

Oracle® Cloud

Using Oracle WebCenter Content on Marketplace in Oracle Cloud Infrastructure



F92088-08
June 2024



Oracle Cloud Using Oracle WebCenter Content on Marketplace in Oracle Cloud Infrastructure,

F92088-08

Copyright © 2024, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	v
Documentation Accessibility	v
Related Resources	v
Conventions	v

1 What's New in Oracle WebCenter Content on Marketplace

2 Get Started with Oracle WebCenter Content on Marketplace

About Oracle WebCenter Content on Marketplace	2-1
About the License for Oracle WebCenter Content on Marketplace	2-1
About Roles and User Accounts	2-2

3 Create and View Oracle WebCenter Content on Marketplace Instances

Before You Begin	3-1
Sign in to Oracle Cloud Infrastructure Console	3-1
Prerequisites	3-1
System Requirements	3-2
Generate SSH key pair	3-2
Create a Compartment	3-3
Create a Master Key	3-4
Create Database	3-4
IDCS	3-6
Create the Object Storage Bucket in OCI	3-6
Create a New User API Key	3-7
Create Vault Secrets	3-7
Provision WebCenter Content Stack	3-8

4 Configure FA Adapter Integration with WebCenter Content

5 Configure SAML2 IDCS Single Sign-On in WebCenter Content

6 Troubleshoot

Preface

This guide describes how to provision and administer Oracle WebCenter Content 12c (12.2.1.4) on Marketplace in Oracle Cloud Infrastructure.

Audience

This guide is intended for users who want to create, manage, and use WebCenter Content instances provisioned from Marketplace in Oracle Cloud Infrastructure.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Resources

The [documentation for Oracle WebCenter Content](#) for 12c (12.2.1.4) is available from the Oracle Help Center.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

What's New in Oracle WebCenter Content on Marketplace

Learn about the new and changed features in Oracle WebCenter Content on Marketplace.

24.6.1— June 2024

Feature	Description
Object Storage for documents is optional	You can choose to store documents in the file system or in Object Storage. See Provision WebCenter Content Stack . Customers can now leverage Object Storage's Infrequent Access storage class tier to address the need for a storage tier that is ideal for data that is accessed infrequently (and optimize cost), but that must also be available immediately when needed. For more details, refer to OCI Object Storage documentation.
PDB name	You can now specify the PDB name when configuring the database. See Provision WebCenter Content Stack .
Database Strategy	You can now specify the Database Strategy (type of database) such as Database System or Autonomous Transaction Processing Database when configuring the database. See Provision WebCenter Content Stack .
Integration with OCI Logging	You can integrate WebCenter Logs with OCI Logging. See Integrating WebCenter Logs with OCI Logging .
REST API	There are new WebCenter Content REST APIs that allow you to interact with content in WebCenter Content. See REST API for Oracle WebCenter Content .
Integration with OCI Process Automation	You can integrate WebCenter Content with OCI Process Automation. See Integrating Oracle WebCenter Content with OCI Process Automation .
Large dID	WebCenter Content on Marketplace now supports very large dID. dIDs of large size can now successfully flow through the system. A dID is an internally generated integer that refers to a specific revision of a content item. To understand what dIDs are, see Developing with Oracle WebCenter Content .
Migration from Oracle Content Management to Oracle WebCenter Content	Oracle provides migration utilities and documentation to migrate from Oracle Content Management to Oracle WebCenter Content. For information about the tools, please raise a support ticket in My Oracle Support .

24.5.1— May 2024

Feature	Description
Object Storage for documents	Object Storage (a storage provider component) is now available to store documents. See Provision WebCenter Content Stack .
Configure FA adapter integration with WebCenter Content	You can install and configure FA integration with WebCenter Content on marketplace. See Configure FA Adapter Integration with WebCenter Content .

Feature	Description
Configure SAML2 IDCS Single Sign-On in WebCenter Content	You can configure SAML2 IDCS Single Sign-On in WebCenter Content on marketplace. See Configure SAML2 IDCS Single Sign-On in WebCenter Content .
WebCenter Content Reports	WebCenter Content Reports feature is now available in WebCenter Content on Marketplace. See Doc ID 3023292.1 in My Oracle Support
Smart Tagging	You can now enable smart tagging feature in WebCenter Content on Marketplace. See Doc ID 3023045.1 in My Oracle Support .
Embeddable Document Viewer	This feature offers a first look at the WebCenter Content user interface using the Redwood design. This new viewer interface is offered as an option to view documents from within the existing native WebCenter Content UI and to reference documents directly using a service URL. See Doc ID 3024420.1 in My Oracle Support .
REST API	The WebCenter Content REST APIs allow you to interact with content in WebCenter Content. See Doc ID 3021636.1 in My Oracle Support .

2

Get Started with Oracle WebCenter Content on Marketplace

Here's information about Oracle WebCenter Content on Marketplace that will help you get started:

- [About Oracle WebCenter Content on Marketplace](#)
- [About the License for Oracle WebCenter Content on Marketplace](#)
- [About Roles and User Accounts](#)

About Oracle WebCenter Content on Marketplace

Oracle WebCenter Content on Marketplace is provided as a VM-based solution on Oracle Cloud Infrastructure.

Oracle WebCenter Content on Marketplace is available in two types of Marketplace offerings: Paid and BYOL. See [About the License for Oracle WebCenter Content on Marketplace](#).

Oracle WebCenter Content on Marketplace helps customers to provision/set up the environment in few clicks and enables to deliver Content solutions on cloud.

About the License for Oracle WebCenter Content on Marketplace

Oracle WebCenter Content on Marketplace is based on Oracle WebCenter Content 12c (12.2.1.4). Oracle WebCenter Content on Marketplace is available in two types of Marketplace offerings:

- **Paid:** Use one of the following Oracle WebCenter Content (Paid) listings to use Universal Credits pricing:
 - Oracle WebCenter Content 12c (Paid)
 - Oracle WebCenter Universal Content Management 12c (Paid)
 - Oracle WebCenter Imaging 12c (Paid)
 - Oracle WebCenter Enterprise Capture 12c (Paid)
 - Oracle WebCenter Enterprise Capture Standard Edition 12c (Paid)

See [Oracle Universal Credits](#).

- **BYOL:** Use the Oracle WebCenter Content (BYOL) listing to Bring Your Own License using your existing Oracle WebCenter Content 12c (12.2.1.4) on-premises license, or you can purchase a new license for Oracle WebCenter Content 12c (12.2.1.4).

When you activate Oracle WebCenter Content on Marketplace using the BYOL listing, you are charged only for the Oracle Cloud Infrastructure resources consumed. You must have sufficient supported on-premises licenses as required and specified in the Service Description for Oracle PaaS.

For the processor conversion ratios and license requirements for the BYOL offering, go to the Cloud Service Descriptions page and go to the [Cloud Service Description](#) PDF. In particular, note the following conversion ratios for BYOL:

- For each supported Processor license, you may activate up to 2 OCPUs of the BYOL Cloud Service.
- For every 10 supported Named User Plus licenses, you may activate 1 OCPU of the BYOL Cloud Service.

About Roles and User Accounts

Oracle WebCenter Content on Marketplace uses roles to control access to tasks and resources. A role assigned to a user gives certain privileges to the user.

Access to Oracle WebCenter Content on Marketplace is based on the roles and users set up for the Oracle Cloud Infrastructure console. You need OCI Administrator role to provision WebCenter Content.

For information about how to add user accounts in Oracle Cloud, see:

- [Add Users to a Cloud Account with Identity Cloud Service](#) in *Getting Started with Oracle Cloud*.
- [Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console](#) in the Oracle Cloud Infrastructure documentation.

3

Create and View Oracle WebCenter Content on Marketplace Instances

The information in this chapter will help you create and view Oracle WebCenter Content on Marketplace instances.

- [Before You Begin](#)
 - [Sign in to Oracle Cloud Infrastructure Console](#)
 - [Prerequisites](#)
- [Provision WebCenter Content Stack](#)

Before You Begin

Before you begin, you would need to complete the following tasks and prerequisites.

Sign in to Oracle Cloud Infrastructure Console

Complete the following steps to sign in to the Oracle Cloud Infrastructure console.

1. Go to <http://cloud.oracle.com>.
2. Enter your cloud account name and click **Next**.
3. Sign in to the Oracle Cloud Infrastructure console:
 - If your cloud account uses identity domains, sign in to the Oracle Cloud Infrastructure console as a user configured in Oracle Cloud Infrastructure Identity and Access Management (IAM).
Select the **default** domain.
 - If your cloud account does not use identity domains, sign in to the Oracle Cloud Infrastructure console as a user federated through Oracle Identity Cloud Service.
Under Single Sign-On (SSO) options, note the identity provider selected in the **Identity Provider** field and click **Continue**.
4. Enter the user name and password provided in the welcome email, and click **Sign In**.

The Oracle Cloud Infrastructure console is shown.

Prerequisites

You'll need to complete the following prerequisites before provisioning the WebCenter Content stack.

- [System Requirements](#)
- [Generate SSH key pair](#)
- [Create a Compartment](#)
- [Create a Master Key](#)

- [Create Database](#)
- [IDCS](#)
- [Create the Object Storage Bucket in OCI](#)
- [Create a New User API Key](#)
- [Create Vault Secrets](#)

After completing the above prerequisites, you can proceed to provision the WebCenter Content stack.

System Requirements

You require access to the following services to use Oracle WebCenter Content on OCI.

- Identity and Access Management (IAM)
- Compute, Network, Block Storage
- Vault, Key, Secret
- Resource Manager
- Database
- Load Balancer
- Tagging

Make sure you have the following minimum limits for the services in your Oracle Cloud Infrastructure tenancy, and if necessary, request for an increase of a service limit.

Service	Minimum Limit
Identity and Access Management (IAM) Policy	1
Compute Shape VM.Standard.E4.Flex or VM.Standard.E5.Flex	1
Virtual Cloud Network	1
Block Storage	1 TB
Vault & Key	1
Secrets	5
Load Balancer	Flexible Load Balancer

In Oracle Cloud Infrastructure Vault (formerly known as Key Management), a standard vault is hosted on a hardware security module (HSM) partition with multiple tenants, and it uses a more cost-efficient, key-based metric for billing purposes. A virtual private vault provides greater isolation and performance by allocating a dedicated partition on HSM. Each type of vault has a separate service limit in your Oracle Cloud Infrastructure tenancy. The limit for secrets spans all the vaults.

See [Service Limits](#) in the Oracle Cloud Infrastructure documentation.

Generate SSH key pair

See [generate_ssh_key](#) for generating an SSH key pair.

This SSH key pair will be used for connecting to Bastion and Compute instances after stack execution.

**Note:**

This will be used to create DB and WebCenter Content nodes.

Create a Compartment

If your tenancy does not already include a compartment for your Oracle WebCenter Content on Marketplace instances, you can create a new one.

**Note:**

To create a compartment, your administrator must first add the following policy for your group:

```
allow group groupName to manage compartments in tenancy
```

To create a compartment in Oracle Cloud Infrastructure:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
 2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Compartments**. A list of the existing compartments in your tenancy is displayed.
 3. Click **Create Compartment**.
 4. Enter the following:
 - Name: Specify a name. For example, wcc-compartment. Restrictions for compartment names are: Maximum 100 characters, including letters, numbers, periods, hyphens, and underscores. The name must be unique across all the compartments in your tenancy.
 - Description: A friendly description.
 5. Click **Create Compartment**.
 6. Once the compartment is created, if you are not an administrator, ask your administrator to grant the following manage and use permissions in the compartment:
 - a. Navigate to Identity and Security, Policies, and then Create Policies.
 - b. To allow a non-administrator to execute the stack, create an IAM group called **wcc** and then create a policy with the following statements.
 - `allow group wcc to manage instance-family in compartment wcc-compartment`
 - `allow group wcc to manage virtual-network-family in compartment wcc-compartment`
 - `allow group wcc to manage volume-family in compartment wcc-compartment`
 - `allow group wcc to manage load-balancers in compartment wcc-compartment`
 - `allow group wcc to manage orm-family in compartment wcc-compartment`
- where `wcc` is the group name and `wcc-compartment` is the compartment name.

 **Note:**

You can use any name (**wcc** and **wcc-compartment** are examples).

Create a Master Key

You'll need to create a master key for the vault.

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu and click **Identity & Security** and then **Vault**.
3. Change the necessary compartment.
4. Click the already created vault name.
5. On the left side, click **Master Encryption keys** and then click **Create Key**.
6. Complete the following:
 - Create In Compartment : Name of the selected compartment
 - Protection Mode: Software
 - Name: Specify a name.
 - For remaining fields, retain the default values.
7. Click **Create Key**.
Wait for the status to show green.

Create Database

You'd need a new DB system only if you want to provision a new database.

 **Note:**

Otherwise, you can use an existing database too.

 **Note:**

Currently, only the Oracle Base Database Service is supported. Support for other versions will be provided in upcoming releases. For any additional questions, contact the Oracle Support team.

Complete the following to create a new DB system:

- [Create VCN](#)
- [Create a New DB System](#)

Create VCN

1. Log in to OCI Console, navigate to Networking, then to Virtual Cloud Networks.
2. Click **Create VCN via Wizard**.

3. Click **Start VCN Wizard**.
4. **VCN name:** Provide a name.
5. **Compartment:** Specify the compartment in which the VCN needs to be created.
6. **VCN IPv4 CIDR block:** Specify IPv4 CIDR block (for example, 10.0.0.0/16).
7. Select the **Use DNS hostnames in this VCN** check box.
8. In the Configure public subnet and Configure private subnet sections, specify the correct CIDR blocks and click **Next**.
9. Make sure to create the necessary gateways such as Internet gateway, NAT gateway, and Service gateway.
10. Click **Create**.

The VCN is created.

Create a New DB System

1. Create a new DB system in [the VCN you created earlier](#).
2. Make a note of the SSH keys used for the DB system creation. This private SSH key will be added to the vault's secret later.

 **Note:**

Ensure to provide a DB System SSH private key without a passphrase as passphrase is not allowed.

- a. Log in to the console.
- b. Click **Oracle Database**.
- c. Click **Oracle Base Database Service** and then click **Create DB Systems**.
- d. Provide the following parameters:
 - Select a Compartment Name: Choose the appropriate compartment name.
 - Name your DB system: Specify a suitable name.
 - Select an availability domain: Choose AD1. You can choose any AD but make sure that WebCenter Content and DB are in the same AD.
 - Configure shape: AMD VM Standard E4 Flex
 - Configure storage: 1 TB
 - Configure the DB system: The total node count is 2 and Oracle Database software edition is Enterprise Edition Extreme Performance.
 - Add SSH keys: Upload the public SSH key you created in [the first step](#). You can either reuse the keys generated in [the first step](#) or you can generate a new pair of keys too for database instances.
 - License: Choose the appropriate license.
 - Virtual cloud network: Choose [the VCN you created earlier](#).
 - Client subnet: Select (either private or public subnet as needed) from the drop-down list.
 - Hostname prefix: Choose an appropriate name.

- Database name: Specify a name for your database. Click **Next**.
 - Database image: Oracle Database 19c.
 - PDB Name: pdb1
 - Create administrator credentials: Specify 'sys' and an appropriate password.
 - Backup destination: Object Storage
 - For remaining input fields: Select the default values.
- e. Click **Create DB System** and wait for the DB provisioning to be completed before you proceed to the next step.

IDCS

1. Create a new IDCS Confidential App for WebCenter Content provisioning. Log in to your IDCS administration console. For example, <https://<your-idcs-link>.identity.oraclecloud.com/ui/v1/adminconsole>. You can find this URL on the *Oracle Identity Cloud Service* section by navigating to Identity, Federation, and then Identity Provider Details. The field name that has this URL is **Oracle Identity Cloud Service Console**.
2. Click **Integrated applications**.
3. Click **Add application** on the Integrated Applications page to create a new confidential app.
4. Choose **Confidential Application** in the Add Application popup.
5. In the Details section, provide a name and click **Next**.
6. In the Client section, choose **Configure this application as client now** and select the following grant types under Authorization:
 - Client Credentials
 - JWT Assertion
 - SAML2 Assertion
7. Skip all other sections by clicking **Next** till you reach the **Finish** button.
8. Make a note of the Client ID and Client Secret for this app. Client Secret will be added to the vault's secret later.
9. Navigate to the application created and click **Activate** to enable this app for use in WebCenter Content provisioning.

Create the Object Storage Bucket in OCI

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Click the navigation menu in the upper left corner of the page and click **Storage**.
3. Click **Buckets**.
4. Confirm that you're in the correct compartment and the correct region.
5. Click **Create Bucket** on the "Buckets in <compartment name> Compartment" page.
6. Provide a value for **Bucket Name**.
7. Leave the **Default Storage Tier** set to **Standard**.
8. Leave the **Encryption** set to **Encrypt using Oracle managed keys**.

9. Click **Create**.

See [Object Storage Buckets](#) for more information.

Create a New User API Key

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Click on your avatar in the upper-right corner of the page.
3. Click **My profile**.
4. In the **Resources** menu on the left side of the page, click **API Keys**.
5. Click **Add API Key**.
6. Download the private key by clicking **Download private key**. The private key will be added to the vault's secret later.
7. Click **Add**.
8. Click **Copy** to copy the content of the configuration file which has user OCID and fingerprint as this will be required later. Close the dialog.

Create Vault Secrets

1. Log in to the OCI console and search for *Vault*, and then create a vault app.
 - a. Click **Create Vault**.
 - b. Select [the compartment you created earlier](#)
 - c. Provide a name and click **Create Vault**.
2. Click the vault app you created earlier. Create a master encryption key by specifying the compartment, protection mode, name, algorithm, length, and so on in the Create Key section.
3. Click **Secrets** on the left side and start adding secrets by specifying the compartment, name, key, secret type template, secret contents, and so on in the Create Secret section.

Secret Name	Secret Description	Comment
wcc-admin-password	Secret for WebCenter Content Admin Password	The Secret Contents field should be populated with the Weblogic password value. The password needs to meet the following password policy: The password must be at least 8 alphanumeric characters with at least one number or a special character.
db-system-sys-password	Secret for DB System SYS Password	SYS user password of DB created in the Create a New DB System section should be used in the Secret Contents field.
db-system-ssh-private-key	Secret for DB System SSH private key	The Secret Contents field should be populated with the private key value that was used to create DB in the Create a New DB System section.
idcs-client-secret	Secret for IDCS Client secret	The Secret Contents field should be populated with the Client Secret value that was noted when the IDCS Confidential App was created in the IDCS section.

Secret Name	Secret Description	Comment
wcc-schema-password	Secret for WCC schema password.	<p>Example: OCI#db#456789123</p> <p>The password needs to meet the following password policy:</p> <ul style="list-style-type: none"> • The password must start with a letter. • The password must contain at least two digits. • The password must contain at least two uppercase letters. • The password must contain at least two lowercase letters. • The password must contain at least two special characters from the set [\$_#_]. • The password must be at least 15 characters long.
oci-user-private-key	Secret for user API private key	The Secret Contents field should be populated with the private key value downloaded earlier in the Create a New User API Key section.

Provision WebCenter Content Stack

You can provision Oracle WebCenter Content on a Marketplace instance in a selected compartment in Oracle Cloud Infrastructure.

To provision Oracle WebCenter Content on a Marketplace instance:

1. Navigate to the WebCenter Content listing on Marketplace by direct URL or by browsing in Oracle Cloud Infrastructure.

Using direct URL:

- a. In your browser, enter https://cloudmarketplace.oracle.com/marketplace/en_US/homePage.jspx?tag=WebCenter+Content.

The Marketplace listings for WebCenter Content are displayed.

- b. Click the title of the listing you want to use. The landing page of that listing is displayed.
- c. Click **Get App**.
- d. Select your Oracle Cloud Infrastructure region and click **Sign In**.
- e. [Sign in to the Oracle Cloud Infrastructure Console](#).

By browsing:

- a. [Sign in to the Oracle Cloud Infrastructure Console](#).
 - b. Open the navigation menu and click **Marketplace**. Under **Marketplace**, click **All Applications**.
 - c. In the Marketplace search field, enter WebCenter Content. The Marketplace listings for WebCenter Content are displayed.
 - d. Click the title of the listing you want to use and review the information on the **Overview** page.
2. Accept the terms and restrictions, and then click **Launch Stack**. The Create Stack wizard is displayed.
 3. Provide information about the stack for the instance.
 - a. Stack information:

- Enter name and description.
 - **Create in Compartment:** Select the compartment.
 - **Terraform version:** Specify the Terraform version and click **Next**.
- b. Configure variables:

Stack Configuration

- **Resource Name Prefix:** Enter a prefix (for example, WCC). The name of all compute and network resources will begin with this prefix. It must begin with a letter and it can contain only letters or numbers.
- **SSH Public key:** Provide the SSH public key (created in [Generate SSH key pair](#)).
- **Enable Object Storage as default storage:** Select this check box if you need object storage as the default storage instead of file system for storing documents. If selected, you need to complete the fields in the Object Storage section.

Virtual Cloud Network

- **Network Compartment:** Select [the compartment you created earlier](#).
- **Network:** Select [the VCN you created earlier](#).

Object Storage

This section is optional. Complete this section only if you selected the **Enable Object Storage as default storage** check box in the Stack Configuration section.

- **Object Storage Compartment:** Select the compartment where the bucket was created.
- **Bucket Name:** Specify the bucket name which you created earlier.
- **User OCID:** This will be pre-populated with the current user's OCID. If you are using a different user for creating the API key, specify the user OCID of that user.
- **Public Key Fingerprint:** Specify the fingerprint from the configuration file (that you copied when you created the user API key as part of the prerequisites).
- **OCI User Private Key Secret Compartment:** Choose the compartment that holds the secret for the user API private key.
- **Secret for OCI User Private Key:** Select the secret for the user API private key.

- c. Database Configuration:

- **Database Strategy:** Select the type of database to use for provisioning. The supported databases are: Database System and Autonomous Transaction Processing Database.

If you selected **Autonomous Transaction Processing Database** as the Database Strategy, then complete the following that are displayed:

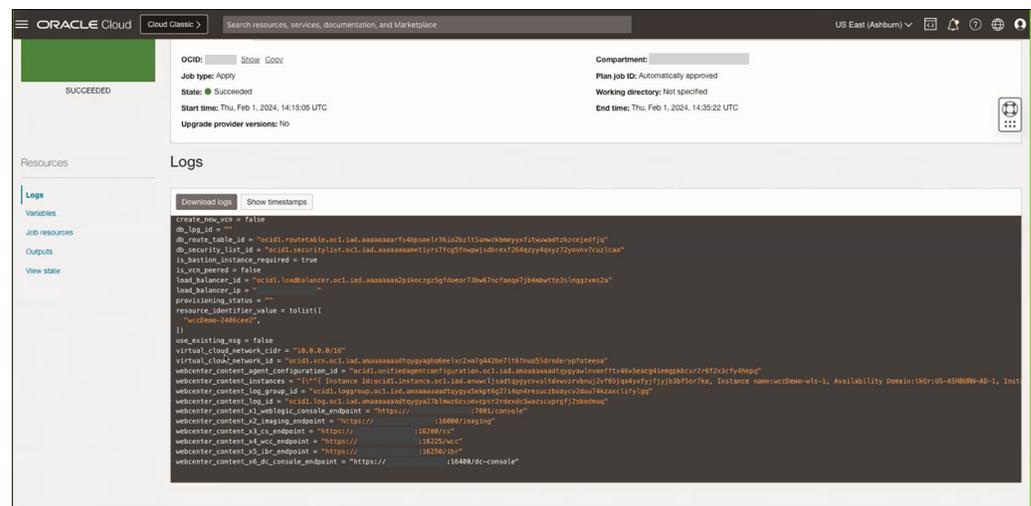
- Select the value for **Autonomous Database compartment**.
- Select the value for **Autonomous Database**.
- **Autonomous Database Admin Password Secret Compartment:** Choose the compartment that holds the secret for the Autonomous Database Admin Password.
- **Secret for Autonomous Database Admin Password:** Select the secret for Autonomous Database Admin Password.

If you selected **Database System** as the Database Strategy, then complete the following that are displayed:

- Select the value for **DB System compartment**.
 - Select the value for **DB System OCID**.
 - **PDB name**: Provide the PDB name of the DB system.
 - Select the value for **DB System Network Compartment**.
 - Select the value for **DB System VCN OCID**.
 - **DB System PDB User**: Leave the value 'sys' as is. Do not change this user name.
 - **DB System Password Secret Compartment**: Choose the compartment that holds the secret for the DB system password.
 - **Secret for DB System Password**: Select the secret for DB system password. When defining the secret key, you must have specified a user friendly name for each secret. Use the same name here so that it is easy.
 - **DB System SSH Private key Secret Compartment**: Choose the compartment that holds the secret for the DB system SSH private key.
 - **Secret for DB System SSH Private key**: Select the secret for DB System SSH private key.
- d. Bastion Instance:
- **Bastion Host Subnet CIDR**: Provide the value for Bastion host subnet CIDR. For example, 10.0.2.0/24.
 - **Bastion Host Shape**: Select the appropriate Bastion host shape (keep the default value).
- e. WebCenter Content Compute Instance:
- **Compute Shape**: Select the appropriate compute shape.
 - **OCPU count**: Select the OCPU count. The default value is 2.
 - **WebCenter Content Subnet CIDR**: Provide the value for WebCenter Content subnet CIDR. For example, 10.0.3.0/24.
 - **Node Count**: Specify the node count. The default value is 2.
- f. File System:
- **File System Compartment**: Choose the compartment where the WebCenter Content stack will be created.
 - **File System Availability Domain**: Select the Availability Domain.
 - **Mount Target Subnet CIDR**: Provide the value for Mount Subnet CIDR. For example, 10.0.5.0/24.
- g. Load Balancer:
- Provide the value for **Load Balancer Subnet CIDR**. For example, 10.0.4.0/24.
 - Provide the value for **Minimum Bandwidth for Flexible Load Balancer**.
 - Provide the value for **Maximum Bandwidth for Flexible Load Balancer**.
- h. Identity Cloud Service Integration:
- **Identity Domain URL**: Provide the value for IDCS domain URL.
 - **Identity Client ID**: Provide the value for IDCS Client ID.
 - **Identity Client Secret Compartment**: Choose the compartment that holds the secret for the IDCS client secret.

- **Secret for the Identity Client Secret:** Select the secret for the IDCS client secret.
- i. **WebCenter Content WebLogic Domain Configuration:**
 - **WebCenter Content Admin User Name:** Leave the value 'weblogic' as is.
 - **WebCenter Content Admin Secret Compartment:** Choose the compartment that holds the secret for the WebCenter Content Server administrator password.
 - **Secret for WebCenter Content Admin Password:** Select the secret for WebCenter Content administrator password.
 - **WebCenter Content Schema Password Secret Compartment:** Choose the compartment that holds the secret for the WebCenter Content schema password.
 - **Secret for the WebCenter Content Schema Password:** Select the secret for the WebCenter Content schema password.

Click **Next**. Review all the configuration variables and then select the **Run apply** check box under **Run apply on the created stack** section. Click **Create**.



If everything goes as expected, then navigate to the WebCenter Content stack and click the **Application Information** tab. Under the Output section, you'll see the end points for the services.

- webcenter_content_x1_weblogic_console_endpoint = "https://<host-IP>:7001/console"
- webcenter_content_x2_imaging_endpoint = "https://<host-IP>:16000/imaging"
- webcenter_content_x3_cs_endpoint = "https://<host-IP>:16200/cs"
- webcenter_content_x4_wcc_endpoint = "https://<host-IP>:16225/wcc"
- webcenter_content_x5_ibr_endpoint = "https://<host-IP>:16250/ibr"
- webcenter_content_x6_dc_console_endpoint = "https://<host-IP>:16400/dc-console"

After provisioning the stack, to create a connection from Imaging to WebCenter Content:

- See [Creating a Content Server Connection](#).

-  **Note:**
You should not use the public IP of load balancer when making the RIDC connection. To get the private IP of WebCenter Content Load Balancer for RIDC connection, log in to OCI console and navigate to the load balancer details page for WebCenter Content load balancer. Click **Backend** sets. From the list of backend sets, click the backend set having a name like **%-intradocsvr-bset**. Hover the mouse over the green tick (next to **OK**) to get the private IP of the load balancer.

 **Note:**

If you see a stale web location when opening content in the Content Server application (when content is created via Imaging application), then do the following to resolve this issue:

- Update the following file in all the WebCenter Content node VMs when you create an application in the Imaging application: `/u01/data/domains/wcc_domain/ucm/cs/data/ipmsys/apps/app<app-no>.hda`
- In the `app<app-no>.hda` file, update the value for `ViewerUrlFormat` with correct host name and port of Imaging application: `ViewerUrlFormat=https://<hostname>:<port>/imaging/faces/Pages/UrlTools.jspx?ToolName=AWVWR&DocumentId=%s`
- After making this change, you need to bounce all the WebCenter Content servers from the Weblogic console.

To navigate to the WebCenter Content stack:

- In the side menu, select **Developer Services, Resource Manager**, and then **Stacks**.
- Select your compartment and click the name of the WebCenter Content stack you created.

If something goes wrong or if for any reason you want to do a clean-up of all the resources that were provisioned as part of the WebCenter Content deployment, use **Destroy Job** to do the clean-up.

4

Configure FA Adapter Integration with WebCenter Content

Learn to install and configure FA integration (using AdapterFA component) with WebCenter Content on marketplace.

1. Install WebCenter Content using Marketplace image and stack if not installed yet.
2. Log in to wls-1 WebCenter Content VM and run the following commands to configure it for FA integration.

```
sudo su - oracle
cd /u01/scripts/sh
```

For non-IDCS SSO-based environment

```
sh configure_wcc_fa_adapter.sh --fa_domain <fa-domain-host> --ucm_domain
<ucm domain host>
```

For example:

```
sh configure_wcc_fa_adapter.sh --fa_domain fa-demo.fa.ocs.oc-test.com --
ucm_domain wccdemo.cec.ocp.oc-test.com
```

For IDCS SSO-based environment

```
sh configure_wcc_fa_adapter.sh --fa_domain <fa-domain-host> --ucm_domain
<ucm domain host> --idcs_user <idcs user with wcc administrator role>
```

For example:

```
sh configure_wcc_fa_adapter.sh --fa_domain fa-demo.fa.ocs.oc-test.com --
ucm_domain wccdemo.cec.ocp.oc-test.com --idcs_user user@oracle.com
```

3. Log in to Webcenter Content as an administrator.
4. Navigate to **Administration** and then to **Configuration for wcc******.
5. On the Configuration Information page, make a note of the value for the search engine under the System Configuration section.
6. Under **Administration**, click **Oracle Advanced Security Configurations**.
7. On the Oracle Advanced Security Configurations page, complete the following updates: If WebCenter Content is set to use `DATABASE.METADATA` as the search engine:
 - a. Select the **Core QueryText Security Config** check box.
 - b. Custom table names: **AFOBJECTS**
 - c. Custom field names: Leave this field blank.

d. Click **Update**.

If WebCenter Content is set to use `DATABASE.FULLTEXT` or `OracleTextSearch` as the search engine:

- a. Select the **Core QueryText Security Config** check box.
- b. Custom table names: **AFOBJECTS**
- c. Custom field names: **dreleasestate**
- d. Click **Update**.

If custom metadata is used with `DATABASE.METADATA`:

- a. Select the **Core QueryText Security Config** check box.
- b. Custom table names: Leave this field blank.
- c. Custom field names: <xCustomMetadataField1; xCustomMetadataField2; xCustomMetadataField3;...>
- d. Click **Update**.

If custom metadata is used with `DATABASE.FULLTEXT` or `OracleTextSearch`:

- a. Select the **Core QueryText Security Config** check box.
- b. Custom table names: Leave this field blank.
- c. Custom field names: <xCustomMetadataField1; xCustomMetadataField2; xCustomMetadataField3;...>
- d. Click **Update**.

8. Log in to Enterprise Manager as administrator.
9. Navigate to **UCM_Server1, Deployments, Oracle UCM Webservices, Modules and Components, Webservices, AfGrantService**, and then to **AfGrantAccessPort**.
10. Click **Attach/Detach policies**.
11. Click **Directly Attached Policies** and then click **Attach/Detach**.
12. In the Available Policies section, search for `oracle/wss_http_token_service_policy`
13. Click **Attach**, click **Validate**, and then click **Ok**.
14. Restart all WebCenter Content servers.

5

Configure SAML2 IDCS Single Sign-On in WebCenter Content

Learn to configure SAML2 IDCS Single Sign-On in WebCenter Content.

Prerequisites

Complete the following before running the configuration script.

Create a WebCenter Content Stack

A WebCenter Content stack should have been created from OCI Marketplace on which SAML2 IDCS SSO configuration needs to be configured.

Create an OAuth Client for IDCS

Follow the below instructions based on whether OCI Tenancy IAM is with Identity Domains or not.

- For OCI accounts where IAM is with Identity Domains (tenancy with IAM domains), complete the following:
 1. Log in to OCI console.
 2. Navigate to **Identity** and then **Domains**.
 3. Select the domain which needs to be used for SSO log-in.
 4. Go to **Integrated Applications** and click **Add application**.
 5. Choose **Confidential Application** and launch the workflow.
 6. On the Add Application Details page, fill the **Name** and **Description** fields, and then click **Next**.
 7. On the Configure OAuth page, select the **Configure this application as a client now** option under Client configuration section.
 8. In the Authorization section, select the **Client credentials** check box for the **Allowed Grant Types** field.
 9. Scroll down and select the **Add app roles** check box. In the App roles section, add the **Identity Domain Administrator** role.
 10. Click **Next**. Leave the default settings for the next page as is and click **Finish**.
 11. Make a note of the client ID and client secret. These values will be needed when you run the script.
 12. Activate the application.
- For OCI accounts where IDCS is not yet migrated to IAM Domains (tenancy without IAM domains), complete the following:
 1. Log in to the IDCS administration console of the federated IDCS.
For example, <https://idcs-abcde.identity.oraclecloud.com/ui/v1/adminconsole>.
 2. Navigate to **Applications**. Click **+** to add an application. Choose **Confidential Application** in the wizard:

- a. Add a name and a description on the App details page.
- b. Click **Next**. Select the **Configure this application as a client now** option.
- c. In the Authorization section, select the **Client credentials** check box for the **Allowed Grant Types** field.
- d. In the Grant the client access to Identity Cloud Service Admin APIs section, click **Add** to add the application roles. You need to add the **Identity Domain Administrator** role.
- e. Click **Next**. Leave the default settings for the next pages as is and click **Finish**.
- f. Make a note of the client ID and client secret. These values will be needed when you run the script.
- g. Activate the application.

Configuration in WebCenter Content Stack

Run the Configuration Script

A configuration helper script will be available in WebCenter Content stack VM. It can be executed from Admin compute VM or VM-1 (*-wls-1).

The script expects the following inputs.

Argument	Description
idcs_tenant	IDCS tenant name For example, if IDCS URL is <code>idcs-abcde.identity.example.com</code> , then IDCS tenant name would be <code>idcs-abcde</code> .
idcs_domain	IDCS domain For example, if IDCS URL is <code>idcs-abcde.identity.example.com</code> , then IDCS domain would be <code>identity.example.com</code> .
idcs_client	Client ID of the OAuth client created in prerequisites
idcs_client_secret	Client secret of the OAuth client created in prerequisites
service_host	WebCenter Content stack service host with DNS record mapped to load balancer IP. For example, <code>wccstack1.xyz.com</code> If service host is not available, WebCenter Content stack load-balancer IP can be provided here for testing.
idcs_user_name	IDCS user who is configured as WebCenter product administrator user

Complete the following steps to execute the script:

```
ssh -o ProxyCommand="ssh -W %h:%p -i <key> opc@<bastion-ip>" -i <key> opc@<vm-ip>
```

```
sudo su - oracle
cd /u01/scripts/sh
```

```
nohup sh configure_sso.sh --idcs_tenant <idcs-tenant> --idcs_domain
identity.oraclecloud.com --idcs_client <idcs_client> --idcs_client_secret
<idcs_client> --idcs_username <idcs_username> --service_host <service_host> &
```

The script execution progress can be monitored from `/u01/logs/provisioning.log`. Once the execution completes without any error, the configuration is completed in WebCenter Content stack environment.

This script covers the steps mentioned in [Configuring SAML 2.0 \(IDCS\) Single Sign-On](#).

 **Note:**

If the configuration was done with load-balancer IP, then the above script needs to be executed again with the service host once the DNS mapping to load-balancer IP is created.

Set Custom Logout URL for WebCenter Content ADF Server MBean

1. Log in to Enterprise Manager as an administrator.
2. Click **Weblogic Domain** and then **System Mbean Browser**.
3. Expand **Application Defined MBeans** and navigate to **oracle.adf.share.config, Server: WCCADF_Server1, Application: Oracle WebCenter Content - Web UI, ADFConfig, ADFConfig**, and then **WCCAdfConfiguration**.
4. Click the **WCCAdfConfiguration** Mbean and set **CustomLogoutUrl** as `https://<idcs_tenant>.<idcs_domain>/sso/v1/user/logout`. For example, <https://idcs-xxxxxxxxxxxxxxxxx.identity.oraclecloud.com/sso/v1/user/logout>. Click **Apply** (on top right).
5. Go back to the ADFConfig MBean page (by navigating to **Application Defined MBeans, oracle.adf.share.config, Server: WCCADF_server1, Application: Oracle WebCenter Content, Web UI**, and **ADFConfig**).
6. On the **Operations** tab, click **Save** and then click **Invoke**.
7. Restart all the WebCenter Content ADF managed servers after completing the above steps.

Configuration in your IDCS Tenant

Once the SAML configuration is completed on WebCenter Content, SAML applications will be created under Integrated Applications in the IDCS domain. The WebCenter Content role mapping groups (as described in the table below) are also created.

WebCenter Content Groups	Description
admin	The admin role is assigned to the system administrator. By default, this role has Admin permission to all security groups and all accounts, and has rights to all the administration tools.
contributor	The contributor role has Read and Write permissions to the Public security group, which enables users to search for, view, check in, and check out content.
guest	The guest role has Read permission to the Public security group, which enables users to search for and view content.
sysmanager	The sysmanager role has privileges to access the Admin Server links from the Administration menu in the user interface.

The Admin user is granted membership to the admin group and can be used to access the service.

The SAML applications will be prefixed with the stack service name. For example, wcc12_ucm_saml, wcc12_capture_saml, wcc12_wcc_saml, and wcc12_imaging_saml.

Add Users to Groups

To add a new user other than the administrator, you would need to add the user to the IDCS WebCenter Content groups based on the permissions required for their usage.

Verification

After the configuration of SAML, verify the WebCenter Content application URLs and validate that the IDCS SSO log-in is working.

Content Server: `https://<service_host|lb_ip>:16200/cs`

Web UI: `https://<service_host|lb_ip>:16225/wcc`

Capture: `https://<service_host|lb_ip>:16400/dc-console`

Imaging: `https://<service_host|lb_ip>:16000/imaging`

6

Troubleshoot

This chapter describes common problems that you might encounter and also provides information that can be helpful with the troubleshooting process.

Issue	Description
Provisioning failed	<p>If you encountered a failure when trying to provision WebCenter Content, do the following to see the logs which might help in troubleshooting:</p> <ol style="list-style-type: none"><li data-bbox="846 657 1127 682">1. Log in to bastion host.<li data-bbox="846 703 1430 814">2. From bastion host perform ssh to wls-1 VM. For example: <code>ssh -I <private key> opc@<IP Address of wls-1 VM></code><li data-bbox="846 835 1110 861">3. <code>sudo su - oracle</code><li data-bbox="846 882 1235 907">4. <code>cd /u01/data/domains/logs</code><li data-bbox="846 928 1154 953">5. <code>vi provisioning.log</code>
Stale web location when opening content in the Content Server application	<p>If you see a stale web location when opening content in the Content Server application (when content is created via Imaging application), then do the following to resolve this issue:</p> <ul style="list-style-type: none"><li data-bbox="846 1100 1468 1247">• Update the following file in all the WebCenter Content node VMs when you create an application in the Imaging application: <code>/u01/data/domains/wcc_domain/ucm/cs/data/ipmsys/apps/app<app-no>.hda</code><li data-bbox="846 1262 1435 1465">• In the <code>app<app-no>.hda</code> file, update the value for <code>ViewerUrlFormat</code> with the correct host name and port of Imaging application: <code>ViewerUrlFormat=https://<hostname>:<port>/imaging/faces/Pages/UrlTools.jspx?ToolName=AWVWR&DocumentId=%s</code><li data-bbox="846 1478 1451 1562">• After making this change, you need to bounce all the WebCenter Content servers from the Weblogic console.