Save**. You Access Role is created.



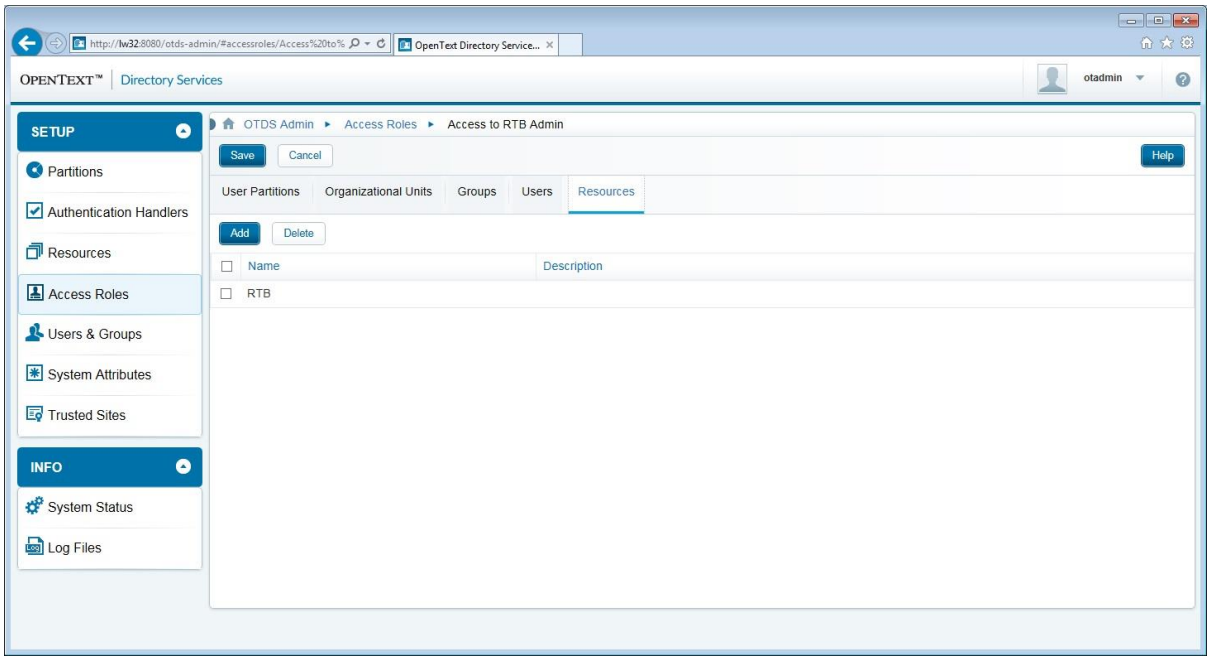
Now **Click** on the option **View Access Role Details** of the **Actions** menu of your Access Role.



In the **Access Roles Details** page, you can associate User Partitions, Organizational Units, Groups, Users and/or Resources to your Access Role. For WEM Audit purposes, you will need to associate **Groups and/or Users** and the **Resource** you've created. Navigate to the **Groups** section, click on the option **Add** and add the groups you will use for Audit purposes. On the **Add Groups to Access Role** pop-up, add the groups you want using the option **Add to Access Role**. Click **Ok** when you've added all the groups needed. We advise you to use **2 different groups**: one for **normal** access to Insights, and another for **administration** access. This 2 groups will be prompted during the WEM Audit installation.



If you wish to add a specific User to the Access Role to access RTB, navigate to the **Users** section and **add** the specific Users you want, the same way you've added the Groups in the last step.



Now navigate to the **Resources** section and add the Resource that you've created using the option **Add**. In the **Add Resources** pop-up, **select** the Resource and click on **Add to Access Role**, then click **Ok**.

At the end of adding the Groups and/or Users and the Resource to the Access Role, click on the **Save** option. This will save the details of your Access Role. The Access Role will function as a bound between the Groups and/or Users and the Resource you've created, which will guarantee access to RTB.

Please remember that the access to Insights console will always depend on the groups that the user belong, as the groups are what RTB uses in order to categorize the users and uses them as RTB Roles. So, the simplest way to guarantee access to RTB is always adding the 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

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

Email: support@opentext.com
Knowledge Center: https://knowledge.opentext.com

For more information, visit www.opentext.com